Infoblox
NEXT LEVEL NETWORKING

WHITE PAPER

# Reliable DNS and DHCP for Microsoft Active Directory

## Protecting and Extending Active Directory Infrastructure with Infoblox Appliances

Microsoft Active Directory (AD) is the distributed directory service and the information hub of Microsoft Windows Server 2016 and 2012R2 Server operating systems. AD provides critical services such as Windows login, and also supports a wide range of directory services that support Microsoft applications. The most critical network service that Active Directory relies on is The Domain Name System (DNS). DNS services are provided as part of Microsoft Active Directory and are often deployed on Microsoft domain controllers (DCs) along with other services, such as print and file sharing. Loss of DNS service results in loss of Microsoft application services (e.g. Windows Domain Login, Exchange, file and print sharing) and also impacts all non-Microsoft (e.g. Unix) applications that use DNS services. As a result, the security and availability of these services are especially critical.

This paper explains how Infoblox core network services appliances can be used to enhance the security, availability, performance, and manageability of DNS services by offloading these services from domain controllers to ensure nonstop availability, improved security, and easier management.

## DNS and DHCP Services Are Central to Microsoft and Non-Microsoft Applications

The Domain Name System is the backbone of Active Directory and the principal name resolution mechanism of Windows servers and clients. DNS is used to map host names (e.g. yahoo.com or mail.mycompany.com) to IP addresses (e.g., 66.94.234.13 or 10.1.1.100) and vice-versa, and can also be used to store and retrieve other information about a host, such as which services it provides. Windows Server 2016 and 2012R2 Server domain controllers use DNS to dynamically register information about their configuration and about the Active Directory system. Other Windows systems that are part of the domain query DNS to locate Active-Directory-related information. If DNS is not functioning correctly domain-wide outages will occur, the DC replication will cease, and replication updates will sit idly in a queue until DNS is restored. Users also will be unable to log on to the domain or to join the domain from a workstation or server in the absence of DNS. Non-Microsoft applications are similarly affected by the loss of DNS services, because everything from web browsing to e-mail and enterprise applications relies on DNS for mapping host names to IP addresses.

Dynamic Host Configuration Protocol (DHCP) is a standard protocol that clients rely on to automatically obtain IP addresses and, thereby, participate in network communications. In addition to IP addresses, a DHCP server can provide a client with its subnet mask, default gateway, DNS server addresses, and other options that enable a client system to establish IP communications. As with DNS, if DHCP services are unavailable, all IP based devices—including desktops, laptops, servers, and IP phones—will be unable to acquire an address and gain network access.

## Infoblox Appliances Deliver Nonstop DNS and DHCP Services for Microsoft AD Environments

Infoblox's core network services appliances are purpose-built to provide nonstop availability of standards-based, Microsoft-compatible DNS and DHCP services. The appliances are based on the security-hardened Infoblox NIOS™ software, which allows no root access and presents no unnecessary open ports, and the DNS protocol implementation uses the latest BIND version and is resilient against cache poisoning and other attacks. Infoblox appliances are easy to install and manage and can load updated software with a single click. They also provide extensive built-in support for high-availability, delegated management, logging, and auditing. Collections of Infoblox appliances can be easily linked into robust Infoblox Grids that extend these capabilities, including real-time data updates, across a distributed enterprise. These features, combined with transparent integration with Microsoft Active Directory, make Infoblox appliances an excellent choice for offloading DNS and DHCP services from domain controllers.

The following sections review the theory, practice, and benefits of implementing DNS and DHCP services using Infoblox appliances in an AD environment.

## Why Not Just Use Microsoft DNS and DHCP?

In an AD environment, DCs are often distributed throughout an enterprise to ensure fast login and directory services, and to provide support for local print and file sharing services. DNS and DHCP services are bundled with domain controller software because they are central to how Microsoft clients and applications locate networked resources. It therefore seems natural to simply use the domain controller's DNS and DHCP services, in as much as they are already available wherever a DC is deployed. There are, however, some challenges associated with using the domain controller's DNS and DHCP services:

### Management Complexity and No IP Address Management

The DNS and DHCP services available with AD are managed separately and do not share data. The extra manual steps required to ensure that DNS changes are reflected in DHCP and vice-versa take time and create opportunities for data entry errors and associated service disruptions. When managing DNS and DHCP, it is also important to manage IP addresses. AD does not maintain a complete view of the IP address space and managing DNS, DHCP, and IP address data cannot be done in the same management tool.

### No Support for Anycast DNS

Anycast DNS allows multiple DNS servers to share the same Anycast IP address and uses the routers in the network to direct DNS queries to the "closest" DNS server. Many organizations are now implementing Anycast DNS to add extra resiliency to the DNS infrastructure. Microsoft DNS does not have the ability to implement Anycast DNS.

### Limited Administrative Flexibility

The Windows Server 2016 operating system supports only a single administrator, so supporting delegated management and role-based administration requires an upgrade to Windows Server 2016. Even with Windows Server 2016, there is no ability to delegate the management of specific resources (e.g. zones, sub-zones, networks, and shared networks).

### Limited Logging and Reporting for Planning and Troubleshooting Sarbanes-Oxley Compliance

There is no logging of administrative changes in the Microsoft DNS and DHCP implementations, and limited ability to delegate management. All administrators have access to view and can edit the same domain space with no integrated audit capability. This makes it extremely difficult to generate the reports necessary to ensure compliance with regulations such as Sarbanes-Oxley.

### Management Platform Limitations

Management of DNS and DHCP services requires the Microsoft management console, which prevents management from UNIX, Linux, Mac, or other non-Microsoft platforms. This can be a significant limitation especially in emergency situations in which there's no access to the Microsoft management application.

### Limited Support for Integration with Customer Applications

The Microsoft AD environment does not support an API that enables users to easily build their own applications that can view and edit DNS and DHCP data.

## Use of Non-Microsoft DNS and DHCP in an AD Environment Is "Legal" and Supported

Use of Non-Microsoft DNS and DHCP services in an AD implementation is a supported configuration. Microsoft Knowledgebase article #237675, "Setting up the Domain Name System for Active Directory," under 'DNS server requirements' clearly states the following:

Microsoft DNS is not required. The DNS server that you use...must support the SRV RR and the dynamic update protocol. Infoblox appliances are standards-based and support SRV resource records and DNS updates, and thus provide transparent and fully compliant DNS services for a Microsoft AD implementation. Infoblox is a Microsoft Gold Certified Partner and we can fully integrate with Microsoft AD, Microsoft DNS and Microsoft DHCP.

## Infoblox Appliances Provide Simple, Secure, Reliable DNS and DHCP Services

Infoblox appliances are purpose-built for delivering reliable, secure, high-performance DNS and DHCP services using the following core technologies:

### High-reliability Hardware Platforms

The Infoblox family of network service appliances are true network devices designed for years of reliable, "lights-out" service. They contain no keyboard, mouse, or serial ports and are robust against physical attack.

### Hardened, Purpose-built OS and Software

The Infoblox NIOS operating system is hardened against attacks and has withstood extensive independent testing by security-sensitive agencies. It includes the zero-administration, bloxSDB™ database that combines DNS and DHCP data and simplifies the development of integrated applications. The Infoblox NIOS software also includes built-in support for high availability and supports a powerful, object-oriented API to enable integration with customer applications.

### Standards-based DNS

The DNSone® package includes ISC BIND, the de-facto industry standard DNS server, which interfaces directly with the bloxSDB database, delivering integrated and high-performance services. The GUI automates many manual tasks and automatically generates DNS records as needed. For example, when the DHCP server issues a lease it updates the database without requiring a DDNS update from the host. The same is true for DNS, in which reverse-mapped zones are generated automatically when forward-mapping data is entered. In addition, the DNSone package provides direct support for easy and transparent integration into Microsoft AD environments.

### One-click DNSSEC

Infoblox has a “one-click DNSSEC” solution that automates the processes of signing and maintaining a signed zone. This eliminates dozens of error-prone, manual operations and eliminates the need to write and maintain custom scripts. Key generation is performed automatically using DNSSEC properties specified at the Grid or zone level; resource record signatures are maintained; and zone signing key rollover occurs seamlessly and automatically according to best practices recommended by the National Institute of Standards and Technology (NIST-800-81) and RFC 4641 standards.

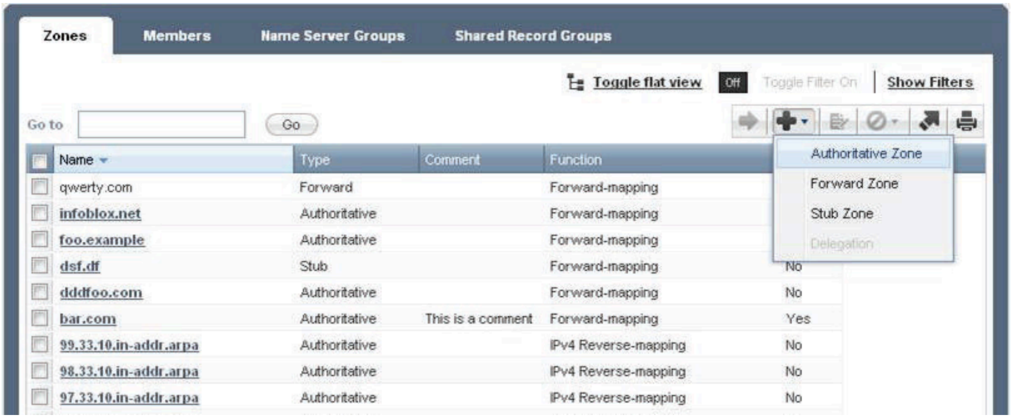
### Distributed Virtual Services Option

Adding the optional Grid module to a collection of appliances running the NS1® package turns the collection into a robust Infoblox Grid. Appliances in the Grid, and the data they serve, are managed as a single entity, eliminating the need to touch individual boxes even for software updates. The Grid also supports real-time data updates, eliminating the latencies inherent in AD replication and BIND zone transfers. It provides self-healing operation that makes the services resilient against almost any combination of device and/or WAN link failures. Infoblox Grids also feature intelligent auto-provisioning for easy pre-staging and auto-recovery of devices. If an appliance in a Grid suffers a hardware failure, recovery is fast and simple and can be accomplished by low-skill personnel, who simply swaps in a replacement unit and gives it the same IP address, membership name, and membership “secret” as the failed unit. The Grid Master then automatically restores all configuration information and data automatically, eliminating the need to send skilled personnel on site. The advanced capabilities and benefits of using Infoblox appliances for DNS and DHCP services are summarized in this table

| Need | Infoblox Solution | Advantages |
|---|---|---|
| Security | Security-hardened Infoblox NIOS software, latest version of ISC BIND and DHCP | No extra open ports, no root access, resilient against attacks (e.g. cache poisoning) |
| Software Updates | Fast, easy, one-button updates of OS and application software | Few updates required, limited time and service impact |
| High Availability | Built-in HA port, VRRP-based network failover, ISC DHCP failover, automatic database sync | Devices share a common address pool and provide true DHCP failover |
| Management Integration | Integrated console for DNS and DHCP, with extensive integration | Auto-generation of records, elimination of manual steps & errors |
| Management Automation | Infoblox Grids™ that provide data-centric view and centralized management | Eliminates box-by-box touches for updating data or software |
| Management Flexibility | Delegated, granular, role-based admin defined to individual zones, sub zones, networks, etc. | Provides administrators with limited access to manage local resources |
| Realtime Data Updates | DNS and DHCP changes immediately propagated across Infoblox Grid™ | Supports mobility and other applications that require up-to-date DNS and DHCP data |
| Logging and Reporting | Extensive syslog facilities and detailed administrative audit log | Supports planning, troubleshooting, and Sarbanes-Oxley compliance |
| Remote Management | Clientless, web-based GUI | Works from any location, any OS, anytime |
| Application Integration | Object-oriented API | Enables integration with legacy applications, development of custom self-service portals, custom reporting tools, and other applications |

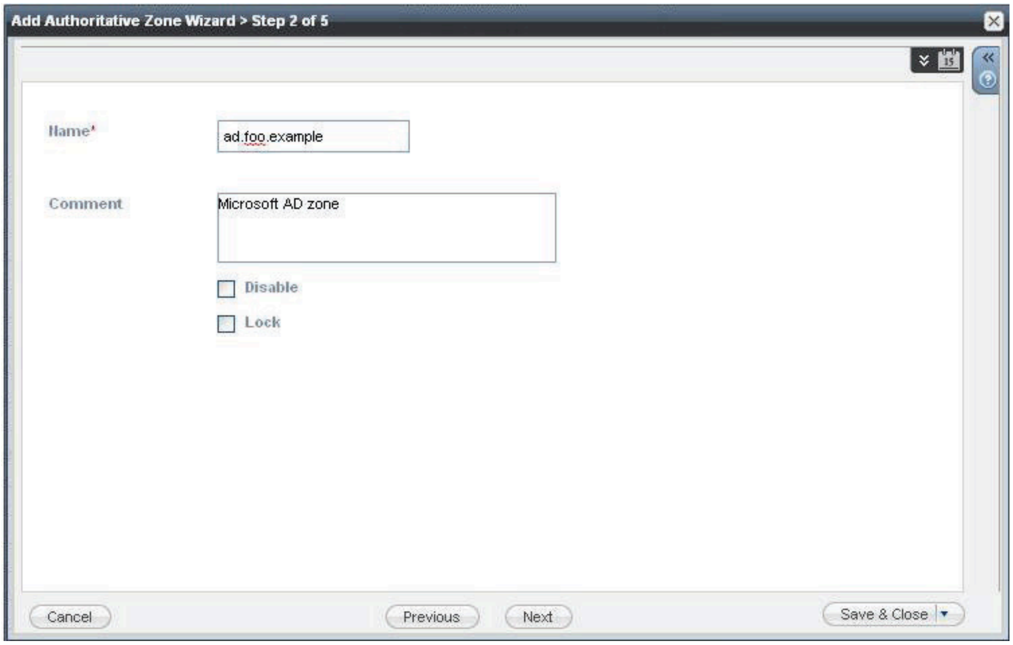
## Infoblox Appliances Integrate Easily and Transparently in AD Environments

Infoblox provides extensive support for integrating with AD, including support for both SRV RR (RFC 2052) and the dynamic update protocol (RFC 2136). Infoblox appliance integration into existing or greenfield AD deployments is simplified by native AD support, streamlined workflow, and auto-generation of AD specific zones, as shown in the screen shots below and on the following pages:



| Name | Type | Comment | Function | |
|---|---|---|---|---|
| qwerty.com | Forward | | Forward-mapping | |
| infoblox.net | Authoritative | | Forward-mapping | |
| foo.example | Authoritative | | Forward-mapping | |
| dsf.df | Stub | | Forward-mapping | No |
| dddfoo.com | Authoritative | | Forward-mapping | No |
| bar.com | Authoritative | This is a comment | Forward-mapping | Yes |
| 99.33.10.in-addr.arpa | Authoritative | | IPv4 Reverse-mapping | No |
| 98.33.10.in-addr.arpa | Authoritative | | IPv4 Reverse-mapping | No |
| 97.33.10.in-addr.arpa | Authoritative | | IPv4 Reverse-mapping | No |

Figure 1: Add new zone



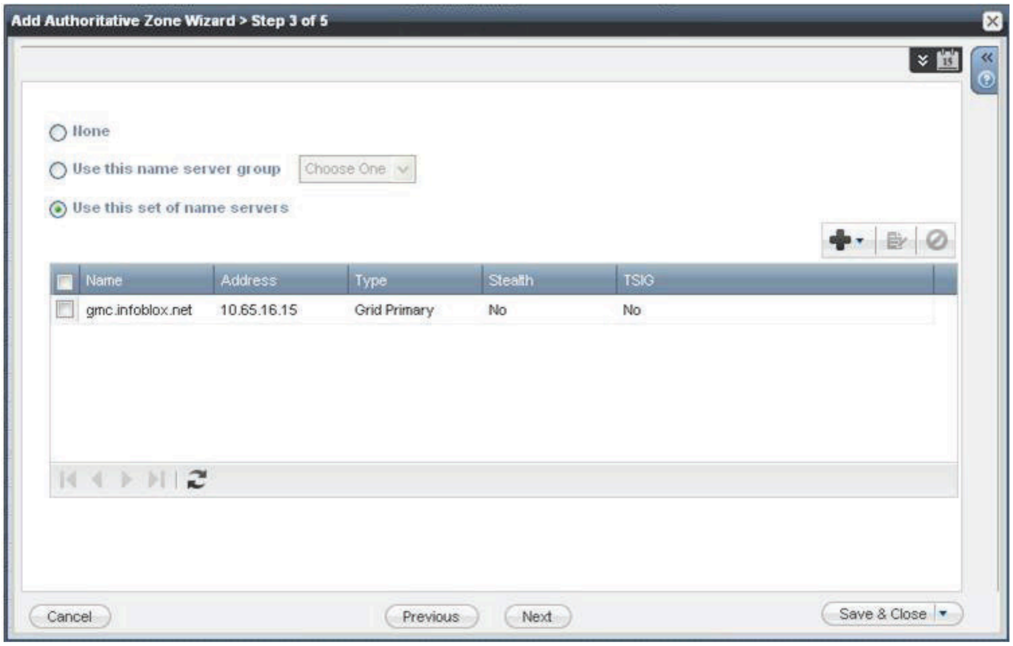
Name*: ad.foo.example

Comment: Microsoft AD zone

□ Disable

□ Lock

Figure 2: Enter zone name



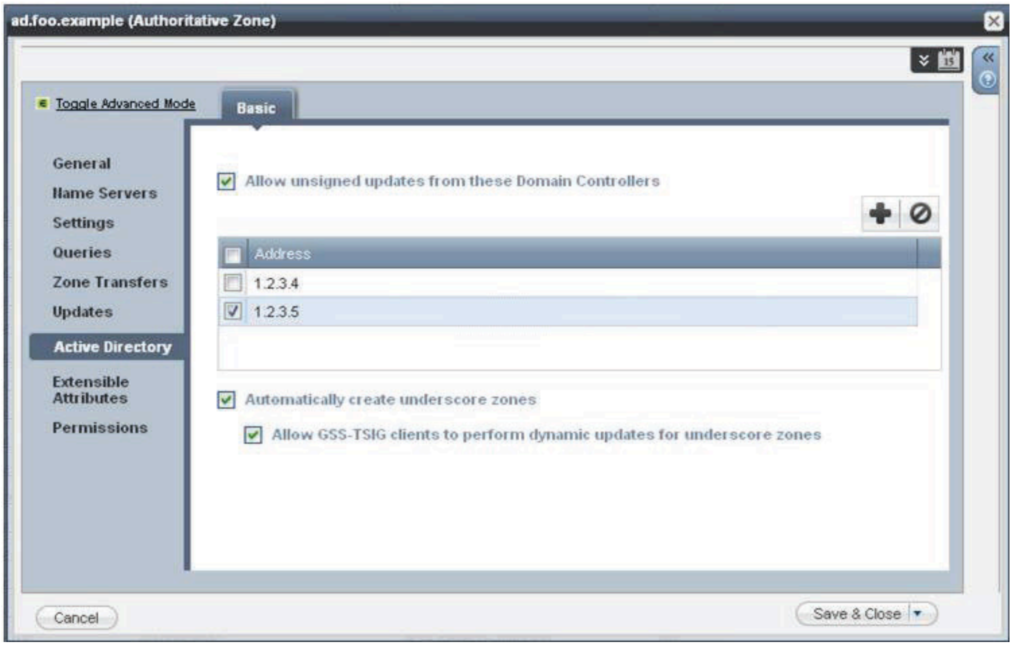
○ None

○ Use this name server group Choose One

● Use this set of name servers

| □ | Name | Address | Type | Stealth | TSIG |
|---|---|---|---|---|---|
| □ | gmc.infoblox.net | 10.65.16.15 | Grid Primary | No | No |

Figure 3: Select appliance to serve this zone name



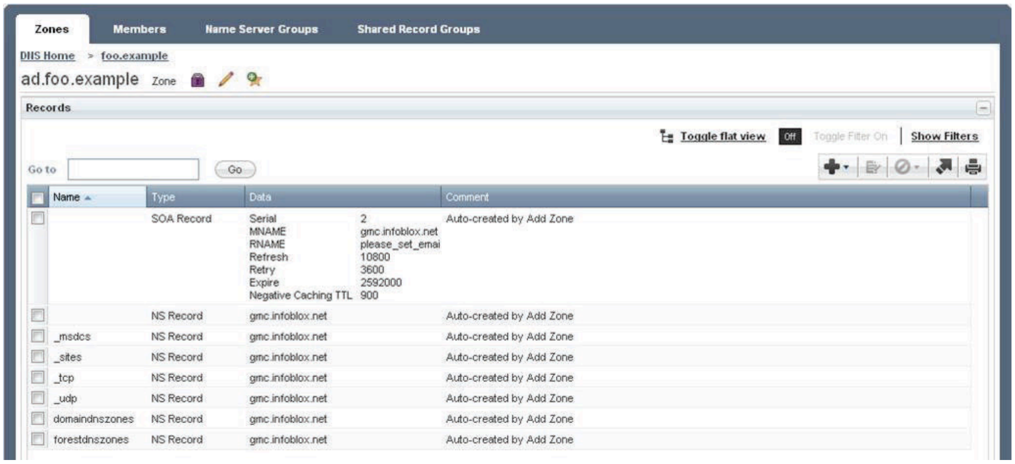
☑ Allow unsigned updates from these Domain Controllers

| □ | Address |
|---|---|
| □ | 1.2.3.4 |
| ☑ | 1.2.3.5 |

☑ Automatically create underscore zones

☑ Allow GSS-TSIG clients to perform dynamic updates for underscore zones

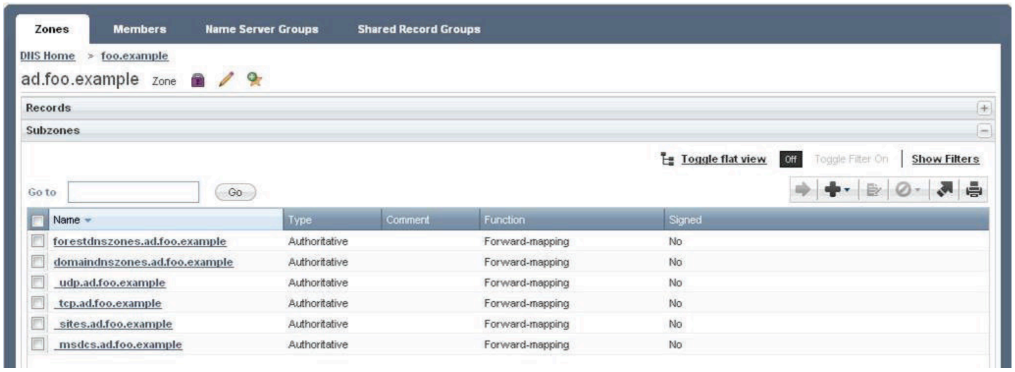
Figure 4: Enter IP addresses of Domain controllers and create underscore zones



ad.foo.example Zone

| Name | Type | Data | Comment |
|---|---|---|---|
| | SOA Record | Serial 2<br>MNAME gmc.infoblox.net<br>RNAME please_set_emai<br>Refresh 10800<br>Retry 3600<br>Expire 2592000<br>Negative Caching TTL 900 | Auto-created by Add Zone |
| | NS Record | gmc.infoblox.net | Auto-created by Add Zone |
| _msdcs | NS Record | gmc.infoblox.net | Auto-created by Add Zone |
| _sites | NS Record | gmc.infoblox.net | Auto-created by Add Zone |
| _tcp | NS Record | gmc.infoblox.net | Auto-created by Add Zone |
| _udp | NS Record | gmc.infoblox.net | Auto-created by Add Zone |
| domaindnszones | NS Record | gmc.infoblox.net | Auto-created by Add Zone |
| forestdnszones | NS Record | gmc.infoblox.net | Auto-created by Add Zone |

Figure 5: The new zone contains the automatically created Microsoft-specific DNS records



ad.foo.example Zone

| Name | Type | Comment | Function | Signed |
|---|---|---|---|---|
| forestdnszones.ad.foo.example | Authoritative | | Forward-mapping | No |
| domaindnszones.ad.foo.example | Authoritative | | Forward-mapping | No |
| _udp.ad.foo.example | Authoritative | | Forward-mapping | No |
| _tcp.ad.foo.example | Authoritative | | Forward-mapping | No |
| _sites.ad.foo.example | Authoritative | | Forward-mapping | No |
| _msdcs.ad.foo.example | Authoritative | | Forward-mapping | No |

Figure 6: Underscore zones

## Infoblox is a Microsoft Gold Certified Partner

Infoblox is a Microsoft Gold Certified Partner with an Advanced Infrastructure Solutions Competency. This competency identifies Infoblox as an experienced partner fully qualified to deploy products with the Active Directory and Identity Management solutions from Microsoft. The Infoblox DNSone appliance-based solution is fully compatible with Microsoft DNS and DHCP services and integrates seamlessly into a Microsoft environment. Similarly, the Network Services for Authentication package offers “point-and-click” integration with Microsoft Active Directory as a user repository. This allows for a reliable, secure solution for supporting wireless deployments, perimeter security, and other applications.

Microsoft®
GOLD CERTIFIED
Partner

## Improve Your Microsoft AD Deployments With Infoblox

Essentially all IP applications—web browsing, e-mail, VoIP, wireless, and many more—rely on the availability of robust DNS and DHCP services. With Active Directory's reliance on DNS as a core network service, this reliance is further increased. While DNS and DHCP services are provided "for free" on domain controllers, the limitations and challenges associated with running these services on general-purpose servers are increasingly of concern for network and application administrators. Offloading DNS and DHCP services from DCs onto Infoblox appliances is easy and improves security, reliability, and availability while simplifying and enhancing manageability and greatly reducing operating costs.

## About Infoblox

Infoblox delivers Actionable Network Intelligence to enterprises, government agencies, and service providers around the world. As the industry leader in DNS, DHCP, and IP address management (DDI), Infoblox provides control and security from the core—empowering thousands of organizations to increase efficiency and visibility, reduce risk, and improve customer experience.

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