

Security Certification

Infoblox is currently working with Computer Sciences Corporation (CSC) and is in the process of certifying the NIOS product for Common Criteria EAL2 as dictated by NIAP. In addition, we are in the process of going through a Cryptographic Algorithm Validation Program (CAVP) to ensure that all FIPS-Approved cryptographic algorithms used in NIOS solution meet the FIPS 140-1 security requirements. We are now listed on NIAP's site in the list of products in evaluation.

http://www.niap-ccevs.org/in_evaluation/

Infoblox Core Technologies

Infoblox solutions rely upon two core underlying technologies: the embedded Infoblox NIOS™ software and our patented Grid technology.

Infoblox NIOS software, running on Infoblox appliances, delivers nonstop core network services—including DNS/DNSSEC, DHCP, IPAM, HTTP, FTP, TFTP, NTP and others—that are critical to the operation of all IP-based networks. Appliance delivery of these services has become a recommended industry best practice for any size organization, because appliances are inherently more reliable, manageable, scalable, and secure than software on general-purpose servers. For large organizations, distributed Infoblox appliances can be connected into unified Grids that provide unparalleled management, control, visibility, and service resiliency.

Infoblox NIOS software is a security-hardened, real-time operating system that includes a built-in, zero-administration database, extensive support for high-availability operation, and comprehensive capabilities that automate appliance deployment and maintenance and simplify data management. Infoblox NIOS supports a series of modules provide a range of network services, including:

- Naming services via Domain Name System (DNS/DNSSEC);
- Addressing services via Dynamic Host Configuration Protocol (DHCP);
- Network visibility and control via IP address management (IPAM);
- Configuration services via Trivial File Transfer Protocol (TFTP) FTP and HTTP;
- Time synchronization services via Network Time Protocol (NTP);
- Dual stack IPv6/IPv4 protocol support
- Logging services via Syslog.

Infoblox NIOS software also supports several additional modules that provide unique capabilities:

- The Grid module provides patented Infoblox technology for linking distributed appliances into an Infoblox Grid: unified, centrally managed system of appliances sharing a common, real-time distributed database. The Infoblox Grid uses a secure SSL-based VPN among appliances and also uses sophisticated transaction management technology to maintain data integrity. This ensures that all appliances in the Grid have the timely and accurate data and that the Grid continues to deliver services without data loss or corruption in the face of device or WAN failures. Infoblox Grid technology also supports intelligent data replication to minimize the use of bandwidth in the Grid and to enable “right-sized” appliances to be deployed at each location.
- The Infoblox Microsoft Management for NIOS solution provides enhanced management capabilities for Microsoft DNS and DHCP services. The solution extends built-in Windows DNS and DHCP management tools with visual IPAM discovery, analysis and change management tools on the Infoblox NIOS platform while preserving investments in currently deployed Microsoft infrastructure. Infoblox Microsoft Management for NIOS does not require any agent software on client or server computers because it uses native Microsoft RPC APIs to

DATASHEET

interface to Microsoft DNS and DHCP services. This integration is so seamless administrators can use either the built-in Microsoft tools or the visual Infoblox management console and be assured their changes will be properly synchronized. The NIOS Microsoft management environment will also integrate with Microsoft System Center Operations Manager (SCOM) via a SCOM Management Pack so that Infoblox appliances can be monitored from an SCOM console.

- The integration module for Alcatel-Lucent VitalQIP® extends the benefits of Infoblox appliances and Grid technology to Alcatel-Lucent VitalQIP Remote Server software.

The Infoblox NIOS software in every Infoblox appliance includes a powerful API that enables external applications to interact with appliance services and applications. Via the API, third-party applications can import data from existing DNS and DHCP systems, read and modify the data in the Infoblox appliance bloxSDB database, perform administrative functions, and export data for archiving and reporting.

NIOS Features and Benefits

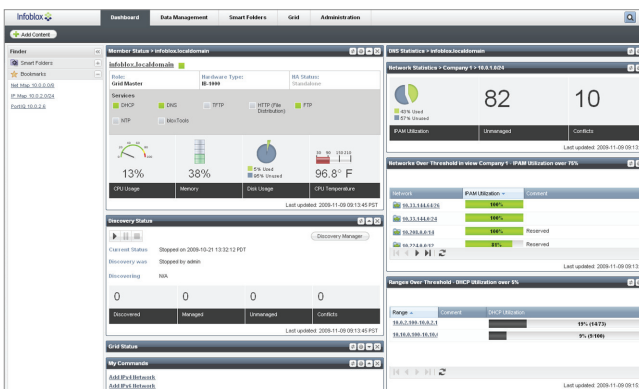
High-availability Services: High-availability (HA) services are supported by bloxHA™ technology, which uses industry-standard Virtual Router Redundancy Protocol (VRRP) for sub-5-second network failover between active and backup appliances, and bloxSYNC™ technology to ensure real-time database synchronization with no loss or duplication of data. Together, these two technologies allow critical DNS/DNSSEC, DHCP, FTP, HTTP, TFTP, and other services to always remain responsive and up to-date and eliminate common but challenging problems such as issuing duplicate IP addresses.

Integrated, Zero-admin Database: Infoblox NIOS software stores all network data—including IP addresses, host names, MAC addresses, user credentials, and other data—in the integrated bloxSDB database, which is designed specifically to support integrated network services and provides unmatched consistency between service and management views of IP network data without compromising performance.

Integrated Web GUI: The Infoblox Web GUI allows administrators to deploy and manage the entire DNS/DNSSEC, DHCP and IPAM infrastructure with just a few mouse clicks. The powerful, Web-based Infoblox GUI is the only solution that manages all aspects of the infrastructure and data—including software updates and upgrades, backup and restore, disaster recovery and all services and data management—without resorting to client

based or command-line interfaces. The Infoblox Web UI manages all aspects of the product including DNS/DNSSEC, DHCP, IPAM and Grid management, monitoring and reporting. Wizards and visual tools are available to make configuration and monitoring error-free.

Closed Loop Automation: Infoblox NIOS software provides practical operational efficiencies that lower total cost of ownership. For example, creating a DHCP range automatically creates an associated DNS record, reducing the number of tasks required of network administrators. Files can be uploaded to the Grid master and automatically distributed to all appliances serving files via FTP, TFTP and HTTP. All of these features save time and improve service delivery.



The Infoblox Grid Manager application unifies the management of all services, devices, and data.

Granular, Role-based Administration: Role-based administration is a powerful way to ensure that administrators are only given access to view and modify specific core network services attributes consistent with their organizational and functional role. For example, this means that a senior DNS administrator could have the ability to define new domains and add new appliances to a Grid, while a help desk administrator might only have the ability to view specific subnets and issue IP addresses to new devices by picking from a pre-defined list. Infoblox has created a very scalable, yet very granular role-based administration framework. The framework provides customers the ability to delegate administration down to the object level and yet maintain permissions for a large, complex administration model. Some specifics include:

- Easy workflow to manage permissions. The administrator can quickly set permissions by right-clicking on any object to bring up a list of permissions. This is much easier than having to switch to a separate administration panel. It also provides a comprehensive list of which permissions have been granted to each administration group.
- Administration is also eased through the use of roles. Roles can be mapped to an organization or job (e.g., Printer Admins, DNS Admins) and then roles can be assigned to administrative groups. This abstraction model allows a set of permissions to be defined once such that any changes to the role are inherited by all groups that are associated with it.

Security Hardened: Infoblox NIOS software is hardened and consistently withstands security scans and attacks from the most demanding government and military organizations. In the event that a new exploit is discovered, the underlying Infoblox NIOS software can be upgraded in minutes via a single, simple operation. This makes it much more difficult to penetrate than general-purpose operating systems with known vulnerabilities. Management communication is secured using Secure Sockets Layer (SSL)-encrypted VPNs for protection against management compromise.

Extensibility and Customization: The bloxTools™ environment (available on NIOS software) is a way for customers to develop, deploy and support customized, web-based applications that extend the power of the Infoblox Grid. Based on powerful and popular Web 2.0 technologies and leveraging the power of Web communities, the bloxTools environment unleashes the full power and potential of the Infoblox NIOSTM platform and the creativity of our customers and partners. bloxTools provides customers the ability to develop light-weight, custom applications (SNAPins) to meet unique workflow and other requirements, and to support integration with other enterprise applications such as asset management, CRM, ERP, etc. Other CNS products have achieved this through complex interfaces that require significant initial and ongoing Professional Services engagements to create, customize and maintain them. The open, community-based model for publishing and supporting SNAPins harnesses the collective power of Infoblox's thousands of customers worldwide.

Simplifies rollouts of new technology initiatives: NIOS software provides a solid foundation for the integration of IPv6 and Virtualization technologies into enterprise networks. Key features such as Dual Stack IPv6/IPv4, DNS64 and VMware integration allow these new technologies to seamlessly coexist with DNS, DHCP and IP Address Management for your traditional applications and network infrastructure.

Infoblox NIOS Modules and Packages

Infoblox software packages combine NIOS software modules to address different customer needs, as shown in the table below. All packages are available on all Infoblox appliance models, except where noted.

Software Packages	NIOS Software Modules							
Infoblox software packages run on Infoblox network services appliances.	DNS	DHCP	IPAM	NTP	TFTP/HTTP	Syslog NG Proxy	Grid	VitalQIP Integration
NS1	◆	◆	◆	◆	◆	◆	--	--
NS1 with Grid	◆	◆	◆	◆	◆	◆	◆	--
Network Services for VitalQIP (NSQ)*	--	--	--	◆	◆	◆	◆	◆

*Available on the Infoblox-550-A, 1050-A, 1550-A, 1552-A, and 2000 appliance models.

DNS Module

The Infoblox DNS module provides high-performance, feature-rich DNS services that use the industry-standard BIND protocol engine modified to work with the bloxSDB database. This combination delivers the benefits of a proven protocol engine with the benefits of a sophisticated data subsystem ensuring transactional integrity to eliminate the data corruption, errors, and loss exhibited by flat-file systems.

DNS Features and Benefits

Flexible Deployment: The Infoblox DNS module can be configured to support any role, including authoritative (primary), secondary, forwarding, and caching—all with high performance.

Reliable DNS Service: If DNS services are not available, the entire network is down. Therefore, this service must be available nonstop. bloxHA technology allows two appliances to be combined into an HA pair for reliable DNS service. If the active appliance fails, the passive appliance takes over and continues to provide DNS service in less than five seconds, without any loss or duplication of data. In addition, the unique combination of the DNS protocol engine and the bloxSDB database enables many changes—such as adding records to a zone—to occur without restarting services. This eliminates many of the service interruptions that occur when updating data in conventional BIND-based DNS servers.

Anycast: In order to achieve a globally distributed, highly-resilient DNS infrastructure, companies can use the Anycast feature to “advertise” a single IP address for DNS services that are served by multiple physical devices. The IP address is advertised via the OSPF routing protocol and is withdrawn from the routing table when DNS is not available. This provides global load distribution and automatically routes queries away from appliances that are out of service.

Real-time Updates: Dynamic DNS (DDNS) updates are replicated in real-time to all DNS servers in an Infoblox Grid. No other DNS server available today provides real-time replication of DDNS updates. This is essential for network environments that require accurate DNS data for security reasons or for locating devices—like printers—on the network by a simple name.

DNS Attack Detection and Mitigation: Infoblox provides the ability to detect, alert and mitigate any attacks against members that are configured as recursive DNS servers. The NIOS software will monitor two key parameters that are indicators of an attack: mis-matched DNS message IDs and mis-matched UDP ports on DNS responses. This happens when an attacker is guessing on those parameters to “spoof” a response with the poisoned data. The administrator can set a threshold for both parameters and when either is exceeded the system will send an email alert and/or SNMP trap (whichever is configured for the system). This feature will give administrators an early warning that one of their servers is under attack.

In addition, Infoblox NIOS allows attack mitigation by implementing query rate-limiting. The administrator can implement a filter on a specific IP or network to limit or stop all traffic. This will slow down or stop the attack, the success of which is based on the attacker’s ability to try as many response “guesses” as possible before the legitimate DNS server can respond.

GSS-TSIG from Clients to Infoblox DNS Servers: Dynamic DNS (DDNS) updates from Microsoft clients can be signed using GSS-TSIG with the client’s Active Directory credentials. The Infoblox DNS server accepts GSS-TSIG-signed DDNS updates and verifies the credentials against the credentials stored in Active Directory. This enables users to offload DNS from Microsoft Windows servers without compromising security. Infoblox offers the only appliance solution that supports GSS-TSIG.

GSS-TSIG from Infoblox DHCP Servers: This feature provides a tighter integration with Infoblox into Microsoft environments. If a customer wants to take advantage of the Infoblox DHCP features (failover, HA, utilization statistics, etc) but also wants to use Microsoft for DNS, this allows the Infoblox DHCP server to send a Microsoft DNS server dynamic DNS updates using GSS-TSIG security.

IPv6 Protocol and DNS Record Support: The Infoblox DNS server provides support for native IPv6 and IPv4 protocols. IPv6 record support includes both forward zone (AAAA) IPv6 DNS records and the ip6.arpa IPv6 DNS reverse zone. The DNS server with IPv6 networking support allows administrators to configure IPv6 addresses for Zone Transfers and Query Access Lists and will respond to both queries and zone transfers on the IPv6 address.

Transition technologies, such as DNS64, allow recursive name servers to synthesize an IPv6 record when none exists to enable IPv6 clients to access legacy IPv4 assets. An IPv6/IPv4 Network Translation Gateway (NAT64) is required at the IPv4/IPv6 subnet point of egress.

Single Graphical Application to Manage DNS Data and Services: The administration of DNS data can be securely delegated to administrators based on appliance, zone, and resource record type.

Zone Locking: Prevents administrative change collisions and enables multiple administrators to work simultaneously without causing unexpected or unpredictable results. When a zone is locked by an administrator, other administrators are prevented from making changes to that zone until it is unlocked. Unlike systems that can only lock on a global basis, the Infoblox zone Locking feature provides granular control and can lock at a zone level.

Hostname Templates: Administrators can enforce naming conventions by defining hostname templates that are applied on a Grid, appliance, or zone basis. Administrators can also easily run reports to find and fix legacy records that don't conform to a selected template.

Name Server Templates: This powerful feature enables administrators to propagate changes automatically to multiple zones on multiple appliances. For example, in a system with 500 zones that are served on 50 appliances, changing the IP address of a name server which is secondary for all zones—an operation that would require 25,000 changes with a conventional system—can be done with a single operation.

DNS Redirection and Filtering: NIOS DNS services support customized NXDomain redirection and policy-based DNS blacklisting. NXDomain redirection allows organizations to send users to a new location when a URL cannot be found, such as an information portal, rather than sending a non-descript “404 Error - Website not available” message. Through policy-based blacklisting, organizations can direct the DNS service to redirect or not resolve DNS requests for prohibited Internet locations.

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.

DHCP Module

The Infoblox DHCP module provides high-performance, feature-rich DHCP services that use an enhanced version of the industry standard ISC DHCP protocol engine and is tightly integrated with Infoblox bloxSDB database technology. Infoblox enhancements enable DHCP “server restarts” to occur in seconds, and avoid restarts completely for operations such as MAC filter updates, minimizing service outages. In addition, the Infoblox implementation of DHCP failover addresses known limitations in the standard approach and has been proven to provide reliable failover operation and avoid the lockups and errors frequently exhibited by standard DHCP implementations.

DHCP Features and Benefits

Reliable DHCP Service: DHCP is a core network service that is widely used to automatically provision IP addresses for PCs and servers and is increasingly essential with the rapid proliferation of new classes of networking devices, such as IP phones, RFID readers, cameras, and others. Infoblox provides multiple approaches to ensuring availability for this critical service. Infoblox bloxHA and bloxSYNC technologies enable sub 5-second failover between appliances deployed in high-availability pairs and also ensure perfect synchronization between active and failover appliances to prevent the issuance of duplicate IP addresses. Infoblox also supports the DHCP failover protocol, allowing high-availability relationships between appliances on different networks. With DHCP failover, a central DHCP server can backup multiple remote DHCP servers, saving on the cost of providing reliability.

IPv6 DHCP: IPv6 DHCP ensures that dynamically addressed network clients are able to get either IPv6 DHCP options and/or an IPv6 address from a highly available DHCP server. Infoblox provides the industry leading appliance based IPv6 DHCP server for delivery of IPv6 information to dynamic clients.

IPv6 prefix delegation: This IPv6 DHCP option allows a large enterprise organization or an Internet Service Provider (ISP) to lease large blocks of IPv6 address space to downstream points of management (such a customer or branch office DHCP server)

Historical Reporting of DHCP Lease Information: The Infoblox DHCP service stores all of the historical information about DHCP leases in the built-in bloxSDB database for future retrieval. This not only helps network administrators quickly troubleshoot problems with DHCP but also is extremely valuable for tracking security problems and meeting compliance requirements.

Split/Join Networks: As companies expand and grow, either organically or through acquisition, they need to be flexible with their DHCP networking configuration. Split/Join networks allows a company to easily adjust to the dynamic nature of today’s networks. Split networks allow an administrator to quickly, easily, and accurately subdivide a network and have the resulting sub-networks inherit the configuration of the parent network. Join/Expand networks is unique in that it allows the administrator to “grow” a series of smaller networks into a bigger network without losing any of the configuration, including fixed addresses, dynamic ranges, and DHCP other options.

Single Graphical Application to Manage DHCP Data & Services: The administration of DHCP and IP address data and DHCP servers running on Infoblox appliances can be securely delegated to administrators based on appliance and subnet. The management of DHCP and IP address data and DHCP services using the graphical Infoblox Grid Manager application is fast, easy, and powerful.

Regulating Network Access: The Infoblox Captive Portal —included in the Infoblox NIOS software - provides intelligent, policy-based control over Infoblox’s DHCP service leasing. The captive portal will regulate guest access and/or limit DHCP address allocation to authorized users via external RADIUS or Active Directory authentication. The Captive Portal holds users in quarantine until they are properly identified and only then gives them a DHCP address lease.

Advanced DHCP Options Editor: Setting DHCP options is critical for many applications including user configuration, VoIP, and wireless access point management. Configuring DHCP options can be complicated. NIOS includes a GUI-driven options editor that simplifies both standard and custom DHCP options configuration.

IPAM Module

IP address management (IPAM) lets customers manage DNS and IP address data at an enterprise-wide level, delivering unified management, monitoring, and administration while providing for appropriate levels of centralized auditing and reporting.

The Infoblox IPAM module has taken a fresh approach to IP address management (IPAM). Specifically, Infoblox has combined today’s state-of-the-art technology for data management (a distributed database) and today’s state-of-the-art vehicle for delivering network services (purpose-built appliances) to provide the first and only integrated DNS/DNSSEC, DHCP, and IPAM appliance. Unlike both new and legacy IPAM systems—that are add-ons to a data delivery infrastructure—the Infoblox approach to IPAM can be best summed up as “built-in, not built-on.”

By taking this unique approach, Infoblox provides several key features that greatly benefit customers and are not readily available in competing IPAM systems, including a rich IPAM feature set, redundancy for all components of the system, seamless software upgrades, single-click disaster recovery, real-time reporting, robust data management, and lower deployment and management costs.

IPAM Features and Benefits

Integrated IP Management Console: Within a single GUI screen, administrators can search through all of their IPv4 and IPv6 networks and can sort based on parameters such as IP address, MAC address, usage status, device type, and location—thereby simplifying many common IP management tasks. And because the IPAM functions and the real-time DNS and DHCP services operate from the same database, all information is guaranteed to stay in sync even in the most dynamic environments.

Address History Tracking: Enables administrators to better plan, manage, and meet compliance requirements through reports based on IP address status (dynamic, static, available, and reserved/disabled), hostnames, MAC address, and DHCP lease information (including lease date/time, time left on lease, time of last renewal, and forced release of IP address).

Dynamic Address Control: Allows administrators to use DHCP to deploy new devices on the network, such as a printer, without having to manually configure the device's network settings. Once the device is configured on the network, the administrator can change the address from "dynamic" to "fixed."

Next Available IP: Next available IP feature produces the next unused IP address in a given network. This feature is extremely useful in assigning fixed IP addresses to network devices such as printers, security cameras etc. Availability of this feature reduces management effort in finding an unused IP address and assigning it to a device. Further the risk of future conflict with another device is reduced since IPAM system will not give out the same IP address for a different device.

Network Discovery: Network Discovery allows administrators to search for active devices on their networks and populate the IPAM database with information discovered during the process. Depending on the method of discovery used, an administrator can:

- **Add new devices to the IPAM system** – Network discovery provides a quick mechanism to add unmanaged devices to the IPAM system without requiring administrators to manually input this information.
- **Resolve conflicts between the IPAM system and actual network state** – If the IPAM system has one view of the system but actual IP address use on the network differs from this e.g. IPAM system as a fixed IP address with a MAC address however in reality it has a different MAC address, a network discovery will show this as a conflict that administrators can correct.
- **Discover unauthorized devices on the network** – Periodically, administrators will discover devices on their network that ought not to be present there and may pose a security risk. Network discovery will show this as an unmanaged device in IPAM report.
- **Reclaim unused IP addresses** – Infoblox network discovery process reports when an IP was last discovered. This information helps in determining whether an IP address can be claimed back and reused.

Overlapping Networks: This is the capability of Infoblox IPAM system to manage two or more overlapping address ranges within the IPAM system. This is a key functionality of an IPAM system and is frequently required when managing networks created by heavy merger and acquisition activity. During M&A activity, IT departments typically do not re-architect the whole network; therefore, if the two merging entities were using same network address ranges in their networks they end up with same address used by multiple devices. The Infoblox IPAM system can handle this easily by using network views functionality. Using network views, administrators can keep two or more overlapping networks separate and still use Infoblox IPAM to manage these.

Split/Join Networks: As companies expand and grow either organically or through acquisition, they need to be flexible with their DHCP networking configuration. Split/Join networks allows a company to easily adjust to the dynamic nature of today's networks. Split networks allows an administrator to quickly, easily, and accurately subdivide a network and have the resulting sub-networks inherit the configuration of the parent network. Join/Expand networks is unique in that it allows the administrator to combine smaller networks into a bigger network without losing any of the configuration including fixed addresses, dynamic ranges, etc.

IPAM Extensible Attributes: IPAM extensible attributes take the anonymity out of IP networks by allowing organizations to fully describe their networks, zones and devices and to search and display them based on a wide range of criteria. Customers have a need to categorize and report on their networks and devices based on several criteria e.g. geographical locations, owners, department, asset class, building, campus, manufacturer, type etc. With IPAM extensible attributes, they can do exactly that. Administrators can define attributes on the fly and specify a data type (e.g. Date, E-Mail, Integer, Lookup list, String and URL) for the attribute. In addition they can also specify if this is a required field and if there are any object type restrictions e.g. if an attribute is valid only for network object types etc.

IP Address Status Viewer and Threshold Alerting: The viewer displays the number of static and dynamic IP addresses in use and the percent utilization. High and low watermark thresholds can be set for each network in an enterprise, and e-mail alerts and SNMP traps tied to these thresholds can be used to signal when ranges need to be increased or re-allocated.

Network Templates: Templates enable automation and enforcement of corporate standards when new networks are provisioned. They include all parameters of a network such as fixed addresses, dynamic IP address ranges, and DHCP options. This allows a company to "clone" the same configuration when performing large-scale provisioning tasks such as branch and retail store roll-outs.

Global Search: Allows the user to search the entire database of objects including dynamic data such as DHCP leases and DDNS hosts with results windows that allow objects to be edited or modified directly from the search results.

Recycle Bin: The Grid Manager places all administrative deletions in a recycle bin file that allows an administrator to recover the deletion in a few clicks. Recycle bin is especially useful if an admin makes an inadvertent deletion of a large amount of data.

Data Consistency Checking: The Infoblox Grid Manager software automatically performs multiple levels of data consistency and checking. With the host object, the administrator can keep DNS forward and reverse zone records in sync to avoid inconsistent zone data. IP addresses are checked dynamically as they're entered and administrators are alerted to errors and prevented from entering invalid data.

Grid Module

The Infoblox Grid module links a collection of appliances into a unified, centrally-managed, core network services platform. At the Grid's foundation is a distributed database called bloxSDB with real-time data replication across all Infoblox member appliances. This essential infrastructure allows organizations to distribute, automate and consolidate critical information and services with assured data integrity, including:

- Protocols (DNS/DNSSEC, DHCP, LDAP, TFTP, FTP, HTTP, NTP, etc.)
- Data (IP addresses, MAC addresses, meta data, user credentials, audit logs, transaction logs, time, etc.)
- Files (appliance software, device firmware and configuration files, policies, etc.)
- The Grid module provides a comprehensive array of system management, data distribution, and system availability functions.

Grid Features and Benefits

Resilient Operation: Enterprises can create resilient Grids using individual (or HA-paired) appliances deployed across a LAN or WAN environment. Infoblox Grids are resilient against the failure of individual appliances, continue to provide service in the face of a failure of a LAN or WAN link, and automatically re-synchronize all units in an Infoblox Grid when a failed device is replaced or a LAN or WAN connection is restored.

Unified Management: Devices and data in an Infoblox Grid can be managed as a single entity, without regard for where data actually resides. This virtualization of services to the Grid level rather than the individual appliance level dramatically reduces administrative overhead and greatly lowers the possibility of configuration errors. An Infoblox Grid can be completely managed remotely, from any location.

Real-time, Secure, System-wide Data Updates: Unlike conventional systems that only propagate DNS and DHCP data on a scheduled basis, the Grid module synchronizes the databases across multiple appliances in real time in response to changes as devices are added, deleted, or changed. Emerging applications such as wireless networking and VoIP can cause frequent changes to IP addressing and DNS data, and require that these changes be made available immediately across the network to ensure that applications continue to operate properly.

No Data Corruption, Errors, or Loss: Data are exchanged among appliances in an Infoblox Grid using sophisticated distributed database technology with full transactional integrity. Data remain complete and correct in the face of WAN and device failures and under high loads. This is critical in today's dynamic network environments in which incorrect data can render applications unusable, create security breaches, and violate compliance requirements.

Simplified, Role-based Management of Network Devices, Data, and Services: With configuration and data entry for a collection of appliances from a single user interface, operations are streamlined. For example, a new DNS zone can be created, mapped to several appliances (as name servers) and configured with specific zone parameters—through a single dialog box. This approach simplifies the initial configuration and the ongoing lifecycle management of a Grid of devices, rather than having to individually set up and administer each device independently.

Intelligent Auto-provisioning for Easy Pre-Staging and Auto-Recovery of Devices: Appliances can be pre-provisioned in the management system even if they are not physically present. Likewise, should an appliance in a Grid suffer a hardware failure, recovery is as fast as swapping in a replacement unit and configuring a few parameters (e.g. IP address). The necessary software, configuration information, and network are loaded and services are restarted automatically.

Disaster Recovery and Grid Master Promotion: Any appliance (or HA pair) in a Grid can be designated as a master candidate and, as such, it will continuously receive a full replication of all data and configurations in the Grid master. Should the Grid master fail or become unreachable, an administrator can “promote” any master candidate to be the Grid master, which will then contact all member appliances, synchronize any data changes, and take over administrative control of the Grid—using a single operation—in minutes.

Base Services (HTTP, FTP, TFTP, NTP, and Syslog NG Proxy)

Infoblox NIOS software provides a set of base services that are valuable in all distributed networks including HTTP, FTP, TFTP, NTP, and Syslog NG Proxy. For applications such as IP telephony, the value of these services alone can provide a fast return-on-investment for an Infoblox solution.

Features and Benefits

Reliable Configuration Services via HTTP, FTP and TFTP: IP phones and other devices require periodic updates of their firmware and configuration files. The traditional way of supporting this requirement—using standard file servers—is difficult to secure and requires extensive effort to ensure that all sites contain the right files. The Infoblox file distribution service provides a secure, reliable, manageable solution. For appliances deployed in an Infoblox Grid, firmware and configuration images are uploaded only once and are then distributed automatically to all appliances in the Grid, saving time and ensuring that devices have access to critical files. The files can then be delivered to the local devices using HTTP, FTP or TFTP.

Time Synchronization Services via Network Time Protocol: Providing accurate time service to devices on a network is not just a convenience to the user but is critical for security and logging services. The Infoblox NTP service supports NTP authentication for environments that need to verify that network time is being supplied by a trusted source.

Consolidated, Reliable Logging via Syslog NG Proxy: Syslog NG proxy allows multiple devices to send logging messages to an Infoblox appliance which will then forward the messages to a central logging server. This simplifies the configuration of logging services for network devices such as firewalls, switches, routers, and wireless access points. The centralized logging server and intervening firewalls and routers with access control lists can be configured once to accept logging messages from the Infoblox appliance and the individual networking devices can be configured to send logging messages to the Infoblox appliance.

Microsoft®
GOLD CERTIFIED

Partner



DNS Technical Specifications	
RFCs Supported	1034 and 1035 Dynamic update, RFC 2136 Incremental zone transfer, RFC 1995 Notification of zone changes, RFC 1996 Secret key transaction authentication (TSIG), RFC 2845 Classless IN-ADDR.ARPA delegation, RFC 2317
Protocol Engine	BIND 9.8.0
Additional Capabilities	<ul style="list-style-type: none"> • DNS64 • DNSSEC Secure dynamic DNS updates using TSIG • Conditional forwarding • Microsoft Active Directory support • Infoblox Views • IP-address-based access lists on queries, zone transfers, and dynamic updates • Zone import tools • Customizable TTL settings
DHCP Technical Specifications	
RFCs Supported	RFCs 3046, 2131 and 1531 BOOTP, RFCs 1534, 2132 and 4388 (Leasequery)
Protocol Engine	DHCP 4.2.0-P2
Additional Capabilities	<ul style="list-style-type: none"> • VLSM (Variable Length Subnet Mask) support • CIDR (Classless Inter-Domain Routing) support • Multiple subnets per segment (supernetting) • “Static leases” based on MAC address (manual allocation) • MAC-address-based filtering • Address availability checking before assignment • IPv6 prefix delegation • DHCP IPv6 • DHCP relay agent/Option 82 support • DHCP Vendor Class Identifier/Option 60 support • Secure DHCP-DNS integration updates DNS when leases are issued • Advanced DHCP Options Editor • Windows, Unix, and Mac OS compatibility • External syslog server supports

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.