

SOLUTION NOTE

HSPD-12:

Focuses on the protection of personally identifiable information (PII) and system integrity.

OMB Memorandum 05-22:

Requires the deployment of IPv6 in all federal backbones.

OMB Memorandum 08-23:

Requires every U.S. federal organization deploy DNSSEC by December 2009.

Maintaining strict security and meeting compliance mandates while ensuring highly available networks and applications for an exceptional citizen experience and daily government operations is a constant challenge for federal government IT departments.

Federal IT groups' challenges are further complicated by reduced staff and budgets, requiring them to do more with less, given the current state of the economy. To address these challenges, robust core network services—IP address assignment and management (DHCP and IPAM), and domain name resolution (DNS), and TFTP for VoIP, among others—are required. If core network services don't work, the network and applications that the federal government and the U.S. citizens rely on don't work.

Technical Issues of Conventional Core Network Services (CNS)

Shortcomings in conventional CNS solutions (i.e., general-purpose servers, operating systems, and freeware) can unexpectedly disrupt availability of the critical federal applications. Specific concerns with conventional solutions, such as Microsoft, in a federal government environment include:

- DNSSEC and IPV6 compliance challenges
- Vulnerable to attacks
- No audit logs, including DNS query logs, to investigate network breaches
- Unreliable with limited DR for consolidated data centers
- Requires many cycles and experts to maintain, upgrade and patch
- No option for real-time, centralized management visibility and/or control

With conventional solutions, servers have to be managed individually and frequent updates/patching can consume IT cycles. On the security front, general-purpose operating systems and older BIND DNS versions are open to attack, which can compromise system integrity and the ability to achieve FISMA compliance.

Also, it is difficult to implement high-availability solutions and achieve failover. In a disaster scenario, there is little to no ability to easily recover because there is no central point of management for administrators to map around failed servers and re-partition the network.

And, with the most commonly available tools, implementing DNSSEC is incredibly complicated, requiring multiple steps and lots of work at the command line to generate key pairs and sign a zone. All of which must be repeated every time there is a change. Further, supporting IPv6 can tax the most experienced network administration team if they have to "cobble together" a solution.

These inadequacies are not easily overcome using band-aids and tools applied to existing systems, such as overlay management and data back-up systems.

Business Impacts

Federal government organizations that use conventional approaches to deliver CNS are subject to:

- Downtime of network and key applications
- Business continuity/DR risks
- Failure to meet compliance mandates
- Cumbersome administrative cycles and high operating costs due to lack of automation
- Attacks and breaches

Ramifications like these merit deployment of a core network services infrastructure that offers unique security and DR advantages, and is manageable and reliable for federal environments.

Infoblox Solutions Offer Unparalleled Advantages for Federal Organizations

To provide nonstop services, improve security, including the ability to achieve regulatory compliance, eliminate reliance on experts and reduce operating costs, federal government organizations need to consider Infoblox's next-generation approach to delivering and managing CNS infrastructure.

- Appliances deliver high availability services and secure infrastructure
- Grid technology ensures continuous uptime and centralized management
- Unique DR capabilities enable "one-click" recovery
- Easy DNSSEC configuration and automated, "one-click" key signature
- Built-in, U.S. government-certified IPv6 support
- Delegated administration provides granular access control to specific zones, records, networks, scopes, and appliances
- Tracks IP allocation history (which device or which user was using an IP address)

Infoblox appliances enable "one-button" upgrades to accommodate new features and easy installation of the latest BIND releases. Additionally, the custom Infoblox operating software is hardened and, therefore, secure from vulnerabilities, meeting compliance requirements.

In the event of a malicious attack, leveraging rich data, such as DHCP lease history, federal IT representatives can easily identify which port had a rogue appliance address on it and stop the incident.

SOLUTION NOTE

Solution Benefits

- Continuous uptime and “touch of a button” DR
- Allow experts to focus their attention on other critical areas
- Enable regulatory compliance
- Reduce administrative overhead and costs
- Increase security
- Increase visibility into and control of who is on the network, when and where

In addition to high availability (HA) between appliances, Infoblox’s Grid technology, which links appliances into a unified, distributed system that is resilient to network and equipment failures and provides central management, enables “one-click” recovery from catastrophic failures of major data centers or WAN links.

On the compliance front, Infoblox has built-in support for DNSSEC. Transparent to end users, DNSSEC by Infoblox can be configured with single clicks, and delivers automated, on-the-fly key generation and management using the latest technology and protocol features (BIND 9.6.1 with NSEC3 support).

And, Infoblox systems have been successfully certified by the Defense Information Systems Agency for Internet Protocol (IP) Version 6 (IPv6) interoperability. This certification is based on testing conducted by the federal government’s Joint Interoperability Test Command (JITC).

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.