INFOBLOX 7.x DOMAIN NAME SYSTEM (DNS) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 1

22 January 2021

Developed by Infoblox and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Infoblox 7.x DNS Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to Infoblox Trinzic DDI implementations.

The scope of this STIG only includes the DNS capabilities of the Infoblox appliance.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. CONCEPTS AND TERMINOLOGY CONVENTIONS

2.1 Terminology

Grid – A collection of Infoblox appliances communicating in a hub and spoke architecture via a secure SSL VPN to a management appliance designated as the Grid Master.

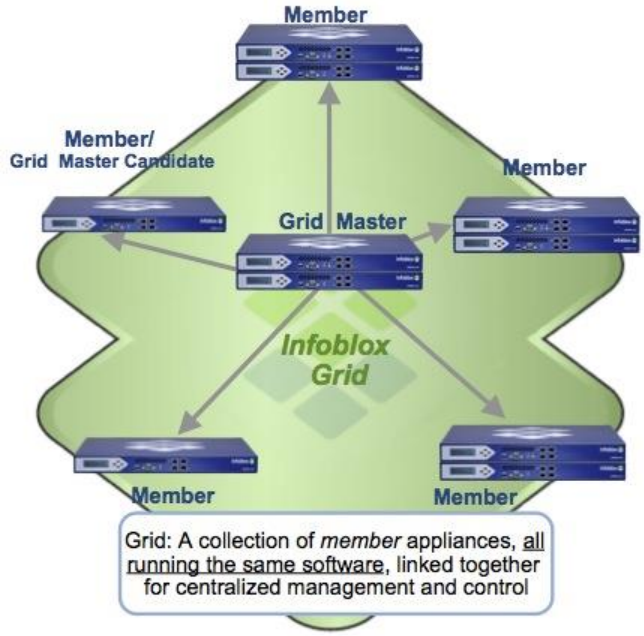
Grid Master (GM) – Any member of the Grid designated to be the primary management and configuration appliance; only one allowed. The GM is the full repository of ALL Grid data and configurations. Typically the Grid Master is deployed on a secure Out Of Band (OOB) network and does not service client requests for DNS or Dynamic Host Configuration Protocol (DHCP).

Grid Master Candidate (GMC) – Any member or members of the Grid designated as a warm backup that has all changes to the Grid Master synchronized. The GMC is a backup system in the event of system failure on the Grid Master. It can be promoted and then serve as the primary management and configuration system.

Network Identity Operating System (NIOS) – NIOS is the operating system for the Grid infrastructure. It is a minimal Linux kernel-based system with only specific components added, resulting in a small, secure, and high-performance total software footprint. Infoblox NIOS systems do not provide shell access, and there are no "root" level privileges. The system is delivered with a single administrator account that can be removed once an additional user account is created. By default, NIOS only runs the services required for management. All protocol services are disabled by default and must be enabled through administrator configuration. A NIOS distribution includes all operating systems and services. The Grid Master distributes upgrades and manages version consistency across all Grid members via a single NIOS upgrade file. DNS and DHCP services are provided using Infoblox modified versions of Internet Systems Consortium (ISC) Berkeley Internet Name Domain (BIND) and Dynamic Host Configuration Protocol Daemon (DHCPD). These are modified to interact with the Infoblox integrated database and include many enhancements over the open source versions distributed by ISC. There are no configuration files written and then read from the disk; rather, information is contained in the single integrated proprietary database and services read information and configurations directly from it. As with the file system, there is no direct access to the database. Each administrative account is validated for access and input is screened through syntax checking. All system and database maintenance activity is automated.

2.2 Architecture Diagram

Figure 1-1: Grid Architecture Diagram



3. GENERAL SECURITY REQUIREMENTS

3.1 Permission Structure

Infoblox NIOS applies permissions hierarchically in a parent-child structure. When you define permissions for a resource, all objects within that resource inherit the same permissions. For example, when you grant an admin group read/write permission for a network, the admin group automatically has read/write permission for objects in that network. To override permissions set at a higher level, you define permissions at a more specific level. For example, to examine an Access Control List (ACL) for zone transfers, validation must be completed on the individual zone. Checking of the ACL at the Grid DNS Properties level is insufficient because that configuration may be overridden in the Member and possibly also at the Zone level. Unless specifically noted, all checks should be performed at the most specific level.

3.2 DNSSEC

The Infoblox GM stores the necessary Domain Name System Security Extensions (DNSSEC) keys within its database. When a zone is DNSSEC signed, the GM will enable its DNS service if not already running and add itself as a stealth name server in the signed zone. Once added, the GM will then perform all signing functions related to DNSSEC and distribute the signed zone to the applicable member servers. For all service-related checks, it must be verified that the stealth setting is preserved. Removal of the GM from a DNSSEC signed zone, or disabling the DNS service on the GM, will result in a loss of service due to the inability to sign and resign zone updates.

3.3 Zone Transfers

Infoblox systems within the same Grid will by default use database updates from the GM to update zone data. Zone transfers to systems external to the Infoblox Grid being examined will use standard DNS zone transfers. For all checks related to zone transfers, those with name servers of the "Type Grid" are not applicable, as these are secured within the Infoblox Grid and updated via the secure connection used to establish the Grid. Zone transfers to external systems or those where the default is overridden by the administrator use standard DNS zone transfers and must be configured with access control via either an ACL or Access Control Entry (ACE). These contain IPv4 and IPv6 address and network restrictions and allow configuration of Transaction Signature (TSIG).

3.4 Configuration Considerations

Check and Fix steps in the STIG are summary instructions to illustrate the required configurations in a secure state. Sites that require reconfiguration of DNS services such as DNSSEC and TSIG must thoroughly review all applicable documentation prior to implementation. Many DNS functions, such as DNSSEC, TSIG, and Dynamic DNS Updates, often require external support and coordination to function properly and may have other system dependencies such as DHCP server support. Implementation or reconfiguration of these and

other DNS features without appropriate understanding and planning may result in service outages.

Infoblox systems that are not configured for Grid operation are designated standalone. Standalone system evaluation will follow the STIG, and each system must be evaluated individually. When reviewing the STIG on a standalone system, note that references to the Grid tab will be under the System tab, and the Grid Properties option is renamed to System Properties.

3.5 Hardware Security Modules (HSM)

A Hardware Security Module (HSM) is a physical computing device that safeguards and manages digital keys. By default, Infoblox systems store digital keys in the Infoblox database. When an HSM is installed and configured to work with the Infoblox Grid, keys are then stored on the HSM. Additional details regarding HSM signing are available in the Administration Guide via the following link:
http://dloads.infoblox.com/direct/appliance/NIOS/NIOS_AdminGuide_7.1.pdf