UNIVERSITY SYSTEM OF GEORGIA

DOMAIN NAME SERVICE (DNS): A USG IT HANDBOOK COMPANION GUIDE

VERSION 1.3

10/9/2020

PUBLIC

Abstract: This companion guide was developed to aid USG organizations concerning the administration of DNS and has been classified as a “Public” document.

Revision & Sign-off

Change Record

Date	Author	Version	Change Reference
20120401		1.0	Draft
20130226		1.1	Software and Configuration: 4 Add recursion.
20130326		1.2	Add References, prepend each section with letter, and add some definitions.
20160219	Alfred Barker	1.3	Replaced “shall” with “should,” removed section B “Rationale” and adjusted section lettering, and clarification of wording and references added.
20201009	Alfred Barker	1.3	Reviewed for Harmful Language.
20201009	Alfred Barker	1.3	Migrated to new format, no content changes.

Document Properties

Item	Details
Document Title	Domain Name Service (DNS): A USG IT Handbook Companion Guide
Document Type	Guideline (Internal Use Only)
Author	Alfred Barker
Document Manager	Alfred Barker
Creation Date	20201009
Last Updated	20201009
Document Classification	Public

Introduction

The *DOMAIN NAME SERVICE (DNS): A USG IT HANDBOOK COMPANION GUIDE* was developed to aid USG organizations concerning the administration of DNS. This guide provides direction to implement available and secure DNS servers critical to the reliability of an information technology (IT) infrastructure. This guide also covers setup and administration of University System of Georgia (USG) organizations' registered internet domains and DNS servers.

As with all of our documents, they are dynamic and considered works in progress. If you discover an error or have an additional standard or regulation that the community would benefit from mapping, please submit your comment to cybersecurity@usg.edu for correction or consideration.

Domain Name System (DNS) Guidelines

A. Internet Domain

- USG organizations should limit personnel access to domain registrar accounts.
- Domain registrar accounts should adhere to organizational password policies standards and guidelines (PSG) unless the domain registrar account password polices differ. In these cases, the domain registrar account password PSG take precedence.
- USG organizations should use a monitored and functional email address in the domain registrar account so appropriate staff can receive relevant electronic communication.
- USG organizations should maintain consistency between Name Server (NS) records defined at the domain registrar and records advertised publicly by DNS servers.
- USG organizations should plan periodic renewal of domains.

B. Hardware/Environment/Operating System

- USG organizations should administer DNS server hardware and/or services as highly available, enterprise level systems in accordance with organizational PSG.
- Hardware for DNS servers should be installed in a controlled access location.
- If applicable, the operating system for DNS servers should be installed and maintained to protect from unauthorized access and use.
- Access to administer DNS server hardware, firmware and operating system should be granted on the principle of least privilege.

C. DNS Software and Configuration

- Software should be maintained at current production release levels supplied by software and/or system vendor.
- Patches should be tested and installed according to organizational PSG.
- Software should run as a non-privileged user.
- Software should not be configured to supply public recursion.
- DNS zone transfers should be strictly controlled by configuration and restricted to specific hosts.

D. DNS Architecture

- External (publicly accessible) DNS servers should be configured to mitigate the potential of cache poisoning and installed in a demilitarized zone (DMZ) or similar network architecture.
- Separate DNS servers should be used for internal and external resolution. Refer to split DNS.
- At least two external DNS servers should be implemented on unique network addresses and separate hardware, ideally on two different networks.
- Host names should comply with RFC 1123.
- DNS uses both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) on port 53. External DNS servers must answer queries over both protocols. Firewalls should be configured to permit inbound and outbound DNS traffic to external servers.
- Develop, document and implement plans to support service resilience.

E. Operational

- Data integrity should be maintained between authoritative DNS servers.
- Internal data consistency, e.g., PTR and A resource record coherence, is desired.
- All public DNS servers should supply identical NS and start of authority (SOA) records.
- Primary (authoritative) DNS records as well as DNS server configurations should be maintained to mitigate loss and facilitate recovery.
- Change management controls are highly recommended for daily operations.
- Principle of least privilege security should apply to the administration of DNS software.
- Two or more individuals should maintain the DNS system.
- Each DNS server should be configured to log zone transfers, configuration issues, security events and system events. System events should log to an external logging server.
- Configurations should be consistently applied to enforce operational PSGs.
- Configuration changes that impact services should be promptly communicated to entities providing secondary DNS services.
- Modifications to configurations should be in accordance with organizational PSG.

F. Validation

- Periodic reviews should be conducted on:
    - Server configuration and consistency;
    - Validity responses provided by internal and external queries;
    - Legitimacy of records within each zone; and,
    - Server logs.
- USG organizations should develop an ongoing program to monitor logs as a part of the normal operational cadence.

G. Definitions

Authoritative Server – A DNS server that provides an authoritative answer to queries of a zone.

Domain Name System (DNS) – A hierarchically distributed database used to name resources connected to a computer network. The system resolves computer host and service names to computer addresses and vice versa.

Domain – An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. (NIST Interagency Report (IR) 7298, Revision 2 (Glossary of Key Information Security Terms)).

Recursion – The process of providing name resolution by relaying the requests to a chain of authoritative name servers.

Request for Comment (RFC) – A memorandum system published by the Internet Engineering Task Force (IETF) to describe practices, methods and innovations germane to network-connected systems. RFCs are generally regarded as operational standards.

Secondary Server – An authoritative DNS server that does not maintain custody of primary (authoritative) data.

Split DNS or Split Horizon DNS – An architectural design which provides selective answers based upon a predefined condition. For example, a split DNS arrangement might supply private network answers to private users while providing different answers to public users.

H. References

- RFC 1034 (Domain Names – Concepts and Facilities)
- RFC 1123 (Requirements for Internet Hosts – Applications and Support)
- RFC 1178 (Choosing a Name for Your Computer)
- RFC 1912 (Common DNS Operational and Configuration Errors)
- RFC 2136 (Dynamic Updates in the Domain Name System (DNS UPDATE))
- RFC 2181 (Clarifications to the DNS Specification)
- RFC 2535 (Domain Name System Security Extensions)
- RFC 2671 (Extension Mechanisms for DNS (EDNS0))
- RFC 2845/4635 (Secret Key Transaction Authentication for DNS (TSIG)/HMAC SHA TSIG Algorithm Identifiers)
- RFC 4033 (DNS Security Introduction and Requirements)
- RFC 4592 (The Role of Wildcards in the Domain Name System)
- NIST Interagency Report (IR) 7298, Revision 2 (Glossary of Key Information Security Terms)
- NIST Special Publication 800-81-2 (Secure Domain Name System (DNS) Deployment Guide)