MICROSOFT WINDOWS SERVER DOMAIN NAME SYSTEM (DNS) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 4

01 April 2026

Developed by DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 1
1.4 STIG Distribution 2
1.5 Document Revisions 2
1.6 Other Considerations 2
1.7 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 Security Assessment Information 4
2.2 How DNSSEC Secures DNS Data 4
2.3 Sinkhole Name Servers 5
2.4 Securing DNS Zone Transfers, Dynamic Updates, and DNS Notify 5
2.5 DNS Zone Transfers and DNS Notify 5
2.6 Dynamic Updates 6

3. DNSSEC-SPECIFIC ENHANCEMENTS IN WINDOWS SERVER 7

3.1 DNS Client 7
3.2 Other Enhancements 7

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

This Microsoft Windows Server Domain Name System (DNS) Security Technical Implementation Guide (STIG) is published as a tool to secure Microsoft Windows DNS implementations.

This STIG will be used for all Windows DNS servers, whether they are Active Directory (AD)-integrated, authoritative file-backed DNS zones, a hybrid of both, or a recursive caching server. This STIG must also be used for Windows DNS servers that are a secondary name server for zones whose master authoritative server is non-Windows.

The direction is to ensure the authentication and integrity of Windows Server DNS data by applying DNS Security Extensions (DNSSEC) as specified by the Internet Engineering Task Force (IETF) Requests for Comment (RFC4641, RFC5011, RFC5155, RFC4033, RFC4034, RFC4035, and RFC3833) and outlined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-81, "Secure Domain Name System (DNS) Deployment Guide." NIST SP 800-81 rev 2, "Secure Domain Name System (DNS) Deployment Guide," has also been a resource in the development of this STIG.

The DNS Server service has greatly enhanced support for DNSSEC in Windows Server DNS. Therefore, these STIG settings are required for all Windows DNS implementations.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that 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 [National Security Agency/Central Security Service], 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 must 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

Category	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 DOD 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 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.

1.6 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 (AO). 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 DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.7 Product Approval Disclaimer

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). Department of Defense 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 in accordance with (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) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW federal/DOD mandated standards.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

This Microsoft Windows Server DNS STIG is intended for use in conjunction with the separate Windows 2022/2019 Active Directory and Domain Controller STIGs. The Microsoft Windows Server DNS STIG does not replace those STIGs.

Check and Fix text may include DNS Manager console instructions, instructions to be executed at a command line prompt, or instructions to be executed at a PowerShell prompt. ***PowerShell commands must be run from a Windows 10 or Windows 2016 or higher operating system to ensure the validity of the results***.

While multiple methods can be used to validate and fix a setting, generally only one is listed for each STIG requirement. Other methods listed for a Fix can feasibly be used to reach the same end result of remediating the vulnerability associated with the requirement.

Multiple requirements in the STIG are deemed compliant by the nature of the zones being signed with DNSSEC and by configuring IPsec for DNS servers.

2.2 How DNSSEC Secures DNS Data

DNSSEC uses asymmetric public/private key cryptography to provide digital signature validations. Once a zone is signed with DNSSEC, every individual DNS Resource Record in a zone is accompanied by a Delegation Signer (DS) Resource Record (RR) and a Resource Record Signature (RRSIG).

- The DS RR is a hash value of that record. The RRSIG record is an encrypted copy of the hash value (encrypted using the DNS Server's private key stored on the DNS server).
- When a resolver, client, or caching server requests to send a query to a DNSSEC-enabled DNS server, the query answer is returned accompanied by the DS and RRSIG.
- The resolver then uses the public key (DNSKEY) obtained from the DNS server to decrypt the RRSIG record and compares the hash value in the DS.
- If the result of the DNSSKEY decryption on the RRSIG matches the DS, the DNS data is approved as a valid source.

Before DNS signatures can be validated, however, all systems must trust a common authority, which is called the "Trust Anchor." The common DNS Trust Authority is the DNS Root Server (e.g., .com, .edu, .org, .mil, etc.). This authority will vouch for any child zones/domains of these Trust Points (e.g., disa.mil) if they are not individually signed. As of 05 May 2012, all internet root DNS servers have been digitally signed.

A caching DNS server will validate DNS query requests from clients if it is pointed to a Trust Anchor or Trust Point that has a stored copy of the public keys for the DNS zone requested in the query or from a parent zone.

Within the DOD, the Enterprise Resolving Server (ERS) holds the public keys for external DNS zones so DNSSEC validation occurs when internal DOD DNS caching servers/clients forward queries to the ERS. DNSSEC validation occurs even if a client is not DNSSEC aware.

While Windows 2008 first introduced some DNSSEC capability, the DNS Server service in Windows Server DNS has greatly enhanced support for DNSSEC.

FRAGO1 to TASKORD 11-0410-2 specified that all Combatant Commands/Services/Field Activities (CC/S/FAs) must implement DNSSEC on their second-level .mil domains by 01 May 2013 and all lower-level .mil subdomains by 03 June 2014. This requirement is for Unclassified networks only. Classified networks are exempt from the DNSSEC requirements, and those requirements may be marked not applicable for such systems.

2.3 Sinkhole Name Servers

Name servers configured as sinkhole name servers will be treated in the STIG as a caching/forwarding name server. This will only apply if the sinkhole name server has manual records added and is not otherwise authoritative for any zones.

In such an environment, clients/resolvers in the organization will point to this sinkhole server to determine whether an intended destination is deny listed.

If an intended destination is not deny listed, the sinkhole server must then default to a forwarding or caching role and point to another internal or DOD name server for completing the external recursive lookup or to the DISA ERS for external recursive lookup.

All STIG requirements referencing caching name servers do apply to a sinkhole name server. Because the server will not be authoritative for any zone, DNSSEC is not required on a sinkhole name server.

2.4 Securing DNS Zone Transfers, Dynamic Updates, and DNS Notify

Threats specific to DNS zone transfers, dynamic updates, and DNS Notify are mitigated by using encryption when transmitting server-to-server, client-to-server, or server-to-client DNS information. This encryption can be accomplished by using Transaction Signature (TSIG), SIG(0), or IPsec. Windows DNS Server does not support TSIG/SIG(0), so IPsec will be required for that protection.

2.5 DNS Zone Transfers and DNS Notify

The AD replication process provides a means of securing to a certain level DNS information transmission between DNS servers in a 100 percent Active Directory-integrated environment. However, Windows servers, whether in an AD-integrated, non-AD-integrated, or mixed configuration, require a means for securing the server-to-server communications.

As Microsoft states in the following Knowledge Base article, zone transfers can be secured using IPsec. Because Windows Server DNS does not support Transaction Signature (TSIG) for zone transfers, IPsec will be required for that protection.

- https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/active-directory-integrated-dns-zones.

Certificate-based authentication can be used to establish an IPsec session between DNS servers. Each endpoint must present a certificate to prove its identity. This method requires certificates to be created and configured on all DNS servers that participate in zone transfers for DNSSEC-signed zones. Procedures for deploying certificates for DNS server authentication can be found at the following Microsoft link:

- https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/server-certificate-deployment-overview.

Procedures for configuring IPsec between DNS servers can be found at the following Microsoft link:

- https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn593634(v=ws.11)?redirectedfrom=MSDN.

2.6 Dynamic Updates

Microsoft has implemented a proprietary version of GSS-TSIG into its Dynamic Update function. When Windows Server DNS is configured with "Secure only" for accepting Dynamic Updates, the clients must be part of AD for the update to the DNS to be accepted. This meets the requirements for authentication for Dynamic Updates in an AD-integrated configuration.

3. DNSSEC-SPECIFIC ENHANCEMENTS IN WINDOWS SERVER

3.1 DNS Client

DNS Client in Windows Server DNS now supports DNS-over-HTTPS (DoH), which encrypts DNS queries using the HTTPS protocol. DoH helps keep traffic as private as possible by preventing eavesdropping and DNS data from being manipulated.

Windows Server isolates the key management process from primary DNS servers that are not the Key Masters of a zone. The signing process can only be initiated from the Key Master; other primary servers can continue the zone signing by accessing these keys.

3.2 Other Enhancements

Other enhancements to DNSSEC in Windows Server DNS include:

- Support for Active Directory-integrated DNS scenarios, including DNS dynamic updates in DNSSEC-signed zones.
- Support for updated DNSSEC standards, including NSEC3 and RSA/SHA-2.
- Automated trust anchor distribution through AD.
- Automated trust anchor rollover support per RFC 5011.
- Updated user interface with deployment and management wizards.
- Validation of records signed with updated DNSSEC standards (NSEC3, RSA/SHA-2).
- Easy extraction of the root trust anchor.