WINDOWS SERVER 2008 R2
DOMAIN CONTROLLER (DC)
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 25

26 January 2018

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The Windows Server 2008 R2 Domain Controller Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed from DoD consensus, as well as the Windows Server 2008 R2 Security Guide and security templates published by Microsoft Corporation. This document is meant for use in conjunction with other applicable STIGs including such topics as Active Directory Domain, Active Directory Forest, and Domain Name Service (DNS).

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 Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.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. 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.

1.7 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. ASSESSMENT CONSIDERATIONS

The Windows Operating Systems Security Technical Implementation Guides (STIGs) Overview, also available on IASE, is a summary-level document for the various Windows operating system STIGs. Additional information can be found there.

2.1 Updating the Windows Security Options File

Some of the requirements in this STIG depend on the use of a Microsoft security options file (sceregvl.inf) that has been updated to include additional security checks ("MSS" settings) that are not visible in policies by default. An updated copy of the security options file is included with the Windows STIGs.

To load the updated Security Options file, complete the following (due to changes in Windows security, the administrator must first take ownership of the file before changes are made):

- Open a command prompt with elevated privileges.
- Take ownership of the file with the command "takeown /f c:\windows\inf\sceregvl.inf".
- Add Full permissions with the command "icacls c:\windows\inf\sceregvl.inf /grant username:f" where "username" is the administrator account.
- Rename the sceregvl.inf file in the %WinDir%\inf directory.
- Copy the updated sceregvl.inf file from the media provided to the %WinDir%\inf directory.
  - The file can be found in the Templates directory included in the STIG zip file.
- Re-register scecli.dll by executing 'regsvr32 scecli.dll' in the command prompt with elevated privileges.

The additional options will now appear in Windows policy tools, such as the Group Policy Editor (a restart of the tool may be required).

2.2 Performing Analysis with the Security Configuration and Analysis Snap-In

The Security Analysis and Configuration tool compares the effective systems settings to a security template, which is configured with STIG requirements. The tool is identified in the Checks section for the individual STIG requirements that can be analyzed using it. The security templates are provided with the STIG zip file in a Templates directory. They are intended for analysis only and can have unknown impacts if used to configure a system without adequate testing.

To load the Security Configuration and Analysis snap-in and analyze the system, perform the following steps:

- Select "Start".
- Enter "MMC" in the "Search programs and files" field and Enter.
- Select "File" from the MMC menu bar.
- Select "Add/Remove snap-in" from the drop-down menu.
- Select the "Security Configuration and Analysis" snap-in and click the "Add" button.
- Select "OK".
- Right-click on the Security Configuration and Analysis object in the left window.
- Select "Open Database" (this will create the database file if one does not exist).
- Enter a name and path for the database file (e.g., "C:\temp\scan\srr.sdb").
  - The path entered must exist prior to this step.
- Select "Open".
- If this was a new database file, a new window will open looking for a template to import. If an existing database file was used, right click on "Security Configuration and Analysis" in the left pane and select "Import Policy".
- In the "Import Template" window select the appropriate file name for the type of system.
  - The security templates can be found in the Templates directory included in the STIG zip file.
  - U_WinVersion_Analyze_Only.inf
- Check the box to "Clear the database before importing".
- Select "Open".
- Right-click on the Security Configuration and Analysis object in the left window.
- Select "Analyze Computer Now…" (Important: DO NOT select "Configure Computer Now…", this will import the settings in the "Analyze_Only" template to the system's local policy and cannot be undone automatically).
- Enter a name and path for the log file (e.g., "C:\temp\scan\srr.log").
- Select "OK".
- The Analyzing System Security windows will appear.
- When the analysis is complete, the Security Configuration and Analysis node can be expanded to view current configurations.
  - "Database Settings" are the required settings imported from the analysis template file.
  - "Computer Settings" are the effective settings on the system.
  - Settings with a green check indicate the Database and Computer settings match.
  - Settings with a red x indicate the Database and Computer settings do not match.