

UNCLASSIFIED



CENTRAL LOG SERVER SECURITY REQUIREMENTS GUIDE (SRG) TECHNOLOGY OVERVIEW

Version 1, Release 2

26 July 2019

Developed by DISA for the DoD

UNCLASSIFIED

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 DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Executive Summary	1
1.1.1 Security Requirements Guides (SRGs)	1
1.1.2 SRG Naming Standards.....	2
1.2 Authority	3
1.2.1 Relationship to STIGs.....	3
1.3 Vulnerability Severity Category Code Definitions	3
1.4 SRG and STIG Distribution	4
1.5 Document Revisions	4
1.6 Other Considerations	4
1.7 Product Approval Disclaimer.....	5
2. ASSESSMENT CONSIDERATIONS.....	6
2.1 NIST SP 800-53 Requirements	6
2.2 General Procedures	6
3. CONCEPTS AND TERMINOLOGY CONVENTIONS	7
3.1 Syslog Protocol	7
3.2 Log Management	7

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	4

1. INTRODUCTION

1.1 Executive Summary

DoD mandates the centralization of event logging to allow security personnel to rapidly visualize data from many sources to spot trends and complex attacks on enterprise assets. The Central Log Server Security Requirements Guide (SRG) supports this goal by providing the technical security policies, requirements, and implementation details for applying security concepts to Security Information and Event Management servers (SIEMs), syslog servers, Network Management Systems (NMSs), and other event-based aggregation and monitoring applications that are part of the events logging, notification, monitoring, and analysis functions in the enterprise. The scope of this document includes applications that leverage aggregated audit logs collected from firewalls, routers, servers, applications, and databases to visualize, monitor, notify, and alert based on identified thresholds.

Log management includes log collection/aggregation, secure storage, normalization, event analysis, reporting, and notification/alert generation. Current DoD requirements state that the organization must store the primary log records on a log server (e.g., syslog, SIEM, events server) that is on a different host than the operating system host that is being audited. This requirement helps ensure that a compromise of the information system being audited does not also result in a compromise of the audit records. DoD also requires centralized management and configuration of the content to be captured in audit records generated by devices and hosts in the enterprise. Thus, there is a requirement for a central log management, analysis, and reporting function that allows management and configuration of log (events) records.

Throughout this SRG, log, audit, and events records are used interchangeably and are understood to have similar meaning. Auditable events are those activities that can be tracked that provide information regarding system resource usage. These events are captured as part of the configuration of the operating systems or network management function of the hosts and devices on the network. In a typical hierarchy, all auditable records are sent to a syslog server that is configured on the host or device. The syslog daemon receives logs directed at it and aggregates the records. In larger networks, there can be multiple syslog servers separated based on network segment or device roles. These servers may then pass the events to an aggregator, which then may pass events of interest to a SIEM or other analysis and reporting servers. While this is not a required hierarchy, it is rapidly emerging as a best practice in log management in an enterprise network.

1.1.1 Security Requirements Guides (SRGs)

SRGs are collections of requirements applicable to a given technology family. SRGs represent an intermediate step between Control Correlation Identifiers (CCIs) and Security Technical Implementation Guides (STIGs). CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in a policy, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product's technology area.

There are four core SRGs: Application, Network, Operating System, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, there are Technology SRGs developed to address the technologies at a more granular level.

This Central Log Server SRG is based on the Application SRG. This Central Log Server SRG contains general check and fix information that can be used for products for which STIGs do not exist.

The STIGs based on this SRG will provide the product-specific technical implementation guidance for that product. The STIG will contain the specific check and fix information for the product it covers.

SRG Hierarchy example:

```
Application SRG
|_ Database SRG
    |_ MS SQL Server 2005 STIG
```

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and provide appropriate justification. It also provides the structure to identify variations in specific values based on the technology family. These variations will be captured once and will propagate down to the Technology SRGs and then to the STIGs. This will eliminate the need for each product-specific STIG to address items that are not applicable.

1.1.2 SRG Naming Standards

In an effort to establish consistency across the SRGs, a naming standard for the Group Title and STIGIDs has been established.

Technology SRG Naming Standards

For Technology SRG Group Title and STIGIDs the following applies:

{Core SRG value}-{Technology SRG}-{5- or 6-digit numeric sequence number}

Examples:

```
SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
SRG-NET-000001-VVSM-00001
SRG-OS-000001-UNIX-000001
```

Checks/fixes will be included at this level in a general form. These checks and fixes will apply for any STIGs that are created for products that do not have product-specific check and fix guidance.

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.

1.2.1 Relationship to STIGs

The SRG defines the requirements for various technology families, and the STIGs are the technical implementation guidelines for specific products. A single SRG/STIG is not all-inclusive for a given system, which may include but is not limited to: Database, Web Server, and Domain Name System (DNS) SRGs/STIGs. For a given system, compliance with all (multiple) SRGs/STIGs applicable to a system is required.

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 SRG and 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 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

2.1 NIST SP 800-53 Requirements

All applicable baseline technical NIST SP 800-53 requirements and security best practice requirements are included in this SRG.

CNSSI 1253 defines the required controls for DoD systems based on confidentiality, integrity, and availability (baseline) of the given information system. In all cases, CNSSI 1253, along with required baselines, will serve as the policy requirement for any given asset or information system.

2.2 General Procedures

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured system. These procedures are not product specific and are intended for use when a product-specific STIG is not available.

Note: The Central Log Server host and operating system, including any local logging functions, must also be secured. The applicable operating system STIG or Network Device Management (NDM) SRG must also be part of the STIG package. If the SIEM, syslog, or events server are hosted, add the applicable operating system STIG to the package. If the SIEM, syslog, or events server are implemented as a network appliance, add the NDM SRG to the STIG package. Many products also use large databases or database servers that also need to be secured.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Syslog Protocol

Syslog is a protocol in which the server is passively waiting for incoming messages. As long as no device sends a message, the syslog server will not log anything. Almost all devices need to be configured with their specific configuration tool. Typically, only two settings need to be made: one to activate syslog messages and one with the syslog server IP address or name.

Although User Datagram Protocol (UDP) has been the de facto communications protocol for syslog, this SRG mandates the use of Transmission Control Protocol (TCP) for DoD. This requirement is based on the NIST 800-53 requirement for assurance that the auditable event has been successfully logged, log failures are reported, and a notification is sent to designated personnel.

3.2 Log Management

Log management considerations should include, at a minimum:

- Centralized log aggregation of log information collected from both syslog hosts, which can communicate using the syslog protocol
- Centralized log aggregation of logs from databases and servers that do not natively send logs using the syslog protocol (examples include, but are not limited to, OS Servers and Application Server).
- The use of event reduction and normalization techniques since the goal of centralized logging is after-the-fact analysis and reporting
- Defining and documenting the scope of coverage for each syslog, SIEM, and aggregation server and documenting which device and hosts are to be collected by each server
- Defining and documenting log retention requirements for each device and host and then configuring the Central Log Server to comply with the required retention period
- Leveraging the robust automation tools of SIEMs and event analysis tools to automate notifications and regular log review for events of interest and indicators of compromise
- Configuring automated ticketing functions for events of interest and indicators of compromise to ensure action is taken and action items are recorded