VMWARE VSPHERE 8.0
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

31 October 2023

Developed by VMware 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 VMware vSphere 8.0 Security Technical Implementation Guides (STIG) provide security policy and configuration requirements for the use of vSphere 8.0 in the Department of Defense (DOD). The following comprise the VMware vSphere 8.0 STIGs:

- VMware vSphere 8.0 vCenter STIG.
- VMware vSphere 8.0 Virtual Machine STIG.
- VMware vSphere 8.0 ESXi STIG.
- VMware vSphere 8.0 vCenter Appliance EAM Service STIG.
- VMware vSphere 8.0 vCenter Appliance Envoy Service STIG.
- VMware vSphere 8.0 vCenter Appliance Lookup Service STIG.
- VMware vSphere 8.0 vCenter Appliance Perfcharts Service STIG.
- VMware vSphere 8.0 vCenter Appliance Photon OS 4.0 STIG.
- VMware vSphere 8.0 vCenter Appliance PostgreSQL STIG.
- VMware vSphere 8.0 vCenter Appliance STS Service STIG.
- VMware vSphere 8.0 vCenter Appliance UI Service STIG.
- VMware vSphere 8.0 vCenter Appliance VAMI Server STIG.

The VMware vSphere 8.0 STIGs presume operation in an environment compliant with all applicable DOD guidance.

The VMware vSphere 8.0 STIGs are for use with vSphere 8.0 Update 2.

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 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 Controlled Unclassified Information (CUI) will be available for 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 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.

1.8 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). 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.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

VMware vSphere 8.0 includes several components, each requiring separate STIG coverage. The following STIGs have been developed for vSphere 8.0 components. As STIGs are developed for other vSphere 8.0 components, they will be included here.

2.1.1 VMware vSphere 8.0 ESXi STIG

The VMware vSphere 8.0 ESXi STIG must be used to enhance the security configuration of the ESXi hypervisor hosting virtual machines.

2.1.2 VMware vSphere 8.0 Virtual Machine STIG

The VMware vSphere 8.0 Virtual Machine STIG must be used to enhance the security configuration of virtual machines hosted by the ESXi 8.0 hypervisor.

2.1.3 VMware vSphere 8.0 vCenter STIG

The VMware vSphere 8.0 vCenter STIG must be used to enhance the security configuration of the vCenter Server management application.

2.1.4 VMware vSphere 8.0 vCenter Appliance ESX Agent Manager (EAM) STIG

The VMware vSphere 8.0 vCenter Appliance EAM automates the process of deploying and managing vSphere ESX Agents while extending the function of an ESXi host to provide additional services that a vSphere solution requires. EAM deploys agent virtual machines (VMs), installs vSphere Installation Bundles (VIBs) in ESX, and integrates with DvFilter.

2.1.5 VMware vSphere 8.0 vCenter Appliance Lookup Service STIG

Lookup Service provides a central location for services to publish their functionalities as service endpoints. vCenter Services and external solutions can query Lookup Service to list the services and their endpoints for specific functionality.

2.1.6 VMware vSphere 8.0 vCenter Appliance Performance Charts (Perfcharts) STIG

The Perfcharts service collects and processes statistical performance data for managed entities into reports in image format. It then provides that image to the vSphere Web Client.

2.1.7 VMware vSphere 8.0 vCenter Appliance Photon Operating System (OS) 4.0 STIG

Photon is the underlying operating system for the vCenter Appliance. It is a lightweight Linux operating system that is optimized to run on vSphere.

2.1.8 VMware vSphere 8.0 vCenter Appliance PostgreSQL STIG

PostgreSQL is the embedded database on the vCenter appliance.

2.1.9 VMware vSphere 8.0 vCenter Appliance Envoy STIG

Envoy aggregates and reverse proxies vCenter services. This simplifies ports and certificate management by having one point of entry from a vCenter component perspective.

2.1.10 VMware vSphere 8.0 vCenter Appliance Secure Token Service (STS) STIG

The Secure Token Service issues, validates, and renews security tokens for vCenter. STS authenticates the vCenter users based on the primary credentials and constructs a SAML token that contains user attributes.

2.1.11 VMware vSphere 8.0 vCenter Appliance User Interface (UI) STIG

This is the HTML5 vCenter web interface.

2.1.12 VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI) STIG

The VAMI is a web interface that manages appliance-level functions such as host name, basic networking, Network Time Protocol (NTP), updates, syslog, root password reset, and more.

3. IMPLEMENTATION CONSIDERATIONS

3.1 Overview

There are many methodologies to audit and remediate STIG controls for vSphere. This section offers a VMware-recommended method that was used during validation and testing of the controls in this guidance. As always, take the necessary steps to back up configurations and protect critical data before performing any changes to the environment. Each environment will differ in how it is operated, and controls must be evaluated with operations in mind for an organization's environment.

3.2 Control Types

For appliance-based products, controls are categorized into either product or appliance controls to help differentiate where and how these controls are handled.

3.2.1 Product Controls

Product controls interact with the product via the traditional administrative user interfaces and/or API (for example, performing an audit or remediation through the vCenter Web Client). These controls are in the ESXi, vCenter, and Virtual Machine STIGs.

3.2.2 Appliance Controls

Appliance controls are involved with the underlying appliance components (Photon OS, databases, web servers, etc.) that make up the products' appliance. These controls are in the vCenter Appliance STIGs.

3.3 Defaults

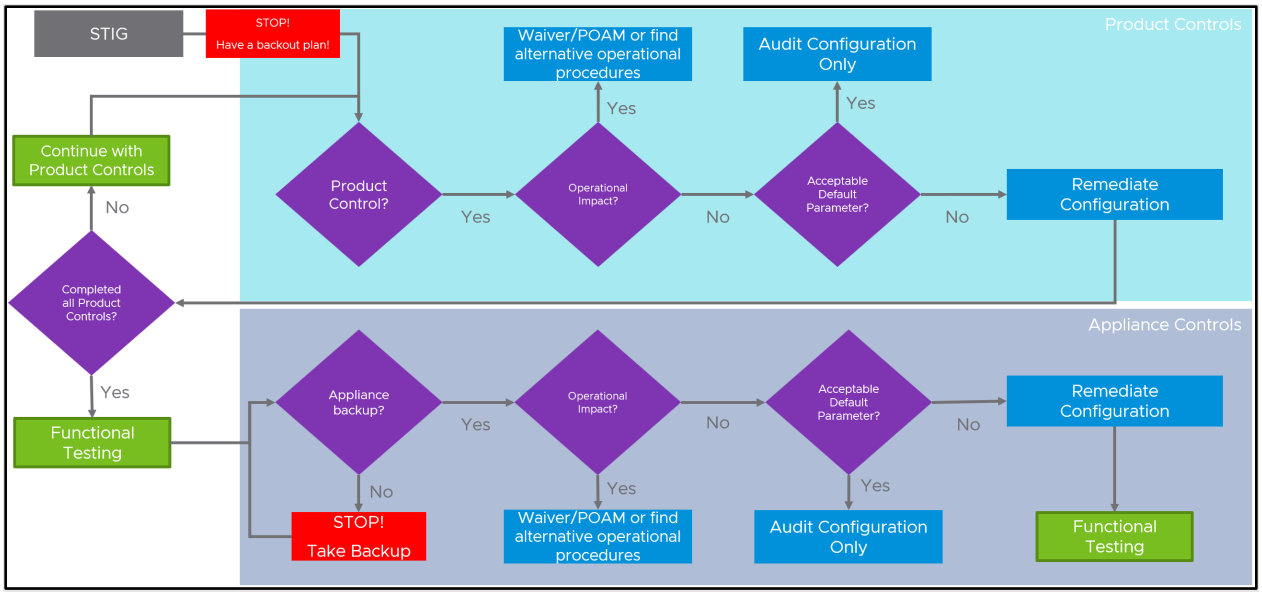
A control can be in a desired or compliant state (default) or in an undesirable (nondefault) state out of the box. Many controls will be in a compliant state upon deployment.

3.4 Methodology

The methodology workflow shown here can be used to evaluate and implement the vSphere STIGs in a consistent manner across an organization's environment.

Product controls should be evaluated and implemented first, followed by the appliance controls. Individual STIGs should be evaluated and tested in their entirety before moving on to the next STIG.

Figure 3-1: STIG Evaluation and Implementation Workflow



3.5 Tips

- Consider backing up any files needing remediation before making changes.
- Perform service restarts and/or appliance restarts after each appliance component is remediated. Many problems will not manifest until this is done.
- If it is not completely clear what a control is requiring the user to do, ask a coworker to review it or reach out for clarification.
- Become familiar with the available automation tools and how they work before using it.
- Run any existing daily health checks or common tasks in the environment to confirm functionality.