vSphere 7.0 STIG Readiness Guide Overview

Version 1 Release 3

Table of contents

Overview

VMware is a trusted partner in highly secure, mission critical systems around the world, including the US Department of Defense (DoD). In the DoD, all IT systems must adhere to the rigorous Risk Management Framework (RMF) as defined in DoDI 8510.01. A critical component of RMF is the mandatory implementation of Security Technical Implementation Guides (STIGs) and Security Requirements Guidelines (SRGs) as maintained by the Defense Information Systems Agency (DISA). Where a product specific STIG is not available, the relevant SRGs must be used instead.

DoDI 8510.01

"STIGs are product-specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 security controls into single, actionable, measurable items. SRGs are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used."

To better serve the needs of our DoD partners, and those who wish to meet the bar set by the DoD, VMware is providing SRG content that is the source material for an existing STIG, the basis for a future or in-process STIG, or that can be used in the absence of a DISA published STIG.

What does STIG Readiness mean?

VMware has published several STIGs with DISA and as such, we are very familiar with the SRGs and what it takes to meet DISA's stringent requirements for risk acceptance and publication. "STIG Readiness" means that we are doing the same level of work as we would do with DISA but self-publishing the content to make it available and usable as soon as possible. The quality is high enough, in our experience, that should a given "STIG Ready" product be put through the DISA process, we are confident that there would be minimal content changes before publication.

This project represents VMware's effort to document our compliance against the SRG requirements and nothing more. A published STIG is our eventual goal, in most cases, but this content should not be viewed to be "as good as a STIG". A DISA published STIG includes technical validation, review of requirement fulfillment, accuracy and style, risk acceptance and is digitally signed by the RME and posted on cyber.mil. Except for products that already have published STIGs, there is no explicit or implied DISA approval of the provided content. We also make no guarantee that any STIG(s) will be published from this content in the future.

Support

As previously stated, this content is produced by VMware without any DISA ownership. As such, any technical issues must go through your usual VMware support channels and not DISA.

Other Considerations

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 as such ensure all steps are taken to back systems up before implementation.

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. Furthermore, VMware implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is intended 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 because some of the settings may not be able to be configured in environments outside the DoD architecture.

Product Summary

VMware vSphere is VMware's virtualization platform, which transforms data centers into aggregated computing infrastructures that include CPU, storage, and networking resources. vSphere manages these infrastructures as a unified operating environment and provides you with the tools to administer the data centers that participate in that environment.

The two core components of vSphere are ESXi and vCenter Server. ESXi is the virtualization platform where you create and run virtual machines and virtual appliances. vCenter Server is the service through which you manage multiple hosts connected in a network and pool host resources.

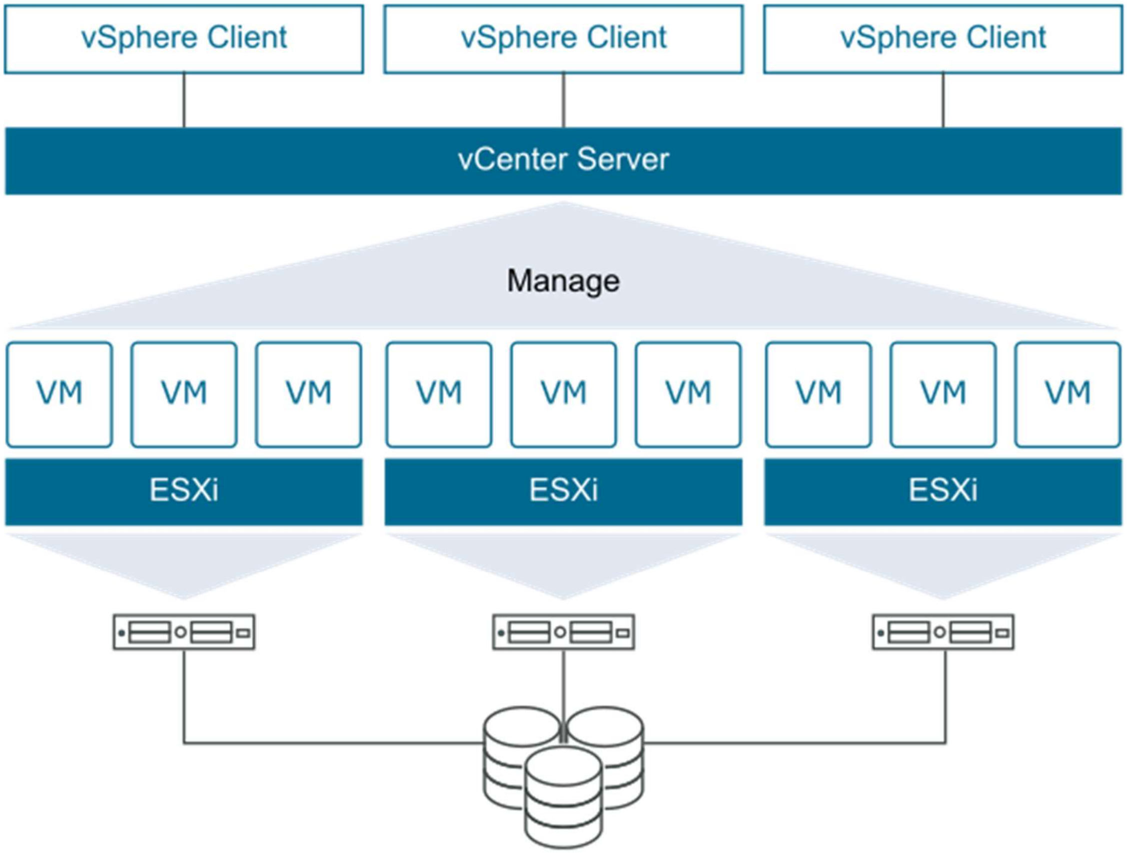


Figure 1 - vSphere Architecture

The VMware vSphere 7.0 STIG Readiness Guide provides security policy and technical configuration requirements for the use of vSphere 7.0 in the Department of Defense (DoD). The content comprises the following individual documents:

- VMware vSphere 7.0 ESXi
- VMware vSphere 7.0 Virtual Machine
- VMware vSphere 7.0 vCenter including vSAN
- VMware vSphere 7.0 vCenter Appliance EAM
- VMware vSphere 7.0 vCenter Appliance Lookup
- VMware vSphere 7.0 vCenter Appliance Perfcharts
- VMware vSphere 7.0 vCenter Appliance Photon OS
- VMware vSphere 7.0 vCenter Appliance PostgreSQL
- VMware vSphere 7.0 vCenter Appliance Rhttpproxy

- VMware vSphere 7.0 vCenter Appliance STS
- VMware vSphere 7.0 vCenter Appliance UI
- VMware vSphere 7.0 vCenter Appliance VAMI

Content Scope

The content was developed for a typical vCenter deployment managing a number of ESXi hosts and virtual machines. Your deployment and operational considerations must be considered when implementing these controls.

Implementation Guidance

Overview

There are many methodologies to audit and remediate STIG controls for vSphere with no right or wrong answer. In this section we will offer one method which was used during validation of the controls in this guide. As always please take the necessary steps to backup configurations and protect your critical data before performing any changes to your environment. Each environment will also differ in how it is operated and must be considered for controls that may hinder operations in your environment.

Control Types

For appliance-based products we refer to the controls as being in one of two categories, Product or Appliance controls to help differentiate where and how these controls are handled.

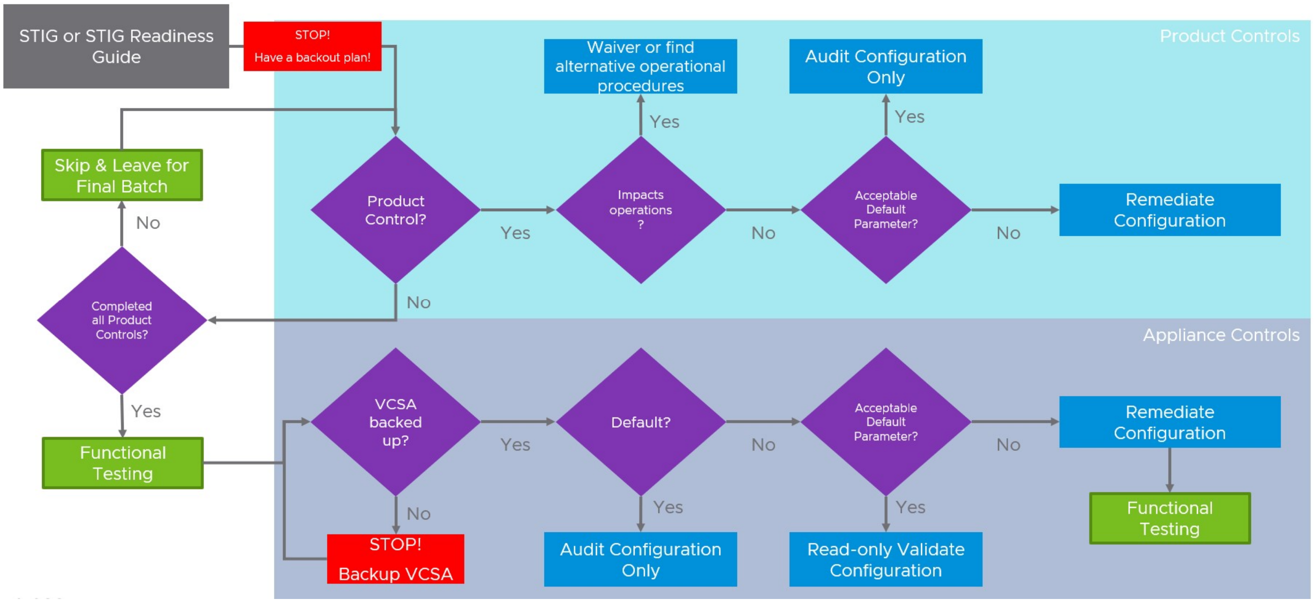
Product Controls: Controls that interact with the product via the traditional administrative User Interfaces and/or API. For example, performing an audit or remediation through the vCenter Web Client.

Appliance Controls: Controls that involve with the underlying appliance components (Photon OS, databases, web servers, etc.) that make up the products appliance.

Defaults

A control can either be in a desired state (default) or in an undesirable (non-default) state out of the box. A large portion of the appliance controls will be in a default state upon deployment with our goal to close that gap over time.

Methodology



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 may not manifest until this is done.
- If you are not 100% sure what a control is asking you to do ask a co-worker to review it.
- Get familiar with the available automation tools and how they work before going all in on the automation content that is available.
- Run any existing daily health checks or common tasks in your environment to confirm functionality along the way.

Frequently Asked Questions

What do the severity codes mean?

As stated in the DISA Security Requirements Guides:

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.

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.

Most of the severity codes in the associated guides are CAT IIs. During STIG development DISA modifies severity codes on a per product and context specific basis.

Can I import the XCCDF files into STIG Viewer?

Yes, the XCCDF files can be imported into STIG Viewer and then used to create STIG Checklists as necessary. They can alternatively be viewed by opening the XML file in Internet Explorer.

Are there any scripts or tools to help audit and remediate these controls?

Yes, there are example scripts and playbooks to aid in these tasks available in the GitHub repo linked below. Please carefully examine and test before running these in a production environment.

https://github.com/vmware/dod-compliance-and-automation/

What requirements were considered when developing this content?

All technical NIST SP 800-53 requirements and applicable SRGs were considered while developing this content. Requirements that are applicable and configurable will be included in the final content.