VMware Cloud Foundation STIG Readiness Guide Overview

4.x Release 4

vmware

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

This guidance is intended for VCF 4.5 and greater. Application of this guidance prior to 4.5 is not recommended.

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

The VMware Cloud Foundation (VCF) DoD STIG Readiness Guide is a document to assist customers that need to comply with DoD security requirements by providing hardening guidance for VCF products based on DISA Security Requirements Guides.

In the accompanying guidance documents, there will be an XCCDF document for each VCF product containing controls for each component that makes up that product.

VCF products covered by this publication:

- vSphere (vCenter, ESXi, Virtual Machines, vSAN)
- NSX-T
- SDDC Manager

For specific versions please refer to the VCF documentation and release notes at: VMware Cloud Foundation Documentation

SDDC Manager

SDDC Manager automates the entire system lifecycle (from configuration and provisioning to upgrades and patching) and simplifies day-to-day management and operations.

The SDDC Manager appliance contains several components in addition to the operating system that are covered:

- SDDC Manager Application
- SDDC Manager Appliance
    - Common Services Service
    - Domain Manager Service
    - Lifecycle Manager Service
    - Nginx Reverse Proxy
    - Operations Manager Service
    - Photon OS
    - PostgreSQL Database
    - SOS Utility
    - UI Service

vSphere

VMware vSphere uses virtualization to transform individual data centers into aggregated computing infrastructures that include CPU, storage, and networking resources. VMware 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.

vSphere comprises of several products that this document will cover including:

- ESXi
- Virtual Machines
- vSAN
- vCenter
- vCenter Server Appliance
    - ESXi Agent Manager Service

- Lookup Service
- Performance Charts Service
- Photon OS
- PostgreSQL Database
- Rhttpproxy
- STS Service
- VAMI Service
- vSphere UI Service

NSX-T

NSX-T Data Center is focused on providing networking, security, automation, and operational simplicity for emerging application frameworks and architectures that have heterogeneous endpoint environments and technology stacks. NSX-T Data Center supports cloud-native applications, bare metal workloads, multi-hypervisor environments, public clouds, and multiple clouds.

NSX-T includes several capabilities that this document will cover including:

- Manager/Controller
- Distributed Firewall
- Tier-0 Gateway Routing
- Tier-1 Gateway Routing
- Tier-0 Gateway Firewall
- Tier-1 Gateway Firewall

Content Scope

The content available in this guide was intended for VCF version 4.5+.

VCF Considerations

vSphere Considerations on VCF

These controls have been identified as known to have additional considerations with VCF deployments depending on the deployed version. Each environment has its own operational needs which may affect which controls can implemented, as always take appropriate steps when implementing controls.

Control ID	Severity	Requirement	Notes
ESXI-70-000042	CAT II	The ESXi host must terminate shell services after ten minutes.	SDDC Manager requires SSH for bring up and periodically lifecycle operations currently. This may interfere with long running operations if SSH times out after it is started.
ESXI-70-000049	CAT II	All management traffic on standard switches must be isolated from other traffic types.	As deployed by VCF the management domain components (vCenter, NSX-T, SDDC Manager, etc.) are on a shared network with ESXi management. This cannot currently be changed after deployment.

ESXI-70-000076	CAT II	The ESXi host must enable Secure Boot.	If the imaging appliance (VIA) is used to image the ESXi hosts, it currently does not support UEFI which is a requirement for enabling secure boot. ESXi installations done through other methods are supported and can enabled UEFI/secure boot.
ESXI-70-000078	CAT II	The ESXi host must use DoD approved certificates.	This is possible but additional steps to trust the certificates must be done on the SDDC manager appliance as detailed in the following article. https://blogs.vmware.com/cloud-foundation/2020/04/14/replacing-vmware-esxi-ssl-certificate-in-vmware-cloud-foundation/

Implementation Guidance

Overview

There are many methodologies to audit and remediate STIG controls for VCF 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.

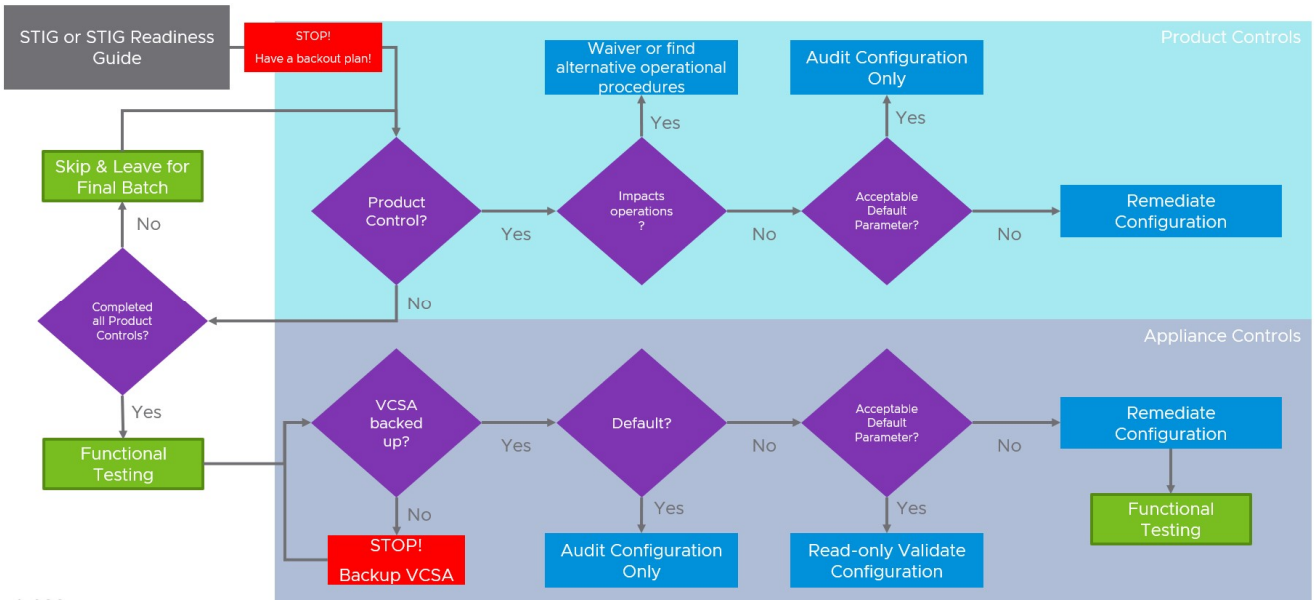
Product Controls: Controls that interact with the product via the traditional administrative User Interfaces and/or API. For example, performing an audit or remediation through the vCenter Web Client.

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.

What is an Extensible Configuration Checklist Description Format (XCCDF) file?

As stated by NIST: *"XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices."*

How do I view this guidance?

DISA STIGs are typically viewed with the STIG Viewer tool. This tool is made available by DISA and can be downloaded from: https://public.cyber.mil/stigs/srg-stig-tools/

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.

Item No: vmw-wp-tech-temp-a4-word-2021 8/21