

UNCLASSIFIED



VMware ESXi5 vCENTER SERVER SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 7

22 April 2016

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
1.2 Authority	1
1.3 Vulnerability Severity Category Code Definitions	2
1.4 STIG Distribution.....	2
1.5 Document Revisions	2
1.6 Other Considerations.....	2
1.7 Product Approval Disclaimer.....	3
2. ASSESSMENT CONSIDERATIONS.....	4
2.1 VMware ESXi Server 5.0, vCenter Server, and Virtual Machine Security Technical Implementation Guides	4
2.1.1 VMware ESXi 5 Security Technical Implementation Guide	4
2.1.2 VMware vCenter Server Security Technical Implementation Guide.....	4
2.1.3 VMware Virtual Machine Security Technical Implementation Guide.....	4
2.2 Command Examples	4
2.3 File Paths	4
2.4 Alternate Software	5
2.5 Requirements for Disabled Functions	5
3. CONCEPTS AND TERMINOLOGY CONVENTIONS.....	6
3.1 The ESXi 5 vSphere Client	6
3.2 The ESXi 5 Server Local Access and Lockdown Mode.....	6
4. SOFTWARE PATCHING GUIDELINES	8
5. OPEN SOURCE SOFTWARE (OSS) USE	9

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2

1. INTRODUCTION

1.1 Executive Summary

This VMware ESXi Version 5 vCenter Server (ESXi 5 vCenter) Technology Overview, along with the ESXi 5 vCenter STIG, provides the technical security policies, requirements, and implementation details for applying security concepts to the vCenter Server.

The VMware vSphere 5 Security Hardening Guide contains product-specific, best-practices requirements for VMware ESXi 5 vCenter Server. This hardening guide describes the ESXi 5 built-in security features, and the measures to safeguard ESXi 5 from attack. This hardening guide may be used to secure the vSphere 5 environment for VMware vCenter Server 5 and VMware ESXi 5. This guide was used as input into this STIG.

The Windows Server 2008 R2 Security Technical Implementation Guide contains product-specific requirements for Windows Server 2008 R2, which is used as the base operating system to support the VMware vCenter Server, VMware vSphere Update Manager, and the VMware vSphere Update Manager Download Server. This STIG may be used as a guide for enhancing the base operating system security configuration of the Windows 2008 R2 Server hosting VMware vSphere applications.

The security requirements contained within this STIG are designed to assist Security Managers (SMs), Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and System Administrators (SAs) with configuring and maintaining security controls in a VMware vSphere environment centrally managed by a vCenter Server.

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 provide 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 configurations 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% 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 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

There are three product specific STIGs related to ESXi 5 vCenter Server. All three must be utilized in securing a VMware vSphere 5 site installation. They refer to the ESXi 5 bare-metal hypervisor running virtual machines, the vCenter Server used to manage the hypervisor, and virtual machines configured to run on the hypervisor.

2.1 VMware ESXi Server 5.0, vCenter Server, and Virtual Machine Security Technical Implementation Guides

2.1.1 VMware ESXi 5 Security Technical Implementation Guide

The VMware ESXi 5 Security Technical Implementation Guide may be used as a guide for enhancing the security configuration of the ESXi 5 Server system, including the server's virtual machines and virtual networking components.

2.1.2 VMware vCenter Server Security Technical Implementation Guide

The VMware vCenter Server Security Technical Implementation Guide may be used as a guide for enhancing the security configuration of the vCenter Server system, including the vSphere Update Manager. This Overview is for ESXi 5 vCenter Server.

2.1.3 VMware Virtual Machine Security Technical Implementation Guide

The VMware Virtual Machine Security Technical Implementation Guide may be used as a guide for enhancing the security configuration of the ESXi 5 Server's virtual machines.

2.2 Command Examples

Some check and fix procedures contain example commands that can be used to obtain information regarding compliance with a requirement or to change a setting to attain compliance with a requirement. The commands used in the ESXi 5 vCenter STIG are intended to only use vSphere Client GUI software and required parameters. If the GUI software used by these commands is not present on the system, or does not recognize the specified options, the SA or the reviewer is responsible for determining compliance with the requirement using the tools available on the system. Check procedures also contain instructions for evaluating compliance based on the output of these commands.

2.3 File Paths

The check and fix procedures for the ESXi 5 vCenter STIG uses absolute file paths where possible.

2.4 Alternate Software

vSphere 5 systems offer extreme flexibility in components provided by the vendor to meet operational needs. Many of the check and fix procedures in the ESXi 5 vCenter STIG assume the use of a specific command line or GUI utility provided by the vendor. If an alternate software method is used to provide a function ordinarily provided by the default specified command line or GUI utility, the specific check and fix information for that function is no longer valid. The SA or the reviewer is responsible for evaluating the requirements based on documentation available for the alternate method used. The system accreditation package must contain information pertaining to the use of the alternate check and fix methodology used.

2.5 Requirements for Disabled Functions

The ESXi 5 vCenter STIG defines requirements for the further hardening and configuration of system functions that are required to be disabled. These requirements exist to address vulnerabilities in the system resulting from accidental activation, malicious intentional activation, or intentional activation of the system function based on acceptance of risk by the Authorizing Official (AO). Requirements for a system function remain applicable even when the system function is disabled. Requirements pertaining to software that is not installed on the system, and which has no remaining configuration files on the system, may be evaluated as not applicable.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

The ESXi 5 vCenter STIG assumes familiarity with some common vSphere 5 concepts and terminology. Some of these concepts and terms are defined and explained in this document in order to facilitate uniform interpretation of the requirements.

3.1 The ESXi 5 vSphere Client

The vSphere Client is an application, included with the ESXi 5 vCenter Server, that enables management of a vSphere ESXi 5 vCenter Server installation. The vSphere Client provides an administrator with access to the key functions of vSphere without the need to access a vSphere server directly. The vSphere Client is the interface that must be used for all day-to-day ESXi 5 vCenter Server management tasks. It is a requirement that the vSphere Client first connect to the vCenter Server that the ESXi 5 vCenter Server is registered with, prior to conducting any day-to-day ESXi 5 vCenter Server management.

vCenter Server provides a single point of control in the datacenter. It provides essential datacenter services such as access control, performance monitoring, and configuration. It unifies the resources from the individual computing servers to be shared among virtual machines in the entire datacenter. It does this by managing the assignment of virtual machines to the computing servers and the assignment of resources to the virtual machines within a given computing server based on the policies that the system administrator sets. Computing servers continue to function even in the unlikely event that vCenter Server becomes unreachable (for example, if the network is severed). Servers can be managed separately and continue to run the virtual machines assigned to them based on the resource assignment that was last set. After connection to vCenter Server is restored, it can manage the datacenter as a whole again.

It is recommended that the vCenter Server be installed as a dedicated, physical machine, running a supported Microsoft Windows Operating System. The vCenter Server physical machine requires running a supported database, hosted on a separate physical machine, running a supported operating system. vCenter Server supports IBM DB2, Oracle, and Microsoft SQL Server databases.

Once an ESXi 5 vCenter Server is registered with and managed by a vCenter Server, it must never be logged in to and managed locally, as any changes to the server or its virtual machines will eventually be overwritten by the configuration registered with the vCenter Server.

3.2 The ESXi 5 Server Local Access and Lockdown Mode

ESXi 5 provides the ability to fully control all direct access to the host via ESXi 5 vCenter Server. After a host has been joined to vCenter Server 5, every direct communication interface with the host is configurable as an independent service in the Configuration tab for the host in the vSphere Client. This includes the following interfaces:

- DCUI (Direct Console User Interface)
 - ESXi 5 Shell
 - SSH

Each of these can be turned on and off individually through either the vSphere Client/vCenter interface or the DCUI.

When Lockdown Mode is enabled on the host, all direct remote access to the host is blocked, including:

- Any vSphere API client
- ESXi 5 Shell
- SSH

Even when Tech Support Mode is enabled, Lockdown Mode effectively overrides this by preventing any connection from succeeding. The only way to manage the host remotely is through vCenter Server. The interaction between the host and vCenter Server occurs through a special-purpose account called “vpxuser”; all other accounts, including root, can no longer connect remotely.

With Lockdown Mode enabled, the only direct access to the host that remains open is through the DCUI. The DCUI allows you to interact with the host locally using text-based menus. You can use the Direct Console User Interface to enable local and remote access to the ESXi 5 Shell. This provides a way to perform limited administrative tasks outside of vCenter Server. The DCUI can also turn off Lockdown Mode, disabling it without going through vCenter Server. This might be useful if vCenter Server is down or otherwise unavailable and users want to revert to direct management of the host. To log in to the DCUI in Lockdown Mode, however, the root password is required. No other user can log in, even if they have been granted an administrator role.

The requirement is that Lockdown Mode, including the DCUI, be enforced in ordinary, day-to-day operations but that it be temporarily disabled, as required, for a host if the need arises to interact with it directly. Note that Lockdown Mode does not apply to standalone ESXi 5.0 installations.

4. SOFTWARE PATCHING GUIDELINES

Maintaining the security of a vSphere 5 system requires frequent reviews of security bulletins. Many security bulletins and IAVM notifications mandate the installation of software patches to overcome noted security vulnerabilities. The SA will be responsible for ensuring the installation of all such patches. The ISSO will ensure the vulnerabilities have been remedied. FSO guidelines for remediation, including IAVMs, are as follows:

- Apply the applicable patch, upgrade to required software release, or remove the binary/application to remediate the finding.
- Or -
- The mode of the vulnerable binary may be changed to 0000 to downgrade the finding (for example, a CAT I finding may be downgraded to a CAT II).

SAs and ISSOs will regularly check the operating system's vendor and third-party application vendor websites for information on new vendor-recommended updates and security patches that are applicable to their site. All applicable vendor-recommended updates and security patches will be applied to the system. A patch is deemed applicable if the product is installed, even if it is not used or is disabled.

Operating system, virtual machine, and virtual network patching is accomplished through the use of three VMware products:

- vCenter Server
- VMware's Update Manager
- VMware's Update Manager Download Service/Server

The vCenter Server (vCS) is the central management system for ESXi 5. The VMware Update Manager (vUM) is responsible for updating the ESXi 5 server and VMs. The VMware vSphere Update Manager Download Service (vUMDS) is an optional module of the Update Manager. The vUMDS downloads software upgrades for virtual appliances, patch metadata, patch binaries, and notifications that would not otherwise be generally available to the Update Manager server.

Virtual installations of the vCenter Server (vCS) and Update Manager (vUM) will require manual management or additional vCS/vUM installations. Note that there is additional risk associated with manually updating a hypervisor (host), its virtual machines (VMs), guest operating systems (gOS), and/or applications. Manual updates will require the discrete identification of patch dependencies in order to ensure host, VM, and/or gOS compliance.

Virtual machine guest operating systems cannot be updated by the vCS, vUM, or vUMDS. A separate product, VMware Protect, centralizes patch management and asset inventory for Windows and third party applications for both virtual and physical machines. The details of VMware Protect are not discussed within the scope of the ESXi 5 vCenter STIG.

5. OPEN SOURCE SOFTWARE (OSS) USE

On October 16th 2009, DoD CIO provided clarifying guidance regarding Open Source Software (OSS), reminding the DoD to take advantage of the capabilities available in the Open Source community as long as certain prerequisites are met. The 2009 memo can be found online at: <http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf>

It reads:

“Software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software. In other words, OSS is software for which the source is “open.””

Additionally, per Section 2(d) of the 16 Oct 2009 DoD CIO memo:

“the use of *any* software without appropriate maintenance and support presents an information assurance risk. Before approving the use of software (including OSS), system/program managers, and ultimately Designated Approval Authorities (DAAs), must ensure that the plan for software support (e.g. commercial or Government program office support) is adequate for mission need.”