VMware® vSphere 5.1 Update 1c

Guidance Documentation Supplement

Evaluation Assurance Level: EAL2+

DOCUMENT VERSION: 0.5

vmware®

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
United States of America

Phone: +1 (650) 475-5000
http://www.vmware.com

VMware Security Advisories, Certifications and Guides
http://www.vmware.com/security/

Prepared for VMware by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America
Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

List of Tables

Table of Figures

1 Introduction

The Target of Evaluation (TOE) is the vSphere 5.1 Update 1c. The TOE is a software-only system, which provides an environment for hosting multiple virtual machines (VMs) on industry standard x86-compatible hardware platforms and provides management of virtual machines.

1.1 Purpose

This document provides guidance on the secure installation of the TOE for the Common Criteria EAL 2+ Evaluated Configuration. This document provides clarifications and changes to the VMware documentation and should be used as the guiding document for installation of the TOE in the Common Criteria evaluated configuration. The official VMware documentation should be referred to and followed only as directed within this guiding document.

Table 1 below lists the guidance documents relevant to the installation and configuration of the TOE.

Table 1 – TOE Guidance Documents

Document Name	Description
• VMware vSphere Installation and Setup, vSphere 5.1 Update 1 • VMware vSphere Upgrade Guide, vSphere 5.1 Update 1	Includes steps for the basic initialization and setup of the TOE.

.

Document Name	Description
• VMware vCenter Server Host Management Guide, Update 1, ESXi 5.1, vCenter 5.1 • VMware vSphere Virtual Machine Administration Guide, Update 1, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Host Profiles Guide, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Networking Guide, Update 1, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Storage Guide, Update 1, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Resource Management Guide, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Availability Guide, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Monitoring and Performance Guide, Update 1, vSphere 5.1, vCenter Server 5.1, ESXi 5.1 • VMware vSphere Troubleshooting, Update 1, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Examples and Scenarios Guide, Update 1, vSphere 5.1, vCenter Server 5.1, ESXi 5.1 • VMware vSphere Command-Line Interface Concepts and Examples, ESXi 5.1, vCenter Server 5.1 • VMware vSphere Getting Started with vSphere Command Line Interfaces, ESXi 5.1, vCenter Server 5.1 • VMware vSphere PowerCLI User's Guide, vSphere PowerCLI 5.1 Release 2 • Installing and Administering VMware vSphere Update Manager, Update 1, vSphere Update Manager 5.1	Contains detailed steps for how to properly configure and maintain the TOE.
• VMware® vSphere 5.1 Update 1c Security Target	Describes the TOE and identifies the Security Functional Requirements and Security Assurance Requirements it meets.

1.2 Target Audience

The audience for this document consists of the end-user, the VMware development staff, the Common Criteria Evaluation Laboratory staff, and the Government Certifier.

1.3 Evaluated TOE Configuration

Figure 1 depicts the evaluation configuration of the TOE, and contains the following previously undefined acronyms:

- OS – Operating System
- SSO – Single Sign-On

- vCSA – vCenter Server Appliance
- VUM – vSphere Update Manager

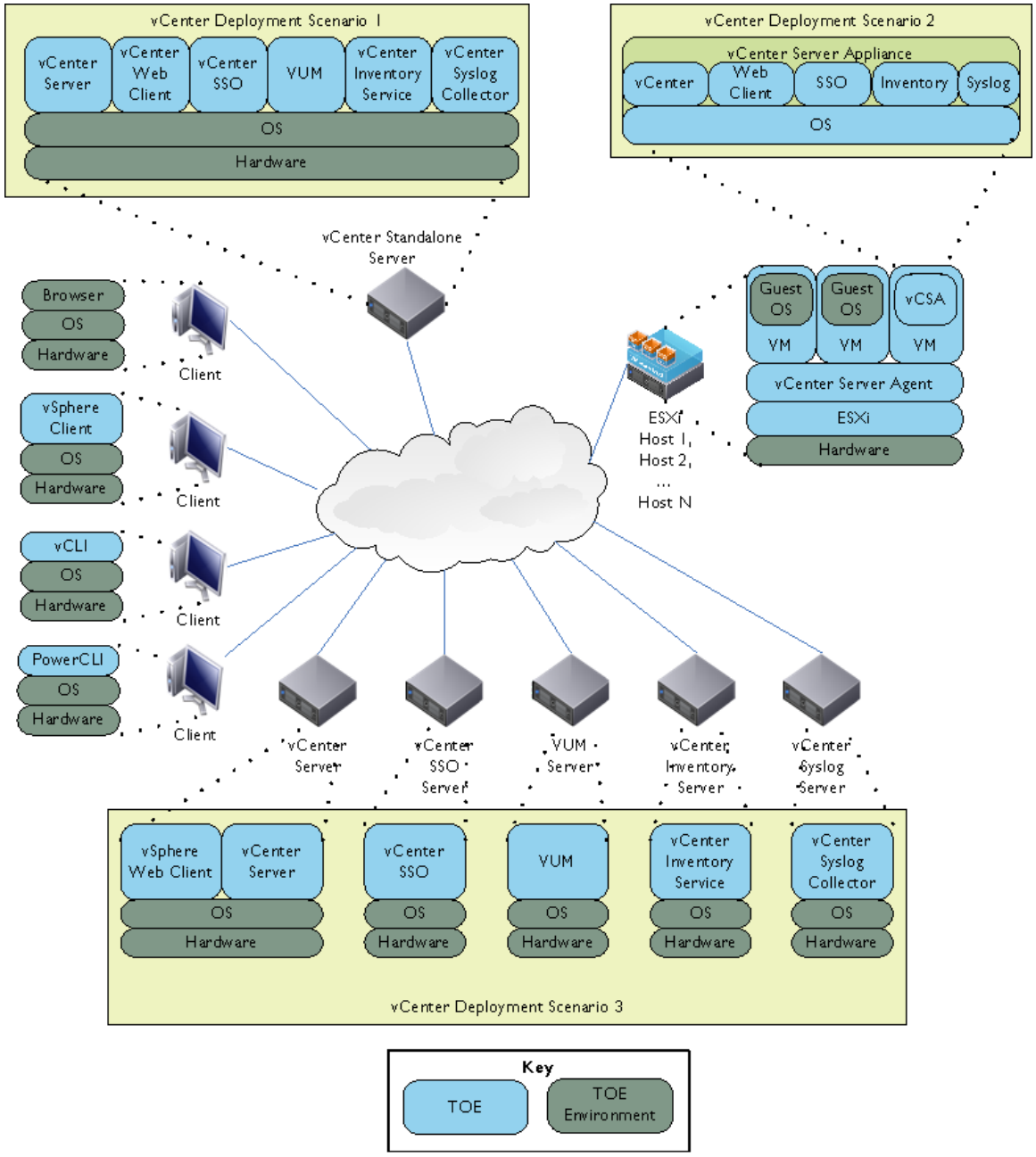

Figure 1 –Deployment Configuration of the TOE

Refer to *VMware® vSphere 5.1 Update 1c Security Target* for a complete description of the components in Figure 1.

.

1.4 Assumptions

The writers of this document assume the following:

- Users are non-hostile, appropriately trained, and follow all user guidance.
- The ESXi host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access. The client components will only connect to the server via networks behind the corporate firewall.
- The administrator is familiar with and knowledgeable on the documents listed above in Table 1 – TOE Guidance Documents.

2 Installation Procedure

This section describes the installation procedure notes and changes.

2.1 Introduction

This section provides guidance for how to properly install and setup the vCenter Server and setup ESXi as documented in the *vSphere Installation and Setup, vSphere 5.1 Update 1* document, along with additions and changes to the instructions contained therein, in order to allow the administrator to properly install and setup the evaluated configuration of the TOE.

Before the administrator begins the installation and setup, he should make certain that he has all the necessary components. The components needed to install and setup the TOE are listed in section 2 "System Requirements" of the *vSphere Installation and Setup, vSphere 5.1 Update 1* document.

The architecture of the evaluated configuration consists of the following components:

- ESXi 5.1 Update 1
- vCenter Server 5.1 Update 1c
- vCenter Inventory Service 5.1 Update 1c
- vCenter Single Sign-On 5.1 Update 1c
- vCenter Syslog Collector 5.1 Update 1c
- vSphere Update Manager 5.1 Update 1c
- vCenter Server Appliance 5.1 Update 1c
- vSphere Client 5.1 Update 1c
- vSphere Web Client 5.1 Update 1c
- vCLI 5.1 Update 1
- VMware PowerCLI 5.1 Release 2
- A supported web browser (Internet Explorer 9.0 or Firefox 20.0)

2.2 Secure Installation

Note: Throughout this section the reader will be instructed to read certain passages from referenced documents. Unless otherwise stated, such instructions refer to the documents listed in Table 1.

2.2.1 Phase 1 – Initial Preparation

The ESXi is a user-installable or OEM[1]-embedded virtualization layer that runs directly on industry standard x86-compatible hardware, which provides the environment for to host multiple virtual machines on one physical server. Virtual machines are the containers in which guest operating systems run. The OEM-Embedded version of ESXi is embedded as firmware on hardware. It is already installed by the hardware manufacturer and just needs to be setup by an administrator.

Sections 9 and 10 of the *vSphere Installation and Setup, vSphere 5.1 Update 1* document list the prerequisite steps before installing vCenter Server. Before beginning the install process for the vCenter Server, the administrator should ensure that he has the necessary system requirements and prerequisites needed. This information is provided in section 2 of the *vSphere Installation and Setup, vSphere 5.1 Update 1* document.

[1] OEM Original Equipment Manufacturer

.

It should be noted that when the vCenter Server is downloaded via VMware's website, a SHA-1[2] hash is provided to the customer on the product download page. To confirm the downloaded TOE's integrity, a SHA-1 hash utility should be used to calculate a SHA-1 hash for the downloaded TOE. If the calculated SHA-1 hash matches the SHA-1 hash provided on VMware's website, the TOE downloaded correctly. Should the TOE fail the SHA-1 hash procedure, the customer should discard the downloaded binaries and download the TOE and SHA-1 hash again and re-check the TOE's integrity with the SHA-1 hash. If the failure persists, the customer should contact VMware Customer Support.

2.2.2 Phase 2 – Installation of the TOE

There are several options for installing the ESXi component of the TOE. Detailed steps for these options can be found in sections 3, 4, 5, and 6 of the *vSphere Installation and Setup, vSphere 5.1 Update 1* document. Detailed steps for setting up the ESXi component of the TOE can be found in section 7 of the *vSphere Installation and Setup, vSphere 5.1 Update 1, vCenter Server 5.1* document.

Detailed steps for installing the vCenter Server component of the TOE can be found in section 11 of the *vSphere Installation and Setup, vSphere 5.1 Update 1* document. Post-installation options for the vCenter Server 5.1 can be found in section 12 of the *vSphere Installation and Setup, vSphere 5.1 Update 1* document .

2.2.3 Phase 3 – Post-Installation Setup of the TOE

The previous sections instruct the installation technician to install and configure a working ESXi and vCenter environment. In addition to that, the following sections provide documentation references that should be used to properly install/configure other components/features of the TOE post-installation.

2.2.3.1 vSphere Update Manager

To install and configure the vSphere Update Manager, follow the instructions provided in *Installing and Administering VMware vSphere Update Manager, Update 1, vSphere Update Manager 5.1*.

2.2.3.2 ESXi Firewall

To properly secure the ESXi management interface, section 3 of the *VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1* should be followed to restrict the allowed services available to hosts on the ESXi management network.

2.2.3.3 ESXi Lockdown

Section 5 of the *VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1* should be used to restrict direct access to the ESXi and force management by means of an authorized vCenter account. Section 11 provides instructions for limiting DCUI access in lockdown mode.

2.2.3.4 ESXi and vCenter Single-Sign On Authentication

Sections 6 and 7 of the *VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1* provide important information on configuring users and authentication for ESXi and vCenter SSO, including assigning of ESXi and vCenter privileges, and configuration of external repositories such as Active Directory for user authentication and authorization.

2.2.3.5 ESXi Log Management

Section 11 provides information on configuring syslog on ESXi hosts to use the vSphere Syslog Collector for centralized log storage, as well as locations of important log files.

The remaining user guidance should be reviewed to properly configure the VMware environment appropriately for the organization that is deploying the TOE. This includes configuring ESXi datastores for

[2] SHA-1 Secure Hash Algorithm 1

.

VM storage, host and VM administration, networking, scripted installation/configuration, high-availability, and performance.

- *VMware vSphere Storage Guide, Update 1, ESXi 5.1, vCenter Server 5.1*
- *VMware vCenter Server Host Management Guide, Update 1, ESXi 5.1, vCenter 5.1*
- *VMware vSphere Virtual Machine Administration Guide, Update 1, ESXi 5.1, vCenter Server 5.1*
- *VMware vSphere Host Profiles Guide, ESXi 5.1, vCenter Server 5.1*
- *VMware vSphere Networking Guide, Update 1, ESXi 5.1, vCenter Server 5.1*
- *VMware vSphere Resource Management Guide, ESXi 5.1, vCenter Server 5.1*
- *VMware vSphere Availability Guide, ESXi 5.1, vCenter Server 5.1*
- *VMware vSphere Monitoring and Performance Guide, Update 1, vSphere 5.1, vCenter Server 5.1, ESXi 5.1*
- *VMware vSphere Command-Line Interface Concepts and Examples, ESXi 5.1, vCenter Server 5.1*
- *VMware vSphere Getting Started with vSphere Command Line Interfaces, ESXi 5.1, vCenter Server 5.1*
- *VMware vSphere PowerCLI User's Guide, vSphere PowerCLI 5.1 Release 2*

3 Administrative Guidance

This section provides guidance for how to properly step through the configuration and maintenance instructions documented in the *vSphere Security, Update 1, ESXi 5.1 vCenter Server 5.1* guide, along with additions and changes to the instructions contained therein, in order to allow the administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should follow all the guidance documentation that is listed in Table 1 to ensure the proper installation, configuration, and management of the TOE Security functions.

3.1 Clarifications

The following sections describe clarifications to the administrative guidance of the TOE.

3.1.1 ESXi and vCenter Single Sign-On Passwords

This section provides guidance for how an authorized TOE user must create a password to be used for the ESXi Direct Console, vCenter Server Appliance Admin Console, vSphere Web Client, and vSphere Client interfaces. Section 6 of *VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1* provides important information on setting password requirements.

An authorized TOE user must use an appropriately complex password to access the TOE. Note that the password complexity enforcement capabilities vary between ESXi accounts and vCenter SSO accounts. These capabilities are outlined in the *VMware vSphere 5.1 Update 1c Security Target.*

To adequately protect the TOE from unauthorized use, administrators are required to enforce a password policy for local vCenter SSO accounts that contains the following rules:

- the password must have a minimum password length of eight characters
- the password must contain at least six alphabetic characters (from a set of 52, since uppercase and lowercase characters are differentiated)
- the password must contain at least one special character (from a set of 32)
- the password must not contain adjacent characters that are identical

It is also recommended to further restrict passwords to include at least one uppercase, one lowercase, and one numeric character. In addition, the TOE administrator should set a maximum lifetime and restrict password reuse in accordance with organizational password policies.

For non-local vCenter SSO identity sources, since passwords are generated and stored in the TOE Environment, Administrators must ensure that the Environment enforces this policy and that users abide by it.

On ESXi the password policy is enforced by the Pam Password Quality-Control module which is enabled by default. By default pam_passwdqc is configured as shown below.

```
pam_passwdqc.so retry=3 min=8,8,8,7,6
```

ESXi passwords may be a minimum length of six if using characters from each class (Uppercase, lowercase, numeric, and special), however it is recommended to use a minimum of eight characters. Refer to the *VMware vSphere Security Guide*, Chapter 6, section entitled “Password Requirements” on page 59 for details on ESXi password policy enforcement.

Administrators creating new ESXi user accounts must ensure that they follow the password policy described above when setting the initial password set for new users, and that they require the users to change their passwords on first login.

.

For local vCenter Server Appliance accounts (e.g. non-SSO), Administrators must take the necessary steps to change the default password and ensure that the password policy is enforced. During initial configuration of the vCenter Server Appliance, the default root password is pre-configured and does not follow the password policy. The default password should always be changed during the vCenter Server Appliance installation. Administrators are responsible for changing the default root password to follow the password policy during initial configuration.

For ease of reference, the following are the default service URLs and credentials for various vCenter components:

- **vCenter Server Appliance Admin Console**
  - **URL:** https://IPorDNS_of_Server:5480
  - **Username:** root
  - **Password:** vmware

- **vCenter Web Client Configuration**
  - **URL:** https://IPorDNS_of_Server:9443/admin-app
  - **Username:** root
  - **Password:** vmware

- **vCenter vSphere Web Client Access**
  - **URL:** https://IPorDNS_of_Server:9443/vsphere-client/
  - **Username:** root
  - **Password:** vmware

- **vCenter Single Sign On (SSO)**
  - **URL:** https://IPorDNS_of_Server:7444/lookupservice/sdk
  - **Windows default username:** admin@System-Domain
  - **Linux (Virtual Appliance) default username:** root@System-Domain
  - **Password:** specified during installation

3.1.2 Maintaining Supported Windows Operating System and Supported Database for vCenter

Because vCenter Server resides (runs) on a Windows-based host operating system, it is especially critical to protect this host operating system against vulnerabilities and attacks. The standard set of recommendations applies, as it would for any host operating system: install antivirus agents, spyware filters, intrusion detection systems, and any other security measures. Administrators must make sure to keep all security measures up-to-date, including the supported MS-Windows operating system and application of patches.

Administrators should consult Microsoft for Windows updates and patches, consult supported database vendors for database-specific updates and patches, and contanct software companies for updates to their respective products and any required datafiles (ie. Virus scan software and definition files)For host and guest Operating System compatibility, administrators should reference the VMware Compatibility Guide at:

- http://www.vmware.com/resources/compatibility/search.php .

For VMware product compatibility, administrators should reference the VMware Product Interoperability Matrix at:

- http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php?

3.1.3 Default Self-Signed Certificates

Client sessions with vCenter Server may be initiated from any vSphere API[3] client, such as vSphere Client, vSphere Web Client, and PowerCLI. By default, SSL[4] encryption protects these connections, but the default certificates generated at the time of install are not signed by a trusted certificate authority and, therefore, do not provide the authentication security one might need in a production environment.

These self-signed certificates are vulnerable to man-in-the-middle attacks, and clients receive a warning about them. If an administrator intends to use encrypted remote connections externally, he should consider purchasing a certificate from a trusted certificate authority or use his own security certificate for his SSL connections.

Self-signed certificates are automatically generated by vCenter Server during the installation process. The certificates should be treated as temporary signatures for initial installation purposes only.

Administrators should replace the default self-signed certificates with those from a trusted certification authority: either a commercial CA or an organizational CA.

For new certificate installations or existing certificate installations on vSphere, administrators should use the *vSphere Security, Update 1, ESXi 5.1 vCenter Server 5.1* guide, section 8. In addition, the following knowledge base article provides instructions for implementing CA signed SSL certificates:

- http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2034833

3.1.4 SSH[5]

ESXi has a standard SSH interface that SSH clients can connect to in order to execute command line functions securely. SSH is disabled by default, but should be enabled for secure command line operations. SSH can be enabled in the Direct Console User Interface. See the vSphere Security Guidance document, section "Use the Direct Console User Interface (DCUI) to Enable Access to the ESXi Shell" for instructions on how to enable SSH. In addition, configure the timeout value for the ESXi Shell to be 15 minutes. The timeout setting is the number of minutes that can elapse before a user must log in after the ESXi Shell is enabled. After the timeout period, if the user has not logged in, the shell is disabled.

If the user is logged in when the timeout period elapses, their session will persist. However, the ESXi Shell will be disabled, preventing other users from logging in.

3.1.5 Secure VMDK[6]

The ESXi hypervisor provides a secure VMDK deletion function[7] which allows an authorized administrator to securely overwrite the VMDK file where the VM's content was stored with zeroes. The zeroization function is not performed automatically at the time the VMDK file is deleted, and therefore an administrator must perform additional steps to ensure that the previous content of the VMDK file is securely overwritten *before the VMDK file is deleted from the ESXi datastore*. To securely erase a VMDK file, please refer to the procedure outlined in *VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1*, Chapter 11, section entitled "Delete VMDK Files Securely".

[3] Application Programming Interface
[4] Secure Sockets Layer
[5] Secure Shell
[6] Virtual Machine Disk
[7] Note: Secure VMDK deletion is an optional feature to be used at the administrator's discretion in scenarios where dictated by an organization's data destruction policies, when handling high-sensitivity VMs, and/or where disk zeroization functionality is not offered by the TOE environment.

4 Acronyms and Terms

This section defines the acronyms and terms.

Table 2 – Acronyms and Terms

Acronym	Definition
API	Application Programming Interface
CA	Certificate Authority
EAL	Evaluation Assurance Level
OEM	Original Equipment Manufacturer
OS	Operating System
SHA-1	Secure Hash Algorithm 1
SSH	Secure Shell
SSL	Secure Sockets Layer
TOE	Target of Evaluation
VCSA	vCenter Server Appliance
VM	Virtual Machine
VMDK	Virtual Machine Disk
VUM	VMware Update Manager

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com