VMware® vSphere 5.5 Update 2

Guidance Documentation Supplement

Evaluation Assurance Level: EAL2+

DOCUMENT VERSION: 0.3

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/

VMware Security Response Center
http://www.vmware.com/support/policies/security_response.html
security@vmware.com

VMware Security Certifications
http://www.vmware.com/security/certifications/

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 VMware vSphere 5.5 Update 2. 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 5.5 Update 2 • VMware vSphere Upgrade Guide, vSphere 5.5 Update 2	Includes steps for the basic initialization and setup of the TOE.
• VMware vCenter Server and Host Management Guide, Update 2, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Virtual Machine Administration Guide, Update 2, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Host Profiles Guide, Update 1, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Networking Guide, Update 2, vSphere 5.5, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Storage Guide, Update 2, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Security Guide, Update 2, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Resource Management Guide, Update 2, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Availability Guide, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Single Host Management Guide, Update 1, vSphere 5.5, ESXi 5.5 • VMware vSphere Monitoring and Performance Guide, Update 2, vSphere 5.5, vCenter Server 5.5, ESXi 5.5 • VMware vSphere Troubleshooting, Update 1, ESXi 5.5, vCenter Server 5.5 • VMware vSphere Command-Line Interface Concepts and Examples, ESXi 5.5 Update 1, vCenter Server 5.5 Update 1 • VMware Command-Line Management in vSphere 5 for Service Console Users, ESXi 5.5 Update 1 • VMware vSphere Getting Started with vSphere Command-Line Interfaces, ESXi 5.5 Update 1, vCenter Server 5.5 Update 1	Contains detailed steps for how to properly configure and maintain the TOE.

Document Name	Description
• VMware vSphere Web Services SDK Programming Guide, vSphere Web Services SDK 5.5 • VMware vSphere PowerCLI User's Guide, vSphere PowerCLI 5.8 Release 1 • Installing and Administering VMware vSphere Update Manager, Update 2, vSphere Update Manager 5.5	
• VMware vSphere 5.5 Update 2 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

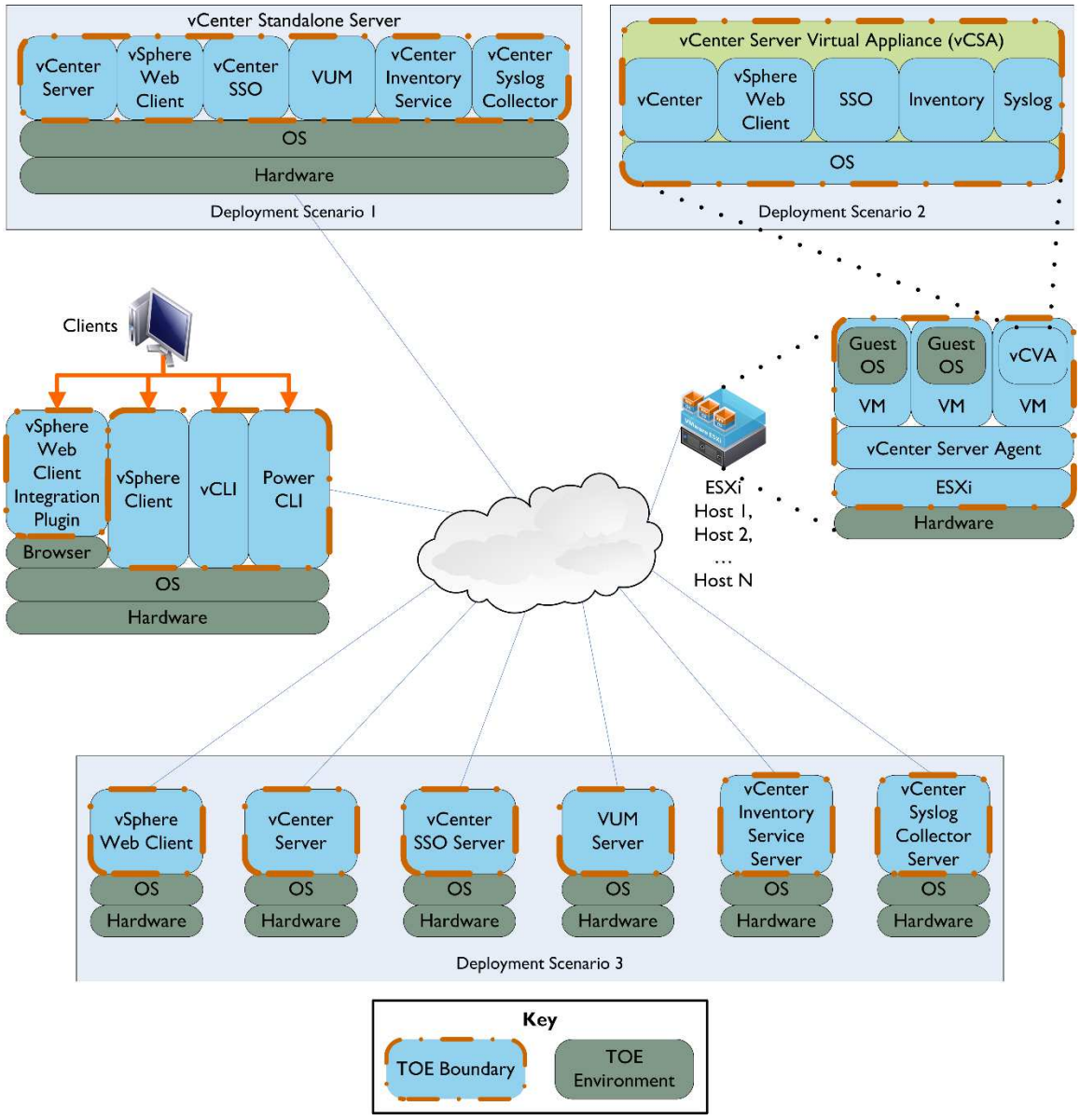

Figure 1 – Deployment Configuration of the TOE

Refer to *VMware vSphere 5.5 Update 2 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 and access is via secured networks (e.g., Virtual Private Networks).
- The administrators are 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 ESXi as documented in the *vSphere Installation and Setup, vSphere 5.5 Update 2* document, along with additions and changes to the instructions contained therein, in order to allow the administrators to properly install and setup the evaluated configuration of the TOE.

Before administrators begin the installation and setup, they should make certain that they have all the required software and hardware components. The components needed to install and setup the TOE are listed in section 2 "System Requirements" of the *vSphere Installation and Setup, vSphere 5.5 Update 2* document.

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

- ESXi 5.5 Update 2
- vCenter Server 5.5 Update 2
- vCenter Inventory Service 5.5 Update 2
- vCenter Single Sign-On 5.5 Update 2
- vCenter Syslog Collector 5.5 Update 2
- vSphere Update Manager 5.5 Update 2
- vCenter Server Virtual Appliance 5.5 Update 2a
- vSphere Client 5.5 Update 2
- vSphere Web Client 5.5 Update 2
- vSphere Web Client Integration Plugin 5.5 Update 2
- vSphere Command-Line Interface (vCLI) 5.5 Update 2
- VMware PowerCLI 5.8 Release 1
- A supported web browser:
    - Microsoft Internet Explorer: versions 8, 9 (64-bit only), and 10
    - Mozilla Firefox and Google Chrome: the latest version and the previous version at the time vSphere 5.5 Update 2 is released.

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 server hardware, which provides the environment for to host multiple virtual machines on one or more physical servers. Virtual machines are the containers in which guest operating system files are stored and run. The OEM-Embedded version of ESXi is embedded as part of the firmware on standards x86 compatible hardware. It is already installed by the hardware manufacturer and only needs to be setup by an administrator.

Section 3 of the *vSphere Installation and Setup, vSphere 5.5 Update 2* document lists the prerequisite steps before installing vCenter Server. Before beginning the install process for the vCenter Server, the

[1] OEM – Original Equipment Manufacturer

administrators should ensure that they have the necessary system requirements and prerequisites needed. This information is provided in section 2 of the *vSphere Installation and Setup, vSphere 5.5 Update 2* document.

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 6, 7, 8, and 9 of the *vSphere Installation and Setup, vSphere 5.5 Update 2* document. Detailed steps for setting up the ESXi component of the TOE can be found in section 8 of the *vSphere Installation and Setup, vSphere 5.5 Update 2, vCenter Server 5.5* document.

Detailed steps for installing the vCenter Server component of the TOE can be found in section 4 of the *vSphere Installation and Setup, vSphere 5.5 Update 2* document. Post-installation options for the vCenter Server 5.5 can be found in section 5 of the *vSphere Installation and Setup, vSphere 5.5 Update 2* document.

After installing the base vCSA software (*.ova file with build number 2063318), administrators must install a patch for the vCSA (*.iso file with build number 2170515). The patch update is made from an ISO file that the appliance reads from the virtual CD-ROM drive. Complete instructions on installing the patch can be found here:

- http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.upgrade.doc%2FGUID-445E55C7-F9D6-49CE-96AD-C3EA11FE3804.html

For more information on the patch release, refer to the following VMware Knowledge Base article:

- http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2091085

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 2, vSphere Update Manager 5.5.*

2.2.3.2 ESXi Firewall

To properly secure the ESXi management interface, section 7 of the *VMware vSphere Security Guide, Update 2, ESXi 5.5, vCenter Server 5.5* should be followed to restrict the allowed services available to hosts on the ESXi management network.

[2] SHA-1 – Secure Hash Algorithm 1

2.2.3.3 ESXi Lockdown

Section 7 of the *VMware vSphere Security Guide, Update 2, ESXi 5.5, vCenter Server 5.5* should be used to restrict direct access to the ESXi and force management by means of an authorized vCenter account. Section 7 also provides instructions for limiting Direct Console User Interface (DCUI) access in lockdown mode.

2.2.3.4 ESXi and vCenter Single-Sign On Authentication

Section 2 of the *VMware vSphere Security Guide, Update 2, ESXi 5.5, vCenter Server 5.5* provides 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 7 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.

2.2.3.6 vMotion and Storage vMotion

The section "Migration with vMotion" in Chapter 12 of *VMware vCenter Server and Host Management Guide, Update 2, ESXi 5.5, vCenter Server 5.5* provides requirements for and guidance on performing VM data migrations while the VM is running. To migrate a running VM's disk files as well, see "Migration with Storage vMotion" in the same chapter.

2.2.3.7 Traffic Filtering and Quality of Service (QoS) Tagging

For guidance on configuring traffic filtering and QoS marking/tagging, see the section "Traffic Filtering and Marking Policy" in Chapter 5 of *VMware vSphere Networking Guide, Update 2, ESXi 5.5, vCenter Server 5.5*.

2.2.3.8 Link Aggregation Control Protocol (LACP)

To use LACP on a vSphere Distributed Switch 5.5 to connect ESXi hosts to physical switches using dynamic link aggregation, see the section "LACP Support on a vSphere Distributed Switch" in Chapter 3 of *VMware vSphere Networking Guide, Update 2, ESXi 5.5, vCenter Server 5.5*.

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

- *VMware vSphere Storage Guide, Update 2, ESXi 5.5, vCenter Server 5.5*
- *VMware vCenter Server and Host Management Guide, Update 2, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere Virtual Machine Administration Guide, Update 2, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere Host Profiles Guide, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere Networking Guide, Update 2, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere Resource Management Guide, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere Availability Guide, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere Monitoring and Performance Guide, Update 2, vSphere 5.5, vCenter Server 5.5, ESXi 5.5*
- *VMware vSphere Command-Line Interface Concepts and Examples, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere Getting Started with vSphere Command Line Interfaces, ESXi 5.5, vCenter Server 5.5*
- *VMware vSphere PowerCLI User's Guide, vSphere PowerCLI 5.8 Release 1*

3 Administrative Guidance

This section provides guidance for how to properly step through the configuration and maintenance instructions documented in the *vSphere Security, Update 2, ESXi 5.5 vCenter Server 5.5* guide, along with additions and changes to the instructions contained therein, in order to allow the administrators to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrators 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 4 of *VMware vSphere Security Guide, Update 2, ESXi 5.5, vCenter Server 5.5* 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 5.5 Update 2 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 one uppercase character
- the password must contain one lowercase character
- the password must contain one numeric digit
- the password must contain at least one special character (from a set of 32)
- the password must not contain adjacent characters that are identical
- password should only use visible ASCII[3] characters

In addition, the TOE administrators 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

[3] ASCII – American Standard Code for Information Interchange

to the *VMware vSphere Security Guide*, Chapter 4, section entitled "Password Requirements" 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 Setting Timeouts for Idle Sessions

An idle timeout is the amount of time that can elapse before the user is logged out of an idle interactive TOE session. Administrators should configure these timeouts. Some are disabled by default, which means a session remains open indefinitely even if it is not being used.

- **ESXi Shell:** See "Setting Timeouts for the ESXi Shell" in *Command-Line Management in vSphere 5 for Service Console Users*.
- **ESXi SSL connections:** See "Configure SSL Timeouts" in Chapter 7 of *vSphere Security*.
- **vSphere Web Client:** See "Configure the vSphere Web Client Timeout Value" in Chapter 3 of *vCenter Server and Host Management*.

3.1.3 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 (e.g., 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?

3.1.4 Default Self-Signed Certificates

Client sessions with vCenter Server may be initiated from any vSphere API[4] client, such as vSphere Client, vSphere Web Client, and PowerCLI. By default, SSL[5] 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 administrators intend to use encrypted remote connections externally, they 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 2, ESXi 5.5 vCenter Server 5.5* guide, section 3. 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

3.1.5 SSH[6]

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, Update 2, ESXi 5.5 vCenter Server 5.5* document, section "Use the 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.

[4] API – Application Programming Interface
[5] SSL – Secure Sockets Layer
[6] SSH – Secure Shell

3.1.6 Secure VMDK[7]

The ESXi hypervisor provides a secure VMDK deletion function[8] which allows authorized administrators 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 administrators 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 Storage Guide, Update 2, ESXi 5.5, vCenter Server 5.5*, Chapter 27, section entitled "Initializing a Virtual Disk".

3.1.7 Networking

When configuring the TOE network, the management components (including the vCenter server network interface and the ESXi management vNIC) must be attached to an isolated network such that all TOE management network is free from interference from untrusted entities.

3.1.8 Disabling Ciphers

The following instructions should be followed to disable weak or sunset ciphers on various ports.

3.1.8.1 Procedure to disable RC4[9] on vCSA 5.5 Update 2 port 12443 (Appliance):

1. At the vCSA console, press return and log in as the root user.
2. Change to the VMware vSphere Web Client configuration directory:

   ```
   cd /usr/lib/vmware-logbrowser/conf/
   ```

3. Make a copy of the server config file as a backup:

   ```
   cp logbrowser.properties logbrowser.properties-backup
   ```

4. Open the logbrowser.properties configuration file with the vi text editor:

   ```
   vi logbrowser.properties
   ```

5. In the log browser.properties file, search for the "exclude-ciphers=" directive and **add** the following to the "exclude cipher" list:

   "ECDHE-RSA-RC4-SHA"

6. Save and exit the configuration file.
7. Either stop and start the "vSphere Log Browser" service from the Services sections of the vCenter Appliance admin interface (<vCSA host / IP>:5480), or restart the appliance.

3.1.8.2 Procedure to disable RC4 on vCenter Windows 5.5 Update 2 port 12443 (Windows):

1. Logon to Windows Server as administrator.

[7] VMDK – Virtual Machine Disk
[8] 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.
[9] RC4 – Rivest Cipher 4

2. Open command prompt.

3. Change to the following directory:

   C:\Program Files\VMware\Infrastructure\vSphereWebClient\logbrowser\conf

4. Make a copy of the logbrowser.properties file:

   ```
   copy logbrowser.properties to logbrowser.properties-backup
   ```

5. Open web server configuration file with txt editor:

   ```
   notepad logbrowser.properties
   ```

6. In the logbrowser.properties file, search for the "exclude-ciphers=" directive and **add** the following cipher to the excluded cipher list:

   "TLS_ECDHE_RSA_WITH_RC4_128_SHA"

7. Save and exit the configuration file.

8. Either stop and start the "vSphere Log Browser" service from the Windows admin control panel or restart Windows system.

3.1.8.3 Procedure to disable Camellia cipher with ESXi 5.5 Update 2 port 5989:

1. At the ESXi DCUI, log on with admin account.

2. Verify the ESXi Shell is enabled, if not "Enable" It.

3. Switch to shell prompt by pressing the key combination "Alt-F1". (FYI: The key combination "Alt-F2" switches the console back to the DCUI)

4. At the shell log on prompt, log in as root user.

5. Open the sfcb configuration file with the vi text editor:

   ```
   vi /etc/sfcb/sfcb.cfg
   ```

6. Add the following line at the bottom of the file:

   sslCipherList:HIGH:!CAMELLIA256:!CAMELLIA128

7. Save and exit text editor.

8. Restart sfcbd service:

   ```
   /etc/init.d/sfcbd-watchdog restart
   ```

9. It is recommended to restart ESXi for the updated configuration info to be captured to config files and persist. If power is removed versus an organized shutdown, this configuration change will not persist.

3.1.8.4 Procedure to disable RC4 on vCSA 5.5 Update 2 port 9443 (Appliance):

1. At the vCSA console, press return and log in as the root user.
2. Change to the VMware vSphere Web Client configuration directory:

   ```
   cd /var/lib/vmware-vsphere-client/server/config
   ```

3. Make copy of server config file as a backup:

   ```
   cp tomcat-server.xml tomcat-server.xml-backup
   ```

4. Open the web server configuration file with the vi text editor:

   ```
   vi tomcat-server.xml
   ```

5. In the tomcat-server.xml file, search for the "ciphers=" directive and **remove** the following from the cipher list:

   "SSL_RSA_WITH_RC4_128_SHA"

6. Save and exit the configuration file.
7. Either stop and start the "vSphere Web Client" service from the Services sections of the vCenter Appliance admin interface (<vCSA host / IP>:5480), or restart the appliance.

3.1.8.5 Procedure to disable RC4 on vCenter Windows 5.5 Update 2 port 9443 (Windows):

1. Logon to Windows Server as administrator.
2. Open command prompt.
3. Change to the following directory:

   C:\Program Files\VMware\Infrastructure\vSphereWebClient\server\configuration\

4. Make copy of tomcat-server.xml file:

   ```
   copy tomcat-server.xml tomcat-server-backup.xml
   ```

5. Open web server configuration file with txt editor:

   ```
   notepad tomcat-server.xml
   ```

6. In the tomcat-server.xml file, search for the "ciphers=" directive and **remove** the following from the cipher list:

   "SSL_RSA_WITH_RC4_128_SHA"

7. Save and exit the configuration file.

   Either stop and start the "vSphere Web Client" service from the Windows admin control panel or restart Windows.

4 Acronyms

Table 2 defines the acronyms used in this document.

Table 2 – Acronyms

Acronym	Definition
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
DCUI	Direct Console User Interface
EAL	Evaluation Assurance Level
LACP	Link Aggregation Control Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
QoS	Quality of Service
RC4	Rivest Cipher 4
SHA-1	Secure Hash Algorithm 1
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
TOE	Target of Evaluation
vCLI	vSphere Command-Line Interface
vCSA	vCenter Server Appliance
VM	Virtual Machine
VMDK	Virtual Machine Disk
VUM	vSphere Update Manager

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