VMware® vSphere 5.1 Update 1c

Security Target

Evaluation Assurance Level: EAL2+

DOCUMENT VERSION: 1.1

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

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

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the VMware® vSphere 5.1 Update 1c, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only system which provides the environment to run multiple virtual machines (VMs) on industry standard x86-compatible hardware platforms and performs the management of these virtual machines.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	VMware, Inc. VMware® vSphere 5.1 Update 1c Security Target
ST Version	Version 1.0
ST Author	Corsec Security Inc.
ST Publication Date	12/19/2013

TOE Reference	VMware® vSphere 5.1 Update 1c: • ESXi 5.1 Update 1 (build 1065491) • vCenter Server 5.1 Update 1c (build 1364037) • vCenter Inventory Service 5.1 Update 1c (build 1364037) • vSphere Client 5.1 Update 1c (1364039) • vSphere Web Client 5.1 Update 1c (build 1364037) • vSphere Update Manager 5.1 Update 1c (build 1364037) • vCenter Single Sign-On 5.1 Update 1c (build 1364037) • vCenter Server Virtual Appliance 5.1 Update 1c (build 1364079) • vSphere Command-Line Interface (vCLI) 5.1 Update 1 (build 1060453) • VMware PowerCLI 5.1 Release 2 (build 1012425)
FIPS[1] 140-2 Status	Refer to Table 19 for the CAVP certificate numbers for all the VMware® vSphere 5.1 Update 1c cryptographic providers.

[1] FIPS – Federal Information Processing Standard

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

One of VMware, Inc.'s core businesses is virtualization software. Specifically, VMware offers its virtualization solution which runs on industry standard x86-compatible hardware platforms. The basic concept of virtualization technology is that a single physical hardware system is used to host multiple logical or "*virtual*" machines (VMs). A host computer runs a layer of software called "*hypervisor*" that enables the system administrators to create virtual machines on which the guest operating system (OS) can be installed. In VMware's virtualization solution, the following components are the essential building blocks that make up the virtualized computing environment:

- A host machine – an x86 compatible hardware.
- Hypervisor (ESXi) – Enterprise class virtualization software from VMware that is installed on the host. The ESXi software provides the environment to run and manage virtual machines on the host.
- The virtual machines themselves, on the host machine.
- The guest operating system that is installed on the virtual machine.

The four components described above make a very basic virtualized computing environment. That is, a single ESXi provides the environment for one or more virtual machines. In a typical enterprise-level deployment, the virtualized computing environment has multiple physical hypervisor (ESXi) hosts running many virtual machines. To effectively manage this type of environment, VMware offers the following software products and hardware support:

- vCenter Server – A software service that provides centralized administration for connected ESXi hosts. The vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESXi hosts). vCenter Server also includes an instance of vCenter Single Sign-On (SSO). Beginning in vSphere v5.1, vCenter user authentication and authorization is handled by vCenter SSO.
- vSphere Update Manager (VUM) – A software service that is used to apply patches and updates across ESXi hosts and select managed virtual machines.
- vSphere Client – Microsoft Windows® based interface for creating, managing, and monitoring virtual machines, their resources, and their host (ESXi). It is also an interface to monitor, manage, and control the vCenter Server. The vSphere Client is installed on a Windows machine and is used to connect to an ESXi host or vCenter Server.
- vSphere CLI[2] (vCLI) – The vCLI is a command-line application which allows scriptable management of ESXi hosts from a machine with network access to the ESXi host. The vCLI command set also includes a set of commands specifically for vCenter Server.
- vSphere Web Client – The vSphere Web Client is a web based client through which the end-user can perform virtual machine management and obtain console access to virtual machines.

[2] CLI – Command Line Interface

Functionally equivalent to the vSphere Client, vSphere Web Client works directly with a vCenter Server to manage ESXi under vCenter Server Management.

- vCenter Syslog Collector – The vCenter Syslog Collector is a vCenter Support Tool that provides for centralized logging management of the ESXi hosts. The vCenter Syslog Collector provides a unified architecture for system logging and enables network logging and centralized storage of logs from multiple hosts.

- VMware PowerCLI - The vSphere PowerCLI is a robust, Windows-based CLI tool for automating all aspects of vSphere management including host, network, storage, virtual machine, guest OS and more. It is distributed as a Windows PowerShell snap-in, with more than 300 PowerShell cmdlets, along with built-in documentation and samples. The PowerCLI integrates seamlessly with Windows and .NET and facilitates working with the vSphere API.

- vCloud Networking and Security (vCNS) – vCNS is a security product for protecting virtualized datacenters from attacks and misuse. vCNS utilizes purpose-built virtual appliances and services essential for protecting virtual machines as well as physical machines. vCNS can be configured through a web-based user interface, a vSphere Client plug-in, vCenter Server snap-in, a command line interface (CLI), and REST[3] API[4].

- vCenter Operations Manager – vCenter Operations Manager is a suite of virtual appliances that perform analytics and provide visibility into a vSphere deployment to effectively manage health, efficiency, and compliance. vCenter Operations Manager is managed through a separate web-based user interface.

- Intel Trusted Platform Module/Trusted Execution Technology (TPM/TXT) integration – The ESXi hypervisor provides support for hardware-based TPMs to compare measurements of the VMkernel, modules, drivers, and boot parameters against values stored in the TPM. These measurements are exposed via the vSphere API, which allows third-party solutions to provide tamper detection capabilities.

The relationship between the vCenter Server and the hypervisor (ESXi) hosts is a one-to-many relationship: A single vCenter Server managing a multiple number of ESXi hosts, and all the virtual machines that reside on those hosts. Also, it should be noted that while it is possible to install and run the vCenter Server and VUM on the same physical machine, in most cases for flexibility and scaling they are installed and run on different machines.

The use of the vCenter Server in managing the hypervisor (ESXi) also allows the following system management services:

- VMware Data Recovery – provides simple, cost effective, agentless backup and recovery for virtual machines.

- VMware Distributed Resource Scheduler (DRS) – monitors available resources and intelligently allocates resources among VMs based on a pre-defined set of rules.

- VMware Fault Tolerance – configures two VMs in parallel to provide continuous availability, without any data loss or downtime, to any application, in the event of hardware failures.

[3] REST – Representational State Transfer
[4] API – Application Programming Interface

- VMware HA[5] – enables automatic restart of virtual machines on a different physical server within a cluster with spare capacity, if the hosting server fails.

- VMware Hot Add – enables CPU[6] and memory to be added to virtual machines when needed without disruption or downtime.

- VMware Host Profiles – standardizes and automates configuration of the hypervisor (ESXi) hosts by capturing a reference host configuration and ensuring compliance for resource, networking, storage and security settings.

- VMware vCenter Linked Mode – enables joining multiple vCenter Server systems with replicated roles, permissions, and licenses along with search capabilities across all linked vCenter Server inventories. When a vCenter Server is connected to other vCenter Server systems using Linked Mode, the user can connect to that vCenter Server system and view and manage the inventories of all the vCenter Server systems that are linked. Linked Mode uses Microsoft Active Directory (AD) Lightweight Directory Services (LDS)[7] to store and synchronize data across multiple vCenter Server systems. AD LDS is installed automatically as part of vCenter Server installation. Each AD LDS instance stores a portion of the data from all of the vCenter Server systems in the group, including information about user accounts, roles, and licenses. This information is regularly replicated across all of the AD LDS instances in the connected group to keep them in sync. The remainder of the information is accessed directly from each vCenter Server instance without having to connect to each individual vCenter Server in a Linked Mode configuration. This is mostly VM and Host information data.

- VMware VMotion – enables the live migration of running VMs from one ESXi host to the other with zero down time. VMotion is capable of migrating virtual machines between ESXi hosts, between legacy ESX hosts, and between ESX and ESXi hosts.

- VMware vStorage Thin Provisioning – provides dynamic allocation of storage capacity and thereby reduces storage consumption.

- VMware vNetwork Distributed Switch – provides a network switch which can span multiple ESXi hosts, enabling simplified on-going administration and control of virtual machine networking across hosts. It also enables third party distributed virtual switches such as the Cisco Nexus 1000v to be used in VMware's virtual networking environment.

- Stateless ESXi – provides central storage and management of ESXi images and host profiles for rapid deployment to hosts without local storage. Upon host startup, a pre-determined ESXi software image and configuration profile is network loaded and configured.

- Client USB[8] – simplifies connecting the VMs to USB devices on the ESXi host machine. This also allows USB smartcards to connect to VMs.

- vSphere Management Assistant (vMA) – A preconfigured software virtual appliance that is used to run scripts and agents to assist with managing ESXi and vCenter Server systems. In addition it is

[5] HA – High Availability
[6] CPU – Central Processing Unit
[7] In previous versions of Windows, AD LDS was Microsoft Active Directory Application Mode (ADAM). In Windows Server 2008, ADAM has been renamed AD LDS.
[8] USB – Universal Serial Bus

bundled with the vSphere CLI (vCLI) for command-line ESXi host and vCenter Server management.

The vCenter Server, vSphere Client, VUM, together with ESXi are the major components of a virtualization suite offered by VMware, Inc. called VMware vSphere 5.1 Update 1.

Components of the VMware vSphere virtualization suite are backwards compatible with properly licensed components of previous VMware virtualization suites; VMware vSphere 4.x and VMware Virtual Infrastructure 3.x (VI3). Prior virtualization suite management components are not forward compatible with vSphere 5.1 Update 1 suite components; however, vSphere 5.1 Update 1 can directly manage 4.x and 3.x suite components. Backwards compatibility includes management of ESX and ESXi hosts from VMware vSphere 4.x and VMware VI3 virtualization suites.

The minimum hardware and software requirements for the major components of VMware vSphere 5.1 Update 1 are located at the following web page:

- http://www.vmware.com/resources/compatibility/search.php?action=base&deviceCategory=server

It should be noted, as indicated in Figure 1 below, the hardware and software requirements for VMware vSphere are outside the scope of evaluation, and are considered to be part of the IT environment.

Supported AMD and Intel 64 bit processors for the ESXi host are described on VMware's Hardware Compatibility List (HCL). For the most recent listing of certified systems, storage and Input/Output (I/O) devices for the VMware ESXi, see the following web page:.

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

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is a system that can provide an environment to host multiple virtual machines on industry standard x86-compatible hardware platforms (64-bit) and provides the management of these virtual machines. Figure 1 shows a sample deployment configuration of the TOE:

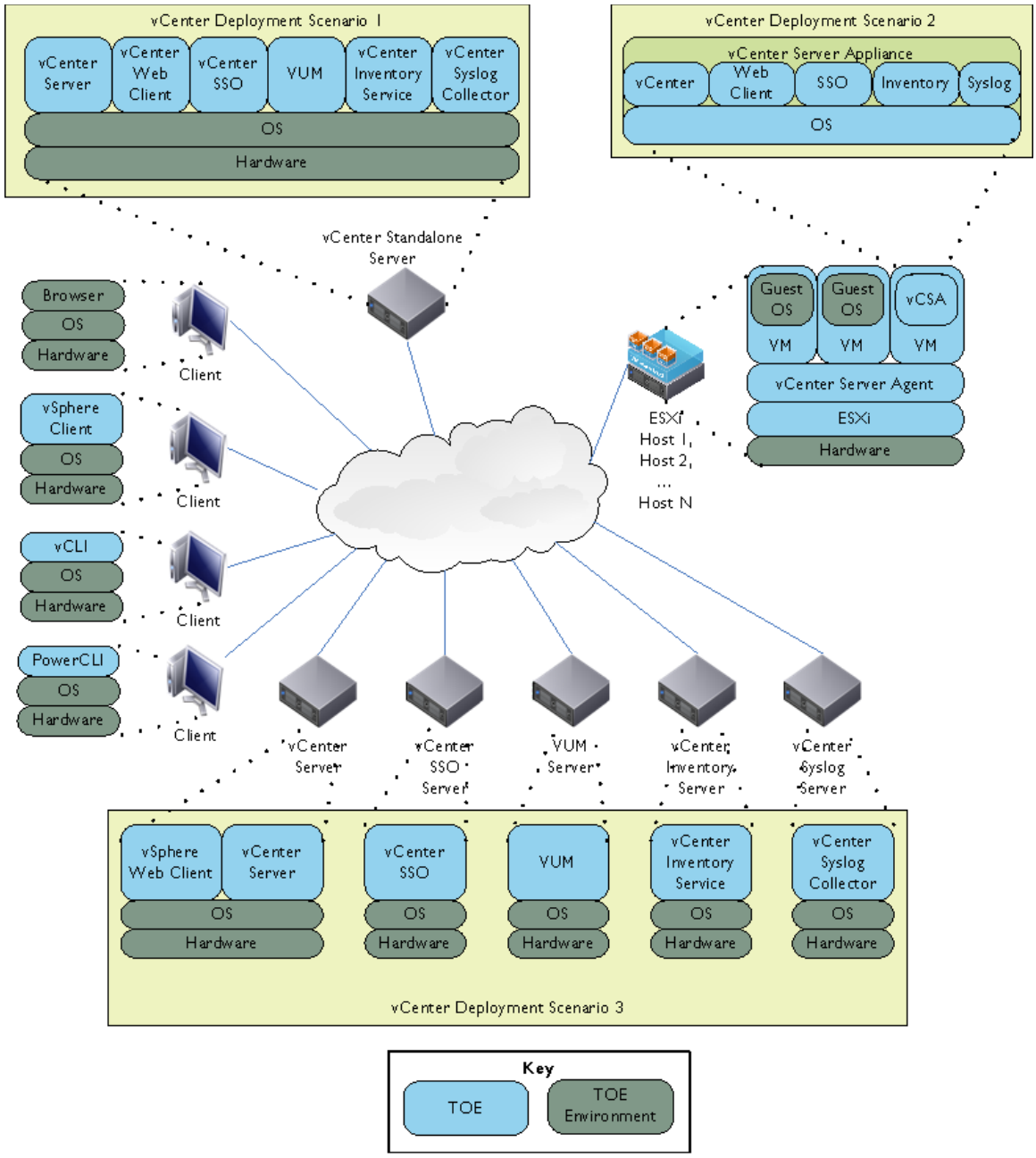

Figure 1 – Sample Deployment Configuration of the TOE

The sample deployment of the TOE shown in Figure 1 is composed of at least one instance of each major TOE component. For vCenter, three deployment scenarios exist:

- vCenter Standalone, which includes the vCenter Server, Web Client, Inventory Service, SSO, VUM, and Syslog Collector (Deployment #1);
- vCenter VA, which includes all vCenter components (except VUM) with a pre-packaged virtual appliance on an ESXi host (Deployment #2);
- and a distributed deployment with each service running on its own dedicated hardware (Deployment #3).

Other major components include ESXi, vCenter Server Agent, vSphere Client, vCLI, PowerCLI and vSphere Web Client.

1.4.1 Brief Description of the Components of the TOE

The following paragraphs provide a brief description of the components of the TOE.

1.4.1.1 vCenter Server

The vCenter Server provides centralized management for ESXi and is distributed as a service for Windows. It may be installed on a dedicated host, together on the same host with other vCenter components, or as part of a pre-packaged Virtual Appliance (VA). Through the vCenter Server, an administrator can configure an ESXi, which includes viewing and managing the networking, data storage, security settings, user privileges and various object permissions. The vCenter Server also provides the provisioning of virtual machines on the ESXi. For example, virtual machines can be created, configured, cloned, and relocated.

The vCenter Server installed as part of a pre-packaged VA is called the vCenter Server Appliance. It provides identical functionality to the vCenter Server, and in addition includes an instance of vSphere Syslog Collector, vCenter Inventory Service, vSphere Web Client, and vCenter SSO. The OS included in the vCenter Server Appliance is SUSE Linux Enterprise Server (SLES) for VMware, which is based on SLES 11 Service Pack 2. In this VA configuration, the vCenter Server communicates with ESXi via the vCenter Server Agent (VPXA) located on the ESXi host. The confidentiality and integrity of this communication is protected using the Transport Layer Security (TLS) protocol and certificates which are system-generated or provided by the end-user. The vCenter Server's TLS implementation uses algorithms that are Cryptographic Algorithm Validation Program (CAVP) validated against FIPS 140-2 requirements.

1.4.1.1.1 vCenter Server Access Methods

The vCenter Server can be accessed by users via two different methods: by using the standalone vSphere Client software or, by using the vSphere Web Client via a web browser.

1.4.1.1.1.1 vSphere Client

Users connect to the vCenter Server via the vSphere Client either locally (on the same machine as the vCenter Server) or remotely, from a workstation running the vSphere Client software. In addition, the vSphere Client is used to manage ESXi hosts well as VMs. Communication with the vSphere Client is protected using TLS.

1.4.1.1.1.2 vCLI

The vCLI allows administrators to run common system administration tasks and perform scripted automation against ESXi systems from a management workstation with network access to the ESXi hosts. vCLI commands may also be run against a vCenter Server to target an ESXi host managed by the vCenter Server.

1.4.1.1.1.3 PowerCLI

Similar to the vCLI, the PowerCLI provides a set of PowerShell cmdlets used for scripting vCenter and ESXi management tasks from any supported Windows operating system.

1.4.1.1.1.4 vSphere Web Client

Users connect to the vCenter Server via the vSphere Web Client through a web browser. The vSphere Web Client interface is a Java-based web application plugin using standard OSGI[9] format. The vSphere Web Client is used to manage ESXi hosts and hosted VMs. Communication between the vSphere Web Client and another VMware component is protected using Secure HyperText Transfer Protocol (HTTPS), as shown in Figure 2.

1.4.1.1.2 vCenter Inventory Service

The vCenter Inventory Service contains information about the configuration and status of all ESXi hosts under management and each of the host's virtual machines. It also stores management information for the ESXi host, including the following:

- Scheduled tasks: a list of activities and a means to schedule them.
- Alarms: a means to create and modify a set of alarms that apply to an organizational structure and contain a triggering event and notification information.
- Events: a list of all the events that occur in the vCenter Server environment. Audit data are stored as events.
- Permissions: a set of user and vCenter Server object permissions.

1.4.1.2 vCenter SSO

vCenter SSO provides a centralized repository of identity information for a VMware deployment, giving administrators a single point of authentication to multiple vCenter instances. vCenter SSO is installed along with vCenter Server, or as a standalone component, and can be configured to use a combination of local database, Active Directory (AD), OpenLDAP, or local OS accounts as its identity sources.

1.4.1.3 vSphere Update Manager

The vSphere Update Manager (VUM) provides automated patch management for the ESXi hosts and its Virtual Machines. VUM scans the state of the ESXi host, and compares it against a default baseline, or against a custom dynamic or defined static baseline set by the administrator. It then invokes the update and patching mechanism of ESXi to enforce compliance to mandated patch standards. VUM is also able to automatically patch and update the select Guest Operating Systems being run as Virtual Machines. However, guest operating systems are not part of this TOE and as such the patching of those operating systems is outside the scope of this evaluation.

After performing a scan against the ESXi host, VUM accesses VMware's website and downloads a key and other metadata about the patches via HTTPS. It then sends the key to an ISP[10] server, which accesses the appropriate server to retrieve updates. VUM then downloads the patches to be installed on the TOE via HTTP[11], and uses a certificate to verify the signature on the downloaded binary, thereby validating the binaries authenticity and integrity. VUM stores the binary locally on the vCenter Server machine. Once instructed by VUM, ESXi then pulls the appropriate updates and patches from VUM's database via HTTP, using a key and signature to verify the downloaded binaries.

[9] OSGI – Open Services Gateway Initiative Alliance is an open standards organization founded in March 1999 that originally specified and continues to maintain the OSGI standard.
[10] ISP – Internet Service Provider; this ISP provides access to patch and update download servers.
[11] HTTP – HyperText Transport Protocol

1.4.1.4 vCenter Syslog Collector

The vCenter Syslog Collector provides for centralized logging management of the ESXi hosts. The vCenter Syslog Collector provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts. It may be installed along with the vCenter Server, or as a standalone component on a dedicated host.

1.4.1.5 ESXi

ESXi is a user-installable or OEM-embedded virtualization layer that runs directly on industry standard x86-compatible hardware, providing an environment where multiple virtual machines can be hosted on one physical server. Virtual machines are the containers in which guest operating systems run. By design, all VMware virtual machines are isolated from one another. Virtual machine isolation is imperceptible to the guest operating system. Even a user with System Administrator privileges on a virtual machine's guest operating system cannot breach this layer of isolation to access another virtual machine. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.

The virtual Symmetric Multi-Processing (vSMP) feature enables a single virtual machine to use multiple physical processor cores simultaneously. The number of virtual processors and processor cores are configurable for each virtual machine.

ESXi also provides a robust virtualized networking mechanism known as "VMware virtual networking". In the VMware virtual networking scheme, ESXi virtualizes the physical network to which it is connected and thus provides virtual switches called "vSwitches" to VMs. This allows properly configured virtual machines to connect to and communicate via the physical network as if they were directly connected to it.

A vSwitch works like a physical Ethernet switch. It detects which virtual machines and physical network interfaces are logically connected to each of its virtual ports and uses that information to forward traffic to the correct destination. The vSwitch is implemented entirely in software as part of ESXi. ESXi vSwitches also implement VLANs[12], which are an IEEE[13] standard networking scheme with specific tagging methods that allow routing of packets to only those ports that are part of the VLAN. The VLAN implementation in ESXi allows the protection of a set of virtual machines from accidental or malicious intrusions.

In addition to offering the vSwitch capability, ESXi also provides an additional choice for VMware virtual networking with the vNetwork Distributed Switch (vDS). Whereas the vSwitch, also known as the Standard Switch in VMware virtual networking, is implemented on a single ESXi host, the vDS spans multiple ESXi hosts. In other words, the vSwitch is used to build virtual networks of virtual machines residing on a single ESXi host, whereas the vDS is used to build virtual networks of virtual machines that can exist across multiple ESXi hosts. Therefore, the vDS greatly simplifies the task of network configuration when migrating virtual machines from one ESXi host to another ESXi host, using VMotion.

It should be noted that the implementation of VLAN, Private VLAN (PVLAN), attaching virtual machines on a vSwitch on a single ESXi host, attaching virtual machines on a vDS across multiple ESXi hosts, and interfacing with third party switch products is possible because the ESXi ensures that network traffic traversing a vSwitch or vDS is only delivered to the intended virtual machines and physical interfaces.

With the vDS feature of VMware virtual networking, ESXi can implement a PVLAN. PVLANs enable users to restrict communication between virtual machines on the same VLAN or network segment, significantly reducing the number of subnets needed for certain network configurations. It should also be noted that VMware's vNetwork Distributed Switch is able to interface with third party switch products such as a Cisco Nexus 1000V Series Switch.

[12] VLAN – Virtual Local Area Network
[13] IEEE – Institute of Electrical and Electronics Engineers

ESXi uses a custom mini-HTTP server to support the ESXi landing page which provides a network location to download the vSphere Client, browse the ESXi host's VM inventory and objects managed by the ESXi host, and links to download remote management tools and user documentation. The confidentiality and integrity of this communication, and communication with a client web browser and the ESXi mini-HTTP server is protected using TLS. In addition, ESXi has a standard SSH[14] interface which SSH clients can connect to execute command line functions via the ESXi Shell. Another remote management interface to the ESXi host, vCLI, is available to perfom scripted maintenance and administration tasks. The confidentiality and integrity of the communication between the ESXi host and the vCLI client is protected using TLS.

ESXi can also be accessed using a local console that is directly attached to the ESXi host. The ESXi host provides the Direct Console User Interface (DCUI), which is a BIOS[15]-like, menu-driven user interface that is displayed only on the local console of an ESXi host. The DCUI is used for the initial configuration, viewing logs, restarting services and agents, resetting admin password, setting lockdown mode[16] configuration, restarting server and resetting system defaults. In addition, administrators may also access the ESXi Shell locally through the DCUI. Only root users, users with the system administrator role, or users with the "DCUI Access" privilege (lockdown mode) can access the ESXi host this way.

1.4.1.5.1 vCenter Server Agent

The vCenter Server Agent forwards requests for services from vCenter Server users, when ESXi is under the management of a vCenter Server. The ESXi hosts can only be managed by a single vCenter Server. The requests from the vCenter Server Agents are handled by the ESXi daemon in a manner similar to requests from users at the vSphere Client or WebClient interfaces.

1.4.2 TOE Environment

For information on the TOE Environment see Section 1.3 above.

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

ESXi is a virtualization layer that runs directly on industry standard x86-compatible hardware, providing an environment where multiple virtual machines can be hosted on one physical server. ESXi abstracts processor, memory, storage, and networking resources to create virtual machines which can run a wide variety of different operating systems. Each virtual machine acts as a physically separated guest and only communicates with other virtual machines using standard networking protocols.

The vCenter Server acts as a management console server, and is responsible for deploying, monitoring, and managing virtual machines that are distributed across multiple hosts running the ESXi software. The Inventory Service maintains information about all the ESXi hosts managed by a vCenter server. vSphere

[14] SSH – Secure Shell

[15] BIOS – Basic Input Output Signal

[16] Lockdown mode – Enabling the lockdown mode disables remote access to the administrator account after the vCenter Server takes control of the ESXi host. Lockdown mode is only available on ESXi host.

Update Manager handles updates and patches for the TOE. SSO performs all authentication for vCenter users. The Syslog Collector manages system logs from distributed TOE components.

On the client machines, the vSphere Client, vCLI, and vSphere Web Client provide interfaces for administrators and users accessing vCenter and ESXi.

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. The TOE is software only and the TOE Components are specified in Figure 2 below.

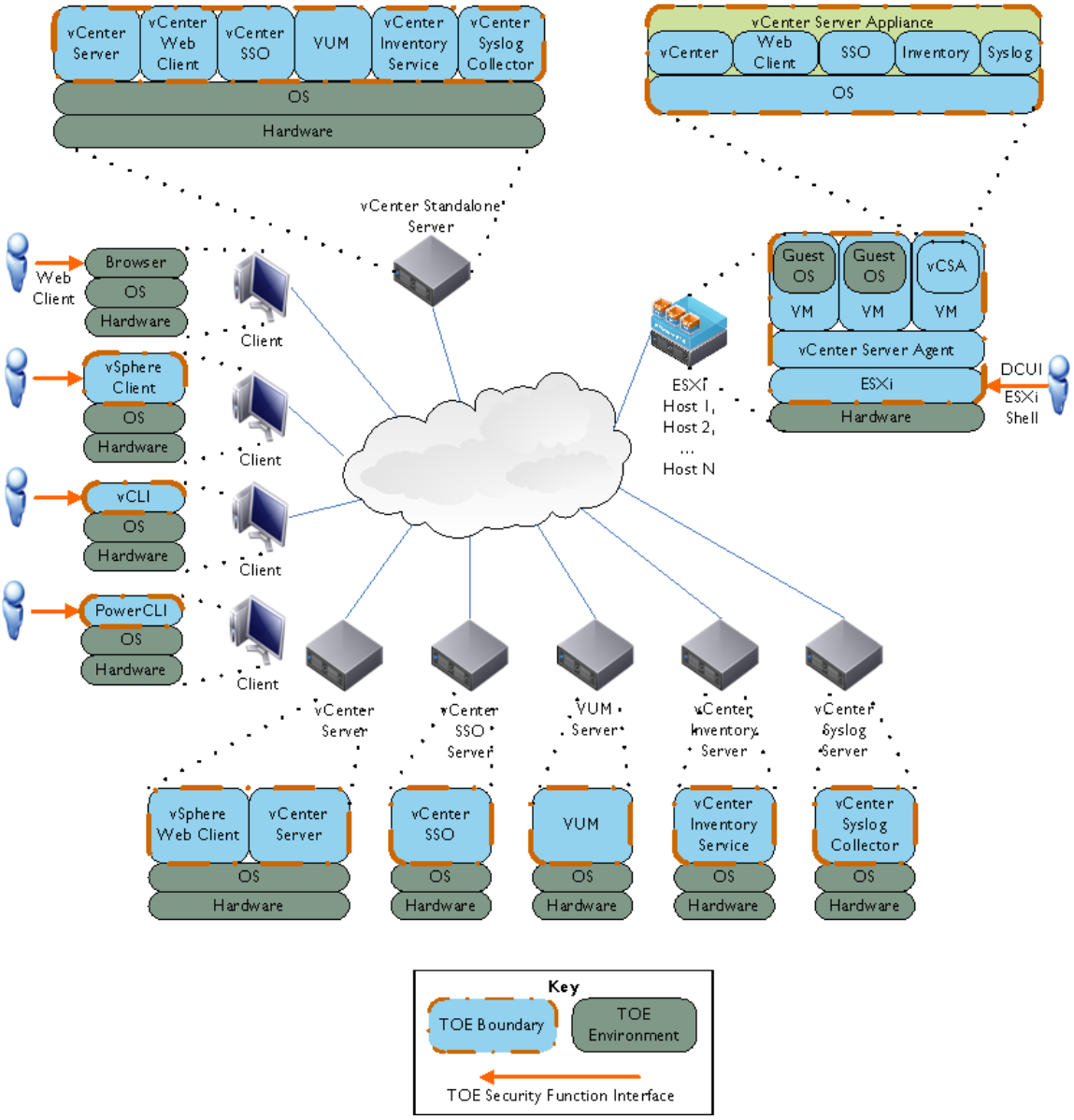

Figure 2 – Physical TOE Boundary

Table 2 below indicates which elements of the product are included in the TOE boundary.

Table 2 – Components of the TOE

Component	TOE	TOE Environment
vCenter Server software	✓	
vCenter SSO software	✓	
vCenter Inventory Service software	✓	
vSphere Update Manager software	✓	
vCenter Syslog Collector software	✓	
vCenter Virtual Appliance software and SLES OS	✓	
ESXi hypervisor software	✓	
vCLI software	✓	
vSphere Client software	✓	
vSphere Web Client software	✓	
VMware PowerCLI software (incl. vSphere API)	✓	
NTP[17] Client on vSphere Client		✓
NTP Client on ESXi host		✓
NTP Server available to ESXi host and vCenter Server		✓
ESXi host hardware (processor and adapters)		✓
Storage Area Network hardware and software to be used with ESXi host		✓
vCenter Server Standalone hardware, operating system, and database		✓
vCenter Server, SSO, Inventory Service, Syslog Collector, and VUM hardware, operating systems, and databases (when installed separately)		✓
vSphere Client and vCLI hardware and operating system		✓
vSphere Web Client hardware and operating system		✓
Operating systems and applications running in VMs		✓

1.5.1.1 Guidance Documentation

The following guides are required reading and part of the TOE:

- *VMware vSphere Installation and Setup, vSphere 5.1 Update 1, EN-001098-00*
- *VMware vSphere Upgrade Guide, vSphere 5.1 Update 1, EN-001099-00*
- *VMware vCenter Server Host Management Guide, Update 1, ESXi 5.1, vCenter 5.1, EN-001100-02*
- *VMware vSphere Virtual Machine Administration Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001095-00*
- *VMware vSphere Host Profiles Guide, ESXi 5.1, vCenter Server 5.1, EN-000795-00*
- *VMware vSphere Networking Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001101-01*
- *VMware vSphere Storage Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001097-00*

[17] NTP – Network Time Protocol

- *VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001181-01*
- *VMware vSphere Resource Management Guide, ESXi 5.1, vCenter Server 5.1, EN-000793-00*
- *VMware vSphere Availability Guide, ESXi 5.1, vCenter Server 5.1, EN-000916-00*
- *VMware vSphere Monitoring and Performance Guide, Update 1, vSphere 5.1, vCenter Server 5.1, ESXi 5.1, EN-001102-01*
- *VMware vSphere Troubleshooting, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001096-00*
- *VMware vSphere Examples and Scenarios Guide, Update 1, vSphere 5.1, vCenter Server 5.1, ESXi 5.1, EN-001178-00*
- *VMware vSphere Command-Line Interface Concepts and Examples, ESXi 5.1, vCenter Server 5.1, EN-000887-00*
- *VMware vSphere Getting Started with vSphere Command Line Interfaces, ESXi 5.1, vCenter Server 5.1, EN-000886-00*
- *VMware vSphere PowerCLI User's Guide, vSphere PowerCLI 5.1 Release 2, EN-001053-00*
- *Installing and Administering VMware vSphere Update Manager, Update 1, vSphere Update Manager 5.1, EN-001119-00*
- *VMware, Inc. vSphere 5.1 Update 1c Update 1 Guidance Documentation Supplement*

1.5.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Alarm Generation
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions (TSF)
- Virtual Machine Domain Separation
- TOE Access
- Trusted Path/Channel

1.5.2.1 Security Audit

The auditing security function of the TOE is provided by both the ESXi and the vCenter Server. Audit data collected by ESXi is stored in a flat file on the ESXi host. Audit data collected by the vCenter Server is stored as events in the vCenter Server Database. Each audit record generated includes the date and time of the event, the type of event, the subject identity (if applicable), and the outcome (success or failure) of the event. The identity of the virtual machine, the scheduled task, or alarm identity is also recorded, if applicable.

The vCenter Server provides the capability to review vCenter Server generated audit records by reviewing the event logs stored on the vCenter Server Database. Only a vCenter Server Administrator can view all of the event logs. Audit events are viewed through the vSphere Client under the event tab for each organizational object. Audit events are viewed through the vSphere Web Client. ESXi provides the same capability, using the syslog command to review its audit records which are stored in /var/log/messages. Reviewing the audit records on ESXi is restricted to the ESXi System Administrator.

The vCenter Syslog Collector provides for centralized logging management of the ESXi hosts. The vCenter Syslog Collector provides a unified architecture for system logging and enables network logging and combining of logs from multiple hosts. The vCenter Syslog Collector is deployed on a protected network so that the data-in-transit when ESXi logs are sent to the vCenter Syslog Collector host are protected by the IT Environment.

1.5.2.2 Alarm Generation

Alarms are notifications that occur in response to selected events, conditions, and states that occur with objects managed by the vCenter Server. The vCenter Server is configured with a set of predefined alarms that monitor clusters, hosts, datacenters, datastores, networks, and virtual machines[18]. Each predefined alarm monitors a specific object and applies it to all objects of that type. For example, by default, the Host CPU Usage alarm is set automatically on each ESXi host in the inventory and triggers automatically when any host's CPU usage reaches the defined CPU value.

If the predefined vCenter Server alarms do not account for the condition, state or the event that needs to be monitored, the TOE users can define custom alarms. The TOE users use the vSphere Client to create, modify, and remove alarms or the vSphere Web Client to view and monitor alarms.

1.5.2.3 Cryptographic Support

The TOE protects the confidentiality and integrity of all data as it passes between the remote components of the TOE, or from the TOE to another trusted IT product. The TOE achieves this by using various cryptographic engines which perform the encryption and the decryption of data that is being passed.

The TOE implements CAVP-validated cryptographic algorithms to handle all cryptographic functions for the encryption and the decryption of data.

1.5.2.4 User Data Protection

The TOE enforces the vSphere Access Control SFP on users accessing objects (VMs, ESXi hosts), based on permissions assigned to a user's role. Permissions grant users the privileges necessary to perform specific tasks. Both ESXi and vCenter Server implement the same set of privileges.

In addition to object permissions, the TOE provides complete access control to ESXi hosts via the ESXi lockdown mode. In this mode, only the *vpxuser* account may authenticate and perform operations directly on the host on behalf of vCenter users. Lockdown mode forces users to access hosts and VMs through the vCenter Server. When in lockdown mode, only users who have been granted the DCUI Access privilege can access the ESXi host directly.

ESXi has the ability for authorized administrators to specify the information flow control security functional policy used to control the flow of user data across the ports of the device. The vSphere Information Flow Control SFP[19] specifies the information flow control behavior for the virtual switch, distributed switch, and ESXi firewall functionality. A virtual switch (vSwitch) works much like a physical Ethernet switch. It detects which virtual machines are logically connected to any of its virtual ports and uses that information to forward traffic to the correct virtual machines on the same host machine. A vNetwork Distributed Switch functions as a single virtual switch across multiple associated hosts. This allows virtual machines to maintain consistent network configuration as they migrate between multiple hosts. The vSwitches and VNetwork Distributed Switches include functionality identical to that of a hardware Ethernet switch, although the implementation is solely in software: the source and destination identifiers of network data packets entering the vSwitch/VNetwork Distributed Switch via any of its virtual interfaces (which can be connected either to physical network interfaces, virtual machine virtual network interfaces, or other vSwitches/VNetwork Distributed Switches) are analyzed and the packet is delivered only to the appropriate virtual interface – the vSwitch/VNetwork Distributed Switch will not deliver packets to unintended virtual interfaces. The ESXi host also provides a basic firewall, which enables an authorized administrator to define a set of allowed IP addresses/subnets to restrict services on the ESXi host to an authorized network device or group of devices.

[18] Refer to Table 25 for the description of these terms: Clusters, Datacenters, Datastores, Networks, and Virtual Machines.

[19] SFP – Security Function Policy

ESXi also supports secure VMDK[20] deletion, which enables administrators to securely overwrite the contents of a virtual hard disk file with zeroes upon decommissioning a virtual disk from a VM.

1.5.2.5 Identification and Authentication

When a user attempts to log into ESXi, a user name and password are requested before access is given. These authentication credentials are compared with the authentication credentials stored on the ESXi host. in a shadow file, where the password is hashed using Secure Hash Algorithm (SHA)-1. In addition, ESXi can participate in an Active Directory (AD) infrastructure and can use the credentials provided by AD for authorization. If the authentication credentials are valid, access to the system is provided, with the privileges appropriate to the role assigned to that user. If the credentials are not valid, the user is presented with another chance to provide valid credentials. Failed and successful user login events are captured in the system logs.

When a user attempts to log into the vCenter Server, the user is presented with a login screen which requests the vCenter Server's network name or IP[21] address, the user name, and the user password. The user information is passed to vCenter SSO which verifies the user identity and password. vCenter SSO provides a central repository of user identity information against which a user can authenticate to multiple vCenter instances using a single login. vCenter SSO may be configured to use SSO-local accounts, OS accounts, or directory accounts. vCenter Server can participate in an Active Directory infrastructure and can use the credentials provided by AD for authorization. No actions may be performed via the vSphere Web Client or the vSphere Client interface prior to successful validation of the user's identity. If the login is valid, the user is presented with the respective interface denoting a successful login. If the login is invalid, a message is displayed, and the login window remains available for the user to retry. Failed and successful user login events are captured in the system logs for both the vSphere Client and the vSphere Web Client.

When vSphere Update Manager (VUM) starts up, it registers with vCenter Server. VUM instructs ESXi to scan for compliance against a pre-defined or custom created baseline and then installs a single image with a selected group of patches to be applied. ESXi will only call the instructed VUM instance, thereby ensuring that only the VUM instance that is installed with the TOE will be used to download updates and patches to the ESXi host.

Note that for purposes of this ST, Administrative users are considered to be the users of the TOE. VM users (individuals who access the guest operating system and applications within a virtual machine) are outside the scope of the TOE and are not discussed any further here.)

When configured to use local accounts for vCenter SSO authentication, passwords must be at least eight characters including one special character and six alphabetic characters. No two adjacent characters may be identical. For ESXi accounts, passwords must be at least six characters and composed of a mix of lowercase letters, uppercase letters, numbers, and special characters.

1.5.2.6 Security Management

Security management specifies how the ESXi manages several aspects of the TSF including TSF data and security functions. TSF data includes configuration data of the TOE, audit data, and system data. For a detailed listing of TSF data managed by the TOE see Table 15 of this ST. The TOE provides authorized administrators with management consoles as described in section 1.4.1 to easily manage the security functions and TSF data of the TOE.

The TOE provides a set of commands for administrators to manage the security functions, configuration, and other features of ESXi. The Security Management function specifies user roles with defined access for

[20] VMDK – Virtual Machine Disk
[21] IP – Internet Protocol

the management of ESXi. The TOE ensures that the ability to modify user privileges on the vCenter Server objects is restricted to a vCenter Server Administrator, or to an administrator-defined role explicitly given the required permissions. The TOE also ensures that the ability to modify permissions of users on ESXi objects is restricted to system administrators.

VM administrators are administrators of one or more VMs on the ESXi host. VM administrators can access the VMs by directly logging into the ESXi host or through the vCenter Server via the *vpxuser* account and password. When logging in through the vCenter Server, the vCenter Server uses the *vpxuse*r account and password to gain access to the ESXi host and process the requests on behalf of the VM administrators.

The TOE supports a combination of access control as detailed in Table 13. Users, groups, roles, and permissions are used to control who is allowed access to the vSphere managed objects and the specific actions that are allowed. vCenter Server and ESXi hosts determine the level of access for the user based on the permissions that are assigned to said user. The combination of user name, password, and permissions is the mechanism by which vCenter Server and ESXi hosts authenticate a user for access and authorize the user to perform activities.

The servers and hosts maintain lists of authorized users and the permissions assigned to each user. Privileges define basic individual rights that are required to perform actions and read properties. ESXi and vCenter Server use sets of privileges or roles to control which users or groups can access particular vSphere objects.

ESXi and vCenter Server provide a set of pre-established roles and allow for roles to be defined by administrators. The privileges and roles assigned on an ESXi host are separate from the privileges and roles assigned on vCenter Server. Only the privileges and roles assigned through the vCenter Server system are available to administrators managing a host through vCenter Server. Refer to Table 13 for a detailed listing of operations that are performed per specific data and role.

The vCenter Server supports three categories of roles: vCenter Server Administrator, vCenter SSO Administrator, and Administrator-defined roles. The vCenter Server Administrator is implemented by membership in the "Administrators" group of the underlying Windows OS for vCenter Server. Users log in using their username and password, and are automatically assigned in this role by virtue of their membership in the Administrators group. The vCenter Server Virtual Appliance Administrator is implemented by the root account on POSIX[22]. The vCenter SSO Administrator is implemented as *admin@system-domain* in the default local SSO domain, and other explicitly assigned users and groups. In addition, Administrators may define other groups (local and directory-based) to which roles and privileges are assigned.

ESXi and vCenter SSO users are provided no privileges by default, and therefore cannot perform operations on ESXi hosts and VMs unless explicitly authorized by an administrator.

1.5.2.7 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that physical connections made to the TOE remain intact and unmodified. The TOE protects the confidentiality and integrity of all data as it is transmitted between the remote components of the TOE, or from the TOE to another trusted IT product by using various cryptographic engines included with the TOE, as follows:

- HTTP communications between VUM and the ISP Server, and between VUM and the ESXi, are protected by signature verification.

[22] vSphere Installation and Setup Guide, section "Download and Deploy the VMware vCenter Server Appliance"

- Client USB redirect from the USB ports on the host machine to the VMs.
- HTTPS is used between the remote web browser and the vSphere Web Client.
- TLS is used to secure communications between the ESXi host/vCenter Server and vCLI/vSphere Client on the remote machine, as well as internal communications between vCenter Server and vCenter Inventory Service, vSphere Web Client, vCenter SSO, VUM, and ESXi.
- ESXi logs sent to the Syslog Collector host are secured with TLS while in transit.
- LDAPS is used to protect credentials sent to a remote LDAP server.

1.5.2.7.1 Virtual Machine Domain Separation

The virtual machine separation security function of the TOE is provided by the ESXi component. The TOE ensures that each virtual machine is isolated from any other virtual machines co-existing on the ESXi. This isolation is provided at the virtualization layer of the ESXi. The virtualization layer of the ESXi ensures that virtual machines are unable to directly interact with other virtual machines yet still allow for physical resources to be shared among the existing virtual machines.

The ESXi provides an idealized hardware environment and virtualization of underlying physical resources. Each virtual machine runs its own operating system and applications: they cannot communicate to each other in unauthorized ways.

1.5.2.8 TOE Access

The TOE Access function enables termination of a user's session after a period of inactivity. The TOE will lock an interactive session after an authorized administrator-specified time period of user inactivity.

1.5.2.9 Trusted Path/Channel

The TOE protects the vSphere Web Client, ESXi Shell, and vCLI communications using a server-authenticated connection between the end-users and the vCenter Server or ESXi host. The TOE contains various cryptographic engines that perform FIPS validated cryptography to support TLS and SSH functionality.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Each virtual machine can have users who are individuals using a virtual machine's guest operating system and applications that reside on the virtualized hardware of the virtual machine that is instantiated on an ESXi host. These users access the VM via a remote workstation called a Remote Console, using an Internet Protocol (IP) address associated with the specific virtual machine. The VMs themselves, their operating systems, applications, and users are outside the scope of the TOE. The claims of the TOE are relevant to the management, separation, isolation, and protection of the virtual machine structures, and not of the functionality and actions that take place within a VM, and as such do not address the security issues within each VM.

The following features of the system were not included in the evaluation.

- Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), Telnet
- VMware Software Development Kit (SDK) tools
- The procfs interface on the ESXi Direct Console User Interface
- VMware Consolidated Backup
- Guest OS patch updates via vSphere Update Manager
- Log Browser
- ESXi Dump Collector
- vSphere Auto Deploy

- VMware vCloud NetWorking and Security
- VMware vCenter Operations Manager
- VMware Management Assistant
- VMware Data Recovery
- Trusted Platform Module
- VMware vNetwork Distributed Switch 3rd party integration

.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 12/11/2012 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.3)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[23] assets against which protection is required by the TOE or by the security environment. One type of threat agent is individuals who are not authorized to use the TOE. The threat agents are assumed to:

- have public knowledge of how the TOE operates
- possess a low skill level
- have limited resources to alter TOE configuration settings
- have no physical access to the TOE
- possess a low level of motivation.

Other types of threat agents are:

- a process running on a Virtual Machine that may cause tampering or interference in another VM's domain of execution, and
- a process running on a Virtual Machine that may attempt to circumvent the operating mechanism of the Virtual Networking scheme.
- a process running on a Virtual Machine or an ESXi host that may cause a system malfunction or a system performance degradation.

The IT assets requiring protection are the virtual machines running on the TOE. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 – Security Objectives.
The following threats are applicable:

Table 4 – Threats

Name	Description
T.COMINT	An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE by bypassing a security mechanism.
T.MISCONFIGURE	An authorized ESXi administrator or unauthorized attacker may directly access a host and modify its configuration in a way that is inconsistent with the vCenter Server.
T.PRIVIL	An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.REUSE	An unauthorized individual with access to a decommissioned hard drive may be able to view the sensitive information contents of a VMDK file.

[23] IT – Information Technology

.

Name	Description
T.VIRTUAL_NETWORK	A process running on a virtual machine attempts to deliver traffic to wrong VM or external entity.
T.VM	A process running on one virtual machine might compromise the security of processes running on other virtual machines.
T.WEAKIA	A user may supply the TOE with a weak password that is easily guessable based on dictionary words.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 – Assumptions

Name	Description
A.NOEVIL	Users are non-hostile, appropriately trained, and follow all user guidance.
A.PHYSCL	The ESXi host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access.

.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUDIT	The TOE must gather audit records of actions on the TOE which may be indicative of misuse.
O.DESTROY	The TOE must provide the ability to securely destroy virtual machine disk images.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.IDAUTH2	The TOE must enforce strong password complexity and minimum length requirements for TOE users.
O.SECURE	The TOE must ensure the confidentiality and integrity of all data as it passes between the remote components of the TOE, from the TOE to another trusted IT product, or between the TOE and remote users.
O.SEPARATE	The TOE must provide capabilities for separation of administrator duties, and prevent ESXi administrators from configuring hosts in a manner that is inconsistent with vCenter policies.
O.VM	The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.
O.VSWITCH	The TOE must ensure that network traffic traversing a vSwitch is only delivered to the intended virtual machines and physical interfaces.

.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 – IT Security Objectives

Name	Description
OE.IDAUTH	The IT Environment will provide reliable verification of the vSphere SSO user credentials for non-TOE accounts.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.SEP	The TOE environment must protect itself and the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

Name	Description
NOE.NOEVIL	Users are non-hostile, appropriately trained, and follow all user guidance.
NOE.PHYSCL	The ESXi host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access.

.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE.

Table 9 – Extended TOE Security Functional Requirements

Name	Description
EXT_FAU_ARP.1	System event automatic response
EXT_FAU_STG.1	External audit trail storage
EXT_FIA_VC_LOGIN.1	vCenter Server user login request
EXT_VDS_VMM.1	ESXi virtual machine domain separation

.

5.1.1 Class FAU: Security Audit

Families in this class address the requirements for functions to recognize, record, store, and analyze information related to security relevant activities. The extended family "EXT_FAU_ARP: System event automatic response" and family "EXT_FAU_STG: External Audit Trail Storage" were modeled after the CC Part 2 SFRs, FAU_ARP.1 and FAU_STG.1 respectively.

5.1.1.1 Security event automatic response (EXT_FAU_ARP)

Family Behavior

This family defines the response to be taken in case of detected events indicative of a potential system malfunction or a potential system performance degradation on the ESXi host and its virtual machines.

Component Leveling

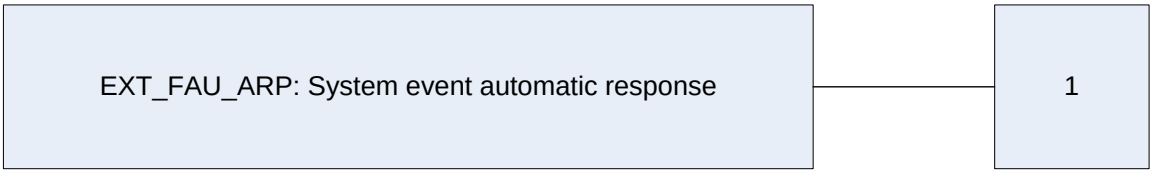

Figure 3 – EXT_FAU_ARP System event automatic response family decomposition

EXT_FAU_ARP.1 System event automatic response, defines the behavior of the vCenter Server when it detects the events indicative of a potential system malfunction or a potential system performance degradation on the ESXi host and its virtual machines. It was modeled after FAU_ARP.1

Management: EXT_FAU_ARP.1

a) There are no management activities forseen.

Audit: EXT_FAU_ARP.1

a) There are no auditable events foreseen.

EXT_FAU_ARP.1 System event automatic response

Hierarchical to: No other components

Dependencies: None

This component will ensure that the TOE users are notified of the events on the ESXi host that may cause a system malfunction or a system performance degradation on the ESXi host and its virtual machines.

EXT_FAU_ARP.1.1 The vCenter Server shall notify the appropriate TOE users upon detection of a potential system malfunction or a potential system performance degradation on the ESXi host and its virtual machines.

.

5.1.1.2 External audit trail storage (EXT_FAU_STG)

Family Behavior

This family defines the log storage capabilities of remote backup.

Component Leveling

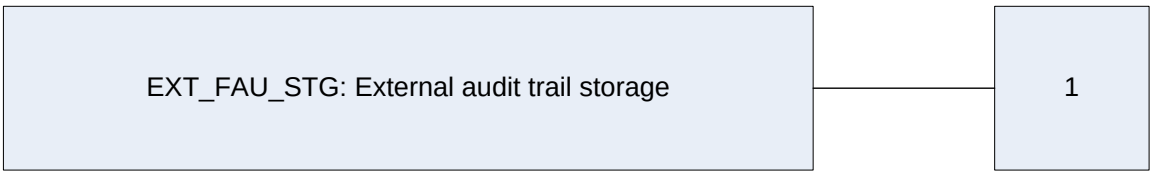

Figure 4 – EXT_FAU_STG External audit trail storage

EXT_FAU_STG.1 External audit trail storage, defines the behavior of the remote backup when ESXi hosts send their logs to the vCenter Syslog Collector. It was modeled after FAU_STG.1.

Management: EXT_FAU_STG.1

a) There are no management activities foreseen.

Audit: EXT_FAU_STG.1

a) There are no auditable events forseen.

EXT_FAU_STG.1 External audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1

This component will ensure that the ESXi log files are successfully backed up and stored by the Syslog Collector.

EXT_FAU_STG.1.1 The TSF shall be able to backup and restore the ESXi log files to a separate part of the TOE.

5.1.2 Class FIA: Identification and authentication

Families in this class address the requirements for functions to establish and verify a claimed user identity. The extended family "EXT_FIA_VC_LOGIN: vCenter SSO user login request" was modeled after the other FIA SFRs.

5.1.2.1 vCenter SSO user login request (EXT_FIA_VC_LOGIN)

Family Behavior

This family defines the identification and authentication behavior of the vCenter Server component of the TOE.

Component Leveling

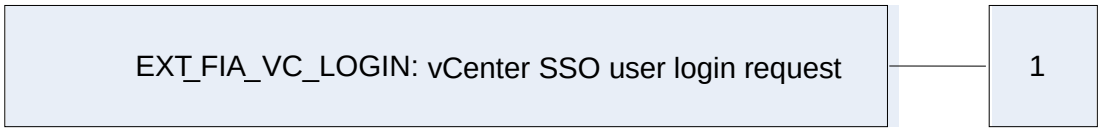

Figure 5 – EXT_FIA_VC_LOGIN vCenter SSO user login request family decomposition

EXT_FIA_VC_LOGIN.1 vCenter SSO user login request, defines the behavior of the vCenter SSO component when identifying and authenticating an administrative user. It was modeled after FIA_UAU.1 and FIA_UID.1.

Management: EXT_FIA_VC_LOGIN.1

a) There are no management activities foreseen

Audit: EXT_FIA_VC_LOGIN.1

b) There are no auditable events foreseen.

EXT_FIA_VC_LOGIN.1 vCenter SSO user login request

Hierarchical to: No other components

Dependencies: None

This component will provide users the capability to identify and authenticate themselves to the vCenter Server, via a credential authority stored in the Environment.

EXT_FIA_VC_LOGIN.1.1 The vCenter Server shall request identification and authentication from vCenter SSO for a vCenter Server user, and receive notification of success, prior to granting any other TSF-mediated actions on behalf of the user.

5.1.3 Class EXT_VDS: Virtual machine domain separation

Virtual machine domain separation functions ensure that virtual machines cannot inappropriately or unintentionally interact with or tamper with each other. The extended class "EXT_VDS: Virtual machine domain separation" was modeled after the class FDP.

5.1.3.1 ESXi virtual machine domain separation (EXT_VDS_VMM)

Family Behavior

This family defines the non-interference requirements for VMs that are running simultaneously on an ESXi host.

Component Leveling

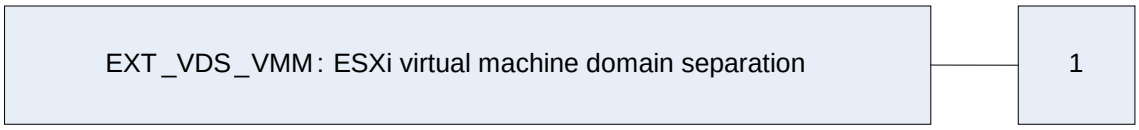

Figure 6 – EXT_VDS_VMM: ESXi Virtual machine domain separation family decomposition

EXT_VDS_VMM.1 ESXi virtual machine domain separation ensures that VMs cannot interfere or tamper with each other. The extended family "EXT_VDS_VMM: ESXi virtual machine domain separation" was modeled after the other FDP SFRs.

Management: EXT_VDS_VMM.1

a) There are no management activities foreseen.

Audit: EXT_VDS_VMM.1

a) There are no auditable events forseen.

EXT_VDS_VMM.1 ESXi virtual machine domain separation

Hierarchical to: No other components

Dependencies: None

This component will ensure that virtual machine resources (CPU, memory, I/O devices, etc.) are only accessible to the virtual machine(s) to which they have been allocated by an authorized administrator.

EXT_VDS_VMM.1.1 The TSF shall maintain a security domain for the execution of each virtual machine that protects the virtual machine from interference and tampering by untrusted subjects or subjects from outside the scope of the VM.

EXT_VDS_VMM.1.2 The TSF shall enforce separation between the security domains of VMs in the TSC[24].

[24] TSC: TOE Scope of Control

.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
EXT_FAU_ARP.1	System event automatic response				
FAU_GEN.1	Audit data generation	✓	✓	✓	
EXT_FAU_STG.1	External audit trail storage				
FAU_SAR.1	Audit review		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.2	Complete access control		✓		
FDP_ACF.1	Security attribute-based access control		✓		
FDP_IFC.2	Complete information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FDP_RIP.1	Subset residual information protection	✓	✓	✓	
FIA_SOS.1	Specification of secrets		✓		
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	

.

Name	Description	S	A	R	I
EXT_FIA_VC_LOGIN.1	vCenter single sign-on user login request				
FMT_MSA.1(a)	Management of security attributes (Virtual and Distributed Switch Information Flow Control)	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes (vSphere Access Control)		✓		✓
FMT_MSA.3(a)	Static attribute initialization (Virtual and Distributed Switch Information Flow Control)	✓	✓	✓	✓
FMT_MSA.3(b)	Static attribute initialization (vSphere Access Control)	✓	✓		✓
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1(a)	Security roles (vCenter Server)		✓	✓	✓
FMT_SMR.1(b)	Security roles (ESXi)		✓	✓	✓
FPT_ITC.1	Inter-TSF confientiality during transmission				
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FTA_SSL.3	TSF-initiated termination		✓		
FTP_TRP.1	Trusted path	✓	✓		
EXT_VDS_VMM.1	ESXi virtual machine domain separation				

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

EXT_FAU_ARP.1 System event automatic response.
Hierarchical to: No other components.

EXT_FAU_ARP.1.1

The vCenter Server shall notify the appropriate TOE users upon detection of a potential system malfunction or a potential system performance degradation on the ESXi host and its virtual machines.

Dependencies: None

FAU_GEN.1 Audit data generation
Hierarchical to: No other components.

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [*not specified*] level of audit; and
c) [*The events specified in the "Audit Event" column of Table 11*].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the information specified in the "Additional Collected Information" column of Table 11*].

Dependencies: FPT_STM.1 Reliable time stamps

Table 11 – Auditable Events on the ESXi

Audit Event	Additional Collected Information
Startup and shutdown of the Auditing functions	<none>
All management operations performed on virtual machines[25]	virtual machine
All changes to the configuration of alarms or scheduled task	The alarm or scheduled task
All use of the identification and authentication mechanisms	The user identity if provided

[25] This audit event refers to management actions taken by an ESXi or a vCenter Server administrator via the ESXi or the vCenter Server management interfaces; it does not refer to the VM guest-OS administrator events which occur within the guest-OS.

.

FAU_SAR.1 Audit review
Hierarchical to: No other components.

FAU_SAR.1.1
The TSF shall provide [*authorized vCenter Server administrators, system administrators, and VM administrators*] with the capability to read [*all audit events in which the authorized administrator has permission to read*] from the audit records.

FAU_SAR.1.2
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

EXT_FAU_STG.1 External audit trail storage.
Hierarchical to: No other components.

EXT_FAU_STG.1.1
The TSF shall be able to backup and restore the ESXi log files to a separate part of the TOE.

Dependencies: FAU_GEN.1

.

6.2.2 Class FCS: Cryptographic Support

FCS_COP.1 Cryptographic Operation.
Hierarchical to: No other components.

FCS_COP.1.1

The TSF shall perform [*the cryptographic operations listed in the Cryptographic Operations column of Table 12*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 12*] and cryptographic key sizes [*the cryptographic key sizes listed in the Key Sizes (bits) column of Table 12*] that meet the following: [*the list of standards in the Standards (Certificate #) column of Table 12*].

Dependencies: None

Table 12 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES[26] (2-Key) CBC[27]	128	CAVP (see Table 19 for Cert #s)
	AES[28] (128, 256) CBC	128, 256	CAVP (see Table 19 for Cert #s)
Message Digest	SHA-1	N/A[29]	CAVP (see Table 19 for Cert #s)
Message Authentication	HMAC[30]-SHA-1	128, 160	CAVP (see Table 19 for Cert #s)
Digital signatures	RSASSA[31] PKCS[32]#1 v1_5	2048, 3072, 4096	CAVP (see Table 19 for Cert #s)

[26] DES – Data Encryption Standard
[27] CBC – Cipher Block Chaining
[28] AES – Advanced Encryption Standard
[29] N/A – Not Applicable
[30] HMAC – Hash-based Message Authentication Code
[31] RSASSA – RSA Signature Scheme with Appendix
[32] PKCS – Public Key Cryptography Standard

.

6.2.3 Class FDP: User Data Protection

FDP_ACC.2 Complete access control
Hierarchical to: FDP_ACC.1 Subset access control

FDP_ACC.2.1
The TSF shall enforce the [*vSphere Access Control SFP*] on [
a. Subjects: ESXi users, vCenter Server users
b. Objects: the objects/resources defined in Table 13 below]
and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2
The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

Table 13 – ESXi and vCenter Server Privileges

Object	All Operations	vCenter or ESXi
Alarms	Acknowledge, Create, Disable, Modify, Remove, Set Status	vCenter
Datacenter	Create, Query IP Pool Configuration, Move, Remove, Rename	vCenter
Datastore	Allocate space, Browse, Configure, Low-level file operations, Move (vCenter-only), Remove, Remove file, Rename, Update virtual machine files	vCenter and ESXi
Datastore Cluster	Configure	vCenter and ESXi
Distributed Virtual Port Group	Create, Delete, Modify, Policy operation, Scope operation	vCenter and ESXi
ESX Agent	Configure, Modify, View	vCenter
Extension	Register, Unregister, Update	vCenter
Folder	Create, Delete, Move Rename	vCenter
Global	Act as vCenter Server (vCenter only), Cancel task, Capacity planning (vCenter only), Run diagnostics (vCenter only), Disable methods (vCenter only), Enable methods (vCenter only), Manage global tag, View health (vCenter only), Manage licenses, Log event, Manage custom attributes (vCenter only), Manage proxy (vCenter only), Schedule script action (vCenter only), Manage services, Manage vCenter configuration (vCenter only), Manage system tag (vCenter only)	vCenter and ESXi
Host CIM[33]	CIM interaction	vCenter and ESXi

[33] CIM – Common Information Model

.

Object	All Operations	vCenter or ESXi
Host Configuration	Set advanced host settings, Configure Active Directory authentication, Change date and time, Change PCI passthru settings, Change lockdown settings, Change SNMP settings, Change host connection status (vCenter only), Update host firmware, Configure host CPU hyperthreading, Set maintenance mode, Configure host memory, Configure host networking, Configure host power, Query host patches, Configure security profile and firewall/services, Configure storage partitions, Configure system management, Configure system resources, Configure VM autostart parameters	vCenter and ESXi
Host Inventory	Add host to cluster, Add standalone host, Create cluster, Modify cluster, Move cluster or standalone host, Move host, Remove cluster, Remove host, Rename cluster	vCenter only
Host Local Operations	Add to vCenter, Create VM, Delete VM, Manage user groups, Reconfigure VM, Change snapshot layout	ESXi only
Host vSphere Replication	Manage vSphere replication	vCenter and ESXi
Host Profile	Clear, Create, Delete, Edit, Export, View	vCenter and ESXi
Network	Assign, Configure, Move, Remove	vCenter and ESXi
Performance	Modify intervals	vCenter only
Permissions	Modify, Modify role, Reassign role permissions	vCenter and ESXi
Profile-driven Storage	Update, View	vCenter only
Resource	Apply recommendation (vCenter only), Assign vApp to resource pool, Assign VM to resource pool, Create resource pool, Migrate VM (vCenter only), Modify resource pool, Move resource pool, Relocate VM (vCenter only), Remove resource pool, Rename resource pool	vCenter and ESXi
Scheduled Task	Create, Modify, Remove, Run	vCenter only
Sessions	Impersonate user, Set login message, Validate session, View session, Stop session	vCenter only
Storage Views	Configure, View	vCenter only
Tasks	Create, Update	vCenter only
vApp	Add VM, Assign resource pool, Assign, Clone, Create, Delete, Export, Import, Move, Power off, Power on, Rename, Suspend, Unregister, Configure, Manage by extension, Modify, View OVF environment	vCenter only

.

Object	All Operations	vCenter or ESXi
VM Configuration	Add existing disk, Add new disk, Add/remove device, Modify advanced configuration, Change CPU count, Change resource configuration, Configure management by extension, Configure disk change tracking, Configure disk leases, Configure remote console options, Extend disk, Attach USB device, Change memory, Modify device settings, Query fault tolerance capability (vCenter only), Query unowned files, Add/remove raw disk mapping/SCSI passthru, Reload configuration from path (vCenter only), Remove disk, Rename VM, Reset guest information, Set annotation, Change general settings, Configure swapfile, Decrypt VM, Upgrade VM hardware	vCenter and ESXi
VM Guest Operations	Modify guest operations, Execute guest program, Query guest OS	vCenter and ESXi
VM Interaction	Acquire guest control ticket, Resolve VM issues, Backup VM, Configure removable storage device, Configure floppy device, Interact with console, Create screenshot, Defragment disks, Change device connection state, Disable fault tolerance (vCenter only), Enable fault tolerance (vCenter only), Power off, Power on, Record session, Replay session, Reset, Suspend, Test failover (vCenter only), Test restart secondary VM (vCenter only), Turn off fault tolerance (vCenter only), Turn on fault tolerance (vCenter only), Install VMware tools	vCenter and ESXi
VM Inventory	Create from existing, Create new, Move (vCenter only), Register, Remove, Unregister	vCenter and ESXi
VM Provisioning	Allow disk access, Allow read-only disk access, Allow VM download, Allow VM upload, Clone template (vCenter only), Clone VM (vCenter only), Create template from VM (vCenter only), Customize VM guest OS (vCenter only), Deploy template (vCenter only), Mark existing VM as template (vCenter only), Mark existing template as VM (vCenter only), Modify customization specifications (vCenter only), Promote VM disks (vCenter only), Read customization specification (vCenter only)	vCenter and ESXi
VM State	Create snapshot, Remove snapshot, Rename snapshot, Revert to snapshot	vCenter and ESXi
VM vSphere Replication	Configure, Manage, Monitor	vCenter and ESXi
vServices	Create dependency, Destroy dependency, Reconfigure dependency, Update dependency	vCenter and ESXi
vSphere Distributed Switch	Create, Delete, Change host members, Modify, Move (vCenter only), Change network I/O settings, Change policy, Change port setting, Change VSPAN setting	vCenter and ESXi
VRM Policy	Query, Update	

.

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components

FDP_ACF.1.1

The TSF shall enforce the [*vSphere Access Control SFP*] to objects based on the following: [

a. *Subjects: ESXi users, vCenter Server users*
b. *Objects: the objects/resources defined in Table 13 above*
c. *Attributes: the attribute groups corresponding to the objects listed in Table 13 above*]

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A subject is granted access to perform an operation on an object if and only if the user has been authorized to do so, based on the privileges associated with the role to which the user is assigned, either explicitly through administrator assignment or implicitly through role inheritance by group membership.*]

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*When operating in ESXi Lockdown mode, only the vpxuser account may perform actions on an ESXi host on behalf of a vCenter user. In addition, only users with the "DCUI Access" permission may directly access the ESXi host via the DCUI.*]

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*When operating in ESXi Lockdown mode, all users other than the vpxuser account and users with the "DCUI Access" permission are denied access to directly manage ESXi hosts.*]

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 (b) Static attribute initialization (vSphere Access Control)

FDP_IFC.2 Complete information flow control
Hierarchical to: FDP_IFC.1 Subset information flow control

FDP_IFC.2.1

The TSF shall enforce the [*vSphere Information Flow Control SFP*] on [

a) Subjects: physical network interfaces, VM virtual network interfaces, and external ESXi users
b) Information: network data packets]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2

The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes
Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [*vSphere Information Flow Control SFP*] based on the following types of subject and information security attributes: [

a) Subjects: physical network interfaces, VM virtual network interfaces, and external ESXi users
b) Subject security attributes: interface identifier, VLAN identifier (if applicable), IP address/subnet mask

.

c) Information: network data packets
d) Information security attributes: source identifier, destination identifier].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a. *if the data packet originates from a recognized and authorized physical network interface or VM virtual network interface as identified by the interface identifier or VLAN identifier (if applicable) which are indicated by the source identifier as defined in this SFP, and is addressed to a recognized and authorized destination which is indicated by the destination identifier as defined in this SFP, then allow the information flow, otherwise deny the information flow*
b. *if the data packet destined for a service running on an ESXi host meets the conditions specified by the firewall ruleset (the source identifier is the IP address/subnet mask or port number of an allowed host/service), then allow the information flow, otherwise deny the information flow*].

FDP_IFF.1.3

The TSF shall enforce [***no additional information flow control SFP rules***].

FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on [***no additional information flow control SFP rules***.]

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on [***no additional information flow control SFP rules***.]

Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_MSA.3 (a) Static attribute initialisation (Virtual and Distributed Switch Information Flow Control)

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1

The TSF shall ensure that any previous information content of a **VMDK file** is made unavailable upon [deallocation of the resource from] the following objects: [*ESXi datastores*].

Dependencies: **No dependencies**

.

6.2.4 Class FIA: Identification and Authentication

FIA_SOS.1 Specification of secrets
Hierarchical to: No other components

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [

a. *ESXi users*
    1. *Passwords must be at least eight characters long if they are composed of one or two character classes.*
    2. *Passwords must be at least seven characters long if they are composed of three of the four character classes.*
    3. *Passwords must be at least six characters long if they are composed of four of the character classes.*
b. *vCenter SSO users*
    1. *Passwords must be between eight and thirty-two characters.*
    2. *Passwords must contain at least six alphabetic characters.*
    3. *Passwords must contain at least one special character.*
    4. *Passwords must not contain adjacent characters that are identical.*]

Dependencies: No dependencies

Application Note: The four character classes are defined as: Uppercase letters, lowercase letters, numeric characters, and special characters.

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

The TSF shall require each **ESXi and vCenter** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each **ESXi and vCenter** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

EXT_FIA_VC_LOGIN.1 vCenter single sign-on user login request
Hierarchical to: No other components.

EXT_FIA_VC_LOGIN.1.1

The vCenter Server shall request identification and authentication from vCenter SSO for a vCenter Server user, and receive notification of success, prior to granting any other TSF-mediated actions on behalf of the user.

Dependencies: No dependencies

.

6.2.5 Class FMT: Security Management

FMT_MSA.1 (a) Management of security attributes (Virtual and Distributed Switch Information Flow Control)
Hierarchical to: No other components.

FMT_MSA.1.1 (a)
The TSF shall enforce the [*Virtual and Distributed Switch Information Flow Control SFP*] to restrict the ability to [*add, modify, delete*] the security attributes [*defined in Table 14 below*] to [*System Administrators*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 (b) Security roles (ESXi)

FMT_MSA.1 (b) Management of security attributes (vSphere Access Control)
Hierarchical to: No other components.

FMT_MSA.1.1 (b)
The TSF shall enforce the [*vSphere Access Control SFP*] to restrict the ability to [*add, remove*] the security attributes [*permissions*] to [*System Administrators, vCenter SSO Administrators, and vCenter Server Administrators*].

Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 (a) Security roles (vCenter Server)
FMT_SMR.1 (b) Security roles (ESXi)

FMT_MSA.3 (a) Static attribute initialization (Virtual and Distributed Switch Information Flow Control)
Hierarchical to: No other components.

FMT_MSA.3.1 (a)
The TSF shall enforce the [*vSphere Information Flow Control Policy*] to provide **default values meeting the characteristics in Table 14 below** for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (a)
The TSF shall allow the [*System Administrators*] to specify alternative initial values to override the default values when a **Virtual Switch is created on the ESXi or when a firewall rule is created**.

Dependencies: FMT_MSA.1 (a) Management of security attributes (Virtual and Distributed Switch Information Flow Control)
FMT_SMR.1 (b) Security roles (ESXi)

Table 14 – vSphere Information Flow Control Security Attribute Value Properties

Attribute	Property
Interface identifier	Restrictive
VLAN identifier	Restrictive
Firewall ruleset	Permissive

.

FMT_MSA.3 (b) Static attribute initialization (vSphere Access Control)

Hierarchical to: No other components.

FMT_MSA.3.1 (b)

The TSF shall enforce the [*vSphere Access Control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (b)

The TSF shall allow the [*System Administrators, vCenter SSO Administrators, and vCenter Administrators*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 (b) Management of security attributes (vSphere Access Control)
FMT_SMR.1 (a) Security roles (vCenter Server)
FMT_SMR.1 (b) Security roles (ESXi)

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*the operations as defined in column 'Operation' of Table 15*] the [*TSF data as defined in column 'TSF Data' of* Table 15] to [*the authorized identified roles as defined in column 'Authorized Role' of* Table 15].

Table 15 – Management of TSF Data

Operation	TSF Data	Authorized Role
vCenter Server		
Change	Own password	*vCenter SSO Users*
Change	Passwords	*vCenter SSO Administrator*
Add, modify, remove	Users	*vCenter Server Administrator*
Add, modify, remove	Groups	*vCenter Server Administrator*
Add, modify, remove	SSO Users	*vCenter SSO Administrator*
Add, modify, remove	SSO Groups	*vCenter SSO Administrator*
Add, modify, remove	vCenter Server user role	*vCenter Server Administrator*
Create	Virtual machine definition	*vCenter Server Administrator*
Edit	VM configuration files	*vCenter Server Administrator*
View, Edit Settings	Inventory data for virtual machines	*vCenter Server Administrator*
Select	Folders	*vCenter Server Administrator*
View	Datacenters	*vCenter Server Administrator*
Select	Hosts	*vCenter Server Administrator*
Select	Clusters	*vCenter Server Administrator*
Select	Resource pools	*vCenter Server Administrator*
Configure	Networks	*vCenter Server Administrator*
Select	Datastores	*vCenter Server Administrator*

.

Operation	TSF Data	Authorized Role
Adding, deleting, or modifying	Permissions associated with a user or group	*vCenter Server Administrator*
Convert	Templates	*vCenter Server Administrator*
View, Filter	Audit events, audit logs	*vCenter Server Administrator*
Set	Alarms	*vCenter Server Administrator*
Create	Scheduled tasks	*vCenter Server Administrator*
Create	Templates	*vCenter Server Administrator*
Modify	Timeout value	*vCenter Server Administrator*
ESXi		
Add, modify, delete	User identity	*System Administrator*
Add, modify, delete	User group	*System Administrator*
Add, modify, delete	ESXi User Role	*System Administrator*
Create, modify, delete, Power Up	Virtual machine definition	*System Administrator or VM Administrator*
Edit	Virtual machine configuration files	*System Administrator or VM Administrator*
Edit	ESXi configuration files	*System Administrator or VM Administrator*
View, Sort	ESXi audit logs	*System Administrator or VM Administrator*
Modify	Read, write, and execute permissions on objects	*System Administrator or VM Administrator*
View	Virtual machine inventory	*System Administrator or VM Administrator*
Add, modify, delete	Object group	*VM Administrator: may change the group of the file to any group the owner is a member of* *System Administrator: may change the group arbitrarily*
Add, modify, delete	User identity of object owner	*System Administrator*
Change	Passwords	*System Administrator*
Change	Own password	*All Users*
Power Up	VM	*System Administrator or VM Administrator*
Modify	Timeout value	*System administrator or VM administrator*

Dependencies: FMT_SMF.1 Specification of management functions

.

FMT_SMR.1 (a) Security roles (vCenter Server)
FMT_SMR.1 (b) Security roles (ESXi)

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*the management of TSF data as stated in FMT_MTD.1, management of security attributes (FMT_MSA.1), management of audit data (FAU_GEN.1), management of cryptography (FCS_COP.1), management of identities and authentication (FIA_UAU.1, FIA_UID.1, EXT_FIA_VC_LOGIN.1), management of information flow policies (FDP_IFF.2, FDP_IFC.1), and management of access control policies (FDP_ACC.2, FDP_ACF.1*].

Dependencies: No dependencies

FMT_SMR.1 (a) Security roles (vCenter Server)
Hierarchical to: No other components.

FMT_SMR.1.1 (a)

The TSF shall maintain the roles **for the vCenter Server users** [*vCenter SSO Administrator, vCenter Server Administrator and Administrator defined roles*].

FMT_SMR.1.2 (a)

The TSF shall be able to associate **the vCenter Server** users with **the above mentioned** roles.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1(b) Security roles (ESXi)
Hierarchical to: No other components.

FMT_SMR.1.1 (b)

The TSF shall maintain the roles **for the ESXi users** [*VM Administrator, System Administrator, and Users*].

FMT_SMR.1.2 (b)

The TSF shall be able to associate **the ESXi** users with **the above mentioned** roles.

Dependencies: FIA_UID.1 Timing of identification

.

6.2.6 Class FPT: Protection of the TSF

FPT_ITC.1 Inter-TSF confidentiality during transmission
Hierarchical to: No other components.

FPT_ITC.1.1
The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Dependencies: No dependencies

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.

FPT_ITT.1.1
The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

.

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The ~~TSF~~ **Web Client, DCUI and ESXi Shell** shall terminate an interactive session after a [*authorized administrator specified time period of user inactivity*].

Dependencies: No dependencies

.

6.2.8 Trusted Path/Channel

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTA_TRP.1.1

The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure, *no other confidentiality violations*].

FTP_TRP.1.2

The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [initial user authentication, *and all other TSF management functions performed via the SSH Interface and Web Client.*]

Dependencies: No dependencies

.

6.2.9 Class EXT_VDS: Virtual Machine Domain Separation

EXT_VDS_VMM.1 ESXi virtual machine domain separation
Hierarchical to: No other components.

EXT_VDS_VMM.1.1
The TSF shall maintain a security domain for the execution of each virtual machine that protects the virtual machine from interference and tampering by untrusted subjects or subjects from outside the scope of the VM.

EXT_VDS_VMM.1.2
The TSF shall enforce separation between the security domains of VMs that the TOE controls.

Dependencies: No dependencies

.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2, augmented with ALC_FLR.2. Table 16 – Assurance Requirements summarizes the requirements.

Table 16 – Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.3 Systematic flaw remediation
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.2 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 17 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	EXT_FAU_STG.1	External audit trail storage
	FAU_SAR.1	Audit review
Alarm Generation	EXT_FAU_ARP.1	System event automatic response
Cryptographic Support	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute-based access control
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
	FDP_RIP.1	Subset residual information protection
Identification and Authentication	FIA_SOS.1	Specification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	EXT_FIA_VC_LOGIN.1	vCenter single sign-on user login request
Security Management	FMT_MSA.1(a)	Management of security attributes (vSphere Information Flow Control)
	FMT_MSA.1(b)	Management of security attributes (vSphere Access Control)
	FMT_MSA.3(a)	Static attribute initialization (vSphere Information Flow Control)

.

TOE Security Function	SFR ID	Description
	FMT_MSA.3(b)	Static attribute initialization (vSphere Access Control)
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1(a)	Security roles (vCenter Server)
	FMT_SMR.1(b)	Security roles (ESXi)
Protection of TOE Security Functions	FPT_ITC.1	Inter-TSF confientiality during transmission
	FPT_ITT.1	Basic internal TSF data transfer protection
Virtual Machine Domain Separation	EXT_VDS_VMM.1	ESXi virtual machine domain separation
TOE Access	FTA_SSL.3	TSF-initiated termination
Trusted Path/Channel	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The auditing security function of the TOE is provided by both the ESXi and vCenter Server. Audit data collected by the ESXi are stored in a flat file on the ESXi. Audit data collected by the vCenter Server are stored as events separately on the vCenter Server Database. Centralized storage of audit data for multiple ESXi hosts is provided by the vCenter Syslog Collector. The TOE audit records contain the following information:

Table 18 – Audit Record Contents

Field	Content
Timestamp	Date and time of the event
Class	Type of event
Source	Subject identity
Event State	Outcome

Each audit record generated includes the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event, and virtual machine, scheduled task, or alarm identity if applicable. For invalid identification attempts, the identity of the user name supplied is also recorded.

The vCenter Server audit records are stored as events, and are managed by the vCenter Server Security Management Functionality. They are stored separate from ESXi audit records on the vCenter Server Database. The vCenter Server provides the capability to review its audit records by reviewing the event logs stored on the vCenter Server Database. Event logs are associated with objects, and access to the event logs is determined by access to the object associated with the event log. Administrators who can access a particular VM or VM Group can access the event logs for that organizational grouping. Audit events are viewed through the vSphere Client under the event tab for each organizational object. Likewise, audit events can be viewed through the vSphere Web Client.

The ESXi audit records are stored in flat files in the underlying filesystem and are accessible via the Direct Console User Interface, and also through the vSphere Client. ESXi provides the capability to review its audit records which are stored in /var/log/*. Review of the the audit records on the ESXi host is restricted to the ESXi System Administrator.

The vSphere Syslog Collector is a software tool that is used to backup and restore ESXi logs and provide separate centralized log storage for one or more ESXi hosts.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, EXT_FAU_STG.1

7.1.2 Alarm generation

Alarms are notifications that occur in response to selected events, conditions, and states that occur with objects managed by the vCenter Server. The vCenter Server is configured with a set of predefined alarms that monitor clusters, hosts, datacenters, datastores, networks, and virtual machines. Each predefined alarm monitors a specific object and applies to all objects of that type. For example, by default, the Host CPU Usage alarm is set automatically on each ESXi host in the inventory and triggers automatically when any host's CPU usage reaches the defined CPU value.

Alarms are composed of two parts, a trigger and an action:

1. Trigger – A set of conditions that must be met for an alarm warning and alert to occur. Most triggers consist of a condition value and a length of time that value is true. For example, the pre-defined virtual machine memory alarm triggers a warning when memory usage is over 75% for one hour and 90% for five minutes. VMware uses colors to denote alarm severity:

    - Normal – Green
    - Warning – Yellow
    - Alert – Red

    The vCenter Server System Administrator can set alarms to trigger when the state changes from green to yellow, yellow to red, red to yellow, and yellow to green. Triggers are defined for the default VMware alarms. The vCenter Server Administrator can change the trigger conditions (thresholds, warning values, and alert values) for the default alarms.

2. Action – The operation that occurs in response to the trigger. For example, an email notification can be sent to one or more administrators when an alarm is triggered. The default vCenter Server alarms are not preconfigured with actions. The vCenter Server Administrator must manually set what action occurs when the triggering event, condition, or state occurs.

If the predefined vCenter Server alarms do not account for the condition, state, or the event that needs to be monitored, the TOE users can define custom alarms, modify or disable the pre-defined alarms. The TOE users also have the option of removing the predefined alarms that are not needed. The TOE users use the vSphere Client and vSphere Web Client to create, modify, and remove alarms.

TOE Security Functional Requirements Satisfied: EXT_FAU_ARP.1

7.1.3 Cryptographic Support

The TOE protects the confidentiality and integrity of all data as it passes between the remote components of the TOE, or from the TOE to another trusted IT product. The TOE achieves this by using TLS and SSH which perform the encryption and the decryption of data that is being passed.

.

The TOE implements CAVP-validated cryptographic algorithms to handle all cryptographic functions for the encryption and the decryption of data. Specifically, the TOE includes cryptographic providers that implement the functionality outlined in Table 19:

Table 19 – vSphere Cryptographic Providers

Cryptographic Provider	Algorithms	Purpose	Certificate No.
VMware ESXi Cryptographic Engine version 5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications; Verification of VUM updates	AES-CBC - #2723 TDES-CBC - #1639 RSA PKCS1 v1_5 - #1416 SHA-1 - #2293 HMAC - #1702
VMware vSphere Web Client Cryptographic Engine v5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications	AES-CBC - #2733 TDES-CBC - #1646 RSA PKCS1 v1_5 - #1425 SHA-1 - #2303 HMAC - #1712
VMware vSphere Cryptographic Engine for Windows v5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications; Verification of VUM updates	AES-CBC - #2731 TDES-CBC - #1644 RSA PKCS1 v1_5 - #1423 SHA-1 - #2301 HMAC - #1710
VMware vCLI Cryptographic Engine for Windows v5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications	AES-CBC - #2727 TDES-CBC - #1641 RSA PKCS1 v1_5 - #1419 SHA-1 - #2297 HMAC - #1706
VMware vSphere Core Cryptographic Engine for Linux v5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications	AES-CBC - #2729 TDES-CBC - #1642 RSA PKCS1 v1_5 - #1421 SHA-1 - #2299 HMAC - #1708
VMware vSphere Common Cryptographic Engine for Linux v5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications	AES-CBC - #2730 TDES-CBC - #1643 RSA PKCS1 v1_5 - #1422 SHA-1 - #2300 HMAC - #1709
VMware vSphere Appliance Cryptographic Engine for Linux v5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications	AES-CBC - #2732 TDES-CBC - #1645 RSA PKCS1 v1_5 - #1424 SHA-1 - #2302 HMAC - #1711
VMware vCenter SSO Cryptographic Engine v5.1	AES-CBC TDES-CBC RSA PKCS1 v1_5 SHA-1 HMAC	Protecting TSF data communications	AES-CBC - #2724 TDES-CBC - #1640 RSA PKCS1 v1_5 - #1417 SHA-1 - #2294 HMAC - #1703

TOE Security Functional Requirements Satisfied: FCS_COP.1

7.1.4 User Data Protection

The ESXi host enforces the vSphere Information Flow Control policy. ESXi implements vSwitches, vNetwork Distributed Switches, VLANs, and a basic ESXi firewall, all of which are configurable by authorized administrators. The vSphere Information Flow Control Policy establishes flow control between virtual machine network adapters and the physical adapters on an ESXi host. VMs are only permitted to communicate with those hosts within the same logical VLAN or subnet, as well as the interface of the virtual switch associated with the network to which the virtual adapter belongs. The evaluated configuration comprises a separate virtual switch attached to a dedicated physical adapter on the ESXi host, which is connected to a dedicated management network isolated from all other VM traffic. This isolation ensures that users with access to the VMs cannot interfere with the operation of the ESXi host by gaining access to its management services. Additionally, the management interface may be further restricted using the ESXi Firewall, which defines the services available to hosts on the management network.

In addition, ESXi and vCenter Server both implement the vSphere Access Control SFP by enforcing access control permissions, which define the privileges granted for vCenter SSO users and ESXi users accessing hosts and VM objects.

7.1.4.1 Virtual Switch

A virtual switch (vSwitch) works like a physical Ethernet switch. It detects which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines on the same host machine. When two or more virtual machines are connected to the same vSwitch, network traffic between them is routed locally. If an uplink adapter is attached to the vSwitch, then each virtual machine can access the external network that is connected to the adapter.

Each virtual machine on a single host that is configured for networking is logically connected to a vSwitch by the ESXi. The vSwitch provides functionality identical to that of a hardware Ethernet switch, although the implementation is solely in software: the source and destination identifiers of network data packets entering the vSwitch via any of its virtual interfaces (which can be connected either to physical network interfaces, virtual machine virtual network interfaces, or other vSwitches) are analyzed and the packet is delivered only to the appropriate virtual interface – the vSwitch will not deliver packets to unintended virtual interfaces. Administrators can also configure VLANs on a vSwitch. A vSwitch VLAN will create a virtual network within the vSwitch that allows specified virtual interfaces to communicate only with other specified virtual interfaces on the same logical broadcast domain – broadcast traffic addressed to or from interfaces that are not part of the VLAN will not be delivered by the vSwitch.

7.1.4.2 Distributed Virtual Switch

A vNetwork Distributed Switch functions similarly to a vSwitch. Each ESXi host can implement one or more switches and they can be any combination of vSwitches and vNetwork Distributed Switch. A vNetwork Distributed Switch allows virtual machines across multiple host machines to be logically connected via the same vNetwork Distributed Switch. Like a vNetwork Standard Switch, each vNetwork Distributed Switch is a network hub that virtual machines can use. A vNetwork Distributed Switch can forward traffic between virtual machines located across hosts or link to an external network by connecting to physical Ethernet adapters, also known as uplink adapters. A vNetwork Distributed Switch functions as a single virtual switch across all associated hosts. This enables an authorized administrator to set network configurations that span across all member hosts, and allows virtual machines to maintain consistent network configuration as they migrate across multiple hosts.

Each virtual machine that is configured for networking is logically connected to a vNetwork Distributed Switch by the ESXi. The vNetwork Distributed Switch provides functionality identical to that of a hardware Ethernet switch. Although the implementation is solely in software, the source and destination

identifiers of network data packets entering the vNetwork Distributed Switch via any of its virtual interfaces (which can be connected either to physical network interfaces, virtual machine virtual network interfaces, or other vNetwork Distributed Switches) are analyzed and the packet is delivered only to the appropriate virtual interface. The vNetwork Distributed Switch will not deliver packets to unintended virtual interfaces. Administrators can also configure VLANs on vNetwork Distributed Switch. A vNetwork Distributed Switch VLAN will create a virtual network within the vNetwork Distributed Switch that allows specified virtual interfaces to communicate only with other specified virtual interfaces – traffic addressed to or from interfaces which are not part of the VLAN will not be delivered by the vNetwork Distributed Switch. Further segmentation may be provided using Private VLANs, which create "private" groups of hosts. Only those hosts within a Private VLAN may see other hosts within the same Private VLAN.

7.1.4.3 ESXi Firewall

The ESXi host contains a basic firewall which enables an administrator to restrict the services accessible to a remote user based on customizable rulesets comprised of source IP addresses/subnets, and destination port numbers for services running on the ESXi host. By default, the firewall permits all traffic to services on the ESXi management interface; however the rulesets may be configured by an administrator to further restrict the network devices which are allowed to communicate with services on the host.

7.1.4.4 ESXi Access Control

The TOE enforces the vSphere Access Control SFP on users accessing objects (VMs, ESXi host resources), based on permissions assigned to a user's role. Permissions grant users the privileges necessary to perform specific tasks. Both ESXi and vCenter Server implement the same set of privileges on objects in the following categories: Alarms, Datacenter, Datastore, Datastore Cluster, Distributed Virtual Port Group, ESX Agent Manager, Extension, Folder, Global, Host CIM, Host Configuration, Host Inventory, Host Local Operations, Host vSphere Replication, Host Profile, Network, Performance, Permissions, Profile-driven Storage, Resource, Scheduled Task, Sessions, Storage Views, Tasks, vApp, Virtual Machine Configuration, Virtual Machine Guest Operations, Virtual Machine Interaction, Virtual Machine Inventory, Virtual Machine Provisioning, Virtual Machine State, Virtual Machine vSphere Replication, vServices, vSphere Distributed Switch, and VRM Policy.

In addition to object permissions, the TOE provides complete access control over ESXi hosts via the ESXi lockdown mode. In this mode, only the *vpxuser* account may authenticate and perform operations directly on the host on behalf of vCenter users. Lockdown mode forces users to access hosts and VMs through the vCenter Server. When in lockdown mode, users are denied direct access to the ESXi host unless they have been granted the DCUI Access privilege.

7.1.4.5 Secure VMDK Deletion

To prevent sensitive data contained with VMDK files from being accessed by users with physical access to a disk once the file has been de-associated from the VM, the ESXi host provides a utility which allows administrators to overwrite the contents of the file with zeroes, making it difficult for the contents to be reconstructed.

TOE Security Functional Requirements Satisfied: FDP_ACC.2, FDP_ACF.1, FDP_IFC.2, FDP_IFF.1, FDP_RIP.1

7.1.5 Identification and Authentication

The TOE enforces identification and authentication in a variety of ways. Users access the ESXi and vCenter servers through the methods described below.

7.1.5.1 ESXi

For each ESXi interface (vSphere Client, DCUI, and ESX Shell), administrators are required to identify and authenticate themselves before any action is allowed to be performed. When a user logs into the ESXi

host, a user name and password are requested before access is given. These authentication credentials are compared with the authentication credentials stored on the ESXi in a shadow file, where the password is hashed using SHA-1. In addition, ESXi can participate in an Active Directory (AD) infrastructure and can use the credentials provided by AD for authorization. If the authentication credentials are valid, access to the system is provided, with the privileges appropriate to the role assigned to that user. If the credentials are not valid, the user is presented with another chance to provide valid credentials. Failed and successful user login events are captured in the system logs.

No users on the ESXi host or the vCenter Server, other than the vCenter Server administrator, have access to the *vpxuser* (defined in Section 7.1.6) passwords stored in the vCenter Server database. These users are fully subject to the access control rules. Below are a few important characteristics of the *vpxuser* password.

- The *vpxuser* password is machine-generated.
- The *vpxuser* password is stored in encrypted form. It is never exposed in plaintext.
- The *vpxuser* password for each ESXi host under the management of a vCenter Server is unique for that ESXi host. Thus, it is a one to many relationships: a single vCenter Server possessing many (and unique) *vpxuser* passwords for all the ESXi hosts it manages.

7.1.5.2 vCenter SSO

vCenter SSO serves as a central repository of user identity information, which enables multiple vCenter instances and other vSphere components to be associated with a single set of authorized accounts. When users log in to the vSphere Web Client with a user name and password, their credentials are sent to the vCenter SSO server. The SSO server validates these credentials against the back-end identity source(s). vCenter SSO is configured to use either a local database, OS accounts, or an external repository, such as AD, as its identity sources. Upon successful validation, it returns a security token to the client, which grants access to other systems within the environment. If the login is valid, the user at the vSphere Web Client is presented with the vSphere Web Client interface denoting a successful login. If the login is invalid, a message is displayed, and the login window remains available for the user to retry. Failed and successful user login events are captured in the system logs for the vSphere Web Client.

When a user logs into vCenter Server and vCenter Server Virtual Appliance using the vSphere Client, they are presented with a login screen, requesting the vCenter Server hostname or IP address, the user name, and the user password. The user information is passed to vCenter SSO, or to the underlying operating system, depending on the type of account used to authenticate. The user credentials are verified, and, if the login is valid, the user at the vSphere Client is presented with the vSphere Client interface denoting a successful login. If the login is invalid, a message is displayed, and the login window remains available for the user to retry. Failed and successful user login events are captured in the system logs for the vSphere Client.

The vCenter SSO Server is installed with a default administrator account (*admin@System-Domain*). This account is only granted permission to configure the SSO parameters using the vSphere Web Client. It does not have access to the vCenter Server. By default, local operating system accounts in the Administrators group can log into the vSphere Web Client and vCenter Server, but cannot configure vCenter SSO parameters.

In addition, vCenter Server authenticates with ESXi on behalf of vSphere Update Manager, which is a software service that is used to apply patches and updates across ESXi hosts and all supported guest operating systems. This is achieved using the *vpxuser* account. When VUM is installed, it registers with the vCenter Server. VUM instructs ESXi to scan for compliance against a pre-defined or custom user created baseline and then installs an ESXi image which could consist of single or selected group of patches. ESXi will only call the instructed VUM instance, thereby ensuring that only the VUM instance that is installed with the TOE will be used to transfer updates and patches to the ESXi.

When configured to use local SSO authentication, SSO accounts must be at least eight characters with at least six alphabetic characters and one special character, and no two adjacent characters may be identical. ESXi account passwords must meet the following password complexity requirements using a mix of lowercase, uppercase, numbers, and special characters:

- Passwords containing characters from one or two character classes must be at least eight characters long.
- Passwords containing characters from three character classes must be at least seven characters long.
- Passwords containing characters from all four character classes must be at least six characters long.

TOE Security Functional Requirements Satisfied: FIA_SOS.1, FIA_UAU.2, FIA_UID.2, EXT_FIA_VC_LOGIN.1

7.1.6 Security Management

Security management specifies how the ESXi manages several aspects of the TSF including TSF data and security functions. TSF data includes configuration data of the TOE, audit data, and system data. For a detailed listing of TSF data managed by the TOE see Table 15 of this ST. The TOE provides authorized administrators with management consoles as described in section 1.4.1 to easily manage the security functions and TSF data of the TOE.

ESXi supports two administrator roles: *system administrator* and *VM administrator*. The *system administrator* role can be assigned to three different kinds of user accounts. These are:

1. *root* – The *system administrator* role is implemented using the *root* account of the underlying POSIX[34] operating environment. Users log into the *root* account and give the *root* password in order to use this role.

2. *individual user* – It is also possible to assign a *system administrator* role to an individual user account. For example, an account name of *jsmith* can be assigned to a role of *system administrator*, thus making that particular individual user (e.g. *John Smith*) a System Administrator on the ESXi host. Assigning the *system administrator* role to different user accounts (rather than *root* account alone) helps in maintaining security through traceability.

3. *vpxuser* – The *vpxuser* account is used by the vCenter Server when it manages activities for the connected ESXi host. The *vpxuser* account is initially created when the vCenter Server adds the ESXi host as one of its managed hosts for the first time.

It should be noted that the vCenter Server administrator supplies the username and password for either the *root* account or the user account with a *system administrator* role, when adding the ESXi host for the first time. When this authentication with the ESXi host is successful, a special account called *vpxuser* is created on the ESXi host along with a *vpxuser* machine generated password known only to the vCenter Server and the specific ESXi host. This login account (*vpxuser* account) and password *(vpxuser* password) are used for all subsequent connections between the ESXi host and the vCenter Server. If the ESXi host is later managed by a different vCenter Server, a new unique *vpxuser* password is generated; passwords for this account are never reused.

VM administrators are administrators of one or more VMs on the ESXi host. VM administrators can access the VMs by directly logging into the ESXi host or through the vCenter Server via the *vpxuser* account and password. When logging in through the vCenter Server, the vCenter Server uses the *vpxuse*r account and password to gain access to the ESXi host and process the requests on behalf of the VM administrators.

[34] Portable Operating System Interface for Unix

The TOE supports a combination of access control as detailed in Table 13. Users, groups, roles, and permissions are used to control who is allowed access to the vSphere managed objects and the specific actions that are allowed. vCenter Server and ESXi hosts determine the level of access for the user based on the permissions associated with the roles assigned to said user. The combination of user name, password, and permissions is the mechanism by which vCenter Server and ESXi hosts authenticate a user for access and authorize the user to perform activities.

The servers and hosts maintain lists of authorized users and the permissions assigned to each user. Privileges define basic individual rights that are required to perform actions and read properties. ESXi and vCenter Server use sets of privileges or roles to control which users or groups can access particular vSphere objects.

ESXi and vCenter Server provide a set of pre-established roles and allow for roles to be defined by administrators. The privileges and roles assigned on an ESXi host are separate from the privileges and roles assigned on vCenter Server. However, the privileges implemented by ESXi and vCenter Server are the same. Only the privileges and roles assigned through the vCenter Server system are available to administrators managing a host through vCenter Server. ESXi privileges may be managed by either an ESXi host or vCenter Server. Refer to Table 13 for a detailed listing of operations that are performed per specific data and role.

The vCenter Server supports three categories of roles: vCenter SSO Administrator, vCenter Server Administrator and Administrator-defined roles. The vCenter SSO Administrator role is responsible for managing vCenter SSO users and groups, and by default does not have vCenter Server access. This is implemented as the *admin@system-domain* user in the default SSO repository. The vCenter SSO Administrator role may be associated with local SSO accounts, as well as local OS accounts or directory accounts. The vCenter Server Administrator is implemented by membership in the "Administrators" group of the underlying Windows OS for vCenter Server. Users log in using their username and password, and are automatically assigned in this role by virtue of their membership in the Administrators group. The vCenter Server Virtual Appliance Administrator is implemented by the root account on the POSIX operating environment. In addition, vCenter SSO users and groups (local and directory-based) can also be associated with vCenter Server roles, as assigned by a vCenter Server Administrator. Administrator-defined roles enable an authorized vCenter Server Administrator to custom tailor a set of privileges and assign them to a custom role.

Note: A vCenter Server Administrator and vCenter SSO Administrator may be associated with the same account; however, by default, SSO Administrator and vCenter Server roles are separate.

All other users (aside from those configured by installation defaults) have no permissions on any objects, and therefore they cannot perform operations on them until an administrator has assigned them the required privilege.

TOE Security Functional Requirements Satisfied: FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_MTD.1, FMT_SMF.1, FMT_SMR.1(a), FMT_SMR.1(b)

7.1.7 Protection of the TOE Security Functions

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that physical connections made to the TOE remain intact and unmodified. The TOE protects information as it is transmitted between distributed components and between the TOE and external entities using FIPS approved algorithms provided by various cryptographic engines within the TOE.

Protection of the TSF is implemented in various ways:

- The vSphere Web Client Cryptographic Engine provides secure TLS connections for communications between a remote web browser and the vSphere Web Client.
- The vSphere Cryptographic Engine for Linux provides TLS support for communications between web browsers and the vCenter Server Appliance, and communications between the vSphere Client and the vCenter Server Appliance.
- The vSphere Client, vCenter Server, vCenter Update Manager, vSphere Syslog Collector, and vCenter Inventory Service all make use of the vSphere Cryptographic Engine for Windows for protected TLS communications between distributed components, as well as protection of syslog data sent from ESXi (vSphere Syslog Collector), and firmware signature verification on ESXi updates (VUM).
- The vCenter SSO Cryptographic Engine provides TLS for communications with vCenter SSO and LDAPS support for remote authentication servers.
- The ESXi Cryptographic Engine provides secure TLS communications for communications between vSphere Client/vCenter Server and ESXi.
- The vCLI Cryptographic Engine for Windows provides secure TLS communications for commands sent to vCenter Server or ESXi from the vCLI running on a Windows platform. The Linux-based vCLI uses the vSphere Cryptographic Engine for Linux.

TOE Security Functional Requirements Satisfied: FPT_ITC.1, FPT_ITT.1

7.1.8 Virtual Machine Domain Separation

The virtual machine separation security function of the TOE is provided by the ESXi component. The TOE ensures that each virtual machine is isolated from any other virtual machines co-existing on the ESXi. This isolation is provided at the virtualization layer, or VMKernel, of the ESXi. The VMKernel of the ESXi ensures that virtual machines are unable to directly interact with other virtual machines yet still allow for physical resources to be shared among the existing virtual machines.

The ESXi VMKernel provides a virtual hardware environment which controls the host hardware and schedules the allocation of the underlying physical resources associated with each virtual machine. Each virtual machine runs its own operating system and applications: they cannot communicate with each other in unacceptable or unauthorized ways. The following mechanisms ensure this:

- Shared memory access: The memory allocation mechanisms prevent the sharing of writable memory. Each VM is assigned memory that belongs exclusively to it.

- Read-only memory: For efficiency, multiple VMs may use the same memory pages , and in these cases, the memory locations are shared, but in a read-only mode. This effectively saves memory without providing a communication channel between VMs.

- Communication between VMs through standard network connections can be permitted or prevented as desired. These standard networking mechanisms are similar to those used to connect separate physical machines.

Each virtual machine appears to run on its own processor, fully isolated from other virtual machines with its own registers, buffers, and other control structures. Most instructions are directly executed on the physical processor, allowing compute-intensive workloads to run at near-native speed. Memory appears contiguous to each virtual machine, but instead, noncontiguous physical pages are remapped efficiently and presented transparently to each virtual machine.

The ESXi VMKernel mediates all access to physical hardware resources[35], including CPU, memory, and I/O devices, ensuring that VMs cannot circumvent this level of isolation and gain access to the physical hardware. A VM can only detect the virtual devices made available to it:

- VM storage: Virtual machines use virtual disks to store OS, program files, and other data. Each VM is given its own virtual disk file that is not visible to other VMs. Virtual disks are accessed using virtual SCSI controllers. Virtual disk files reside on vSphere Virtual Machine File System (VMFS) or an NFS-based datastore. The virtual disk appears to the VM as if it is a SCSI drive attached to a physical SCSI controller. VMware supports parallel SCSI, iSCSI, network, Fibre Channel, or FCoE[36] based storage. The physical access method is completely transparent to the guest OS and applications residing within a VM.

- Removable storage: ESXi also provides virtualization of removable storage by enabling access to the client machine's CD-ROM[37] or floppy drive, or using a logical CD or floppy image file mounted from ESXi storage, or remotely via the vSphere Client and Web Client interfaces. It also provides Client USB redirection to allow devices on the remote client to be attached to the VM.

- Input/output devices: Input to the machine running the vSphere Client or Web Client is redirected through a Mouse-Keyboard-Screen session. Video output is directed back to the client interface through this session.

- Serial and parallel communications: A virtual serial or parallel port may be attached to a VM which allows connection of a physical serial port or to a file on the host computer. A direct connection may also be established between two virtual machines or between a virtual machine and an application on the host computer.

TOE Security Functional Requirements Satisfied: EXT_VDS_VMM.1

7.1.9 TOE Access

The TOE Access function provides for controlling the establishment of a user's session. The TOE will terminate an interactive DCUI, Web Client, or ESXi Shell session after an authorized administrator specified time period of user inactivity. Only once a user successfully identifies and authenticates to the TOE again will they resume access to the TOE.

TOE Security Functional Requirements Satisfied: FTA_SSL.3

7.1.10 Trusted Path/Channel

The TOE is protected using a server-authenticated HTTPS connection between the end-user web browser and the external web-enabled interfaces of the TOE. The TLS handshake protocol and the algorithms for encryption/message authentication are provided by the vSphere Web Client Cryptographic Engine, vSphere Cryptographic Engine for Windows, and the vSphere Cryptographic Engine for Linux. The vCenter Server and ESXi host may use a self-signed certificate, or a certificate issued by a trusted certificate authority. This certificate is presented to the user during the handshake and is used to establish a secure management path for the TOE. In addition, the ESXi Shell interface is protected via SSH, which is provided by the ESXi Cryptographic Engine.

TOE Security Functional Requirements Satisfied: FTP_TRP.1

[35] For a full list of hardware available to VMs, please refer to the vSphere Virtual Machine Administration Guide, section "Virtual Machine Hardware Available to vSphere Virtual Machines"
[36] FCoE – Fibre Channel over Ethernet
[37] CD-ROM – Compact Disc Read-Only Memory

8 Rationale

8.1 Conformance Claims Rationale

There are no protection profile conformance claims for this security target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 20 displays the mapping of threats to objectives.

Table 20 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.COMINT An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE by bypassing a security mechanism.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective ensures that unauthorized modifications and access to functions and data is prevented. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The O.ADMIN objective requires that only authorized users are able to manage the security attributes of the TOE.
	O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The O.IDAUTH objective, supported by the OE.IDAUTH objective, requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data.

.

Threats	Objectives	Rationale
	O.SECURE The TOE must ensure the confidentiality and integrity of all data as it passes between the remote components of the TOE, from the TOE to another trusted IT product, or between the TOE and remote users.	The O.SECURE objective ensures that TOE data is protected when transmitted between remote components of the TOE.
	OE.IDAUTH The IT Environment will provide reliable verification of the vSphere SSO user credentials for non-TOE accounts.	The O.IDAUTH objective, supported by the OE.IDAUTH objective, requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.
	OE.SEP The TOE environment must protect itself and the TOE from external interference or tampering.	The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
T.MISCONFIGURE An authorized ESXi administrator or unauthorized attacker may directly access a host and modify its configuration in a way that is inconsistent with the vCenter Server.	O.SEPARATE The TOE must provide capabilities for separation of administrator duties, and prevent ESXi administrators from configuring hosts in a manner that is inconsistent with vCenter policies.	O.SEPARATE ensures that ESXi hosts may only be accessed by vCenter users or users given explicit direct console access.
T.PRIVIL An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective provides that all access is compliant with the TSP.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage the functions and data of the TOE.

.

Threats	Objectives	Rationale
	O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	This threat is primarily diminished by the O.IDAUTH objective, supported by the OE.IDAUTH objective, which requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	OE.IDAUTH The IT Environment will provide reliable verification of the vSphere SSO user credentials for non-TOE accounts.	This threat is primarily diminished by the O.IDAUTH objective, supported by the OE.IDAUTH objective, which requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps which includes the date and time of any action done on the TOE. If an intrusion occurs, a reliable audit entry with the date and timestamp will be recorded.
T.REUSE An unauthorized individual with access to a decommissioned hard drive may be able to view the sensitive information contents of a VMDK file.	O.DESTROY The TOE must provide the ability to securely destroy virtual machine disk images.	O.DESTROY ensures that the contents of a VMDK are securely overwritten with zeroes to prevent residual reuse.
T.VIRTUAL_NETWORK A process running on a virtual machine attempts to deliver traffic to wrong VM or external entity.	O.VSWITCH The TOE must ensure that network traffic traversing a vSwitch is only delivered to the intended virtual machines and physical interfaces.	O.VSWITCH requires that the vSwitch must deliver network traffic only to the virtual machines and/or physical interfaces for which it is intended.

.

Threats	Objectives	Rationale
T.VM A process running on one virtual machine might compromise the security of processes running on other virtual machines.	O.VM The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.	This threat is mitigated by the O.VM objective which requires the ESXi host component to provide a domain of execution in order to protect from interference and tampering by virtual machines. The virtualization layer of the ESXi host ensures that virtual machines are unable to directly interact with other virtual machines.
	OE.SEP The TOE environment must protect itself and the TOE from external interference or tampering.	The OE.SEP mitigates this threat by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.
T.WEAKIA A user may supply the TOE with a weak password that is easily guessable based on dictionary words.	O.IDAUTH2 The TOE must enforce strong password complexity and minimum length requirements for TOE users.	O.IDAUTH2 ensures that users are required to supply the TOE with strong passwords that are not easily guessed or brute-forced.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 21 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.	NOE.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.	The NOE.NOEVIL objective ensures that operators are non-hostile, appropriately trained, and follow all operator guidance.
A.PHYSCL The ESXi host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access.	NOE.PHYSCL The ESXi host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access.	The NOE.PHYSCL objective requires that the ESXi and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

.

8.3 Rationale for Extended Security Functional Requirements

The TOE contains the following explicitly stated security functional requirements:

- EXT_FAU_ARP.1
- EXT_FAU_STG.1
- EXT_FIA_VC_LOGIN.1
- EXT_VDS_VMM.1

EXT_FAU_ARP.1 was explicitly stated because the vCenter Server is configured with a set of predefined alarms that monitor the status of the TOE components. When the vCenter Server detects a potential system malfunction or a system performance degradation, it generates an alarm for such event. This requirement is based in part on FAU_ARP.1.

EXT_FAU_STG.1 was explicitly stated because the backup and restore of audit data onto a remote machine is not directly provided in the standard CC PART 2 FAU SFRs. This SFR describes the backup and restore capabilities of the vCenter Syslog Collector. This requirement is based in part on FAU_STG.1.

EXT_FIA_VC_LOGIN.1 was explicitly stated because authentication and identification of the vCenter Server users is performed by vCenter SSO, which may use a combination of accounts managed by both the TOE and the TOE Environment. This explicit requirement was written to make the link between the Identification and Authentication security function provided by the environment, and the actions that the vCenter SSO Server takes to ensure that only identified and authenticated users can access the TOE via the vCenter Server, because there is no CC requirement that can quite do this. This requirement is based in part on FIA_UAU.1 and FIA_UID.1.

EXT_VDS_VMM.1 is an explicitly-stated functional requirement. The SFR family "Virtual machine domain separation" was created to specifically address the separation of virtual machines from each other when running within the TOE, as opposed to separation of the TOE's domain of execution from outside entities. The SFR in this family has no dependencies since the stated requirement embodies all necessary security functions. This requirement exhibits functionality that can easily be documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security assurance requirements.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 22 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	EXT_FIA_VC_LOGIN.1 vCenter single sign-on user login request	For vCenter SSO, the TOE requires support from the TOE environment to verify non-local SSO user credentials.
	FDP_ACC.2 Complete access control	The TOE provides total access control over host and VM resources based on permissions.
	FDP_ACF.1 Security attribute-based access control	The TOE only permits operations to be performed on objects based on the permissions associated with a user's role.
	FIA_UAU.2 User authentication before any action	The TOE will not give any access to a user until the TOE has identified (FIA_UID.2) and authenticated (FIA_UAU.2).
	FIA_UID.2 User identification before any action	The TOE will not give any access to a user until the TOE has identified (FIA_UID.2) and authenticated (FIA_UAU.2).
	FTA_SSL.3 TSF-initiated termination	The requirement meets the objective by locking an unattended session when it has exceeded the time limit configured by the VM Administrator.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MSA.1(a) Management of security attributes (Virtual and Distributed Switch Information Flow Control)	Only the roles defined in FMT_SMR.1 are given the right to modify or set defaults for TOE security attributes.
	FMT_MSA.1(b) Management of security attributes (vSphere Access Control)	Only the roles defined in FMT_SMR.1 are given the right to modify or set defaults for TOE security attributes.
	FMT_MSA.3(a) Static attribute initialization (Virtual and Distributed Switch Information Flow Control)	Restrictive default values for the security attributes of the Virtual Switch are provided and the authorized administrator can change them.
	FMT_MSA.3(b) Static attribute initialization (vSphere Access Control)	Restrictive default values for the ESXi and vCenter permissions are provided and only the authorized administrator can change them.

.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that only authorized users are allowed access to TSF data.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1(a) Security roles (vCenter Server)	The requirement meets the objective by ensuring that the TOE provides roles with differing privileges for the management of the TOE.
	FMT_SMR.1(b) Security roles (ESXi)	The requirement meets the objective by ensuring that the TOE provides roles with differing privileges for the management of the TOE.
O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	EXT_FAU_STG.1 External audit trail storage	The TOE ensures the backup of the ESXi log files to a separate part of the TOE.
	FAU_GEN.1 Audit data generation	Security-relevant events must be audited by the TOE.
	FAU_SAR.1 Audit review	The TOE must provide the ability to review the audit trail of the system.
O.DESTROY The TOE must provide the ability to securely destroy virtual machine disk images.	FDP_RIP.1 Subset residual information protection	The TOE provides cabilities to overwrite virtual disk images with zeroes to prevent reuse or disclosure of the information contained within the images.
O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	EXT_FIA_VC_LOGIN.1 vCenter single sign-on user login request	For non-local vCenter SSO users, the TOE requires support from the TOE environment to verify the user credentials.
	FIA_UAU.2 User authentication before any action	The TOE will not give any security sensitive access to a user until the user has been identified (FIA_UID.2) and authenticated (FIA_UAU.2).
	FIA_UID.2 User identification before any action	The TOE will not give any security sensitive access to a user until the user has been identified (FIA_UID.2) and authenticated (FIA_UAU.2).

.

Objective	Requirements Addressing the Objective	Rationale
O.IDAUTH2 The TOE must enforce strong password complexity and minimum length requirements for TOE users.	FIA_SOS.1 Specification of secrets	The vCenter SSO Server and ESXi host both enforce strong password complexity and minimum length requirements.
O.SECURE The TOE must ensure the confidentiality and integrity of all data as it passes between the remote components of the TOE, from the TOE to another trusted IT product, or between the TOE and remote users.	FCS_COP.1 Cryptographic operation	The System must protect the confidentiality of information during transmission to a remote component of the TOE.
	FPT_ITC.1 Inter-TSF confientiality during transmission	The TOE shall protect all TOE data transmitted from the TOE to another trusted IT product from unauthorized disclosure during transmission.
	FPT_ITT.1 Basic internal TSF data transfer protection	The System must protect the confidentiality of information during transmission to a remote component of the TOE.
	FTP_TRP.1 Trusted path	The TOE protects authentication data and other TSF data from modification and disclosure using a trusted path between itself and remote users.
O.SEPARATE The TOE must provide capabilities for separation of administrator duties, and prevent ESXi administrators from configuring hosts in a manner that is inconsistent with vCenter policies.	FDP_ACC.2 Complete access control	The TOE provides separation of duties by assigning a unique set of privileges to each role appopriate for each level of access.
	FDP_ACF.1 Security attribute-based access control	The TOE prevents non-vCenter users from accessing and modifying ESXi hosts directly.
	FMT_SMR.1(a) Security roles (vCenter Server)	The vCenter Server provides separation of administrator duties by associating a unique set of privileges with the defined administrator roles.
	FMT_SMR.1(b) Security roles (ESXi)	The ESXi hypervisor provides separation of duties by associating a unique set of privileges with the defined administrator roles.
O.VM The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.	EXT_FAU_ARP.1 System event automatic response	The TOE generates automated alarms that notify the appropriate users of the TOE when there is a potential system malfunction or system performance degradation. This prevents virtual machines from not receiving the resources they require.

.

Objective	Requirements Addressing the Objective	Rationale
	EXT_VDS_VMM.1 ESXi virtual machine domain separation	The TOE must isolate each virtual machine by providing a domain of execution which is protected from interference and tampering by virtual machines.
O.VSWITCH The TOE must ensure that network traffic traversing a vSwitch is only delivered to the intended virtual machines and physical interfaces.	FDP_IFC.2 Complete information flow control	The TOE must ensure that network traffic traversing a vSwitch is only delivered to virtual machines and physical interfaces that are part of the intended VLAN.
	FDP_IFF.1 Simple security attributes	All data transmitted from or to a VM or a physical interface associated with a vSwitch will only be delivered to the intended destination.

8.5.2 Security Assurance Requirements Rationale

EAL2, augmented with ALC_FLR.3 was chosen to provide a low-to-moderate level of assurance that is consistent with secure commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. At EAL2+, the TOE will have an undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

8.5.3 Dependency Rationale

This ST satisfies all the requirement dependencies of the Common Criteria. Table 23 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 23 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
EXT_FAU_ARP.1	No dependencies	✓	
FAU_GEN.1	FPT_STM.1	No	FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable timestamps.
EXT_FAU_STG.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_COP.1	No dependencies	✓	FCS_CKM.1 and FCS_CKM.4 are not

.

SFR ID	Dependencies	Dependency Met	Rationale
			included, following the guidance of CCS Instruction #4. The cryptographic keys must be generated and destroyed by the TOE.
FDP_ACC.2	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.1(b)	✓	
	FDP_ACC.1	No	Although FDP_ACC.1 is not included, FDP_ACC.2, which is hierarchical to FDP_ACC.1, is included. This satisfies the dependency.
FDP_IFC.2	FDP_IFF.1	✓	
FDP_IFF.1	FMT_MSA.3(a)	✓	
	FDP_IFC.1	No	Although FDP_IFC.1 is not included, FDP_IFC.2, which is hierarchical to FDP_IFC.1, is included. This satisfies the dependency.
FDP_RIP.1	No dependencies	✓	
FIA_SOS.1	No dependencies	✓	
FIA_UAU.2	FIA_UID.1	No	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
EXT_FIA_VC_LOGIN.1	No dependencies	✓	
FMT_MSA.1(a)	FMT_SMF.1	✓	
	FDP_IFC.1	✓	
	FMT_SMR.1(b)	✓	
FMT_MSA.1(b)	FMT_SMR.1(a)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1(b)	✓	
	FDP_ACC.1	No	Although FDP_ACC.1 is not included, FDP_ACC.2, which is

.

SFR ID	Dependencies	Dependency Met	Rationale
			hierarchical to FDP_ACC.1, is included. This satisfies the dependency.
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_SMR.1(b)	✓	
FMT_MSA.3(b)	FMT_SMR.1(a)	✓	
	FMT_SMR.1(b)	✓	
	FMT_MSA.1(b)	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1(b)	✓	
	FMT_SMR.1(a)	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1(a)	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FMT_SMR.1(b)	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FPT_ITC.1	No dependencies	✓	
FPT_ITT.1	No dependencies	✓	
FTA_SSL.3	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	
EXT_VDS_VMM.1	No dependencies	✓	

9 Acronyms and Terms

This section describes the acronyms and terms used in this document.

Table 24 below lists the acronyms used in this document.

Table 24 – Acronyms

Acronym	Definition
ADAM	Microsoft Active Directory Application Mode
AD	Microsoft Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input Output Signal
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CD-ROM	Compact Disc Read-Only Memory
CIM	Common Information Model
CLI	Command Line Interface
CPU	Central Processing Unit
DB	Database
DES	Data Encryption Standard
DCUI	Direct Console User Interface
DRS	Distributed Resource Scheduler
EAL	Evaluation Assurance Level
FCoE	Fibre Channel over Ethernet
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GB	Gigabyte
HA	High Availability
HCL	Hardware Compatibility List
HMAC	Hash-based Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output

.

Acronym	Definition
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
ISP	Internet Service Provider
IT	Information Technology
LDS	Lightweight Directory Services
MB	Megabyte
NFS	Network File System
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OSGI	Open Services Gateway Initiative
PKCS	Public Key Cryptography Standard
POSIX	Portable Operating System Interface for Unix
PP	Protection Profile
PVLAN	Private Virtual Local Area Network
R2	Release 2
RAM	Random Access Memory
REST	Representational State Transfer
RSASSA	RSA Signature Scheme with Appendix
SAN	Storage Area Network
SAR	Security Assurance Requirement
SCSI	Small Computer Systems Interface
SDK	Software Development Kit
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SLES	SUSE Linux Enterprise Server
SMP	Symmetric Multiprocessing
SNMP	Simple Network Management Protocol
SP	Service Pack
SQL	Structured Query Language
SSH	Secure Shell
SSO	Single Sign-On
ST	Security Target
TLS	Transport Layer Security

.

Acronym	Definition
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSC	TOE Scope of Control
TSF	TOE Security Functionality
TSP	TOE Security Policy
TXT	Trusted Execution Technology
USB	Universal Serial Bus
vCLI	vSphere Command Line Interface
vCNS	vCloud Networking and Security
vDS	vNetwork Distributed Switch
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMDK	Virtual Machine Disk
vMA	VMware Management Assistant
VMFS	Virtual Machine File System
VPXA	vCenter Server Agent
vSMP	Virtual Symmetric Multi-Processing
VUM	vSphere Update Manager

Table 25 below lists the VMware vSphere terms used in this document and gives brief descriptions.

Table 25 – VMware vSphere Terms

Term	Description
Clusters	A collection of ESXi hosts and associated virtual machines intended to work together as a unit.
Datacenters	An aggregation of all the different types of objects needed to work in virtualized computing environments: hosts, virtual machines, networks, and datastores.
Datastores	A virtual representation of combinations of underlying physical storage resources in the data center. A datastore is the storage location for virtual machine files.
Folders	A top-level structure for vCenter Server only. Folders allow the users to group objects of the same type so they can be easily managed. A folder can contain other folders, or a group of objects of the same type: datacenters, clusters, datastores, networks, virtual machines, templates, or hosts.
Hosts	The physical computer on which the virtualization platform software (hypervisor), such as ESXi, is installed and on which all virtual machines reside.

.

Term	Description
Networks	A set of virtual network interface cards (virtual NIC), virtual switches (vSwitch), and port groups that connect virtual machines to each other or to the physical network outside of the virtual datacenter.
Resource Pools	A structure that allows delegation of control over the resource of a host. Resource pools are used to compartmentalize all resources in a cluster. The managed resources are CPU and memory.
Templates	A master copy of a virtual machine that can be used to create and provision new virtual machines.
Virtual Machines	A virtualized x86 or x64 personal computer environment in which a guest operating system and associated application software can run.

Table 26 – Documentation References below lists the VMware vSphere 5.1 Guidance Documents that are referenced in this document.

Table 26 – Documentation References

Reference	Document
vSphere Virtual Machine Admin Guide	vSphere Virtual Machine Administration, ESXi 5.1, vCenter Server 5.1
vSphere Install Guide	vSphere Installation and Setup, vSphere 5.1 Update 1

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