VMware, Inc.

VMware® ESXi 4.0 Update 1 and vCenter Server 4.0 Update 1

Security Target

Evaluation Assurance Level: EAL4+
Document Version: 1.4

Prepared for:

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304

Phone: (650) 475-5000

http://www.vmware.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050

http://www.corsec.com

Table of Contents

1 INTRODUCTION 4
1.1 PURPOSE 4
1.2 SECURITY TARGET AND TOE REFERENCES 4
1.3 PRODUCT OVERVIEW 5
1.4 TOE OVERVIEW 9
1.4.1 Brief Description of the Components of the TOE 10
1.4.2 TOE Environment 13
1.5 TOE DESCRIPTION 13
1.5.1 Physical Scope 13
1.5.2 Logical Scope 16
1.5.3 Product Physical/Logical Features and Functionality not included in the TOE 18

2 CONFORMANCE CLAIMS 20

3 SECURITY PROBLEM 21
3.1 THREATS TO SECURITY 21
3.2 ORGANIZATIONAL SECURITY POLICIES 22
3.3 ASSUMPTIONS 22

4 SECURITY OBJECTIVES 23
4.1 SECURITY OBJECTIVES FOR THE TOE 23
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 24
4.2.1 IT Security Objectives 24
4.2.2 Non-IT Security Objectives 24

5 EXTENDED COMPONENTS 25
5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS 25
5.1.1 Class FAU: Security Audit 26
5.1.2 Class FIA: Identification and authentication 26
5.1.3 Class EXT_VDS: Virtual machine domain separation 27
5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS 29

6 SECURITY REQUIREMENTS 30
6.1 CONVENTIONS 30
6.2 SECURITY FUNCTIONAL REQUIREMENTS 30
6.2.1 Class FAU: Security Audit 32
6.2.2 Class FCS: Cryptographic Support 34
6.2.3 Class FDP: User Data Protection 35
6.2.4 Class FIA: Identification and Authentication 39
6.2.5 Class FMT: Security Management 40
6.2.6 Class FPT: Protection of the TSF 44
6.2.7 Class EXT_VDS: Virtual Machine Domain Separation 45
6.3 SECURITY ASSURANCE REQUIREMENTS 46

7 TOE SUMMARY SPECIFICATION 47
7.1 TOE SECURITY FUNCTIONS 47
7.1.1 Security Audit 48
7.1.2 Alarm generation 49
7.1.3 Cryptographic Support 49
7.1.4 User Data Protection 49
7.1.5 Identification and Authentication 51
7.1.6 Security Management 52
7.1.7 Protection of the TOE Security Functions 53
7.1.8 Virtual Machine Domain Separation 54

8 RATIONALE 55
8.1 CONFORMANCE CLAIMS RATIONALE 55
8.2 SECURITY OBJECTIVES RATIONALE 55
8.2.1 Security Objectives Rationale Relating to Threats 55
8.2.2 Security Objectives Rationale Relating to Policies 58
8.2.3 Security Objectives Rationale Relating to Assumptions 58
8.3 RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS 59
8.4 RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS 59
8.5 SECURITY REQUIREMENTS RATIONALE 60
8.5.1 Rationale for Security Functional Requirements of the TOE Objectives 60
8.5.2 Security Assurance Requirements Rationale 63
8.5.3 Dependency Rationale 63

9 ACRONYMS AND TERMS 65

Table of Figures

FIGURE 1 – EVALUATED DEPLOYMENT CONFIGURATION OF THE TOE 9
FIGURE 2 – PHYSICAL TOE BOUNDARY 14
FIGURE 3 - EXT_FAU_ARP SYSTEM EVENT AUTOMATIC RESPONSE FAMILY DECOMPOSITION 26
FIGURE 4 – EXT_FIA_VC_LOGIN VCENTER SERVER USER LOGIN REQUEST FAMILY DECOMPOSITION 27
FIGURE 5 – EXT_VDS_VMM: ESXI VIRTUAL MACHINE DOMAIN SEPARATION FAMILY DECOMPOSITION 27

List of Tables

TABLE 1 – ST AND TOE REFERENCES 4
TABLE 2 – SUMMARY OF NAME CHANGES FOR THE TOE COMPONENTS 10
TABLE 3 – COMPONENTS OF THE TOE 15
TABLE 4 – CC AND PP CONFORMANCE 20
TABLE 5 – THREATS 21
TABLE 6 – ASSUMPTIONS 22
TABLE 7 – SECURITY OBJECTIVES FOR THE TOE 23
TABLE 8 – IT SECURITY OBJECTIVES 24
TABLE 9 – NON-IT SECURITY OBJECTIVES 24
TABLE 10 – EXTENDED TOE SECURITY FUNCTIONAL REQUIREMENTS 25
TABLE 11 – TOE SECURITY FUNCTIONAL REQUIREMENTS 30
TABLE 12 – AUDITABLE EVENTS ON THE ESXI 32
TABLE 13 – CRYPTOGRAPHIC OPERATIONS 34
TABLE 14 – FMT_MSA.1(B) – SECURITY ATTRIBUTES, ACTIONS, ROLES 40
TABLE 15 – FMT_MSA.3(B) – ROLES AND OBJECTS/INFORMATION 41
TABLE 16 – ASSURANCE REQUIREMENTS 46
TABLE 17 – MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS 47
TABLE 18 – AUDIT RECORD CONTENTS 48
TABLE 19 – THREATS:OBJECTIVES MAPPING 55
TABLE 20 – ASSUMPTIONS:OBJECTIVES MAPPING 58
TABLE 21 – OBJECTIVES:SFRS MAPPING 60
TABLE 22 – FUNCTIONAL REQUIREMENTS DEPENDENCIES 63
TABLE 23 – ACRONYMS 65
TABLE 25 – VMWARE VSPHERE 4.0 TERMS 67

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the VMware® ESXi 4.0 Update 1 and vCenter Server 4.0 Update 1, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-only system which provides 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® ESXi 4.0 Update 1 and vCenter Server 4.0 Update 1 Security Target
ST Version	Version 1.4
ST Author	Corsec Security, Inc.
ST Publication Date	2010/09/07
TOE Reference	VMware® ESXi 4.0 Update 1 and vCenter Server 4.0 Update 1
Keywords	Virtualization, Virtual Machines, Hypervisor

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.

VMware, Inc. specializes in 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 end-users to create virtual machines on which the guest operating system 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 (ESX/ESXi) – Virtualization software[1] from VMware that is installed on the host. The ESX/ESXi software provides and manages the 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 host (or a single ESX host) provides one or more virtual machines. In a typical enterprise-level deployment, the virtualized computing environment has multiple physical hypervisor (ESX/ESXi) hosts running many virtual machines. To effectively manage this type of environment, VMware offers the following software products:

- vCenter Server – A software service that acts as a central administrator for connected ESX/ESXi hosts. The vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).
- VMware Update Manager (VUM) – A software service that is used to apply patches and updates across ESX/ESXi hosts and all managed virtual machines.

The relationship between the vCenter Server and the hypervisor (ESX/ESXi) hosts is a one-to-many relationship: A single vCenter Server managing a multiple number of ESXi and/or ESX 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 a same physical machine, they are installed and run on different machines, in most cases.

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

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

[1] VMware offers two kinds of virtualization software (hypervisor). These are called VMware ESX and VMware ESXi, respectively. ESX and ESXi are mostly identical. Some notable differences are:

- ESX – provides a console operating system (COS) as a part of the software.
- ESXi – does not contain a COS. ESXi is either embedded in a host machine's flash memory by an Other Equipment Manufacturer (OEM) or can be installed on a host by an end user.

- VMware Distributed Resource Scheduler (DRS) – automatically migrates VMs in a cluster to rebalance work load.

- VMware Fault Tolerance – provides continuous availability, without any data loss or downtime, to any application, in the event of hardware failures.

- VMware HA[2] – enables automatic restart of virtual machines on a different physical server within a cluster if the hosting server fails.
- VMware Hot Add – enables CPU and memory to be added to virtual machines when needed without disruption or downtime.

- VMware Host Profiles – standardizes and automates configuration of the hypervisor (ESX/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 using vCenter Linked Mode to allow them to share information. 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 Application Mode (ADAM) to store and synchronize data across multiple vCenter Server systems. ADAM is installed automatically as part of vCenter Server installation. Each ADAM 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 ADAM 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 migration of a running VM from one host to the other.

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

- VMware vNetwork Distributed Switch – simplifies and enhances the provisioning, administration and control of virtual machine networking. It also enables third party distributed virtual switches such as the Cisco Nexus 1000v to be used in VMware's virtual networking environment.

- VMware vShield Zones – simplifies application security by enforcing corporate security policies at the application level in a shared environment while still maintaining trust and network segmentation of users and sensitive data.

In addition to the vCenter Server and VUM, VMware provides the following access mechanisms to the end-users in order to access the TOE:

- vSphere Client – This is the primary interface for creating, managing, and monitoring virtual machines, their resources, and their host (ESX/ESXi). It is also the primary 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 ESX/ESXi host or to a vCenter Server.

[2] HA – High Availability

- A Web interface through which the end-user can perform basic virtual machine configuration and get console access to virtual machines. Similar to the vSphere Client, vSphere Web Access works directly with a host (ESX/ESXi) or with a vCenter Server.

The vCenter Server 4.0 Update 1, vSphere Client 4.0 Update 1, VUM 4.0 Update 1, together with ESX 4.0 Update 1 and ESXi 4.0 Update 1 are the major components of a virtualization suite offered by VMware, Inc. called VMware vSphere 4.0 Update 1.

The minimum hardware and software requirements for the major components of the VMware vSphere 4.0 Update 1 are summarized below.

The vCenter Server hardware must meet the following minimum requirements:

- CPU[3] 2 x86-comaptible CPUs
- Processor (type and speed) – 2.0 GHz or faster Intel or AMD processor. Processor requirements might be higher if the database runs on the same machine.
- Memory – 3 Gigabytes (GB) RAM[4]. Memory requirements might be higher if the database runs on the same machine,
- Disk storage – 2 GB. Disk requirements might be higher if the database runs on the same machine.
- Networking – 10/100/1000 Gigabit connection recommended.

The vCenter Server supports the following operating systems:

- Windows XP Pro SP[5]2
- Windows XP Pro SP3
- Server 2003 SP1
- Server 2003 SP2
- Server 2003 64-bit, SP2
- Server 2003 R2[6]
- Server 2003 R2 64-bit
- Server 2003 64-bit
- Server 2003 64-bit SP1
- Server 2008 Enterprise, Standard, & Datacenter (32 & 64 bit)
- Server 2008 SP2 (32 & 64 bit).

The vCenter Server installer requires Internet Explorer 5.5 or higher in order to run.

The vCenter Server supports the following databases:

- Microsoft SQL Server 2005 Express
- Microsoft SQL Server 2005 Standard Edition (SP1, SP2, and SP 3)
- Microsoft SQL Server 2005 Enterprise Edition (SP1, SP2, and SP 3)
- Microsoft SQL Server 2005 Standard Edition 64-bit (SP2, and SP 3)
- Microsoft SQL Server 2005 Enterprise Edition 64-bit (SP2 and SP 3)
- Microsoft SQL Server 2008 Standard Edition
- Microsoft SQL Server 2008 Enterprise Edition
- Microsoft SQL Server 2008 Standard Edition 64-bit

[3] CPU – Central Processing Unit

[4] RAM – Random Access Memory

[5] SP – Service Pack

[6] R2 – Release 2

- Microsoft SQL Server 2008 Enterprise Edition 64-bit
- Oracle 10g Standard Edition, Release 2 [10.2.0.3.0]
- Oracle 10g Enterprise Edition, Release 2 [10.2.0.3.0]
- Oracle 10g Enterprise Edition, Release 2 [10.2.0.3.0] 64-bit
- Oracle 11g Standard Edition
- Oracle 11g Enterprise Edition.

The vSphere Client hardware must meet the following minimum requirements:

- CPU – 1 x86-compatible CPU
- Processor (type and speed) – 266 MHz or faster Intel or AMD processor (500 MHz recommended).
- Memory – 200MB RAM
- Disk storage – 1GB free disk space for a complete installation
- Networking – 10/100/1000 Gigabit connection recommended.

The vSphere Client is designed for these operating systems:

- Windows Server 2003, SP1
- Windows Server 2003, SP2
- Windows Server 2003, R2
- Windows Server 2003 64-bit
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Business 64-bit
- Windows Vista Enterprise 64-bit
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard
- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise 64-bit
- Windows Server 2008 Standard 64-bit.

The vSphere Web Access client is designed for these browsers:

- Internet Explorer 6.0 or higher
- Firefox 2.0.x or higher.

The host for the ESXi 4.0 must meet the following hardware requirements:

- VMware ESXi 4.0 requires servers[7] with x86 64-bit CPUs. Known 64-bit processors are:
  - All AMD Opterons support 64-bit
  - All Intel Xeon 3000/3200, 3100/3300, 5100/5300, 5200/5400, 7100/7300, and 7200/7400 support 64-bit
  - All Intel Nehalem support 64-bit
- 2GB RAM minimum
- One or more supported network adapters
- One or more supported storage controllers.

[7] See 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, on 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 multiple virtual machines on industry standard x86-compatible hardware platforms (64-bit) and allows the management of these virtual machines. Figure 1 shows the detailed view of the CC-evaluated deployment configuration of the TOE:

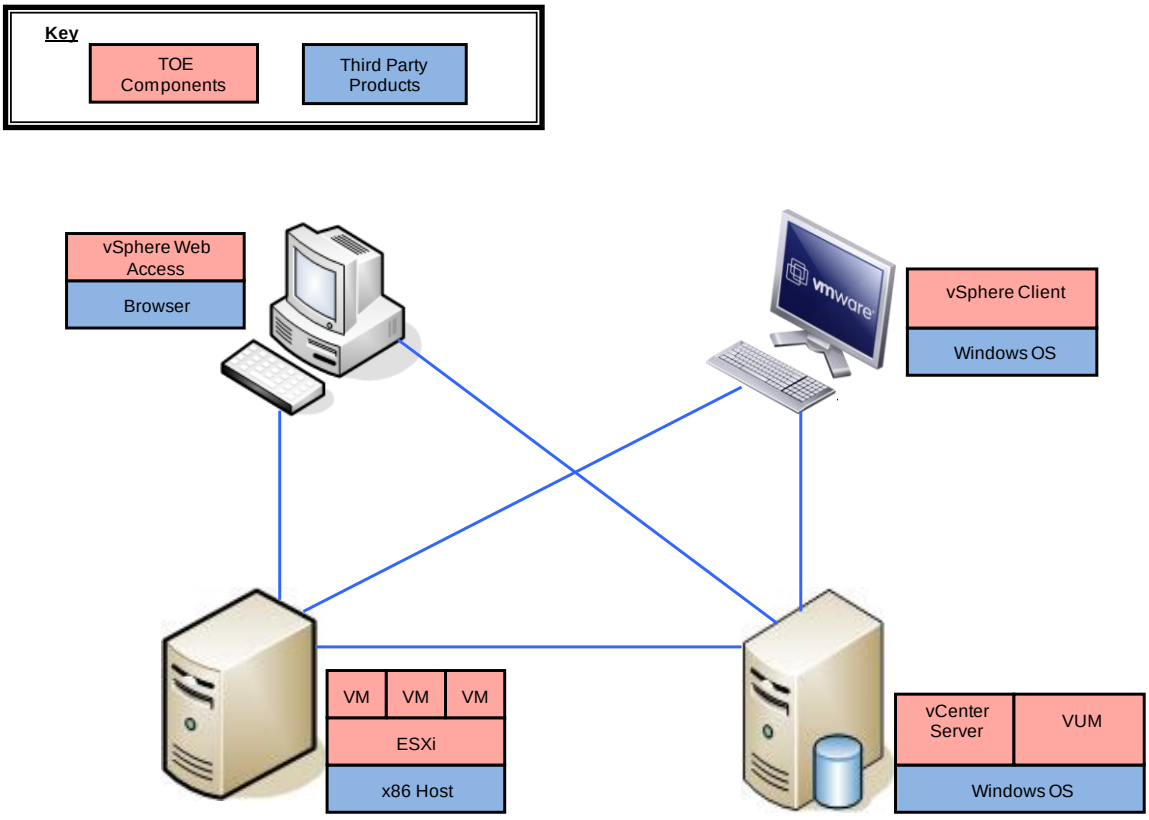

Figure 1 – Evaluated Deployment Configuration of the TOE

The acronym(s) appearing in Figure 1 and not previously defined are:

- OS – Operating System

The CC-evaluated test deployment of the TOE shown in Figure 1 is composed of a single instance of each major TOE component. These are ESXi 4.0 Update 1, vCenter Server 4.0 Update 1, VUM 4.0 Update 1, vSphere Client 4.0 Update 1, and the vSphere Web Access 4.0 Update 1 Machine. In the CC-evaluated deployment of the TOE, the vCenter Server 4.0 and the VUM 4.0 Update 1 are installed and run on the same Windows machine.

The TOE components have recently undergone name changes. In September 2008, VMware announced name changes for the TOE components included in this evaluation. "VMware ESXi Server" was renamed to "VMware ESXi" and "VMware VirtualCenter Server" was renamed "VMware vCenter Server".

Table 2 below summarizes the name changes for the TOE components. The third column of the table shows the shortened TOE component names used in this document.

Table 2 – Summary of Name Changes for the TOE Components

Official TOE component Name	Current Version	Shortened TOE component Name	Previous Name
VMware ESXi	4.0 Update 1	ESXi	VMware ESXi Server
VMware vCenter Server	4.0 Update 1	vCenter Server	VMware VirtualCenter Server
VMware vSphere Client	4.0 Update 1	vSphere Client	VMware Virtual Infrastructure Client
VMware Update Manager	4.0 Update 1	VUM	VMware Update Manager

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 of ESXi. 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 allows the provisioning of virtual machines on the ESXi. For example, virtual machines can be created, configured, cloned, and relocated.

The vCenter Server communicates with the ESXi via the vCenter Server Agent (VPXA) located on the ESXi host. The confidentiality and integrity of this communication is protected using the Secure Sockets Layer (SSL) protocol and certificates which are system-generated or provided by the end-user. The vCenter Server's SSL implementation uses algorithms that are Cryptographic Algorithm Validation Program (CAVP) validated against FIPS 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 Access client via a web browser.

1.4.1.1.1.1 vSphere Client

Users connect to 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. Communication with the vSphere Client is protected using SSL.

1.4.1.1.1.2 vSphere Web Access

Users connect to the vCenter Server via the vSphere Web Access client through a web browser. The vSphere Web Access client interface is provided by a Tomcat servlet engine in the TOE. The vSphere Web Access client provides a subset of the functionality provided by the vSphere Client. Communication between the vSphere Web Access client and the web browser is protected using Secure HyperText Transfer Protocol (HTTPS), as shown in Figure 2.

1.4.1.2 vCenter Server Database

The vCenter Server database 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, 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 VMware Update Manager

The VMware Update Manager (VUM) provides automated patch management for the ESXi and its Virtual Machines. VUM scans the state of the ESXi, and compares it against a default baseline, or against a custom dynamic or 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 Guest Operating Systems being run in the 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, 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[8] server, which accesses the appropriate server to retrieve updates. VUM then downloads the patches to be installed on the TOE via HTTP[9], 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.

1.4.1.3 ESXi

The ESXi is a user-installable or OEM-embedded virtualization layer that runs directly on industry standard x86-compatible hardware, allowing multiple virtual machines to 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 is configurable for each virtual machine.

The 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

[8] ISP – Internet Service Provider; this ISP provides access to patch and update download servers.

[9] HTTP – HyperText Transport Protocol

the correct destination. The vSwitch is implemented entirely in software as part of the ESXi. The ESXi vSwitches also implement VLANs[10], which are an IEEE[11] 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 4.0 Update 1 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 a virtual network of virtual machines residing on a single ESXi host, whereas the vDS is used to build a virtual network of virtual machines that can exist across multiple ESXi hosts. Therefore, the vDS greatly simplifies the task of network configuration when there is need to migrate virtual machines from one ESXi host to another ESXi host, using VMotion.[12]

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 is only delivered to the intended virtual machines and physical interfaces.

With the vDS feature of VMware virtual networking, ESXi 4.0 Update 1 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 be also noted that VMware's vNetwork Distributed Switch is able to interface with the third party switch products such as a Cisco Nexus 1000V Series Switch.

The ESXi uses a custom mini-HTTP server to support the ESXi landing page which allows the user 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 SSL. In addition to the vSphere Client and the vSphere Web Access, there is another remote management interface to the ESXi host, called Remote Command Line Interface (RCLI) client. The confidentiality and integrity of the communication between the ESXi host and the RCLI client is also protected using SSL.

The ESXi can also be accessed using a local console that is directly attached to the ESXi host. Only root users or the users with system administrator role can access the ESXi host this way. The ESXi host provides the Direct Console User Interface (DCUI), which is a BIOS[13]-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, lockdown mode[14] configuration, restarting server and resetting system defaults.

The ESXi can be installed in three distinct configurations.

---

[10] VLAN – Virtual Local Area Network

[11] IEEE – Institute of Electrical and Electronics Engineers

[12] VMware VMotion is also capable of migrating virtual machines between:

- One ESX host and another ESX host
- An ESX host and an ESXi host (and vice versa)

[13] BIOS – Basic Input Output Signal

[14] 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.

- **Installation Configuration 1: OEM:** ESXi is provided pre-installed in flash-memory on a server purchased from select OEMs.

- **Installation Configuration 2: Installable Flash:** ESXi is installed by the end-user in local flash-memory.

- **Installation Configuration 3: Installable Local Storage:** ESXi is installed by the end-user on local storage (such as a hard disk).

ESXi data can be stored in two different ways:

- **VM Storage Configuration 1: Local Storage Only:** ESXi is installed on local storage, and uses local disk for storage for VM images and other VM data.

- **VM Storage Configuration 2: ESXi Local/Virtual Machines on Storage Area Network (SAN) or Other Supported Datastore:** ESXi is installed on local storage, and Virtual Machines are installed on a SAN, NFS[15] or iSCSI[16] datastore.

In all configurations, the separation of virtual machine data and images is performed and managed by the ESXi.

1.4.1.3.1 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 console or browser interface.

1.4.2 TOE Environment

For information on the TOE Environment see Section 1.3.

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

The ESXi is a virtualization layer that runs directly on industry standard x86-compatible hardware, allowing multiple virtual machines to be hosted on one physical server. The 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 networking protocols.

The vCenter Server acts as a management console, deploying, monitoring, and managing virtual machines that are distributed across multiple hosts running the ESXi software. VMware Update Manager handles updates and patches for the TOE.

[15] NFS – Network File System

[16] iSCSI – Internet Small Computer System Interface

The TOE includes the following software only components:

- vSphere Client
- vSphere WebAccess
- vSphere ESXi Server

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.

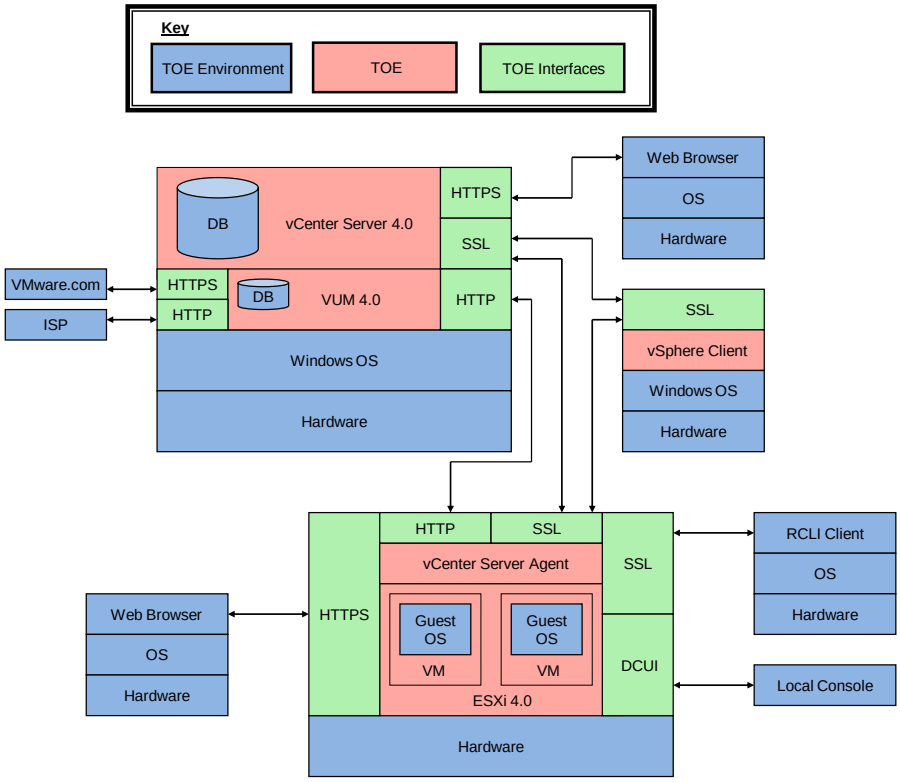

Figure 2 – Physical TOE Boundary

The acronym(s) appearing in Figure 2 and not previously define are:

- DB – Database

Table 3 below indicates which elements of the product are included in the TOE boundary. For more information on the TOE Environment see section 1.3.

Table 3 – Components of the TOE

Component	TOE	TOE Environment
vCenter Server 4.0 Software Update 1	✓	
VMware Update Manager 4.0 Software (on the vCenter Server machine) Update 1	✓	
ESXi 4.0 Software Update 1	✓	
vSphere Client 4.0 Update 1	✓	
vSphere Web Access Machine 4.0 Update 1	✓	
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 Hardware, operating system, and database.		✓
vSphere Client hardware and operating system		✓
Operating systems and applications running in VMs		✓
Hardware, OS, and software (as identified in the previous sections) for remote workstations		✓

1.5.1.1 Guidance Documentation

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

- vSphere Availability Guide ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000-108-00
- vSphere Basic System Administration ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000105-01
- ESXi Configuration Guide ESXi 4.0, vCenter Server 4.0 Revision: EN-000114-00
- Fibre Channel SAN Configuration Guide ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000109-01
- Getting Started with ESX ESX 4.0, vCenter Server 4.0 Revision: EN-000118-00
- Introduction to VMware vSphere ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000102-00
- iSCSI[18] SAN Configuration Guide ESX 4.0, ESXi 4.0, vCenter 4.0 Revision: EN-000110-00
- vSphere Resource Management Guide ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000107-00
- Setup for Failover Clustering and Microsoft Cluster Service ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000121-00
- vSphere Upgrade Guide ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000112-00
- vSphere Web Access Administrator's Guide ESX 4.0, ESXi 4.0, vCenter Server 4.0 Revision: EN-000128-01
- ESXi Installable and vCenter Server Installation Guide ESXi 4.0 Installable, vCenter Server 4.0 Revision: EN-000113-01

[17] NTP – Network Time Protocol

[18] iSCSI – Internet Small Computer System Configuration

- VMware, Inc. ESX 4.0 Update 1, ESXi 4.0 Update 1, and vCenter Server 4.0 Update 1 Guidance Documentation Supplement v1

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

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 the 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 its audit records by reviewing the event logs stored on the vCenter Server Database. Only a vCenter Server Administrator can view all the event logs. Audit events are viewed through the vSphere Client under the event tab for each organizational object. The 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 the ESXi is restricted to the ESXi System Administrator.

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[19]. 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.

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.

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 OpenSSL which perform sthe 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.

[19] Refer to Table 24 for the description of these terms: Clusters, Datacenters, Datastores, Networks, and Virtual Machines.

1.5.2.4 User Data Protection

The TOE provides two distinct access control mechanisms. One is used for verifying access to objects under the control of the ESXi by users logged into the ESXi and users who make requests on the ESXi from the vCenter Server. The other is used for verifying access to objects on the vCenter Server by users logged into the vCenter Server. Each access control mechanism is described below. 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.

The vCenter Server access control mechanism controls access to objects stored on the vCenter Server, such as virtual machines, and VM Groups. The vCenter Server access control mechanism also controls access to file events, alarm, and scheduled event information. This information is stored in the vCenter Server Database. The vCenter Server access control mechanism also controls access by a vCenter Server user to data and operations specific to the definition, configuration, and management of virtual machines. The ESXi-specific information is physically stored on the machine hosting the ESXi, and is made available to the vCenter Server user via the vCenter Server Agent installed on the ESXi host.

The ESXi supports the roles of system administrator and VM administrator. Users of the system administrator role have unrestricted access in the ESXi. Once an ESXi is placed under the management of a vCenter Server, requests from the vCenter Server users are processed using the account, *vpxuser*, which uses the system administrator role. From the local console or from the management interface, system administrator or root user access requests are processed in a manner similar to Linux operating systems. They have access to any ESXi or VM data on the system. In contrast, the VM administrators cannot modify the ESXi configuration files or data. User access control for VM administrators is the standard user, /group, /and other access control mechanism found in Linux operating systems.

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 Virtual Switch Information Flow Control SFP[20] includes the information flow control SFP for both the virtual switch and distributed switch functionality. A virtual switch, vSwitch, works much 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. 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 across 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.

1.5.2.5 Identification and Authentication

When a user attempts log into the 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-1 (SHA-1). 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.

[20] SFP = Security Function Policy

When a user attempts to log into the vCenter Server, the user is presented with a login screen which requests the vCenter Server name or IP[21] address, the user name, and the user password. The user information is passed to the underlying Windows operating system which verifies the user identity and password. If login is valid, the user at the vSphere Client is presented with the vSphere Client interface denoting a successful login. If 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.

When VMware Update Manager starts up, it authenticates with vCenter Server. VUM instructs ESXi to scan for compliance against a pre-defined or custom created baseline and then installs a 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 download updates and patches to the ESXi host.

1.5.2.6 Security Management

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.

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

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.

1.5.3 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.

[21] IP: Internet Protocol

- Simple Network Management Protocol (SNMP), File Transfer Protocol (FTP), Telnet
- The use of any authentication method on ESXi other than the local password database
- VMware Software Development Kit (SDK) tools
- The procfs[22] interface on the ESXi host Service Console
- VMware Scripting Application Programming Interface (API) on the ESXi host
- VMware Consolidated Backup
- Guest OS patch updates via Update Manager

[22] The procfs interface can be used to manage CPU resources.

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 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 2009/12/11 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL4+ augmented with Flaw Remediation (ALC_FLR.2)

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 or the protected network. 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 5 – Threats

Name	Description
T.AVAILABILITY	A process running on a virtual machine or an ESXi host may cause a system malfunction or system performance degradation to the extent that the Virtual Machine or the ESXi host becomes unavailable to the TOE users.
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.PRIVIL	An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.VM	A process running on one virtual machine might compromise the

[23] IT – Information Technology

Name	Description
	security of processes running on other virtual machines.
T.VIRTUAL_NETWORK	A process running on a virtual machine attempts to deliver traffic to wrong VM or external entity.

3.2 Organizational Security Policies

There are no Organization Security Policies.

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 6 – Assumptions

Name	Description
A.NOEVIL	Users are non-hostile, appropriately trained, and follw 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. The vSphere Client component will only connect to the server via the protected management network.

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 7 – Security Objectives for the TOE

Name	Description
O.CONTINUITY	The TOE must ensure the availability of both the Virtual Machine and the ESXi host unless the Virtual Machine and the ESXi host are explicitly powered off by the System Administrator.
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.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.SECURE	The TOE must ensure 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.
O.VLAN	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.
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 8 – IT Security Objectives

Name	Description
OE.IDAUTH	The IT Environment will provide reliable verification of the vSphere Client user credentials.
OE.SEP	The TOE environment will protect the TOE from external interference or tampering.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

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 9 – 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. The vSphere Client component will only connect to the server via the protected management network.

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 10 identifies all extended SFRs implemented by the TOE.

Table 10 – Extended TOE Security Functional Requirements

Name	Description
EXT_FAU_ARP.1	System event automatic response
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" was modeled after the other FAU SFRs.

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

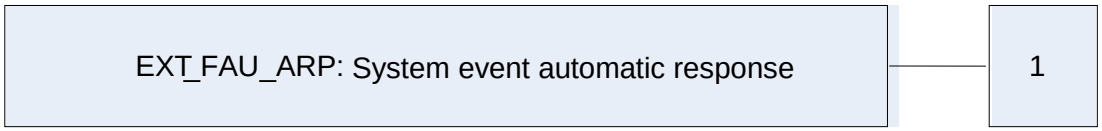

Figure 3 - EXT_FAU_ARP System event automatic response family decomposition

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

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.

5.1.2 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 Server user login request" was modeled after the other FIA SFRs.

5.1.2.1 vCenter Server 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 4 – EXT_FIA_VC_LOGIN vCenter Server user login request family decomposition

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

EXT_FIA_VC_LOGIN.1 vCenter Server 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 the vCenter Server environment 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 Behaviour

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

Component Leveling

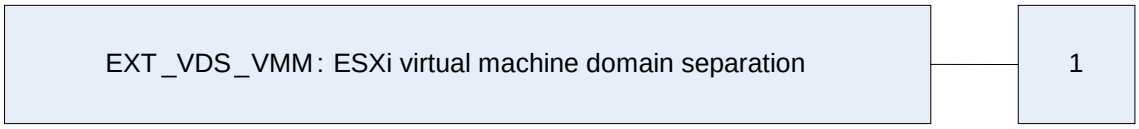

Figure 5 – EXT_VDS_VMM: ESXi Virtual machine domain separation family decomposition

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.

EXT_VDS_VMM.1 ESXi virtual machine domain separation

Hierarchical to: No other components

Dependencies: None

This component will ensure that network traffic is only delivered to the intended recipients(s).

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 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FCS_COP.1	Cryptographic Operation		✓		
FDP_ACC.1(a)	Subset access control (vCenter Server)		✓		✓
FDP_ACC.1(b)	Subset access control (ESXi)		✓		✓
FDP_ACF.1(a)	Security attribute based access control (vCenter Server)		✓		✓
FDP_ACF.1(b)	Security attribute based access control (ESXi)		✓	✓	✓
FDP_IFC.2	Complete information flow control		✓	✓	
FDP_IFF.1	Simple security attributes		✓	✓	
FIA_UAU.2	User authentication before any action	✓	✓	✓	
FIA_UID.2	User identification before any action			✓	
FMT_MSA.1(a)	Management of security attributes (vCenter Server)	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes (ESXi)	✓	✓		✓

Name	Description	S	A	R	I
FMT_MSA.1(c)	Management of security attributes (Virtual Switch Information Flow Control)	✓	✓		
FMT_MSA.3(a)	Static attribute initialisation (vCenter Server)	✓	✓	✓	✓
FMT_MSA.3(b)	Static attribute initialisation (ESXi)	✓	✓	✓	✓
FMT_MSA.3(c)	Static attribute initialisation (Virtual Switch Information Flow Control)		✓		
FMT_SMF.1	Specification of management function		✓		
FMT_SMR.1(a)	Security roles (vCenter Server)		✓	✓	✓
FMT_SMR.1(b)	Security roles (ESXi)		✓	✓	✓
FPT_ITC.1	Inter-TSF confidentiality during transmission				
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
EXT_FAU_ARP.1	System event automatic response				
EXT_FIA_VC_LOGIN.1	vCenter Server user login request				
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 12*].

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 12*].

Dependencies: FPT_STM.1 Reliable time stamps

Table 12 – 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 [*users who are granted access to the requested object by the Access Control Policy*] with the capability to read [*all audit events*] 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

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 13*] in accordance with a specified cryptographic algorithm [*the cryptographic algorithms listed in the Cryptographic Algorithm column of Table 13*] and cryptographic key sizes [*the cryptographic key sizes listed in the Key Sizes (bits) column of Table 13*] that meet the following: [*the list of standards in the Standards (Certificate #) column of Table 13*].

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

Table 13 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Symmetric encryption and decryption	Triple-DES[26] (2-Key) CBC	128	CAVP(cert #970)
	AES[27] (128, 256) CBC	128, 256	CAVP (cert #1422)
Message Digest	SHA-1	N/A[28]	CAVP (cert #1290)
Digital signature verification of VPXA bundle	RSA digital signature	1024 bit	CAVP (cert #697)
Digital signatures for patch bundles (used by VUM)	RSA digital signature	1024 bit	CAVP (cert #697)

[26] DES – Data Encryption Standard

[27] AES – Advanced Encryption Standard

[28] N/A – Not Applicable

6.2.3 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control (vCenter Server)
Hierarchical to: No other components.

FDP_ACC.1.1(a)

The TSF shall enforce the [*vCenter Server Access Control Policy*] on [

a) Subjects: processes acting on behalf of vCenter Server users

b) Objects: virtual machine definition and configuration files; inventory data for virtual machines, folders[29], datacenters, clusters, resource pools[30], networks, datastores, templates[31], and hosts; scheduled events, alarms, events, and templates

c) Operations: all operations between the listed subjects and the listed objects].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1(b) Subset access control (ESXi)
Hierarchical to: No other components.

FDP_ACC.1.1(b)

The TSF shall enforce the [*ESXi Access Control Policy*] on [

a) Subjects: processes acting on behalf of ESXi users

b) Objects: virtual machine definition and configuration files; ESXi configuration files; ESXi audit logs

c) Operations: all operations between the listed subjects and the listed objects].

Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1.1(a)

The TSF shall enforce the [*vCenter Server Access Control Policy*] to objects based on the following: [

a) Subjects: Processes acting on behalf of users of the vCenter Server

b) Subject security attributes: User identity or User group(s), vCenter Server User Role

c) Objects: virtual machine definition and configuration files; inventory data for virtual machines, folders, datacenters, clusters, resource pools, networks, datastores, templates, and hosts; scheduled events, alarms, tasks, and templates

d) Object attributes: A set of permission pairs (User identity or User Group, vCenter Server User Role)].

FDP_ACF.1.2(a)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

[29] Refer to Table 24 for description.

[30] Refer to Table 24 for description.

[31] Refer to Table 24 for description.

a) Access is granted if the user is a member of the administrators group of the underlying Windows operating system of the vCenter Server, also known as a vCenter Server Administrator.
b) Access to perform a given activity on an object is allowed on the vCenter Server if there is a permission pair associated with the object having a user identity component that matches the user identity of the subject, and a vCenter Server User Role, allowing the activity requested by the subject.
c) Access to perform a given activity on an object is allowed on the vCenter Server if there is a permission pair associated with the object having a user group component that matches a group to which the subject belongs, and a vCenter Server User Role, allowing the activity requested by the subject.
d) If the user of the subject does not match the user identity of any permission pair associated with the object, or the User identity is not a member of any group of any permission pair associated with the object, or the vCenter Server User Role of any such matching permission pair does not permit the activity requested by the user, then access is denied[32]].

FDP_ACF.1.3(a)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4(a)

The TSF shall explicitly deny access of subjects to objects based on the [*none*].

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ACF.1(b) Security attribute based access control (ESXi)

Hierarchical to: No other components.

FDP_ACF.1.1(b)

The TSF shall enforce the [*ESXi Access Control Policy*] to objects based on the following: [
a) Subjects: Processes acting on behalf of users of the ESXi Server
b) Subject security attributes: User identity or User group(s), ESXi User role
c) Objects: virtual machine definition and configuration files; ESXi configuration files, ESXi audit logs
d) *Object attributes: User identity of object owner, object group, read/write/execute permissions for owner/group/other*].

FDP_ACF.1.2(b)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects **of the ESXi** is allowed: [
a) Access is granted if the ESXi role is system administrator.
b) Access is granted if the ESXi role is not system administrator and the user id is the user id of the object owner and the requested access is allowed for the owner of the object.
c) Access is granted if the ESXi role is not system administrator and the user belongs to the group of the object and the requested access is allowed for members of the object's group.
d) Access is granted if the ESXi role is not system administrator and the requested access is allowed for anyone.

[32] All vCenter Server objects are contained within an object hierarchy. Newly created objects inherit the permissions of the parent object. When an object is moved within the hierarchy, the object loses its previous permissions and assumes the permission settings of the new parent object.

e) If the user is a VM administrator and the requested action is register or unregister[33] a VM, then the user must have read, write, and execute access to the VM's configuration file for the operation to be allowed.

f) *If the user is a VM administrator and the requested action is a power operation on a VM, then the user must have execute access to the VM's configuration file for the operation to be allowed*].

FDP_ACF.1.3(b)

The TSF shall explicitly authorise access of subjects to objects **or operations of the ESXi** based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(b)

The TSF shall explicitly deny access of subjects to objects **of the ESXi** based on the **following rules:** [*no additional rules*].

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

FDP_IFC.2.1

The TSF **of the ESXi** shall enforce the [*virtual switch information flow control SFP*] on [

a) Subjects: physical network interfaces and VM virtual network interfaces

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 **of the ESXi** shall enforce the [*virtual switch information flow control SFP*] based on the following types of subject and information security attributes: [

a) Subjects: physical network interfaces and VM virtual network interfaces

b) Subject security attributes: interface identifier, VLAN identifier (if applicable)

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: [*if the data packet originates from a recognized and authorized source, indicated by the source identifier as defined in this SFP, and is*

[33] "Register" refers to the act of associating a VM with an ESXi host. "Unregister" refers to the act of disassociating a VM from an ESXi host.

addressed to a recognized and authorized destination, indicated by the destination identifier as defined in this SFP, 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 Static attribute initialisation

6.2.4 Class FIA: Identification and Authentication

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** 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** 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 user login request
Hierarchical to: No other components.

The vCenter Server shall request identification and authentication from the vCenter Server environment 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 (vCenter Server)
Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*vCenter Server Access Control Policy*] to restrict the ability to [*change_default, modify, delete*] the security attributes [*the set of permission pairs (User identity or User Group, vCenter Server User Role) for all subjects and all objects in the vCenter Server*] to [*vCenter Server Administrators and vCenter Server Administrator defined roles*].

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

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

FMT_MSA.1.1(b)

The TSF shall enforce the [*ESXi Access Control Policy*] to restrict the ability to [*modify, delete, [add]*] the security attributes [*For ESXi users: user id; user groups; ESXi User Role; For ESXi objects: object owner; object group; object read, write, and execute permissions of security attributes*] to [*the role as described in Table 14]*.

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

Table 14 – FMT_MSA.1(b) – Security Attributes, Actions, Roles

Action	Attribute	Role
Modify	Read, write, and execute permissions on objects	System Administrator or VM Administrator
Add, Delete, Modify	User identity of object owner, object group	System Administrator
Add, Delete, Modify	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, Delete, Modify	User identity, User Group, ESXi User Role	System Administrator

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

FMT_MSA.1.1(c)
The TSF shall enforce the [*Virtual Switch Information Flow Control SFP*] to restrict the ability to [*add, modify, delete*] the security attributes [*interface identifier, VLAN identifier*] to [*System Administrators*].

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

FMT_MSA.3(a) Static attribute initialization (vCenter Server)
Hierarchical to: No other components.

FMT_MSA.3.1(a)
The TSF shall enforce the [*vCenter Server Access Control Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the **vCenter Server Access Control Policy** SFP.

FMT_MSA.3.2(a)
The TSF shall allow the [*vCenter Server Administrators and Administrator defined roles*] to specify alternative initial values to override the default values when an object or information is created **on the vCenter Server**.

Dependencies: FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3(b) Static attribute initialization (ESXi)
Hierarchical to: No other components.

FMT_MSA.3.1(b)
The TSF shall enforce the [*ESXi Access Control Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the **ESXi Access Control Policy** SFP.

FMT_MSA.3.2(b)
The TSF shall allow the [*System Administrator and VM administrator(s)*] to specify alternative initial values to override the default values when an object or information is created **on the ESXi, as described in** Table 15.

Dependencies: FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

Table 15 – FMT_MSA.3(b) – Roles and objects/Information

Role	Type of Object or Information
System Administrator	Any
VM Administrator(s)	Objects they create

FMT_MSA.3(c) Static attribute initialization (Virtual Switch Information Flow Control)

Hierarchical to: No other components.

FMT_MSA.3.1(c)

The TSF shall enforce the [*Virtual Switch Information Flow Control Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the **Virtual Switch Information Flow Control** SFP.

FMT_MSA.3.2(c)

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**.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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 security management functions: [

a) Adding, deleting, or modifying the object permissions associated with a user or group on the vCenter Server
b) Adding, deleting, or modifying user or group membership on the ESXi
c) Modification of permissions associated with an object on the ESXi
d) Functions to create, modify, or delete virtual machines
e) Users can change their own passwords on the ESXi
f) Power operations on a virtual machine].

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 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 and System Administrator*].

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 [selection: *disclosure*, *modification*] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

6.2.7 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 EAL4, 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.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: Basic Design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused 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
	FAU_SAR.1	Audit review
Cryptographic Support	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_ACC.1(a)	Subset access control (vCenter Server)
	FDP_ACC.1(b)	Subset access control (ESXi)
	FDP_ACF.1(a)	Security attribute based access control (vCenter Server)
	FDP_ACF.1(b)	Security attribute based access control (ESXi)
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Alarm Generation	EXT_FAU_ARP.1	System event automatic response
Identification and Authentication	EXT_FIA_VC_LOGIN.1	vCenter Server user login request
Security Management	FMT_MSA.1(a)	Management of security attributes (vCenter Server)
	FMT_MSA.1(b)	Management of security attributes (ESXi)
	FMT_MSA.1(c)	Management of security attributes (Virtual Switch Information Flow Control)
	FMT_MSA.3(a)	Static attribute initialisation (vCenter Server)
	FMT_MSA.3(b)	Static attribute initialisation (ESXi)

TOE Security Function	SFR ID	Description
	FMT_MSA.3(c)	Static attribute initialisation (Virtual Switch Information Flow Control)
	FMT_SMF.1	Specification of management function
	FMT_SMR.1(a)	Security roles (vCenter Server)
	FMT_SMR.1(b)	Security roles (ESXi)
Protection of the TSF	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITT.1	Basic internal TSF data transfer protection
Virtual Machine Domain Separation	EXT_VDS_VMM.1	ESXi virtual machine domain separation

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 on the vCenter Server Database. 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 Access Control Policy. They are stored on the vCenter Sever 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. Users 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.

The ESXi audit records are stored in a flat file on the Service Console of the ESXi. The ESXi provides the capability using the syslog command to review its audit records which are stored in /var/log/messages. Reviewing the audit records on the ESXi is restricted to the ESXi System Administrator.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.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 or modify 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 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 OpenSSL which performs 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.

TOE Security Functional Requirements Satisfied: FCS_COP.1

7.1.4 User Data Protection

The TOE provides two distinct access control mechanisms. One is used for verifying access to objects under the control of the ESXi by users logged into the ESXi and users who make requests on the vCenter Server, and another for verifying access to objects on the vCenter Server by users logged into the vCenter Server. Each access control mechanism is described below.

VM users (individuals who access the guest operating system and applications within a virtual machine) access data, operations, and files within the scope of the VM, and this access control is determined by the access control methods of the guest operating system and its applications. Such access control is outside the scope of the TOE and is not discussed any further here. Furthermore, VM Administration tasks that can be performed from within the VM are also outside the scope of the TOE, as they do not impact the operation or data of the TOE.

7.1.4.1 vCenter Server Access Control Policy

The vCenter Server access control mechanism controls access to objects stored on the vCenter Server, such as virtual machines, and VM Groups. The vCenter Server access control mechanism also controls access to files containing templates as well as event, alarm, and scheduled event information. This information is stored in the vCenter Server Database. The vCenter Server access control mechanism also controls access by a vCenter Server user to data and operations specific to the definition, configuration, and management of virtual machines. ESXi-specific information is physically stored on the ESXi host, and is made available to the vCenter Server user via the vCenter Server Agents installed on the ESXi.

TOE users on the vCenter Server are administrators who have been assigned to one of two roles categories: vCenter Server Administrator and Administrator-defined roles. Subjects are processes acting on behalf of the logged-in user, and have user identities and may belong to one or more groups, identified by a group identity.

When a vCenter Server user requests an operation to be performed on a particular object, the access control security function first determines if the user is a vCenter Server Administrator by virtue of being a member of the operating system's administrator group. If so, access is granted. If not, the access control security function determines if the user's role(s) for the object contain permissions sufficient for performing the requested operation on the requested object on behalf of the requesting user.

The security attributes for subjects on the vCenter Server are user identity, group membership, and role (vCenter Server Administrator or Limited access user). For objects stored on the vCenter Server, the security attributes are sets of permission pairs consisting of user identity or group and vCenter Server role. When a subject requests access to such an object, the subject user identity or group is compared with the user identity and group identity for each permission pair of the requested object until either a match is found or the object permission pair set is exhausted. A match is determined if the user identity of the subject matches the user identity of the object or the user identity of the subject is a member of the group of the object and the requested operation is allowed for the vCenter Server-role of a matching permission pair. If a match is found, the requested access is granted. If no match is found, the access request is denied.

7.1.4.2 ESXi Access Control Policy

When an ESXi host is first placed under a vCenter Server control, the username and the password for either the root account or the user account with system administrator role for that ESXi host must be supplied. At that time, a new password for the *vpxuser* account is generated to use in all future transactions between the ESXi host and the vCenter Server.

When a user wants to perform tasks on data that is stored in an ESXi host managed by the vCenter Server, the same access control checks described above are performed on the vCenter Server. If the requested access is permitted, then a request, along with the password for the *vpxuser* account described above, is passed to the vCenter Server Agent on the ESXi host, by the vCenter Server. Note that when a user possesses multiple roles or permissions, the access control security function uses any of the associated roles or permissions pertaining to the user that will satisfy the request of the operation and grant access to be allowed. However, if the user does not possess the required permissions from any of the user's associated roles or permissions, then access or the requested action is denied.

The ESXi Access Control policy controls access by subjects directly logged into the ESXi host, and by subjects requesting services from the managing vCenter Server, to objects stored on the ESXi host. These

objects include data and operations specific to the definition, configuration, and management of virtual machines as well as system logs, which contain audit data.

The ESXi supports the two roles: system administrator and VM administrator. The users with the system administrator role have unrestricted access in the ESXi, whereas the users with the VM administrator role may be controlled by group membership or by user identity. The ESXi is designed so that the same access control mechanisms can be used for direct ESXi users who log into the ESXi host via the local console or the management interface, and for indirect ESXi users who access the ESXi host from the vCenter Server. Once an ESXi host is placed under the management of a vCenter Server, requests from the vCenter Server users are processed using the *vpxuser* account. The *vpxuser* account is set up granting access to all VM configuration files (.vmx files).

From the local console or from the management interface, system administrator or root user access requests are processed in ways similar to most Linux operating systems. They have access to any ESXi or VM data on the system. The VM administrators cannot modify the ESXi configuration files or data. User access control for VM administrators is the standard user/group/other access control mechanism found in Linux operating systems. If the user identity of the subject is the owner of the object operation and the requested access type is allowed for the object owner, then access is granted. If a group the user belongs to matches the group of the object and the requested access type is allowed for the group, access is granted. For other users, if the access requested is allowed for "others," then access is granted. Otherwise, access is denied.

7.1.4.3 Virtual Switch Information Flow Control Policy

The ESXi implements vSwitches, VNetwork Distributed Switches, and VLANs, all of which are configurable by authorized administrators. A virtual switch, vSwitch, works much 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. A vNetwork Distributed Switch functions similarly except it allows virtual machines across multiple host machines to be logically connected via the same VNetwork Distributed Switch.

Each virtual machine that is configured for networking is logically connected to a vSwitch or VNetwork Distributed Switch by the ESXi. The vSwitch and the VNetwork Distributed Switch provide 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. Administrators can also configure VLANs on a vSwitch / VNetwork Distributed Switch. A vSwitch / VNetwork Distributed Switch VLAN will create a virtual network within the vSwitch vSwitch / 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 vSwitch / VNetwork Distributed Switch.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b), FDP_IFC.2, FDP_IFF.1

7.1.5 Identification and Authentication

When a user logs into the 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 in a shadow file, where the password is hashed using SHA[34]-1. 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

[34] SHA – Secure Hash Algorithm

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 logs into vCenter Server, they are presented with a login screen, requesting the vCenter Server name or IP address, the user name, and the user password. The user information is passed to the underlying Windows operating system which verifies the user identity and password. If login is valid, the user at the vSphere Client is presented with the vSphere Client interface denoting a successful login. If 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.

When VMware Update Manager starts up, it authenticates with vCenter Server. VUM instructs ESXi to scan for compliance against a pre-defined or custom user created baseline and then installs a 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 download updates and patches to the ESXi.

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

7.1.6 Security Management

The ESXi supports the two 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 Linux operating system. 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 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* 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.

No users on the ESXi host or the vCenter Server, other than the vCenter Server administrator, have access to the *vpxuser* 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.
- There is no way to change the *vpxuser* password manually.

- 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.

VM administrators are administrators of individual VMs on the ESXi host. VM administrators can access the VMs by directly logging into the ESXi host or 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 ensures that the ability to modify permissions of users on ESXi objects is restricted to ESXi System Administrators. The capability to modify permissions of users on objects is provided by functions of the ESXi that are inherited from the customized Linux kernel which the ESXi leverages. These operations include chmod, group management functions, and user account management functions. Only System Administrators can change the object owner of a file. However, the owner of a file may change the group of the file to any group of which that owner is a member. The System Administrator may change the group arbitrarily. The ESXi defaults for access permission are controlled by the umask setting. The default value can only be changed by an ESXi System Administrator.

The TOE provides security management functions that address the management of security attributes for the ESXi (role, user id for subjects, and owner, group, and r,w,x permissions for owner, object group, and other for objects) and vCenter Server (user identity role permission pairs for both subjects and objects). In addition the TOE provides security management functions for the creation, deletion, registration, modification, and power operations[35] on virtual machines.

The vCenter Server supports two categories of roles: vCenter Server Administrator and Administrator defined roles. The vCenter Server Administrator is implemented by membership in the "administrators" group of the underlying Windows OS. Users log in using their username and password, and are automatically in this role by virtue of their membership in the administrators group.

In the CC-evaluated configuration, all administrators using the vSphere Client connect to the TOE via the controlled and protected management network (as assumed in A.PHYSCL), and the TOE environment is configured only to allow TOE administration from this network. This ensures that administrative traffic is protected in transit between the vSphere Client and the ESXi host, or between the vSphere Client and the vCenter Server.

TOE Security Functional Requirements Satisfied: FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.1(c), FMT_MSA.3(a), FMT_MSA.3(b), FMT_MSA.3(c), 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 remote components of the TOE by protecting the information using OpenSSL. HTTP communications between VUM and the ISP Server, and between VUM and the ESXi, are protected by signature verification.

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

[35] "Power operations" on a virtual machine refers to the act of starting, stopping, or suspending a virtual machine in a manner which simulates the application or removal of "virtual power" to or from the VM. For example, if a "power off" event is initiated the VM's OS might receive notice from the virtual power supply that the virtual power button has been pressed – this allows the VM's OS to take whatever steps are necessary to safely shut down before and to inform the virtual power supply when it is ready for full power-off. This behavior simulates the behavior of an OS installed on a physical machine.

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 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 with each other in unacceptable or unauthorized ways. The following mechanisms ensure this:

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

- Read-only Memory: Multiple VMs may require the same OS or application images, 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 network connections can be permitted or prevented as desired. These 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.

TOE Security Functional Requirements Satisfied: EXT_VDS_VMM.1

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 19 displays the mapping of threats to objectives.

Table 19 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.AVAILABILITY A process running on a virtual machine or an ESXi host may cause a system malfunction or system performance degradation to the extent that the Virtual Machine or the ESXi host becomes unavailable to the TOE users.	O.CONTINUITY The TOE must ensure the availability of both the Virtual Machine and the ESXi host unless the Virtual Machine and the ESXi host are explicitly powered off by the System Administrator.	This threat is primarily diminished by the O.CONTINUITY which ensures that the Virtual Machine and the ESXi host stay accessible to the TOE users, unless they are explicitly powered off by the System Administrator.
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 objectives ensure 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.
	OE.IDAUTH The IT Environment will provide reliable verification of the vSphere Client user credentials.	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.
	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	The O.ADMIN objective requires that only authorized users are able to manage the security attributes of the TOE.

Threats	Objectives	Rationale
	and only those TOE users, may exercise such control.	
	OE.SEP The TOE environment will protect 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.
	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.
	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.
	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.
	O.SECURE The TOE must ensure 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 O.SECURE objective ensures that TOE data is protected when transmitted between remote components of the TOE.
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.
	OE.IDAUTH The IT Environment will provide reliable verification of the vSphere Client user credentials.	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.
	O.ADMIN The TOE must include a set of functions that allow efficient	The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage

Threats	Objectives	Rationale
	management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	the functions and data of the TOE
	OE.SEP The TOE environment will protect 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.
	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.
	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.
	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.
T.VM A process running on one virtual machine might compromise the security of processes running on other virtual machines.	OE.SEP The TOE environment will protect 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.
	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 makes information on the unavailability or poor performance of IP networks and servers available to administrators in a timely and clear manner. This allows the administrators to take action to limit the impact of current problems and avoid future problems.
T.VIRTUAL_NETWORK A process running on a virtual machine attempts to deliver traffic	O.VLAN The TOE must ensure that network traffic traversing a	O.VLAN requires that the vSwitch must deliver network traffic only to virtual machines

Threats	Objectives	Rationale
to wrong VM or external entity.	vSwitch is only delivered to virtual machines and physical interfaces that are part of the intended VLAN.	and/or physical interfaces that have been grouped into the intended VLAN.
	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.

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 Organization Security Policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 20 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.NOEVIL Users are non-hostile, appropriately trained, and follw 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. The vSphere Client component will only connect to the server via the protected management network.	NOE.PHYSCL The ESXi host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access. The vSphere Client component will only connect to the server via the protected management network.	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, and that the vSphere Client component will only connect to the server via the protected management network.

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_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_FIA_VC_LOGIN.1 was explicitly stated because authentication and identification of the vCenter Server users is performed by the TOE Environment, and not by the TOE. 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 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 21 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.CONTINUITY The TOE must ensure the availability of both the Virtual Machine and the ESXi host unless the Virtual Machine and the ESXi host are explicitly powered off by the System Administrator.	EXT_FAU_ARP.1 System event automatic response	The TOE ensures the continued availability of the ESXi host and its virtual machines by generating automated alarms that notify the appropriate users of the TOE when there is a potential system malfunction or system performance degradation.
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FDP_ACC.1(a) Subset access control (vCenter Server)	All access control requests must be checked for compliance with the TSP before execution.
	FDP_ACC.1(b) Subset access control (ESXi)	All access control requests must be checked for compliance with the TSP before execution.
	FDP_ACF.1(a) Security attribute based access control (vCenter Server)	All access control requests must be checked for compliance with the TSP before execution.
	FDP_ACF.1(b) Security attribute based access control (ESXi)	All access control requests must be checked for compliance with the TSP before execution.
	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).
	EXT_FIA_VC_LOGIN.1 vCenter Server user login request	For vCenter Server, the TOE requires support from the TOE environment to verify the user credentials.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and	FMT_MSA.1(a) Management of security attributes (vCenter Server)	Only the roles defined in FMT_SMR.1 are given the right to modify or set defaults for TOE security attributes.

Objective	Requirements Addressing the Objective	Rationale
data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MSA.1(b) Management of security attributes (ESXi)	Only the roles defined in FMT_SMR.1 are given the right to modify or set defaults for TOE security attributes.
	FMT_MSA.1(c) Management of security attributes (Virtual 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.3(a) Static attribute initialisation (vCenter Server)	Restrictive values for the vCenter Server functions and data are provided, and the authorized administrator can change them.
	FMT_MSA.3(b) Static attribute initialisation (ESXi)	Restrictive values for the ESXi functions and data are provided, and the authorized administrator can change them.
	FMT_MSA.3(c) Static attribute initialisation (Virtual 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_SMF.1 Specification of management function	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.	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.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	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).

Objective	Requirements Addressing the Objective	Rationale
	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).
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 Server user login request	For vCenter Server, the TOE requires support from the TOE environment to verify the user credentials.
O.SECURE The TOE must ensure 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.	FCS_COP.1 Cryptographic Operation	The System must protect the confidentiality of information during transmission to a remote component of the TOE.
O.SECURE The TOE must ensure 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.	FPT_ITC.1 Inter-TSF confidentiality 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.
O.VLAN 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_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.
O.VM The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.	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_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

EAL4, augmented with ALC_FLR.2 was chosen to provide a moderate- to high-level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. At EAL4+, the TOE will have an undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with an enhanced-basic attack potential.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 22 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 22 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
EXT_FAU_ARP.1	No dependencies	✓	
EXT_FIA_VC_LOGIN.1	No dependencies	✓	
EXT_VDS_VMM.1	No dependencies	✓	
FAU_GEN.1	FPT_STM.1	✓	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.
FAU_SAR.1	FAU_GEN.1	✓	
FCS_COP.1	No dependencies	✓	FCS_CKM.1 and FCS_CKM.4 are not included, following the guidance of CCS Instruction #4. The cryptographic keys must be generated and destroyed by the TOE.
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACF.1(a)	FDP_ACC.1(a)	✓	
	FMT_MSA.3(a)	✓	
FDP_ACF.1(b)	FMT_MSA.3(b)	✓	
	FDP_ACC.1(b)	✓	
FDP_IFC.2	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.2	FIA_UID.1	✓	
FIA_UID.2	No dependencies	✓	
FMT_MSA.1(a)	FMT_SMR.1(a)	✓	
	FDP_ACC.1(a)	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(b)	FDP_ACC.1(b)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1(b)	✓	
FMT_MSA.1(c)	FDP_IFC.2	✓	
	FMT_SMR.1(b)	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_SMR.1(a)	✓	
FMT_MSA.3(b)	FMT_MSA.1(b)	✓	
	FMT_SMR.1(b)	✓	
FMT_MSA.3(c)	FMT_MSA.1(c)	✓	
	FMT_SMR.1(b)	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1(a)	FIA_UID.1	✓	
FMT_SMR.1(b)	FIA_UID.1	✓	
FPT_ITC.1	No dependencies	✓	
FPT_ITT.1	No dependencies	✓	

9 Acronyms and Terms

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

Table 23 below lists the acronyms used in this document.

Table 23 – Acronyms

Acronym	Definition
ADAM	Microsoft Active Directory Application Mode
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input Output Signal
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
COS	Console Operating System
CPU	Central Processing Unit
DB	Database
DCUI	Direct Console User Interface
DRS	Distributed Resource Scheduler
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GB	Gigabyte
HA	High Availability
HCL	Hardware Compatibility List
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
ISP	Internet Service Provider
IT	Information Technology
MB	Megabyte
NFS	Network File System
NTP	Network Time Protocol

Acronym	Definition
OEM	Other Equipment Manufacturer
OS	Operating System
PP	Protection Profile
PVLAN	Private Virtual Local Area Network
R2	Release 2
RCLI	Remote Command Line Interface
RAM	Random Access Memory
SAN	Storage Area Network
SAR	Security Assurance Requirement
SDK	Software Development Kit
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMP	Symmetric Multiprocessing
SNMP	Simple Network Management Protocol
SP	Service Pack
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functionality
TSP	TOE Security Policy
vDS	vNetwork Distributed Switch
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPXA	vCenter Server Agent
vSMP	Virtual Symmetric Multi-Processing
VUM	VMware Update Manager

Table 24 below lists the VMware vSphere 4.0 terms used in this document and gives brief descriptions.

Table 24 – VMware vSphere 4.0 Terms

Term	Description
Clusters	A collection of ESX/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 ESX/ESXi, is installed and on which all virtual machines reside.
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.

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com