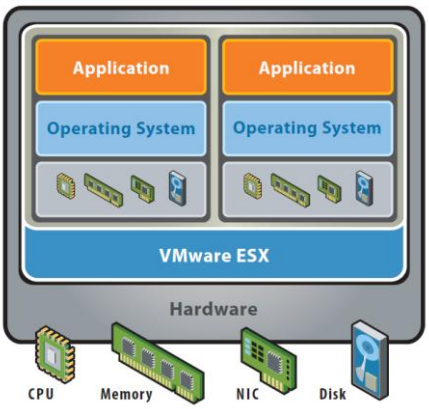
VMware, Inc.
ESX Server 3.5 and VirtualCenter 2.5



Security Target

Evaluation Assurance Level: EAL4+
Document Version: 0.6

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

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is VMware ESX Server 3.5 and VirtualCenter 2.5, and will hereafter be referred to as the TOE throughout this document. The TOE is a system which can provide multiple virtual machines (VMs) on industry standard x86-compatible hardware platform and allows the management of these virtual machines.

The TOE components are undergoing name changes. In September 2008, VMware announced name changes for the TOE components included in this evaluation. "VMware ESX Server" was renamed to "VMware ESX" and "VMware VirtualCenter Server" was renamed "VMware vCenter Server". Current web pages, electronic media, and new literature have adopted the new name changes; however, text contained in the TOE components and TOE literature have not fully implemented the name changes.

1.1 Purpose

This ST provides contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- Security Target 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 Definition (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 Definition (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 (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	VMware, Inc. ESX Server 3.5 and VirtualCenter 2.5 Security Target
ST Version	Version 0.6
ST Author	Justin Yu
ST Publication Date	1/26/2010
TOE Reference	VMware ESX Server 3.5 and VirtualCenter 2.5

1.3 Product Overview

This section provides a high level product overview of the VMware ESX Server 3.5 and VirtualCenter 2.5 products.

1.3.1 ESX Server

ESX is a "bare metal" hypervisor, meaning it installs directly on top of the physical server and partitions it into multiple virtual machines that can run simultaneously, sharing the physical resources of the underlying server. Each virtual machine represents a complete system, with processors, memory, networking, storage and BIOS[1], and can run an unmodified operating system and applications.

1.3.2 VirtualCenter

VMware VirtualCenter delivers centralized management, operational automation, resource optimization and high availability to IT[2] environments. Virtualization-based distributed services equip the data center with unprecedented levels of responsiveness, serviceability, efficiency and reliability. VirtualCenter delivers the highest levels of simplicity, efficiency, security and reliability required to manage virtualized IT environment of any size.

VirtualCenter uses a database (called "VirtualCenter Database") to store information about the configuration and status of all ESX Server hosts under management and each of the host's virtual machines. VirtualCenter Database also stores management information for the ESX Server, 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 triggering event and notification information
- Events: a list of all the events that occur in the VirtualCenter environment. Audit data are stored as events.
- Stores user and VirtualCenter object permissions

[1] BIOS – Basic Input Output Signal

[2] IT – Information Technology

VirtualCenter Database is implemented by installing 3rd party DBMS[3] products. Section 1.5.2 (TOE Environment) lists the database products supported by VMware VirtualCenter, for the implementation of VirtualCenter Database.

The use of VirtualCenter also provides the following system management services:

- VMotion – Allows the migration of running virtual machines between physical servers without disruption to end users.
- Distributed Resource Scheduler (DRS) – dynamically allocates and balances computing capacity across collections of hardware resources aggregated into unified resource pools.
- VMware HA[4] – High availability provided by VMware HA enables a broad-based and cost-effective application failover that is independent of hardware and operating systems.

1.4 TOE Overview

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

1.4.1 Physical Scope

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

Figure 1 below 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. Table 2 indicates which elements of the product are included in the TOE boundary.

Table 2 - Components of the TOE

Component	TOE	TOE Environment
VirtualCenter 2.5 Software (includes VirtualCenter Server, VirtualCenter agent, and Virtual Infrastructure Client (VIC), VMotion, Distributed Resource Scheduler, VMware HA, Tomcat, OpenSSL)	✓	
VMware Update Manager (VUM) v1.0 U4 Software (on the VirtualCenter machine)	✓	
ESX Server 3.5 Software (includes virtual symmetric multiprocessing (SMP), Console OS[5], OpenSSL, OpenSSH)	✓	
NTP Client on Virtual Infrastructure Client		✓

[3] DBMS – Database Management System

[4] HA – High Availability

[5] OS – Operating System

Component	TOE	TOE Environment
NTP Client on ESX Server		✓
NTP Server available to ESX Server and VirtualCenter		✓
ESX Server hardware (processor and adapters) including blade servers		✓
Storage Area Network hardware and software to be used with ESX Server in Configuration 2 and 3.		✓
VirtualCenter Hardware, operating system, and VirtualCenter Database.		✓
Virtual Infrastructure 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		✓

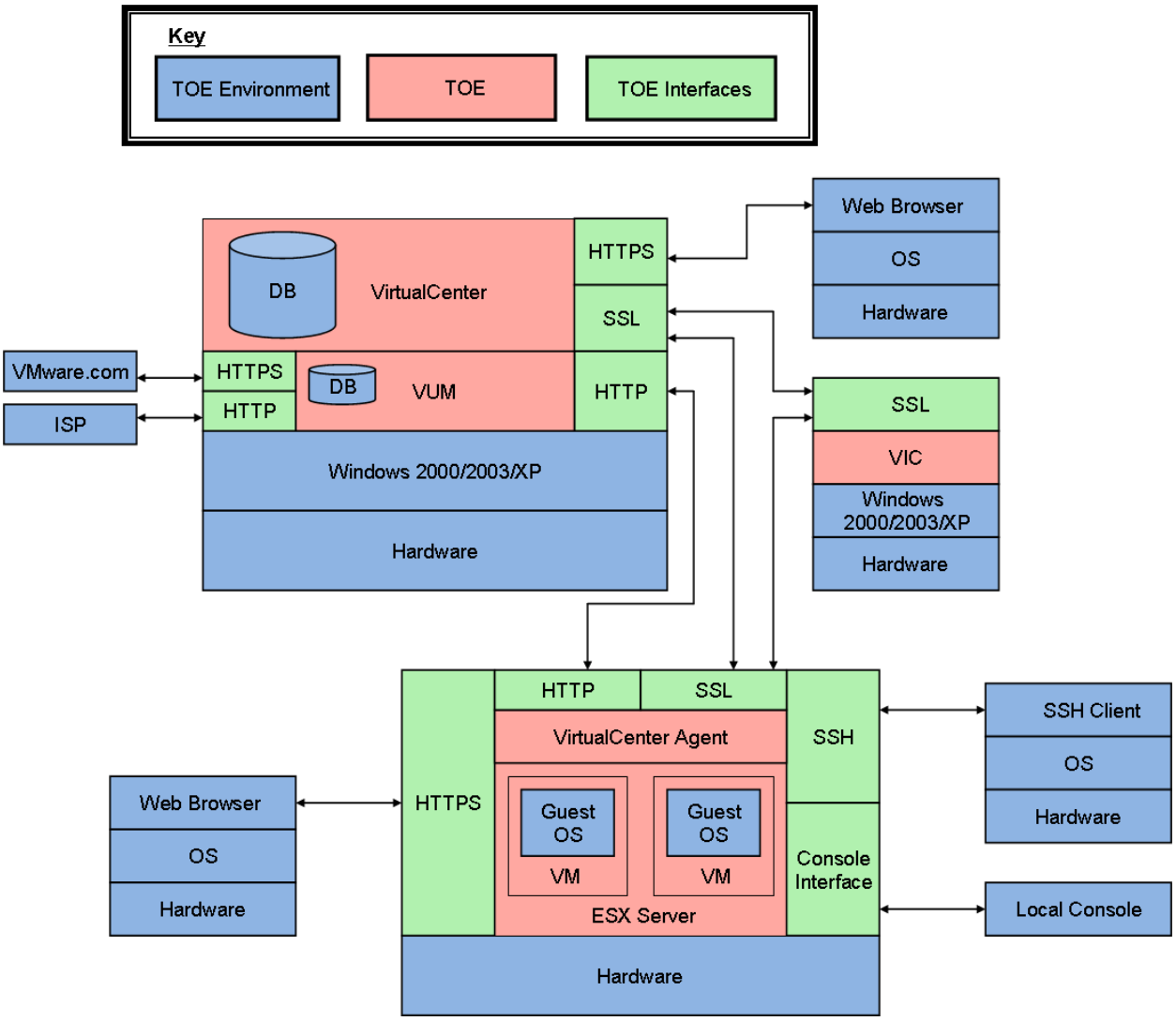


Figure 1 – Physical TOE Boundary

The undefined acronyms that appear in Figure 1 are:

- DB – Database
- HTTP – HyperText Transfer Protocol
- HTTPS – Secure Hypertext Transfer Protocol
- ISP – Internet Service Provider
- SSL – Secure Sockets Layer

1.4.2 Logical Scope

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

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication

- Security Management
- Protection of the TOE Security Functions (TSF)
- Virtual Machine Domain Separation

1.4.2.1 Security Audit

The auditing security function of the TOE is provided by both the ESX Server and VirtualCenter. Audit data collected by the ESX Server is stored in a flat file on the ESX Server. Audit data collected by the VirtualCenter is stored as events in the VirtualCenter 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 will also be recorded, if applicable.

The VirtualCenter provides the capability to review its audit records by reviewing the event logs stored on the VirtualCenter Database. Only a VirtualCenter Administrator can view all the event logs. Audit events are viewed through the Virtual Infrastructure Client under the event tab for each organizational object. The ESX Server stores its audit records in */var/log/messages* and */var/log/vmwar* directories. Reviewing the audit records on the ESX Server is restricted to the ESX System Administrator.

1.4.2.2 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 and OpenSSH which perform the encryption and the decryption of data that is being passed.

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

1.4.2.3 User Data Protection

The TOE provides two distinct access control mechanisms. One is used for verifying access to objects under the control of the ESX Server by users logged into the ESX Server and users who make requests on the ESX Server from the VirtualCenter. The other is used for verifying access to objects on the VirtualCenter by users logged into the VirtualCenter. 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 VirtualCenter access control mechanism controls access to objects stored on the VirtualCenter, such as virtual machines, and VM Groups. The VirtualCenter access control mechanism also controls access to file events, alarm, and scheduled event information. This information is stored in the VirtualCenter Database. It should be noted that the VirtualCenter access control mechanism is enforced when the VirtualCenter accesses the VirtualCenter data stored in VirtualCenter Database. The VirtualCenter access control mechanism also controls access by a VirtualCenter user to data and operations specific to the definition, configuration, and management of virtual machines. ESX Server-specific information is physically stored on the hosting ESX Server, and is made available to the VirtualCenter user via the VirtualCenter Agent installed on the ESX Server.

EXT_FDP_VC_ETC.1 was explicitly stated because there is a transfer of TOE data between VirtualCenter (TOE component) and the VirtualCenter database (IT Environmental component). VirtualCenter stores TOE data such as scheduled tasks, alarms, events, and permissions in the VirtualCenter database. EXT_FDP_VC_ETC.1 addresses the export of VirtualCenter data to the VirtualCenter database.

The ESX Server supports the roles of system administrator and VM administrator. Users of the system administrator role have unrestricted access in the ESX Server. Once an ESX Server is placed under the management of a VirtualCenter, requests from the VirtualCenter users are processed using the account, *vpxuser,* which uses the system administrator role. From the console, system administrator or root user access requests are processed as in any Linux system. They have access to any ESX or VM data on the system. The VM administrators cannot modify

ESX Server configuration files or data. User access control for VM administrators is the standard user, /group, /and other access control mechanism provided by the Console Operating system.

1.4.2.4 Identification and Authentication

When a user logs into the ESX Server, a user name and password are requested before any access is given. These authentication credentials are compared with the authentication credentials stored on the ESX Server 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.

When a user logs into VirtualCenter, the user is presented with a login screen, requesting the VirtualCenter name or IP[6] 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 Virtual Infrastructure Client is presented with the Virtual Infrastructure 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.

When VMware Update Manager starts up, it authenticates with VirtualCenter. VUM does not access the ESX Server; rather the ESX Server will always call VUM, thereby ensuring that only the VUM that is installed with the TOE will be able to download updates and patches to the ESX Server.

1.4.2.5 Security Management

The TOE ensures that the ability to modify user privileges on VirtualCenter objects is restricted to a VirtualCenter Administrator, or to an administrator-defined role explicitly given the required permissions.

The TOE ensures that the ability to modify permissions of users on ESX objects is restricted to system administrators. The capability to modify permissions of users on objects is provided by functions of the ESX Server that are inherited from the customized Console Operating System (COS) incorporated with the ESX Server.

1.4.2.6 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 information as it is transmitted between remote components of the TOE by using OpenSSL & OpenSSH. HTTP communications between VUM and the ISP Server[7], and between VUM and the ESX Server, are protected by signature verification.

Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. Each subject's and user's security privileges are separated. It is not possible to perform any actions on the system without successfully authenticating. Once a user has been authenticated, the user is bound to the appropriate roles and any privileges defined by the TOE access control. All access control rights are checked by the TOE's mechanisms and the TOE uses unique attributes for each user, then the TSF maintains separation between different users. As an example, if a user without explicit permission tries to configure a virtual machine, the user will not be able to save the changes.

1.4.2.7 Virtual Machine Domain Separation

The virtual machine separation security function of the TOE is provided by the ESX Server component. The TOE ensures that each virtual machine is isolated from any other virtual machines co-existing on the ESX Server. This

[6] IP – Internet Protocol

[7] This ISP server provides access to the servers for downloading patches and updates.

isolation is provided at the virtualization layer of the ESX Server. The virtualization layer of the ESX Server 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 ESX Server 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, nor can they leak data.

1.4.3 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 ESX Server. 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 are excluded from the evaluation.

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

1.5 TOE Description

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.

This evaluation is of the VMware ESX Server 3.5 and VirtualCenter 2.5. The ESX Server is a platform for hosting virtual machines. It runs directly on industry standard x86-compatible hardware and abstracts the resources to provide multiple virtual machines. VirtualCenter is a centralized management tool for one or more ESX Servers.[8]

Figure 2 shows the details of the deployment configuration of the TOE:

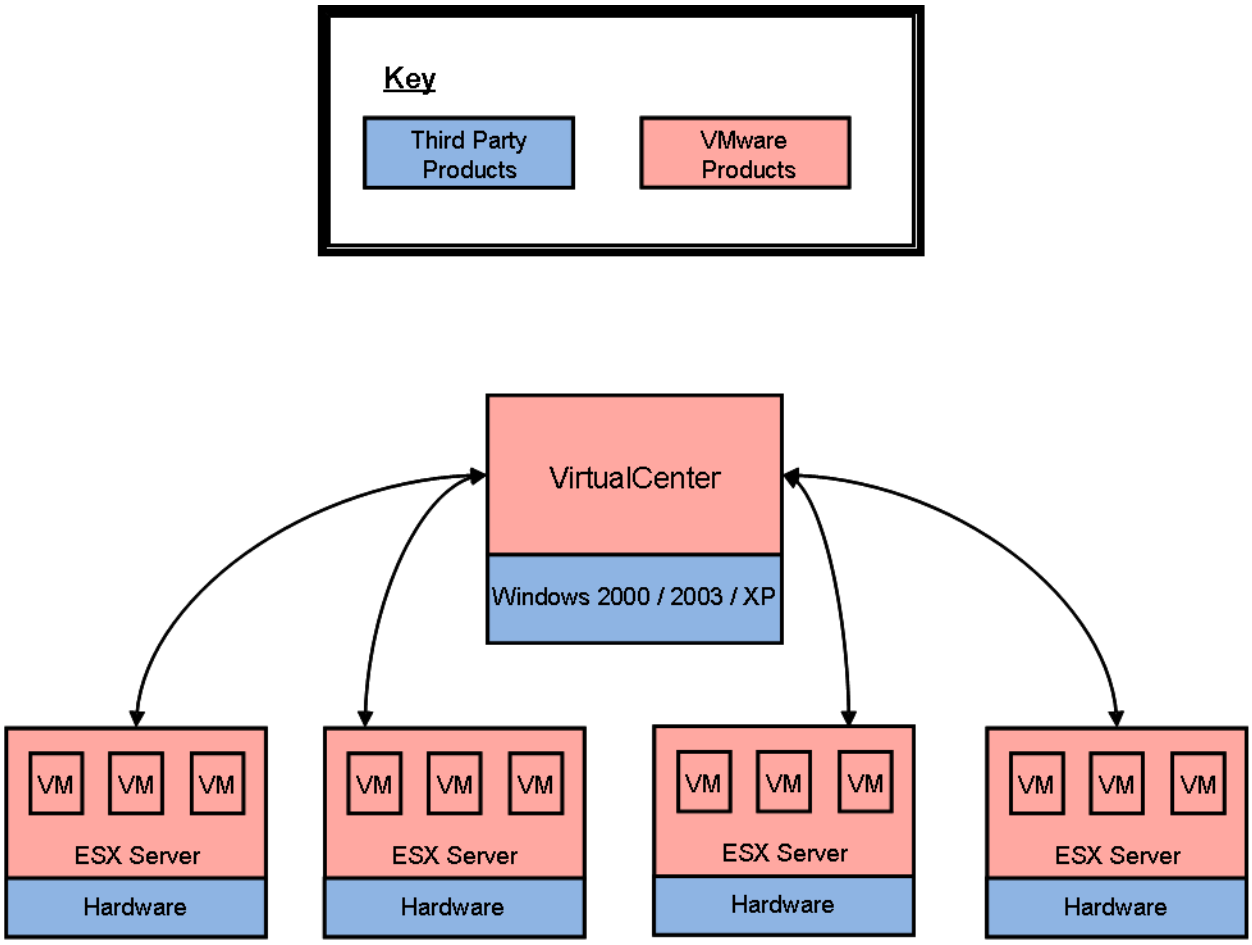


Figure 2 – Deployment Configuration of the TOE

[8] VirtualCenter also provides centralized management of VMware ESXi Servers.

1.5.1 Brief Description of the Components of the TOE

1.5.1.1 VirtualCenter

The VirtualCenter provides centralized management of ESX Servers. Through VirtualCenter, an administrator can configure an ESX Server, which includes viewing and managing the networking, data storage, security settings, user privileges and various object permissions. The VirtualCenter also allows the provisioning of virtual machines on the ESX Server. For example, virtual machines can be created, configured, cloned and relocated. VirtualCenter communicates with the ESX Server via the VirtualCenter agent located on the ESX Server. The confidentiality and integrity of this communication is protected using the Secure Sockets Layer (SSL) protocol and, optionally, certificates. SSL is provided using the OpenSSL embedded within VirtualCenter. The VirtualCenter's SSL implementation uses algorithms that are CAVP-validated against FIPS[9] requirements.

1.5.1.1.1 VirtualCenter Access Methods

VirtualCenter can be accessed by users via two different methods: by using the standalone Virtual Infrastructure Client software, or by using the Virtual Infrastructure Web Access client via a web browser.

1.5.1.1.1.1 Virtual Infrastructure Client

Users connect to VirtualCenter via the Virtual Infrastructure Client either locally (on the same machine as the VirtualCenter) or remotely, from a workstation running the Virtual Infrastructure Client software. Communication with the Virtual Infrastructure Client is protected using SSL.

1.5.1.1.1.2 Virtual Infrastructure Web Access Client

Users connect to VirtualCenter via the Virtual Infrastructure (VI) Web Access Client through a web browser. The VI Web Access client interface is provided by a Tomcat servlet engine in VirtualCenter. Thus, the VI Web Access Client is a component of VirtualCenter and a part of the TOE. The VI Web Access Client provides a subset of the functionality provided by the Virtual Infrastructure Client. Communication between the Virtual Infrastructure Web Access Client and the web browser is protected using HyperText Transfer Protocol over SSL (HTTPS), as shown in Figure 1.

1.5.1.2 VMware Update Manager

The VMware Update Manager (VUM) provides automated patch management for the ESX Server and its Virtual Machines. VUM scans the state of the VMware ESX host, and compare it with a baseline set by the administrator. It then applies updates and patches 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, but this is outside of the scope of this evaluation.

After performing a scan against the ESX Server, VUM accesses VMware's website to download keys and other metadata about the patches via HTTPS. It then sends the key to an ISP server, which accesses the appropriate server to retrieve updates. VUM then downloads the patches to be installed on the TOE via HTTP, and uses a certificate to verify the signature on the downloaded binary, thereby ensuring that it is the correct one. VUM stores the binary locally on the VirtualCenter machine. The ESX Server then pulls the appropriate updates and patches from VUM's database via HTTP, using a key and signature to verify the downloaded binaries[10].

[9] Federal Information Processing Standard

[10] It should be noted that the use of the VUM feature can result in modifications to the CC-configuration of the TOE.

1.5.1.3 ESX Server

The ESX Server is a 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 without privileges explicitly granted by the ESX Server system administrator. 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 feature enables a single virtual machine to use multiple physical processor cores simultaneously. The number of virtual processors is configurable for each virtual machine.

ESX Server also provides robust virtual and virtualized networking. ESX Server virtualizes the physical network to which it is connected, allowing properly configured virtual machines to connect to and communicate via the physical network as if they were directly connected to it. ESX Server also implements virtual network switches, called "vSwitches". A vSwitch works much like a physical Ethernet switch – it detects which virtual machines and physical network interfaces are logically connected to each of its virtual ports and uses that information to forward traffic to the correct destination – but the vSwitch is implemented entirely in software as part of the ESX Server. ESX vSwitches also implement VLANs[11], which are an IEEE[12] 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 ESX Server allows the protection of a set of virtual machines from accidental or malicious intrusions.

ESX Server uses Tomcat to support the Virtual Infrastructure Client. Tomcat is used as a web server that also supports server-side java code. These servlets support the use of the browser interface. The confidentiality and integrity of this communication, and communication with the Virtual Infrastructure Client is protected using SSL, provided by OpenSSL. The ESX Server can also be accessed using a console. When the console is used remotely the confidentiality and integrity of the communication is protected using OpenSSH.

ESX Server can be installed in three distinct configurations.

- **Configuration 1: Local Storage Only:** In the first configuration, the ESX Server is installed on a server and uses local disk for storage for VM images, VM data, and ESX data.

- **Configuration 2: ESX Local/virtual machines on Storage Area Network (SAN) or other supported datastore:** In the second configuration, the ESX Server is installed on a server and uses local storage for ESX data. Virtual machines are installed on a SAN, NFS[13] or iSCSI[14] datastore.

- **Configuration 3: Boot from SAN:** In the third configuration, the ESX Server is installed on the SAN. Local storage is disabled. VM images and VM data are stored on the SAN or other supported datastore.

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

1.5.1.3.1 VirtualCenter Agent

The VirtualCenter Agent forwards requests for services from VirtualCenter users, when the ESX Server is under the management of a VirtualCenter. ESX Servers can only be managed by a single VirtualCenter. The requests from

[11] VLAN – Virtual Local Area Network

[12] IEEE – Institute of Electrical and Electronics Engineers

[13] NFS – Network File System

[14] iSCSI – Internet Small Computer System Interface

the VirtualCenter Agents are handled by the ESX Server daemon in a manner similar to requests from users at the console or browser interface.

1.5.2 TOE Environment

The VirtualCenter Server hardware must meet the following requirements:

- 2.0 Gigahertz (GHz) or higher Intel or AMD x86 processor.
- 2 Gigabytes (GB) RAM[15]
- 560 Megabytes (MB) minimum free disk space, 2GB recommended.[16]
- 10/100 Ethernet adapter minimum

The VirtualCenter Server supports the following operating systems:

- Windows 2000 Server SP[17]4 with Update Rollup 1
- Windows XP Pro SP2
- Windows 2003 SP1 and SP2 (all releases except 64 bit)

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

The VirtualCenter Server supports the following databases:

- Microsoft SQL Server 2000 (SP4 only),
- Microsoft SQL Server 2000 Enterprise,
- Microsoft SQL Server 2005 Standard or Enterprise SP1 or SP2,
- Microsoft SQL Server 2005 Express SP2,
- Oracle 9i Release 2 Standard or Enterprise, or
- Oracle 10g Release 1 or Release 2 (versions 10.1.0.3.0 and higher only)

The Virtual Infrastructure Client hardware must meet the following requirements:

- 266 Megahertz (MHz) or higher Intel or AMD x86 processor
- 256MB RAM, 512 or higher recommended
- 150MB free disk space
- 10/100 Ethernet adapter

The virtual Infrastructure Client is designed for the 32 bit versions of these operating systems:

- Windows 2000 Pro SP4
- Windows 2000 Server SP4
- Windows XP Pro SP2 or higher
- Windows 2003 R2
- Windows Vista Business

---

[15] RAM: Random Access Memory

[16] Disk space requirements for VirtualCenter Server (including VUM) vary greatly as they are dependent factors such as the number of ESX Servers and/or ESXi Servers managed, number of Virtual Machines managed, types of Guest Operating System installed, and etc. VMware Update Manager Sizing Estimator on URL below can be used to estimate disk space needed.

http://www.vmware.com/support/vi3/doc/vi3_vum_10_sizing_estimator.xls

[17] SP – Service Pack/Service Package

- Windows Vista Enterprise

The VI Web Access client is designed for these browsers:

- Windows: Internet Explorer 6.0 or higher, Netscape Navigator 7.0, Mozilla 1.X, Firefox 1.0.7 and higher
- Linux: Netscape Navigator 7.0 or later, Mozilla 1.x, Firefox 1.0.7 and higher

You need the following hardware and system resources to install and use ESX Server.

The ESX Server hardware must meet the following requirements:

- 2 1500 MHz Intel Xeon and later, or AMD Opteron (32 bit mode) or 1 1500 MHz Intel Viiv or AMD A64 x2 dual core processors
- 1GB RAM minimum
- One or more supported Ethernet controllers.
- One or more supported storage controllers

2 Conformance Claims

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

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007; CC Part 2 extended; CC Part 3 conformant; PP claim (none).
PP Identification	None
Evaluation Assurance Level	EAL4 (Augmented with Flaw Remediation (ALC_FLR.1))

3 Security Problem Definition

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 deployed. 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 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
- have a low attack potential

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.
- a process running on a Virtual Machine that may attempt to circumvent the operating mechanism of the Virtual Networking scheme.

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

The following threats are applicable:

Table 4 – Threats

Name	Description
T.COMINT	An unauthorized individual may attempt to compromise the security of the data collected and produced by the TOE by bypassing a security mechanism.
T.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 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 5 – Assumptions

Name	Description
A.DBMS	The VirtualCenter database is configured so that it is only accessible to the VirtualCenter processes and the VirtualCenter system administrator.
A.NOEVIL	Users are non-hostile, appropriately trained, and follow all user guidance.
A.PHYSCL	The ESX Server and VirtualCenter components will be located within controlled access facilities which will prevent unauthorized physical access. The Virtual Infrastructure 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 6 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, can 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 System data as it passes between remote components of the TOE.
O.VM	The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.
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.VSWITCH	The TOE must ensure that network traffic traversing a vSwitch is only delivered to the intended virtual machines and physical interfaces.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

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

Table 7 – IT Security Objectives

Name	Description
OE.DBMS	The IT Environment will only allow the VirtualCenter processes and the VirtualCenter system administrator to access the VirtualCenter database.
OE.IDAUTH	The IT Environment will provide reliable verification of the Virtual Infrastructure Client user credentials.
OE.SEP	The IT Environment will protect the TOE from external interference or tampering.
OE.TIME	The IT Environment will 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 8 – Non-IT Security Objectives

Name	Description
NOE.NOEVIL	Users are non-hostile, appropriately trained, and follow all user guidance.
NOE.PHYSCL	The ESX Server and VirtualCenter components will be located within controlled access facilities which will prevent unauthorized physical access. The Virtual Infrastructure Client component will only connect to the server via the protected management network.

5 Extended Components Definition

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

5.1 Extended TOE Security Functional Components

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

Table 9 – Extended TOE Security Functional Requirements

Name	Description
EXT_FDP_VC_ETC.1	Export of VirtualCenter data
EXT_FDP_VC_ITC.1	Import of VirtualCenter data
EXT_FIA_VC_LOGIN.1	VirtualCenter user login request
EXT_VDS_VMM.1	ESX virtual machine domain separation

5.1.1 Class FDP: User Data Protection

Families in this class address the requirements for functions to establish and verify a claimed user identity. The extended family "EXT_FDP_VC_ETC: Export of VirtualCenter data", and "EXT_FDP_VC_ITC: Import of VirtualCenter data" was modeled after FDP_ETC.1 and FDP_ITC.1, respectively.

5.1.1.1 Export of VirtualCenter data (EXT_FDP_VC_ETC)

Family Behavior

This family defines the behavior of the VirtualCenter when it exports VirtualCenter data to the VirtualCenter database.

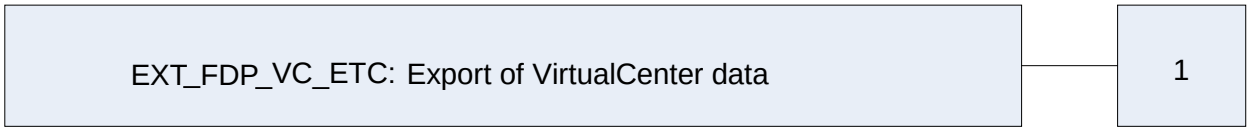


Figure 3 – EXT_FDP_VC_ETC Export of VirtualCenter Data Family decomposition

EXT_FDP_VC_ETC.1 Export of VirtualCenter data, defines the behavior of the VirtualCenter when exporting VirtualCenter data to the VirtualCenter database. It was modeled after FDP_ETC.1.

EXT_FDP_VC_ETC.1 Export of VirtualCenter data

Hierarchical to: No other components

Dependencies: FDP_ACC.1(a)

This component will ensure that VirtualCenter data is exported to VirtualCenter, from VirtualCenter database.

EXT_FDP_VC_ETC.1.1 VirtualCenter shall enforce the VirtualCenter Access Control Policy when exporting VirtualCenter data, controlled under the SFP, to the VirtualCenter database.

5.1.1.2 Import of VirtualCenter data (EXT_FDP_VC_ITC)

Family Behavior

This family defines the behavior of the VirtualCenter when it imports VirtualCenter data from the VirtualCenter database.

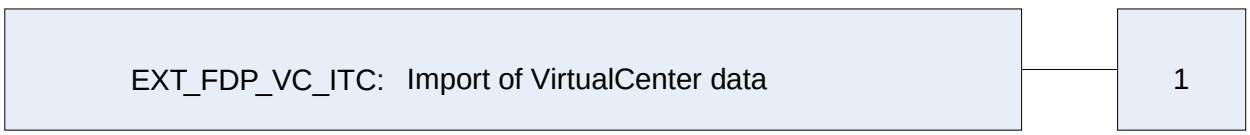


Figure 4 – EXT_FDP_VC_ITC Import of VirtualCenter Data Family decomposition

EXT_FDP_VC_ITC.1 Import of VirtualCenter data, defines the behavior of the VirtualCenter when importing VirtualCenter data from VirtualCenter database. It was modeled after FDP_ITC.1.

EXT_FDP_VC_ITC.1 Import of VirtualCenter data

Hierarchical to: No other components

Dependencies: FDP_ACC.1(a)

This component will ensure that VirtualCenter imports VirtualCenter data from the VirtualCenter database and that the VirtualCenter Access Control Policy is enforced on VirtualCenter data that are imported.

EXT_FDP_VC_ITC.1.1 VirtualCenter shall enforce the VirtualCenter Access Control Policy when importing VirtualCenter data, controlled under the SFP, from the VirtualCenter database.

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: VirtualCenter user login request" was modeled after the other FIA SFRs.

5.1.2.1 VirtualCenter user login request (EXT_FIA_VC_LOGIN)

Family Behavior

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

Component Leveling

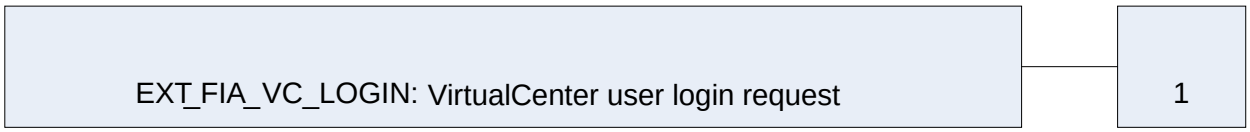


Figure 5 – EXT_FIA_VC_LOGIN VirtualCenter user login request family decomposition

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

EXT_FIA_VC_LOGIN.1 VirtualCenter user login request

Hierarchical to: No other components

Dependencies: None

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

EXT_FIA_VC_LOGIN.1.1 VirtualCenter shall request identification and authentication from the VirtualCenter environment for a VirtualCenter 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 ESX virtual machine domain separation (EXT_VDS_VMM)

Family Behavior

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

Component Leveling

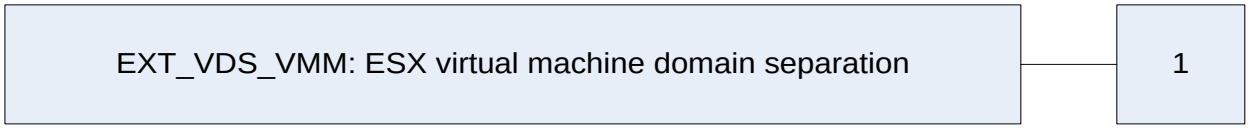


Figure 6 – EXT_VDS_VMM: ESX virtual machine domain separation family decomposition

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

EXT_VDS_VMM.1 ESX 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[18].

[18] 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 Parts 2 and 3 of the CC, and are shown as follows:

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

6.2 Security Functional Requirements

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

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1(a)	Subset access control (VirtualCenter)		✓		✓
FDP_ACC.1(b)	Subset access control (ESX Server)		✓		✓
FDP_ACF.1(a)	Security attribute based access control (VirtualCenter)		✓	✓	✓
FDP_ACF.1(b)	Security attribute based access control (ESX Server)		✓	✓	✓
FDP_IFC.2	Complete information flow control		✓	✓	

Name	Description	S	A	R	I
FDP_IFF.1	Simple security attributes		✓	✓	
EXT_FDP_VC_ETC.1	Export of VirtualCenter data				
EXT_FDP_VC_ITC.1	Import of VirtualCenter data				
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
EXT_FIA_VC_LOGIN.1	VirtualCenter user login request				
FMT_MSA.1(a)	Management of security attributes (VirtualCenter)	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes (ESX Server)	✓	✓		✓
FMT_MSA.1(c)	Management of security attributes (Virtual Switch Information Flow Control)	✓	✓		✓
FMT_MSA.3(a)	Static attribute initialization (VirtualCenter)	✓	✓	✓	✓
FMT_MSA.3(b)	Static attribute initialization (ESX Server)	✓	✓	✓	✓
FMT_MSA.3(c)	Static attribute initialization (Virtual Switch Information Flow Control)	✓	✓	✓	✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1(a)	Security roles (VirtualCenter)		✓	✓	
FMT_SMR.1(b)	Security roles (ESX Server)		✓	✓	
FPT_ITC.1	Inter-TSF confidentiality during transmission				
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
EXT_VDS_VMM.1	ESX virtual machine domain separation				

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

6.2.1 Class FAU: Security Audit

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:

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

FAU_GEN.1.2

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

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

Dependencies: FPT_STM.1 Reliable time stamps

Table 11 – Auditable Events on the ESX Server

Audit Event	*Additional Collected Information*
Startup and shutdown of the Auditing functions	*<none>*
All management operations performed on virtual machines[19]	*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*

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

[19] This audit event refers to management actions taken by an ESX or VirtualCenter administrator via the ESX or VirtualCenter management interfaces; it does not refer to VM guest-OS administrator events which occur within the guest-OS.

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

Table 12 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standard	Certificate #
Symmetric encryption and decryption	Triple-DES[20] (2-Key) CBC[21]	128	FIPS 46-3	CAVP (cert #902)
	AES[22] (128, 256) CBC	128, 256	FIPS 197	CAVP (cert #1271, #1274)
Message Authentication	HMAC[23]	1024	FIPS 198	CAVP (cert #741)
Message Digest	SHA-1	N/A[24]	FIPS 180-3	CAVP (cert #1174)
Digital signature verification of VPXA bundle	RSA digital signature	1024, 2048, 3072, 4096	FIPS 186-2	CAVP (cert #612)
Digital signatures for patch bundles (used by VUM)	RSA digital signature	1024, 2048, 3072, 4096	FIPS 186-2	CAVP (cert #612)

Dependencies: N/A[25]

[20] DES – Data Encryption Standard

[21] CBC – Cipher Block Chaining

[22] AES – Advanced Encryption Standard

[23] HMAC – Hash-based Message Authentication Code

[24] N/A – Not Applicable

[25] FCS_CKM.1 and FCS_CKM.4 are not listed as dependencies, following the guidance of CCS Instruction #4, version 1.0.

6.2.3 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control (VirtualCenter)

Hierarchical to: No other components.

FDP_ACC.1.1(a)

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

a. Subjects: processes acting on behalf of VirtualCenter users

b. 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, 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 (ESX Server)

Hierarchical to: No other components.

FDP_ACC.1.1(b)

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

a. Subjects: processes acting on behalf of ESX Server users

b. Objects: virtual machine definition and configuration files; ESX Server configuration files; ESX Server 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(a) Security attribute based access control (VirtualCenter)

Hierarchical to: No other components.

FDP_ACF.1.1(a)

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

a. Subjects: Processes acting on behalf of users of the VirtualCenter

b. Subject security attributes: User identity or User group(s), VC-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, VC-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: [

1. Access is granted if the user is a member of the administrators group of the underlying Windows operating system of the VirtualCenter, also known as a VirtualCenter Administrator.

2. Access to perform a given activity on an object is allowed on the VirtualCenter 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 VC-role allowing the activity requested by the subject.

3. Access to perform a given activity on an object is allowed on the VirtualCenter 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 VC-role allowing the activity requested by the subject.

4. 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 VC-role of any such matching permission pair does not permit the activity requested by the user, then access is denied[26]].

FDP_ACF.1.3(a)

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

FDP_ACF.1.4(a)

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

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

FDP_ACF.1(b) Security attribute based access control (ESX Server)

Hierarchical to: No other components.

FDP_ACF.1.1(b)

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

a. Subjects: Processes acting on behalf of users of the ESX Server

b. Subject security attributes: User identity or User group(s), ESX Server User role

c. Objects: virtual machine definition and configuration files; ESX Server configuration files, ESX Server audit logs

[26] All VirtualCenter 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.

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 ESX Server** is allowed: [

1. Access is granted if the ESX Server role is system administrator.

2. Access is granted if the ESX Server 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.

3. Access is granted if the ESX Server 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.

4. Access is granted if the ESX Server role is not system administrator and the requested access is allowed for anyone.

5. If the user is a VM administrator and the requested action is register or unregister[27] *a VM, then the user must have read, write, and execute access to the VM's configuration file for the operation to be allowed.*

6. 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 authorize access of subjects to objects **or operations of the ESX Server** 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 ESX Server** 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 ESX Server** shall enforce the [*virtual switch information flow control SFP*[28]] on [

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

b. Information: network data packets]

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

[28] SFP – Security Functional Policy

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 ESX Server** 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 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 authorize 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 initialization

EXT_FDP_VC_ETC.1 Export of VirtualCenter data

Hierarchical to: No other components.

EXT_FDP_VC_ETC.1.1

VirtualCenter shall enforce the VirtualCenter Access Control Policy when exporting VirtualCenter data, controlled under the SFP, to the VirtualCenter database.

Dependencies: FDP_ACC.1(a) Subset access control (VirtualCenter)

EXT_FDP_VC_ITC.1 Import of VirtualCenter data

Hierarchical to: No other components.

EXT_FDP_VC_ITC.1.1

VirtualCenter shall enforce the VirtualCenter Access Control Policy when importing VirtualCenter data, controlled under the SFP, from the VirtualCenter database.

Dependencies: FDP_ACC.1(a) Subset access control (VirtualCenter)

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 **ESX Server** 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 **ESX Server** 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 VirtualCenter user login request

Hierarchical to: No other components.

EXT_FIA_VC_LOGIN.1.1

VirtualCenter shall request identification and authentication from the VirtualCenter environment for a VirtualCenter 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 (VirtualCenter)

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*VirtualCenter 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, VC-role) for all subjects and all objects in the VirtualCenter*] to [*VirtualCenter Administrators and VirtualCenter 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 (ESX Server)

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*ESX Server Access Control Policy*] to restrict the ability to [*modify, delete, [add]*] the security attributes [*For ESX Server users: user id; user groups; ESX Server User Role; For ESX Server objects: object owner; object group; object read, write, and execute permissions of security attributes*] to [*the role as described in Table 13*].

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 13 – FMT_MSA.1(b) – Security Attributes, Actions, and 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, ESX Server 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 (VirtualCenter)

Hierarchical to: No other components.

FMT_MSA.3.1(a)

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

FMT_MSA.3.2(a)

The TSF shall allow the [*VirtualCenter Administrators and Administrator defined roles*] to specify alternative initial values to override the default values when an object or information is created **on the VirtualCenter**.

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

FMT_MSA.3(b) Static attribute initialization (ESX Server)

Hierarchical to: No other components.

FMT_MSA.3.1(b)

The TSF shall enforce the [*ESX Server Access Control Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the **ESX Server 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 ESX Server, as described in Table 14**.

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

Table 14 – 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 ESX Server**.

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: [

1. Adding, deleting, or modifying the object permissions associated with a user or group on the VirtualCenter

2. Adding, deleting, or modifying user or group membership on the ESX Server

3. Modification of permissions associated with an object on the ESX Server

4. Functions to create, modify, or delete virtual machines

5. Users can change their own passwords on the ESX Server

6. Power operations on a virtual machine].

Dependencies: No Dependencies

FMT_SMR.1 (a) Security roles (VirtualCenter)

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles **for VirtualCenter users** [*VirtualCenter Administrator and Administrator defined roles*].

FMT_SMR.1.2

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

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1 (b) Security roles (ESX Server)

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles **for ESX Server users** [*VM Administrator and System Administrator*].

FMT_SMR.1.2

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

Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

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

Dependencies: No dependencies

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 a remote trusted IT product from unauthorized disclosure during transmission.

Dependencies: No dependencies

6.2.7 Class EXT_VDS: Virtual Machine Domain Separation

EXT_VDS_VMM.1 ESX 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.1. Table 15 – Assurance Requirements summarizes the requirements.

Table 15 – 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.1 Basic Flaw Remediation
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_FUN.1 Functional testing
	ATE_DPT.2 Testing: security enforcing modules
	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 16 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR	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 (VirtualCenter)
	FDP_ACC.1(b)	Subset access control (ESX Server)
	FDP_ACF.1(a)	Security attribute based access control (VirtualCenter)
	FDP_ACF.1(b)	Security attribute based access control (ESX Server)
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
	EXT_FDP_VC_ETC.1	Export of VirtualCenter data
	EXT_FDP_VC_ITC.1	Import of VirtualCenter data
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	EXT_FIA_VC_LOGIN.1	VirtualCenter user login request

TOE Security Function	SFR	Description
Security Management	FMT_MSA.1(a)	Management of security attributes (VirtualCenter)
	FMT_MSA.1(b)	Management of security attributes (ESX Server)
	FMT_MSA.1(c)	Management of security attributes (Virtual Switch Information Flow Control)
	FMT_MSA.3(a)	Static attribute initialization (VirtualCenter)
	FMT_MSA.3(b)	Static attribute initialization (ESX Server)
	FMT_MSA.3(c)	Static attribute initialization (Virtual Switch Information Flow Control)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1(a)	Security roles (VirtualCenter)
	FMT_SMR.1(b)	Security roles (ESX Server)
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	ESX virtual machine domain separation

7.1.1 Security Audit

The auditing security function of the TOE is provided by both the ESX Server and VirtualCenter. Audit data collected by the ESX Server is stored in a flat file on the ESX Server. Audit data collected by the VirtualCenter is stored as events on the VirtualCenter Database.

The TOE audit records contain the following information:

Table 17 – Audit Record Contents

Field	Content
Timestamp	Date and time of the event
Class	Type of event

Field	Content
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. These audit records are stored as events, and are managed by the VirtualCenter Access Control Policy. They are stored on the VirtualCenter Database.

The VirtualCenter provides the capability to review its audit records by reviewing the event logs stored on the VirtualCenter 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 Virtual Infrastructure Client under the event tab for each organizational object.

The ESX Server audit records are stored in a flat file on the Service Console of the ESX Server. They are stored in */var/log/messages* and */var/log/vmware* directories. Reviewing the audit records on the ESX Server is restricted to the ESX System Administrator.

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

7.1.2 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 and OpenSSH which perform the encryption and the decryption of data that is being passed.

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

TOE Security Functional Requirements Satisfied: FCS_COP.1

7.1.3 User Data Protection

The TOE provides two distinct access control mechanisms. One is used for verifying access to objects under the control of the ESX Server by users logged into the ESX Server and users who make requests on the ESX Server from the VirtualCenter, and another for verifying access to objects on the VirtualCenter by users logged into the VirtualCenter. 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.

7.1.3.1 VirtualCenter Access Control Policy

The VirtualCenter access control mechanism controls access to objects stored on the VirtualCenter, such as virtual machines, and VM Groups. The VirtualCenter 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 VirtualCenter Database. It should be noted that the VirtualCenter access control mechanism is enforced when the VirtualCenter accesses the VirtualCenter data stored in VirtualCenter Database. The VirtualCenter access control mechanism also

controls access by a VirtualCenter user to data and operations specific to the definition, configuration, and management of virtual machines. ESX Server-specific information is physically stored on the hosting ESX Server, and is made available to the VirtualCenter user via the VirtualCenter Agents installed on the ESX Server.

TOE users on the VirtualCenter are administrators who have been assigned to one of two roles categories: VirtualCenter 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 VirtualCenter user requests an operation to be performed on a particular object, the access control security function first determines if the user is a VirtualCenter 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 VirtualCenter are user identity, group membership, and role (VirtualCenter Administrator or Limited access user). For objects stored on the VirtualCenter, the security attributes are sets of permission pairs consisting of user identity or group and VirtualCenter 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 VirtualCenter-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.

7.1.3.2 ESX Server Access Control Policy

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

When a user wants to perform tasks on data that is stored in an ESX Server managed by the VirtualCenter, the same access control checks described above are performed on the VirtualCenter. If the requested access is permitted, then a request, along with the password for the *vpxuser* account described above, is passed to the VirtualCenter Agent on the ESX Server, by the VirtualCenter. 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 is denied.

The ESX Server mechanism controls access by subjects logged into the ESX Server, and by subjects requesting services from the managing VirtualCenter, to objects stored on the ESX Server. 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 ESX Server supports the two roles: system administrator and VM administrator. The users with the system administrator role have unrestricted access in the ESX, whereas the users with the VM administrator role may be controlled by group membership or by user identity. The ESX is designed so that the same access control mechanisms can be used for direct ESX users who log into the ESX Server via the service console or the management interface, and for indirect ESX users who access the ESX Server from the VirtualCenter. Once an ESX Server is place under the management of a VirtualCenter, requests from the VirtualCenter users are processed using the *vpxuser* account. The *vpxuser* account is set up granting access to all VM configuration files (.vmx files).

From the console, system administrator or root user access requests are processed in ways similar to most Linux operating system. They have access to any ESX or VM data on the system. The VM administrators cannot modify ESX Server configuration files or data. User access control for VM administrators is the standard user/group/other access control mechanism provided by the Console Operating System (COS). 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.

7.1.3.3 Virtual Switch Information Flow Control Policy

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

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, EXT_FDP_VC_ETC.1, EXT_FDP_VC_ITC.1

7.1.4 Identification and Authentication

When a user logs into the ESX Server, a user name and password are requested before any access is given. These authentication credentials are compared with the authentication credentials stored on the ESX Server in a shadow file, where the password is hashed using 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.

When a user logs into VirtualCenter they are presented with a login screen, requesting the VirtualCenter 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 Virtual Infrastructure Client is presented with the Virtual Infrastructure 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.

When VMware Update Manager starts up, it authenticates with VirtualCenter. VUM does not access the ESX Server; rather the ESX Server will always call VUM, thereby ensuring that only the VUM that is installed with the TOE will be able to download updates and patches to the ESX Server.

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

7.1.5 Security Management

The ESX 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 ESX Server. 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 VirtualCenter when it manages activities for the connected ESX Server. The *vpxuser* account is initially created when the VirtualCenter adds the ESX Server as one of its managed hosts for the first time.

It should be noted that the VirtualCenter supplies the username and password for either the *root* account or the user account with a *system administrator* role, when adding the ESX Server for the first time. When this authentication with the ESX Server is successful, a special account called *vpxuser* is created on the ESX Server along with a *vpxuser* password known only to the VirtualCenter and the specific ESX Server. This login account (*vpxuser* account) and password *(vpxuser* password) are used for all subsequent connections between the ESX Server and the VirtualCenter.

No users on the ESX Server or the VirtualCenter, other than the VirtualCenter administrator, have access to the *vpxuser* passwords stored in the VirtualCenter 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 plain text.
- There is no way to change the *vpxuser* password manually.
- The *vpxuser* password for each ESX Server under the management of a VirtualCenter is unique for that ESX Server. Thus, it is a one to many relationship: A single VirtualCenter machine possessing many (and unique) *vpxuser* passwords for all the ESX Servers it manages.

VM administrators are administrators of individual VMs on the ESX Server. VM administrators can access the VMs by directly logging into the ESX Server or through the VirtualCenter. The VirtualCenter uses the *vpxuse*r account and password to gain access to the ESX Server and process the requests on behalf of the VM administrators.

The TOE ensures that the ability to modify permissions of users on ESX objects is restricted to ESX System Administrators. The capability to modify permissions of users on objects is provided by functions of the ESX that are inherited from the customized Linux kernel which the ESX 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 ESX defaults for access permission are controlled by the umask setting. The default value can only be changed by an ESX System Administrator.

The TOE provides security management functions that address the management of security attributes for the ESX Server (role, user id for subjects, and owner, group, and r,w,x permissions for owner, object group, and other for objects) and VirtualCenter (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[29] on virtual machines.

The VirtualCenter supports two categories of roles: VirtualCenter Administrator and Administrator defined roles. The VirtualCenter 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.

[29] "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.

In the CC-evaluated configuration, all administrators using the Virtual Infrastructure 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 Virtual Infrastructure Client and the ESX Server, or between the Virtual Infrastructure Client and the VirtualCenter.

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)

7.1.6 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 information as it is transmitted between remote components of the TOE by protecting the information using OpenSSL & OpenSSH. HTTP communications between VUM and the ISP Server, and between VUM and the ESX Server, are protected by signature verification.

Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. Each subject's and user's security privileges are separated. It is not possible to perform any actions on the system without successfully authenticating. Once a user has been authenticated, the user is bound to the appropriate roles and any privileges defined by the TOE access control. All access control rights are checked by the TOE's mechanisms and the TOE uses unique attributes for each user, then the TSF maintains separation between different users. As an example, if a user without explicit permission tries to configure a virtual machine, the user will not be able to save the changes.

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

7.1.7 Virtual Machine Domain Separation

The virtual machine separation security function of the TOE is provided by the ESX Server component. The TOE ensures that each virtual machine is isolated from any other virtual machines co-existing on the ESX Server. This isolation is provided at the virtualization layer of the ESX Server. The virtualization layer of the ESX Server 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 ESX Server 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 unacceptable/unauthorized ways, nor can they leak data. 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. Table 18 and 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.

Table 18 – Relationship of Security Threats to Objectives

Objectives / Threats, Assumptions		TOE Objectives									Environmental Objectives				
											IT			Non-IT	
		O.ADMIN	O.AUDIT	O.IDAUTH	O.ACCESS	O.SECURE	O.VM	O.VLAN	O.VSWITCH	OE.DBMS	OE.IDAUTH	OE.TIME	OE.SEP	NOE.NOEVIL	NOE.PHYSCL
Threats	T.VM						✓						✓		
	T.COMINT	✓	✓	✓		✓					✓	✓	✓		
	T.PRIVIL	✓	✓	✓	✓						✓	✓	✓		
	T.VIRTUAL_NETWORK							✓	✓						
Assumptions	A.DBMS									✓					
	A.NOEVIL													✓	
	A.PHYSCL														✓

8.2.1 Security Objectives Rationale Relating to Threats

Table 19 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.VM A process running on one virtual machine might compromise the security of processes running on other virtual machines.	O.VM The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.	This threat is mitigated by the O.VM objective which 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.

Threats	Objectives	Rationale
	OE.SEP The IT 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.
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.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, can exercise such control.	The O.ADMIN objective requires that only authorized users are able to manage the security attributes of the TOE.
	O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The O.IDAUTH objective, supported by the OE.IDAUTH objective, requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	O.SECURE The TOE must ensure the confidentiality and integrity of all System data as it passes between remote components of the TOE.	The O.SECURE objective ensures that TOE data is protected when transmitted between remote components of the TOE.
	OE.IDAUTH The IT Environment will provide reliable verification of the Virtual Infrastructure 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.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.
	OE.SEP	The OE.SEP objective also supports these objectives by requiring that the

Threats	Objectives	Rationale
	The IT Environment will protect the TOE from external interference or tampering.	IT environment protect the TOE from interference that would prevent it from performing its functions.
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[30].
	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, can exercise such control.	The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage the functions and data of the TOE.
	O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.	The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	This threat is primarily diminished by the O.IDAUTH objective, supported by the OE.IDAUTH objective, which requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data.
	OE.IDAUTH The IT Environment will provide reliable verification of the Virtual Infrastructure 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.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE.

[30] TSP: TOE Security Policy

Threats	Objectives	Rationale
	OE.SEP The IT 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.
T.VIRTUAL_NETWORK A process running on a virtual machine attempts to deliver traffic to wrong VM or external entity.	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.VLAN requires that the vSwitch must deliver network traffic only to virtual machines 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.DBMS The VirtualCenter database is configured so that it is only accessible to the VirtualCenter processes and the VirtualCenter system administrator.	OE.DBMS The IT Environment will only allow the VirtualCenter processes and the VirtualCenter system administrator to access the VirtualCenter database.	The OE.DBMS objective ensures that there cannot be any unauthorized individual compromising the security of the TOE data by gaining access to the VirtualCenter DBMS.
A.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.	NOE.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.	The NOE.NOEVIL objective ensures that operators are non-hostile, appropriately trained, and follow all operator guidance.
A.PHYSCL	NOE.PHYSCL	The NOE.PHYSCL objective requires that the ESX Server and VirtualCenter

Assumptions	Objectives	Rationale
The ESX Server and VirtualCenter components will be located within controlled access facilities which will prevent unauthorized physical access. The Virtual Infrastructure Client component will only connect to the server via the protected management network.	The ESX Server and VirtualCenter components will be located within controlled access facilities which will prevent unauthorized physical access. The Virtual Infrastructure Client component will only connect to the server via the protected management network.	components will be located within controlled access facilities which will prevent unauthorized physical access, and that the VI 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_FDP_VC_ETC.1
- EXT_FDP_VC_ITC.1
- EXT_FIA_VC_LOGIN.1
- EXT_VDS_VMM.1

EXT_FDP_VC_ETC.1 was explicitly stated because there is a transfer of TOE data between VirtualCenter (TOE component) and the VirtualCenter database (IT Environmental component). VirtualCenter stores TOE data such as scheduled tasks, alarms, events, and permissions in the VirtualCenter database. EXT_FDP_VC_ETC.1 addresses the export of VirtualCenter data to the VirtualCenter database.

EXT_FDP_VC_ITC.1 was explicitly stated because there is a transfer of TOE data between VirtualCenter (TOE component) and the VirtualCenter database. VirtualCenter accesses TOE data such as scheduled tasks, alarms, events, and permissions that are stored in the VirtualCenter database. EXT_FDP_VC_ITC.1 addresses the import of VirtualCenter data from the VirtualCenter database.

EXT_FIA_VC_LOGIN.1 was explicitly stated because authentication and identification of VirtualCenter users is performed by the TOE Environment, and not by the TOE. This explicit requirement was written to make the link between the I&A provided by the environment, and the actions that VirtualCenter takes to ensure that only identified and authenticated users can access the TOE via VirtualCenter, 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.

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 requirements 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.

Table 21 – Relationship of Security Requirements to Objectives

Objectives / Requirements		TOE							
		O.ADMIN	O.AUDIT	O.IDAUTH	O.ACCESS	O.SECURE	O.VM	O.VLAN	O.VSWITCH
TOE	FAU_GEN.1		✓						
	FAU_SAR.1		✓						
	FCS_COP.1					✓			
	FDP_ACC.1(a)				✓				
	FDP_ACC.1(b)				✓				
	FDP_ACF.1(a)				✓				
	FDP_ACF.1(b)				✓				
	FDP_IFC.2							✓	✓
	FDP_IFF.1							✓	✓
	EXT_FDP_VC_ETC.1				✓				
	EXT_FDP_VC_ITC.1				✓				
	FIA_UAU.2			✓	✓				
	FIA_UID.2			✓	✓				
	EXT_FIA_VC_LOGIN.1			✓	✓				
	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)	✓		✓					
	FPT_ITT.1					✓			

Objectives / Requirements	TOE							
	O.ADMIN	O.AUDIT	O.IDAUTH	O.ACCESS	O.SECURE	O.VM	O.VLAN	O.VSWITCH
FPT_ITC.1					✓			
EXT_VDS_VMM.1						✓		

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 22 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FDP_ACC.1(a) Subset access control (VirtualCenter)	All access control requests must be checked for compliance with the TSP before execution.
	FDP_ACC.1(b) Subset access control (ESX Server)	
	FDP_ACF.1(a) Security attribute based access control (VirtualCenter)	
	FDP_ACF.1(b) Security attribute based access control (ESX Server)	
	EXT_FDP_VC_ETC.1 Export of VirtualCenter data	
	EXT_FDP_VC_ITC.1 Import of VirtualCenter data	
	FIA_UAU.2	The TOE will not give any access to a

Objective	Requirements Addressing the Objective	Rationale
	User authentication before any action	user until the TOE has identified (FIA_UID.2) and authenticated (FIA_UAU.2).
	FIA_UID.2 User identification before any action	
	EXT_FIA_VC_LOGIN.1 VirtualCenter user login request	For VirtualCenter 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 data, ensuring that TOE users with the appropriate privileges, and only those TOE users, can exercise such control.	FMT_MSA.1(a) Management of security attributes (VirtualCenter)	Only the roles defined in FMT_SMR.1 are given the right to modify or set defaults for TOE security attributes.
	FMT_MSA.1(b) Management of security attributes (ESX Server)	
	FMT_MSA.1(c) Management of security attributes (Virtual Switch Information Flow Control SFP)	
	FMT_MSA.3(a) Static attribute initialization (VirtualCenter)	
	FMT_MSA.3(b) Static attribute initialization (ESX Server)	
	FMT_MSA.3(c) Static attribute initialization (Virtual Switch Information Flow Control)	
	FMT_SMF.1 Specification of management functions	Mechanisms exist to enforce the rules specified in FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), and FMT_MSA.3(b).
	FMT_SMR.1(a) Security roles (VirtualCenter)	The TOE defines a set of roles supported by VirtualCenter.
	FMT_SMR.1(b) Security roles (ESX Server)	The TOE defines a set of roles supported by ESX Server.
O.AUDIT The TOE must gather audit	FAU_GEN.1 Audit data generation	Security-relevant events must be audited by the TOE.

Objective	Requirements Addressing the Objective	Rationale
records of actions on the TOE which may be indicative of misuse.	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).
	FIA_UID.2 User identification before any action	
	EXT_FIA_VC_LOGIN.1 VirtualCenter user login request	For VirtualCenter the TOE requires support from the TOE environment to verify the user credentials.
	FMT_SMR.1(a) Security roles (VirtualCenter)	The TOE must be able to recognize the different user roles that exist for the TOE.
	FMT_SMR.1(b) Security roles (ESX Server)	The TOE must be able to recognize the different user roles that exist for the TOE.
O.SECURE The TOE must ensure the confidentiality and integrity of all System data as it passes between remote components of the TOE.	FCS_COP.1 Cryptographic Operation	The TOE protects the confidentiality of information for data transmitted between the TOE components and also for data transmitted between the TOE and another trusted IT product, by applying data encryption.
	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.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 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.VLAN The TOE must ensure that	FDP_IFC.2 Complete information flow control	All data transmitted from or to a VM or a physical interface associated with a vSwitch will only be delivered to the

Objective	Requirements Addressing the Objective	Rationale
network traffic traversing a vSwitch is only delivered to virtual machines and physical interfaces that are part of the intended VLAN.		intended destination.
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	

8.5.2 Security Assurance Requirements Rationale

EAL4, augmented with ALC_FLR.1 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 a low attack potential.

8.5.3 Dependency Rationale

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

Table 23 – Functional Requirements Dependencies

SFR	Dependencies	Dependency Met	Rationale
EXT_FDP_VC_ETC.1	FDP_ACC.1(a)	✓	
EXT_FDP_VC_ITC.1	FDP_ACC.1(a)	✓	
EXT_FIA_VC_LOGIN.1	None	N/A	
EXT_VDS_VMM.1	None	N/A	
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 time stamps.
FAU_SAR.1	FAU_GEN.1	✓	
FCS_COP.1	N/A	N/A	FCS_CKM.1 and FCS_CKM.4 are not included, following the guidance of CCS Instruction #4, version 1.0.
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	

SFR	Dependencies	Dependency Met	Rationale
FDP_ACF.1(a)	FDP_ACC.1(a) FMT_MSA.3(a)	✓	
FDP_ACF.1(b)	FDP_ACC.1(b) FMT_MSA.3(b)	✓	
FDP_IFC.2	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3(c)	✓	FDP_IFC.1 dependency met by FDP_IFC.2, which is hierarchical to FDP_IFC.1
FIA_UAU.2	FIA_UID.1	✓	Met by FIA_UID.2, which is hierarchical to FIA_UID.1
FMT_MSA.1(a)	FDP_ACC.1(a) FMT_SMR.1(a) FMT_SMF.1(a)	✓	
FMT_MSA.1(b)	FDP_ACC.1(b) FMT_SMR.1(b) FMT_SMF.1(b)	✓	
FMT_MSA.1(c)	FPT_IFC.2 FMT_SMR.1(b) FMT_SMF.1(b)	✓	
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_SMR.1(a)	FIA_UID.1	✓	
FMT_SMR.1(b)	FIA_UID.1	✓	
FPT_ITC.1	None	N/A	
FPT_ITT.1	None	N/A	

9 Acronyms

Table 24 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input Output Signal
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CM	Configuration Management
DB	Database
DBMS	Database Management System
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GB	Gigabyte
GHZ	Gigahertz
HA	High Availability
HMAC	Hash-based Message Authentication Code)
HTTP	Hypertext Transport Protocol
HTTPS	Secure Hypertext Transport Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LAN	Local Area Network
MB	Megabytes
N/A	Not Applicable
NFS	Network File System
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
SAN	Storage Area Network
SAR	Security Assurance Requirement
SDK	Software Development Kit

Acronym	Definition
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMP	Symmetric Multiprocessing
SNMP	Simple Network Management Protocol
SP	Service Pack/ Service Package
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VC	VirtualCenter
VI	Virtual Infrastructure
VIC	VirtualCenter Infrastructure Client
VLAN	Virtual Local Area Network
VM	Virtual Machine
VUM	VMware Update Manager