VMware ESX Server 2.5.0 and

VMware VirtualCenter 1.2.0

Security Target

Release Date: March 10, 2006

Document ID: 04-695-R-0628

Version: 1.6.7

Prepared By: InfoGard Laboratories, Inc.

Prepared For: VMware, Inc.
3145 Porter Drive
Palo Alto CA 94304

Table of Contents

1.1 ST Identification......1

1.2 CC Conformance......1

1.3 TOE Overview......1

1.4 ST Organization......1

1.5 Document Conventions......2
1.5.1 Convention for Operations......2
1.5.2 Convention for Interpretations......3
1.5.3 Convention for Explicit Requirements......3

1.6 Terminology......3
1.6.1 CC Terms......3
1.6.2 ST Specific Terms......4

2.1 Overview......6

2.2 Architecture......7
2.2.1 ESX Server Architecture......8
2.2.2 VirtualCenter Architecture......11

2.3 The TOE and its Operating Environment......14
2.3.1 Physical External Interfaces and Users......14
2.3.2 Hardware and Software Requirements......18
2.3.3 TOE Time Synchronization requirements......23

2.4 TOE Physical Scope and Boundaries......23

2.5 TOE Logical Scope and Boundaries......24
2.5.1 Access Control......24
2.5.2 Auditing......25
2.5.3 Identification & Authentication......25
2.5.4 Security Management......25
2.5.5 Virtual Machine Domain Separation......26
2.5.6 TOE Protection......26

2.6 Items not included in the TOE or not claimed in the TOE......26
2.6.1 Rationale for excluding Virtual Machine guest operating systems and applications from the TOE.27

3.1 Assumptions......29

3.2 Threats......30

3.3 Organizational Security Policies......30

4.1 Security Objectives for the TOE......31

4.2 Security Objectives for the Environment......32

4.2.1 Security Objectives for the IT Environment....32
4.2.2 Security Objectives for the Non-IT Environment 32

4.3 Security Objectives Rationale 33
4.3.1 Tracing for Threats....33
4.3.2 Security Objectives Rationale: Threats to the TOE....34
4.3.3 Security Objectives Rationale: Organizational Security Policies....35
4.3.4 Security Objectives Rationale: Assumptions 35

5.1 Security Functional Requirements for the TOE 37
5.1.1 FAU: Security Audit 37
5.1.2 FDP: User Data Protection....38
5.1.3 FIA: Identification and Authentication 42
5.1.4 FMT: Security Management 43
5.1.5 FPT: Protection of the TOE functions....45

5.2 Explicitly Stated Security Functional Requirements for the TOE 46
5.2.1 FAU Audit....47
5.2.2 FIA: Identification and Authentication 48
5.2.3 VDS: VM Domain Separation 48

5.3 Security Functional Requirements for the IT Environment 48
5.3.1 FIA: Identification and Authentication 48
5.3.2 FMT: Security Management 49
5.3.3 FPT: Protection of the TSF 49

5.4 Security Assurance Requirements for the TOE 49
5.4.1 ACM: Configuration Management....49
5.4.2 ADO: Delivery and Operation 50
5.4.3 ADV: Development....51
5.4.4 AGD: Guidance Documents....53
5.4.5 ATE: Tests 54
5.4.6 AVA: Vulnerability Assessment....56

5.5 Strength of Function Claim....57

5.6 Security Requirements Rationale 57
5.6.1 Security Functional Requirements to Objectives Tracing....57
5.6.2 Rationale for Security Requirements on the TOE. 58
5.6.3 Rationale for Security Requirements on the TOE Environment 61
5.6.4 Rationale For SOF Claim for Security Functional Requirements 61
5.6.5 Rationale for Explicitly Stated SFRs....61
5.6.6 Security Functional Requirements Dependencies and Rationale 62
5.6.7 Rationale for the TOE Assurance Requirements....63

6.1 TOE Security Functions 64
6.1.1 Access Control 64
6.1.2 Auditing 67
6.1.3 Identification & Authentication....68
6.1.4 Security Management....70
6.1.5 TOE Protection....72
6.1.6 Virtual Machine Separation....74

6.2 Assurance Measures 75
6.2.1 EAL Justification 79

6.3 TOE Summary Specification Rationale 79
6.3.1 Rationale that Assurance Measures meet the Security Assurance Requirements 80

7.1 PP Reference 84

7.2 PP Tailoring 84

7.3 PP Additions 84

8.1 Rationale for Security Objectives 85

8.2 Rationale for Security Functional Requirements 85

8.3 Rationale for Security Assurance Requirements 85

8.4 TOE Security Functions Rationale 85

8.5 TOE Assurance Measures Rationale 85

8.6 Protection Profile Rationale 85

8.7 Rationale for Strength of Function 85

List of Figures

Figure 2-1: High level architecture of the VMware ESX Server with VirtualCenter 7

Figure 2-2: ESX Server Architecture... 8

Figure 2-3: VirtualCenter Architecture.. 13

Figure 4: human users of the TOE.. 15

List of Tables

Table 3-1: TOE Assumptions, Treats, and Organizational Security policies........................ 29

Table 4-1 :Objectives for the TOE and the TOE Environment 31

Table 4-2: TOE Threats Tracing.. 33

Table 5-1: IT Security Requirements.. 37

Table 5-2: Auditable events of the ESX Server... 38

Table 5-3: Auditable Events on the VirtualCenter 47

Table 5-4 : Tracing SFR for the TOE and IT Environment to Objectives for the TOE & IT Environment... 58

Table 5-5: Security Functional Requirements Dependencies... 63

Table 6-1: TOE Security Functions 64

Table 6-2: TOE Assurance Measures 78

Table 6-3: Mapping of TOE SFRs to TOE Security Functions... 80

Table 6-4 Rationale for Assurance Measures Satisfying SARs... 83

1. ST Introduction

1.1 ST Identification

TOE Identification:	VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0
ST Identification:	VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Security Target
ST Version Publication Date:	March 10, 2006
ST version number:	Version 1.6.7
Author(s):	Elisabeth C. Sullivan

1.2 CC Conformance

- The TOE is Common Criteria Version 2.2 (ISO/IEC 15408) Part 2 extended.
- The TOE is Common Criteria Version 2.2 (ISO/IEC 15408) Part 3 conformant.
- The TOE is conformant with Assurance Package EAL2.
- The TOE is compliant with all International interpretations with effective dates on or before 12/28/2004, if any.
- This TOE is not conformant to any Protection Profiles (PPs).

1.3 TOE Overview

VMware ESX Server and VirtualCenter are products for building a virtual infrastructure on top of multiple network-connected physical hosts. Each host provides a virtual machine platform that transforms the physical hardware into a pool of virtual computing resources. The ESX software provides a set of virtual hardware including processors, memory, disks, and network cards, to each Virtual Machine on the host. By design, guest operating systems are isolated within the Virtual Machines. Users of a Virtual Machine can only communicate with users of another Virtual Machine via networking or other mechanisms that might be used to connect separate physical machines. The allocation of resources on ESX Server is dynamic. The VirtualCenter software provides the ability to deploy, monitor and manage multiple ESX server hosts as well as all guest Virtual Machines associated with the hosts.

1.4 ST Organization

This Security Target (ST) defines the security environment, security requirements, and security functions of the VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0.

- Security Target Introduction (Section 1) – Provides identification of the TOE and ST, conformance claims, an overview of the TOE, this overview of the content of the ST, document conventions, and relevant terminology.
- TOE Description (Section 2) – Provides a description of the TOE, its architecture, hardware, software, firmware, security features, as well as the physical and logical boundaries for the TOE. This section clarifies what is in the TOE, in the operating environment of the TOE, and what is excluded from the TOE.
- TOE Security Environment (Section 3) – Describes the threats, organizational security policies, and assumptions pertaining to the TOE and the TOE environment.
- TOE Security Objectives (Section 4) – Identifies the security objectives for the TOE and its supporting environment and provides a rationale that objectives are sufficient to counter the threats identified for the TOE.
- Functional and Assurance Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) met by the TOE, the Strength of Function claims for the requirements, and the security functional requirements rationale. In addition this section presents Security Assurance Requirements (SARs) met by the TOE and the assurance requirements rationale.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE that satisfy the security functional requirements, provides the rationale for the security functions. It also describes the security assurance measures for the TOE as well as the rationales for the assurance measures.
- Protection Profile Claims (Section 7) – Presents the rationale concerning compliance of the ST with Protection Profile (PP) conformance.
- Rationale (Section 8) – Provides pointers to all rationale sections, to include the rationale for the selection of IT security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

1.5 Document Conventions

1.5.1 Convention for Operations

The CC defines four operations on security functional requirements. The conventions below are used in this ST to identify the operations performed.

Assignment	Made within the ST:	[**bold text in square brackets**]
Selection	Made within the ST:	[underlined text in square brackets]
Refinement	Made within the ST:	[***bold italicized text in square brackets***]
Iteration	Made within the ST:	indicated with a typical CC requirement naming followed by a lower case letter enclosed in square brackets e.g. FAU_SEL.1.1[a].

1.5.2 Convention for Interpretations

There are no applicable CCIMB or NIAP interpretations to CC v2.2 in this document.

1.5.3 Convention for Explicit Requirements

This ST has explicitly stated requirements. These new requirements contain the text "_EXP" in the requirement name (e.g. IDS_SCP_EXP.1).

1.6 Terminology

1.6.1 CC Terms

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. A subset of those definitions is included in the list below. They are listed here to aid the reader of the Security Target.

Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.
Object	An entity within the TSC that contains or receives information and upon which subjects perform operations.
role	A predefined set of rules establishing the allowed interactions between a user and the TOE. Note that this is the traditional use of the term role, which is different from the usage of the term in the VMware documentation. The VMware special usage of the term role is called VC-role in this ST, and is defined below.
Subject	An entity within the TSC that causes operations to be performed.
Strength of Function (SOF).	A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.
SOF-basic	A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.
Security attribute	Information associated with subjects, users, and/or objects that is used for the enforcement of the TSP.
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed protected and distributed within a TOE.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
TSF Scope of Control	The set of interactions that can occur with or within a TOE and

(TSC)	are subject to the rules of the TSP

1.6.2 ST Specific Terms

These terms are specific to this ST, or are refinements of CC terminology to clarify specific meanings of the term in this ST.

ESX, ESX Server	In this document, ESX Server 2.5.0
Farm	A set of hosts and their associated Virtual Machines that are managed by the VirtualCenter Management Server, which can support multiple Farms. A host can be managed by only one Farm at a time.
Farm Groups	An optional grouping structure that is hierarchically contained within the Server Farm structure. The VirtualCenter Management Server supports multiple Farm Groups, and Farm Groups can contain other Farm Groups and Farms.
Guest Operating System	A guest operating system runs within a Virtual Machine.
Host	The hardware that supports an ESX Server installation
Management Interface, Management User interface (MUI)	Equivalent names for the web based interface to the ESX Server
VMware term “role”, called VC-role in this ST.	One of four hierarchical permission levels defined in the VirtualCenter. A permission pair, which consists of a userID and VC-role, can be assigned to a VirtualCenter object. This is used in determining access control to VirtualCenter objects. The VC-roles define what activities the user id is allowed to perform on the VirtualCenter object.
Server Farms	The top level structure for the VirtualCenter Management Server. Only one Server Farm exists for each VirtualCenter Management Server. Server Farms can contain multiple Farm Groups and Farms
VirtualCenter	In this document, VirtualCenter 1.2.0
Virtual Machine Groups	An optional grouping structure contained within a Farm. The VMs in a VM Group can span multiple host machines. They can contain Virtual Machines and other virtual

	machine groups.
Virtual Machine (VM)	A virtual machine is a virtualized x86 personal computer environment in which a guest operating system and associated application software can run. Multiple Virtual Machines can operate on the same host concurrently.

The following table presents frequently used acronyms used in this ST. Some are defined in the previous tables. Others are commonly used acronyms in IT technology, and are provided for the convenience of the reader.

CC	Common Criteria
ESX	No known expansion
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IT	Information Technology
NTP	Network Time Protocol
PP	Protection Profile
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SMP	Symmetric Multiprocessing
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TOE	Target Of Evaluation

2. TOE Description

2.1 Overview

The TOE consists of the VMware ESX Server 2.5.0 (ESX, ESX Server) and VMware VirtualCenter 1.2.0 (VirtualCenter), which provide an operating system product. VMware ESX Server provides virtual infrastructure software for partitioning, consolidating and managing systems. VMware VirtualCenter is a system management application that deploys, monitors, and manages Virtual Machines that are distributed across multiple hosts running ESX Server software. VirtualCenter Clients can attach to a VirtualCenter server through any personal computer running a Microsoft Windows operating system and the VirtualCenter Client software. The VirtualCenter Clients can monitor and manage Virtual Machines registered to the VirtualCenter, as well as their associated ESX Servers, or hosts, and host resources.

ESX Servers provide a highly scalable virtual machine platform with advanced resource management capabilities. These ESX Servers can also be managed by VirtualCenter.

ESX Server transforms physical systems into a pool of logical computing resources. Operating systems and applications are isolated in Virtual Machines that reside on a single piece of hardware. System resources are dynamically allocated to any operating system based on need, providing mainframe-class capacity utilization, and control of server resources.

ESX Server simplifies server infrastructure by partitioning and isolating server resources, such as CPU usage, memory, and hardware devices, in secure and portable[1] Virtual Machines. ESX Server enables these server resources to be remotely managed, automatically provisioned, and standardized on a uniform platform. Advanced resource management controls allow IT administrators to guarantee service levels across the enterprise. ESX Server runs directly on the system hardware to provide a secure, uniform platform for deploying, managing, and remotely controlling multiple Virtual Machines.

ESX Server with the optional Virtual Symmetric Multi Processing (VSMP, Virtual SMP) package that allows creation of dual virtual CPU SMP Virtual Machines. With VMware Virtual SMP, two processors can share the workload of resource-intensive applications and tasks running in a guest operating system. VMware Virtual SMP is licensed separately from ESX. The functionality is built into the base product and requires the proper license key to activate it.

VirtualCenter provides the central point of control for workload management, provisioning, and availability. The VirtualCenter Management Server collects and stores persistent data in a dedicated database that contains per-system and environmental information. Each ESX Server under the control of a VirtualCenter communicates with the VirtualCenter through a VirtualCenter Agent installed on the ESX Server. The VirtualCenter Management Server

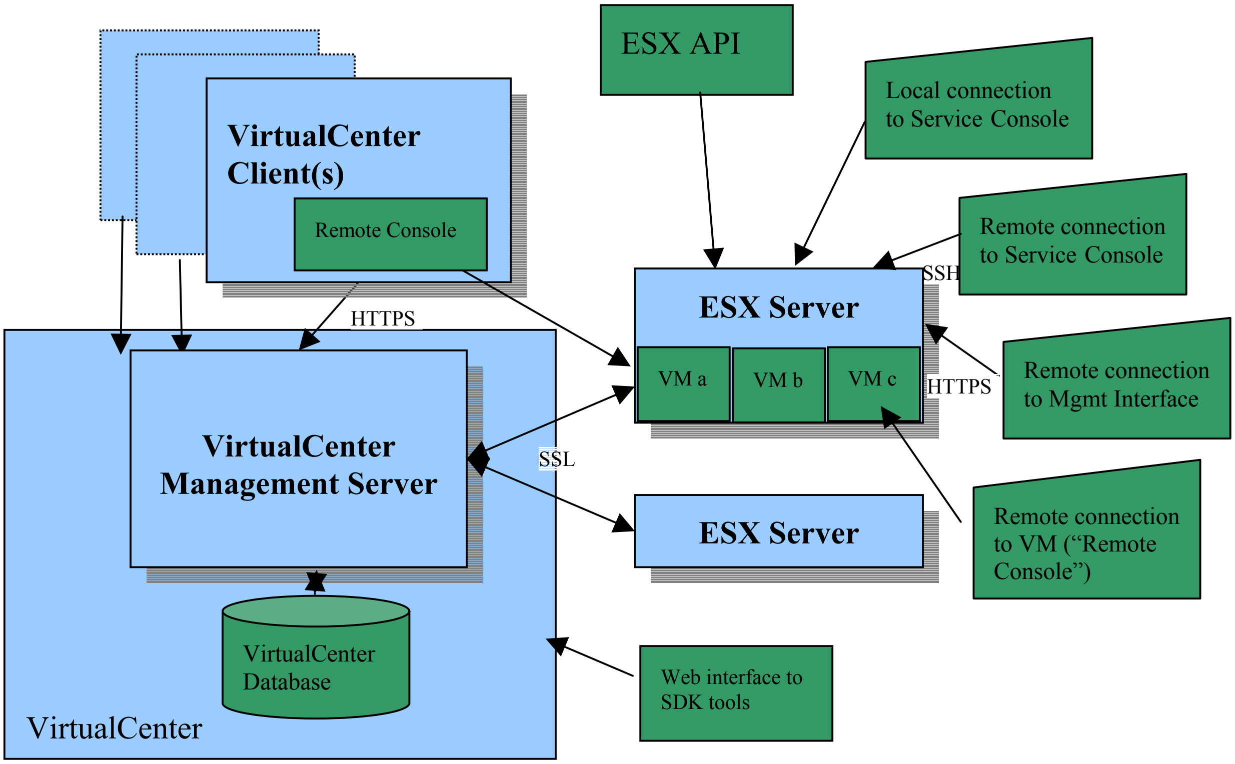
[1] Virtual Machines can be imported or exported. As such, VMs can be moved from one ESX Server installation to another.

automatically executes user-specified scheduled tasks, such as powering on, or moving powered-off Virtual Machines.

VirtualCenter with the optional VMotion package enabled supports moving a virtual machine from one host to another, while the virtual machine continues operation. Migration with VMotion occurs without service interruption on the virtual machine. VirtualCenter provides a visible interface for monitoring system availability and performance of the Virtual Machines in the VirtualCenter configuration. VirtualCenter runs as a service on Windows 2000, Windows XP Professional, and Windows 2003. As with Virtual SMP, VMotion is licensed separately from ESX. The functionality is built into the base product and requires the proper license key to activate it.

2.2 Architecture

Figure 2-1 below provides a high level overview of the physical architecture of the VMware ESX Server with VirtualCenter. No effort is made to distinguish hardware and software components in this diagram. However, elements shown in blue (the VirtualCenter client(s), the VirtualCenter Management Server, and the ESX Server) have elements of the TOE. The items shown in green are outside the scope of the TOE or are parts of the TOE environment. Specific elements of the TOE and the TOE Environment are list in a later section of this chapter. The architecture of the individual software elements is described in section 2.2.1 and 2.2.2.



ESX API
Local connection to Service Console
VirtualCenter Client(s)
Remote Console
Remote connection to Service Console
SSH
ESX Server
HTTPS
VM a
VM b
VM c
HTTPS
Remote connection to Mgmt Interface
VirtualCenter Management Server
SSL
ESX Server
Remote connection to VM ("Remote Console")
VirtualCenter Database
VirtualCenter
Web interface to SDK tools

Figure 2-1: High level architecture of the VMware ESX Server with VirtualCenter

2.2.1 ESX Server Architecture

The ESX Server architecture provides an operating environment dedicated to hosting multiple Virtual Machines. ESX Server's virtualization layer runs directly on the system hardware.[2]. The essential elements of the system's design are:

- The Service Console, which provides a command line interface to the ESX server and performs many standard operating system activities, and to VMware-written commands that can be used for specific ESX server management tasks.
- The VMware ESX server management application, (not shown in figure 2.2) which performs actions in the service console on behalf of ESX Server users from the management interface.
- The VMware virtualization layer, which provides the idealized hardware environment and virtualization of underlying physical resources. It enables the partitioning and guaranteed delivery of CPU memory, network bandwidth, and disk bandwidth to each virtual machine.
- The hardware interface components, including device drivers, which enable hardware-specific service delivery.

Figure 2-2 below illustrates an ESX Server implementation with four Virtual Machines.

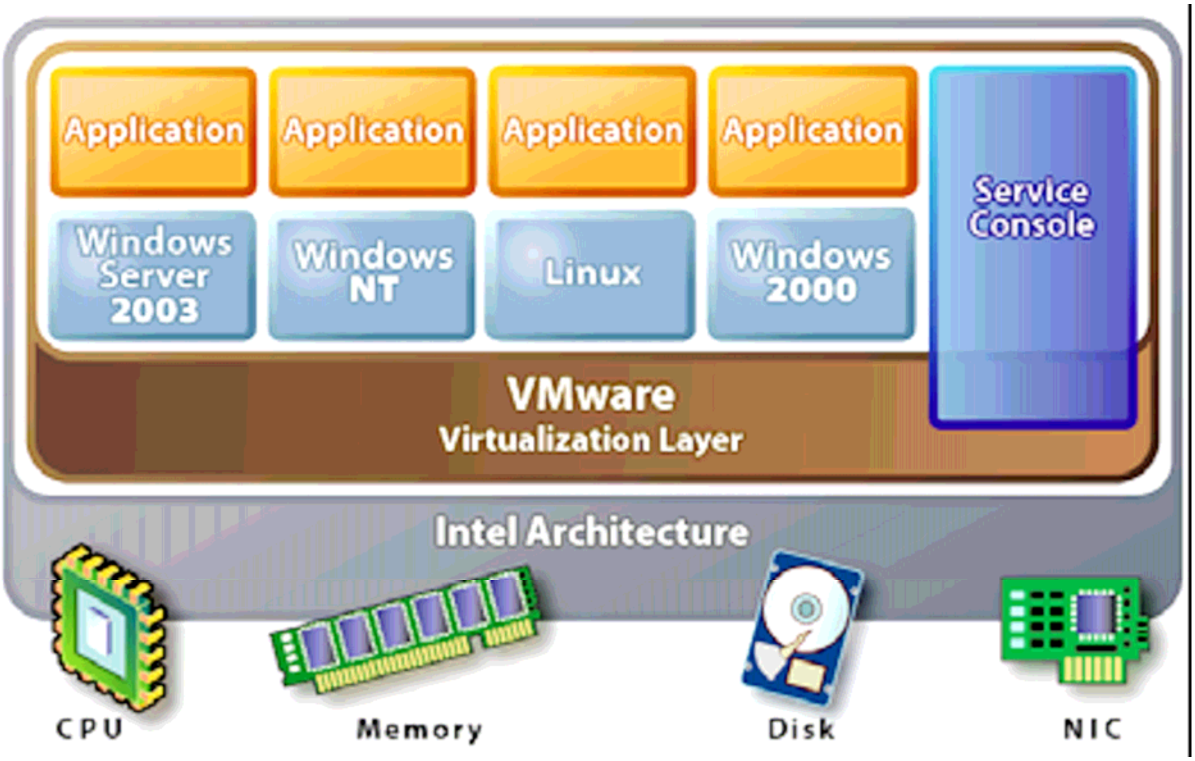


Figure 2-2: ESX Server Architecture

[2] This is different from VMware's GSX and Workstation products where the virtualization layer resides on top of a host operating system.

The Management Interface is a web-based software feature that allows administrators of the ESX Server to perform management functions through a protected HTTPS connection from the Internet. Management users can also access the ESX Server through the Service Console[3], a software feature which provides a command line interface that can be used to perform many of the same functions provided by the VMware management interface. The Service Console can be used directly via an attached keyboard, mouse, and monitor, or from a remote workstation, using SSH. Requests for services are processed by the ESX Server daemon.

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 the VirtualCenter Agents are handled by the ESX server daemon in a manner similar to requests from users at the CLI or Management Interface.

The ESX Server provides a “full service” Remote Console, consisting of a remote terminal running the VMware ESX Remote Console software to access a specific Virtual Machine. These users access their VMs directly by URL or IP address. From the Remote Console to a particular VM, VM users can access their files and applications on the VM and the administrator of the VM and can perform certain administrative functions in the guest OS operating environment of the VM being accessed.[4] No claims are made about the Remote Console in this evaluation, but the Remote Console is included here for completeness.

The API is a programmatic interface that allows the use of scripts to perform operations on VMs. It is not a part of the TOE and its use is not allowed in the TOE.

2.2.1.1 Virtualization

ESX Server provides *virtualization* in the following ways:

- CPU virtualization: Each virtual machine appears to run on its own CPU, or set of CPUs, fully isolated from other Virtual Machines, with its own registers, translation lookaside buffer, and other control structures.
- Memory Virtualization: While a contiguous memory space is visible to each virtual machine, the physical memory allocated may not be contiguous. Instead, noncontiguous physical pages are remapped efficiently and presented to each virtual machine.
- Disk virtualization: Support of disk devices in ESX Server is an example of hardware independence. Each virtual disk is presented as a SCSI drive connected to a SCSI adapter. This device is the only disk storage controller used by the guest operating system, despite the wide variety of SCSI, RAID, and Fibre Channel adapters that might actually be used in the system.

[3] also called the Console OS or COS in the product documentation

[4] Actions VM users and VM administrators that take place on the VMs are outside the scope of the evaluation. No security claims are made on these actions. See section 2.6.

- Network Virtualization: It is possible to define up to four network cards within each virtual machine. Each virtual network has its own IP address(es). ESX Server manages both the allocation of resources and secure isolation of traffic meant for different Virtual Machines even when they are connected to the same physical network card.

2.2.1.2 ESX Server Software Components

The ESX Server software consists of the following components:

ESX Server application	The ESX Server management application consists of • The ESX Server Daemon, *ccagent*, which performs actions in the service console of a VirtualCenter-managed ESX Server, on behalf of the web based VMware Management Interface and on behalf of requests from the VirtualCenter. • The ESX Server Management Interface, a web-based interface to the ESX Server. The ESX Server has an embedded copy of Apache 1.3.31, an httpd daemon which communicates with OpenSSL via the mod-ssl module. This module provides strong cryptography for the Apache 1.3.31 web server via SSL and TLS protocols, and was developed using OpenSSL.
VMkernel	The VMkernel manages the hardware resources of the ESX Server host and provides their services to the guest Virtual Machines.
VMware Service Console	• The VMware Service Console is a operating system that has been modified for ESX Server. It includes the software that manages the ESX Server groups, user databases, as well as a few ESX server specific management commands. It contains the logging function that collects and manages the audit data as well as the identification and authentication mechanisms used for remote users of the management interface, users of the Service console, and users from the managing VirtualCenter. Identification and authentication use the local username/password database. • The VMware Service console provides a Command Line Interface (CLI) that facilitates administration services.

Virtual SMP	Virtual Symmetric Multi Processing (SMP, VSMP) is a separately licensed module of the ESX Server. It is delivered with the product and can be activated during ESX Server installation, or at any time after installation, once a special license is purchased. With VirtualSMP, a Virtual Machine can be created as dual-virtual CPU SMP Virtual Machines.
Remote Console Software and VMtools	The Remote Console is a software package installed on a remote workstation. Using the Remote Console, a VM administrator can attach directly to an individual virtual machine via a window directly into that VM. From this console, the administrator can start and stop programs running on a virtual machine, install or change the configuration of the guest operating system operating in the virtual machine, and do other tasks as if the virtual machine were a physical computer. The VMware tools are used on a guest operating system to support management from the Remote Console. Note that there are no security claims made in this ST regarding the Remote Console or the VMware Tools.

2.2.1.3 ESX Server Configurations

ESX server can be installed in three distinct configurations.

- Configuration 1: Local Storage Only: In the first configuration, the ESX Server application is installed on a server and uses local disk for storage for VM images, VM data, and ESX data. This configuration can be installed on simple servers or on blade servers, as described below in section 2.3.2.
- Configuration 2: ESX Local/VMs on SAN: In the second configuration, the ESX Server application is installed on a server and uses local storage for ESX data. Virtual Machines are installed on a Storage Area Network (SAN). The ESX Server can be installed on simple servers or on blade servers.
- 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.

In all configurations, the separation of Virtual Machine data and images is performed and managed by the ESX Server's VMKernel.

2.2.2 VirtualCenter Architecture

The VirtualCenter architecture is designed to allow remote administration of a collection of ESX Server hosts. VirtualCenter relies on a management server and a database containing information about the configuration and status of one or more ESX Server hosts and each of the host's Virtual Machines.

The VirtualCenter may optionally be installed in a network with a domain server.

Users connect to the VirtualCenter using the VirtualCenter Client. This can be done either locally (on the same machine as the VirtualCenter) or remotely, from a workstation running the VirtualCenter Client software. The VirtualCenter Client can also spawn a limited version of the Remote Console to access a Virtual Machine on a managed ESX Server host. Note there are no security claims made in this ST about either the ESX Remote Console or the VirtualCenter limited Remote Console.

VirtualCenter Clients connect to the VirtualCenter Management Server in order to manage inventory objects (see below) as well as to maintain and administer an ESX Server host and its Virtual Machines. A VirtualCenter Agent resides in each ESX Server to perform actions on behalf of VirtualCenter and provide status of the ESX Server host and the state of its Virtual Machines. Note that an ESX Server can only be managed by one VirtualCenter, and as such, there is only one VirtualCenter Agent on a managed host running ESX Server.

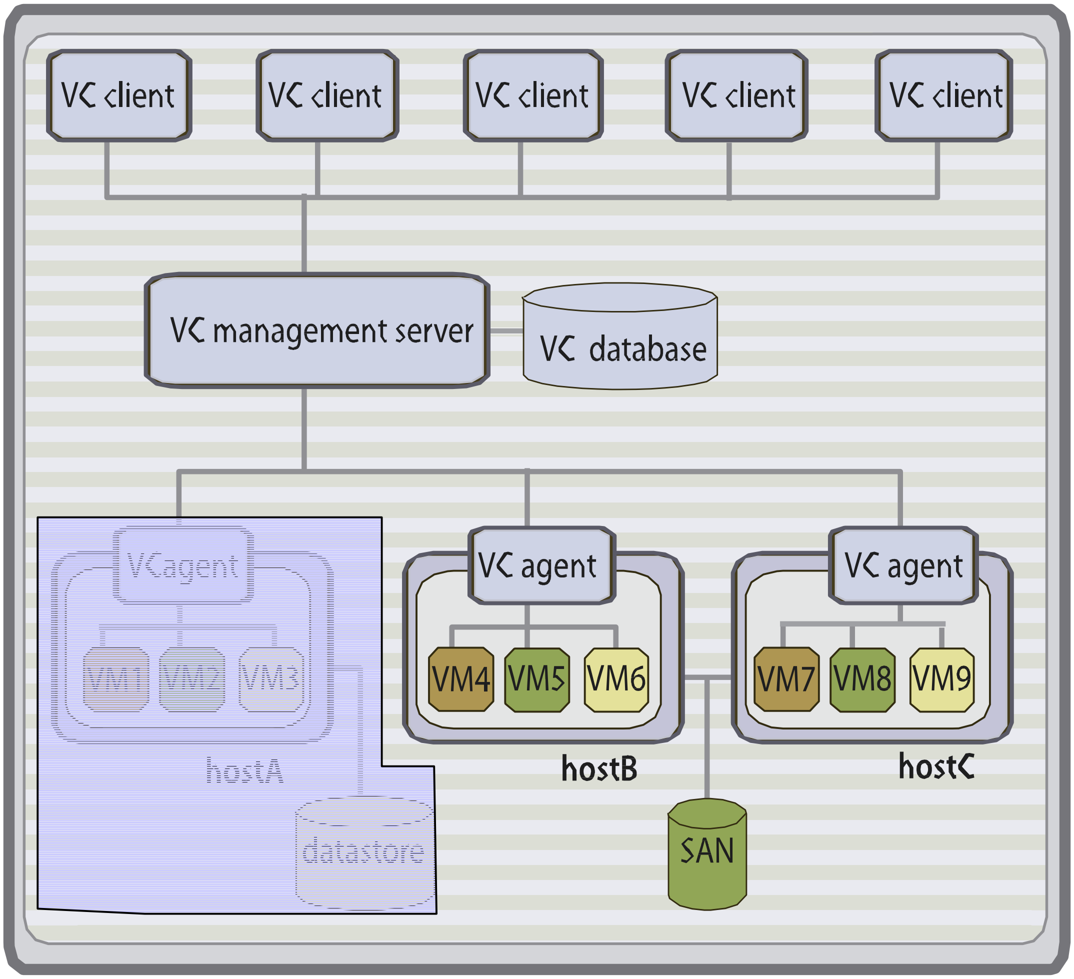


Figure 2-3: VirtualCenter Architecture[5]

Note that in the evaluated configuration of the TOE, the VirtualCenter Management Server and the VirtualCenter Database are required to be collocated on the same hardware.

2.2.2.1 VirtualCenter Inventory Objects

The VirtualCenter manages the following organizational objects, also called inventory objects. The data relevant to the VMs is stored on the ESX Server, and communicated to the VirtualCenter via the VirtualCenter Agents on each ESX Server. Data about all other inventory objects is stored on the VirtualCenter Database.

- Server Farm: This is the full set of VMs registered to the VirtualCenter. It contains all the farms, farm groups, ESX Server hosts, and their respective Virtual Machines.
- Farms: A Farm is the main logical grouping of ESX Server hosts and their Virtual Machines.
- Farm Groups: an optional structure contained within a Server Farm. A Farm Group may contain Farms and/or other Farm Groups.
- Virtual Machine Groups: this is another optional grouping structure, which allows grouping Virtual Machines within a Farm. The VMs in the VM Group must be in the same Farm but do not have to be on the same host.
- Virtual Machines: the lowest atomic element of the organizational objects of the TOE.

The functional components are the monitoring and managing tasks, also stored on the VirtualCenter Database. They are:

- inventory : A view of all monitored objects in an organizational structure,
- scheduled tasks: a list of activities and a means to schedule them
- Templates: a means to import Virtual Machines and store them as templates for deploying at a later time
- 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.

2.2.2.2 VirtualCenter Software components

The VirtualCenter software has the following components:

VirtualCenter Agent	The VirtualCenter Agent collects, communicates, and executes actions on the ESX Server that hosts it, and on behalf of the VirtualCenter Management Server. In addition, it monitors the status of the ESX Server host and its Virtual Machines, returning the status information on the host and the VMs.

[5] Note that hostA, hostB, and hostC in the diagram are ESX Server hosts. Additionally, in this diagram, the datastore in hostA is conceptual in nature, and is not intended to represent a physically separate storage capability.

VirtualCenter Client	The VirtualCenter Client provides a user interface to the VirtualCenter Management Server. It may be installed on the same machine as the VirtualCenter Management Server, or it may be installed on multiple remote workstations.
VirtualCenter Management Server	The VirtualCenter Management Server is a service that acts as a central administrator for VMware ESX Server hosts. Actions from a VirtualCenter Client intended for ESX Server hosts are received by the VirtualCenter Management Server and sent to the appropriate VirtualCenter Agent on the ESX Server. The management server uses
VMotion	VMotion is a separately licensed software module that is delivered with the product and can be activated only if a special license is purchased. VirtualCenter with VMotion moves a virtual machine from one managed ESX Server to another, while the virtual machine continues operation. It is only applicable to ESX Servers having VMs stored on a SAN (configurations 2 and 3). This form of migration with VMotion occurs without service interruption on the virtual machine. A VMotion license must be applied to each ESX Server that is involved in the migration.

2.3 The TOE and its Operating Environment

The following subsections describe users, physical external interfaces, hardware, software, and other requirements for the TOE and its operating environment. The TOE itself is a complex collection of products and services, and not all of the architectural parts of the two products described in the previous section are included within the scope of the Target of Evaluation. Some hardware and software components that are required for the TOE Environment are not a part of the evaluated configuration. This section attempts to clarify what is in the TOE, what is in the TOE Environment, special configuration restrictions, and items that are expressly excluded from the TOE. Section 2.4 provides a summary table which identifies TOE components and TOE Environment components.

2.3.1 Physical External Interfaces and Users

There are external interfaces to ESX Server and VirtualCenter. The potential users of the VMware products and the specific users of the TOE and the evaluated configuration are summarized in this section.

The following figure shows the ways a user may access the TOE and which types of users can access which physical interfaces. Details are contained in subsequent sections.

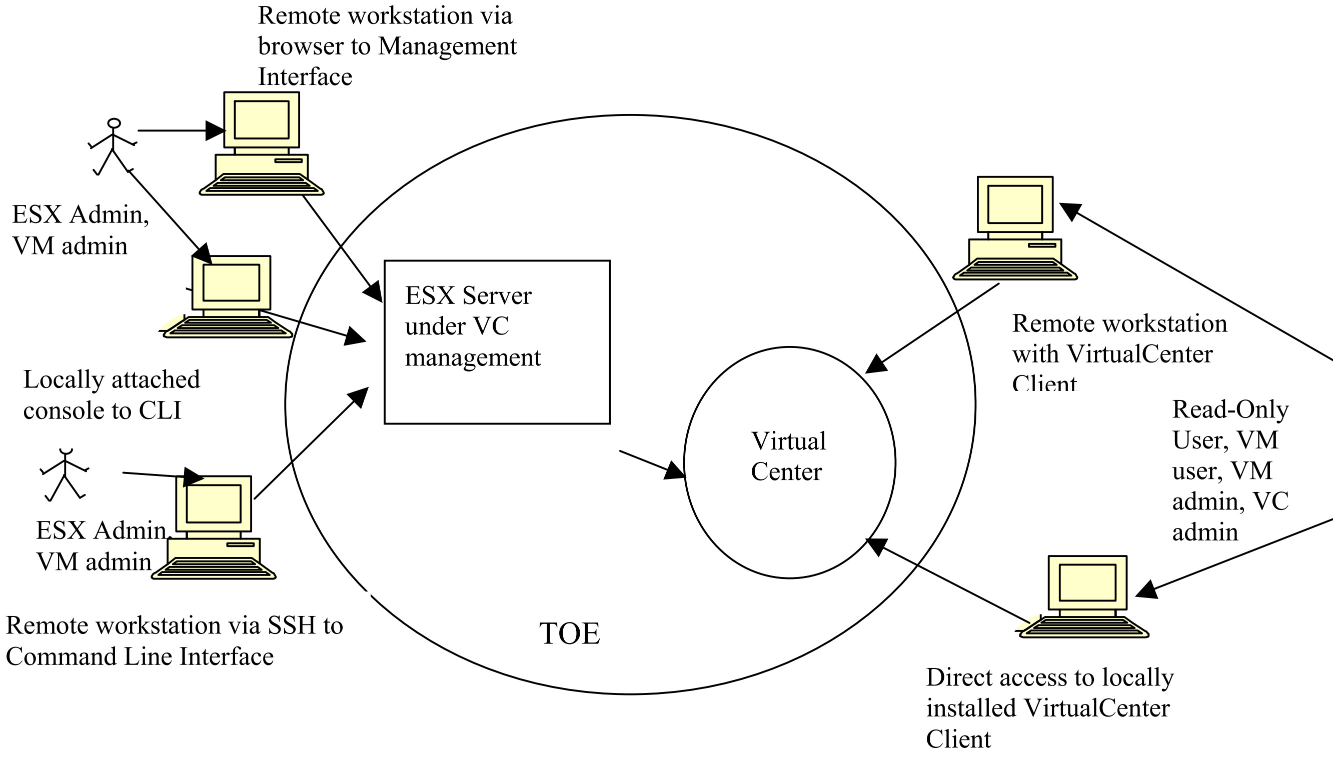

Remote workstation via browser to Management Interface
ESX Admin, VM admin
Locally attached console to CLI
ESX Admin, VM admin
Remote workstation via SSH to Command Line Interface
ESX Server under VC management
Virtual Center
TOE
Remote workstation with VirtualCenter Client
Read-Only User, VM user, VM admin, VC admin
Direct access to locally installed VirtualCenter Client

Figure 4: human users of the TOE

2.3.1.1 ESX Server Physical Interfaces, Users, and Roles

There are 5 distinct ways to access the ESX Server.

- Management Interface
- Command Line Interface (CLI) to the Service Console (locally and remotely)
- From the VC Via the VirtualCenter Agent
- Remote Console directly to a Virtual Machine
- Application Program Interface

ESX server users are individuals who connect to a physical host in a system of ESX Servers, and authorized requests for services on an ESX Server from a VirtualCenter user. There are several types of ESX Server users, not all of whom are considered users of the TOE.

The following potential ESX users are not users of the TOE:

VM Users: Each Virtual Machine can have users who are individuals using a Virtual Machine's (VM) 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 IP address associated with the specific virtual machine. From the user point of view, it is just like accessing a single server machine directly. They operate in a non-privileged state (e.g. they do not have access to the root account of the ESX Server or of the Virtual Machine). These users have no access to the TOE data and functions that are defined for the TOE. They only work within the confines of the VM to which they have access. The VMs themselves, their operating systems, applications, and users are outside the scope of the TOE. Thus the VM users are not users or administrators of the TOE.

Scripting API users: The scripting API feature requires additional software and is not included in the TOE, and hence its users are not TOE users. Use of the Scripting API is forbidden by administrative measures for the Evaluated Configuration of the TOE.

The following are users of the TOE from the ESX Server connections:

ESX Administrators also called system administrators, root users, and superusers: ESX administrators are individuals charged with the responsibility to perform management and configuration functions for the ESX Server. These administrators can access the ESX Server from the Management interface and the interface(s) to the CLI of the Service Console, as well as from the VirtualCenter via the VirtualCenter Agent.

VM administrators: These are administrators of specific Virtual Machines on an ESX server. They also can access the ESX Server from the Management Interface and the interface(s) to the CLI of the Service Console, as well as from the VirtualCenter via the VirtualCenter Agent. VM administrators are individuals charged with the responsibility to perform management and configuration functions for a specific VM supported by ESX server. They may perform administrative actions on their VM's operating system and applications. Such actions are outside the scope of the TOE. However, when the VM administrators manage the virtual machine configuration from the ESX Server, they are administrative users of the TOE. These tasks include performing setting the maximum and minimum memory required, number of CPUs (in a multi-CPU ESX Server), and the like. These administrators have a privileged status on the Virtual Machine they administer, (e.g. they may be the root user of the underlying OS of the VM they administer), but they do not have privilege on the ESX Server (access to the root account of the ESX Server).

There are no non-administrative users of the TOE via the ESX Server. All ESX Server users of the TOE are administrative users. This grouping of users into ESX administrators and VM administrators creates two distinct traditional roles on the ESX server.

2.3.1.2 VirtualCenter Users, Roles, and VirtualCenter Roles (VC-Roles)

Any user of the underlying operating system of the VirtualCenter is a VirtualCenter user. The operating system creates and manages all user accounts. For the VirtualCenter, these users fall into two fundamental types—those who have VirtualCenter Administrator privileges to all VirtualCenter objects, and those who don't. This creates a pair of traditional roles for the VirtualCenter, which are called VirtualCenter Administrators and Limited Access Users. VirtualCenter OS System administrators, who are members of the Windows operating system's administrator group, and automatically have all access to all VirtualCenter objects, are de facto members of the VirtualCenter Administrator role. All other users fall into the Limited Access User role.

VirtualCenter users are granted access to VirtualCenter objects based on their identity and access permissions groupings that are called Roles in the VMware documentation. They will be referred to as VC-Roles in this ST, a distinction that will only be made in this ST and internal documentation to avoid confusion. These permissions are assigned to VirtualCenter objects using access control lists called permission pairs. A permission pair is a userID or Group ID and a VC-role.

The VC-roles are described below

> *Read Only User access rights (*also called "read only User" in the documentation*):* A user with Read Only User access rights to a VirtualCenter object can view the object in the inventory panel and the related detail screens. This may apply to VMs, Farms, Farm Groups, Server Farms, or VM Groups as well as event files and alarms related to the inventory objects. All actions through menus and toolbars are disabled. A Read Only User can view templates, scheduled tasks associated with the inventory object but cannot perform any actions with them.
>
> *Virtual Machine User access rights (*also called *"Virtual Machine User*" in the documentation*)* : A user with Virtual Machine User access rights for a VirtualCenter object can do anything for that object that Read Only User access rights allow, as well as power operations (power on, power off) for Virtual Machines to which they have Virtual Machine User access. These access rights grant very limited capabilities. Users with this VC-role for a VM can connect to an individual VM with a Remote Console, which is a limited version of the ESX Server Remote console. This Remote Console allows the qualified user to create a connection directly to a Virtual Machine on an ESX Server (host) managed by the VirtualCenter. From this remote console, the qualified user can view the states of Virtual Machines but cannot modify VirtualCenter configuration of hosts or Virtual Machines.
>
> *Virtual Machine Administrators access rights,* also called *Virtual Machine Administrator* in the documentation*)*: A user with Virtual Machine Administrator access rights to a VirtualCenter object can to do anything for that object that Virtual Machine User access rights allow as well as add, remove, or modify the VirtualCenter object. Users with this VC-role for the appropriate object can connect or disconnect host devices, migrate, clone, remove, and configure Virtual Machines. They can create, import, and deploy templates. Such users can add and remove hosts from a Farm and create, remove, or modify Farms, Farm Groups, and virtual machine groups and their content. Note that virtual machine administrators from the VirtualCenter are not necessarily Virtual Machine Administrators on a specified ESX Server host.
>
> *VirtualCenter Administrator access rights*, (also called *VirtualCenter Administrator* in the documentation*)* : A user with VirtualCenter Administrator access rights to a VirtualCenter object allows the user to do anything for that object which are the same as the VC Administrator privileges as well as to change privilege pairs for the object.

When a Limited Access User is assigned a privilege pair to the VirtualCenter's Server Farm that has VirtualCenter Administrator access rights, the user acquires privileges on the VirtualCenter objects which are the same as the privileges on the VirtualCenter of the VirtualCenter Administrator. This access also gives the user the capability to add and change VirtualCenter licenses as well as to change and add permission pairs on objects. Note that this does not grant the Limited Access User rights on the underlying OS, such as the ability to create users. In other words, the VirtualCenter Administrator has all the privileges of the Limited Access User with VirtualCenter administrator access rights to the VirtualCenter Server farm, but not vice-versa.

A Limited Access User who has no permission pairs on VirtualCenter objects that include a user's ID or a group to which the user has no access at all to VirtualCenter objects, but remains a VirtualCenter user.

Web service users: An optional web service can be installed with the VirtualCenter server. It is a programmatic interface that allows customer-written or third –party applications to access services provided by VirtualCenter. As this interface is not included in the TOE, its users are not TOE users. This is not a user interface for configuring VirtualCenter, and is not a part of the TOE, nor is the VMware SDK package, which is used write programs that use the VirtualCenter Web Service. Administrative documentation expressly forbids the use of the web interface in the TOE.

2.3.1.3 Services from the TOE Environment

The VirtualCenter relies on its environment to provide reliable time stamps, identification and authentication of its users, role distinction, and management of VirtualCenter users and groups. If the VirtualCenter is not joined to a Domain Server, these functions are provided by the underlying operating system of the VirtualCenter. The VirtualCenter can optionally be joined to a Domain Server, and in this case, the reliable time stamp functions are provided by the Domain Server in conjunction with the VirtualCenter, and some user account management functions may optionally be performed by Domain Server administrators.

2.3.2 Hardware and Software Requirements

The following hardware and software are required for this TOE

- Hardware platform(s) and software for the VMware ESX Server(s)
- Hardware platforms and software for the VMware remote workstations used to access the ESX Management User Interface and/or the ESX Service Console.
- Hardware platform and software for the VirtualCenter
- Hardware platform(s) and software for the VirtualCenter Client(s)

2.3.2.1 VMware ESX Server Hardware and Software Requirements

The hardware and software required for the VMware ESX Server is determined by the possible configurations of the ESX Server.

2.3.2.1.1 ESX Server Hardware

ESX Local configuration hardware requirements are as follows:

- At least two and up to sixteen processors: 700 MHz Intel Pentium III Xeon and above or AMD Opteron (32-bit mode) for ESX Server without Virtual SMP. Note that this can be a blade server, and supported blade server products are described below.

- At least two and up to sixteen processors: 900 MHz Intel Pentium III Xeon and above or AMD Opteron (32-bit mode) for ESX Server with Virtual SMP. Note that this can be a blade server, and supported blade server products are described below. Note that this can be a blade server, and supported blade server products are described below.
- Minimum 512MB RAM
- Two or more Ethernet adapters
- SCSI adapter, Fiber Channel adapter, or internal RAID controller

VMware ESX Server 2.5.0 supports the following adapters:

NETWORK ADAPTERS
Broadcom® NetXtreme 570x Gigabit controllers
Intel PRO/100 adapters
Intel PRO/1000 adapters
3Com® 9xx based adapters
SCSI ADAPTERS
Adaptec®, LSI Logic
NCR™/ Symbios™ SCSI adapters
HP® Smart Array
Dell® PercRAID (Adaptec RAID and LSI MegaRAID)
ServeRAID™ and Mylex® RAID devices
FIBRE CHANNEL ADAPTERS
Emulex™ adapters
QLogic™ adapters
SCSI CONTROLLERS
Adaptec® Ultra-160 and Ultra-320
LSI Logic Fusion-MPT and most NCR/Symbios™ SCSI controllers
HP® Smart Array
Dell® PercRAID (Adaptec RAID and LSI MegaRAID)
IBM® (Adaptec) ServeRAID and Mylex RAID controllers
SCSI DISK
Fibre Channel LUN or RAID LUN with unpartitioned space

The ESX Server can be installed on three different types of Blade Server. They and their specific hardware requirements are listed below.

- HP Blade Server
    - Blade server enclosure
    - BL20 p, BL20p G2, BL20p G3, and BL40 Blade Servers
    - GbE or GbE2 interconnect switch (GbE2 is required for Fibre Channel (FC) connectivity with BL20p G2 blade servers).
    - Dual Port Fibre Channel Mezzanine card (GbE2 is required for Fibre Channel (FC) connectivity with BL20p G2 blade servers).
    - Sufficient physical memory to prevent virtual machine swapping from being a significant performance issue.

- IBM Blade Server.
  - Blade server enclosure
  - IBM HS20 and HS40 Blade Servers
  - Two BladeCenter 4 port gigabit Ethernet Switch modules
  - BladeCenter Fibre Channel expansion card (one for each blade, if FC connectivity is required)
  - BladeCenter 2 port Fibre Channel switch Module (for FC Connectivity)
  - Sufficient physical memory to prevent virtual machine swapping from being a significant performance issue.
- Intel Blade Server.
  - Blade server enclosure
  - Intel SBX and SBXL52 Blade Servers
  - Two BladeCenter 4 port gigabit Ethernet Switch modules
  - BladeCenter Fibre Channel expansion card (one for each blade, if FC connectivity is required)
  - BladeCenter 2 port Fibre Channel switch Module (for FC Connectivity)
  - Sufficient physical memory to prevent virtual machine swapping from being a significant performance issue.

ESX Local / VMs on SAN configuration hardware requirements
Hardware requirements if using a SAN for VMs only are the same as the above, excluding the adapter options. The additional hardware described for the Boot From SAN configuration is also required for this configuration.

Boot From SAN configuration hardware requirements
The following list describes the complete set of hardware requirements for the Boot from SAN configuration.

- QLogic HBA Fibre Channel 23xx host bus adapter (HBA)
- One of the following storage systems:
  - IBM TotalStorage (formerly FAStT) disk storage systems
  - EMC Symmetrix storage systems
  - EMC CLARiiON storage systems
  - Dell/EMC Fibre Channel CX300, CX500, CX700 RAID array storage system
  - HP StorageWork modules, smart array storage array systems

- SAN Firmware —Refer to the *VMware ESX Server SAN Compatibility Guide* for current information.

2.3.2.1.2 ESX Server Software Requirements include the following:

The TOE requires the following software components for the ESX Server installations:

- ESX Server software package as described in section 2.2.1.2 above.
- OpenSSH 3.5p1-11 server on ESX Server.
- OpenSSL 0.9.7d server on ESX Server
- VirtualCenter Agent (Installed by VirtualCenter when the ESX server is placed under VirtualCenter management).
- NTP Client

2.3.2.2 VMware ESX 2.5.0 Remote Workstations

Hardware platforms for the remote workstations used to access the ESX Management Interface must meet the following requirements:

- Standard x86 based computer
- 266MHz or faster processor
- 64MB RAM minimum
- 10 MB free disk space required for basic installation

The remote management workstation used to attach to the Management Interface must be OpenSSL compatible. The following windows operating systems are supported:

- Windows XP Professional
- Windows 2000 Professional, Server or Advanced Server
- Windows 2003 Enterprise, Standard , Web Editions, and Small Business
- Windows NT 4.0 Workstation or Server, Service Pack 6a

If a windows operating system is used, any of the following browsers can be used.

- Internet Explorer 6.0 or higher
- Netscape Navigator® 7.0
- Mozilla 1.x

The TOE also supports a Linux remote workstation for connecting to the Management interface with the following conditions:

- The remote workstation is compatible with standard Linux distributions with glibc version 2 or higher,
- The workstation has one of the following Browsers:
  - Netscape Navigator 7.0
  - Mozilla 1.x

The TOE also supports a remote connection to the Service Console CLI. This connection can be made from any computer that meets the following requirements.

- SSH client compatible with ESX Server's OpenSSH server
- Capable of communication with Linux based Command Line Interface on ESX Server.

2.3.2.3 Domain server Hardware and Software Requirements

Optionally, the TOE environment may use a domain server. The hardware and software requirements for this domain server include the following

- Windows operating system Windows 2000 Server, Windows 2000 Advanced Server, Windows XP Professional, or Windows Server 2003 (Web, Standard, or Enterprise), or any later release.
- Hardware that can support the operating system above.

2.3.2.4 VMware VirtualCenter 1.2.0

VMware VirtualCenter 1.2.0 has the following hardware requirements:

- A minimum of 2GB RAM for VirtualCenter configurations managing 50 managed hosts or fewer. For greater than 50 managed hosts configurations, use 3GB RAM. For configurations with 100 managed hosts running 2000 Virtual Machines, use 4GB RAM.
- As a minimum a Pentium IV 2.0Ghz processor, or other x86 compatible architectures. Dual processors are recommended for deployments with more than 25 managed hosts.
- A minimum of 1 10/100Mbps NIC (1Gbps NIC recommended).

The software required for the VirtualCenter includes the following:

- The operating system for VirtualCenter can be any of the following, and must meet the requirements listed
    - Windows 2000 Server, Windows 2000 Advanced Server, Windows XP Professional, or Windows Server 2003 (Web, Standard, or Enterprise).
    - Windows Script 5.6 or later. If not available on the host machine, it is automatically installed when VirtualCenter is installed.
    - The VirtualCenter server must have administrator privileges on the installing system to install VirtualCenter Management Server
    - Sufficient disk space on the machine to support the VirtualCenter Database and the template upload directory.
- OpenSSL 0.9.7d Server on VirtualCenter
- Database: Microsoft SQL Server 2000, Microsoft SQL server 7 or Oracle 8i installed on the same physical hardware as the VirtualCenter. Microsoft ACCESS database is also supported, and if used, is installed automatically on the same physical hardware as the VirtualCenter.
- VirtualCenter Management Server software and optional VMotion software as described in section 2.2.2.2

2.3.2.5 VMware VirtualCenter Client Hardware and software requirements

The VirtualCenter client is installed on any remote workstation meeting the following requirements. The VirtualCenter client can be installed on multiple Windows systems and access the VirtualCenter server through the network. These Windows systems can be on any desktop, laptop, or another virtual machine, so long as the hardware can support the software requirements listed below.

- Minimum of 256 MB RAM
- SSL client compatible with VirtualCenter OpenSSL Server
- .NET Framework version 1.1. If this is not available on the machine where VirtualCenter Client is installed, VirtualCenter automatically updates to .NET Framework 1.1.
- Operating system: Windows 2000, Windows XP Professional, Windows XP Home, Windows Server 2003, Windows 98, Windows 98 SE, Windows ME, or windows NT4 with SP6a.

2.3.3 TOE Time Synchronization requirements

The TOE uses a Network Time Protocol (NTP) server to support time synchronization between the VirtualCenter and the ESX Servers it manages. The NTP Server is a part of the TOE environment. The NTP clients, on each ESX Server and the managing VirtualCenter and/or domain server, must be configured to use the same NTP server with similar periodicity. This is required by administrator documentation. Note that the NTP clients are included in the ESX software installation, and are built into VirtualCenter and/or domain server windows operating systems.

2.4 TOE Physical Scope and Boundaries

The physical scope and boundaries of the TOE are the hardware and software components that make up the TOE. The following table identifies those hardware and software items that are required to be within the TOE, and those which are required to be in the TOE's operating environment.

Component	**TOE or TOE Environment?**
VirtualCenter 1.2.0 Software (includes VMotion, VirtualCenter Server, VirtualCenter agent, and Virtual Center Client)	TOE
ESX Server 2.5.0 Software (includes Virtual SMP, Console OS, ESX management server, Apache 1.3.31 httpd)	TOE
OpenSSL 0.9.7d on ESX Server and VirtualCenter	TOE
OpenSSH 3.5p1-11 on ESX Server	TOE
NTP Client on ESX Server	TOE Environment
Optional domain server for VirtualCenter, to include its hardware, Operating system and	TOE Environment

Component	TOE or TOE Environment?
software.	
NTP Server available to ESX Server and VirtualCenter	TOE Environment
ESX Server hardware (processor and adapters) including blade servers	TOE Environment
Storage Area Network hardware and software to be used with ESX Server in configuration 2 and 3.	TOE Environment
VirtualCenter Hardware, operating system, and DBMS	TOE Environment
VirtualCenter Client hardware, operating system,	TOE Environment
Operating systems and applications for VMs	TOE Environment
Hardware, OS, and software (as identified in the previous sections) for remote workstations	TOE Environment

2.5 TOE Logical Scope and Boundaries

The logical scope and boundaries of the TOE are the security functions that it provides. The following sections describe the TOE security functions and their associated IT environment security functions in order to present a clear picture. Details of the TOE security functions are found in section 6, the TOE Summary Specification.

2.5.1 Access Control

Access control is provided in both the ESX Server and the VirtualCenter.

The ESX server controls access to files pertaining to VM definition and configuration as well as ESX Server configuration. The root account is granted unlimited access to these items. For all other users, ESX Server uses explicit permissions defined for users and groups with the user/group/other access controls of the underlying Linux kernel, as well as permissions to perform certain operations based on a user's access permissions to the VM's configuration file.

The access control method for the VirtualCenter uses both traditional role enforcement and access control checks made based on permission pairs assigned to objects. VirtualCenter Administrators (who are members of the administrator's group of the underlying OS) are granted all accesses.. All other access control is based on the UserID and group membership of the subject and the user id/ group id and VC-role permission pair assigned to the object requested.. VirtualCenter objects , including event files, alarms, templates and inventory objects (VMs, Farms, Farm Groups, Server Farms, and VM Groups) are assigned permission pair(s), each of which identifies a userID or groupID, and VC-role that identifies the functions the userID/group member can perform on the object. If the user id/group of the requesting user/subject is a match with a userID/group of a permission pair associated with the object, then the user is allowed to perform the activities allowed by the VC-role of the permission pair on the object. The VirtualCenter can access data on the VirtualCenter Database as well as some information that is stored on the ESX Servers.

2.5.2 Auditing

The TOE provides audit data collection for both the ESX Server and the VirtualCenter. Each component has facilities to review audit data, and the VirtualCenter provides selectable audit data review. Reliable time stamps are provided by the IT Environment.

Appropriately qualified users can review audit data collected at the VirtualCenter. Auditable events for the ESX Server include start-up and shutdown of the local audit mechanism, all unsuccessful use of the identification and authentication mechanisms, and successful use of the identification and authentication mechanisms when logging into the Command Line Interface. Audit records collected by the VirtualCenter include start-up of the local audit mechanism, all use of the identification and authentication mechanisms, and all requests to perform an operation on an inventory object, scheduled events, templates, alarms, and events. Note that on the ESX Server, audit records are stored in syslogs, and on the VirtualCenter, audit records are stored as events.

2.5.3 Identification & Authentication

The identification and authentication is performed at both the VirtualCenter and the ESX Server. When a user attempts to use the VirtualCenter, it requests identification and authentication from the underlying operating system of the VirtualCenter. I&A for the ESX Server from a remote workstation to the Management Interface, a remote workstation to the Service Console, or a direct connection to the ESX Server host to the Service Console is performed by the Service Console. In all cases, I&A is performed using a password-based authentication mechanism.

Identification and authentication are also performed between an ESX Server and the VirtualCenter that manages it. The first time the VirtualCenter requests actions to be taken on an ESX Server under its control, the VirtualCenter presents the root password for the ESX Server to the ESX Server. If it is successfully authenticated, 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 and password are used for all subsequent connections between the ESX Server and the VirtualCenter.

2.5.4 Security Management

The TOE provides roles for the ESX Server user community. One role is that of System Administrator. TOE users assume this role when they log directly into the root account, or switch to the root account from another valid login account. All other valid users who log into the ESX Server, including *vpxuser* requests from the managing VirtualCenter, are VM administrators. Role enforcement is implemented by verifying if the user is a root user or other non-root user.

The Security Management features for the TOE include management of security attributes for users and resources and management of separation of Virtual Machines on an ESX Server.

For the ESX Server, security attributes include User ID, group associated with both users and resources (files), and read, write, and execute permissions associated with objects. The management activities are performed by the functions of the underlying Linux kernel upon which the ESX Server is built.

For the VirtualCenter, roles are provided by the TOE Environment. There are two roles, VirtualCenter Administrator and all other users, called Limited Access User. A user is a VirtualCenter Administrator if the user is made a member of the “administrators” group of the underlying operating system. Role enforcement is implemented by verifying if the user is a VirtualCenter Administrator or not.

Subject security attributes are the UserID and the group(s) to which the user belongs. Object security attributes include privilege pairs (user id/group id, VC-role) for all resources resident in the VirtualCenter. The TOE restricts access to security relevant functions and TSF data using the access control mechanisms described in section 2.5.1. The TOE provides security management in the VirtualCenter component for security attributes.

The management of separation of Virtual Machines is provided by a collection of ESX Server functions. The ability to perform specific functions on specific data is controlled by the ESX Server access control policy described above.

2.5.5 Virtual Machine Domain Separation

The virtual machine domain 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. VM administrators “configure” the CPU, memory, disk, and network requirements for their VMs. These requests are actually requests for resources, which are managed entirely by the VM kernel.

2.5.6 TOE Protection

The TOE provides a secure domain for its own execution, and also ensures that the security features of the TOE cannot be bypassed. The TOE also provides protection of data in transit between the TOE components. Specifically, communications between the VirtualCenter Client and the VirtualCenter Management Server are protected using SSL. Communication between the VirtualCenter and the ESX Server is also protected by SSL.

The TOE provides protection for communication between the TOE and remote trusted IT products as follows. Protection between the ESX Server’s Management Interface and a remote workstation is provided by SSL in an HTTPS session. Protection of administrator sessions between the ESX Service Console and a remote workstation is provided by SSH.

2.6 Items not included in the TOE or not claimed in the TOE

The following items are excluded from the TOE and are not to be used with the evaluated configuration of the products:

- SNMP, FTP, Telnet
- VMware GSX Servers and VMware workstations
- The use of any authentication method on ESX other than the local password database
- VirtualCenter Web Interface
- VMware SDK tools
- The *procfs* interface on the ESX Server Service Console
- Third party products other than those explicitly listed in sections 2.3 and 2.4 of this Security Target
- VMware Scripting API on the ESX Server.
- Activities involving Parallel and Serial ports on the ESX Server

No claims are made for the following functions of the products that make up the TOE. These functions may be required to use the TOE, but are not considered in the evaluation of the TOE.

- Activities dealing with the use of Virtual Machines
  - ➢ Remote Console functionality of the ESX Server or the VirtualCenter to manage or use software on individual Virtual Machines
  - ➢ Guest Operating systems on Virtual Machines
  - ➢ Applications running in guest operating systems
  - ➢ Actions of VM users and VM administrators that take place on the VMs
  - ➢ VMware Tools
  - ➢ VMware Guest Operating System Service
- VirtualCenter DBMS, operating systems of the VirtualCenter and remote workstations, acceptable browsers, SAN software.
- Backup functionality for Virtual Machines
- Clustering
- Failover
- Functionality specific to performance enhancement

2.6.1 Rationale for excluding Virtual Machine guest operating systems and applications from the TOE

This TOE addresses the Virtual Machine infrastructure, including creation and management of Virtual Machines, which appear to be individual physical machines to their users. 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 operating systems and applications of the VMs are excluded from the TOE.

Note that the evaluated configuration must use the “high” security option for the VirtualCenter and the ESX Server.

3. TOE Security Environment

Assumptions
A.DBMS
A.GENPUR
A.NOEVIL
A.PHYSICAL
A.SANS
Threats
T.AUDGEN
T.AUDMOD
T.AUDREV
T.LEAKAGE
T.MEDIATE
T.NOAUTH
T.PROCOM
T.SLFPRO
Organizational Security Policies
NONE

Table 3-1: TOE Assumptions, Treats, and Organizational Security policies

3.1 Assumptions

The following conditions are assumed to exist in the operational environment.

A.DBMS	The VirtualCenter and the VirtualCenter Database are installed on the same physical server.
A.GENPUR	There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE except within a Virtual Machine on the ESX Server. Furthermore, the VirtualCenter Database is not used for any purpose except that of the VirtualCenter.
A.NOEVIL	Administrators of the TOE are non-hostile, appropriately trained, and follow all user and administrator guidance.
A.PHYSICAL	The TOE is located within a physical area that protects the TOE from unauthorized physical access.

A.SANS	When the TOE uses a Storage Area Network, it is on a private, physically protected network and is protected from unauthorized physical access.

3.2 Threats

The following are threats identified for the TOE. The assumed level of expertise of the attacker for all the threats is *unsophisticated*. The threat agents are users authorized to use the TOE as well as unauthorized users (persons or external IT entities) not authorized to use the TOE.

T.AUDGEN	An unauthorized user may perform unauthorized actions that go undetected because of the failure of the system to record actions.
T.AUDMOD	A user modifies or deletes audit records in an attempt to hide any actions the user may have performed.
T.AUDREV	Illegal actions performed by users may not be detected because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.LEAKAGE	An authorized user of a virtual machine may access the virtual CPU, memory, disk, or network from the unshared resources of another virtual machine.
T.MEDIATE	A user may access files, data, or functions for which he is not authorized because of inadequate access control measures.
T.NOAUTH	An unauthorized user may gain access to system data due to failure of the system to enforce identification and authentication.
T.PROCOM	An unauthorized user may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.
T.SLFPRO	An unauthorized user may bypass, deactivate, or tamper with TOE security functions.

3.3 Organizational Security Policies

There are no organizational security policies defined for the TOE.

4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

Objectives
O.ACCTL_VC
O.ACCTL_ESX
O.AUDGEN
O.AUDMOD
O.AUDREV
O.ENCRYP
O.I&A
O.PRODAT
O.SECFUN
O.SLFPRO
O.VMSEP
Security Objectives for the IT Environment
OE.I&A
OE.ROLES
OE.TIMSTP
Security Objectives for the Non-IT Environment
OE.DBMS
OE.GENPUR
OE.NOEVIL
OE.PHYSICAL
OE.SANS

Table 4-1 :Objectives for the TOE and the TOE Environment

4.1 Security Objectives for the TOE

O. ACCTL_VC	The TOE must provide the means of controlling and limiting access by VirtualCenter users to VirtualCenter objects.
O.ACCTL_ESX	The TOE must provide the means of controlling and limiting access by ESX Server users to ESX Server objects.
O.AUDGEN	The TOE must provide the means of recording any security relevant events that contain security relevant information including the time of the event to hold users accountable for any security relevant actions they perform.
O.AUDMOD	The TOE must protect audit records against unauthorized modification or deletion to ensure accountability of user actions.

O.AUDREV	The TOE must provide a means of viewing, and ordering audit data generated by the VirtualCenter, and a means of viewing the audit data generated by the ESX Server.
O.ENCRYP	The TOE must protect the confidentiality and integrity of its dialogue with an authorized administrator using a remote connection.
O.I&A	The ESX Server must uniquely identify all users of the ESX server, and will authenticate the claimed identity before granting a user any access. The VirtualCenter must request identification and authentication from the underlying operating system, and must receive a positive authentication result before granting any user any access.
O.PRODAT	The TOE must protect the confidentiality and integrity of TOE data in transit.
O.SECFUN	The TOE shall provide functionality that enables an authorized administrator to use the TOE security functions and must ensure that only authorized administrators are able to access such functionality.
O.SLFPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.VMSEP	The TSF must create and maintain Virtual Machines and ensure that users of one VM cannot access unshared resources of another VM.

4.2 Security Objectives for the Environment

The following objectives address non-IT issues that are satisfied by procedural or administrative means, as well as IT objectives addressed by the TOE Environment.

4.2.1 Security Objectives for the IT Environment

OE.I&A	The IT Environment must identify all users of the VirtualCenter, and will authenticate the claimed identity before the VirtualCenter grants a user access to the TOE facility.
OE.ROLES	The IT Environment must provide roles for all users of the VirtualCenter.
OE.TIMSTP	The IT Environment must provide a mechanism capable of providing reliable source for time.

4.2.2 Security Objectives for the Non-IT Environment

OE.DBMS	The VirtualCenter and the VirtualCenter Database are installed on the same physical server.

OE.GENPUR	There are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE except within a Virtual Machine on the ESX Server. Furthermore, the VirtualCenter Database is not used for any purpose except that of the VirtualCenter.
OE.NOEVIL	Administrators of the TOE are non-hostile, appropriately trained, and follow all user and administrator guidance.
OE.PHYSICAL	The TOE is located within a physical area that protects the TOE from unauthorized physical access.
OE.SANS	When the TOE uses a Storage Area Network, it is on a private, physically protected network and is protected from unauthorized physical access.

4.3 Security Objectives Rationale

4.3.1 Tracing for Threats

Table 4-2 demonstrates that all security objectives for the TOE and its supporting environment trace to aspects of the identified threats to be countered and/or aspects of the organizational security policies to be met by the TOE.

	T.AUDGEN	T.AUDMOD	T.AUDREV	T.LEAKAGE	T.MEDIATE	T.NOAUTH	T.PROCOM	T.SLFPRO
O. ACCTL_VC					X			
O.ACCTL_ESX				X	X			
O.AUDGEN	X							
O.AUDMOD		X						
O.AUDREV			X					
O.ENCRYP							X	
O.I&A						X		
O.PRODAT							X	
O.SLFPRO								X
O.VMSEP				X				
O.SECFUN						X		
OE.ROLES					X			
OE.I&A						X		
OE.TIMSTP	X							

Table 4-2: TOE Threats Tracing

4.3.2 Security Objectives Rationale: Threats to the TOE

T.AUDGEN An unauthorized user may perform unauthorized actions that go undetected because of the failure of the system to record actions.

The objective O.AUDGEN counters this threat by providing an audit mechanism that collects audit data about security relevant events. The objective for the IT Environment, OE.TIMSTP, ensures that reliable time stamps are provided for the audit records generated.

T.AUDMOD A user modifies or deletes audit records in an attempt to hide any actions the user may have performed.

The objective O.AUDMOD counters this threat by ensuring that only authorized administrators can modify or delete the audit records.

T.AUDREV Users may not be accountable for the actions they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.

The Objective O.AUDREV counters this threat by providing a facility to review the audit records to authorized administrators.

T.LEAKAGE An authorized user of a virtual machine may access the virtual CPU, memory, disk, or network from the unshared resources of another virtual machine.

The objectives O.VMSEP and O.ACCTL_ESX counter this threat. O.VMSEP provides for separation of Virtual Machines, ensuring that users of one VM cannot access unshared resources of another VM, and O.ACCTL_ESX provides access controls that restrict users from accessing files to which they have no access permissions.

T.MEDIATE A user may access files, data, or functions for which he is not authorized because of inadequate access control measures.

This threat is countered by O.ACCTL_VC, O.ACCTL_ESX, and OE.ROLES. The first two objectives describe access controls on VirtualCenter objects and ESX objects, respectively. OE.ROLES supports the objective O.ACCTL_VC by providing roles from the underlying operating system.

T.NOAUTH An unauthorized user may gain access to system data due to failure of the system to enforce identification and authentication.

This threat is met by O.I&A, OE.I&A, and O.SECFUN. Identification and authentication for the ESX server is addressed by O.I&A, and identification and authentication to the VirtualCenter is addressed by O.I&A and OE.I&A. There are no other ways a user may access the ESX Server or the VirtualCenter. O.SECFUN guarantees that there are adequate security functions to manage the I&A functionality.

T.PROCOM An unauthorized user may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

This threat is met by objectives O.ENCRYPT and O.PRODAT. O. ENCRYP ensures the confidentiality and integrity of an administrator's dialog with the TOE, and O.PROCOM protects the confidentiality and integrity of TOE data in transit.

T.SLFPRO An unauthorized user may bypass, deactivate, or tamper with TOE security functions.

This threat is met by objectives O.SLFPRO which ensures that unauthorized users may not bypass, deactivate, or tamper with the TOE security functions.

4.3.3 Security Objectives Rationale: Organizational Security Policies

This ST has no Organizational Policies.

4.3.4 Security Objectives Rationale: Assumptions

This section provides a justification that for each assumption, the security objectives for the environment cover that assumption.

The following security objectives for the environment are a re-statement of the security assumptions, so those security objectives trace to all aspects of the assumptions.

A.DBMS and OE.DBMS

A.GENPUR and OE.GENPUR

A.NOEVIL and OE.NOEVIL

A.PHYSICAL and OE.PHYSICAL

A.SANS and OE.SANS

5. IT Security Requirements

The following table describes the security functional requirements for the TOE that are conformant with part 2 of the CC, the explicitly stated security requirements for the TOE, and the security functional requirements on the TOE environment

Security Functional Requirement	**Name of requirement**
The following requirements on the TOE have been taken from CC part 2.	
FAU_GEN.1 [b]	Audit data generation
FAU_SAR.1 [a] and [b]	Audit Review
FDP_ACC.1 [a] and [b]	Subset Access control
FDP_ACF.1 [a] and [b]	Security attribute based access control
FIA_UAU.1 [b] and [c]	Timing of authentication
FIA_UID.1 [b] and [c]	Timing of identification
FMT_MSA.1 [a] and [b]	Management of security attributes
FMT_MSA.3 [a] and [b]	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1 [b]	Security roles
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1 [b] and [c]	Inter-TSF detection of modification
FPT_ITT.1	Basic Internal TSF Data transfer protection
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
The following requirements on the TOE are explicitly defined requirements	
FAU_GEN_EXP.1 [a]	Audit Data Generation
FAU_SAR_EXP.3	Selectable Audit Review
FIA_VC_LOGIN_EXP.1	VirtualCenter Login Request
VDS_VMM_EXP.1	ESX Virtual MachineDomain Separation
The following are requirements on the IT Environment and are taken from CC part 2.	
FIA_UAU.1 [a]	Timing of authentication
FIA_UID.1 [a]	Timing of identification
FMT_SMR.1 [a]	Security roles
FPT_STM.1	Reliable time stamps

Table 5-1: IT Security Requirements

5.1 Security Functional Requirements for the TOE

5.1.1 FAU: Security Audit

5.1.1.1 FAU_GEN: Security audit data generation

5.1.1.1.1 FAU_GEN.1 [b]: Audit data generation [ESX Server]

FAU_GEN.1.1 [b]

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

a) Start-up and shutdown of the audit functions [***of the ESX Server***];

b) All auditable events for the [not specified] level of audit; and

c) [The events specified in column 2 of the following table].

FAU_GEN.1.2 [b]

The TSF shall record within each audit record [***of the ESX Server]*** at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[The information found in column three of Table 5-2]**

Functional Component:	**Audit Event:**	**Additional information to be collected**
FIA_UAU.1 [b] and FIA_UAU.1 [c]	**Unsuccessful use of an authentication mechanism on the ESX;**	**The user identity if provided**
FIA_UID.1 [b] and FIA_UID.1 [c]	**Unsuccessful use of an identification mechanism on the ESX,**	**The user identity if provided.**
FIA_UAU.1 [b] and FIA_UAU.1	**Successful use of the authentication mechanism when logging in to the**	**The user identity if provided**

[c]	**Command Line Interface of the ESX Server**	
FIA_UID.1 [b] and FIA_UID.1 [c]	**Successful use of the user identification mechanism when logging in to the Command Line Interface of the ESX Server.**	**The user identity if provided.**

Table 5-2: Auditable events of the ESX Server

5.1.1.2 FAU_SAR: Security audit review

5.1.1.2.1 FAU_SAR.1 [a]: Audit review [VirtualCenter]

FAU_SAR.1.1 [a]

The TSF shall provide [**users who are granted access to the requested object by the VirtualCenter Access Control Policy**] with the capability to read [**VirtualCenter audit events**] from the audit records.

FAU_SAR.1.2 [a]

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

5.1.1.2.2 FAU_SAR.1[b]: Audit review [ESX Server]

FAU_SAR.1.1 [b]

The TSF shall provide [**users who are granted access to the requested object by the ESX Server Access Control Policy**] with the capability to read [**ESX Server audit events**] from the audit records.

FAU_SAR.1.2 [b]

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

5.1.2 FDP: User Data Protection

5.1.2.1 FDP_ACC: Access control policy

5.1.2.1.1 FDP_ACC.1 [a]: Subset access control [VirtualCenter]

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, Farms, Farm Groups, virtual machine groups, and Server Farms; scheduled events, alarms, events, and templates.**

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

5.1.2.1.2 FDP_ACC.1 [b]: Subset access control [ESX Server]

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, system logs.

c. Operations: all operations between the listed subjects and the listed objects, power operations, and register/unregister a VM operations].

5.1.2.2 FDP_ACF: Access control functions

5.1.2.2.1 FDP_ACF.1 [a]: Security attribute based access control [VirtualCenter]

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 ID or User group(s), User role.**

c. **Objects: Inventory data for Virtual Machines, Farms, Farm Groups, VM Groups, the Server Farm; events, alarms, scheduled tasks, and templates.**

d. **Object attributes: A set of permission pairs (User Id/ 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 ID component that matches the userID 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 ID of the subject does not match the userID of any permission pair associated with the object, or the User ID 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.**

5. **All VirtualCenter objects are contained within an object hierarchy.**

6. **Newly created objects inherit the permissions of the parent object.**

7. **When an object is moved within the hierarchy, the object loses its previous permissions and assumes the permission settings of the new parent object.].**

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].**

5.1.2.2.2 FDP_ACF.1: Security attribute based access control [ESX Server]

FDP_ACF.1.1 [b]

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

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

2. **Subject security attributes: User ID, User group(s), ESX User role.**

3. **Objects: Virtual machine definition and configuration files; ESX Server configuration files, ESX Server audit logs.**

4. **Object attributes: user id 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 role is system administrator.**

2. **Access is granted if the ESX 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 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 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 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 other 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: **[none].**

5.1.3 FIA: Identification and Authentication

5.1.3.1 FIA_UAU: User authentication

5.1.3.1.1 FIA_UAU.1 [b]: Timing of authentication[local authentication, ESX Server]

FIA_UAU.1.1 [b]

The TSF shall allow [**no other actions**] on behalf of the user to be performed before the user is authenticated [***from the locally attached keyboard, monitor, and mouse to the Service Console]***.

FIA_UAU.1.2 [b]

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

5.1.3.1.2 FIA_UAU.1 [c]: Timing of authentication [remote authentication, ESX Server]

FIA_UAU.1.1 [c]

The TSF shall allow [**no other actions**] on behalf of the user to be performed before the user is authenticated [***from a remote connection to the Service Console on the ESX Serve, from a remote connection from the VMware management interface on the ESX Server, or from the VirtualCenter to the ESX Server via the VirtualCenter].***

FIA_UAU.1.2 [c]

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

5.1.3.2 FIA_UID: User identification

5.1.3.2.1 FIA_UID.1 [b]: Timing of identification [Local identification ESX Server]

FIA_UID.1.1 [b]

The TSF shall allow [**no actions**] on behalf of the user to be performed before the user is identified [***from the local console to the Service Console of the ESX Server[***.

FIA_UID.1.2 [b]

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

5.1.3.2.2 FIA_UID.1 [c]: Timing of identification [Remote identification ESX Server]

FIA_UID.1.1 [c]

The TSF shall allow [**a connection establishment**] on behalf of the user to be performed before the user is identified [***from a remote connection to the Service Console of the ESX Server, from a remote connection to the VMware management interface of the ESX Server, or from the VirtualCenter to the ESX Server via the VirtualCenter Agent].***

FIA_UID.1.2 [c]

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

5.1.4 FMT: Security Management

5.1.4.1 FMT_MSA: Management of security attributes

5.1.4.1.1 FMT_MSA.1[a]: Management of security attributes [VirtualCenter]

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 [**permission pairs for VirtualCenter users and all objects in the VirtualCenter]** to [**VirtualCenter Administrators and Limited Access Users having a permission pair on the VirtualCenter Server Farm that includes VirtualCenter Administrator access rights**].

5.1.4.1.2 FMT_MSA.1[b]: Management of security attributes [ESX Server]

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; For ESX Server objects: object owner; object group; object read, write, and execute permissions**] to [**as described in the following table**].

Action	**Attribute**	**Role**
Modify	**Read, write, and execute permissions on objects**	**System Administrator or object owner**
Add, Delete, Modify	**User id of object owner, object group**	**System Administrator**
Add, Delete, Modify	**object group**	**Object owner: 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 id, user group**	**System Administrator**

5.1.4.1.3 FMT_MSA.3 [a]: Static attribute initialization [VirtualCenter]

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 Administrator and Limited Access Users having a permission pair on the VirtualCenter Server Farm that includes VirtualCenter Administrator access rights**] to specify alternative initial values to override the default values when an object or information is created ***[on the VirtualCenter].***

5.1.4.1.4 FMT_MSA.3 [b]: Static attribute initialization [ESX Server]

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**] to specify alternative initial values to override the default values when an object or information is created ***[on the ESX Server, as described in the following table].***

[Role	**Type of object or information**
System administrator	**Any**
VM administrator	**Objects they create]**

5.1.4.2 FMT_SMF: Specification of Management Functions

5.1.4.2.1 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: **[**

1. **Adding, deleting, or modifying a user/group role permission pair of an object 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.]

5.1.4.3 FMT_SMR: Security management roles

5.1.4.3.1 FMT_SMR.1 [b]: Security roles [ESX Server]

FMT_SMR.1.1 [b]

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

FMT_SMR.1.2 [b]

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

5.1.5 FPT: Protection of the TOE functions

5.1.5.1 FPT_ITC: Confidentiality of exported TSF data

5.1.5.1.1 FPT_ITC.1: Inter-TSF confidentiality during transmission

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.

5.1.5.2 FPT_ITI: Integrity of exported TSF data

5.1.5.2.1 FPT_ITI.1 [b]: Integrity of exported TSF data [remote workstation to ESX Server Management Interface]

FPT_ITI.1.1[b]

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **[at least one MAC error in SSL transmissions].**

FPT_ITI.1.2 [b]

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **[resend of network packet(s) that caused the error]** if modification is detected.

5.1.5.2.2 FPT_ITI.1 [c]: Integrity of exported TSF data [from remote workstation to ESX Server Service Console]

FPT_ITI.1.1[c]

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **[at least one MAC error in SSH transmissions].**

FPT_ITI.1.2 [c]

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **[a re-send of network packet(s) that caused the error]** if modification is detected.

5.1.5.3 FPT_ITT: Internal TOE TSF data transfer

5.1.5.3.1 FPT_ITT.1: Basic internal TSF data transfer protection

FPT_ITT.1.1

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

5.1.5.4 FPT_RVM: Reference mediation

5.1.5.4.1 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.5 FPT_SEP: Domain separation

5.1.5.5.1 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC**.**

5.2 Explicitly Stated Security Functional Requirements for the TOE

5.2.1 FAU Audit

5.2.1.1 _GEN_EXP.1 [a]: Audit data generation [VirtualCenter]

FAU_GEN_EXP.1.1 [a]

The TSF shall be able to generate an audit record of the following auditable events specified in column 2 of table Table **5-3:** Auditable Events on the VirtualCenter

FAU_GEN_EXP.1.2 [a]

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information provided in column 3 of the following table].

Functional Component:	Audit Event:	Additional information
	Startup of the Auditing functions	
FDP_ACF.1 [a]	Operations on Virtual Machines: power operations, remove Virtual Machine, create Virtual Machine	Virtual Machine
FDP_ACF.1 [a]	Alarm/scheduled task reconfigured	alarm/scheduled task
FIA_UAU.1 [a] and FIA_UID.1 [a]	All use of the user identification and authentication mechanisms.	The user identity if provided

Table 5-3: Auditable Events on the VirtualCenter

5.2.1.2 FAU_SAR_EXP.3: Selectable audit review [VirtualCenter]

FAU_SAR_EXP.3.1

The TSF shall provide the ability to perform [ordering] of ***[VirtualCenter]*** audit data based on [**the Description, Type, or Time]**.

5.2.2 FIA: Identification and Authentication

5.2.2.1 FIA_VC_LOGIN_EXP.1: User Login Request

FIA_VC_LOGIN_EXP.1.1

The 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.

5.2.3 VDS: VM Domain Separation

5.2.3.1 VDS_VMM_EXP.1: ESX Virtual Machine domain separation

VDS_VMM_EXP.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.

VDS_VMM_EXP.1.2

The TSF shall enforce separation between the security domains of VMs in the TSC.

5.3 Security Functional Requirements for the IT Environment

5.3.1 FIA: Identification and Authentication

5.3.1.1 FIA_UAU: User authentication

5.3.1.1.1 FIA_UAU.1 [a]: Timing of authentication [VirtualCenter]

FIA_UAU.1.1 [a]

The [***IT environment]*** shall allow [**identification**] on behalf of the user [***of the VirtualCenter***] to be performed before the user is authenticated.

FIA_UAU.1.2 [a]

The [***IT environment]*** shall require each user ***[of the VirtualCenter]*** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.3.1.2 FIA_UID: User identification

5.3.1.2.1 FIA_UID.1 [a]: Timing of identification [VirtualCenter]

FIA_UID.1.1 [a]

The [***IT environment]*** shall allow [**connection establishment**] on behalf of the user ***[of the VirtualCenter]*** to be performed before the user is identified.

FIA_UID.1.2 [a]

The [*IT environment]* shall require each user ***[of the VirtualCenter]*** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.2 FMT: Security Management

5.3.2.1 FMT_SMR: Security Management Roles

5.3.2.1.1 FMT_SMR.1 [a]: Security roles [VirtualCenter]

FMT_SMR.1.1 [a]

The [***IT environment]*** shall maintain the roles ***[for VirtualCenter users]*** [**VirtualCenter Administrator and Limited Access User**].

FMT_SMR.1.2 [a]

The [***IT environment]*** shall be able to associate users ***[of the VirtualCenter]*** with ***[the above mentioned]*** roles.

5.3.3 FPT: Protection of the TSF

5.3.3.1 FPT_STM: Time stamps

5.3.3.1.1 FPT_STM.1: Reliable time stamps

FPT_STM.1.1

The [***IT environment***]shall be able to provide reliable time stamps for its own use.

5.4 Security Assurance Requirements for the TOE

The TOE is defined at EAL2 and thus contains the following Security Assurance Requirements. These requirements are taken from Part 3 of the CC as stated in Chapter 1 of this ST.

5.4.1 ACM: Configuration Management

5.4.1.1 ACM_CAP.2: Configuration items

Developer action elements:	
ACM_CAP.2.1D	The developer shall provide a reference for the TOE.
ACM_CAP.2.2D	The developer shall use a CM system.
ACM_CAP.2.3D	The developer shall provide CM documentation.
Content and presentation of evidence elements:	

ACM_CAP.2.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2C	The TOE shall be labelled with its reference.
ACM_CAP.2.3C	The CM documentation shall include a configuration list.
ACM_CAP.2.4C	The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7C	The CM system shall uniquely identify all configuration items.
Evaluator action elements:	
ACM_CAP.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2 ADO: Delivery and Operation

5.4.2.1 ADO_DEL.1: Delivery procedures

Developer action elements:	
ADO_DEL.1.1D	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D	The developer shall use the delivery procedures.
Content and presentation of evidence elements:	
ADO_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
Evaluator action elements:	
ADO_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.2.2 ADO_IGS.1: Installation, generation and start-up procedures

Developer action elements:

ADO_IGS.1.1D	The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
Content and presentation of evidence elements:	
ADO_IGS.1.1C	The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
Evaluator action elements:	
ADO_IGS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E	The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.4.3 ADV: Development

5.4.3.1 ADV_FSP.1: Informal functional specification

Developer action elements:	
ADV_FSP.1.1D	The developer shall provide a functional specification.
Content and presentation of evidence elements:	
ADV_FSP.1.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C	The functional specification shall be internally consistent.
ADV_FSP.1.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C	The functional specification shall completely represent the TSF.
Evaluator action elements:	
ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.4.3.2 ADV_HLD.1: Descriptive high-level design

Developer action elements:	
ADV_HLD.1.1D	The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:	
ADV_HLD.1.1C	The presentation of the high-level design shall be informal.
ADV_HLD.1.2C	The high-level design shall be internally consistent.
ADV_HLD.1.3C	The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4C	The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5C	The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6C	The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7C	The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
Evaluator action elements:	
ADV_HLD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2E	The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.4.3.3 ADV_RCR.1: Informal correspondence demonstration

Developer action elements:	
ADV_RCR.1.1D	The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
Content and presentation of evidence elements:	
ADV_RCR.1.1C	For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
Evaluator action elements:	
ADV_RCR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4 AGD: Guidance Documents

5.4.4.1 AGD_ADM.1: Administrator guidance

Developer action elements:	
AGD_ADM.1.1D	The developer shall provide administrator guidance addressed to system administrative personnel.
Content and presentation of evidence elements:	
AGD_ADM.1.1C	The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2C	The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C	The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C	The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5C	The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6C	The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C	The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8C	The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
Evaluator action elements:	
AGD_ADM.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.4.2 AGD_USR.1: User guidance

Developer action elements:	
AGD_USR.1.1D	The developer shall provide user guidance.
Content and presentation of evidence elements:	

AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
Evaluator action elements:	
AGD_USR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5 ATE: Tests

5.4.5.1 ATE_COV.1: Evidence of coverage

Developer action elements:	
ATE_COV.1.1D	The developer shall provide evidence of the test coverage.
Content and presentation of evidence elements:	
ATE_COV.1.1C	The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
Evaluator action elements:	
ATE_COV.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5.2 ATE_FUN.1: Functional testing

Developer action elements:	
ATE_FUN.1.1D	The developer shall test the TSF and document the results.

ATE_FUN.1.2D	The developer shall provide test documentation.
Content and presentation of evidence elements:	
ATE_FUN.1.1C	The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
Evaluator action elements:	
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.4.5.3 ATE_IND.2: Independent testing – sample

Developer action elements:	
ATE_IND.2.1D	The developer shall provide the TOE for testing.
Content and presentation of evidence elements:	
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
Evaluator action elements:	
ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.4.6 AVA: Vulnerability Assessment

5.4.6.1 AVA_SOF.1: Strength of TOE security function evaluation

Developer action elements:	
AVA_SOF.1.1D	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
Content and presentation of evidence elements:	
AVA_SOF.1.1C	For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C	For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
Evaluator action elements:	
AVA_SOF.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2E	The evaluator shall confirm that the strength claims are correct.

5.4.6.2 AVA_VLA.1: Developer vulnerability analysis

.

Developer action elements:	
AVA_VLA.1.1D	The developer shall perform a vulnerability analysis.
AVA_VLA.1.2D	The developer shall provide vulnerability analysis documentation.
Content and presentation of evidence elements:	
AVA_VLA.1.1C	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2C	The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3C	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
Evaluator action elements:	
AVA_VLA.1.1E	The evaluator shall confirm that the information provided meets all

	requirements for content and presentation of evidence.
AVA_VLA.1.2E	The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.5 Strength of Function Claim

This ST claims a minimum strength of function level of SOF-basic for the TOE security functional requirements.

5.6 Security Requirements Rationale

The selected requirements selected for this TOE internally consistent and mutually supportive. The ST includes security functional requirements that address the security functionality provided by the TOE, with no contradictory requirements. All operations performed on the security requirements comply with the rules and intent required by the operation in the CC.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in Table 5-5
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.6.1
- including the SFRs FPT_RVM.1 and FPT_SEP.1 as appropriate on the TOE to protect the TSF
- including audit requirements to detect security-related actions and potential attacks
- including security management requirements to ensure that the TOE is managed and configured securely.

5.6.1 Security Functional Requirements to Objectives Tracing

Table 5-4 : Tracing SFR for the TOE and IT Environment to Objectives for the TOE demonstrates that all security functional requirements for the TOE trace to the objectives for the TOE. The table also includes the tracing for the objectives and requirements for the IT Environment.

	O.ACCTL_VC	O.ACCTL_ESX	O.AUDGEN	O.AUDMOD	O.AUDREV	O.ENCRYP	O.I&A	O.PRODAT	O.SECFUN	O.SLFPRO	O.VMSEP	OE.I&A	OE.ROLES	OE.TIMSTP	
FAU_GEN_EXP.1 [a]			X												
FAU_GEN.1 [b]			X												

	O.ACCTL_VC	O.ACCTL_ESX	O.AUDGEN	O.AUDMOD	O.AUDREV	O.ENCRYP	O.I&A	O.PRODAT	O.SECFUN	O.SLFPRO	O.VMSEP	OE.I&A	OE.ROLES	OE.TIMSTP	
FAU_SAR.1 [a] and [b]					X										
FDP_ACC.1 [a]	X			X					X						
FDP_ACF.1 [a]	X			X					X						
FMT_MSA.1 [a]	X														
FMT_MSA.3 [a]	X														
FDP_ACC.1 [b]		X		X					X						
FDP_ACF.1 [b]		X		X					X						
FIA_UAU.1 [b] and [c]							X		X						
FIA_UID.1 [b] and [c]							X		X						
FMT_MSA.1 [b]		X													
FMT_MSA.3 [b]		X													
FMT_SMF.1				X					X						
FMT_SMR.1 [a]	X												X		
FMT_SMR.1 [b]		X													
FPT_ITC.1						X		X							
FPT_ITI.1 [b], [c]						X		X							
FPT_ITT.1						X		X							
FPT_RVM.1										X					
FPT_SEP.1										X					
FAU_SAR_EXP.3					X										
VDS_VMM_EXP.1											X				
FIA_VC_LOGIN_EXP.1							X								
FIA_UAU.1 [a]												X			
FIA_UID.1 [a]												X			
FPT_STM.1			X											X	

Table 5-4 : Tracing SFR for the TOE and IT Environment to Objectives for the TOE & IT Environment.

5.6.2 Rationale for Security Requirements on the TOE.

O. ACCTL_VC The TOE must provide the means of controlling and limiting access by VirtualCenter users to VirtualCenter objects.

This objective is met by the following SFR for the TOE and the IT environment: FDP_ACC.1 [a], FDP_ACF.1 [a], FMT_MSA.1 [a], and FMT_MSA.3 [a], and FMT_SMR.1 [a]. FDP_ACC.1 [a] describes the access control policy that controls access to VirtualCenter objects by VirtualCenter subjects, and identifies the operations that apply. FDP_ACF.1 [a] describes the subjects, objects, subject security attributes, object security attributes and the rules that are used to determine access. FMT_MSA.1 [a] provides for management of the security attributes of subjects and objects that are used in making access control decisions. FMT_MSA.3 [a] provides for static initialization of security attributes. Finally, FMT_SMR.1 [a] ensures that the TOE provides the roles used in the access control decisions on the VirtualCenter.

O.ACCTL_ESX The TOE must provide the means of controlling and limiting access by ESX Server users to ESX Server objects.

This objective is met by the following SFR for the TOE and the TOE IT environment: FDP_ACC.1 [b], FDP_ACF.1 [b], FMT_MSA.1 [b], FMT_MSA.3 [b], and FMT_SMR.1 [b]. FDP_ACC.1 [b] describes the access control policy that controls access to ESX Server objects by ESX Server subjects, and identifies the operations that apply. FDP_ACF.1 [b] describes the subjects, objects, subject security attributes, object security attributes and the rules that are used to determine access. FMT_MSA.1 [b] provides for management of the security attributes of subjects and objects that are used in making access control decisions. FMT_MSA.3 [b] provides for static initialization of security attributes. Finally, FMT_SMR.1 [b] ensures that the TOE provides the roles used in access control decisions for System administrators.

O.AUDGEN The TOE must provide the means of recording any security relevant events which contain security relevant information including the time of the event to hold users accountable for any security relevant actions they perform.

This objective is met by FAU_GEN_EXP.1 [a], FAU_GEN.1 [b], and FPT_STM.1. FAU_GEN_EXP.1 [a] and FAU_GEN.1 [b] provide for the existence of auditing functionality on the VirtualCenter and the ESX Server respectively. FPT_STM .1 provides reliable timestamps for the audit records.

O.AUDMOD The TOE must protect audit records against unauthorized modification or deletion to ensure accountability of user actions.

This objective is met by FDP_ACC.1 [a] and [b], FDP_ACF.1 [a] and [b], and FMT_SMF.1. Audit records are collected on both the VirtualCenter and the ESX Server, and the access control policy mechanisms protect the records from unauthorized access. FMT_SMF.1 provides for security management functions.

O.AUDREV The TOE must provide a means of viewing, sorting, and ordering audit data generated by the VirtualCenter.

FAU_SAR.1 and FAU_SAR.3 meet this objective by providing for viewing, sorting, and ordering functionality on the audit records stored on the VirtualCenter.

O.ENCRYP The TOE must protect the confidentiality and integrity of its dialogue with an authorized administrator using a remote connection.

This objective is met by FPT_ITT.1, FPT_ITC.1 and FPT_ITI.1 [b], and [c]. FPT_ITT.1 ensures that data in transit between physically separate parts of the TOE is protected from unauthorized disclosure or modification. The remaining requirements ensure the confidentiality and integrity of data in transit between the TOE and remote trusted IT products.

O.I&A The ESX Server must uniquely identify all users logging into the ESX server, and will authenticate the claimed identity before granting a user any access. The VirtualCenter must request identification and authentication from the underlying operating system, and must receive a positive authentication result before granting any user any access. VirtualCenter user requests for services on a managed ESX Server

When attempting to connect to the TOE via the ESX server, FIA_UAU.1 [b], [c], and FIA_UID.1 [b], [c] ensure that once a connection is made, a user is identified and authenticated before allowing other actions to take place. When attempting to access the TOE via the VirtualCenter, FIA_VC_LOGIN_EXP.1 ensures that Identification and authentication are requested from the underlying VirtualCenter environment, and that a positive authentication result be received prior to granting any access.

O.PRODAT The TOE must protect the confidentiality and integrity of TOE data in transit.

This objective is met by FPT_ITT.1, FPT_ITI.1 [b], and [c], and FPT_ITC. FPT_ITT.1 requires the confidentiality and integrity of TOE data that is in transit between physically separated parts of the TOE. FPT_ITC.1 and FPT_ITI.1 [a] and [b] require confidentiality and integrity of data that is transmitted between the TOE and a remote trusted IT product.

O.SECFUN The TOE shall provide functionality that enables an authorized administrator to use the TOE security Functions and must ensure that only authorized administrators are able to access such functionality.

FMT_SMF.1 meets this objective by listing the security management functions of the TOE Other SFR that contribute to meeting this objective are FDP_ACC.1 [a] and [b], FDP_ACF.1 [a] and [b], which provide access checks to ensure that only authorized users can address functionality and data. FIA_UAU.1 [b] and [c] as well as FIA_UID.1 [b] and [c] contribute to this objective by controlling who can access the ESX Server. FIA_UID.1 [a] and FIA_UAU.1 [a], requirements on the environment, together with FIA_VC_LOGIN_EXP.1, control who can access the VirtualCenter.

O.SLFPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.

This objective is met by FPT_RVM.1 and FPT_SEP.1. FPT_RVM.1 requiring that all TOE security policy functions are invoked and succeed before each function in the TOE may proceed. FPT_SEP.1 requires that the TOE protect itself from interference and tampering of untrusted subjects. This objective is also contributed to by FIA_UID.1 [a], [b], [c], and

FUA_UAU.1 [a],[b], [c], and FIA_VC_LOGIN_EXP.1, which guarantee that no unauthorized users can access the TOE.

O.VMSEP The TSF must create and maintain Virtual Machines and ensure that users of one VM cannot access unshared resources of another VM.

VDS_VMM_EXP.1 meets this objective by requiring a separate domain for each VM and requiring that domain separation be enforced. FMT_SMF.1 also meets this objective by requiring that TOE to provide the ability to create, modify, or delete VMs.

5.6.3 Rationale for Security Requirements on the TOE Environment

OE.I&A The IT Environment must identify all users of the VirtualCenter, and will authenticate the claimed identity before granting a user access to the TOE facility.

This objective is met by the requirements FIA_UAU.1 [a] and FIA_UID.1 [a], which require that the environment of the VirtualCenter provide identification and authentication capabilities for the VirtualCenter.

OE.ROLES The IT Environment must provide roles for all users of the VirtualCenter.

This objective is met by the requirement FMT_SMR.1 [a] which require that the environment of the VirtualCenter provide roles capabilities for the VirtualCenter.

OE.TIMSTP The IT Environment must provide a mechanism capable of providing reliable source for time.

This objective is met by requirement FPT_STM.1, which requires the environment to provide reliable timestamps for the TOE.

5.6.4 Rationale For SOF Claim for Security Functional Requirements

The rationale for the chosen level of SOF-basic is based on the low attack potential of the threat agents identified. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. The security objectives imply probabilistic or permutational security mechanism and the metrics defined are the minimal “industry” accepted (for the passwords) metrics that should be good enough for SOF-Basic.

The minimum strength level for the TOE security functions realized by a probabilistic or permutational mechanism is SOF-basic. Specific strength of function metrics are defined for the following requirements:

FIA_UAU.1 [b] and [c]

5.6.5 Rationale for Explicitly Stated SFRs

This TOE contains the following explicit security functions:

- FAU_GEN_EXP.1 [a]
- FAU_SAR_EXP.3
- FIA_VC_LOGIN_EXP.1
- VDS_VMM_EXP.1

FAU_GEN_EXP.1 [a] was explicitly stated because the VirtualCenter, while it audits startup of the VirtualCenter event logs, it does not audit the shutdown of the VirtualCenter Server, making it unable to meet the requirement FAU_GEN.1. This explicit requirement is based on FAU_GEN.1.

FAU_SAR_EXP.3 was explicitly stated because it only applies to the VirtualCenter part of the TOE. There are no TOE functions on the ESX Server for searches and sorts of the audit data stored on the ESX Server. This functionality is available for the vast majority of the audit records, which are stored on the VirtualCenter. This explicit requirement is based on FAU_SAR.3.

FIA_VC_LOGIN_EXP.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 the VirtualCenter takes to ensure that only identified and authenticated users can access the TOE via the 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.

VDS_VMM_EXP.1 was explicitly stated to address the separation of Virtual Machines . It is based on FPT_SEP.1, which describes the requirement for a separated domain for the TOE's execution. FPT_SEP.1 appears in this ST to address the issue of a security domain for the execution of the TOE. Since VMs are not subjects in this TOE, it does not address security domains of individual VMs. VDS_VMM_EXP.1 provides the same type of protection for each Virtual Machine domain as FPT_SEP.1 does for the TOE as a whole.

5.6.6 Security Functional Requirements Dependencies and Rationale

Security Functional Requirement	**Dependencies**
FAU_GEN_EXP.1 [a] (on env)	FPT_STM.1
FAU_GEN.1 [b]	FPT_STM.1
FAU_SAR.1 [a]	FAU_GEN_EXP.1 [a]
FAU_SAR.1 [b]	FAU_GEN.1 [b]
FDP_ACC.1 [a]	FDP_ACF.1 [a]
FDP_ACF.1 [a]	FDP_ACC.1 [a], FMT_MSA.3 [a]
FDP_ACC.1 [b]	FDP_ACF.1 [b]
FDP_ACF.1 [b]	FDP_ACC.1 [b], FMT_MSA.3 [b]
FIA_UAU.1 [a] (on TOE Env)	FIA_UID.1 [a]

Security Functional Requirement	Dependencies
FIA_UID.1 [a] (on TOE Env)	None
FIA_UAU.1 [b]	FIA_UID.1 [b]
FIA_UID.1 [b]	None
FIA_UAU.1 [c]	FIA_UID.1 [c]
FIA_UID.1 [c]	None
FMT_MSA.1 [a]	FDP_ACC.1 [a], FMT_SMR.1 [a], FMT_SMF.1
FMT_MSA.3 [a]	FMT_MSA.1 [a]. FMT_SMR.1 [a]
FMT_MSA.1 [b]	FDP_ACC.1 [b], FMT_SMR.1 [b], FMT_SMF.1
FMT_MSA.3 [b]	FMT_MSA.1 [b]. FMT_SMR.1 [b]
FMT_SMF.1	None
FMT_SMR.1 [a] (on TOE Env)	FIA_UID.1 [a]
FMT_SMR.1 [b]	FIA_UID.1 [b] and [c]
FPT_ITC.1	None
FPT_ITI.1 [b], [c]	None
FPT_ITT.1	None
FPT_RVM.1	None
FPT_SEP.1	None
FPT_STM.1 (on TOE Env)	None
FAU_SAR_EXP.3	FAU_SAR.1
FIA_VC_LOGIN_EXP.1	None
VDS_VMM_EXP.1	None

Table 5-5: Security Functional Requirements Dependencies

There are no unsatisfied dependencies identified for the security requirements of TOE.

5.6.7 Rationale for the TOE Assurance Requirements

VMware has chosen to pursue a Common Criteria evaluation in support of the government customer requirements mandated by NSTISSC 11. This policy requires a Common Criteria certification for all products to be used within systems used for entering, processing, storing, displaying, or transmitting national security information.

VMware has chosen evaluation assurance level EAL2 to meet the requirements mandated by the DoD and the U. S. Air Force divisions of the government in accordance with the USDoD NSTISSP #11 Interpretation and the USAF CIO Memorandum.

6. TOE Summary Specification

6.1 TOE Security Functions

TOE SECURITY FUNCTIONS
Access Control
Auditing
Identification & Authentication
Security Management
TOE Protection
Virtual Machine Domain Separation

Table 6-1: TOE Security Functions

6.1.1 Access Control

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

Note that there are no non-administrative users of the TOE. 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.

FDP_ACC.1 [a] and FDP_ACF.1 [a]: The VirtualCenter Access Control Policy

The VirtualCenter access control mechanism controls access to objects stored on the VirtualCenter, to include data and operations specific to definition, configuration, and management of the organizational objects Server Farms, Farms, Farm Groups, Virtual Machines, and VM Groups. Note that access to hosts is controlled by access to the Farm to which a host belongs, and as such, hosts are addressed by the access control policy only indirectly. The VirtualCenter access control mechanism also controls access to files containing templates as well as event[6], alarm, and scheduled event information. This information is stored in the VirtualCenter Database. The VirtualCenter access control mechanism also controls access by subjects acting on behalf of a VirtualCenter user to data and operations specific to the definition, configuration, and management of Virtual Machines. This 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.

[6] Recall that audit logs are a part of the event files in VirtualCenter terminology.

TOE users on the VirtualCenter are administrators who have been assigned to one of two roles: VirtualCenter Administrator (by default every member of the underlying OS administrator group falls into this role) and Limited Access user (by default any user who is not in the VirtualCenter Administrator role is in the Limited access user role).

Subjects are processes acting on behalf of the logged in user, and have userIDs and may belong to one or more groups, identified by a groupID.

Objects of the VirtualCenter are assigned permission pairs to determine which users have what kind of access to the objects. The permission pair contains a userID or group ID, and one of four hierarchical “VC-roles” and are described in section 2.3.1.2. The VC-roles, which are actually permission definitions, are: Read Only Users, Virtual Machine Users, Virtual Machine Administrator, and VirtualCenter Administrator. Note that there is a traditional role called VirtualCenter administrator as well as a VC-role called VirtualCenter Administrator. If a Limited Access User is granted access to an object in the VirtualCenter Administrator VC-role then that user has unlimited access rights to the particular object.

Note also that Limited Access Users can acquire rights similar to those of the VirtualCenter Administrators if a user in the traditional role of VirtualCenter Administrator assigns a permission pair to the VirtualCenter Server Farm that contains the user’s UserID and the VC-Role VirtualCenter Administrator. This gives the user unlimited access to all objects in the VirtualCenter, as well as the rights to change and add VMware licenses, but does not give the user full VirtualCenter administrator rights. For example, the Limited Access User with VirtualCenter Administrator access to the VirtualCenter’s Server farm does not have the capability to add, delete, or modify users. Thus, even with VirtualCenter Administrator VC-role to the server farm, the user’s capabilities are still a subset of those of a full VirtualCenter Administrator. .

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 OS’s administrator group. If so, access is granted. If not, the access control security function determines if either the user’s explicitly specified permissions or the user’s associated vc-role(s) for the object contain permissions sufficient for performing the requested operation on the requested object on behalf of the requesting user. The explicitly specified permissions are used to verify access for objects on the ESX Server, and the vc-roles are used for verifying objects on the VirtualCenter.

The security attributes for subjects on the VirtualCenter are userID, 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 userID or group and vc-role. When a subject requests access to such an object, the subject userID or group is compared with the userID and groupID 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 userID of the subject matches the userID of the object or the userID of the subject is a member of the group of the object and the requested operation is allowed for the VC-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.

When an ESX Server is first placed under VirtualCenter control, the root password for the ESX Server must be supplied. At that time, a password 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 described above, are passed to the ESX Server VirtualCenter Agent 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.

FDP_ACC.1 [b] and FDP_ACF.1 [b]: The ESX Server Access Control Policy

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. Which role is applicable is determined by whether or not the user has supplied the root password and it has been successfully authenticated. If the root password is supplied and successfully authenticated, then the actions are processed under the *root* account in the system administrator role. If the root password has not been supplied, the requested actions are performed under an individual account in the VM administrator role. Users of the system administrator role have unrestricted access in the ESX Server, and VM administrators' capabilities may be controlled by group membership or by userID. The ESX Server is designed so that the same access control mechanisms can be used for direct ESX users (users logged into the ESX server via the service console or the management interface) and for requests from VirtualCenter users. Once an ESX Server is placed under the management of a VirtualCenter[7], requests from the VirtualCenter users are processed using the distinguished account, *vpxuser,* which uses the VM administrator role. The account *vpxuser* is set up granting access to all .vmx files.

From the CLI, 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 access ESX Server configuration files or data. User access control for VM administrators is the standard user/group/other access control mechanism provided by the Linux kernel. If the userID 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] See section 6.1.3 for a description of this process.

When a user logs into the system from the Management interface, and for the distinguished user *vpxuser,* the ESX Server determines the privileges the VM administrator has for each virtual machine based on the user's access permissions to a virtual machine's configuration file (.vmx extension). Root users, or system administrators, automatically have all permissions. The distinguished user *vpxuser* has access to all .vmx files. A non-root user who has read access to the .vmx file for a particular VM has read access to view or attach to the virtual machine. A user who has write access to the .vmx file has permission to modify the virtual machine's configuration parameters. The user who has execute access to the .vmx file has permission to perform power operations on the virtual machine. In addition, the user needs read, write, and execute access to the .vmx file to register or unregister the virtual machine. This information is used to determine what information is provided on each web page presented to the user. Users of the Management Interface do not have the capability to access information or functionality that they are not allowed to use, because the information is not presented on the web pages the user receives.

When a user possesses multiple permissions, the access control security function uses any of the associated 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 permissions, then access is denied.

6.1.2 Auditing

The auditing security function of the TOE is provided by both the ESX Server and VirtualCenter components for audit data generation. The audit mechanisms, audit storage, and other mechanisms are different for each of the major components of the TOE. Audit data collected by the ESX Server is stored in a flat file on the ESX server, and audit data collected by the VirtualCenter is stored as events on the VirtualCenter Database.

FAU_GEN_EXP.1 [a] Audit Data generation [VirtualCenter]

The VirtualCenter generates audit records for the following events:

- start-up of the audit functions,
- The following operations on Virtual Machines
    a. Power operations
    b. Removal of a Virtual Machine
    c. Creating a Virtual Machine
- Reconfiguring an alarm or a scheduled task
- all use of the identification and authentication mechanisms.

Each audit record generated includes the date and time of the event, type of event, subject identity (if applicable), 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.

FAU_SAR.1 [a]: Audit review [VirtualCenter]

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 Farm, Farm Group, VM, or VM Group can access the event logs for that organizational grouping. Only a VirtualCenter Administrator can view all the event logs of the entire Server Farm, which includes all the organizational objects. Audit events are viewed though web pages under the event tab for each organizational object.

FAU_SAR_EXP.3: Selectable Audit Review

The VirtualCenter provides ordering capabilities for the event data. Ordering is used when a user wishes to display the audit data in a sequential manner according to a specific field. The TOE allows a user to order audit data based on description, type, or time.

FAU_GEN.1 [b]: Audit Data generation [ESX Server]

The ESX Server generates audit records for the start-up and shutdown of the audit functions (via startup and shutdown of the syslogs), all unsuccessful use of the identification and authentication mechanisms, and successful use of the identification and authentication mechanisms when logging into the Console OS (either directly via the local console or remotely using an SSH connection). Each audit record generated includes the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event, and userID used for a failed identification or authentication attempt. This data is stored in a flat file on the Service Console of the ESX Server.

FAU_SAR.1 [b] Audit Review [ESX Server]

The ESX Server provides the capability using the syslog command to review its audit records which are stored in /var/log/messages. Reviewing the audit records on the ESX Server is restricted to the ESX System Administrator.

FPT_STM.1: Reliable Time Stamps

Reliable time stamps are provided by the TOE environment. The ESX Server is capable of synchronizing time with a Network Time Protocol (NTP) server, and VirtualCenter synchronizes time with the network windows domain controller, which synchronizes time with the NTP server. Administrative documentation requires that the ESX Server and the VirtualCenter synchronize their clocks periodically, and that this synchronization be performed on the same periodicity as the Network windows domain controller.

6.1.3 Identification & Authentication

Users of the TOE can access the TOE in several different ways. They include the following:

- Accessing the ESX Server from the Service Console. This can be performed remotely by connecting a remote workstation via SSH or directly by using the console physically attached to the ESX Server. The TOE uses Red Hat Linux mechanisms to perform login and password verification for Service Console users, using the username/password database.

- Accessing the ESX Server from a remote workstation using the VMware Management Interface, a web-based a management interface. The VMware Management Interface is part of the TOE and provides identification and authentication mechanisms to perform identification and authentication of MUI users, using the local login and password database.
- Accessing the ESX Server via the VirtualCenter Agent on the ESX Server, from the VirtualCenter via the VirtualCenter Client. Identification and authentication are provided by the same I&A mechanisms as MUI logins using the login and password database.
- Accessing the VirtualCenter via a VirtualCenter Client. Identification and authentication are provided by the underlying operating system of the VirtualCenter. The VirtualCenter Client offers a login screen to the VirtualCenter user, and the VirtualCenter then requests the underlying OS to perform the identification and authentication.

The identification and authentication mechanism for the ESX Server is described in more detail below.

FIA_UAU.1[b] and [c]: Timing of Authentication and FIA_UID.1 [b] and [c] Timing of identification

For login to the TOE from the ESX Server via the local console on the host, to the Service Console, there are no allowed TSF mediated actions prior to the identification and authentication of the user. For login to the TOE from the ESX Server via a remote connection to the Service Console, via the VMware management interface, or via the VirtualCenter Agent, the TOE allows connection establishment prior to identification and authentication. If logging in from the Service Console locally, or logging in remotely after connection establishment, the Red Hat Linux authentication process is invoked. If logging in via the MUI, the vmware-authd process is invoked to perform authentication. Both the Linux process and vmware-authd authenticate users with the local username/password database.

VirtualCenter users who access the ESX Server from the VirtualCenter have already been identified and authenticated to the TOE when they sign into the VirtualCenter. To make changes on a managed ESX server, the permissions are verified on the VirtualCenter. When the ESX Server is first placed under control of the VirtualCenter, the ESX Server root password must be supplied, and a copy of the VirtualCenter Agent is installed on the ESX Server. It requests the creation of the *vpxuser* account, a group account used by all VirtualCenter users who request service on an ESX Server. A unique 32 bit password is created for the *vpxuser* account. This password is stored in encrypted form on the ESX Server, and in the VirtualCenter database in a obfuscated form in the Virtual Center Database. The password is unique for each managed ESX Server. A *vpxuser* group is also created on the ESX Server. The *vpxuser* group is assigned all permissions to all Virtual Machines on the ESX Server, and the *vpxuser* is made the only member of the group. The *vpxuser* account has a VM Administrator role on the ESX Server with permissions for any VM on the ESX server. After identification and authentication, requests for actions on behalf of VirtualCenter users are forwarded to the ESX Server for processing and are treated as any other ESX user requests.

When future connections are requested between the VirtualCenter and the ESX Server, the VirtualCenter supplies the unique *vpxuser* password, and ESX Server's *vmware-authd* verifies the *vpxuser* password to ensure that the connecting server is the managing VirtualCenter for the ESX Server.

In all cases, authentication data is stored on the ESX Server in a shadow file that is hashed using a SHA1 hashing algorithm.

The minimum password requirements on the ESX Server are a password of 8 characters in length, except for the *vpxuser* password, which is 32 bits. This is enforced by Administrator guidance. On the ESX Server, The *vpxuser* password is machine generated by the VirtualCenter and is stored in database after XORing it with a fixed string.

The I&A security function is realized by a probabilistic or permutational mechanism. The I&A security function provides minimum strength of function of SOF-basic. The I&A Function is the only function of this TOE that is reached by a probabilistic or permutational mechanism.

FIA_VC_LOGIN_EXP.1 and from the TOE Environment, FIA_UAU.1 [a] and FIA_UID.1 [a]: VC Login Request, Timing of authentication, and timing of identification.

The VirtualCenter_Client offers a login screen, requesting the VirtualCenter name or IP address, the user name, and the user password. This information is passed to the VirtualCenter, which then requests login from the underlying windows operating system. Users and groups are created through the Windows domain of Active Directory database. Windows verifies the user id and password. If login is valid, the user at the VirtualCenter Client is presented with the VirtualCenter 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.

On the VirtualCenter, minimum password length is 8 characters (note this is consistent with the *vpxuser* password as described above). User password constraints are enforced by setting the minpwd variable to 8. The minimum password length is set and enforced by the underlying windows operating system.

6.1.4 Security Management

The security management functions of the TOE include the following:

Management of security attributes

Static Security Attributes definition

Roles on both the ESX server and the VirtualCenter,

Definition of security management functions.

FMT-MSA.1 [a]: Management of security attributes on the VirtualCenter

The set of VC-roles defined in the VirtualCenter is fixed and cannot be added to, modified, or deleted. The TOE ensures that the ability to modify permission pairs of users on VirtualCenter objects is restricted to a VirtualCenter Administrator, or to a Limited Access User who has the VC-role VirtualCenter Administrator assigned to the VirtualCenter's

Server farm. The Permission pair modification is controlled by the VirtualCenter Access Control Policy. This policy also permits VirtualCenter Administrators to change the explicit permissions associated with a VM through the VirtualCenter Agent resident on the VM's host.

FMT_MSA.1 [b]: Management of security attributes on the ESX Server

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 Linux kernel on which the ESX Server is built. 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.

FMT_MSA.3 [a] Static Attribute definition [VirtualCenter]

The TOE only allows attribute definition to be set by the VirtualCenter administrator, or to a Limited Access User who has the VC-role VirtualCenter Administrator assigned to the VirtualCenter's Server farm. The default value for VC-role is none.

FMT_MSA.3 [b] Static Attribute definition [ESX Server]

The ESX Server defaults for access permission are controlled by the umask setting. The default value can only be changed by an ESX System administrator.

FMT_SMF.1: Security Management Functions

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 (userID 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 on Virtual Machines.

FMT_SMR.1 [a]: Roles [VirtualCenter]

The VirtualCenter and its underlying Windows Operating System provides two distinct roles for the Virtual Center. Thus VirtualCenter roles are provided by the TOE environment. They are VirtualCenter Administrator and Limited Access User. These roles apply to users of the VirtualCenter who log into the VirtualCenter Server via the VirtualCenter Client.

VirtualCenter Administrator: 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.

Limited Access Users are all other users of the VirtualCenter Server. When the user logs in using a username and password, if the username is not a member of the Windows OS administrators group, the user is automatically in the Limited Access Users role.

FMT_SMR.1 [b] [ESX Server]

The ESX server supports the two roles system administrator and VM administrator. These roles apply to users of the ESX Server who log into the ESX Server directly from one of the external user interfaces (CLI or Management Interface), and to requests from a managing VirtualCenter.

System Administrator: The system administrator 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. Requests from the VirtualCenter which supply the ESX Server root password also use the root account, and thus are in this role. Root users have unlimited access in the ESX Server.

VM administrators are administrators of individual VMs, who have logged into the ESX Server using a personal account and password. Requests from the VirtualCenter which do not provide the ESX Server root password use the distinguished account, vpxuser, which also belongs to the VM administrator role. VM administrators do not have access to the root account or the root password. No users on the ESX Server or the VirtualCenter, other than the VirtualCenter administrator, have access to the *vpxuser* passwords in the VirtualCenter database. They are fully subject to the access control rules described in section 6.1.1. Thus, the root group defines both the system administrator and VM administrator roles.

6.1.5 TOE Protection

The TOE protects its data in transmission, as well as a dialog between a remote user and the TOE, via encryption.

The ESX Server provides both OpenSSH and OpenSSL to protect communications between remote users and the ESX Server. The VirtualCenter also provides OpenSSL to protect communications between the VirtualCenter Client and the VirtualCenter, as well as between the VirtualCenter and a VirtualCenter Agent installed on a managed ESX Server.

OpenSSH is used on the ESX Server for remote sessions to the ESX Service Console. The ESX Server's OpenSSH server uses the SSH2 protocol, which supports 3DES, Blowfish, CAST128 or Arcfour encryption. The specific algorithm is negotiated between ESX's OpenSSH server and the user's SSH client. SSH starts encrypting the session after successful negotiation and before authentication takes place. No information, including password or user identification, is passed in the clear.

The VirtualCenter uses OpenSSL to secure communications between a VirtualCenter Client, and between the VirtualCenter and a managed ESX Server. The Client SSL implementation and the Server SSL implementation negotiate a symmetric algorithm, symmetric key and key agreement protocol. Once connected via SSL, The remote user and the Server can now perform identification and authentication if required, and can exchange data at will. OpenSSL supports CAST5, DES, 3DES, IDEA, AES, RC2, RC4, and RC5. The choice of algorithm is negotiated between ESX's OpenSSH server and the SSL client.

The ESX Server uses HTTPS and OpenSSL 0.9.7d for web-based sessions between a remote user and the Management Interface. HTTPS is a secure version of HTTP which uses SSL to provide secure communications. The remote user's workstation must have a browser that has an appropriate SSL client. HTTPS sends data to the ESX server's web server over port 443, which must be SSL-enabled. A remote user must get a digital certificate from a third-party certificate provider that ensures that the web server is valid. This certificate gets installed on the web server, and verifies for a set period of time that that server is a proper secure server.

FPT_ITC.1: Inter-TSF confidentiality during transmission and FPT_ITI.1 [b] and [c]

The TOE protects data for confidentiality and integrity on all transmissions from remote trusted IT products to the TOE. This includes transmissions from remote workstations to the ESX Management Interface (via HTTPS), and transmissions from a remote workstation to the Service Console (Via SSH). A message authentication code (MAC) is generated for the transmitted data, and is transmitted with the data. This provides the ability to detect modifications to transmitted data, thereby protecting its integrity.

.

FPT_ITT.1: Basic internal TSF data transfer protection

The TOE protects data in transmission between the VirtualCenter and the ESX Server for both integrity and confidentiality using SSL. The TOE protects data in transmission between the VirtualCenter Client software installed on a remote host and the VirtualCenter via SSL.. Administrator sessions with the ESX Management Interface are also protected by SSL over an HTTPS session.

FPT_SEP.1: TSF Domain Separation

Domain separation is provided by the mechanisms of the TOE that support controlled access to the TOE via identification and authentication mechanisms and by security mechanisms that further restrict and control access to TOE functions for authorized users of the system.

Furthermore, the three identification and authentication interfaces to the TOE that provides access to TSF internal objects are protected in the following ways:

- The TOE is physically protected by its environment, which protects access to the TOE from the local console.
- The I&A interfaces require login, password, and role enforcement which protects access to the TOE from the local console as well as from remote access.

In addition, the TOE processes, administrative processes to manage the TOE, and authorized user processes are all trusted.

The location of the TOE I&A interfaces are not known to external, unknown and untrusted subjects. While this does not ensure domain separation, it does provide support to it.

FPT_RVM.1*:* Non-Bypassability of the TSP

FPT_RVM.1: The TSP enforcement functions that must be invoked and succeed before the functions within the TSC are allowed to proceed include the following:

- Identification and authentication: these functions ensure that no unauthorized users can gain access to the TOE.

• Access control functions on both the ESX Server and the VirtualCenter are required to be passed prior to access to any operation: these functions ensure that authorized users only gain access to the functions to which they are authorized.

6.1.6 Virtual Machine Separation

The virtual machine separation security function of the TOE is provided by the ESX Server component.

VDS_VMM_EXP.1: ESX Virtual Machine Domain Separation

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 VMkernel 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 communication shared memory, except as described in “copy on write” below. Each VM is assigned memory that belongs exclusively to it.
- Copy on write: 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 space without providing a communication channel between VMs. The VMKernel exercises a “copy on write” policy: if a VM needs to customize read-only memory, a unique and private read-write copy is made for that VM when it attempts to write to the read-only segments.
- File server communication can be allowed or disallowed, based on permissions to specific data.
- Communication between VMs through network connections can be permitted or prevented as desired. These networking mechanisms similar to those used to connect separate physical machines.

Each virtual machine appears to run on its own CPU or set of CPUs, fully isolated from other Virtual Machines with its own registers, translation lookaside buffer, and other control structures. Most instructions are directly executed on the physical CPU, 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 to each virtual machine.

Virtual disks appear to VMs as a SCSI drive connected to a SCSI adapter, while in reality, a wide variety of SCSI, RAID, and Fibre Channel adapters might actually be used in the system. Each VM may define up to four virtual network cards, with their own MAC address and potentially, their own IP address(s). These may be mapped to dedicated network interfaces on the physical server, or may be mapped to virtual network interfaces connected to a single physical network card. ESX server manages both the allocation of resources and the secure isolation of traffic meant for different Virtual Machines even when they are connected to the same physical network card.

Hardware interface components, including device drivers, enable hardware specific service delivery while hiding hardware differences from other parts of the system. Hardware interface consist of vendor specific drivers for networking and storage. These drivers have been modified to work with VMkernel to provide direct management of their resources to the guest Virtual Machines.

There are two options for devices; they can be dedicated to a VM or can be fully virtualized. In the case of a dedicated device, the VMK performs minimal manipulation, such as inspecting parameters and ensuring the associated traffic reaches its correct destination. Fully virtualized devices, the guest VM is given an instance implementation in software. It intercepts all commands, and runs an emulation to produce response. It interprets the VM command to a physical command and returns appropriate responses to the VM.

6.2 Assurance Measures

The TOE Assurance measures are listed below.

[ADMSUP] VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Administrator Guidance Supplement, version 1.0.7, Doc. No._05-695-R-0048,_February 23, 2006.

[ATR]

- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 3.1 v1.0 (Accounts)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 3.2 v1.0 (Common Used Routines)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.1 v1.0 (Reading the Audit Records)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.2 v1.0 (Generating Audit Records)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.3 v1.0 (Ordering the Audit Records)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.4 v1.0 (Communication between the VirtualCenter and remote VC client)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.5 v1.0 (VirtualCenter – ESX Communication is encrypted)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.6 v1.0 (VirtualCenter Clock)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.7 v1.0 (VirtualCenter Permissions)

- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.8 v1.0 (VirtualCenter authentication of Managed ESX Server)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.9 v1.4 (Access Control on Virtual Center)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.10 v1.0 (Identification and Authentication of VirtualCenter)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 4.11 v1.0 (VirtualCenter Revocation of Permission)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 3.1 v1.0 (Test Accounts)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 3.2 v1.0 (root Test VMs)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.1 v1.0 (ESX Access Control: Access to Virtual Machines)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.2 v1.0 (ESX Access Control: Access to ESX Server Configuration Data)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.3 v1.0 (Auditing for startup and shutdown of Syslogs)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.4 v1.0 (Local Login to the Service Console)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.5 v1.0 (Remote Login)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.6 v1.1 (ESX Security Attribute Management)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.7 v1.1 (ESX Manages Virtual Machines)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.8 v1.0 (ESX Revocation of security permissions on ESX Server)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.9 v1.1 (ESX Revocation of security permissions on ESX Server)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.10 v1.0 (ESX Default Security Attributes)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.11 v1.0 (ESX Clock)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.12 v1.0 (SSH Sessions)

- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.13 v1.0 (SSL Sessions)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For ESXTDS 5.14 v1.0 (SSL Sessions)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For VCTDS 5.15 v1.0 (VM Separation: Controlled Sharing.)
- VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Actual Test Results For TSUP 6 Appendix A v1.0 (TestCase for vmkfstools)

[CM] EAL 2 Configuration Management Documentation, VMware ESX Server 2.5.0 and VirtualCenter 1.2.0, Doc. No. 05-695-R-0046, Version: 1.2.2, February 23, 2006.

[DEL] ESX Server 2.5.0 and Virtual Center 1.2.0 Delivery Procedures Document (ADO_DEL), Doc. No. 05-695-R-0006, Version 1.0, February 21, 2006.

[DESIGN] VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Design Documentation and Correspondence, Doc. No. 05-695-R-0047, Version 1.0.7, February 23, 2006.

[ESXADM] VMware ESX 2.5 Administrator Guide Revision: 20041129. Item: ESX-ENG-Q304-002

[ESXINS] VMware ESX Server Installation Guide, Version 2.5, #20041206 ESX-ENG 0304-001, December 2004.

[ESXMANP] VMware ESX Server Manual Pages, extracted from ESX Server 2.5.0 code.

[ESXSAN] ESX Server SAN Configuration Guide, revision 20041217 Version: 2.5, Item: ESX-ENG-Q404-026

[ESXTDS] VMware ESX Server 2.5.0 EAL2 Test Design Specification, Doc. No. 05-695-R-0113, Version 1.7.8, February 23, 2006.

[INSSUP] VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Installation Guidance Supplement, Doc. No. 05-695-R-0008, Version 1.9.3, February 23, 2006.

[OSINS] VMware, Guest Operating System Installation Guide, Revision: 20050912 Item: GSTOS-ENG-Q105-053, May 12, 2005.

[SOF] VMware ESX Server v2.5.0 and VMware VirtualCenter 1.2.0 Strength of Function Analysis, Doc. No. 05-695-R-0049, Version 0.8, February 23, 2006.

[TOE] TOE, TOE Test resources

[TSUP] VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 Test Documentation Supplement, Doc. No. 05-695-R-0114, Version 1.0.5, February 23, 2006.

[VCADM] VMware VirtualCenter User's Manual Version 1.2, Revision 20041118, Item No. VC-ENG-Q404-037, December 2, 2004

[VCTDS] VMware VirtualCenter 1.2.0 EAL2 Test Design Specification, Doc. No. 05-695-R-0115, Version 1.6, February 23, 2006.

[VLA] VMware ESX Server 2.5.0 and VirtualCenter 1.2.0 Common Criteria Vulnerability Analysis, Doc No 05-695-R-0075, V0.9, February 15, 2006.

The following table identifies assurance measures with assurance requirements. Note that there is no assurance measure identified with the requirement ADM_USR.1, as there are no administrative users of the TOE, and as such, there is no requirement for user guidance documentation.

Table 6-2: TOE Assurance Measures

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1[8]	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
ADMSUP			X	X	X	X	X						
ATR										X			
CM	X												
DEL		X											
DESIGN				X	X	X							
ESXADM			X	X	X	X	X						
ESXINS			X	X	X	X	X						
ESXMANP			X	X	X	X	X						
ESXSAN			X										
ESXTDS										X			
INSSUP			X	X	X	X	X						
SOF												X	
TOE											X		
TSUP									X	X			
VCADM			X	X	X	X	X						
VCTDS										X			

[8] Note that there are no administrative users of the TOE, and as such, ADM_USR.1 is vacuously satisfied as per PD 0106.

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1[8]	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
VLA													X

6.2.1 EAL Justification

EAL 2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

VMware has chosen to pursue a Common Criteria evaluation because of the government customer requirements that are mandated by NSTISSC Policy 11. This policy requires a Common Criteria certification for all products to be used within systems used for entering, processing, storing, displaying, or transmitting national security information.

VMware has specifically chosen an EAL2 evaluation assurance level to meet the requirements mandated by the DoD and Air Force divisions of the government in accordance with the US DoD NSTISSP #11 Interpretation and the USAF CIO Memorandum.

6.3 TOE Summary Specification Rationale

The justification that the security functions meet the SFRs is included in section 6.1. These rationales are summarized in the following table.

	Access Control	Auditing	I&A	Security Mgmt	TOE Protection	VM Separation
FAU_GEN_EXP.1 [a]		X				
FAU_GEN.1 [b]		X				
FAU_SAR.1 [a] and [b]		X				
FAU_SAR_EXP.3		X				

	Access Control	Auditing	I&A	Security Mgmt	TOE Protection	VM Separation
FDP_ACC.1 [a] and [b]	X					
FDP_ACF.1 [a] and [b]	X					
FIA_UAU.1 [b] and [c]			X			
FIA_UID.1 [b] and [c]			X			
FMT_MSA.1 [a] and [b]				X		
FMT_MSA.3 [a] and [b]				X		
FMT_SMF.1		X				
FMT_SMR.1 [a] *				X		
FMT_SMR.1 [b]				X		
FPT_ITC.1					X	
FPT_ITI.1 [b], [c]					X	
FPT_ITT.1					X	
FPT_RVM.1					X	
FPT_SEP.1					X	
VDS_VMM_EXP.1						X
FIA_VC_LOGIN_EXP.1			X			
FIA_UAU.1 [a]*			X			
FIA_UID.1 [a]*			X			
FPT_STM.1*		X				

Table 6-3: Mapping of TOE SFRs to TOE Security Functions

* Requirements on the environment

6.3.1 Rationale that Assurance Measures meet the Security Assurance Requirements

Assurance Requirements	Assurance Measures	Rationale

Assurance Requirements	Assurance Measures	Rationale
ACM_CAP.2.1D	CM	The configuration items that comprise the TOE are specified in the document listed here.
ADO_DEL.1.1D	DEL	Procedures defining the delivery method of the TOE to the consumer are provided in the document listed here.
ADO_IGS.1.1D	ADMSUP ESXADM ESXINS ESXMANP ESXSAN INSSUP VCADM	The steps necessary for secure installation, generation, and start-up of the TOE are described within the documents listed here.
ADV_FSP.1.1D, ADV_HLD.1D, ADV_RCR.1D	DESIGN ESXINS INSSUP VCADM ESXADM ESXMANP ADMSUP	The Design document includes the functional specification, the high level design, and the correspondence representation. The functional specification describes the TSF and the external interface to the TOE. The high-level design describes the TOE subsystems and identifies their interfaces. The correspondence provides or identifies mappings between all adjacent pairs of available TSF representations, from the TSF summary specification through the high level design.
AGD_ADM.1.1D	ADMSUP ESXADM ESXINS ESXMANP INSSUP VCADM	Administrative guidance provides the TOE administrators with detailed, accurate information of how to administer the TOE in a secure manner. Documents listed here satisfy these requirements.

Assurance Requirements	Assurance Measures	Rationale
AGD_USR.1.1D		Note that there are no administrative users of the TOE, and as such, ADM_USR.1 is vacuously satisfied as per PD 0106.
ATE_COV.1.1D	TSUP	Testing coverage shows the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. The testing coverage is provided within the testing procedure document as it is listed here.
ATE_FUN.1.1D	ESXTDS TSUP VCTDS ATR	Functional testing of the TOE involves providing a test plan, test procedure descriptions, expected test results and actual test results.
ATE_IND.2.1D	VMware ESX Server 2.5.0 and VMware VirtualCenter 1.2.0 software	Independent testing requires VMware to provide the TOE suitable for testing and VMware has fulfilled this requirement.
AVA_SOF.1.1D	SOF	Strength of function analysis requires the developer to provide an analysis of the strength of function claimed in this ST. However, no strength of function claim has been made and is therefore, not applicable.

Assurance Requirements	Assurance Measures	Rationale
AVA_VLA.1.1D	VLA	A vulnerability analysis of the TOE involves describing the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP as to ensure that all obvious vulnerabilities have been addressed. The document listed here satisfies these requirements.

Table 6-4 Rationale for Assurance Measures Satisfying SARs

7. PP Claims

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

7.1 PP Reference

NONE

7.2 PP Tailoring

NONE

7.3 PP Additions

NONE

8. Rationale

8.1 Rationale for Security Objectives

The rational for the security objectives is found in section 4.3 Security Objectives Rationale, including sections 4.3.1 through 4.3.4.

8.2 Rationale for Security Functional Requirements

The rationale for the security functional requirements is found in section 5 of this document.

8.3 Rationale for Security Assurance Requirements

The security assurance rationale is found in section 5 of this document.

8.4 TOE Security Functions Rationale

The TOE Summary specification rationale is found in section 6 of this document.

8.5 TOE Assurance Measures Rationale

The TOE assurance measures rationale is found in section 6 of this document.

8.6 Protection Profile Rationale

The Protection Profile rationale is found in section 7 of this document.

8.7 Rationale for Strength of Function

The Strength of Functions rationale is found in section **5.6.4**.