VMware Inc
ESX Server 3.0.2 and VirtualCenter 2.0.2

Security Target

Evaluation Assurance Level: EAL4+
Document Version: 0.7

Prepared for:

VMware Inc
3401 Hillview Ave
Palo Alto, CA 94304
Phone: (650) 475-5000

http://www.vmware.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2006-12-14	Adam O'Brien	Initial draft.
0.2	2007-12-22	Nathan Lee	Updates based on PETR.
0.3	2008-03-04	Nathan Lee	Corrected SPM reference.
0.4	2008-03-08	Nathan Lee	Updated A.PHYSCL based on feedback from lab.
0.5	2008-03-20	Nathan Lee	Updated Table 12 based on lab OR.
0.6	2008-04-03	Nathan Lee	Corrected typo.
0.7	2008-04-23	Nathan Lee	Removed “Confidential and Proprietary” marking and packaged for public release.

Table of Contents

1 SECURITY TARGET INTRODUCTION 5
1.1 PURPOSE 5
1.2 SECURITY TARGET, TOE AND COMMON CRITERIA (CC) IDENTIFICATION AND CONFORMANCE 5
1.3 CONVENTIONS, ACRONYMS, AND TERMINOLOGY 6
1.3.1 Conventions 6
1.3.2 Acronyms and Terminology 6

2 TOE DESCRIPTION 7
2.1 PRODUCT TYPE 7
2.2 PRODUCT DESCRIPTION 7
2.2.1 VirtualCenter 9
2.2.2 ESX Server 9
2.3 TOE BOUNDARIES AND SCOPE 10
2.3.1 Physical Boundary 10
2.3.2 Logical Boundary 13
2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE 14

3 SECURITY ENVIRONMENT 16
3.1 ASSUMPTIONS 16
3.2 THREATS TO SECURITY 16
3.3 ORGANIZATIONAL SECURITY POLICIES 16

4 SECURITY OBJECTIVES 17
4.1 SECURITY OBJECTIVES FOR THE TOE 17
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 17
4.2.1 IT Security Objectives 17
4.2.2 Non-IT Security Objectives 17

5 SECURITY REQUIREMENTS 18
5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 18
5.1.1 Class FAU: Security Audit 19
5.1.2 Class FDP: User Data Protection 21
5.1.3 Class FIA: Identification and Authentication 24
5.1.4 Class FMT: Security Management 25
5.1.5 Class FPT: Protection of the TSF 28
5.1.6 Class VDS: Virtual Machine Domain Separation 29
5.2 SECURITY FUNCTIONAL REQUIREMENTS ON THE IT ENVIRONMENT 30
5.3 ASSURANCE REQUIREMENTS 32

6 TOE SUMMARY SPECIFICATION 33
6.1 TOE SECURITY FUNCTIONS 33
6.1.1 Security Audit 33
6.1.2 User Data Protection 34
6.1.3 Identification and Authentication 36
6.1.4 Security Management 36
6.1.5 Protection of the TSF 37
6.1.6 Virtual Machine Domain Separation 37
6.2 TOE SECURITY ASSURANCE MEASURES 38
6.2.1 Assurance Documentation 39

7 PROTECTION PROFILE CLAIMS 41
7.1 PROTECTION PROFILE REFERENCE 41

8 RATIONALE 42
8.1 SECURITY OBJECTIVES RATIONALE 42

8.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE 44
8.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE..46
8.4 DEPENDENCY RATIONALE 46
8.5 TOE SUMMARY SPECIFICATION RATIONALE..47
8.5.1 TOE Summary Specification Rationale for the Security Functional Requirements 47
8.5.2 TOE Summary Specification Rationale for the Security Assurance Requirements..............................48
8.6 STRENGTH OF FUNCTION 49

9 ACRONYMS..50

Table of Figures

FIGURE 1 - DEPLOYMENT CONFIGURATION OF THE TOE..7
FIGURE 2 - PHYSICAL TOE BOUNDARY..8

Table of Tables

TABLE 1 - ST, TOE, AND CC IDENTIFICATION AND CONFORMANCE 5
TABLE 2 - COMPONENTS OF THE TOE 10
TABLE 3 - TOE SECURITY FUNCTIONAL REQUIREMENTS..18
TABLE 4 - AUDITABLE EVENTS ON THE ESX SERVER 19
TABLE 5 - FMT_MSA.1(B) - SECURITY ATTRIBUTES, ACTIONS, AND ROLES 25
TABLE 6 - FMT_MSA.3(B) - ROLES AND OBJECTS/INFORMATION..26
TABLE 7 – ASSURANCE REQUIREMENTS..32
TABLE 8 – MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS...............................33
TABLE 9 – AUDIT RECORD CONTENTS 34
TABLE 10 - ASSURANCE MEASURES MAPPING TO TOE SECURITY ASSURANCE REQUIREMENTS.................................38
TABLE 11 - RELATIONSHIP OF SECURITY THREATS TO OBJECTIVES 42
TABLE 12 - RELATIONSHIP OF SECURITY REQUIREMENTS TO OBJECTIVES..44
TABLE 13 - FUNCTIONAL REQUIREMENTS DEPENDENCIES 47
TABLE 14 - MAPPING OF SECURITY FUNCTIONAL REQUIREMENTS TO TOE SECURITY FUNCTIONS 48
TABLE 15 - ACRONYMS 50

1 Security Target Introduction

This section identifies the Security Target (ST), the Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the ESX Server 3.0.2 and VirtualCenter 2.0.2, and will hereafter be referred to as the TOE throughout this document. The TOE is a system which can provide multiple virtual machines (VM's) on a hardware platform and allows the management of these virtual machines.

1.1 Purpose

This ST contains the following sections:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile (PP) claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the consistency, completeness, and suitability of the security objectives, requirements, and the TOE summary specifications.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and Common Criteria (CC) Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	VMware ESX Server 3.0.2 and VirtualCenter 2.0.2 Security Target
ST Version	Version 0.7
Author	Corsec Security, Inc. Adam O'Brien and Nathan Lee
TOE Identification	ESX Server 3.0.2 and VirtualCenter 2.0.2
Common Criteria Identification and Conformance	Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CC Evaluation Methodology as of December 14, 2006 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level (EAL)	EAL4+

1.3 Conventions, Acronyms, and Terminology

1.3.1 Conventions

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

The CC allows for several operations to be performed on security requirements: assignment, refinement, selection and iteration. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [<u>*underlined italicized text within brackets*</u>].
- Refinements are identified using **bold text**.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

1.3.2 Acronyms and Terminology

The acronyms and terms used within this ST are described in Section 9 – “Acronyms.”

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the capabilities and security functions of the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

This evaluation is of the VMware ESX Server 3.0.2 and VirtualCenter 2.0.2. The ESX Server is a platform for hosting virtual machines. It runs directly on hardware and abstracts the resources to provide multiple virtual machines. VirtualCenter is a centralized management tool for one or more ESX Servers.

Figure 1 below shows the details of the deployment configuration of the TOE:

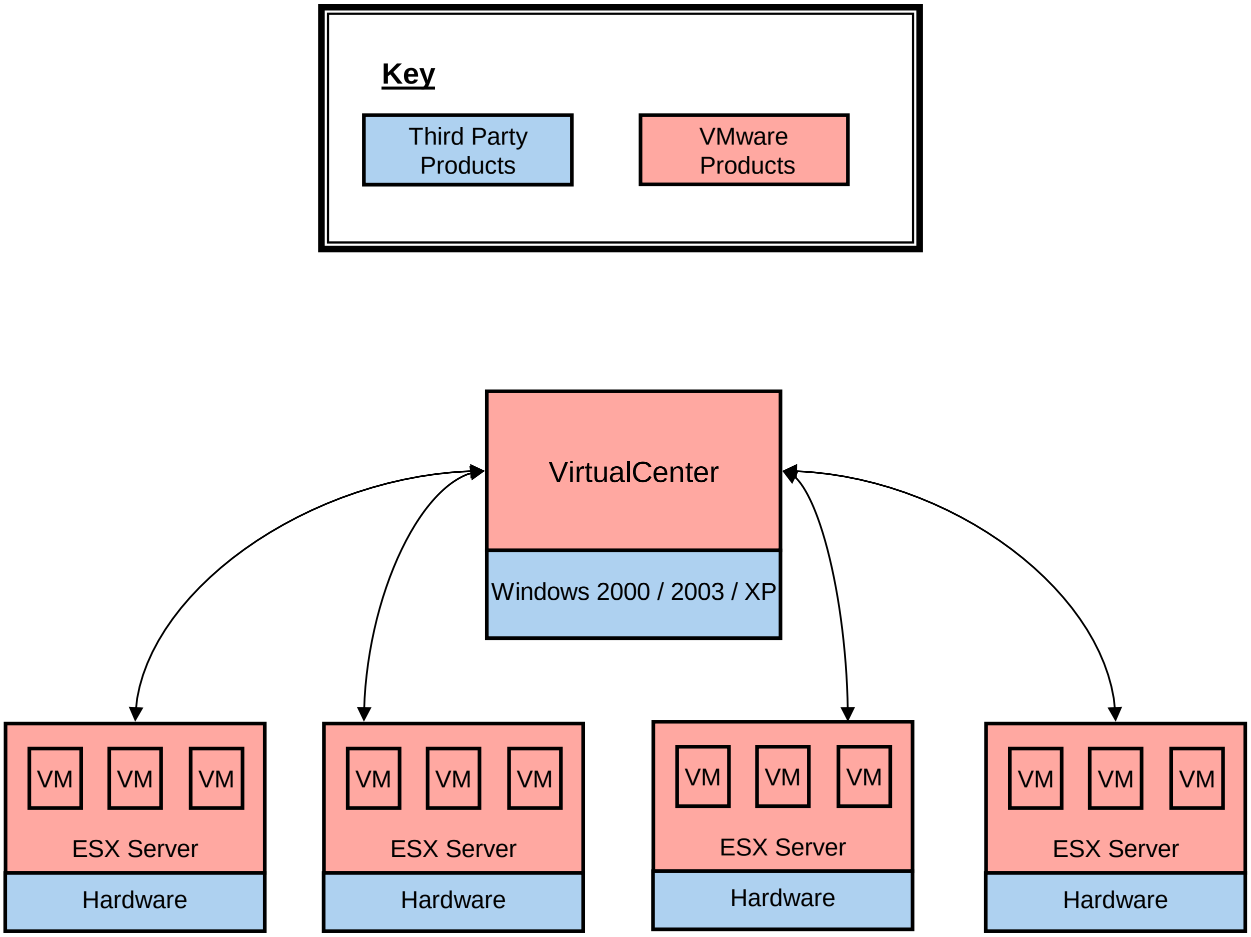
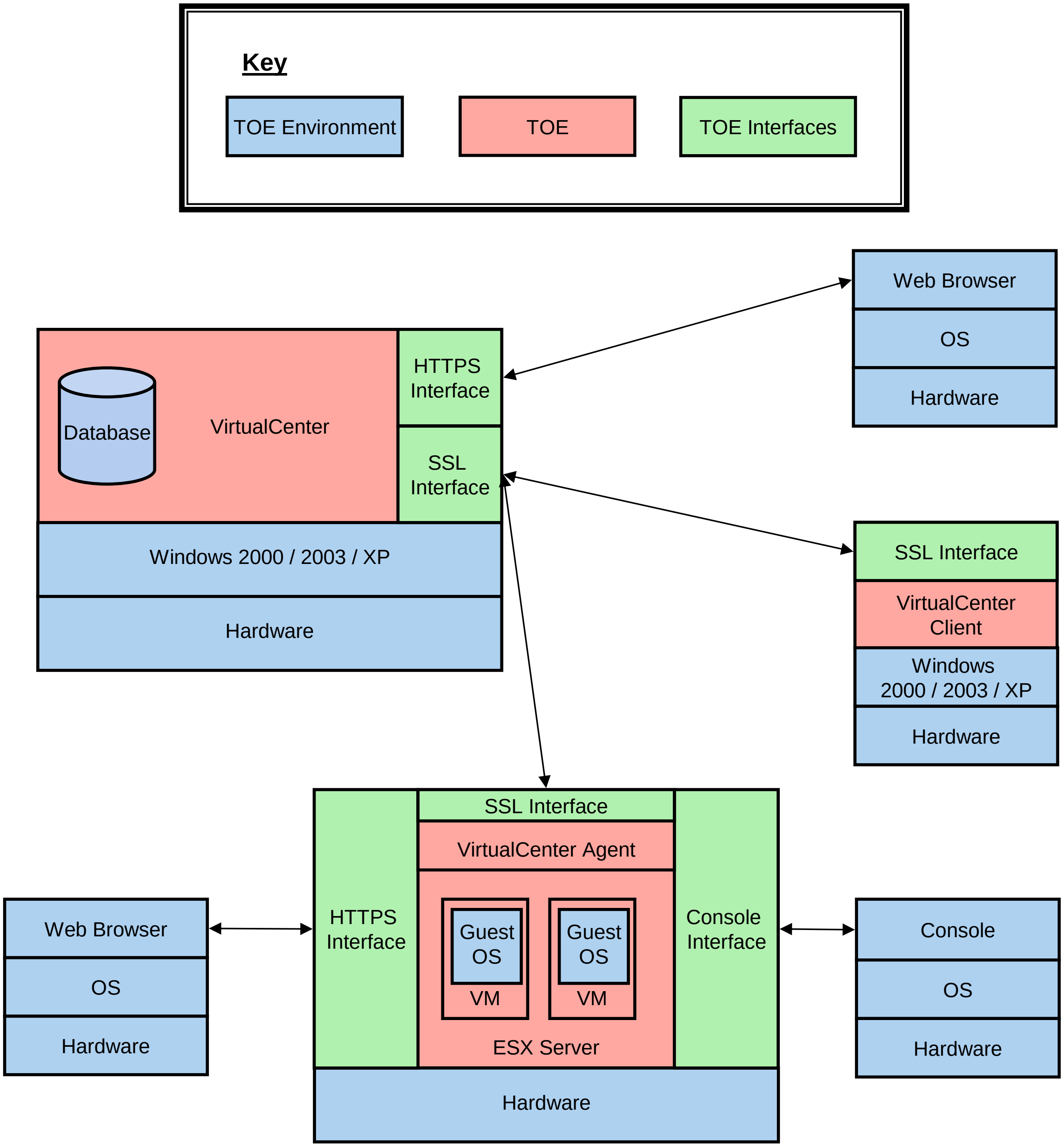


Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

The ESX Server is a virtualization layer that runs directly on hardware, allowing multiple virtual machines to be hosted on one physical server. The ESX Server abstracts processor, memory, storage, and networking resources to create virtual machines which can run a wide variety of different operating systems (OS's). Each virtual machine acts as a physically separated host and only communicates with other virtual machines using networking protocols. The VirtualCenter acts as a management console, deploying, monitoring, and managing virtual machines that are distributed across multiple hosts running ESX Server software.

Figure 2 - Physical TOE Boundary



2.2.1 VirtualCenter

The VirtualCenter allows centralized management of ESX Servers. Through VirtualCenter an administrator can configure an ESX Server which includes viewing and managing the networking, data storage and security settings. The VirtualCenter also allows the provisioning of virtual machines on the ESX Server. For example, virtual machines can be created, configured, cloned and relocated. VirtualCenter communicates with the ESX Server via the VirtualCenter agent located on the ESX Server. The confidentiality and integrity of this communication is protected using Secure Sockets Layer (SSL). SSL is provided using OpenSSL embedded within VirtualCenter. VirtualCenter includes a Network Time Protocol (NTP) Client but this feature is not used in the evaluated configuration.

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

- VMotion – enables the migration of a running VM from one host to the other
- Distributed Resource Scheduler - automatically migrates VM's in a cluster to rebalance work load
- VMware HA – enables quick restart of virtual machines on a different physical server within a cluster automatically if the hosting server fails.

2.2.1.1 VirtualCenter Access Methods

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

2.2.1.1.1 Virtual Infrastructure Client

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

2.2.1.1.2 Virtual Infrastructure Web Access

Users connect via the Virtual Infrastructure Web Access client through a web browser. The VI Web Access client provides a subset of the functionality provided by the Virtual Infrastructure Client. The VI Web Access client interface is provided by a Tomcat servlet engine in the TOE. Communication with the web browser is protected using HyperText Transfer Protocol over SSL (HTTPS).

2.2.1.2 VirtualCenter Database

The VirtualCenter database contains information about the configuration and status of one or more ESX Server hosts and each of the host's virtual machines. It also stores management information for the ESX Server, including the following:

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

2.2.2 ESX Server

The ESX Server is a virtualization layer that runs directly on hardware, allowing multiple virtual machines to be hosted on one physical server. Virtual machines are the containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. Virtual machine isolation is imperceptible to the guest operating system. Even a user with system administrator privileges on a virtual machine's guest operating system cannot breach this layer of isolation to access another virtual machine without privileges explicitly granted by the ESX Server system administrator from the console interface. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance. The optional virtual Symmetric Multi-Processing feature enables a single virtual machine to use multiple physical processors simultaneously.

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

ESX Server can be installed in three distinct configurations.

- Configuration 1: Local Storage Only: In the first configuration, the ESX Server 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/virtual machines on Storage Area Network (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 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.

2.2.2.1 VirtualCenter Agent

The VirtualCenter Agent forwards requests for services from VirtualCenter users, when the ESX Server is under the management of a VirtualCenter. ESX Servers can only be managed by a single VirtualCenter. The requests from the VirtualCenter Agents are handled by the ESX Server daemon in a manner similar to requests from users at the console or browser interface.

2.3 TOE Boundaries and Scope

This section will address what physical and logical components of the TOE are included in evaluation.

2.3.1 Physical Boundary

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment. Table 2 indicates which elements of the product are included in the TOE boundary.

Table 2 - Components of the TOE

Component	TOE	TOE Environment
VirtualCenter 2.0.2 Software (includes , VirtualCenter Server, VirtualCenter agent, and Virtual Infrastructure Client, VMotion, Distributed Resource Scheduler, VMware HA, Tomcat, OpenSSL)	✓	
ESX Server 3.0.2 Software (includes virtual SMP, Console OS, ESX management server, apache-tomcat, jakarta-tomcat, OpenSSL, OpenSSH)	✓	
NTP Client on Virtual Infrastructure Client		✓
NTP Client on ESX Server		✓
NTP Server available to ESX Server and VirtualCenter		✓

Component	TOE	TOE Environment
ESX Server hardware (processor and adapters) including blade servers		✓
Storage Area Network hardware and software to be used with ESX Server in configuration 2 and 3.		✓
VirtualCenter Hardware, operating system, and database.		✓
Virtual Infrastructure Client hardware and operating system		✓
Operating systems and applications for VM's		✓
Hardware, OS, and software (as identified in the previous sections) for remote workstations		✓

2.3.1.1 Requirement for the TOE Environment

The VirtualCenter Server hardware must meet the following requirements:

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

The VirtualCenter Server supports the following operating systems:

- Windows 2000 Server SP4 with Update Rollup 1
- Windows XP Pro (at any SP level)
- Windows 2003 (all releases except 64 bit)

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

The VirtualCenter Server supports the following databases:

- Microsoft SQL Server 2000 (SP 4 only)
- Oracle 9iR2, 10gR1 (versions 10.1.0.3 and higher only), or 10gR2

The Virtual Infrastructure Client hardware must meet the following requirements:

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

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

- Windows 2000 Pro SP4
- Windows 2000 Server SP4
- Windows XP Pro (at any SP level)
- Windows 2003 (all releases except 64 bit)

The VI Web Access client is designed for these browsers:

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

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

The ESX Server hardware must meet the following requirements:

- 2 1500 MHz Intel Xeon and later, or AMD Opteron (32 bit mode) or 1 1500 MHz Intel Viiv or AMD A64 x2 dual core processors
- 1GB RAM minimum
- One or more Ethernet controllers. Supported controllers include:
  - Broadcom NetXtreme 570x Gigabit controllers
  - Intel PRO/100 adapters

2.3.2 Logical Boundary

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functions (TSF)
- Virtual Machine Domain Separation

2.3.2.1 Security Audit

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

The VirtualCenter provides the capability to review its audit records by reviewing the event logs stored on the VirtualCenter Database. Only a VirtualCenter Administrator can view all the event logs. Audit events are viewed through web pages under the event tab for each organizational object. 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.

2.3.2.2 User Data Protection

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

Note that there are no non-administrative users of the TOE. VM users (individuals who access the guest operating system and applications within a virtual machine) are outside the scope of the TOE and are not discussed any further here.

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

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

2.3.2.3 Identification and Authentication

When a user logs into the ESX Server a user name and password are requested before any access is given. These authentication credentials are compared with the authentication credentials stored on the ESX Server in a shadow file, where the password is hashed using Secure Hash Algorithm-1 (SHA-1). If the authentication credentials are valid, access to the system is provided, with the privileges appropriate to the role assigned to that user. If the credentials are not valid the user is presented with another chance to provide valid credentials.

When a user logs into VirtualCenter they are presented with a login screen, requesting the VirtualCenter name or IP address, the user name, and the user password. The user information is passed to the underlying Windows operating system which verifies the user identity and password. If login is valid, the user at the Virtual Infrastructure Client is presented with the Virtual Infrastructure Client interface denoting a successful login. If login is invalid, a message is displayed, and the login window remains available for the user to retry.

2.3.2.4 Security Management

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

The TOE ensures that the ability to modify permissions of users on ESX objects is restricted to system administrators. The capability to modify permissions of users on objects is provided by functions of the ESX Server that are inherited from the customized Linux kernel on which the ESX Server is built.

2.3.2.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that physical connections made to the TOE remain intact and unmodified. The TOE protects information as it is transmitted between remote components of the TOE by encrypting the information using SSL.

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

2.3.2.6 Virtual Machine Domain Separation

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

The ESX Server provides an idealized hardware environment and virtualization of underlying physical resources. Each virtual machine runs its own operating system and applications: they cannot communicate to each other in unauthorized ways, nor can they leak data.

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

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

The following features of the system are excluded from the evaluation.

- Simple network management Protocol (SNMP), File Transfer Protocol (FTP), Telnet
- The use of any authentication method on ESX other than the local password database
- VMware Software Development Kit (SDK) tools
- The procfs interface on the ESX Server Service Console
- VMware Scripting Application Programming Interface (API) on the ESX Server
- VMware Consolidated Backup

.

3 Security Environment

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

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

3.1 Assumptions

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

A.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.

A.PHYSCL The ESX Server and VirtualCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access. The Virtual Infrastructure Client component will only connect to the server via the protected management network..

3.2 Threats to Security

This section identifies the threats to the IT assets against which the TOE must protect. The threat agents are individuals who are not authorized to use the TOE or the protected network. The threat agents are assumed to:

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

The following threats are to be addressed by the TOE:

T.VM A process running on one virtual machine might compromise the security of processes running on other virtual machines.

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

T.PRIVIL An unauthorized individual may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

3.3 Organizational Security Policies

There are no Organization Security Policies.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, can exercise such control.

O.AUDIT The TOE must gather audit records of actions on the TOE which may be indicative of misuse.

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.SECURE The TOE must ensure the confidentiality and integrity of all System data as it passes between remote components of the TOE.

O.VM The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

OE.IDAUTH The IT Environment will provide reliable verification of the Virtual Infrastructure Client user credentials.

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

OE.SEP The IT Environment will protect the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. They will be satisfied through application of procedural or administrative measures.

NOE.NOEVIL Users are non-hostile, appropriately trained, and follow all user guidance.

NOE.PHYSCL The ESX Server and VirtualCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access. The Virtual Infrastructure Client component will only connect to the server via the protected management network.

5 Security Requirements

This section defines the Security Functional Requirements and Security Assurance Requirements met by the TOE as well as Security Functional Requirements met by the TOE environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 3 identifies all SFRs implemented by the TOE.

Table 3 - TOE Security Functional Requirements

SFR	Description	Refinement
FAU_GEN.1	Audit Data Generation	
FAU_SAR.1	Audit review	
FDP_ACC.1(a)	Subset access control (VirtualCenter)	
FDP_ACC.1(b)	Subset access control (ESX Server)	
FDP_ACF.1(a)	Security attribute based access control (VirtualCenter)	✓
FDP_ACF.1(b)	Security attribute based access control (ESX Server)	✓
FIA_UAU.1(a)	Timing of authentication (ESX Server)	✓
FIA_UID.1(a)	Timing of identification (ESX Server)	✓
FIA_VC_LOGIN_EXP.1	VirtualCenter User Login Request	
FMT_MSA.1(a)	Management of security attributes (VirtualCenter)	
FMT_MSA.1(b)	Management of security attributes (ESX Server)	
FMT_MSA.3(a)	Static attribute initialisation (VirtualCenter)	✓
FMT_MSA.3(b)	Static attribute initialisation (ESX Server)	✓
FMT_SMF.1	Specification of Management Functions	
FMT_SMR.1(b)	Security roles (ESX Server)	✓
FPT_ITT.1	Basic internal TSF data transfer protection	
FPT_RVM.1	Non-bypassability of the TOE Security Policy (TSP)	
FPT_SEP.1(a)	TSF domain separation	
VDS_VMM_EXP.1	ESX virtual machine Domain Separation	

Section 5.1 contains the functional components from the Common Criteria Part 2 and explicitly stated requirements, with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

a) Start-up and shutdown of the audit functions;

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

c) [*The events specified in Column 1 ("Audit Event") of* Table 4].

FAU_GEN.1.2

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the information specified in Column 2 ("Additional Collected Information") of* Table 4].

Dependencies: FPT_STM.1 Reliable time stamps

Table 4 - Auditable Events on the ESX Server

Audit Event	*Additional Collected Information*
Startup and shutdown of the Auditing functions	*<none>*
All management operations performed on virtual machines[1]	*virtual machine*
All changes to the configuration of alarms or scheduled task	*The alarm or scheduled task*
All use of the identification and authentication mechanisms	*The user identity if provided*

FAU_SAR.1 Audit review

Hierarchical to: No other components.

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

FAU_SAR.1.1

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

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 Class FDP: User Data Protection

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

Hierarchical to: No other components.

FDP_ACC.1.1(a)

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

a. Subjects: processes acting on behalf of VirtualCenter users

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

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

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1(b) Subset access control (ESX Server)

Hierarchical to: No other components.

FDP_ACC.1.1(b)

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

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

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

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

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1(a) Security attribute based access control (VirtualCenter)

Hierarchical to: No other components.

FDP_ACF.1.1(a)

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

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

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

c. Objects: virtual machine definition and configuration files; inventory data for virtual machines, folders, datacenters, clusters, resource pools, networks, datastores, templates, and hosts; scheduled events, alarms, tasks, and templates *d. Object attributes: A set of permission pairs (User identity or User Group, VC-role)*].

FDP_ACF.1.2(a)

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

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

2. Access to perform a given activity on an object is allowed on the VirtualCenter if there is a permission pair associated with the object having a user identity component that matches the user identity of the subject, and a VC-role allowing the activity requested by the subject.

3. Access to perform a given activity on an object is allowed on the VirtualCenter if there is a permission pair associated with the object having a user group component that matches a group to which the subject belongs, and a VC-role allowing the activity requested by the subject.

4. If the user of the subject does not match the user identity of any permission pair associated with the object, or the User identity is not a member of any group of any permission pair associated with the object, or the VC-role of any such matching permission pair does not permit the activity requested by the user, then access is denied[2]].

FDP_ACF.1.3(a)

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

FDP_ACF.1.4(a)

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

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

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

Hierarchical to: No other components.

FDP_ACF.1.1(b)

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

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

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

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

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

d. Object attributes: User identity of object owner, object group, read/write/execute permissions for owner/group/other].

FDP_ACF.1.2(b)

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

1. Access is granted if the ESX 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[3] *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 authorise access of subjects to objects **or operations of the ESX Server** based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(b)

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

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

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

5.1.3 Class FIA: Identification and Authentication

FIA_UAU.1(a) Timing of authentication (ESX Server)

Hierarchical to: No other components.

FIA_UAU.1.1(a)

The TSF shall allow [*no other actions*] on behalf of the user **of the ESX Server** to be performed before the user is authenticated.

FIA_UAU.1.2(a)

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1(a) Timing of identification (ESX Server)

Hierarchical to: No other components.

FIA_UID.1.1(a)

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

FIA_UID.1.2(a)

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

Dependencies: No dependencies

FIA_VC_LOGIN_EXP.1 VirtualCenter 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.

5.1.4 Class FMT: Security Management

FMT_MSA.1(a) Management of security attributes (VirtualCenter)

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*VirtualCenter Access Control Policy*] to restrict the ability to [*change_default, modify, delete*] the security attributes [*permission pairs for VirtualCenter users and all objects in the VirtualCenter*] to [*VirtualCenter Administrators and Administrator defined roles*].

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

FMT_MSA.1(b) Management of security attributes (ESX Server)

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*ESX Server Access Control Policy*] to restrict the ability to [*modify, delete, [add]*] the security attributes [*For ESX Server users: user id; user groups; For ESX Server objects: object owner; object group; object read, write, and execute permissions of security attributes*] to [*the as described in Table 5*].

Table 5 - FMT_MSA.1(b) - Security Attributes, Actions, and Roles

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

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

FMT_MSA.3(a) Static attribute initialisation (VirtualCenter)

Hierarchical to: No other components.

FMT_MSA.3.1(a)

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

FMT_MSA.3.2(a)

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

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

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

Hierarchical to: No other components.

FMT_MSA.3.1(b)

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

FMT_MSA.3.2(b)

The TSF shall allow the [*System Administrator and VM administrator(s)*] to specify alternative initial values to override the default values when an object or information is created **on the ESX Server, as described in Table 6**.

Table 6 - FMT_MSA.3(b) - Roles and Objects/Information

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

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

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

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

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

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

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

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

6. Power operations on a virtual machine].

Dependencies: No Dependencies

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

Hierarchical to: No other components.

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.

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

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

Dependencies: No dependencies

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC[4] is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1(a) TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1(a)

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(a)

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

Dependencies: No dependencies

[4] TOE Scope of Control (TSC)

5.1.6 Class VDS: Virtual Machine Domain Separation

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 VM's in the TSC.

5.2 Security Functional Requirements on the IT Environment

The TOE has the following security requirements for its IT environment. The stated Security Functional Requirement on the IT Environment of the TOE presented in this section has been drawn from Part 2 of CC Version 2.3 and hence conformant to CC Version 2.2 Part 2.

SFR	Description
FIA_UAU.1(b)	Timing of authentication (VirtualCenter)
FIA_UID.1(b)	Timing of identification (VirtualCenter)
FMT_SMR.1(a)	Security roles (VirtualCenter)
FPT_SEP.1(b)	TSF domain separation
FPT_STM.1	Reliable time stamps

FIA_UAU.1(b) Timing of authentication (VirtualCenter)

Hierarchical to: No other components.

FIA_UAU.1.1(b)

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(b)

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.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1(b) Timing of identification (VirtualCenter)

Hierarchical to: No other components.

FIA_UID.1.1(b)

The **IT Environment** shall allow [*no other actions*] on behalf of the user **of the VirtualCenter** to be performed before the user is identified.

FIA_UID.1.2(b)

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.

Dependencies: No dependencies

FMT_SMR.1(a) Security roles (VirtualCenter)

Hierarchical to: No other components.

FMT_SMR.1.1(a)

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

FMT_SMR.1.2(a)

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

Dependencies: FIA_UID.1 Timing of identification

FPT_SEP.1(b) TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1(b)

The **TOE environment** shall maintain a security domain for **the TOE's** execution that protects **the TOE** from interference and tampering by untrusted subjects.

FPT_SEP.1.2(b)

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

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

The **TOE environment** shall be able to provide reliable time stamps for **the use of the TOE**.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL4 augmented with ALC_FLR.1. Table 7 – Assurance Requirements summarizes the requirements.

Table 7 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
Class ADO: Delivery and operation	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_FLR.1 Basic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

6 TOE Summary Specification

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

6.1 TOE Security Functions

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

Table 8 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1(a)	Subset access control (VirtualCenter)
	FDP_ACC.1(b)	Subset access control (ESX Server)
	FDP_ACF.1(a)	Security attribute based access control (VirtualCenter)
	FDP_ACF.1(b)	Security attribute based access control (ESX Server)
Identification and Authentication	FIA_UAU.1(a)	Timing of authentication (ESX Server)
	FIA_UID.1(a)	Timing of identification (ESX Server)
	FIA_VC_LOGIN_EXP.1	VirtualCenter User Login Request
Security Management	FMT_MSA.1(a)	Management of security attributes (VirtualCenter)
	FMT_MSA.1(b)	Management of security attributes (ESX Server)
	FMT_MSA.3(a)	Static attribute initialisation (VirtualCenter)
	FMT_MSA.3(b)	Static attribute initialisation (ESX Server)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1(b)	Security roles (ESX Server)
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1(a)	TSF domain separation
Virtual Machine Domain Separation	VDS_VMM_EXP.1	ESX virtual machine Domain Separation

6.1.1 Security Audit

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

The TOE audit records contain the following information:

Table 9 – Audit Record Contents

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

Each audit record generated includes the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event, and virtual machine, scheduled task, or alarm identity if applicable. For invalid identification attempts, the identity of the user name supplied is also recorded. These audit records are stored as events, and are managed by the VirtualCenter Access Control Policy. They are stored on the VirtualCenter Database.

The VirtualCenter provides the capability to review its audit records by reviewing the event logs stored on the VirtualCenter Database. Event logs are associated with objects, and access to the event logs is determined by access to the object associated with the event log. Users who can access a particular VM or VM Group can access the event logs for that organizational grouping. Audit events are viewed through web pages under the event tab for each organizational object.

The ESX Server audit records are stored in a flat file on the Service Console of the ESX Server. 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.

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

6.1.2 User Data Protection

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

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.

The VirtualCenter access control mechanism controls access to objects stored on the VirtualCenter, such as virtual machines, and VM Groups. The VirtualCenter access control mechanism also controls access to files containing templates as well as event, alarm, and scheduled event information. This information is stored in the VirtualCenter Database. The VirtualCenter access control mechanism also controls access by a VirtualCenter user to data and operations specific to the definition, configuration, and management of virtual machines. 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.

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

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

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

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, is 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.

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 user identity. 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, 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 console, system administrator or root user access requests are processed as in any Linux system. They have access to any ESX or VM data on the system. The VM administrators cannot 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 user identity of the subject is the owner of the object operation and the requested access type is allowed for the object owner, then access is granted. If a group the user belongs to matches the group of the object and the requested access type is allowed for the group, access is granted. For other users, if the access requested is allowed for "others," then access is granted. Otherwise, access is denied.

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

6.1.3 Identification and Authentication

When a user logs into the ESX Server a user name and password are requested before any access is given. These authentication credentials are compared with the authentication credentials stored on the ESX Server in a shadow file, where the password is hashed using SHA-1. If the authentication credentials are valid, access to the system is provided, with the privileges appropriate to the role assigned to that user. If the credentials are not valid the user is presented with another chance to provide valid credentials.

When a user logs into VirtualCenter they are presented with a login screen, requesting the VirtualCenter name or IP address, the user name, and the user password. The user information is passed to the underlying Windows operating system which verifies the user identity and password. If login is valid, the user at the Virtual Infrastructure Client is presented with the Virtual Infrastructure Client interface denoting a successful login. If login is invalid, a message is displayed, and the login window remains available for the user to retry.

TOE Security Functional Requirements Satisfied: FIA_UAU.1(a), FIA_UID.1(a), FIA_VC_LOGIN_EXP.1

6.1.4 Security Management

The ESX Server supports the two roles: system administrator and VM 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 VM's, 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 6.1.2.

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. 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.

The TOE provides security management functions that address the management of security attributes for the ESX Server (role, user id for subjects, and owner, group, and r,w,x permissions for owner, object group, and other for objects) and VirtualCenter (user identity role permission pairs for both subjects and objects). In addition the TOE provides security management functions for the creation, deletion, registration, modification, and power operations[5] on virtual machines.

Virtual Center supports two categories of roles: VirtualCenter Administrator and Administrator defined roles. The VirtualCenter Administrator is implemented by membership in the "administrators" group of the underlying

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

Windows OS. Users log in using their username and password, and are automatically in this role by virtue of their membership in the administrators group.

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

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

6.1.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that physical connections made to the TOE remain intact and unmodified. The TOE protects information as it is transmitted between remote components of the TOE by encrypting the information using SSL.

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

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FPT_RVM.1, FPT_SEP.1(a)

6.1.6 Virtual Machine Domain Separation

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

The ESX Server provides an idealized hardware environment and virtualization of underlying physical resources. Each virtual machine runs its own operating system and applications: they cannot communicate to each other in unacceptable/unauthorized ways, nor can they leak data. The following mechanisms ensure this:

- Shared memory: The memory allocation mechanisms prevent the sharing of writable memory. Each VM is assigned memory that belongs exclusively to it.
- Read only Memory: Multiple VM’s 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 VM’s.
- Communication between VM’s through network connections can be permitted or prevented as desired. These networking mechanisms are similar to those used to connect separate physical machines.

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

TOE Security Functional Requirements Satisfied: VDS_VMM_EXP.1

6.2 TOE Security Assurance Measures

EAL4+ was chosen to provide a moderate level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL4+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 10 - Assurance Measures Mapping to TOE Security Assurance Requirements

Assurance Component	Assurance Measure
ACM_AUT.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Configuration Management
ACM_CAP.4	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Configuration Management
ACM_SCP.2	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Configuration Management
ADO_DEL.2	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Secure Delivery
ADO_IGS.1	‘Installation and Upgrade Guide’ Revision: 20060925
ADV_FSP.2	ESX Server 3.0.2 and VirtualCenter 2.0.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.2	ESX Server 3.0.2 and VirtualCenter 2.0.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_IMP.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_LLD.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_SPM.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Informal Security Policy Model
AGD_ADM.1	‘Introduction’ Revision: 20060925 ‘Basic System Administration’ Revision: 2006105 ‘Server Configuration Guide’ Revision: 20060925
AGD_USR.1	NA
ALC_DVS.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 – Lifecycle
ALC_FLR.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 – Lifecycle
ALC_LCD.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 – Lifecycle
ALC_TAT.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 – Lifecycle
ATE_COV.2	ESX Server 3.0.2 and VirtualCenter 2.0.2 – Functional Tests and Coverage
ATE_DPT.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 – Functional Tests and Coverage

Assurance Component	Assurance Measure
ATE_FUN.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 – Functional Tests and Coverage
AVA_MSU.2	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Vulnerability Assessment
AVA_SOF.1	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Vulnerability Assessment
AVA_VLA.2	ESX Server 3.0.2 and VirtualCenter 2.0.2 - Vulnerability Assessment

6.2.1 Assurance Documentation

At EAL4+ the following set of documents are provided to satisfy the assurance requirements.

6.2.1.1 ACM_CAP.2: Configuration Management Document, ACM_AUT.1 Partial CM automation, ACM_CAP.4 Generation support and acceptance procedures, ACM_SCP.2 Problem tracking CM coverage

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at VMware. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.1.2 ADO_DEL.2 Detection of modification, ADO_IGS.1 Installation, generation, and start-up procedures

The Delivery and Operation document provides a description of the secure delivery procedures implemented by VMware to protect against TOE modification during product delivery. The Installation Documentation provided by VMware details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE User(s) on configuring the TOE and how TOE configurations affect the TSF.

6.2.1.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for administrators and users of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they need to be exercised.

6.2.1.4 ADV_FSP.2 Fully defined external interfaces, ADV_HLD.2 Security enforcing high-level design, ADV_IMP.1 Subset of the implementation of the TSF, ADV_LLD.1 Descriptive low-level design, ADV_RCR.1 Informal correspondence demonstration, ADV_SPM.1 Informal TOE security policy model

The VMware design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Low-Level Design provides a lower level design specification that refines the subsystems of the TSF into modules. The low-level design identifies the structure and purpose of the modules, a listing of all interfaces, and the purpose and method of use for each interface.
- The Implementation Representation maps elements of the low-level design to the TSF implementation.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided.
- The Informal Security Policy provides a model of the TOE security policy.

6.2.1.5 ALC_DVS.1 Identification of security measures, ALC_FLR.1 Basic flaw remediation, ALC_LCD.1 Developer defined life-cycle model, ALC_TAT.1 Well-defined development tools

The lifecycle document outlines the physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE. It shows how discovered security flaws are tracked and corrected by the developer. The lifecycle document also provides a model for the development and maintenance of a TOE and the tools used to develop, analyze and implement the TOE.

6.2.1.6 ATE_COV.2 Analysis of coverage, ATE_DPT.1 Testing: high-level design, ATE_FUN.1 Functional testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. The Depth Analysis describes the level of detail to which the TSF is tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing.

6.2.1.7 AVA_MSU.2 Validation of analysis, AVA_SOF.1 Strength of TOE security function evaluation, AVA_VLA.2 Independent vulnerability analysis

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks and misuse. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum Strength of Function (SOF) requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. Table 11 demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 11 - Relationship of Security Threats to Objectives

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

T.VM **A process running on one virtual machine might compromise the security of processes running on other virtual machines.**

This threat is mitigated by the O.VM objective which makes information on the unavailability or poor performance of IP networks and servers available to administrators in a timely and clear manner. This allows the administrators to take action to limit the impact of current problems and avoid future problems. The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.

T.COMINT **An unauthorized user may attempt to compromise the security of the data collected and produced by the TOE by bypassing a security mechanism.**

The O.IDAUTH objective, supported by the OE.IDAUTH objective, requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data. The O.ADMIN objective requires that only authorized users are able to manage the security attributes of the TOE. The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE. The O.SECURE objective ensures that TOE data is protected when transmitted between remote components of the TOE. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.

T.PRIVIL **An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.**

This threat is primarily diminished by the O.IDAUTH objective, supported by the OE.IDAUTH objective, requires that the TOE, with support from the environment, must be able to identify and authenticate operators prior to allowing access to TOE functions and data. The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage the functions and data of the TOE. The O.ACCESS objective provides that all access is compliant with the TSP. The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.

A.NOEVIL **Operators are non-hostile, appropriately trained, and follow all operator guidance.**

The NOE.NOEVIL objective ensures that operators are non-hostile, appropriately trained, and follow all operator guidance.

A.PHYSCL **The ESX Server and VirtualCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access. The Virtual Infrastructure Client component will only connect to the server via the protected management network.**

The NOE.PHYSCL objective requires that the ESX Server and VirtualCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access, and that the VI Client component will only connect to the server via the protected management network.

8.2 Security Functional Requirements Rationale

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

Table 12 - Relationship of Security Requirements to Objectives

	Objectives	TOE						Env		
	Requirements	O.ADMIN	O.AUDIT	O.IDAUTH	O.ACCESS	O.SECURE	O.VM	OE.IDAUTH	OE.TIME	OE.SEP
TOE	FAU_GEN.1		✓							
	FAU_SAR.1		✓							
	FDP_ACC.1(a)				✓					
	FDP_ACC.1(b)				✓					
	FDP_ACF.1(a)				✓					
	FDP_ACF.1(b)				✓					
	FIA_UAU.1(a)			✓	✓					
	FIA_UID.1(a)			✓	✓					
	FIA_VC_LOGIN_EXP.1			✓	✓					
	FMT_MSA.1(a)	✓								
	FMT_MSA.1(b)	✓								
	FMT_MSA.3(a)	✓								
	FMT_MSA.3(b)	✓								
	FMT_SMF.1	✓								
	FMT_SMR.1(b)	✓		✓						
	FPT_ITT.1					✓				
	FPT_RVM.1	✓	✓	✓	✓	✓	✓			
	FPT_SEP.1(a)	✓	✓	✓	✓	✓	✓			
	VDS_VMM_EXP.1						✓			
Env	FIA_UAU.1(b)							✓		
	FIA_UID.1(b)							✓		
	FMT_SMR.1(a)							✓		
	FPT_SEP.1(b)									✓
	FPT_STM.1								✓	

O.AUDIT **The TOE must gather audit records of actions on the TOE which may be indicative of misuse.**

Security-relevant events must be audited by the TOE (FAU_GEN.1). The TOE must provide the ability to review the audit trail of the system (FAU_SAR.1). The TOE must provide secure domains to protect trusted subjects from interference from untrusted subjects (FPT_SEP.1(a)). The TOE must ensure that all security functions are invoked and succeed before each function may proceed (FPT_RVM.1). FAU_GEN.1, FAU_SAR.1, FPT_SEP.1(a) and FPT_RVM.1 together satisfy this objective.

O.ADMIN **The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges, and only those TOE users, can exercise such control.**

The TOE defines a set of roles (FMT_SMR.1(a) and FMT_SMR.1(b)). Only those roles are given the right to modify or set defaults for TOE security attributes (FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a) and FMT_MSA.3(b)). Mechanisms exist to enforce these rules (FMT_SMF.1). The TOE must provide secure domains to protect trusted subjects from interference from untrusted subjects (FPT_SEP.1(a)). The TOE must ensure that all security functions are invoked and succeed before each function may proceed (FPT_RVM.1). FMT_SMR.1(b), FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_SMF.1, FPT_SEP.1(a) and FPT_RVM.1 together satisfy this objective.

O.IDAUTH **The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.**

The TOE will not give any security sensitive access to a user until the user has been identified (FIA_UID.1(a)) and authenticated (FIA_UAU.1(a)) the user. For VirtualCenter the TOE requires support from the TOE environment to verify the user credentials (FIA_VC_LOGIN_EXP.1). The TOE must be able to recognize the different user roles that exist for the TOE (FMT_SMR.1(b)). The TOE must provide secure domains to protect trusted subjects from interference from untrusted subjects (FPT_SEP.1(a)). The TOE must ensure that all security functions are invoked and succeed before each function may proceed (FPT_RVM.1). FIA_UID.1(a), FIA_UAU.1(a), FIA_VC_LOGIN_EXP.1, FMT_SMR.1(b), FPT_SEP.1(a) and FPT_RVM.1 together satisfy this objective.

O.ACCESS **The TOE must allow authorized users to access only appropriate TOE functions and data.**

The TOE will not give any access to a user until the TOE has identified (FIA_UID.1(a)) and authenticated (FIA_UAU.1(a)) the user. For VirtualCenter the TOE requires support from the TOE environment to verify the user credentials (FIA_VC_LOGIN_EXP.1). All access control requests must be checked for compliance with the TSP before execution (FDP.ACC.1(a), FDP.ACC.1(b), FDP.ACF.1(a) and FDP.ACF.1(b)). The TOE must provide secure domains to protect trusted subjects from interference from untrusted subjects (FPT_SEP.1(a)). The TOE must ensure that all security functions are invoked and succeed before each function may proceed (FPT_RVM.1). FIA_UID.1(a), FIA_UAU.1(a), FIA_VC_LOGIN_EXP.1, FDP.ACC.1(a), FDP.ACC.1(b), FDP.ACF.1(a), FDP.ACF.1(b), FPT_SEP.1(a) and FPT_RVM.1 together satisfy this objective.

O.SECURE **The TOE must ensure the confidentiality and integrity of all System data as it passes between remote components of the TOE.**

The System must protect the confidentiality of information during transmission to a remote component of the TOE (FPT_ITT.1). The TOE must provide secure domains to protect trusted subjects from interference from untrusted subjects (FPT_SEP.1(a)). The TOE must ensure that all security functions are invoked and succeed before each function may proceed (FPT_RVM.1). FPT_ITT.1, FPT_SEP.1(a) and FPT_RVM.1 together satisfy this objective.

O.VM **The TOE must provide virtual machines with a domain of execution which is protected from interference and tampering by virtual machines.**

The TOE must isolate each virtual machine by providing a domain of execution which is protected from interference and tampering by virtual machines (VDS_VMM_EXP.1). The TOE must provide secure domains to protect trusted subjects from interference from untrusted subjects (FPT_SEP.1(a)). The TOE must ensure that all security functions are invoked and succeed before each function may proceed (FPT_RVM.1). VDS_VMM_EXP.1, FPT_SEP.1(a) and FPT_RVM.1 together satisfy this objective.

OE.IDAUTH **The IT Environment will provide reliable verification of the Virtual Infrastructure Client user credentials.**

The IT Environment is required to verify identify (FIA_UID(b)) and authenticate (FIA_UAU(b)) a user before the user is given access to the TOE. FIA_UID(b) and FIA_UAU(b) together satisfy this objective.

OE.TIME **The IT Environment will provide reliable timestamps to the TOE.**

The IT Environment is required to provide reliable timestamps to the TOE (FPT_STM.1).

OE.SEP **The IT Environment will protect the TOE from external interference or tampering.**

The IT Environment must protect the TOE from interference that would prevent it from performing its functions (FPT_SEP.1(b)).

8.3 Security Assurance Requirements Rationale

EAL4, augmented with AFC_FLR.1 was chosen to provide a moderate to high level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. At EAL4+ the TOE will have an undergone an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

8.4 Rationale for Explicitly Stated SFRs

The TOE contains the following explicitly stated security functional requirements:

- FIA_VC_LOGIN_EXP.1
- VDS_VMM_EXP.1

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 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.

8.5 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 13 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included.

Table 13 - Functional Requirements Dependencies

SFR	Dependencies	Dependency Met
FAU_GEN.1	FPT_STM.1	✓
FAU_SAR.1	FAU_GEN.1	✓
FDP_ACC.1(a)	FDP_ACF.1(a)	✓
FDP_ACC.1(b)	FDP_ACF.1(b)	✓
FDP_ACF.1(a)	FDP_ACC.1(a), FMT_MSA.3(a)	✓
FDP_ACF.1(b)	FDP_ACC.1(b), FMT_MSA.3(b)	✓
FIA_UAU.1(a)	FIA_UID.1(a)	✓
FIA_UAU(b)	FIA_UID.1(b)	✓
FMT_MSA.1(a)	FDP_ACC.1(a), FMT_SMR.1(a), FMT_SMF.1(a)	✓

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(b)	✓

FMT_MSA.3(b)	FMT_MSA.1(b)
	FMT_SMR.1(b)
		✓

FMT_SMR.1(a)	FIA_UID.1(a)	✓
FMT_SMR.1(b)	FIA_UID.1(b)	✓

8.6 TOE Summary Specification Rationale

8.6.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 14 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

Table 14 - Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1 FAU_SAR.1	Audit records are generated by the TOE for events indicative of a misuse of the TOE or a lack of availability or poor performance in the monitored network (FAU_GEN.1). The TSF provides the users with the capability to read the audit data through the web browser and the Global Console (FAU_SAR.1). Together these contribute to a coherent security audit function.

User Data Protection	FDP_ACC.1(a)
	FDP_ACC.1(b)
	FDP_ACF.1(a)
	FDP_ACF.1(b)
		The TOE ensures that all access control requests are checked for compliance with the TSP before execution (FDP.ACC.1(a), FDP.ACC.1(b), FDP.ACF.1(a) and FDP.ACF.1(b)). Together these contribute to a coherent user data protection function.

Identification and Authentication	FIA_UAU.1 FIA_UID.1 FIA_VC_LOGIN_EXP.1	The TOE will not give any access to a user until the TOE has identified (FIA_UID.1(a)) and authenticated (FIA_UAU.1(a)) the user. For VirtualCenter the TOE requires support from the TOE environment to verify the user credentials (FIA_VC_LOGIN_EXP.1). Together these contribute to a coherent identification and authentication function.

Security Management	FMT_MSA.1(a)
	FMT_MSA.3(a)
	FMT_MSA.1(b)
	FMT_MSA.3(b)
	FMT_SMF.1
	FMT_SMR.1(a)
	FMT_SMR.1(b)
		The TOE and TOE Environment maintain two roles for the VirtualCenter - VM Administrator and System Administrator, and two categories of roles for the ESX sever – Administrator and Administrator defined roles (FMT_SMR.1(a), FMT_SMR.1(b)). The TOE prevents unauthorized users from modifying or setting default values for TOE security attributes (FMT_MSA.1(a), FMT_MSA.3(a), FMT_MSA.1(b) and FMT_MSA.3(b)). The TOE can control the management of TSF data, security attributes and security functions (FMT_SMF.1). Together these contribute to a coherent security management function.

Protection of the TSF	FPT_ITT.1 FPT_RVM.1 FPT_SEP.1(a)	The TSF data is protected from disclosure when it is transmitted between separate parts of the TOE, because it is transmitted protected using SSL (FPT_ITT.1). The TOE must provide secure domains to protect trusted subjects from interference from untrusted subjects (FPT_SEP.1(a)). The functions that enforce the TSP must succeed first before any other function can proceed. No other administrator functions can be performed before identification and authentication of the user is completed. (FPT_RVM.1) Together these contribute to a coherent TOE protection function.

8.6.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL4+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. The chosen assurance level was also selected for conformance with the client's needs. Please refer to Section 6.2 above for details about the assurance measures which meet the EAL4+ assurance requirements.

8.7 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL4+ assurance requirements, this SOF is sufficient to resist the threats identified in Section 3 The evaluated TOE is intended to operate in commercial and DOD low robustness environments processing unclassified information.

The only security functional requirement which has a probabilistic or permutational function is FIA_UAU.1(a). The probabilistic function is password based authentication.

9 Acronyms

Table 15 - Acronyms

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
GB	Gigabyte
GHZ	Gigahertz
HTTPS	HyperText Transfer Protocol over SSL
IP	Internet Protocol
MB	Megabyte
MHZ	Megahertz
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
SAN	Storage Area Network
SAR	Security Assurance Requirement
SDK	Software Development Kit
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm-1
SNMP	Simple Network Management Protocol
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VM	Virtual Machine