Certification Report

EAL 4+ Evaluation of VMware® ESX Server 3.5 and VirtualCenter 2.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-104-CR
Version: 1.0
Date: 9 February 2010
Pagination: i to iii, 1 to 12

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for IT Security Evaluation, Version 3.1 Revision 2*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 9 February 2010, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademarks:

- VMware® is a registered trademark of VMware Incorporated;
- Red Hat® is a registered trademark of Red Hat, Incorporated; and
- Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

TABLE OF CONTENTS

Executive Summary

The VMware® ESX Server 3.5 and VirtualCenter 2.5 (herefter referred to as VMware® ESX Server and VirtualCenter) is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

VMware® ESX Server and VirtualCenter is an operating system comprising the two main components VMware® ESX Server 3.5 and VMware® VirtualCenter 2.5.

VMware® ESX Server 3.5 (hereafter referred to as VMware® ESX Server) provides the virtualization layer that allows multiple virtual machines to be hosted on one physical server. VMware® ESX Server abstracts processor, memory, storage and networking resources to create virtual machines that run unmodified host operating systems and applications. Each virtual machine acts as a physically separated guest, communicating with other virtual machines using networking protocols.

VMware® VirtualCenter 2.5 (hereafter referred to as VMware® VirtualCenter) provides centralized management and operational automation. Management services include the migration of virtual machines between physical servers without disruption to end users and dynamic allocation and balancing of computing capacity across collections of hardware resources.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 26 January 2010 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the VMware® ESX Server and VirtualCenter, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed:

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

ALC_FLR.1 - Basic Flaw Remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that the VMware® ESX Server and VirtualCenter evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is VMware® ESX Server 3.5 and VirtualCenter 2.5 (hereafter referred to as VMware® ESX Server and VirtualCenter), from VMware Incorporated.

2 TOE Description

VMware® ESX Server and VirtualCenter is an operating system comprising the two main components VMware® ESX Server 3.5 and VMware® VirtualCenter 2.5.

VMware® ESX Server 3.5 (hereafter referred to as VMware® ESX Server) provides the virtualization layer that allows multiple virtual machines to be hosted on one physical server. VMware® ESX Server abstracts processor, memory, storage and networking resources to create virtual machines that run unmodified host operating systems and applications. Each virtual machine acts as a physically separated guest, communicating with other virtual machines using networking protocols.

VMware® VirtualCenter 2.5 (hereafter referred to as VMware® VirtualCenter) provides centralized management and operational automation. Management services include the migration of virtual machines between physical servers without disruption to end users and dynamic allocation and balancing of computing capacity across collections of hardware resources.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for VMware® ESX Server and VirtualCenter is identified in Section 5 of the Security Target (ST).

The following Government of Canada approved algorithms were evaluated for correct implementation in VMware® ESX Server and VirtualCenter:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	902
Advanced Encryption Standard (AES)	FIPS 197	1271, 1274
Rivest Shamir Adleman (RSA)	FIPS 186-2	612
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1174
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	741

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: VMware Inc., ESX Server 3.5 and VirtualCenter 2.5 Security Target
Version: 0.6
Date: 26 January 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*.

VMware® ESX Server and VirtualCenter is:

a. *Common Criteria Part 2 extended*, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - EXT_FDP_VC_ETC.1 - Export of VirtualCenter data;
   - EXT_FDP_VC_ITC.1 - Import of VirtualCenter data;
   - EXT_FIA_VC_LOGIN.1 - VirtualCenter user login request; and
   - EXT_VDS_VMM.1 - ESX virtual machine domain separation.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based on assurance components in Part 3; and

c. *Common Criteria EAL 4 augmented*, containing all the security assurance requirements in the EAL 4 assurance package, as well as the following: ALC_FLR.1: Basic Flaw Remediation.

6 Security Policies

VMware® VirtualCenter implements an access control policy that controls user[2] access to data and operations specific to the definition, configuration, and management of virtual machines.

VMware® ESX Server implements an access control policy that controls user access to virtual machine definition and configuration files and to audit data.

VMware® ESX Server implements an information flow control policy that governs the flow of information between virtual machines.

[2] The term “user” is defined in the ST to mean “administrative user”. For consistency, the term “user” in this Report is also defined to mean “administrative user”.

Additional detail on the access control and flow control policies is found in the ST.

VMware® ESX Server and VirtualCenter implements other policies pertaining to security audit, import and export of security data, identification and authentication, security management and protection of TSF data. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of VMware® ESX Server and VirtualCenter should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Users of the TOE are non-hostile, are appropriately trained, and follow all user guidance.
- The VMware® VirtualCenter database is configured such that it is accessible only by VMware® VirtualCenter.

7.2 Environmental Assumptions

VMware® ESX Server and VirtualCenter is located within a controlled access facility that prevents unauthorized physical access. The VMware® VirtualCenter and VMware® Server components are connected via a protected network connection.

7.3 Clarification of Scope

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 virtual machine.

VMware® ESX Server and VirtualCenter incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Architectural Information

VMware® ESX Server and VirtualCenter is an operating system that comprises the two main components VMware® VirtualCenter and VMware® ESX Server.

The VMware® VirtualCenter component comprises the following Subsystems:

VirtualCenter Management. The VirtualCenter Management Subsystem authenticates users and authorizes user actions. User access to the Subsystem is via the Virtual Infrastructure Client and Web interfaces described below.

Virtual Infrastructure Client. The Virtual Infrastructure Client Subsystem provides the user interface to VMware® ESX servers via the VMware® VirtualCenter.

VirtualCenter Secure Web. The VirtualCenter Secure Web Subsystem provides the user interface to a subset of the functionality provided by the Virtual Infrastructure Client Subsystem.

VirtualCenter Communications. The VirtualCenter Communication Subsystem provides the secure communications channel between VMware® VirtualCenter and VMware® ESX Server.

Database. The VMware® VirtualCenter database stores information on the configuration and status of VMware® ESX servers and virtual machines, and audit data.

The VMware® ESX Server component comprises the following Subsystems:

ESX Console Operating System (COS). The ESX COS Subsystem primarily manages the VMware® ESX Servers and virtual machines. Users can connect either from the Virtual Infrastructure Client Subsystem or from the VirtualCenter Secure Web Subsystem. The ESX COS Subsystem is based on a subset of Red Hat® Enterprise Linux® 3.0 Update 9 plus security fixes.

ESX VMkernel. The ESX VMkernel Subsystem performs the hardware virtualization. It provides the virtual devices including virtualized CPU, memory, I/O busses, network interfaces, storage adapters, human interface devices, BIOS and others devices that map to the physical devices.

ESX CLI. The ESX CLI Subsystem is a command line interface providing users the ability to perform low-level configuration of the VMware® ESX server. This interface is intended to be used primarily for initial installation and configuration, and for troubleshooting.

ESX Audit. The ESX Audit Subsystem is the audit logging Subsystem. The Subsystem receives audit data from other Subsystems; audit information is made available to users through the Virtual Infrastructure Client.

9 Evaluated Configuration

The VMware® ESX Server and VirtualCenter is a software-only TOE comprising:

- VMware® ESX Server 3.5, Update 4, Build 153875; and
- VMware® VirtualCenter 2.5, Update 4, Build 147658.

The ESX Server can be installed in three distinct configurations, all of which were subjected to analysis and testing.

Local Storage Only. In this configuration, VMware® ESX Server is installed on a server and uses local disk for storage of Virtual Machine (VM) images, VM data, and other data.

ESX Local/virtual machines on Storage Area Network (SAN). In this configuration, VMware® ESX Server is installed on a server and uses local storage for data. Virtual machines are installed on a SAN using Network File System (NFS) or Internet Small Computer System Interface (iSCSI).

Boot from SAN. In this configuration, VMware® ESX Server is installed on a SAN. Local storage is disabled, VM images and VM data are stored on the SAN.

10 Documentation

The VMware Incorporated documents provided to the consumer are:

- VMware® Update Manager Administration Guide, Revision 20090709;
- VMware® ESX Server 3.5 and VirtualCenter 2.5 Guidance Document Supplement, Document Version 0.1, 19 June 2009;
- VMware® Basic System Administration, Update 2 and later for ESX Server 3.5, ESX Server 3i Version 3.5, VirtualCenter 2.5, Revision 20090213;
- VMware® ESX Server 3 Configuration Guide, Update 2 and later for ESX Server 3.5 and VirtualCenter 2.5, Revision 20090313;
- VMware® ESX Server 3 and VirtualCenter Installation Guide, Update 2 and later for ESX Server 3.5 and VirtualCenter 2.5, Revision 20090612;
- VMware® Quick Start Guide, Update 2 and later for ESX Server 3.5 and VirtualCenter 2.5, Revision 20090612;
- VMware® Security Hardening Best Practices for VMware® Infrastructure 3 (VMware® ESX 3.5 and VirtualCenter 2.5), Revision 20080708; and
- Whitepaper: Security Design of the VMware® Infrastructure 3 Architecture, Revision 20070215.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the VMware® ESX Server and VirtualCenter, including the following areas:

Development: The evaluators analyzed the VMware® ESX Server and VirtualCenter functional specification, design documentation, and a subset of the implementation representation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the VMware® ESX Server and VirtualCenter security architectural description and determined that the initialization process was secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance Documents: The evaluators examined the VMware® ESX Server and VirtualCenter preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Life-cycle Support: An analysis of the VMware® ESX Server and VirtualCenter configuration management system and associated documentation was performed. The evaluators found that the VMware® ESX Server and VirtualCenter configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of VMware® ESX Server and VirtualCenter during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the VMware® ESX Server and VirtualCenter design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by VMware Incorporated for VMware® ESX Server and VirtualCenter. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the

procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of VMware® ESX Server and VirtualCenter. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the VMware® ESX Server and VirtualCenter in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation;

c. Users and Roles: The objective of this test goal is to ensure correct users and roles functionality;

d. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;

e. Audit: The objective of these tests is to ensure that User Access Events Logging requirements have been met; and

f. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data; and

g. Basic Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

VMware® ESX Server and VirtualCenter was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the VMware® ESX Server and VirtualCenter behaves as specified in its ST, functional specification, TOE design, and security architecture description.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The VMware® ESX Server and VirtualCenter is a complex IT product capable of providing virtualization services for a large scale corporate network. It is supported by a large documentation suite which includes comprehensive Installation, Administration, Configuration and Security Best Practice guidance.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
COS	Console Operating System
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SAN	Storage Area Network
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine

16 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. VMware Inc., ESX Server 3.5 and VirtualCenter 2.5 Security Target, Revision No. 0.6, 26 January 2010.

e. Evaluation Technical Report (ETR) VMware® ESX Server and VirtualCenter, EAL 4+ Evaluation, Common Criteria Evaluation Number: 383-4-104 Document No. 1610-000-D002, Version 1.5, 26 January 2010.