Certification Report

EAL 4+ Evaluation of VMware® ESX 4.0 Update 1 and vCenter Server 4.0 Update 1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-145-CR
Version:	1.0
Date:	15 October 2010
Pagination:	i to iii, 1 to 13

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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. 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, 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 15 October 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 trademark:

- VMware® is a registered trademark of VMware Incorporated.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

VMware® ESX 4.0 Update 1 and vCenter Server 4.0 Update 1 (hereafter referred to as ESX and vCenter Server 4.0 Update 1), from VMware Incorporated, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

ESX and vCenter Server 4.0 Update 1 is a virtualization technology comprising the two main components VMware ESX and VMware vCenter Server.

VMware ESX is a virtualization layer that runs directly on industry standard x86-compatible hardware, allowing multiple virtual machines to be hosted on one physical server. VMware ESX abstracts processor, memory, storage, and networking resources to create virtual machines which can run a wide variety of different operating systems. Each virtual machine acts as a physically separated guest, communicating with other virtual machines using networking protocols.

VMware vCenter Server is a management console used to deploy, monitor, and manage virtual machines that are distributed across multiple server running VMware ESX.

Users can access ESX and vCenter Server 4.0 Update 1 using the interface applications vSphere Client or vSphere Web Access from a web browser.

ESX and vCenter Server 4.0 Update 1 incorporates CAVP-validated cryptography.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 20 September 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 ESX and vCenter Server 4.0 Update 1, 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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation,*

[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.

version 3.1 Revision 3. The following augmentation is claimed: ALC_FLR.2 - Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that ESX and vCenter Server 4.0 Update 1 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 4.0 Update 1 and vCenter Server 4.0 Update 1 (hereafter referred to as ESX and vCenter Server 4.0 Update 1), from VMware Incorporated.

2 TOE Description

ESX and vCenter Server 4.0 Update 1 is a virtualization technology comprising the two main components VMware ESX and VMware vCenter Server.

VMware ESX is a virtualization layer that runs directly on industry standard x86-compatible hardware, allowing multiple virtual machines to be hosted on one physical server. VMware ESX abstracts processor, memory, storage, and networking resources to create virtual machines which can run a wide variety of different operating systems. Each virtual machine acts as a physically separated guest, communicating with other virtual machines using networking protocols.

VMware vCenter Server is a management console used to deploy, monitor, and manage virtual machines that are distributed across multiple servers running VMware ESX.

Users can access ESX and vCenter Server 4.0 Update 1 using the interface applications vSphere Client or vSphere Web Access from a web browser.

ESX and vCenter Server 4.0 Update 1 incorporates CAVP-validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the ESX and vCenter Server 4.0 Update 1 is identified in Sections 6 and 7 of the Security Target (ST).

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in ESX and vCenter Server 4.0 Update 1:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	980
Advanced Encryption Standard (AES)	FIPS 197	1421
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1289
Rivest Shamir Adleman (RSA)	FIPS 186-2	696

4 Security Target

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

Title: VMware, Inc. VMware® ESX 4.0 Update 1 and vCenter Server 4.0 Update 1
Security Target
Version: 1.4
Date: 3 September 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*.

ESX and vCenter Server 4.0 Update 1 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_FAU_ARP.1 - System event automatic response;
   - EXT_FIA_VC_LOGIN.1 - vCenter Server 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*, with all the security assurance requirements in the EAL 4, as well as the following: ALC_FLR.2 - Flaw Reporting Procedures.

6 Security Policies

ESX and vCenter Server 4.0 Update 1 implements access control policies that controls user[2] access to data and operations specific to the definition, configuration, and management of virtual machines and to audit data.

ESX and vCenter Server 4.0 Update 1 implements an information flow control policy that governs the flow of information between virtual machines.

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

ESX and vCenter Server 4.0 Update 1 implements other policies pertaining to security audit, alarm generation, cryptographic support, user data protection, identification and authentication, security management and protection of the TSF. Further details on these security policies may be found in Sections 5 and 6 of the ST.

[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”.

7 Assumptions and Clarification of Scope

Consumers of ESX and vCenter Server 4.0 Update 1 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 Assumption is listed in the ST:

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

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- The ESX host and the vCenter Server components will be located within controlled access facilities which will prevent unauthorized physical access.

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.

ESX and vCenter Server 4.0 Update 1 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

ESX and vCenter Server 4.0 Update 1 is a software-only TOE comprising:

- ESX 4.0 Update 1, Build 208167;
- vCenter Server 4.0 Update 1, Build 208111;
- Update Manager 4.0 Update 1, Build 208126; and
- vSphere Client 4.0 Update 1, Build 208111.

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

- Local Storage Only. In this configuration, VMware ESX is installed on a server and uses local disk for storage for Virtual Machine (VM) images, VM data, and other data.
- VMware ESX local/virtual machines on Storage Area Network (SAN), Network File System (NFS), and Internet Small Computer System Interface (iSCSI). In this configuration, ESX is installed on a server and uses local storage for ESX data. Virtual machines are installed on a SAN, NFS, or iSCSI datastore.
- Boot from SAN. In this configuration, VMware ESX is installed on the SAN. Local storage is disabled; VM images and VM data are stored on the SAN, NFS, or iSCSI datastore.

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

9 Documentation

The VMware Incorporated documents provided to the consumer are:

- ESX and vCenter Server Installation Guide ESX 4.0 vCenter Server 4.0, EN-000104-01, 2009;

- ESX Configuration Guide ESX 4.0 vCenter Server 4.0, EN-000106-05, 2009;

- Fibre Channel SAN Configuration Guide Update 1 ESX 4.0 ESXi 4.0 vCenter Server 4.0, EN-000266-03, 2009;

- Getting Started with ESX 4.0 vCenter Server 4.0, EN-000118-00, 2009;

- Guest Operating System Installation Guide, March 5, 2010;

- Introduction to VMware vSphere ESX 4.0 ESXi 4.0 vCenter Server 4.0, EN-000102-00, 2009;

- iSCSI SAN Configuration Guide Update 1 ESX 4.0 ESXi 4.0 vCenter Server 4.0, EN-000267-03, 2010;

- Setup for Failover Clustering and Microsoft Cluster Service Update 1 ESX 4.0 ESXi 4.0 vCenter Server 4.0, EN-000269-01, 2010;

- VMware, Inc. ESX 4.0 and VMware vCenter Server 4.0 Guidance Documentation Supplement Evaluation Assurance Level: EAL4+ Document Version: 0.1, 17 May 2010;

- vSphere Availability Guide Update 1 ESX 4.0 ESXi 4.0 vCenter Server 4.0, EN-000265-02, 2010;

- vSphere Basic System Administration Update 1 ESX 4.0 ESXi 4.0 vCenter Server 4.0, EN-000260-02, 2010;

- vSphere Resource Management Guide Update 1 ESX 4.0 ESXi 4.0 vCenter Server 4.0, EN-000264-01, 2010;

- vSphere Upgrade Guide Update 1 ESX 4.0 ESXi 4.0 vCenter Server 4.0 vSphere Client 4.0, EN-000259-02, 2010; and

- vSphere Web Access Administrator's Guide vSphere Web Access 4.0 vCenter Server 4.0 ESX 4.0, EN-000128-01, 2009.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of ESX and vCenter Server 4.0 Update 1, including the following areas:

Development: The evaluators analyzed the ESX and vCenter Server 4.0 Update 1 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, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the ESX and vCenter Server 4.0 Update 1 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 ESX and vCenter Server 4.0 Update 1 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 ESX and vCenter Server 4.0 Update 1 configuration management system and associated documentation was performed. The evaluators found that the ESX and vCenter Server 4.0 Update 1 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 ESX and vCenter Server 4.0 Update 1 during distribution to the consumer.

The evaluators examined the development security procedures during a previous site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the ESX and vCenter Server 4.0 Update 1 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 ESX and vCenter Server 4.0 Update 1. During a previous 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 ESX and vCenter Server 4.0 Update 1. 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 and vCenter Server in its operational environment.

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

11 ITS Product Testing

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

11.1 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.

11.2 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:

- 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

[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.

the Security Target, by following all instructions in the developer’s Installation and Administrative guidance;

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

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

- Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;

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

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

- Basic Product 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.

11.3 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:

- Scanning ports to ensure unnecessary ports are not open;
- Scanning ports for responses that reveal detail about applications;
- Scanning for leakage information at start up that reveals detail about applications; and
- Testing that the TOE is not vulnerable to SQL injection within user input fields.

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

11.4 Conduct of Testing

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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the ESX and vCenter Server 4.0 Update 1 behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 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.

13 Evaluator Comments, Observations and Recommendations

ESX and vCenter Server 4.0 Update 1 is supported by a large documentation suite that includes comprehensive Installation, Administration, Configuration and Security Best Practice guidance.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation / Initialization	Description
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
iSCSI	Internet Small Computer System Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NFS	Network File System
PALCAN	Program for the Accreditation of Laboratories Canada
SAN	Storage Area Network
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Acronym/Abbreviation / Initialization	Description
VM	Virtual Machine
x86-compatible	A computer system that is compatible with Intel's x86 CPU family.

15 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 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. VMware, Inc. VMware® ESX 4.0 Update 1 and vCenter Server 4.0 Update 1 Security Target, Version 1.4, 3 September 2010.

e. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of VMware® ESX 4.0 Update 1 and vCenter Server 4.0 Update 1, Document No. 1651-000-D002, Version 2.1, 20 September 2010.