Certification Report

EAL 4+ Evaluation of VMware® ESX Server 3.0.2 and VirtualCenter 2.0.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-72-CR
Version: 1.0
Date: 20 May 2008
Pagination: i to iv, 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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. 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 Standard 17025, General requirements for the accreditation of calibration and testing 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 23 May 2008, 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 at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and http://www.commoncriteriaportal.org/

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

- VMware® is either a trademark or registered trademark of VMware®, Inc. in the United States.

TABLE OF CONTENTS

Executive Summary

The VMware® ESX Server 3.0.2 and VirtualCenter 2.0.2, from VMware®, Inc., (hereafter 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 is the foundation for dynamic, self-optimizing IT infrastructure. ESX Server is a virtualization layer that abstracts processor, memory, storage and networking resources into multiple virtual machines. ESX Server allows IT organizations to increase hardware utilization and decrease capital and operating cost by sharing hardware resources across a large number of virtual machines that run side-by-side on the same server.

VMware® VirtualCenter delivers centralized management, operational automation, resource optimization and high availability to IT environments providing the data center with increased . levels of responsiveness, serviceability, efficiency and reliability.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 2 May 2008 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 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 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed:

- 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

[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.

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 the VMware® ESX Server 3.0.2 and VirtualCenter 2.0.2 (hereafter referred to as VMware® ESX Server and VirtualCenter), from VMware®, Inc.

2 TOE Description

The TOE comprises the main systems VMware® ESX Server 3.0.2 and VMware® VirtualCenter 2.0.2.

VMware® ESX Server is the foundation for dynamic, self-optimizing IT infrastructure. ESX Server is a virtualization layer that abstracts processor, memory, storage and networking resources into multiple virtual machines. ESX Server allows IT organizations to increase hardware utilization and decrease capital and operating cost by sharing hardware resources across a large number of virtual machines that run side-by-side on the same server.

VMware® VirtualCenter delivers centralized management, operational automation, resource optimization and high availability to IT environments providing the data center with increased . levels of responsiveness, serviceability, efficiency and reliability.

3 Evaluated Security Functionality

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

4 Security Target

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

Title: VMware® Inc ESX Server 3.0.2 and VirtualCenter 2.0.2 Security Target
Version: 0.7
Date: 23 April 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

The VMware® ESX Server and VirtualCenter is:

a. Common Criteria Part 2 extended, with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - FIA_VC_LOGIN_EXP.1 VirtualCenter User Login Request; and
   - VDS_VMM_EXP.1 ESX virtual machine Domain Separation.
b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 4 augmented, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

The VMware® VirtualCenter implements a role-based access control policy, VirtualCenter Access Control Policy, to control user access to the Virtual Center. The VMware® ESX Server implements a role-based access control policy, ESX Server Access Control Policy, to control user access to the ESX Server. Details of these security policies can be found in Section 5 of the ST.

In addition, the VMware® ESX Server and VirtualCenter implements other policies pertaining to security audit, identification and authentication, virtual machine domain separation, TSF Invocation and Isolation and Data Transfer Protection. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the VMware® ESX Server and VirtualCenter product 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:

- Personnel authorized to install, configure, and operate the VMware® ESX Server and VirtualCenter 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 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.

For more information about the TOE security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

VMware® ESX Server and VirtualCenter provides a level of protection that is appropriate for low robustness environments processing unclassified information. VMware® ESX Server and VirtualCenter offers protection against inadvertent or casual attempts to breach system security, by unsophisticated attackers possessing a low attack potential. VMware® ESX Server and VirtualCenter is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Architectural Information

VMware® ESX Server and VirtualCenter comprises two components: VMware® ESX Server; and VMware® VirtualCenter.

VMware® ESX Server is a virtualization layer that runs directly on standard x86 compatible hardware, allowing multiple virtual machines to be hosted on one physical server. VMware® ESX Server comprises the subsystems:

ESX subsystem. Through the ESX subsystem, users can provision and manage virtual machines. The subsystem provides the hardware virtualization to support an idealized physical machine that is isolated from other virtual machines. It provides the virtual devices, including virtualized CPU, memory, I/O busses, network interfaces, storage adapters and human interface devices.

ESX CLI subsystem. This subsystem provides a command line interface allowing administrators the ability to perform low-level configuration of the VMware® ESX Server. This interface is intended to be used for initial installation and configuration and for troubleshooting.

ESX Secure Web subsystem. This subsystem provides a web interface to the VMware® ESX Server.

VMware® VirtualCenter acts as a management console, deploying, monitoring, and managing virtual machines that are distributed across multiple hosts running VMware® ESX Server. VMware® VirtualCenter also manages supporting virtual infrastructure features such as resources pools, high-availability, disaster recovery and consolidated backup. VMware® VirtualCenter comprises the subsystems:

VirtualCenter Management Subsystem. This subsystem authenticates users and authorizes user actions. It manages inventory items, scheduled tasks, events and templates, groupings of ESX servers and individual virtual machines, and VMware® VirtualCenter users and groups.

VirtualCenter database. The database stores information about the configuration and status of VMware® ESX Server hosts and each of the host's virtual machines, user, group and object permissions, management information for the VMware® ESX Server, performance data and all events (audit data) that occur in the VMware® VirtualCenter environment.

Virtual Infrastructure Client Subsystem. This subsystem provides the interface to the VMware® VirtualCenter. It can connect to any other VMware® VirtualCenter or VMware® ESX Server.

VirtualCenter Secure Web. This subsystem provides web access to VMware® VirtualCenter.

Further details about the system architecture are proprietary to the vendor, and are not provided in this report.

9 Evaluated Configuration

The evaluated configuration for VMware® ESX Server and VirtualCenter comprises:

- VMware® ESX Server 3.0.2 Update 1 (build 61618) with VMware® ESX Server 3.0.2 November 15, 2007 & November 30, 2007 patches; and
- VMware® VirtualCenter 2.0.2 Update 2 (build 62327).

10 Documentation

The VMware®, Inc. documents provided to the consumer are as follows:

a. ESX Server 3.0.2 and VirtualCenter 2.0.2 Common Criteria Administrative Guide Supplement Version 0.3, 2008-03-20;

b. Basic System Administration ESX Server 3.0.1 and Virtual Center 2.0.1 Revision: 2006105, VI-ENG-Q306-293;

c. Server Configuration Guide ESX Server 3.0.1 and VirtualCenter 2.0.1 Revision: 20060925, VI-ENG-Q206-215;

d. SAN Configuration Guide ESX Server 3.0.1 and VirtualCenter 2.0.1 Revision: 20060925, VI-ENG-Q206-220; and

e. Installation and Upgrade Guide ESX 3.0.1 and VirtualCenter 2.0.1 Revision: 20060925, VI-ENG-Q306-292.

11 Evaluation Analysis Activities

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

Configuration management: 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. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the VMware® ESX Server and VirtualCenter during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the VMware® ESX Server and VirtualCenter functional specification, high-level design, low-level design, and a subset of the implementation representation; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. 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 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: 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 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®, Inc. for the 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 VMware® ESX Server and VirtualCenter ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the VMware® ESX Server and VirtualCenter and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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[2].

VMware®, Inc. employs a rigorous testing process that tests the changes and fixes in each release of the VMware® ESX Server and VirtualCenter. Comprehensive regression testing is conducted for all releases.

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 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. These tests focused on:

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

[2] 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. Audit: The objective of this test goal was to ensure that the audit data is recorded and can be viewed;
c. Identification and Authentication: The objective of this test goal was to ensure that identification and authentication requirements have been met;
d. Security Management: The objective of this test goal was to ensure an administrator can manage security attributes; and
e. Virtual Machine Domain Separation: The objective of this test goal was to determine the TOE's ability to isolate separate virtual machines co-existing on the ESX Server.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, independent vulnerability analysis, and 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 evaluator conducted a port scan of the VMware® ESX Server and VirtualCenter. Only the ports required for operation of the TOE were found to be open. The evaluator used a publicly available tool to scan the VMware® ESX Server and VirtualCenter for generic vulnerabilities, and none were found. In addition, the evaluator performed direct attacks on the VMware® ESX Server and VirtualCenter, attempting to bypass or break the TOE's access control security mechanisms.

The independent penetration testing did not uncover any exploitable vulnerabilities for the VMware® ESX Server and VirtualCenter in the anticipated operating environment.

12.4 Conduct of Testing

The 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 Test (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 and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4 augmented 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 complete documentation for the VMware® ESX Server and VirtualCenter includes a comprehensive Installation and Security Guide and a Users Guide.

The VMware® ESX Server and VirtualCenter is straightforward to configure, use and integrate into a corporate network.

Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
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
QA	Quality Assurance
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d. VMware® Inc ESX Server 3.0.2 and VirtualCenter 2.0.2 Security Target, Version 0.7, April 23, 2008.

e. Evaluation Technical Report (ETR) for Common Criteria EAL 4+ Evaluation of VMware® ESX Server 3.0.2 and VirtualCenter 2.0.2, Document No. 1538-000-D002, Version 1.0, 2 May 2008.