Certification Report

EAL 4+ Evaluation of VMware® vSphere 5.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-189-CR
Version:	1.0
Date:	18 May 2012
Pagination:	i to iii, 1 to 9

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, 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 CGI Information Systems and Management Consultants Inc. located in Ottawa, Canada.

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 18 May 2012, 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 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® vSphere 5.0 (hereafter referred to as vSphere 5.0), from VMware, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

vSphere 5.0 is a virtualization solution that provides an environment for the hosting and management of virtual machines on industry standard x86-compatible hardware platforms. vSphere 5.0 incorporates CAVP-validated cryptography to protect communications between its components.

CGI Information Systems and Management Consultants Inc. is the CCEF that conducted the evaluation. This evaluation was completed on 8 May 2012 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 vSphere 5.0, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.2 – Basic Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the vSphere 5.0 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is VMware® vSphere 5.0 (hereafter referred to as vSphere 5.0), from VMware, Inc.

2 TOE Description

vSphere 5.0 is a virtualization solution that provides an environment for the hosting and management of virtual machines on industry standard x86-compatible hardware platforms. vSphere 5.0 comprises the components:

- ESXi, which is the virtualization layer that runs directly on industry standard x86-compatible hardware;
- vCenter Server, that provides for central management of ESXi and the virtual machines running on ESXi;
- vSphere Client and vSphere Web Client, that provide user interfaces to vCenter Server; and
- VMware Update Manager that provides automated patch management of ESXi.

A detailed description of the vSphere 5.0 architecture is found in Section 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for vSphere 5.0 is identified in Sections 5 and 6 of the ST.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in vSphere 5.0:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	970, 971, 972, 973
Advanced Encryption Standard (AES)	FIPS 197	1421, 1422, 1423
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1289 1290, 1291
Keyed-Hash Message Authentication Code	FIPS 198	840, 841, 842, 843

Cryptographic Algorithm	Standard	Certificate #
(HMAC-SHA-1)		
Rivest Shamir Adleman (RSA)	FIPS 186-2	696, 697, 698, 699

4 Security Target

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

Title: VMware, Inc. VMware® vSphere 5.0 Security Target
Version: 0.7
Date: 19 April 2012

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.*

vSphere 5.0 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_FAU_STG.1 - External Audit Trail Storage;
   - EXT_FIA_VC_LOGIN.1 - vCenter Server User Login Request; and
   - EXT_VDS_VMM.1 - ESXi Virtual Machine Domain Separation.

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

Common Criteria EAL 4 augmented, with all the security assurance requirements in EAL 4, as well as the following: ALC_FLR.2 - Flaw Reporting Procedures.

6 Security Policies

vSphere 5.0 implements access control policies that control user access to data and operations specific to the definition, configuration, and management of virtual machines and to audit data.

vSphere 5.0 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 Section 6 of the ST.

In addition, vSphere 5.0 implements policies pertaining to security audit, alarm generation, cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, virtual machine domain separation, and TOE access. Further details on these security policies may be found in Sections 6.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of vSphere 5.0 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:

- vSphere 5.0 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. vSphere 5.0 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

vSphere 5.0 is a software-only TOE comprising ESXi 5.0, vCenter Server 5.0, VMware Update Manager 5.0, vSphere Client 5.0, and vSphere Web Client 5.0.

The publication entitled *VMware, Inc. vSphere 5.0 Guidance Documentation Supplement, Version 0.2, 3 May 2012* describes the procedures necessary to install and operate vSphere 5.0 in its evaluated configuration.

9 Documentation

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

a. VMware, Inc. VMware® ESXi 5.0 and vCenter Server 5.0 Guidance Documentation Supplement v0.1 July 18, 2011;

b. vSphere Installation and Setup, vSphere 5.0, ESXi 5.0, vCenter Server 5.0 EN-000588-00 July 2011;

c. vSphere Networking ESXi 5.0.0, vCenter Server 5.0.0 EN-000599-00 July 2011;

d. vSphere Virtual Machine Administration ESXi 5.0 vCenter Server 5.0 EN-000523-00 July 2011;

e. vSphere PowerCLI User's Guide VMware vSphere PowerCLI 5.0 EN-000462-00;

f. vSphere Command-Line Interface Concepts and Examples EN-000489-00;

g. Getting Started with vSphere Command-Line Interfaces ESXi 5.0 vCenter Server 5.0 EN-000488-00;

h. Installing and Administering VMware vSphere Update Manager vSphere Update Manager 5.0 EN-000457-00; and

i. VMware, Inc. vSphere 5.0 Guidance Documentation Supplement, Version 0.2, 3 May 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of vSphere 5.0, including the following areas:

Development: The evaluators analyzed the vSphere 5.0 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the vSphere 5.0 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the vSphere 5.0 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes 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 are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the vSphere 5.0 configuration management system and associated documentation was performed. The evaluators found that the vSphere 5.0 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 vSphere 5.0 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 vSphere 5.0 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 vSphere 5.0. 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 vSphere 5.0. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to vSphere 5.0 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[2].

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 is the following list of evaluator test goals:

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

b. Centralized logging and cryptography: The objective of this test goal is to configure and exercise remote logging, and verify traffic encryption;

c. vSphere environment management: The objective of this test goal is to exercise the vSphere management functions by creating and managing virtual networks and virtual machines; and

d. Web, CLI, and vSphere PowerCLI interfaces: The objective of this test goal is to exercise the management of vSphere over these interfaces.

11.3 Independent Penetration Testing

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

- Scanning ports to ensure unnecessary ports are not open; and

[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.

- Testing that the TOE is not vulnerable to vulnerabilities by running test tools (e.g. Nessus, HP WebInspect, Medusa).

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

11.4 Conduct of Testing

vSphere 5.0 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 CGI Information Systems and Management Consultants Inc. 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 vSphere 5.0 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 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
IT	Information Technology

Acronym/Abbreviation / Initialization	**Description**
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
x86-compatible	A computer system that is compatible with Intel's x86 CPU family.

14 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

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® vSphere 5.0 Security Target, Version 0.7, 2012/04/19.

e. VMware, Inc. VMware vSphere 5.0 Common Criteria EAL4+ Evaluation Technical Report (ETR), Version 1.0, May 8, 2012.