Certification Report

VMware® vSphere 5.1 Update 1c

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment 2014

Document number:	383-4-255-CR
Version:	1.0
Date:	24 March 2014
Pagination:	i to iii, 1 to 10

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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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, 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, 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.

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 IT Security Evaluation & Test Facility.

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 24 March 2014, 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 trademarks or registered trademarks:

- 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 5.1 Update 1c (hereafter referred to as vSphere 5.1), from VMware, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

vSphere 5.1 is a virtualization solution that provides an environment for the hosting and management of virtual machines on industry standard x86-compatible hardware platforms. vSphere 5.1 comprises the components:

- ESXi, which is the virtualization layer that runs directly on industry standard x86-compatible hardware;
- vCenter Server, vCenter Server Appliance, with vCenter Inventory Service and vCenter Single Sign-On, that provides for central management of ESXi and the virtual machines running on ESXi;
- vCLI and PowerCLI allows administrators to run common administration tasks against ESXi or vCenter Server;
- vSphere Client and vSphere Web Client, that provide user interfaces to vCenter Server; and
- VMware Update Manager that provides automated patch management of ESXi.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 24 February 2014 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 5.1, 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 2 *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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation

[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.

Communications Security Establishment, as the CCS Certification Body, declares that the vSphere 5.1 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) 2 augmented evaluation is VMware® vSphere 5.1 Update 1c (hereafter referred to as vSphere 5.1), from VMware, Inc..

2 TOE Description

vSphere 5.1 is a virtualization solution that provides an environment for the hosting and management of virtual machines on industry standard x86-compatible hardware platforms. vSphere 5.1 comprises the components:

- ESXi, which is the virtualization layer that runs directly on industry standard x86-compatible hardware;
- vCenter Server, vCenter Server Appliance, with vCenter Inventory Service and vCenter Single Sign-On, that provides for central management of ESXi and the virtual machines running on ESXi;
- vCLI and PowerCLI allows administrators to run common administration tasks against ESXi or vCenter Server;
- vSphere Client and vSphere Web Client, that provide user interfaces to vCenter Server; and
- VMware Update Manager, that provides automated patch management of ESXi.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for vSphere 5.1 is identified in Section 6 of the ST.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in vSphere 5.1:

Cryptographic Algorithm	**Certificate #**
Triple-DES Cipher Block Chaining (3DES-CBC)	1639,1640,1641,1642,1643,1644,1645,1646
Advanced Encryption Standard-Cipher Block Chaining (AES-CBC)	2723,2724,2727,2729,2730,2731,2732,2733
Rivest Shamir Adleman – Public Key Cryptography Standard 1(RSA-PKCS1)	1416,1417,1419,1421,1422,1423, 1424,1425
Secure Hash Algorithm (SHA-1)	2293,2294,2297,2299,2300,23011,2302,2303
Keyed-Hash Message Authentication Code (HMAC)	1702,1703,1706,1708,1709,1710,1712, 1711

4 Security Target

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

Title: VMware® vSphere 5.1 Update 1c Security Target
Version: 1.1
Date: 28 January 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

vSphere 5.1 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:

- EXT_FAU_ARP – Systems Event Automatic Response;
- EXT_FAU_STG – External Audit Trail Storage;
- EXT_FIA_VC_LOGIN – vCenter Server user login Request; and
- EXT_VDS_VMM – ESXi 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 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.3, Systematic Flaw Remediation

6 Security Policy

vSphere 5.1 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 5.1 also implements an information flow control policy that governs the flow of information between virtual machines.; details of these security policies can be found in Section 6 of the ST.

In addition, vSphere 5.1 implements other policies pertaining to security audit, alarm generation, cryptographic support, user data protection, identification and authentication, security management, protection of the TOE Security Functions, virtual machine domain separation, TOE access, and trusted path. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of vSphere 5.1 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 Assumptions are listed in the ST:

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

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- vSphere 5.1 will be located within controlled access facilities which will prevent unauthorized physical access.

7.3 Clarification of Scope

vSphere 5.1 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

vSphere 5.1 is a software-only TOE comprising ESXi 5.1, VMware Virtual Center 5.1, vCenter Server Appliance, with vCenter Inventory Service and vCenter Single Sign-On, vSphere Client 5.1, vSphere PowerCLI, and vSphere Web Client 5.1. and VMware Update Manager.

The publications entitled:

- VMware vSphere Installation and Setup, vSphere 5.1 Update 1, EN-001098-00; and
- VMware, Inc. vSphere 5.1 Update 1c Update 1 Guidance Documentation Supplement.

describe the procedures necessary to install and operate vSphere 5.1 in its evaluated configuration.

9 Documentation

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

- VMware vSphere Installation and Setup, vSphere 5.1 Update 1, EN-001098-00;
- VMware vSphere Upgrade Guide, vSphere 5.1 Update 1, EN-001099-00;
- VMware vCenter Server Host Management Guide, Update 1, ESXi 5.1, vCenter 5.1, EN-001100-02;
- VMware vSphere Virtual Machine Administration Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001095-00;
- VMware vSphere Host Profiles Guide, ESXi 5.1, vCenter Server 5.1, EN-000795-00;
- VMware vSphere Networking Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001101-01;
- VMware vSphere Storage Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001097-00;
- VMware vSphere Security Guide, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001181-01;
- VMware vSphere Resource Management Guide, ESXi 5.1, vCenter Server 5.1, EN-000793-00;

- VMware vSphere Availability Guide, ESXi 5.1, vCenter Server 5.1, EN-000916-00;
- VMware vSphere Monitoring and Performance Guide, Update 1, vSphere 5.1, vCenter Server 5.1, ESXi 5.1, EN-001102-01;
- VMware vSphere Troubleshooting, Update 1, ESXi 5.1, vCenter Server 5.1, EN-001096-00;
- VMware vSphere Examples and Scenarios Guide, Update 1, vSphere 5.1, vCenter Server 5.1, ESXi 5.1, EN-001178-00;
- VMware vSphere Command-Line Interface Concepts and Examples, ESXi 5.1, vCenter Server 5.1, EN-000887-00;
- VMware vSphere Getting Started with vSphere Command Line Interfaces, ESXi 5.1, vCenter Server 5.1, EN-000886-00;
- VMware vSphere PowerCLI User's Guide, vSphere PowerCLI 5.1 Release 2, EN-001053-00;
- Installing and Administering VMware vSphere Update Manager, Update 1, vSphere Update Manager 5.1, EN-001119-00; and
- VMware, Inc. vSphere 5.1 Update 1c Update 1 Guidance Documentation Supplement.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of vSphere 5.1, including the following areas:

Development: The evaluators analyzed the vSphere 5.1 functional specification and design documentation; 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 vSphere 5.1 security architectural description and determined that the initialization process is secure, 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 5.1 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 5.1 configuration management system and associated documentation was performed. The evaluators found that the vSphere 5.1 configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of vSphere 5.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the vSphere 5.1. 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.

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

11 ITS Product Testing

Testing 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 analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification 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 CGI IT Security Evaluation & Test Facility 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. Identification and Authentication: The objective of this test goal is to demonstrate that the ESXi Server authenticates accounts properly and produces log records;

c. Management of SSO Users: The objective of this test goal is to demonstrate that only a user with SSO Admin privileges can create and delete SSO Users;

d. ESXi Firewall: The objective of this test goal is to verify that only authorized hosts can access services on the ESXi host;

[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.

e. Virtual Switch: The objective of this test goal is to demonstrate that groups on a single server can be isolated from each other with a virtual switch;

f. VM Domain Separation: The objective of this test goal is to show that two virtual machines running on the same system do not interfere with each other;

g. Cryptographic zeroizing: The objective is to verify that a files content can be over written with zeroes using a specific ESXi command;

h. Access Control: The objective of this test goal is to test a users access role in that the user can only access objects to which he has explicitly been given permission; and

i. PowerCLI Interface: The objective of this test goal is to demonstrate the management and automation functionality present when using the PowerCLI Interface.

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:

a. PowerCLI: The objective of this test goal is to attempt to bypass or confuse PowerCLI's authentication mechanism;

b. Web Interface: The objective of this test goal is analyze the vSphere Web Interface for vulnerabilities using the Acunetix web testing tool;

c. Log Attack; The objective of this test goal is to verify that syslogs are properly logged and no information is lost;

d. Password Guessing: The objective of this test goal is to test the TOE's ability to react to online password guess attacks using Burpsuite; and

e. OpenVAS Scan: The objective of this test goal is to analyze the vSphere components using the OpenVAS vulnerability scanner for any well known vulnerabilities.

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

11.4 Conduct of Testing

vSphere 5.1 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 IT Security Evaluation & Test Facility. 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, providing assurance that vSphere 5.1 behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 + 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

vSphere 5.1 and all its components form a complex product. Consumers of the TOE should be familiar with the excluded functionality as detailed in the Security target, section 1.5.3 “Product Physical/Logical Features and Functionality not included in the TOE”. No claims are made against them and no vulnerability analysis was performed on them.

The evaluator recommends that administrators of the TOE regularly review the VMware Knowledge Base, and Security Advisories, and adhere to the VMware® vSphere 5.1 Update 1c Guidance Documentation Supplement.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
3-DES-CBC	Triple Data Encryption Algorithm, Cipher Block Chaining
AES-CBC	Advanced Encryption Standard – Cipher Block Chaining
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Keyed-Hash Message Authentication Code
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
RSA-PKCS1	Rivest Shamir Adleman – Public Key Cryptography Standard
SHA-1	Secure Hash Algorithm
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. VMware® vSphere 5.1 Update 1c Security Target, 1.1, 28 January 2014.

e. VMware® vSphere 5.1U1c ETR 1.0 February 24, 2014.