Certification Report

VMware® vSphere 5.5 Update 2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-300-CR
Version:	1.0
Date:	30 June 2015
Pagination:	i to iii, 1 to 11

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, applies 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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 30 June 2015, 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 5.5 Update 2 (hereafter referred to as VMware® vSphere 5.5), from VMware, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that TOE short name meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 30 June 2015 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 VMware® vSphere 5.5, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the VMware® vSphere 5.5 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

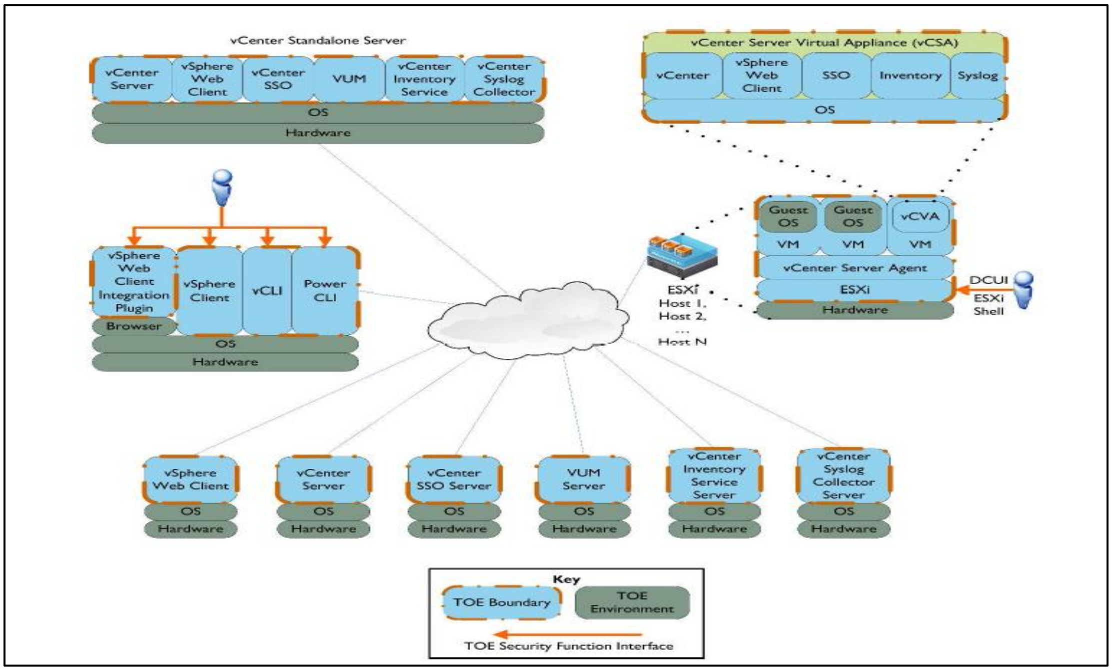
The Target of Evaluation (TOE) for this EAL 2+ evaluation is VMware® vSphere 5.5 Update 2 (hereafter referred to as VMware® vSphere 5.5), from VMware, Inc..

2 TOE Description

The TOE is a system that provides an environment to host multiple virtual machines on industry standard x86-compatible hardware platforms (64-bit) and provides the management of these virtual machines. Each virtual machine acts as a physically separated guest and only communicates with other virtual machines using standard networking protocols.

The vCenter Server acts as a management console server, and is responsible for deploying, monitoring, and managing virtual machines that are distributed across multiple hosts running the ESXi software. The Inventory Service maintains information about all the ESXi hosts managed by a vCenter server. vSphere Update Manager handles updates and patches for the TOE. SSO performs all authentication for vCenter users. The Syslog Collector manages system logs from distributed TOE components. On the client machines, the vSphere Client, vCLI, and vSphere Web Client provide interfaces for administrators and users accessing vCenter and ESXi.

A diagram of the VMware® vSphere 5.5 architecture is as follows:



3 Security Policy

VMware® vSphere 5.5 implements a role-based access control policy to control administrative access to the system. In addition, VMware® vSphere 5.5 implements policies pertaining to the following security functional classes:

- *Security Audit*
- *Cryptographic Support*
- *User Data Protection*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TOE Security Functions (TSF)*
- *Resource Utilization*
- *Virtual Machine Domain Separation*
- *TOE Access*
- *Trusted Path/Channel*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in VMware® vSphere 5.5:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1956, 1955, 1945, 1956, 1949
Advanced Encryption Standard (AES)	FIPS 197	3467, 3466, 3454, 3455, 3458
Rivest Shamir Adleman (RSA)	ANSI X9.31	1778, 1777, 1769, 1770, 1773
Secure Hash Algorithm (SHA-1)	FIPS 180-4	2862, 2861, 2850, 2851, 2854
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	2212, 2211, 2200, 2201, 2204
Random Number Generator (RNG)	ANSI X9.31	1386, 1385, 1377, 1380
Digital Signature Algorithm (DSA)	FIPS 186-4	980, 979, 972, 975

4 Security Target

The ST associated with this Certification Report is identified below:

VMware® vSphere 5.5 Update 2 Security Target, Version 0.6, 28 June 2015

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.*

VMware® vSphere 5.5 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:

- *ALC_FLR.3 Systematic flaw remediation*

b. *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.1	*System event automatic response*
EXT_FAU_STG.1	*External audit trail storage*
EXT_FIA_VC_LOGIN.1	*vCenter SSO user login request*
EXT_VDS_VMM.1	*ESXi virtual machine domain separation*

c. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of VMware® vSphere 5.5 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

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

6.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- VMware® vSphere 5.5 will be located within controlled access facilities which will prevent unauthorized physical access.

6.3 Clarification of Scope

VMware® vSphere 5.5 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

7 Evaluated Configuration

The evaluated configuration for VMware® vSphere 5.5 comprises:

- ESXi 5.5 Update 2 (build 2075275)
- vCenter Inventory Service 5.5 Update 2 (build 2105955)
- vSphere Client 5.5 Update 2 (1993072)
- vSphere Web Client 5.5 Update 2 (build 2105955)
- vSphere Web Client Integration Plugin 5.5 Update 2 (build 2105955)
- vSphere Update Manager 5.5 Update 2 (build 2105955)
- vCenter Server Virtual Appliance 5.5 Update 2 (build 2063318)
- vCenter Server Virtual Appliance 5.5 Update 2a Patch (build 2170515)
- vSphere Command-Line Interface (vCLI) 5.5 Update 2 (build 2043780)

On a GPC running Windows Server 2008 R2.

- vCenter Server 5.5 Update 2 (build 2105955) and vCenter Single Sign-On 5.5 Update 2 (build 2105955) was tested as part of vCenter Server Appliance running on Suse Linux Enterprise 11.
- vCenter Server 5.5 Update 2 (build 2105955) and vSphere PowerCLI 5.8 Release 1 (build 2057893) were installed and tested on Windows 7 Enterprise SP1 64 Bit.

The publications entitled VMware vSphere Installation and Setup, vSphere 5.5 Update 2 as well as VMware vSphere 5.5 Update 2 Guidance Document Supplement version 0.2 describe the procedures necessary to install and operate vSphere 5.5 Update 2 in its evaluated configuration.

8 Documentation

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

a. VMware vSphere Installation and Setup, vSphere 5.5 Update 2, EN-001515-01

b. VMware vSphere Upgrade Guide, vSphere 5.5 Update 2, EN-001516-00

c. VMware vCenter Server Host Management Guide, Update 2, ESXi 5.5, vCenter 5.5, EN-001520-00

d. VMware vSphere Virtual Machine Administration Guide, Update 2, ESXi 5.5, vCenter Server 5.5, EN-001518-00

e. VMware vSphere Host Profiles Guide, Update 1, ESXi 5.5, vCenter Server 5.5, EN 001347-01

f. VMware vSphere Networking Guide, Update 2, vSphere 5.5, ESXi 5.5, vCenter Server 5.5, EN-001549-00

g. VMware vSphere Storage Guide, Update 2, ESXi 5.5, vCenter Server 5.5, EN-001523-00

h. VMware vSphere Security Guide, Update 2, ESXi 5.5, vCenter Server 5.5, EN-001517-00

i. VMware vSphere Resource Management Guide, Update 2, ESXi 5.5, vCenter Server 5.5, EN-001584-00

j. VMware vSphere Availability Guide, ESXi 5.5, vCenter Server 5.5, EN-001254-00

k. VMware vSphere Monitoring and Performance Guide, Update 2, vSphere 5.5, vCenter Server 5.5, ESXi 5.5, EN-001557-00

l. VMware vSphere Single Host Management Guide, Update 1, vSphere 5.5, ESXi 5.5, EN-001355-01

m. VMware vSphere Troubleshooting, Update 1, ESXi 5.5, vCenter Server 5.5, EN-001419-00

n. VMware vSphere Command-Line Interface Concepts and Examples, ESXi 5.5 Update 1, vCenter Server 5.5 Update 1, EN-001406-00

o. VMware Command-Line Management in vSphere 5 for Service Console Users, ESXi 5.5 Update 1, EN-001405-00

p. VMware vSphere Getting Started with vSphere Command Line Interfaces, ESXi 5.5 Update 1,vCenter Server 5.5 Update 1, EN-001404-00

q. VMware vSphere Web Services SDK Programming Guide, vSphere Web Services SDK 5.5, EN-001153-00

r. VMware vSphere PowerCLI User’s Guide, vSphere PowerCLI 5.8 Release 1, EN-001550-00

s. Installing and Administering VMware vSphere Update Manager, Update 2, vSphere Update Manager 5.5, EN-001542-00

t. VMware, Inc. vSphere 5.5 Update 2 Guidance Documentation Supplement, Version 0.3

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of VMware® vSphere 5.5, including the following areas:

Development: The evaluators analyzed the VMware® vSphere 5.5 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 VMware® vSphere 5.5 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 VMware® vSphere 5.5 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 VMware® vSphere 5.5 configuration management system and associated documentation was performed. The evaluators found that the TOE short name configuration items were clearly marked.

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

The evaluators reviewed the flaw remediation procedures used by developer for the VMware® vSphere 5.5. 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.

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 test goals:

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

[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.

   a. Management of SSO Users: The objective of this test goal is to show that only a user with SSO Admin privileges can manage SSO Users and Identity sources;

   b. Reading Audit Records: The objective of this test case is to demonstrate that a valid vCenter Server User can view audit logs collected by the Syslog Collector available to the user according to the vCenter Server Access Control Policy;

   c. User and Role Management: The objective of this test goal is to demonstrate that users of different roles have different access levels; and

   d. Secure Communication: The objective of this test goal is to demonstrate secure communication with TLS.

b. Access Control on the vSphere Client, vSphere Web Client and Single Sign-On Modules: The objective of this test case is to show a user can only see the inventory objects to which he has explicitly been given permission. The test also shows that there are two distinct roles for the vCenter Server, by showing that users in the vCenter Server's Administrator role can alter permission pairs (on objects and users) which the limited access User role cannot; and

c. PowerCLI VM and Authentication Manipulation: The objective of this test goal is to demonstrate the management functionality present over the PowerCLI interface (as the evaluator noted that there was only account creation tested by the Vendor on this interface.) The test will demonstrate some of the other management functionality that is present over this interface such as creating a VM and demonstrate the access control is respected. Additionally the lab provides a negative test for the user authentication in this test case.

10.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. PowerCLI Manipulation of VMs: The objective of this test case is to show that ESXi hosts have the ability to invoke operating-system-level commands on guest operating systems from the vSphere host. This raises the risk that separation of domains might be broken. The defense against this is user authentication. This test will try to bypass that authentication using users of different authorization levels available on the ESXi host, and different levels and methods for login to the guest operating system; and

c. Password Guessing: The objective of this test goal is to demonstrate how the TOE will react against online password guess attacks on the web interface, either by throttling attempts or logging the attack for notification of an administrator.

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

10.4 Conduct of Testing

VMware® vSphere 5.5 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that VMware® vSphere 5.5 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

VMware® vSphere 5.5 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 5.5 Update 2 Guidance Documentation Supplement.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
3DES	Triple-DES
AES	Advanced Encryption standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DSA	Digital Signature Algorithm
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
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm
SSO	Single sign-on
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
RNG	Random Number Generator
RSA	Rivest Shamir Adleman

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 4, September 2012.

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

d. VMware® vSphere 5.5 Update 2 Security Target, Version 0.6, 28 June 2015

e. VMware Inc. VMware vSphere 5.5 Update 2 Common Criteria EAL 2+ Evaluation Technical Report, Version 1.0, 30 June 2015.