Certification Report

Nutanix Virtual Computing Platform v3.5.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-272-CR
Version: 1.0
Date: 22 September 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, 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 22 September 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).

TABLE OF CONTENTS

Executive Summary

Nutanix Virtual Computing Platform v3.5.1 (hereafter referred to as Nutanix VCP v3.5.1), from Nutanix, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Nutanix VCP v3.5.1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Nutanix VCP v3.5.1 is a virtualization platform composed of a networked cluster of nodes that can host VMs offering services to users (typically as virtual servers). These virtual servers can be used for any application the users of the server require, such as web, email, or others. Nutanix VCP v3.5.1also offers storage for those VMs to use when offering services. The unification of storage and virtualization on a single platform eliminates the need for a separate storage network.

Nodes are hardware boards housed within one or more chassis running the NOS (Nutanix Operating System) software and provide all of the functionality for the cluster except data storage. Data storage is provided by the disk hardware housed within the chassis. Each node provides storage and virtualization services to users, with multiple nodes being used for redundancy.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 26 August 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 Nutanix VCP v3.5.1, 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 Nutanix VCP v3.5.1 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

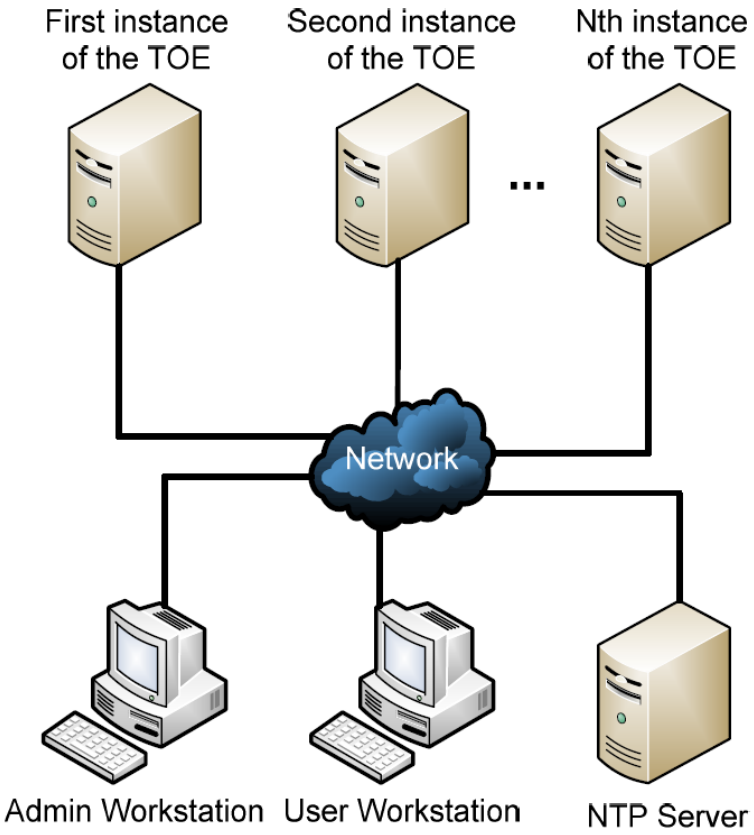
The Target of Evaluation (TOE) for this EAL 2+ evaluation is Nutanix Virtual Computing Platform v3.5.1 (hereafter referred to as Nutanix VCP v3.5.1), from Nutanix, Inc..

2 TOE Description

Nutanix VCP v3.5.1 is a virtualization platform composed of a networked cluster of nodes that can host VMs offering services to users (typically as virtual servers). These virtual servers can be used for any application the users of the server require, such as web, email, or others. The Nutanix VCP v3.5.1also offers storage for those VMs to use when offering services. The unification of storage and virtualization on a single platform eliminates the need for a separate storage network.

Nodes are hardware boards housed within one or more chassis running the NOS software and provide all of the functionality for the cluster except data storage. Data storage is provided by the disk hardware housed within the chassis. Each node provides storage and virtualization services to users, with multiple nodes being used for redundancy.

A diagram of the Nutanix VCP v3.5.1 architecture is as follows:



3 Security Policy

Nutanix VCP v3.5.1 implements a role-based access control policy to control administrative access to the system. In addition, Nutanix VCP v3.5.1 implements policies pertaining to the following security functional classes:

- *Security Audit;*
- *User Data Protection;*
- *Identification and Authentication;*
- *Security Management;*
- *Protection of the TSF;*
- *Resource Utilization; and*
- *TOE Access.*

4 Security Target

The ST associated with this Certification Report is identified below:

Nutanix, Inc. Virtual Computing Platform v3.5.1 Security Target v0.11, 27 August 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.*

Nutanix VCP v3.5.1 is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
    - *ALC_FLR.2 – Flaw reporting procedures*

b. *Common Criteria Part 2 conformant; with security functional requirements based only upon functional components in Part 2;*

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 Nutanix VCP v3.5.1 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *Administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance;*
- *TOE users accessing the storage on the TOE reside on the internal network and are not careless, negligent, or willfully hostile with regard to their access of the TOE.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE is located within a controlled access facility and is physically available to authorized administrators only;*
- *The IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE;*
- *The IT Environment will provide the time for the TOE from a reliable source;*
- *The network that the TOE uses for storage transfer is intended to be an internal private network that is protected from access by entities outside of the organization. External access to storage services are blocked by the TOE environment.*

6.3 Clarification of Scope

- Guest VMs are not included within the TOE boundary and none of the functionality they provide has been tested as part of this evaluation
- The management interfaces for the hypervisor are not included within the TOE boundary and should be considered part of the IT environment.
- The cryptography used in the HTTPS connections for management sessions via the GUI and the CLI has not been tested as part of this evaluation.

7 Evaluated Configuration

The evaluated configuration for Nutanix VCP v3.5.1 comprises:

The NOS v3.5.1 running on one of the following supported chassis with VMware ESXi v5.1 U1;

- *NX-1050 series,*
- *NX-3050 series,*
- *NX-3051 series,*
- *NX-3060 series,*
- *NX-3061 series,*
- *NX-6020 series,*
- *NX-6050 series,*
- *NX-6060 series,*
- *NX-6070 series,*
- *NX-6080 series,*
- *NX-7110 series.*

The publication entitled Nutanix, Inc. Virtual Computing Platform v3.5.1 Guidance Supplement v0.6 describes the procedures necessary to install and operate Nutanix VCP v3.5.1 in its evaluated configuration.

8 Documentation

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

a. Nutanix, Inc. Virtual Computing Platform v3.5.1 Guidance Supplement v0.6;

b. Nutanix Platform Administration Guide NOS 3.5 15-April-2014;

c. Nutanix Web Console Guide NOS 3.5 15-April-2014;

d. Nutanix Command Reference Guide NOS 3.5 13-March-2014;

e. Nutanix Setup Guide NOS 3.5 15-April-2014;

f. Nutanix REST API Reference NOS 3.5 03-January-2014;

g. Nutanix Physical Installation Guide NX-1000, NX-3050,NX-6000, and NX-7000 Series 764-0015-0004 Rev A 15-April-2014;

h. Nutanix Upgrade Guide NOS 3.5.1 27-March-2014; and

i. *Nutanix Release Notes NOS 3.5.1 18-February-2014.*

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Nutanix VCP v3.5.1, including the following areas:

Development: The evaluators analyzed the Nutanix VCP v3.5.1 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 Nutanix VCP v3.5.1 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 Nutanix VCP v3.5.1 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 Nutanix VCP v3.5.1 configuration management system and associated documentation was performed. The evaluators found that the Nutanix VCP v3.5.1 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 Nutanix VCP v3.5.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Nutanix VCP v3.5.1. 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.

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;

b. Privilege escalation: The objective of this test goal is to confirm that a user cannot escalate their privileges from one type of administrator to another;

c. Audit generation: The objective of this test goal is to test the audit generation functionality using a variety of parameters; and

d. REST API: The objective of this test goal is to test the ability of an administrator to manage the TOE using the Nutanix REST API.

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. HeartBleed: The objective of this test goal is to determine if the TOE is susceptible to HeartBleed;

c. NFS Whitelist: The objective of this test goal is to attempt to gain access to restricted storage using Whitelisted IPs; and

[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.

d. IPMI port vulnerability: The objective of this test goal is to connect to the IPMI port and attempt to gain access to protected user credentials.

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

10.4 Conduct of Testing

Nutanix VCP v3.5.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Nutanix VCP v3.5.1 behaves as specified in its ST and functional specification.

11 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.

12 Evaluator Comments, Observations and Recommendations

TOE users should be aware that at least four (4) independent nodes are required to comprise the evaluated configuration. These nodes are not required to be situated within a single chassis, but users should consult appropriate Nutanix documentation to ensure their node selection is appropriate for their needs.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application programming interface
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
IPMI	Intelligent Platform Management Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NOS	Nutanix Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
REST	Representational State Transfer
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VCP	Virtual Computing Platform
VM	Virtual Machine

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. Nutanix, Inc. Virtual Computing Platform v3.5.1 Security Target v0.11, 27 August 2014

e. Nutanix, Inc. Virtual Computing Platform v3.5.1 Common Criteria EAL2+ Evaluation Evaluation Technical Report (ETR) v1.0, Aug 26, 2014.