Certification Report

Tintri VMstore v3.1.2.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-318-CR
Version:	1.0
Date:	10 August 2015
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 10 August 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).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Tintri VMstore v3.1.2.1, from Tintri, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Tintri VMstore v3.1.2.1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Tintri VMstore v3.1.2.1 is a hybrid storage solution designed exclusively for virtual machines (VMs). It utilizes both flash-based solid-state drives (SSD) and hard-disk drives (HDD) for storage. The TOE provides administrative users with a single view of all the VMs registered, allowing them to manage, monitor and control the VMs and their mounted vDisks without having detailed knowledge of the underlying storage infrastructure.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 10 August 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 Tintri VMstore v3.1.2.1, 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 Tintri VMstore v3.1.2.1 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).

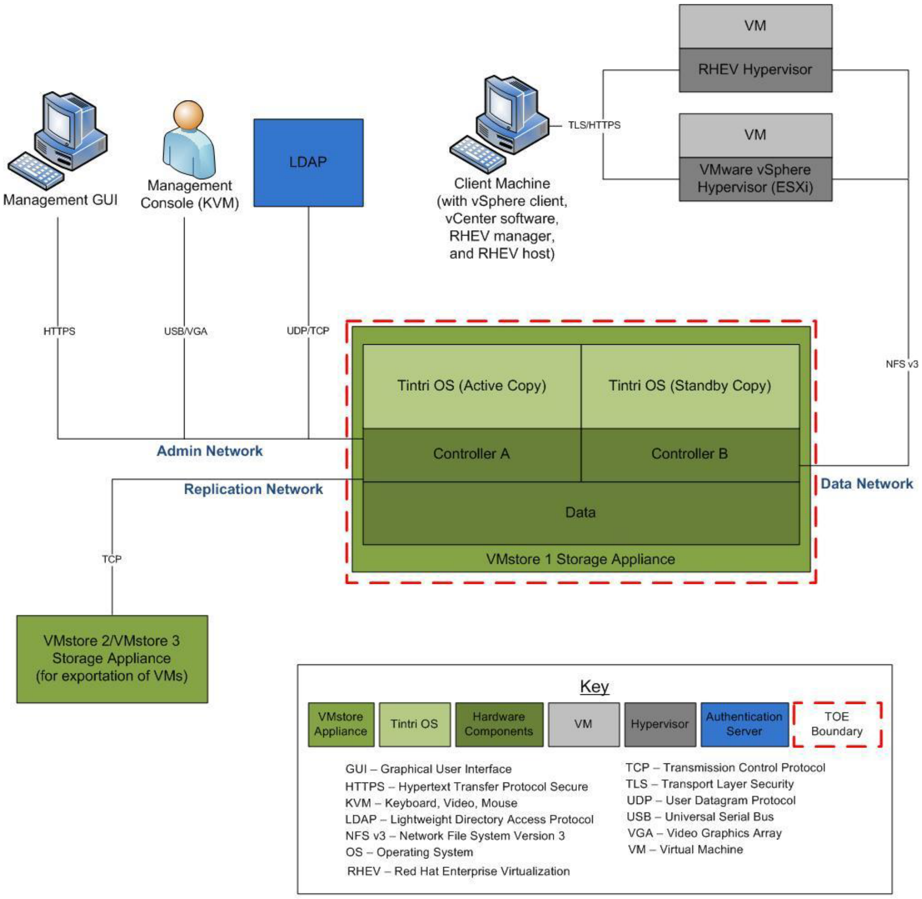
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is Tintri VMstore v3.1.2.1, from Tintri, Inc..

2 TOE Description

Tintri VMstore v3.1.2.1 is a hybrid storage solution designed exclusively for VMs. It utilizes both flash-based solid-state drives (SSD) and hard-disk drives (HDD) for storage. The TOE provides administrative users with a single view of all the VMs registered, allowing them to manage, monitor and control the VMs and their mounted vDisks without having detailed knowledge of the underlying storage infrastructure.

A diagram of the Tintri VMstore v3.1.2.1 architecture is as follows:


VM
RHEV Hypervisor
VM
VMware vSphere Hypervisor (ESXi)
TLS/HTTPS
Management GUI
Management Console (KVM)
LDAP
Client Machine (with vSphere client, vCenter software, RHEV manager, and RHEV host)
HTTPS
USB/VGA
UDP/TCP
NFS v3
Tintri OS (Active Copy)
Tintri OS (Standby Copy)
Admin Network
Controller A
Controller B
Replication Network
Data Network
Data
VMstore 1 Storage Appliance
TCP
VMstore 2/VMstore 3 Storage Appliance (for exportation of VMs)
Key
VMstore Appliance
Tintri OS
Hardware Components
VM
Hypervisor
Authentication Server
TOE Boundary
GUI – Graphical User Interface
HTTPS – Hypertext Transfer Protocol Secure
KVM – Keyboard, Video, Mouse
LDAP – Lightweight Directory Access Protocol
NFS v3 – Network File System Version 3
OS – Operating System
RHEV – Red Hat Enterprise Virtualization
TCP – Transmission Control Protocol
TLS – Transport Layer Security
UDP – User Datagram Protocol
USB – Universal Serial Bus
VGA – Video Graphics Array
VM – Virtual Machine

3 Security Policy

Tintri VMstore v3.1.2.1 implements a role-based access control policy to control administrative access to the system. In addition, Tintri VMstore v3.1.2.1 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
- TOE Access

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target: Tintri VMstore v3.1.2.1, version 1.4, 10 August 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.*

Tintri VMstore v3.1.2.1 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 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - FIA_UIA_EXT.1 - Administrative User Identification and Authentication
    - FPT_TST_EXT.1 - TSF Testing

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 Tintri VMstore v3.1.2.1 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:

- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- Only trusted devices will have access to the TOE data path. Users are assumed to be trusted not to spoof the IP address used for accessing the TOE data path.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located within a controlled access facility and appropriately located within the network to perform its functions. The connection between the TOE and the target appliance for the exportation of data is also located within a controlled access facility.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or administrative user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
- The TOE is protected from external tampering and interferences.
- The TOE is protected from hostile or unauthorized access to the TOE management interface.

6.3 Clarification of Scope

The following functionality is excluded from the scope of the evaluation;

- SSH
- Management Console Access via KVM
- Autosupport
- Tintri VAAI plug-in
- SMTP services
- SNMPv3 services
- NTP services

7 Evaluated Configuration

The evaluated configuration for Tintri VMstore v3.1.2.1 comprises:

The VMstore firmware (v3.1.2.1) running on one of the following Tintri appliances;

- T820
- T850
- T880

With support from the environment;

- LDAP server
- VMstore 2/VMstore 3 storage appliance
- VMware vSphere and Red Hat Enterprise Virtualization (RHEV) Hypervisors

8 Documentation

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

a. Tintri VMstore v3.1.2.1 Development and Architecture Document, Version 0.6;

b. Guidance Documentation Supplement Tintri VMstore v3.1.2.1 version 0.4 ;

c. 750-5000-6001-Q Tintri VMstore System Administration Manual;

d. 761-6001-0001-E Tintri VMstore T800 Series Reference Guide; and

e. 65-0301-0201-RevB Tintri VMstore Release Notes.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Tintri VMstore v3.1.2.1, including the following areas:

Development: The evaluators analyzed the Tintri VMstore v3.1.2.1 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 Tintri VMstore v3.1.2.1 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 Tintri VMstore v3.1.2.1 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 Tintri VMstore v3.1.2.1 configuration management system and associated documentation was performed. The evaluators found that the Tintri VMstore v3.1.2.1 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 Tintri VMstore v3.1.2.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Tintri VMstore v3.1.2.1. 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. Identification and authentication via REST API call: The objective of this test goal is to confirm that users and authenticate via the REST API call;

c. User roles: The objective of this test goal is to confirm that users can be created/modified/deleted and that user roles can be assigned;

d. Configuring Active directory Services: The objective of this test goal is to confirm that the TOE can be configured to use active directory;

e. Failure with preservation of secure state: The objective of this test goal is to confirm that the TOE and preserve a secure state in the event of a system failure;

f. Configuring NFS: The objective of this test goal is to confirm that the TOE can be configured to use NFS; and

g. Configuring Exportation & Snapshot services: The objective of this test goal is to confirm that the exportation and snapshot services offered by the TOE can be properly configured.

[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.

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. NFS IP spoofing: The objective of this test goal is to gain access to restricted storage using IP spoofing; and

c. DOS attack: The objective of this test goal is to cause the TOE to fail using a DOS attack.

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

10.4 Conduct of Testing

Tintri VMstore v3.1.2.1 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 Tintri VMstore v3.1.2.1 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

Consumers of the Tintri VMstore v3.1.2.1 should be aware that at least two appliances are required to comprise the evaluated configuration. This is required to enforce the VM HA Access Control Policy and export the stored VM’s to another VMstore appliance.

13 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
DOS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NFS	Network File System
PALCAN	Program for the Accreditation of Laboratories - Canada
REST API	Representational State Transfer Application Programming Interface
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

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. Security Target: Tintri VMstore v3.1.2.1, version 1.4, 10 August 2015

e. Tintri VMstore v3.1.2.1 Common Criteria EAL2+ Evaluation Evaluation Technical Report v1.0, 10 August 2015.