Certification Report

EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-330-CR
Version: 1.0
Date: 15 July 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 EWA-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, 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 15 July 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:

- VNXe™ and VNXe3200™ are trademarks of EMC Corporation.

TABLE OF CONTENTS

Executive Summary

EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware (hereafter referred to as VNXe3200™), from EMC Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that VNXe3200™ meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

VNXe3200™ allows an organization to manage its storage needs separately from its application and file servers. This allows for control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application or file servers.

The VNXe Operating Environment v3.1.1 provides Redundant Array of Independent Disks (RAID) and storage capabilities and provides administrators the ability to manage and configure the TOE via the Unified Element Manager Command Line Interface (UEMCLI) and the Unisphere Graphical User Interface (GUI). The VNXe3200™ hardware platform includes the back-end disk arrays. Together, these components provide Block and File access to internal storage for external entities.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 15 July 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 VNXe3200™, 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 VNXe3200™ 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

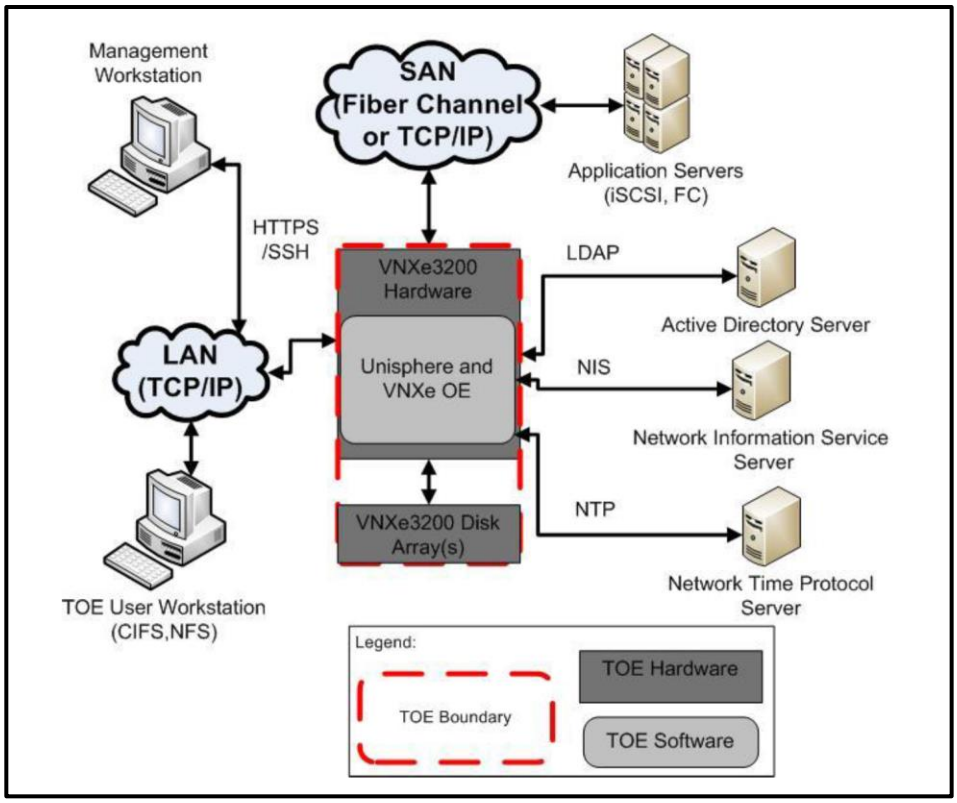
The Target of Evaluation (TOE) for this EAL 2+ evaluation is EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware (hereafter referred to as VNXe3200™), from EMC Corporation.

2 TOE Description

VNXe3200™ allows an organization to manage its storage needs separately from its application and file servers. This allows for control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application or file servers.

The VNXe Operating Environment v3.1.1 provides Redundant Array of Independent Disks (RAID) and storage capabilities and provides administrators the ability to manage and configure the TOE via the Unified Element Manager Command Line Interface (UEMCLI) and the Unisphere Graphical User Interface (GUI). The VNXe3200™ hardware platform includes the back-end disk arrays. Together, these components provide Block and File access to internal storage for external entities.

A diagram of the VNXe3200™ architecture is as follows:



3 Security Policy

VNXe3200™ implements a role-based access control policy to control administrative access to the system. In addition, VNXe3200™ implements policies pertaining to the following security functional classes:

- *Security Audit*
- *User Data Protection*
- *Identification and Authentication*
- *Security Management*

4 Security Target

The ST associated with this Certification Report is identified below:

EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware Security Target, Version 1.2, July 8, 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.*

VNXe3200™ 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 VNXe3200™ 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:

- *There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.*
- *Administrators are non-hostile, appropriately trained, and follow all administrator guidance.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *Physical security will be provided for the TOE and its environment.*
- *The IT environment provides the TOE with the necessary reliable timestamps.*

7 Evaluated Configuration

The evaluated configuration for VNXe3200™ comprises EMC VNXe Operating Environment v3.1.1 software (includes EMC VNXe Unisphere) and EMC VNXe Unisphere UEMCLI v3.0 running on the EMC VNXe3200™ hardware platform.

The TOE requires the following components in the operational environment:

- Management workstation used to access the Unisphere GUI via a web browser or the UEMCLI
- LDAPv3-compatible Server
- NTP Server
- NIS Server
- Application Servers accessing Block storage
- Client Systems accessing File storage

The publication entitled EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware Guidance Documentation Supplement, Version 0.3, June 5, 2015 describes the procedures necessary to install and operateVNXe3200™ in its evaluated configuration.

8 Documentation

The EMC Corporation documents provided to the consumer are as follows:

a. EMC Unisphere for VNXe Online Help, January 2015;

b. EMC VNXe Unisphere CLI User Guide, January 2015;

c. EMC VNXe Security Configuration Guide, May 2014;

d. EMC VNXe Series Quick Start, Revision 01;

e. EMC VNXe Series Using a VNXe3200 System with Fibre Channel or iSCSI LUNs, June 2014;

f. EMC VNXe Series Using a VNXe3200 System with NFS File Systems, November 2014;

g. EMC VNXe Series Using a VNXe3200 System with CIFS File Systems, November 2014;

h. VNXe Series VNXe3200 Hardware Information Guide, January 2015;

i. EMC VNXe3200 Installation Guide, July 2014; and

j. EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware Guidance Documentation Supplement, Version 0.3, June 5, 2015.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of TOE short name, including the following areas:

Development: The evaluators analyzed the VNXe3200™ 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 TOE short name 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 VNXe3200™ 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 VNXe3200™ configuration management system and associated documentation was performed. The evaluators found that the VNXe3200™ 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 VNXe3200™ during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the VNXe3200™. 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. Local User Roles and Access Control Lists: The objective of this test goal is to verify the enforcement of password composition rules and the use of the administrator role for password changes;

c. Trusted Path: The objective of this test goal is to confirm that communication between the TOE and the remote administrator is appropriately protected; and

d. Health Check: The objective of this test goal is to verify that the TOE can initiate a system health check.

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; and

b. Misuse: The objective of this test goal is to deny real-time access to user data by causing a network outage.

[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.

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

10.4 Conduct of Testing

VNXe3200™ 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 VNXe3200™ 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 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIFS	Common Internet File System
CPL	Certified Products list
CM	Configuration Management
DAE	Disk Array Enclosure
DPE	Disk Processor Enclosure
EAL	Evaluation Assurance Level
EFD	Enterprise Flash Drive
ETR	Evaluation Technical Report
FC	Fibre Channel
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NFS	Network File System
NIS	Network Information Service
NTP	Network Time Protocol
OE	Operating Environment
PALCAN	Program for the Accreditation of Laboratories - Canada
RAID	Redundant Array of Independent Disks
SAS	Serial Attached SCSI
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UEMCLI	Unified Element Manager Command Line Interface

13 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. EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware Security Target, Version 1.2, July 8, 2015.

e. Evaluation Technical Report for EMC Corporation EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware Document No. 1894-000 D002, Version 1.0, 15 July 2015.