Certification Report

EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-280-CR
Version: 1.0
Date: 27 August 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) provide 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 27 August 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:

- EMC, Unisphere, VNX5200, VNX5400, VNX5600, VNX5800, VNX7600 and VNX8000 are registered trademarks of EMC Corporation.

TABLE OF CONTENTS

Executive Summary

EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ (hereafter referred to as EMC VNX OE with Unisphere), from EMC Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that EMC VNX OE with Unisphere meets the requirements of Evaluation Assurance Level (EAL) 2 for the evaluated security functionality.

EMC VNX OE with Unisphere 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.

EMC VNX OE with Unisphere can be divided into three main components. VNX OE is the software portion of the product responsible for access controls and management of storage. Unisphere, Navisphere CLI, and Control Station CLI comprise the management software that allows administrators to maintain and configure the product. VNX is the hardware portion of the product. 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 2 June 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 EMC VNX OE with Unisphere, 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 EMC VNX OE with Unisphere 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

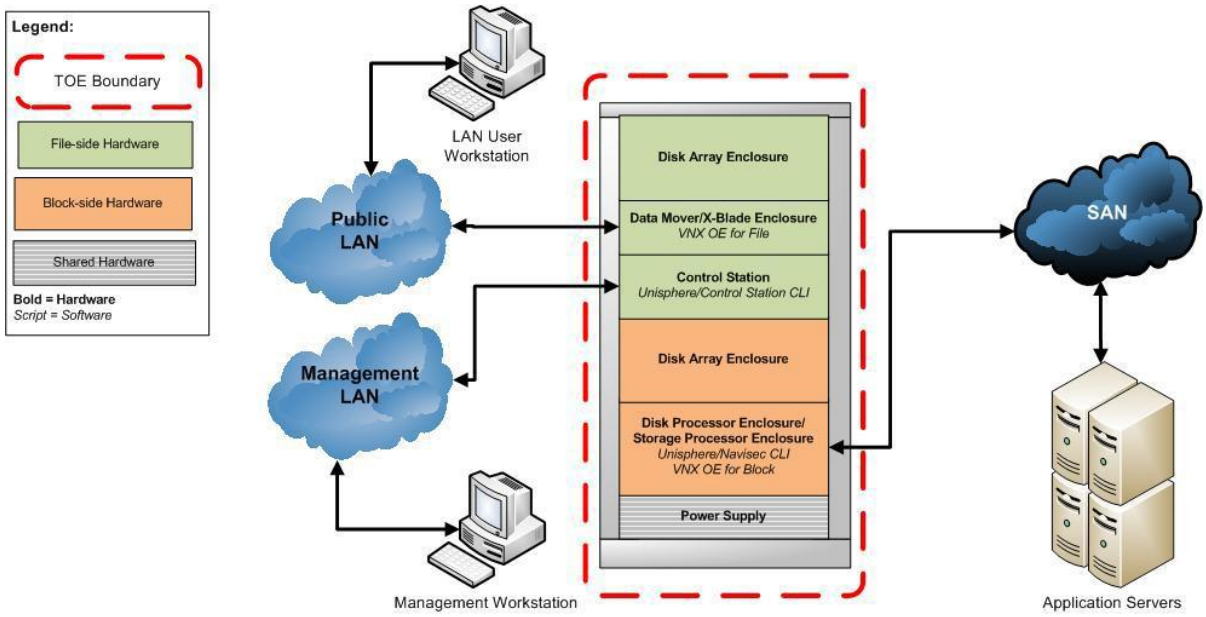
The Target of Evaluation (TOE) for this EAL 2 evaluation is EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ (hereafter referred to as EMC VNX OE with Unisphere), from EMC Corporation.

2 TOE Description

EMC VNX OE with Unisphere 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.

EMC VNX OE with Unisphere can be divided into three main components. VNX OE is the software portion of the product responsible for access controls and management of storage. Unisphere, Navisphere CLI, and Control Station CLI comprise the management software that allows administrators to maintain and configure the product. VNX is the hardware portion of the product. Together, these components provide Block and File access to internal storage for external entities.

A diagram of the EMC VNX OE with Unisphere architecture is as follows;



3 Security Policy

EMC VNX OE with Unisphere enforces a discretionary access control policy to control access to the TOE. In addition, EMC VNX OE with Unisphere implements policies pertaining to the following security functional classes:

- *Security Audit;*
- *User Data Protection;*
- *Identification and Authentication;*
- *Security Management;*
- *Cryptographic Support;*
- *Protection of the TSF; and*
- *Trusted Path/Channel.*

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
OSSI OpenSSL	*1051*
RSA BSAFE Crypto-C ME	*1092*

4 Security Target

The ST associated with this Certification Report is identified below:

EMC® Corporation EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ Security Target v0.5, 24 April 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.*

EMC VNX OE with Unisphere is:

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

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 EMC VNX OE with Unisphere 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 TOE will be managed by competent individuals that are non-hostile, appropriately trained, and follow all 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 shall provide a secure place to store user-data of which access to that data will be mediated by the TOE;
- The TOE Environment will provide identification and authentication of application server users before allowing any other TSF-mediated action on behalf of those users; and
- The IT Environment provides the TOE with the necessary reliable timestamps.

7 Evaluated Configuration

The evaluated configuration for EMC VNX OE with Unisphere comprises:

The following software:

- VNX OE for Block v05.33.000.5.035;
- VNX OE for File v8.1.1.33;
- Unisphere v1.3.1.1.0033; and
- Navisphere CLI v7.33.1.0.33.

running on one of the following hardware models:

VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ .

The following publications describe the procedures necessary to install and operate EMC VNX OE with Unisphere in its evaluated configuration:

- EMC, Setting up a Unisphere Management Station for the VNX Series, P/N 300-015-123, Rev 01;

Each of the hardware models listed above have the following documents specific to the model number:

- Unified Installation Guide;
- Block Installation Guide; and
- File Installation Guide.

8 Documentation

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

- EMC, Setting up a Unisphere Management Station for the VNX Series, P/N 300-015-123, Rev 01;
- EMC VNX, VNX5200 Unified Installation Guide, P/N 300-999-780, Rev 01;
- EMC VNX, VNX5200 Block Installation Guide, P/N 300-999-786, Rev 01;
- EMC VNX, VNX5200 File Installation Guide, P/N 300-999-792, Rev 01;
- EMC VNX Family, VNX5200, Parts Location Guide, PN 300-015-012, Rev 01;
- EMC VNX Family, VNX5200, Hardware Information Guide, P/N 300-014-323, Rev 01;
- EMC VNX, VNX5400 Unified Installation Guide, P/N 300-999-781, Rev 03;
- EMC VNX, VNX5400 Block Installation Guide, P/N 300-999-787, Rev 03;
- EMC VNX, VNX5400 File Installation Guide, P/N 300-999-793, Rev 03;
- EMC VNX Family, VNX5400, Parts Location Guide, PN 300-015-013, Rev 01;
- EMC VNX Family, VNX5400, Hardware Information Guide, P/N 300-014-324, Rev 02;
- EMC VNX, VNX5600 Unified Installation Guide, P/N 300-999-782, Rev 03;
- EMC VNX, VNX5600 Block Installation Guide, P/N 300-999-788, Rev 03;
- EMC VNX, VNX5600 File Installation Guide, P/N 300-999-794, Rev 03;
- EMC VNX Family, VNX5600, Parts Location Guide, PN 300-015-014, Rev 01;
- EMC VNX Family, VNX5600, Hardware Information Guide, P/N 300-014-325, Rev 01;
- EMC VNX, VNX5800 Unified Installation Guide, P/N 300-999-783, Rev 03;
- EMC VNX, VNX5800 Block Installation Guide, P/N 300-999-789, Rev 03;
- EMC VNX, VNX5800 File Installation Guide, P/N 300-999-795, Rev 03;
- EMC VNX Family, VNX5800, Parts Location Guide, PN 300-015-015, Rev 01;
- EMC VNX Family, VNX5800, Hardware Information Guide, P/N 300-014-326, Rev 02;
- EMC VNX, VNX7600 Unified Installation Guide, P/N 300-999-790, Rev 03;
- EMC VNX, VNX7600 Block Installation Guide, P/N 300-999-784, Rev 03;
- EMC VNX, VNX7600 File Installation Guide, P/N 300-999-796, Rev 03;
- EMC VNX Family, VNX7600, Parts Location Guide, PN 300-015-016, Rev 01;
- EMC VNX Family, VNX7600, Hardware Information Guide, P/N 300-014-327, Rev 02;
- EMC VNX, VNX8000 Unified Installation Guide, P/N 300-999-791, Rev 03;
- EMC VNX, VNX8000 Block Installation Guide, P/N 300-999-785, Rev 03;
- EMC VNX, VNX8000 File Installation Guide, P/N 300-999-797, Rev 03;
- EMC VNX Family, VNX8000, Parts Location Guide, PN 300-015-017, Rev 01;
- EMC VNX Family, VNX8000, Hardware Information Guide, P/N 300-014-328, Rev 02;
- EMC VNX Series, Release 5.33, Command Line Interface Reference for Block P/N 300-015-135 Rev 01;

- EMC VNX Series, Release 8.1, Command Line Interface Reference for File P/N 300-014-338 Rev 01;
- EMC VNX Series, Release 8.1, Security Configuration Guide for VNX, P/N 300-015-128, Rev 01;
- EMC VNX Series, Release 8.1, System Operations, P/N 300-015-124, Rev 02;
- EMC VNX Series, Release 8.1, Configuring NFS on VNX, P/N 300-014-336, Rev 01;
- EMC VNX Series, Release 8.1, Configuring and Managing CIFS on VNX, P/N 300-014-332, Rev 01;
- EMC VNX Series, Release 8.1, Controlling Access to VNX System Objects, P/N 300-015-106, Rev 01;
- EMC VNX Series, Release 8.1, Using FTP, TFTP, and SFTP on VNX, P/N 300-015-134, Rev 01;
- EMC VNX, Configuring Time Services on VNX, P/N 300-015-103, Rev 01;
- EMC VNX, VNX Operating Environment for Block 05.33.000.5.035, VNX Operating Environment for File 8.1.1.33, EMC Unisphere 1.3.1.1.0033, Release Notes, P/N 32-000-403, Rev 02;
- EMC VNX Unisphere Online Help 1.3;

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of EMC VNX OE with Unisphere, including the following areas:

Development: The evaluators analyzed the EMC VNX OE with Unisphere functional specification and determined that the functional specification and TOE design describes the purpose and method of use for each TSF interface and that the EMC VNX OE with Unisphere functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the EMC VNX OE with Unisphere 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 EMC VNX OE with Unisphere configuration management system and associated documentation was performed. The evaluators found that the EMC VNX OE with Unisphere 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 EMC VNX OE with Unisphere during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the EMC VNX OE with Unisphere. 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. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the ST;

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

c. Audit log creation and review: The objective of this test goal is to confirm that the TOE records administrative actions that result in a configuration change as well as all administrative login attempts;

d. RAID 1, RAID 1+0, RAID 3: The objective of these test goals is to demonstrate that the TOE supports RAID 1, RAID 1+0 and RAID 3;

e. Verification of Roles: The objective of this test goal is to confirm that the authorized roles as described in the ST have been implemented; and

f. Trusted Path; The objective of this test goal is to confirm that communications between the TOE and remote users is appropriately protected.

[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; and
b. Search of public domain information sources for vulnerabilities for the TOE, its underlying software, applications, and specific hardware or design components used in the TOE.

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

10.4 Conduct of Testing

EMC VNX OE with Unisphere 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 EMC VNX OE with Unisphere 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

TOE customers must pay particular attention to the installation guidance to ensure that the TOE is implemented in the evaluated configuration.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ANSI	American National Standards Institute
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
DES	Data Encryption Algorithm
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Hash-Based Message Authentication Code
IT	Information Technology
PALCAN	Program for the Accreditation of Laboratories - Canada
PRNG	Psueudorandom number generator
RAID	Redundant Array of independent disks
RSA	|Rivest, Shamir, Aldeman
SFR	Security Functional Requirement
SHA	Secure hash Algorithm
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. EMC® Corporation EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ Security Target v0.5, 24 April 2014.

e. Evaluation Technical Report EMC® Corporation VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3, v 0.4, 2 June 2014.