Certification Report

EAL 3+ Evaluation of EMC® Corporation

EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-172-CR
Version:	1.0
Date:	17 June 2011
Pagination:	i to iii, 1 to 8

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 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1R3*. 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 Canada, 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 Canada, 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 Canada.

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, 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 located in Ottawa, 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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 15 June 2011, 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 trademarked or registered trademarks:

- *EMC® VNX OE is a registered trademark of EMC Corporation.*
- *Unisphere™ is a trademark of EMC Corporation.*
- *Access Logix™ is a trademark of EMC Corporation.*

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

TABLE OF CONTENTS

Executive Summary

The EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ (hereafter referred to as EMC® VNX OE), from EMC, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

The software-only TOE is a combination File Network Attached Storage (NAS) and Block Storage Area Network (SAN) operating environment with Unified Management (Unisphere). It includes a Storage Operating Environment (SOE), which provides Redundant Array of Independent Disks (RAID) and storage provisioning capabilities, one or more NAS servers that allow Local Area Network (LAN) clients to connect and use internal storage, and a set of interfaces administrators can use to manage the TOE and access controls for internal storage.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 30 May 2011 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 the EMC® VNX OE, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 3 Augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 3.1R3*. The following augmentation is claimed:

- ALC_FLR.2 - Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the EMC® VNX OE 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ (hereafter referred to as EMC® VNX OE), from EMC.

2 TOE Description

The software-only TOE is a combination File Network Attached Storage (NAS) and Block Storage Area Network (SAN) operating environment with Unified Management (Unisphere). It includes a Storage Operating Environment (SOE), which provides Redundant Array of Independent Disks (RAID) and storage provisioning capabilities, one or more NAS servers that allow Local Area Network (LAN) clients to connect and use internal storage, and a set of interfaces administrators can use to manage the TOE and access controls for internal storage.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the EMC® VNX OE is identified in Section 6 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: EMC® VNX OE for Block v5.31 with Unisphere™ running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE (VNX for File v7.0 and VNX for Block v5.31) with Unisphere™ running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ Security Target
Version: 0.8
Date: 27 May 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1R3*.

The EMC® VNX OE is:

a. Common Criteria Part 2 conformant, with security functional requirements based on functional components in Part 2;
b. Common Criteria Part 3 conformant, with security assurance requirements based on assurance components in Part 3; and
c. Common Criteria EAL 3 Augmented, containing all the security assurance requirements in the EAL 3, as well as the following: ALC_FLR.2 - Flaw Reporting Procedures.

6 Security Policy

The EMC® VNX OE implements a Discretionary Access Control Policy on subjects trying to read or write from the storage in the TOE environment.

In addition, the EMC® VNX OE enforces a File and Directory Access Security Functional Policy (SFP) on Data Mover user(s) based on attributes of that user and group membership. Whenever a Data Mover User requests access to a file or directory, the TOE utilizes its File and Directory Access SFP to decide whether or not that access is permitted. The TOE uses the UserID and GroupIDs of the user and the contents of the Access Control List (ACL) to determine if the operation should be allowed to proceed. EMC® VNX OE also implements policies pertaining to security audit, user data protection and security management; details of these security policies can be found in section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the EMC® VNX OE product 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

a. The TOE will be managed by competent individuals that are non-hostile, appropriately trained, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. The TOE is protected from physical access by being located in a controlled access facility.

b. The IT Environment will provide a secure place to store user data and provide identification and authentication of users before allowing and actions on behalf of those users.

c. The TOE will have access to a hardware clock in the TOE environment.

8 Evaluated Configuration

The evaluated configuration for the EMC® VNX OE comprises the following:

VNX OE for Block v5.31.000.5.006 with Unisphere™ v7.0.12.0 running on VNX Series Hardware Model VNX5100™

VNX OE for File v7.0.12.0 and VNX OE for Block v5.31 with Unisphere™ v7.0.12.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™

The correct configuration is described in the EMC VNX Security Configuration Guide.

9 Documentation

The EMC documents provided to the consumer are as follows:

EMC Setting up a Unisphere Management Station for the VNX Series;

EMC VNX Getting Started with VNX Installation Assistant for File/Unified;

EMC VNX for Block Command Line Interface Reference;

EMC VNX Series Command Line Interface Reference for File;

EMC VNX Security Configuration Guide on VNX for File; and

EMC VNX Unisphere Online Help.html.

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the EMC® VNX OE 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 EMC® VNX OE security architectural description and determined that the initialization process was secure and 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 were correct.

Guidance Documents: The evaluators examined the EMC® VNX OE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the EMC® VNX OE configuration management system and associated documentation was performed. The evaluators found that the EMC® VNX OE configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the EMC® VNX OE design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of EMC® VNX OE during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by EMC for EMC® VNX OE. 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.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of EMC® VNX OE. Additionally, the evaluators conducted a review of public domain vulnerability databases. The evaluators did not identify and potential vulnerabilities applicable to the EMC® VNX OE in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 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[2].

The evaluators analyzed the developer’s test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 was the following list of EWA-Canada 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 TOE Description of the Security Target, by following all instructions in the developer’s Installation and Administrative guidance;

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator’s TOE installation; and

c. Independent Evaluator Testing: The objective of this test goal is to exercise the TOE’s claimed functionality through evaluator independent testing and to augment any areas that were not covered during the repeat of developer testing.

11.3 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:

- Search for Generic Vulnerabilities: Vulnerability sites were searched for EMC® VNX OE vulnerabilities. No vulnerabilities were found;

- Bypassing by attempting to exploit the capabilities of TOE interfaces in an unexpected way which could result in a violation of a TOE security policy. The TOE could not be bypassed.

- Misuse of the TOE such that an administrator performs an error in the setup of the TOE leading it to fault in a safe manner.

EMC® VNX OE is a product that attaches through fiber switches to the back end storage, therefore is not susceptible to certain attacks such as network scanning and port scanning.

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

11.4 Conduct of Testing

EMC® VNX OE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the EMC development and testing location in Hopkinton, Massachusetts. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Procedures and Test Results document.

11.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that the EMC® VNX OE behaves as specified in its ST, functional specification, TOE design, and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The complete documentation for the EMC® VNX OE includes a comprehensive Installation, Administration, and Security Configuration Guide.

The EMC® VNX OE can be integrated into an existing network infrastructure and provide SAN and NAS services to authorized clients.

Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ACL	Access Control List
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
IT	Information Technology
LAN	Local Are Network
NAS	Network Attached Storage
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SFP	Security Function Policy
SFR	Security Functional Requirement
SOE	Storage Operating Environment
SP	Storage Processor
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WAN	Wide Area Network

15 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1R3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1R3, July 2009.

d. EMC® VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Model VNX5100™ and EMC® VNX OE for File v7.0 and VNX OE for Block v5.31 with Unisphere™ v7.0 running on VNX Series Hardware Models VNX5300™, VNX5500™, VNX5700™, and VNX7500™ Security Target, Revision No. 0.8, 27 May 2011.

e. Evaluation Technical Report (ETR) EMC VNX OE for Block v5.31 with Unisphere running on VNX Series Hardware Model VNX5100 and EMC VNX OE (VNX for File v7.0 and VNX for Block v5.31) with Unisphere running on VNX Series Hardware Models VNX5300, VNX5500, VNX5700, and VNX7500 , EAL 3+ Evaluation, Common Criteria Evaluation Number: 383-4-172, Document No. 1683-000-D002, Version 1.2, 30 May 2011.