Certification Report

EAL 2+ Evaluation of EMC Corporation

EMC® Celerra® Network Server Version 5.5 running on EMC® Celerra® NSX and EMC® Celerra® NS series

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-62-CR
Version: 1.0
Date: 15 October 2007
Pagination: i to v, 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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. 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 (CSE), 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 CSE, 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 (CSE).

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 Standard 17025, General requirements for the accreditation of calibration and testing 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 Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

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 October 2007, 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 at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked or registered trademarks:

- EMC®, Celerra® and CLARiiON® are registered trademark symbols of EMC Corporation;
- Microsoft, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

TABLE OF CONTENTS

Executive Summary

The EMC® Celerra® Network Server Version 5.5 running on EMC® Celerra® NSX and EMC® Celerra® NS series from EMC Corporation (hereafter referred to as EMC® Celerra® Network Server Version 5.5) is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation.

The EMC® Celerra® Network Server Version 5.5 is a Network Attached Storage (NAS) server that provides Internet Protocol (IP) or Fibre Channel[1] access to storage, either locally or on a Storage Area Network (SAN). The purpose of a SAN is to allow many different application servers to share storage provided by centrally managed storage devices. The EMC® Celerra® Network Server Version 5.5 supports several protocols to provide file sharing access to centrally managed storage.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 21 September 2007 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® Celerra® Network Server Version 5.5 , 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)[2] for this product provide sufficient evidence that it meets the EAL 2+ assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

[1] Fibre Channel is a serial data transfer interface that operates over copper wire and/or optical fiber at data rates currently supported at 400 MB/s.

[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.

The Communications Security Establishment, as the CCS Certification Body, declares that the EMC® Celerra® Network Server Version 5.5 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) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation is the EMC® Celerra® Network Server Version 5.5 running on EMC® Celerra® NSX and EMC® Celerra® NS series from EMC Corporation (hereafter referred to as EMC® Celerra® Network Server Version 5.5).

2 TOE Description

The EMC® Celerra® Network Server Version 5.5 is a Network Attached Storage (NAS) server that provides Internet Protocol (IP) or Fibre Channel access to storage, either locally or on a Storage Area Network (SAN). The purpose of a SAN is to allow many different application servers to share storage provided by centrally managed storage devices. The EMC® Celerra® Network Server Version 5.5 supports several protocols to provide file sharing access to centrally managed storage.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the EMC® Celerra® Network Server Version 5.5 is identified in Section 5 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature: Title: EMC Corporation EMC Celerra Network Server Version 5.5 running on EMC® Celerra® NSX series and EMC® Celerra® NS series Security Target, Version: 1.0, Date: 20 September 2007.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

The EMC® Celerra® Network Server Version 5.5 is:

a. Common Criteria Part 2 conformant; with functional requirements based only upon functional components in Part 2;
b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 2 augmented, with all the security assurance requirements in the EAL 2 package as well as ALC_FLR.1 – Basic flaw remediation.

6 Security Policy

The following statements are representative of the Security Policy:

Authentication and Security Management. Users must authenticate to the EMC® Celerra® Network Server Version 5.5 before being able to perform any TSF-mediated actions. A user authenticating to the EMC® Celerra® Network Server Version 5.5 must provide a user name and password for a valid user account. The EMC® Celerra® Network Server Version 5.5 implements role-based security management. Roles are assigned to individuals at the time their user accounts are established.

Discretionary Access Control. The TOE enforces the Discretionary Access Control Security Functional Policy (SFP) on Users by assigning access privileges to Users based on their UserID and GroupIDs. The ability to perform operations on objects, which are governed by the Discretionary Access Control SFP, is granted to Users by an object's owner. Thus, a User is allowed to perform an operation on an object so long as permission is granted to the User within the object's Access Control List (ACL). A User can also be denied the ability to perform an operation on an object if the contents of the object's ACL deny the desired operation based on the UserID or GroupID of the User.

For security policy enforcement please refer to the Security Target.

7 Assumptions and Clarification of Scope

Consumers of the EMC® Celerra® Network Server Version 5.5 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 assumptions are listed in the ST:

- There will be one or more appropriately trained individuals assigned to manage the EMC® Celerra® Network Server Version 5.5 and the security information it contains; and

- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the EMC® Celerra® Network Server Version 5.5 documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The array(s) upon which the EMC® Celerra® Network Server Version 5.5 is installed resides in a physically secure location and only authorized individuals are granted physical access to the host.

For more information about the EMC® Celerra® Network Server Version 5.5 security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The EMC® Celerra® Network Server Version 5.5 is intended for use by a non-hostile and well-managed user community. It relies on the environment to provide it physical and logical protection.

8 Architectural Information

The TOE is composed of software running on purpose-built hardware, both of which are developed by EMC Corporation. The software operates on the Control Station and Data Mover hardware. The EMC® Celerra® Network Server Version 5.5 is composed of the following:

- Control Station – 1 to 2 Control Stations v5.5 are present in the Celerra® Network Server. The Control Station is a dedicated management computer that monitors and controls all components of the EMC® Celerra® Network Server Version 5.5. The Control Station provides access to the administrative functionality of the EMC® Celerra® Network Server Version 5.5 software. It contains utilities for installing and configuring the EMC® Celerra® Network Server Version 5.5, maintaining the system, and monitoring system performance. The Control Station runs a set of programs that are collectively referred to as the Control Station software. The Control Station connects internally to each of the Data Movers within the EMC® Celerra® Network Server Version 5.5. Only Control Station Administrators are granted access to the Control Station.

- Data Movers – 1 to 8 Data Movers are present in a Celerra® Network Server running Data Access in Real Time (DART) operating system v5.5. The Data Movers are the Celerra® Network Server Version 5.5 components that perform the actual transfer of data between the storage system and the network client. Administrators do not typically manage a Data Mover directly. Rather, the Control Station is used to send commands to an individual Data Mover. There are several different models of Data Movers. However, use and management of all Data Movers is performed the same way.
- Optional internal CLARiiON® storage array, which provides midrange Storage Area Network storage.

9 Evaluated Configuration

The TOE is a NAS product which runs on the following Celerra® Network Server models: NS20, NS40, NS40G, NS80, NS80G, NS350, NS500, NS500G, NS700, NS700G, NS704, NS704G, and NSX.

The evaluated configuration of the TOE includes the following Data Mover models: X-Blade 40 (installed on the NS20, NS40, and NS40G models), X-Blade 60 and X-Blade 65 (installed on the NS80, NS80G, and NSX models), NS500 (installed on the NS350, NS500, and NS500G models), and NS700 (installed on the NS700, NS700G,NS704, and NS704G models).

The evaluated configuration includes software components Control Station version 5.5 and DART version 5.5.

For more information on the evaluated configuration, refer to the Security Target.

10 Documentation

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

a. Configuring Celerra® – Quick Start;
b. Celerra® Network Server Integrated Configuration – Phase 1 and Phase 2 Setup Guide;
c. Celerra® Network Server v5.5 Release Notes; and
d. EMC Corporation Celerra® Network Server Version 5.5 running on EMC Celerra® NSX and EMC Celerra® NS series Common Criteria Administrative Guide Supplement.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the EMC® Celerra® Network Server Version 5.5, including the following areas:

Configuration management: An analysis of the EMC® Celerra® Network Server Version 5.5 CM system and associated documentation was performed. The evaluators found that the EMC® Celerra® Network Server Version 5.5 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the EMC® Celerra® Network Server Version 5.5 during distribution to the consumer. The evaluators examined the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the EMC® Celerra® Network Server Version 5.5 functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the EMC® Celerra® Network Server Version 5.5 administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life cycle: The flaw remediation process was carefully reviewed. There are adequate procedures in place to track and correct security flaws, identify corrective actions, and distribute the flaw information and corrections. A verification of this process was performed during the site visit.

Vulnerability assessment: The EMC® Celerra® Network Server Version 5.5 ST's strength of function claims were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL 2+ consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer had met their testing responsibilities by reviewing the developer's test plan, test approach, test procedure and test results, and examining their test evidence, as documented in the Evaluation Technical Report (ETR)[3].

The evaluators analyzed the developer's test coverage analysis, and found that the correspondence between tests identified in the developer's test documentation and the functional specification was complete and accurate.

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

12.2 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. These tests focused on:

- Initialization;
- Identification and authentication;
- Security Management;
- Access control; and
- User Data protection.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks.

Penetration testing included data interception attacks, attempting to access data while in transmission between mutually authenticated servers as well as denial-of-service attacks, attempting to prevent legitimate users of a service from using that service.

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

12.4 Conduct of Testing

The EMC® Celerra® Network Server Version 5.5 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer’s Massachusetts facility.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the EMC® Celerra® Network Server Version 5.5 behaves as specified in its ST and functional specification. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the EMC® Celerra® Network Server Version 5.5 in its intended operating environment.

13 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.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the EMC® Celerra® Network Server Version 5.5 includes a comprehensive set of Installation, Configuration and Administration Guide's. There are also numerous other EMC-generated technical guides and white papers on the Celerra®.

The EMC® Celerra® Network Server Version 5.5 is straightforward to configure, use and integrate into a corporate network.

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

EWA-Canada performed separate site visits to review developer processes (ACM, ADO, ALC, and ATE) and to repeat a sample of developer's tests. Though development security was not part of the evaluation, the evaluators observed that the developer was exceptionally conscious of security. The physical, procedural, and personnel security measures meet or exceed the assurance requirements of higher-level CC evaluations. This is reported on in the CC Evaluation Site Visit Report. This document contains proprietary and confidential EMC information.

15 Acronyms, Abbreviations and Initialisations

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
CSE	Communications Security Establishment

Acronym/Abbreviation/ Initialization	Description
DART	Data Access in Real Time
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SAN	Storage Area Network
SFP	Security Function Policy
SP	Storage Processor
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

16 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 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3, August 2005.

d. EMC Corporation Celerra® Network Server v5.5 Security Target, Revision No. 1.0, 20 September 2007.

e. Evaluation Technical Report (ETR) EMC® Celerra® Network Server Version 5.5 running on EMC® Celerra® NSX and EMC® Celerra® NS series, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-62, Document No. 1544-000-D002, Version 3, 21 September 2007.