Certification Report

EAL 2+ Evaluation of

EMC ControlCenter® 5.2 Service Pack 5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-60-CR
Version: 0.9
Date: 13 November 2007
Pagination: i to v, 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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply 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 13 November 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®, EMC ControlCenter®, and Symmetrix® are registered trademarks of EMC Corporation,
- SAN Manager™, and StorageScope™ are trademarks of EMC Corporation,
- Solaris™ is a trademark of Sun Microsystems,
- AIX® is a registered trademark of IBM,
- 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 ControlCenter® 5.2 Service Pack 5, from EMC Corporation (hereafter referred to as EMC ControlCenter® 5.2) was the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2+ evaluation.

The EMC ControlCenter® 5.2 family of products enables administrators to discover, monitor, automate, provision, and report on host storage resources, networks, and storage across their entire information environment from a single console.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 8 October 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 ControlCenter® 5.2, 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 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*.

The Communications Security Establishment, as the CCS Certification Body, declares that the EMC ControlCenter® 5.2 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] 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 2+ evaluation is the EMC ControlCenter® 5.2 Service Pack 5 , from EMC Corporation (hereafter referred to as EMC ControlCenter® 5.2).

2 TOE Description

The EMC ControlCenter® 5.2 family of products enables administrators to discover, monitor, automate, provision, and report on host storage resources, networks, and storage across their entire information environment from a single console. EMC ControlCenter® 5.2 provides a consolidated view of the storage environment. This view allows administrators to monitor the health of, track the status of, report on, and control each managed object. From a single console, EMC ControlCenter® 5.2 can manage or monitor:

- Storage components – such as EMC® Symmetrix® and other vendors' storage arrays.
- Connectivity components – such as Fibre Channel switches and hubs.
- Host components – such as host operating systems, file systems, volume managers, databases, and backup applications.

EMC ControlCenter® 5.2 is designed for use in a heterogeneous environment of multi-vendor storage, multi-vendor storage networks, and multi-vendor storage hosts. Information can reside on technologically disparate devices running a variety of operating systems, in geographically diverse locations. From a single console, EMC ControlCenter® 5.2 can monitor or manage many types of storage arrays, storage network connectivity components, and hosts.

Administrators can continue to leverage the individual strengths of each of their storage assets while EMC ControlCenter® 5.2 masks their complexity, bringing all the components together in one view.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the EMC ControlCenter® 5.2 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 ControlCenter® 5.2 Service Pack 5 Security Target, Version: 1.01, Date: 11 October 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 ControlCenter® 5.2 Service Pack 5 is:

a. Common Criteria Part 2 conformant; with security 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. An administrator must authenticate to the IT Environment before being able to perform any TSF-mediated actions. The TSF enforces the Access Control SFP to restrict the ability to modify or delete usernames and permissions to the administrator.

User Data Protection. All user data stored on the TOE is protected by assigned permissions.

For security policy enforcement please refer to the EMC ControlCenter® 5.2 Security Target.

7 Assumptions and Clarification of Scope

Consumers of the EMC ControlCenter® 5.2 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:

- Administrators and TOE users are non-hostile, appropriately trained, and follow all administrator guidance.

7.2 Environmental Assumptions

The following Environmental assumption is listed in the ST:

- Physical security will be provided for the TOE and its environment.

For more information about the EMC ControlCenter® 5.2 security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The EMC ControlCenter® 5.2 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 comprises three main components:

- EMC ControlCenter Console – provides administrative access to the ControlCenter Infrastructure
- ControlCenter Infrastructure – acts as the centralized management, storage, and decision-making point for the TOE
- Agents – provide intelligence to manage or monitor specific object domains (such as Symmetrix storage arrays; Windows NT, Windows 2000, Windows 2003, Solaris, HP-UX, AIX, Linux, or Multiple Virtual Storage (MVS) hosts; and Fibre Channel switches)

The Console Component is a Java-based Graphical User Interface (GUI) software suite which allows users to view, monitor, and administer the managed storage environment. It includes SAN Manager, StorageScope, and Symmetrix Manager. SAN Manager allows management of complex SAN environments. StorageScope provides integrated asset and utilization reporting across multi-vendor storage infrastructures where Symmetrix Manager allows administrators to monitor and configure Symmetrix platforms.

The ControlCenter Infrastructure Component controls web-based communications to the TOE. The WebConsole Server Component allows the user to connect to the TOE via the web-based programs “Web Console” or “StorageScope”. Both Web Console and StorageScope allow users to monitor and report on a managed storage infrastructure.

The Agent Component consists of Agents that monitor specific physical and logical elements within a storage environment. Agents are applications that collect data and monitor the health of storage environment objects. There are several types of Agents - Host Agents, Storage Agents, Database Agents, Backup Agents, Tape Agents, Connectivity Agents, and Other Agents.

9 Evaluated Configuration

The TOE is a software-only TOE consisting of EMC ControlCenter® 5.2 Service Pack 5. EMC ControlCenter® 5.2 runs on general purpose computing hardware running a general purpose operating system. The ControlCenter Infrastructure and the Console Software Components were tested on Windows Server 2003 SP2. The Agent Component was tested

on Windows Server 2003 SP2, Windows 2000 SP4, Red Hat Linux ES4 Nahant Update 2, HP-UX B11.11, Sun Solaris 2.9, and IBM AIX 5.2.

10 Documentation

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

a. EMC ControlCenter 5.2 Service Pack 5 Planning And Installation Guide; and
b. EMC Corporation ControlCenter® 5.2 Service Pack 5 Common Criteria Administrative Guide Supplement.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the EMC ControlCenter® 5.2, including the following areas:

Configuration management: An analysis of the EMC ControlCenter® 5.2 CM system and associated documentation was performed. The evaluators found that the EMC ControlCenter® 5.2 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 ControlCenter® 5.2 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

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.

Design documentation: The evaluators analysed the EMC ControlCenter® 5.2 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 ControlCenter® 5.2 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.

Vulnerability assessment: The evaluators 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)[2].

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.

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:

- Identification and authentication;
- Audit; and
- Users and Roles.

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;

[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.

- Tampering; and
- Direct attacks.

Penetration tests included buffer overflow attacks, data interception attacks, denial of service attacks, and attacks against externally accessible TOE components.

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

12.4 Conduct of Testing

The EMC ControlCenter® 5.2 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 ControlCenter® 5.2 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 ControlCenter® 5.2 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 ControlCenter® 5.2 includes a comprehensive Installation and Administration Guide.

The EMC ControlCenter® 5.2 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 Initializations

Acronym/Abbreviation/ Initialization	Description
CC	Common Criteria
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IT	Information Technology
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SAN	Storage Area Network
SFP	Security Function Policy
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) 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, version 2.3, August 2005.

d. EMC Corporation EMC ControlCenter® 5.2 Service Pack 5 Security Target, Revision No. 1.01, 11 October 2007.

e. Evaluation Technical Report (ETR) EMC ControlCenter® 5.2 Service Pack 5, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-60, Document No. 1545-000-D002, Version 1.6, 12 October 2007.