Certification Report

EMC® ViPR® Controller v2.1.0.3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2015

Document number: 383-4-329-CR
Version: 1.0
Date: 20 November 2015
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 3.1 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 20 November 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 or registered trademarks:

- EMC and ViPR are registered trademarks of EMC Corporation.

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

TABLE OF CONTENTS

Executive Summary

EMC® ViPR® Controller v2.1.0.3 (hereafter referred to as EMC® ViPR®), from EMC Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that EMC® ViPR® meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

EMC® ViPR® is a storage management virtual appliance product that is capable of managing external storage resources of different types and supporting different storage protocols. EMC® ViPR® allows administrators a single point of management for their entire storage network.

EMC® ViPR® provides access to provision and backup external storage in the form of a Virtual Data Center (VDC). Within a VDC there are one or more tenants, each tenant representing a specific user or user group. A tenant allows the storage to be managed and provisioned on a per-tenant basis. In a multi-tenant environment, each tenant is configured to use specific resources within the VDC, and users are mapped to particular tenants. This allows the storage allocated to a given group within an organization to be isolated from other groups. Projects are tenant resources and are created within a tenant. All file and block resources provisioned using EMC® ViPR® must be associated with a project.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 20 November 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 EMC® ViPR®, 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® ViPR® 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

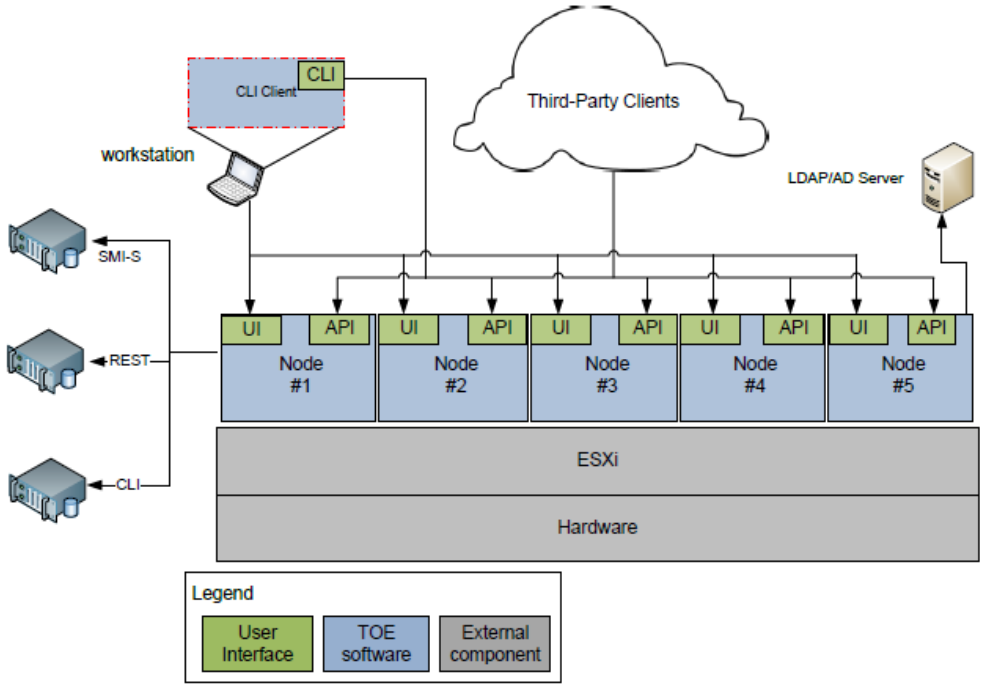
The Target of Evaluation (TOE) for this EAL 2+ evaluation is EMC® ViPR® Controller v2.1.0.3 (hereafter referred to as EMC® ViPR®), from EMC Corporation.

2 TOE Description

EMC® ViPR® is a storage management virtual appliance product that is capable of managing external storage resources of different types and supporting different storage protocols. EMC® ViPR® allows administrators a single point of management for their entire storage network.

EMC® ViPR® provides access to provision and backup external storage in the form of a Virtual Data Center (VDC). Within a VDC there are one or more tenants, each tenant representing a specific user or user group. A tenant allows the storage to be managed and provisioned on a per-tenant basis. In a multi-tenant environment, each tenant is configured to use specific resources within the VDC, and users are mapped to particular tenants. This allows the storage allocated to a given group within an organization to be isolated from other groups. Projects are tenant resources and are created within a tenant. All file and block resources provisioned using EMC® ViPR® must be associated with a project.

A diagram of the EMC® ViPR® architecture is as follows:



3 Security Policy

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

Security Audit;

User Data Protection;

Identification and Authentication;

Security Management;

Protection of the TOE Security Functionality;

Resource Utilization; and

TOE Access.

4 Security Target

The ST associated with this Certification Report is identified below:

EMC Corporation ViPR® Controller v2.1.0.3 Security Target version 0.10, November 06, 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.*

EMC® ViPR® 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 extended,* with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST*:*

- *EXT_FPT_RTC.I – Replicated TSF Data consistency.*

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® ViPR® 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 software will be protected from unauthorized modification;*
- *There are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and*
- *The users who manage the TOE are non-hostile, appropriately trained and follow all guidance.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE environment provides the network connectivity required to allow the TOE to perform its function;*
- *The TOE is installed on the appropriate, dedicated hardware and hypervisor; and*
- *The TOE is located within a controlled access facility.*

7 Evaluated Configuration

The evaluated configuration for EMC® ViPR® comprises:

- *The software ViPR Controller v2.1.0.3 running in a three node or five node cluster deployed in the form of a virtual appliance;*
- *User Interface (UI);*
- *Command Line Interface (CLI); and*
- *REST API (Representational State Transfer, Application Programming Interface) available through the CLI Client.*

The publication, EMC ViPR 2.1 Product Documentation Index Version 12, available through EMC's online community site, describes the procedures necessary to install and operate EMC® ViPR® in its evaluated configuration.

8 Documentation

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

EMC provides EMC ViPR 2.1 Product Documentation Index Version 12 through EMC's online community site, which includes the following:

- ViPR 2.1 – Understanding ViPR Users, Roles, and ACLs;
- ViPR 2.1 – Installing the ViPR CLI;

- ViPR 2.1 – Access the ViPR REST API; and
- ViPR 2.1 – Install EMC ViPR Controller.

The following additional guides are also part of the TOE:

- EMC ViPR Release Notes, Release number 2.1.0, 302-001-392, 02, October, 2014;
- EMC ViPR v2.1 Security Configuration Guide, 302-001-391, 02, October 2014; and
- EMC ViPR v2.1 Command Line Reference, 302-001-390, September, 2014.

9 Evaluation Analysis Activities

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

Development: The evaluators analyzed the EMC® ViPR® 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® ViPR® 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 EMC® ViPR® 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® ViPR® configuration management system and associated documentation was performed. The evaluators found that the EMC® ViPR® 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® ViPR® during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the EMC® ViPR®. 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 TOE;

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

c. Concurrent User Login Separation: This objective of this test case is to demonstrate that the TOE provides separation of concurrent logins;

d. NFS File Export Access: The objective of this test case will verify that only intended clients will be able to access an NFS share; and

e. Node Failure Due To Power Loss: The objective of this test case is to demonstrate the ability of the TOE to preserve a secure state and ensure consistent replication between components of the TOE after power failure of a single node.

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;

b. Port Scan: The TOE will be scanned to ensure only those ports that are allowed to be are open; and

c. Information Leakage Verification: In this test case the TOE will be monitored for leakage of information during login attempts.

[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

EMC® ViPR® 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® ViPR® behaves as specified in its ST and functional specification.

11 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.

12 Evaluator Comments, Observations and Recommendations

The evaluator recommends that potential operators of the TOE familiarize themselves with relevant product documentation before operating ViPR Controller in a production environment. Given that the appliance is installed in a virtual environment, it is also required that personnel deploying the TOE are properly trained in the operation and security requirements of the underlying hypervisor.

13 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
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
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
REST API	Representational State Transfer,

Acronym/Abbreviation/ Initialization	Description
	Application Programming Interface
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
VDC	Virtual Data Center

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 ViPR® Controller v2.1.0.3 Security Target version 0.10, November 06, 2015.

e. EMC Corporation ViPR® Controller v 2.1.0.3 Evaluation Technical Report, version 1.0, November 20, 2015.