# Certification Report

## EMC ScaleIO® v1.32.3

Issued by:

**Communications Security Establishment**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**

| | |
|---|---|
| **Document number**: | 383-4-348-CR |
| **Version**: | 1.0 |
| **Date**: | 25 April 2016 |
| **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 25 April 2016, 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:

- ScaleIO® is a registered trademark of EMC Corporation.

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

**TABLE OF CONTENTS**

## Executive Summary

EMC ScaleIO® v1.32.3 (hereafter referred to as ScaleIO® v1.32.3), from EMC Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that ScaleIO® v1.32.3 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

ScaleIO® v1.32.3 is a software-only server-based Storage Area Network (SAN) that converges storage and computer resources to form a single-layer, enterprise grade storage product. Its scale-out server SAN architecture can grow from a few to thousands of servers. ScaleIO® v1.32.3 uses existing servers' local disks and Local Area Network (LAN) to create a virtual SAN.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 25 April 2016 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 ScaleIO® v1.32.3, 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 ScaleIO® v1.32.3 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 ScaleIO® v1.32.3 (hereafter referred to as ScaleIO® v1.32.3), from EMC Corporation.

# 2 TOE Description

ScaleIO® v1.32.3 is a software-only server-based Storage Area Network (SAN) that converges storage and computer resources to form a single-layer, enterprise grade storage product. Its scale-out server SAN architecture can grow from a few to thousands of servers. ScaleIO® v1.32.3 uses existing servers' local disks and Local Area Network (LAN) to create a virtual SAN.

ScaleIO® v1.32.3 is made up of three major components:

- MDM (Meta Data Manager) Manages the system;
- SDS (ScaleIO Data Server) manages the capacity of a single server; and
- SDC (ScaleIO Data Client) exposes ScaleIO volumes as block devices to the applications residing on the same server.

A diagram of the ScaleIO® v1.32.3 architecture is as follows:

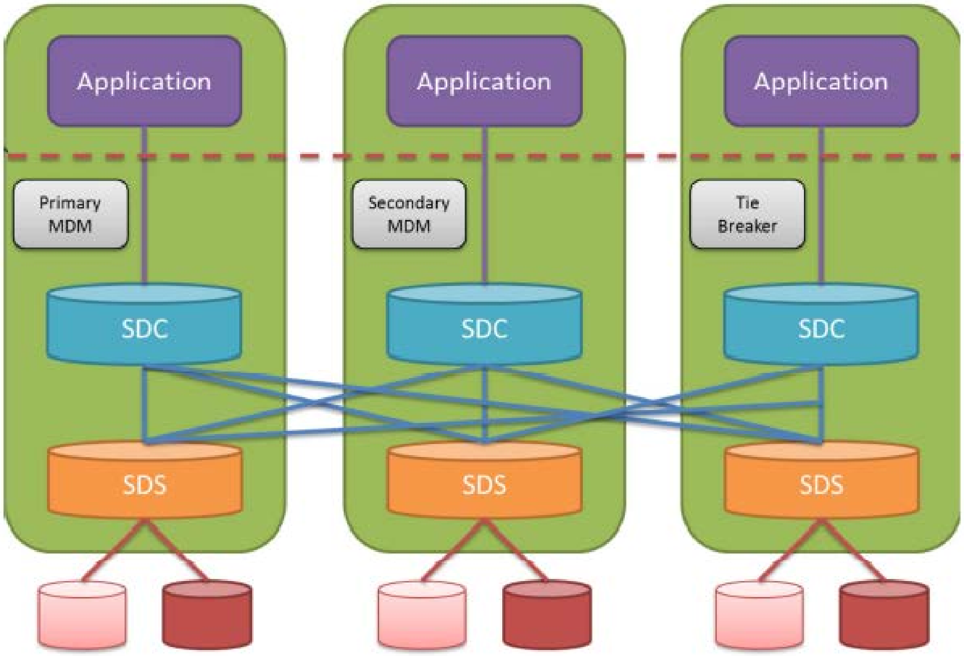

**Figure 1 – ScaleIO Architecture**

# 3 Security Policy

ScaleIO® v1.32.3 implements a role-based access control policy to control administrative access to the system. In addition, ScaleIO® v1.32.3 implements policies pertaining to the following security functional classes:

*Security Audit;*

*User Data Protection;*

*Identification and Authentication;*

*Security Management; and*

*TOE Access.*

# 4 Security Target

The ST associated with this Certification Report is identified below:

EMC ScaleIO® v1.32.3 Security Target version 0.6, 8 February 2016

# 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.*

ScaleIO® v1.32.3 is:

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

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 ScaleIO® v1.32.3 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:

- *There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains; and*
- *The authorized administrators are not careless, willfully negligent, or hostile, and follow and abide by the instructions provided by the TOE documentation.*

## 6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification; and*
- *The TOE and the servers accessing them will be interconnected by a segregated LAN that protects the user traffic from disclosure to or modification by untrusted systems or users.*

# 7 Evaluated Configuration

The evaluated configuration for ScaleIO® v1.32.3 comprises:

- Three instances of MDM instantiated within VMware SUSE-based virtual machines (SVM);
- Three or more instances of SDS instantiated within VMware SUSE-based virtual machine (SVM);
- One or more instance of SDC instantiated within VMware ESXi 5.5; and
- The Command Line Interface (CLI) or graphical User Interface (GUI) application on a Windows 7 system.

*The publication entitled EMC ScaleIO® v1.32.3Common Criteria Supplement (December 2015) describes the procedures necessary to install and operate ScaleIO® v1.32.3 in its evaluated configuration.*

# 8 Documentation

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

a. *EMC ScaleIO v1.32.1 User Guide (July 2015);*

b. *ScaleIO v1.32 Security Configuration guide (302-001-368 Rev 03);*

c. *EMC ScaleIO v1.32.1 Installation Guide (July 2015);*

d. *How to obtain your ScaleIO Licence Key (November 2013); and*

e. EMC ScaleIO v1.32 Common Criteria Supplement (December 2015).

# 9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of ScaleIO® v1.32.3, including the following areas:

**Development:** The evaluators analyzed the ScaleIO® v1.32.3 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 ScaleIO® v1.32.3 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 ScaleIO® v1.32.3 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 ScaleIO® v1.32.3 configuration management system and associated documentation was performed. The evaluators found that the ScaleIO® v1.32.3 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 ScaleIO® v1.32.3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the ScaleIO® v1.32.3. 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. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Initialization, Configuration, and TOE Verification: The objective of this test goal is to ensure that the TOE is correctly initialized, verified, and configured prior to the start of testing;

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

d. MDM Failure: The objective of this test goal is to demonstrate the ability of the TOE to function during a failure to the primary MDM.

## 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 to identify services running and open ports;

c. Nessus scan: The objective of this test goal is to detect if the TOE is vulnerable to GHOST, FREAK, Heartbleed, POODLE, or Shellshock; and

[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.

d. Information Leakage: The objective of this test goal is to monitor for leakage of information during login attempts.

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

### 10.4 Conduct of Testing

ScaleIO® v1.32.3 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 ScaleIO® v1.32.3 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 Acronyms, Abbreviations and Initializations

| Acronym/Abbreviation/ Initialization | Description |
|---|---|
| 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 |
| ITSET | Information Technology Security Evaluation and Testing |
| LAN | Local Area Network |
| MDM | Meta Data Manager |
| PALCAN | Program for the Accreditation of Laboratories - Canada |
| SAN | Storage Area Network |
| SDC | ScaleIO Data Client |
| SDS | ScaleIO Data Server |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |

# 13 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 ScaleIO® v1.32.3 Security Target version 0.6, 8 February 2016

e. Evaluation Technical Report EMC ScaleIO® v1.32.3 version 1.2, 25 April 2016.