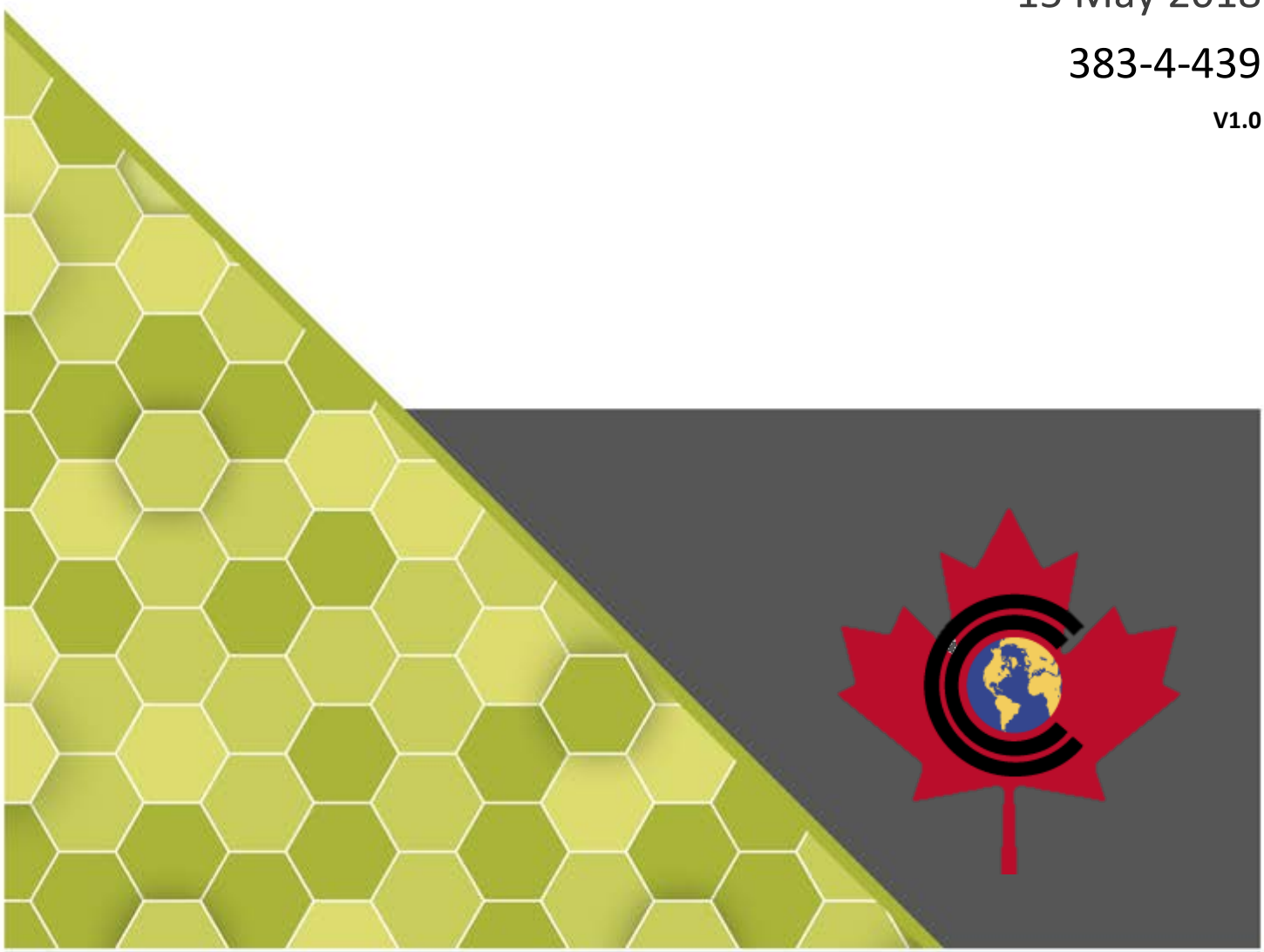
COMMON CRITERIA CERTIFICATION REPORT

Dell EMC™ Elastic Cloud Storage™ v3.2

15 May 2018

383-4-439

V1.0



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. 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 Canadian CC Scheme, 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.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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.

By awarding a Common Criteria certificate, the 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.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Dell EMC™ Elastic Cloud Storage™ v3.2 (hereafter referred to as the Target of Evaluation, or TOE), from Dell EMC, was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed 15 May 2018 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, 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 Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Canadian Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	Dell EMC™ Elastic Cloud Storage™ v3.2
Developer	Dell EMC
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

1.2 TOE DESCRIPTION

Elastic Cloud Storage (ECS) is a software-defined cloud storage platform that supports the storage, manipulation, and analysis of unstructured data on commodity hardware. ECS is specifically designed to support mobile, cloud, big data, and social networking applications. It is deployed as a turnkey storage appliance using qualified commodity servers and disks. ECS provides object and file user access to stored data. At a high level ECS is composed of the following main components:

- ECS Portal and Provisioning Services – provides a Web-based portal that allows self-service, automation, reporting and management of ECS nodes. It also handles licensing, authentication, multi-tenancy, and provisioning services.
- Data Services – provides services, tools and Application Programming Interfaces to support Object and Network File System version 3.
- Storage Engine – responsible for storing and retrieving data, managing transactions, and protecting and replicating data.
- Fabric – provides clustering, health, software and configuration management as well as upgrade capabilities and alerting.
- Infrastructure – uses SUSE Linux Enterprise Server (SLES) 12 SP2 as the base operating system.
- Hardware – the hardware is provided as a turnkey appliance made up of industry standard hardware components.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

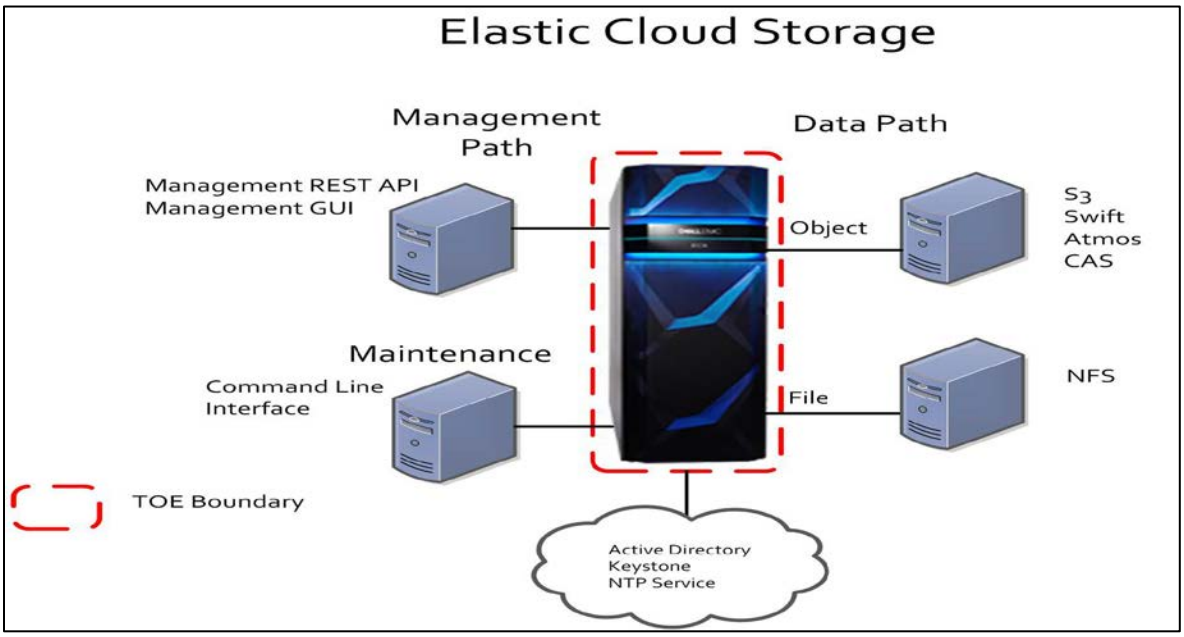


Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic module was evaluated by the CMVP and used by the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
RSA BSAFE® Crypto-J JSAFE and JCE Software Module (Software Version: 6.1)	2057

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The operational environment provides authentication services to the TOE in support of access control decisions.
- The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The operational environment will provide secure network communications to protect data that is sent to and received from the TOE.
- The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

3.2 CLARIFICATION OF SCOPE

The following features are excluded from this evaluation:

- Hadoop Distributed File System user access to stored data
- Transfer of audit records to a syslog server
- Advanced Retention Management
- Geo-Federation and Geo-Replication (Multi-site deployment)

The CLI is used only during installation in the evaluated configuration.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises the ECS Gen 2, 5 nodes, and 30 disk hardware running ECS Version 3.2 build 531.

The following components in the TOE environment are required for operation of the TOE:

- Management workstation running Windows 10
- Maintenance workstation running Windows 10
- Data Path workstation running SLES 12 SP2
- Domain Controller running Windows Server 2012 R2 with Active Directory
- Keystone Server running SLES 12 SP2

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a. Elastic Cloud Storage (ECS) Version 3.2 Security Configuration Guide (302-004-495 01 Published March 2018)

b. Elastic Cloud Storage (ECS) Version 3.2 Administrator's Guide (302-004-490 01 Published March 2018)

c. EMC Elastic Cloud Storage (ECS) CLI Quick Reference (302-001-998 Rev 01 dated June 2015)

d. EMC® Centera®, SDK Version 3.3, Programmers Guide (069001127 RevA13 dated July 2012)

e. EMC® Centera®, SDK Version 3.3, API Reference Guide (069001185 REV A09 dated July 2012)

f. EMC® Atmos™, Version 2.4, Programmer's Guide (302-002-655 Rev01 dated March 2016)

g. Elastic Cloud Storage (ECS), version 3.2, Data Access Guide (302-004-491 01 Published March 2018)

h. Dell EMC™ Elastic Cloud Storage™ v3.2 Common Criteria Guidance Supplement, Version: 1.0, 6 April 2017

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE 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 the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

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

6.1 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. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE 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.

6.3 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. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Default Password Change: The objective of this test goal is to confirm that administrators are required to change default passwords prior to login;

c. Administrator Account Permissions: The objective of this test goal is to confirm that access to the root account is disabled;

d. Node Locking: The objective of this test goal is to confirm that only the Lock Admin can lock/unlock remote access sessions to the ECS Nodes;

e. Logging: The objective to this test goal is to confirm that administrative actions are logged;

f. Compliance and Retention Policy: The objective of this test goal is to confirm that the TOE enforces rules for compliance and retention policies; and

g. Network Encryption: The objective of this test goal is to confirm that all communication via the management and data paths are encrypted.

6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 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 such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and

b. Information Leakage: The evaluator monitored the TOE during start-up and shutdown to determine if any sensitive information was made available during these times.

c. Misuse: The evaluator physically disconnected the TOE from the management console during use to determine if any sensitive information was made available during this time and that user had to log back in.

d. Direct Attack: The evaluator unplugged the power to the TOE during use and plugged it back in to verify that a secure state was maintained after the power outage.

6.4.1 PENETRATION TEST RESULTS

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target for Dell EMC™ Elastic Cloud Storage™ v3.2, v1.0, 6 April 2018
Evaluation Technical Report for Dell EMC™ Elastic Cloud Storage™ v3.2, v1.0, 15 May 2018