Certification Report

EAL 2+ Evaluation of EMC® Greenplum® 4.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-196-CR
Version:	1.0
Date:	12 April 2012
Pagination:	i to iii, 1 to 9

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 3,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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 Canada, 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 Canada, 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 Canada.

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 located in Ottawa, 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, 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 12 April 2012, 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 is a registered trademark symbol of EMC Corporation;
- Greenplum is a registered trademark of EMC Corporation; and
- Red Hat Enterprise Linux is a registered trademark of Linus Torvalds Inc.

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

TABLE OF CONTENTS

Executive Summary

EMC® Greenplum® 4.2 (hereafter referred to as Greenplum 4.2), from EMC Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The software-only TOE is the Greenplum 4.2 data analysis platform. The TOE includes a Relational Database Management System (RDBMS) and a standards-compliant (Open Database Connectivity and Java Database Connectivity) interface to run queries and data analysis jobs. The TOE is designed to be distributed across multiple physical nodes, but maintains the functionality of a single RDBMS. Users access the RDBMS via the master host, while the TOE stores data on segment servers. The master host also stores a data catalog that records where data is distributed across the segment servers.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 26 March 2012 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 Greenplum 4.2, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.2 Flaw reporting procedures.

Greenplum 4.2 is conformant with the *U.S. Government Protection Profile for Database Management Systems, Version 1.3, December 24, 2010.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Greenplum 4.2 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) and the Common Criteria portal (the official website of the Common Criteria Project).

[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 augmented evaluation is EMC® Greenplum® 4.2 (hereafter referred to as Greenplum 4.2), from EMC Corporation.

2 TOE Description

The software-only TOE is the Greenplum 4.2 data analysis platform. The TOE includes a Relational Database Management System (RDBMS) and a standards-compliant (Open Database Connectivity and Java Database Connectivity) interface to run queries and data analysis jobs. The TOE is designed to be distributed across multiple physical nodes, but maintains the functionality of a single RDBMS. Users access the RDBMS via the master host, while the TOE stores data on segment servers. The master host also stores a data catalog that records where data is distributed across the segment servers.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Greenplum 4.2 is identified in Section 6 of the ST.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: EMC Corporation EMC® Greenplum® 4.2 Security Target
Version: 0.9
Date: 22 March 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Greenplum 4.2 is:

a. *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:
   - FAU_GEN_(EXT).2 - User and/or group identity association;
   - FMT_MSA_(EXT).3 - Static attribute initialisation;
   - FPT_TRC_(EXT).1 - Internal TSF consistency; and

- FTA_TAH_(EXT).1 - TOE access history.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3;

c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 Flaw reporting procedures; and

d. Greenplum 4.2 is conformant with the *U.S. Government Protection Profile for Database Management Systems, Version 1.3, December 24, 2010.*

6 Security Policy

Greenplum 4.2 controls access to user data via a Data Access Security Functional Policy (SFP). The Data Access SFP relies on role-based permissions and built-in access control mechanisms to ensure that only authorized users can access data. Details of this security policy can be found in Section 6 of the ST.

In addition, Greenplum 4.2 implements policies pertaining to security audit, identification and authentication, security management, protection of the TSF, resource utilization, and TOE access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Greenplum 4.2 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:

- Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained, and follow all administrator guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The operational environment will provide an isolated domain for the execution of the TOE;

- The operational environment will contain identification and authentication mechanisms for administrator access to database control utilities and other utilities;

- The operational environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources;

- There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS;

- The underlying operating system will be configured with only those user accounts required for access by authorized security administrators;

- The operational environment will provide a secure line of communications between the remote user and the TOE;

- The operational environment will provide reliable time stamps;

- Each operational entity the TOE relies on for security functions will be installed, configured, managed and maintained in a manner appropriate to the IT entity, and consistent with the security policy of the TOE and the relationship between them; and

- Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.

7.3 Clarification of Scope

Greenplum 4.2 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Greenplum 4.2 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for Greenplum 4.2 comprises two master servers (one active and one backup) running Greenplum v4.2.0.0 build 5 on Red Hat® Enterprise Linux® version 5.5, 5.7 and 6.1, and two segment servers running Greenplum v4.2.0.0 build 5 on Red Hat® Enterprise Linux® version 5.5, 5.7 and 6.1 along with two primary database copies and two mirror database copies of each other.

In addition to general-purpose commodity hardware, the TOE requires the following environmental components in order to function properly:

- cables, connectors, and switching and routing devices that allow all of the TOE and environmental components to communicate with each other;
- an administrator workstation with a PostgreSQL compatible client program; and

- a Lightweight Directory Access Protocol Server to perform remote authentication of TOE users.

The publication entitled *EMC® Greenplum® 4.2 Guidance Documentation Supplement* describes the procedures necessary to install and operate Greenplum 4.2 in its evaluated configuration.

9 Documentation

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

a. Greenplum® Database 4.2 Installation Guide, Revision A01;

b. Greenplum® Database 4.2 Administration Guide, Revision A01;

c. Greenplum® Database 4.2 Release Note; and

d. EMC® Greenplum® 4.2 Guidance Documentation Supplement, version 0.2.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Greenplum 4.2, including the following areas:

Development: The evaluators analyzed the Greenplum 4.2 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 Greenplum 4.2 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 Greenplum 4.2 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 Greenplum 4.2 configuration management system and associated documentation was performed. The evaluators found that the Greenplum 4.2 configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Greenplum 4.2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by EMC Corporation for Greenplum 4.2. 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.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Greenplum 4.2. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Greenplum 4.2 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Greenplum 4.2 in its operational environment.

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

11 ITS Product Testing

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

11.1 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[2].

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.

11.2 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.

[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.

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 EWA-Canada 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. Segment failure: The purpose of this test case is to verify the redundancy of the distributed database;

c. Authentication: The purpose of this test case is to verify the authentication mechanism of the TOE and to verify that the TOE is only open to SSH sessions for authentication; and

d. Multiple sessions: The purpose of this test case is to verify that access to the TOE terminates when the administrator performs a shutdown.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases, extensive developer vulnerability scanning results and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration test focused on:

a. Misuse Testing: The purpose of this test case is to verify that the TOE database engine will not start when important configuration files are not available or corrupted.

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

11.4 Conduct of Testing

Greenplum 4.2 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer’s testing facility located in San Mateo, California. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that Greenplum 4.2 behaves as specified in its ST and functional specification.

12 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.

13 Evaluator Comments, Observations and Recommendations

The TOE comes with a complete set of easy to follow guidance documentation.

14 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
PALCAN	Program for the Accreditation of Laboratories - Canada
RDMS	Relational Database Management System
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation

15 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 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. U.S. Government Protection Profile for Database Management Systems, Version 1.3, December 24, 2010.

e. EMC Corporation EMC® Greenplum® 4.2 Security Target, 0.9, 22 March 2012.

f. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC Corporation EMC® Greenplum® 4.2 Document No. 1716-000-D002 Version 1.3, 26 March 2012.