Certification Report

EAL 2+ Evaluation of CA GigaStor 14.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-174-CR
Version: 1.0
Date: 26 August 2011
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 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, 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, 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 26 August 2011, 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 registered trademark:

- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

CA GigaStor 14.1, from CA Technologies, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

CA GigaStor 14.1 comprises the hardware appliances Gigastor, Gigastor Expandable, and Gigastor Portable and the control and analysis application Observer Expert Console that is installed by the consumer on a separate workstation. CA GigaStor 14.1 connects to a network tap or switch port mirror [1]. Network traffic is captured and stored to a high-capacity RAID [2] array for analysis. Users may define traffic conditions that if met, trigger an alarm.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 5 August 2011 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 CA GigaStor 14.1, 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)[3] 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.1 - Basic Flaw Remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that the CA GigaStor 14.1 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] Port Mirroring is used on a network switch to send a copy of network packets seen on one switch port to a monitoring connection on another switch port.

[2] RAID - Redundant Array of Independent Disks.

[3] 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 CA GigaStor 14.1, from CA Technologies.

2 TOE Description

CA GigaStor 14.1 comprises the hardware appliances Gigastor, Gigastor Expandable, and Gigastor Portable with NI Capture Card and capture application Observer Expert Gigastor, and the control and analysis application Observer Expert Console that is installed by the consumer on a separate workstation.

The CA GigaStor 14.1 architecture and functionality is described in detail in Sections 1 and 2 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for CA GigaStor 14.1 is identified in Sections 6 and 7 of the ST.

4 Security Target

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

Title: CA GigaStor 14.1 Security Target
Version: 1.3
Date: 4 August 2011

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*.

CA GigaStor 14.1 is:

a. *Common Criteria Part 2 extended*, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - FAU_ARP_EXT.1 - Traffic Alarms;
   - FAU_GEN_EXT.1 - Traffic Capture;
   - FAU_SAA_EXT.1 - Potential Traffic Alarm Analysis;
   - FAU_SAR_EXT.1 - Captured Traffic Review;
   - FAU_SAR_EXT.3 - Selectable Captured Traffic Review;
   - FAU_SEL_EXT.1 - Selective Traffic Capture;

- FAU_STG_EXT.2 - Guarantees of captured traffic availability; and
- FAU_STG_EXT.3 - Action in case of possible captured traffic loss.

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

c. *Common Criteria EAL 2 augmented*, with all the security assurance requirements in the EAL 2, as well as the following: ALC_FLR.1.

6 Security Policy

CA GigaStor 14.1 implements a DAC [4] Policy to control user access to TOE resources.

In addition, CA GigaStor 14.1 implements policies pertaining to Traffic Capture and Analysis, User Data Protection, Identification and Authentication, and Security Management. Further details on these security policies may be found in Section 9 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the CA GigaStor 14.1 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 Assumptions are listed in the ST:

a. One or more authorized administrators are assigned to install, configure and manage the TOE and the security of the information it contains;

b. Users of the TOE are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation;

c. System administrators exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks; and

d. Users select strong passwords according to the policy described in the administrative guidance and will protect their own authentication data.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

[4] DAC - Discretionary Access Control.

a. The Operational Environment will provide measures for recording security relevant events that will assist the authorized users in detecting misuse of the TOE, the information it collects, and/or its security features that would compromise the integrity of the TOE and violate the security objectives of the TOE;

b. The security features offered by the Operational Environment protect the files used by the TOE;

c. There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) on the TOE, and administrators will not install any general-purpose computing functionality to the Operational Environment upon which the TOE resides; and

d. The TOE will be located within controlled access facilities that will prevent unauthorized physical or logical access.

8 Evaluated Configuration

The evaluated configuration for CA GigaStor 14.1 comprises:

a. The appliances Gigastor, Gigastor Expandable, and Gigastor Portable including the NI Capture Card and the application Observer Expert Gigastor 14.1; and

b. Observer Expert Console 14.1 that is installed by the consumer on a workstation running Microsoft Windows XP SP3.

The publication entitled NetQoS GigaStor 14.1 Supplemental Guidance for Common Criteria version 1.2 describes the procedures necessary to install and operate CA GigaStor 14.1 in its evaluated configuration.

9 Documentation

The Network Instruments documents provided to the consumer are as follows:

a. Observer User Guide rev. 2;

b. NetQoS GigaStor User Guide rev. 2; and

c. NetQoS GigaStor 14.1 Supplemental Guidance for Common Criteria version 1.2.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the CA GigaStor 14.1, including the following areas:

Development: The evaluators analyzed the CA GigaStor 14.1 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 CA GigaStor 14.1 security architectural description and determined that the initialization process

is secure and 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 CA GigaStor 14.1 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 CA GigaStor 14.1 configuration management system and associated documentation was performed. The evaluators found that the CA GigaStor 14.1 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 CA GigaStor 14.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by CA/Network Instuments for CA GigaStor 14.1. 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 CA GigaStor 14.1. Additionally, the evaluators conducted a review of public domain vulnerability databases. The evaluators did not find any potential vulnerabilities for testing applicable to the CA GigaStor 14.1 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[5].

[5] 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 evaluators analyzed the developer's test coverage and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design 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.

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 was the following list of EWA-Canada 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 Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat the developer's tests on the evaluator's TOE installation. In order to avoid test case dependency issues, all of the developer's tests as documented in the developer's Test Procedure document were repeated in the order presented;

c. Traffic Capture and Analysis: The objective of this test goal is to exercise the TOE's claimed traffic capture and analysis functionality;

d. DAC Policy: The objective of this test goal is to exercise the TOE's claimed DAC Policy to control user access to TOE resources;

e. Identification and Authentication: The objective of this test goal is to exercise the TOE's claimed identification and authentication functionality; and

f. Alert Logging: The objective of this test goal is to exercise the TOE's claimed alert logging functionality.

11.3 Conduct of Testing

CA GigaStor 14.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the ITSET Facility at EWA-Canada. The CCS Certification Body witnessed the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a Test Procedures and Test Results document.

11.4 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the CA GigaStor 14.1 behaves as specified in its ST, functional specification, TOE design, and security architecture description.

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 user documentation for CA GigaStor 14.1 includes the Observer User Guide, the GigaStor User Guide, and the GigaStor Supplemental Guidance for Common Criteria. These documents provide comprehensive installation, connection, and usage instructions.

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
DAC	Discretionary Access Control
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
RAID	Redundant Array of Independent Disks
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyzer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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. CA GigaStor 14.1 Security Target, v1.3, 4 August 2011.

e. Evaluation Technical Report (ETR) CA GigaStor 14.1 EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-175, Document No. 1686-000-D002, Version 1.4, 5 August 2011.