Certification Report

EAL 2+ Evaluation of Data ONTAP® 8.0.0 7-Mode and Data ONTAP® 8.0.1 7-Mode

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment Canada, 2011

Document number: 383-4-154-CR
Version: 1.0
Date: 27 October 2011
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, 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 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 27 October 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 trademarked or registered trademarks:

- NetApp and Data ONTAP are registered trademarks of NetApp, Inc.
- Windows is a registered trademark of Microsoft.

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

TABLE OF CONTENTS

Executive Summary

Data ONTAP® 8.0.0 7-Mode and Data ONTAP® 8.0.1 7-Mode (hereafter referred to as Data ONTAP), from NetApp, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 Augmented evaluation.

Data ONTAP is a microkernel operating system included in the distribution of several of NetApp's storage solutions, including the *Fabric Attached Storage* (FAS) and *V-Series appliances*. Data ONTAP is divided into three components: *Write Anywhere File Layout*® (WAFL), *Operating System Kernel* and *System Administration*. The WAFL component is responsible for implementing the discretionary access control policy. The Operating System Kernel component provides the communications between the components of the Operating System. The System Administration component provides an administrator with an interface supporting operator functions, including enforcing identification and authentication and managing user roles, as well as providing support for the Data ONTAP security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 14 October 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 Data ONTAP, 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)[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.3 - Systematic Flaw Remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Data ONTAP 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

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and may not be releasable for public review.

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 Evaluation Assurance Level (EAL) 2 Augmented evaluation is Data ONTAP® 8.0.0 7-Mode and Data ONTAP® 8.0.1 7-Mode (hereafter referred to as Data ONTAP), from NetApp.

2 TOE Description

Data ONTAP is a microkernel operating system included in the distribution of several of NetApp's storage solutions, including the *Fabric Attached Storage* (FAS) and *V-Series appliances*. Data ONTAP is divided into three components: *Write Anywhere File Layout*® (WAFL), *Operating System Kernel* and *System Administration*. The WAFL component is responsible for implementing the discretionary access control policy. The Operating System Kernel component provides the communications between the components of the Operating System. The System Administration component provides an administrator with an interface supporting operator functions, including enforcing identification and authentication and managing user roles, as well as providing support for the Data ONTAP security functionality.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Data ONTAP is identified in Section 6 of the Security Target (ST).

4 Security Target

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

Title: Security Target Data ONTAP® 8.0.0 7-Mode and Data ONTAP® 8.0.1 7-Mode
Version: 0.9
Date: 20 June 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*.

The Data ONTAP is:

a. Common Criteria Part 2 extended, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirement defined in the ST;
   - EXT_FPT_SEP.1, TSF Domain Separation for Software TOEs;

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.3 – Systematic Flaw Remediation.

6 Security Policy

Data ONTAP implements a role-based access control policy to control an administrative user's access to the system configuration, as well as a discretionary access control policy to control users' access to the data stored on the system; details of these security policies are found in Sections 5 and 6 of the ST.

In addition, Data ONTAP implements policies pertaining to security audit, user data protection, identification and authentication, protection of the TOE, TOE access and security management. Further details on these security policies are found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Data ONTAP 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 Data ONTAP.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The administrative personnel are not hostile, are competent and will follow and abide by the instructions provided by the administrator documentation; and
- Authorized users will maintain strong passwords.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Data ONTAP is assumed to be located at a physically secure location, with appropriate security measures; and
- Any other networks with which the Data ONTAP communicates are assumed to be securely managed and capable of supporting the operation and security of Data ONTAP.

7.3 Clarification of Scope

Data ONTAP is designed and intended for use in a structured corporate environment. It cannot prevent authorized administrators from carelessly configuring the TOE such that the TOE security or the security of IT system monitored by the TOE is compromised.

Data ONTAP provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

While its user guidance documents do provide adequate advice for securing its operational environment, it is primarily the user's responsibility in ensuring that the networks and the systems to which Data ONTAP is connected or installed upon are protected adequately.

8 Evaluated Configuration

The evaluated configuration consists of Data ONTAP Version 8.0.0 7-Mode and Data ONTAP Version 8.0.1 7-Mode installed on the following hardware appliances:

- FAS; and
- V-Series.

9 Documentation

The NetApp documents provided to the consumer are as follows:

a. Data ONTAP® 8.0 7-Mode System Administration Guide;

b. Data ONTAP® 8.0 7-Mode Software Setup Guide;

c. Data ONTAP® 8.0 7-Mode Upgrade Guide; and

d. Data ONTAP® 8.0.0 7-Mode and Data ONTAP® 8.0.1 7-Mode Guidance Documentation Supplement.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Data ONTAP, including the following areas:

Development: The evaluators analyzed the Data ONTAP 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 Data ONTAP security

architectural description and determined that the initialization process was 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 Data ONTAP preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 Data ONTAP configuration management system and associated documentation was performed. The evaluators found that the Data ONTAP 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 Data ONTAP during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by NetApp for Data ONTAP. 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 Data ONTAP. Additionally, the evaluators conducted a review of public domain vulnerability databases. The evaluators identified potential vulnerabilities for testing applicable to Data ONTAP 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 the 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's 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 a subset of the developer's tests on the evaluator's TOE installation;

c. Concurrent Logins: The objective of this test is to show that two concurrent logins of the same user do not interfere with each other;

d. Authentication Failure: The objective of this test is to confirm that a user will be locked out after a configured number of unsuccessful authentication attempts, that the requested audit data is generated and can be reviewed by users with appropriate roles; and

e. Password Strength: The objective of this test is to verify that password strength can be reconfigured, and to test that strength.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and may not be releasable for public review.

11.3 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. Port Scanning: The objective of this test is to confirm that only those ports that should be are open are;

b. Banner Grabbing: The objective of this test is to determine if any useful information can be gained about the TOE; and

c. Leakage Verification: The objective of this test is monitor for leakage during start-up and shut down.

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

11.4 Conduct of Testing

Data ONTAP® was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. 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 the Data ONTAP 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

NetApp, Inc. provides comprehensive guidance documents for the installation, configuration and operation of Data ONTAP. It should be operated in accordance with these documents.

Data ONTAP is designed for and should operate in a corporate environment, where any other IT based system/network with which Data ONTAP communicates should also be securely managed and be capable of supporting the operation and security of Data ONTAP.

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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FAS	Fabric Attached Storage
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WAFL	Write Anywhere File Layout®

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. Security Target Data ONTAP® 8.0.0 7-Mode and Data ONTAP® 8.0.1 7-Mode, Revision No. 0.9, 20 June 2011.

e. Evaluation Technical Report (ETR) Data ONTap®, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-154, Document No. 1709-000-D002, Version 1.0, 14 October 2011.