Certification Report

NetApp Data ONTAP® v8.1.1 7-Mode

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-223-CR
Version:	1.0
Date:	13 June 2013
Pagination:	i to iii, 1 to 11

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, 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.

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 13 June 2013, 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:

- ONTAP® is a registered trademark of NetApp, Inc.

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

TABLE OF CONTENTS

Executive Summary

NetApp Data ONTAP® v8.1.1 7-Mode (hereafter referred to as NetApp Data ONTAP v8.1.1), from NetApp, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

NetApp Data ONTAP v8.1.1 is a proprietary microkernel operating system developed by NetApp, Inc. The microkernel is included in the distribution of several of NetApp's storage solution products including the Fabric Attached Storage (FAS) and V-Series appliances. NetApp Data ONTAP v8.1.1 provides data management functions that include providing secure data storage and multi-protocol access.

NetApp Data ONTAP v8.1.1 is divided into four components: Write Anywhere File Layout® (WAFL), System Administration, Operating System Kernel, and the System Manager GUI. The four components are:

WAFL
The TOE's WAFL component is responsible for implementing the TOE's Discretionary Access Control (DAC) Security Functional Policy (SFP).

System Administration
The System Administration component provides an administrator with a Command Line Interface (CLI) that supports administrator functions including enforcing identification and authentication, user roles, and providing the necessary user interface commands that enable an authorized administrator to support the TOE's security functionality.

Operating System Kernel
The Kernel facilitates communication between the components of the Operating System.

System Manager GUI
The System Manager GUI component provides an authorized administrator with a web based GUI that supports administrator functions including enforcing identification and authentication, user roles, and providing the necessary user interface commands that enable an authorized administrator to support the TOE's security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 2 May 2013 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 NetApp Data ONTAP v8.1.1, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.3 – Flaw Remediation

Communications Security Establishment Canada, as the CCS Certification Body, declares that the NetApp Data ONTAP v8.1.1 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] 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 NetApp Data ONTAP® v8.1.1 7-Mode (hereafter referred to as NetApp Data ONTAP v8.1.1), from NetApp, Inc.

2 TOE Description

NetApp Data ONTAP® v8.1.1 7-Mode (hereafter referred to as NetApp Data ONTAP v8.1.1), from NetApp, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

NetApp Data ONTAP v8.1.1 is a proprietary microkernel operating system developed by NetApp, Inc. The microkernel is included in the distribution of several of NetApp's storage solution products including the Fabric Attached Storage (FAS) and V-Series appliances. NetApp Data ONTAP v8.1.1 provides data management functions that include providing secure data storage and multi-protocol access.

NetApp Data ONTAP v8.1.1 is divided into four components: Write Anywhere File Layout® (WAFL), System Administration, Operating System Kernel, and the System Manager GUI. The four components are:

WAFL
The TOE's WAFL component is responsible for implementing the TOE's Discretionary Access Control (DAC) Security Functional Policy (SFP).

System Administration
The System Administration component provides an administrator with a Command Line Interface (CLI) that supports administrator functions including enforcing identification and authentication, user roles, and providing the necessary user interface commands that enable an authorized administrator to support the TOE's security functionality.

Operating System Kernel
The Kernel facilitates communication between the components of the Operating System.

System Manager GUI
The System Manager GUI component provides an authorized administrator with a web based GUI that supports administrator functions including enforcing identification and authentication, user roles, and providing the necessary user interface commands that enable an authorized administrator to support the TOE's security functionality.

A detailed description of the NetApp Data ONTAP v8.1.1 architecture is found in Section 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for NetApp Data ONTAP v8.1.1 is identified in Section 1.5 of the ST.

4 Security Target

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

Title:	NetApp, Inc. Data ONTAP® v8.1.1 7-Mode Security Target
Version:	0.7
Date:	22 Oct 2012

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.*

NetApp Data ONTAP v8.1.1 is:

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

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

c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation

6 Security Policy

NetApp Data ONTAP v8.1.1 implements a role-based access control policy to control user access to the system, details of which can be found in Section 7 of the ST.

In addition, NetApp Data ONTAP v8.1.1 implements policies pertaining to security audit, user data protection, identification and authentication, security management, protection of TOE security functions, and TOE access. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of NetApp Data ONTAP v8.1.1 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:

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not hostile and will follow and abide by the instructions provided by the administrator documentation.
- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and act in a cooperating manner in a benign environment.
- Administrative functionality shall be restricted to authorized administrators.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Any other systems with which the TOE communicates are under the same management control and use a consistent representation for specific user and group identifiers.
- Security Management shall be provided to protect the confidentiality and integrity of transactions on the network.
- The processing resources of the TOE critical to the security policy enforcement will be protected from unauthorized physical modification by potentially hostile outsiders.

- The IT Environment will be configured to provide the TOE reliable time stamps by implementing the Network Time Protocol (NTP).

8 Evaluated Configuration

The evaluated configuration for NetApp Data ONTAP v8.1.1 comprises:

The TOE running on the following hardware;

- FAS appliances; and
- V-Series appliances.

The publication entitled NetApp Inc. Data ONTAP® 8.1.1 7-Mode Guidance Documentation Supplement, Version 0.5, 30 April 2013 describes the procedures necessary to install and operate NetApp Data ONTAP v8.1.1 in its evaluated configuration.

9 Documentation

The NetApp, Inc. documents provided to the consumer are as follows:

a. NetApp Inc. Data ONTAP® 8.1.1 7-Mode Guidance Documentation Supplement, Version 0.5, 30 April 2013;

b. Data ONTAP® 8.1 Commands: Manual Page Reference For 7-Mode, Volume 1, Part number: 210-05619_A0 (updated for Data ONTAP 8.1.1), 14 June 2012;

c. Data ONTAP® 8.1 Commands: Manual Page Reference For 7-Mode, Volume 2, Part number: 210-05620_A0 (updated for Data ONTAP 8.1.1), 14 June 2012;

d. Data ONTAP® 8.1 File Access and Protocols Management Guide For 7-Mode, Part number: 210-05621_A0 (updated for Data ONTAP 8.1.1), 14 June 2012;

e. Data ONTAP® 8.1 High-Availability and MetroCluster Configuration Guide for 7-Mode, Part number 210-05622_A0, 14 June 2012;

f. Data ONTAP® 8.1 MultiStore Management Guide For 7-Mode, Part number: 210-05624_A0 (updated for Data ONTAP 8.1.1), 14 June 2012

g. OnCommand System Manager 2.0.2 Help for Use With Data ONTAP 7-Mode, Part number: 215-07095_A0, August, 2012;

h. OnCommand® System Manager 2.0.2 Quick Start Guide, Part number: 215-07093_A0, August, 2012;

i. Data ONTAP® 8.1 System Administration Guide for 7-Mode, Part number: 210-05630_A0 (updated for Data ONTAP 8.1.1), 14 June 2012; and

j. Data ONTAP® 8.1 Software Setup Guide For 7-Mode, Part number: 210-05623_B0 Updated for Data ONTAP 8.1.1, 16 August 2012

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of NetApp Data ONTAP v8.1.1, including the following areas:

Development: The evaluators analyzed the NetApp Data ONTAP v8.1.1 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 NetApp Data ONTAP v8.1.1 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 NetApp Data ONTAP v8.1.1 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 NetApp Data ONTAP v8.1.1 configuration management system and associated documentation was performed. The evaluators found that the NetApp Data ONTAP v8.1.1 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 NetApp Data ONTAP v8.1.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the NetApp Data ONTAP v8.1.1. 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 NetApp Data ONTAP v8.1.1. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify NetApp Data ONTAP v8.1.1 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to NetApp Data ONTAP v8.1.1 in its operational environment.

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

11 ITS Product Testing

Testing 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.

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. Non-Interference of Concurrent Logins: The objective of this test goal is to confirm that concurrent logins do not interfere with each other;

c. Authentication Failure Handling, and Audit Data Generation, Review, and Event Storage: The objective of this test goal is to confirm how the TOE handles authentication failures; and

[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.

d. Login Password Strength Verification and Reconfiguration: The objective of this test goal is to confirm that the TOE enforces password strength and allows the password rules to be defined.

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 use automated tools 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 by grabbing the available system banners; and

c. Information Leakage Verification: The objective of this test is monitor for information 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

NetApp Data ONTAP v8.1.1 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 Test (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 NetApp Data ONTAP v8.1.1 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

In order to install the TOE, correct placement within the network is important. It is recommended that the administrator consult with their IT architect to ensure proper support for the appliance in the environment as incorrect placement within the network could lead to traffic not being detected.

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
SFR	Security Functional Requirement
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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. NetApp, Inc. Data ONTAP® v8.1.1 7-Mode Security Target, 0.7, 22 Oct 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of NetApp, Inc. Data ONTAP® 8.1.1 7-Mode, Version 1.0, 2 May 2013.