Certification Report

NetApp Clustered Data ONTAP® 8.2.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-263-CR
Version: 1.0
Date: 5 January 2015
Pagination: i to iii, 1 to 10

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, 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, 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.

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.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 5 January 2015, 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:

- NetApp®, ONTAP® and WAFL®, are registered trademarks of NetApp, Inc.
- OnCommand™ is a trademark of NetApp, Inc.

TABLE OF CONTENTS

Executive Summary

NetApp Clustered Data ONTAP® 8.2.1 (hereafter referred to as Data ONTAP), from NetApp, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Data ONTAP meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Data ONTAP is a microkernel operating system that supports multi-protocol services and data management capabilities for consolidating and protecting data for enterprise applications and users as well as the hardware appliances on which it runs. The TOE includes a separate software-only management Graphical User Interface (GUI) called the OnCommand System Manager. This GUI is used to manage the TOE security functionality (TSF). The TOE also includes a separate software-only monitoring and diagnostic component called the OnCommand™ Unified Manager (OCUM). The OCUM allows administrators to quickly identify and troubleshoot problems that arise in the monitored storage cluster.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 11 November 2014 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 Data ONTAP, 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 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 Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

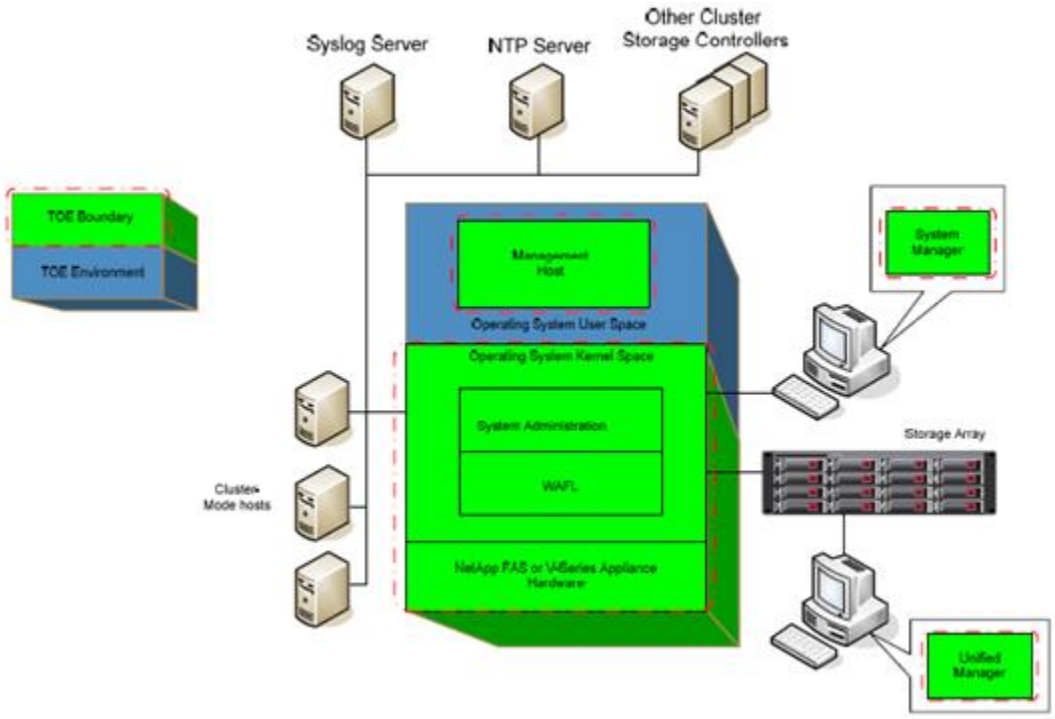
The Target of Evaluation (TOE) for this EAL 2+ evaluation is NetApp Clustered Data ONTAP® 8.2.1 (hereafter referred to as Data ONTAP), from NetApp, Inc.

2 TOE Description

Data ONTAP is a microkernel operating system that supports multi-protocol services and data management capabilities for consolidating and protecting data for enterprise applications and users as well as the hardware appliances on which it runs. The microkernel is included in the distribution of several of NetApp's storage solutions, including the Fabric Attached Storage (FAS) and V-Series appliances. The software component of the TOE is divided into six primary components, briefly described below:

- Write Anywhere File Layout® (WAFL) which is responsible for implementing the TOE's Discretionary Access Control (DAC) Security Function Policy (SFP).
- System Administration which provides an administrator with an interface supporting operator functions and providing the necessary user interface commands that enable an operator to support the TOE's security functionality.
- Operating System (OS) Kernel which facilitates communication between the components of the OS.
- Management Host which is responsible for host management and services applications for the node.
- OnCommand™ System Manager which provides an authorized administrator with a web-based GUI that supports administrator functions
- OnCommand™ Unified Manager which provides an authorized administrator with a web-based GUI, a console interface, and an exposed API. Together, these interfaces provide an authorized administrator the ability to view the status for capacity, availability, and protection relationships of the monitored systems in the storage cluster.

A diagram of the Data ONTAP architecture is as follows:



3 Security Policy

Data ONTAP implements a role-based access control policy to control administrative access to the system. In addition, Data ONTAP implements policies pertaining to the following security functional classes:

Security Audit
User Data protection
Identification and Authentication
Security Management
Protection of the TOE Security Functionality
TOE Access

4 Security Target

The ST associated with this Certification Report is identified below:

Clustered Data ONTAP® 8.2.1 Security Target, version 1.0, November 7, 2014

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.*

Data ONTAP is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:

ALC_FLR.3 - Systematic Flaw Remediation.

b. *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:*

FPT_SEP_EXT.1 - TSF domain separation for software TOEs.

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

6 Assumptions and Clarification of Scope

Consumers of Data ONTAP 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.

6.1 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 are expected to act in a cooperating manner in a benign environment.*
- *Administrative functionality shall be restricted to authorized administrators.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *Any other systems with which the TOE communicates are assumed to be under the same management control.*
- *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 SFP enforcement will be protected from unauthorized physical modification by potentially hostile outsiders.*
- *The IT Environment will be configured to allow the TOE to retrieve reliable time stamps by implementing the Network Time Protocol (NTP).*

- *Physical security of the TOE and network, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.*

7 Evaluated Configuration

The evaluated configuration for Data ONTAP comprises:

The software Data ONTAP® 8.2.1 Cluster-Mode running on one of the following hardware platforms:

- FAS8060;
- FAS8040;
- FAS8020;
- FAS6290 and V-Series 6290;
- FAS6280 and V-Series 6280;
- FAS6250 and V-Series 6250;
- FAS6240 and V-Series 6240;
- FAS6220 and V-Series 6220;
- FAS6210 and V-Series 6210;
- FAS6080;
- FAS6040;
- FAS3270 and V-Series 3270;
- FAS3250 and V-Series 3250;
- FAS3240 and V-Series 3240;
- FAS3220 and V-Series 3220;
- FAS3210 and V-Series 3210;
- FAS3170;
- FAS3160;
- FAS3140;
- FAS2240-2 and FAS2240-4; and
- FAS2220.

The publication entitled Clustered Data ONTAP® 8.2.1 Guidance Documentation Supplement version 0.6 describes the procedures necessary to install and operate Data ONTAP in its evaluated configuration.

8 Documentation

In addition to the documents identified in section 7, the following additional NetApp, Inc. documents are provided to the consumer:

- Clustered Data ONTAP® 8.2.1 Guidance Documentation Supplement version 0.6
- Clustered Data ONTAP® 8.2 Commands: Manual Page Reference

- Clustered Data ONTAP® 8.2 System Administration Guide For Cluster Administrators
- Clustered Data ONTAP® 8.2 System Administration Guide for SVM Administrators
- Clustered Data ONTAP® 8.2 File Access and Protocols Management Guide for NFS
- Clustered Data ONTAP® 8.2 File Access and Protocols Management Guide for CIFS
- Clustered Data ONTAP® 8.2 Software Setup Guide
- Clustered Data ONTAP® 8.2 High-Availability Configuration Guide
- Clustered Data ONTAP® 8.2 Network Management Guide
- V-Series Systems Installation Requirements and Reference Guide
- Clustered Data ONTAP® 8.2 Physical Storage Management Guide
- Clustered Data ONTAP® 8.2 Logical Storage Management Guide
- Clustered Data ONTAP® 8.2 Data Protection Tape Backup and Recovery Guide
- Clustered Data ONTAP Security Guidance
- Clustered Data ONTAP® 8.2.1 Release Notes For Cluster-Mode
- OnCommand® Unified Manager 6.1 Administration Guide
- OnCommand® Unified Manager 6.1 Installation and Setup Guide
- OnCommand® System Manager 3.1 Managing Clustered Data ONTAP® Using the GUI
- OnCommand® System Manager 3.1 Installation and Setup Guide.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of 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 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 Data ONTAP 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 Data ONTAP configuration management system and associated documentation was performed. The evaluators found that the Data ONTAP 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 Data ONTAP during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the 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.

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

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 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. Resulting from this test coverage approach is the following list of 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. Single Client Login: the objective of this test goal is to confirm that the System Manager will not allow multiple connections under the same session;

c. Authentication Failure Handling, and Audit Data Generation and Audit Review: the objective of this test goal is to confirm that users can be created and deleted; a user will be locked out after a configured number of unsuccessful authentication attempts; a locked out user can be unlocked; audit data can be generated and can be reviewed by users with the appropriate roles; and

[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.

d. Login Password Strength Verification and Reconfiguration: the objective of this test goal is to confirm that the login password strength is enforced and that password strength requirements can be reconfigured.

10.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

b. Banner Grab: The objective of this test goal is to determine if any useful information can be gained from a Banner; and

c. Leakage Verification: The objective of this test goal is to monitor for leakage during start up, shutdown , login and other scenarios.

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

10.4 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 Test Facility. 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.

10.5 Testing Results

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

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

The evaluator recommends that potential operators of the TOE familiarize themselves with the ST and relevant setup documentation before operating the device. The TOE should only be operated by competent personnel and special care should be taken when setting access controls for CIFS and NFS shares to prevent unintentional access.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIFS	Common Internet File System
CPL	Certified Products list
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
FAS	Fabric Attached Storage
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NTP	Network Time Protocol
NFS	Network File System
OCUM	OnCommand Unified Manager
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
WAFL	Write Anywhere File Layout

14 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. Clustered Data ONTAP® 8.2.1 Security Target, version 1.0, November 7, 2014

e. Evaluation Technical Report for NetApp, Inc. Clustered Data ONTAP® 8.2.1, Document No. 1817-000-D002 Version 1.0, 11 November 2014.