Certification Report

EAL 2+ Evaluation of

Data ONTAP Version 7.2.5.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-73-CR
Version: 1.0
Date: 4 February 2009
Pagination: i to iv, 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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.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 (CSEC).

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 Standard 17025, General requirements for the accreditation of calibration and testing 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 DOMUS IT Security Laboratory 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 4 February 2009, 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 at: http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org

This certification report makes reference to the following trademarked or registered trademarks:

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

TABLE OF CONTENTS

Executive Summary

Data ONTAP Version 7.2.5.1 (hereafter referred to as Data ONTAP), from NetApp, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Data ONTAP 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 Filer, V-Series Virtual Filer, and NearStore. Data ONTAP provides data management functions that include providing secure data storage and multi-protocol access.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 8 January 2009 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, 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 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed:

- ALC_FLR.3 – Systematic flaw remediation.

Communication Security Establishment Canada, as the CCS Certification Body, declares that 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] 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 Data ONTAP Version 7.2.5.1 (hereafter referred to as Data ONTAP), from NetApp, Inc.

2 TOE Description

Data ONTAP is a proprietary microkernel operating system developed by NetApp, Inc. It provides data management functions that include providing secure data storage and multi-protocol access.

Data ONTAP is a software product that is distributed with the following Network Appliance storage solution products:

Filer NetApp's Filer systems offer seamless access to a full range of enterprise data for users on a variety of platforms. Filer systems support NFS and CIFS for file access, as well as FCP and iSCSI for block-storage access.

Virtual Filer The Virtual Filer product family (V-Series) provides unified NAS and SAN access to data stored in Fibre Channel SAN storage arrays enabling data center storage deployment.

NearStore NearStore is a disk-based nearline storage solution and offers additional functionality including simplified backup, accelerated recovery and robust remote disaster recovery.

Both single controller and High Availability controller pairs, where the platform allows, are supported by Data ONTAP.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Data ONTAP is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: NetApp Data ONTAP Version 7.2.5.1 Security Target
Version: 37
Date: 09 January 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

Data ONTAP 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:
   - FPT_RVM_SW_EXP.1 - Non-Bypassability of the TOE Security Policies
   - FPT_SEP_SW_EXP.1 - 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

Data ONTAP implements a role-based access control policy to control administrators and non-administrators. Administrators may access the TOE via the local console and have access to the Command Line Interface (CLI). Non-administrators are users that do not have administrative access to the TOE. Data ONTAP also implements a discretionary access control policy to control users' access to the data stored on the system; details of these security policies are found in Section 5 and 6 of the ST.

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

7 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 Data ONTAP.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- The administrative and non-administrative users are assumed to be trusted and not careless, wilfully negligent, or hostile. The administrative users must follow and abide by

the instructions provided by the user guidance documentations (as identified in section 10 of this report).

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 physical security measures.
- Any other IT based systems (networks) with which 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.

It 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 users' responsibility in ensuring that the networks and the systems to which Data ONTAP is connected or installed upon are adequately protected.

8 Architectural Information

Data ONTAP is divided into three subsystems: Operating System Kernel, WAFL File System and System Administration.

Operating System Kernel	The operating system kernel subsystem provides scheduling services, manages memory, and provides services to allow the other components of the system to communicate with each other. Although critical for the correct operation of the system, the kernel does not perform any security functions.
WAFL File System	The TOE's WAFL File subsystem is responsible for implementing the TOE's Discretionary Access Control (DAC)

Security Function Policy (SFP). The DAC SFP includes enforcing access rules to user data based on client type, client security attributes, file types, file security attributes and access request (create, read, write, execute, delete, change permission, and change owner).

System Administration — The System Administration subsystem includes providing an operator interface supporting operator functions including enforcing identification and authentication, user roles and providing the necessary user interface commands that enable an operator to support the TOE's security functionality. The System Administration function is performed by the NetApp Administrator role, and this functionality is only available via the local Command Line Interface (CLI) on the TOE. System Administration functions performed at the CLI are audited by default.

9 Evaluated Configuration

The evaluated configuration consists of Data ONTAP Version 7.2.5.1 Target of Evaluation installed on the following hardware appliances.

Family	**Series**	**Model**
Filer	FAS2000	FAS2050
	FAS3100	FAS3170

The interfaces which must be disabled or maintained in a Common Criteria environment are:

Service's	**Default State**	**Evaluated State**
Command Line Interface (CLI)	ON	ON
File Transfer Protocol (FTP)	OFF	OFF
Network Data Management Protocol (NDMP)	OFF	OFF
Remote Shell (rsh)	ON	OFF
Secure Shell (ssh)	OFF	OFF
Serial Console	ON	ON
Simple Network Management Protocol (SNMP)	ON	OFF
Telnet	ON	OFF
Trivial File Transfer Protocol (TFTP)	OFF	OFF

10 Documentation

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

a. Installation, Generation and Startup Procedures for Common Criteria Deployments Version 006 (and its attachments);

b. Administrator and User Guidance for Data ONTAP Common Criteria Deployments Revision 11 (and its supplements with details provided in the document).

11 Evaluation Analysis Activities

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

Configuration management: An analysis of Data ONTAP configuration management system and associated documentation was performed. The evaluators found that 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.

Secure delivery and operation: 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 examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed Data ONTAP functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined Data ONTAP administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the flaw remediation procedures used by NetApp, Inc. 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: Data ONTAP ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's

vulnerability analysis for Data ONTAP and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

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

12.1 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].

NetApp employs a rigorous testing process that tests all releases.

The evaluators analyzed the developer's test coverage analysis and found it to be accurate.

12.2 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 DOMUS IT Security Laboratory 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. Identification and Authentication: The objective of these tests is to determine the TOE's ability to establish and verify the claimed identity of an operator who accesses the TOE;

c. System Data Protection: The objective of these tests is to determine the TOE's ability to protect itself, its system data and system configuration and provide for non-bypassibility;

[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. Audit: The objective of these tests is to ensure that Administrative User Access Events Logging requirements have been met;

e. Discretionary Access Control: The objective of these tests is to determine the TOE's ability in managing and protecting user data placed under its control.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks

The evaluator conducted a port scan. The only ports found to be open were ones that would be expected to be. The evaluator used tools such as NMAP and NESSUS to scan for network security weaknesses, and no applicable ones were found. The evaluator also directed attacks aimed at tampering with the security operation of the TOE, and none were successful.

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

12.4 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 (ITSET) Facility at DOMUS IT Security Laboratory located in Ottawa, Ontario, 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.

12.5 Testing Results

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

13 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.

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

Data ONTAP is straightforward to securely configure, manage and integrate in its intended environment.

15 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
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FCP	Fibre Channel Protocol
iSCSI	Internet small computer system interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NAS	Network-attached storage
NFS	Network File System
PALCAN	Program for the Accreditation of Laboratories Canada
SAN	Storage Area Network
ST	Security Target
TOE	Target of Evaluation
WAFL	Write Anywhere File Layout

16 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3, August 2005.

d. NetApp Data ONTAP Version 7.2.5.1 Security Target , version 37, 09 January 2009

e. NetApp, Inc., Data ONTAP Version 7.2.5.1 Target of Evaluation, Evaluation Technical Report, Version 1.0, 08 January 2009