National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

Data ONTAP Version 6.5.2R1 Operating System

Report Number: CCEVS-VR-05- 0122

Dated: 29 September 2005

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Thomas P. Murphy
Mitretek Systems
Linthicum Maryland

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Alton Lewis
National Security Agency
Linthicum, Maryland

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

List of Figures

List of Tables

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the Network Appliance Data ONTAP 6.5.2R1 Operating System at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on August 29, 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is a pair of software modules that reside within several families of hardware storage solutions developed by Network Appliance. All of the supporting platforms for the evaluated TOE contain the Data ONTAP Operating System Version 6.5.2 R1. Data ONTAP is a proprietary microkernel operating system developed by Network Appliance. The TOE is composed of only 2 modules: System Administration and Write Anywhere File Layout (WAFL). The remainder of the OS and the supporting hardware platforms were treated as part of the IT Environment for this evaluated TOE. The software is preinstalled in the distribution of the NearStore, gFiler, and Filer products developed by Network Appliance. The microkernel software operates on an embedded processor within the storage hardware appliance. The appliance also contains all the disk drives needed to store user data. The Data ONTAP TOE provides data management functions that include secure data storage and multi-protocol access. Secure storage is provided by Data ONTAP through implementation of strict access control rules to obtain data managed by Data ONTAP. Multi-protocol access support is provided by Data ONTAP through operation of both NFS and CIFS clients and providing transparent access to all data including cross-protocol access requests.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desire a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP CCEVS' Validated Products List. Table 1 provides information needed to completely identify the product, including:

- the Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated,
- the Security Target (ST), describing the security features, claims, and assurances of the product,
- the conformance result of the evaluation,
- The organizations and individuals participating in the evaluation.

Table 1 - Evaluation Identifiers

Evaluation Identifiers for Data ONTAP Version 6.5.2 R1 Operating System	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Network Appliance Data ONTAP 6.5.2R1 Operating System
Protection Profile	N/A
Security Target	Network Appliance Data ONTAP 6.5.2R1 Operating System Security Target, dated October 13, 2005
Evaluation Technical Report	Network Appliance Data ONTAP 6.5.2R1 Operating System Evaluation Technical Report, Document No. F2-0805-005, Dated October 13, 2005
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on July 26, 2004.
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on July 26, 2004
Sponsor	Network Appliance 495 East Java Drive Sunnyvale, CA 94089
Developer	Network Appliance 495 East Java Drive Sunnyvale, CA 94089
Evaluator(s)	**COACT Incorporated** Brian Pleffner Anthony Busciglio Ching Lee
Validator(s)	**NIAP CCEVS** Thomas P. Murphy Dr. Jerome Myers Alton Lewis

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0405 – American English Is an Acceptable Refinement

I-0422 – Clarification Of ``Audit Records''

I-0423 – Some Modifications to the Audit Trail Are Authorized

I-0427 – Identification of Standards

International Interpretations

RI#003 – Unique identification of configuration items in the configuration list (11 February 2002)

RI#008 – Augmented and Conformant overlap (31 July 2001)

RI#016 – Objective for ADO_DEL (11 February 2002)

RI#019 – Assurance Iterations (11 February 2002)

RI#031 – Obvious vulnerabilities (25 October 2002)

RI#049 – Threats met by environment (16 February 2001)

RI#064 – Apparent higher standard for explicitly stated requirements (16 February 2001)

RI#065 – No component to call out security function management (31 July 2001)

RI#075 – Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1 (15 October 2000)

RI#084 – Aspects of objectives in TOE and environment (31 July 2001)

RI#085 – SOF Claims additional to the overall claim (11 February 2002)

RI#116 – Indistinguishable work units for ADO_DEL (31 July 2001)

RI#127 – Work unit not at the right place (25 October 2002)

3 Security Policy

The TOE resides in an appliance that functions as a Network Attached Storage Device. The TOE protects users' files from access by any unauthorized user or groups of users. The TOE also implements a security policy that restricts the management of the TOE to properly identified and authenticated local administrators.

The TOE mediates access of subjects to objects. The subjects covered are NFS Clients and CIFS Clients. The objects covered are files (user data). The TOE maintains files with either NTFS-Style security attributes or UNIX-Style security attributes or both. The access modes covered by the DAC SFP are: create, read, write, execute, change permission and change owner. Since the rules governing file access are complex, interested parties should examine the Administrator's documentation to determine the specific Security Functions implemented by the TOE in detail.

3.1 Administrative Security

The Administrative Security provides the necessary functions to allow an administrator to manage and support the TOE Security Function (TSF). Included in this functionality are the rules enforced by the TOE that defines access to TOE maintained TSF Data and TSF Functions. The TSF Data includes both authentication data used to authenticate administrators, security attribute data used for Direct Access Control SFP enforcement and other TSF data used for DAC SFP subject security attribute resolution. The Command Line Interface (CLI)

provides the necessary Administrative operator functions to allow an administrator to manage and support the TSF. The Administrator Guide provides information and guidance on the use of CLI for Administrator functions.

The TOE maintains two roles for users: administrators and non-administrators. Administrators are required to identify and authenticate themselves to the TOE before allowing any modifications to TOE- managed TSF Data. The authentication data used for I&A, username and password, is maintained locally by the TOE; Administrators are allowed to modify TOE-managed TSF data including authentication data, security attributes and other TSF Data.

Non-administrators are users who access the TOE via a remote system using NFS or CIFS client software. Non-administrators have access to TOE-managed user data, but do not have authority to modify TOE-managed TSF data. Access to TOE-managed user data by non-administrators is covered by the TOE's DAC SFP.

The TOE's TSF Data Management includes management of both authentication data and security attributes

3.2 Discretionary Access Control (DAC) Security

The DAC mediates access of subjects to objects. The subjects are NFS Clients and CIFS Clients. The objects covered are stored files (TSF user data). The TOE maintains files with either NTFS-Style security attributes or UNIX-Style security attributes or both. The access modes covered by the DAC SFP are: create, read, write, execute, change permission and change owner. Each file style is assigned different security attributes that are used by the DAC SFP to determine if access is granted for a subject.

The DAC SFP protects user data. The DAC SFP uses the subject type, subject's security attributes, the object, the object's security attributes and the access mode (operation) to determine if access is granted. The subjects that apply to the DAC SFP are administrators, NFS Clients and CIFS Clients. The latter two subjects access the TOE via remote systems as a process acting on behalf of a user. To determine if access is permitted for an object, the TOE requires the security attributes associated with the client. Access controls are implemented based upon the user identity that is presented along with the access request on the network interface. The TOE relies upon the requesting client in the IT Environment to have properly identified and authenticated the user associated with the request. The only identification and authentication functionality that is directly provided by the TOE is for the serial interface that is used to perform TOE administration.

The DAC SFP rules that apply depend on the subject, the operation, and the object. In addition, the objects file type (directory, symbolic link and regular file) are used to determine access and the type of qtree (directory) the file is stored in is considered for cross-protocol access requests. The TOE does not support cross-protocol support of the Change Owner access request. Only NFS Clients can change ownership of UNIX-Style files. Only CIFS Clients can change ownership of NTFS-Style files.

3.3 TOE Separation

The TOE ensures that all functions are invoked and succeed before the next function may proceed.

3.4 Security Function Strength of Function Claim

The only mechanism in the TOE for which an SOF claim is required is the Password mechanism which is SOF-basic.

3.5 Protection Profile Claim

This Security Target does not claim conformance to any registered Protection Profile

4 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's IT Environment. This includes information about the connectivity, personnel, and physical side of the environment plus potential threats.

4.1 Connectivity Assumptions

The TOE is intended for use in areas that have physical control and monitoring. It is assumed that:

- Any other systems with which the TOE communicates are under the same management control and operate under the same security policy constraints.

4.2 Personnel Assumptions

The TOE is intended to be managed by competent non-hostile individuals. It is assumed that:

- 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 careless, willfully negligent or 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.

4.3 Physical Assumptions

The TOE is intended for use in areas that have physical control and monitoring. It is assumed that:

- The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.
- The processing resources of the TOE critical to the security policy enforcement will be protected from unauthorized physical modification by potentially hostile outsiders.
- All devices on which the TOE resides and their connections will be housed within a controlled access facility.

4.4 Potential Threats

Potential threats are:

- Improper administration may result in defeat of specific security features.
- Configuration data or other trusted data may be tampered with by unauthorized users due to failure of the system to protect this data.
- An unauthorized user may attempt to access TOE data or Security Functions by bypassing a security mechanism.
- User data may be tampered with by other users.

5 Clarification of Scope

The primary function of the TOE is to provide controlled access to files through its network interface. Access controls are implemented based upon the user identity that is presented along with the access request on the network interface. The TOE relies upon the requesting client in the IT Environment to have properly identified and authenticated the user associated with the request. The only identification and authentication functionality that is directly provided by the TOE is for the serial interface that is used to perform TOE administration.

The TOE is a subset of a proprietary microkernel operating system developed by Network Appliance. The TOE consists of the System Administration and Write Anywhere File Layout (WAFL) modules. The TOE works in conjunction with a microprocessor card embedded in storage products to control access to data stored within the storage product. The microkernel is included in the distribution of several of Network Appliance's storage solution hardware products including NearStore, gFiler, and Filer. As part of the evaluation, it was determined that those three families of hardware platforms met the IT Environmental requirements necessary for the TOE to meet its claims. The results of this evaluation are only valid for the TOE when it resides in one of those three families of hardware appliances.

6 Architecture Information

Data ONTAP is a proprietary microkernel operating system developed by Network Appliance. The microkernel's two modules are included in the distribution of several of Network Appliance's storage solution hardware products including NearStore, gFiler, and Filer. The Data ONTAP modules perform data management functions that include enforcing secure data storage and multi-protocol access. Secure data storage is enforced by implementing strict access control rules to obtain data managed by Data ONTAP. Multi-protocol access support is provided by supporting both NFS and CIFS clients with transparent access to data including cross-protocol support.

6.1 TOE Security Functions

The properties of the TOE necessary for the TOE to provide its security functionality are:

- The TOE will ensure that users gain only authorized access to the TOE and to the data the TOE manages.
- The TOE will provide administrative roles to isolate administrative actions.
- The TOE will control access to user data based on the identity of users and groups of users.
- The TOE is designed and implemented in a manner that insures the organizational policies are enforced in the target environment.
- The TOE will require users to identify and authenticate themselves.
- The TSF will provide functions and facilities necessary to support the authorized administrators that are responsible for the management of TOE security.

6.2 IT Environment Security Functions

The properties of the IT operational Environment of the TOE necessary for the TOE to be able to provide its security functionality are:

- The IT Environment will ensure that users gain only authorized access to the data the IT Environment manages.
- The IT Environment will provide administrative roles to isolate administrative actions.

- The IT Environment must allow authorized users to access only appropriate TOE functions and data.
- The IT Environment will provide the TOE with the appropriate subject security attributes.

6.3 Non-IT Environment Security Functions

The properties of the non- IT operational Environment of the TOE necessary for the TOE to be able to provide its security functionality are:

- Those responsible for the TOE must ensure that all access credentials, such as passwords, are protected by the users in a manner that maintains IT security objectives.
- Those responsible for the TOE and hardware required by the TOE, must ensure that the TOE is delivered, installed, configured, managed, and operated in a manner which maintains IT security objectives.
- Those responsible for the TOE must ensure that the TOE modules critical to security policy are protected from physical attack that might compromise the IT security objectives.
- Those responsible for the TOE will be properly trained and provided the necessary information that ensures secure management of the TOE and the IT Environment.
- The TOE must provide secure management of the Configurable Policy, users, user attributes, auditing, and device configuration.
- The TOE must protect itself against external interference or tampering by untrusted subjects, or attempts by untrusted subjects to bypass the TOE security functions. All access to TOE functions requires Password authorization.

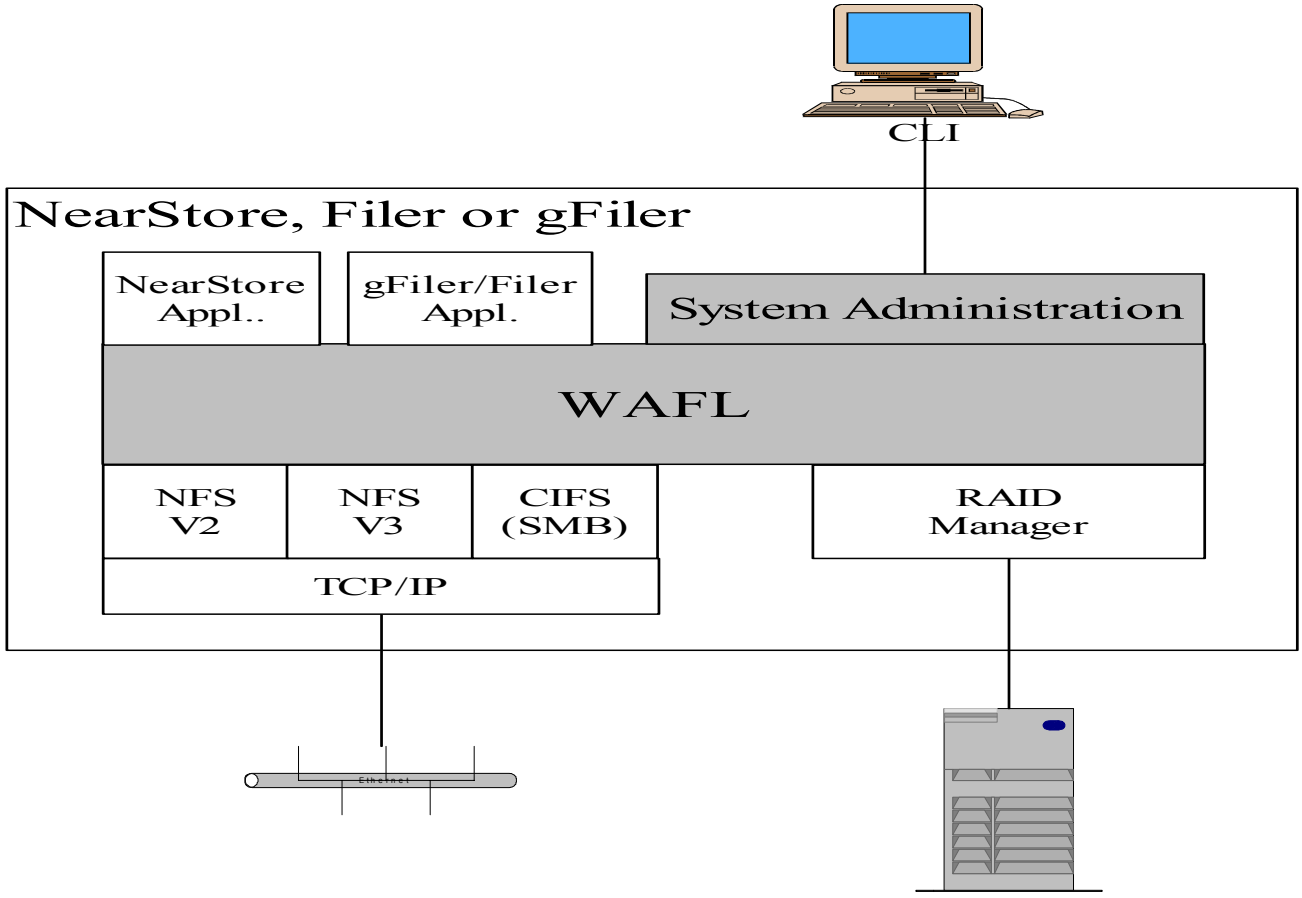
6.4 Physical Boundary

The TOE software is delivered preinstalled on one of Network Appliance's storage solution hardware products (see Section 7 for hardware product list) including NearStore, gFiler, and Filer. The TOE processor is on a card installed in the hardware filer with the TOE preinstalled as part of the operating system for the processor. When purchasing a Network Appliance storage product, users must ensure that **Data ONTAP Version 6.5.2R1 Operating System** is included as part of the product to ensure conformance with the validated product as tested.

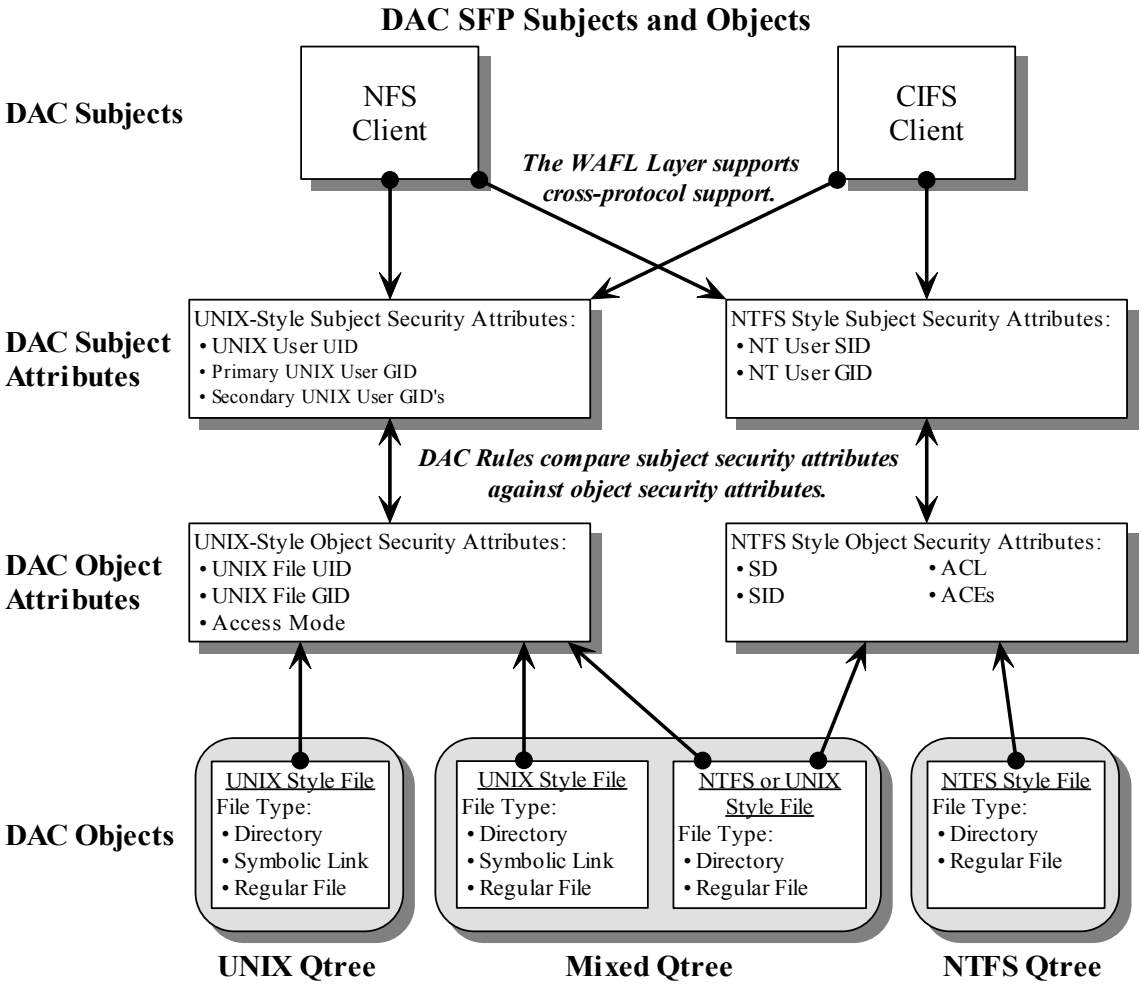
6.5 Logical Boundary

Data ONTAP is divided into two modules: System Administration and Write Anywhere File Layout (WAFL). The WAFL module implements the DAC 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). The System Administration module includes an operator CLI interface supporting **administrator** functions for enforcing identification and authentication, user roles and user interface commands that enable an **administrator** to support the TOE's security functionality. **The shaded areas in** Figure 1 depict the TOE's logical boundaries.

Figure 1 - Internal Logical Boundaries



The logical boundaries of the TOE include DAC and Administrative functionality. The dministrative functionality includes supporting operator functions for 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 DAC logical boundary includes enforcing access rules to data based on client type, client security attributes, file type, file security attributes and operation. DAC is implemented by the TOE's WAFL module. The DAC SFP protects User data. The DAC SFP uses the subject, the subject's security attributes, the object, the object's security attributes and the access mode to determine if access is granted. Figure 2 depicts the DAC SFP relationships.



The resolution of subject security attributes is processed differently by the TOE for each type of client because the two protocols are different. Cross-protocol access requires additional TSF data (usernames) to resolve the appropriate subject security attributes. UNIX User UIDs and NT User UIDs (NT User SIDs) are not directly mapped by the TOE. Instead, UIDs are mapped to the username associated with the UID, the username is then mapped to the other protocol's username and then this new username is used to find the new protocol's UID.

7 Product Delivery

As stated previously the software is delivered installed on one of Network Appliance's storage solution hardware products including NearStore, gFiler, and Filer. The vendor considers all delivered embedded processors to have identical attributes, instruction sets and operation. The TOE as tested was delivered pre-installed on a hardware filer system tied to a standard size-shipping palette. The delivered box contains the installed TOE and two additional boxes with mounting brackets, power cables, and start up documentation. The TOE processor is on a card installed in the hardware filer with the TOE preinstalled as part of the operating system for the processor. The main difference between specific hardware models are the microprocessor speed and size of the disk storage available. Only a product with the **Data ONTAP Version 6.5.2R1 Operating System** installed meets the conformance requirements of the TOE as tested. Therefore purchasers of the product must specify that the **Data ONTAP Version 6.5.2R1 Operating System** is preinstalled on their hardware product. Product Documentation

should explicitly state that the **Data ONTAP Version 6.5.2R1 Operating System** is installed on the delivered product.

The full range of Network Appliance storage appliances products that support the TOE are listed below:

- STANDALONE:
  - FAS900 series
  - FAS200 series
  - NearStore R200
  - NearStore R150
  - NearStore R100
  - F800 series
  - F700 series
  - F87
  - F85

- CLUSTERED:
  - FAS980c
  - FAS960c
  - FAS940c
  - FAS270c
  - F880c
  - F840c
  - F825c
  - F820c
  - F810c
  - F760c
  - F740c

Clustered units are connected via installed fiber channel links.

The delivered TOE documentation included *Installation Instructions for NetApp FAS250 Storage Appliances* (Part No. 210-00713+A0), *Appliance Grounding Procedure* (Part No. 210-00573+A0), *Telco Tray and Rail Kit Installation Instructions* (Part No. 210-00623+A0), Registration Card, *Documentation and software are online* (Part No. 210-00718+A0) (instructions to download software and documentation), and *Warranty Agreement, Safety Information, and Regulatory Notices* (Part No. 210-00653+A0). A serial number identification was labeled on all of the materials and parts that came with the TOE packaging. The Filer system (FAS 250) was also identified with an individual serial number.

To retrieve the documentation from the website the user must have the TOE serial number to show actual purchase of the product and the website verifies such before allowing access to the documentation pages. The website clearly states the version of the TOE is described in each document. Only **Data ONTAP Version 6.5.2R1 Operating System** conforms to the TOE as tested. Each document can be downloaded in HTML format and PDF format.

Documentation online pertaining to the TOE:

- *Installation, Generation, and Start-Up Procedures* (Version 3, July 27, 2005)
- *Data ONTAP 6.5 Software Set Up Guide* (Part No. 210-00478)
- *Data ONTAP 6.5 System Administration Storage Management Guide* (Part No. 210-00472) *Data ONTAP 6.5 System Administration File Access Management Guide* (Part No.210-00473)
- *Administrator and User Guidance for Data ONTAP Common Criteria Deployments For Data ONTAP 6.5.2R1* (Version 3, July 27, 2005)
- *Commands Manual Page Reference* (Part No. 210-00480)

8 IT Product Testing

Testing was performed on Thursday, July 21, 2005 at the COACT Laboratory in Columbia, MD. Two COACT employees performed the tests in the presence of the Lead Validator and a Vendor's Representative. All test configurations operated properly and tests were completed in an expeditious manner.

8.1 Evaluator Functional Test Environment

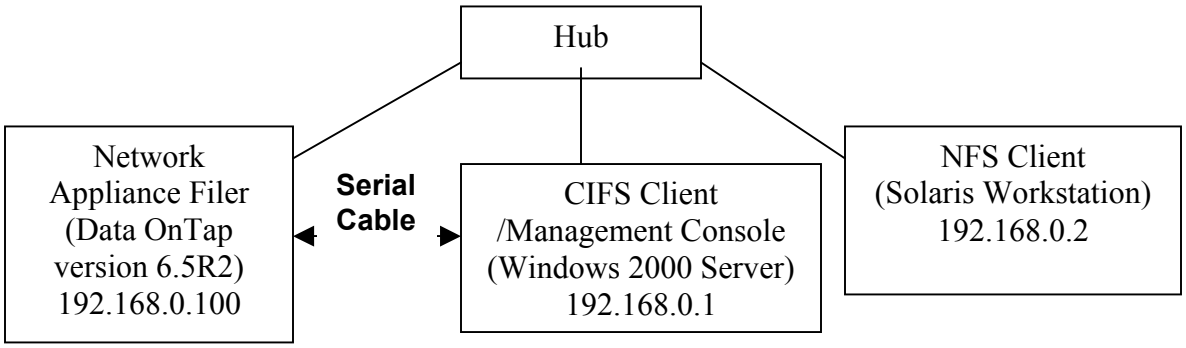
The functional test configuration included four major components, a PC with the necessary software (listed below) installed for use as the TOE management console/CIFS client, the TOE factory installed on a Network Appliance Filer series 250 appliance, a Hub, and a Solaris Workstation for use as the NFS client.

The Network Appliance Data ONTAP Version 6.5.2R1 (i.e., the TOE) was installed on the Network Appliance Series 250 Filer.

- CIFS Client/Management Console (PC) with the following software installed, Windows 2000 Server Service Pack 3, HyperTerminal, Ethereal version 0.10.11 & Nmap version 1.3.1
- Serial Cable
- Linksys 5-Port Hub (model: EW5HUB)
- NFS Client (Sun Blade Workstation) with the following software installed: Solaris 8 patch 117350-21
- (3) Ethernet cables

The following figure graphically displays the test configuration used for functional testing.

Test Configuration Diagram



8.2 Test Assumptions

The functional test environment/configuration requires no test specific assumptions outside of those identified in the ST. The test bed setup used for this set of tests is the same as that used for the functional test suite. Two users are established and four groups are established.

The evaluated configuration includes the three Network Appliance products: gFiler , Filer, and NearStore. All these products are distributed with Data ONTAP 6.5.2R1 and are described below.

gFiler: The gFiler product family provides unified NAS and SAN access to data stored in Fibre Channel SAN storage arrays enabling data centered storage deployment.

Filer: The Filer product family provides unified NAS and SAN access to data.

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

8.3 Data ONTAP Evaluated Configuration Options

The evaluated configuration options were set as follows:

- Access Protocol Options- The IT Environment supports multiple protocol servers. The evaluated configuration supports NFS and CIFS clients only. The following services are disabled: *telnet, tftp, ftp, ndmp* and *http.*

- Name Service Options - The evaluated configuration supports both local and remote resolution (NIS or LDAP) of TSF Data used to support the DAC SFP, but does not support remote resolution of authentication data (*nsswitch.conf passwd* file).

- Test Conditions – In addition to the disabled servers:
  - The wafl.root_only_chown option for the evaluated configuration is disabled.
  - Shared level ACLs are not evaluated.
  - The password field in the /etc/groups file is not used (should be blank).
  - The evaluated configuration will not include the bypass traverse checking option.
  - The evaluated configuration does not support changing a qtrees style once the qtree is configured.

8.4 Repeated Developer Tests to Confirm Developer Test Results

This section lists tests required to confirm the developer test results. The evaluation team selected all of the vendor tests to be reproduced due to the dependencies they have on one another. The following list presents the tests:

- NFS.01 Create Dir in UNIX Qtree
- NFS.02 Create Dir in NTFS Qtree
- NFS.03 Create Dir in Mixed Qtree
- NFS.04 NFS Change Ownership
- NFS.05 Create u1 and u2 Files
- NFS.06 Multiprotocol Success
- NFS.07 NFS Multiprotocol Failure
- NFS.08 NFS access from unauthorized NFS client system
- CIFS.01 Set up directories with ACLs
- CIFS.02 Set up CIFS user files with ACLs.

- CIFS.03 CIFS Multiprotocol Success
- CIFS.04 CIFS Multiprotocol Failure
- CIFS.05 CIFS Login
- SM.01 CLI Login
- SM.02 User Admin Command
- SM.03 Create Qtrees and Shares
- SM.04 Change type of ntfsqt

8.5 Functional Test Results

All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the Data ONTAP 6.5.2R1 Test Documentation for Common Criteria EAL2 Evaluation.

8.6 Evaluator Independent Testing

The tests chosen for independent testing allow the evaluation team to exercise the TOE in a different manner than that of the developer's testing. The intent of the independent tests is to give the evaluation team confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. The selected independent tests allow for a finer level of granularity of testing compared to the developer's testing, or provide additional testing of functions that were not exhaustively tested by the developer. The tests allow specific functions and functionality to be tested. The tests reflect knowledge of the TOE gained from performing other work units in the evaluation. For example, specific TSFI behaviors were identified while performing the ADV work units, and tests have been developed to test specific behaviors.

To determine the independent testing to be performed, the evaluators first assessed the level of developer testing corresponding to all TSFIs. The Independent Tests performed were:

- Test the ability to modify the file wafl.default_unix_user by users and administrators.
- Test the ability to modify the file wafl.default_nt_user by users and administrators.
- Test the ability to modify the file /etc/passwd by users and administrators.
- Test the ability to modify the file /etc/groups by users and administrators.
- Test the ability to modify the file usermap.cfg by users and administrators.
- Test different administrator identification and authentication combinations to verify SFR claims.
- Test the ability to turn the NFS module on and off and verify users are identified correctly by the operating system.
- Test the ability to terminate and restart the CIFS module and verify users are identified correctly by the operating system.

8.6.1 Evaluator Independent Test Environment

The test environment used to conduct these tests consisted of:

- A Network Appliance FAS250 Filer, running Data ONTAP 6.5.2R1 as described in the Security Target documentation. (Note that the vendor states that any NetApp Filer, gFiler, or NearStore system may be used to duplicate these tests, as none of the TSF behavior is dependent on the underlying hardware platform selected.)
    - The TOE was configured as described in the Delivery and Installation, and Administrator Guidance documentation.

  - In particular, to match the specifications in the Security Target documentation the TOE was configured with NFS and CIFS enabled, but with all other optional services and protocols disabled. Disabled services included FTP, Telnet, TFTP, HTTP, SNMP, RSH, NDMP, FCP, and iSCSI.
  - Data ONTAP is capable of enabling additional software components to provide data backup and recovery services, storage virtualization, and other functions. These additional software components (for example SnapMirror, SnapVault, MultiStore, SnapDrive, etc.) are enabled through the installation of license keys for each component. No such license keys were installed, and none of these additional software components were enabled.

- A PC running Microsoft Windows 2000 Server installed.
  - This device was used both as the CIFS client for testing, and was used to connect to the Filer's serial port for access to the command line interface (CLI). (Note that the version of Windows selected for use as a CIFS client is unimportant for this test process. The TSF behavior does not depend on the version of Windows being used on the remote client system, as changes in TSF behavior based on client version would simply allow an attacker to select the client version with the worst security attributes when performing an attack. While Data ONTAP does have provisions for configuring authentication behavior for support of older client systems, this behavior is configured by an administrator on the TOE, rather than being specified by the CIFS client. Furthermore, these configuration options do not change the overall behavior of the TSP/TSF from that tested below.)

- A Sun Workstation running Solaris 8 (SunOS 5.8) with kernel patch 117350-21.
  - This system was used as the authorized NFS client for the bulk of the testing.

- Test Conditions
  - The following services are disabled: FTP, Telnet, TFTP, HTTP, SNMP, RSH, NDMP, FCP, and iSCSI.
  - The wafl.root_only_chown option for the evaluated configuration is disabled.
  - Shared level ACLs are not evaluated.
  - The password field in the /etc/groups file is not used (should be blank).
  - The evaluated configuration will not include the bypass traverse checking option.
  - The evaluated configuration does not support changing a qtrees style once the qtree is configured.

8.7 Evaluator Independent Test Results

All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the:

- Data ONTAP 6.5.2R1 Test Documentation for Common Criteria EAL2 Evaluation.

8.8 Evaluator Penetration Tests

8.8.1 Evaluator Assessment of Developer Analysis

The evaluator examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. After consulting the sources identified by the developer used during the initial vulnerability analysis, the evaluator consulted other vulnerability relevant sources of information to verify that the developer considered all available information when developing the non-exploitation rationale. These additional sources include:

- https://cirdb.cerias.purdue.edu/coopvdb/public/
- http://www.securityfocus.com
- http://www.osvdb.org/
- http://xforce.iss.net/
- http://icat.nist.gov/icat.cfm

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluator made an assessment of the rationales provided by the developer indicating that the vulnerability is non-exploitable in the intended environment of the TOE. Any possible vulnerability that requires further evaluator analysis, such as, an Attack Potential Calculation is identified as suspect.

The evaluator found two of the developer rationales describing why a particular possibly relevant vulnerability of the TOE was not exploitable to be suspect. Therefore the evaluator tested the TOE to ensure the TOE was properly resistant to the relevant vulnerabilities.

8.8.2 Additional Vulnerabilities

While verifying the information found in the developer's vulnerability assessment the evaluator conducted a search to verify if additional obvious vulnerabilities exist for the TOE. This search included examining the websites identified in section 3.1 of this document. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities. The additional analysis conducted by the evaluator identified several additional vulnerabilities that may possibly be relevant to the TOE. Therefore the evaluator tested the TOE to ensure the TOE was properly resistant to the additional identified vulnerabilities. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator.

8.9 Evaluator Penetration Test Identification

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search for obvious TOE vulnerabilities, the evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the vulnerabilities. The following Penetration tests were performed by the evaluator:

- The evaluator will examine the descriptions and guidance regarding the network the TOE resides within provided to the administrators to verify that it is communicated that the administrator must ensure that IP address integrity is ensured.
- This test will use a Port Scan of the device the TOE is shipped on to verify that any protocol identified in the ST as being disabled is actually not available.
- The test will attempt to remotely navigate to the /etc directory.
- This test will include multiple incorrect login attempts to verify that the TOE presents a 3-second delay each time three consecutive failed login attempts are detected.

- This test will attempt to circumvent the DAC policy by changing the user's access permissions while the user is accessing the file using a NFS client.
- This test will attempt to circumvent the DAC policy by changing the user's access permissions while the user is accessing the file using a CIFS client.
- This test will attempt administratively connect to the TOE using HTTP and Telnet

8.10 Actual Penetration Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to the all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

9 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document *Evaluation Technical Report for the Network Appliance Data ONTAP 6.5.2R1* contains the verdicts of "PASS" for all the work units.

The evaluation determined the product to meet the requirements for EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

This evaluated TOE consists of a portion of a software product that is delivered with the network hardware storage appliance. The TOE does not operate separately from the network hardware storage appliance but only as an integral part of the data storage device. The security performance of the TOE is dependent on the rules and restrictions entered by the system administrator during initial set-up and during registration of users. Access to data is controlled by the permissions and constraints developed and created by the system administrator. The administrative functions are directly entered into the TOE by a Command Line Interface from a connected Windows server.

The evaluation results depended upon the fact that all of the evaluation platforms operated identically from the perspective of the TOE. This conclusion was reached by analysis. The TOE was only tested on one hardware platform. The specific NetAppliance hardware used during the evaluation functioned properly. Any differences among the hardware appliance microprocessors due to future changes in the appliance environment may compromise the result. Such changes would require retest and re-evaluation.

The CCTL evaluation of the TOE was both rigorous and comprehensive. The test bed and test plan were well thought out. The tests were conducted professionally and promptly. Developer

functional tests were repeated to assure TOE maturity. Both positive and negative tests were performed to determine that the TOE performed properly to permit access as well as constrict access when appropriate. The independent tests were well thought out and provided additional assurance that the TOE performed as planned and desired. The penetration tests properly completed the test cycle by stressing the TOE and NetAppliance hardware through persistent attempts to compromise the data and data access. Throughout the evaluation the TOE performed as expected and met all requirements of the ST.

11. Security Target

The Security Target document, Document No. E2-0504-007(8) Data ONTAP Version 6.5.2R1 Security Target dated July 26, 2005 is incorporated here by reference.

12. Glossary

CC	Common Criteria
EAL2	Evaluation Assurance Level 2
IT	Information Technology
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13. Bibliography

The following list of standards were used in the evaluation of the Network Appliance Data ONTAP 6.5.2R1:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.2, dated January 2004

- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.2, dated January 2004
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000