National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13

Report Number: CCEVS-VR-VID11175-2021
Dated: 8 September 2021
Version: 1.0

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

Acknowledgements

Validation Team

Jerome F. Myers, PhD

James J. Donndelinger

Marybeth S. Panock

The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 3
3 TOE Architecture 5
4 Security Policy 8
4.1 Cryptographic Support 8
4.2 User Data Protection 8
4.3 Security Management 8
4.4 Protection of the TSF 8
5 Assumptions and Clarification of Scope 9
5.1 Assumptions ..... **Error! Bookmark not defined.**
5.2 Clarification of Scope 10
6 Documentation 11
7 IT Product Testing 12
7.1 Test Configuration 12
8 Evaluated Configuration 14
9 Results of the Evaluation 16
9.1 Evaluation of the Security Target (ST) (ASE) 16
9.2 Evaluation of the Development (ADV) 16
9.3 Evaluation of the Guidance Documents (AGD) 16
9.4 Evaluation of the Life Cycle Support Activities (ALC) 16
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 17
9.6 Vulnerability Assessment Activity (AVA) 17
9.7 Summary of Evaluation Results 18
10 Validator Comments/Recommendations 19
11 Security Target 20
12 Abbreviations and Acronyms 21
13 Bibliography 22

List of Tables

Table 1: Evaluation Identifiers 3

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 11, where any restrictions on the evaluated configuration are highlighted.

The evaluation was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Leidos. The evaluation determined that the TOE is:

- Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant

and demonstrates exact conformance to:

- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata, February 1, 2019 [5]
- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0 + Errata, February 1, 2019 [6]

as clarified by all applicable Technical Decisions.

The TOE is NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13.

The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5). The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units documented in the Evaluation Technical Report (ETR) and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profiles (PPs) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST [9].

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT products desiring 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's Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP/PP-Modules to which the product is conformant
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13
Security Target	NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target, Version 1.0, 14 June 2021
Sponsor & Developer	NetApp, Inc. 1395 Crossman Avenue Sunnyvale, CA 94089
Completion Date	August 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
PPs	*collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata, February 1, 2019 *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0 + Errata, February 1, 2019
Conformance Result	PP Compliant, CC Part 2 Extended, CC Part 3 Conformant

Item	Identifier
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Anthony Apted Kevin Steiner Punit Patel
Validation Personnel	Jerome F. Myers, PhD James J. Donndelinger Marybeth Panock

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13. It provides software-based encryption technology that ensures data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen. The TOE supports data encryption on a volume-granular basis.

The ONTAP 9.7P13 component of the TOE is a proprietary operating system and data management software which is installed on the appliances identified in Section 1.1 of the ST that offers unified storage for applications that read and write data over block- or file-access protocols.

3.1 TOE Evaluated Configuration

Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The TOE comprises a range of disk storage appliances, consisting of storage controllers and one or more enclosures of disk storage devices (which could be HDD, SDD, or NVMe flash), running ONTAP 9.7P13. The NetApp appliances included in the TOE are listed in the table below.

ONTAP 9.7P13 is a proprietary operating system and data management software that provides storage for applications that read and write data over block- or file-access protocols, in storage configurations that range from high-speed flash, to lower-priced spinning media, to cloud-based object storage (not included in the evaluated configuration). All of the disk drives used in the TOE appliances are third party devices.

The TOE provides a software-based encryption technology for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen. The software-based encryption supports data encryption on a volume granular basis. Volume data is encrypted using 256 bit AES in XTS mode. Physical storage volumes are abstracted as logical entities called storage virtual machines (SVMs). In Common Criteria mode, an internal Onboard Key Manager (OKM) is used to manage the system's cryptographic keys.

The TOE implements both the encryption engine functionality for encrypting all user data stored on its disk storage and the authorization acquisition functionality for obtaining an authorization factor from an administrator that the TOE uses to access the keys that protect stored user data.

The TOE supports a single authorization factor, the Cluster Passphrase (CP), which is a 64-256 byte, user-defined ASCII string. The TOE uses its approved CTR_DRBG function to generate a 256 bit random number called the Cluster Salt (CS). The CS is concatenated with the CP to form a bit string of between 512 and 2560 bits (depending on the length of CP). The TOE uses the PBKDFv2 function to derive the Cluster Passphrase Key Encryption Key (CP-KEK) from the concatenation of CS and CP.

The TOE additionally uses its approved CTR_DRBG function to generate the following keys: Cluster Key Encryption Key (CKEK); Storage Virtual Machine Key Encryption Key (SVM-KEK); and Volume Data Encryption Key (VDEK). The CKEK and SVM-KEK are 256 bit AES keys. The TOE uses the KWP-AE(P) key wrapping function to wrap the CKEK using the CP-KEK, and to wrap the SVM-KEK using the CKEK.

The TOE uses its approved CTR_DRBG function to generate two 256 bit random numbers that it concatenates to form the 512 bit VDEK. This is an AES-XTS key with a 256 bit encryption/decryption key

and a 256 bit “tweak” key, as defined in IEEE 1619. The TOE uses the KWP-AE(P) function to wrap the VDEK using the SVM-KEK.

NetApp appliances typically are configured in cluster nodes in high-availability (HA) pairs for fault tolerance and non-disruptive operations. The nodes communicate with each other over a private, dedicated cluster interconnect. The HA interconnect allows each node to continually check whether its partner is functioning and to mirror log data for the other’s non-volatile memory. If a node fails or if a node needs to be brought down for routine maintenance, its partner can take over its storage and continue to serve data from it. The partner gives back storage when the node is brought back on-line. The HA functionality was not covered in the scope of the evaluation or testing.

Depending on the controller model, node storage consists of flash disks, HDDs, or both. Network ports on the controller provide access to data. Physical storage and network connectivity resources are virtualized, visible to cluster administrators only, not to NAS clients or SAN hosts.

Customers use SVMs to serve data to clients and hosts. An SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.

In addition to data SVMs, the TOE deploys special SVMs for administration:

- An admin SVM is created when the cluster is set up.
- A node SVM is created when a node joins a new or existing cluster.
- A system SVM is automatically created for cluster-level communications in an IP space.

The administrative SVMs listed above cannot be used to serve data.

In addition to data volumes, ONTAP also uses the following special volumes (note: these volumes, as with all volumes on the TOE, are hosted on third party SEDs):

- A node root volume (typically “vol0”) contains node configuration information and logs
- An SVM root volume serves as the entry point to the namespace provided by the SVM and contains namespace directory information
- System volumes contain special metadata such as service audit logs.

The TOE prevents customers from storing user data on these special volumes.

NetApp Volume Encryption may be configured via the appliance’s RS-232 console port. NetApp Volume Encryption also supports various networking protocols including SSH, CIFS, NFS, HTTP, HTTPs, DHCP, SNMP, Fibre Channel, and iSCSI, among others. The cPPs associated with this product do not include networking protocols as part of the security functional requirements and, as a result, do not include any requirements for addressing those protocols. Consequently, the protocols have not been examined as part of the required assurance activities and, therefore, no claims are made about the TOE’s networking protocols.

The only evaluated interface is the RS-232 interface. As noted in the Excluded Functionality Section 9.2, networking protocols such as SSH or HTTPS, while supported by the product , were not covered by the evaluation. This is because the Protection Profile ([CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]) do not include networking protocols as part of the security functional requirements. The customer should

consider the impact of using the product's SSH or HTTPS interfaces for administration, with the understanding that the protection of user data in transit was not evaluated and the Security Target assumes that the environment is appropriately protected.

3.3 Physical Boundaries

The TOE is the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 which provides a software-based encryption technology for third party disk drives and which is provided in the NetApp appliances described in the ST in Section 2.3.1 Physical Boundaries; they include the following models: FAS2620, FAS2650, FAS2720, FAS2750, FAS8200, AFF A200, AFF A220, AFF A300, AFF C190, FAS9000, AFF A700, AFF A700s, AFF A800, AFF A320, FAS8300, FAS8700, and AFF A400.

4 Security Policy

The TOE enforces the following security policies as described in the ST.

4.1 Cryptographic Support

The TOE includes NIST CAVP-validated cryptographic algorithms supporting cryptographic functions. The TOE provides key wrapping, key derivation, BEV validation, and data encryption.

4.2 User Data Protection

The TOE performs Full Drive Encryption such that the drive contains no plaintext user data. The TOE performs user data encryption by default in the out-of-the-box configuration using XTS-AES-256 mode.

4.3 Security Management

The TOE supports management functions for changing and erasing the DEK and initiating the TOE firmware updates using a command line interface.

4.4 Protection of the TSF

The TOE provides trusted firmware updates, protects keys and key material, and supports Compliant power saving states. The TOE runs a suite of self-tests during initial start-up (on power on).

5 Assumptions

The ST references the PPs to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, are as follows:

- Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible – for example, data contained in "bad" sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.
- Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.
- Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
- Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.
- Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.
- The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
- External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
- The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a "hibernation mode".
- Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
- The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the operating system's login interface, but it will not change or degrade the functionality of the actual interface.

- All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPPs. This includes generation of external token authorization factors by a RBG.
- The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform's correct operation.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition*, Version 2.0+Errata 20190201, 1 February 2019 [7] and *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Encryption Engine*, Version 2.0+Errata 20190201, 1 February 2019 [8], and performed by the evaluation team). The functionality evaluated is scoped exclusively to the security functional requirements specified in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata, February 1, 2019, the collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata, February 1, 2019 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, the functionality listed in Section 9.2 is excluded from the scope of the evaluation.
- This evaluation covers only the specific software distributions and versions identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target, Version 1.0, 14 June 2021 [9].
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured, and managed as described in the documentation referenced in Section 7 of this Validation Report.
- As noted in the TOE Architecture Section 3.2, the only evaluated interface is the RS-232 interface. The Excluded Functionality Section 9.2 states that networking protocols, such as SSH or HTTPS, while supported by the product, were not covered by the evaluation. This is because the Protection Profiles ([CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]) do not include networking protocols as part of the security functional requirements.
- The customer should consider the impact of using eh product's SSH or HTTPS interfaces for administration, with the understanding that the protection of user data in transit was not evaluated and the Security Target assumes that the environment is appropriately protected.

7 Documentation

NetApp offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The following documents, part of the ONTAP 9.7P13 documentation set, are included in the TOE documentation and were examined during the evaluation:

- Commands: Manual Page Reference, November 2019
- NetApp Encryption Power Guide, June 2021
- System Administration Reference, April 2020
- Upgrade Express Guide, January 2020
- Upgrade and Revert/Downgrade Guide, April 2020.

To use the product in the evaluated configuration, the product must be configured as specified in these guides.

These documents are available via the following URLs:

- http://docs.netapp.com/ontap-9/index.jsp
- https://docs.netapp.com/us-en/ontap/
- https://www.netapp.com/us/documentation/ontap-and-oncommand-system-manager.aspx

Additional customer documentation available via these URLs was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

8 IT Product Testing

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary document:

- *NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Common Criteria Test Report and Procedures*, Version 1.0, 31 August 2021 [17]

A non-proprietary description of the tests performed and their results is provided in the following document:

- *Assurance Activities Report for NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13*, Version 1.0, 31 August 2021 [16]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition* ([5]) and *collaborative Protection Profile for Full Drive Encryption – Encryption Engine* ([6]).

The evaluation team devised a Test Plan based on the Test Activities specified in *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition* and *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Encryption Engine*. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland, from 17 September through 22 December 2020.

The evaluators received the TOE in the form that customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition* and *collaborative Protection Profile for Full Drive Encryption – Encryption Engine* were fulfilled.

8.3 Test Configuration

The evaluation team established a test configuration comprising:

- TOE components:
    - ONTAP 9.7P6 installed on following NetApp Storage Encryption appliances:
        - FAS 2650
        - FAS 8300

        - FAS 9000
        - AFF A800

- Test environment components:
    - Kali Linux Server (Release 2019.3), used as a storage client (i.e., client to access the storage arrays and disk volumes managed on the NetApp appliances under test)
    - Microsoft Windows 10 Enterprise workstation, supporting the following testing tools:
        - WinHex 19.9
        - HxD 2.4.0.0.

Subsequent to the conclusion of functional testing, NetApp issued the following patches: 9.7P7; 9.7P8; 9.7P9; 9.7P10; 9.7P11; 9.7P12; and 9.7P13. Of these patches, 9.7P8, 9.7P9, and 9.7P13 address published vulnerabilities (CVE-2021-26988, CVE-2021-26989, and CVE-2021-26994 respectively). The evaluation team reviewed the list of changes for each patch release and did not identify any changes as relevant to the claimed security functional requirements. As such, the evaluated version of the TOE (9.7P13) can be considered equivalent to the version on which evaluation testing was performed (9.7P6).

9 TOE Evaluated Configuration

9.1 Evaluated Configuration

The TOE is NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13. The NVE appliances included in the evaluated configuration are as follows:

Storage Array	Disk Type	Controller Form Factor	Processor
FAS2620	HDD/SSD	2U/12 internal drives	Intel Xeon D-1528 (Broadwell)
FAS2650	HDD/SSD	2U/24 internal drives	Intel Xeon D-1528 (Broadwell)
FAS2720	HDD/SSD	2U/12 internal drives	Intel Xeon D-1557 (Broadwell)
FAS2750	HDD/SSD	2U/24 internal drives	Intel Xeon D-1557 (Broadwell)
FAS8200 Hybrid Flash	HDD/SSD	3U	Intel Xeon D-1587 (Broadwell)
AFF A200	SSD	2U	Intel Xeon D-1528 (Broadwell)
AFF A220	NVMe Flash	2U/24 internal drives	Intel Xeon D-1557 (Broadwell)
AFF A300	SSD	3U	Intel Xeon D-1587 (Broadwell)
AFF C190	SSD	2U/24 internal drives	Intel Xeon D-1557 (Broadwell)
AFF A800	NVMe Flash	4U/48 internal drives	Intel Xeon Platinum 8160 (Skylake-SP)
AFF A320	SSD	2U	Intel Xeon Silver 4114 (Skylake-SP)
FAS9000	HDD	8U	Intel Xeon E5-2697v4 (Broadwell)
AFF A700	SSD	8U	Intel Xeon E5-2697v4 (Broadwell)
AFF A700s	SSD	4U/24 internal drives	Intel Xeon E5-2697v4 (Broadwell)
FAS8300	HDD	4U	Intel Xeon Silver 4210 (Cascade Lake)
FAS8700	HDD	4U	Intel Xeon Gold 5218 (Cascade Lake)
AFF A400	SSD	4U	Intel Xeon Silver 4210 (Cascade Lake)

9.2 Excluded Functionality

Excluded functionality was not specifically identified in the ST as a separate section. However, the information here was collected from the ST and is considered accurate.

The cloud-based storage is considered out of scope for the evaluation and has not been tested or evaluated.

Protected data does not include the Master Boot Record or Pre-authentication area of the drive – areas of the drive that are necessarily unencrypted.

The TOE supports these various networking protocols, including SSH, CIFS, NFS, HTTP, HTTPs, DHCP, SNMP, Fibre Channel, and iSCSI, among others. However, the Protection Profile ([CPP_FDE_AA_V2.0E])

associated with this product did not consider, nor did it include, networking protocols as part of the security functional requirements and, as a result, did not include any requirements for addressing those protocols. Consequently, the protocols have not been examined as part of the required assurance activities and, therefore, no claims are made about the TOE's networking protocols.

NetApp appliances typically are configured in cluster nodes in high-availability (HA) pairs for fault tolerance and non-disruptive operation. The HA functionality was not covered in the scope of the evaluation or testing.

10 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary Evaluation Technical Report for NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Part 2 ([15]). The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 5 ([1], [2], [3]) and CEM version 3.1, revision 5 ([4]), and the specific evaluation activities specified in *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition*, Version 2.0+Errata 20190201, 1 February 2019 ([7]) and *Supporting Document – Mandatory Technical Document – Full Drive Encryption: Encryption Engine*, Version 2.0+Errata 20190201, 1 February 2019 ([8]). The evaluation determined the TOE satisfies the conformance claims made in the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target, of Part 2 Extended and Part 3 Conformant. The TOE satisfies the requirements specified in *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0+Errata, 1 February 2019 ([5]) and *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0+Errata, 1 February 2019 ([6]).

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

10.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed Protection Profile, and security function descriptions that satisfy the requirements.

10.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance assurance activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed Protection Profiles. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE

identification in the evaluation evidence, and that the ST describes how timely security updates are made to the TOE.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each test activity and applied each ATE_FUN.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

10.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PP. The vulnerability analysis comprised a public domain search for potential vulnerabilities.

Searches of public vulnerability repositories were performed on 31 August 2021.

The evaluation team searched the following public vulnerability repositories.

- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
- National Vulnerability Database: http://nvd.nist.gov/vuln/search
- US-CERT Vulnerability Notes Database: https://www.kb.cert.org/vuls/.

The evaluation team used the following search terms in the searches of these repositories:

- Product name—the evaluation team searched on the following terms:
  - “netapp”/ “netapp ontap”
  - “netapp fas”
  - “netapp aff”
  - “network volume encryption”
- Underlying components—the evaluation team searched on the following terms:
  - “ontap 9.7p13”
  - “openssl 1.0.2s”
  - “intel isa-l crypto library 2.22”
  - “intel storage acceleration library”
  - “x440_phm2800mcto”
  - “x440_tpm3v800amd”
  - “x4010s172b1t9nte”
  - “x417_hcbfe900a10”
  - “x417_sltng900a10”
- Search terms specified in [SD]—the evaluation team searched on the following terms:
  - “drive encryption”
  - “disk encryption”
  - “key destruction”
  - “key sanitization”
  - “key caching”.

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

10.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed Protection Profiles. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

The validators recommend that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target, and the only evaluated functionality was that which was described by the SFRs claimed in the Security Target. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Of note, while the TOE supports various networking protocols, including SSH, CIFS, NFS, HTTP, HTTPs, DHCP, SNMP, Fibre Channel, and iSCSI, among others, as noted in Section 6, Clarification of Scope, these protocols have not been examined as part of the required assurance activities and, therefore, no claims are made about the TOE's networking protocols. The only evaluated interface is the RS-232 interface. The customer should consider the impact of using the product's SSH or HTTPS interfaces for administration, with the understanding that the protection of user data in transit was not evaluated and the Security Target assumes that the environment is appropriately protected.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

12 Security Target

The ST for this product's evaluation is *NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target*, Version 1.0, 14 June 2021 [9].

13 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
AFF	All Flash FAS
AK	Authentication Key
BEV	Border Encryption Value
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
CIFS	Common Internet File System
DEK	Data Encryption Key
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
FAS	Fabric Attached Storage
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
HA	High Availability
HDD	Hard disk drive
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IT	Information Technology
NAS	Network Attached Storage
NFS	Network File System
NIST	National Institute of Standards and Technology
NVE	Network Volume Encryption
NVMe	Non-Volatile Memory express
OKM	Onboard Key Manager
PCL	Product Compliant List
SAN	Storage Area Network
SAR	Security Assurance Requirement
SED	Self-Encrypting Drive
SFR	Security Functional Requirement
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSD	Solid state drive
ST	Security Target
SVM	Storage Virtual Machine
TCG	Trusted Computing Group
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

14 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017

[2] Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 5, April 2017

[3] Criteria for Information Technology Security Evaluation: Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017

[4] Common Evaluation Methodology for Information Technology Security, Version 3.1, Revision 5, April 2017.

[5] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0+Errata, 1 February 2019.

[6] collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0+Errata, 1 February 2019.

[7] Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition, Version 2.0+Errata 20190201, 1 February 2019

[8] Supporting Document – Mandatory Technical Document – Full Drive Encryption: Encryption Engine, Version 2.0+Errata 20190201, 1 February 2019

[9] NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target, Version 1.0, 14 June 2021

[10] ONTAP® 9.7 Commands: Manual Page Reference, November 2019

[11] ONTAP® 9.7 NetApp Encryption Power Guide, June 2021

[12] ONTAP® 9.7 System Administration Reference, April 2020

[13] ONTAP® 9.7 Upgrade Express Guide, January 2020

[14] ONTAP® 9.7 Upgrade and Revert/Downgrade Guide, April 2020

[15] Evaluation Technical Report for NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13, Part 1 (Non-Proprietary), Version 1.0, 31 August 2021 (ETR P1)

[16] Evaluation Technical Report for NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13, Part 2 (Proprietary), Version 1.0, 31 August 2021 (ETR P2)

[17] Assurance Activities Report for NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13, Version 1.0, 31 August 2021 (AAR)

[18] NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Common Criteria Test Report and Procedures, Version 1.0, 31 August 2021 (DTR)

[19] NetApp Volume Encryption (NVE) running ONTAP 9.7P13 Vulnerability Assessment Version 1.0, 31 August 2021 (AVA)