CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

NetApp Volume Encryption (NVE) Running ONTAP 9.10.1P7

Maintenance Report Number: CCEVS_VR_VID11175_2022

Date of Activity: 30 September 2022

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." March 20, 2013

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 2.1 June 2012

NetApp Volume Encryption (NVE) Appliances Running ONTAP 9.10.1P7 Security Target Version 1.2 1 September 2022

NetApp Volume Encryption (NVE) Appliances Running ONTAP 9.10.1P7 Impact Analysis Report Version 1.3 September 27, 2022

Affected Evidence:

NetApp Volume Encryption (NVE) Running ONTAP 9.10.1P7 Security Target Version 1.2 1 September 2022

Affected Developer Evidence:

This section identifies all of the CC evidence previously subject to evaluation along with a summary of how each has been affected by the product updates for the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.10.1P7.

(Note that the evidence identified in the left column identifies the original versions; and the second column identifies the changes in this maintenance).

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target, Version 1.0, 14 June 2021	**Maintained Security Target:** NetApp Volume Encryption (NVSE) Appliances running ONTAP 9.10.1P7 Security Target, Version 1.2, 1 September 2022 Changes in the maintained ST are: 1. Section 1.1 - Updated identification of ST 2. Section 1.1 - Updated TOE software version 3. Section 1.3.1 – Terminology 4. Section 2 – product version number and additional platform appliances 5. Section 2.3.1 – added the additional platform appliances 6. Section 2.4 - excluded functionality 7. Section 3 - documentation
Common Criteria Guidance Documentation: 1. Commands: Manual Page Reference, November 2019 [CMPR] 2. NetApp Encryption Power Guide, May 2021 [NEPG] 3. System Administration Reference, April 2020 [SAR] 4. Upgrade Express Guide, January 2020 [UEG] 5. Upgrade and Revert/Downgrade Guide, April 2020 [URDG]	**Common Criteria Maintained Guidance Documentation:** 1. “ONTAP 9.10.1 Commands”, July 20, 2022 2. “Security and Data Encryption”, August 25, 2022 3. “Volume Administration -ONTAP 9”, August 25, 2022 4. “Cluster Administration -ONTAP 9”, August 25, 2022 5. “Set Up, Upgrade and Revert ONTAP -ONTAP 9”, August 25, 2022

Maintained Version

[SDE] “Security and data encryption”, August 25, 2022

[CLI] “ONTAP 9.10.1 commands”, August 25, 2022

[CLU] “Cluster administration”, August 25, 2022

[SUR] “Set up, upgrade and revert ONTAP”, August 25, 2022

[VA] “Volume administration - ONTAP 9”, August 25, 2022

[ONTAP 9 doc] == https://docs.netapp.com/us-en/ontap

Description of ASE Changes:

The Impact Analysis Report (IAR) identifies many new features. It indicates that these new features do not impact the security functionality of the TOE nor do they impact its NVE portion. The features that are excluded from the evaluation are identified in the ST. The IAR also identifies when the ST has been updated to include the new appliances.

The SAN enhancements do not affect the claimed security functionality identified in the security target. The secure configuration guidance was not affected by the addition of the new arrays as the new models/appliances do not have any impact the guidance documentation. However, the documentation has been repackaged. These documents will be the replacement for the AGD regression testing.

The AGD assurance activities for most of the SFRs covered in the evaluation were not impacted. For those that were impacted, the documents referenced in the AAR were not affected by the additional arrays. This includes the NetApp Encryption Power Guide [NEPG] (same version as in the initial evaluation), the Commands Manual [CMPR], the System Administration Reference [SAR], and the Upgrade/Downgrade Guides [UEG] and [URDG]. For the SFRs that have guidance assurance activities, the references to the new documents are shown below. The IAR includes the details for each.

Administrators: when you see this in the AGD AAR, look here instead

1. **FCS_AFA_EXT.1**
   Administrators: when you see *this* (Section "Configuring NetApp hardware-based encryption > Configuring onboard key management > Enabling onboard key management in ONTAP 9.6 and later" of [NEPG]) in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [SDE] instead.
2. **FCS_AFA_EXT.2**
   Administrators: when you see *this* (Section "Configuring NetApp hardware-based encryption > Configuring onboard key management > Enabling onboard key management in ONTAP 9.6 and later" of [NEPG]) in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [SDE] instead.
3. **FCS_CKM.4(d)**
   Administrators: when you see *this* ("Managing NetApp encryption > Deleting an encrypted volume" of [NEPG])in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [VA] instead.
4. **FCS_CKM_EXT.4(b)**
   Administrators: when you see *this* ([CMPR] and [SAR]) in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [CLI] instead.
5. **FCS_VAL_EXT.1**
   Administrators: when you see *this* (Section "Configuring NetApp hardware-based encryption > Configuring onboard key management > Enabling onboard key management in ONTAP 9.6 and later" of [NEPG]) in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [SDE] instead.
6. **FDP_DSK_EXT.1**
   Administrators: when you see *this* ("Configuring NetApp Volume Encryption", subsection "Configuring NVE", topic "Enabling onboard key management in ONTAP 9.6 and later (NVE)" of [NEPG]" in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [SDE] instead.
7. **FMT_SMF.1:**
   Administrators: when you see *this* ("storage/security/cluster commands" in [CMPR]) in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [CLI] instead.
8. **FPT_PWR_EXT.1**
   Administrators: when you see *this* ([CMPR] and [SAR]) in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [CLI] instead.
9. **FPT_PWR_EXT.2**

Administrators: when you see *this* ([CMPR] and [SAR]) in the AGD AAR, look at the [ONTAP 9 doc] and in the hardcopy [CLI] instead.

10. **FPT_TUD_EXT.1**
    Administrators: when you see *this* (Configuring NetApp hardware-based encryption > Configuring onboard key management > Enabling onboard key management in ONTAP 9.6 and later" of [NEPG]) in the AGD AAR, look in the hardcopy [SDE] and [SUR] instead.

The following is a summary of the changes of this Assurance Maintenance with respect to the amount of actual product changes:

- Percent of the Product code overall that was changed since the original evaluation: ~10% (includes changes to third-party libraries, new features, etc.). There were no identified bug fixes in the IAR.
- Percent of the Product code that specifically enforces the TOE security Functions that was changed since the original evaluation: < 0.1%
- Percent of the changes that impact code that isn't even included in the evaluated configuration: ~90% (includes new features, support for new platforms, etc.)

Rationale

- The System Manager enhancements are for a GUI, the TOE is managed by the CLI. Both the NVE and the NSE/NVE security targets exclude this functionality. Therefore, it does not impact the security functionality of the TOE.
- The NetApp REST API was not included in the original NetApp ONTAP 9.7P13 and is not included in the maintained ONTAP 9.10.1P7 evaluation. it does not impact the security functionality of the TOE.
- The All-SAN Array (ASA) addition to the IAR. The new ASA models consist of the same hardware, disk type, and processors as the models in the previous evaluation. Hardware for ASA platform XYZ is identical to AFF platform XYZ. The only difference is that the ASA platform will have a bootarg set at manufacturing which changes some ONTAP software behavior (examples: protocols allowed, SAN multi-pathing, max LUN size, etc.). None of these changes are NVE or NVE specific or impact the security functionality identified in the ST.
- The MetroCluster was not included in the evaluation and was not tested in the evaluated configuration. The maintained security targets for both the NVE and NSE/NVE have been updated to exclude this functionality.
- The VMware Virtualization was not included in the evaluation and was not tested in the evaluated configuration. The maintained security targets for both the NVE and NSE/NVE have

The evaluated version of the product was NetApp Volume Encryption (NVE) Running ONTAP 9.7P13. This assurance maintenance version is a few versions beyond that. There were 3 sets of changes described in detail in the IAR and one feature is no longer supported. New features were introduced in NetApp ONTAP 9.8, NetApp ONTAP 9.9.1, and NetApp ONTAP 9.10.1**.** The list below identifies the features by release. The IAR includes a description and rationale for each. All changes were considered minor.

Features Introduced in NetApp ONTAP 9.10.1

1. Data protection enhancements
    a. Set SnapLock retention up to 100 years -Minor

    b. Ability to create SnapLock and non-SnapLock volumes on the same aggregate – Minor
    c. Consistency groups
    d. Public cloud data archiving of backups
    e. Public cloud data archiving of backups
2. File access protocol enhancements
    a. AES support for secure Netlogon channel communication
    b. Kerberos for SMB domain-tunnel authentication
    c. Channel binding for increased LDAP communication security
    d. NFS over RDMA (NVIDIA only)
3. Hardware support updates
    a. New platform support for FAS and AFF systems
4. Manageability enhancements
    a. Simplified licensing with NetApp License Files (NLFs)
    b. Use System Manager to update firmware automatically
    c. Use System Manager to review risk mitigation recommendations and acknowledge the risks reported by Active IQ
    d. Use System Manager to configure how EMS event notifications are sent to administrator
    e. Use System Manager to manage certificates
    f. Use System Manager to view historical use of capacity and to predict future capacity needs
    g. Use System Manager to back up data to StorageGRID using the Cloud Backup Service
    h. Usability enhancements

Features Introduced in NetApp ONTAP 9.9.1

1. System Manager enhancements
2. SAN enhancements
3. Single LUN performance
4. Data protection enhancements
5. MetroCluster over IP
6. FlexGroup volume data protection
7. SnapLock enhancements
8. Logical space accounting/enforcement – FlexGroup volumes
9. ONTAP S3 user-defined metadata tags
10. NFSv4.2 security labels

Features Introduced in NetApp ONTAP 9.8

1. System Manager – enhancements
2. REST API Enhancements
3. NAS Protocol Enhancements
4. SAN Enhancements
5. S3 Enhancements
6. Storage Efficiencies
7. Data Protection
8. SnapMirror Cloud
9. SnapMirror Business Continuity (SM-BC)

10. MetroCluster
11. VMware Virtualization

Features No Longer Supported

1. OnCommand System Manager (classic UI)

Description of ALC Changes:

Changes to the Security Target revision were made, going from version 1.0 (14 June 2021) to 1.2 (1 September 2022) with the update of the TOE software version, the product version number, additional platform appliances, and the identification of the excluded functionality. The guidance documentation was also updated as noted in the of the table above. No other documentation was affected.

Changes to the Developer Evidence:

- **TSF Interfaces:** No changes to TSF Interfaces – There is no difference in the mapping of the SFRs to interfaces and no additional testing is required. Tests from the previous evaluation will be covered in the regression testing.
- **TSF Platform (TOE Hardware):** New components added – The NetApp ONTAP 9.10.1P7 NVE is a software TOE with the new hardware affecting the TOE operation. The NetApp ONTAP 9.10.1P7 NVE includes the NetApp ONTAP 9.10.1P7 software and the appliances. The addition of the new appliances does not have any impact on the TOE. The new appliances vary in storage capacity which does not any impact on the operation of the TOE.
- **SFRs:** There have no changes to the SFRs identified in the ST.
- **New Security Functions:** No new security features have been added.
- **Assumptions and Objectives:** No changes to assumptions and objectives.
- **Assurance Documents:**
    - AGD Changes – Changes to the guidance documents have been identified in the IAR. The guidance documents were mapped by SFR. Reference to the evaluated version was identified and mapped the new maintained documents.
    - AVA changes – Vulnerability searches were conducted to ensure the TOE is free of vulnerabilities.
    - ASE Changes – The ST was updated to reflect the new version of the TOE, excluded functionality not included in the evaluation, and a reference to new CAVP certificates.
- **Bug Fixes** – No bug fixes were identified.
- **TOE Environment** – Changes to the TOE Environment consisted of the addition of new NetApp appliances. The new appliances are identified in the IAR and the ST. The addition of the new appliances does not violate any of the assumptions identified in the ST.

Assurance Continuity Maintenance Report:

- Leidos submitted "NetApp Volume Encryption (NVE) Appliances Running ONTAP 9.10.1P7 Impact Analysis Report Version 1.3 September 27, 2022" an Impact Analysis Report (IAR) on behalf of NetApp, Inc.
- The Impact Analysis Report (IAR) documents all changes made to the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.10.1P7 since the previous Common Criteria evaluation (CCEVS-VR-VID11175-2021).
- The IAR indicates that the impact of all the individual changes is minor, so it concludes that the sum of all the changes to the TOE have only minor impact.
- Changes to the Security Target are detailed in the table above.
- The IAR adds 7 new storage arrays which are specified in the updated ST. These are AFF A250, ASA AFF A220, ASA AFF A250, ASA AFF A400, ASA AFF A700, ASA AFF A800, and FAS500f. AFF A220 was removed.

Assurance Maintenance TOE Identification – The Target of Evaluation (TOE) is the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.10.1P7, comprising the following specific storage array devices:

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

Storage Array	Disk Type	Controller Form Factor	Processor (Microarchitecture)
			(Skylake-SP)
AFF C190	SSD	2U/24 internal drives	Intel Xeon D-1557 (Broadwell)
AFF A250	NVMe Flash	2U	Intel Xeon D-2164IT (Skylake-D)
ASA AFF A220	NVMe Flash	2U/24 internal drives	Intel Xeon D-1557 (Broadwell)
ASA AFF A250	NVMe Flash	2U	Intel Xeon D-2164IT (Skylake-D)
ASA AFF A400	SSD	4U	Intel Xeon Silver 4210 (Cascade Lake)
ASA AFF A700	SSD	8U	Intel Xeon E5-2697 v4 (Broadwell)
ASA AFF A800	NVMe Flash	4U with 48 SSD slots	Intel Xeon Platinum 8160 (Skylake-SP)
FAS500f	NVMe Flash	2U	Intel Xeon D-2164IT (Skylake-D)

All TOE cryptographic services are provided by the following cryptographic modules: NetApp CryptoMod with AES-NI version 2.2; NetApp Cryptographic Security Module (NCSM) version 1.0.

The product updates affect the CAVP certificates. The NetApp CryptoMod version 2.2 (CAVP C1884/1885) remained unchanged since the previous NetApp Volume Encryption (NVE) running ONTAP 9.7P13 evaluation. The cryptographic primitives have not been affected by the product updates and the CAVP certificates remain valid for the 9.10.1P7 evaluation.

NetApp Cryptographic Security Module (NCSM): NCSMv1 was changed to NCSMv2 in order to be compliant to updated IGs (CAVP A2157).

The cryptographic primitives have not been affected by the product updates and the CAVP certificates remain valid for the 9.10.1P7 evaluation.

Due to vulnerabilities in OpenSSL, the “OpenSSL 1.0.2s-fips” was updated to “OpenSSL 1.0.2zd-fips”. The changes are not with NCSMv2 (i.e., the FIPS module). The changes are only with the non-FIPS code associated with OpenSSL.

Description of Regression Testing:

Vendor regression test results were produced and found consistent with the previous test results. NetApp performs extensive regression testing for every release including NetApp Volume Encryption (NVE) Appliances running ONTAP 9.10.1P7. NetApp conducts automation test suites and also performed manual testing.

NetApp uses a continuous integration testing (CIT) model. A system build (which must be done before code can be checked in will run over 900 unit test executables, with each unit test executable performing anywhere from 1—30 individual tests.

After checking in code, an ML assisted script will select up to 10 CIT scripts that are run before code can be submitted into the branch. The CIT scripts run the code either on hardware or on a hardware

simulator. Each individual CIT can take up to an hour to execute all of the tests within the CIT script (there may be 100s).

In addition, all code that is checked into the branch then undergoes another set of tier 1, tier 2, and tier 3 automated testing by yet another set of CIT suites.

After that, software is then tested both manually by QA teams and via another set of automated scripts.

Before being released, the software, as a whole, is then subjected to ~3 months of regression testing by a dedicated team.

Overall, testing occupies ~4 months of the 6 month release cycle.

Vulnerability Assessment:

A public search for new vulnerabilities that might affect the TOE since the evaluation was completed was performed. In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the firmware minor version update.

The vulnerability searches were performed on the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 that are posted on the NIAP Product Compliant List web page. (CCEVS-VR-VID11175-2021 - NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13. Certificate Date: 2021.09.07.)

The original search terms for the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 are listed below. All new searches for the assurance maintenance are shown below were performed on **9/27/2022** and go back to the date of the previous maintained evaluation date of 8/31/2021.

NetApp -- Search Terms:

1. netapp

These search criteria were applied as follows:

2. Product name—the evaluation team searched on the following terms:
    1. “netapp”/ “netapp ontap”
    2. “netapp fas”
    3. “netapp aff”
    4. “network storage encryption”
3. Underlying components—the evaluation team searched on the following terms:
    1. “ontap 9.10.1”
    2. “openssl 1.0.2s”
    3. “intel isa-l crypto library 2.22”
    4. “intel storage acceleration library”
    5. “x440_phm2800mcto”
    6. “x440_tpm3v800amd”
    7. “x4010s172b1t9nte”
    8. “x417_hcbfe900a10”
    9. “x417_sltng900a10”
4. Search terms specified in [SD-AA] the evaluation team searched on the following terms:
    1. “drive encryption”
    2. “disk encryption”

3. “key destruction”
4. “key sanitization”
5. “opal management software”/ ”opal”
6. “sed management software”/ “self encrypting drive”
7. “password caching”.

NetApp’s Response to Customers Regarding the Log4j Vulnerability Threat

https://www.netapp.com/newsroom/netapp-apache-log4j-response/

Note: the vulnerabilities listed below are only for the NetApp ONTAP TOE. The NetApp ONTAP TOE is identified as “Clustered Data ONTAP” on the vendor vulnerability URL links below.

NetApp’s Response to Customers Regarding the Log4j Vulnerability Threat

https://www.netapp.com/newsroom/netapp-apache-log4j-response/

Vendor Conclusion:

The changes to the TOE can be considered MINOR. The documents have been updated and regression testing identified the correct operation of the TOE and the claimed security functionality identified in the ST.

Vendor regression test results were produced and found consistent with the previous test results. NetApp performs extensive regression testing for every release including NetApp Volume Encryption (NVE) running ONTAP 9.10.1P7. NetApp conducts automation test suites and also performed manual testing.

NetApp uses a continuous integration testing (CIT) model. A system build (which must be done before code can be checked in will run over 900 unit test executables, with each unit test executable performing anywhere from 1—30 individual tests.

After checking in code, an ML assisted script will select up to 10 CIT scripts that are run before code can be submitted into the branch. The CIT scripts run the code either on hardware or on a hardware simulator. Each individual CIT can take up to an hour to execute all of the tests within the CIT script (there may be 100s).

In addition, all code that is checked into the branch then undergoes another set of tier 1, tier 2, and tier 3 automated testing by yet another set of CIT suites.

After that, software is then tested both manually by QA teams and via another set of automated scripts.

Before being released, the software, as a whole, is then subjected to ~3 months of regression testing by a dedicated team.

Overall, testing occupies ~4 months of the 6 month release cycle.

The NetApp proprietary custom-build hardware appliances with All SAN Array build on top of AFF platform, and provides only SAN-based data protocol connectivity.

The regression testing included in-depth exercising of the security functionality claimed in the security target. Testing included exercising the cryptographic functionality (creating, storing, and deleting keys),

NSE:

- forwarding requests to change the DEK to the EE,
- forwarding requests to cryptographically erase the DEK to the EE
- initiate TOE firmware/software updates

NVE:

- change the DEK, as specified in FCS_CKM.1, when re-provisioning or when commanded,
- erase the DEK, as specified in FCS_CKM.4(a),
- initiate TOE firmware/software updates

The security functionality identified in the security target was exercised in the NetApp regression/production testing.

The product updates affect the CAVP certificates. The NetApp CryptoMod version 2.2 (CAVP C1884) remained unchanged since the previous NetApp Volume Encryption (NVE) running ONTAP 9.7P13 evaluation.

NetApp Cryptographic Security Module (NCSM): NCSMv1 was changed to NCSMv2 in order to be compliant to updated IGs (CAVP A2157).

The cryptographic primitives have not been affected by the product updates and the CAVP certificates remain valid for the 9.10.1P7 evaluation.

The IAR concludes that all changes to the TOE are minor and the overall impact to the TOE is minor. It is the conclusion of this report that assurance has been maintained in the changed TOE.

Validation Team Conclusion:

The Validation team has reviewed the changes and concurs that the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cider version of this product.