Assurance Activities Report

for

NetApp Volume Encryption (NVE) Appliances running ONTAP 9.14.1

Version 1.1

8 November 2024

Prepared by:

Leidos Inc.
https://www.leidos.com/CC-FIPS140
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

© 2024 Leidos. All rights reserved

The Developer of the TOE:

NetApp, Inc.
3060 Olsen Drive
San Jose, CA 95128

The TOE Evaluation was Sponsored by:

NetApp, Inc.
3060 Olsen Drive
San Jose, CA 95128

Evaluation Personnel:

Greg Beaver
Pascal Patin
Anthony Apted

Common Criteria Version:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.

Common Evaluation Methodology Version:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Protection Profile:

- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata 20190201, 1 February 2019
- *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0 + Errata 20190201, 1 February 2019

© 2024 Leidos. All rights reserved

Revision History

Version	Date	Description
0.1	18 April 2024	Initial draft
0.2	25 June 2024	Updated per vendor revised documents.
0.3	10 July 2024	Updated per vendor revised documents.
0.4	7 August 2024	Updated per vendor revised documents.
0.5	13 August 2024	Updated per vendor revised documents.
0.6	8 September 2024	Updated per vendor revised documents.
1.0	25 September 2024	Released version
1.1	8 November 2024	Addressed validator comments.

© 2024 Leidos. All rights reserved

Contents

© 2024 Leidos. All rights reserved

© 2024 Leidos. All rights reserved

© 2024 Leidos. All rights reserved

1 Introduction

This document presents results from performing assurance activities associated with the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.14.1 evaluation. This report contains sections documenting the performance of evaluation activities associated with each of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) as specified in the following Protection Profiles:

- collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0+Errata 20190201, 1 February 2019
- collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0+Errata 20190201, 1 February 2019.

Note that, in accordance with NIAP Policy Letter #5, all cryptography in the TOE for which NIST provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components must be NIST validated. The CCTL will verify that the claimed NIST validation complies with the NIAP-approved PP requirements the TOE claims to satisfy. The CCTL verification of the NIST validation will constitute performance of the associated assurance activity. As such, Test activities associated with functional requirements within the scope of Policy Letter #5 are performed by verification of the relevant CAVP certification and not through performance of any testing as specified in the supporting documents.

1.1 Technical Decisions

The following subsections list the Technical Decisions that have been issued by NIAP against each of the claimed Protection Profiles, along with rationale as to their applicability or otherwise to this evaluation.

1.1.1 Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition

- TD0458: FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities

  The TD is applicable to the evaluation. Modifies the evaluation activity associated with the SFR.

- TD0606: FIT Technical Recommendation for Evaluating a NAS against the FDE AA and FDE EE

  The TD is applicable to the evaluation. The TOE can be utilized as a NAS device.

- TD0759: FIT Technical Decision for FCS_AFA_EXT.1.1

  The TD is applicable to the evaluation. Although the TOE does not make use of the modified selection, the SFR itself was modified by the TD.

- TD0760: FIT Technical Decision for FCS_SNI_EXT.1.3, FCS_COP.1(f)

  The TD is applicable to the evaluation. The TD modifies an SFR and associated evaluation activity wording.

- TD0764: FIT Technical Decision for FCS_PCC_EXT.1

  The TD is applicable to the evaluation. Although the TOE does not make use of the modified selection, the SFR itself was modified by the TD.

- TD0765: FIT Technical Decision for FMT_MOF.1

  The TD is applicable to the evaluation. The TD modifies the associated evaluation activity wording.

© 2024 Leidos. All rights reserved

- TD0766: FIT Technical Decision for FCS_CKM.4(d) Test Notes

  The TD is applicable to the evaluation. The TD modifies the SFR and associated evaluation activity wording.

- TD0767: FIT Technical Decision for FMT_SMF.1.1

  The TD is applicable to the evaluation. The TD modifies the SFR and associated evaluation activity wording.

- TD0769: FIT Technical Decision for FPT_KYP_EXT.1.1

  This TD is applicable to this evaluation. Although the TOE does not make use of the modified selection, the SFR itself was modified by the TD.

1.1.2 Collaborative Protection Profile for Full Drive Encryption – Encryption Engine

- TD0458: FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities

  The TD is applicable to the evaluation. Modifies the evaluation activity associated with the SFR.

- TD0460: FIT Technical Decision for FPT_PWR_EXT.1 non-compliant power saving states

  The TD is applicable to the evaluation. The TD modifies the evaluation activity associated with the SFR.

- TD0464: FIT Technical Decision for FPT_PWR_EXT.1 compliant power saving states

  The TD is applicable to the evaluation. The TD modifies the SFR wording.

- TD0606: FIT Technical Recommendation for Evaluating a NAS against the FDE AA and FDE EE

  The TD is applicable to the evaluation. The TOE can be utilized as a NAS device.

- TD0766: FIT Technical Decision for FCS_CKM.4(d) Test Notes

  The TD is applicable to the evaluation. The TD modifies the SFR and associated evaluation activity wording.

- TD0769: FIT Technical Decision for FPT_KYP_EXT.1.1

  This TD is applicable to this evaluation. Although the TOE does not make use of the modified selection, the SFR itself was modified by the TD.

1.2 References

[CPP_FDE_AA_V2.0E]	collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0+Errata 20190201, 1 February 2019
[CPP_FDE_AA_SD_V2.0E]	Supporting Document – Mandatory Technical Document – Full Drive Encryption: Authorization Acquisition, Version 2.0+Errata 20190201, 1 February 2019
[CPP_FDE_EE_V2.0E]	*collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0+Errata 20190201, 1 February 2019
[CPP_FDE_EE_SD_V2.0E]	Supporting Document – Mandatory Technical Document – Full Drive

© 2024 Leidos. All rights reserved

	Encryption: Encryption Engine, Version 2.0+Errata 20190201, 1 February 2019
[ST]	NetApp Volume Encryption (NVE) Appliances running ONTAP 9.14.1 Security Target, Version 1.6, November 7, 2024
[KMD]	NetApp ONTAP 9.14.1with NetApp Volume Encryption and Onboard Key Manager Common Criteria Full Drive Encryption – Authorization Acquisition/Encryption Engine Key Management Description, Version 1.1, 18 January 2024
[CCCG]	NetApp Volume Encryption: Common Criteria Configuration Guide, Version 1.5, November 7, 2024
[ONTAP CR]	NetApp ONTAP 9.14.1 commands, June 26, 2024
[SUUR]	NetApp Set up, upgrade and revert ONTAP- ONTAP 9, July 02, 2024

1.3 Security Assurance Requirements (SARs)

The following Security Assurance Requirements (SARs) were evaluated during the evaluation of the TOE:

SAR	Verdict
ASE_CCL.1	Pass
ASE_ECD.1	Pass
ASE_INT.1	Pass
ASE_OBJ.1	Pass
ASE_REQ.1	Pass
ASE_SPD.1	Pass
ASE_TSS.1	Pass
ADV_FSP.1	Pass
AGD_OPE.1	Pass
AGD_PRE.1	Pass
ALC_CMC.1	Pass
ALC_CMS.1	Pass
ATE_IND.1	Pass
AVA_VAN.1	Pass

© 2024 Leidos. All rights reserved

The evaluation work units are listed in the proprietary ETR. The evaluators note per the PP evaluation activities that many of the SARs were successfully evaluated through completion of the associated evaluation activities present in the claimed PP.

2 TOE Identification

The TOE consists of a NetApp storage controller running ONTAP 9.14.1 along with any accompanying storage enclosures. The TOE provides Full Disk Encryption of HDD/SSD drives via NetApp Volume Encryption (NVE), which fulfills the [CPP_FDE_EE_V2.0E] requirements. The TOE also provides the authorization acquisition to send a Border Encryption Value (BEV) to the encryption engine which fulfills the [CPP_FDE_AA_V2.0E] requirements. The NetApp controllers included in the evaluated configuration are as follows:

NetApp Controllers Covered by the Evaluation

NetApp Controllers	Disk Type	Controller Form Factor
AFF A150	SSD	2U/24 internal drives
AFF A220	SSD	2U/24 internal drives
AFF A250	NVMe/SSD	2U/24 internal drives
AFF A300	SSD	3U
AFF A320	NVMe	2U
AFF A400	NVMe/SSD	4U
AFF A800	NVMe/SSD	4U/48 internal drives
AFF A900	NVMe/SSD	8U
AFF C190	SSD	2U/24 internal drives
AFF C250	NVMe	2U/24 internal drives
AFF C400	NVME	4U
AFF C800	NVMe	4U
ASA A150	SSD	2U/24 internal drives
ASA A250	NVMe	2U/24 internal drives
ASA A400	NVMe/SSD	4U
ASA A800	NVMe/SSD	4U/48 internal drives
ASA A900	NVMe/SSD	8U
ASA C250	NVMe	2U/24 internal drives
ASA C400	NVMe	4U
ASA C800	NVMe	4U
ASA AFF A220	SSD	2U/24 internal drives
FAS2720	HDD/SSD	2U/12 internal drives
FAS2750	HDD/SSD	2U/24 internal drives
FAS2820	HDD/SSD	2U/12 internal drives
FAS500f	NVMe	2U/24 internal drives
FAS8200	HDD/SSD	3U
FAS8300	HDD/SSD	4U
FAS8700	HDD/SSD	4U
FAS9500	HDD/SSD	8U

© 2024 Leidos. All rights reserved

© 2024 Leidos. All rights reserved

3 Security Functional Requirement Evaluation Activities

This section describes the evaluation activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The evaluation activities are drawn from [CPP_FDE_AA_SD_V2.0E] and [CPP_FDE_EE_SD_V2.0E].]. As such, this report identifies the source of each SFR and evaluation activity, using the abbreviations [AA] and [EE] as appropriate. NIAP Technical Decisions have been applied and are identified as appropriate.

3.1 Cryptographic Support (FCS)

All TOE cryptographic services are provided by the NetApp software modules CryptoMod version 2.2 and the NetApp Cryptographic Security Module (NCSM). NetApp's CryptoMod module is used to:

- Generate salts and keying material via a validate DRBG.
- Derive keys via PBKDFv2.
- Calculate cryptographic hashes.
- Encrypt/decrypt data using validated AES encryption/decryption modes.
- Calculate HMACs.
- Encrypt keys using KWP-AE.
- Decrypt keys using KWP-AD.
- Store volatile keys.
- Zeroize volatile keys.

The NetApp Cryptographic Security Module is used to validate the TOE's cryptographically signed images using approved cryptographic hash and digital signature validation algorithms. All cryptographic algorithms are NIST CAVP certified. The following tables identify the cryptographic algorithms used by the TSF, the associated standards to which they conform, and the NIST certificates that demonstrate that the claimed conformance has been met.

CryptoMod version 2.2 Algorithm Certificates

SFR	Algorithm	Standard	Certificate
Cryptographic Operation (Hash Algorithm)			
FCS_COP.1.1(b)	SHA-256, SHA-512	ISO/IEC 10118-3:2004	A4794, A4795: SHA2-256 A4794, A4795: SHA2-512
Cryptographic Operation (Keyed Hash Algorithm)			
FCS_COP.1.1(c)	HMAC-512	ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"	A4794, A4795: HMAC-SHA2-512

© 2024 Leidos. All rights reserved

SFR	Algorithm	Standard	Certificate
Cryptographic Operation (Key Wrapping)			
FCS_COP.1.1(d)	AES-KWP-256	NIST SP 800-38F	A4794, A4795: AES-KWP
Cryptographic Operation (AES Data Encryption/Decryption)			
FCS_COP.1.1(f)	AES-XTS-256	XTS as specified in [IEEE 1619].	A4794, A4795: AES-XTS
Cryptographic Operation (Random Bit Generation)			
FCS_RBG_EXT.1	AES-256 (CTR_DRBG)	NIST SP 800-90A	A4794, A4795: Counter DRBG

NetApp Cryptographic Security Module (NCSM v3.0.8) Algorithm Certificates

SFR	Algorithm	Standard	Certificate
Cryptographic Operation (Signature Verification)			
FCS_COP.1.1(a)	RSA 3072	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes	A4858: RSA SigVer (FIPS186-4)
Cryptographic Operation (Hash Algorithm)			
FCS_COP.1.1(b)	SHA-256 SHA-384 SHA-512	ISO/IEC 10118-3:2004	A4858: SHA2-256 A4858: SHA2-384 A4858: SHA2-512

© 2024 Leidos. All rights reserved

3.1.1 Authorization Factor Acquisition (FCS_AFA_EXT.1) ([AA])

3.1.1.1 TSS Activities

The evaluator shall first examine the TSS to ensure that the authorization factors specified in the ST are described. For password-based factors the examination of the TSS section is performed as part of FCS_PCC_EXT.1 Evaluation Activities. Additionally in this case, the evaluator shall verify that the operational guidance discusses the characteristics of external authorization factors (e.g., how the authorization factor must be generated; format(s) or standards that the authorization factor must meet) that are able to be used by the TOE.

Section 6.2.1.1 in [ST] ("FCS_AFA_EXT.1 Authorization Factor Acquisition (FDE_AA)") specifies in FCS_AFA_EXT.1.1 the TSF accepts a submask derived from a password authorization factor. Refer to the TSS Activities for FCS_PCC_EXT.1.

If other authorization factors are specified, then for each factor, the TSS specifies how the factors are input into the TOE.

The password-based factor is the only authorization factor accepted by the TOE.

3.1.1.2 Guidance Activities

The evaluator shall verify that the AGD guidance includes instructions for all of the authorization factors. The AGD will discuss the characteristics of external authorization factors (e.g., how the authorization factor is generated; format(s) or standards that the authorization factor must meet, configuration of the TPM device used) that are able to be used by the TOE.

[CCCG] Section 2.1 "Configuration" provides instructions for configuring the Cluster Passphrase authorization factor.

To configure ONTAP 9.14.1 for use with NetApp Volume Encryption (NVE), the Onboard Key Manager (OKM) must be enabled for the admin Vserver in Common Criteria (CC) mode. The following command will enable OKM in CC mode:

```
security key-manager onboard enable -cc-mode-enabled yes
```

When CC mode is enabled, the cluster administrator will be required to provide a cluster passphrase that is between 64 and 256 ASCII characters long. This passphrase must be entered at the console each time that a node in the cluster boots.

3.1.1.3 KMD Activities

The evaluator shall examine the Key Management Description to confirm that the initial authorization factors (submasks) directly contribute to the unwrapping of the BEV.

Section 2.1 of [KMD] ("Border Encryption Values") describes how the initial authorization factor directly contributes to unwrapping the BEV. The Cluster Passphrase (CP) entered by the user is concatenated with the Cluster Salt (CS) and this bit string is passed through the PBKDF2 function to produce the Cluster Passphrase Key Encryption Key (CP-KEK). The CP-KEK is then used to unwrap the Cluster Key Encryption Key (CKEK) and the CKEK is used to unwrap the Storage Virtual Machine Key Encryption Key (SVM-KEK), which in TOE terms is the BEV.

© 2024 Leidos. All rights reserved

The evaluator shall verify the KMD describes how a submask is produced from the authorization factor (including any associated standards to which this process might conform), and verification is performed to ensure the length of the submask meets the required size (as specified in this requirement).

Section 2.1.1 of [KMD] ("Cluster Passphrase") describes the method by which the password is encoded and fed to the SHA algorithm. The password is a 64 to 256 byte ASCII string that is concatenated with a salt generated by the TOE's DRBG and fed to the PBKDF2 function that meets NIST SP 800-132 to derive the Cluster Passphrase Key Encryption Key (CP-KEK). Section 2.1.5 of [KMD] ("Cluster Passphrase Key Encryption Key (CP-KEK)") describes the parameters of the PBKDF2 function, consistent with the selections in the ST—using the HMAC-SHA-512 algorithm with 1024 iterations and an output size of 256 bits.

3.1.1.4 Test Activities

The password authorization factor is tested in FCS_PCC_EXT.1.

The evaluator shall also perform the following tests:

Test 1 (conditional): If there is more than one authorization factor, ensure that failure to supply a required authorization factor does not result in access to the decrypted plaintext data.

This test is not applicable because the ST only claims one authorization factor.

3.1.2 Timing of Authorization Factor Acquisition (FCS_AFA_EXT.2) ([AA])

3.1.2.1 TSS Activities

The evaluator shall examine the TSS for a description of authorization factors and which of the factors are used to gain access to user data after the TOE entered a Compliant power saving state. The TSS is inspected to ensure it describes that each authorization factor satisfies the requirements of FCS_AFA_EXT.1.1.

Section 7.1.1 of [ST] ("FCS_AFA_EXT.1: Authorization Factor Acquisition (FDE_AA)") states the Cluster Passphrase serves as the password authorization factor—it is the only authorization factor specified in the ST. It is required to be entered at system boot in order for the user to gain access to user data.

Section 7.1.2 of [ST] ("FCS_AFA_EXT.2: Timing of Authorization Factor Acquisition (FDE_AA)") states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). After the TOE has entered either state, the Cluster Passphrase must be entered in order for the user to gain access to user data.

Section 7.1.17 of [ST] ("FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning (FDE_AA)") describes how the Cluster Passphrase satisfies the requirements of FCS_AFA_EXT.1.1.

3.1.2.2 Guidance Activities

The evaluator shall examine the guidance documentation for a description of authorization factors used to access plaintext data when resuming from a Compliant power saving state.

[CCCG] Section 2.4 "Compliant Power Saving States" when either Compliant power saving state is entered G3 (mechanical off) and G2(S5) (soft off), the non-persistent/unencrypted BEV and DEK key material is destroyed.

[CCCG] Section 2.1 "Configuration" provides instructions for configuring the Cluster Passphrase authorization factor.

© 2024 Leidos. All rights reserved

When CC mode is enabled, the cluster administrator will be required to provide a cluster passphrase that is between 64 and 256 ASCII characters long. This passphrase must be entered at the console each time that a node in the cluster boots.

3.1.2.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.1.2.4 Test Activities

The evaluator shall also perform the following test:

- Enter the TOE into a Compliant power saving state
- Force the TOE to resume from a Compliant power saving state
- Release an invalid authorization factor and verify that access to decrypted plaintext data is denied
- Release a valid authorization factor and verify that access to decrypted plaintext data is granted.

The evaluator rebooted the TOE and entered the incorrect cluster passphrase then attempted to mount the volume and confirmed the mount failed and no plaintext data was accessible. The evaluator then rebooted the TOE and input the correct cluster passphrase and successfully mounted the volume and access the decrypted data.

3.1.3 Cryptographic Key Generation (Symmetric Keys) (FCS_CKM.1(b)) ([AA], [EE])

3.1.3.1 TSS Activities

The evaluator shall review the TSS to determine that a symmetric key is supported by the product, that the TSS includes a description of the protection provided by the product for this key. The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE.

Section 7.1.3 of [ST] ("FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys) (FDE_AA) (FDE_EE)") states the TOE generates the following 256 bit AES symmetric keys that are used as key encryption keys along the key chain: Cluster Key Encryption Key (CKEK); the Storage Virtual Machine Key Encryption Key (SVM-KEK). The TOE protects the CKEK by using the AES-256 key CP-KEK to wrap the CKEK. The TOE protects the SVM-KEK by using the AES-256 key CKEK to wrap the SVM-KEK.

3.1.3.2 Guidance Activities

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key size(s) for all uses specified by the AGD documentation and defined in this cPP.

[CCCG] Section 2.6 "Cryptography" states that NetApp Volume Encryption (NVE) supports 256-bit volume DEKs (AES-XTS-256) and BEVs. As such, there is no configuration required to configure the TOE to use selected key sizes, and no guidance instructions are necessary.

3.1.3.3 KMD Activities

If the TOE uses a symmetric key as part of the key chain, the KMD should detail how the symmetric key is used as part of the key chain.

Section 2 of [KMD] ("Keys and Key Hierarchy") describes the Cluster Key Encryption Key (CKEK) and the Storage Virtual Machine Key Encryption Key (SVM-KEK) and how they are used as part of the key chain.

© 2024 Leidos. All rights reserved

3.1.3.4 Test Activities

There are no test evaluation activities for this SFR.

3.1.4 Cryptographic Key Generation (Data Encryption Key) (FCS_CKM.1(c)) ([EE])

3.1.4.1 TSS Activities

The evaluator shall examine the TSS to determine that it describes how the TOE obtains a DEK (either generating the DEK or receiving from the environment).

Section 7.1.4 of [ST] ("FCS_CKM.1(c): Cryptographic Key Generation (Data Encryption Key) (FDE_EE)") states the TOE generates AES-XTS-256 keys to use as its own DEK.

If the TOE generates a DEK, the evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked. If the DEK is generated outside of the TOE, the evaluator checks to ensure that for each platform identified in the TOE the TSS, it describes the interface used by the TOE to invoke this functionality. The evaluator uses the description of the interface between the RBG and the TOE to determine that it requests a key greater than or equal to the required key sizes.

Section 7.1.4 of [ST] states the TOE generates its DEK using its internal cryptomodule's implementation of the CTR_DRBG deterministic random bit generation algorithm. The TOE generates a 256 bit AES key and a 256 bit tweak key that are used together in AES-XTS mode of operation.

If the TOE received the DEK from outside the host platform, then the evaluator shall examine the TSS to determine that the DEK is sent wrapped using the appropriate encryption algorithm.

As specified in FCS_CKM.1(c) and described in Section 7.1.4 of [ST], the TOE generates its own DEK and does not receive it from outside the host platform.

3.1.4.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.4.3 KMD Activities

If the TOE received the DEK from outside the host platform, then the evaluator shall verify that the KMD describes how the TOE unwraps the DEK.

The TOE does not receive the DEK from outside the host platform.

3.1.4.4 Test Activities

The evaluator shall also perform the following tests:

Test 1: The evaluator shall configure the TOE to ensure the functionality of all selections.

The evaluator began by confirming that no keys had been generated on the TOE. The evaluator then performed actions to generate the DEK and confirmed it was successfully created.

© 2024 Leidos. All rights reserved

3.1.5 Cryptographic Key Destruction (Power Management) (FCS_CKM.4(a)) ([AA], [EE])

3.1.5.1 TSS Activity

The evaluator shall verify the TSS provides a high level description of how keys stored in volatile memory are destroyed. The valuator to verify that TSS outlines:

- if and when the TSF or the Operational Environment is used to destroy keys from volatile memory;

- if and how memory locations for (temporary) keys are tracked;

- details of the interface used for key erasure when relying on the OE for memory clearing.

Section 7.1.5 of [ST] ("FCS_CKM.4(a): Cryptographic Key Destruction (Power Management) (FDE_AA) (FDE_EE)") states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). All keys in volatile memory are destroyed when entering the G2(S5) or G3 Compliant power saving state. In both states, power is removed from memory and all values drain to a zero state.

3.1.5.2 Guidance Activities

The evaluator shall check the guidance documentation if the TOE depends on the Operational Environment for memory clearing and how that is achieved.

The TOE does not depend on the Operational Environment for memory clearing.

3.1.5.3 KMD Activities

The evaluator shall check to ensure the KMD lists each type of key, its origin, possible memory locations in volatile memory.

Section 2.5 of [KMD] ("Critical Security Parameters Summary") provides information for each of the keys and critical security parameters required by the TOE, including for each key and parameter its type, origin, and possible memory locations in volatile memory.

3.1.5.4 Test Activities

There are no test evaluation activities for this SFR.

3.1.6 Cryptographic Key Destruction (Software TOE, 3rd Party Storage) (FCS_CKM.4(d)) ([AA], [EE])

3.1.6.1 TSS + KMD Activities (KMD may be used if necessary details describe proprietary information)

The evaluator examines the TSS to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.

Section 2.5 of [KMD] ("Critical Security Parameters Summary"), Table 4 ("Critical Security Parameters") provides the following information regarding management in volatile memory for each of the keys and critical security parameters required by the TOE:

- Cluster Passphrase—is temporarily stored as a variable or a CPU register value by functions involved in the calculation of the CP-KEK. It is supplied by the cluster administrator when the

© 2024 Leidos. All rights reserved

`security key-manager onboard enable` and `security key-manager onboard update-passphrase` commands are executed.

- Cluster Salt—is temporarily stored as a variable or a CPU register value by functions involved in the calculation of the CP-KEK, or functions that need to store the Cluster Salt in non-volatile memory. It is generated by the TOE's cryptomodule.
- CP-Salt—is temporarily stored as a variable or a CPU register value by functions involved in the calculation of the CP-KEK, or functions that need to store the CP-Salt in non-volatile memory. It is generated by the TOE's cryptomodule.
- CP-Hash—is temporarily stored as a variable or a CPU register value by functions that need to validate the cluster passphrase, or functions that need to store the CP-Hash in non-volatile memory. It is calculated by the TOE's cryptomodule as the SHA-256 hash of the CP-Salt concatenated with the Cluster Passphrase.
- Cluster Passphrase Key Encryption Key (CP-KEK)—is temporarily stored as a variable or a CPU register value by functions that need to wrap or unwrap the CKEK. It is additionally stored in the key table of the TOE's cryptomodule. It is derived from the Cluster Passphrase and Cluster Salt using PBKDFv2.
- Cluster Key Encryption Key (CKEK)—is temporarily stored as a variable or a CPU register value by functions that need to wrap or unwrap SVM-KEKs. It is additionally stored in the key table of the TOE's cryptomodule. It is generated by the TOE's cryptomodule.
- Wrapped CKEK (wCKEK)—is temporarily stored as a variable or a CPU register value by functions that need to wrap the CKEK, unwrap the wCKEK, or store the wCKEK in non-volatile memory. It is created by cryptographically wrapping the CKEK using the KWP algorithm with the CP-KEK as the wrapping key.
- Storage Virtual Machine Key Encryption Key (SVM-KEK)—is temporarily stored as a variable or a CPU register value by functions that need to wrap or unwrap VDEKs. It is additionally stored in the key table of the TOE's cryptomodule. It is generated by the TOE's cryptomodule.
- Wrapped Storage Virtual Machine Key Encryption Key (wSVM-KEK)—is temporarily stored as a variable or a CPU register value by functions that need to wrap the SVM-KEK, unwrap the wSVM-KEK, or store the wSVM-KEK in non-volatile memory. It is created by cryptographically wrapping the SVM-KEK using the KWP algorithm with the CKEK as the wrapping key.
- Volume Data Encryption Key (VDEK)—is temporarily stored as a variable or a CPU register value by functions that need to encrypt and decrypt user data stored on a disk volume. It is additionally stored in the key table of the TOE's cryptomodule. It is generated by the TOE's cryptomodule.
- Wrapped Volume Data Encryption Key (VDEK)—is temporarily stored as a variable or a CPU register value by functions that need to wrap the VDEK, unwrap the wVDEK, or store the wVDEK in non-volatile memory. It is created by cryptographically wrapping the VDEK using the KWP algorithm with the SVM-KEK as the wrapping key.

Section 4.5 of [KMD] ("Key Lifetime and Key Destruction") states keys stored in volatile memory are destroyed in the following manner:

- Memory location overwritten with DRBG generated random data
- Memory location overwritten with zeroes
- Memory location read and compared with zero.

© 2024 Leidos. All rights reserved

All keys and CSPs in volatile memory are also destroyed by removal of power to memory when the TOE enters the G2(S5) or G3 Compliant power saving state.

The evaluator shall check to ensure the TSS lists each type of key that is stored in in non-volatile memory, and identifies how the TOE interacts with the underlying platform to manage keys (e.g., store, retrieve, destroy). The description includes details on the method of how the TOE interacts with the platform, including an identification and description of the interfaces it uses to manage keys (e.g., file system APIs, platform key store APIs).

The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) and description in the TSS.

Section 2 of [KMD] ("Keys and Key Hierarchy") states the ONTAP Onboard Key Manager component of the TOE uses the OKM database (file location: `/cfcard/kmip/km_onboard.wkeydb`) and ONTAP's replicated database (RDB) (directory location: `/mroot/etc/cluster_config/rdb/Management`) when storing data in non-volatile memory.

Section 2.5 of [KMD], Table 4 identifies the following keys and key material that are stored in non-volatile memory:

- Cluster Salt—stored in an RDB table and the OKM database
- CP-Salt—stored in an RDB table and the OKM database
- CP-Hash—stored in an RDB table
- Wrapped CKEK (wCKEK)—stored in an RDB table and the OKM database
- Wrapped Storage Virtual Machine Key Encryption Key (wSVM-KEK)—stored in an RDB table and Configuration Database (CDB) table
- Wrapped Volume Data Encryption Key (VDEK)—stored with Write Anywhere File Layout (WAFL) on-disk data structures.

Section 7.1.6 of [ST] ("FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage) (FDE_AA)") states the TOE uses `SecureFileDeleter::remove()` to clear keys in non-volatile storage. Storage locations used by the file are overwritten with random bytes from the DRBG, then overwritten with zeroes, then read-verified for zeroes, and then the file is deleted.

Section 1.3 of [KMD] ("Authorization Acquisition/Encryption Engine Overview") describes how the TOE abstracts physical storage devices and can be used with HDD, SSD, hybrid, and array LUN technologies, and with any RAID type. Section 2 of [KMD] describes the keys and key material stored in non-volatile memory and identifies how the TOE interacts with the underlying platform to manage the keys.

The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.

Section 7.3.3 of [ST] ("FMT_SMF.1: Specification of Management Functions (FDE_EE)") identifies the `volume delete` command, used to cryptographically erase the VDEK. Section 7.1.6 of [ST] describes the `-force` optional parameter, which will immediately delete the VDEK associated with a volume. When this parameter is not used, the keys associated with the volume are deleted only when the volume is automatically deleted from the recovery-queue, or when the volume is purged from the recovery-queue. By default, the TOE automatically deletes volumes from the recovery-queue after 24 hours.

© 2024 Leidos. All rights reserved

If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.

The ST does not make use of the open assignment.

3.1.6.2 Guidance Activities

There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.

For example, when the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-leveling and garbage collection. This may create additional copies of the key that are logically inaccessible but persist physically. In this case, it is assumed the drive supports the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.

Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. It is assumed the operating system and file system of the OE support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion.

It is assumed that if a RAID array is being used, only set-ups that support TRIM are utilized. It is assumed if the drive is connected via PCI-Express, the operating system supports TRIM over that channel. It is assumed the drive is healthy and contains minimal corrupted data and will be end of life before a significant amount of damage to drive health occurs, it is assumed there is a risk small amounts of potentially recoverable data may remain in damaged areas of the drive.

Finally, it is assumed the keys are not stored using a method that would be inaccessible to TRIM, such as being contained in a file less than 982 bytes which would be completely contained in the master file table.

[CCCG] Section 2.5.2 “Request Cryptographic Erase of a Volume’s DEK” describes use of the `volume delete` command to delete an encrypted volume, including that a deleted volume can be recovered from the recovery-queue during the 24 hour retention period, and use of the `-force` parameter to immediately delete the volume and destroy the VDEK associated with the volume. This description is consistent with the description in [ST].

The guidance documentation does not identify any circumstances in which key destruction is delayed at the physical layer.

3.1.6.3 Test Activities

Test 1: Applied to each key held as plaintext in volatile memory and subject to destruction by overwrite by the TOE (whether or not the plaintext value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator shall:

1. Record the value of the key in the TOE subject to clearing.

© 2024 Leidos. All rights reserved

2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

3. Cause the TOE to clear the key.

4. Cause the TOE to stop the execution but not exit.

5. Cause the TOE to dump the entire memory of the TOE into a binary file.

6. Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.

7. Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece.

Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.

Step 7 ensures that partial key fragments do not remain in memory. If a fragment is found, there is a miniscule chance that it is not within the context of a key (e.g., some random bits that happen to match). If this is the case the test should be repeated with a different key in Step #1. If a fragment is found the test fails.

The evaluator confirmed the keys were generated and recorded their values. The evaluator then deleted the keys and confirmed via memory dumps that no traces of the full or partial keys remained in memory.

Modified by TD0766

The following tests apply only ~~to selection a),~~ ***for the selection of "logically addresses the storage location"*** *since the TOE in this instance has more visibility into what is happening within the underlying platform (e.g., a logical view of the media).* ~~*In selection b),*~~ ***For the selection of "instructs the underlying platform"*** *the TOE has no visibility into the inner workings and completely relies on the underlying platform, so there is no reason to test the TOE beyond test 1.*

For ***the*** *selection* ~~*a),*~~ ***of logically addresses the storage location,*** *the following tests are used to determine the TOE is able to request the platform to overwrite the key with a TOE supplied pattern.*

Test 2: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use a tool that provides a logical view of the media (e.g., MBR file system):

1. Record the value of the key in the TOE subject to clearing.

2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

3. Cause the TOE to clear the key.

4. Search the logical view that the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.

5. Break the key value from Step #1 into 3 similar sized pieces and perform a search using each piece. If a fragment is found then the test is repeated (as described for Use Case 1 test 1 above), and if a fragment is found in the repeated test then the test fails.

This test is not applicable because no keys are held in non-volatile memory.

Modified by TD0766

© 2024 Leidos. All rights reserved

The following tests apply only ~~to selection a),~~ ***for the selection of "logically addresses the storage location"*** *since the TOE in this instance has more visibility into what is happening within the underlying platform (e.g., a logical view of the media).* ~~*In selection b),*~~ ***For the selection of "instructs the underlying platform"*** *the TOE has no visibility into the inner workings and completely relies on the underlying platform, so there is no reason to test the TOE beyond test 1.*

For ***the*** *selection* ~~*a),*~~ ***of logically addresses the storage location,*** *the following tests are used to determine the TOE is able to request the platform to overwrite the key with a TOE supplied pattern.*

Test 3: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use a tool that provides a logical view of the media:

1. Record the logical storage location of the key in the TOE subject to clearing.

2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.

3. Cause the TOE to clear the key.

4. Read the logical storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.

The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

This test is not applicable because no keys are held in non-volatile memory.

3.1.7 Cryptographic Key and Key Material Destruction (Destruction Timing) (FCS_CKM_EXT.4(a)) ([AA], [EE])

3.1.7.1 TSS Activities

The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.

Section 7.1.7 of [ST] ("FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing) (FDE_EE)") states the TOE deletes all keys and key material when the storage volume they are protecting has been deleted. The VDEKs are automatically deleted when the corresponding volume is deleted. The key hierarchy itself is deleted when all volumes are deleted and the following command is run: `security key-manager onboard disable`. The CP-KEK is destroyed when the Onboard Key Manager is deleted, with the CP-KEK being zeroized in the cryptomod key table.

3.1.7.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.7.3 KMD Activities

The evaluator shall verify the KMD includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed.

Section 2.5 of [KMD] ("Critical Security Parameters Summary") describes each of the keys, key material, and critical security parameters in the key hierarchy and where they reside, while Section 4.5 ("Key Destruction") describes the circumstances under which keys and key material are no longer needed and are destroyed.

© 2024 Leidos. All rights reserved

The evaluator shall verify the KMD includes a key lifecycle, that includes a description where key material reside, how the key material is used, how it is determined that keys and key material are no longer needed, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4(a) for the destruction.

Section 2 of [KMD] ("Keys and Key Hierarchy") provides the key lifecycle, including descriptions of where key material resides and how it is used. Section 4.5 describes how it is determined keys and key material are no longer needed and how they are destroyed. The descriptions are consistent with the requirements in FCS_CKM.4(a).

3.1.7.4 Test Activities

There are no test evaluation activities for this SFR.

3.1.8 Cryptographic Key and Key Material Destruction (Power Management) (FCS_CKM_EXT.4(b)) ([AA], [EE])

3.1.8.1 TSS Activities

The evaluator shall verify the TSS provides a description of what keys and key material are destroyed when entering any Compliant power saving state.

Section 7.1.8 of [ST] ("FCS_CKM_EXT.4(b): Cryptographic Key and Key Material Destruction (Power Management) (FDE_EE)") states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). The following keys, held in volatile memory, are destroyed when the TOE enters either of the Compliant power saving states: CP-KEK; CKEK; SVM-KEK; VDEK.

3.1.8.2 Guidance Activities

The evaluator shall validate that guidance documentation contains clear warnings and information on conditions in which the TOE may end up in a non-Compliant power saving state indistinguishable from a Compliant power saving state. In that case it must contain mitigation instructions on what to do in such scenarios.

Section 7.4.2 of [ST] ("FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States (FDE_AA) (FDE_EE)") states the TOE enters the G3 (mechanical off) state when the administrator removes the device's power via a mechanical switch, and enters the G2 (S5) (soft off) state when an authorized user executes the `system halt` command.

Section 7.4.2 of [ST] further states the TOE must be fully rebooted from each Compliant power saving state. As such, the TOE is either operational, or is in a state that requires it to be fully rebooted in order to resume operation, and there are no other power saving states, Compliant or otherwise.

[CCCG] Section 2.3 "Compliant Power Saving States" and Section 2.2 "Authorization Factors" provide the guidance on how to boot the TOE and how to transition the TOE to either of the Compliant power saving states.

3.1.8.3 KMD Activities

The evaluator shall verify the KMD includes a description of the areas where keys and key material reside.

Section 2.5 of [KMD] ("Critical Security Parameters Summary") describes where keys and key material reside.

© 2024 Leidos. All rights reserved

The evaluator shall verify the KMD includes a key lifecycle that includes a description where key material resides, how the key material is used, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM_EXT.6 for the destruction.

Section 2 of [KMD] ("Keys and Key Hierarchy") provides the key lifecycle, including descriptions of where key material resides and how it is used. Section 4.5 describes how it is determined keys and key material are no longer needed and how they are destroyed. The descriptions are consistent with the requirements in FCS_CKM_EXT.6.

3.1.8.4 Test Activities

There are no test evaluation activities for this SFR.

3.1.9 Cryptographic Key Destruction Types (FCS_CKM_EXT.6) ([EE])

3.1.9.1 TSS + KMD Activities (KMD may be used if necessary details describe proprietary information)

The evaluator shall examine the TOE's keychain in the TSS/KMD and verify all keys subject to destruction are destroyed according to one of the specified methods.

The ST specifies in FCS_CKM_EXT.6 the TSF shall use the key destruction methods specified in FCS_CKM.4(d), which are as follows:

- For volatile memory, destruction is accomplished using a single overwrite of a pseudo-random pattern using the TOE's DRBG, followed by overwriting with zeroes, or by removal of power to memory
- For non-volatile memory, destruction is accomplished using a single overwrite of a pseudo-random pattern using the TOE's DRBG, followed by overwriting with zeroes.

Section 4.5 of [KMD] ("Key Lifetime and Key Destruction") describes the following approaches for destroying keys stored in volatile memory and keys stored in non-volatile memory:

- Key stored in volatile memory:
  - Memory location overwritten with DRBG generated random data
  - Memory location overwritten with zeroes
  - Memory location read and compared with zero.
- Key stored in non-volatile memory:
  - Storage location overwritten with DRBG generated random data
  - Storage location overwritten with zeroes
  - Storage location read and compared with zero.

In addition, keys stored in volatile memory are deleted when the system is powered down.

The appropriate key destruction method is applied to all keys in the TOE's keychain subject to destruction, depending on whether the key is in volatile or non-volatile memory.

3.1.9.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.9.3 Test Activities

There are no test evaluation activities for this SFR.

© 2024 Leidos. All rights reserved

3.1.10 Cryptographic Operation (Signature Verification) (FCS_COP.1(a)) ([AA], [EE])

3.1.10.1 TSS Activities

The evaluator shall check the TSS to ensure that it describes the overall flow of the signature verification. This should at least include identification of the format and general location (e.g., "firmware on the hard drive device" rather than “memory location 0x00007A4B") of the data to be used in verifying the digital signature; how the data received from the operational environment are brought on to the device; and any processing that is performed that is not part of the digital signature algorithm (for instance, checking of certificate revocation lists).

Section 7.1.10 of [ST] (“FCS_COP.1(a): Cryptographic Operation (Signature Verification) (FDE_AA) (FDE_EE)”) states the TOE implements the RSA digital signature algorithm with a key size (modulus) of 3072 bits and SHA-384 signatures to verify authenticity of trusted updates.

Upon receiving an update and the signature file, the TOE uses the embedded public key stored in the firmware on the NetApp appliance. The TOE will verify the signature before installing the update and reject any update with an invalid signature.

3.1.10.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.10.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.1.10.4 Test Activities

SD section 4.1.2.1.4 contains the tests the evaluators must perform for each type of digital signature scheme. Based on the assignments and selections in the requirement, the evaluators choose the specific activities that correspond to those selections. In this case RSA signature algorithm is selected.

Performed in accordance with NIAP Policy Letter #5.

Section 7.1 of [ST] (“Cryptographic Support”), Table 9 (“NetApp Cryptographic Security Module (NCSM) Algorithm Certificates”) identifies the CAVP certification verifying RSA signature verification, as follows.

Algorithm	Tested Capabilities	Certificates
RSA as defined in FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes	Signature Verification Signature Type: PKCS 1.5 Modulo: 3072 Hash Algorithm: SHA2-384 Signature Type: PKCSPSS Modulo: 3072 Hash Algorithm: SHA2-384	A4858: RSA SigVer (FIPS186-4)

The testing activities for the algorithm certificates listed above require the TOE to pass the tests described in FCS_COP.1(a).

© 2024 Leidos. All rights reserved

3.1.11 Cryptographic Operation (Hash Algorithm) (FCS_COP.1(b)) ([AA], [EE])

3.1.11.1 TSS Activities

The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

Section 7.1.11 of [ST] ("FCS_COP.1(b): Cryptographic Operation (Hash Algorithm) (FDE_AA) (FDE_EE)") states the TOE performs SHA-256, SHA-384, and SHA-512 for the following purposes:

- SHA-256—used in generating the CP-Hash value used in validating the CP when it is entered by an administrator
- SHA-384—used as part of the RSA signature verification function for trusted updates
- SHA-512—used as part of the PBKDF2 to derive the Cluster Passphrase Key Encryption Key (CP-KEK).

3.1.11.2 Guidance Activities

The evaluator checks the operational guidance documents to determine that any system configuration necessary to enable required hash size functionality is provided.

[CCCG] Section 2.6 "Cryptography" states that the hash size functionality is fixed for each of the individual hash sizes and uses described in Section 7.1.11 of [ST]. As such, no configuration guidance is necessary.

3.1.11.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.1.11.4 Test Activities

The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the PP SD for the bit-oriented vs. the byte-oriented test mode. See section 4.1.2.2.4 for a full description of the required test activities.

Performed in accordance with NIAP Policy Letter #5.

Section 7.1 of [ST] ("Cryptographic Support"), Table 14 ("CryptoMod version 2.2 Algorithm Certificates") identifies the CAVP certification verifying the SHA hash algorithm implemented by CryptoMod, as follows.

Algorithm	Tested Capabilities	Certificates
SHS as defined in ISO/IEC 10118-3:2004	SHA-256 SHA-512	A4794: SHA2-256 A4794: SHA2-512 A4795: SHA2-256, A4795: SHA2-512

© 2024 Leidos. All rights reserved

Section 7.1 of [ST] ("Cryptographic Support"), Table 15 ("NetApp Cryptographic Security Module (NCSM v3.0.8) Algorithm Certificates") identifies the CAVP certification verifying the SHA hash algorithm implemented by NCSM, as follows.

Algorithm	Tested Capabilities	Certificates
SHS as defined in ISO/IEC 10118-3:2004	SHA-256 SHA-384 SHA-512	A4858: SHA2-256 A4858: SHA2-384 A4858: SHA2-512

The testing activities for the algorithm certificates listed above require the TOE to pass the tests described in FCS_COP.1(b).

3.1.12 Cryptographic Operation (Keyed Hash Algorithm) (FCS_COP.1(c)) ([AA])

3.1.12.1 TSS Activities

If HMAC was selected:

The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

Section 7.1.12 of [ST] ("FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm) (FDE_AA)") specifies the key lengths, block sizes, output MAC lengths, and hash functions used by the TOE's HMAC implementation.

If CMAC was selected:

The evaluator shall examine the TSS to ensure that it specifies the following values used by the CMAC function: key length, block cipher used, block size (of the cipher), and output MAC length used.

The ST does not select CMAC.

3.1.12.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.12.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.1.12.4 Test Activities

If HMAC was selected:

For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key using a known good implementation.

If CMAC was selected:

For each of the supported parameter sets, the evaluator shall compose at least 15 sets of test data. Each set shall consist of a key and message data. The test data shall include messages of different lengths, some

© 2024 Leidos. All rights reserved

with partial blocks as the last block and some with full blocks as the last block. The test data keys shall include cases for which subkey K1 is generated both with and without using the irreducible polynomial R_b, as well as cases for which subkey K2 is generated from K1 both with and without using the irreducible polynomial R_b. (The subkey generation and polynomial R_b are as defined in SP800-38E.) The evaluator shall have the TSF generate CMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating CMAC tags with the same key using a known good implementation.

Performed in accordance with NIAP Policy Letter #5.

Section 7.1 of [ST] ("Cryptographic Support"), Table 14 ("CryptoMod version 2.2 Algorithm Certificates") identifies the CAVP certification verifying HMAC keyed hash algorithm, as follows.

Algorithm	Tested Capabilities	Certificates
HMAC that meets : FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code", and FIPS Pub 180-4, "Secure Hash Standard"	HMAC-SHA2-512	A4794: HMAC-SHA2-512 A4795: HMAC-SHA2-512

The testing activities for the algorithm certificates listed above require the TOE to pass the tests described in FCS_COP.1(c).

3.1.13 Cryptographic Operation (Key Wrapping) (FCS_COP.1(d)) ([AA], [EE])

3.1.13.1 TSS Activities

The evaluator shall verify the TSS includes a description of the key wrap function(s) and shall verify the key wrap uses an approved key wrap algorithm according to the appropriate specification.

Section 7.1.13 of [ST] ("FCS_COP.1(d): Cryptographic Operation (Keyed Wrapping) (FDE_AA) (FDE_EE)") states the TOE uses the KWP-AE(P) key wrapping function defined in NIST 800-38F to wrap keys, and the corresponding KWP-AD(C) function to unwrap keys. These are approved algorithms, consistent with the selections made in FCS_COP.1(d).

3.1.13.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.13.3 KMD Activities

The evaluator shall review the KMD to ensure that all keys are wrapped using the approved method and a description of when the key wrapping occurs.

Section 2.5 of [KMD] ("Critical Security Parameters Summary") identifies three keys in the key hierarchy that are wrapped: Cluster Key Encryption Key (CKEK); Storage Virtual Machine Key Encryption Key (SVM-KEK); and Volume Data Encryption Key (VDEK).

KMD Section 2.1.6 states that the CKEK is wrapped using KWP-AE as defined in NIST SP 800-38F, using the Cluster Passphrase Key Encryption Key (CP-KEK) as the encryption key. The CKEK is wrapped to produce the wCKEK as soon as it has been generated by the TOE's cryptomodule.

© 2024 Leidos. All rights reserved

KMD Section 2.1.6 states that the SVM-KEK is wrapped using KWP-AE as defined in NIST SP 800-38F, using the CKEK as the encryption key. The SVM-KEK is wrapped as soon as it has been generated by the TOE's cryptomodule and the wrapped key is stored in the TOE's replicated database and the Config database.

KMD Section 2.2 states the VDEK is wrapped using KWP-AE as defined in NIST SP 800-38F, using the SVM-KEK as the encryption key. The VDEK is wrapped as soon as it has been generated by the TOE's cryptomodule and the wrapped key is stored with Write Anywhere File Layout (WAFL) on-disk data structures.

KMD Figures 7 and 8 specifically state "when" the keys are wrapped.

3.1.13.4 Test Activities

There are no test evaluation activities for this SFR.

3.1.14 Cryptographic Operation (AES Data Encryption/Decryption) (FCS_COP.1(f)) ([AA], [EE])

3.1.14.1 TSS Activities

The evaluator shall verify the TSS includes a description of the key size used for encryption and the mode used for encryption.

Section 7.1.14 of [ST] ("FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption) (FDE_EE)") states the TOE performs data encryption and decryption using AES in XTS mode with 256 bit keys.

3.1.14.2 Guidance Activities

If multiple encryption modes are supported, the evaluator examines the guidance documentation to determine that the method of choosing a specific mode/key size by the end user is described.

The TOE supports AES-XTS mode for data encryption and decryption.

[CCCG] Section 2.6 "Cryptography" states that ONTAP 9.14.1 with NetApp Volume Encryption (NVE) supports 256-bit volume DEKs (AES-XTS-256) and 256-bit BEVs (AES-KWP).

3.1.14.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.1.14.4 Test Activities

AES-XTS was selected in the SFR.

XTS-AES Test

The evaluator shall test the encrypt functionality of XTS-AES for each combination of the following input parameter lengths:

256 bit (for AES-128) and 512 bit (for AES-256) keys

Three data unit (i.e., plaintext) lengths. One of the data unit lengths shall be a non-zero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported.

© 2024 Leidos. All rights reserved

The third data unit length shall be either the longest supported data unit length or 216 bits, whichever is smaller.

using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt.

The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally.

The evaluator shall test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTS-AES encrypt with XTS-AES decrypt.

Performed in accordance with NIAP Policy Letter #5.

Section 7.1 of [ST] ("Cryptographic Support"), Table 14 ("CryptoMod version 2.2 Algorithm Certificates") identifies the CAVP certification verifying AES data encryption and decryption, as follows.

Algorithm	Tested Capabilities	Certificates
AES-XTS as defined in NIST SP 800-38E	AES-XTS: Key Size: 256 bits Modes: Decrypt, Encrypt	A4794: AES-XTS A4795: AES-XTS

The testing activities for the algorithm certificates listed above require the TOE to pass the tests described in FCS_COP.1(f).

3.1.15 Cryptographic Key Derivation (FCS_KDF_EXT.1) ([AA], [EE])

3.1.15.1 TSS Activities

The evaluator shall verify the TSS includes a description of the key derivation function and shall verify the key derivation uses an approved derivation mode and key expansion algorithm according to SP 800-108 and SP 800-132.

Section 7.1.15 of [ST] ("FCS_KDF_EXT.1: Cryptographic Key Derivation (FDE_AA) (FDE_EE)") states the TOE implements PBKDFv2 with HMAC-SHA-512, 1024 iterations, and a salt value of 512 bits to transform the user password into a derived key as specified in SP 800-132.

3.1.15.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.15.3 KMD Activities

The evaluator shall examine the vendor's KMD to ensure that all keys used are derived using an approved method and a description of how and when the keys are derived.

Section 2.3 of [KMD] ("Key Hierarchy") describes the source of each of the keys and critical security parameters in the key hierarchy. Only the Cluster Passphrase Key Encryption Key (CP-KEK) is derived from other material—all other keys and critical security parameters (with the exception of the Cluster Passphrase entered by the user) are generated by the TOE using its approved CTR_DRBG function. The

© 2024 Leidos. All rights reserved

CP-KEK is derived using PBKDFv2 as specified in NIST SP 800-132, using HMAC-SHA-512 as the pseudo-random function, with a 512 bit random salt and 1,024 iterations.

KMD Figure 7 covers what happens when "OKM setup" is run (i.e. everything happens prior to command completion). The same is true for Figure 8, items all happen before "SVM create" command completes. Likewise, everything happens in Figure 9 before the "volume create" command completes.

3.1.15.4 Test Activities

There are no test evaluation activities for this SFR.

3.1.16 Key Chaining (Initiator) (FCS_KYC_EXT.1) ([AA])

3.1.16.1 TSS Activities

The evaluator shall verify the TSS contains a high-level description of the BEV sizes – that it supports BEV outputs of no fewer 128 bits for products that support only AES-128, and no fewer than 256 bits for products that support AES-256.

Section 7.1.16 of [ST] ("FCS_KYC_EXT.1: Key Chaining (initiator) (FDE_AA), FCS_KYC_EXT.2 Key Chaining (Recipient) (FDE_EE)") states the TOE derives a 256-bit BEV from the user's password (the Cluster Passphrase), using the PBKDFv2 function. This is consistent with the TOE's support of 256 bit AES keys.

3.1.16.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.16.3 KMD Activities

The evaluator shall examine the KMD describes a high level description of the key hierarchy for all authorizations methods selected in FCS_AFA_EXT.1 that are used to protect the BEV. The evaluator shall examine the KMD to ensure it describes the key chain in detail. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap or key derivation methods that meet FCS_COP.1(d) and FCS_KDF_EXT.1.

Section 2 of [KMD] ("Keys and Key Hierarchy") describes the various keys within the key hierarchy and how they are used to protect the BEV. It provides a detailed description of the key chain.

The TOE supports a single authorization factor (FCS_AFA_EXT.1), 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 (FCS_KDF_EXT.1, FCS_PCC_EXT.1).

The TOE uses its approved CTR_DRBG function to generate a 256 bit random number called the Cluster Key Encryption Key (CKEK). The TOE uses the KWP-AE(P) function to wrap the CKEK using the CP-KEK (FCS_COP.1(d)).

The TOE uses its approved CTR_DRBG function to generate a 256 bit random number called the Storage Virtual Machine Key Encryption Key (SVM-KEK). The TOE uses the KWP-AE(P) function to wrap the SVM-KEK using the CKEK (FCS_COP.1(d)).

© 2024 Leidos. All rights reserved

The TOE uses its approved CTR_DRBG function to generate two 256 bit random numbers that it concatenates to form the 512 bit Volume Date Encryption Key (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 (FCS_COP.1(d)).

The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the key chain.

Section 2.3 of [KMD] ("Key Hierarchy") describes how the key chain process functions. The key chain process does not expose any material that might compromise a key in the chain. When keys are generated, they either are stored in non-persistent storage in the key table of the TOE's cryptomodule, or they are wrapped before being stored in persistent storage.

Section 2.3 includes Figure 6 ("Key Hierarchy"), which illustrates the key hierarchy implemented by the TOE. Section 2.5 ("Critical Security Parameters Summary") includes a table that details where all keys and keying material are stored and how each key and critical security parameter originates or is derived.

The evaluator's examination of the key hierarchy determined that at no point can the chain be broken without a cryptographic exhaust or possession of the initial authorization value. The effective strength of the BEV of 256 bits is maintained throughout the key hierarchy.

The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

Figure 6 in Section 2.3 describes the strength of every key and piece of keying material used throughout the key chain.

3.1.16.4 Test Activities

There are no test evaluation activities for this SFR.

3.1.17 Key Chaining (Recipient) (FCS_KYC_EXT.2) ([EE])

3.1.17.1 TSS Activities

There are no TSS evaluation activities for this SFR.

3.1.17.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.17.3 KMD Activities

The evaluator shall examine the KMD to ensure it describes a high level key hierarchy and details of the key chain. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap or key derivation methods that meet FCS_KDF_EXT.1, FCS_COP.1(d), FCS_COP.1(e), and/or FCS_COP.1(g).

Section 2 of [KMD] ("Keys and Key Hierarchy") describes the various keys within the key hierarchy and how they are used to protect the BEV. It provides a detailed description of the key chain.

© 2024 Leidos. All rights reserved

The TOE supports a single authorization factor (FCS_AFA_EXT.1), 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 (FCS_KDF_EXT.1, FCS_PCC_EXT.1).

The TOE uses its approved CTR_DRBG function to generate a 256 bit random number called the Cluster Key Encryption Key (CKEK). The TOE uses the KWP-AE(P) function to wrap the CKEK using the CP-KEK (FCS_COP.1(d)).

The TOE uses its approved CTR_DRBG function to generate a 256 bit random number called the Storage Virtual Machine Key Encryption Key (SVM-KEK). The TOE uses the KWP-AE(P) function to wrap the SVM-KEK using the CKEK (FCS_COP.1(d)).

The TOE uses its approved CTR_DRBG function to generate two 256 bit random numbers that it concatenates to form the 512 bit Volume Date Encryption Key (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 (FCS_COP.1(d)).

The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or knowledge of the BEV and the effective strength of the DEK is maintained throughout the Key Chain.

Section 2.3 of [KMD] ("Key Hierarchy") describes how the key chain process functions. The key chain process does not expose any material that might compromise a key in the chain. When keys are generated, they either are stored in non-persistent storage in the key table of the TOE's cryptomodule, or they are wrapped before being stored in persistent storage.

Section 2.3 includes Figure 6 ("Key Hierarchy"), which illustrates the key hierarchy implemented by the TOE. Section 2.5 ("Critical Security Parameters Summary") includes a table that details where all keys and keying material are stored and how each key and critical security parameter originates or is derived.

The evaluator's examination of the key hierarchy determined that at no point can the chain be broken without a cryptographic exhaust or knowledge of the BEV. The effective strength of the DEK of 256 bits is maintained throughout the key hierarchy.

The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

Figure 6 in Section 2.3 describes the strength of every key and piece of keying material used throughout the key chain.

3.1.17.4 Test Activities

There are no test evaluation activities for this SFR.

© 2024 Leidos. All rights reserved

3.1.18 Cryptographic Password Construct and Conditioning (FCS_PCC_EXT.1) ([AA])

3.1.18.1 TSS Activities

The evaluator shall ensure the TSS describes the manner in which the TOE enforces the construction of passwords, including the length, and requirements on characters (number and type). The evaluator also verifies that the TSS provides a description of how the password is conditioned and the evaluator ensures it satisfies the requirement.

Section 7.1.17 of [ST] ("FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning (FDE_AA)") states the TOE accepts passwords up to 256 characters. The character set can consist of all upper case characters, lower case characters, numbers, and all printable ASCII characters. The password is conditioned using PBDKFv2 that meets SP 800-132. The cryptographic algorithm implements HMAC-SHA-512, a salt value of 512 bits from the DRBG, and 1024 iterations to produce a cryptographic key size of 256-bits. This description satisfies the statement of FCS_PCC_EXT.1.1 in Section 6.2.1.19 of [ST] ("FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning (FDE_AA)").

3.1.18.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.18.3 KMD Activities

The evaluator shall examine the KMD to ensure that the formation of the BEV and intermediary keys is described and that the key sizes match that selected by the ST author.

Section 2.1 of [KMD] ("Border Encryption Values") describes the formation of the Border Encryption Value (BEV) and intermediary keys. In TOE terms, the Storage Virtual Machine Key Encryption Key (SVM-KEK) is the BEV, linking the AA and EE key chains. The SVM-KEK is 256 bits, consistent with the key size selected by the ST author.

The evaluator shall check that the KMD describes the method by which the password/passphrase is first encoded and then fed to the SHA algorithm. The settings for the algorithm (padding, blocking, etc.) shall be described, and the evaluator shall verify that these are supported by the selections in this component as well as the selections concerning the hash function itself. The evaluator shall verify that the KMD contains a description of how the output of the hash function is used to form the submask that will be input into the function and is the same length as the BEV as specified above.

Section 2.1.1 of [KMD] ("Cluster Passphrase") describes the method by which the password is encoded and fed to the SHA algorithm. The password is a 64 to 256 byte ASCII string that is concatenated with a salt generated by the TOE's DRBG and fed to the PBKDF2 function that meets NIST SP 800-132 to derive the Cluster Passphrase Key Encryption Key (CP-KEK). Section 2.1.5 of [KMD] ("Cluster Passphrase Key Encryption Key (CP-KEK)") describes the parameters of the PBKDF2 function, consistent with the selections in the ST—using the HMAC-SHA-512 algorithm with 1024 iterations and an output size of 256 bits.

3.1.18.4 Test Activities

The evaluator shall also perform the following tests:

Test 1: Ensure that the TOE supports passwords/passphrases of a minimum length of 64 characters.

The evaluator attempted to configure a cluster passphrase on the TOE of 64 characters and verified it was accepted.

© 2024 Leidos. All rights reserved

Test 2: If the TOE supports a password/passphrase length up to a maximum number of characters, n (which would be greater than 64), then ensure that the TOE will not accept more than n characters.

The TOE only accepts passphrases up to 256 characters. The evaluator attempted to configure a cluster passphrase on the TOE that was 257 characters and confirmed this attempt was denied.

Test 3: Ensure that the TOE supports passwords consisting of all characters assigned and supported by the ST author.

The evaluator attempted to configure the TOE with a passphrase consisting of at least one of each printable ASCII character and confirmed that it was accepted.

3.1.19 Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT.1) ([AA], [EE])

3.1.19.1 TSS Activities

For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.

Section 7.1.18 of [ST] ("FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) (FDE_AA) (FDE_EE)") states random bits are produced by a DRBG implemented within the TOE's own cryptographic module. As such, there is no reliance on third party RBG services.

Section 7.1.18 of [ST] also indicates the TOE implements a single DRBG mechanism, CTR_DRBG using AES-256.

3.1.19.2 Guidance Activities

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected DRBG mechanism(s), if necessary, and provides information regarding how to instantiate/call the DRBG for RBG services needed in this cPP.

The TOE provides a single DRBG mechanism implemented within its own cryptographic module and used by default. As such, no configuration is required and no guidance documentation is necessary.

The ONTAP "end user" (i.e. storage admin) does not explicitly instantiate/call the DRBG. The DRBG is called when the key hierarchy is set up. The key hierarchy is automatically set up when OKM is configured.

ST Section 7.2.1 states that the TOE ensures that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE. Configuring OKM in CC mode constitutes "first time provisioning".

3.1.19.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.1.19.4 Test Activities

The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable by the TOE, the evaluator shall perform 15 trials for each configuration. The evaluator shall verify that the instructions

© 2024 Leidos. All rights reserved

in the operational guidance for configuration of the RNG are valid. See section 4.1.5.1.4 for full details on how the tests for this SFR are to be performed.

Performed in accordance with NIAP Policy Letter #5.

Section 7.1 of [ST] ("Cryptographic Support"), Table 14 ("CryptoMod version 2.2 Algorithm Certificates") identifies the CAVP certifications verifying random bit generation, as follows.

Algorithm	Tested Capabilities	Certificates
CTR_DRBG (AES)	Counter: Modes: AES-256	A4794: Counter DRBG A4795: Counter DRBG

The testing activities for the algorithm certificates listed above require the TOE to pass the tests described in FCS_RBG_EXT.1.

3.1.20 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FCS_SNI_EXT.1) ([AA], [EE])

3.1.20.1 TSS Activities

Modified by TD0760

If salts are used t~~T~~he evaluator shall ensure the TSS describes how salts are generated. The evaluator shall confirm that the salt is generating using an RBG described in FCS_RBG_EXT.1 or by the Operational Environment. If external function is used for this purpose, the TSS should include the specific API that is called with inputs.

Section 7.1.19 of [ST] ("FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FDE_AA) (FDE_EE)") describes how salts are generated. It states the TOE generates salts using its own DRBG as specified in FCS_RBG_EXT.1.

Modified by TD0760

If IVs or nonces are used, t~~T~~he evaluator shall ensure the TSS describes how nonces are created uniquely and how IVs and tweaks are handled (based on the AES mode). The evaluator shall confirm that the nonces are unique and the IVs and tweaks meet the stated requirements.

Section 7.1.19 of [ST] states the TOE does not use nonces or IVs. It further states tweak values are non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer. This meets the requirements for tweak values specified in FCS_SNI_EXT.1.

3.1.20.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.1.20.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.1.20.4 Test Activities

There are no test evaluation activities for this SFR.

© 2024 Leidos. All rights reserved

3.1.21 Validation (FCS_VAL_EXT.1/AA) ([AA])

3.1.21.1 TSS Activities

The evaluator shall examine the TSS to determine which authorization factors support validation.

Section 7.1.20 of [ST] ("FCS_VAL_EXT.1/AA Validation (FDE_AA)") states the Cluster Passphrase authorization factor is used to support validation.

The evaluator shall examine the TSS to review a high-level description if multiple submasks are used within the TOE, how the submasks are validated (e.g., each submask validated before combining, once combined validation takes place).

Section 7.1.1 of [ST] ("FCS_AFA_EXT.1: Authorization Factor Acquisition (FDE_AA)") states the Cluster Passphrase serves as the password authorization factor—it is the only submask used by the TOE.

3.1.21.2 Guidance Activities

(conditional) If the validation functionality is configurable, the evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.

The validation functionality is not configurable. The administrator has one attempt to enter the correct Cluster Passphrase at boot or after recovering from a failure in the boot media, and five attempts to enter the correct current Cluster Passphrase when attempting to modify the Cluster Passphrase.

(conditional) If the validation functionality is specified by the ST author, the evaluator shall examine the operational guidance to ensure that it states the values that the TOE uses for limits regarding validation attempts.

[CCCG] Section 2.6.1 "Validation" states that when modifying the cluster passphrase, an administrator is allowed 5 consecutive failed attempts to authenticate with the current cluster passphrase. After 5 consecutive failed attempts, the cluster passphrase may be modified only by (a) rebooting one or more nodes within the cluster, or (b) waiting for 24 hours to elapse before re-attempting to modify the cluster passphrase.

3.1.21.3 KMD Activities

The evaluator shall examine the KMD to verify that it described the method the TOE employs to limit the number of consecutively failed authorization attempts.

Section 2.1.1 of [KMD] ("Cluster Passphrase") describes the TOE's methods for limiting the number of consecutive failed authentication attempts. The TOE allows five such attempts when a user attempts to change the Cluster Passphrase (the authorization factor). When five consecutive failed attempts occur, one or more nodes within the cluster must be successfully rebooted, or a period of 24 hours needs to elapse before the user is allowed to change the Cluster Passphrase.

When booting the TOE or when attempting to recover from a failure in the boot media, only one attempt to enter the passphrase is allowed. If an incorrect Cluster Passphrase is entered at boot, then the TOE's operating system will boot, but the Write Anywhere File Layout (WAFL) component will be unable to mount any user data volumes. As a consequence, the TOE will be unable to service any user data. This condition can only be cleared by rebooting the node.

© 2024 Leidos. All rights reserved

The evaluator shall examine the vendor's KMD to ensure it describes how validation is performed. The description of the validation process in the KMD provides detailed information how the TOE validates the submasks. The KMD describes how the process works, such that it does not expose any material that might compromise the submask(s).

Section 2.1.3 of [KMD] ("CP-Salt") describes the CP-Salt value, while Section 2.1.4 of [KMD] ("CP-Hash") describes the CP-Hash value. The CP-Hash is used by the OKM component of the TOE when there is a need to validate that the Cluster Passphrase (the only submask defined for the TOE) has been entered correctly. The CP-Hash is formed as follows: the TOE uses its cryptomodule to generate a random 64-byte value, the CP-Salt; the CP-Salt is concatenated with the CP and a SHA-256 hash is calculated over this string; the result is the CP-Hash, which is stored persistently in the RDB. Anytime the CP is entered (e.g., at boot or when the administrator attempts to change the CP), the TOE validates the CP by concatenating the entered CP with the persistently stored CP-Salt, calculating the SHA-256 hash of the concatenated string, and comparing the result with the stored CP-Hash. If the values match, the correct CP has been entered and the TOE can proceed. Otherwise, an incorrect CP has been entered and the requested operation will fail.

Once the CP has been validated, it is used to derive the Cluster Passphrase Key Encryption Key (CP-KEK). The CP-KEK in turn is used to unwrap the Cluster Key Encryption Key (CKEK). The CKEK in turn is used to unwrap the Storage Virtual Machine Key Encryption Key (SVM-KEK), and finally the SVM-KEK is used to unwrap the Volume Data Encryption Key (VDEK) which is used to encrypt and decrypt data stored on the volume.

Section 2.3 of [KMD] ("Key Hierarchy") Figure 6 illustrates the key hierarchy. KMD Sections 2.1 – 2.2 describe what is in the diagram.

3.1.21.4 Test Activities

The evaluator shall perform the following tests:

Test 1: The evaluator shall determine the limit on the average rate of the number of consecutive failed authorization attempts. The evaluator will test the TOE by entering that number of incorrect authorization factors in consecutive attempts to access the protected data. If the limit mechanism includes any "lockout" period, the time period tested should include at least one such period. Then the evaluator will verify that the TOE behaves as described in the TSS.

The evaluator confirmed that the encrypted volume was online then rebooted the TOE and input the incorrect cluster passphrase then confirmed the volume was offline. The evaluator then rebooted the TOE again and input the correct cluster passphrase and confirmed that the volume was online.

Note that the TOE does not have a lockout period. There is only one opportunity to enter the cluster passphrase into the TOE. If an incorrect passphrase is entered then encrypted volumes are inaccessible.

Test 2: The evaluator shall force the TOE to enter a Compliant power saving state, attempt to resume it from this state, and verify that only a valid authorization factor as defined by the guidance documentation is sufficient to allow the TOE to exit the Compliant power saving state.

The evaluator confirmed that the encrypted volume was online then power cycled the TOE and input the incorrect cluster passphrase then confirmed the volume was offline. The evaluator then rebooted the TOE again and input the correct cluster passphrase and confirmed that the volume was online.

© 2024 Leidos. All rights reserved

3.1.22 Validation (FCS_VAL_EXT.1/EE) ([EE])

3.1.22.1 TSS Activities

The evaluator shall examine the TSS to determine which authorization factors support validation.

Section 7.1.21 of [ST] ("FCS_VAL_EXT.1/EE Validation (FDE_EE)") states the Cluster Passphrase authorization factor is used to support validation.

The evaluator shall examine the TSS to review a high-level description if multiple submasks are used within the TOE, how the submasks are validated (e.g., each submask validated before combining, once combined validation takes place).

Section 7.1.1 of [ST] ("FCS_AFA_EXT.1: Authorization Factor Acquisition (FDE_AA)") states the Cluster Passphrase serves as the password authorization factor—it is the only submask used by the TOE.

The evaluator shall also examine the TSS to determine that a subset or all of the authorization factors identified in the SFR can be used to exit from a Compliant power saving state.

Section 7.4.2 of [ST] ("FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States (FDE_AA) (FDE_EE)") states the TOE must be fully rebooted to exit from either of the TOE's Compliant power saving states (G2(S5) and G3). Section 7.1.21 of [ST] describes the use of the Cluster Passphrase to exit from the Compliant power saving states supported by the TOE. The Cluster Passphrase has to be entered at boot time. When the TOE boots, if the Cluster Passphrase is incorrect, the TOE is unable to unwrap its DEK and consequently there is no access to stored encrypted data. The only way to recover is to reboot and enter the correct Cluster Passphrase.

3.1.22.2 Guidance Activities

(conditional) If the validation functionality is configurable, the evaluator shall examine the operational guidance to ensure it describes how to configure the TOE to ensure the limits regarding validation attempts can be established.

The validation functionality is not configurable. The administrator has one attempt to enter the correct Cluster Passphrase at boot or after recovering from a failure in the boot media, and five attempts to enter the correct current Cluster Passphrase when attempting to modify the Cluster Passphrase.

(conditional) If the validation functionality is specified by the ST author, the evaluator shall examine the operational guidance to ensure that it states the values that the TOE uses for limits regarding validation attempts.

[CCCG] Section 2.6.1 "Validation" states that when modifying the cluster passphrase, an administrator is allowed 5 consecutive failed attempts to authenticate with the current cluster passphrase. After 5 consecutive failed attempts, the cluster passphrase may be modified only by (a) rebooting one or more nodes within the cluster, or (b) waiting for 24 hours to elapse before re-attempting to modify the cluster passphrase.

The evaluator shall verify that the guidance documentation states which authorization factors are allowed to exit a compliant power saving state.

[CCCG] Section 2.1 "Configuration" provides instructions for configuring the Cluster Passphrase authorization factor.

© 2024 Leidos. All rights reserved

To configure ONTAP 9.14.1 for use with NetApp Volume Encryption (NVE), the Onboard Key Manager (OKM) must be enabled for the admin Vserver in Common Criteria (CC) mode. The following command will enable OKM in CC mode:

```
security key-manager onboard enable -cc-mode-enabled yes
```

When CC mode is enabled, the cluster administrator will be required to provide a cluster passphrase that is between 64 and 256 ASCII characters long. This passphrase must be entered at the console each time that a node in the cluster boots.

3.1.22.3 KMD Activities

The evaluator shall examine the KMD to verify that it described the method the TOE employs to limit the number of consecutively failed authorization attempts.

Section 2.1.1 of [KMD] ("Cluster Passphrase") describes the TOE's methods for limiting the number of consecutive failed authentication attempts. The TOE allows five such attempts when a user attempts to change the Cluster Passphrase (the authorization factor). When five consecutive failed attempts occur, one or more nodes within the cluster must be successfully rebooted, or a period of 24 hours needs to elapse before the user is allowed to change the Cluster Passphrase.

When booting the TOE or when attempting to recover from a failure in the boot media, only one attempt to enter the passphrase is allowed. If an incorrect Cluster Passphrase is entered at boot, then the TOE's operating system will boot, but the Write Anywhere File Layout (WAFL) component will be unable to mount any user data volumes. As a consequence, the TOE will be unable to service any user data. This condition can only be cleared by rebooting the node.

The evaluator shall examine the vendor's KMD to ensure it describes how validation is performed. The description of the validation process in the KMD provides detailed information how the TOE validates the submasks. The KMD describes how the process works, such that it does not expose any material that might compromise the submask(s).

Section 2.1.3 of [KMD] ("CP-Salt") describes the CP-Salt value, while Section 2.1.4 of [KMD] ("CP-Hash") describes the CP-Hash value. The CP-Hash is used by the OKM component of the TOE when there is a need to validate that the Cluster Passphrase (the only submask defined for the TOE) has been entered correctly. The CP-Hash is formed as follows: the TOE uses its cryptomodule to generate a random 64-byte value, the CP-Salt; the CP-Salt is concatenated with the CP and a SHA-256 hash is calculated over this string; the result is the CP-Hash, which is stored persistently in the ONTAP's replicated database (RDB). Anytime the CP is entered (e.g., at boot or when the administrator attempts to change the CP), the TOE validates the CP by concatenating the entered CP with the persistently stored CP-Salt, calculating the SHA-256 hash of the concatenated string, and comparing the result with the stored CP-Hash. If the values match, the correct CP has been entered and the TOE can proceed. Otherwise, an incorrect CP has been entered and the requested operation will fail.

Once the CP has been validated, it is used to derive the Cluster Passphrase Key Encryption Key (CP-KEK). The CP-KEK in turn is used to unwrap the Cluster Key Encryption Key (CKEK). The CKEK in turn is used to unwrap the Storage Virtual Machine Key Encryption Key (SVM-KEK), and finally the SVM-KEK is used to unwrap the Volume Data Encryption Key (VDEK) which is used to encrypt and decrypt data stored on the volume.

3.1.22.4 Test Activities

The evaluator shall perform the following tests:

© 2024 Leidos. All rights reserved

Test 1: The evaluator shall determine the limit on the average rate of the number of consecutive failed authorization attempts. The evaluator will test the TOE by entering that number of incorrect authorization factors in consecutive attempts to access the protected data. If the limit mechanism includes any "lockout" period, the time period tested should include at least one such period. Then the evaluator will verify that the TOE behaves as described in the TSS.

The evaluator confirmed that the encrypted volume was online then rebooted the TOE and input the incorrect cluster passphrase then confirmed the volume was offline. The evaluator then rebooted the TOE again and input the correct cluster passphrase and confirmed that the volume was online.

Test 2: The evaluator shall force the TOE to enter a Compliant power saving state, attempt to resume it from this state, and verify that only a valid authorization factor as defined by the guidance documentation is sufficient to allow the TOE to exit the Compliant power saving state.

The evaluator confirmed that the encrypted volume was online then power cycled the TOE and input the incorrect cluster passphrase then confirmed the volume was offline. The evaluator then rebooted the TOE again and input the correct cluster passphrase and confirmed that the volume was online.

3.2 User Data Protection (FDP)

3.2.1 Protection of Data on Disk (FDP_DSK_EXT.1) ([EE])

3.2.1.1 TSS Activities

The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the disk and the point at which the encryption function is applied. The TSS must make the case that standard methods of accessing the disk drive via the host platforms operating system will pass through these functions.

Section 7.2.1 of [ST] ("FDP_DSK_EXT.1 Protection of Data on Disk (FDE_EE)") describes the process by which data is written to disk and the point at which the encryption function is applied.

The TOE ensures that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE. Configuring OKM in CC mode constitutes "first time provisioning".

The encryption of any protected data does not depend on a user electing to protect that data. The drive encryption occurs transparently to the user and the decision to protect the data is outside the discretion of the user. The RAID layer encrypts (decrypts) 4k block of user data using AES-XTS-256 when writing to (reading from) the drives.

Provided that the write-path buffer received by RAID from WAFL needs to be encrypted, the RAID component:

- Passes the data, along with the VEK key ID (which RAID gets from WAFL) to the NetApp CryptoMod;
- Calculates a checksum over the unencrypted and encrypted data;
- Writes the encrypted data (and encrypted checksum) to disk;
- Sets an on-disk flag indicating that the checksum is calculated over the encrypted data.

Only Data Volumes are encrypted. Data on a root volume, an SVM root volume is not encrypted.

WAFL encrypts all user data, there is metadata (not available to a user) that is not encrypted.

© 2024 Leidos. All rights reserved

For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke this functionality.

All cryptographic functions are implemented by the TOE.

The evaluator shall verify the TSS in performing the evaluation activities for this requirement. The evaluator shall ensure the comprehensiveness of the description, confirms how the TOE writes the data to the disk drive, and the point at which it applies the encryption function.

Section 7.2.1 of [ST] states when data is to be written encrypted to disk, the TOE's RAID component passes the data along with the DEK to the TOE's Cryptomodule, which returns the encrypted data, which the RAID component then passes to the TOE's Storage component, which performs the actual write to disk.

The evaluator shall verify that the TSS describes the initialization of the TOE and the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE. The evaluator shall verify the TSS describes areas of the disk that it does not encrypt (e.g., portions associated with the Master Boot Records (MBRs), boot loaders, partition tables, etc.). If the TOE supports multiple disk encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all storage devices on the platform.

Section 7.2.1 of [ST] states the TOE ensures that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE.

Section 7.2.1 of [ST] states only Data Volumes are encrypted. Data on a node root volume, an SVM root volume, or a MetroCluster metadata volume is not encrypted. In addition, the TOE does not encrypt the following persistent data: the root aggregate (which does not contain any user data); the boot media (which does not contain any user data); and fingerprint data, which is used in deduplicating client read requests.

[CCCG] Section "Cryptography" states that volume encryption is enabled by default, no other configuration of cryptographic parameters is possible/required.

3.2.1.2 Guidance Activities

The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to enable the FDE function, including any necessary preparatory steps. The guidance shall provide instructions that are sufficient, on all platforms, to ensure that all hard drive devices will be encrypted when encryption is enabled.

[CCCG] Section "Cryptography" states that volume encryption is enabled by default, no other configuration of cryptographic parameters is possible/required.

© 2024 Leidos. All rights reserved

3.2.1.3 KMD Activities

The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the product, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions associated with the Master Boot Record (MBRs), partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the device's host interface and the device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine.

Section 3 of [KMD] ("Encryption Engine") describes the data encryption engine. It comprises a software implementation of XTS-AES, contained within the TOE's cryptographic module. The appropriate encryption and decryption functions are called whenever user data needs to be encrypted and decrypted respectively. Section 1.3 of [KMD] ("Authorization Acquisition/Encryption Engine Overview") includes a functional block diagram showing the main components of the TOE and interactions between them. Section 3.2 of [KMD] ("Initialization") describes initialization of the TOE from power on to the point where it is ready to write encrypted data to disk and decrypt data read from disk.

The evaluator shall verify the KMD provides sufficient instructions for all platforms to ensure that when the user enables encryption, the product encrypts all hard storage devices. The evaluator shall verify that the KMD describes the data flow from the device's host interface to the device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted Master Boot Record area).

Section 3 of [KMD] states when the TOE is in its evaluated configuration, all client hard storage devices are created as encrypted volumes, with each volume using a unique DEK. Section 1.3 of [KMD] describes the data flow from the TOE's external user interface to the persistent media storing encrypted data. Section 3.3 of [KMD] ("Operation") identifies the system volumes, which never contain user data and are not encrypted.

The evaluator shall verify that the KMD provides a description of the platform's boot initialization, the encryption initialization process, and at what moment the product enables the encryption. The evaluator shall validate that the product does not allow for the transfer of user data before it fully initializes the encryption. The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.

Section 3.2 of [KMD] describes initialization of the TOE from power on to the point where it is ready to write encrypted data to disk and decrypt data read from disk. The evaluator determined the TOE does not allow for the transfer of user data before encryption on the storage volumes is fully initialized.

3.2.1.4 Test Activities

The evaluator shall perform the following tests:

© 2024 Leidos. All rights reserved

Test 1: Write data to random locations, perform required actions and compare:

• Ensure TOE is initialized and, if hardware, encryption engine is ready;

• Provision TOE to encrypt the storage device. For SW Encryption products, or hybrid products use a known key and the developer tools.

• Determine a random character pattern of at least 64 KB;

• Retrieve information on what the device TOE's lowest and highest logical address is for which encryption is enabled.

Test 2: Write pattern to storage device in multiple locations:

• For HW Encryption, randomly select several logical address locations within the device's lowest to highest address range and write pattern to those addresses;

• For SW Encryption, write the pattern using multiple files in multiple logical locations.

Test 3: Verify data is encrypted:

• For HW Encryption:

▪ engage device's functionality for generating a new encryption key, thus performing an erase of the key per FCS_CKM.4(a);

▪ Read from the same locations at which the data was written;

▪ Compare the retrieved data to the written data and ensure they do not match

• For SW Encryption, using developer tools;

▪ Review the encrypted storage device for the plaintext pattern at each location where the file was written and confirm plaintext pattern cannot be found.

▪ Using the known key, verify that each location where the file was written, the plaintext pattern can be correctly decrypted using the key.

▪ If available in the developer tools, verify there are no plaintext files present in the encrypted range.

The evaluator created three files that all contained character patterns and were at least 64KB each. The evaluator then wrote the files to the volume and dumped the raw data from the volume and confirmed that the data was encrypted. The evaluator then queried the TOE's volume after decrypt and confirmed that the character patterns were successfully written. Additionally the evaluator ran a command to gather information on the logical address range of the encrypted TOE volumes.

© 2024 Leidos. All rights reserved

3.3 Security Management (FMT)

3.3.1 Management of Functions Behavior (FMT_MOF.1) ([AA])

3.3.1.1 TSS Activities

If support for Compliant power saving state(s) are claimed in the ST, the evaluator shall ensure the TSS describes how these are managed and shall ensure that TSS describes how only privileged users (administrators) are allowed to manage the states.

Section 7.3.1 of [ST] ("FMT_MOF.1 Management of Functions Behavior (FDE_AA)") states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). The TOE transitions to the G2(S5) state through execution of the `system halt` command. This command is restricted to cluster administrators at the ***admin*** privilege level. The TOE transitions to the G3 state when the administrator removes device power via mechanical switch.

3.3.1.2 Guidance Activities

The evaluator to check if guidance documentation describes which authorization factors are required to change Compliant power saving state behavior and properties.

The TOE does not support modification of the behavior of Compliant power saving states or their properties. The TOE supports only a single powered state and the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). The TOE enters the powered state when power is applied to the TOE and it boots up. The TOE enters the G2(S5) state when an administrator executes the `system halt` command, and enters the G3 state via removal of power.

3.3.1.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.3.1.4 Test Activities

The evaluator shall perform the following tests:

Modified per TD0765

Test 1: **(conditional): If the product supports changes to compliant power saving states, t**~~T~~heThe evaluator presents a privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior and properties are allowed.

The evaluator logged in to TOE as an authorized user and confirmed that the user could change the compliant power state.

Modified per TD0765

Test 2: **(conditional): If the product supports changes to compliant power saving states, t**~~T~~he evaluator presents a non-privileged authorization credential to the TSF and validates that changes to Compliant power saving state behavior are not allowed.

The evaluator logged in to TOE as an unauthorized user and confirmed that the user could not change the compliant power state.

© 2024 Leidos. All rights reserved

3.3.2 Specification of Management Functions (FMT_SMF.1/AA) ([AA])

3.3.2.1 TSS Activities

If item a) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE sends the request to the EE to change the DEK.

Section 7.3.2 of [ST] ("FMT_SMF.1: Specification of Management Functions (FDE_AA)") states the TOE forwards requests to change the DEK to the EE when the authorized user executes the `volume encryption rekey` command.

If item b) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE sends the request to the EE to cryptographically erase the DEK.

Section 7.3.2 of [ST] states the TOE cryptographically erases the DEK via the authorized user execution of the `volume delete` command.

If item c) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes the methods by which users may change the set of all authorization factor values supported.

Section 7.3.2 of [ST] states the TOE permits users to change the TOE's authorization factor via execution of the `security key-manager onboard update-passphrase` command.

If item d) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes the process to initiate TOE firmware/software updates.

Section 7.3.2 of [ST] states the TOE initiates TOE firmware/software updates via execution of the `cluster image update` command.

If item e) is selected in FMT_SMF.1.1: If power saving states can be managed, the evaluator shall ensure that the TSS describes how this is performed, including how the TOE supports disabling certain power saving states if more than one are supported. If additional management functions are claimed in the ST, the evaluator shall ensure the TSS describes the additional functions.

The ST selects "no other functions" for item e) in FMT_SMF.1/AA.

3.3.2.2 Guidance Activities

If item a) and/or b) is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how the functions for A and B can be initiated by the user.

[CCCG] Section 2.5.1 "Request Change of a Volume's DEK" provides the instructions to initiate a change to the DEK and [CCCG] Section 2.5.2 "Request Cryptographic Erase of a Volume's DEK"

The commands to initiate a change to the DEK (`volume encryption rekey`) and to cryptographically erase the DEK (`volume delete`).

If item c) is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how selected authorization factor values are changed.

[CCCG] Section 2.5.3 "Request change of Authorization Factors" states that the cluster passphrase associated with the Onboard Key Manager (OKM) may be modified by the cluster admin. The command to modify the cluster passphrase is `security key-manager onboard update-passphrase`.

© 2024 Leidos. All rights reserved

If item d) is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how to initiate TOE firmware/software updates.

[CCCG] Section 2.5.4 "Initiate ONTAP Software Updates" states that ONTAP cluster admins are allowed to update the TOE via the `cluster image update` CLI command. ONTAP CC updates are cryptographically signed using a 3072-bit RSA digital signature on SHA-384 hashes.

If item e) is selected in FMT_SMF.1.1: Default Authorization Factors: It may be the case that the TOE arrives with default authorization factors in place. If it does, then the selection in section E must be made so that there is a mechanism to change these authorization factors. The operational guidance shall describe the method by which the user changes these factors when they are taking ownership of the device. The TSS shall describe the default authorization factors that exist.

Disable Key Recovery: The guidance for disabling this capability shall be described in the AGD documentation.

Power Saving: The guidance shall describe the power saving states that are supported by the TSF, how these states are applied, how to configure when these states are applied (if applicable), and how to enable/disable the use of specific power saving states (if applicable).

The ST selects “no other functions” for item e) in FMT_SMF.1/AA.

3.3.2.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.3.2.4 Test Activities

If item a) and/or b) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to forward a command to the EE to change and cryptographically erase the DEK. The actual testing of the cryptographic erase will take place in the EE.

The evaluator recorded the value of the VDEK and then issued a rekey command on the TOE. The evaluator then queried the VDEK and confirmed that it was a new value.

If item c) is selected in FMT_SMF.1.1: The evaluator shall initialize the TOE such that it requires the user to input an authorization factor in order to access encrypted data.

Test 1: The evaluator shall first provision user authorization factors, and then verify all authorization values supported allow the user access to the encrypted data. Then the evaluator shall exercise the management functions to change a user’s authorization factor values to a new one. Then he or she will verify that the TOE denies access to the user’s encrypted data when he or she uses the old or original authorization factor values to gain access.

The evaluator booted the TOE and input the correct cluster passphrase and confirmed that the volume was online. The evaluator then changed the cluster passphrase, rebooted the TOE and provided the previous (incorrect) cluster passphrase. The evaluator confirmed that the volume was offline and not accessible.

If item d) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to initiate TOE firmware/software updates.

© 2024 Leidos. All rights reserved

If item e) is selected in FMT_SMF.1.1: If additional management functions are claimed, the evaluator shall verify that the additional features function as described.

Modified by TD0767

Test 2 (conditional): If the TOE provides default authorization **values** ~~factors~~, the evaluator shall change these **values** ~~factors~~ in the course of taking ownership of the device as described in the operational guidance. The evaluator shall then confirm that the (old) authorization **values** ~~factors~~ are no longer valid for data access.

Test 3 (conditional): If the TOE provides key recovery capability whose effects are visible at the TOE interface, then the evaluator shall devise a test that ensures that the key recovery capability has been or can be disabled following the guidance provided by the vendor.

Test 4 (conditional): If the TOE provides the ability to configure the power saving states that are entered by certain events, the evaluator shall devise a test that causes the TOE to enter a specific power saving state, configure the TSF so that this activity causes a different state to be entered, repeat the activity, and observe the new state is entered as configured.

Test 5 (conditional): If the TOE provides the ability to disable the use of one or more power saving states, the evaluator shall devise a test that enables all supported power saving states and demonstrates that the TOE can enter into each of these states. The evaluator shall then disable the supported power saving states one by one, repeating the same set of actions that were performed at the start of the test, and observe each time that when a power saving state is configured to no longer be used, none of the behavior causes the disabled state to be entered.

Testing for item d) is performed in conjunction with FPT_TUD_EXT.1 testing. The ST selects “no other functions” for item e) in FMT_SMF.1. Therefore, none of these tests are applicable.

3.3.3 Specification of Management Functions (FMT_SMF.1/EE) ([EE])

3.3.3.1 TSS Activities

If item a) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE changes the DEK.

Section 7.3.3 of [ST] (“FMT_SMF.1: Specification of Management Functions (FDE_EE)”) states the administrator changes the DEK in accordance with FCS_CKM.1 through use of the `volume encryption rekey` command.

If item b) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes how the TOE cryptographically erases the DEK.

Section 7.3.3 of [ST] states the administrator instructs the TOE to cryptographically erase the DEK in accordance with FCS_CKM.4(a) through use of the `volume delete` command.

If item c) is selected in FMT_SMF.1.1: The evaluator shall ensure the TSS describes the process to initiate TOE firmware/software updates.

Section 7.3.3 of [ST] states the administrator initiates firmware/software updates through use of the `cluster image update` command.

© 2024 Leidos. All rights reserved

If item d) is selected in FMT_SMF.1.1: If additional management functions are claimed in the ST, the evaluator shall verify that the TSS describes those functions.

The ST does not claim any additional management functions.

3.3.3.2 Guidance Activities

If item a) is selected in FMT_SMF.1.1: The evaluator shall review the AGD guidance and shall determine that the instructions for changing a DEK exist. The instructions must cover all environments on which the TOE is claiming conformance, and include any preconditions that must exist in order to successfully generate or re-generate the DEK.

[CCCG] Section 2.5.1 "Request Change of a Volume's DEK" provides the instructions to initiate a change to the DEK.

While in CC mode, ONTAP volumes are automatically encrypted using AES-XTS-256 DEKs. Volumes can be either be rekeyed “in-place” or “migrated” to use a new AES-XTS-256 DEK.

In-place rekeying is performed with the `volume encryption rekey` set of commands. See the CLI command volume encryption rekey in [ONTAP CR].

If item c) is selected in FMT_SMF.1.1: The evaluator shall examine the operational guidance to ensure that it describes how to initiate TOE firmware/software updates.

[CCCG] Section 2.5.4 "Initiate ONTAP Software Updates" states that ONTAP cluster admins are allowed to update the TOE via the `cluster image update` CLI command. ONTAP CC updates are cryptographically signed using a 3072-bit RSA digital signature on SHA-384 hashes.

If item d) is selected in FMT_SMF.1.1: Default Authorization Factors: It may be the case that the TOE arrives with default authorization factors in place. If it does, then the selection in item D must be made so that there is a mechanism to change these authorization factors. The operational guidance shall describe the method by which the user changes these factors when they are taking ownership of the device. The TSS shall describe the default authorization factors that exist.

Disable Key Recovery: The guidance for disabling this capability shall be described in the AGD documentation.

The ST does not claim any additional management functions.

3.3.3.3 KMD Activities

If item d) is selected in FMT_SMF.1.1: If the TOE offers the functionality to import an encrypted DEK, the evaluator shall ensure the KMD describes how the TOE imports a wrapped DEK and performs the decryption of the wrapped DEK.

The ST does not claim any additional management functions.

3.3.3.4 Test Activities

If item a) and/or b) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to change and cryptographically erase the DEK (effectively removing the ability to retrieve previous user data).

© 2024 Leidos. All rights reserved

Covered by testing under FMT_SMF.1 (cPP_FDE_AA_V2.0E).

If item c) is selected in FMT_SMF.1.1: The evaluator shall verify that the TOE has the functionality to initiate TOE firmware/software updates.

This test is performed in conjunction with FPT_TUD_EXT.1.

If item d) is selected in FMT_SMF.1.1: If additional management functions are claimed, the evaluator shall verify that the additional features function as described.

This test is not applicable because d) is not selected by the ST.

3.3.4 Security Roles (FMT_SMR.1) ([AA])

3.3.4.1 TSS Activities

There are no TSS evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.

3.3.4.2 Guidance Activities

There are no guidance evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.

3.3.4.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.3.4.4 Test Activities

There are no test evaluation activities for this SFR. Evaluation of this SFR is performed as part of evaluating FMT_MOF.1 and FMT_SMF.1.

3.4 Protection of the TSF (FPT)

3.4.1 Protection of Key and Key Material (FPT_KYP_EXT.1) ([AA], [EE])

3.4.1.1 TSS Activities

Modified in accordance with TD0458.

The evaluator shall examine the TSS and verify it identifies the methods used to protect keys stored in non-volatile memory.

Section 7.4.1 of [ST] (“FPT_KYP_EXT.1: Protection of Key and Key Material (FDE_AA)(FDE_EE)”) states the TOE stores keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d) (i.e., only wrapped keys are ever stored in non-volatile memory).

3.4.1.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.4.1.3 KMD Activities

Modified in accordance with TD0458.

© 2024 Leidos. All rights reserved

The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in non-volatile memory. The description of the key chain shall be reviewed to ensure the selected method is followed for the storage of wrapped or encrypted keys in non-volatile memory and plaintext keys in non-volatile memory meet one of the criteria for storage.

Section 2.5 of [KMD] ("Critical Security Parameters Summary") describes the storage location of all keys and how all keys are protected.

All keys and CSPs are stored temporarily as a variable or a CPU register value when being operated on by the TOE. The following are stored in volatile memory in the CryptoMod key table:

- CP-KEK
- CKEK
- SVM-KEK
- VDEK.

The following are stored in non-volatile memory in the OKM database and/or an RDB table:

- CP-Salt—does not require confidentiality protection
- CP-Hash—does not require confidentiality protection
- Cluster-Salt—does not require confidentiality protection
- wCKEK—cryptographically wrapped using CP-KEK as the wrapping key
- wSVM-KEK—cryptographically wrapped using CKEK as the wrapping key

KMD Section 2.2 states that the following are stored in non-volatile memory on the WAFL on-disk data structure:

- wVDEK—cryptographically wrapped using SVM-KEK as the wrapping key.

3.4.1.4 Test Activities

There are no test evaluation activities for this SFR.

3.4.2 Power Saving States (FPT_PWR_EXT.1) ([AA])

3.4.2.1 TSS Activities

The evaluator shall validate the TSS contains a list of Compliant power saving states.

Section 7.4.2 of [ST] ("FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States (FDE_AA) (FDE_EE)") states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off).

3.4.2.2 Guidance Activities

The evaluator shall ensure that guidance documentation contains a list of Compliant power saving states. If additional power saving states are supported, then the evaluator shall validate that the guidance documentation states how non-Compliant power states are disabled.

Section 7.4.2 of [ST] states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). It further states the TOE must be fully rebooted from each Compliant power saving

© 2024 Leidos. All rights reserved

state. As such, the TOE is either operational, or is in a state that requires it to be fully rebooted in order to resume operation, and there are no other power saving states, Compliant or otherwise.

[CCCG] Section 2.4 "Compliant Power Saving States" states that the TOE enters the G3 (mechanical off) state when a cluster admin removes the node's power via a mechanical switch. Only an authorized cluster admin can execute the command (`system halt`) for the G2(S5) Compliant power saving state.

When either Compliant power saving state is entered, non-persistent/unencrypted BEV and DEK key material is destroyed.

An administrator can reboot the TOE via the `system node reboot` CLI command. See the CLI command `system node reboot` in [ONTAP CR].

3.4.2.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.4.2.4 Test Activities

The evaluator shall confirm that for each listed compliant state all key/key materials are removed from volatile memory by using the test defined in FCS_CKM.4(d).

The evaluator repeated the test defined in FCS_CKM.4(d) by testing for volatile keys after a soft reboot and hard power cycle and confirmed that the no traces of the full or partial key remained for each case.

3.4.3 Power Saving States (FPT_PWR_EXT.1) ([EE])

3.4.3.1 TSS Activities

The evaluator shall validate the TSS contains a list of Compliant power saving states.

Section 7.4.2 of [ST] ("FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States (FDE_AA) (FDE_EE)") states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off).

3.4.3.2 Guidance Activities

Modified in accordance with TD0460.

The evaluator shall ensure that guidance documentation contains a list of Compliant power saving states. If additional power saving states are supported, then the evaluator shall validate that the guidance documentation states how the use of non-Compliant power saving states are disabled.

Section 7.4.2 of [ST] states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). It further states the TOE must be fully rebooted from each Compliant power saving state. As such, the TOE is either operational, or is in a state that requires it to be fully rebooted in order to resume operation, and there are no other power saving states, Compliant or otherwise.

[CCCG] Section 2.4 "Compliant Power Saving States" states that the TOE enters the G3 (mechanical off) state when a cluster admin removes the node's power via a mechanical switch. Only an authorized cluster admin can execute the command (system halt) for the G2(S5) Compliant power saving state.

When either Compliant power saving state is entered, non-persistent/unencrypted BEV and DEK key material is destroyed.

© 2024 Leidos. All rights reserved

When the TOE is fully rebooted from either Compliant power saving state is entered, non-persistent/unencrypted BEV and DEK key material contained within volatile memory is cleared within 30 seconds of the system halting.

An administrator can reboot the TOE via the `system node reboot` CLI command. See the CLI command `system node reboot` in [ONTAP CR].

3.4.3.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.4.3.4 Test Activities

The evaluator shall confirm that for each listed Compliant state all key/key materials are removed from volatile memory by using the test indicated by the selection in FCS_CKM_EXT.6.

This test is performed in conjunction with FPT_PWR_EXT.1/AA.

3.4.4 Timing of Power Saving States (FPT_PWR_EXT.2/AA) ([AA])

3.4.4.1 TSS Activities

The evaluator shall validate that the TSS contains a list of conditions under which the TOE enters a Compliant power saving state.

Section 7.4.2 of [ST] ("FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States") states the TOE enters the G3 (mechanical off) state when the administrator removes the device's power via a mechanical switch, and enters the G2 (S5) (soft off) state when an authorized user executes the `system halt` command.

The TOE must be fully rebooted from each Compliant power saving state.

3.4.4.2 Guidance Activities

The evaluator shall check that the guidance contains a list of conditions under which the TOE enters a Compliant power saving state. Additionally, the evaluator shall verify that the guidance documentation states whether unexpected power-loss events may result in entry to a non-Compliant power saving state and, if that is the case, validate that the documentation contains information on mitigation measures.

Section 7.4.2 of [ST] states the TOE provides the Compliant power saving states of G2(S5) (soft off) and G3 (mechanical off). It further states the TOE must be fully rebooted from each Compliant power saving state. As such, the TOE is either operational, or is in a state that requires it to be fully rebooted in order to resume operation, and there are no other power saving states, Compliant or otherwise.

[CCCG] Section 2.4 "Compliant Power Saving States" states that the TOE enters the G3 (mechanical off) state when a cluster admin removes the node's power via a mechanical switch. Only an authorized cluster admin can execute the command (`system halt`) for the G2(S5) Compliant power saving state.

When either Compliant power saving state is entered, non-persistent/unencrypted BEV and DEK key material is destroyed.

3.4.4.3 KMD Activities

There are no KMD evaluation activities for this SFR.

© 2024 Leidos. All rights reserved

3.4.4.4 Test Activities

The evaluator shall trigger each condition in the list of identified conditions and ensure the TOE ends up in a compliant power saving state by running the test identified in FCS_CKM.4(d).

The evaluator tested the TOE can transition to both compliant power saving states in conjunction with FPT_PWR_EXT.1/AA.

3.4.5 Timing of Power Saving States (FPT_PWR_EXT.2/EE) ([EE])

3.4.5.1 TSS Activities

The evaluator shall validate that the TSS contains a list of conditions under which the TOE enters a Compliant power saving state.

Section 7.4.2 of [ST] ("FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States (FDE_AA) (FDE_EE)") states the TOE enters the G3 (mechanical off) state when the administrator removes the device's power via a mechanical switch, and enters the G2 (S5) (soft off) state when an authorized user executes the `system halt` command.

The TOE must be fully rebooted from each Compliant power saving state.

3.4.5.2 Guidance Activities

The evaluator shall check that the guidance contains a list of conditions under which the TOE enters a Compliant power saving state. Additionally, the evaluator shall verify that the guidance documentation provides information on how long it is expected to take for the TOE to fully transition into the Compliant power saving state (e.g. how many seconds for the volatile memory to be completely cleared).

[CCCG] Section 2.4 "Compliant Power Saving States" states that the TOE enters the G3 (mechanical off) state when a cluster admin removes the node's power via a mechanical switch. Only an authorized cluster admin can execute the command (`system halt`) for the G2(S5) Compliant power saving state.

When either Compliant power saving state is entered, non-persistent/unencrypted BEV and DEK key material is destroyed.

When the TOE is fully rebooted from either Compliant power saving state is entered, non-persistent/unencrypted BEV and DEK key material contained within volatile memory is cleared within 30 seconds of the system halting.

An administrator can reboot the TOE via the `system node reboot` CLI command. See the CLI command `system node reboot` in [ONTAP CR].

3.4.5.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.4.5.4 Test Activities

The evaluator shall trigger each condition in the list of identified conditions and ensure the TOE ends up in a Compliant power saving state by using the test indicated by the selection in FCS_CKM_EXT.6.

The evaluator tested the TOE can transition to both compliant power saving states in conjunction with FPT_PWR_EXT.1/AA.

© 2024 Leidos. All rights reserved

3.4.6 TSF Testing (FPT_TST_EXT.1) ([EE])

3.4.6.1 TSS Activities

The evaluator shall verify that the TSS describes the known-answer self-tests for cryptographic functions.

Section 7.4.3 of [ST] ("FPT_TST_EXT.1: TSF Testing (FDE_AA) (FDE_EE)") include the following known-answer tests:

- AES-128 CBC, AES-256 CBC – encryption/decryption test
- DRBG – Tested per SP800-90A, including the Health Testing identified in Section 11.3.
- HMAC SHA-512 - keyed-hash message authentication code test
- PBKDF2 - Password-Based Key Derivation Function 2 test
- SHA-1, SHA-256, SHA-384, SHA-512 - hashing test
- XTS-AES-128, XTS-AES-256 – AES encryption/decryption
- RSA Signature Generation/Verification – 2048 bits and 3072 bits.

The evaluator shall verify that the TSS describes, for some set of non-cryptographic functions affecting the correct operation of the TOE and the method by which the TOE tests those functions. The evaluator shall verify that the TSS includes each of these functions, the method by which the TOE verifies the correct operation of the function. The evaluator shall verify that the TSF data are appropriate for TSF Testing. For example, more than blocks are tested for AES in CBC mode, output of AES in GCM mode is tested without truncation, or 512-bit key is used for testing HMAC-SHA-512.

Section 7.4.3 of [ST] describes the software integrity test performed by the TOE. During power-on self-testing, the module performs a self-integrity check and compares the results against the build time generated hash digests. During power on, the bootloader validates the whitelist database of secure boot keys with the signature associated with each module that is loaded. After each module is validated and loaded, the boot process continues with the ONTAP initialization. If signature validation fails for any module, the system reboots.

If FCS_RBG_EXT.1 is implemented by the TOE and according to NIST SP 800-90, the evaluator shall verify that the TSS describes health tests that are consistent with section 11.3 of NIST SP 800-90.

Section 7.4.3 of [ST] states the TOE's DRBG implementation is tested in accordance with SP 800-90A, including the Health Tests identified in Section 11.3.

If any FCS_COP functions are implemented by the TOE, the TSS shall describe the known-answer self-tests for those functions.

Section 7.4.3 of [ST] describes the known-answer self-tests for algorithms specified in the FCS_COP.1 requirements, as follows:

- FCS_COP.1(a): RSA signature generation and verification with 2048 and 3072 bit keys
- FCS_COP.1(b): SHA-384 and SHA-512
- FCS_COP.1(c): HMAC-SHA-512

© 2024 Leidos. All rights reserved

- FCS_COP.1(d): not applicable – key wrap with padding uses AES, which is covered in other testing
- FCS_COP.1(f): XTS-AES-128 and XTS-AES-256
- FCS_COP.1(g): AES-128 CBC, AES-256 CBC.

The evaluator shall verify that the TSS describes, for some set of non-cryptographic functions affecting the correct operation of the TSF, the method by which those functions are tested. The TSS will describe, for each of these functions, the method by which correct operation of the function/component is verified. The evaluator shall determine that all of the identified functions/components are adequately tested on start-up.

Section 7.4.3 of [ST] describes the software integrity test performed by the TOE. During power-on self-testing, the module performs a self-integrity check and compares the results against the build time generated hash digests. During power on, the bootloader validates the whitelist database of secure boot keys with the signature associated with each module that is loaded. After each module is validated and loaded, the boot process continues with the ONTAP initialization. If signature validation fails for any module, the system reboots.

3.4.6.2 Guidance Activities

There are no AGD evaluation activities for this SFR.

3.4.6.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.4.6.4 Test Activities

There are no test evaluation activities for this SFR.

3.4.7 Trusted Update (FPT_TUD_EXT.1) ([AA], [EE])

3.4.7.1 TSS Activities

The evaluator shall examine the TSS to ensure that it describes information stating that an authorized source signs TOE updates and will have an associated digital signature. The evaluator shall examine the TSS contains a definition of an authorized source along with a description of how the TOE uses public keys for the update verification mechanism in the Operational Environment. The evaluator ensures the TSS contains details on the protection and maintenance of the TOE update credentials.

Section 7.4.4 of [ST] ("FPT_TUD_EXT.1: Trusted Update (FED_AA)(FDE_EE)") states NetApp code signing ensures that TOE images installed through non-disruptive image updates or automated non-disruptive image updates are authentically produced by NetApp and have not been tampered with. The NetApp updates are cryptographically signed using a RSA Digital Signature algorithm with a key size of 3072-bits with a SHA-384 signature. The TOE will verify the signature before installing the update and reject any update with an invalid signature. The private key used for code signing is stored in a limited access hardware security module at NetApp. If the TOE's public keys are tampered with, then an update will fail.

If the Operational Environment performs the signature verification, then the evaluator shall examine the TSS to ensure it describes, for each platform identified in the ST, the interface(s) used by the TOE to invoke this cryptographic functionality.

© 2024 Leidos. All rights reserved

All cryptographic operations, including signature verification, are performed by the TOE.

3.4.7.2 Guidance Activities

The evaluator ensures that the operational guidance describes how the TOE obtains vendor updates to the TOE; the processing associated with verifying the digital signature of the updates (as defined in FCS_COP.1(a)); and the actions that take place for successful and unsuccessful cases.

[CCCG] Section 2.5.4 "Initiate ONTAP Software Updates" states that ONTAP cluster admins are allowed update the TOE via the `cluster image update` CLI command. ONTAP CC updates are cryptographically signed using a 3072-bit RSA digital signature on SHA-384 hashes. If the signature validation fails, then the update is stopped and, an error message is displayed ("Failed to verify the signatures of the image. The image might have been corrupted. Replace the image, and then try the command again.").

For specific instructions on how to update the TOE, refer to [SUUR].

3.4.7.3 KMD Activities

There are no KMD evaluation activities for this SFR.

3.4.7.4 Test Activities

The evaluators shall perform the following tests (if the TOE supports multiple signatures, each using a different hash algorithm, then the evaluator performs tests for different combinations of authentic and unauthentic digital signatures and hashes, as well as for digital signature alone):

Test 1: The evaluator performs the version verification activity to determine the current version of the TOE. After the update tests described in the following tests, the evaluator performs this activity again to verify that the version correctly corresponds to that of the update.

The evaluator verified the version of the TOE then initiated a TOE update. The evaluator confirmed that the TOE successfully accepted the update and confirmed that the version number had incremented to the expected number.

Test 2: The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that an update successfully installs on the TOE. The evaluator shall perform a subset of other evaluation activity tests to demonstrate that the update functions as expected.

After updating the TOE the evaluator created a new administrative user. That user was then used to create a new encrypted volume on the TOE.

© 2024 Leidos. All rights reserved

4 Security Assurance Requirements

4.1 ASE: Security Targeted Evaluation

An evaluation activity is defined here for evaluation of Exact Conformance claims against a cPP in a Security Target. Other aspects of ASE remain as defined in the CEM.

4.1.1 Conformance Claims (ASE_CCL.1)

The table below indicates the actions to be taken for particular ASE_CCL.1 elements in order to determine exact conformance with a cPP.

ASE_CCL.1 element	Evaluation Action
ASE_CCL.1.8C	The evaluator shall check that the statements of security problem definition in the PP and ST are identical.
ASE_CCL.1.9C	The evaluator shall check that the statements of security objectives in the PP and ST are identical.
ASE_CCL.1.10C	The evaluator shall check that the statements of security requirements in the ST include all the mandatory SFRs in the cPP, and all of the selection-based SFRs that are entailed by selections made in other SFRs (including any SFR iterations added in the ST). The evaluator shall check that if any other SFRs are present in the ST (apart from iterations of SFRs in the cPP) then these are taken only from the list of optional SFRs specified in the cPP (the cPP will not necessarily include optional SFRs, but may do so). If optional SFRs from the cPP are included in the ST then the evaluator shall check that any selection-based SFRs entailed by the optional SFRs adopted are also included in the ST.

4.1.1.1 ASE_CCL.1.8C

Section 4 of [ST] includes by reference the security problem definition from [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. As such, the security problem definition in [ST] is identical to the statement of security problem definition specified in [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E].

4.1.1.2 ASE_CCL.1.9C

Section 5 of [ST] includes by reference the statement of security objectives from [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E]. As such, the statement of security objectives in [ST] is identical to the statement of security objectives specified in [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E].

4.1.1.3 ASE_CCL.1.10C

Section 6 of [ST] indicates that security functional requirements included in the ST are drawn from [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E].

The evaluator examined the requirements specified in Section 6 of [ST] and confirmed the following:

- All mandatory functional requirements from [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] are included in [ST] through reproduction. This includes one requirement (FPT_TST_EXT.1) that is optional in [CPP_FDE_AA_V2.0E], but mandatory in [CPP_FDE_EE_V2.0E]

© 2024 Leidos. All rights reserved

- All selection-based requirements from [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] indicated by selections made in the mandatory requirements are included in [ST] through reproduction
- No requirements not specified in [CPP_FDE_AA_V2.0E] or [CPP_FDE_EE_V2.0E] have been specified in [ST].

4.2 Development (ADV)

4.2.1 Basic Functional Specification (ADV_FSP.1)

The EAs for this assurance component focus on understanding the interfaces (e.g., application programing interfaces, command line interfaces, graphical user interfaces, network interfaces) described in the AGD documentation, and possibly identified in the TOE Summary Specification (TSS) in response to the SFRs. Specific evaluator actions to be performed against this documentation are identified (where relevant) for each SFR in Section 2 (*Evaluation Activities for SFRs*), and in EAs for AGD, ATE and AVA SARs in other parts of Section 5.

The EAs presented in this section address the CEM work units ADV_FSP.1- 1, ADV_FSP.1-2, ADV_FSP.1-3, and ADV_FSP.1-5.

The EAs are reworded for clarity and interpret the CEM work units such that they will result in more objective and repeatable actions by the evaluator. The EAs in this SD are intended to ensure the evaluators are consistently performing equivalent actions.

The documents to be examined for this assurance component in an evaluation are therefore the Security Target, AGD documentation, and any required supplementary information required by the cPP: no additional "functional specification" documentation is necessary to satisfy the EAs. The interfaces that need to be evaluated are also identified by reference to the EAs listed for each SFR, and are expected to be identified in the context of the Security Target, AGD documentation, and any required supplementary information defined in the cPP rather than as a separate list specifically for the purposes of CC evaluation. The direct identification of documentation requirements and their assessment as part of the EAs for each SFR also means that the tracing required in ADV_FSP.1.2D (work units ADV_FSP.1-4, ADV_FSP.1-6 and ADV_FSP.1-7) is treated as implicit and no separate mapping information is required for this element.

4.2.1.1 Evaluation Activity

The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.

In this context, TSFI are deemed security relevant if they are used by the administrator to configure the TOE, or to perform other administrative functions (e.g. audit review or performing updates). Additionally, those interfaces that are identified in the ST, or guidance documentation, as adhering to the security policies (as presented in the SFRs), are also considered security relevant. The intent is that these interfaces will be adequately tested, and having an understanding of how these interfaces are used in the TOE is necessary to ensure proper test coverage is applied.

The set of TSFI that are provided as evaluation evidence are contained in the Administrative Guidance and User Guidance.

Through review of [ST] and [ONTAP CR], the evaluation team identified that the CLI is the only security relevant TSFI. In particular, the following CLI commands are specifically identified in [ST] and were exercised during testing:

© 2024 Leidos. All rights reserved

- system halt
- system node image update
- security key-manager onboard disable
- security key-manager onboard enable
- storage encryption disk sanitize
- storage encryption disk destroy
- security key-manager onboard update-passphrase
- cluster image update
- cluster image show
- version
- volume encryption rekey.

The evaluation team determined the interface documentation described the purpose and method of use for each TSFI identified as being security relevant, sufficient to enable each of the evaluation activities to be completed satisfactorily. The evaluation team's results from performing the evaluation activities are documented in Section 3 of this AAR.

4.2.1.2 Evaluation Activity

The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.

The evaluation team determined the interface documentation identified and described the parameters for each TSFI identified as being security relevant, sufficient to enable each of the evaluation activities to be completed satisfactorily. The evaluation team's results from performing the evaluation activities are documented in Section 3 of this AAR.

4.2.1.3 Evaluation Activity

The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.

The evaluator uses the provided documentation and first identifies, and then examines a representative set of interfaces to perform the EAs presented in Section 2 (*Evaluation Activities for SFRs*), including the EAs associated with testing of the interfaces.

It should be noted that there may be some SFRs that do not have an interface that is explicitly "mapped" to invoke the desired functionality. For example, generating a random bit string, destroying a cryptographic key that is no longer needed, or the TSF failing to a secure state, are capabilities that may be specified in SFRs, but are not invoked by an interface.

However, if the evaluator is unable to perform some other required EA because there is insufficient design and interface information, then the evaluator is entitled to conclude that an adequate functional specification has not been provided, and hence that the verdict for the ADV_FSP.1 assurance component is a 'fail'.

The evaluation team examined the interface documentation and was able to map interfaces to SFRs, sufficient to enable each of the evaluation activities to be completed satisfactorily. The evaluation team's results from performing the evaluation activities are documented in Section 3 of this AAR.

© 2024 Leidos. All rights reserved

4.3 Guidance Documents (AGD)

It is not necessary for a TOE to provide separate documentation to meet the individual requirements of AGD_OPE and AGD_PRE. Although the Evaluation Activities in this section are described under the traditionally separate AGD families, the mapping between real TOE documents and AGD_OPE and AGD_PRE requirements may be many-to-many, as long as all requirements are met in documentation that is delivered to administrators and users (as appropriate) as part of the TOE.

4.3.1 Operational User Guidance (AGD_OPE.1)

Specific requirements and checks on the user guidance documentation are identified (where relevant) in the individual Evaluation Activities for each SFR, and for some other SARs (e.g. ALC_CMC.1).

4.3.1.1 Evaluation Activity

The evaluator shall check the requirements below are met by the operational guidance. It should be noted that operational guidance may take the form of an "integrator's guide", where the TOE developer provides a description of the interface (e.g., commands that the Host Platform may invoke to configure a SED).

Operational guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.

The guidance documentation specific to the evaluation is identified in Section 3 of [ST]. The NIAP portal provides the documentation in .PDF format.

Operational guidance must be provided for every Operational Environment that the TOE supports as claimed in the Security Target and must adequately address all platforms claimed for the TOE in the Security Target. This may be contained all in one document.

The ST identifies the TOE is supported on a range of Fibre Attached Storage (FAS) and All Flash FAS (AFF) network storage controllers, but the same TOE software runs on each controller. As such, the guidance documentation adequately addresses all platforms claimed for the TOE in the ST.

The contents of the operational guidance will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in sections 2, 3, and 4 above.

In addition to SFR-related Evaluation Activities, the following information is also required.

- The operational guidance shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
- The operational guidance shall describe how to configure the IT environments that are supported to shut down after an administratively defined period of inactivity.
- The operational guidance shall identify system "sleeping" states for all supported operating environments and for each environment, provide administrative guidance on how to disable the sleep state. As stated above, the TOE developer may be providing an integrator's guide and "power states" may be an abstraction that SEDs provide at various levels – e.g., may simply provide a command that the Host Platform issues to manage the state of the device, and the Host Platform is responsible for providing a more sophisticated power management scheme.

© 2024 Leidos. All rights reserved

- The TOE will likely contain security functionality that does not fall under the scope of evaluation under this cPP. The operational guidance shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.

The cryptographic modules included in the TOE do not require any configuration, and the TOE does not incorporate any unevaluated cryptographic module. The guidance documentation identifies and describes commands used to place the TOE into its Common Criteria mode of operation and the need to enable the Onboard Key Manager when using the product in its evaluated configuration.

4.3.2 Preparative Procedures (AGD_PRE.1)

As for the operational guidance, specific requirements and checks on the preparative procedures are identified (where relevant) in the individual Evaluation Activities for each SFR.

4.3.2.1 Evaluation Activity

The evaluator shall check the requirements below are met by the preparative procedures.

The contents of the preparative procedures will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in section 2 above.

Preparative procedures shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.

The guidance documentation specific to the evaluation is identified in Section 3 of [ST]. The NIAP portal provides the documentation in .PDF format.

The contents of the preparative procedures will be verified by the Evaluation Activities defined below and as appropriate for each individual SFR in section 2 above.

In addition to SFR-related Evaluation Activities, the following information is also required.

Preparative procedures must include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target). The documentation should be in an informal style and should be written with sufficient detail and explanation that they can be understood and used by the target audience (which will typically include IT staff who have general IT experience but not necessarily experience with the TOE itself).

The vendor provides guides for installing each of the storage controllers identified in [ST] as part of the evaluated configuration. The guides are listed at the NIAP portal.

The guides also provide preparative procedures for configuring ONTAP. Guidance covers how the administrator verifies the operational environment can fulfil its role to support the security functionality.

Preparative procedures must be provided for every Operational Environment that the TOE supports as claimed in the Security Target and must adequately address all platforms claimed for the TOE in the Security Target. This may be contained all in one document.

The ST identifies the TOE is supported on a range of Fibre Attached Storage (FAS) and All Flash FAS (AFF) network storage controllers, but the same TOE software runs on each controller. As such, the guidance documentation adequately addresses all platforms claimed for the TOE in the ST.

© 2024 Leidos. All rights reserved

The preparative procedures must include

- instructions to successfully install the TSF in each Operational Environment; and
- instructions to manage the security of the TSF as a product and as a component of the larger operational environment; and
- instructions to provide a protected administrator capability.

The vendor provides guides for installing each of the storage controllers identified in [ST] as part of the evaluated configuration. The guides are listed at the NIAP portal.

The [CCCG] and the guides also provide preparative procedures for configuring ONTAP.

The guidance includes instructions for managing the security of the TOE as a product and as a component of the operational environment and provides instructions for providing a protected administrator capability.

The guides also provide preparative procedures for configuring ONTAP. Guidance covers how the administrator verifies the operational environment can fulfil its role to support the security functionality.

4.4 Life-Cycle Support (ALC)

4.4.1 Labeling of the TOE (ALC_CMC.1)

When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.

4.4.2 TOE CM Coverage (ALC_CMS.1)

When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.

4.5 Tests (ATE)

4.5.1 Independent Testing Conformance (ATE_IND.1)

Testing is performed to confirm the functionality described in the TSS as well as the operational guidance documentation. The focus of the testing is to confirm that the requirements specified in the SFRs are being met.

The evaluator should consult Appendix B FDE Equivalency Considerations when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.

The SFR-related Evaluation Activities in the SD identify the specific testing activities necessary to verify compliance with the SFRs. The tests identified in these other Evaluation Activities constitute a sufficient set of tests for the purposes of meeting ATE_IND.1.2E. It is important to note that while the Evaluation Activities identify the testing that is necessary to be performed, the evaluator is responsible for ensuring that the interfaces are adequately tested for the security functionality specified for each SFR.

Evaluation Activity: The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.

© 2024 Leidos. All rights reserved

The evaluator received the TOE from the vendor and confirmed that it conforms to the hardware, configuration and firmware described in the ST.

Evaluation Activity: The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state

The evaluator received the TOE from the vendor and powered it on. The evaluator confirmed it presented no errors and entered a running state. The evaluator performed a version and model verification activity prior to testing.

Evaluation Activity: The evaluator shall prepare a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. While it is not necessary to have one test case per test listed in an Evaluation Activity, the evaluator must show in the test plan that each applicable testing requirement in the SFR-related Evaluation Activities is covered.

The test plan identifies the platforms to be tested, and for any platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition and configuration of each platform to be tested, and any setup actions that are necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of any cryptographic engine to be used (e.g. for cryptographic protocols being evaluated).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives, and the expected results.

The test report (which could just be an updated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure, so that a fix was then installed and then a successful re-run of the test was carried out, then the report would show a “fail” result followed by a “pass” result (and the supporting details), and not just the “pass” result.

The evaluator prepared a test plan prior to testing outlining the required test activities to be performed. Throughout testing the test plan was updated with results to eventually become the test report.

The test plan laid out a subset of all instances of the TOE in the evaluation to be tested. Similar instances of the TOE were grouped together based on hardware. Each instance of the TOE did not have any variations with software dependencies, software binaries, libraries used, management interfaces or functional differences so hardware only needed to be considered. When an instance or instances of the TOE were not tested justification was provided in the test report via equivalency rationale.

The test report lists each instance of the TOE tested for each SFR and details it as defined in the ST.

© 2024 Leidos. All rights reserved

The test plan established and set of procedures to follow with steps and configuration necessary to achieve the expected result.

The test report describes in detail the activities the evaluator performed along with actual results in the form of evidence to accomplish each test. Each test account is accompanied by a test result in the form of 'pass' or 'fail'. The test report also establishes an overall result for the cumulative test activities stated by a 'pass' or 'fail'.

Independent testing took place from June to October 2024. All testing artifacts were collected during on-site testing at Netapp's facility in Raleigh, North Carolina, from June 24 to June 26, 2024. Due to the requirement to use the vendor's proprietary coretool program to decompress core dumps the analysis of those dumps only took place after artifact collection was complete.

The evaluation team established a test configuration comprising:

- TOE components:
  - ONTAP 9.14.1 installed on following NetApp Storage Encryption appliances:
    - A150
    - A320
    - A400
    - FAS9500
- Test environment components:
  - Kali Linux Server.
  - Microsoft Windows Workstation

4.6 Vulnerability Assessment (AVA)

4.6.1 Vulnerability Survey (AVA_VAN.1)

While vulnerability analysis is inherently a subjective activity, a minimum level of analysis can be defined and some measure of objectivity and repeatability (or at least comparability) can be imposed on the vulnerability analysis process. In order to achieve such objectivity and repeatability it is important that the evaluator follows a set of well-defined activities, and documents their findings so others can follow their arguments and come to the same conclusions as the evaluator. While this does not guarantee that different evaluation facilities will identify exactly the same type of vulnerabilities or come to exactly the same conclusions, the approach defines the minimum level of analysis and the scope of that analysis, and provides Certification Bodies a measure of assurance that the minimum level of analysis is being performed by the evaluation facilities.

4.6.1.1 Evaluation Activity

The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components apply to all systems claimed in the ST, and should identify at a minimum the processors used by the TOE. Software components include any libraries used by the TOE, such as cryptographic libraries. This additional documentation is merely a list of the name and version number of the components, and will be used by the evaluators in formulating hypotheses during their analysis.

The evaluator shall examine the documentation outlined below provided by the vendor to confirm that it contains all required information. This documentation is in addition to the documentation already required to be supplied in response to the EAs listed previously.

© 2024 Leidos. All rights reserved

The TOE consists of NetApp Volume Encryption (NVE) Appliances running ONTAP 9.14.1. The NetApp controllers included in the evaluated configuration are as follows:

NetApp Controllers Covered by the Evaluation

NetApp Controllers	Disk Type	Controller Form Factor
AFF A150	SSD	2U/24 internal drives
AFF A220	SSD	2U/24 internal drives
AFF A250	NVMe/SSD	2U/24 internal drives
AFF A300	SSD	3U
AFF A320	NVMe	2U
AFF A400	NVMe/SSD	4U
AFF A800	NVMe/SSD	4U/48 internal drives
AFF A900	NVMe/SSD	8U
AFF C190	SSD	2U/24 internal drives
AFF C250	NVMe	2U/24 internal drives
AFF C400	NVME	4U
AFF C800	NVMe	4U
ASA A150	SSD	2U/24 internal drives
ASA A250	NVMe	2U/24 internal drives
ASA A400	NVMe/SSD	4U
ASA A800	NVMe/SSD	4U/48 internal drives
ASA A900	NVMe/SSD	8U
ASA C250	NVMe	2U/24 internal drives
ASA C400	NVMe	4U
ASA C800	NVMe	4U
ASA AFF A220	SSD	2U/24 internal drives
FAS2720	HDD/SSD	2U/12 internal drives
FAS2750	HDD/SSD	2U/24 internal drives
FAS2820	HDD/SSD	2U/12 internal drives
FAS500f	NVMe	2U/24 internal drives
FAS8200	HDD/SSD	3U
FAS8300	HDD/SSD	4U
FAS8700	HDD/SSD	4U
FAS9500	HDD/SSD	8U

The TOE is evaluated on NetApp storage controllers equipped with the following Intel processors:

- Broadwell Xeon D Processor microarchitecture:
  - Intel Xeon D-1557
  - Intel Xeon D-1587
- Skylake Xeon Scalable Processors microarchitecture:
  - Intel Xeon Silver 4114

© 2024 Leidos. All rights reserved

- Intel Xeon Platinum 8160

- Skylake Xeon D Processor microarchitecture:
  - Intel Xeon D-2164-IT

- Cascade Lake 2nd Gen Xeon Scalable Processors microarchitecture:
  - Intel Xeon Silver 4210
  - Intel Xeon Gold 5218
  - Intel Xeon Gold 5220R

- Ice Lake Xeon D Processor microarchitecture:
  - D-1735TR

- Ice Lake 3rd Gen Xeon Scalable Processors microarchitecture:
  - Platinum 8352Y

The TOE includes the following software libraries:

- NetApp Cryptographic Security Module (NCSM v3.0.8)
- NetApp CryptoMod version 2.2.

In addition to the activities specified by the CEM in accordance with Table 2 above, the evaluator shall perform the following activities.

4.6.1.2 Evaluation Activity

The evaluator formulates hypotheses in accordance with process defined in Appendix A.1. The evaluator documents the flaw hypotheses generated for the TOE in the report in accordance with the guidelines in Appendix A.3. The evaluator shall perform vulnerability analysis in accordance with Appendix A.2. The results of the analysis shall be documented in the report according to Appendix A.3.

The evaluation team performed a search of the following public sources of vulnerability information as selected by the iTC:

- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
- National Vulnerability Database: https://nvd.nist.gov/
- US-CERT: http://www.kb.cert.org/vuls/html/search.
- OpenSSL: https://www.openssl.org/news/fips-cve.html

The list of sources above was searched with the following terms:

- General (for all):
  - Product name
  - Underlying components (e.g., OS, software libraries (crypto libraries), chipsets)
  - Drive encryption, disk encryption
  - Key destruction/sanitization

- AA:

© 2024 Leidos. All rights reserved

    - Underlying components (e.g., smart card libraries)
    - Opal management software, SED management software
    - Password caching

- EE:
    - Underlying components (e.g., chipsets, firmware)
    - Opal management software, SED management software
    - Password caching

- For SEDs (for EE):
    - Self Encrypting Drive (SED)
    - OPAL

- For Software FDE (AA or EE):
    - Key caching.

In order to successfully complete this activity, the evaluator will use the developer provided list of all of 3rd party library information that is used as part of their product, along with the version and any other identifying information (this is required in the cPP as part of the ASE_TSS.1.1C requirement). This applies to hardware (including chipsets, etc.) that a vendor utilizes as part of their TOE. This TOE-unique information will be used in the search terms the evaluator uses in addition to those listed above.

The evaluator will also consider the requirements that are chosen and the appropriate guidance that is tied to each requirement. For example, with FCS_AFA_EXT.1, if the Smartcard selection is chosen, then the evaluator will use the appropriate search terms for smart cards.

In order to supplement this list, the evaluators shall also perform a search on the sources listed above to determine a list of potential flaw hypotheses that are more recent that the publication date of the cPPs, and those that are specific to the TOE and its components as specified by the additional documentation mentioned above. Any duplicates – either in a specific entry, or in the flaw hypothesis that is generated from an entry from the same or a different source – can be noted and removed from consideration by the evaluation team.

As part of type 1 flaw hypothesis generation for the specific components of the TOE, the evaluator shall also search the component manufacturer's websites to determine if flaw hypotheses can be generated on this basis (for instance, if security patches have been released for the version of the component being evaluated, the subject of those patches may form the basis for a flaw hypothesis).

These search criteria were applied as follows:

- Product name—the evaluation team searched on the following terms:
    - "netapp"/ "netapp ontap"
    - "ontap"
    - "netapp fas"
    - "netapp aff"
    - "network volume encryption"
- Underlying components—the evaluation team searched on the following terms:
    - "ontap 9.14.1"
    - "OpenSSL 3.0.8 FIPS
    - "Intel ISA-L_crypto v 2.2"
    - "intel storage acceleration library"
    - Solid State drives (SSD) used with the TOE

© 2024 Leidos. All rights reserved

        - AFF A150: KPM6WRUG960G (960GB SAS SSD)
        - AFF A320: MZWLJ3T8HBLS-000G6 (3.8TB NVMe)
        - AFF A400: XS960SE70104 (960GB SAS SSD)
    - Hard Disk Drive (HDD) used with the TOE
        - FAS9500: WUS721010AL5205 (10TB SAS HDD)
    - Third Party Hardware Components available for use with NetApp Controllers
        - Solid State Drives (SSD/SSD-NVMe)
            - MZWLJ3T8HBLS-00AG6 (3.8TB NVMe)
            - MZWLJ15THALA-00AG6 (15.3TB NVMe)
            - XS3840SE70104 (3.8TB SAS SSD)
            - TC58NC1132GTC (3.8TB SAS SSD)
            - XS3840SE70104 (960GB SAS SSD)
            - TC58NC1132GTC (960GB SAS SSD)
        - Hard Drives (SSD/SSD-NVMe)
            - ST1800MM0149 (1.8TB SAS HDD)
            - WUS721010AL5205 (10TB SAS HDD)
- Search terms specified in [CPP_FDE_AA_SD_V2.0E] and [CPP_FDE_AA_SD_V2.0E]—the evaluation team searched on the following terms:
    - “drive encryption”
    - “disk encryption”
    - “key destruction”
    - “key sanitization”
    - “password caching”
    - “key caching”.

The evaluator performed searches of the specified public vulnerability databases on 22 July 2024, 9 September 2024, 24 September 2024, and 8 November 2024.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

© 2024 Leidos. All rights reserved