Encryption Verification Report

Thursday, April 11, 2019
Encryption Verification Report
Media ID: 6140251_A1-12
Encryption Verification Result: **Passed**

This document contains the summary and detailed report of the Encryption Verification Services provided by Ontrack to NetApp. Ontrack's Encryption Verification Services provide an in-depth analysis and verification of customer provided hardware and software. Using advanced laboratory techniques and state-of-the-art proprietary data recovery tools, Ontrack inspects the media to confirm that the target data has been effectively encrypted and/or sanitized.

The goal of this report is to evaluate NetApp's Secure Purge data sanitization product on their All Flash FAS array. NetApp's description of the product is as follows:

> "NetApp ONTAP enabled a command to cryptographically shred deleted files on NVE (NetApp Volume Encryption) volumes by moving good files and deleting the key used to encrypt infected files called Secure Purge. This capability can also be helpful for data spillage—for example, when classified data inadvertently ends up in an unclassified location."

Specific technical and procedural details are included in the remainder of this document. This report can be used to supply vendor-reported information as described in NIST SP800-88 Appendix E.

Ontrack Media Preparation Process

To verify the effectiveness of the sanitization, Ontrack wrote a 0x00 pattern to all the media before placing them in the AFF-A300 filer to establish a known base pattern.

Minimum Sanitization Recommendations – NIST 800-88R1

The tables in Appendix A of the Guidelines for Media Sanitization can be used to determine recommended sanitization of specific media. That recommendation should reflect the FIPS 199 security categorization of the system confidentiality to reduce the impact of harm of unauthorized disclosure of information from the media.

Although use of the tables in Appendix A is recommended, other methods exist to satisfy the intent of Clear, Purge, and Destroy. Methods not specified in this table may be suitable as long as they are verified and found satisfactory by the organization. Not all types of available media are specified in this table. If your media are not included in this guide, organizations are urged to identify and use processes that will fulfill the intent to Clear, Purge, or Destroy their media.

Ontrack Verification Process and Levels of Verification

Ontrack performed the following 4 step process for this verification**.**

- **Unencrypted Data Verification** – Baseline check to ensure that the system and media are performing as expected. System is configured with a single aggregate/volume and known data is written to the system. The drives are then imaged and the aggregate virtually rebuilt using Ontrack's proprietary tools from the disk images to ensure unencrypted data integrity.

- **Encrypted Data Verification** – Second baseline check to ensure that the data written is encrypted.
- **Encrypted Data with Contaminated Data Verification** – Third baseline check to ensure that the contaminated data written to the volume is also encrypted.
- **Secure-Purge Verification** – Full verification to ensure that the contaminated data is not recoverable.

The Ontrack® verification is intended to evidence the independent recognition of a well-known industry leader in Encryption Verification Services for NetApp. This information is provided on an 'as is' basis. Ontrack and assume no direct, indirect or consequential liability to any third party for the information contained in this report. This report does not constitute a recommendation, endorsement or approval of any kind with respect to any product or service and should not be relied upon as such under any circumstances.

About Ontrack

Ontrack provides technology-driven services and software to help legal, corporate and government entities as well as consumers manage, recover, search, analyze, and produce data efficiently and cost-effectively. In addition to its award-winning suite of software, Ontrack provides data recovery, data destruction, electronic discovery and document review. For more information about Ontrack and its offerings please visit: www.ontrack.com or follow @Ontrack on Twitter.

Customer Information			
Company name	NetApp	**Service Order Number**	6140251
Media Information			
Filer Make / Vendor	NetApp	**Filer Model Number**	AFF-A300
System Serial Number:	721653000314	**OS Version**	OnTap 9.4P3
Disk Shelf Model Number	DS224-12	**Disk Shelf Serial Number**	SHFGD1725000233
Drive Make / Vendor	Samsung	**Drive Model**	MZ-ILT960A
Drive S/N(s)	S3SENE0K510671 S3SENY0K305655 S3SENE0K510651 S3SENY0K506583 S3SENE0K510648 S3SENE0K510650 S3SENE0K510639 S3SENY0K506580 S3SENE0K510665 S3SENE0K510640 S3SENE0K510613	**Firmware Version**	NA50

	S3SENY0K305632		
Media Type	SSD	**Media Interface**	12 Gbps SAS
Capacity	960GB	**LBA**	1,875,385,008
External Key Management Server Information			
Tool Used	Gemalto KeySecure 150v	**Revision / Build**	8.9.0
ID	8QN6-68BH-YTK2-P	**Protocol**	KMIP
Sanitization Details			
Method Type	☐Clear ☒ Purge☐ Damage☐Destruct		
Method Used	☐Degauss ☐Overwrite ☐Block Erase ☒Crypto Erase ☐Other:		
Tool Vendor	Secure-Purge	**Revision/Build**	9.4P3
Encryption Verification Details			
Verification Method	Full	**Erasure Pattern**	N/A
Percent Matching Pattern	N/A	**Percent Not Matching Pattern**	N/A
Data Found			N/A
Engineer Comments	☐File System Structures ☐Simulated User Data ☐No Data Found ☒Other (See engineer comments)		

The Level 1 encryption verification result is: Passed

Ontrack installed the AFF-A300 that was provided for this project and then upgraded OnTap to 9.4P3. Ontrack performed the following verification tests to verify that the secure purge data sanitization process removed access to the data.

1) **Unencrypted Data Verification**
   10GB volume UTest1 was created and hydrated with 10 500MB text documents filled with a known pattern. Ontrack then shutdown the system and imaged all 12 disks. These images were loaded into our proprietary tools and verified we were able to trace the file system pointers to the data blocks and view the file data without any decryption needed.

2) **Encrypted Data Verification**
   First, encryption was enabled by configuring an external key manager with the NetApp cluster. A 10GB encrypted volume ETest1 was created and 10 500MB text documents filled with a known pattern were created. Ontrack then shutdown the system and imaged all 12 disks. These images were loaded into our proprietary tools. Ontrack was able to extract the encryption keys from the external key manager listed above and using a custom script supplied by NetApp. These keys were also loaded in our tools and applied to the ETest1 volume. Ontrack was then able to trace the file system pointers to the data blocks and view the unencrypted data.
   NOTE: These data blocks were unreadable without decrypting first.

3) **Encrypted Data with Contaminated Data Verification**
One more 10MB text file with a known pattern was created in the encrypted volume. Once the file was created, Ontrack shutdown the system and imaged all 12 drives. These images along with the encryption keys were loaded in our proprietary tools. Ontrack was again able to follow file system structures to the encrypted volume, decrypt the volume, and view the data blocks including the contaminated file.
NOTE: Please see supporting documents to view the physical location of the data blocks of the contaminated file and our ability to view decrypted data that it contained.

4) **Secure-Purge Verification**
The contaminated file was first deleted and then the secure-purge command was run in accordance to NetApp documentation. Ontrack once again shutdown the system and imaged all 12 drives. Ontrack was able to extract the new encryption keys from the external key manager listed above and using a custom script supplied by NetApp. The new encryption keys and the images were loaded into our proprietary tools. Ontrack was able to follow file system structures to find the ETest1 volume and decrypt it. The volume and its files were in new locations on the disks and the contaminated file was not present.
NOTE: Ontrack was able to go back to the previous physical block location of the contaminated file and the encrypted data was still present but not readable. If users had the original encryption keys, they could be applied, and data recovered.
NOTE: An ASCII search for the contaminated file contents was performed across all images and no unencrypted data was found.
NOTE: In this engagement verification of the Key Management Server was out of scope.

Details on the verification steps can be found in Appendix A.
Additional documentation on the Secure Purge process can be found in Appendix B.

Appendix A – Verification Project Plan

Project Details

- **Equipment Details**
  - Receive FAS and External Key Management Server
    - Model Name: AFF-A300
    - System Serial Number: 721653000314
    - NetApp Release 9.4P3
    - Disk Shelf Model: DS224-12
    - Disk Shelf Serial Number: SHFGD1725000233
    - Media
      - 1.10.0 S3SENE0K510671 894.0GB
      - 1.10.1 S3SENY0K305655 894.0GB
      - 1.10.2 S3SENE0K510651 894.0GB
      - 1.10.3 S3SENY0K506583 894.0GB

      - 1.10.4 S3SENE0K510648 894.0GB
      - 1.10.5 S3SENE0K510650 894.0GB
      - 1.10.6 S3SENE0K510639 894.0GB
      - 1.10.7 S3SENY0K506580 894.0GB
      - 1.10.8 S3SENE0K510665 894.0GB
      - 1.10.9 S3SENE0K510640 894.0GB
      - 1.10.10 S3SENE0K510613 894.0GB
      - 1.10.11 S3SENY0K305632 894.0GB
    - Gemalto Product: KeySecure 150v
      - Box ID: 8QN6-68BH-YTK2-P
      - Software Version: 8.9.0
- **Unencrypted Data Verification Details**
  - Create unencrypted RAID Groups, Aggregate and Volume (UTest1)
    - Vserver Name: data_001
    - Volume Name: UTest1
    - Aggregate Name: aggr1_data_n01
    - List of Aggregates for FlexGroup Constituents: aggr1_data_n01
    - Volume Size: 10GB
    - Volume Data Set ID: 1027
    - Volume Master Data Set ID: 2155614596
    - Volume State: online
    - Volume Style: flex
    - Extended Volume Style: flexvol
    - Is Cluster-Mode Volume: true
    - Is Constituent Volume: false
    - Export Policy: default
    - Security Style: ntfs
    - Junction Path: /UTest1
    - Junction Path Source: RW_volume
    - Junction Active: true
    - Junction Parent Volume: data_001_root
    - Filesystem Size: 10GB
    - Enable Encryption: false
    - Is Volume Encrypted: false
    - Volume Encryption State: none
    - Encryption Key ID: N/A
  - Write test data to the new volume
    - 10 text documents each 500MB in size with a known data pattern
  - Power Down the system
  - Image the disks (base line)

  - Verify can rebuild RAID Groups, Aggregate, Volumes from images
    - After tweaking our tools to accept Ontap 9.4 data structure changes, we were able to load up the images of all 12 drives and find the unencrypted data that is contained in volume UTest1 on aggregate aggr1_data_01
- **Encrypted Data Verification Details**
  - Power on the system
  - Enable NetApp NVE using external key manager

Node	Registered Key Manager
ontrack-netapp-1-01	10.25.5.205
ontrack-netapp-1-02	10.25.5.205

  - Create encrypted volume (ETest1)
    - Vserver Name: data_001
    - Volume Name: ETest1
    - Aggregate Name: aggr1_data_n01
    - List of Aggregates for FlexGroup Constituents: aggr1_data_n01
    - Volume Size: 10GB
    - Volume Data Set ID: 1029
    - Volume Master Data Set ID: 2155614597
    - Volume State: online
    - Volume Style: flex
    - Extended Volume Style: flexvol
    - Is Cluster-Mode Volume: true
    - Is Constituent Volume: false
    - Export Policy: default
    - Security Style: ntfs
    - Junction Path: /ETest1
    - Junction Path Source: RW_volume
    - Junction Active: true
    - Junction Parent Volume: data_001_root
    - Filesystem Size: 10GB
    - Enable Encryption: true
    - Is Volume Encrypted: true
    - Volume Encryption State: full
    - Encryption Key ID: 000000000000000002000000000005000c4fdf518156736bd6c963e949bcb62c0000000000000000
  - Write test data to the new volume
    - 10 text documents each 500MB in size.
  - Extract the A01 key from the Key Manager

    Get Symmetric Key

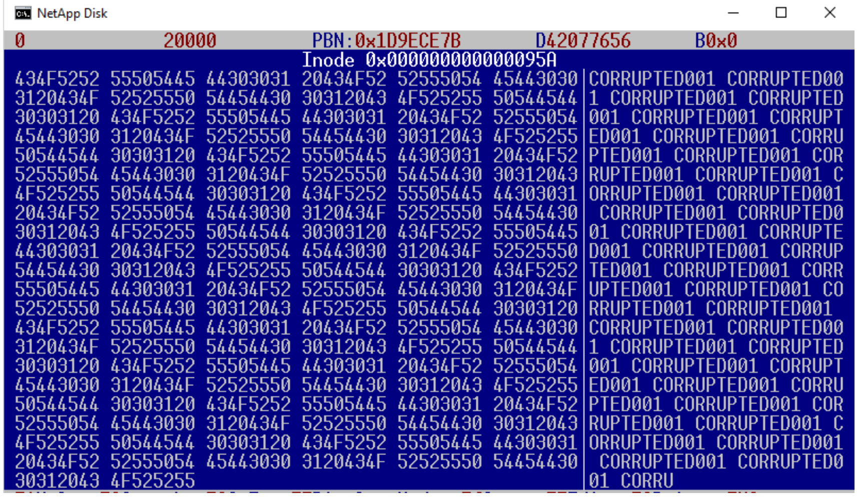
UUID=792744075C0F80D6416E7A472C5404E675930EABD6619188D05C1091E624B413
Key=d427494ad69732a641a396ed0392efd0cfc85ef0b3758626459976cf46307bf3
KeyID=0000000000000000020000000000005000c4fdf518156736bd6c963e949bcb62c0000000000000000

Get Symmetric Key

UUID=20DA6ED877801CA81FD6492C4F7A2AEC5D2D5CD9DD80DF1C717D48D371B5160D
Key=7a529d0c1fcbfd29b61a2ac06ebfdf6f2cf93ddc2885ed3d7f7bbfa92666dc77
KeyID=0000000000000000020000000000005000c4fdf518156736bd6c963e949bcb62c0000000000000000

- Power Down the system
- Image the disks
- Verify can rebuild RAID Groups, Aggregate, Volumes from images
- Decrypt data using the A01 Key
  -

- **Encrypted Data with Contaminated Data Verification Details**
  - Power on the system
  - Add contaminated file data to the encrypted volume
    - Added 1 10MB file was named “Corrupted001“ and fill pattern was as follows:



```
0           20000        PBN:0x1D9ECE7B      D42077656      B0x0
                    Inode 0x000000000000095A
434F5252 55505445 44303031 20434F52 52555054 45443030 |CORRUPTED001 CORRUPTED00
3120434F 52525550 54454430 30312043 4F525255 50544544 |1 CORRUPTED001 CORRUPTED
30303120 434F5252 55505445 44303031 20434F52 52555054 |001 CORRUPTED001 CORRUPT
45443030 3120434F 52525550 54454430 30312043 4F525255 |ED001 CORRUPTED001 CORRU
50544544 30303120 434F5252 55505445 44303031 20434F52 |PTED001 CORRUPTED001 COR
52555054 45443030 3120434F 52525550 54454430 30312043 |RUPTED001 CORRUPTED001 C
4F525255 50544544 30303120 434F5252 55505445 44303031 |ORRUPTED001 CORRUPTED001
20434F52 52555054 45443030 3120434F 52525550 54454430 | CORRUPTED001 CORRUPTED0
30312043 4F525255 50544544 30303120 434F5252 55505445 |01 CORRUPTED001 CORRUPTE
44303031 20434F52 52555054 45443030 3120434F 52525550 |D001 CORRUPTED001 CORRUP
54454430 30312043 4F525255 50544544 30303120 434F5252 |TED001 CORRUPTED001 CORR
55505445 44303031 20434F52 52555054 45443030 3120434F |UPTED001 CORRUPTED001 CO
52525550 54454430 30312043 4F525255 50544544 30303120 |RRUPTED001 CORRUPTED001
434F5252 55505445 44303031 20434F52 52555054 45443030 |CORRUPTED001 CORRUPTED00
3120434F 52525550 54454430 30312043 4F525255 50544544 |1 CORRUPTED001 CORRUPTED
30303120 434F5252 55505445 44303031 20434F52 52555054 |001 CORRUPTED001 CORRUPT
45443030 3120434F 52525550 54454430 30312043 4F525255 |ED001 CORRUPTED001 CORRU
50544544 30303120 434F5252 55505445 44303031 20434F52 |PTED001 CORRUPTED001 COR
52555054 45443030 3120434F 52525550 54454430 30312043 |RUPTED001 CORRUPTED001 C
4F525255 50544544 30303120 434F5252 55505445 44303031 |ORRUPTED001 CORRUPTED001
20434F52 52555054 45443030 3120434F 52525550 54454430 | CORRUPTED001 CORRUPTED0
30312043 4F525255                                     |01 CORRU
```

  - Power Down the system
  - Image the disks
  - Verify can rebuild RAID Groups, Aggregate, Volumes from images
  - Decrypt data using the A01 Key
    - Was able to decrypt the volume and find the contaminated file which is located on the physical disk at Inode 0x95A = PBN (Aggr block #):0x1D9ECE7B, File Block 0x2A, comes from 6140251A9_3 at phy 42,077,656
- **Secure Purge Verification Details**
  - Power on the system
  - Run NetApp Secure Purge

- First, I deleted Corrupted001 file and then ran secure-purge on the encrypted volume ETest1

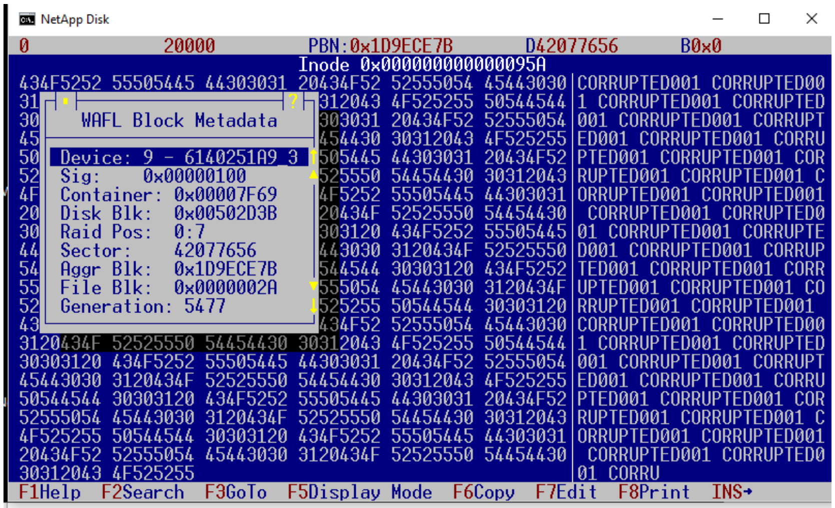
```
Vserver      Volume        Secure Purge Phase
-----------  -------------  ----------------------
data_001     ETest1        success
```

- New volume is created
    - New volume does not get a new name as it is a clone of the original volume minus the deleted blocks
    - New Key is created
        - Verified through the user interface and KMIP commands that the old A01 Keys had been removed and new keys A02 were created. We did not forensically evaluated the Gemalto servers storage for remanence of old keys deleted data blocks.
- Extract the A02 key from the Key Manager

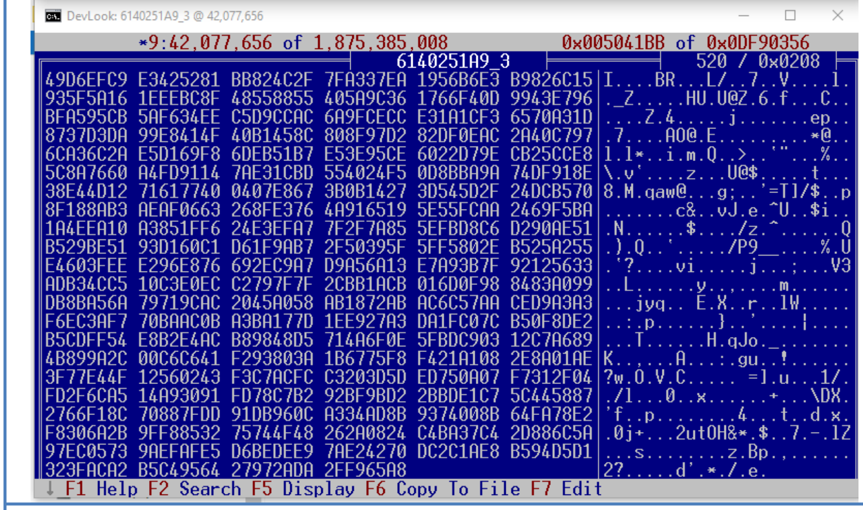
```
Get Symmetric Key
        UUID=67F09BF2463BE59DAB27187A5B8640F9016105137B2C6691F3DE4512F0A809FB

        Key=05846570ab6906caf9804f92b90f30f6f87092b4c3fe01651e00cce39bd01288

        KeyID=000000000000000002000000000005004a6b1d992f0d02d059b1275da96775990
        000000000000000

Get Symmetric Key
        UUID=BCC09DF92D856C6C323908BC94709F46E52C7516437F6F15B6431AE0B9B31C69

        Key=db8b6b85421c9e906a753b521bf48d5f33a4aea0ad4bcb6c41e1c335cca7b311

        KeyID=000000000000000002000000000005004a6b1d992f0d02d059b1275da96775990
        000000000000000
```

- Power Down the system
- Image the disks
- Verify can rebuild RAID Groups, Aggregate, Volumes from images
- Decrypt ETest1 data using the A02 Key
    - Was able to apply the new keys to decrypt the new volume post secure-purge. The file Corrupted001 first block of file data was deallocated (block now sparse) but still in the same location only still encrypted.
    - NOTE: if someone had a copy of the old A01 key, they could apply it to file data block and retrieve data.
    - Performed a full ASCII scan of the images for “Corrupted001” with no data found on the encrypted images of the drives.
- Attempt decrypt with ETest1 with the A01 key
    - Was not able to decrypt the ETest1 volume using the A01 keys once secure-purge was performed.

- Here is a picture of the first file data block of file “Corrupted001”. The top picture is before secure-purge was run and decrypted using A01 key. The bottom picture is the same block after secure-purge is performed and the volume is decrypted using A02 keys.

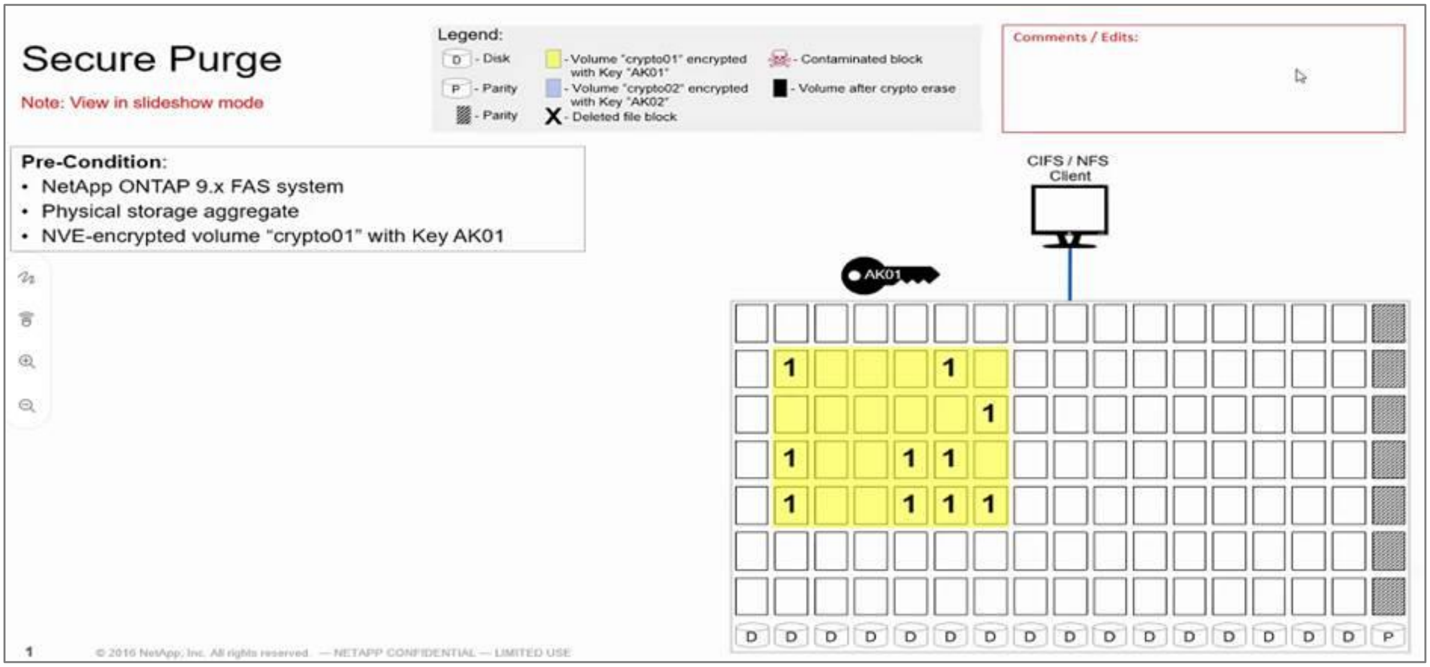


```
0            20000          PBN:0x1D9ECE7B      D42077656      B0x0
                          Inode 0x000000000000095A
434F5252 55505445 44303031 20434F52 52555054 45443030|CORRUPTED001 CORRUPTED00
31                                312043 4F525255 50544544|1 CORRUPTED001 CORRUPTED
30   WAFL Block Metadata          303031 20434F52 52555054|001 CORRUPTED001 CORRUPT
45                                454430 30312043 4F525255|ED001 CORRUPTED001 CORRU
50  Device: 9 - 6140251A9_3       505445 44303031 20434F52|PTED001 CORRUPTED001 COR
52  Sig:     0x00000100           525550 54454430 30312043|RUPTED001 CORRUPTED001 C
4F  Container: 0x00007F69         4F5252 55505445 44303031|ORRUPTED001 CORRUPTED001
20  Disk Blk:  0x00502D3B         20434F 52525550 54454430| CORRUPTED001 CORRUPTED0
30  Raid Pos:  0:7                303120 434F5252 55505445|01 CORRUPTED001 CORRUPTE
44  Sector:    42077656           443030 3120434F 52525550|D001 CORRUPTED001 CORRUP
54  Aggr Blk:  0x1D9ECE7B         544544 30303120 434F5252|TED001 CORRUPTED001 CORR
55  File Blk:  0x0000002A         555054 45443030 3120434F|UPTED001 CORRUPTED001 CO
52  Generation: 5477              525255 50544544 30303120|RRUPTED001 CORRUPTED001
43                                434F52 52555054 45443030|CORRUPTED001 CORRUPTED00
3120434F 52525550 54454430 30312043 4F525255 50544544|1 CORRUPTED001 CORRUPTED
30303120 434F5252 55505445 44303031 20434F52 52555054|001 CORRUPTED001 CORRUPT
45443030 3120434F 52525550 54454430 30312043 4F525255|ED001 CORRUPTED001 CORRU
50544544 30303120 434F5252 55505445 44303031 20434F52|PTED001 CORRUPTED001 COR
52555054 45443030 3120434F 52525550 54454430 30312043|RUPTED001 CORRUPTED001 C
4F525255 50544544 30303120 434F5252 55505445 44303031|ORRUPTED001 CORRUPTED001
20434F52 52555054 45443030 3120434F 52525550 54454430| CORRUPTED001 CORRUPTED0
30312043 4F525255                                    |01 CORRU
F1Help  F2Search  F3GoTo  F5Display Mode  F6Copy  F7Edit  F8Print  INS→
```



```
        *9:42,077,656 of 1,875,385,008           0x005041BB of 0x0DF90356
                          6140251A9_3                  520 / 0x0208
49D6EFC9 E3425281 BB824C2F 7FA337EA 1956B6E3 B9826C15|I....BR...L/..7..V....l.
935F5A16 1EEEBC8F 48558855 405A9C36 1766F40D 9943E796|._Z.....HU.U@Z.6.f...C..
BFA595CB 5AF634EE C5D9CCAC 6A9FCECC E31A1CF3 6570A31D|....Z.4.....j.......ep..
8737D3DA 99E8414F 40B1458C 808F97D2 82DF0EAC 2A40C797|.7....AO@.E.........*@..
6CA36C2A E5D169F8 6DEB51B7 E53E95CE 6022D79E CB25CCE8|l.l*..i.m.Q..>..`"...%..
5C8A7660 A4FD9114 7AE31CBD 554024F5 0D8BBA9A 74DF918E|\.v`....z...U@$.....t...
38E44D12 71617740 0407E867 3B0B1427 3D545D2F 24DCB570|8.M.qaw@...g;..'=T]/$..p
8F188AB3 AEAF0663 268FE376 4A916519 5E55FCAA 2469F5BA|.......c&..vJ.e.^U..$i..
1A4EEA10 A3851FF6 24E3EFA7 7F2F7A85 5EFBD8C6 D290AE51|.N......$..../z.^......Q
B529BE51 93D160C1 D61F9AB7 2F50395F 5FF5802E B525A255|.).Q..`...../P9__....%.U
E4603FEE E296E876 692EC9A7 D9A56A13 E7A93B7F 92125633|.`?....vi.....j...;...V3
ADB34CC5 10C3E0EC C2797F7F 2CBB1ACB 016D0F98 8483A099|..L......y.,.....m......
DB8BA56A 79719CAC 2045A058 AB1872AB AC6C57AA CED9A3A3|...jyq.. E.X..r..lW.....
F6EC3AF7 70BAAC0B A3BA177D 1EE927A3 DA1FC07C B50F8DE2|..:.p......}..'....|....
B5CDFF54 E8B2E4AC B89848D5 714A6F0E 5FBDC903 12C7A689|...T......H.qJo._.......
4B899A2C 00C6C641 F293803A 1B6775F8 F421A108 2E8A01AE|K.,....A...:.gu..!......
3F77E44F 12560243 F3C7ACFC C3203D5D ED750A07 F7312F04|?w.O.V.C..... =].u...1/.
FD2F6CA5 14A93091 FD78C7B2 92BF9BD2 2BBDE1C7 5C445887|./l...0..x......+...\DX.
2766F18C 70887FDD 91DB960C A334AD8B 9374008B 64FA78E2|'f..p.......4...t..d.x.
F8306A2B 9FF88532 75744F48 262A0824 C4BA37C4 2D886C5A|.0j+...2utOH&*.$..7.-.lZ
97EC0573 9AEFAFE5 D6BEDEE9 7AE24270 DC2C1AE8 B594D5D1|...s........z.Bp.,......
323FACA2 B5C49564 27972ADA 2FF965A8                  |2?.....d'.*./.e.
↓ F1 Help F2 Search F5 Display F6 Copy To File F7 Edit
```

Appendix B – NetApp Secure Purge Documentation



Secure Purge

Note: View in slideshow mode

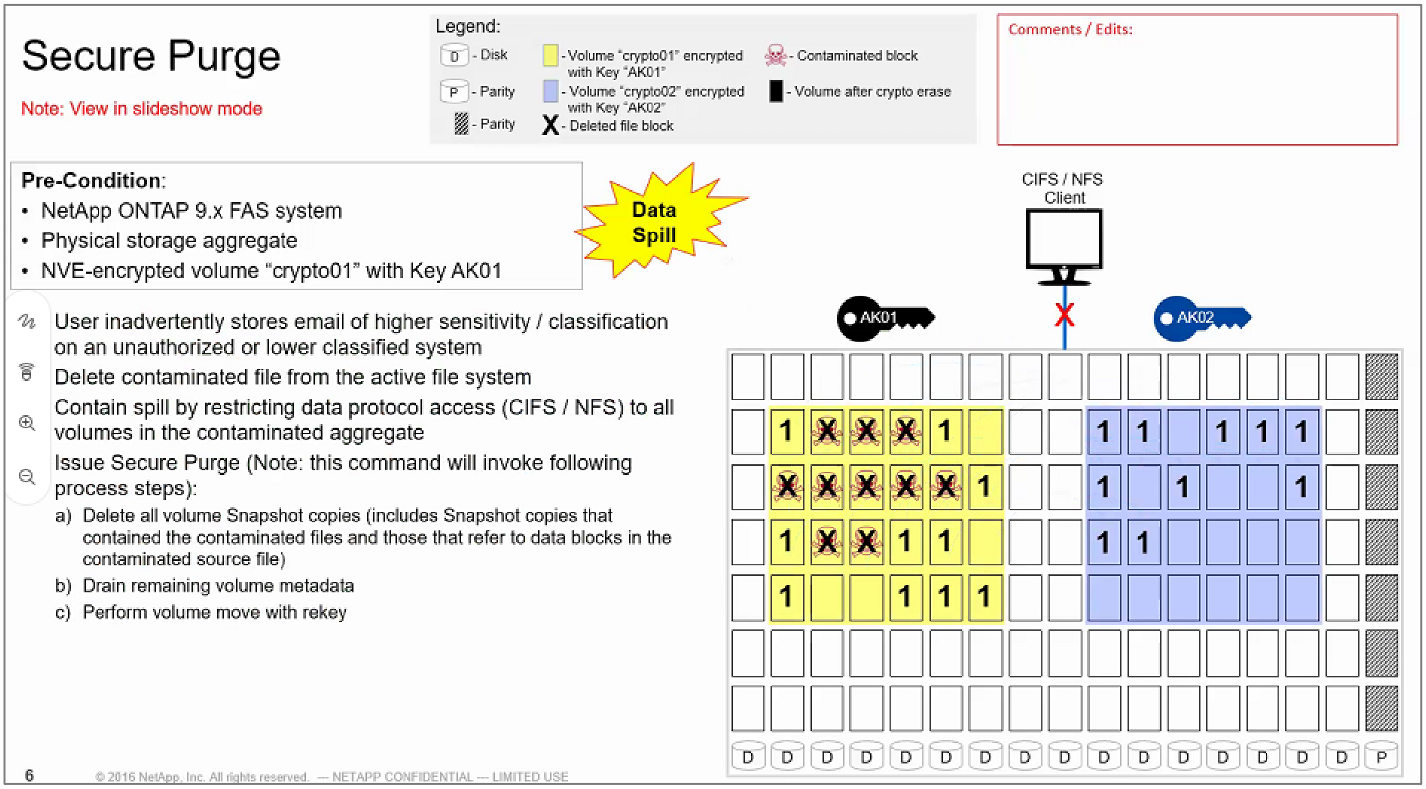
Legend:
- D - Disk
- P - Parity
- ▨ - Parity
- 🟨 - Volume "crypto01" encrypted with Key "AK01"
- 🟦 - Volume "crypto02" encrypted with Key "AK02"
- X - Deleted file block
- ☠ - Contaminated block
- ■ - Volume after crypto erase

Comments / Edits:

Pre-Condition:
- NetApp ONTAP 9.x FAS system
- Physical storage aggregate
- NVE-encrypted volume "crypto01" with Key AK01

																▨
	1	🟨	🟨	🟨	1	🟨										▨
	🟨	🟨	🟨	🟨	🟨	1										▨
	1	🟨	🟨	1	1	🟨										▨
	1	🟨	🟨	1	1	1										▨
																▨
																▨
D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	P

1 © 2016 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL — LIMITED USE



Secure Purge

Note: View in slideshow mode

Legend:
- D - Disk
- P - Parity
- ▨ - Parity
- 🟨 - Volume "crypto01" encrypted with Key "AK01"
- 🟦 - Volume "crypto02" encrypted with Key "AK02"
- X - Deleted file block
- ☠ - Contaminated block
- ■ - Volume after crypto erase

Comments / Edits:

Pre-Condition:
- NetApp ONTAP 9.x FAS system
- Physical storage aggregate
- NVE-encrypted volume "crypto01" with Key AK01

User inadvertently stores email of higher sensitivity / classification on an unauthorized or lower classified system

Delete contaminated file from the active file system

Contain spill by restricting data protocol access (CIFS / NFS) to all volumes in the contaminated aggregate

Issue Secure Purge (Note: this command will invoke following process steps):

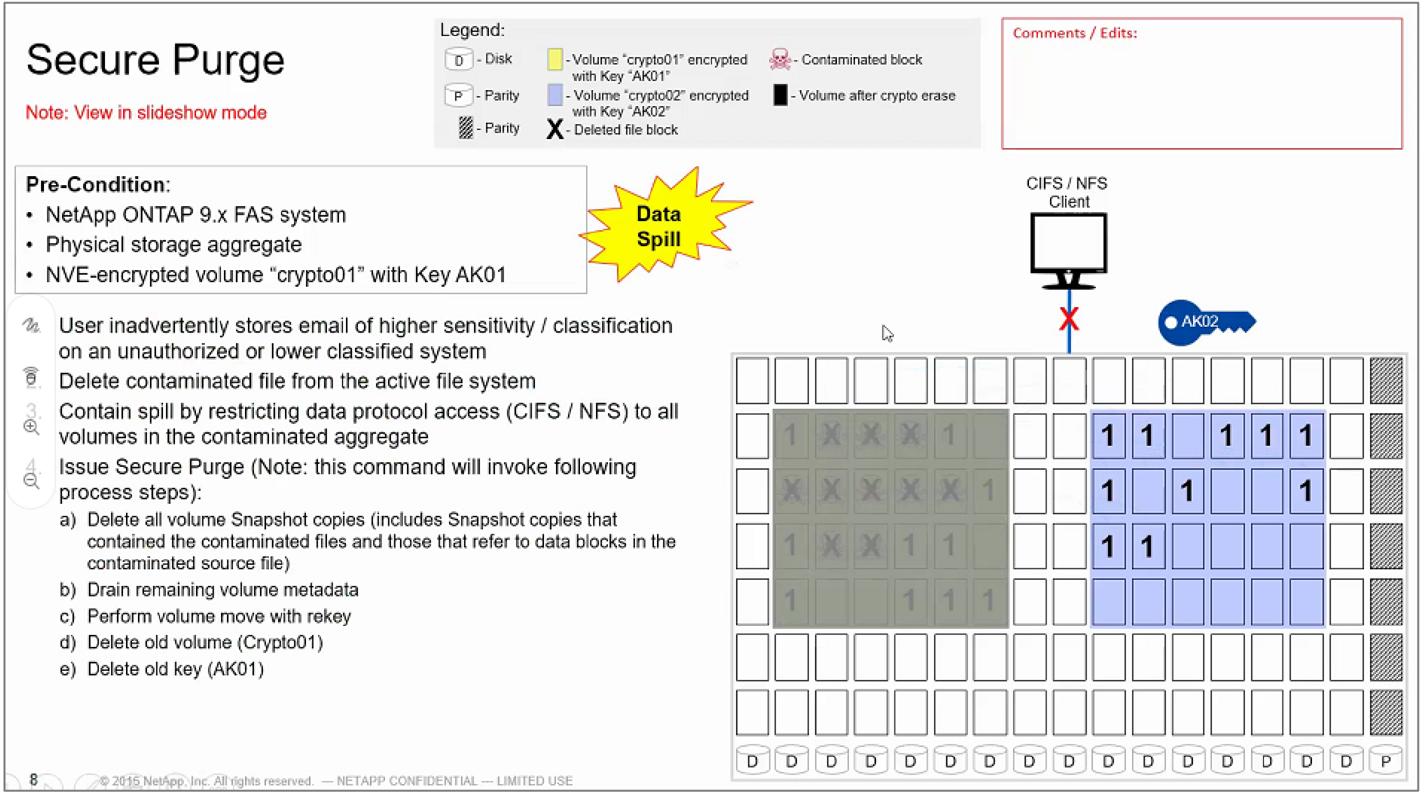
a) Delete all volume Snapshot copies (includes Snapshot copies that contained the contaminated files and those that refer to data blocks in the contaminated source file)

b) Drain remaining volume metadata

c) Perform volume move with rekey

																▨
	1	X	X	X	1	🟨			1	1	🟦	1	1	1		▨
	X	X	X	X	X	1			1	🟦	1	🟦	🟦	1		▨
	1	X	X	1	1	🟨			1	1	🟦	🟦	🟦	🟦		▨
	1	🟨	🟨	1	1	1			🟦	🟦	🟦	🟦	🟦	🟦		▨
																▨
																▨
D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	P

6 © 2016 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL — LIMITED USE



Secure Purge

Note: View in slideshow mode

Legend:

- D - Disk
- P - Parity
- ▨ - Parity
- 🟨 - Volume "crypto01" encrypted with Key "AK01"
- 🟦 - Volume "crypto02" encrypted with Key "AK02"
- X - Deleted file block
- ☠ - Contaminated block
- ■ - Volume after crypto erase

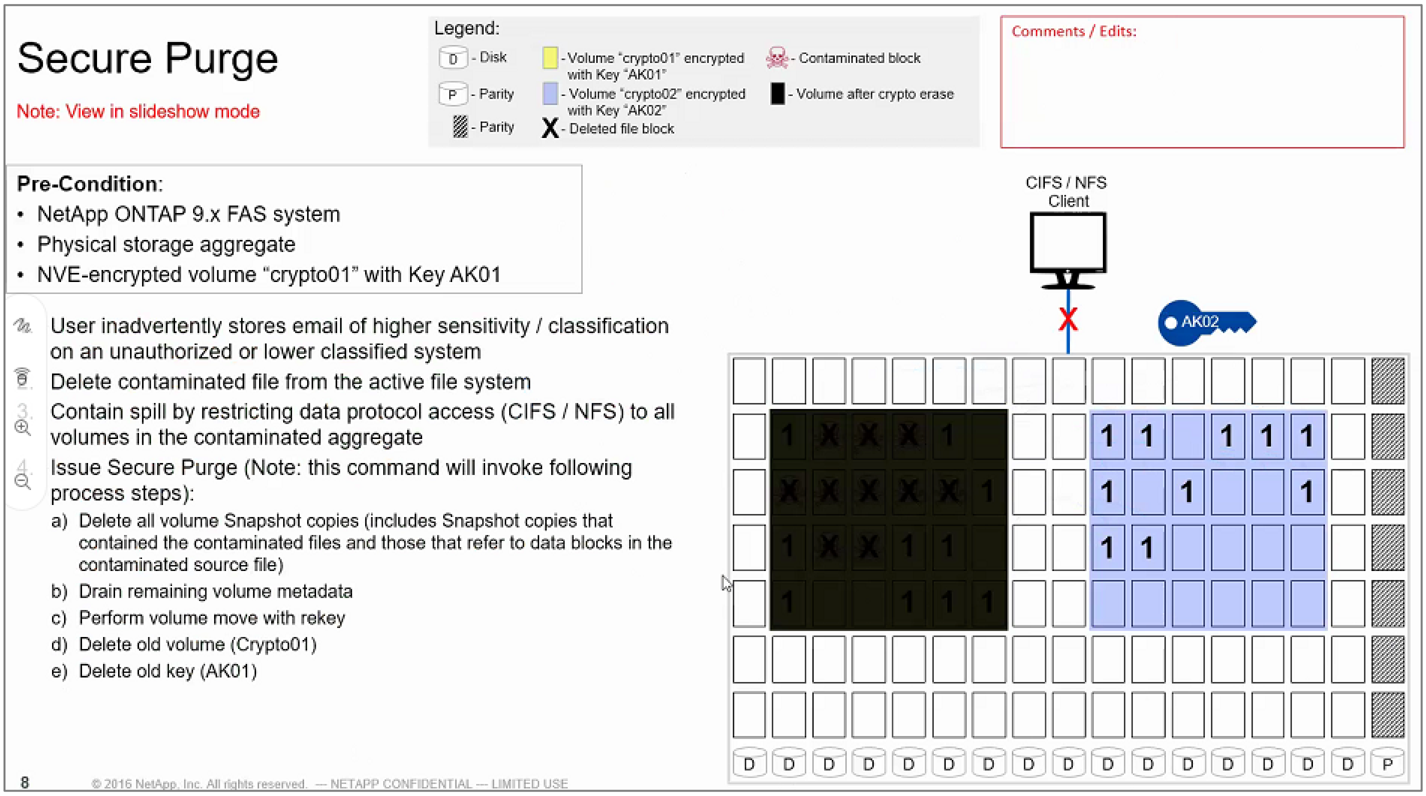
Comments / Edits:

Pre-Condition:

- NetApp ONTAP 9.x FAS system
- Physical storage aggregate
- NVE-encrypted volume "crypto01" with Key AK01

1. User inadvertently stores email of higher sensitivity / classification on an unauthorized or lower classified system
2. Delete contaminated file from the active file system
3. Contain spill by restricting data protocol access (CIFS / NFS) to all volumes in the contaminated aggregate
4. Issue Secure Purge (Note: this command will invoke following process steps):
   a) Delete all volume Snapshot copies (includes Snapshot copies that contained the contaminated files and those that refer to data blocks in the contaminated source file)
   b) Drain remaining volume metadata
   c) Perform volume move with rekey
   d) Delete old volume (Crypto01)
   e) Delete old key (AK01)

8 © 2016 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL — LIMITED USE



Secure Purge

Note: View in slideshow mode

Legend:

- D - Disk
- P - Parity
- ▨ - Parity
- 🟨 - Volume "crypto01" encrypted with Key "AK01"
- 🟦 - Volume "crypto02" encrypted with Key "AK02"
- X - Deleted file block
- ☠ - Contaminated block
- ■ - Volume after crypto erase

Comments / Edits:

Pre-Condition:

- NetApp ONTAP 9.x FAS system
- Physical storage aggregate
- NVE-encrypted volume "crypto01" with Key AK01

1. User inadvertently stores email of higher sensitivity / classification on an unauthorized or lower classified system
2. Delete contaminated file from the active file system
3. Contain spill by restricting data protocol access (CIFS / NFS) to all volumes in the contaminated aggregate
4. Issue Secure Purge (Note: this command will invoke following process steps):
   a) Delete all volume Snapshot copies (includes Snapshot copies that contained the contaminated files and those that refer to data blocks in the contaminated source file)
   b) Drain remaining volume metadata
   c) Perform volume move with rekey
   d) Delete old volume (Crypto01)
   e) Delete old key (AK01)

8 © 2016 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL — LIMITED USE