Make data on a FIPS drive or SED inaccessible

ONTAP 9

NetApp
September 01, 2022

Table of Contents

Make data on a FIPS drive or SED inaccessible

Make data on a FIPS drive or SED inaccessible overview

If you want to make data on a FIPS drive or SED permanently inaccessible, but keep the drive's unused space available for new data, you can sanitize the disk. If you want to make data permanently inaccessible and you do not need to reuse the drive, you can destroy it.

- Disk sanitization

  When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

- Disk destroy

  When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the disk irreversibly. Doing so renders the disk permanently unusable and the data on it permanently inaccessible.

You can sanitize or destroy individual self-encrypting drives, or all the self-encrypting drives for a node.

Sanitize a FIPS drive or SED

If you want to make data on a FIPS drive or SED permanently inaccessible, and use the drive for new data, you can use the `storage encryption disk sanitize` command to sanitize the drive.

What you'll need
You must be a cluster administrator to perform this task.

About this task
When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

Steps
1. Migrate any data that needs to be preserved to an aggregate on another disk.

2. Delete the aggregate on the FIPS drive or SED to be sanitized:

   `storage aggregate delete -aggregate aggregate_name`

   For complete command syntax, see the man page.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identify the disk ID for the FIPS drive or SED to be sanitized:

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk     Mode Data Key ID
-----    ----
-----------------------------------------------------------------
0.0.0    data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1    data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.2   data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Sanitize the drive:

```
storage encryption disk sanitize -disk disk_id
```

You can use this command to sanitize hot spare or broken disks only. To sanitize all disks regardless of type, use the `-force-all-state` option. For complete command syntax, see the man page.

> (i) You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
          To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

Destroy a FIPS drive or SED

If you want to make data on a FIPS drive or SED permanently inaccessible and you do not need to reuse the drive, you can use the `storage encryption disk destroy` command to destroy the disk.

What you'll need

You must be a cluster administrator to perform this task.

About this task

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the drive irreversibly. Doing so renders the disk virtually unusable and the data on it permanently inaccessible. However, you can reset the disk to its factory-configured settings using the physical secure ID (PSID) printed on the disk's label. For more information, see Returning a FIPS drive or SED to service when authentication keys are lost.

> ⓘ   You should not destroy a FIPS drive or SED unless you have the Non-Returnable Disk Plus service (NRD Plus). Destroying a disk voids its warranty.

Steps

1. Migrate any data that needs to be preserved to an aggregate on another different disk.

2. Delete the aggregate on the FIPS drive or SED to be destroyed:

   `storage aggregate delete -aggregate aggregate_name`

   For complete command syntax, see the man page.

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

3. Identify the disk ID for the FIPS drive or SED to be destroyed:

   `storage encryption disk show`

   For complete command syntax, see the man page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.2  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Destroy the disk:

   `storage encryption disk destroy -disk disk_id`

   For complete command syntax, see the man page.

   > (i) You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Emergency shredding of data on a FIPS drive or SED

In case of a security emergency, you can instantly prevent access to a FIPS drive or SED, even if power is not available to the storage system or the KMIP server.

What you'll need

- If you are using a KMIP server that has no available power, the KMIP server must be configured with an easily destroyed authentication item (for example, a smart card or USB drive).
- You must be a cluster administrator to perform this task.

Step

1. Perform emergency shredding of data on a FIPS drive or SED:

If…	Then…

Power is available to the storage system and you have time to take the storage system offline gracefully	a. If the storage system is configured as an HA pair, disable takeover.
	
	b. Take all aggregates offline and delete them.
	
	c. Set the privilege level to advanced:
	`set -privilege advanced`
	
	d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:
	`storage encryption disk modify -disk * -fips-key -id 0x0`
	
	e. Halt the storage system.
	
	f. Boot into maintenance mode.
	
	g. Sanitize or destroy the disks:
	
	  ◦ If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:
	    `disk encrypt sanitize -all`
	
	  ◦ If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:
	    `disk encrypt destroy disk_id1 disk_id2 …`
	
	    ⓘ The `disk encrypt sanitize` and `disk encrypt destroy` commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.
	
	h. Repeat these steps for the partner node. This leaves the storage system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.

Power is available to the storage system and you must shred the data immediately	a. **If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:**	a. **If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:**
	b. If the storage system is configured as an HA pair, disable takeover.	b. If the storage system is configured as an HA pair, disable takeover.
	c. Set the privilege level to advanced: `set -privilege advanced`	c. Set the privilege level to advanced: `set -privilege advanced`
	d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID: `storage encryption disk modify -disk * -fips-key-id 0x0`	d. Destroy the disks: `storage encryption disk destroy -disk * -force -all-states true`
	e. Sanitize the disk: `storage encryption disk sanitize -disk * -force-all-states true`	
	The storage system panics, leaving the system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.	
Power is available to the KMIP server but not to the storage system	a. Log in to the KMIP server. b. Destroy all keys associated with the FIPS drives or SEDs that contain the data you want to prevent access to. This prevents access to disk encryption keys by the storage system.	
Power is not available to the KMIP server or the storage system	Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.	

For complete command syntax, see the man pages.