



Make data on a FIPS drive or SED inaccessible

ONTAP 9

NetApp
June 26, 2023

Table of Contents

- Make data on a FIPS drive or SED inaccessible 1
 - Make data on a FIPS drive or SED inaccessible overview 1
 - Sanitize a FIPS drive or SED 1
 - Destroy a FIPS drive or SED 3
 - Emergency shredding of data on a FIPS drive or SED 4

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
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

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.



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
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Destroy the disk:

```
storage encryption disk destroy -disk disk_id
```

For complete command syntax, see the man page.



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 | <ul style="list-style-type: none">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: <code>set -privilege advanced</code>d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID: <code>storage encryption disk modify -disk * -fips-key -id 0x0</code>e. Halt the storage system.f. Boot into maintenance mode.g. Sanitize or destroy the disks:<ul style="list-style-type: none">◦ If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks: <code>disk encrypt sanitize -all</code>◦ If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks: <code>disk encrypt destroy disk_id1 disk_id2 ...</code> <div><p>The <code>disk encrypt sanitize</code> and <code>disk encrypt destroy</code> commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.</p></div> <ul style="list-style-type: none">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. |

| | | |
|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Power is available to the storage system and you must shred the data immediately</p> | <p>a. If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:</p> <p>b. If the storage system is configured as an HA pair, disable takeover.</p> <p>c. Set the privilege level to advanced:</p> <pre>set -privilege advanced</pre> <p>d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Sanitize the disk:</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre> | <p>a. If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:</p> <p>b. If the storage system is configured as an HA pair, disable takeover.</p> <p>c. Set the privilege level to advanced:</p> <pre>set -privilege advanced</pre> <p>d. Destroy the disks: <code>storage encryption disk destroy -disk * -force -all-states true</code></p> |
| | <p>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.</p> | |
| <p>Power is available to the KMIP server but not to the storage system</p> | <p>a. Log in to the KMIP server.</p> <p>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.</p> | |
| <p>Power is not available to the KMIP server or the storage system</p> | <p>Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.</p> | |

For complete command syntax, see the man pages.

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.