storage encryption commands

ONTAP 9.3 commands

NetApp
February 12, 2024

Table of Contents

storage encryption commands

storage encryption disk destroy

Cryptographically destroy a self-encrypting disk

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `storage encryption disk destroy` command cryptographically destroys a self-encrypting disk (SED), making it incapable of performing I/O operations. This command performs the following operations:

- Employs the inherent erase capability of SEDs to cryptographically sanitize the disk
- Permanently locks the disk to prevent further data access
- Changes the data and FIPS authentication keys to random values that are not recorded except within the SED.

Use this command with extreme care. The only mechanism to restore the disk to usability (albeit without the data) is the storage encryption disk revert-to-original-state operation that is available only on disks that have the physical secure ID (PSID) printed on the disk label.

The destroy command requires you to enter a confirmation phrase before proceeding with the operation.

The command releases the cluster shell after launching the operation. Monitor the output of the storage encryption disk show-status command for command completion.

Upon command completion, remove the destroyed SED from the system.

Parameters

`-disk <disk path name>` - Disk Name

This parameter specifies the name of the disk you want to cryptographically destroy. See the man page for the `storage disk modify` command for information about disk-naming conventions.

`[-force-all-states <true>]` - Destroy All Matching Disks

When this parameter is *`false`* or not specified, the operation defaults to spare and broken disks only, as reported in the output of the storage disk show command. When you specify this parameter as *`true`* , it allows you to cryptographically destroy all matching disk names regardless of their state, including those in active use in aggregates. This allows a quick destroy of all system disks if you use the `-disk` parameter with the asterisk wildcard (*). If you destroy active disks, the nodes might not be able to continue operation, and might halt or panic.

Examples

The following command cryptographically destroys the disk 1.10.20:

```
cluster1::> storage encryption disk destroy 1.10.20

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.

cluster1::>
```

If you do not enter the correct confirmation phrase, the operation is aborted:

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

Warning: This operation will cryptographically destroy 5 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
         :yes
No disks destroyed.

cluster1::>
```

The following command quickly cryptographically destroys all system disks:

```
cluster1::> storage encryption disk destroy -force-all-states -disk *

Warning: This operation will cryptographically destroy 96
         self-encrypting disks on 4 nodes.
         To continue, enter
          destroy disk
   :destroy disk

Info: Starting destroy on 96 disks.
      View the status of the operation by using the
      xref:{relative_path}storage-encryption-disk-show-status.html[storage
encryption disk show-status] command.

cluster1::>
```

Related Links

- storage encryption disk revert-to-original-state
- storage encryption disk show-status
- storage disk show

storage encryption disk modify

Modify self-encrypting disk parameters

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `storage encryption disk modify` command changes the data and FIPS-compliance protection parameters of self-encrypting disks (SEDs). The current data AK and FIPS AK of the SED are required to effect changes to the respective AKs and FIPS compliance, and must also be available from the key servers.

The command releases the cluster shell after launching the operation. Monitor the output of the storage encryption disk show-status command for command completion.

> To properly protect data at rest on a SED and place it into compliance with its FIPS certification requirements, set both the Data and FIPS-compliance AKs to a value other than the default manufacture secure ID (MSID), indicated by a key ID with the special value *0x0* . Verify the key IDs by using the storage encryption disk show and `storage encryption disk show-fips` commands.

Parameters

`-disk <disk path name>` - Disk Name

This parameter specifies the name of the SED that you want to modify.

{ [-data-key-id <text>] - Key ID of the New Data Authentication Key

This parameter specifies the key ID associated with the data AK that you want the SED to use for future authentications. When the provided key ID is the MSID, data at rest on the SED is not protected from unauthorized access. Setting this parameter to a non-MSID value automatically engages the power-on-lock protections of the device, so that when the device is power-cycled, the system must authenticate with the device using the AK to reenable I/O operations.

| [-fips-key-id <text>] - Key ID of the New Authentication Key for FIPS Compliance }

This parameter specifies the key ID associated with the FIPS AK that you want the SED to apply to SED credentials other than the one that protects the data. When the value is not the MSID, these credentials are changed to the indicated AK, and other security-related items are set to conform to the FIPS certification requirements ("FIPS compliance mode") of the device. You may set the `-fips-key-id` to any one of the key IDs known to the system. The FIPS key ID may, but does not have to, be the same as the data key ID parameter. Setting `-fips-key-id` to the MSID key ID value disables FIPS compliance mode and restores the FIPS-related authorites and other components as required (other than data) to their default settings. The MSID is required when reverting to a version of Data ONTAP that does not manipulate the FIPS-compliance device components.

Examples

The following command changes both the AK and the power-cycle protection to values that protect the data at rest on the disk. Note that the `-data-key-id` and `-fips-key-id` parameters require one of the key IDs that appear in the output of the security key-manager query command.

```
cluster1::> storage encryption disk modify -data-key-id
6A1E21D8000000000100000000000000F5A1EB48EF26FD6A8E76549C019F2350 -disk
2.10.*

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

The following command changes the FIPS AK and sets the device into FIPS-compliance mode. Note that the `-fips-key-id` parameter requires one of the key IDs that appear in the output of the security key-manager query command.

```
cluster1::> storage encryption disk modify -fips-key-id
6A1E21D8000000000100000000000000005A1FB4EE8F62FD6D8AE6754C9019F35A 2.10.*

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Related Links

- storage encryption disk show-status
- storage encryption disk show

- security key-manager query

storage encryption disk revert-to-original-state

Revert a self-encrypting disk to its original, as-manufactured state

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

Some self-encrypting disks (SEDs) are capable of an operation that restores them as much as possible to their as-manufactured state. The `storage encryption disk revert-to-original-state` command invokes this special operation that is available only in SEDs that have the physical secure ID (PSID) printed on their labels.

The PSID is unique to each SED, meaning the command can revert only one SED at a time. The disk must be in a "broken" or "spare" state as shown by the output of the storage disk show command.

The operation in the SED accomplishes the following changes:

- Sanitizes all data by changing the disk encryption key to a new random value
- Sets the data authentication key (AK) and FTPS AK to the default manufacture secure ID (MSID)
- Unlocks the data band
- Resets the power-on lock state to *`false`*
- Initializes other vendor-unique encryption-related parameters

The command releases the cluster shell after launching the operation. Monitor the output of the storage encryption disk show-status command for command completion.

When the operation is complete, it is possible to return the SED to service using the storage disk unfail command in *`advanced`* privilege mode. To do so, you might also need to reestablish ownership of the SED using the storage disk assign command.

Parameters

`-disk <disk path name>` - Disk Name

The name of the SED to be reverted to its as-manufactured state. See the man page for the `storage disk modify` command for information about disk-naming conventions.

`-psid <text>` - Physical Secure ID

The PSID printed on the SED label.

Examples

The following command shows a SED being returned to its as-manufactured state:

```
cluster1::> storage encryption disk revert-to-original-state -disk 01.10.0
-psid AC65PYF8CG45YZABUQJKM98WV2VZGRLD
```

Related Links

- storage disk show
- storage encryption disk show-status
- storage disk unfail
- storage disk assign

storage encryption disk sanitize

Cryptographically sanitize a self-encrypting disk

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `storage encryption disk sanitize` command cryptographically sanitizes one or more self-encrypting disks (SEDs), making the existing data on the SED impossible to retrieve. This operation employs the inherent erase capability of SEDs to perform all of the following changes:

- Sanitizes all data by changing the disk encryption key to a new random value
- Sets the data authentication key (AK) to the default manufacture secure ID (MSID)
- Unlocks the data band
- Resets the power-on lock state to *`false`*

There is no method to restore the disk encryption key to its previous value, meaning that you cannot recover the data on the SED. Use this command with extreme care.

The sanitize command requires you to enter a confirmation phrase before proceeding with the operation.

The command releases the cluster shell after launching the operation. Monitor the output of the storage encryption disk show-status command for command completion.

When the operation is complete, it is possible to return the SED to service using the storage disk unfail command in *`advanced`* privilege mode. To do so, you might also need to reestablish ownership of the SED using the storage disk assign command.

Parameters

`-disk <disk path name>` - Disk Name

This parameter specifies the name of the SEDs you want to cryptographically sanitize. See the man page for the `storage disk modify` command for information about disk-naming conventions.

`[-force-all-states <true>]` - Sanitize All Matching Disks

When this parameter is *`false`* or not specified, the operation defaults to spare and broken disks only, as reported in the output of the storage disk show command. When you specify this parameter as *`true`* , it allows you to cryptographically sanitize all matching disk names regardless of their state, including those in active use in aggregates. This allows a quick erasure of all system data if you use the `-disk` parameter with the asterisk wildcard (*). If you sanitize active disks, the nodes might not be able to continue operation, and might halt or panic.

Examples

The following command sanitizes the disk 1.10.20:

```
cluster1::> storage encryption disk sanitize 1.10.20

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
      xref:{relative_path}storage-encryption-disk-show-status.html[storage
encryption disk show-status] command.

cluster1::>
```

If you do not enter the correct confirmation phrase, the operation is aborted:

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

Warning: This operation will cryptographically sanitize 5 spare or broken
         self-encrypting disks on 1 node.
         To continue, enter
          sanitize disk
         :yes
No disks sanitized.

cluster1::>
```

The following command quickly cryptographically sanitizes all system disks:

```
cluster1::> storage encryption disk sanitize -force-all-states -disk *

Warning: This operation will cryptographically sanitize 96
         self-encrypting disks on 4 nodes.
         To continue, enter
          sanitize disk
   :sanitize disk

Info: Starting sanitize on 96 disks.
      View the status of the operation by using the
      xref:{relative_path}storage-encryption-disk-show-status.html[storage
encryption disk show-status] command.

cluster1::>
```

Related Links

- storage encryption disk show-status
- storage disk unfail
- storage disk assign
- storage disk show

storage encryption disk show-status

Display status of disk encryption operation

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `storage encryption disk show-status` command displays the results of the latest `destroy` , `modify` , or `sanitize` operation of the `storage encryption disk` command family. Use this command to view the progress of these operations on self-encrypting disks (SEDs).

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-node <nodename>] - Node Name

If you specify this parameter, the command displays disk encryption status for the nodes that match this parameter.

[-is-sed-support {true|false}] - Node Supports Self-Encrypting Disks

If you specify this parameter, the command displays disk encryption status for the nodes that match this parameter (*true* means the node supports SEDs).

[-latest-op <Storage Disk Encryption Operation>] - Latest Operation Requested

If you specify this parameter, the command displays disk encryption status for the nodes with a most recent `storage encryption disk` operation that matches this parameter (one of `destroy` , `modify` , `revert-to-original-state` , `sanitize` , or `unknown`).

[-op-start-time <MM/DD/YYYY HH:MM:SS>] - Operation Start Time

Selects the nodes with operation start times that match this parameter.

[-op-execute-time <integer>] - Execution Time in Seconds

If you specify this parameter, the command displays disk encryption status for the nodes with operation execution time that matches this parameter. The operation may be partial or completed.

[-disk-start-count <integer>] - Number of Disks Started

If you specify this parameter, the command displays disk encryption status for the nodes that started this number of SEDs in their latest operation.

[-disk-done-count <integer>] - Number of Disks Done

Selects the nodes that report this number of SEDs having completed the latest operation, successfully or not.

[-disk-success-count <integer>] - Number of Disks Successful

If you specify this parameter, the command displays disk encryption status for the nodes that report this number of SEDs that successfully completed the latest operation. When the operation is finished, if the success count is not the same as the started count, some additional detail is available using the `-instance` or `-node` parameters.

[-disk-no-key-id-count <integer>] - Number of Disks with Key ID Not Found

If you specify this parameter, the command displays disk encryption status for the nodes that report this number of SEDs that failed the latest operation because Data ONTAP could not find the Key IDs associated with the required authentication key of the SED.

[-disk-no-authent-count <integer>] - Number of Disks Not Authenticated

If you specify this parameter, the command displays disk encryption status for the nodes that report this number of SEDs that failed the latest operation because the identified Authentication Key could not authenticate with the SED.

Examples

When no operation has been requested since node boot, the status for that node is empty. If you enter a node name, the output is in the same format as for the `-instance` parameter.

```
cluster1::> storage encryption disk show-status -node node
Node Name: node
  Node Supports Self-Encrypting Disks: true
          Latest Operation Requested: unknown
                Operation Start Time: -
             Execution Time in Seconds: -
               Number of Disks Started: -
                  Number of Disks Done: -
              Number of Disks Successful: -
Number of Disks with Key ID Not Found: -
    Number of Disks Not Authenticated: -
```

Once an operation begins, the status is dynamic until all devices have completed. When disks are modified, sanitized, or destroyed, sequential executions of `storage encryption disk show-status` appear as in this example that shows the progress of a modify operation on three SEDs on each node of a two-node cluster:

```
cluster1::> storage encryption disk show-status
        SED     Latest   Start               Execution  Disks  Disks
Disk
Node    Support Request  Timestamp          Time (sec)  Begun   Done
Successful
------- ------- -------- ------------------ ---------- ------ ------
----------
node    true    modify   9/22/2014 13:58:53          4      3      0
0
node1   true    modify   9/22/2014 13:58:53          4      3      0
0

cluster1::> storage encryption disk show-status
        SED     Latest   Start               Execution  Disks  Disks
Disk
Node    Support Request  Timestamp          Time (sec)  Begun   Done
Successful
------- ------- -------- ------------------ ---------- ------ ------
----------
node    true    modify   9/22/2014 13:58:53          7      3      3
3
node1   true    modify   9/22/2014 13:58:53          7      3      3
3
```

storage encryption disk show

Display self-encrypting disk attributes

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `storage encryption disk show` command displays information about self-encrypting disks (SEDs). By default, the command displays the following information about all SEDS:

- Disk name
- The protection mode of the SED
- The key ID associated with the data authentication key (data AK)

You can use the following parameters together with the `-disk` parameter to narrow the selection of displayed SEDs or the information displayed about them.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-fips]

If you specify this parameter, the command displays the key ID associated with the FIPS-compliance authentication key ("FIPS AK") instead of the data key ID.

| [-instance] }

If you specify this parameter, the command displays detailed disk information about all disks, or only those specified by a -disk parameter.

[-disk <disk path name>] - Disk Name

If you specify this parameter, the command displays information about the specified disks. If you specify a single disk path name, the output is the same as when you use the -instance parameter. See the man page for the `storage disk modify` command for information about disk-naming conventions. Default is all self-encrypting disks.

[-container-name <text>] - Container Name

This parameter specifies the container name associated with a SED. If you specify an aggregate name or other container name, only the SEDs in that container are displayed. See the man page for the storage disk show command for a description of the container name. Use the storage aggregate show-status and storage disk show commands to determine which aggregates the SEDs are in.

[-container-type {aggregate | broken | foreign | labelmaint | maintenance | mediator | remote | shared | spare | unassigned | unknown | unsupported}] - Container Type

This parameter specifies the container type associated with a SED. If you specify a container type, only the SEDs with that container type are displayed. See the man page for the storage disk show command for a description of the container type.

[-data-key-id <text>] - Key ID of the Current Data Authentication Key

This parameter specifies the key ID associated with the data AK that the SED requires for authentication with the data-protection authorities in the SED. The special key ID *0x0* indicates that the current data AK of the SED is the default manufacture secure ID (MSID) that is not secret. To properly protect data at rest on

the device, modify the data AK using a key ID that is not the MSID. When you modify the data AK with a non-MSID key ID, the system automatically sets the device's power-on lock enable control so that authentication with the data AK is required after a device power-cycle. Use storage encryption disk modify -data-key-id`*key-id* to protect the data. Use storage encryption disk modify-fips -key-id`*key-id* to place the SED into FIPS-compliance mode.

[-fips-key-id <text>] - Key ID of the Current FIPS Authentication Key

This parameter specifies the key ID associated with the FIPS authentication key ("FIPS AK") that the system must use to authenticate with FIPS-compliance authorities in the SED.

[-is-power-on-lock-enabled {true|false}] - Is Power-On Lock Protection Enabled?

This parameter specifies the state of the SED control that determines whether the SED requires authentication with the data AK after a power-cycle. The system enables this control parameter automatically when you use the storage encryption disk modify-data-key-id command to set the data AK to a value other than the MSID. Data is protected only when this parameter is *true* and the data AK is not the MSID. Compare with the values of the -protection-mode parameter below.

[-protection-mode <text>] - Mode of SED Data and FIPS-Compliance Protection

The protection mode that the SED is in:

- open - data is unprotected; SED is not in FIPS-compliance mode
- data - data is protected; SED is not in FIPS-complance mode
- part - data is unprotected; SED is in FIPS-compliance mode
- full - data is protected; SED is in FIPS-compliance mode

Examples

The following command displays information about all SEDs:

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
------- ----
------------------------------------------------------------------------
0.0.0   open 0x0
0.0.1   part 0x0
0.0.2   data
0A9C9CFC0000000001000000000000000345CFD1BAD310CA8EDB377D439FB5C9A
1.10.0  open
0A53ED2A0000000001000000000000000BEDC1B27AD3F0DB8891375AED2F34D0B
1.10.1  part
0A9C9CFC0000000001000000000000000345CFD1BAD310CA8EDB377D439FB5C9A
1.10.2  full
0A9C9CFC0000000001000000000000000345CFD1BAD310CA8EDB377D439FB5C9A
[...]
```

Note in the example that only disk 1.10.2 is fully protected with FIPS mode, power-on-lock enable, and an AK that is not the default MSID.

The following command displays information about the protection mode and FIPS key ID for all SEDs:

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------- ----
--------------------------------------------------------------------
0.0.0   open 0x0
0.0.1   part
0A53ED2A000000000100000000000000C1B27AD3F0DB8891375AED2F34D0BBED
0.0.2   data 0x0
1.10.0  open
0A53ED2A000000000100000000000000BEDC1B27AD3F0DB8891375AED2F34D0B
1.10.1  part
0A9C9CFC000000000100000000000000345CFD1BAD310CA8EDB377D439FB5C9A
1.10.2  full
0A9C9CFC000000000100000000000000345CFD1BAD310CA8EDB377D439FB5C9A
[...]
```

Note again that only disk 1.10.2 is fully protected with FIPS-compliance mode set, power-on-lock enabled, and a data AK that is not the default MSID.

The following command displays the individual fields for disk 1.10.1:

```
cluster1::> storage encryption disk show -disk 1.10.1
Disk Name: 1.10.1
  Key ID of the Current Data Authentication Key:
0A9C9CFC000000000100000000000000345CFD1BAD310CA8EDB377D439FB5C9A
  Key ID of the Current FIPS Authentication Key:
0A9C9CFC000000000100000000000000345CFD1BAD310CA8EDB377D439FB5C9A
           Is Power-On Lock Protection Enabled?: true
Mode of SED Data and FIPS-Compliance Protection: open
```

Related Links

- storage disk show
- storage aggregate show-status
- storage encryption disk modify

Copyright information

Trademark information