Disk sanitization

ONTAP 9

NetApp
August 10, 2023

Table of Contents

Disk sanitization

Disk sanitization overview

Disk sanitization is the process of physically obliterating data by overwriting disks or SSDs with specified byte patterns or random data so that recovery of the original data becomes impossible. Using the sanitization process ensures that no one can recover the data on the disks.

This functionality is available through the nodeshell in all ONTAP 9 releases, and starting with ONTAP 9.6 in maintenance mode.

The disk sanitization process uses three successive default or user-specified byte overwrite patterns for up to seven cycles per operation. The random overwrite pattern is repeated for each cycle.

Depending on the disk capacity, the patterns, and the number of cycles, the process can take several hours. Sanitization runs in the background. You can start, stop, and display the status of the sanitization process. The sanitization process contains two phases: the "Formatting phase" and the "Pattern overwrite phase".

Formatting phase

The operation performed for the formatting phase depends on the class of disk being sanitized, as shown in the following table:

Disk class	Formatting phase operation
Capacity HDDs	Skipped
Performance HDDs	SCSI format operation
SSDs	SCSI sanitize operation

Pattern overwrite phase

The specified overwrite patterns are repeated for the specified number of cycles.

When the sanitization process is complete, the specified disks are in a sanitized state. They are not returned to spare status automatically. You must return the sanitized disks to the spare pool before the newly sanitized disks are available to be added to another aggregate.

When disk sanitization cannot be performed

Disk sanitization is not supported for all disk types. In addition, there are circumstances in which disk sanitization cannot be performed.

- It is not supported on all SSD part numbers.

  For information about which SSD part numbers support disk sanitization, see the Hardware Universe.

- It is not supported in takeover mode for systems in an HA pair.
- It cannot be performed on disks that were failed due to readability or writability problems.
- It does not perform its formatting phase on ATA drives.

- If you are using the random pattern, it cannot be performed on more than 100 disks at one time.
- It is not supported on array LUNs.
- If you sanitize both SES disks in the same ESH shelf at the same time, you see errors on the console about access to that shelf, and shelf warnings are not reported for the duration of the sanitization.

  However, data access to that shelf is not interrupted.

What happens if disk sanitization is interrupted

If disk sanitization is interrupted by user intervention or an unexpected event such as a power outage, ONTAP takes action to return the disks that were being sanitized to a known state, but you must also take action before the sanitization process can finish.

Disk sanitization is a long-running operation. If the sanitization process is interrupted by power failure, system panic, or manual intervention, the sanitization process must be repeated from the beginning. The disk is not designated as sanitized.

If the formatting phase of disk sanitization is interrupted, ONTAP must recover any disks that were corrupted by the interruption. After a system reboot and once every hour, ONTAP checks for any sanitization target disk that did not complete the formatting phase of its sanitization. If any such disks are found, ONTAP recovers them. The recovery method depends on the type of the disk. After a disk is recovered, you can rerun the sanitization process on that disk; for HDDs, you can use the `-s` option to specify that the formatting phase is not repeated again.

Tips for creating and backing up local tiers (aggregates) containing data to be sanitized

If you are creating or backing up local tiers (aggregates) to contain data that might need to be sanitized, following some simple guidelines will reduce the time it takes to sanitize your data.

- Make sure your local tiers containing sensitive data are not larger than they need to be.

  If they are larger than needed, sanitization requires more time, disk space, and bandwidth.

- When you back up local tiers containing sensitive data, avoid backing them up to local tier that also contain large amounts of nonsensitive data.

  This reduces the resources required to move nonsensitive data before sanitizing sensitive data.

Sanitize a disk

Sanitizing a disk allows you to remove data from a disk or a set of disks on decommissioned or inoperable systems so that the data can never be recovered.

Two methods are available to sanitize disks using the CLI:

Sanitize a disk with “maintenance mode” commands (ONTAP 9.6 and later releases)

Beginning with ONTAP 9.6, you can perform disk sanitization in maintenance mode.

Before you begin

- The disks cannot be self-encrypting disks (SED).

  You must use the `storage encryption disk sanitize` command to sanitize an SED.

  Encryption of data at rest

Steps

1. Boot into maintenance mode.
   a. Exit the current shell by entering `halt`.

      The LOADER prompt is displayed.

   b. Enter maintenance mode by entering `boot_ontap maint`.

      After some information is displayed, the maintenance mode prompt is displayed.
2. If the disks you want to sanitize are partitioned, unpartition each disk:

   > The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. It is highly recommended that you contact NetApp Support before you proceed. You can also refer to the Knowledge Base article How to unpartition a spare drive in ONTAP

   `disk unpartition` *`disk_name`*
3. Sanitize the specified disks:

   `disk sanitize start [-p` *`pattern1`*`|-r [-p` *`pattern2`*`|-r [-p` *`pattern3`*`|-r]]] [-c` *`cycle_count`*`] ` *`disk_list`*

   > Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting phase must be restarted and allowed to finish before the disks are sanitized and ready to be returned to the spare pool. If you need to abort the sanitization process, you can do so by using the `disk sanitize abort` command. If the specified disks are undergoing the formatting phase of sanitization, the abort does not occur until the phase is complete.

   `-p` *`pattern1`* `-p` *`pattern2`* `-p` *`pattern3`* specifies a cycle of one to three user-defined hex byte overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

   `-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

   `-c` *`cycle_count`* specifies the number of times that the specified overwrite patterns are applied. The default value is one cycle. The maximum value is seven cycles.

disk_list specifies a space-separated list of the IDs of the spare disks to be sanitized.

4. If desired, check the status of the disk sanitization process:

   `disk sanitize status [disk_list]`

5. After the sanitization process is complete, return the disks to spare status for each disk:

   `disk sanitize release disk_name`

6. Exit maintenance mode.

Sanitize a disk with “nodeshell” commands (all ONTAP 9 releases)

For all versions of ONTAP 9, when disk sanitization is enabled using nodeshell commands, some low-level ONTAP commands are disabled. After disk sanitization is enabled on a node, it cannot be disabled.

Before you begin

- The disks must be spare disks; they must be owned by a node, but not used in a local tier (aggregate).

  If the disks are partitioned, neither partition can be in use in a local tier (aggregate).

- The disks cannot be self-encrypting disks (SED).

  You must use the `storage encryption disk sanitize` command to sanitize an SED.

  Encryption of data at rest

- The disks cannot be part of a storage pool.

Steps

1. If the disks you want to sanitize are partitioned, unpartition each disk:

   > The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. **It is highly recommended that you contact NetApp Support before you proceed.** You can also refer to the Knowledge Base article How to unpartition a spare drive in ONTAP.

   ```
   disk unpartition disk_name
   ```

2. Enter the nodeshell for the node that owns the disks you want to sanitize:

   ```
   system node run -node node_name
   ```

3. Enable disk sanitization:

   ```
   options licensed_feature.disk_sanitization.enable on
   ```

   You are asked to confirm the command because it is irreversible.

4. Switch to the nodeshell advanced privilege level:

   ```
   priv set advanced
   ```

5. Sanitize the specified disks:

   ```
   disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c
   cycle_count] disk_list
   ```

Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting phase must be restarted and allowed to finish before the disks are sanitized and ready to be returned to the spare pool. If you need to abort the sanitization process, you can do so by using the disk sanitize abort command. If the specified disks are undergoing the formatting phase of sanitization, the abort does not occur until the phase is complete.

`-p pattern1 -p pattern2 -p pattern3` specifies a cycle of one to three user-defined hex byte overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

`-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

`-c cycle_count` specifies the number of times that the specified overwrite patterns are applied.

The default value is one cycle. The maximum value is seven cycles.

`disk_list` specifies a space-separated list of the IDs of the spare disks to be sanitized.

6. If you want to check the status of the disk sanitization process:

   `disk sanitize status [disk_list]`

7. After the sanitization process is complete, return the disks to spare status:

   `disk sanitize release` *`disk_name`*

8. Return to the nodeshell admin privilege level:

   `priv set admin`

9. Return to the ONTAP CLI:

   `exit`

10. Determine whether all of the disks were returned to spare status:

    `storage aggregate show-spare-disks`

If…	Then…
All of the sanitized disks are listed as spares	You are done. The disks are sanitized and in spare status.

Some of the sanitized disks are not listed as spares	Complete the following steps:
	a. Enter advanced privilege mode:
	`set -privilege advanced`
	b. Assign the unassigned sanitized disks to the appropriate node for each disk:
	`storage disk assign -disk disk_name -owner node_name`
	c. Return the disks to spare status for each disk:
	`storage disk unfail -disk disk_name -s -q`
	d. Return to administrative mode:
	`set -privilege admin`

Result

The specified disks are sanitized and designated as hot spares. The serial numbers of the sanitized disks are written to `/etc/log/sanitized_disks`.

The specified disks' sanitization logs, which show what was completed on each disk, is written to `/mroot/etc/log/sanitization.log`.

Copyright information

Trademark information