Disk sanitization

ONTAP 9

NetApp
January 23, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap/disks-aggregates/sanitization-overview-concept.html on January 23, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Disk sanitization . . . 1
Learn about ONTAP disk sanitization . . . 1
Learn about when ONTAP disk sanitization cannot be performed . . . 1
What happens if ONTAP disk sanitization is interrupted . . . 2
Tips for creating and backing up ONTAP local tiers containing data to be sanitized . . . 2
Sanitize an ONTAP disk . . . 2

Disk sanitization

Learn about ONTAP disk sanitization

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 local tier.

Learn about when ONTAP disk sanitization cannot be performed

Disk sanitization cannot be performed under these circumstances.

- 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.
- 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.

What happens if ONTAP 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 ONTAP local tiers containing data to be sanitized

If you are creating or backing up local tiers 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 an ONTAP 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

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

  Learn more about `storage encryption disk sanitize` in the ONTAP command reference.

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 NetApp Knowledge Base: 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)

After the disk sanitization feature is enabled using nodeshell commands 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.

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

- 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 NetApp Knowledge Base: 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`

Learn more about `storage aggregate show-spare-disks` in the ONTAP command reference.

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, are written to `/mroot/etc/log/sanitization.log`.

Related information

- storage aggregate show
- storage disk assign
- storage disk unfail
- storage encryption disk sanitize

Copyright information

Copyright © 2026 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.