



Manage drives

SANtricity 11.8

NetApp
February 12, 2024

Table of Contents

- Manage drives 1
 - Drive states 1
 - Solid State Disks (SSDs) 2
 - Limit the drive view 3
 - Turn on drive locator light 4
 - View drive status and settings 4
 - Replace drive logically 8
 - Reconstruct drive manually 9
 - Initialize (format) drive 9
 - Fail drive 10
 - Erase drives 11
 - Unlock or reset locked NVMe or FIPS drives 12

Manage drives

Drive states

System Manager reports various states for drives.

Accessibility states

State	Definition
Bypassed	The drive is physically present, but the controller cannot communicate with it on either port.
Incompatible	One of the following conditions exists: <ul style="list-style-type: none">• The drive is not certified for use in the storage array.• The drive has a different sector size.• The drive has unusable configuration data from an older or newer firmware version.
Removed	The drive has been improperly removed from the storage array.
Present	The controller can communicate with the drive on both ports.
Unresponsive	The drive is not responding to commands.

Role states

State	Definition
Assigned	The drive is a member of a pool or volume group.
In-use hot spare	The drive is currently being used as a replacement for a drive that has failed. Hot spares are used only in volume groups, not pools.
Standby hot spare	The drive is ready to be used as a replacement for a drive that has failed. Hot spares are used only in volume groups, not pools.
Unassigned	The drive is not a member of a pool or volume group.

Availability states

State	Definition
Failed	The drive is not working. The data on the drive is not available.

State	Definition
Impending Failure	It has been detected that the drive could fail soon. The data on the drive is still available.
Offline	The drive is not available for storing data usually because it is part of a volume group that is being exported or it is undergoing a firmware upgrade.
Optimal	The drive is working normally.

Solid State Disks (SSDs)

Solid-state disks (SSDs) are data storage devices that use solid state memory (flash) to store data persistently. SSDs emulate conventional hard drives, and are available with the same interfaces that hard drives use.

Advantages of SSDs

The advantages of SSDs over hard drives include:

- Faster start up (no spin up)
- Lower latency
- Higher I/O operations per second (IOPS)
- Higher reliability with fewer moving parts
- Lower power usage
- Less heat produced and less cooling required

Identifying SSDs

From the Hardware page, you can locate the SSDs in the front-shelf view. Look for drive bays that display a lightning bolt icon, which indicates an SSD is installed.

Volume groups

All drives in a volume group must be of the same media type (either all SSDs or all hard drives). Volume groups cannot have a mixture of media types or interface types.

Caching

The controller's write caching is always enabled for SSDs. Write caching improves performance and extends the life of the SSD.

In addition to the controller cache, you can implement the SSD cache feature to improve overall system performance. In SSD cache, the data is copied from volumes and stored on two internal RAID volumes (one per controller).

Limit the drive view

If the storage array includes drives with different types of physical and logical attributes, the Hardware page provides filter fields that help you limit the drive view and locate specific drives.

About this task

The drive filters can limit the view to only certain types of physical drives (for example, all SAS), with certain security attributes (for example, secure-capable), at certain logical locations (for example, Volume Group 1). You can use these filters together or separately.



If all drives share the same physical attributes, the **Show drives that are...** filter field does not appear. If all drives share the same logical attributes, the **Anywhere in the storage array** filter field does not appear.

Steps

1. Select **Hardware**.
2. In the first filter field (under **Show drives that are...**), click the drop-down arrow to display the available drive types and security attributes.

Drive types might include:

- Drive media type (SSD, HDD)
 - Drive interface type
 - Drive capacity (highest to lowest)
 - Drive speed (highest to lowest)
- Security attributes might include:
- Secure-capable
 - Secure-enabled
 - DA (Data Assurance) capable
 - FIPS compliant
 - FIPS compliant (FIPS 140-2)
 - FIPS compliant (FIPS 140-3)

If any of these attributes are the same for all drives, they are not shown in the drop-down list. For example, if the storage array includes all SSD drives with SAS interfaces and speeds of 15000 RPM, but some SSDs have different capacities, the drop-down list displays only the capacities as a filtering choice.

When you select an option from the field, the drives that do not match your filter criteria are grayed out in the graphic view.

3. In the second filter box, click the drop-down arrow to display the available logical locations for the drives.



If you need to clear your filter criteria, select **Clear** on the far right of the filter boxes.

Logical locations might include:

- Pools
- Volume Groups
- Hot spare
- SSD Cache
- Unassigned

When you select an option from the field, the drives that do not match your filter criteria are grayed out in the graphic view.

4. Optionally, you can select **Turn on locator lights** at the far right of the filter fields to turn on the locator lights for the displayed drives.

This action helps you physically locate the drives in the storage array.

Turn on drive locator light

From the Hardware page, you can turn on the locator light to find the physical location of a drive in the storage array.

About this task

You can locate single drives or multiple drives shown on the Hardware page.

Steps

1. Select **Hardware**.
2. To locate one or more drives, do one of the following:
 - **Single drive** — From the shelf graphic, find the drive you want to physically locate in the array. (If the graphic shows the controllers, click **Show front of shelf**.) Click the drive to display its context menu, and then select **Turn on locator light**.

The drive's locator light turns on. When you have physically located the drive, return to the dialog and select **Turn off**.

- **Multiple drives** — In the filter fields, select a physical drive type from the left drop-down list and a logical drive type from the right drop-down list. The number of drives matching your criteria is shown on the far right of the fields. Next, you can either click **Turn on locator lights** or select **Locate all filtered drives** from the context menu. When you have physically located the drives, return to the dialog and select **Turn off**.

View drive status and settings

You can view status and settings for the drives, such as the media type, interface type, and capacity.

Steps

1. Select **Hardware**.
2. If the graphic shows the controllers, click **Show front of shelf**.

The graphic changes to show the drives instead of the controllers.

3. Select the drive for which you want to view status and settings.

The drive's context menu opens.


4. Select **View settings**.

The Drive Settings dialog box opens.

5. To see all settings, click **Show more settings** in the upper right of the dialog box.

Field details

Settings	Description
Status	Displays Optimal, Offline, Non-critical fault, and Failed. Optimal status indicates the desired working condition.
Mode	Displays Assigned, Unassigned, Hot Spare Standby, or Hot Spare in Use.
Location	Shows the shelf and bay number where the drive is located.
Assigned to/Can protect for/Protecting	<p>If the drive is assigned to a pool, volume group, or SSD cache, this field displays "Assigned to." The value can be a pool name, volume group name, or SSD cache name. If the drive is assigned to a hot spare and its mode is Standby, this field displays "Can protect for." If the hot spare can protect one or more volume groups, the volume group names appear. If it cannot protect a volume group, it displays 0 volume groups.</p> <p>If the drive is assigned to a hot spare and its mode is In Use, this field displays "Protecting." The value is the name of the affected volume group.</p> <p>If the drive is unassigned, this field does not appear.</p>
Media type	Displays the type of recording media the drive uses, which can be either hard disk drive (HDD) or solid state disk (SSD).
Percent endurance used (only shown if SSD drives are present)	The amount of data written to the drive to date, divided by the total theoretical write limit.
Interface type	Displays the type of interface the drive uses, such as SAS.
Drive path redundancy	Shows whether connections between the drive and controller are redundant (Yes) or not (No).
Capacity (GiB)	Shows the usable capacity (total configured capacity) of the drive.
Speed (RPM)	Shows the speed in RPM (does not appear for SSDs).
Current data rate	Shows the data transfer rate between the drive and the storage array.
Logical sector size (bytes)	Shows the logical sector size that the drive uses.
Physical sector size (bytes)	Shows the physical sector size that the drive uses. Typically, the physical sector size is 4096 bytes for hard disk drives.
Drive firmware version	Shows the revision level of the drive firmware.

Settings	Description
World-wide identifier	Shows the unique hexadecimal identifier for the drive.
Product ID	Shows the product identifier, which is assigned by the manufacturer.
Serial number	Shows the serial number of the drive.
Manufacturer	Shows the vendor of the drive.
Date of manufacture	Shows the date the drive was built.  Not available for NVMe drives.
Secure-capable	Shows whether the drive is secure-capable (Yes) or not (No). Secure-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives (level 140-2 or 140-3), which encrypt data during writes and decrypt data during reads. These drives are considered <i>secure-capable</i> because they can be used for additional security using the Drive Security feature. If the Drive Security feature is enabled for volume groups and pools used with these drives, the drives become <i>secure-enabled</i> .
Secure-enabled	Shows whether the drive is secure-enabled (Yes) or not (No). Secure-enabled drives are used with the Drive Security feature. When you enable the Drive Security feature and then apply Drive Security to a pool or volume group on <i>secure-capable</i> drives, the drives become <i>secure-enabled</i> . Read and write access is available only through a controller that is configured with the correct security key. This added security prevents unauthorized access to the data on a drive that is physically removed from the storage array.
Read/write accessible	Shows whether the drive is read/write accessible (Yes) or not (No).
Drive security key identifier	Shows the security key for secure-enabled drives. Drive Security is a storage array feature that provides an extra layer of security with either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives. When these drives are used with the Drive Security feature, they require a security key for access to their data. When the drives are physically removed from the array, they cannot operate until they are installed in another array, at which point, they will be in a Security Locked state until the correct security key is provided.
Data Assurance (DA) capable	Shows whether the Data Assurance (DA) feature is enabled (Yes) or not (No). Data Assurance (DA) is a feature that checks for and corrects errors that might occur as data is transferred through the controllers down to the drives. Data Assurance can be enabled at the pool or volume group level, with hosts using a DA-capable I/O interface such as Fibre Channel.

Settings	Description
DULBE capable	Indicates whether the option for Deallocated or Unwritten Logical Block Error (DULBE) is enabled (Yes) or not (No). DULBE is an option on NVMe drives that allows the EF300 or EF600 storage array to support resource-provisioned volumes.

6. Click **Close**.

Replace drive logically

If a drive fails or you want to replace it for any other reason, you can logically replace the failed drive with an unassigned drive or a fully integrated hot spare.

About this task

When you logically replace a drive, it becomes assigned and is then a permanent member of the associated pool or volume group.

You use the logical replace option to replace the following types of drives:

- Failed drives
- Missing drives
- SSD drives that the Recovery Guru has notified you that are nearing their end of life
- Hard drives that the Recovery Guru has notified you that have an impending drive failure
- Assigned drives (available only for drives in a volume group, not in a pool)

Before you begin

The replacement drive must have the following characteristics:

- In the Optimal state
- In the Unassigned state
- The same attributes as the drive being replaced (media type, interface type, and so on)
- The same FDE capability (recommended, but not required)
- The same DA capability (recommended, but not required)

Steps

1. Select **Hardware**.
2. If the graphic shows the controllers, click **Show front of shelf**.

The graphic changes to show the drives instead of the controllers.

3. Click the drive that you want to logically replace.

The drive's context menu appears.

4. Click **Logically replace**.

5. **Optional:** Select the **Fail drive after it is replaced** check box to fail the original drive after it is replaced.

This check box is enabled only if the original assigned drive is not failed or missing.

6. From the **Select a replacement drive** table, select the replacement drive that you want to use.

The table lists only those drives that are compatible with the drive that you are replacing. If possible, select a drive that will maintain shelf loss protection and drawer loss protection.

7. Click **Replace**.

If the original drive is failed or missing, data is reconstructed on the replacement drive using the parity information. This reconstruction begins automatically. The drive's fault indicator lights go off, and the activity indicator lights of the drives in the pool or volume group start flashing.

If the original drive is not failed or missing, its data is copied to the replacement drive. This copy operation begins automatically. After the copy operation completes, the system transitions the original drive to the Unassigned state, or if the check box was selected, to the Failed state.

Reconstruct drive manually

Drive reconstruction normally starts automatically after you replace a drive. If drive reconstruction does not start automatically, you can start reconstruction manually.



Perform this operation only when instructed to do so by technical support or the Recovery Guru.

Steps

1. Select **Hardware**.
2. If the graphic shows the controllers, click **Show front of shelf**.

The graphic changes to show the drives instead of the controllers.

3. Click the drive that you want to manually reconstruct.

The drive's context menu appears.

4. Select **Reconstruct**, and confirm that you want to perform the operation.

Initialize (format) drive

If you move assigned drives from one storage array to another, you must initialize (format) the drives before they can be used in the new storage array.

About this task

Initializing removes the previous configuration information from a drive and returns it to the Unassigned state. The drive is then available for adding to a new pool or volume group in the new storage array.

Use the initialize drive operation when you are moving a single drive. You do not need to initialize drives if you are moving an entire volume group from one storage array to another.



Possible loss of data — When you initialize a drive, all data on the drive is lost. Perform this operation only when instructed to do so by technical support.

Steps

1. Select **Hardware**.
2. If the graphic shows the controllers, click **Show front of shelf**.

The graphic changes to show the drives instead of the controllers.

3. Click the drive that you want to initialize.

The drive's context menu appears.

4. Select **Initialize**, and confirm that you want to perform the operation.

Fail drive

If instructed to do so, you can manually fail a drive.

About this task

System Manager monitors the drives in the storage array. When it detects that a drive is generating a lot of errors, the Recovery Guru notifies you of an impending drive failure. If this happens and you have a replacement drive available, you might want to fail the drive to take preemptive action. If you do not have a replacement drive available, you can wait for the drive to fail on its own.



Possible loss of data access — This operation could result in data loss or the loss of data redundancy. Perform this operation only when instructed to do so by technical support or the Recovery Guru.

Steps

1. Select **Hardware**.
2. If the graphic shows the controllers, click **Show front of shelf**.

The graphic changes to show the drives instead of the controllers.

3. Click the drive that you want to fail.

The drive's context menu appears.

4. Select **Fail**.
5. Keep the **Copy contents of drive before failing** check box selected.

The copy option appears only for assigned drives and for non-RAID 0 volume groups.

Before you fail the drive, make sure that you copy the drive's contents. Depending on your configuration, you could potentially lose all data or data redundancy on the associated pool or volume group if you do not copy the drive's contents first.

The copy option allows faster drive recovery than reconstruction and reduces the possibility of a volume failure if another drive were to fail during the copy operation.

6. Confirm that you want to fail the drive.

After the drive has failed, wait at least 30 seconds before you remove it.

Erase drives

You can use the Erase option to prepare an unassigned drive for removal from the system. This procedure permanently removes data, ensuring that the data cannot be read again.

Before you begin

The drive must be in an Unassigned state.

About this task

Use the Erase option only if you want to permanently remove all data on a drive. If the drive is secure-enabled, the Erase option performs a cryptographic erase and resets the drive's security attributes back to secure-capable.



The Erase feature does not support some older drive models. If you attempt to erase one of these older models, an error message appears.

Steps

1. Select **Hardware**.
2. If the graphic shows the controllers, click **Show front of shelf**.

The graphic changes to show the drives instead of the controllers.

3. Optionally, you can use the filter fields to view all the unassigned drives in the shelf. From the **Show drives that are...** drop-down list, select **Unassigned**.

The shelf view shows only the unassigned drives; all others are grayed out.

4. To open the drive's context menu, click on a drive that you want to erase. (If you want to select multiple drives, you can do so in the Erase Drives dialog box.)



Possible loss of data — The Erase operation cannot be undone. Make sure you select the correct drives during the procedure.

5. From the context menu, select **Erase**.

The Erase Drives dialog box opens, showing all the eligible drives for an erase operation.

6. If desired, select additional drives from the table. You cannot select *all* drives; be sure one drive remains deselected.
7. Confirm the operation by typing `erase`, and then click **Erase**.



Be sure you want to continue with this operation. Once you click Yes in the next dialog, the operation cannot be aborted.

8. In the Estimated Completion Time dialog box, click **Yes** to continue with the erase operation.

Results

The Erase operation might take several minutes or several hours. You can view the status in **Home > View Operations in Progress**. When the Erase operation completes, the drives are available for use in another volume group or disk pool, or in another storage array.

After you finish

If you want to use the drive again, you must initialize it first. To do this, select **Initialize** from the drive's context menu.

Unlock or reset locked NVMe or FIPS drives

If you insert one or more locked NVMe or FIPS drives into a storage array, you can unlock the drive data by adding the security key file associated with the drives. If you do not have a security key, you can perform a reset on each locked drive by entering its Physical Security ID (PSID) to reset its security attributes and erase the drive data.

Before you begin

- For the Unlock option, make sure the security key file (with an extension of `.slk`) is available on the management client (the system with a browser used for accessing System Manager). You must also know the pass phrase associated with the key.
- For the Reset option, you must find the PSID on each drive you want to reset. To locate the PSID, physically remove the drive and locate the PSID string (32 characters maximum) on the drive's label, and then reinstall the drive.

About this task

This task describes how to unlock data in NVMe or FIPS drives by importing a security key file into the storage array. For situations where the security key is not available, this task also describes how to perform a reset on a locked drive.



If the drive was locked using an external key management server, select **Settings > System > Security key management** in System Manager to configure external key management and unlock the drive.

You can access the Unlock feature from either the Hardware page or from **Settings > System > Security key management**. The task below provides instructions from the Hardware page.

Steps

1. Select **Hardware**.
2. If the graphic shows the controllers, click **Show front of shelf**.

The graphic changes to show the drives instead of the controllers.

3. Select the NVMe or FIPS drive you want to unlock or reset.

The drive's context menu opens.

4. Select **Unlock** to apply the security key file or **Reset** if you do not have a security key file.

These options only appear if you select a locked NVMe or FIPS drive.



During a Reset operation, all data is erased. Only perform a Reset if you do not have a security key. Resetting a locked drive permanently removes all data on the drive and resets its security attributes to "secure-capable," but not enabled. **This operation is not reversible.**

5. Do one of the following:

- a. **Unlock:** In the **Unlock Secure Drive** dialog box, click **Browse**, and then select the security key file that corresponds to the drive you want to unlock. Next, enter the pass phrase, and then click **Unlock**.
- b. **Reset:** In the **Reset Locked Drive** dialog box, enter the PSID string in the field, and then type `RESET` to confirm. Click **Reset**.

For an Unlock operation, you only need to perform this operation once to unlock all the NVMe or FIPS drives. For a Reset operation, you must individually select each drive you want to reset.

Results

The drive is now available for use in another volume group or disk pool, or in another storage array.

Copyright information

Copyright © 2024 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.