Manage drives

SANtricity 11.6

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity-116/sm-storage/turn-on-locator-lights-in-a-pool-volume-group-or-ssd-cache.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Manage drives . . . 1
- Turn on locator lights in a pool, volume group, or SSD Cache . . . 1
- Remove capacity from a pool or SSD Cache . . . 1
- Enable security for a pool or volume group . . . 2
- Assign hot spares . . . 3
- Replace drive logically . . . 4

Manage drives

Turn on locator lights in a pool, volume group, or SSD Cache

You can locate drives to physically identify all of the drives that comprise a selected pool, volume group, or SSD Cache. An LED indicator lights up on each drive in the selected pool, volume group, or SSD Cache.

Steps

1. Select **Storage › Pools & Volume Groups**.
2. Select the pool, volume group, or SSD Cache you want to locate, and then click **More › Turn on locator lights**.

   A dialog box appears that indicates the lights on the drives comprising the selected pool, volume group, or SSD Cache are turned on.

3. After you successfully locate the drives, click **Turn Off**.

Remove capacity from a pool or SSD Cache

You can remove drives to decrease the capacity of an existing pool or SSD Cache. After you remove drives, the data in each volume of the pool or SSD Cache is redistributed to the remaining drives. The removed drives become unassigned and their capacity becomes part of the total free capacity of the storage array.

About this task

Follow these guidelines when you remove capacity:

- You cannot remove the last drive in an SSD Cache without first deleting the SSD Cache.
- You cannot reduce the number of drives in a pool to be less than 11 drives.
- You can remove a maximum of 12 drives at a time. If you need to remove more than 12 drives, repeat the procedure.
- You cannot remove drives if there is not enough free capacity in the pool or SSD Cache to contain the data, when that data is redistributed to the remaining drives in the pool or SSD Cache.

Read about potential performance impacts

- Removing drives from a pool or SSD Cache might result in reduced volume performance.
- The preservation capacity is not consumed when you remove capacity from a pool or SSD Cache. However, the preservation capacity might decrease based on the number of drives remaining in the pool or SSD Cache.

Read about impacts to secure-capable drives

- If you remove the last drive that is not secure-capable, the pool is left with all secure-capable drives. In this situation, you are given the option to enable security for the pool.
- If you remove the last drive that is not Data Assurance (DA) capable, the pool is left with all DA-capable drives.

Any new volumes that you create on the pool will be DA-capable. If you want existing volumes to be DA-capable, you need to delete and then re-create the volume.

Steps

1. Select **Storage › Pools & Volume Groups**.
2. Select the pool or SSD Cache, and then click **More › Remove capacity**.

   The **Remove Capacity** dialog box appears.
3. Select one or more drives in the list.

   As you select or de-select drives in the list, the **Total capacity selected** field updates. This field shows the total capacity of the pool or SSD Cache that results after you remove the selected drives.
4. Click **Remove**, and then confirm you want to remove the drives.

Results

The newly reduced capacity of the pool or SSD Cache is reflected in the Pools and Volume Groups view.

Enable security for a pool or volume group

You can enable Drive Security for a pool or volume group to prevent unauthorized access to the data on the drives contained in the pool or volume group. Read and write access for the drives is only available through a controller that is configured with a security key.

Before you begin

- The Drive Security feature must be enabled.
- A security key must be created.
- The pool or volume group must be in an Optimal state.
- All of the drives in the pool or volume group must be secure-capable drives.

About this task

If you want to use Drive Security, select a pool or volume group that is secure-capable. A pool or volume group can contain both secure-capable and non-secure-capable drives, but all drives must be secure-capable to use their encryption capabilities.

After enabling security, you can only remove it by deleting the pool or volume group, and then erasing the drives.

Steps

1. Select **Storage › Pools & Volume Groups**.

2. Select the pool or volume group on which you want to enable security, and then click **More › Enable security**.

   The **Confirm Enable Security** dialog box appears.

3. Confirm that you want to enable security for the selected pool or volume group, and then click **Enable**.

Assign hot spares

You can assign a hot spare as a standby drive for additional data protection in RAID 1, RAID 5, or RAID 6 volume groups. If a drive fails in one of these volume groups, the controller reconstructs data from the failed drive to the hot spare.

Before you begin

- RAID 1, RAID 5, or RAID 6 volume groups must be created. (Hot spares cannot be used for pools. Instead, a pool uses spare capacity within each drive for its data protection.)
- A drive that meets the following criteria must be available:
  - Unassigned, with Optimal status.
  - Same media type as the drives in the volume group (for example, SSDs).
  - Same interface type as the drives in the volume group (for example, SAS).
  - Capacity equal to or larger than the used capacity of the drives in the volume group.

About this task

This task describes how to manually assign a hot spare from the Hardware page. The recommended coverage is two hot spares per drive set.

Hot spares can also be assigned from the Initial Setup wizard. You can determine if hot spares are already assigned by looking for drive bays shown in pink on 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 an unassigned drive (shown in gray) that you want to use as a hot spare.

   The drive's context menu opens.

4. Select **Assign hot spare**.

   If the drive is secure-enabled, the **Secure Erase Drive** dialog box opens. To use a secure-enabled drive as a hot spare, you must first perform a Secure Erase operation to remove all its data and reset its security attributes.

   Possible loss of data — Make sure that you have selected the correct drive. After completing the Secure Erase operation, you cannot recover any of the data.

   If the drive is **not** secure-enabled, the **Confirm Assign Hot Spare Drive** dialog box opens.

5. Review the text in the dialog box, and then confirm the operation.

   The drive is displayed in pink on the Hardware page, which indicates it is now a hot spare.

Results

If a drive within a RAID 1, RAID 5, or RAID 6 volume group fails, the controller automatically uses redundancy data to reconstruct the data from the failed drive to the hot spare.

Replace drive logically

If a drive fails or you want to replace it for any other reason, and you have an unassigned drive in your storage array, you can logically replace the failed drive with the unassigned drive. If you do not have an unassigned drive, you can physically replace the drive instead.

About this task

When you logically replace a drive with an unassigned drive, the unassigned drive 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)

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.

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.