Preparing storage systems for SnapMirror and SnapVault replication

SnapManager for SAP

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/snapmanager-sap/unix-installation-7mode/concept-understanding-the-differences-between-snapmirror-and-snapvault.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Preparing storage systems for SnapMirror and SnapVault replication 1
Understanding the differences between SnapMirror and SnapVault 1
Prepare storage systems for SnapMirror replication 1
Prepare storage systems for SnapVault replication 3

Preparing storage systems for SnapMirror and SnapVault replication

You can use SnapManager with ONTAP SnapMirror technology to create mirror copies of backup sets on another volume, and with ONTAP SnapVault technology to perform disk-to-disk backup replication for standards compliance and other governance-related purposes. Before you perform these tasks, you must configure a *data-protection relationship* between the source and destination volumes and *initialize* the relationship.

A data protection relationship replicates data on primary storage (the source volume) to secondary storage (the destination volume). When you initialize the relationship, ONTAP transfers the data blocks referenced on the source volume to the destination volume.

Understanding the differences between SnapMirror and SnapVault

SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. SnapVault is disk-to-disk backup replication technology, designed for standards compliance and other governance-related purposes.

These objectives account for the different balance each technology strikes between the goals of backup currency and backup retention:

- SnapMirror stores *only* the Snapshot copies that reside in primary storage, because, in the event of a disaster, you need to be able to fail over to the most recent version of primary data you know to be good.

  Your organization, for example, might mirror hourly copies of production data over a ten-day span. As the failover use case implies, the equipment on the secondary system must be equivalent or nearly equivalent to the equipment on the primary system to serve data efficiently from mirrored storage.

- SnapVault, in contrast, stores Snapshot copies *whether or not* they currently reside in primary storage, because, in the event of an audit, access to historical data is likely to be as important as access to current data.

  You might want to keep monthly Snapshot copies of your data over a 20-year span, for example, to comply with government accounting regulations for your business. Because there is no requirement to serve data from secondary storage, you can use slower, less expensive disks on the vault system.

The different weights that SnapMirror and SnapVault give to backup currency and backup retention ultimately derive from the limit of 255 Snapshot copies for each volume. While SnapMirror retains the most recent copies, SnapVault retains the copies made over the longest period of time.

Prepare storage systems for SnapMirror replication

Before you can use SnapManager's integrated SnapMirror technology to mirror Snapshot copies, you must configure and initialize a *data-protection relationship* between the source and destination volumes. On initialization, SnapMirror makes a Snapshot copy of

the source volume, then transfers the copy and all the data blocks it references to the destination volume. It also transfers any other, less recent Snapshot copies on the source volume to the destination volume.

About this task

You can use the ONTAP CLI or OnCommand System Manager to perform these tasks. The procedure below is based on the assumption that you are using the CLI. For more information, see the Data ONTAP 8.2 Data Protection Online Backup and Recovery Guide for 7-Mode.

You cannot use SnapManager to mirror qtrees. SnapManager supports volume mirroring only.

You cannot use SnapManager for synchronous mirroring. SnapManager supports asynchronous mirroring only.

If you are storing database files and transaction logs on different volumes, you must create relationships between the source and destination volumes for the database files and between the source and destination volumes for the transaction logs.

1. On the source system console, use the `options snapmirror.access` command to specify the host names of systems that are allowed to copy data directly from the source system.

   Example

   The following entry allows replication to destination_systemB:

   ```
   options snapmirror.access host=destination_systemB
   ```

2. On the destination system, create or edit the `/etc/snapmirror.conf` file to specify the volume to be copied.

   Example

   The following entry specifies replication from vol0 of source_systemA to vol2 of destination_systemB:

   ```
   source_systemA:vol0 destination_systemB:vol2
   ```

3. On both the source and destination system consoles, use the `snapmirror on` command to enable SnapMirror.

   Example

   The following command enables SnapMirror:

   ```
   snapmirror on
   ```

4. On the destination system console, use the `vol create` command to create a SnapMirror destination volume that is the same or greater in size than the source volume.

Example

The following command creates a 2-GB destination volume named vol2 on the aggregate aggr1:

```
vol create vol2 aggr1 2g
```

5. On the destination system console, use the vol restrict command to mark the destination volume as restricted.

   Example

   The following command marks the destination volume vol2 as restricted:

   ```
   vol restrict vol2
   ```

6. On the source system console, use the `snap sched` command to disable any scheduled transfers.

   Example

   You must disable scheduled transfers to avoid scheduling conflicts with SnapDrive.

   The following command disables scheduled transfers:

   ```
   snap sched vol1 -----
   ```

7. On the destination system console, use the `snapmirror initialize` command to create a relationship between the source and destination volumes, and initialize the relationship.

   The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume. It also transfers any other Snapshot copies on the source volume to the destination volume.

   Example

   The following command creates a SnapMirror relationship between the source volume vol0 on source_systemA and the destination volume vol2 on destination_systemB, and initializes the relationship:

   ```
   snapmirror initialize -S source_systemA:vol0 destination_systemB:vol2
   ```

Prepare storage systems for SnapVault replication

Before you can use SnapManager's integrated SnapVault technology to archive Snapshot copies to disk, you must configure and initialize a *data-protection relationship* between the source and destination volumes. On initialization, SnapVault makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it

references to the destination volume.

What you'll need

- You must have configured a dataset for the primary storage location in the SnapManager Configuration wizard.
- All LUNs must be in qtrees, with one LUN per qtree.

> If you are storing database files and transaction logs on different volumes, you must create relationships between the source and destination volumes for the database files and between the source and destination volumes for the transaction logs.

Steps

1. On both the source and destination system consoles, enable SnapVault:

   Example

   ```
   options snapvault.enable on
   ```

2. On the source system console, use the `options snapvault.access` command to specify the host names of systems that are allowed to copy data directly from the source system.

   Example

   The following command allows replication to destination_systemB:

   ```
   options snapvault.access host=destination_systemB
   ```

3. On the destination system console, use the `options snapvault.access` command to specify the host names of systems to which copied data can be restored.

   Example

   The following command allows copied data to be restored to source_systemA:

   ```
   options snapvault.access host=destination_systemA
   ```

4. On the source system console, use the `ndmpd on` command to enable NDMP.

   Example

   The following command enables NDMP:

   ```
   ndmpd on
   ```

5. On the destination system console, use the `vol create` command to create a SnapMirror destination

volume that is the same or greater in size than the source volume.

Example

The following command creates a 2-GB destination volume named vol2 on the aggregate aggr1:

```
vol create vol2 aggr1 2g
```

6. In the OnCommand Unified Manager (UM) NetApp Management Console, add the resource pool for the destination volume:
   a. Click **Data** > **Resource Pools** to open the **Resource Pools** page.
   b. On the Resource Pools page, click **Add** to start the **Add Resource Pool** wizard.
   c. Follow the prompts in the wizard to specify the aggregate for the destination volume.
   d. Click **Finish** to exit the wizard.
7. In the UM NetApp Management Console, assign the resource pool to the dataset you created in the SnapManager Configuration wizard:
   a. Click **Data** > **Datasets** to open the Datasets page.
   b. On the **Datasets** page, select the dataset you created and click **Edit**.
   c. On the **Edit Dataset** page, click **Backup** > **Provisioning/Resource Pools** to open the **Configure Dataset Node** wizard.
   d. Follow the prompts in the wizard to assign the resource pool to the dataset.

      Resource pool assignment specifies the data-protection relationship between the source and destination volumes.

   e. Click **Finish** to exit the wizard and initialize the data-protection relationship.

      The initialization process performs a *baseline transfer* to the destination volume. SnapVault makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks it references to the destination volume.

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.