Volume Disaster Recovery Preparation Express Guide
Contents

Deciding whether to use this guide ............................................................. 4
Volume disaster recovery preparation workflow ................................. 5
  Verifying the cluster peer relationship and SVM peer relationship ................. 5
  Creating the SnapMirror relationship (starting with ONTAP 9.3) .................. 6
  Creating the SnapMirror relationship (ONTAP 9.2 or earlier) ......................... 8
  Setting up the destination SVM for data access .............................................. 11
  Monitoring the status of SnapMirror data transfers ......................................... 11
Where to find additional information ............................................................ 13
Copyright ........................................................................................................ 14
Trademark ...................................................................................................... 15
How to send comments about documentation and receive update notifications .......................................................... 16
Index ............................................................................................................... 17
Deciding whether to use the Volume Disaster Recovery Preparation Express Guide

This guide describes how to quickly protect a source volume on a peered ONTAP cluster in preparation for disaster recovery. You should use this guide if you want to configure and monitor SnapMirror relationships between peered clusters for volume disaster recovery and do not need a lot of conceptual background for the tasks.

SnapMirror provides scheduled asynchronous, block-level data protection. SnapMirror replicates Snapshot copies and can replicate NAS or SAN volumes on which deduplication, data compression, or both are run, including volumes containing qtrees and LUNs. SnapMirror configuration information is stored in a database that ONTAP replicates to all the nodes in the cluster.

You should use this guide if you want to create SnapMirror relationships for volume-level disaster recovery in the following way:

• You are working with clusters running ONTAP 9.
• You are a cluster administrator.
• You have configured the cluster peer relationship and the SVM peer relationship.

Cluster and SVM peering express configuration

• You have enabled the SnapMirror license on both the source and the destination clusters.
• You want to use default policies and schedules, and not create custom policies.
• You want to use best practices, not explore every available option.
• You do not want to read a lot of conceptual background.
• You want to use ONTAP System Manager, not the ONTAP command-line interface or an automated scripting tool.

If these assumptions are not correct for your situation, or if you want more conceptual background information, you should see the following resources:

• Data protection
• Logical storage management
• NetApp Documentation: OnCommand Workflow Automation (current releases)

OnCommand Workflow Automation enables you to run prepackaged workflows that automate management tasks such as the workflows described in Express Guides.

• ONTAP 9 commands

Provides the set of commands for configuring and managing SnapMirror relationships. You might want to use the SnapMirror commands to write a script that creates multiple SnapMirror relationships.
Volume disaster recovery preparation workflow

Preparing volumes for disaster recovery involves verifying the cluster peer relationship, creating the SnapMirror relationship between volumes residing on peered clusters, setting up the destination SVM for data access, and monitoring the SnapMirror relationship periodically.

Verifying the cluster peer relationship and SVM peer relationship

Before you set up a volume for disaster recovery, you must verify that the source and destination clusters are peered and are communicating with each other through the peer relationship.

Choices

- If you are running ONTAP 9.3 or later, perform the following steps to verify the cluster peer relationship and SVM peer relationship:
  1. Click Configuration > Cluster Peers.
  2. Verify that the peered cluster is authenticated and is available.
  3. Click Configuration > SVM Peers.
  4. Verify that the destination SVM is peered with the source SVM.

- If you are running ONTAP 9.2 or earlier, perform the following steps to verify the cluster peer relationship and SVM peer relationship:
  1. Click the Configurations tab.
2. In the Cluster Details pane, click Cluster Peers.

3. Verify that the peered cluster is authenticated and available.

4. Click the SVMs tab and select the source SVM.

5. In the Peer Storage Virtual Machines area, verify the destination SVM is peered with the source SVM.

   If you do not see any peered SVM in this area, you can create the SVM peer relationship when creating the SnapMirror relationship.

   *Creating the SnapMirror relationship (ONTAP 9.2 or earlier)* on page 8

---

**Creating the SnapMirror relationship (starting with ONTAP 9.3)**

You must create a SnapMirror relationship between the source volume on one cluster and the destination volume on the peered cluster for replicating data for disaster recovery.

**Before you begin**

- The destination aggregate must have available space.
- Both the clusters must be configured and set up appropriately to meet the requirements of your environment for user access, authentication, and client access.

**About this task**

You must perform this task from the source cluster.

**Steps**

1. Click Storage > Volumes.

2. Select the volume for which you want to create a mirror relationship, and then click Actions > Protect.

3. In the Relationship Type section, select Mirror from the Relationship Type drop-down list.

4. In the Volumes: Protect Volumes page, provide the following information:

   a. Select Mirror as the relationship type.

   b. Select the destination cluster, destination SVM, and the suffix for the name of the destination volume.

      Only peered SVMs and allowed SVMs are listed under destination SVMs.

   c. Click ⚙.

   d. In the Advanced Options dialog box, verify that MirrorAllSnapshots is set as the protection policy.
DPDefault and MirrorLatest are the other default protection policies that are available for SnapMirror relationships.

e. Select a protection schedule.
   By default, the hourly schedule is selected.

f. Verify that Yes is selected for initializing the SnapVault relationship.
   All of the data protection relationships are initialized by default. Initializing the SnapMirror relationship ensures that the destination volume has a baseline to start protecting the source volume.

g. Click Apply to save the changes.

Advanced Options

<table>
<thead>
<tr>
<th>Protection Policy</th>
<th>MirrorAllSnapshots</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnapMirror Labels</td>
<td>Retention Count</td>
</tr>
<tr>
<td>sm_created</td>
<td>1</td>
</tr>
<tr>
<td>all_source_snapshots</td>
<td>1</td>
</tr>
</tbody>
</table>

Protection Schedule: hourly
Every hour at 05 minute(s)

Initialize Protection: Yes

SnapLock for SnapVault is not supported for the selected destination or the selected relationship type.

FabricPool: There is no FabricPool assigned to the destination SVM.

Apply

5. Click Save to create the SnapMirror relationship.

6. Verify that the relationship status of the SnapMirror relationship is in the Snapmirrored state.
   a. Navigate to the Volumes window, and then select the volume that the volume for which you created the SnapMirror relationship.
   b. Double-click the volume to view the volume details, and then click PROTECTION to view the data protection status of the volume.
After you finish
You must make a note of the settings for the source volume such as thin provisioning, deduplication, compression, and autogrow. You can use this information to verify the destination volume settings when you break the SnapMirror relationship.

Creating the SnapMirror relationship (ONTAP 9.2 or earlier)
You must create a SnapMirror relationship between the source volume on one cluster and the destination volume on the peered cluster for replicating data for disaster recovery.

Before you begin
• You must have the cluster administrator user name and password for the destination cluster.
• The destination aggregate must have available space.
• Both the clusters must be configured and set up appropriately to meet the requirements of your environment for user access, authentication, and client access.

About this task
You must perform this task from the source cluster.

Steps
1. Click Storage > SVMs.
2. Select the SVM, and then click SVM Settings.
3. Click the Volumes tab.
4. Select the volume for which you want to create a mirror relationship, and then click Protect.
   The Create Protection Relationship window is displayed.
5. In the Relationship Type section, select Mirror from the Relationship Type drop-down list.
6. In the Destination Volume section, select the peered cluster.
7. Specify the SVM for the destination volume:
<table>
<thead>
<tr>
<th>If the SVM is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peered</td>
<td>Select the peer SVM from the list.</td>
</tr>
<tr>
<td>Not peered</td>
<td>a. Select the SVM.</td>
</tr>
<tr>
<td></td>
<td>b. Click Authenticate.</td>
</tr>
<tr>
<td></td>
<td>c. Enter the cluster administrator's credentials of the peer cluster, and then click Create.</td>
</tr>
</tbody>
</table>
8. Create a new destination volume:
a. Select the **New Volume** option.

b. Use the default volume name or specify a new volume name.

c. Select the destination aggregate.

9. In the **Configuration Details** section, select **MirrorAllSnapshots** as the mirror policy.

   **DPDefault** and **MirrorLatest** are the other default mirror policies that are available for SnapMirror relationships.

10. Select a protection schedule from the list of schedules.

11. Ensure that the **Initialize Relationship** check box is selected, and then click **Create**.

   Initializing the SnapMirror relationship ensures that the destination volume has a baseline to start protecting the source volume.

The relationship is initialized by starting a baseline transfer of data from the source volume to the destination volume.

The initialization operation might take some time. The Status section shows the status of each job.
12. Verify the relationship status of the SnapMirror relationship:

   a. Select the volume for which you created the SnapMirror relationship from the **Volumes** list, and then click **Data Protection**.

   b. In the **Data Protection** tab, verify that the SnapMirror relationship that you created is listed and that the relationship state is **Snapmirrored**.

After you finish

You must make a note of the settings for the source volume such as thin provisioning, deduplication, compression, and autogrow. You can use this information to verify the destination volume settings when you break the SnapMirror relationship.
Setting up the destination SVM for data access

You can minimize data access disruption when activating the destination volume by setting up required configurations such as LIFs, CIFS shares, and export policies for the NAS environment, and LIFs and initiator groups for the SAN environment on the SVM containing the destination volume.

About this task
You must perform this task on the destination cluster for the SVM containing the destination volume.

Choices
• NAS environment:
  1. Create NAS LIFs.
  2. Create CIFS shares with the same share names that were used on the source.
  3. Create appropriate NFS export policies.
  4. Create appropriate quota rules.
• SAN environment:
  1. Create SAN LIFs.
  2. Optional: Configure portsets.
  3. Configure initiator groups.
  4. For FC, zone the FC switches to enable the SAN clients to access the LIFs.

After you finish
If any changes were made on the SVM containing the source volume, you must replicate the changes manually on the SVM containing the destination volume.

Related information
ONTAP 9 Documentation Center

Monitoring the status of SnapMirror data transfers

You should periodically monitor the status of the SnapMirror relationships to ensure that the SnapMirror data transfers are occurring as per the specified schedule.

About this task
You must perform this task from the destination cluster.

Steps
1. Depending on the System Manager version that you are running, perform one of the following steps:
   • ONTAP 9.4 or earlier: Click Protection > Relationships.
   • Starting with ONTAP 9.5: Click Protection > Volume Relationships.
2. Select the SnapMirror relationship between the source and the destination volumes, and then verify the status in the **Details** bottom tab.

The Details tab displays the health status of the SnapMirror relationship and shows the transfer errors and lag time.

- The **Is Healthy** field must display **Yes**.
  For most SnapMirror data transfer failures, the field displays **No**. In some failure cases, however, the field continues to display **Yes**. You must check the transfer errors in the Details section to ensure that no data transfer failure occurred.

- The **Relationship State** field must display **Snapmirrored**.

- The **Lag Time** must be no more than the transfer schedule interval.
  For example, if the transfer schedule is hourly, then the lag time must not be more than an hour.

You should troubleshoot any issues in the SnapMirror relationships.

Where to find additional information

Additional documentation is available to help you activate the destination volume to test the disaster recovery setup or when a disaster occurs. You can also learn more about how to reactivate the source volume after the disaster.

Express guide

- Volume disaster express recovery
  Describes how to quickly activate a destination volume after a disaster and then reactivate the source volume in ONTAP.

Power guide

- Data protection
  Describes how to prevent data loss using Snapshot copies and SnapMirror replication to a remote system

Comprehensive guides

- Active IQ Unified Manager 9.6 Workflow Guide for Managing Cluster Health
  Provides information about performing Active IQ Unified Manager (formerly OnCommand Unified Manager) tasks using the web UI and information about troubleshooting, as well as providing in-depth conceptual information.

- ONTAP concepts
  Provides conceptual information about disaster recovery using SnapMirror technology.
Copyright

Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

A
about this guide
deciding whether to use the Volume Disaster Recovery Preparation Express Guide 4

C
cluster peer relationships
verifying the status 5
comments
how to send feedback about documentation 16

D
data access
setting up the destination SVM 11
data protection
where to get additional information about 13
destination volumes
setting up for data access from 11
disaster recovery
creating SnapMirror relationships between volumes on different clusters for disaster recovery 6, 8
requirements for using the Volume Disaster Recovery Preparation Express Guide to configure mirror relationships for 4
where to get additional information about volumes 13
workflow for volume 5
documentation
how to receive automatic notification of changes to 16
how to send feedback about 16

F
feedback
how to send comments about documentation 16
flowcharts
volume disaster recovery preparation workflow 5

I
information
how to send feedback about improving documentation 16

L
lag times
monitoring SnapMirror relationship health 11

M
mirror relationships
creating between volumes on different clusters for disaster recovery 6, 8
initializing 8
monitoring health of 11

P
peer relationships
verifying the status of cluster 5
verifying the status of SVMs 5
protection
where to get additional information about data 13

R
relationships
monitoring health of SnapMirror 11

S
setting up
destination volume 11
SnapMirror
workflow for volume disaster recovery preparation 5
SnapMirror relationships
creating between volumes on different clusters for disaster recovery, ONTAP 9.2 or earlier 8
creating between volumes on different clusters for disaster recovery, starting with ONTAP 9.3 6
See also mirror relationships
suggestions
how to send feedback about documentation 16
SVM peer relationships
verifying the status 5

T
Twitter
how to receive automatic notification of documentation changes 16

V
volume disaster recovery preparation
where to get additional information about 13
volumes
setting up data access from destination 11
SnapMirror for disaster recovery preparation workflow 5

W
workflows
volume disaster recovery preparation 5