# Contents

Deciding whether to use this guide ............................................................. 4  
Volume disaster recovery workflow ........................................................... 5  
  Activating the destination volume .............................................................. 6  
  Verifying the source volume status ............................................................ 6  
  Breaking the SnapMirror relationship ......................................................... 7  
  Verifying the destination volume status ..................................................... 8  
Configuring the destination volume for data access ......................................... 10  
  Reactivating the source volume ................................................................. 11  
  Rescynchronizing the source volume .......................................................... 11  
  Updating the source volume .................................................................... 13  
  Reactivating the source volume .................................................................. 14  
Where to find additional information ...................................................... 18  
Copyright information .............................................................................. 19  
Trademark information ............................................................................... 20  
How to send your comments ..................................................................... 21  
Index ............................................................................................................. 22
Deciding whether to use this guide

This guide describes how to quickly activate a destination volume after a disaster and then reactivate the source volume in clustered Data ONTAP.

You should use this guide if you want to perform a volume-level disaster recovery procedure in the following way:

• You are working with clusters running Data ONTAP 8.3 or later.

• You are a cluster administrator.

• You have configured the SnapMirror relationship following the Volume Disaster Recovery Preparation Express Guide.

• The cluster administrator of the source cluster has declared that the data in the source volume is unavailable due to events such as virus infection leading to data corruption or accidental deletion of data.

• You want to use OnCommand System Manager, not the command-line interface or an automated scripting tool.

• You want to use best practices, not explore every available option.

• You do not want to read a lot of conceptual background.

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

• Clustered Data ONTAP 8.3 Data Protection Guide

• Clustered Data ONTAP 8.3 Logical Storage Management Guide

• 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.
Volume disaster recovery workflow

The volume disaster recovery workflow includes activating the destination volume, configuring the destination volume for data access, and reactivating the original source volume.

---

Activate the destination volume:

- Verify the source volume status.
- Quiesce and break the SnapMirror relationship.
- Verify the destination volume status.

Configure the destination volume for data access.

Reactivate the original source volume:

- Resynchronize the source volume.
- Update the source volume, if necessary.
- Activate the source volume.
Activating the destination volume

When the source volume is unable to serve data due to events such as data corruption, accidental deletion or an offline state, you must activate the destination volume to provide data access until you recover the data on the source volume. Activation involves stopping future SnapMirror data transfers and breaking the SnapMirror relationship.

**Steps**

1. Verifying the source volume status on page 6
2. Breaking the SnapMirror relationship on page 7
3. Verifying the destination volume status on page 8

Verifying the source volume status

When the source volume is unavailable, you must verify that the source volume is offline and identify the destination volume that must be activated for providing data access.

**About this task**

You must perform this task from the source cluster.

**Steps**

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Expand the Storage Virtual Machines hierarchy in the left navigation pane.
3. Select the source SVM that contains the source volume, and then select Storage > Volumes.
4. Select the source volume in the Volumes list and verify that the source volume is offline.

   ![Volumes](image)

5. Click the Data Protection bottom tab to identify the destination volume in the SnapMirror relationship and the name of the SVM that contains the volume.
Breaking the SnapMirror relationship

You must quiesce and break the SnapMirror relationship to activate the destination volume. After quiescing, future SnapMirror data transfers are disabled.

Before you begin

The destination volume must be mounted on the destination SVM namespace.

About this task

You must perform this task from the destination cluster.

Steps

1. Expand the Storage Virtual Machines hierarchy in the left navigation pane.
2. Select the SVM that contains the destination volume, and then click Protection.
3. Select the SnapMirror relationship between the source and the destination volumes.
4. Click Operations > Quiesce to disable future data transfers.
5. Select the confirmation check box, and then click Quiesce.
   The quiesce operation might take some time; you must not perform any other operation on the SnapMirror relationship until the transfer status is displayed as Quiesced.
6. Click Operations > Break.
7. Select the confirmation check box, and then click Break.
The SnapMirror relationship is in **Broken Off** state.

### Verifying the destination volume status

After breaking the SnapMirror relationship, you must verify that the destination volume has read/write access and the destination volume settings match the settings of the source volume.

**About this task**

You must perform this task from the destination cluster.

**Steps**

1. Select the SVM that contains the destination volume, and then select **Storage > Volumes**.
2. Select the destination volume from the Volumes list, and verify that the destination volume type is **rw**, which indicates read/write access.
3. Verify that the volume settings, such as thin provisioning, deduplication, compression, and autogrow, on the destination volume match the settings of the source volume.
   
   You can use the volume settings information that you noted after creating the SnapMirror relationship to verify the destination volume settings.

4. If the volume settings do not match, modify the settings on the destination volume as required:
   
   a. Click **Edit**.
   
   b. Modify the general, storage efficiency, and advanced settings for your environment.
   
   c. Click **Save and Close**.
   
   d. Verify that the columns in the Volumes list are updated with the appropriate values.

5. Select the destination volume from the Volumes list, and then click **Snapshot Copies > Configure**.

6. Select the **Enable scheduled Snapshot Copies** check box, and then click **OK**.
Configuring the destination volume for data access

After activating the destination volume, you must configure the volume for data access. NAS clients and SAN hosts can access the data from the destination volume until the source volume is reactivated.

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

Choices

- NAS environment:
  1. Mount the NAS volumes to the namespace using the same junction path that the source volume was mounted to in the source SVM.
  2. Apply the appropriate ACLs to the CIFS shares at the destination volume.
  3. Assign the NFS export policies to the destination volume.
  4. Apply the quota rules to the destination volume.
5. Redirect clients to the destination volume by performing the necessary steps such as changing the DNS name resolution.

6. Remount the NFS and CIFS shares on the clients.

- SAN environment:
  1. Map the LUNs to the appropriate initiator group to make the LUNs in the volume available to the SAN clients.
  2. For iSCSI, create iSCSI sessions from the SAN host initiators to the SAN LIFs.
  3. On the SAN client, perform a storage re-scan to detect the connected LUNs.

After you finish
You should resolve the problem that caused the source volume to become unavailable. You must bring the source volume back online when possible, and then resynchronize and reactivate the source volume.

Related information
   * NetApp Documentation: Clustered Data ONTAP Express Guides

Reactivating the source volume

When the source volume becomes available, you must resynchronize the data from the destination volume to the source volume, update any modifications after the resynchronization operation, and activate the source volume.

Steps
1. Rescynchronizing the source volume on page 11
2. Updating the source volume on page 13
3. Reactivating the source volume on page 14

Rescynchronizing the source volume

When the source volume is online, you must resynchronize the data between the destination volume and the source volume to replicate the latest data from the destination volume.

Before you begin
The source volume must be online.
About this task

You must perform the task from the destination cluster.

The following image shows that the data is replicated from the active destination volume to the read-only source volume:

---

Steps

1. Expand the **Storage Virtual Machines** hierarchy in the left navigation pane.
2. Select the Storage Virtual Machine (SVM) that contains the destination volume, and then click **Protection**.
3. Select the SnapMirror relationship between the source and destination volumes.
4. Make a note of the transfer schedule and the policy configured for the SnapMirror relationship.
5. Click **Operations > Reverse Resync**.
6. Select the confirmation check box, and then click **Reverse Resync**.

---

The SnapMirror relationship is displayed in the Protection window of the source SVM.
The SnapMirror policy of the relationship is set to \texttt{DPDefault} and the mirror schedule is set to \texttt{None}.

7. On the source cluster, specify a SnapMirror policy and schedule that match the protection configuration of the original SnapMirror relationship:
   
a. In the navigation pane, select the SVM that contains the source volume, and then click \texttt{Protection}.
   
b. Select the SnapMirror relationship between the resynchronized source volume and the destination volume, and then click \texttt{Edit}.
   
c. Select the SnapMirror policy and schedule, and then click \texttt{OK}.

**Updating the source volume**

After resynchronizing the source volume, you might want to ensure that all the latest changes are updated on the source volume before activating the source volume.

**About this task**

You must perform this task from the source cluster.

**Steps**

1. Expand the \texttt{Storage Virtual Machines} hierarchy in the left navigation pane.
2. Select the SVM that contains the source volume, and then click \texttt{Protection}.
3. Select the SnapMirror relationship between the source and the destination volumes, and then click \texttt{Operations > Update}.
4. Select \texttt{On demand} to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
5. Optional: Select \texttt{Limit transfer bandwidth to} in order to limit the network bandwidth used for transfers, and then specify the maximum transfer speed.
6. Click \texttt{Update}. 
7. Verify that the transfer status is **Idle** and last transfer type is **Update** in the **Details** tab.

---

**Reactivating the source volume**

After resynchronizing the data from the destination volume to the source volume, you must activate the source volume by breaking the SnapMirror relationship. You should then resynchronize the destination volume to protect the reactivated source volume.

**About this task**

Both the break and reverse resync operations are performed from the **source** cluster.
The following image shows that the source and destination volumes are read/write when you break the SnapMirror relationship. After the reverse resync operation, the data is replicated from the active source volume to the read-only destination volume.

**Steps**

1. Expand the **Storage Virtual Machines** hierarchy in the left navigation pane.
2. Select the SVM that contains the source volume, and then click **Protection**.
3. Select the SnapMirror relationship between the source and the destination volumes.
4. Click **Operations > Quiesce**.
5. Select the confirmation check box, and then click **Quiesce**.
6. Click **Operations > Break**.
7. Select the confirmation check box, and then click **Break**.

9. Select the confirmation check box, and then click Reverse Resync.

![Reverse Resync dialog box](image)

- The SnapMirror policy of the relationship is set to DPDefault and the SnapMirror schedule is set to None.

- The SnapMirror relationship is removed from the Protection list. Because SnapMirror relationships are always listed for the destination volume, you can view the new relationship from the Protection page of the new destination volume.

10. In the Data Protection tab, verify that the SnapMirror relationship you created is listed and the relationship state is Snapmirrored.
11. On the destination cluster, specify a SnapMirror policy and schedule that match the protection configuration of the original SnapMirror relationship for the new SnapMirror relationship:

   a. In the navigation pane, select the SVM that contains the destination volume, and then click **Protection**.

   b. Select the SnapMirror relationship between the reactivated source and the destination volumes, and then click **Edit**.

   c. Select the SnapMirror policy and schedule, and then click **OK**.

**Result**

The source volume has read/write access and is protected by the destination volume.
Additional information is available to help you to manage the volume-level disaster recovery relationships and provides other methods of disaster recovery to protect the availability of your data resources.

**Express guides**

- *Clustered Data ONTAP 8.3 Volume Backup Using SnapVault Express Guide*
  Describes how to quickly configure backup vault relationships between volumes that are located in different Data ONTAP clusters.

- *Clustered Data ONTAP 8.3 Volume Restore Using SnapVault Express Guide*
  Describes how to quickly restore a volume from a backup vault in clustered Data ONTAP.

**Comprehensive guides**

  Describes information and best practices about configuring replication in clustered Data ONTAP.

- *Clustered Data ONTAP 8.3 Data Protection Guide*
  Describes how to plan and manage disaster recovery and disk-to-disk backup of clustered systems.

- *Clustered Data ONTAP 8.3 Data Protection Tape Backup and Recovery Guide*
  Describes how to back up and recover data using tape backup and recovery features in clusters, using NDMP and dump technologies.
Copyright information

Copyright © 1994–2014 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).
Trademark information


Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.
How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to 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.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277
Index

A
activating
  destination volume for disaster recovery 6
ADR
  See asynchronous disaster recovery
asynchronous disaster recovery
  requirements for Volume Disaster Recovery Express
  Guide to perform 4

B
breaking
  SnapMirror relationships 7

C
comments
  how to send feedback about documentation 21
configuring
  data access on the destination volume 10

D
data access
  configuring the destination volume 10
destination volumes
  activating for disaster recovery 6
  breaking the mirror relationship to activate 7
  configuring data access for 10
  verifying the status 8
diagrams
  volume disaster recovery workflow 5
disaster recovery
  activating the destination volume 6
  reactivating the source volume 11
requirements for using Volume Disaster Recovery Express Guide to perform asynchronous 4
where to get additional information about 18

E
express guides
requirements for using volume disaster recovery 4

F
failover
  requirements for using Volume Disaster Recovery Express Guide to perform 4
  where to get additional information about 18
feedback
  how to send comments about documentation 21
flowcharts
  volume disaster recovery workflow 5

G
guides
  requirements for using Volume Disaster Recovery Express 4

I
information
  how to send feedback about improving documentation 21
intercluster SnapMirror relationships
  volume disaster recovery workflow for 5

M
mirror relationships
  breaking 7
requirements for using Volume Disaster Recovery Express for configuring 4
  reverse resynchronizing 11
  updating 13

R
reactivating
  source volume 11
recovered volumes
  returning to source role 14
relationships
  mirror, reverse resynchronizing 11