ONTAP® 9

Volume Disaster Recovery Express Guide

November 2018 | 215-11188_G0
doccomments@netapp.com

Updated for ONTAP 9.5
Deciding whether to use the Volume Disaster Recovery Express Guide

This guide describes how to quickly activate a destination volume after a disaster and then reactivate the source volume in 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 ONTAP 9.
• You are a cluster administrator.
• You have configured the SnapMirror relationship following the Volume Disaster Recovery Preparation Express Guide.

**Volume disaster recovery express preparation**

• 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 ONTAP command-line interface or an automated scripting tool.

The UI navigation in OnCommand System Manager 9.3 is different from the UI navigation in previous releases. This guide provides the common steps that you must perform for completing a task in any ONTAP 9 release. If you want the exact steps for navigating to a particular screen or window, you should view the OnCommand System Manager Online Help for your version of ONTAP.

• 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:

• *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.
**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.

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

Verifying the status of the source volume

When the source volume is unavailable, you must verify that the source volume is offline and then 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. Navigate to the Volumes window.
2. Select the source volume, and then verify that the source volume is offline.
3. Identify the destination volume in the SnapMirror relationship.
   - Starting with ONTAP 9.3: Double-click the source volume to view the details, and then click PROTECTION to identify the destination volume in the SnapMirror relationship and the name of the SVM that contains the volume.
   - ONTAP 9.2 or earlier: Click the Data Protection tab at the bottom of the Volumes page 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. 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.
3. Click Operations > Quiesce to disable future data transfers.
4. 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.
5. Click Operations > Break.
6. 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 that 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. Navigate to the **Volumes** window.

2. Select the destination volume from the **Volumes** list, and then 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 settings, storage efficiency settings, and advanced settings for your environment, as required.
      
   c. Click **Save and Close**.

   d. Verify that the columns in the **Volumes** list are updated with the appropriate values.

5. Enable Snapshot copy creation for the destination volume.

   a. Depending on your ONTAP version, navigate to the **Configure Volume Snapshot Copies** page in one of the following ways:
      
      Starting with ONTAP 9.3: Select the destination volume, and then click **Actions > Manage Snapshots > Configure**.
      
      ONTAP 9.2 or earlier: Select the destination volume, and then click **Snapshot Copies > Configure**.
      
   b. 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
ONTAP 9 Documentation Center

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. Resynchronizing the source volume on page 10
2. Updating the source volume on page 11
3. Reactivating the source volume on page 12

Resynchronizing 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. 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 destination volumes.
3. Make a note of the transfer schedule and the policy configured for the SnapMirror relationship.
5. Select the confirmation check box, and then click **Reverse Resync**.

![Reverse Resync dialog box](image)

Starting with ONTAP 9.3, the SnapMirror policy of the relationship is set to **MirrorAllSnapshots** and the mirror schedule is set to **None**.

If you are running ONTAP 9.2 or earlier, the SnapMirror policy of the relationship is set to **DPDefault** and the mirror schedule is set to **None**.

6. On the source cluster, specify a SnapMirror policy and schedule that match the protection configuration of the original SnapMirror relationship:

   a. 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**.
   
   b. Select the SnapMirror relationship between the resynchronized source volume and the destination volume, and then click **Edit**.

   c. Select the SnapMirror policy and schedule, and then click **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. 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 click **Operations > Update**.
3. Perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
   - Starting with ONTAP 9.3: Select the **As per policy** option.
   - ONTAP 9.2 or earlier: Select the **On demand** option.

4. Optional: Select **Limit transfer bandwidth to** in order to limit the network bandwidth used for transfers, and then specify the maximum transfer speed.

5. Click **Update**.

6. 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. 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.

3. Click Operations > Quiesce.

4. Select the confirmation check box, and then click Quiesce.

5. Click Operations > Break.

6. Select the confirmation check box, and then click Break.

7. Click Operations > Reverse Resync.

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

Starting with ONTAP 9.3, the SnapMirror policy of the relationship is set to MirrorAllSnapshots and the SnapMirror schedule is set to None.

If you are running ONTAP 9.2 or earlier, the SnapMirror policy of the relationship is set to DPDefault and the SnapMirror schedule is set to None.
9. Navigate to the source volume in the volumes page, and verify that the SnapMirror relationship you created is listed and the relationship state is *Snapmirrored*.

10. 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. 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**.

   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.
Where to find additional information

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

- **Volume express backup using SnapVault**
  Describes how to quickly configure backup vault relationships between volumes that are located in different ONTAP clusters.

- **Volume restore express management using SnapVault**
  Describes how to quickly restore a volume from a backup vault in ONTAP.

Power guide

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

Comprehensive guides

  Describes information and best practices about configuring replication in ONTAP.

- **Data protection using tape backup**
  Describes how to back up and recover data using tape backup and recovery features in clusters, using NDMP and dump technologies.

- **ONTAP concepts**
  Provides conceptual information about disaster recovery and disk-to-disk backup of clustered systems.
Copyright information

Copyright © 2018 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 information

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 Express Guide 4
activating
destination volume for disaster recovery 5

C
comments
how to send feedback about documentation 18
configuring
data access on the destination volume 9

D
data access
configuring the destination volume 9
destination volumes
activating for disaster recovery 5
breaking the mirror relationship to activate 6
configuring data access for 9
verifying the status 7
diagrams
volume disaster recovery workflow 5
disaster recovery
activating the destination volume 5
reactivating the source volume 10
where to get additional information about 15
documentation
how to receive automatic notification of changes to 18
how to send feedback about 18

F
failover
where to get additional information about 15
feedback
how to send comments about documentation 18
flowcharts
volume disaster recovery workflow 5

I
information
how to send feedback about improving documentation 18
intercluster SnapMirror relationships
volume disaster recovery workflow for 5

M
mirror relationships

R
reactivating
source volume 10
relationships
mirror, reverse resynchronizing 10
resynchronization
where to get additional information about 15
reverse resync
mirror relationships 10
returning source volume to RW role 12

S
SnapMirror
volume disaster recovery workflow 5
SnapMirror relationships
See mirror relationships
cource volumes
considerations for recovering 12
reactivating for disaster recovery 10
returning RW role to 12
verifying the status 6
suggestions
how to send feedback about documentation 18

T
Twitter
how to receive automatic notification of documentation changes 18

V
volume-level disaster recovery
requirements for using Volume Disaster Recovery Express Guide to perform 4
volumes
activating the destination 5
reactivating the source 10
updating the source 11
verifying status of the source volume 6
verifying the destination volume status 7

W
workflows
disaster recovery flowchart 5