



Volume disaster recovery

System Manager Classic

NetApp

December 09, 2021

Table of Contents

- Volume disaster recovery 1
 - Volume disaster recovery overview 1
 - Volume disaster recovery workflow 1
 - Where to find additional information 12

Volume disaster recovery

Volume disaster recovery overview

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

You should use this content 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 [Volume disaster recovery 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 System Manager, not the ONTAP command-line interface or an automated scripting tool.
- You want to use the *Classic* System Manager UI for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.

[ONTAP System Manager documentation](#)

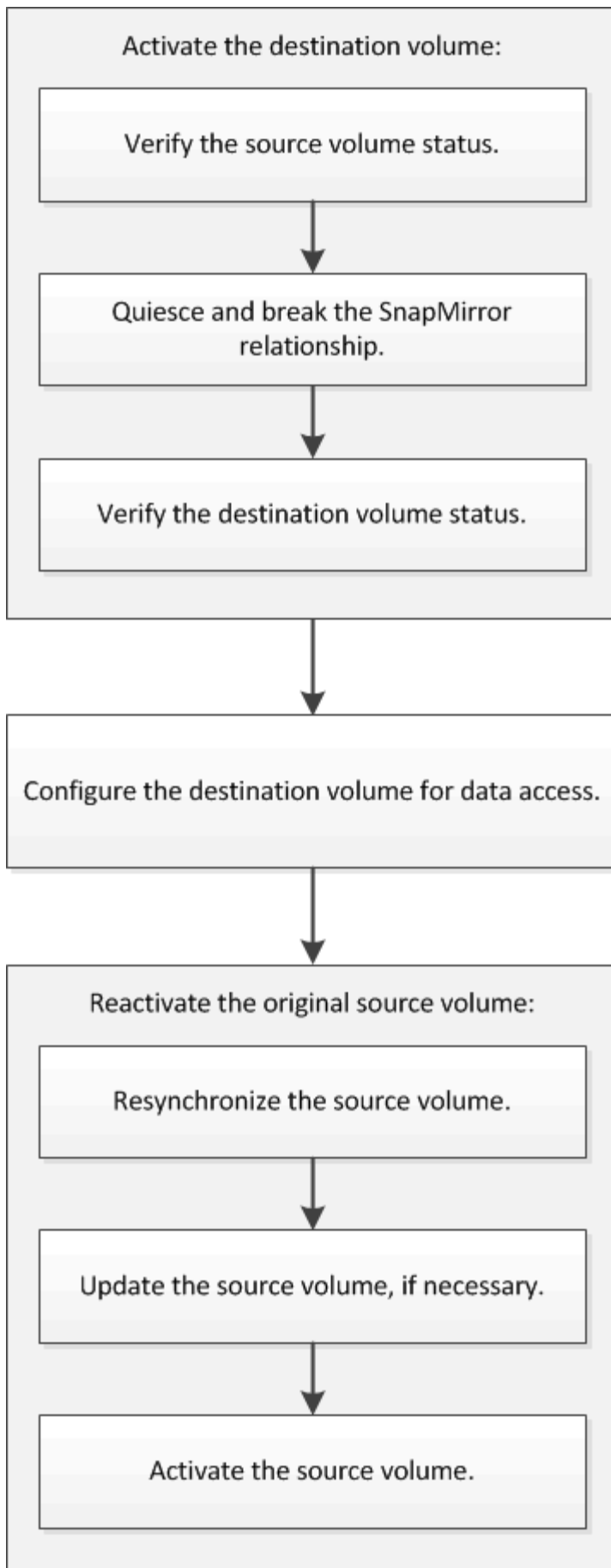
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.

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](#)

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

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.

Verify 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.

Volume: vol_mirror_src [Back to All volumes](#) [Edit](#) [Delete](#) [Actions](#) [Refresh](#)

Overview Snapshots Copies **Data Protection** Storage Efficiency Performance

Health	Destination SVM	Destination Volume	Destination Clu...	Relationship...	Transfer S...	Type	Lag Time	Policy
	svm2	vol_mirror_src_dst	cluster2	Snapmirrored	Idle	Version-Flexible ...	45 min(s)	MirrorAllSnaps...

- 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.

Create	Edit	Delete	Status	Snapshots Copies	Resize	Storage Efficiency	Move	Storage QoS	Protect	Re...
Name	Aggregate	Status	Thin Pro...	% Used	Availabl...	Total Sp...	Storage	Is Volu...	Encrypted	
svm1_svm1_root...	aggr2	Online	No	5	970.48 MB	1 GB	Disabled	No	No	
svm1_vol123_vault	aggr2	Online	No	5	121.35 MB	128.02 MB	Enabled	No	No	
Vol1	aggr3	Offline	-NA-	-NA-	-NA-	-NA-	Disabled	No	No	
svm2_root	aggr1	Online	No	5	971.12 MB	1 GB	Disabled	No	No	
Destination St...	Destination Vo...	Is Healthy	Relationship St...	Transfer Status	Type	Lag Time	Policy			
svm1	vol1	Yes	Snapmirrored	Idle	Mirror	7 day(s) 12 hr(s)...	DPDefault			
Details	Space Allocation	Snapshot Copies	Storage Efficiency	Data Protection	Volume Move Det	Performance				

Break 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

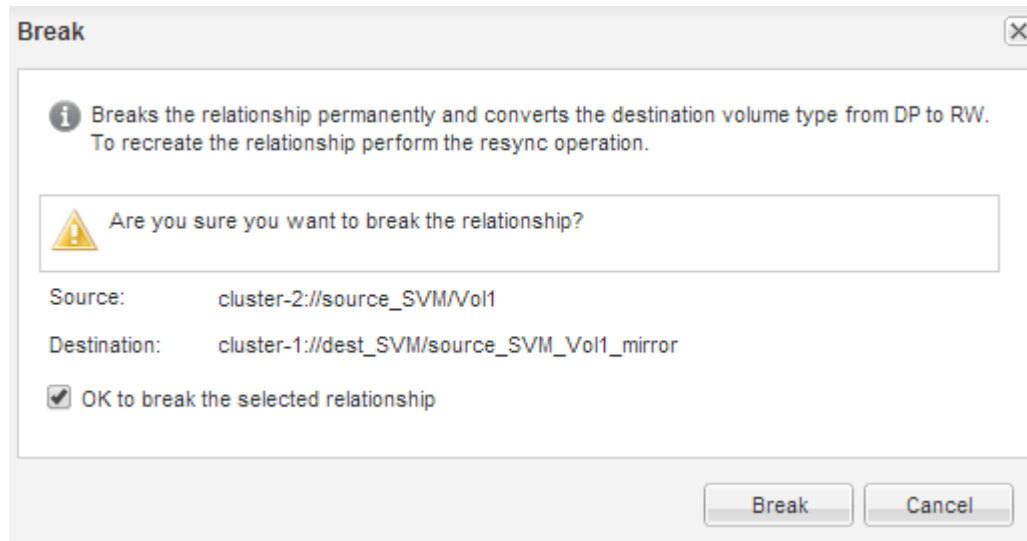
You must perform this task from the **destination** cluster.

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.

Source Sto...	Source Vol...	Destinatio...	Destination...	Is Healthy	Relationship...	Transfer St...	Relationship	Lag Time	Policy Name	Policy Type
svm1	svm1_root	svm1_svm1_j...	svm2	Yes	Snapmirrored	Idle	Mirror	25 min(s)	DPDefault	Asynchronous...
svm1	vol1	svm1_vol1_m...	svm2	Yes	Broken Off	Idle	Mirror	None	DPDefault	Asynchronous...

Source Location:	svm1.vol1	Is Healthy:	Yes	Transfer Status:	Idle
Destination Location:	svm2:svm1_vol1_mirror	Relationship State:	Broken Off	Current Transfer Type:	None
Source Cluster:	cluster-1	Network Compression Ratio:	Not Applicable	Current Transfer Error:	None
Destination Cluster:	cluster-1			Last Transfer Error:	None
Transfer Schedule:	hourly			Last Transfer Type:	Update
Data Transfer Rate:	Unlimited			Latest Snapshot Timestamp:	02/22/2017 13:05:00
Lag Time:	None			Latest Snapshot Copy:	snapmirror-9b4das7c-e5d0-11e6-b44e-00a08981a1bd_2149622820_2017-02-22-13-05-00

Verify 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**.

The screenshot shows the 'Edit Volume' dialog box with the 'General' tab selected. The 'Name' field contains 'vol123' and the 'Security style' is set to 'Mixed'. The 'Configure UNIX permissions (Optional)' checkbox is checked, and a table shows permissions for Owner, Group, and Others. The 'Thin Provisioned' checkbox is also checked, with a descriptive text block below it. At the bottom, there are 'Save', 'Save and Close', and 'Cancel' buttons.

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Thin Provisioned

When a volume is thin provisioned, space for the volume is not allocated in advance. Instead, space is allocated as data is written to the volume. The unused aggregate space is available to other thin provisioned volumes and LUNs.

[Tell me more about Thin Provisioning](#)

- 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**.

Configure Volume Snapshot Copies

? Snapshot Reserve (%): 5

☒ Make Snapshot directory (.snapshot) visible
Visibility of .snapshot directory on this volume at the client mount points.

☒ Enable scheduled Snapshot Copies

Snapshot Policies and Schedules

Select a Snapshot policy that has desired schedules for Snapshot copies:

Snapshot Policy: default

Schedules of Selected Snapshot Policy:

Schedul...	Retained S...	Schedule	SnapMirror Label
hourly	6	Advance cron - {Minu...	-
daily	2	Daily - Run at 0 hour 1...	daily
weekly	2	On weekdays - Sund...	weekly

Current Timezone: US/Pacific

[Tell me more about Snapshot configurations](#)

OK Cancel

Configure 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.

Procedure

- NAS environment:
 - a. Mount the NAS volumes to the namespace using the same junction path that the source volume was mounted to in the source SVM.
 - b. Apply the appropriate ACLs to the CIFS shares at the destination volume.
 - c. Assign the NFS export policies to the destination volume.
 - d. Apply the quota rules to the destination volume.
 - e. Redirect clients to the destination volume by performing the necessary steps such as changing the DNS name resolution.
 - f. Remount the NFS and CIFS shares on the clients.
- SAN environment:
 - a. Map the LUNs to the appropriate initiator group to make the LUNs in the volume available to the SAN clients.
 - b. For iSCSI, create iSCSI sessions from the SAN host initiators to the SAN LIFs.
 - c. On the SAN client, perform a storage re-scan to detect the connected LUNs.

What to do next

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](#)

Reactivate 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.

Resynchronize 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

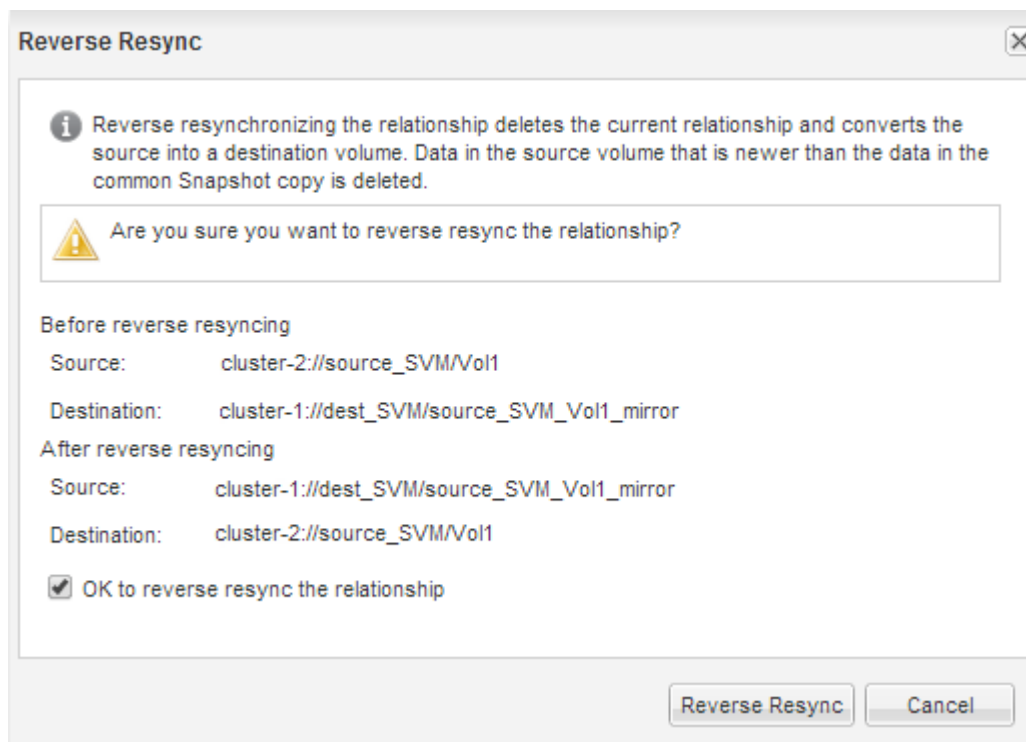
You must perform the task from the **destination** cluster.

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.
4. Click **Operations > Reverse Resync**.
5. 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 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**.

Update 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

- 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**.
- Select the SnapMirror relationship between the source and the destination volumes, and then click **Operations > Update**.
- 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.
- Select **Limit transfer bandwidth to** in order to limit the network bandwidth used for transfers, and then specify the maximum transfer speed.
- Click **Update**.
- Verify that the transfer status is **Idle** and last transfer type is **Update** in the **Details** tab.

The screenshot shows the 'Relationships' interface in ONTAP. The top section is a table listing relationships. The bottom section shows the 'Details' tab for a selected relationship.

Source Sto...	Source Vol...	Destinatio...	Destinatio...	Is Healthy	Relationsh...	Transfer St...	Relationship	Lag Time	Policy Name	Policy Type
svm1	svm1_root	svm1_svm1_r...	svm2	Yes	Snapmirrored	Idle	Mirror	44 min(s)	DPDefault	Asynchronous...
svm1	vol123	svm1_vol123...	svm2	Yes	Snapmirrored	Idle	Vault	4 h(s) 56 min...	XDPDefault	Vault
svm2	svm1_vol1_m...	vol1	svm1	Yes	Snapmirrored	Idle	Mirror	2 min(s)	DPDefault	Asynchronous...

Source Location:	svm2:svm1_vol1_mirror	Is Healthy:	Yes	Transfer Status:	Idle
Destination Location:	svm1:vol1	Relationship State:	Snapmirrored	Current Transfer Type:	None
Source Cluster:	cluster-1	Network Compression Ratio:	Not Applicable	Current Transfer Error:	None
Destination Cluster:	cluster-1			Last Transfer Error:	None
Transfer Schedule:	None			Last Transfer Type:	Update
Data Transfer Rate:	Unlimited			Latest Snapshot Timestamp:	02/22/2017 16:47:10
Lag Time:	2 min(s)			Latest Snapshot Copy:	snapmirror.20c56fe5-e6d8-11e6-b4de-00a0951a1bda_2149622807.2017-1

At the bottom, there are tabs for 'Details', 'Policy Details', and 'Snapshot Copies'. The 'Details' tab is currently selected.

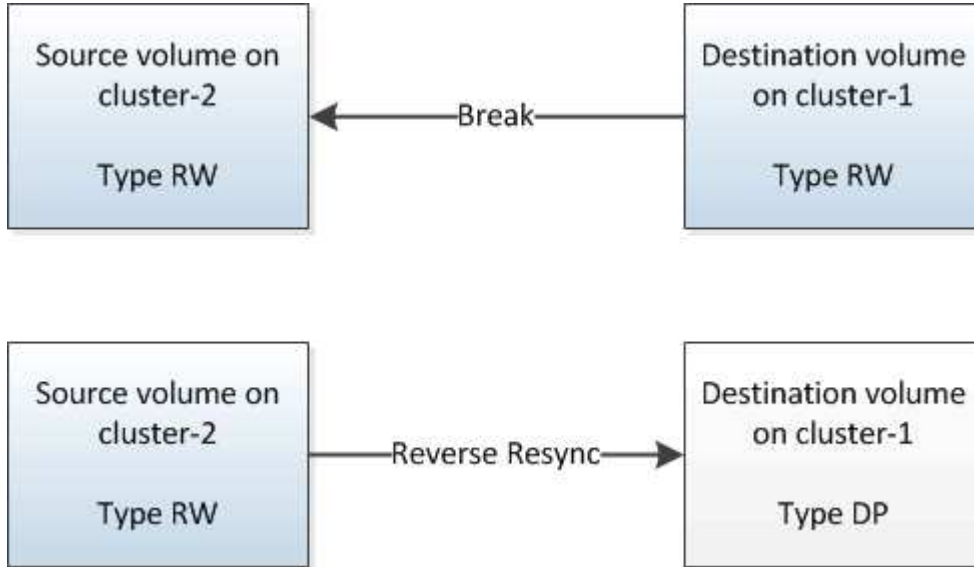
Reactivate the source volume

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

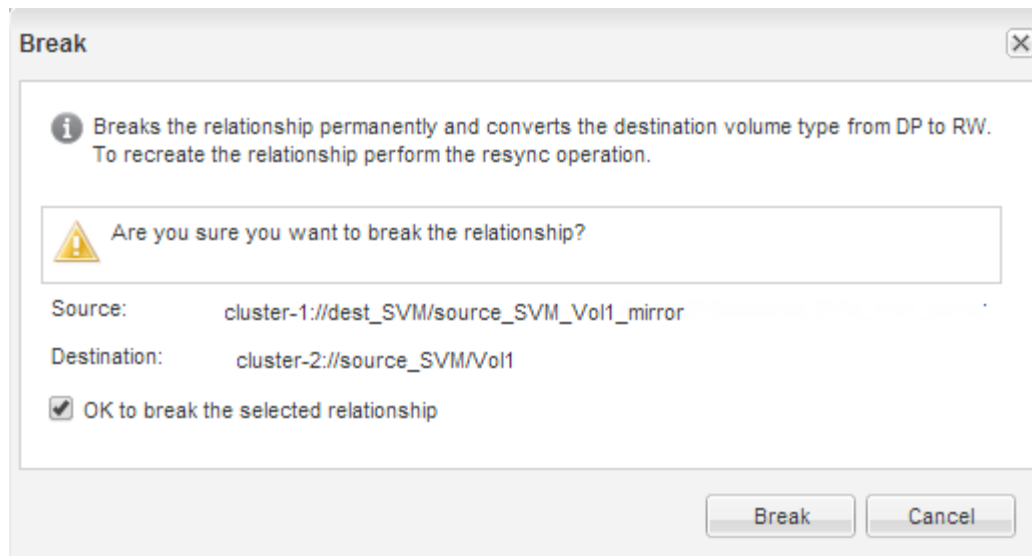
Both the break and reverse resync operations are performed from the **source** cluster.

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.

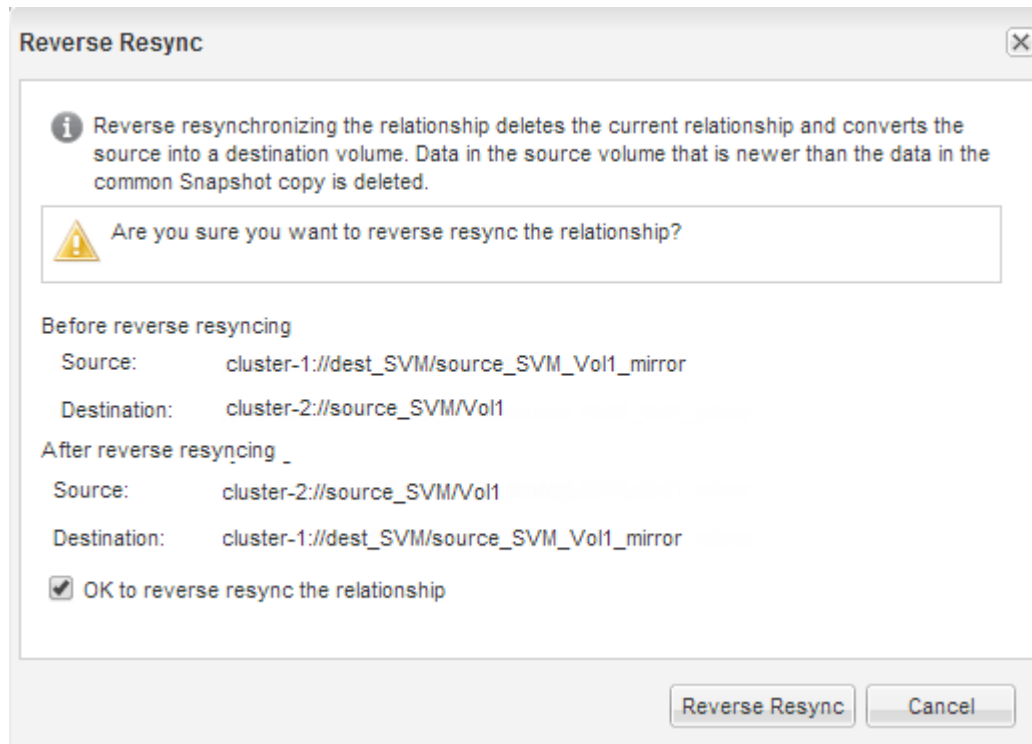


Steps

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**.

Results

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.

- [Volume backup using SnapVault](#)

Describes how to quickly configure backup vault relationships between volumes that are located in different ONTAP clusters.

- [Volume restore management using SnapVault](#)

Describes how to quickly restore a volume from a backup vault in ONTAP.

- [Data protection](#)

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

- [NetApp Technical Report 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2](#)

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 © 2021 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

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.