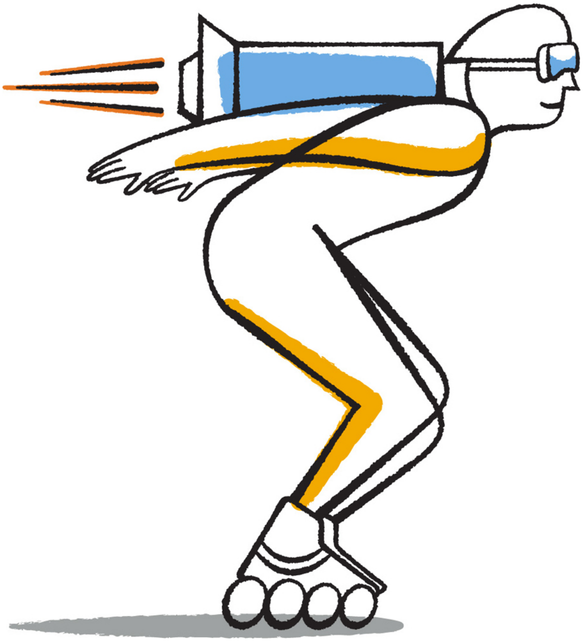
Clustered Data ONTAP® 8.3

Volume Disaster Recovery Express Guide



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
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-09377_A0
November 2014

Contents

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:

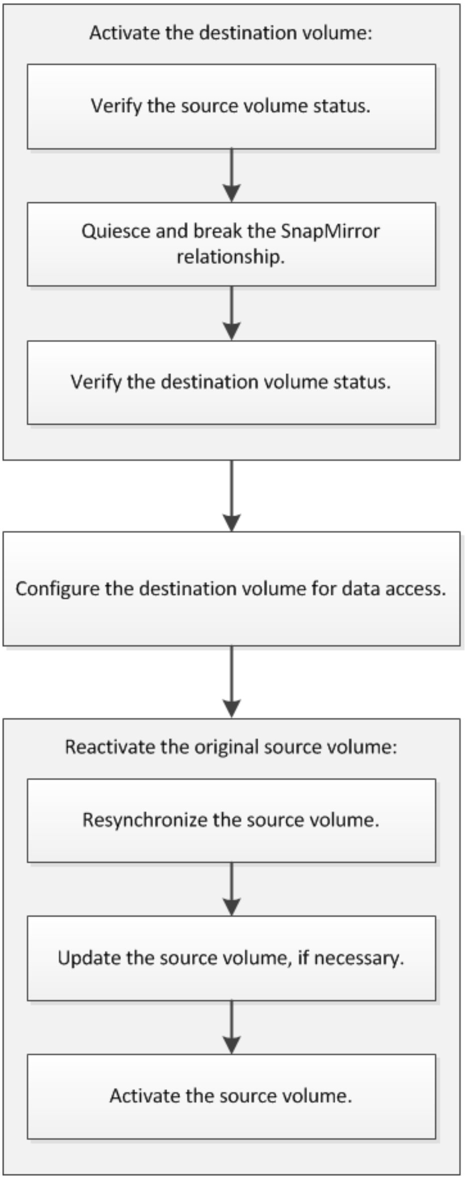
- You are working with clusters running Data ONTAP 8.3 or later.
- You are a cluster administrator.
- You have configured the SnapMirror relationship following the *Volume Disaster Recovery Preparation Express Guide*.
  Clustered Data ONTAP 8.3 Volume Disaster Recovery Preparation Express Guide
- The 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.

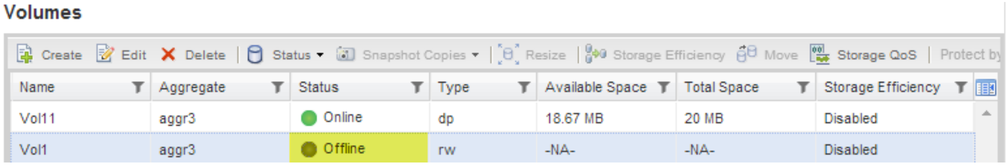
Steps

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.

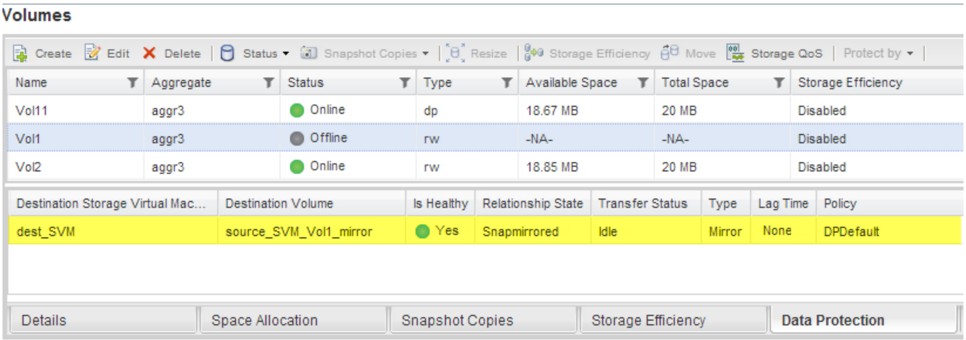
3. Select the source SVM that contains the source volume, and then select **Storage** > **Volumes**.

4. Select the source volume in the Volumes list and verify that the source volume is offline.



Name	Aggregate	Status	Type	Available Space	Total Space	Storage Efficiency
Vol11	aggr3	● Online	dp	18.67 MB	20 MB	Disabled
Vol1	aggr3	● Offline	rw	-NA-	-NA-	Disabled

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.



Name	Aggregate	Status	Type	Available Space	Total Space	Storage Efficiency
Vol11	aggr3	● Online	dp	18.67 MB	20 MB	Disabled
Vol1	aggr3	● Offline	rw	-NA-	-NA-	Disabled
Vol2	aggr3	● Online	rw	18.85 MB	20 MB	Disabled

Destination Storage Virtual Mac...	Destination Volume	Is Healthy	Relationship State	Transfer Status	Type	Lag Time	Policy
dest_SVM	source_SVM_Vol1_mirror	● Yes	Snapmirrored	Idle	Mirror	None	DPDefault

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.

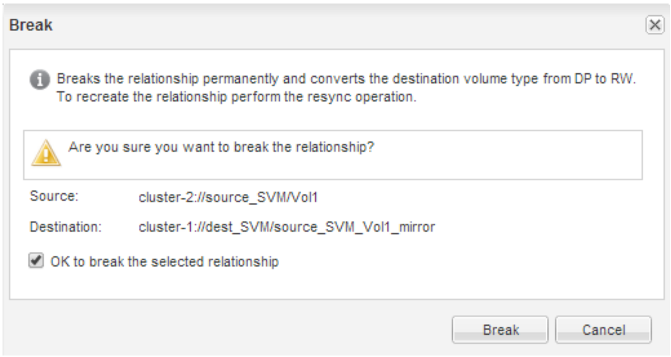
About this task

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**.



Break

Breaks the relationship permanently and converts the destination volume type from DP to RW. To recreate the relationship perform the resync operation.

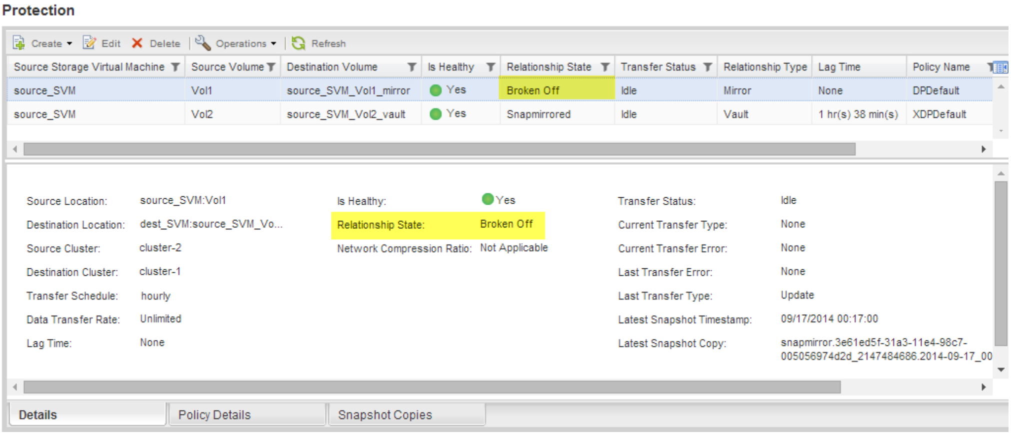
Are you sure you want to break the relationship?

Source: cluster-2://source_SVM/Vol1

Destination: cluster-1://dest_SVM/source_SVM_Vol1_mirror

☑ OK to break the selected relationship

The SnapMirror relationship is in `Broken Off` state.



Protection

Source Storage Virtual Machine	Source Volume	Destination Volume	Is Healthy	Relationship State	Transfer Status	Relationship Type	Lag Time	Policy Name
source_SVM	Vol1	source_SVM_Vol1_mirror	● Yes	Broken Off	Idle	Mirror	None	DPDefault
source_SVM	Vol2	source_SVM_Vol2_vault	● Yes	Snapmirrored	Idle	Vault	1 hr(s) 38 min(s)	XDPDefault

Source Location: source_SVM:Vol1
Destination Location: dest_SVM:source_SVM_Vo...
Source Cluster: cluster-2
Destination Cluster: cluster-1
Transfer Schedule: hourly
Data Transfer Rate: Unlimited
Lag Time: None

Is Healthy: ● Yes
Relationship State: Broken Off
Network Compression Ratio: Not Applicable

Transfer Status: Idle
Current Transfer Type: None
Current Transfer Error: None
Last Transfer Error: None
Last Transfer Type: Update
Latest Snapshot Timestamp: 09/17/2014 00:17:00
Latest Snapshot Copy: snapmirror.3e61ed5f-31a3-11e4-98c7-005056974d2d_2147484686.2014-09-17_00

Verifying the destination volume status

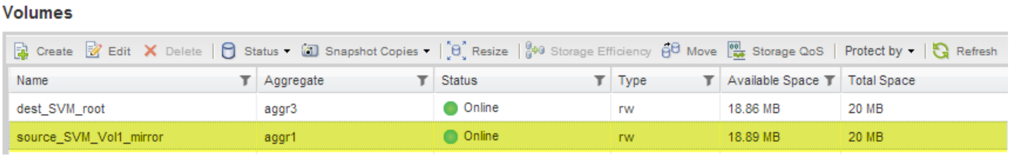
After breaking the SnapMirror relationship, you must verify that the destination volume has read/write access and the destination volume settings match the settings of the source volume.

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.



Name	Aggregate	Status	Type	Available Space	Total Space
dest_SVM_root	aggr3	Online	rw	18.86 MB	20 MB
source_SVM_Vol1_mirror	aggr1	Online	rw	18.89 MB	20 MB

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.

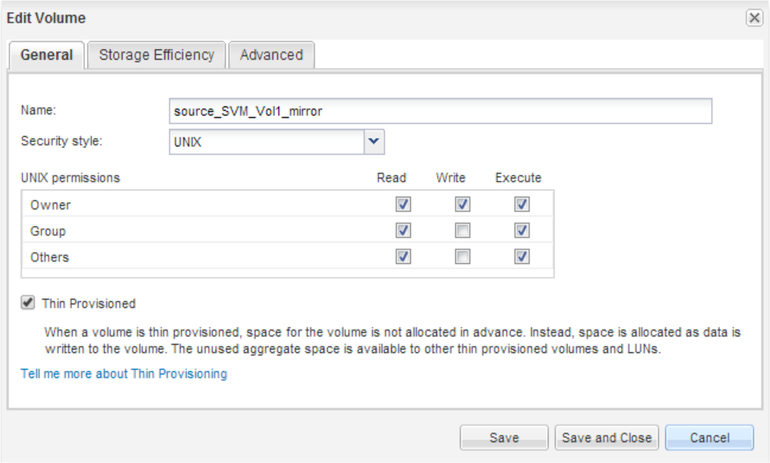
   You can use the volume settings information that you noted after creating the SnapMirror relationship to verify the destination volume settings.

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**.



Name: source_SVM_Vol1_mirror

Security style: UNIX

UNIX permissions	Read	Write	Execute
Owner	☑	☑	☑
Group	☑	□	☑
Others	☑	□	☑

☑ Thin Provisioned

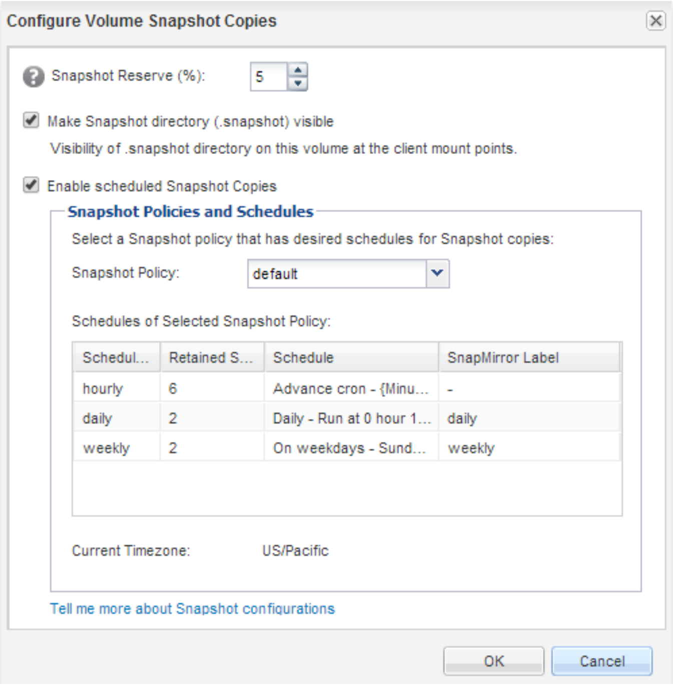
When a volume is thin provisioned, space for the volume is not allocated in advance. Instead, space is allocated as data is written to the volume. The unused aggregate space is available to other thin provisioned volumes and LUNs.

Tell me more about Thin Provisioning

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

5. 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**.



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

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.

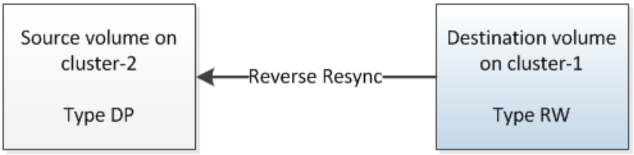
Before you begin

The source volume must be online.

About this task

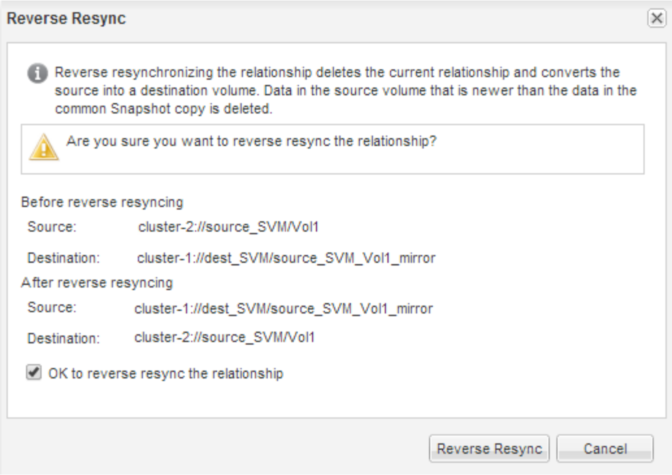
You must perform the task from the **destination** cluster.

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**.



Reverse resynchronizing the relationship deletes the current relationship and converts the source into a destination volume. Data in the source volume that is newer than the data in the common Snapshot copy is deleted.

Are you sure you want to reverse resync the relationship?

Before reverse resyncing
Source: cluster-2://source_SVM/Vol1
Destination: cluster-1://dest_SVM/source_SVM_Vol1_mirror

After reverse resyncing
Source: cluster-1://dest_SVM/source_SVM_Vol1_mirror
Destination: cluster-2://source_SVM/Vol1

☑ OK to reverse resync the relationship

The SnapMirror relationship is displayed in the Protection window of the source SVM.

The SnapMirror policy of the relationship is set to **`DPDefault`** and the mirror schedule is set to **`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 **Protection**.
    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

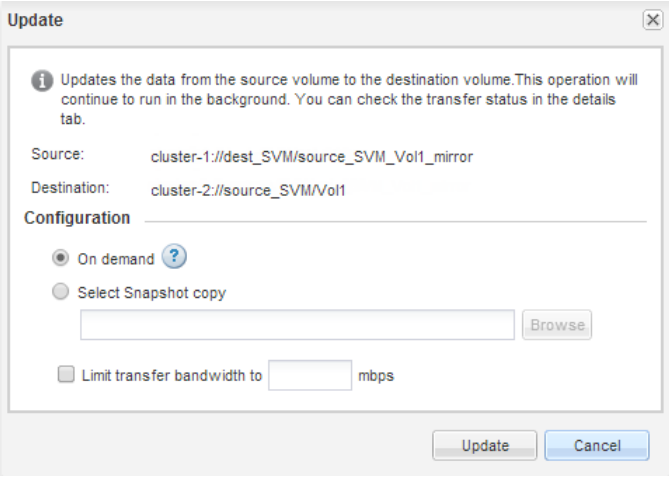
After resynchronizing the source volume, you might want to ensure that all the latest changes are updated on the source volume before activating the source volume.

About this task

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

Steps

1. 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, and then click **Operations > Update**.
4. Select **On demand** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
5. Optional: Select **Limit transfer bandwidth to** in order to limit the network bandwidth used for transfers, and then specify the maximum transfer speed.
6. Click **Update**.



Updates the data from the source volume to the destination volume.This operation will continue to run in the background. You can check the transfer status in the details tab.

Source: cluster-1://dest_SVM/source_SVM_Vol1_mirror

Destination: cluster-2://source_SVM/Vol1

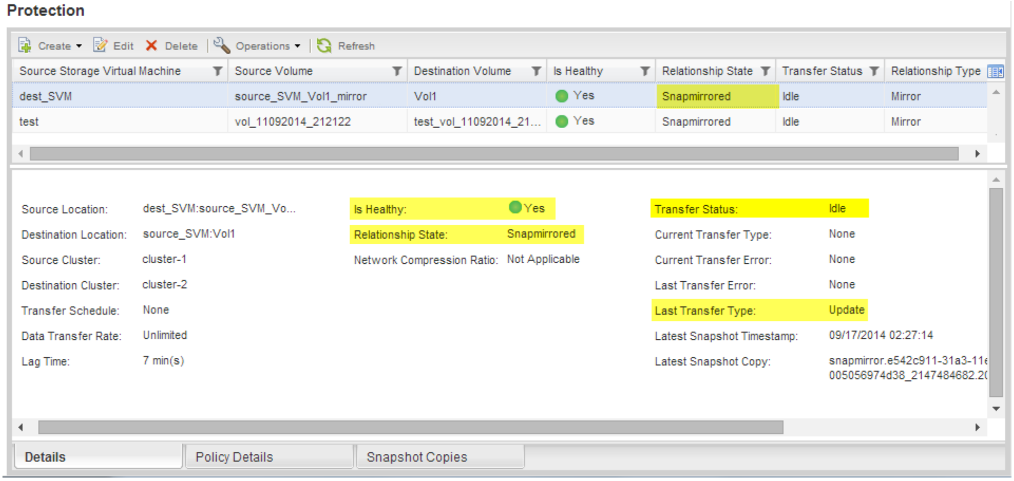
Configuration

● On demand

○ Select Snapshot copy

□ Limit transfer bandwidth to mbps

7. Verify that the transfer status is **`Idle`** and last transfer type is **`Update`** in the **Details** tab.



Source Storage Virtual Machine	Source Volume	Destination Volume	Is Healthy	Relationship State	Transfer Status	Relationship Type
dest_SVM	source_SVM_Vol1_mirror	Vol1	● Yes	Snapmirrored	Idle	Mirror
test	vol_11092014_212122	test_vol_11092014_21...	● Yes	Snapmirrored	Idle	Mirror

Source Location: dest_SVM:source_SVM_Vo...
Destination Location: source_SVM:Vol1
Source Cluster: cluster-1
Destination Cluster: cluster-2
Transfer Schedule: None
Data Transfer Rate: Unlimited
Lag Time: 7 min(s)

Is Healthy: ● Yes
Relationship State: Snapmirrored
Network Compression Ratio: Not Applicable

Transfer Status: Idle
Current Transfer Type: None
Current Transfer Error: None
Last Transfer Error: None
Last Transfer Type: Update
Latest Snapshot Timestamp: 09/17/2014 02:27:14
Latest Snapshot Copy: snapmirror.e542c911-31a3-11e
005056974d38_2147484682.20

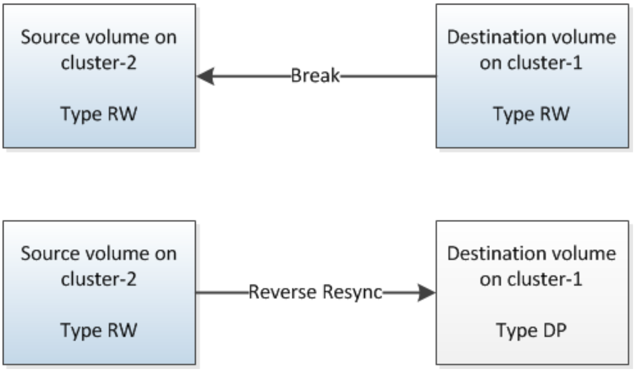
Reactivating the source volume

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

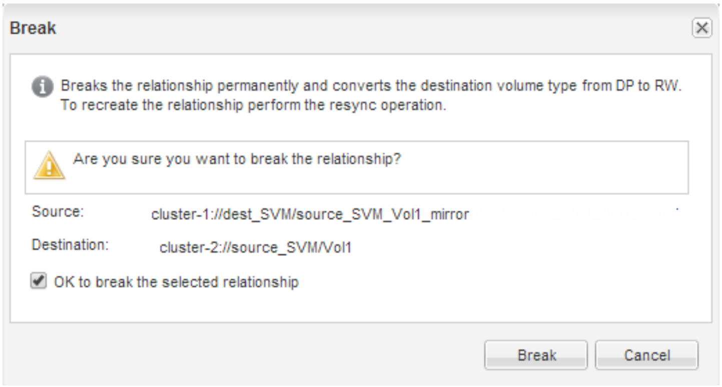
Both the break and reverse resync operations are performed from the **source** cluster.

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.


Source volume on cluster-2
Type RW
Break
Destination volume on cluster-1
Type RW
Source volume on cluster-2
Type RW
Reverse Resync
Destination volume on cluster-1
Type DP

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**.



Breaks the relationship permanently and converts the destination volume type from DP to RW. To recreate the relationship perform the resync operation.

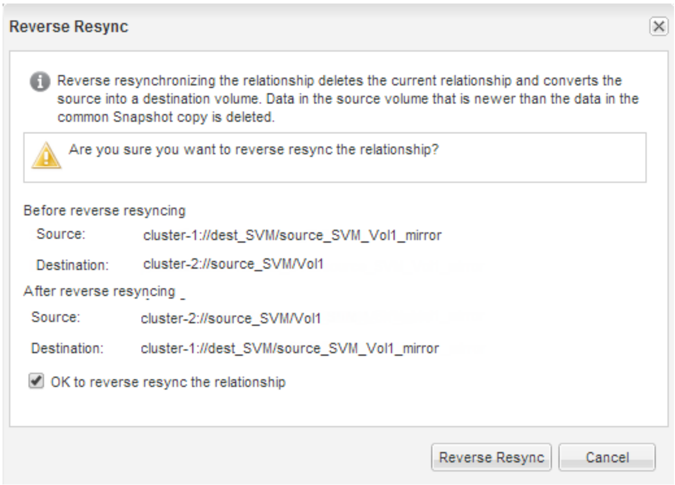
Are you sure you want to break the relationship?

Source: cluster-1://dest_SVM/source_SVM_Vol1_mirror

Destination: cluster-2://source_SVM/Vol1

☑ OK to break the selected relationship

8. Click **Operations > Reverse Resync**.
9. Select the confirmation check box, and then click **Reverse Resync**.



Reverse Resync

Reverse resynchronizing the relationship deletes the current relationship and converts the source into a destination volume. Data in the source volume that is newer than the data in the common Snapshot copy is deleted.

Are you sure you want to reverse resync the relationship?

Before reverse resyncing

Source:	cluster-1://dest_SVM/source_SVM_Vol1_mirror
Destination:	cluster-2://source_SVM/Vol1

After reverse resyncing

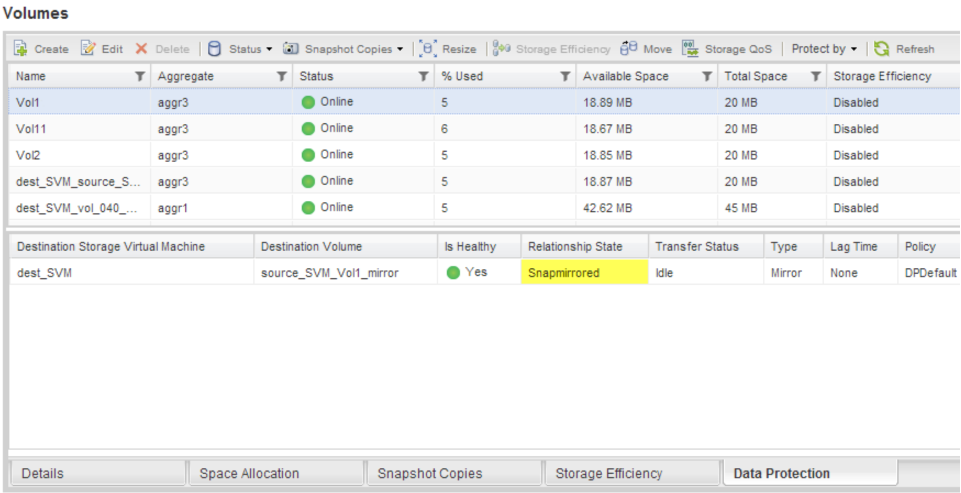
Source:	cluster-2://source_SVM/Vol1
Destination:	cluster-1://dest_SVM/source_SVM_Vol1_mirror

☑ OK to reverse resync the relationship

- 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`**.



Name	Aggregate	Status	% Used	Available Space	Total Space	Storage Efficiency
Vol1	aggr3	● Online	5	18.89 MB	20 MB	Disabled
Vol11	aggr3	● Online	6	18.67 MB	20 MB	Disabled
Vol2	aggr3	● Online	5	18.85 MB	20 MB	Disabled
dest_SVM_source_S...	aggr3	● Online	5	18.87 MB	20 MB	Disabled
dest_SVM_vol_040_...	aggr1	● Online	5	42.62 MB	45 MB	Disabled

Destination Storage Virtual Machine	Destination Volume	Is Healthy	Relationship State	Transfer Status	Type	Lag Time	Policy
dest_SVM	source_SVM_Vol1_mirror	● Yes	Snapmirrored	Idle	Mirror	None	DPDefault

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.

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

- *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

- *NetApp Technical Report 4015: SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP*
  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

Trademark information

NetApp, the NetApp logo, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at *http://www.netapp.com/us/legal/netapptmlist.aspx*.

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