



# **Volume disaster recovery preparation**

## **System Manager Classic**

NetApp  
December 09, 2021

# Table of Contents

- Volume disaster recovery preparation ..... 1
  - Volume disaster recovery preparation overview ..... 1
  - Volume disaster recovery preparation workflow ..... 2
  - Where to find additional information ..... 9

# Volume disaster recovery preparation

## Volume disaster recovery preparation overview

This content describes how to quickly protect a source volume on a peered ONTAP cluster in preparation for disaster recovery. You should use this content 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 content 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 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 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](#)

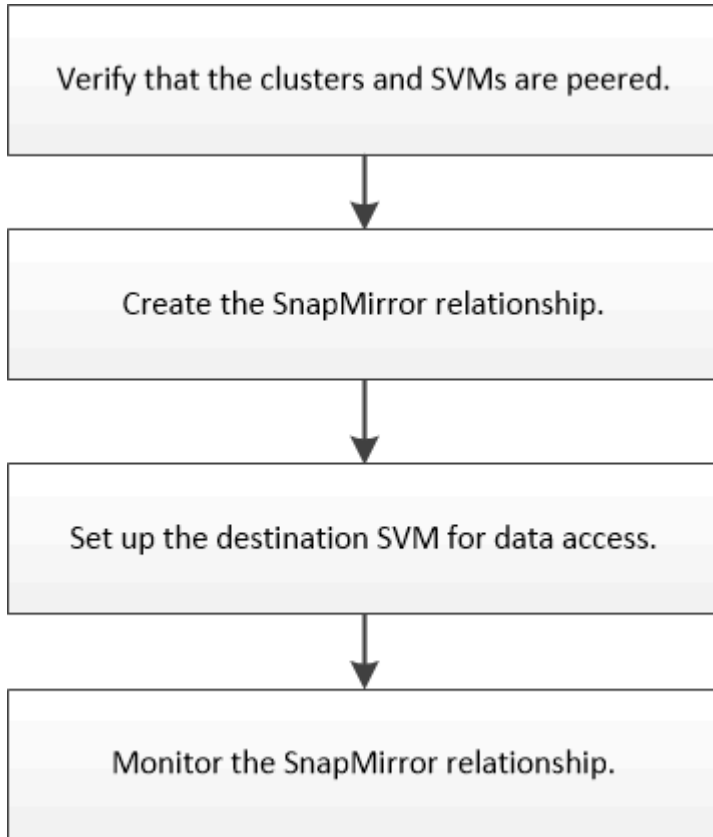
If these assumptions are not correct for your situation, or if you want more conceptual background information, you should see the following resources:

- [Data protection](#)
- [NetApp Technical Report 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2](#)
- [Logical storage management](#)
- [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.



## Verify 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.

### Procedure

- If you are running ONTAP 9.3 or later, perform the following steps to verify the cluster peer relationship and SVM peer relationship:
  - a. Click **Configuration > Cluster Peers**.
  - b. Verify that the peered cluster is authenticated and is available.

+ Create   Edit   Delete   Refresh   Manage SVM Permissions						
<input checked="" type="checkbox"/>	Peer Cluster	Availability	Authentication Status	Local Cluster IPspace	Peer Cluster Intercluster IP Addresses	Last Updated Time
<input checked="" type="checkbox"/>	cluster2	Available	OK	Default	10.237.213.119, 10.237.213.127	Nov 27, 2017, 2:13 PM

- c. Click **Configuration > SVM Peers**.

- d. 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:
  - a. Click the **Configurations** tab.
  - b. In the **Cluster Details** pane, click **Cluster Peers**.
  - c. Verify that the peered cluster is authenticated and available.

'Availability' and 'Authentication Status' information might be stale for up to several minutes.

Peer Cluster	Availability	Authentication Status
cluster-1	available	ok

- d. Click the **SVMs** tab and select the source SVM.
- e. 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 \(ONTAP 9.2 or earlier\)](#)

## Create 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** ✕

Protection Policy MirrorAllSnapshots ▼

SnapMirror Labels	Retention Count
sm_created	1
all_source_snapshots	1

Protection Schedule hourly ▼

Every hour at 05 minute(s)

i Initialize Protection ☒ Yes ☐ No

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

i 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.

Volume: vol\_mirror\_src

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	clv00872	Snapmirrored	Idle	Version-Flexible ...	None	MirrorAllSnap...

## What to do next

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.

## Create 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:

If the SVM is...	Then...
Peered	Select the peered SVM from the list.
Not peered	<ol style="list-style-type: none"> <li>a. Select the SVM.</li> <li>b. Click <b>Authenticate</b>.</li> <li>c. Enter the cluster administrator's credentials of the peered cluster, and then click <b>Create</b>.</li> </ol>

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.

**Destination Volume**

Cluster: cluster.1

Storage Virtual Machine: svm2(peered) [Browse...](#)

Volume: ☒ New Volume ☐ Select Volume

Volume name: svm1\_svm1\_root\_mirror

Aggregate: aggr2 [Browse...](#)  
387.19 GB available (of 390.21 GB)

Space Reserve (optional): Default

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.

**Configuration Details**

Mirror Policy: MirrorAllSnapshots [Browse...](#) [Create Policy](#)  
SnapMirror labels: sm\_created

Schedule: ☒ hourly [Browse...](#) [Create Schedule](#)  
Every hour at 05 minute(s)  
☐ None

☒ Initialize Relationship

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.



## Create Protection Relationship

### Source Volume

Cluster: cluster-1  
Storage Virtual Machine: svm1  
Volume: svm1\_root { Used space 844 KB }

### Destination Volume

Cluster: cluster-1  
Storage Virtual Machine: svm2  
Volume: svm1\_svm1\_root\_mirror

### Configuration Details

Mirror Policy: DPDefault  
Schedule: hourly

### Status

Create volume	✓ Completed successfully
Create relationship	✓ Completed successfully
Initialize relationship	✓ Started successfully

12. Verify the relationship status of the SnapMirror relationship:

- Select the volume for which you created the SnapMirror relationship from the **Volumes** list, and then click **Data Protection**.
- In the **Data Protection** tab, verify that the SnapMirror relationship that you created is listed and that the relationship state is Snapmirrored.

Destination Storage Virtual Mach...	Destination Volume	Is Healthy	Relationship State	Transfer Status	Type	Lag Time	Policy
svm2	svm1_svm1_root_mirror	Yes	Snapmirrored	Idle	Mirror	13 mins	DPDefault

## What to do next

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.

## Set 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.

## Procedure

- NAS environment:
  - a. Create NAS LIFs.
  - b. Create CIFS shares with the same share names that were used on the source.
  - c. Create appropriate NFS export policies.
  - d. Create appropriate quota rules.
- SAN environment:
  - a. Create SAN LIFs.
  - b. Configure portsets.
  - c. Configure initiator groups.
  - d. For FC, zone the FC switches to enable the SAN clients to access the LIFs.

## What to do next

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](#)

## Monitor 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.

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

Source Location:	source_SVM/Vol1	Is Healthy:	Yes	Transfer Status:	idle
Destination Location:	dest_SVM:source_SVM_Vol1	Relationship State:	Snapshotred	Current Transfer Type:	None
Source Cluster:	cluster-2	Network Compression Ratio:	Not Applicable	Current Transfer Error:	None
Destination Cluster:	cluster-1			Last Transfer Error:	None
Transfer Schedule:	hourly			Last Transfer Type:	Initialize
Data Transfer Rate:	Unlimited			Latest Snapshot Timestamp:	09/16/2014 23:42:24
Lag Time:	None			Latest Snapshot Copy:	snapmirror.3e51ed5f-31a3-11e4-80c7-005056974d2d_2147484686.2014-09-16_233529

## 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.

- [Volume disaster recovery](#)

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

- [Data protection](#)

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

- [Active IQ Unified Manager 9.8 Workflow 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 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.