Volume disaster recovery preparation

System Manager Classic

NetApp
December 09, 2021

Table of Contents

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

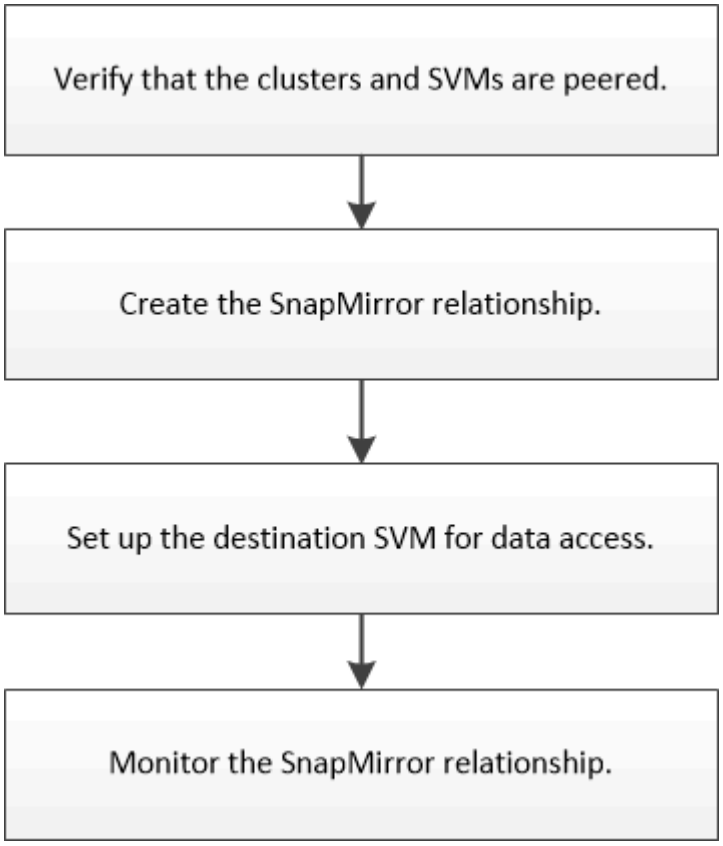
If these assumptions are not correct for your situation, or if you want more conceptual background information, you should see the following resources:

- 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.

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

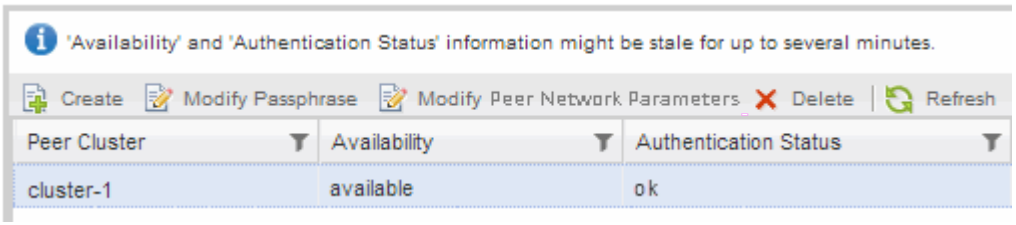
d. Verify that the destination SVM is peered with the source SVM.

- 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.



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.

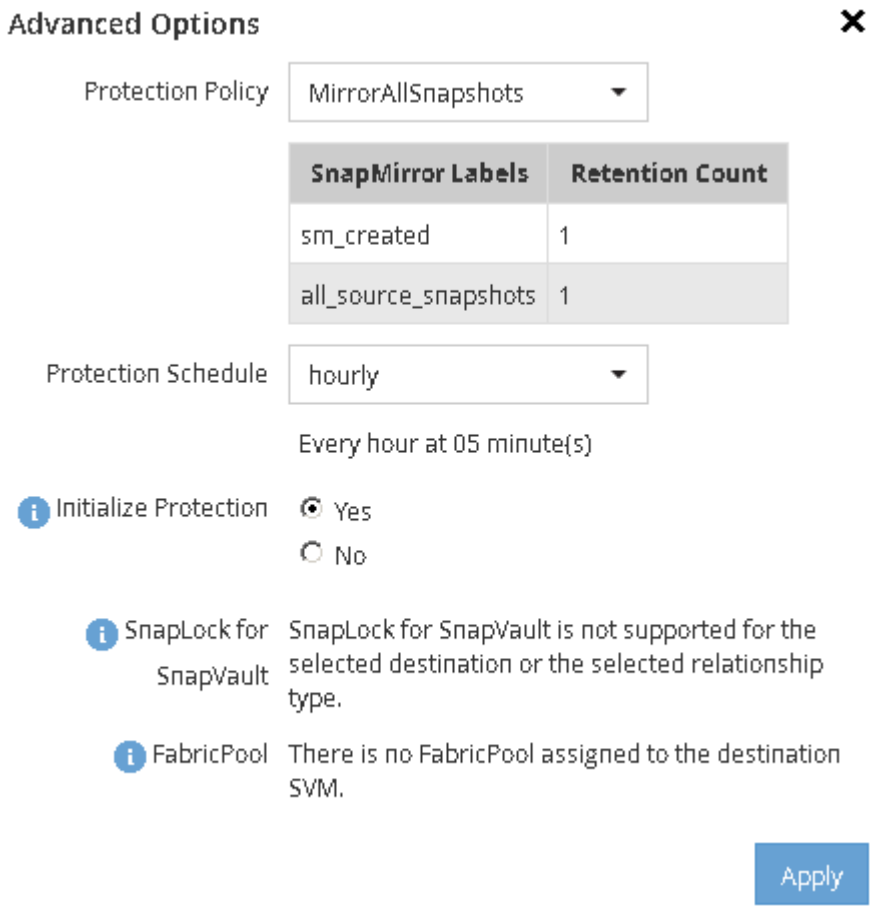
e. Select a protection schedule.

   By default, the `hourly` schedule is selected.

f. Verify that **Yes** is selected for initializing the SnapVault relationship.

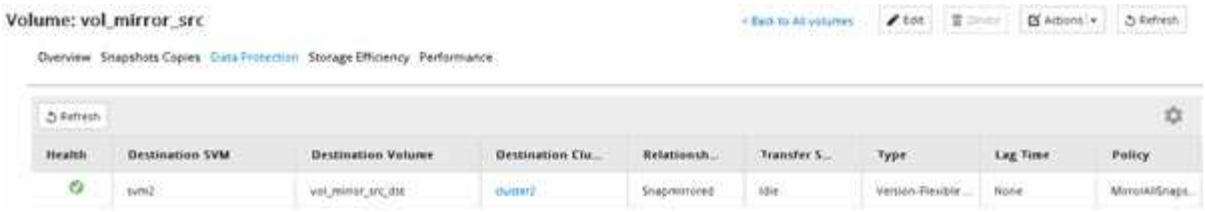
   All of the data protection relationships are initialized by default. Initializing the SnapMirror relationship ensures that the destination volume has a baseline to start protecting the source volume.

g. Click **Apply** to save the changes.



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.



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	a. Select the SVM. b. Click **Authenticate**. c. Enter the cluster administrator's credentials of the peered cluster, and then click **Create**.

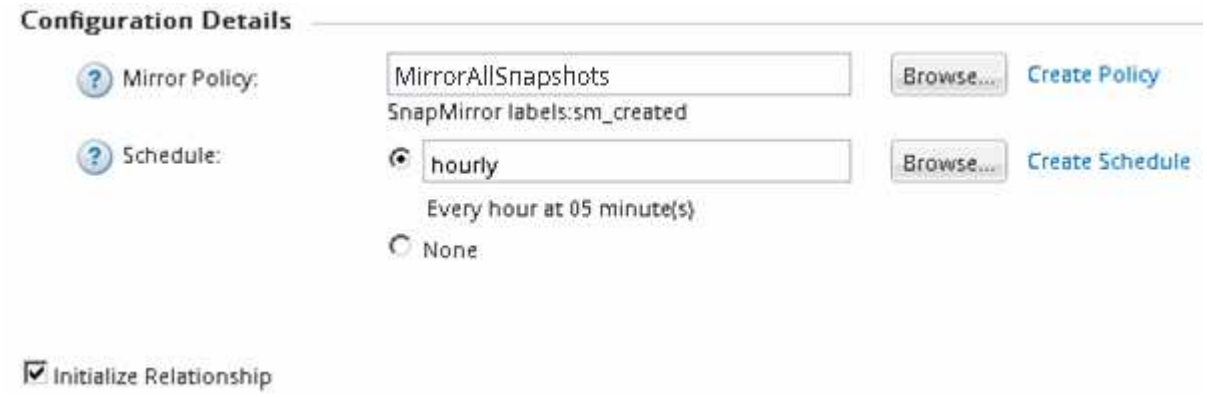
8. Create a new destination volume:
   a. Select the **New Volume** option.
   b. Use the default volume name or specify a new volume name.
   c. Select the destination aggregate.

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.

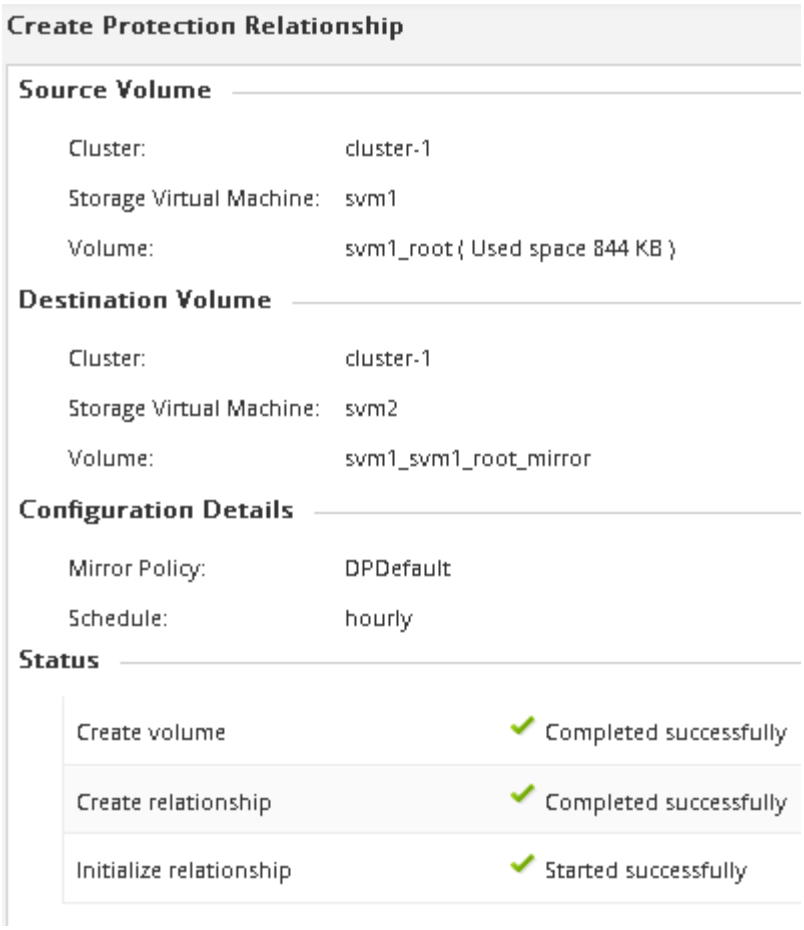
10. Select a protection schedule from the list of schedules.
11. Ensure that the **Initialize Relationship** check box is selected, and then click **Create**.

    Initializing the SnapMirror relationship ensures that the destination volume has a baseline to start protecting the source volume.



    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.



12. Verify the relationship status of the SnapMirror relationship:
    a. Select the volume for which you created the SnapMirror relationship from the **Volumes** list, and then click **Data Protection**.
    b. In the **Data Protection** tab, verify that the SnapMirror relationship that you created is listed and that the relationship state is `Snapmirrored`.

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

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.