Mirror relationships

System Manager Classic

NetApp
January 13, 2022

Table of Contents

Mirror relationships

You can use System Manager to create and manage mirror relationships by using the mirror policy.

Create a mirror relationship from a destination SVM

You can use ONTAP System Manager to create a mirror relationship from the destination storage virtual machine (SVM) and to assign a policy and schedule to the mirror relationship. The mirror copy enables quick availability of data if the data on the source volume is corrupted or lost.

Before you begin

- The source cluster must be running ONTAP 8.2.2 or later.
- The SnapMirror license must be enabled on the source cluster and destination cluster.

  For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization (DPO) license enabled.

- While mirroring a volume, if you select a SnapLock volume as the source, then the SnapMirror license and SnapLock license must be installed on the destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination SVM must have space available.
- A source volume of type read/write (rw) must exist.
- The FlexVol volumes must be online and must be of type read/write.
- The SnapLock aggregate type must be of the same type.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.

About this task

- System Manager does not support a cascade relationship.

  For example, a destination volume in a relationship cannot be the source volume in another relationship.

- You cannot create a mirror relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a mirror relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a mirror relationship from a volume on a sync-source SVM to a volume on a data-serving SVM.
- You can create a mirror relationship from a volume on a data-serving SVM to a data protection (DP) volume on a sync-source SVM.
- You can create a mirror relationship between SnapLock volumes of the same type only.

  For example, if the source volume is a SnapLock Enterprise volume, then the destination volume must also

be a SnapLock Enterprise volume. You must ensure that the destination SVM has aggregates of the same SnapLock type available.

- The destination volume that is created for a mirror relationship is not thin provisioned.
- A maximum of 25 volumes can be protected in one selection.
- You cannot create a mirror relationship between SnapLock volumes if the destination cluster is running a version of ONTAP that is older than the ONTAP version that the source cluster is running.

Steps

1. Click **Protection** > **Volume Relationships**.
2. In the **Volume Relationships** window, click **Create**.
3. In the **Browse SVM** dialog box, select an SVM for the destination volume.
4. In the **Create Protection Relationship** dialog box, select **Mirror** from the **Relationship Type** drop-down list.
5. Specify the cluster, the SVM, and the source volume.

   If the specified cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the specified cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

6. For FlexVol volumes, specify a volume name suffix.

   The volume name suffix is appended to the source volume names to generate the destination volume names.

7. Click **Browse**, and then change the mirror policy.
8. Select a schedule for the relationship from the list of existing schedules.
9. Select **Initialize Relationship** to initialize the mirror relationship.
10. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.
11. Click **Create**.

Results

If you chose to create a destination volume, a destination volume of type *dp* is created, with the language attribute set to match the language attribute of the source volume.

A mirror relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

Related information

Protection window

Deleting mirror relationships

You can delete a mirror relationship and permanently end the mirror relationship between the source and destination volumes. When a mirror relationship is deleted, the base Snapshot copy on the source volume is deleted.

About this task

It is a best practice to break the mirror relationship before deleting the relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to delete and click **Delete**.
3. Select the confirmation check boxes to delete the mirror relationship and to release the base Snapshot copies, and then click **Delete**.

Results

The relationship is deleted, and the base Snapshot copy on the source volume is deleted.

Related information

Protection window

Editing mirror relationships

You can use System Manager to edit a mirror relationship either by selecting an existing policy or schedule in the cluster, or by creating a policy or schedule.

About this task

- You cannot edit a mirror relationship that is created between a volume in Data ONTAP 8.2.1 and a volume in ONTAP 8.3 or later.
- You cannot edit the parameters of an existing policy or schedule.
- You can modify the relationship type of a version-flexible mirror relationship, vault relationship, or mirror and vault relationship by modifying the policy type.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship for which you want to modify the policy or schedule, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select an existing policy or create a policy:

If you want to…	Do the following…
Select an existing policy	Click **Browse**, and then select an existing policy.

If you want to…	Do the following…
Create a policy	a. Click **Create Policy**. b. Specify a name for the policy. c. Set the priority for scheduled transfers. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal. d. Select the **Transfer All Source Snapshot Copies** check box to include the "all_source_snapshots" rule to the mirror policy, which enables you to back up all of the Snapshot copies from the source volume. e. Select the **Enable Network Compression** check box to compress the data that is being transferred. f. Click **Create**.

4. Specify a schedule for the relationship:

If…	Do the following…
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a schedule	a. Click **Create Schedule**. b. Specify a name for the schedule. c. Select either **Basic** or **Advanced**. ◦ Basic specifies only the day of the week, time, and the transfer interval. ◦ Advanced creates a cron-style schedule. d. Click **Create**.
You do not want to assign a schedule	Select **None**.

5. Click **OK** to save the changes.

Related information

Protection window

Initializing mirror relationships

When you start a mirror relationship, you must initialize that relationship. Initializing a

relationship consists of a complete baseline transfer of data from the source volume to the destination. You can use System Manager to initialize a mirror relationship if you have not already initialized the relationship while creating it.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to initialize.
3. Click **Operations** > **Initialize**.
4. Select the confirmation check box and click **Initialize**.
5. Verify the status of the mirror relationship in the **Protection** window.

Results

A Snapshot copy is created and transferred to the destination. This Snapshot copy is used as a baseline for subsequent incremental Snapshot copies.

Related information

Protection window

Updating mirror relationships

You can initiate an unscheduled mirror update of the destination. You might have to perform a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

Before you begin

The mirror relationship must be in a Snapmirrored state.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship for which you want to update the data, and click **Operations** > **Update**.
3. Choose one of the following options:
   - Select **On demand** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
   - Select **Select Snapshot copy** and specify the Snapshot copy that you want to transfer.
4. Select **Limit transfer bandwidth to** to limit the network bandwidth used for transfers and specify the maximum transfer speed.
5. Click **Update**.
6. Verify the transfer status in the **Details** tab.

Related information

Protection window

Quiescing mirror relationships

You can use System Manager to quiesce a mirror destination to stabilize it before creating a Snapshot copy. The quiesce operation enables active mirror transfers to finish and disables future transfers for the mirroring relationship.

About this task

You can quiesce only mirror relationships that are in the Snapmirrored state.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to quiesce.
3. Click **Operations** > **Quiesce**.
4. Select the confirmation check box and click **Quiesce**.

Related information

Protection window

Resuming mirror relationships

You can resume a quiesced mirror relationship. When you resume the relationship, normal data transfer to the mirror destination is resumed and all the mirror activities are restarted.

About this task

If you have quiesced a broken mirror relationship from the command-line interface (CLI), you cannot resume the relationship from System Manager. You must use the CLI to resume the relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to resume.
3. Click **Operations** > **Resume**.
4. Select the confirmation check box and click **Resume**.

Results

Data transfer to the mirror destination resumes for the selected mirror relationship.

Related information

Protection window

Breaking SnapMirror relationships

You must break a SnapMirror relationship if a SnapMirror source becomes unavailable and you want client applications to be able to access the data from the mirror destination. After the SnapMirror relationship is broken, the destination volume type changes from

"data protection" (DP) to "read/write" (RW).

Before you begin

- The SnapMirror destination must be in the quiesced state or idle state.
- The destination volume must be mounted on the destination storage virtual machine (SVM) namespace.

About this task

- You can use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.
- You can break SnapMirror relationships between ONTAP systems and SolidFire storage systems.
- If you are breaking a FlexGroup volume relationship, you must refresh the page to view the updated status of the relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to break.
3. Click **Operations** > **Break**.
4. Select the confirmation check box, and then click **Break**.

Results

The data protection SnapMirror relationship is broken. The destination volume type changes from data protection (DP), read-only, to read/write (RW). The system stores the base Snapshot copy for the data protection mirror relationship for later use.

Related information

Protection window

Resynchronizing mirror relationships

You can reestablish a mirror relationship that was broken earlier. You can perform a resynchronization operation to recover from a disaster that disabled the source volume.

Before you begin

The source cluster and destination cluster and the source SVM and destination SVM must be in peer relationships.

About this task

- When you perform a resynchronization operation, the contents on the mirror destination are overwritten by the contents on the source volume.

- For SnapLock compliance volumes, all data changes in the active file system with reference to the common Snapshot copy are preserved in a locked Snapshot copy until the expiry time that is set for the current volume.

  If the volume expiry time is in the past or has not been set, then the Snapshot copy and the common Snapshot copy are locked for a duration of 30 days. All of the intermediate Snapshot copies between the common Snapshot copy and the latest locked Snapshot copy are deleted.

- For all volumes other than SnapLock compliance volumes, the resynchronization operation might cause loss of newer data that is written to the destination volume after the base Snapshot copy was created.

- If the Last Transfer Error field in the Protection window recommends a resynchronization operation, you must first break the relationship, and then perform the resynchronization operation.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to resynchronize.
3. Click **Operations** > **Resync**.
4. Select the confirmation checkbox, and then click **Resync**.

Related information

Protection window

Reverse resynchronizing mirror relationships

You can use System Manager to reestablish a mirror relationship that was previously broken. In a reverse resynchronization operation, you reverse the functions of the source volume and destination volume.

Before you begin

The source volume must be online.

About this task

- You can use the destination volume to serve data while you repair or replace the source volume, update the source volume, and reestablish the original configuration of the systems.
- When you perform reverse resynchronization, the contents on the mirror source are overwritten by the contents on the destination volume.

- For SnapLock compliance volumes, all data changes in the active file system with reference to the common Snapshot copy are preserved in a locked Snapshot copy until the expiry time that is set for the current volume.

  If the volume expiry time is in the past or has not been set, then the Snapshot copy and the common Snapshot copy are locked for a duration of 30 days. All of the intermediate Snapshot copies between the common Snapshot copy and the latest locked Snapshot copy are deleted.

- For all volumes other than SnapLock compliance volumes, the resynchronization operation might cause loss of newer data that is written to the source volume after the base Snapshot copy was created.

- When you perform reverse resynchronization, the mirror policy of the relationship is set to DPDefault, and the mirror schedule is set to None.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to reverse.
3. Click **Operations** > **Reverse Resync**.
4. Select the confirmation checkbox, and then click **Reverse Resync**.

Related information

Protection window

Aborting a mirror transfer

You can abort a volume replication operation before the data transfer is complete. You can abort a scheduled update, a manual update, or an initial data transfer.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to stop the data transfer, and click **Operations** > **Abort**.
3. Click the **Yes, I want to abort the transfer** check box to confirm the operation.
4. Click the **Keep any partially transferred data** check box to retain the data that is already transferred to the destination volume.
5. Click **Abort**.

   The transfer status is displayed as “Aborting” until the operation is complete and displayed as “Idle” after the operation is complete.

Related information

Protection window

Restoring a volume in a mirror relationship

For a version-independent mirror relationship, you can use System Manager to restore Snapshot copies to a source volume or to other volumes if the source data is corrupted and is no longer usable. You can replace the original data with the Snapshot copies in the destination volume.

Before you begin

- The SnapMirror license must be enabled on both the source cluster and the destination cluster or on the nodes that contain the source volume and destination volume.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The source aggregate or any other aggregate that you select for the restore operation must be a 64-bit aggregate.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must also be enabled on the remote cluster.

About this task

- You cannot restore a volume that is in a mirror relationship between a source storage virtual machine (SVM) and a destination SVM in a MetroCluster configuration.
- You cannot perform a restore operation on SnapLock volumes.
- You can restore a mirror relationship between sync-source SVMs in a MetroCluster configuration.
- You can restore a mirror relationship from a volume on a sync-source SVM to a default SVM.
- You can restore a mirror relationship from a volume on a default SVM to a DP volume on a sync-source SVM.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship, and then click **Operations** > **Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the mirror relationship or select any other volume:

If you want to restore the data to…	Do this…
The source volume	a. Select **Source volume**. b. Go to Step 7.
Any other volume	Select **Other volume**, and then select the cluster and SVM from the list.

4. Restore the data to a new volume or to an existing volume:

If you want to restore the data to…	Do this…
A new volume	If you want to change the default name, displayed in the format `destination_SVM_name_destination_volume_name_` restore, specify a new name, and then select the containing aggregate for the volume.
An existing volume	Select the **Select Volume** option. You must select a volume other than the source volume, or a read/write volume with some data in it and with a common Snapshot copy. Only those volumes with the same language attribute as the source volume are listed.

5. Select either the latest Snapshot copy or the specific Snapshot copy that you want to restore.
6. Select the confirmation checkbox to restore the volume from the Snapshot copy.
7. Select the **Enable Network Compression** checkbox to compress the data that is being transferred during the restore operation.
8. Click **Restore**.

How SnapMirror relationships work

You can create a data protection mirror relationship to a destination within a cluster to protect your data. For greater disaster protection, you can also create a mirror relationship to a destination in a different cluster in a different location.

A data protection mirror configuration consists of a source volume that can be replicated to one or more destination volumes. Each data protection mirror relationship is independent from the other data protection mirror relationships.

The destination volume must be running either the same ONTAP version as that of the source volume or a later version of ONTAP than that of the source volume.

Snapshot copies are used to update destination volumes. Snapshot copies are transferred from the source volume to the destination volume by using an automated schedule or manually; therefore, mirrors copies are updated asynchronously.

You can create data protection mirror relationships to destinations that are on the same aggregate as the source volume as well as to destinations that are on the same storage virtual machine (SVM) or on a different SVM. For greater protection, you can create the relationships to destinations on a different aggregate, which enables you to recover from any failure of the source volume's aggregate. However, these two configurations do not protect against a cluster failure.

To protect against a cluster failure, you can create a data protection mirror relationship in which the source volume is on one cluster and the destination volume is on a different cluster. If the cluster on which the source volume resides experiences a disaster, you can direct user clients to the destination volume on the cluster peer until the source volume is available again.