Manage data protection

System Manager Classic

NetApp
January 21, 2022

Table of Contents

Managing data protection

You can use System Manager to protect your data by creating and managing mirror relationships, vault relationships, and mirror and vault relationships. You can also create and manage the Snapshot policies and schedules.

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.

Vault relationships

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

Create a vault relationship from a destination SVM

You can use System Manager to create a vault relationship from the destination storage virtual machine (SVM), and to assign a vault policy to create a backup vault. In the event of data loss or corruption on a system, backed-up data can be restored from the backup vault destination.

Before you begin

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

> For some platforms, it is not mandatory for the source cluster to have the SnapVault license or the SnapMirror license enabled if the destination cluster has the SnapVault license or the SnapMirror license, and DPO license enabled.

- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination SVM must have space available.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- A source volume of type read/write (rw) must exist.
- A vault (XDP) policy must exist.

If a vault policy does not exist, you must create a vault policy or accept the default vault policy (XDPDefault) that is automatically assigned.

- FlexVol volumes must be online and read/write.
- The SnapLock aggregate type must be the same.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which 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 vault relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a vault relationship from a volume on a sync-source SVM to a volume on a data-serving SVM.
- You can create a vault relationship from a volume on a data-serving SVM to a data protection (DP) volume on a sync-source SVM.
- You can create a vault relationship only between a non-SnapLock (primary) volume and a SnapLock destination (secondary) volume.
- A maximum of 25 volumes can be protected in one selection.

Steps

1. Click **Protection** > **Volume Relationships**.
2. In the **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 **Vault** 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. Enter a volume name suffix.

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

7. If you are creating a SnapLock volume, specify the default retention period.

   The default retention period can be set to any value between 1 day through 70 years or Infinite.

8. Click **Browse**, and then change the vault policy.
9. Select a schedule for the relationship from the list of existing schedules.
10. Select **Initialize Relationship** to initialize the vault relationship.

11. Enable SnapLock aggregates, and then select a SnapLock Compliance aggregate or a SnapLock Enterprise aggregate.
12. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.
13. Click **Validate** to verify whether the selected volumes have matching labels.
14. Click **Create**.

Results

If you chose to create a destination volume, a volume of type *dp* is created with the following default settings:

- Autogrow is enabled.
- Deduplication is enabled or disabled according to the user preference or the source volume deduplication setting.
- Compression is disabled.
- The language attribute is set to match the language attribute of the source volume.

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

Related information

Protection window

Deleting vault relationships

You can use System Manager to end a vault relationship between a source and destination volume, and release the Snapshot copies from the source.

About this task

Releasing the relationship permanently removes the base Snapshot copies used by the vault relationship on the source volume. To re-create the vault relationship, you must run the resynchronization operation from the source volume by using the command-line interface (CLI).

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the volume for which you want to delete the vault relationship, and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

   You can also select the release base Snapshot copies check box to delete the base Snapshot copies used by the vault relationship on the source volume.

   If the relationship is not released, then you must use the CLI to run the release operation on the source cluster to delete the base Snapshot copies that were created for the vault relationship from the source volume.

Related information

Protection window

Editing vault relationships

You can use System Manager to edit a vault relationship either by selecting an existing policy or schedule in the cluster, or by creating a new policy or schedule. However, you cannot edit the parameters of an existing policy or schedule.

Before you begin

The source and destination clusters must be in a healthy peer relationship.

Steps

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

If you want to…	Do the following…
Select an existing policy	Click **Browse**, and then select an existing policy. You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.
Create a new 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 **Enable Network Compression** check box to compress the data that is being transferred. e. Specify a SnapMirror label and destination retention count for the vault policy. You must ensure that a Snapshot copy with the same label is created on the source volume for the new SnapMirror label to be effective. f. Click **Create**.

4. Specify a schedule for the relationship:

If…	Do the following…
You want to assign an existing schedule	Select an existing schedule from the list.

If…	Do the following…
You want to create a new schedule	a. Click **Create Schedule**. b. Specify a name for the schedule. c. Select one of the following options: ◦ **Basic** You can select this option to specify only the day of the week, time, and the transfer interval. ◦ **Advanced** You can select this option to specify a cron-style schedule. d. Click **Create**.
You do not want to assign a schedule	Select **None**.

5. Click **OK**.

Related information

Protection window

Initializing a vault relationship

You can use System Manager to initialize a vault relationship if you have not already initialized it while creating the relationship. A baseline transfer of data is initiated from the source FlexVol volume to the destination FlexVol volume.

Before you begin

The source and destination clusters must be in a healthy peer relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship you want to initialize, and click **Operations** > **Initialize**.
3. In the **Initialize** window, click **Initialize**.

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 a vault relationship

You can use System Manager to manually initiate an unscheduled incremental update. You might require a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

Before you begin

The vault relationship must be initialized.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to update the data, and click **Operations** > **Update**.
3. Choose one of the following options:
   - Select **As Per Policy** 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 that is 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 a vault relationship

You can use System Manager to disable data transfers to the destination FlexVol volume by quiescing the vault relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to stop the scheduled data transfers, and click **Operations** > **Quiesce**.
3. In the **Quiesce** window, click **Quiesce**.

Results

If there is no transfer in progress, the transfer status is displayed as Quiesced. If a transfer is in progress, the transfer is not affected, and the transfer status is displayed as Quiescing until the transfer is complete.

Related information

Protection window

Resuming a vault relationship

You can resume a quiesced vault relationship by using System Manager. When you resume the relationship, normal data transfer to the destination FlexVol volume is

resumed and all vault activities are restarted.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to resume the data transfer, and click **Operations** > **Resume**.
3. In the **Resume** window, click **Resume**.

Results

Normal data transfers are resumed. If there is a scheduled transfer for the relationship, the transfer is started from the next schedule.

Related information

Protection window

Aborting a Snapshot copy transfer

You can use System Manager to abort or stop a data transfer that is currently in progress.

Steps

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

Results

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 vault 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 storage system and the destination storage system 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 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 vault relationship between a source storage virtual machine (SVM) and a destination SVM in a MetroCluster configuration.
- You can restore a vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can restore a vault relationship from a volume on a sync-source SVM to a default SVM.
- You can restore a vault 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 vault relationship, and then click **Operations** > **Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the vault 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 6.
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 select any 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 check box to restore the volume from the Snapshot copy.
7. Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.

8. Click **Restore**.

Related information

Protection window

What a SnapVault backup is

A SnapVault backup is a collection of Snapshot copies on a FlexVol volume that you can restore data from if the primary data is not usable. Snapshot copies are created based on a Snapshot policy. The SnapVault backup backs up Snapshot copies based on its schedule and SnapVault policy rules.

A SnapVault backup is a disk-to-disk backup solution that you can also use to offload tape backups. In the event of data loss or corruption on a system, backed-up data can be restored from the SnapVault secondary volume with less downtime and uncertainty than is associated with conventional tape backup and restore operations.

The following terms are used to describe SnapVault backups:

- **baseline transfer**

  An initial complete backup of a primary storage volume to a corresponding volume on the secondary system.

- **secondary volume**

  A volume to which data is backed up from a primary volume. Such a volume can be a secondary or tertiary (and onward) destination in a cascade or fanout backup configuration. The SnapVault secondary system maintains Snapshot copies for long-term storage and possible restore operations.

- **incremental transfer**

  A follow-up backup to the secondary system that contains only the changes to the primary data since the last transfer action.

- **SnapMirror label**

  An attribute that identifies Snapshot copies for the purpose of selection and retention in SnapVault backups. Each SnapVault policy configures the rules for selecting Snapshot copies on the primary volume and transferring the Snapshot copies that match a given SnapMirror label.

- **Snapshot copy**

  The backup images on the source volume that are created manually or automatically as scheduled by an assigned policy. Baseline Snapshot copies contain a copy of the entire source data being protected; subsequent Snapshot copies contain differential copies of the source data. Snapshot copies can be stored on the source volume or on a different destination volume in a different storage virtual machine (SVM) or cluster.

  Snapshot copies capture the state of volume data on each source system. For SnapVault and mirror relationships, this data is transferred to destination volumes.

- **primary volume**

A volume that contains data that is to be backed up. In cascade or fanout backup deployments, the primary volume is the volume that is backed up to a SnapVault backup, regardless of where in the chain the SnapVault source is. In a cascade chain configuration in which A has a mirror relationship to B and B has a SnapVault relationship to C, B serves as the source for the SnapVault backup even though it is a secondary destination in the chain.

- **SnapVault relationship**

  A backup relationship, configured as a SnapVault relationship, between a primary volume and a secondary volume.

Related information

Protection window

Mirror and vault relationships

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

Create a mirror and vault relationship from a destination SVM

You can use System Manager to create a mirror and vault relationship from the destination storage virtual machine (SVM). Creating this relationship enables you to better protect your data by periodically transferring data from the source volume to the destination volume. It also enables you to retain data for long periods by creating backups of the source volume.

Before you begin

- The destination cluster must be running ONTAP 8.3.2 or later.
- 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.

- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination SVM must have space available.
- The source aggregate and destination aggregate must be 64-bit aggregates.
- A source volume of type read/write (rw) must already exist.
- The SnapLock aggregate type must be the same.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which 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 and vault relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a mirror and vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a mirror and vault relationship from a volume on a sync-source SVM to a volume of a data-serving SVM.
- You can create a mirror and vault relationship from a volume on a data-serving SVM to a DP volume on a sync-source SVM.
- A maximum of 25 volumes can be protected in one selection.

Steps

1. Click **Protection** > **Volume Relationships**.
2. In the **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 and Vault** 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. Enter 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 and vault policy.

   You can select the policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.

8. Select a schedule for the relationship from the list of existing schedules.
9. Select **Initialize Relationship** to initialize the relationship.
10. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.
11. Click **Validate** to verify whether the selected volumes have matching labels.
12. Click **Create**.

Deleting mirror and vault relationships

You can use System Manager to end a mirror and vault relationship between a source and destination volume, and release the Snapshot copies from the source volume.

About this task

- It is a best practice to break the mirror and vault relationship before deleting the relationship.
- To re-create the relationship, you must run the resynchronization operation from the source volume by using the command-line interface (CLI).

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to delete and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

   You can also select the release base Snapshot copies check box to delete the base Snapshot copies used by the mirror and vault relationship on the source volume.

   If the relationship is not released, then you must use the CLI to run the release operation on the source cluster to delete the base Snapshot copies that were created for the mirror and vault relationship from the source volume.

Results

The relationship is deleted and the base Snapshot copies on the source volume are permanently deleted.

Editing mirror and vault relationships

You can use System Manager to edit a mirror and vault relationship by modifying the selected policy or schedule. However, you cannot edit the parameters of an existing policy or schedule.

Before you begin

The source and destination clusters must be in a healthy peer relationship.

About this task

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 and vault relationship that you want to modify, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select the appropriate action:

If you want to…	Do the following…
Select an existing policy	Click **Browse**, and then select an existing policy. You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.

If you want to…	Do the following…
Create a new 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 **Enable Network Compression** check box to compress the data that is being transferred. e. Specify a SnapMirror label and destination retention count for the vault policy. You must ensure that a Snapshot copy with the same label is created on the source volume for the new SnapMirror label to be effective. f. Click **Create**.

4. Specify a schedule for the relationship:

If…	Do the following…
You want to assign an existing schedule	Click **Browse**, and then select an existing schedule.
You want to create a new schedule	a. Click **Create Schedule**. b. Specify a name for the schedule. c. Select one of the following options: ◦ **Basic** You can select this option to specify only the day of the week, time, and the transfer interval. ◦ **Advanced** You can select this option to specify a cron style schedule. d. Click **Create**.
You do not want to assign a schedule	Select **None**.

5. Click **OK**.

Initializing mirror and vault relationships

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

Before you begin

The source and destination clusters must be in a healthy peer relationship.

Steps

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

Updating mirror and vault relationships

You can use System Manager to manually initiate an unscheduled incremental update. You might require a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

Before you begin

The mirror and vault relationship must be initialized and in a Snapmirrored state.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship for which you want to update the data, and then click **Operations** > **Update**.
3. Choose one of the following options:
   - Select **As Per Policy** 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 that is used for transfers, and then specify the maximum transfer speed.
5. Click **Update**.
6. Verify the transfer status in the **Details** tab.

Quiescing mirror and vault relationships

You can use System Manager to quiesce a destination volume to stabilize the destination before creating a Snapshot copy. The quiesce operation enables active data transfers to

finish and disables future transfers for the mirror and vault relationship.

Before you begin

The mirror and vault relationship must be in a Snapmirrored state.

Steps

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

Results

If there is no transfer in progress, the transfer status is displayed as Quiesced. If a transfer is in progress, the transfer is not affected, and the transfer status is displayed as Quiescing until the transfer is complete.

Resuming mirror and vault relationships

If you have a quiesced mirror and vault relationship, you can resume the relationship by using System Manager. When you resume the relationship, normal data transfer to the destination volume is resumed and all the protection activities are restarted.

About this task

If you have quiesced a broken mirror and vault 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 and vault relationship that you want to resume, and then click **Operations** > **Resume**.
3. Select the confirmation check box, and then click **Resume**.

Results

Normal data transfers are resumed. If there is a scheduled transfer for the relationship, the transfer is started from the next schedule.

Breaking mirror and vault relationships

You can use System Manager to break a mirror and vault relationship if a source volume becomes unavailable and you want client applications to access the data from the destination volume. 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.

Before you begin

- The mirror and vault relationship 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 break mirror relationships between ONTAP systems and SolidFire storage systems.

Steps

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

Results

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

Resynchronizing mirror and vault relationships

You can use System Manager to reestablish a mirror and vault 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 and destination clusters and the source and destination storage virtual machines (SVMs) must be in peer relationships.

About this task

You should be aware of the following before performing a resynchronization operation:

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

  The resynchronization operation can cause loss of newer data 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 and vault relationship that you want to resynchronize, and then click **Operations** > **Resync**.
3. Select the confirmation check box, and then click **Resync**.

Reverse resynchronizing mirror and vault relationships

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

Before you begin

The source volume must be online.

About this task

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

  The reverse resynchronization operation can cause data loss on the source volume.

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

Steps

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

Aborting mirror and vault relationships

You can abort a volume replication operation if you want to stop the data transfer. You can abort a scheduled update, a manual update, or an initial data transfer.

Steps

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

Results

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

Restoring a volume in a mirror and vault 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 and SnapVault 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 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 and vault relationship between a source storage virtual machine (SVM) and a destination SVM in a MetroCluster configuration.
- You can restore a mirror and vault relationship for the following configurations:
  - Between sync-source SVMs in a MetroCluster configuration
  - From a volume on a sync-source SVM to a default SVM
  - 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 and vault relationship that you want to restore, and then click **Operations** > **Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the 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 6.
Any other volume	Select **Other volume**, and then select the cluster and the SVM.

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 check box to restore the volume from the Snapshot copy.
7. Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.
8. Click **Restore**.

What lag time is

Lag time is the amount of time by which the destination system lags behind the source system.

The lag time is the difference between the current time and the timestamp of the Snapshot copy that was last successfully transferred to the destination system. The lag time will always be at least as much as the duration of the last successful transfer, unless the clocks on the source and destination systems are not synchronized. The time zone difference is automatically calculated into the lag time.

Types of data protection relationships

Depending on your data protection and backup requirements, ONTAP System Manager provides different types of protection relationships that enable you to protect data against accidental, malicious, or disaster-induced loss of data.

Asynchronous replication type

Mirror relationship

A mirror relationship provides asynchronous disaster recovery. Data protection mirror relationships enable you to periodically create Snapshot copies of the data on one volume, to copy those Snapshot copies to a partner volume (the destination volume), which is usually on another cluster, and then to retain those Snapshot copies. If the data on the source volume is corrupted or lost, the mirror copy on the destination volume ensures quick availability and restoration of data from the time of the latest Snapshot copy.

For mirror relationships, the version of ONTAP that is running on the destination cluster must be the same version as or a later version than the ONTAP version running on the source cluster. However, version-flexible mirror relationships are not dependent on the ONTAP version. Therefore, you can create a version-flexible mirror relationship with a destination cluster that is running either a later ONTAP version or an earlier ONTAP version than the ONTAP version of the source cluster or an earlier version of ONTAP than the ONTAP version of the source cluster.

- The SnapMirror license is required to enable mirror relationship.
- The version-flexible mirror relationship feature is available only from ONTAP 8.3 onward. You cannot have a version-flexible mirror relationship with a volume in Data ONTAP 8.3 or earlier.

Vault relationship

A vault relationship provides storage-efficient and long-term retention of backups. Vault relationships enable you to back up selected Snapshot copies of volumes to a destination volume and to retain the backups.

The SnapMirror or SnapVault license is required to enable vault relationship.

Mirror and vault relationship

A mirror and vault relationship provides data protection by periodically transferring data from the source volume to the destination volume and also facilitates long-term retention of data by creating backups of the source volume.

- The SnapMirror license is required to enable mirror and vault relationship.
- The mirror and vault relationship feature is available only from ONTAP 8.3.2 onward. You cannot have a mirror and vault relationship with a volume in Data ONTAP 8.3.2 or earlier.

Synchronous replication policy (SnapMirror Synchronous license required)

StrictSync

A StrictSync replication policy will impose input/output (I/O) restrictions on the source volume in case of a replication failure post initialization. A StrictSync replication policy provides data protection by ensuring that the source volume and the destination volume are up to date.

- If the destination is not Data Protection Optimization (DPO), then the SnapMirror license is required on the source cluster and the destination cluster and the SnapMirror Synchronous license is required on the source cluster.
- If the destination is DPO, then the SnapMirror Synchronous license and the SnapMirror license is required on the source cluster and the DPO license is required on the destination cluster.

Sync

A Sync replication policy does not impose I/O restrictions on the source volume in case of a replication failure post initialization. A Sync replication policy does not transfer data to destination volume after the failure. You need to perform a resynchronization operation to ensure that the source volume and destination volume are up to date.

- If the destination is not Data Protection Optimization (DPO), then the SnapMirror license is required on the source cluster and the destination cluster and the SnapMirror Synchronous license is required on the source cluster.
- If the destination is DPO, then the SnapMirror Synchronous license and the SnapMirror license is required on the source cluster and the DPO license is required on the destination cluster.

Understanding workloads supported by StrictSync and Sync policies

StrictSync and Sync policies support all LUN-based applications with FC, iSCSI, and FC-NVMe protocols, as well as NFSv3 and NFSv4 protocols for enterprise applications such as databases, VMWare, quota, CIFS, and so on. Starting with ONTAP 9.6, SnapMirror Synchronous can be used for enterprise file services such as electronic design automation (EDA), home directories, and software build workloads.

In ONTAP 9.5, for a Sync policy, you need to consider a few important aspects while selecting the NFSv3 or NFSv4 workloads. The amount of data read or write operations by workloads is not a consideration, as Sync policy can handle high read or write IO workloads. In ONTAP 9.5, workloads that have excessive file creation, directory creation, file permission changes, or directory permission changes may not be suitable (these are referred to as high-metadata workloads). A typical example of a high-metadata workload is a DevOps workload in which you create multiple test files, run automation, and delete the files. Another example is parallel build workload that generate multiple temporary files during compilation. The impact of a high rate of write metadata

activity is that it can cause synchronization between mirrors to temporarily break which stalls the read and write IOs from the client.

Starting with ONTAP 9.6, these limitations are removed and SnapMirror Synchronous can be used for enterprise file services workloads that include multiuser environments, such as home directories and software build workloads.

Related information

NetApp Technical Report 4733: SnapMirror Synchronous for ONTAP 9.6

SnapMirror licensing

With the introduction of ONTAP 9.3, licensing has been simplified for replicating between ONTAP instances. In ONTAP 9 releases, the SnapMirror license supports both vault and mirror relationships. Users can now purchase a SnapMirror license to support ONTAP replication for both backup and disaster recovery use cases.

Prior to the ONTAP 9.3 release, two licenses were available to support different replication use cases. A SnapVault license was needed to configure *vault* relationships between ONTAP instances, where the DP instance could retain a higher number of Snapshot copies to support backup use cases where retention times are longer. A SnapMirror license was needed to configure *mirror* relationships between ONTAP instances, where each ONTAP instance would maintain the same number of snapshot copies (that is, a *mirror* image) to support disaster recovery use cases where cluster failovers would be possible. Both SnapMirror and SnapVault licenses can continue to be used and supported for ONTAP 8.x and 9.x releases.

SnapVault licenses continue to function and are supported for both ONTAP 8.x and 9.x releases, but they are no longer being sold. The SnapMirror license continues to be available and can be used in place of SnapVault and can be used for both mirror and vault configurations.

For ONTAP asynchronous replication, beginning with ONTAP 9.3 a single unified replication engine is used to configure extended data protection mode (XDP) policies, where the SnapMirror license can be configured for a mirror policy, a vault policy, or a mirror-vault policy. A SnapMirror license is required on both the source and destination clusters. A SnapVault license is not required if a SnapMirror license is already installed.

SnapMirror Synchronous license

Starting with ONTAP 9.5, SnapMirror Synchronous relationships are supported. You require the following licenses for creating a SnapMirror Synchronous relationship:

- The SnapMirror Synchronous license is required on both the source cluster and the destination cluster.

  If your system was purchased before June 2019 with a Premium or Flash Bundle, you can download a NetApp master key to get the required SnapMirror Synchronous license from the NetApp Support Site: Master License Keys

- The SnapMirror license is required on both the source cluster and the destination cluster.

SnapMirror Cloud license

Starting with ONTAP 9.8, the SnapMirror Cloud license provides asynchronous replication of Snapshot copies from ONTAP instances to object storage endpoints. Replication targets can be configured using both on-premises object stores as well as S3 and S3-compatible public cloud object storage services. SnapMirror

Cloud relationships are supported from ONTAP systems to pre-qualified object storage targets. ONTAP 9.8 approved object storage targets include ONTAP S3, StorageGRID, AWS S3 and S3-IA, Microsoft Azure Blob Hot, and GCP Standard storage.

SnapMirror Cloud is not available as a standalone license and is available only with purchase of the Hybrid Cloud Bundle. Beginning with ONTAP 9.8, the Hybrid Cloud Bundle includes licenses for both SnapMirror Cloud and FabricPool. Similarly, the SnapMirror license is not available as a standalone license and is available only with purchase of the Data Protection Bundle.

You require the following licenses for creating a SnapMirror Cloud relationship:

- Both a SnapMirror license (purchased through Data Protection Bundle, or through Premium Bundle) and a SnapMirror Cloud license (purchased through Hybrid Cloud Bundle) is replicating directly to the object store endpoint.
- When configuring a multi-policy replication workflow (for example, Disk-to-Disk-to-Cloud), a SnapMirror license is required on all ONTAP instances, while the SnapMirror Cloud license is only required for the source cluster which is replicating directly to the object storage endpoint.

SnapMirror Cloud is an end user license which can be purchased from NetApp or from an approved NetApp reseller partner. The SnapMirror Cloud license provides end user entitlement but does not enable asynchronous ONTAP to object storage replication. To invoke ONTAP APIs for SnapMirror Cloud, a unique API key from an authorized application is required. Authorized and licensed applications used to orchestrate SnapMirror Cloud replication are available from multiple third-party application providers. These authorized applications will embed the unique API key to invoke ONTAP APIs. A combination of the SnapMirror Cloud end user license and an authorized third-party backup application is required to orchestrate and enable SnapMirror Cloud replication.

A list of authorized SnapMirror Cloud third-party applications is published on the NetApp web site.

Data Protection Bundle

Starting with ONTAP 9.1, new ONTAP data protection features were packaged with the FAS8200 as part of a solution called the Data Protection Bundle. This new hardware and software bundle included a new DP_Optimized (DPO) license that provided unique ONTAP features for secondary workloads. With the introduction of ONTAP 9.3 the DPO license increased the number of volumes per node from 1,000 to 1,500. Also introduced with ONTAP 9.3 were new configurations of the Data Protection Bundle based on configurations of FAS2620.

The DPO license was specifically designed for ONTAP clusters that were to be dedicated as secondary targets for SnapMirror replication. In addition to increasing the maximum volumes per node on the DPO controller, the DPO license also modified controller QoS settings to support greater replication traffic at the expense of application I/O. For this reason, the DPO license should never be installed on a cluster that supports application I/O, as application performance would be impacted. Later, Data Protection Bundles based on the FAS8200 and FAS2620 were offered as a solution and included programmatic free licenses based on the customer environment. When purchasing the solution bundles, free SnapMirror licenses would be provided for select older clusters which replicated to the DPO secondary. While the DPO license is needed on the Data Protection solution cluster, primary clusters from the following platform list would be provided free SnapMirror licenses. Primary clusters not included in this list would require purchase of SnapMirror licenses.

- FAS2200 Series
- FAS3000 Series
- FAS6000 Series
- FAS8000 Series

Data Protection Optimized (DPO) License

Data Protection hardware and software solution bundles introduced with ONTAP 9.1 and 9.3 were based on FAS8200 and FAS2620 only. As these platforms matured and new platforms were introduced new requests to support ONTAP features for secondary replication use cases increased. As a result, a new standalone DPO license was introduced in November 2018 with ONTAP 9.5 release.

The standalone DPO license was supported on both FAS and AFF platforms and could be purchased pre-configured with new clusters or added to deployed clusters as a software upgrade in the field. Because these new DPO licenses were not part of a hardware and software solution bundle they carried a lower price and free SnapMirror licenses for primary clusters were not provided. Secondary clusters configured with the a la carte DPO license must also purchase a SnapMirror license, and all primary clusters replicating to the DPO secondary cluster must purchase a SnapMirror license.

Additional ONTAP features were delivered with the DPO across multiple ONTAP releases.

Feature	9.3	9.4	9.5	9.6	9.7a	Max vols/node
1500	1500	1500	1500/2500	1500/2500	Max concurrent repl sessions	100
200	200	200	200	Workload bias*	client apps	Apps/SM
SnapMirror	SnapMirror	SnapMirror	Cross volume aggregate deduplication for HDD	No	Yes	Yes

- Details about priority for the SnapMirror backoff (workload bias) feature:
- Client: cluster I/O priority is set to client workloads (production apps), not SnapMirror traffic.
- Equality: SnapMirror replication requests have equal priority to I/O for production apps.
- SnapMirror: all SnapMirror I/O requests have higher priority that I/O for production apps.

	9.3—9.5 Without DPO	9.3—9.5 With DPO	9.6 Without DPO	9.6 With DPO	9.7 Without DPO	9.7 With DPO
FAS2620	1000	1500	1000	1500	1000	1500
FAS2650	1000	1500	1000	1500	1000	1500
FAS2720	1000	1500	1000	1500	1000	1500
FAS2750	1000	1500	1000	1500	1000	1500
A200	1000	1500	1000	1500	1000	1500

	9.3—9.5 Without DPO	9.3—9.5 With DPO	9.6 Without DPO	9.6 With DPO	9.7 Without DPO	9.7 With DPO
A200	1000	1500	1000	1500	1000	1500
FAS8200/8300	1000	1500	1000	2500	1000	2500
A300	1000	1500	1000	2500	2500	2500
A400	1000	1500	1000	2500	2500	2500
FAS8700/9000	1000	1500	1000	2500	1000	2500
A700	1000	1500	1000	2500	2500	2500
A700s	1000	1500	1000	2500	2500	2500
A800	1000	1500	1000	2500	2500	2500

Considerations for all new DPO installations

- Once enabled, the DPO license feature cannot be disabled or undone.
- Installation of the DPO license requires a re-boot of ONTAP or failover to enable.
- The DPO solution is intended for secondary storage workloads; application workload performance on DPO clusters may be impacted
- The DPO license is supported on a select list of NetApp storage platform models.
- DPO features vary by ONTAP release. Refer to the compatibility table for reference.

Protection window

You can use the Protection window to create and manage mirror relationships, vault relationships, and mirror and vault relationships and to display details about these relationships. The Protection window does not display load-sharing (LS) relationships and transition data protection (TDP) relationships.

Command buttons

- **Create**

  Opens the Create Protection Relationship dialog box, which you can use to create a mirror relationship, vault relationship, or mirror and vault relationship from a destination volume.

  System Manager does not display any storage virtual machine (SVM) that is configured for disaster recovery (DR) in the Create Protection Relationship dialog box.

- **Edit**

  Opens the Edit Protection Relationship dialog box, which you can use to edit the schedule and policy of a relationship.

  For a vault relationship, mirror and vault relationship, or version-flexible mirror relationship, you can modify the relationship type by modifying the policy type.

- **Delete**

  Opens the Delete Protection Relationship dialog box, which you can use to delete a relationship.

- **Operations**

  Displays the operations that can be performed on a protection relationship.

- **Refresh**

  Updates the information in the window.

Protection relationships list

- **Source Storage Virtual Machine**

  Displays the SVM that contains the volume from which data is mirrored or vaulted in a relationship.

- **Source Volume**

  Displays the volume from which data is mirrored or vaulted in a relationship.

- **Destination Volume**

  Displays the volume to which data is mirrored or vaulted in a relationship.

- **Is Healthy**

  Displays whether the relationship is healthy or not.

- **Object Type**

  Displays the object type of the relationship, such as Volume, FlexGroup, or SVM.

- **Relationship State**

  Displays the state of the relationship, such as Snapmirrored, Uninitialized, or Broken Off.

- **Transfer Status**

  Displays the status of the relationship.

- **Relationship Type**

  Displays the type of relationship, such as mirror, vault, or mirror and vault.

- **Lag Time**

Lag time is the difference between the current time and the timestamp of the last Snapshot copy that was successfully transferred to the destination system. The lag time will always be at least as much as the duration of the last successful transfer, unless the clocks on the source and destination systems are not synchronized. The time zone difference is automatically calculated into the lag time.

- **Policy Name**

  Displays the name of the policy that is assigned to the relationship.

- **Policy Type**

  Displays the type of policy that is assigned to the relationship. The policy type can be StrictSync, Sync, Asynchronous Mirror, Asynchronous Vault, or Asynchronous Mirror Vault.

Details area

- **Details tab**

  Displays general information about the selected relationship, such as the source cluster and destination cluster, data transfer rate, state of the relationship, details about the network compression ratio, data transfer status, type of current data transfer, type of last data transfer, latest Snapshot copy, and timestamp of the latest Snapshot copy.

- **Policy Details tab**

  Displays details about the policy that is assigned to the selected protection relationship. This tab also displays the SnapMirror label and the Snapshot copy schedules in the source volume that match the specified label.

- **Snapshot Copies tab**

  Displays the count of Snapshot copies with the SnapMirror label attribute for the selected protection relationship and the timestamp of the latest Snapshot copy.

Related information

Creating a mirror relationship from a source SVM

Creating a mirror relationship from a destination SVM

Deleting mirror relationships

Editing mirror relationships

Initializing mirror relationships

Updating mirror relationships

Quiescing mirror relationships

Resuming mirror relationships

Breaking SnapMirror relationships

Resynchronizing mirror relationships

Reverse resynchronizing mirror relationships

Aborting a mirror transfer

What a SnapVault backup is

Creating a vault relationship from a source SVM

Creating a vault relationship from a destination SVM

Deleting vault relationships

Editing vault relationships

Initializing a vault relationship

Updating a vault relationship

Quiescing a vault relationship

Resuming a vault relationship

Aborting a Snapshot copy transfer

Restoring a volume in a vault relationship

SVM Relationships

Storage virtual machine (SVM) disaster recovery (DR) provides disaster recovery capability at the SVM level by enabling the recovery of the data that is present in the constituent volumes of the SVM and the recovery of the SVM configuration.

You can use System Manager to create and manage mirror relationships and mirror and vault relationships between SVMs.

Create SVM relationships

You can use System Manager to create SVM relationships to transfer data from the source SVM to the destination SVM. Creating an SVM relationship helps in recovering from a disaster as data is available on the source SVM and on the destination SVM.

Before you begin

- The destination cluster and source cluster must be running ONTAP 9.5 or later.
- The destination cluster must not be in a MetroCluster configurations.
- Starting with System Manager 9.6, Fabric Pool is supported.

Steps

1. Click **Protection** > **SVM Relationship** > **Create**.
2. Select the SVM relationship type from the **SVM Relationship Type** list.
3. From the **Source Storage Virtual Machine** pane, select the cluster and the SVM.

4. To view SVMs that do not have the required permissions, click **Navigate to the source cluster**, and then provide the required permissions.
5. From the **Destination Storage Virtual Machine** pane, specify the name of the SVM that will be created on the destination cluster.
6. Select the option to copy the source SVM configuration.
7. Click , update the protection policy and protection schedule, select aggregate, and then initialize the protection relationship.
8. Click **Save** to create the SVM relationship.

   The SVM Relationships: Summary window is displayed.

9. Click **Done** to complete the process.

Editing SVM relationships

You can use System Manager to modify the properties of an SVM relationship.

Steps

1. Click **Protection** > **SVM Relationship**.
2. Select the SVM relationship that you want to modify, and then click **Edit**.
3. Select the SVM relationship type.

   If the SVM relationships were created before ONTAP 9.3, then changing the SVM relationship type from mirror to mirror and vault is not allowed.

4. Modify the protection policy, the protection schedule, and the option to copy the source SVM configuration, as required.
5. Click **Save** to save the changes.

Managing SVM relationships

You can use System Manager to perform various operations on SVM relationships such as initializing SVM relationships, updating SVM relationships, activating the destination SVM, resynchronizing data from the source SVM, resynchronizing data from the destination SVM, and reactivating the source SVM.

Before you begin

- To initialize the SVM relationship, the source and destination clusters must be in a healthy peer relationship.
- To update the SVM relationship, the SVM relationship must be initialized and in a Snapmirrored state.
- To reactivate the source SVM, the resynchronize data from the destination SVM (reverse resync) operation must have been performed.
- If you had selected the option to copy the source SVM configuration while creating the SVM relationship, then to activate the SVM relationship, the source SVM must be stopped.
- SnapMirror license must be enabled on the source cluster and destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.

- The destination cluster must have space available.
- The source SVM must have permission for SVM peering.
- You must break the SVM relationship to activate destination SVM, resync from source SVM, resync from destination SVM (Reverse Resync), and reactivate source SVM.
- To reactivate the source SVM, the SVM reverse relationship must exist and be in a Snapmirrored state.

Steps

1. Click **Protection** > **SVM Relationship**.
2. Select the SVM relationship, and then perform the appropriate action:

If you want to…	Do the following…
Initialize the SVM relationship	a. Click **Operations** > **Initialize**. The Initialize dialog box is displayed. b. Click **Initialize**.
Update the SVM relationship	a. Click **Operations** > **Update**. The Update dialog box is displayed. b. Click **Update**.
Activate the destination SVM Activating the destination SVM involves quiescing scheduled SnapMirror transfers, aborting any ongoing SnapMirror transfers, breaking the SVM relationship, and starting the destination SVM.	a. Click **Operations** > **Activate Destination SVM**. The Activate Destination SVM dialog box is displayed. b. Select the **Ok to activate destination SVM and break the relationship** checkbox. c. Click **Activate**.
Resynchronize data from the source SVM The resync operation performs a rebaseline of the SVM configuration. You can resync from the source SVM to reestablish a broken relationship between the two SVMs. When the resync is complete, the destination SVM contains the same information as the source SVM and is scheduled for further updates.	a. Click **Operations** > **Resync from Source SVM**. The Resync from Source SVM dialog box is displayed. b. Select the **Ok to delete any newer data in the destination SVM** checkbox. c. Click **Resync**.

If you want to…	Do the following…
Resynchronize data from the destination SVM (Reverse Resync) You can resync from the destination SVM to create a new relationship between the two SVMs. During this operation, the destination SVM continues to serve data with the source SVM backing up the configuration and data of the destination SVM.	a. Click **Operations** > **Resync from Destination SVM (Reverse ReSync)**. The Resync from Destination SVM (Reverse Resync) dialog box is displayed. b. If the SVM has multiple relationships, select the **This SVM has multiple relationships, Ok to release to other relationships** checkbox. c. Select the **Ok to delete the new data in the source SVM** checkbox. d. Click **Reverse Resync**.
Reactivate the source SVM Reactivating the source SVM involves protecting and recreating the SVM relationships between the source and destination SVM. If you had selected the option to copy the source SVM configuration while creating the SVM relationship, then the destination SVM will stop processing data.	a. Click **Operations** > **Reactivate Source SVM**. The Reactivate Source SVM dialog box is displayed. b. Click **Initiate Reactivation** to initiate reactivation to the destination SVM. c. Click **Done**.

SVM Relationships Window

You can use the SVM Relationships window to create and manage mirror relationships, and mirror and vault relationships between SVMs.

Command buttons

- **Create**

  Opens the SVM Disaster Recovery page, which you can use to create a mirror relationship, or mirror and vault relationship from a destination volume.

- **Edit**

  Enables you to edit the schedule and policy of a relationship.

  For mirror and vault relationship, or version-flexible mirror relationship, you can modify the relationship type by modifying the policy type.

- **Delete**

  Enables you to delete a relationship.

- **Operations**

  Provides the following options:

- **Initialize**

  Enables you to initialize the SVM relationship to perform a baseline transfer from the source SVM to the destination SVM.

- **Update**

  Enables you to update data from the source SVM to the destination SVM.

- **Activate Destination SVM**

  Enables you to activate the destination SVM.

- **Resync from Source SVM**

  Enables you to initiate resynchronization of a broken relationship.

- **Resync from Destination SVM (Reverse Resync)**

  Enables you to resynchronize the relationship from the destination SVM to the source SVM.

- **Reactivate Source SVM**

  Enables you to reactivate the source SVM.

- **Refresh**

  Updates the information in the window.

SVM relationships list

- **Source Storage Virtual Machine**

  Displays the SVM that contains the volume from which data is mirrored and vaulted in a relationship.

- **Destination Storage Virtual Machine**

  Displays the SVM that contains the volume to which data is mirrored and vaulted in a relationship.

- **Is Healthy**

  Displays whether the relationship is healthy or not.

- **Relationship State**

  Displays the state of the relationship, such as Snapmirrored, Uninitialized, or Broken Off.

- **Transfer Status**

  Displays the status of the relationship.

- **Relationship Type**

  Displays the type of relationship, such as mirror, or mirror and vault.

- **Lag Time**

  Lag time is the difference between the current time and the timestamp of the last Snapshot copy that was successfully transferred to the destination system. The lag time will always be at least as much as the duration of the last successful transfer, unless the clocks on the source and destination systems are not synchronized. The time zone difference is automatically calculated into the lag time.

- **Policy Name**

  Displays the name of the policy that is assigned to the relationship.

- **Policy Type**

  Displays the type of policy that is assigned to the relationship. The policy type can be StrictSync, Sync, Asynchronous Mirror, Asynchronous Vault, or Asynchronous Mirror Vault.

Details area

- **Details tab**

  Displays general information about the selected relationship, such as the source cluster and destination cluster, the protection relationship that is associated with the SVM, data transfer rate, state of the relationship, details about the network compression ratio, data transfer status, type of current data transfer, type of last data transfer, latest Snapshot copy, timestamp of the latest Snapshot copy, the status of the identity preserve, and the number of volumes protected.

- **Policy Details tab**

  Displays details about the policy that is assigned to the selected protection relationship.

Protection policies

You can use System Manager to create, edit, and delete protection policies.

Create protection policies

You can use System Manager to create cluster-level asynchronous mirror policies, vault policies, or mirror and vault policies, and to apply these policies to a cluster-level data protection relationship.

Steps

1. Click **Protection** > **Protection Policies**.
2. Click **Create**.
3. In the **Create Policy** dialog box, select the type of policy that you want to create.
4. Specify the policy name and transfer priority.

   Low indicates that the transfer has the lowest priority. Low priority transfers are usually scheduled after normal priority transfers. By default, the transfer priority is set to Normal.

5. Select the **Enable Network Compression** check box to compress the data that is being transferred during a data transfer.

6. For an asynchronous mirror policy, select the **Transfer All Source Snapshot Copies** check box to include the “all_source_snapshots” rule to the mirror policy, which backs up all of the Snapshot copies from the source volume.
7. Click **Add Comments** to add additional comments for the policy.
8. For a vault policy or mirror vault policy, specify a SnapMirror label and a destination retention count.
9. Click **Create**.

Protection Policies window

You can use the Protection Policies window to create, manage, and display information about mirror, vault, and mirror vault policies.

Command buttons

- **Create**

  Opens the Create Policy dialog box, which enables you to create a mirror, vault, or mirror vault policy.

- **Edit**

  Opens the Edit Policy dialog box, which enables you to edit a policy.

- **Delete**

  Opens the Delete Policy dialog box, which enables you to delete a policy.

- **Refresh**

  Updates the information in the window.

Protection policies list

- **Name**

  Displays the name of the protection policy.

- **Type**

  Displays the policy type, which can be Vault, Mirror Vault, or Asynchronous Mirror.

- **Comment**

  Displays the description specified for the policy.

- **Transfer Priority**

  Displays the data transfer priority, such as Normal or Low.

Details area

- **Policy Details tab**

Displays details of the protection policy, such as the user who created the policy, number of rules, retention count, and status of network compression.

- **Policy Rules tab**

  Displays details of the rules that are applied to the policy. The Policy Rules tab is displayed only if the selected policy contains rules.

Snapshot policies

You can use System Manager to create and manage Snapshot policies in your storage system.

Create Snapshot policies

You can create a Snapshot policy in System Manager to specify the maximum number of Snapshot copies that can be automatically created and the frequency of creating them.

Steps

1. Click **Protection** > **Snapshot Policies**.
2. Click **Create**.
3. In the **Create Snapshot Policy** dialog box, specify the policy name.
4. Click **Add**, and then specify the schedule name, the maximum number of Snapshot copies that you want to retain, and the SnapMirror label name.

   The maximum number of Snapshot copies that can be retained by the specified schedules must not exceed 254.

5. Click **OK**, and then click **Create**.

Editing Snapshot policies

You can modify the details of an existing Snapshot policy, such as the schedule name, SnapMirror label, or the maximum number of Snapshot copies that are created, by using the Edit Snapshot Policy dialog box in System Manager.

Steps

1. Click **Protection** > **Snapshot Policies**.
2. In the **Snapshot Policies** window, select the Snapshot policy that you want to modify and click **Edit**.
3. In the **Edit Snapshot Policy** dialog box, select the schedule that you want to modify and click **Edit**.
4. Click **OK**.
5. Verify the changes you made to the selected Snapshot policy in the **Edit Snapshot Policy** dialog box and click **Save**.

Deleting Snapshot policies

You can use System Manager to delete Snapshot policies. If you delete a Snapshot

policy that is being used by one or more volumes, Snapshot copies of the volume or volumes are no longer created according to the deleted policy.

Before you begin

You must have dissociated the Snapshot policy from each volume that uses it.

Steps

1. Click **Protection** > **Snapshot Policies**.
2. Select the Snapshot policy and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

About Snapshot policies

When applied to a volume, a Snapshot policy specifies a schedule or schedules according to which Snapshot copies are created and specifies the maximum number of Snapshot copies that each schedule can create. A Snapshot policy can include up to five schedules.

For vault relationships, the SnapMirror Label attribute is used to select Snapshot copies on the source volumes. Only Snapshot copies with the labels configured in the vault policy rules are replicated in backup vault operations. The Snapshot policy assigned to the source volume must include the SnapMirror Label attribute.

Snapshot Policies window

You can use the Snapshot Policies window to manage Snapshot policy tasks, such as adding, editing, and deleting Snapshot policies.

Command buttons

- **Create**

  Opens the Create Snapshot Policy dialog box, which enables you to add backup schedules and specify the maximum number of Snapshot copies to be retained in a policy.

- **Edit**

  Opens the Edit Snapshot Policy dialog box, which enables you to modify the frequency at which Snapshot copies should be created and the maximum number of Snapshot copies to be retained.

- **Delete**

  Opens the Delete dialog box, which enables you to delete the selected Snapshot policy.

- **View as**

  Enables you to view the Snapshot policies either as a list or as a tree.

- **Status**

  Opens the menu, which you can use to either enable or disable the selected Snapshot policy.

- **Refresh**

  Updates the information in the window.

Snapshot policy list

- **Policy/Schedule Name**

  Specifies the name of the Snapshot policy and the schedules in the policy.

- **Storage Virtual Machine**

  Specifies the name of the storage virtual machine (SVM) to which the Snapshot copies belong.

- **Status**

  Specifies the status of the Snapshot policy, which can be Enabled or Disabled.

- **Maximum Snapshots to be retained**

  Specifies the maximum number of Snapshot copies to be retained.

- **SnapMirror Label**

  Specifies the name of the SnapMirror label attribute of the Snapshot copy generated by the backup schedule.

Schedules

You can use System Manager to create and manage schedules in your storage system.

Create schedules

You can create schedules to run a job at a specific time or at regular periods by using System Manager.

About this task

When you create a schedule in a MetroCluster configuration, it is a best practice to create an equivalent schedule on the cluster in the surviving site as well.

Steps

1. Click **Protection** > **Schedules**.
2. Click **Create**.
3. In the **Create Schedule** dialog box, specify the schedule name.
4. Create a schedule based on your requirements:

If you want to create…	Do this…
A daily or a specific schedule on certain days	Select **Basic**, and specify the schedule and recurrence details (in hours and minutes).

If you want to create…	Do this…
A schedule that runs at a specific interval	Select **Interval**, and specify the schedule and recurrence details (in days, hours, and minutes).
A schedule that runs at a specific period	Select **Advanced**, and specify the schedule and recurrence details (in months, days, weekdays, hours, and minutes).

5. Click **Create**.

Editing schedules

You can make changes to a previously created cron schedule or an interval schedule if it does not meet your requirements by using System Manager. You can modify schedule details such as recurring days and hours, interval options, and advanced cron options.

About this task

When you edit a schedule in a MetroCluster configuration, it is a best practice to edit the equivalent schedule on the surviving site cluster as well.

Steps

1. Click **Protection** > **Schedules**.
2. Select the schedule that you want to modify and click **Edit**.
3. In the **Edit Schedule** dialog box, modify the schedule by performing the appropriate action:

If you select the schedule option as…	Do this..
Basic	Specify the recurring days and recurring schedule details.
Interval	Specify the interval options in days, hours, and minutes.
Advanced	Specify the advanced cron options in months, days, week days (if applicable), hours, and minutes.

4. Click **OK**.

Deleting schedules

You can use System Manager to delete the schedules that run specific storage management tasks.

Steps

1. Click **Protection** > **Schedules**.
2. Select the schedule that you want to delete and click **Delete**.

3. Select the confirmation check box, and then click **Delete**.

Schedules

You can configure many tasks (for instance, volume Snapshot copies and mirror replications) to run on specified schedules. Schedules that are run at specified schedules are known as *cron* schedules because of their similarity to UNIX `cron` schedules. Schedules that are run at intervals are known as *interval* schedules.

You can manage schedules in the following ways:

- Creating a cron schedule or an interval schedule
- Displaying information about all the schedules
- Modifying a cron schedule or an interval schedule
- Deleting a cron schedule or an interval schedule

  You cannot delete a schedule that is currently in use by a running job.

The cluster administrator can perform all the schedule management tasks.

Schedules window

You can use the Schedules window to manage scheduled tasks, such as creating, displaying information about, modifying, and deleting schedules.

Command buttons

- **Create**

  Opens the Create Schedule dialog box, which enables you to create time-based and interval schedules.

- **Edit**

  Opens the Edit Schedule dialog box, which enables you to edit the selected schedules.

- **Delete**

  Opens the Delete Schedule dialog box, which enables you to delete the selected schedules.

- **Refresh**

  Updates the information in the window.

Schedules list

- **Name**

  Specifies the name of the schedule.

- **Type**

Specifies the type of the schedule—time-based or interval-based.

Details area

The details area displays information about when a selected schedule is run.