Vault relationships

System Manager Classic

NetApp
January 13, 2022

Table of Contents

Vault relationships . . . 1
- Create a vault relationship from a destination SVM . . . 1
- Deleting vault relationships . . . 3
- Editing vault relationships . . . 3
- Initializing a vault relationship . . . 5
- Updating a vault relationship . . . 5
- Quiescing a vault relationship . . . 6
- Resuming a vault relationship . . . 6
- Aborting a Snapshot copy transfer . . . 6
- Restoring a volume in a vault relationship . . . 7
- What a SnapVault backup is . . . 8

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.

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	Select an existing schedule from the list.
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.

If you want to restore the data to…	Do this…
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