Protect data

ONTAP 9

NetApp
May 18, 2021

Table of Contents

Protect data

The topics in this section show you how to configure and manage data protection with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage data protection, see this content:

- Archive and Compliance Using SnapLock Technology Power Guide
- Cluster and SVM Peering Power Guide
- Data Protection Power Guide
- Data Protection Tape Backup and Recovery Guide
- NDMP Configuration Express Guide
- Replication between NetApp Element Software and ONTAP

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage data protection, see the content for your ONTAP release:

- Cluster and SVM Peering Express Guide
- Volume Disaster Recovery Express Guide
- Volume Disaster Recovery Preparation Express Guide
- Volume Backup Using SnapVault Express Guide
- Volume Restore Using SnapVault Express Guide
- Cluster management using System Manager 9.6 and 9.7
- Cluster management using System Manager 9.5
- Cluster management using System Manager 9.3 and 9.4
- Cluster management using System Manager 9.2 and earlier

Data protection overview

Protect your data by creating and managing Snapshot copies, mirrors, vaults, and mirror-and-vault relationships.

SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or mirror, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

A *vault* is designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a vault destination typically retains point-in-time Snapshot copies created over a much longer period.

Create custom data protection policies

You can create custom data protection policies in System Manager when the existing default protection policies are not appropriate for your needs.

Create custom protection policies on both the source and destination cluster.

Steps

1. Click Protection > Local Policy Settings.
2. Under **Protection Policies**, click →.
3. In the **Protection Policies** pane, click + Add .
4. Complete the required fields.
5. Click **Save**.
6. Repeat these steps on the other cluster.

Configure Snapshot copies

You can create Snapshot copy policies to specify the maximum number of Snapshot copies that are automatically created and how frequently they are created. The policy specifies when to create Snapshot copies, how many copies to retain, and how to name them.

This procedure creates a Snapshot copy policy on the local cluster only.

Steps

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Snapshot Policies**, click →, and then click + Add .
3. Type the policy name, select the policy scope, and under **Schedules**, click + Add to enter the schedule details.

Recover from Snapshot copies

You can recover a volume to an earlier point in time by restoring from a Snapshot copy.

This procedure restores a volume from a Snapshot copy.

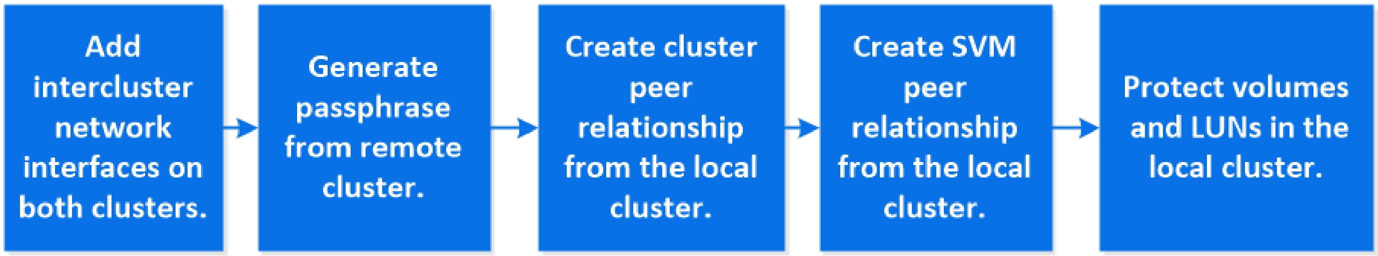
Steps

1. Click **Storage** and select a volume.
2. Under **Snapshot Copies**, click ⋮ next to the Snapshot copy you want to restore, and select **Restore**.

Prepare for mirroring and vaulting

You can protect your data by replicating it to a remote cluster for data backup and disaster recovery purposes.

Several default protection policies are available. You must have created your protection policies if you want to use custom policies.


Add intercluster network interfaces on both clusters.
Generate passphrase from remote cluster.
Create cluster peer relationship from the local cluster.
Create SVM peer relationship from the local cluster.
Protect volumes and LUNs in the local cluster.

Steps

1. In the local cluster, click **Protection > Overview**.
2. Expand **Intercluster Settings**. Click **Add Network Interfaces** and add intercluster network interfaces for the cluster.

   Repeat this step on the remote cluster.

3. In the remote cluster, click **Protection > Overview**. Click ⋮ in the Cluster Peers section and click **Generate Passphrase**.
4. Copy the generated passphrase and paste it in the local cluster.
5. In the local cluster, under Cluster Peers, click **Peer Clusters** and peer the local and remote clusters.
6. Optionally, under Storage VM Peers, click ⋮ and then **Peer Storage VMs** to peer the storage VMs.
7. Click **Protect Volumes** to protect your volumes. To protect your LUNs, click **Storage > LUNs**, select a LUN to protect, and then click 🛡 Protect.

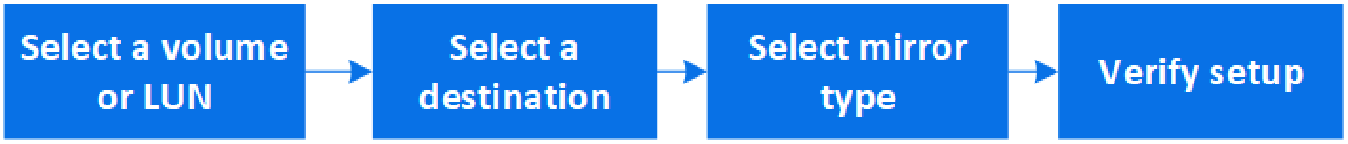
   Select the protection policy based on the type of data protection you need.

8. To verify the volumes and LUNs are successfully protected from the local cluster, click **Storage > Volumes** or **Storage > LUNs** and, expand the volume/LUN view.

Configure mirrors and vaults

Create a mirror and vault of a volume to protect data in case of a disaster and to have multiple archived versions of data to which you can roll back. Only the combined mirror-and-vault policy is supported. You cannot specify separate mirror and vault policies.

This procedure creates a mirror-and-vault policy on a remote cluster. The source cluster and destination cluster use intercluster network interfaces for exchanging data. The procedure assumes the intercluster network interfaces are created and the clusters containing the volumes are peered (paired). You can also peer storage VMs for data protection; however, if storage VMs are not peered, but permissions are enabled, storage VMs are automatically peered when the protection relationship is created.



Steps

1. Select the volume or LUN to protect: click **Storage > Volumes** or **Storage > LUNs**, and then click the desired volume or LUN name.
2. Click 🛡 Protect.

3. Select the destination cluster and storage VM.
4. The asynchronous policy is selected by default. To select a synchronous policy, click **More Options**.
5. Click **Protect**.
6. Click the **SnapMirror (Local or Remote)** tab for the selected volume or LUN to verify that protection is set up correctly.

Configure storage VM disaster recovery

You can create an storage VM disaster recovery (storage VM DR) relationship to replicate one storage VM configuration to another. In the event of a disaster at the primary site, you can quickly activate the destination storage VM.

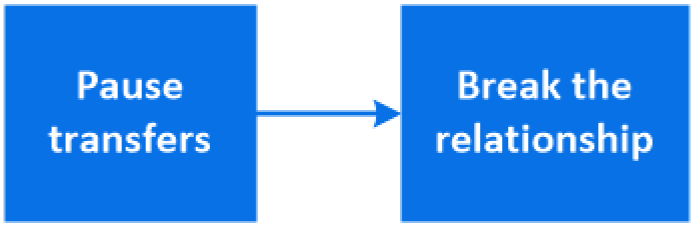
Complete this procedure from the destination. If you need to create a new protection policy, for instance, when your source storage VM has CIFS configured, you should use System Manager to create the policy and select the **Copy source storage VM configuration** option in the **Add Protection Policy** window.
For details see Create custom data protection policies.

Steps

1. On the destination cluster, click Protection > Relationships.
2. Under **Relationships**, click Protect and choose **Storage VMs (DR)**.
3. Select a protection policy. If you created a custom protection policy, select it, then choose the source cluster and storage VM you want to replicate. You can also create a new destination storage VM by entering a new storage VM name.
4. Click **Save**.

Serve data from a SnapMirror destination

To serve data from a mirror destination when a source becomes unavailable, stop scheduled transfers to the destination, and then break the SnapMirror relationship to make the destination writable.



Steps

1. Select the desired protection relationship: click **Protection > Relationships**, and then click the desired volume name.
2. Click ⋮.
3. Stop scheduled transfers : click **Pause**.
4. Make the destination writable: click **Break**.
5. Go to the main **Relationships** page to verify that the relationship state displays as "broken off".

Next steps:

When the disabled source volume is available again, you should resynchronize the relationship to copy the current data to the original source volume. This process replaces the data on the original source volume.

Resynchronize a protection relationship

When your original source volume is available again after a disaster, you can resynchronize data from the destination volume and reestablish the protection relationship.

This procedure replaces the data in the original source volume in an asynchronous relationship so that you can start serving data from the original source volume again and resume the original protection relationship.

Steps

1. Click **Protection > Relationships** and then click the broken off relationship you want to resynchronize.
2. Click ⋮ and then select **Resync**.
3. Under **Relationships**, monitor the resynchronization progress by checking the relationship state. The state changes to "Mirrored" when resynchronization is complete.

Restore a volume from an earlier Snapshot copy

When data in a volume is lost or corrupted, you can roll back your data by restoring from an earlier Snapshot copy.

This procedure replaces the current data on the source volume with data from an earlier Snapshot copy version. You should perform this task on the destination cluster.

Steps

1. Click **Protection > Relationships**, and then click the source volume name.
2. Click ⋮ and then select **Restore**.
3. Under **Source**, the source volume is selected by default. Click **Other Volume** if you want to choose a different volume.
4. Under **Destination**, choose the Snapshot copy you want to restore.
5. If your source and destination are located on different clusters, on the remote cluster, click **Protection > Relationships** to monitor the restore progress.

Restore to a new volume

Starting in System Manager 9.8, you can restore backed up data on the destination volume to a volume other than the original source.

When you restore to a different volume, you can select an existing volume, or you can create a new volume.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click ⋮ and click **Restore**.

3. Under **Relationships**, monitor the restore progress by viewing **Transfer Status** for the relationship.

Reverse Resynchronizing a Protection Relationship

Starting in System Manager 9.8, you can perform a reverse resynchronization operation to delete an existing protection relationship and reverse the functions of the source and destination volumes. Then you 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.

When you perform a reverse resynch operation, any data on the source volume that is newer than the data in the common Snapshot copy is deleted.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click ⋮ and click **Reverse Resync**.
3. Under **Relationships**, monitor the reverse resynchronization progress by viewing **Transfer Status** for the relationship.

Reactivate a source storage VM

Starting in System Manager 9.8, you can reactivate a source storage VM after a disaster. Reactivating the source storage VM stops the destination storage VM, and it reenables replication from the source to the destination.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click ⋮ and click **Reactivate Source Storage VM**.
3. Under **Relationships**, monitor the source reactivation progress by viewing **Transfer Status** for the protection relationship.

Resynchronize a destination storage VM

You can resynchronize the data and configuration details from the source SVM to the destination SVM in a broken protection relationship and reestablish the relationship.

You perform the resync operation only from the destination of the original relationship. The resync deletes any data in the destination storage VM that is newer than the data in the source storage VM.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click ⋮ and click **Resync**.
3. Under **Relationships**, monitor the resynchronization progress by viewing **Transfer Status** for the relationship.

Back up to the cloud

Starting in System Manager 9.9.1, you can use System Manager to back up your data to the cloud and to restore your data from cloud storage to a different volume. You can use either StorageGRID or ONTAP S3 as your cloud object store.

Before you use SnapMirror Cloud with System Manager, you should generate a SnapMirror Cloud API license key on the NetApp Support Site: Generate SnapMirror Cloud API license key

Add a cloud object store

Before you configure SnapMirror Cloud backups, you should add a StorageGRID or ONTAP S3 cloud object store.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Click + Add .

Back up using the default policy

You can quickly configure a SnapMirror Cloud backup for an existing volume using the default cloud protection policy, DailyBackup.

Steps

1. Click **Protection > Overview** and select **Back Up Volumes to Cloud**.
2. If this is your first time backing up to the cloud, enter your SnapMirror Cloud API license key in the license field as indicated.
3. Click **Authenticate and Continue**.
4. Select a source volume.
5. Select a cloud object store.
6. Click **Save**.

Create a custom cloud backup policy

If you do not want to use the default DailyBackup cloud policy for your SnapMirror Cloud backups, you can create your own policy.

Steps

1. Click **Protection > Overview > Local Policy Settings** and select **Protection Policies**.
2. Click **Add** and enter the new policy details.
3. In the **Policy Type** section, select **Back up to Cloud** to indicate that you are creating a cloud policy.
4. Click **Save**.

Create a backup from the Volumes page

You can use the System Manager **Volumes** page to when you want to select and create cloud backups for multiple volumes at one time or when you want to use a custom protection policy.

Steps

1. Click **Storage > Volumes**.
2. Select the volumes you want to back up to the cloud, and click **Protect**.
3. In the **Protect Volume** window, click **More Options**.
4. Select a policy.

   You can select the default policy, DailyBackup, or a custom cloud policy you created.

5. Select a cloud object store.
6. Click **Save**.

Restore from the cloud

You can use System Manager to restore backed up data from cloud storage to a different volume on the source cluster.

Steps

1. Click **Storage > Volumes** and select the volume you want to restore.
2. Click ⋮ next to the source volume and select **Restore**.
3. Under **Source**, select a storage VM and then enter the name of the volume to which you want the data restored.
4. Under **Destination**, select the Snapshot copy you want to restore.
5. Click **Save**.

Delete a SnapMirror Cloud relationship

You can use System Manager to delete a cloud relationship.

Steps

1. Click **Storage > Volumes** and select the volume you want to delete.
2. Click ⋮ next to the source volume and select **Delete**.
3. Select **Delete the cloud object store endpoint (optional)** if you want to delete the cloud object store endpoint.
4. Click **Delete**.

Remove a cloud object store

You can use System Manager to remove a cloud object store if it is not part of a cloud backup relationship. When a cloud object store is part of a cloud backup relationship, it cannot be deleted.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Select the object store you want to delete, click ⋮ and select **Delete**.

Copyright Information

Trademark Information