Data protection with System Manager

ONTAP 9

NetApp
February 28, 2022

Table of Contents

Data protection with System Manager

Data protection overview with System Manager

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

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see this topic:

- Managing data protection

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.

Beginning with ONTAP 9.10.1, you can create data protection relationships between S3 buckets using S3 SnapMirror. Destination buckets can be on local or remote ONTAP systems, or on non-ONTAP systems such as StorageGRID and AWS. For more information, see S3 SnapMirror overview.

Create custom data protection policies

You can create custom data protection policies with 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.

Calculate reclaimable space before deleting Snapshot copies

Beginning with ONTAP 9.10.1, you can use System Manager to select Snapshot copies you want to delete and calculate the reclaimable space before you delete them.

Steps

1. Click **Storage > Volumes**.
2. Select the volume from which you want to delete Snapshot copies.
3. Click **Snapshot Copies**.
4. Select one or more Snapshot copies.
5. Click **Calculate Reclaimable Space**.

Enable or disable client access to Snapshot copy directory

Beginning with ONTAP 9.10.1, you can use System Manager to enable or disable client systems to access to a Snapshot copy directory on a volume. Enabling access makes the Snapshot copy directory visible to clients and allows Windows clients to map a drive to the Snapshot copies directory to view and access its contents.

You can enable or disable access to a volume's Snapshot copy directory by editing the volume settings or by editing the volume's share settings.

Enable or disable client access to Snapshot copy directory by editing a volume

The Snapshot copy directory on a volume is accessible to clients by default.

Steps

1. Click **Storage > Volumes**.
2. Select the volume containing the Snapshot copies directory you want to either show or hide.
3. Click ⋮ and select **Edit**.
4. In the **Snapshot Copies (Local) Settings** section, select or deselect **Show the Snapshot copies directory to clients**.
5. Click **Save**.

Enable or disable client access to Snapshot copy directory by editing a share

The Snapshot copy directory on a volume is accessible to clients by default.

Steps

1. Click **Storage > Shares**.
2. Select the volume containing the Snapshot copies directory you want to either show or hide.
3. Click ⋮ and select **Edit**.
4. In the **Share Properties** section, select or deselect **Allow clients to access Snapshot copies directory**.
5. Click **Save**.

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.

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.

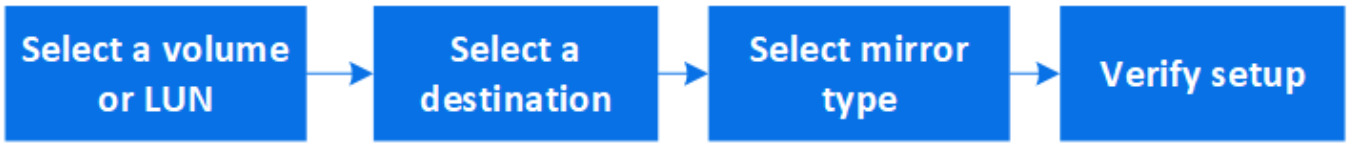
Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume disaster recovery preparation overview
The ONTAP command line interface	Create a cluster peer relationship (ONTAP 9.3 and later)

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.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume backup using SnapVault overview
The ONTAP command line interface	Create a replication relationship

Configure storage VM disaster recovery

Using System Manager, 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.

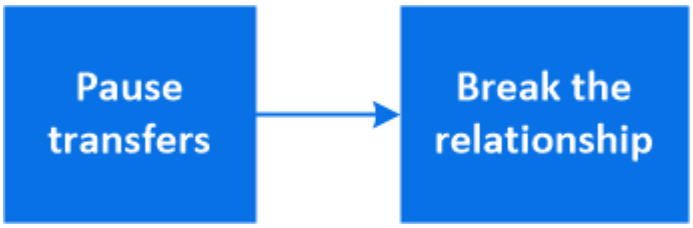
Complete this procedure from the destination. If you need to create a new protection policy, for instance, when your source storage VM has SMB configured, you should use System Manager to create the policy and select the **Copy source storage VM configuration** option in the **Add Protection Policy**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

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume disaster recovery overview
The ONTAP command line interface	Activate the destination 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 volume other than the source.
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.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume restore using SnapVault overview
The ONTAP command line interface	Restore the contents of a volume from a SnapMirror destination

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**.

Restore to a new volume

Beginning with ONTAP 9.8, you can use System Manager to 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

Beginning with ONTAP 9.8, you can use System Manager to 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

Beginning with ONTAP 9.8, you can use System Manager to 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

Beginning with ONTAP 9.8, you can use System Manager to resynchronize the data and configuration details from the source storage VM to the destination storage VM 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 data to the cloud using SnapMirror

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

Before using the SnapMirror Cloud feature, 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 need to 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**.
2. Select the **Back Up to Cloud** tab.
3. Click ⋮ next to the source volume you want to restore, and select **Restore**.
4. Under **Source**, select a storage VM and then enter the name of the volume to which you want the data restored.
5. Under **Destination**, select the Snapshot copy you want to restore.
6. 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**.

Back up data using Cloud Backup

Beginning with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using Cloud Backup.

ⓘ Cloud Backup supports FlexVol read-write volumes and data-protection (DP) volumes. FlexGroup volumes and SnapLock volumes are not supported.

Before you begin

You should perform the following procedures to establish an account in Cloud Manager. For the service account, you need to create the role as "Account Admin". (Other service account roles do not have the required privileges needed to establish a connection from System Manager.)

1. Create an account in Cloud Manager.
2. Create a connector in Cloud Manager with one of the following cloud providers:
   - Microsoft Azure
   - Amazon Web Services (AWS)

- Google Cloud Platform (GCP)
- StorageGrid (ONTAP 9.10.1)

> Beginning with ONTAP 9.10.1, you can select StorageGrid as a cloud backup provider, but only if Cloud Manager is deployed on premises. The Cloud Manager connector must be installed on premises and available through the Cloud Manager software-as-a-service (SaaS) application.

3. Subscribe to Cloud Backup Service in Cloud Manager (requires the appropriate license).
4. Generate an access key and a secret key using Cloud Manager.

Register the cluster with Cloud Manager

You can register the cluster with Cloud Manager by using either Cloud Manager or System Manager.

Steps

1. In System Manager, go to **Protection Overview**.
2. Under **Cloud Backup Service**, provide the following details:
   - Client ID
   - Client secret key
3. Select **Register and Continue**.

Enable Cloud Backup

After the cluster is registered with Cloud Manager, you need to enable the Cloud Backup and initiate the first backup to the cloud.

Steps

1. In System Manager, click **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Enter the **Client ID** and **Client Secret**.

> Beginning with ONTAP 9.10.1, you can learn about the cost of using the cloud by clicking **Learn more about the cost of using the cloud**.

3. Click **Connect and Enable Cloud Backup Service**.
4. On the **Enable Cloud Backup Service** page, provide the following details, depending on the provider you selected.

For this cloud provider…	Enter the following data…
Azure	• Azure Subscription ID • Region • Resource group name (existing or new)

AWS	• AWS Account ID • Access key • Secret key • Region
Google Cloud Project (GCP)	• Google Cloud Project name • Google Cloud Access key • Google Cloud Secret key • Region
StorageGrid (ONTAP 9.10.1 and later, and only for on-premises deployment of Cloud Manager)	• Server • SG Access Key • SG Secret Key

5. Select a **Protection policy**:
   - **Existing policy**: Choose an existing policy.
   - **New Policy**: Specify a name and set up a transfer schedule.

     Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.

     If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

     If you enable archiving for Azure or AWS, specify the following:

     - The number of days after which the volume is archived.
     - The number of backups to retain in the archive. Specify “0” (zero) to archive up to the latest backup.
     - For AWS, select the archive storage class.
6. Select the volumes you want to back up.
7. Select **Save**.

Edit the protection policy used for Cloud Backup

You can change which protection policy is used with Cloud Backup.

Steps

1. In System Manager, click **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Click ⋮, then **Edit**.
3. Select a **Protection policy**:
   - **Existing policy**: Choose an existing policy.

◦ **New Policy**: Specify a name and set up a transfer schedule.

> Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.

> If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

If you enable archiving for Azure or AWS, specify the following:

- The number of days after which the volume is archived.
- The number of backups to retain in the archive. Specify “0” (zero) to archive up to the latest backup.
- For AWS, select the archive storage class.

4. Select **Save**.

Protect new volumes or LUNs on the cloud

When you create a new volume or LUN, you can establish a SnapMirror protection relationship that enables backing up to the cloud for the volume or LUN.

Before you begin

- You should have a SnapMirror license.
- Intercluster LIFs should be configured.
- NTP should be configured.
- Cluster must be running ONTAP 9.9.1.

About this task

You cannot protect new volumes or LUNs on the cloud for the following cluster configurations:

- The cluster cannot be in a MetroCluster environment.
- SVM-DR is not supported.
- FlexGroups cannot be backed up using Cloud Backup.

Steps

1. When provisioning a volume or LUN, on the **Protection** page in System Manager, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
2. Select the Cloud Backup policy type.
3. If the Cloud Backup is not enabled, select **Enable Cloud Backup Service**.

Protect existing volumes or LUNs on the cloud

You can establish a SnapMirror protection relationship for existing volumes and LUNs.

Steps

1. Select an existing volume or LUN, and click **Protect**.
2. On the **Protect Volumes** page, specify **Backup using Cloud Backup Service** for the protection policy.

3. Click **Protect**.
4. On the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
5. Select **Enable Cloud Backup Service**.

Restore data from backup files

You can perform backup management operations, such as restoring data, updating relationships, and deleting relationships, only when using the Cloud Manager interface. Refer to Restoring data from backup files for more information.