Replicate ONTAP data

Cloud Manager

NetApp
October 26, 2021

Table of Contents

Replicate ONTAP data

Learn about the Replication service

NetApp SnapMirror replicates data at high speeds over LAN or WAN, so you get high data availability and fast data replication in both virtual and traditional environments. When you replicate data to NetApp storage systems and continually update the secondary data, your data is kept current and remains available whenever you need it. No external replication servers are required.

Features

- Replicate data between ONTAP storage systems to support backup and disaster recovery to the cloud or between clouds.
- Ensure the reliability of your DR environment with high availability.
- Efficient block-level replication between ONTAP storage is fast and efficient, with granular recovery points for both DR and backup.

Cost

NetApp doesn't charge you for using the Replication service, but you'll need to check your cloud provider for applicable data ingress and egress charges.

Supported working environments

Cloud Manager enables data replication between the following types of working environments.

Source working environment	Supported target working environments
Cloud Volumes ONTAP	• Amazon FSx for ONTAP • Cloud Volumes ONTAP • On-prem ONTAP cluster
On-prem ONTAP cluster	• Amazon FSx for ONTAP • Cloud Volumes ONTAP • On-prem ONTAP cluster

How data replication works

Cloud Manager simplifies data replication between volumes on separate ONTAP systems using SnapMirror and SnapVault technologies. You simply need to identify the source volume and the destination volume, and then choose a replication policy and schedule.

For Cloud Volumes ONTAP, Cloud Manager purchases the required disks, configures relationships, applies the replication policy, and then initiates the baseline transfer between volumes.

The baseline transfer includes a full copy of the source data. Subsequent transfers contain differential copies of the source data.

Supported data protection configurations

Cloud Manager supports simple, fanout, and cascade data protection configurations:

- In a simple configuration, replication occurs from volume A to volume B.
- In a fanout configuration, replication occurs from volume A to multiple destinations.
- In a cascade configuration, replication occurs from volume A to volume B and from volume B to volume C.

Replicating data between systems

You can replicate data between ONTAP working environments by choosing a one-time data replication for data transfer, or a recurring schedule for disaster recovery or long-term retention. For example, you can set up data replication from an on-prem ONTAP system to Cloud Volumes ONTAP for disaster recovery.

Data replication requirements

Before you can replicate data, you should confirm that specific requirements are met for Cloud Volumes ONTAP, on-prem ONTAP clusters, or Amazon FSx for ONTAP.

Working environments

If you haven't done so already, you need to create the working environments for the source and target in the data replication relationship.

- Create an Amazon FSx for ONTAP working environment
- Launch Cloud Volumes ONTAP in AWS
- Launch Cloud Volumes ONTAP in Azure
- Launch Cloud Volumes ONTAP in GCP
- Add existing Cloud Volumes ONTAP systems
- Discover ONTAP clusters

Version requirements

You should verify that the source and destination volumes are running compatible ONTAP versions before replicating data. For details, see the Data Protection Power Guide.

Requirements specific to Cloud Volumes ONTAP

- The instance's security group must include the required inbound and outbound rules: specifically, rules for ICMP and ports 11104 and 11105.

  These rules are included in the predefined security group.

- To replicate data between two Cloud Volumes ONTAP systems in different subnets, the subnets must be routed together (this is the default setting).
- To replicate data between two Cloud Volumes ONTAP systems in different cloud providers, you must have a VPN connection between the virtual networks.

Requirements specific to ONTAP clusters

- An active SnapMirror license must be installed.
- If the cluster is on your premises, you should have a connection from your corporate network to your virtual network in AWS, Azure, or GCP. This is typically a VPN connection.
- ONTAP clusters must meet additional subnet, port, firewall, and cluster requirements.

  For details, see the Cluster and SVM Peering Express Guide.

Requirements specific to Amazon FSx for ONTAP

- An Amazon FSx for ONTAP working environment must be the target in the data replication relationship.

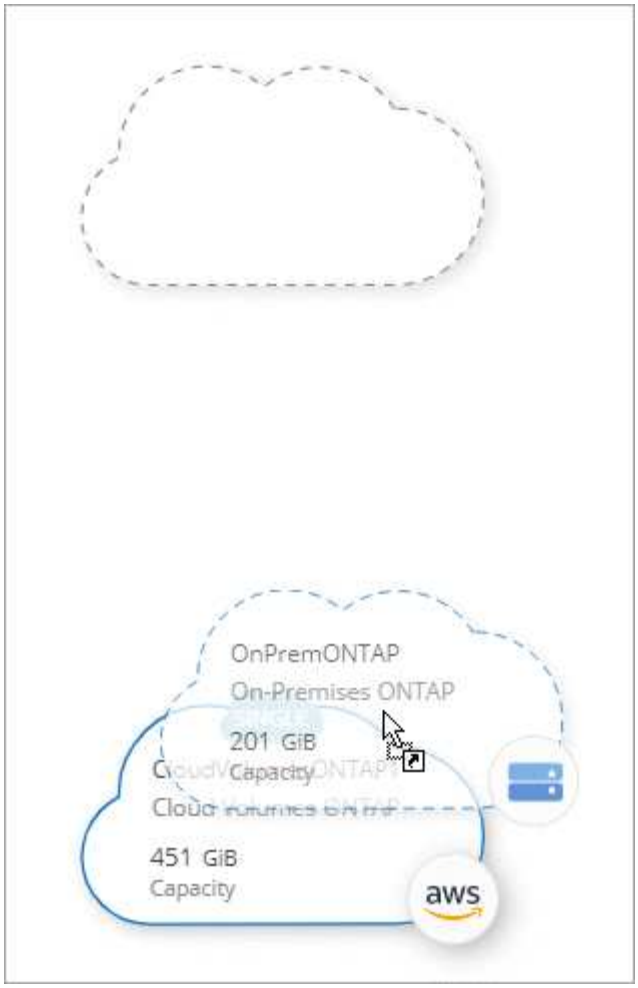
  The source can be Cloud Volumes ONTAP or an on-prem ONTAP cluster.
- If Cloud Volumes ONTAP is the source, ensure connectivity between VPCs by enabling VPC peering or by using a Transit Gateway.
- If an on-prem ONTAP cluster is the source, ensure connectivity between your on-premises network and the AWS VPC by using a Direct Connect or VPN connection.

Setting up data replication between systems

You can replicate data by choosing a one-time data replication, which can help you move data to and from the cloud, or a recurring schedule, which can help with disaster recovery or long-term retention.

Steps

1. On the Canvas page, select the working environment that contains the source volume, and then drag it to the working environment to which you want to replicate the volume.



2. **Source and Destination Peering Setup**: If this page appears, select all of the intercluster LIFs for the cluster peer relationship.

   The intercluster network should be configured so that cluster peers have *pair-wise full-mesh connectivity*, which means that each pair of clusters in a cluster peer relationship has connectivity among all of their intercluster LIFs.

   These pages appear if an ONTAP cluster that has multiple LIFs is the source or destination.

3. **Source Volume Selection**: Select the volume that you want to replicate.
4. **Destination Disk Type and Tiering**: If the target is a Cloud Volumes ONTAP system, select the destination disk type and choose whether you want to enable data tiering.
5. **Destination Volume Name**: Specify the destination volume name and choose the destination aggregate.

   If the destination is an ONTAP cluster, you must also specify the destination storage VM.

6. **Max Transfer Rate**: Specify the maximum rate (in megabytes per second) at which data can be transferred.

   You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your internet performance.

7. **Replication Policy**: Choose a default policy or click **Additional Policies**, and then select one of the advanced policies.

For help, learn about replication policies.

If you choose a custom backup (SnapVault) policy, the labels associated with the policy must match the labels of the Snapshot copies on the source volume. For more information, learn how backup policies work.

8. **Schedule**: Choose a one-time copy or a recurring schedule.

   Several default schedules are available. If you want a different schedule, you must create a new schedule on the *destination* cluster using System Manager.

9. **Review**: Review your selections and click **Go**.

Result

Cloud Manager starts the data replication process. You can view details about the volume relationship in the Replication service.

Managing data replication schedules and relationships

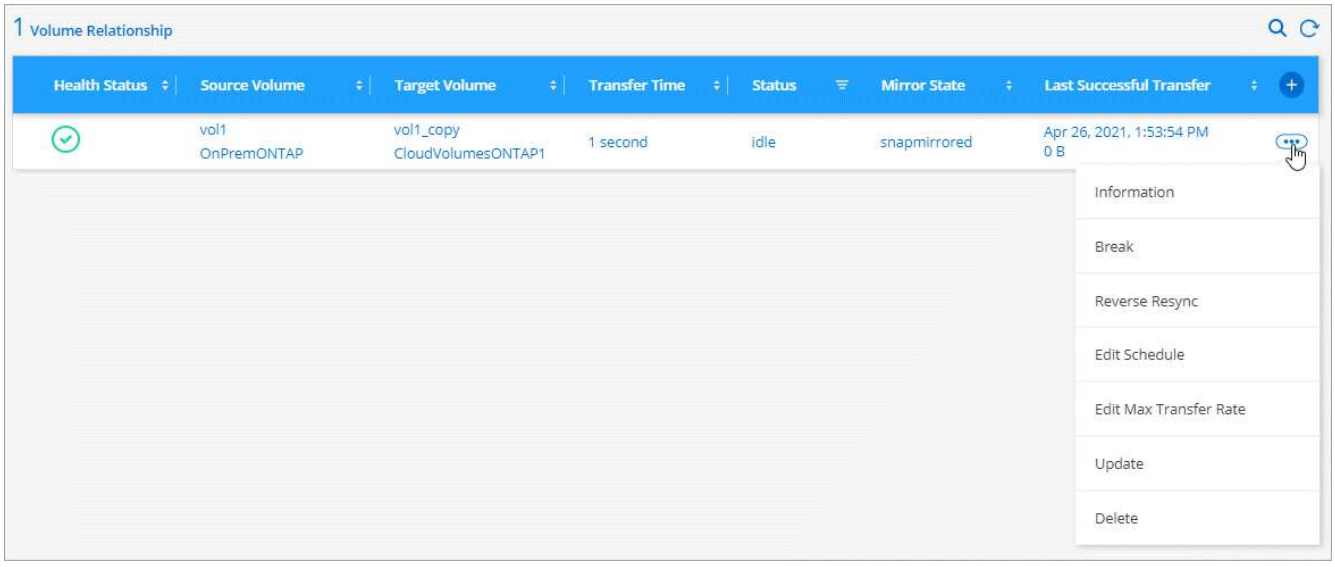
After you set up data replication between two systems, you can manage the data replication schedule and relationship from Cloud Manager.

Steps

1. Click **Replication**.
2. Review the status of the data replication relationships to verify that they are healthy.

   If the Status of a relationship is idle and the Mirror State is uninitialized, you must initialize the relationship from the destination system for the data replication to occur according to the defined schedule. You can initialize the relationship by using System Manager or the command-line interface (CLI). These states can appear when the destination system fails and then comes back online.

3. Click the action menu for a volume relationship and choose one of the available actions.



The following table describes the available actions:

Action	Description
Information	Shows you details about the volume relationship: transfer information, last transfer information, details about the volume, and information about the protection policy assigned to the relationship.
Break	Breaks the relationship between the source and destination volumes, and activates the destination volume for data access. This option is typically used when the source volume cannot serve data due to events such as data corruption, accidental deletion, or an offline state. For information about configuring a destination volume for data access and reactivating a source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide.
Resync	Reestablishes a broken relationship between volumes and resumes data replication according to the defined schedule. When you resynchronize the volumes, the contents on the destination volume are overwritten by the contents on the source volume. To perform a reverse resync, which resynchronizes the data from the destination volume to the source volume, see the ONTAP 9 Volume Disaster Recovery Express Guide.
Reverse Resync	Reverses the roles of the source and destination volumes. Contents from the original source volume are overwritten by contents of the destination volume. This is helpful when you want to reactivate a source volume that went offline. Any data written to the original source volume between the last data replication and the time that the source volume was disabled is not preserved.
Edit Schedule	Enables you to choose a different schedule for data replication.
Edit Max Transfer Rate	Enables you to edit the maximum rate (in kilobytes per second) at which data can be transferred.
Update	Starts an incremental transfer to update the destination volume.
Delete	Deletes the data protection relationship between the source and destination volumes, which means that data replication no longer occurs between the volumes. This action does not activate the destination volume for data access. This action also deletes the cluster peer relationship and the storage VM (SVM) peer relationship, if there are no other data protection relationships between the systems.

Result

After you select an action, Cloud Manager updates the relationship or schedule.

Learn about replication policies

You might need help choosing a replication policy when you set up data replication in Cloud Manager. A replication policy defines how the storage system replicates data from a source volume to a destination volume.

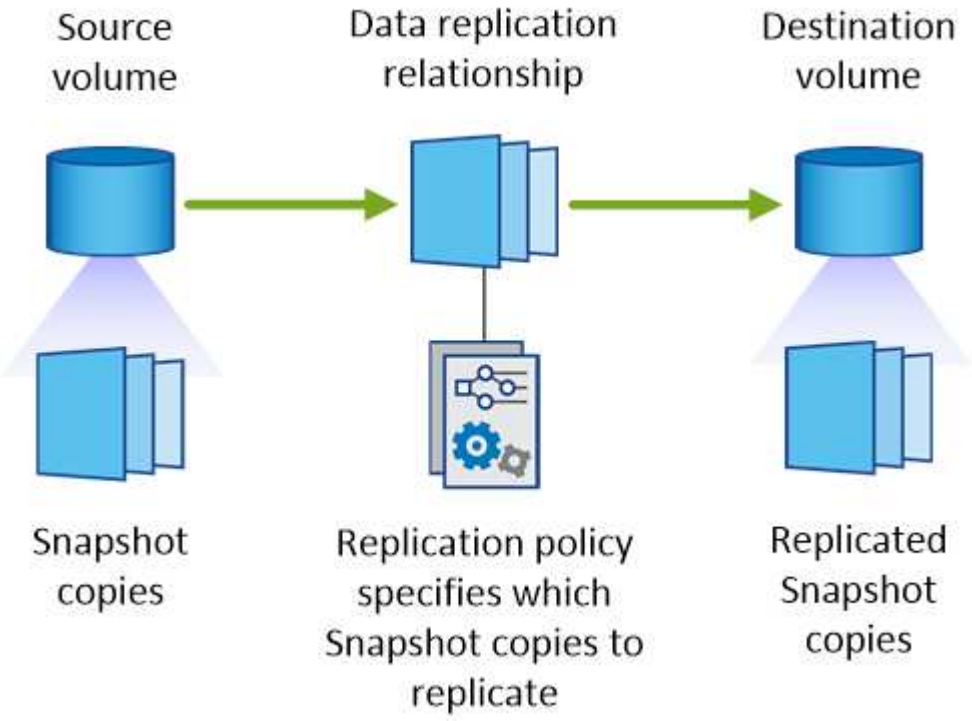
What replication policies do

The ONTAP operating system automatically creates backups called Snapshot copies. A Snapshot copy is a read-only image of a volume that captures the state of the file system at a point in time.

When you replicate data between systems, you replicate Snapshot copies from a source volume to a destination volume. A replication policy specifies which Snapshot copies to replicate from the source volume to the destination volume.

Replication policies are also referred to as *protection* policies because they are powered by SnapMirror and SnapVault technologies, which provide disaster recovery protection and disk-to-disk backup and recovery.

The following image shows the relationship between Snapshot copies and replication policies:



Types of replication policies

There are three types of replication policies:

- A *Mirror* policy replicates newly created Snapshot copies to a destination volume.

  You can use these Snapshot copies to protect the source volume in preparation for disaster recovery or for one-time data replication. You can activate the destination volume for data access at any time.

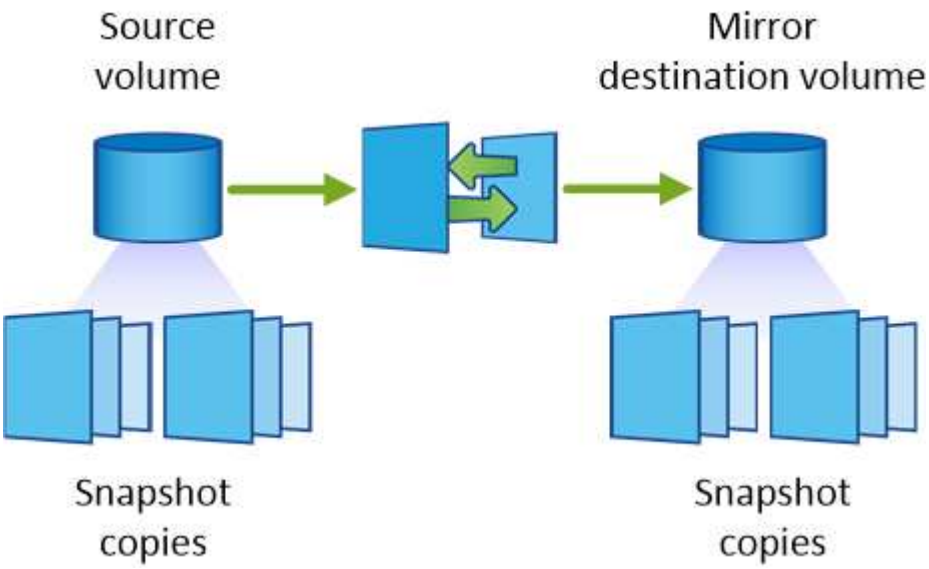
- A *Backup* policy replicates specific Snapshot copies to a destination volume and typically retains them for a longer period of time than you would on the source volume.

  You can restore data from these Snapshot copies when data is corrupted or lost, and retain them for standards compliance and other governance-related purposes.

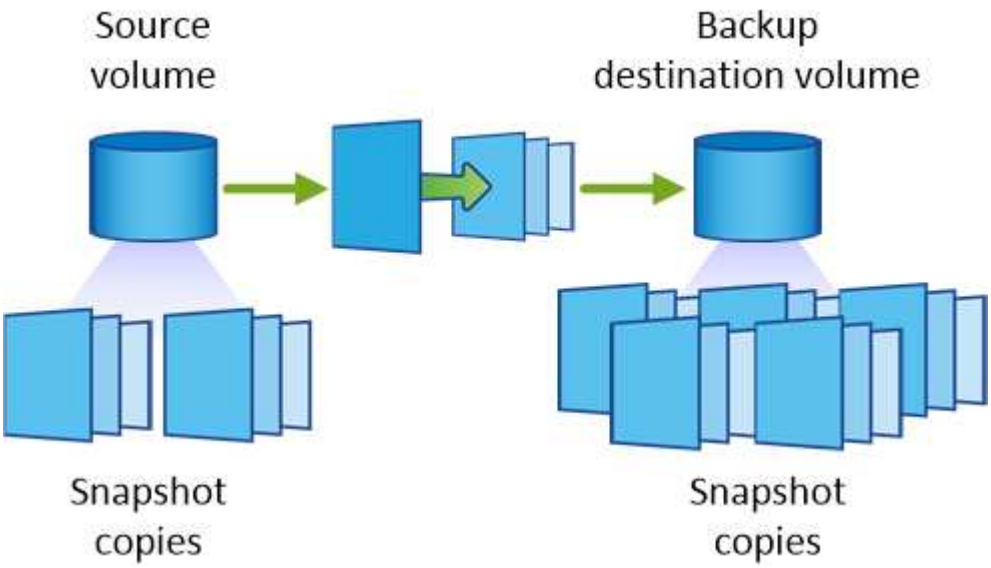
- A *Mirror and Backup* policy provides both disaster recovery and long-term retention.

Each system includes a default Mirror and Backup policy, which works well for many situations. If you find that you need custom policies, you can create your own using System Manager.

The following images show the difference between the Mirror and Backup policies. A Mirror policy mirrors the Snapshot copies available on the source volume.



A Backup policy typically retains Snapshot copies longer than they are retained on the source volume:



How Backup policies work

Unlike Mirror policies, Backup (SnapVault) policies replicate specific Snapshot copies to a destination volume. It is important to understand how Backup policies work if you want to use your own policies instead of the default policies.

Understanding the relationship between Snapshot copy labels and Backup policies

A Snapshot policy defines how the system creates Snapshot copies of volumes. The policy specifies when to create the Snapshot copies, how many copies to retain, and how to label them. For example, a system might

create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, and label them "daily".

A Backup policy includes rules that specify which labeled Snapshot copies to replicate to a destination volume and how many copies to retain. The labels defined in a Backup policy must match one or more labels defined in a Snapshot policy. Otherwise, the system cannot replicate any Snapshot copies.

For example, a Backup policy that includes the labels "daily" and "weekly" results in replication of Snapshot copies that include only those labels. No other Snapshot copies are replicated, as shown in the following image:

Default policies and custom policies

The default Snapshot policy creates hourly, daily, and weekly Snapshot copies, retaining six hourly, two daily, and two weekly Snapshot copies.

You can easily use a default Backup policy with the default Snapshot policy. The default Backup policies replicate daily and weekly Snapshot copies, retaining seven daily and 52 weekly Snapshot copies.

If you create custom policies, the labels defined by those policies must match. You can create custom policies using System Manager.