Replication

ONTAP 9

NetApp
February 22, 2022

Table of Contents

Replication . . . 1
- Snapshot copies . . . 1
- SnapMirror disaster recovery and data transfer . . . 2
- SnapMirror Cloud backups to object storage . . . 3
- SnapVault archiving . . . 4
- Cloud backup and support for traditional backups . . . 5
- MetroCluster continuous availability . . . 6

Replication

Snapshot copies

Traditionally, ONTAP replication technologies served the need for disaster recovery (DR) and data archiving. With the advent of cloud services, ONTAP replication has been adapted to data transfer between endpoints in the NetApp data fabric. The foundation for all these uses is ONTAP Snapshot technology.

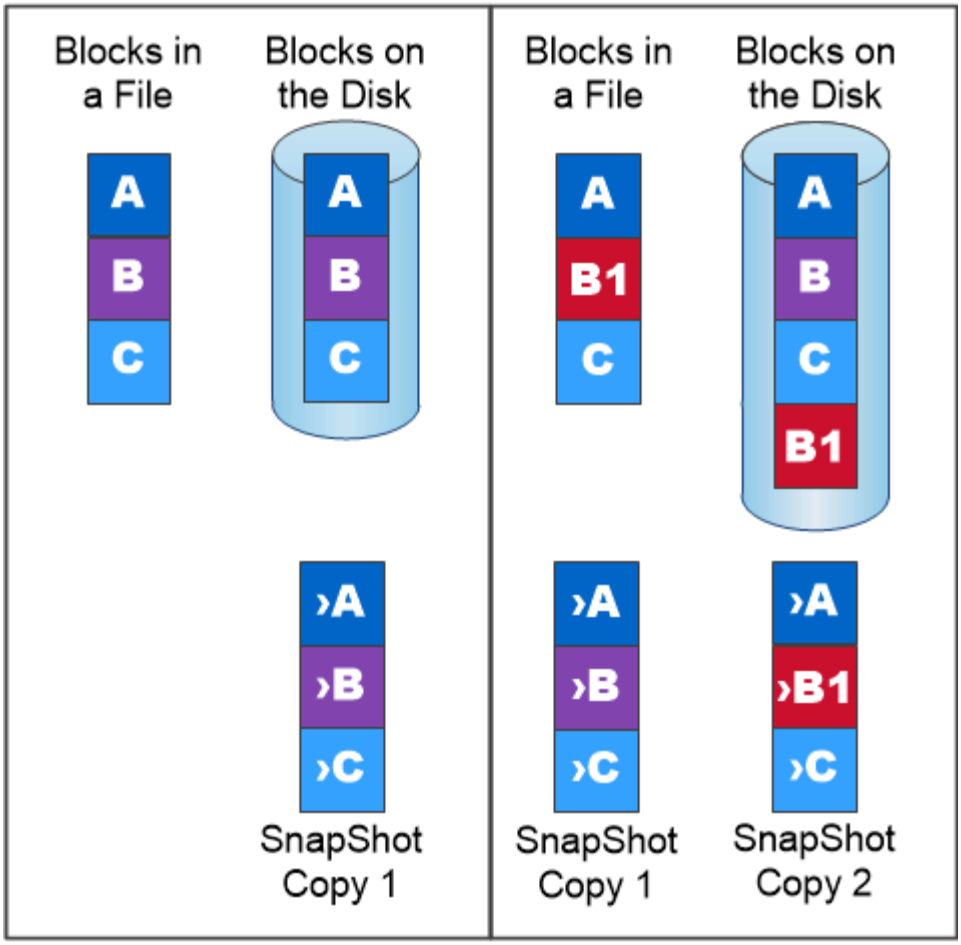
A *Snapshot copy* is a read-only, point-in-time image of a volume. The image consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the last Snapshot copy was made.

Snapshot copies owe their efficiency to ONTAP's core storage virtualization technology, its *Write Anywhere File Layout (WAFL).* Like a database, WAFL uses metadata to point to actual data blocks on disk. But, unlike a database, WAFL does not overwrite existing blocks. It writes updated data to a new block and changes the metadata.

It's because ONTAP references metadata when it creates a Snapshot copy, rather than copying data blocks, that Snapshot copies are so efficient. Doing so eliminates the "seek time" that other systems incur in locating the blocks to copy, as well as the cost of making the copy itself.

You can use a Snapshot copy to recover individual files or LUNs, or to restore the entire contents of a volume. ONTAP compares pointer information in the Snapshot copy with data on disk to reconstruct the missing or damaged object, without downtime or a significant performance cost.

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, how to name them, and how to label them for replication. For example, a system might create one Snapshot copy every day at 12:10 a.m., retain the two most recent copies, name them "daily" (appended with a timestamp), and label them "daily" for replication.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

SnapMirror disaster recovery and data transfer

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.

Data is mirrored at the volume level. The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship.* The clusters in which the volumes reside and the SVMs that serve data from the volumes must be *peered.* A peer relationship enables clusters and SVMs to exchange data securely.

You can also create a data protection relationship between SVMs. In this type of relationship, all or part of the SVM's configuration, from NFS exports and SMB shares to RBAC, is replicated, as well as the data in the volumes the SVM owns.

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.

The first time you invoke SnapMirror, it performs a *baseline transfer* from the source volume to the destination volume. The baseline transfer typically involves the following steps:

- Make a Snapshot copy of the source volume.
- Transfer the Snapshot copy and all the data blocks it references to the destination volume.
- Transfer the remaining, less recent Snapshot copies on the source volume to the destination volume for use in case the “active” mirror is corrupted.

Once a baseline transfer is complete, SnapMirror transfers only new Snapshot copies to the mirror. Updates are asynchronous, following the schedule you configure. Retention mirrors the Snapshot policy on the source. You can activate the destination volume with minimal disruption in case of a disaster at the primary site, and reactivate the source volume when service is restored.

Because SnapMirror transfers only Snapshot copies after the baseline is created, replication is fast and nondisruptive. As the failover use case implies, the controllers on the secondary system should be equivalent or nearly equivalent to the controllers on the primary system to serve data efficiently from mirrored storage.

A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

Using SnapMirror for data transfer

You can also use SnapMirror to replicate data between endpoints in the NetApp data fabric. You can choose between one-time replication or recurring replication when you create the SnapMirror policy.

2021-12-16, Jira IE-412

SnapMirror Cloud backups to object storage

SnapMirror Cloud is a backup and recovery technology designed for ONTAP users who want to transition their data protection workflows to the cloud. Organizations moving away from legacy backup-to-tape architectures can use object storage as an alternative repository for long-term data retention and archiving. SnapMirror Cloud provides ONTAP-

to-object storage replication as part of an incremental forever backup strategy.

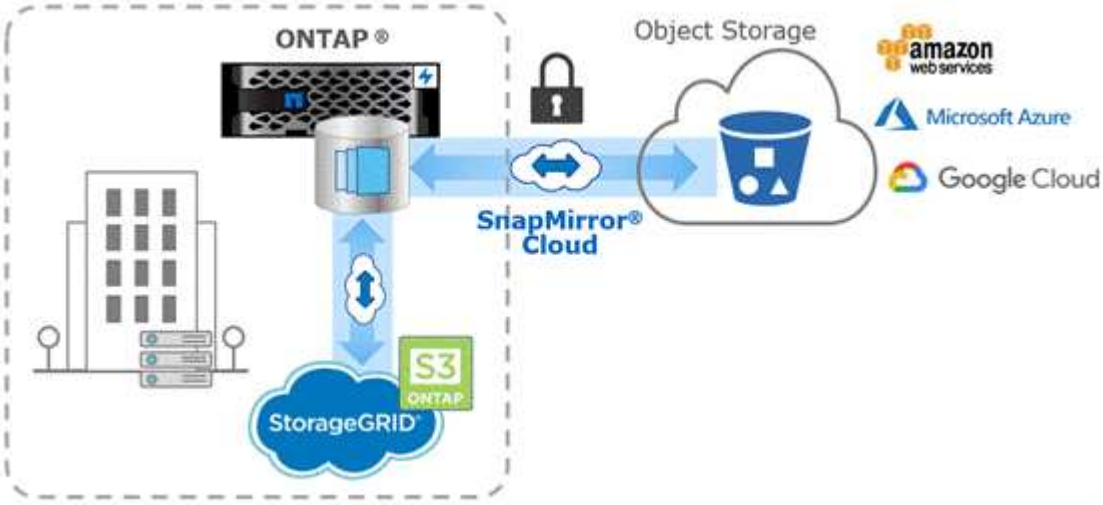
SnapMirror Cloud was introduced in ONTAP 9.8 as an extension to the family of SnapMirror replication technologies. While SnapMirror is frequently used for ONTAP-to-ONTAP backups, SnapMirror Cloud uses the same replication engine to transfer Snapshot copies for ONTAP to S3-compliant object storage backups.

Targeted for backup use cases, SnapMirror Cloud supports both long-term retention and archives workflows. As with SnapMirror, the initial SnapMirror Cloud backup performs a baseline transfer of a volume. For subsequent backups, SnapMirror Cloud generates a snapshot copy of the source volume and transfers the snapshot copy with only the changed data blocks to an object storage target.

SnapMirror Cloud relationships can be configured between ONTAP systems and select on-premises and public cloud object storage targets - including AWS S3, Google Cloud Storage Platform, and Microsoft Azure Blob Storage. Additional on-premises object storage targets include StoragGRID and ONTAP S3.

SnapMirror Cloud replication is a licensed ONTAP feature and requires an approved application to orchestrate data protection workflows. Several orchestration options are available for managing SnapMirror Cloud backups:

- Multiple 3rd party backup partners who offer support for SnapMirror Cloud replication. Participating vendors are available on the NetApp blog.
- Cloud Manager and Cloud Backup for a NetApp-native solution for ONTAP environments
- APIs for developing custom software for data protection workflows or leveraging automation tools



SnapVault archiving

The SnapMirror license is used to support both SnapVault relationships for backup, and SnapMirror relationships for disaster recovery. SnapVault licenses were deprecated, and SnapMirror licenses can now be used to configure vault, mirror, and mirror-and-vault relationships. SnapMirror replication is used for ONTAP-to-ONTAP replication of Snapshot copies, supporting both backup and disaster recovery use cases.

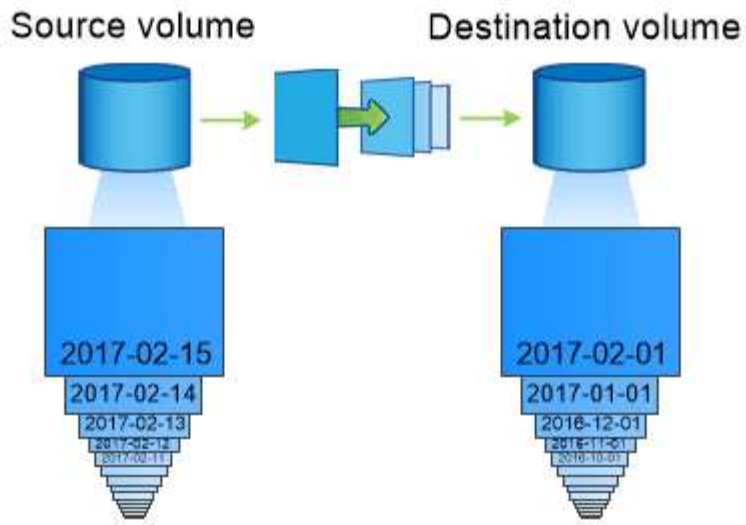
SnapVault is archiving technology, designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a SnapVault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

You might want to keep monthly Snapshot copies of your data over a 20-year span, for example, to comply with government accounting regulations for your business. Since there is no requirement to serve data from vault storage, you can use slower, less expensive disks on the destination system.

As with SnapMirror, SnapVault performs a baseline transfer the first time you invoke it. It makes a Snapshot copy of the source volume, then transfers the copy and the data blocks it references to the destination volume. Unlike SnapMirror, SnapVault does not include older Snapshot copies in the baseline.

Updates are asynchronous, following the schedule you configure. The rules you define in the policy for the relationship identify which new Snapshot copies to include in updates and how many copies to retain. The labels defined in the policy ("monthly," for example) must match one or more labels defined in the Snapshot policy on the source. Otherwise, replication fails.

SnapMirror and SnapVault share the same command infrastructure. You specify which method you want to use when you create a policy. Both methods require peered clusters and peered SVMs.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Cloud backup and support for traditional backups

In addition to SnapMirror and SnapVault data protection relationships, which were previously disk-to-disk only, there are now several backup solutions that offer a less expensive alternative for long-term data retention.

Numerous third-party data protection applications offer traditional backup for ONTAP-managed data. Veeam, Veritas, and Commvault, among others, all offer integrated backup for ONTAP systems.

Beginning with ONTAP 9.8, SnapMirror Cloud provides asynchronous replication of Snapshot copies from ONTAP instances to object storage endpoints. SnapMirror Cloud replication requires a licensed application for orchestration and management of data protection workflows. SnapMirror Cloud relationships are supported from ONTAP systems to select on-premises and public cloud object storage targets — including AWS S3, Google Cloud Storage Platform, or Microsoft Azure Blob Storage — which provides enhanced efficiency with

vendor backup software. Contact your NetApp representative for a list of supported certified applications and object storage vendors.

If you are interested in cloud-native data protection, Cloud Manager can be used to configure SnapMirror or SnapVault relationships between on-premises volumes and Cloud Volumes ONTAP instances in the public cloud.

Cloud Manager also provides backups of Cloud Volumes ONTAP instances using a Software as a Service (SaaS) model. Users can back up their Cloud Volumes ONTAP instances to S3 and S3-compliant public cloud object storage using Cloud Backup found on NetApp Cloud Central.

Cloud Volumes ONTAP and Cloud Manager documentation resources

NetApp Cloud Central

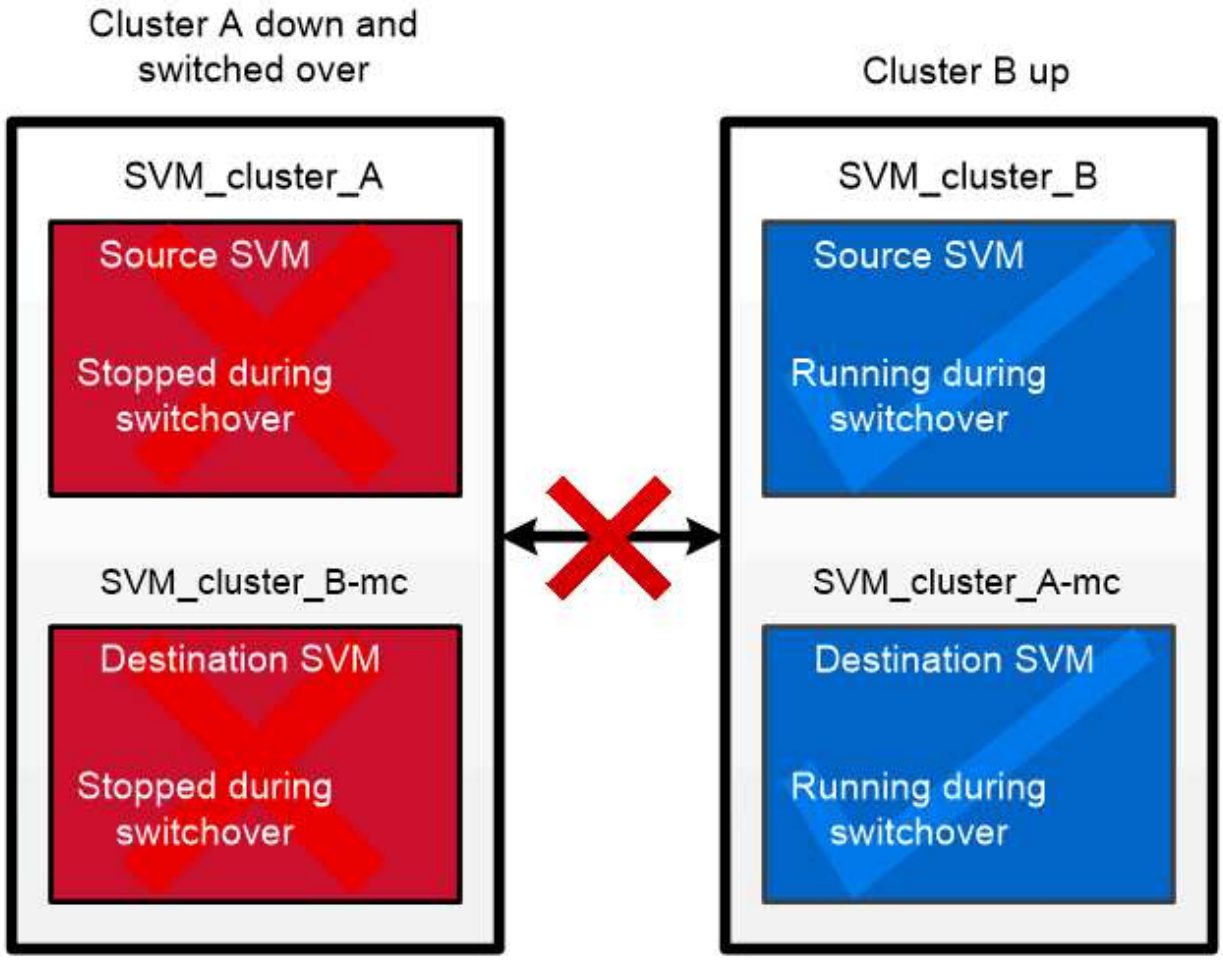
MetroCluster continuous availability

MetroCluster configurations protect data by implementing two physically separate, mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. In the event of a disaster at one site, an administrator can activate the mirrored SVM and begin serving data from the surviving site.

- *Fabric-attached MetroCluster* configurations support metropolitan-wide clusters.
- *Stretch MetroCluster* configurations support campus-wide clusters.

Clusters must be peered in either case.

MetroCluster uses an ONTAP feature called *SyncMirror* to synchronously mirror aggregate data for each cluster in copies, or *plexes*, in the other cluster's storage. If a switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

Using SyncMirror in non-MetroCluster implementations You can optionally use SyncMirror in a non-MetroCluster implementation to protect against data loss if more disks fail than the RAID type protects against, or if there is a loss of connectivity to RAID group disks. The feature is available for HA pairs only.

Aggregate data is mirrored in plexes stored on different disk shelves. If one of the shelves becomes unavailable, the unaffected plex continues to serve data while you fix the cause of the failure.

Keep in mind that an aggregate mirrored using SyncMirror requires twice as much storage as an unmirrored aggregate. Each plex requires as many disks as the plex it mirrors. You would need 2,880 GB of disk space, for example, to mirror a 1,440 GB aggregate, 1,440 GB for each plex.

SyncMirror is also available for FlexArray Virtualization implementations.