SnapMirror volume replication

ONTAP 9

NetApp
February 02, 2026

Table of Contents

SnapMirror volume replication

Learn about SnapMirror volume replication

Learn about ONTAP SnapMirror asynchronous disaster recovery

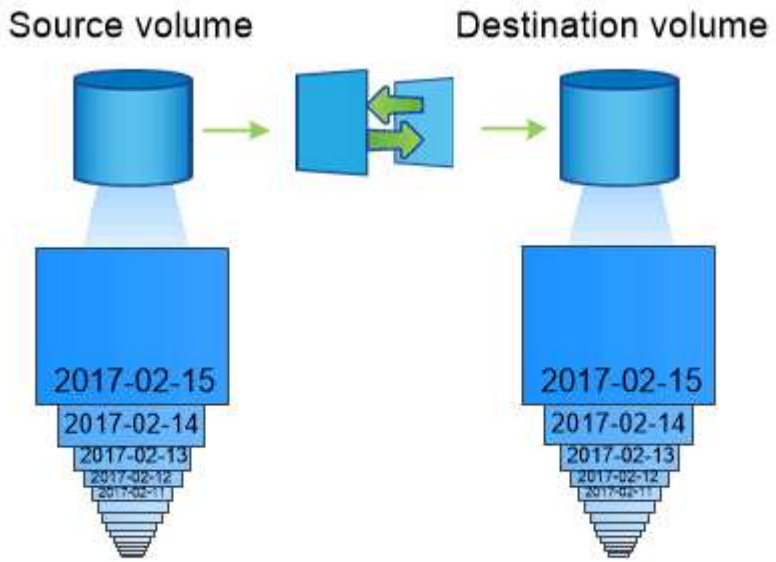
SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or *mirror,* of your working data in secondary storage from which you can continue to serve data in the event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

If the primary site is still available to serve data, you can simply transfer any needed data back to it, and not serve clients from the mirror at all. 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.

Data protection relationships

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.

This figure illustrates SnapMirror data protection relationships:



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

Scope of data protection relationships

You can create a data protection relationship directly between volumes or between the SVMs that own the volumes. In an *SVM data protection relationship,* all or part of the SVM configuration, from NFS exports and SMB shares to RBAC, is replicated, as well as the data in the volumes that the SVM owns.

You can also use SnapMirror for special data protection applications:

- A *load-sharing mirror* copy of the SVM root volume ensures that data remains accessible in the event of a node outage or failover.
- A data protection relationship between *SnapLock volumes* lets you replicate WORM files to secondary storage.

  Archive and compliance using SnapLock technology

- Beginning with ONTAP 9.13.1, you can use SnapMirror asynchronous to protect consistency groups. Beginning with ONTAP 9.14.1, you can use SnapMirror asynchronous to replicate volume-granular snapshots to the destination cluster using the consistency group relationship. For more information, see Configure SnapMirror asynchronous protection.

How SnapMirror data protection relationships are initialized

The first time you invoke SnapMirror, it performs a *baseline transfer* from the source volume to the destination volume. The *SnapMirror policy* for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default SnapMirror policy `MirrorAllSnapshots` involves the following steps:

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

How SnapMirror data protection relationships are updated

Updates are asynchronous, following the schedule you configure. Retention mirrors the snapshot policy on the source.

At each update under the `MirrorAllSnapshots` policy, SnapMirror creates a snapshot of the source volume and transfers that snapshot and any snapshots that have been made since the last update. In the following output from the `snapmirror policy show` command for the `MirrorAllSnapshots` policy, note the following:

- `Create Snapshot` is “true”, indicating that `MirrorAllSnapshots` creates a snapshot when SnapMirror updates the relationship.
- `MirrorAllSnapshots` has rules “sm_created” and “all_source_snapshots”, indicating that both the snapshot created by SnapMirror and any snapshots that have been made since the last update are transferred when SnapMirror updates the relationship.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

MirrorLatest policy

The preconfigured `MirrorLatest` policy works exactly the same way as `MirrorAllSnapshots`, except that only the snapshot created by SnapMirror is transferred at initialization and update.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

Related information

- snapmirror policy show

Learn about ONTAP SnapMirror synchronous disaster recovery

Beginning with ONTAP 9.5, SnapMirror synchronous (SM-S) technology is supported on all FAS and AFF platforms that have at least 16 GB of memory and on all ONTAP Select

platforms. SnapMirror synchronous technology is a per-node, licensed feature that provides synchronous data replication at the volume level.

This functionality addresses the regulatory and national mandates for synchronous replication in financial, healthcare, and other regulated industries where zero data loss is required.

SnapMirror synchronous operations allowed

The limit on the number of SnapMirror synchronous replication operations per HA pair depends on the controller model.

The following table lists the number of SnapMirror synchronous operations that are allowed per HA pair according to platform type and ONTAP release.

Platform	ONTAP 9.14.1 through ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	Releases earlier than ONTAP 9.9.1
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

Supported features

The following table indicates the features supported with SnapMirror synchronous and the ONTAP releases in which support is available.

Feature	Release first supported	Additional information
Antivirus on the primary volume of the SnapMirror synchronous relationship	ONTAP 9.6	
Application-created snapshot replication	ONTAP 9.7	If a snapshot is tagged with the appropriate label at the time of the `snapshot create` operation, using the CLI or the ONTAP API, SnapMirror synchronous replicates the snapshots, both user created or those created with external scripts, after quiescing the applications. Scheduled snapshots created using a snapshot policy are not replicated. For more information about replicating application-created snapshots, see the NetApp Knowledge Base: How to replicate application created snapshots with SnapMirror synchronous.
Clone auto delete	ONTAP 9.6	

FabricPool aggregates with tiering policy of None, Snapshot, or Auto are supported with SnapMirror synchronous source and destination.	ONTAP 9.5	The destination volume in a FabricPool aggregate cannot be set to All tiering policy.
FC	ONTAP 9.5	Over all networks for which latency does not exceed 10ms
FC-NVMe	ONTAP 9.7	
File clones	ONTAP 9.7	
FPolicy on the primary volume of the SnapMirror synchronous relationship	ONTAP 9.6	
Hard and soft quotas on the primary volume of the SnapMirror synchronous relationship	ONTAP 9.6	The quota rules are not replicated to the destination; therefore, the quota database is not replicated to the destination.
Intra-cluster synchronous relationships	ONTAP 9.14.1	High availability is provided when source and destination volumes are placed on different HA pairs. If the entire cluster goes down, access to volumes will not be possible until the cluster is recovered. Intra-cluster SnapMirror synchronous relationships will contribute to the overall limit of simultaneous relationships per HA pair.
iSCSI	ONTAP 9.5	
LUN clones and NVMe namespace clones	ONTAP 9.7	
LUN clones backed by application-created snapshots	ONTAP 9.7	
Mixed protocol access (NFS v3 and SMB)	ONTAP 9.6	
NDMP/NDMP restore	ONTAP 9.13.1	Both the source and destination cluster must be running ONTAP 9.13.1 or later to use NDMP with SnapMirror Synchronous. For more information, see Transfer data using ndmp copy.
Non-disruptive SnapMirror synchronous operations (NDO) on AFF/ASA platforms, only.	ONTAP 9.12.1	Support for non-disruptive operations enables you to perform many common maintenance tasks without scheduling down time. Operations supported include takeover and giveback, and volume move, provided that a single node is surviving among each of the two clusters.
NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/TCP	9.10.1	
Removal of high metadata operation frequency limitation	ONTAP 9.6	

Security for sensitive data in-transit using TLS 1.2 encryption	ONTAP 9.6	
Single file and partial file restore	ONTAP 9.13.1	
SMB 2.0 or later	ONTAP 9.6	
SnapMirror synchronous mirror-mirror cascade	ONTAP 9.6	The relationship from the destination volume of the SnapMirror synchronous relationship must be an SnapMirror asynchronous relationship.
SVM disaster recovery	ONTAP 9.6	* A SnapMirror synchronous source can also be a SVM disaster recovery source, for example, a fan-out configuration with SnapMirror synchronous as one leg and SVM disaster recovery as the other. * A SnapMirror synchronous source cannot be an SVM disaster recovery destination because SnapMirror synchronous does not support cascading a data protection source. You must release the synchronous relationship before performing an SVM disaster recovery flip resync in the destination cluster. * A SnapMirror synchronous destination cannot be an SVM disaster recovery source because SVM disaster recovery does not support replication of DP volumes. A flip resync of the synchronous source would result in the SVM disaster recovery excluding the DP volume in the destination cluster.
Tape-based restore to the source volume	ONTAP 9.13.1	
Timestamp parity between source and destination volumes for NAS	ONTAP 9.6	If you have upgraded from ONTAP 9.5 to ONTAP 9.6, the timestamp is replicated only for any new and modified files in the source volume. The timestamp of existing files in the source volume is not synchronized.

Unsupported features

The following features are not supported with SnapMirror synchronous relationships:

- Autonomous Ransomware Protection
- Consistency groups
- DP_Optimized (DPO) systems
- FlexGroup volumes
- FlexCache volumes
- Global throttling
- In a fan-out configuration, only one relationship can be a SnapMirror synchronous relationship; all the other relationships from the source volume must be SnapMirror asynchronous relationships.
- LUN move

- MetroCluster configurations
- Mixed SAN and NVMe access
  LUNs and NVMe namespaces are not supported on the same volume or SVM.
- SnapCenter
- SnapLock volumes
- Tamperproof snapshots
- Tape backup or restore using dump and SMTape on the destination volume
- Throughput floor (QoS Min) for source volumes
- Volume SnapRestore
- VVol

Modes of operation

SnapMirror synchronous has two modes of operation based on the type of the SnapMirror policy used:

- **Sync mode**
  In Sync mode, application I/O operations are sent in parallel to the primary and secondary storage systems. If the write to the secondary storage is not completed for any reason, the application is allowed to continue writing to the primary storage. When the error condition is corrected, SnapMirror synchronous technology automatically resynchronizes with the secondary storage and resumes replicating from primary storage to secondary storage in synchronous mode.
  In Sync mode, RPO=0 and RTO is very low until a secondary replication failure occurs at which time RPO and RTO become indeterminate, but equal the time to repair the issue that caused secondary replication to fail and for the resync to complete.
- **StrictSync mode**
  SnapMirror synchronous can optionally operate in StrictSync mode. If the write to the secondary storage is not completed for any reason, the application I/O fails, thereby ensuring that the primary and secondary storage are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to the `InSync` status. If the primary storage fails, application I/O can be resumed on the secondary storage, after failover, with no loss of data.
  In StrictSync mode RPO is always zero, and RTO is very low.

Relationship status

The status of a SnapMirror synchronous relationship is always in the `InSync` status during normal operation. If the SnapMirror transfer fails for any reason, the destination is not in sync with the source and can go to the `OutofSync` status.

For SnapMirror synchronous relationships, the system automatically checks the relationship status (`InSync` or `OutofSync`) at a fixed interval. If the relationship status is `OutofSync`, ONTAP automatically triggers the auto resync process to bring back the relationship to the `InSync` status. Auto resync is triggered only if the transfer fails due to any operation, such as unplanned storage failover at source or destination or a network outage. User-initiated operations such as `snapmirror quiesce` and `snapmirror break` do not trigger auto resync.

If the relationship status becomes `OutofSync` for a SnapMirror synchronous relationship in the StrictSync mode, all I/O operations to the primary volume are stopped. The `OutofSync` state for SnapMirror synchronous relationship in the Sync mode is not disruptive to the primary and I/O operations are allowed on the primary volume.

Related information

- NetApp Technical Report 4733: SnapMirror synchronous configuration and best practices
- snapmirror break
- snapmirror quiesce

Default ONTAP data protection policies

ONTAP includes several default protection policies you can use for your data protection relationships. The policy you use depends on the protection relationship type.

If the default policies don't meet your data protection relationships needs, you can create a custom policy.

List of default protection policies and descriptions

Default protection policies and their associated policy types are described below.

Name	Description	Policy type
Asynchronous	A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots with an hourly transfer schedule.	Asynchronous
AutomatedFailOver	Policy for SnapMirror synchronous with zero RTO guarantee where client I/O will not be disrupted on replication failure.	Synchronous
AutomatedFailOverDuplex	Policy for SnapMirror synchronous with zero RTO guarantee and bi-directional sync replication.	Synchronous
CloudBackupDefault	Vault policy with daily rule.	Asynchronous
Continuous	Policy for S3 bucket mirroring.	Continuous
DailyBackup	Vault policy with a daily rule and a daily transfer schedule.	Asynchronous
DPDefault	SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system.	Asynchronous
MirrorAllSnapshots	SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system.	Asynchronous
MirrorAllSnapshotsDiscardNetwork	SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system excluding the network configurations.	Asynchronous
MirrorAndVault	A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots.	Asynchronous
MirrorAndVaultDiscardNetwork	A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots excluding the network configurations.	Asynchronous

Name	Description	Policy type
MirrorLatest	SnapMirror asynchronous policy for mirroring the latest active file system.	Asynchronous
SnapCenterSync	Policy for SnapMirror synchronous for SnapCenter with Application Created Snapshot configuration.	Synchronous
StrictSync	Policy for SnapMirror synchronous where client access will be disrupted on replication failure.	Synchronous
Synchronous	Policy for SnapMirror synchronous where client access will not be disrupted on replication failure.	Synchronous
Unified7year	Unified SnapMirror policy with 7-year retention.	Asynchronous
XDPDefault	Vault policy with daily and weekly rules.	Asynchronous

Learn about workloads supported by ONTAP StrictSync and Sync policies

StrictSync and Sync policies support all LUN-based applications with FC, iSCSI, and FC-NVMe protocols, as well as NFSv3 and NFSv4 protocols for enterprise applications such as databases, VMWare, quota, SMB, and so on. Beginning with ONTAP 9.6, SnapMirror synchronous can be used for enterprise file services such as electronic design automation (EDA), home directories, and software build workloads.

In ONTAP 9.5, for a Sync policy, you need to consider a few important aspects while selecting the NFSv3 or NFSv4 workloads. The amount of data read or write operations by workloads is not a consideration, as Sync policy can handle high read or write IO workloads. In ONTAP 9.5, workloads that have excessive file creation, directory creation, file permission changes, or directory permission changes may not be suitable (these are referred to as high-metadata workloads). A typical example of a high-metadata workload is a DevOps workload in which you create multiple test files, run automation, and delete the files. Another example is parallel build workload that generate multiple temporary files during compilation. The impact of a high rate of write metadata activity is that it can cause synchronization between mirrors to temporarily break which stalls the read and write IOs from the client.

Beginning with ONTAP 9.6, these limitations are removed and SnapMirror synchronous can be used for enterprise file services workloads that include multiuser environments, such as home directories and software build workloads.

Related information

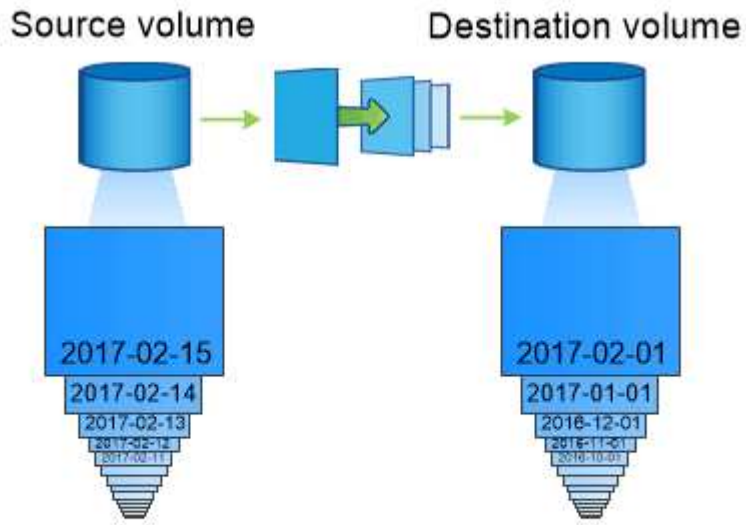
SnapMirror synchronous Configuration and Best Practices

Learn about vault archiving using ONTAP SnapMirror technology

SnapMirror vault policies replace SnapVault technology in ONTAP 9.3 and later. You use a SnapMirror vault policy for disk-to-disk snapshot replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the snapshots currently in the source volume, a vault destination typically retains point-in-time snapshots created over a much longer period.

You might want to keep monthly snapshots 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.

The figure below illustrates SnapMirror vault data protection relationships.



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.

How vault data protection relationships are initialized

The SnapMirror policy for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default vault policy `XDPDefault` makes a snapshot of the source volume, then transfers that copy and the data blocks it references to the destination volume. Unlike SnapMirror relationships, a vault backup does not include older snapshots in the baseline.

How vault data protection relationships are updated

Updates are asynchronous, following the schedule you configure. The rules you define in the policy for the relationship identify which new snapshots 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.

At each update under the `XDPDefault` policy, SnapMirror transfers snapshots that have been made since the last update, provided they have labels matching the labels defined in the policy rules. In the following output from the `snapmirror policy show` command for the `XDPDefault` policy, note the following:

- `Create Snapshot` is "false", indicating that `XDPDefault` does not create a snapshot when SnapMirror updates the relationship.
- `XDPDefault` has rules "daily" and "weekly", indicating that all snapshots with matching labels on the source are transferred when SnapMirror updates the relationship.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                    Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
            Create Snapshot: false
                    Comment: Default policy for XDP relationships with
daily and weekly
                             rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                             ----------------     ----  -------- ----
-------- ------
                             daily                   7  false       0 -
-
                             weekly                 52  false       0 -
-
```

Related information

- snapmirror policy show

Learn about ONTAP SnapMirror unified replication

SnapMirror *unified replication* allows you to configure disaster recovery and archiving on the same destination volume. When unified replication is appropriate, it offers benefits in reducing the amount of secondary storage you need, limiting the number of baseline transfers, and decreasing network traffic.

How unified data protection relationships are initialized

As with SnapMirror, unified data protection performs a baseline transfer the first time you invoke it. The SnapMirror policy for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default unified data protection policy `MirrorAndVault` makes a snapshot of the source volume, then transfers that copy and the data blocks it references to the destination volume. Like vault archiving, unified data protection does not include older snapshots in the baseline.

How unified data protection relationships are updated

At each update under the `MirrorAndVault` policy, SnapMirror creates a snapshot of the source volume and transfers that snapshot and any snapshots that have been made since the last update, provided they have labels matching the labels defined in the snapshot policy rules. In the following output from the `snapmirror policy show` command for the `MirrorAndVault` policy, note the following:

- `Create Snapshot` is “true”, indicating that `MirrorAndVault` creates a snapshot when SnapMirror updates the relationship.
- `MirrorAndVault` has rules “sm_created”, “daily”, and “weekly”, indicating that both the snapshot created by SnapMirror and the snapshots with matching labels on the source are transferred when SnapMirror updates the relationship.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Unified7year policy

The preconfigured `Unified7year` policy works exactly the same way as `MirrorAndVault`, except that a fourth rule transfers monthly snapshots and retains them for seven years.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
                              monthly                84  false       0 -
-
```

Protect against possible data corruption

Unified replication limits the contents of the baseline transfer to the snapshot created by SnapMirror at initialization. At each update, SnapMirror creates another snapshot of the source and transfers that snapshot and any new snapshots that have labels matching the labels defined in the snapshot policy rules.

You can protect against the possibility that an updated snapshot is corrupted by creating a copy of the last transferred snapshot on the destination. This “local copy” is retained regardless of the retention rules on the source, so that even if the snapshot originally transferred by SnapMirror is no longer available on the source, a copy of it will be available on the destination.

When to use unified data replication

You need to weigh the benefit of maintaining a full mirror against the advantages that unified replication offers in reducing the amount of secondary storage, limiting the number of baseline transfers, and decreasing network traffic.

The key factor in determining the appropriateness of unified replication is the rate of change of the active file system. A traditional mirror might be better suited to a volume holding hourly snapshots of database transaction logs, for example.

Related information

- snapmirror policy show

When an ONTAP data protection destination volume grows automatically

During a data protection mirror transfer, the destination volume grows automatically in size if the source volume has grown, provided there is available space in the aggregate that contains the volume.

This behavior occurs irrespective of any automatic growth setting on the destination. You cannot limit the volume’s growth or prevent ONTAP from growing it.

By default, data protection volumes are set to the `grow_shrink` autosize mode, which enables the volume to grow or shrink in response to the amount of used space. The max-autosize for data protection volumes is equal to the maximum FlexVol size and is platform dependent. For example:

- FAS8200, default DP volume max-autosize = 100TB

For more information, see NetApp Hardware Universe.

Learn about ONTAP data protection fan-out and cascade deployments

You can use a *fan-out* deployment to extend data protection to multiple secondary systems. You can use a *cascade* deployment to extend data protection to tertiary systems.

Both fan-out and cascade deployments support any combination of SnapMirror DR, SnapVault, or unified replication. Beginning with ONTAP 9.5, SnapMirror synchronous relationships support fan-out deployments with one or more SnapMirror asynchronous relationships. Only one relationship in the fan-out configuration can be a SnapMirror synchronous relationship, all the other relationships from the source volume must be SnapMirror asynchronous relationships. SnapMirror synchronous relationships also support cascade deployments (beginning with ONTAP 9.6); however, the relationship from the destination volume of the SnapMirror synchronous relationship must be a SnapMirror asynchronous relationship. SnapMirror active sync (supported beginning with ONTAP 9.13.1) also supports fan-out configurations.

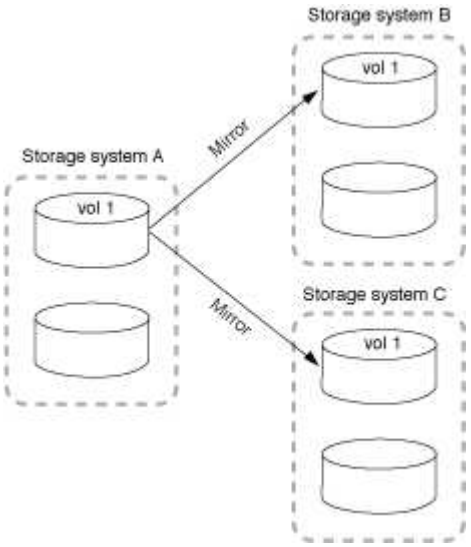
ⓘ You can use a *fan-in* deployment to create data protection relationships between multiple primary systems and a single secondary system. Each relationship must use a different volume on the secondary system.

ⓘ You should be aware that volumes that are part of a fan-out or cascade configuration can take longer to
resynchronize. It is not uncommon to see the SnapMirror relationship reporting
the status "preparing" for an extended time period.

How fan-out deployments work

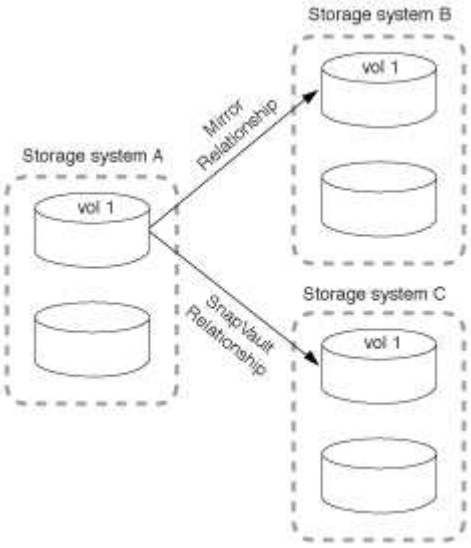
SnapMirror supports *multiple-mirrors* and *mirror-vault* fan-out deployments.

A multiple-mirrors fan-out deployment consists of a source volume that has a mirror relationship to multiple secondary volumes.

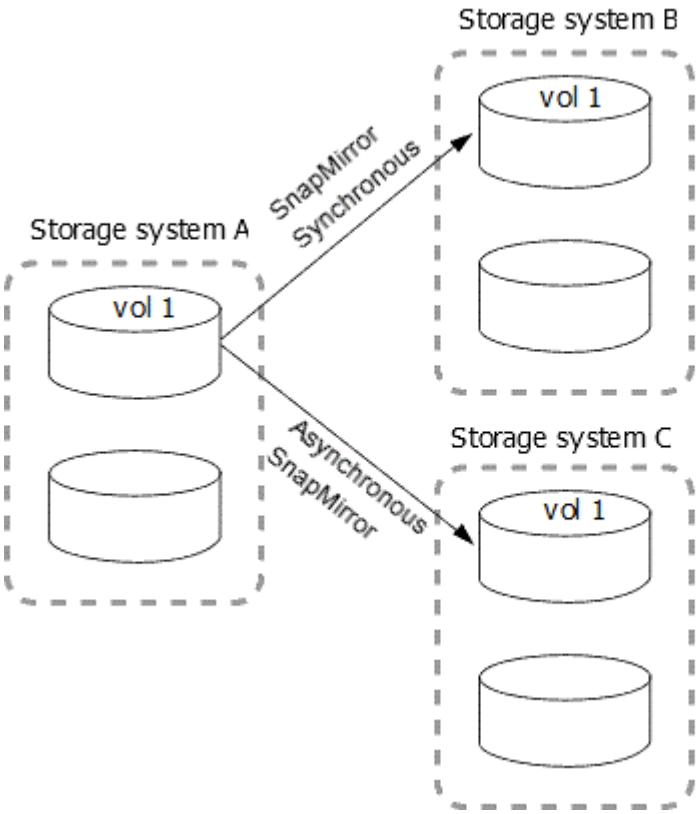


A mirror-vault fan-out deployment consists of a source volume that has a mirror relationship to a secondary

volume and a SnapVault relationship to a different secondary volume.



Beginning with ONTAP 9.5, you can have fan-out deployments with SnapMirror synchronous relationships; however, only one relationship in the fan-out configuration can be a SnapMirror synchronous relationship, all the other relationships from the source volume must be SnapMirror asynchronous relationships.



How cascade deployments work

SnapMirror supports *mirror-mirror*, *mirror-vault*, *vault-mirror*, and *vault-vault* cascade deployments.

A mirror-mirror cascade deployment consists of a chain of relationships in which a source volume is mirrored to a secondary volume, and the secondary volume is mirrored to a tertiary volume. If the secondary volume becomes unavailable, you can synchronize the relationship between the primary and tertiary volumes without

performing a new baseline transfer.

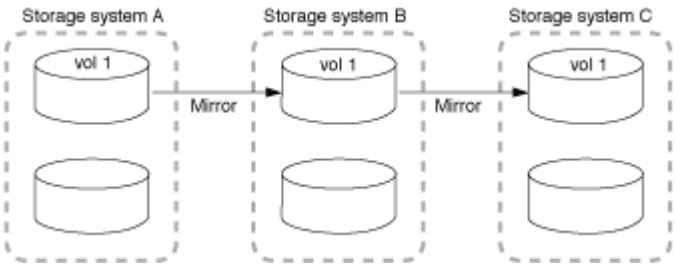
In a relationship of cascaded volumes, long-term retention snapshots are supported only on the final SnapMirror destination volume of the cascade in all versions of ONTAP 9. Enabling long-term retention snapshots on any middle volume in the cascade results in missed backups and snapshots. If you have an unsupported configuration in which long-term retention snapshots have been enabled on any middle volume of a cascade, contact technical support and reference the NetApp Knowledge Base: Cascading a volume with Long-Term Retention (LTR) snapshots enabled is not supported for assistance.

The following ONTAP versions do not allow you to enable long-term retention snapshots on any volume in a cascade except the final SnapMirror destination volume.

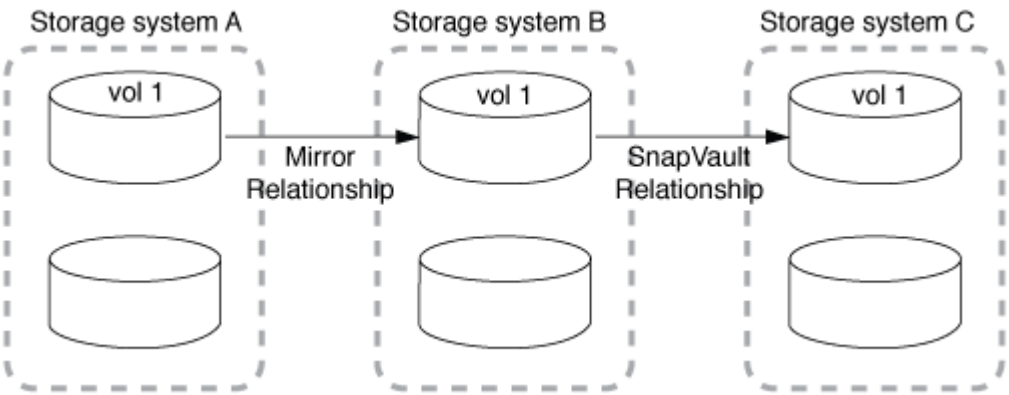
- 9.15.1 and later
- 9.14.1P2 and P4 through P14
- 9.13.1P9 through P17
- 9.12.1 P12 through P19
- 9.11.1P15 through P20
- 9.10.1P18 through P20
- 9.9.1P20

Learn more about long-term retention snapshots.

Beginning with ONTAP 9.6, SnapMirror synchronous relationships are supported in a mirror-mirror cascade deployment. Only the primary and secondary volumes can be in a SnapMirror synchronous relationship. The relationship between the secondary volumes and tertiary volumes must be asynchronous.



A mirror-vault cascade deployment consists of a chain of relationships in which a source volume is mirrored to a secondary volume, and the secondary volume is vaulted to a tertiary volume.



Vault-mirror and vault-vault cascade deployments are also supported:

- A vault-mirror cascade deployment consists of a chain of relationships in which a source volume is vaulted to a secondary volume, and the secondary volume is mirrored to a tertiary volume.
- A vault-vault cascade deployment consists of a chain of relationships in which a source volume is vaulted to a secondary volume, and the secondary volume is vaulted to a tertiary volume.

Related information

- Resume protection in a fan-out configuration with SnapMirror active sync

Learn about ONTAP SnapMirror licensing

Beginning with ONTAP 9.3, licensing has been simplified for replicating between ONTAP instances. In ONTAP 9 releases, the SnapMirror license supports both vault and mirror relationships. You can use a SnapMirror license to support ONTAP replication for both backup and disaster recovery use cases.

Prior to the ONTAP 9.3 release, a separate SnapVault license was needed to configure *vault* relationships between ONTAP instances, where the DP instance could retain a higher number of snapshots to support backup use cases with longer retention times, and a SnapMirror license was needed to configure *mirror* relationships between ONTAP instances, where each ONTAP instance would maintain the same number of snapshots (that is, a *mirror* image) to support disaster recovery use cases to make cluster failovers possible. Both SnapMirror and SnapVault licenses continue to be used and supported for ONTAP 8.x and 9.x releases.

While SnapVault licenses continue to function and are supported for both ONTAP 8.x and 9.x releases, the SnapMirror license can be used in place of a SnapVault license and can be used for both mirror and vault configurations.

For ONTAP asynchronous replication, beginning with ONTAP 9.3 a single unified replication engine is used to configure extended data protection mode (XDP) policies, where the SnapMirror license can be configured for a mirror policy, a vault policy, or a mirror-vault policy. A SnapMirror license is required on both the source and destination clusters. A SnapVault license is not required if a SnapMirror license is already installed. The SnapMirror asynchronous perpetual license is included in the ONTAP One software suite that's installed on new AFF and FAS systems.

Data protection configuration limits are determined using several factors, including your ONTAP version, hardware platform, and the licenses installed. For more information, see Hardware Universe.

SnapMirror synchronous license

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported. You require the following licenses for creating a SnapMirror synchronous relationship:

- The SnapMirror synchronous license is required on both the source cluster and the destination cluster.

  The SnapMirror synchronous license is part of the ONTAP One license suite.

  If your system was purchased before June 2019 with a Premium or Flash Bundle, you can download a NetApp master key to get the required SnapMirror synchronous license from the NetApp Support Site: Master License Keys.

- The SnapMirror license is required on both the source cluster and the destination cluster.

SnapMirror cloud license

Beginning with ONTAP 9.8, the SnapMirror cloud license provides asynchronous replication of snapshots from ONTAP instances to object storage endpoints. Replication targets can be configured using both on-premises object stores as well as S3 and S3-compatible public cloud object storage services. SnapMirror cloud relationships are supported from ONTAP systems to pre-qualified object storage targets.

SnapMirror cloud is not available as a standalone license. Only one license is needed per ONTAP cluster. In addition to a SnapMirror cloud license, the SnapMirror asynchronous license is also required.

You require the following licenses for creating a SnapMirror cloud relationship:

- Both a SnapMirror license and a SnapMirror cloud license for replicating directly to the object store endpoint.
- When configuring a multi-policy replication workflow (for example, Disk-to-Disk-to-Cloud), a SnapMirror license is required on all ONTAP instances, while the SnapMirror cloud license is only required for the source cluster which is replicating directly to the object storage endpoint.

Beginning with ONTAP 9.9.1, you can use System Manager for SnapMirror cloud replication.

A list of authorized SnapMirror cloud third-party applications is published on the NetApp web site.

Data Protection Optimized license

Data Protection Optimized (DPO) licenses are no longer being sold, and DPO is not supported on current platforms; however, if you have a DPO license installed on a supported platform, NetApp continues to provide support until the end of availability of that platform.

DPO is not included with the ONTAP One license bundle, and you cannot upgrade to the ONTAP One license bundle if the DPO license is installed on a system.

For information about supported platforms, see Hardware Universe.

ONTAP DPO systems feature enhancements

Beginning with ONTAP 9.6, the maximum number of FlexVol volumes supported increases when the DP_Optimized (DPO) license is installed. Beginning with ONTAP 9.4, systems with the DPO license support SnapMirror backoff, cross-volume background deduplication, use of snapshot blocks as donors, and compaction.

Beginning with ONTAP 9.6, the maximum supported number of FlexVol volumes on secondary or data protection systems has increased, enabling you to scale up to 2,500 FlexVol volumes per node, or up to 5,000 in failover mode. The increase in FlexVol volumes is enabled with the DP_Optimized (DPO) license. A SnapMirror license is still required on both the source and destination nodes.

Beginning with ONTAP 9.4, the following feature enhancements are made to DPO systems:

- SnapMirror backoff: In DPO systems, replication traffic is given the same priority that client workloads are given.

  SnapMirror backoff is disabled by default on DPO systems.

- Volume background deduplication and cross-volume background deduplication: Volume background deduplication and cross-volume background deduplication are enabled in DPO systems.

You can run the `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` command to deduplicate the existing data. The best practice is to run the command during off-peak hours to reduce the impact on performance.

Learn more about `storage aggregate efficiency cross-volume-dedupe start` in the ONTAP command reference.

- Increased savings by using snapshot blocks as donors: The data blocks that are not available in the active file system but are trapped in snapshots are used as donors for volume deduplication.

  The new data can be deduplicated with the data that was trapped in snapshots, effectively sharing the snapshot blocks as well. The increased donor space provides more savings, especially when the volume has a large number of snapshots.

- Compaction: Data compaction is enabled by default on DPO volumes.

Learn about path name pattern matching in ONTAP SnapMirror commands

You can use pattern matching to specify the source and destination paths in `snapmirror` commands.

`snapmirror` commands use fully qualified path names in the following format: `vserver:volume`. You can abbreviate the path name by not entering the SVM name. If you do this, the `snapmirror` command assumes the local SVM context of the user.

Assuming that the SVM is called “vserver1” and the volume is called “vol1”, the fully qualified path name is `vserver1:vol1`.

You can use the asterisk (*) in paths as a wildcard to select matching, fully qualified path names. The following table provides examples of using the wildcard to select a range of volumes.

`*`	Matches all paths.
`vs*`	Matches all SVMs and volumes with SVM names beginning with `vs`.
`:*src`	Matches all SVMs with volume names containing the `src` text.
`:vol`	Matches all SVMs with volume names beginning with `vol`.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------ ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                Snapmirrored  Idle           -
true    -
```

Learn more about `snapmirror show` in the ONTAP command reference.

Learn about extended queries for ONTAP SnapMirror relationship operations

You can use *extended queries* to perform SnapMirror operations on many SnapMirror relationships at one time. For example, you might have multiple uninitialized SnapMirror relationships that you want to initialize using one command.

About this task

You can apply extended queries to the following SnapMirror operations:

- Initializing uninitialized relationships
- Resuming quiesced relationships
- Resynchronizing broken relationships
- Updating idle relationships
- Aborting relationship data transfers

Step

1. Perform a SnapMirror operation on many relationships:

   `snapmirror command` `{-state state } *`

   The following command initializes SnapMirror relationships that are in an `Uninitialized` state:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

   Learn more about `snapmirror initialize` in the ONTAP command reference.

Compatible ONTAP versions for SnapMirror relationships

The source and destination volumes must be running compatible ONTAP versions before creating a SnapMirror data protection relationship. Before you upgrade ONTAP, you should verify that your current ONTAP version is compatible with your target ONTAP version for SnapMirror relationships.

Unified replication relationships

For SnapMirror relationships of type “XDP”, using on premises or Cloud Volumes ONTAP releases:

Beginning with ONTAP 9.9.0:

- ONTAP 9.x.0 releases are cloud-only releases and support Cloud Volumes ONTAP systems. The asterisk (*) after the release version indicates a cloud-only release.

  ⓘ ONTAP 9.16.0 is an exception to the cloud-only rule because it provides support for ASA r2 systems. The plus sign (+) after the release version indicates both an ASA r2 and cloud supported release. ASA r2 systems support SnapMirror relationships only to other ASA r2 systems.

- ONTAP 9.x.1 releases are general releases and support both on-premises and Cloud Volumes ONTAP systems.

  ⓘ When advanced capacity balancing is enabled on volumes in clusters running ONTAP 9.16.1 or later, SnapMirror transfers are not supported to clusters running ONTAP versions earlier than ONTAP 9.16.1.

ⓘ Interoperability is bidirectional.

Interoperability for ONTAP version 9.4 and later

ONTAP version…	**Interoperates with these previous ONTAP versions…**																				
	9.18.1	9.17.1	9.16.1	9.16.0+	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5
9.18.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	**Yes**	No	No	No	No	No	No	No	No	No	No	No	No
9.17.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No	No	No	No	No
9.16.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No	No	No

9.16.0+	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No	No	No
9.15.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No
9.15.0*	No	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No
9.14.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No
9.14.0*	No	**Yes**	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No
9.13.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.13.0*	No	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No
9.12.1	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.12.0*	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	No	No
9.11.1	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.11.0*	No	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No
9.10.1	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.10.0*	No	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**
9.9.1	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.9.0*	No	No	No	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.8	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.7	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.6	No	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

9.5	No	No	No	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

SnapMirror synchronous relationships

SnapMirror synchronous is not supported for ONTAP cloud instances.

ONTAP version…	Interoperates with these previous ONTAP versions…													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.18.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No
9.17.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No
9.16.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No
9.15.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No
9.14.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.13.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.12.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.11.1	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No
9.10.1	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.9.1	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.8	No	No	No	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.7	No	No	No	No	No	**Yes**	**Yes**	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.6	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**
9.5	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**

SnapMirror SVM disaster recovery relationships

- This matrix applies to the SVM data mobility migration feature beginning with ONTAP 9.10.1.
- You can use SVM DR to migrate an SVM that does not meet the restrictions indicated for SVM migration (SVM data mobility).
- In both cases, a maximum of 2 major **newer** ONTAP versions can separate the source and destination clusters, with the requirement that the destination be same version or newer than source ONTAP version.

For SVM disaster recovery data and SVM protection:

SVM disaster recovery is supported only between clusters running the same version of ONTAP. **Version-independence is not supported for SVM replication**.

For SVM disaster recovery for SVM migration:

- Replication is supported in a single direction from an earlier version of ONTAP on the source to the same

or later version of ONTAP on the destination.

- The ONTAP version on the target cluster must be no more than two major on-premises versions newer or two major cloud versions newer (beginning with ONTAP 9.9.0), as shown in the table below.
  - Replication is not supported for long-term data protection use cases.

The asterisk (*) after the release version indicates a cloud-only release.

To determine support, locate the source version in the left table column, and then locate the destination version on the top row (DR/Migration for like versions and Migration only for newer versions).

If you are using ONTAP 9.10.1 or later, you can use the SVM data mobility feature instead of SVM DR to migrate SVMs from one cluster to another.

Source	**Destination**																				
	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1
9.5	DR/Migration	Migration	Migration																			
9.6		DR/Migration	Migration	Migration																		
9.7			DR/Migration	Migration	Migration																	
9.8				DR/Migration	Migration	Migration		Migration														
9.9.0*					DR/Migration	Migration	Migration	Migration	Migration	Migration												
9.9.1						DR/Migration	Migration	Migration	Migration	Migration												
9.10.0*							DR/Migration	Migration	Migration	Migration	Migration	Migration										

9.10.1								DR/Migration	Migration	Migration	Migration	Migration									
9.11.0*									DR/Migration	Migration	Migration	Migration	Migration	Migration							
9.11.1										DR/Migration	Migration	Migration	Migration	Migration							
9.12.0*											DR/Migration	Migration	Migration	Migration	Migration	Migration					
9.12.1												DR/Migration	Migration	Migration	Migration	Migration					
9.13.0*													DR/Migration	Migration	Migration	Migration	Migration	Migration			
9.13.1														DR/Migration	Migration	Migration	Migration	Migration			
9.14.0*															DR/Migration	Migration	Migration	Migration	Migration	Migration	
9.14.1																DR/Migration	Migration	Migration	Migration	Migration	
9.15.0*																	DR/Migration	Migration	Migration	Migration	Migration
9.15.1																		DR/Migration	Migration	Migration	Migration

9.16.0																		DR/Migration	Migration	Migration	Migration
9.16.1																			DR/Migration	Migration	Migration
9.17.1																				DR/Migration	Migration
9.18.1																					DR/Migration

SnapMirror disaster recovery relationships

For SnapMirror relationships of type “DP” and policy type “async-mirror”:

DP-type mirrors cannot be initialized beginning with ONTAP 9.11.1 and are completely deprecated in ONTAP 9.12.1. For more information, see Deprecation of data protection SnapMirror relationships.

In the following table, the column on the left indicates the ONTAP version on the source volume, and the top row indicates the ONTAP versions you can have on your destination volume.

Source	Destination								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	Yes	No	No	No	No	No	No	No	No
9.10.1	Yes	Yes	No	No	No	No	No	No	No
9.9.1	Yes	Yes	Yes	No	No	No	No	No	No
9.8	No	Yes	Yes	Yes	No	No	No	No	No
9.7	No	No	Yes	Yes	Yes	No	No	No	No
9.6	No	No	No	Yes	Yes	Yes	No	No	No
9.5	No	No	No	No	Yes	Yes	Yes	No	No
9.4	No	No	No	No	No	Yes	Yes	Yes	No
9.3	No	No	No	No	No	No	Yes	Yes	Yes

Interoperability is not bidirectional.

Learn about ONTAP SnapMirror limitations

You should be aware of basic SnapMirror limitations before creating a data protection relationship.

- A destination volume can have only one source volume.

  A source volume can have multiple destination volumes. The destination volume can be the source volume for any type of SnapMirror replication relationship.

- Depending on the array model, you can fan out a maximum of eight or sixteen destination volumes from a single source volume. See the Hardware Universe to learn details for your specific configuration.
- You cannot restore files to the destination of a SnapMirror DR relationship.
- Source or destination SnapVault volumes cannot be 32-bit.
- The source volume for a SnapVault relationship should not be a FlexClone volume.

  The relationship will work, but the efficiency offered by FlexClone volumes will not be preserved.

Configure SnapMirror volume replication

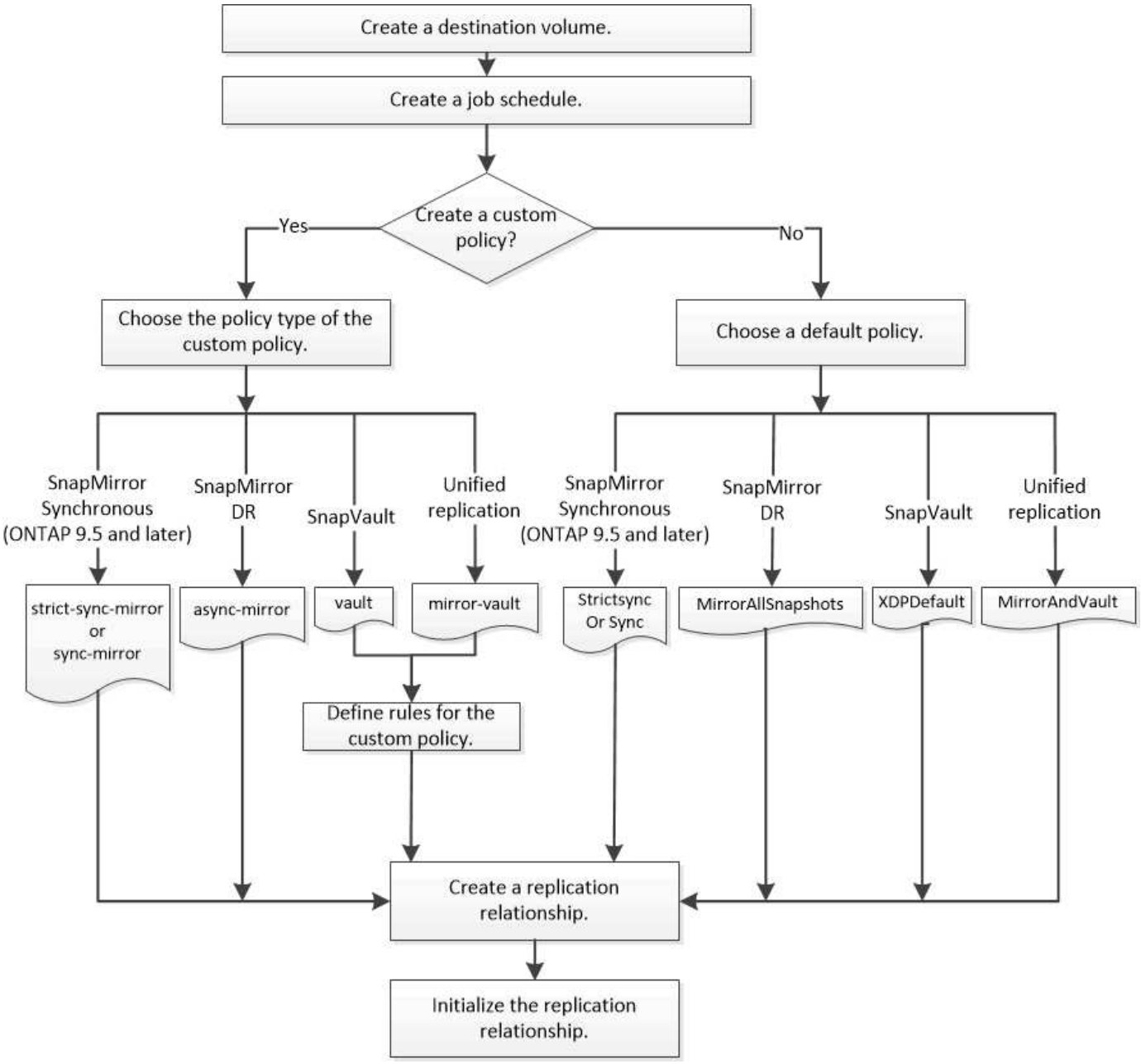
ONTAP SnapMirror replication workflow

SnapMirror offers three types of data protection relationship: SnapMirror DR, archive (previously known as SnapVault), and unified replication. You can follow the same basic workflow to configure each type of relationship.

Beginning with general availability in ONTAP 9.9.1, SnapMirror active sync provides Zero Recovery Time Objective (Zero RTO) or Transparent Application Failover (TAF) to enable automatic failover of business-critical applications in SAN environments.

For each type of SnapMirror data protection relationship, the workflow is the same: create a destination volume, create a job schedule, specify a policy, create and initialize the relationship.

Beginning with ONTAP 9.3, you can use the `snapmirror protect` command to configure a data protection relationship in a single step. Even if you use `snapmirror protect`, you need to understand each step in the workflow.



Related information

- snapmirror protect

Configure an ONTAP SnapMirror replication relationship in one step

Beginning with ONTAP 9.3, you can use the `snapmirror protect` command to configure a data protection relationship in a single step. You specify a list of volumes to be replicated, an SVM on the destination cluster, a job schedule, and a SnapMirror policy. `snapmirror protect` does the rest.

Before you begin

- The source and destination clusters and SVMs must be peered.

  Cluster and SVM peering

- The language on the destination volume must be the same as the language on the source volume.

About this task

The `snapmirror protect` command chooses an aggregate associated with the specified SVM. If no aggregate is associated with the SVM, it chooses from all the aggregates in the cluster. The choice of aggregate is based on the amount of free space and the number of volumes on the aggregate.

The `snapmirror protect` command then performs the following steps:

- Creates a destination volume with an appropriate type and amount of reserved space for each volume in the list of volumes to be replicated.
- Configures a replication relationship appropriate for the policy you specify.
- Initializes the relationship.

The name of the destination volume is of the form *`source_volume_name_dst`*. In case of a conflict with an existing name, the command appends a number to the volume name. You can specify a prefix and/or suffix in the command options. The suffix replaces the system-supplied `dst` suffix.

In ONTAP 9.4 and later, a destination volume can contain up to 1019 snapshots.
In ONTAP 9.3 and earlier, a destination volume can contain up to 251 snapshots.

Initialization can be time-consuming. `snapmirror protect` does not wait for initialization to complete before the job finishes. For this reason, you should use the `snapmirror show` command rather than the `job show` command to determine when initialization is complete.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships can be created by using the `snapmirror protect` command.

Learn more about `snapmirror protect` in the ONTAP command reference.

Step

1. Create and initialize a replication relationship in one step:

   You must replace the variables in angle brackets with the required values before running this command.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   You must run this command from the destination SVM or the destination cluster. The `-auto -initialize` option defaults to “true”.

   The following example creates and initializes a SnapMirror DR relationship using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

You can use a custom policy if you prefer. For more information, see Creating a custom replication policy.

The following example creates and initializes a SnapVault relationship using the default `XDPDefault` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

The following example creates and initializes a unified replication relationship using the default `MirrorAndVault` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

The following example creates and initializes a SnapMirror synchronous relationship using the default `Sync` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

For SnapVault and unified replication policies, you might find it useful to define a schedule for creating a copy of the last transferred snapshot on the destination. For more information, see Defining a schedule for creating a local copy on the destination.

After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

Learn more about `snapmirror show` in the ONTAP command reference.

Related information

- job show

Configure a replication relationship one step at a time

Create an ONTAP SnapMirror destination volume

You can use the `volume create` command on the destination to create a destination

volume. The destination volume should be the same or greater in size than the source volume. Learn more about `volume create` in the ONTAP command reference.

Step

1. Create a destination volume:

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

   The following example creates a 2-GB destination volume named `volA_dst`:

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

Create an ONTAP SnapMirror replication job schedule

The job schedule determines when SnapMirror automatically updates the data protection relationship to which the schedule is assigned. You can use System Manager or the `job schedule cron create` command to create a replication job schedule. Learn more about `job schedule cron create` in the ONTAP command reference.

About this task

You assign a job schedule when you create a data protection relationship. If you do not assign a job schedule, you must update the relationship manually.

Steps

You can create a replication job schedule using System Manager or the ONTAP CLI.

System Manager

1. Navigate to **Protection > Overview** and and expand **Local policy settings**.
2. In the **Schedules** pane, click →.
3. In the **Schedules** window, click + Add .
4. In the **Add schedule** window, enter the schedule name, and choose the context and schedule type.
5. Click **Save**.

CLI

1. Create a job schedule:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

Beginning with ONTAP 9.10.1, you can include the Vserver for your job schedule:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

ⓘ The minimum supported schedule (RPO) for FlexVol volumes in a volume SnapMirror relationship is 5 minutes. The minimum supported schedule (RPO) for FlexGroup volumes in a volume SnapMirror relationship is 30 minutes.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Customize a SnapMirror replication policy

Create a custom ONTAP SnapMirror replication policy

You can create a custom replication policy if the default policy for a relationship is not suitable. You might want to compress data in a network transfer, for example, or modify the number of attempts SnapMirror makes to transfer snapshots.

You can use a default or custom policy when you create a replication relationship. For a custom archive (formerly SnapVault) or unified replication policy, you must define one or more *rules* that determine which

snapshots are transferred during initialization and update. You might also want to define a schedule for creating local snapshots on the destination.

The *policy type* of the replication policy determines the type of relationship it supports. The table below shows the available policy types.

Policy type	Relationship type
async-mirror	SnapMirror DR
vault	SnapVault
mirror-vault	Unified replication
strict-sync-mirror	SnapMirror synchronous in the StrictSync mode (supported beginning with ONTAP 9.5)
sync-mirror	SnapMirror synchronous in the Sync mode (supported beginning with ONTAP 9.5)

When you create a custom replication policy, it is a good idea to model the policy after a default policy.

Steps

You can create custom data protection policies with System Manager or the ONTAP CLI. Beginning with ONTAP 9.11.1, you can use System Manager to create custom mirror and vault policies, and to display and select legacy policies. This capability is also available in ONTAP 9.8P12 and later patches of ONTAP 9.8.

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

System Manager

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Protection Policies**, click →.
3. In the **Protection Policies** pane, click + Add .
4. Enter the new policy name, and select the policy scope.
5. Choose a policy type. To add a vault-only or mirror-only policy, choose **Asynchronous**, and click **Use a legacy policy type**.
6. Complete the required fields.
7. Click **Save**.
8. Repeat these steps on the other cluster.

CLI

1. Create a custom replication policy:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

Beginning with ONTAP 9.5, you can specify the schedule for creating a common snapshot schedule for SnapMirror synchronous relationships by using the `-common-snapshot-schedule` parameter. By default, the common snapshot schedule for SnapMirror synchronous relationships is one hour. You can specify a value from 30 minutes to two hours for the snapshot schedule for SnapMirror synchronous relationships.

The following example creates a custom replication policy for SnapMirror DR that enables network compression for data transfers:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

The following example creates a custom replication policy for SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

The following example creates a custom replication policy for unified replication:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

The following example creates a custom replication policy for SnapMirror synchronous relationship in the StrictSync mode:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Learn more about `snapmirror policy create` in the ONTAP command reference.

After you finish

For “vault” and “mirror-vault” policy types, you must define rules that determine which snapshots are transferred during initialization and update.

Use the `snapmirror policy show` command to verify that the SnapMirror policy was created.

Learn more about `snapmirror policy show` in the ONTAP command reference.

Define a rule for an ONTAP SnapMirror policy

For custom policies with the `vault` or `mirror-vault` policy type, you must define at least one rule that determines which snapshots are transferred during initialization and update. You can also define rules for default policies with the `vault` or `mirror-vault` policy type.

About this task

Every policy with the `vault` or `mirror-vault` policy type must have a rule that specifies which snapshots to replicate. The rule `bi-monthly`, for example, indicates that only snapshots assigned the SnapMirror label `bi-monthly` should be replicated. You specify the SnapMirror label when you configure the snapshot policy on the source.

Each policy type is associated with one or more system-defined rules. These rules are automatically assigned to a policy when you specify its policy type. The table below shows the system-defined rules.

System-defined rule	Used in policy types	Result
sm_created	async-mirror, mirror-vault, Sync, StrictSync	A snapshot created by SnapMirror is transferred on initialization and update.
all_source_snapshots	async-mirror	New snapshots on the source are transferred on initialization and update.
daily	vault,mirror-vault	New snapshots on the source with the SnapMirror label `daily` are transferred on initialization and update.

weekly	vault,mirror-vault	New snapshots on the source with the SnapMirror label `weekly` are transferred on initialization and update.
monthly	mirror-vault	New snapshots on the source with the SnapMirror label `monthly` are transferred on initialization and update.
app_consistent	Sync, StrictSync	Snapshots with the SnapMirror label `app_consistent` on source are synchronously replicated to the destination. Supported beginning with ONTAP 9.7.

Except for the “async-mirror” policy type, you can specify additional rules as needed, for default or custom policies. For example:

- For the default `MirrorAndVault` policy, you might create a rule called `bi-monthly` to match snapshots on the source with the `bi-monthly` SnapMirror label.
- For a custom policy with the `mirror-vault` policy type, you might create a rule called `bi-weekly` to match snapshots on the source with the `bi-weekly` SnapMirror label.

Step

1. Define a rule for a policy:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   The following example adds a rule with the SnapMirror label `bi-monthly` to the default `MirrorAndVault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   The following example adds a rule with the SnapMirror label `bi-weekly` to the custom `my_snapvault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   The following example adds a rule with the SnapMirror label `app_consistent` to the custom `Sync` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Learn more about `snapmirror policy add-rule` in the ONTAP command reference.

You can then replicate snapshots from the source cluster that match this SnapMirror label:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Define an ONTAP SnapMirror schedule to create a local copy on the destination

For SnapVault and unified replication relationships, you can protect against the possibility that an updated snapshot is corrupted by creating a copy of the last transferred snapshot on the destination. This "local copy" is retained regardless of the retention rules on the source, so that even if the snapshot originally transferred by SnapMirror is no longer available on the source, a copy of it will be available on the destination.

About this task

You specify the schedule for creating a local copy in the `-schedule` option of the `snapmirror policy add-rule` command.

Step

1. Define a schedule for creating a local copy on the destination:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   For an example of how to create a job schedule, see Creating a replication job schedule.

   The following example adds a schedule for creating a local copy to the default `MirrorAndVault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   The following example adds a schedule for creating a local copy to the custom `my_unified` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_unified -snapmirror-label my_monthly -schedule my_monthly
   ```

   Learn more about `snapmirror policy add-rule` in the ONTAP command reference.

Create an ONTAP SnapMirror replication relationship

The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship.* You can use the `snapmirror create` command to create SnapMirror DR, SnapVault, or unified replication data protection relationships.

> This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to create a replication relationship. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Beginning with ONTAP 9.11.1, you can use System Manager to select pre-created and custom mirror and vault policies, to display and select legacy policies, and to override the transfer schedules defined in a protection policy when protecting volumes and storage VMs. This capability is also available in ONTAP 9.8P12 and later patches of ONTAP 9.8.

> If you are using ONTAP 9.8P12 or later ONTAP 9.8 patch release and you configured SnapMirror using System Manager, you should use ONTAP 9.9.1P13 or later and ONTAP 9.10.1P10 or later patch releases if you plan to upgrade to ONTAP 9.9.1 or ONTAP 9.10.1 releases.

Before you begin

- The source and destination clusters and SVMs must be peered.

  Cluster and SVM peering

- The language on the destination volume must be the same as the language on the source volume.

About this task

Until ONTAP 9.3, SnapMirror invoked in DP mode and SnapMirror invoked in XDP mode used different replication engines, with different approaches to version-dependence:

- SnapMirror invoked in DP mode used a *version-dependent* replication engine in which the ONTAP version was required to be the same on primary and secondary storage:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror invoked in XDP mode used a *version-flexible* replication engine that supported different ONTAP versions on primary and secondary storage:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

With improvements in performance, the significant benefits of version-flexible SnapMirror outweigh the slight advantage in replication throughput obtained with version-dependent mode. For this reason, beginning with ONTAP 9.3, XDP mode has been made the new default, and any invocations of DP mode on the command

line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. The table below shows the behavior you can expect.

If you specify…	The type is…	The default policy (if you do not specify a policy) is…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nothing	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	XDPDefault (SnapVault)

See also the examples in the procedure below.

The only exceptions to conversion are as follows:

- SVM data protection relationships continue to default to DP mode.

  Specify XDP explicitly to obtain XDP mode with the default `MirrorAllSnapshots` policy.

- Load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode.
- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  This option is ignored if you do not explicitly invoke DP.

Beginning with ONTAP 9.14.1, the `-backoff-level` option is added to the `snapmirror create`, `snapmirror modify`, and `snapmirror restore` commands to enable you to specify the backoff level per relationship. The option is supported only with FlexVol SnapMirror relationships. The optional command specifies the SnapMirror backoff level due to client ops. Backoff values can be high, medium or none. The default value is high.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported.

In ONTAP 9.4 and later, a destination volume can contain up to 1019 snapshots.
In ONTAP 9.3 and earlier, a destination volume can contain up to 251 snapshots.

Steps

You can use System Manager or the ONTAP CLI to create a replication relationship.

System Manager

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.

CLI

1. From the destination cluster, create a replication relationship:

   You must replace the variables in angle brackets with the required values before running this command.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   The `schedule` parameter is not applicable when creating SnapMirror synchronous relationships.

   The following example creates a SnapMirror DR relationship using the default `MirrorLatest` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   The following example creates a SnapVault relationship using the default `XDPDefault` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   The following example creates a unified replication relationship using the default `MirrorAndVault` policy:

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorAndVault
   ```

The following example creates a unified replication relationship using the custom `my_unified` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

The following example creates a SnapMirror synchronous relationship using the default `Sync` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

The following example creates a SnapMirror synchronous relationship using the default `StrictSync` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

The following example creates a SnapMirror DR relationship. With the DP type automatically converted to XDP and with no policy specified, the policy defaults to the `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

The following example creates a SnapMirror DR relationship. With no type or policy specified, the policy defaults to the `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

The following example creates a SnapMirror DR relationship. With no policy specified, the policy defaults to the `XDPDefault` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

The following example creates a SnapMirror synchronous relationship with the predefined policy `SnapCenterSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

The predefined policy `SnapCenterSync` is of type `Sync`. This policy replicates any snapshot that is created with the `snapmirror-label` of "app_consistent".

After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

Learn more about `snapmirror show` in the ONTAP command reference.

Related information

- Create and delete SnapMirror failover test volumes.

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

Related information

- snapmirror create

Initialize an ONTAP SnapMirror replication relationship

For all relationship types, initialization performs a *baseline transfer*: it makes a snapshot of the source volume, then transfers that copy and all the data blocks it references to the destination volume. Otherwise, the contents of the transfer depend on the policy.

Before you begin

The source and destination clusters and SVMs must be peered.

Cluster and SVM peering

About this task

Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported.

You should be aware that if a filesystem is rebooted for any reason, such as a node reboot, takeover/giveback, or panic, then initialization will not automatically resume and must be restarted manually.

Step

1. Initialize a replication relationship:

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

You must run this command from the destination SVM or the destination cluster.

The following example initializes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror initialize` in the ONTAP command reference.

Ensure a common snapshot in an ONTAP mirror-vault deployment

You can use the `snapmirror snapshot-owner create` command to preserve a labeled snapshot on the secondary in a mirror-vault deployment. Doing so ensures that a common snapshot exists for the update of the vault relationship.

About this task

If you use a combination mirror-vault fan-out or cascade deployment, you should keep in mind that updates will fail if a common snapshot does not exist on the source and destination volumes.

This is never an issue for the mirror relationship in a mirror-vault fan-out or cascade deployment, since SnapMirror always creates a snapshot of the source volume before it performs the update.

It might be an issue for the vault relationship, however, because SnapMirror does not create a snapshot of the source volume when it updates a vault relationship. You need to use the `snapmirror snapshot-owner create` to ensure that there is at least one common snapshot on both the source and destination of the vault relationship. Learn more about data protection fan-out and cascade deployments.

Steps

1. On the source volume, assign an owner to the labeled snapshot you want to preserve:

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   The following example assigns `ApplicationA` as the owner of the `snap1` snapshot:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   Learn more about `snapmirror snapshot-owner create` in the ONTAP command reference.

2. Update the mirror relationship, as described in Updating a replication relationship manually.

   Alternatively, you can wait for the scheduled update of the mirror relationship.

3. Transfer the labeled snapshot to the vault destination:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

`-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot snapshot`

The following example transfers the `snap1` snapshot

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

The labeled snapshot will be preserved when the vault relationship is updated.

Learn more about `snapmirror update` in the ONTAP command reference.

4. On the source volume, remove the owner from the labeled snapshot:

`snapmirror snapshot-owner delete -vserver *SVM* -volume *volume* -snapshot *snapshot* -owner *owner*`

The following examples removes `ApplicationA` as the owner of the `snap1` snapshot:

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

Learn more about `snapmirror snapshot-owner delete` in the ONTAP command reference.

Example: Configure an ONTAP SnapMirror vault-vault cascade

An example will show in concrete terms how you can configure replication relationships one step at a time. You can use the vault-vault cascade deployment configured in the example to retain more than 251 snapshots labeled `my-weekly`.

Before you begin

The source and destination clusters and SVMs must be peered.

About this task

The example assumes the following:

- You have configured snapshots on the source cluster with the SnapMirror labels `my-daily`, `my-weekly`, and `my-monthly`.
- You have configured destination volumes named `volA` on the secondary and tertiary destination clusters.
- You have configured replication job schedules named `my_snapvault` on the secondary and tertiary destination clusters.

The example shows how to create replication relationships based on two custom policies:

- The `snapvault_secondary` policy retains 7 daily, 52 weekly, and 180 monthly snapshots on the secondary destination cluster.
- The `snapvault_tertiary policy` retains 250 weekly snapshots on the tertiary destination cluster.

Steps

1. On the secondary destination cluster, create the `snapvault_secondary` policy:

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment "Policy on secondary for vault to vault cascade" -vserver
   svm_secondary
   ```

2. On the secondary destination cluster, define the `my-daily` rule for the policy:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. On the secondary destination cluster, define the `my-weekly` rule for the policy:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-weekly -keep 52 -vserver svm_secondary
   ```

4. On the secondary destination cluster, define the `my-monthly` rule for the policy:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-monthly -keep 180 -vserver svm_secondary
   ```

5. On the secondary destination cluster, verify the policy:

   ```
   cluster_secondary::> snapmirror policy show snapvault_secondary -instance
   ```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily                7  false       0 -
-
                              my-weekly              52  false       0 -
-
                              my-monthly            180  false       0 -
-
```

6. On the secondary destination cluster, create the relationship with the source cluster:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. On the secondary destination cluster, initialize the relationship with the source cluster:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. On the tertiary destination cluster, create the `snapvault_tertiary` policy:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. On the tertiary destination cluster, define the `my-weekly` rule for the policy:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. On the tertiary destination cluster, verify the policy:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                    Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. On the tertiary destination cluster, create the relationship with the secondary cluster:

    ```
    cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
    -destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
    snapvault_tertiary
    ```

12. On the tertiary destination cluster, initialize the relationship with the secondary cluster:

    ```
    cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
    -destination-path svm_tertiary:volA
    ```

Related information

- snapmirror create
- snapmirror initialize
- snapmirror policy add-rule
- snapmirror policy create
- snapmirror policy show

Manage SnapMirror volume replication

Convert an existing ONTAP SnapMirror DP-type relationship to XDP

If you are upgrading to ONTAP 9.12.1 or later, you must convert DP-type relationships to XDP before upgrading. ONTAP 9.12.1 and later does not support DP-type relationships. You can easily convert an existing DP-type relationship to XDP to take advantage of version-flexible SnapMirror.

Before upgrading to ONTAP 9.12.1, you must convert existing DP-type relationships to XDP before you can upgrade to ONTAP 9.12.1 and later releases.

About this task

- SnapMirror does not automatically convert existing DP-type relationships to XDP. To convert the relationship, you need to break and delete the existing relationship, create a new XDP relationship, and resync the relationship.
- When planning your conversion, you should be aware that background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

> After you convert a SnapMirror relationship type from DP to XDP, space-related settings, such as autosize and space guarantee are no longer replicated to the destination.

Steps

1. From the destination cluster, ensure that the SnapMirror relationship is type DP, that the mirror state is SnapMirrored, the relationship status is Idle, and the relationship is healthy:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   The following example shows the output from the `snapmirror show` command:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

You might find it helpful to retain a copy of the `snapmirror show` command output to keep track existing of the relationship settings. Learn more about `snapmirror show` in the ONTAP command reference.

2. From the source and the destination volumes, ensure that both volumes have a common snapshot:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the `volume snapshot show` output for the source and the destination volumes:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. To ensure scheduled updates will not run during the conversion, quiesce the existing DP-type relationship:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

You must run this command from the destination SVM or the destination cluster.

The following example quiesces the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror quiesce` in the ONTAP command reference.

4. Break the existing DP-type relationship:

```
snapmirror break -destination-path <SVM:volume>
```

You must run this command from the destination SVM or the destination cluster.

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror break` in the ONTAP command reference.

5. If automatic deletion of snapshots is enabled on the destination volume, disable it:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

The following example disables snapshot autodelete on the destination volume `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Delete the existing DP-type relationship:

```
snapmirror delete -destination-path <SVM:volume>
```

Learn more about `snapmirror-delete` in the ONTAP command reference.

You must run this command from the destination SVM or the destination cluster.

The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Release the origin SVM disaster recovery relationship on the source:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

The following example releases the SVM disaster recovery relationship:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

Learn more about `snapmirror release` in the ONTAP command reference.

8. You can use the output you retained from the `snapmirror show` command to create the new XDP-type relationship:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

The new relationship must use the same source and destination volume. Learn more about the commands described in this procedure in the ONTAP command reference.

You must run this command from the destination SVM or the destination cluster.

The following example creates a SnapMirror disaster recovery relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup` using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resync the source and destination volumes:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

To improve resync time, you can use the `-quick-resync` option, but you should be aware that storage efficiency savings can be lost.

> You must run this command from the destination SVM or the destination cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror resync` in the ONTAP command reference.

10. If you disabled automatic deletion of snapshots, reenable it:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

After you finish

1. Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

   Learn more about `snapmirror show` in the ONTAP command reference.

2. Once the SnapMirror XDP destination volume begins updating snapshots as defined by the SnapMirror policy, use the output of `snapmirror list-destinations` command from the source cluster to display the new SnapMirror XDP relationship.

Additional information about DP-type relationships

Beginning with ONTAP 9.3, XDP mode is the default, and any invocations of DP mode on the command line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. Beginning with ONTAP 9.5, MirrorAndVault is the default policy when no data protection mode is specified or when XDP mode is specified as the relationship type. The table below shows the expected behavior.

If you specify…	The type is…	The default policy (if you do not specify a policy) is…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)

Nothing	XDP	MirrorAndVault (unified replication)
XDP	XDP	MirrorAndVault (unified replication)

As the table shows, the default policies assigned to XDP in different circumstances ensure that the conversion maintains the functional equivalence of the previous types. Of course, you can use different policies as needed, including policies for unified replication:

If you specify…	And the policy is…	The result is…
DP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication
XDP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication

The only exceptions to conversion are as follows:

- SVM data protection relationships continue to default to DP mode in ONTAP 9.3 and earlier.

  Beginning with ONTAP 9.4, SVM data protection relationships default to XDP mode.

- Root volume load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode in ONTAP 9.4 and earlier.

  Beginning with ONTAP 9.5, SnapLock data protection relationships default to XDP mode.

- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  This option is ignored if you do not explicitly invoke DP.

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Convert the type of an ONTAP SnapMirror relationship

Beginning with ONTAP 9.5, SnapMirror synchronous is supported. You can convert an SnapMirror asynchronous relationship to a SnapMirror synchronous relationship or vice versa without performing a baseline transfer.

About this task

You cannot convert an SnapMirror asynchronous relationship to a SnapMirror synchronous relationship or vice versa by changing the SnapMirror policy.

Steps

- **Converting an SnapMirror asynchronous relationship to a SnapMirror synchronous relationship**
  a. From the destination cluster, delete the SnapMirror asynchronous relationship:

     ```
     snapmirror delete -destination-path <SVM:volume>
     ```

     ```
     cluster2::>snapmirror delete -destination-path vs1_dr:vol1
     ```

  b. From the source cluster, release the SnapMirror relationship without deleting the common snapshots:

     ```
     snapmirror release -relationship-info-only true -destination-path
     <destination_SVM>:<destination_volume>
     ```

     ```
     cluster1::>snapmirror release -relationship-info-only true
     -destination-path vs1_dr:vol1
     ```

  c. From the destination cluster, create a SnapMirror synchronous relationship:

     ```
     snapmirror create -source-path src_SVM:src_volume -destination-path
     <destination_SVM>:<destination_volume> -policy sync-mirror
     ```

     ```
     cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
     vs1_dr:vol1 -policy sync
     ```

  d. Resynchronize the SnapMirror synchronous relationship:

     ```
     snapmirror resync -destination-path <destination_SVM:destination_volume>
     ```

     ```
     cluster2::>snapmirror resync -destination-path vs1_dr:vol1
     ```

- **Converting a SnapMirror synchronous relationship to an SnapMirror asynchronous relationship**
  a. From the destination cluster, quiesce the existing SnapMirror synchronous relationship:

     ```
     snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
     ```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. From the destination cluster, delete the SnapMirror asynchronous relationship:

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. From the source cluster, release the SnapMirror relationship without deleting the common snapshots:

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. From the destination cluster, create an SnapMirror asynchronous relationship:

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Resynchronize the SnapMirror synchronous relationship:

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Convert the mode of an ONTAP SnapMirror synchronous relationship

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported. You can convert the mode of a SnapMirror synchronous relationship from StrictSync to Sync

or vice versa.

About this task

You cannot modify the policy of a SnapMirror synchronous relationship to convert its mode.

Steps

1. From the destination cluster, quiesce the existing SnapMirror synchronous relationship:

   `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
   ```

2. From the destination cluster, delete the existing SnapMirror synchronous relationship:

   `snapmirror delete -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror delete -destination-path vs1_dr:vol1
   ```

3. From the source cluster, release the SnapMirror relationship without deleting the common snapshots:

   `snapmirror release -relationship-info-only true -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster1::> snapmirror release -relationship-info-only true -destination
   -path vs1_dr:vol1
   ```

4. From the destination cluster, create a SnapMirror synchronous relationship by specifying the mode to which you want to convert the SnapMirror synchronous relationship:

   `snapmirror create -source-path vs1:vol1 -destination-path <destination_SVM>:<destination_volume> -policy Sync|StrictSync`

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. From the destination cluster, resynchronize the SnapMirror relationship:

   `snapmirror resync -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror resync -destination-path vs1_dr:vol1
   ```

Related information

- snapmirror create

- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Create and delete ONTAP SnapMirror failover test volumes

Beginning with ONTAP 9.14.1, you can use System Manager to create a volume clone to test SnapMirror failover and disaster recovery without disrupting the active SnapMIrror relationship. When you finish testing, you can clean up the associated data and delete the test volume.

Create a SnapMirror failover test volume

About this task

- You can perform failover tests on synchronous and SnapMirror asynchronous relationships.
- A volume clone is created to perform the disaster recovery test.
- The clone volume is created on the same storage VM as the SnapMirror destination.
- You can use FlexVol and FlexGroup SnapMirror relationships.
- If a test clone already exists for the selected relationship, you cannot create another clone for that relationship.
- SnapLock vault relationships are not supported.

Before you begin

- You must be a cluster administrator.
- The SnapMirror license must be installed on the source and destination cluster.

Steps

1. On the destination cluster, select **Protection > Relationships**.
2. Select ⋮ next to the relationship source and choose **Test Failover**.
3. In the **Test Failover** window, select **Test Failover**.
4. Select **Storage > Volumes**, and verify that the test failover volume is listed.
5. Select **Storage > Shares**.
6. Select + Add and choose **Share**.
7. In the **Add share** window, type a name for the share in the **Share Name** field.
8. In the **Folder** field, select **Browse**, select the test clone volume, and **Save**.
9. At the bottom of the **Add share** window, choose **Save**.
10. In the **Storage > Shares** pane, locate the share you created and select ⌄ to view the share information.
11. Under **SMB/CIFS Access**, copy or make note of the access path for the share; for example, `\\123.456.7.890\failover_test`.
12. Use the SMB access path to open the share on the client and verify that the test volume has read and write capabilities.

Clean up failover data and delete the test volume

After you have completed failover testing, you can clean up all data associated with the test volume and delete it.

Steps

1. On the destination cluster, select **Protection > Relationships**.
2. Select ⋮ next to the relationship source and choose **Clean Up Test Failover**.
3. In the **Clean Up Test Failover** window, select **Clean Up**.
4. Select **Storage > Volumes** and verify that the test volume was deleted.

Serve data from a SnapMirror DR destination volume

Make the ONTAP SnapMirror destination volume writeable

You need to make the destination volume writeable before you can serve data from the volume to clients. 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.

About this task

You must perform this task from the destination SVM or the destination cluster.

Steps

You can use System Manager or the ONTAP CLI to make a destination volume writable.

System Manager

1. Select the 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

You need to reverse resynchronize the replication relationship after you make a destination volume writeable.

When the disabled source volume is available again, you should reverse resynchronize the relationship again to copy the current data to the original source volume.

CLI

1. Stop scheduled transfers to the destination:

   ```
   snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   The following example stops scheduled transfers between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path svm1:volA
   -destination-path svm_backup:volA_dst
   ```

   Learn more about `snapmirror quiesce` in the ONTAP command reference.

2. Stop ongoing transfers to the destination:

   ```
   snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   ⓘ This step is not required for SnapMirror synchronous relationships (supported beginning with ONTAP 9.5).

   The following example stops ongoing transfers between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Learn more about `snapmirror abort` in the ONTAP command reference.

3. Break the SnapMirror DR relationship:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror break` in the ONTAP command reference.

Next steps

You need to resynchronize the replication relationship after you make a destination volume writeable.

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

Configure the ONTAP SnapMirror destination volume for data access

After making the destination volume writeable, you must configure the volume for data access. NAS clients, NVMe subsystem, and SAN hosts can access the data from the destination volume until the source volume is reactivated.

NAS environment:

1. Mount the NAS volume to the namespace using the same junction path that the source volume was mounted to in the source SVM.
2. Apply the appropriate ACLs to the SMB shares at the destination volume.
3. Assign the NFS export policies to the destination volume.
4. Apply the quota rules to the destination volume.
5. Redirect clients to the destination volume.
6. Remount the NFS and SMB shares on the clients.

SAN environment:

1. Map the LUNs in the volume to the appropriate initiator group.
2. For iSCSI, create iSCSI sessions from the SAN host initiators to the SAN LIFs.

3. On the SAN client, perform a storage re-scan to detect the connected LUNs.

For information about NVMe environment, see SAN administration.

Reactivate the original ONTAP SnapMirror source volume

You can reestablish the original data protection relationship between the source and destination volumes when you no longer need to serve data from the destination.

About this task

- The procedure below assumes that the baseline in the original source volume is intact. If the baseline is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume before performing the procedure.
- Background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

Steps

1. Reverse the original data protection relationship:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Learn more about `snapmirror resync` in the ONTAP command reference.

   > You must run this command from the original source SVM or the original source cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours. The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship. Learn more about `snapmirror initialize` in the ONTAP command reference.

   The following example reverses the relationship between the original source volume, `volA` on `svm1`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. When you are ready to reestablish data access to the original source, stop access to the original destination volume. One way to do this is to stop the original destination SVM:

   `vserver stop -vserver` *`SVM`*

   > You must run this command from the original destination SVM or the original destination cluster. This command stops user access to the entire original destination SVM. You may want to stop access to the original destination volume using other methods.

   The following example stops the original destination SVM:

```
cluster_dst::> vserver stop svm_backup
```

Learn more about `vserver stop` in the ONTAP command reference.

3. Update the reversed relationship:

   `snapmirror update -source-path SVM:volume -destination-path SVM:volume`

   You must run this command from the original source SVM or the original source cluster.

   The following example updates the relationship between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror update` in the ONTAP command reference.

4. From the original source SVM or the original source cluster, stop scheduled transfers for the reversed relationship:

   `snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

   You must run this command from the original source SVM or the original source cluster.

   The following example stops scheduled transfers between the original destination volume, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror quiesce` in the ONTAP command reference.

5. When the final update is complete and the relationship indicates "Quiesced" for the relationship status, run the following command from the original source SVM or the original source cluster to break the reversed relationship::

   `snapmirror break -source-path SVM:volume -destination-path SVM:volume`

   You must run this command from the original source SVM or the source cluster.

   The following example breaks the relationship between the original destination volume, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Learn more about `snapmirror break` in the ONTAP command reference.

6. From the original source SVM or the original source cluster, delete the reversed data protection relationship:

   `snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

   You must run this command from the original source SVM or the original source cluster.

   The following example deletes the reversed relationship between the original source volume, `volA` on `svm1`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

   ```
   cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror delete` in the ONTAP command reference.

7. Release the reversed relationship from the original destination SVM or the original destination cluster.

   `snapmirror release -source-path SVM:volume -destination-path SVM:volume`

   You must run this command from the original destination SVM or the original destination cluster.

   The following example releases the reversed relationship between the original destination volume, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

   ```
   cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror release` in the ONTAP command reference.

8. Reestablish the original data protection relationship from the original destination:

   `snapmirror resync -source-path SVM:volume -destination-path SVM:volume`

   The following example reestablishes the relationship between the original source volume, `volA` on `svm1`, and the original destination volume, `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Learn more about `snapmirror resync` in the ONTAP command reference.

9. If needed, start the original destination SVM:

   `vserver start -vserver SVM`

   The following example starts the original destination SVM:

   ```
   cluster_dst::> vserver start svm_backup
   ```

   Learn more about `vserver start` in the ONTAP command reference.

After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

Learn more about `snapmirror show` in the ONTAP command reference.

Restore files from a SnapMirror destination volume

Restore a file, LUN, or NVMe namespace from an ONTAP SnapMirror destination

You can restore a single file, LUN, a set of files or LUNs from a snapshot, or an NVMe namespace from a SnapMirror destination volume. Beginning with ONTAP 9.7, you can also restore NVMe namespaces from a SnapMirror synchronous destination. You can restore files to the original source volume or to a different volume.

Before you begin

To restore a file or LUN from a SnapMirror synchronous destination (supported beginning with ONTAP 9.5), you must first delete and release the relationship.

About this task

The volume to which you are restoring files or LUNs (the destination volume) must be a read-write volume:

- SnapMirror performs an *incremental restore* if the source and destination volumes have a common snapshot (as is typically the case when you are restoring to the original source volume).
- Otherwise, SnapMirror performs a *baseline restore*, in which the specified snapshot and all the data blocks it references are transferred to the destination volume.

Steps

1. List the snapshots in the destination volume:

   `volume snapshot show -vserver <SVM> -volume volume`

   Learn more about `volume snapshot show` in the ONTAP command reference.

   The following example shows the snapshots on the `vserverB:secondary1` destination:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restore a single file or LUN or a set of files or LUNs from a snapshot in a SnapMirror destination volume:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
snapshot -file-list <source_file_path,@destination_file_path>
```

You must run this command from the destination SVM or the destination cluster.

The following command restores the files `file1` and `file2` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`, to the same location in the active file system of the original source volume `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

The following command restores the files `file1` and `file2` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`, to a different location in the active file system of the original source volume `primary1`.

The destination file path begins with the @ symbol followed by the path of the file from the root of the original source volume. In this example, `file1` is restored to `/dir1/file1.new` and file2 is restored to `/dir2.new/file2` on `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

The following command restores the files `file1` and `file3` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`, to different locations in the active file system of the original source volume `primary1`, and restores `file2` from `snap1` to the same location in the active file system of `primary1`.

In this example, the file `file1` is restored to `/dir1/file1.new` and `file3` is restored to `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Related information

- snapmirror restore

Restore volume contents from an ONTAP SnapMirror destination

You can restore the contents of an entire volume from a snapshot in a SnapMirror destination volume. You can restore the volume's contents to the original source volume or to a different volume.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to restore data. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

The destination volume for the restore operation must be one of the following:

- A read-write volume, in which case SnapMirror performs an *incremental restore*, provided that the source and destination volumes have a common snapshot (as is typically the case when you are restoring to the original source volume).

The command fails if there is not a common snapshot. You cannot restore the contents of a volume to an empty read-write volume.

- An empty data protection volume, in which case SnapMirror performs a *baseline restore*, in which the specified snapshot and all the data blocks it references are transferred to the source volume.

Restoring the contents of a volume is a disruptive operation. SMB traffic must not be running on the SnapVault primary volume when a restore operation is running.

If the destination volume for the restore operation has compression enabled, and the source volume does not have compression enabled, disable compression on the destination volume. You need to re-enable compression after the restore operation is complete.

Any quota rules defined for the destination volume are deactivated before the restore is performed. You can use the `volume quota modify` command to reactivate quota rules after the restore operation is complete.

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

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

Steps

You can restore a volume's contents using System Manager or the ONTAP CLI.

System Manager

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 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.

CLI

1. List the snapshots in the destination volume:

   ```
   volume snapshot show -vserver <SVM> -volume <volume>
   ```

   The following example shows the snapshots on the `vserverB:secondary1` destination:

   ```
   cluster_dst::> volume snapshot show -vserver vserverB -volume
   secondary1

   Vserver     Volume      Snapshot                State    Size
   Total% Used%
   -------     ------      ---------- ----------- ------   -----
   ------ -----
   vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
   0%
                           daily.2013-01-25_0010   valid   92KB      0%
   0%
                           hourly.2013-01-25_0105  valid   228KB     0%
   0%
                           hourly.2013-01-25_0205  valid   236KB     0%
   0%
                           hourly.2013-01-25_0305  valid   244KB     0%
   0%
                           hourly.2013-01-25_0405  valid   244KB     0%
   0%
                           hourly.2013-01-25_0505  valid   244KB     0%
   0%

   7 entries were displayed.
   ```

2. Restore the contents of a volume from a snapshot in a SnapMirror destination volume:

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
   ```

`<snapshot>`

> You must run this command from the original source SVM or the original source cluster.

The following command restores the contents of the original source volume `primary1` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than snapshot daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Remount the restored volume and restart all applications that use the 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 restore using SnapVault overview

Related information

- snapmirror restore
- volume snapshot show

Update an ONTAP SnapMirror replication relationship manually

You might need to update a replication relationship manually if an update fails because the source volume has been moved.

About this task

SnapMirror aborts any transfers from a moved source volume until you update the replication relationship manually.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported. Although the source and destination volumes are in sync at all times in these relationships, the view from the secondary cluster is synchronized with the primary only on an hourly basis. If you want to view the point-in-time data at the destination, you should perform a manual update by running the `snapmirror update` command.

Step

1. Update a replication relationship manually:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

> You must run this command from the destination SVM or the destination cluster. The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship. Learn more about `snapmirror initialize` in the ONTAP command reference.

The following example updates the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror update` in the ONTAP command reference.

Resynchronize an ONTAP SnapMirror replication relationship

You need to resynchronize a replication relationship after you make a destination volume writeable, after an update fails because a common snapshot does not exist on the source and destination volumes, or if you want to change the replication policy for the 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.

> System Manager does not support reverse resynchronization with intracluster relationships. You can use the ONTAP CLI to perform reverse resync operations with intracluster relationships.

About this task

- Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.
- Volumes that are part of a fan-out or cascade configuration can take longer to resynchronize. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.
- Beginning with ONTAP 9.13.1, ONTAP attempts to use quick-resync by default to reduce resync time. The following conditions must be present for quick-resync to be used by default:
  - FlexVol volumes have no clones on the volume
  - When using the MirrorAllSnapshots policy

Using `-quick-resync` can consume additional space on the resync destination volume due to removal of storage efficiency on transferred data blocks. This additional space consumption is recovered as part of the inline or post-replication storage efficiency application on the resync destination.

The `-quick-resync` parameter is optional. You can enable or disable quick-resync by using the `-quick-resync true|false` parameter with the `snapmirror resync` command.

For more information about `-quick-resync`, see the ONTAP command reference.

Steps

You can use System Manager or the ONTAP CLI to perform this task. If you use the ONTAP CLI, the procedure is the same regardless of whether you are making a destination volume writable or you are updating the replication relationship.

System Manager reverse resync

After you break a relationship to make a destination writable, reverse resynchronize the relationship:

1. On the destination cluster, click **Protection > Relationships**.
2. Hover over the broken off relationship you want to reverse, click ⋮, and select **Reverse Resync**.
3. In the **Reverse resync relationship** window, click **Reverse resync**.
4. Under **Relationships**, monitor the reverse resynchronization progress by viewing **Transfer Status** for the relationship.

Next steps

When the original source is available again, you can reestablish the original relationship by breaking the reversed relationship and performing another reverse resync operation. The reverse resync process will copy any changes from the site that is serving data to the original source and make the original source read-writable again.

System Manager resync

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

CLI

1. Resync the source and destination volumes:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

ⓘ You must run this command from the destination SVM or the destination cluster.

The following example resynchronizes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror resync` in the ONTAP command reference.

Related information

- Resynchronize the data on an ONTAP SnapMirror destination SVM

Delete an ONTAP SnapMirror volume replication relationship

You can use the `snapmirror delete` and `snapmirror release` commands to delete a volume replication relationship. You can then delete unneeded destination volumes manually.

About this task

The `snapmirror release` command deletes any SnapMirror-created snapshots from the source. You can use the `-relationship-info-only` option to preserve the snapshots.

Steps

1. Quiesce the replication relationship:

   `snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>`

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   Learn more about `snapmirror quiesce` in the ONTAP command reference.

2. (Optional) Break the replication relationship if you require the destination volume to be a read/write volume. You can skip this step if you plan to delete the destination volume or if you don't need the volume to be read/write:

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, …`
   `-destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

   Learn more about `snapmirror break` in the ONTAP command reference.

3. Delete the replication relationship:

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, …`
   `-destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   You must run this command from the destination cluster or destination SVM.

   The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   Learn more about `snapmirror delete` in the ONTAP command reference.

4. Release replication relationship information from the source SVM:

   ```
   snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   You must run this command from the source cluster or source SVM.

   The following example releases information for the specified replication relationship from the source SVM `svm1`:

   ```
   cluster_src::> snapmirror release -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   Learn more about `snapmirror release` in the ONTAP command reference.

Manage storage efficiency on ONTAP SnapMirror volumes

SnapMirror preserves storage efficiency on the source and destination volumes except when postprocess data compression is enabled on the destination volume. In that case, all storage efficiency is lost on the destination volume. To correct this issue, you need to disable postprocess compression on the destination volume, update the relationship manually, and re-enable storage efficiency.

About this task

You can use the `volume efficiency show` command to determine whether efficiency is enabled on a volume.
Learn more about `volume efficiency show` in the ONTAP command reference.

You can check if SnapMirror is maintaining storage efficiency by viewing the SnapMirror audit logs and locating the transfer description. If the transfer description displays `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror is maintaining storage efficiency. If the transfer description displays `transfer_desc=Logical Transfer`, SnapMirror is not maintaining storage efficiency. For example:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Before you begin

- The source and destination clusters and SVMs must be peered.

  Cluster and SVM peering

- You must disable postprocess compression on the destination volume.

- Logical Transfer with storage: Beginning with ONTAP 9.3, manual update is no longer required to re-enable storage efficiency. If SnapMirror detects that postprocess compression has been disabled, it automatically re-enables storage efficiency at the next scheduled update. Both the source and the destination must be running ONTAP 9.3.
- Beginning with ONTAP 9.3, AFF systems manage storage efficiency settings differently from FAS systems after a destination volume is made writeable:
  - After you make a destination volume writeable using the `snapmirror break` command, the caching policy on the volume is automatically set to `auto` (the default).

    This behavior is applicable to FlexVol volumes, only, and it does not apply to FlexGroup volumes.

    Learn more about `snapmirror break` in the ONTAP command reference.

  - On resync, the caching policy is automatically set to `none`, and deduplication and inline compression are automatically disabled, regardless of your original settings. You must modify the settings manually as needed.

Manual updates with storage efficiency enabled can be time-consuming. You might want to run the operation in off-peak hours.

Steps

1. Update a replication relationship and re-enable storage efficiency:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

You must run this command from the destination SVM or the destination cluster. The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship. Learn more about `snapmirror initialize` in the ONTAP command reference.

The following example updates the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`, and re-enables storage efficiency:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

Learn more about `snapmirror update` in the ONTAP command reference.

Use ONTAP SnapMirror global throttling

Global network throttling is available for all SnapMirror and SnapVault transfers at a per-node level.

About this task

SnapMirror global throttling restricts the bandwidth used by incoming and/or outgoing SnapMirror and SnapVault transfers. The restriction is enforced cluster wide on all nodes in the cluster.

For example, if the outgoing throttle is set to 100 MBps, each node in the cluster will have the outgoing bandwidth set to 100 MBps. If global throttling is disabled, it is disabled on all nodes.

Although data transfer rates are often expressed in bits per second (bps), the throttle values must be entered in kilobytes per second (KBps).

> In ONTAP 9.9.1 and earlier releases, the throttle has no effect on `volume move` transfers or load-sharing mirror transfers. Beginning with ONTAP 9.10.0, you can specify an option to throttle a volume move operation. For details, see How to throttle volume move in ONTAP 9.10 and later.

Global throttling works with the per-relationship throttle feature for SnapMirror and SnapVault transfers. The per-relationship throttle is enforced until the combined bandwidth of per-relationship transfers exceeds the value of the global throttle, after which the global throttle is enforced. A throttle value `0` implies that global throttling is disabled.

> SnapMirror global throttling has no effect on SnapMirror synchronous relationships when they are In-Sync. However, the throttle does effect SnapMirror synchronous relationships when they perform an asynchronous transfer phase such as an initialization operation or after an Out Of Sync event. For this reason, enabling global throttling with SnapMirror synchronous relationships is not recommended.

Steps

1. Enable global throttling:

   `options -option-name replication.throttle.enable on|off`

   The following example shows how to enable SnapMirror global throttling on `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Specify the maximum total bandwidth used by incoming transfers on the destination cluster:

   `options -option-name replication.throttle.incoming.max_kbs <KBps>`

   The recommended minimum throttle bandwidth is 4 kilobytes per second (KBps) and the maximum is up to 2 terabytes per second (TBps). The default value for this option is `unlimited`, which means there is no limit on total bandwidth used.

   The following example shows how to set the maximum total bandwidth used by incoming transfers to 100 megabits per second (Mbps):

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

100 megabits per second (Mbps) = 12500 kilobytes per second (KBps)

3. Specify the maximum total bandwidth used by outgoing transfers on the source cluster:

   `options -option-name replication.throttle.outgoing.max_kbs <KBps>`

   The recommended minimum throttle bandwidth is 4 KBps and the maximum is up to 2 TBps. The default value for this option is `unlimited`, which means there is no limit on total bandwidth used. Parameter values are in kilobytes per second (KBps).

   The following example shows how to set the maximum total bandwidth used by outgoing transfers to 100 Mbps:

   ```
   cluster_src::> options -option-name
   replication.throttle.outgoing.max_kbs 12500
   ```