



SnapMirror volume replication

ONTAP 9

NetApp
September 18, 2024

This PDF was generated from <https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html> on September 18, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- SnapMirror volume replication 1
 - SnapMirror asynchronous disaster recovery basics 1
 - SnapMirror synchronous disaster recovery basics 3
 - About workloads supported by StrictSync and Sync policies. 8
 - Vault archiving using SnapMirror technology 8
 - SnapMirror unified replication basics 10
 - XDP replaces DP as the SnapMirror default 12
 - When a destination volume grows automatically 14
 - Fan-out and cascade data protection deployments 14
 - SnapMirror licensing 17
 - DPO systems feature enhancements 19

SnapMirror volume replication

SnapMirror asynchronous disaster recovery basics

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.

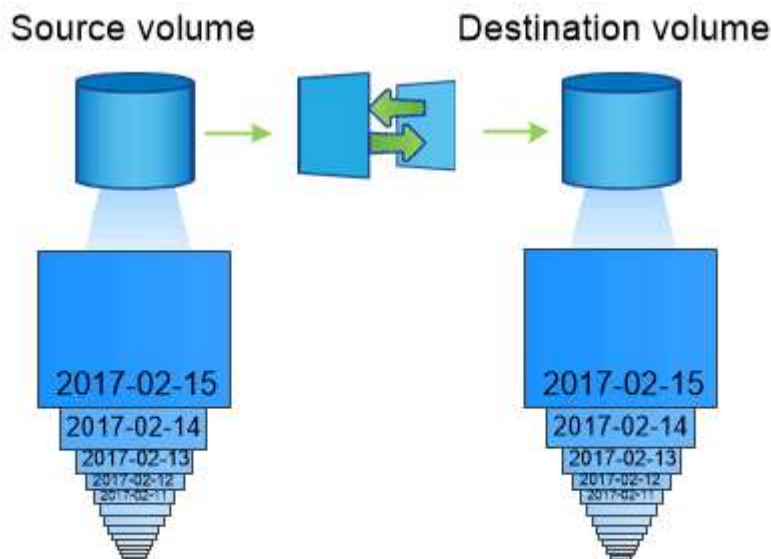
If the primary site is still available to serve data, you can simply transfer any needed data back to it, and not serve clients from the mirror at all. As the failover use case implies, the controllers on the secondary system should be equivalent or nearly equivalent to the controllers on the primary 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.

Cluster and SVM peering

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

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 copy of the source volume and transfers that Snapshot copy and any Snapshot copies 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 copy when SnapMirror updates the relationship.
- `MirrorAllSnapshots` has rules “`sm_created`” and “`all_source_snapshots`”, indicating that both the Snapshot copy created by SnapMirror and any Snapshot copies 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 copy created by SnapMirror is transferred at initialization and update.

```

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

```

SnapMirror synchronous disaster recovery basics

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

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 copy replication	ONTAP 9.7	If a Snapshot copy is tagged with the appropriate label at the time of the <code>snapshot create</code> operation, using the CLI or the ONTAP API, SnapMirror synchronous replicates the Snapshot copies, both user created or those created with external scripts, after quiescing the applications. Scheduled Snapshot copies created using a Snapshot policy are not replicated. For more information about replicating application-created Snapshot copies, see the Knowledge Base article: 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 Snapshot copies	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 v4.3	ONTAP 9.5	
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	<p>* 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.</p> <p>* 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.</p> <p>* 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.</p>
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:

- 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 Snapshot copies
- 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](#)

About workloads supported by 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

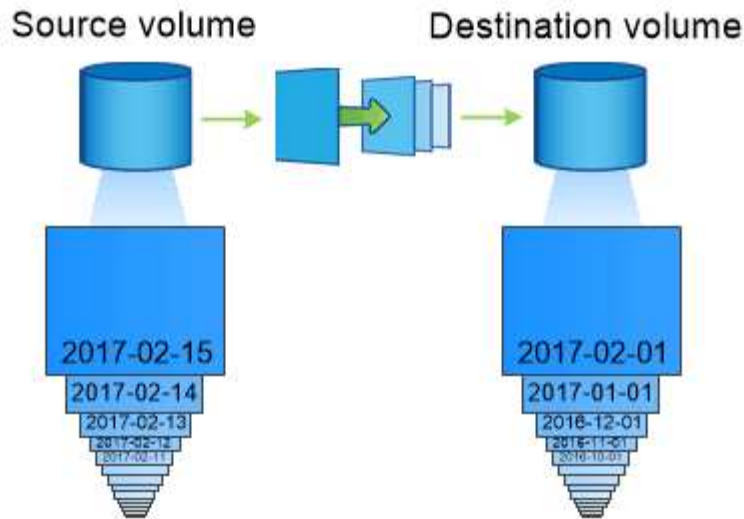
[SnapMirror synchronous Configuration and Best Practices](#)

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

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

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 copy 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 Snapshot copies 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 Snapshot copies to include in updates and how many copies to retain. The labels defined in the policy (“monthly,” for example) must match one or more labels defined in the Snapshot policy on the source. Otherwise, replication fails.

At each update under the `XDPDefault` policy, SnapMirror transfers Snapshot copies 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 copy when SnapMirror updates the relationship.
- `XDPDefault` has rules “daily” and “weekly”, indicating that all Snapshot copies 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 -
-
```

SnapMirror unified replication basics

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 copy 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 Snapshot copies in the baseline.

How unified data protection relationships are updated

At each update under the `MirrorAndVault` policy, SnapMirror creates a Snapshot copy of the source volume and transfers that Snapshot copy and any Snapshot copies 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 copy when `SnapMirror` updates the relationship.
- `MirrorAndVault` has rules “sm_created”, “daily”, and “weekly”, indicating that both the Snapshot copy created by `SnapMirror` and the Snapshot copies 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 Snapshot copies and retains them for seven years.

Schedule Prefix	Rules: SnapMirror Label	Keep	Preserve	Warn
-----	-----	----	-----	----
-	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 copy created by SnapMirror at initialization. At each update, SnapMirror creates another Snapshot copy of the source and transfers that Snapshot copy and any new Snapshot copies that have labels matching the labels defined in the Snapshot policy rules.

You can protect against the possibility that an updated Snapshot copy is corrupted by creating a copy of the last transferred Snapshot copy 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 Snapshot copies of database transaction logs, for example.

XDP replaces DP as the SnapMirror default

Beginning with ONTAP 9.3, SnapMirror extended data protection (XDP) mode replaces SnapMirror data protection (DP) mode as the SnapMirror default.

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. For more information, see [Convert an existing DP-type relationship to XDP](#).

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. Beginning with ONTAP 9.5, MirrorAndVault is the new default policy when no data protection mode is specified or when XDP mode is specified as the relationship type. 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	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 old 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.

When a 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:

- FAS6220, default DP volume max-autosize = 70TB
- FAS8200, default DP volume max-autosize = 100TB

For more information, see [NetApp Hardware Universe](#).

Fan-out and cascade data protection 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; however, SnapMirror synchronous relationships (supported beginning with ONTAP 9.5) support only fan-out deployments with one or more SnapMirror asynchronous relationships and do not support cascade deployments. 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 active sync](#) (supported beginning with ONTAP 9.3.1) 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.

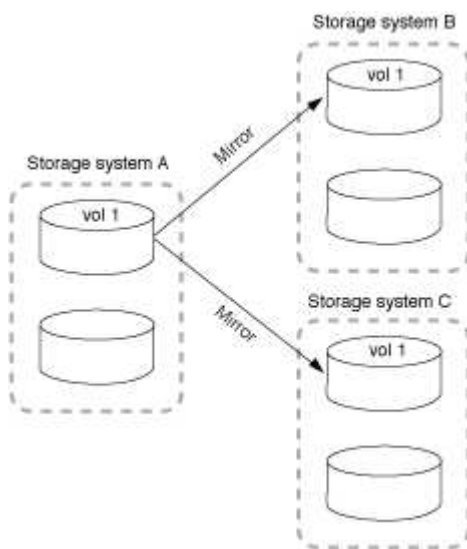


You should be aware that volumes that are part of a fan-out or cascade configuration can take longer to resynchronize. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

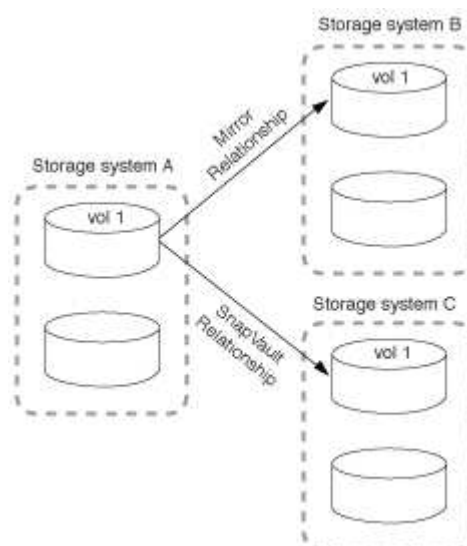
How fan-out deployments work

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

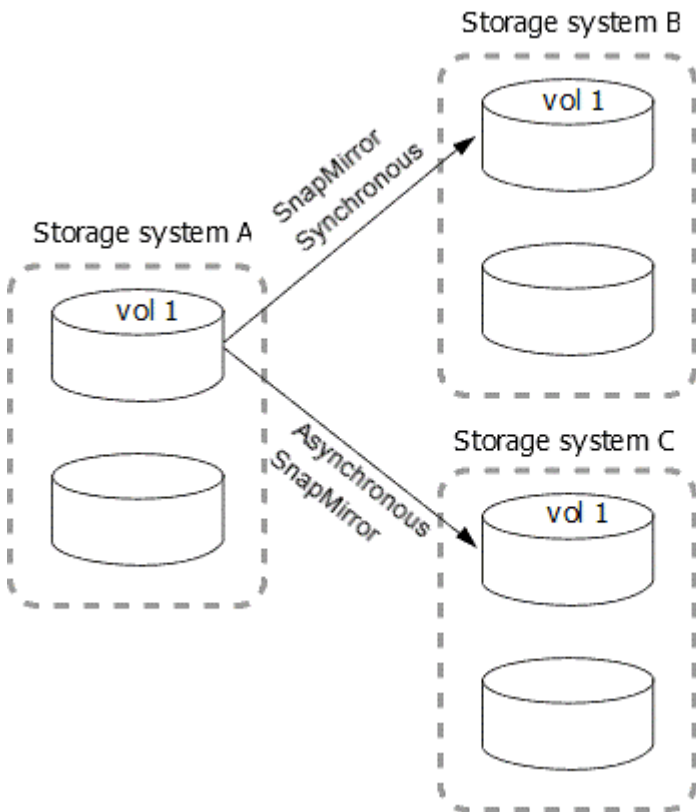
A multiple-mirrors fan-out deployment consists of a source volume that has a mirror relationship to multiple secondary volumes.



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.

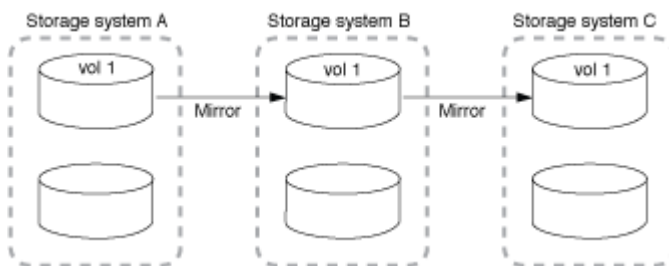


How cascade deployments work

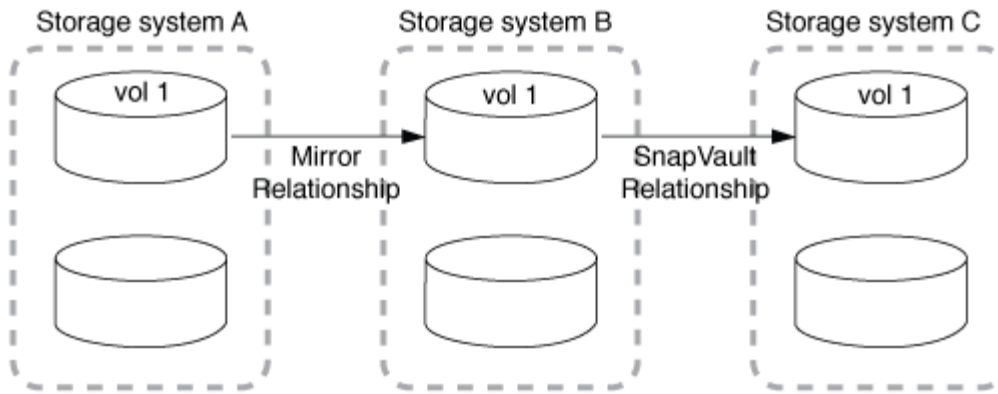
SnapMirror supports *mirror-mirror*, *mirror-vault*, *vault-mirror*, and *vault-vault* cascade deployments.

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.

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, beginning with ONTAP 9.2, 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.
- (Beginning with ONTAP 9.2) 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.

Further Reading

- [Resume protection in a fan-out configuration with SnapMirror active sync](#)

SnapMirror licensing

SnapMirror licensing overview

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 Snapshot copies 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 Snapshot copies (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 Snapshot copies 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](#).

Install SnapMirror cloud licenses

SnapMirror cloud relationships can be orchestrated using pre-qualified third-party backup

applications. Beginning with ONTAP 9.9.1, you can also use System Manager to orchestrate SnapMirror cloud replication. Both SnapMirror and SnapMirror cloud capacity licenses are required when using System Manager to orchestrate on-premises ONTAP to object storage backups. You will also need to request and install the SnapMirror cloud API license.

About this task

The SnapMirror cloud and SnapMirror S3 licenses are cluster licenses, not node licenses, so they are *not* delivered with the ONTAP One license bundle. These licenses are included in the separate ONTAP One Compatibility bundle. If you want to enable SnapMirror cloud, you need to request this bundle.

Additionally, System Manager orchestration of SnapMirror cloud backups to object storage requires a SnapMirror cloud API key. This API license is a single-instance cluster-wide license, meaning it does not need to be installed on every node in the cluster.

Steps

You need to request and download the ONTAP One Compatibility bundle and the SnapMirror cloud API license and then install them using System Manager.

1. Locate and record the cluster UUID for the cluster you want to license.

The cluster UUID is required when you submit your request to order the ONTAP One Compatibility bundle for your cluster.

2. Contact your NetApp sales team and request the ONTAP One Compatibility bundle.
3. Request the SnapMirror cloud API license by following the instructions provided on the NetApp Support Site.

[Request SnapMirror cloud API license key](#)

4. When you've received and downloaded the license files, use System Manager to upload the ONTAP Cloud Compatibility NLF and the SnapMirror cloud API NLF to the cluster:
 - a. Click **Cluster > Settings**.
 - b. In the **Settings** window, click **Licenses**.
 - c. In the **Licenses** window, click **+ Add**.
 - d. In the **Add License** dialog box, click **Browse** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

Related information

[Back up data to the cloud using SnapMirror](#)

[NetApp Software License Search](#)

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.

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

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

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

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.