



Technical Report

Architecture and Configuration of SnapMirror on Element software

Erik Kemp, NetApp
September 2018 | TR-4651

Abstract

This document outlines the architecture and configuration of NetApp® SnapMirror® technology when you use NetApp Element® software.

TABLE OF CONTENTS

| | | |
|-----------|---|-----------|
| 1 | Executive Summary | 4 |
| 2 | SnapMirror Technology | 4 |
| 2.1 | Components of a Mirror Relationship | 5 |
| 3 | Architecture Overview | 5 |
| 3.1 | Functionality of Element SnapMirror Replication to ONTAP | 6 |
| 3.2 | Management in the Element UI | 7 |
| 3.3 | Management in OnCommand System Manager | 7 |
| 3.4 | Uses and Benefits of Element SnapMirror replication | 7 |
| 3.5 | SnapMirror for Disaster Recovery | 8 |
| 3.6 | Data Distribution and Remote Data Access | 9 |
| 3.7 | Data Copy Offloading and Remote Disk Archiving | 9 |
| 3.8 | Architecture Flexibility | 10 |
| 3.9 | Application Testing and Development | 10 |
| 3.10 | Element with NetApp Private Storage for Cloud | 10 |
| 4 | Replication Rules | 11 |
| 4.1 | Scale Support and Limitations | 11 |
| 5 | Default Policies | 12 |
| 6 | SnapMirror Labels | 12 |
| 7 | Prerequisites for Element to ONTAP Replication | 12 |
| 8 | Support Details for Element to ONTAP Replication | 13 |
| 9 | Support Details for ONTAP to Element Replication | 14 |
| 10 | How Element SnapMirror Replication Works | 14 |
| 10.1 | Baseline Transfers | 14 |
| 10.2 | Incremental Transfers | 14 |
| 10.3 | Resynchronization | 15 |
| 10.4 | Workflow for SnapMirror Replication from Element to ONTAP | 15 |
| 10.5 | Workflow for SnapMirror Replication from ONTAP to Element | 15 |
| 10.6 | SnapMirror Configuration Options | 18 |
| 10.7 | Transfer from Element to ONTAP | 24 |
| 10.8 | Transfer from ONTAP to Element | 25 |
| 11 | Element to ONTAP Workflow | 25 |
| 11.1 | Volume Disaster Recovery Workflow | 26 |

| | |
|--|-----------|
| 11.2 Reactivating the Original Source Volume | 27 |
| 12 Throttling SnapMirror Replication | 28 |
| 12.1 Bandwidth Throttling | 28 |
| 13 Scheduling | 28 |
| 14 Basic Troubleshooting | 29 |
| 14.1 Transfer Interruption | 29 |
| 14.2 Connectivity Issues | 29 |
| 14.3 Configuration Issues | 30 |
| 15 Summary..... | 30 |
| Where to Find Additional Information | 30 |
| Version History | 31 |

LIST OF TABLES

| | |
|---|----|
| Table 1) SnapMirror policies and policy behavior. | 12 |
| Table 2) Support details for Element to ONTAP replication. | 13 |
| Table 3) Support details for ONTAP to Element replication. | 14 |
| Table 4) ONTAP throttling. | 28 |
| Table 5) Types of ONTAP Snapshot schedules..... | 29 |

LIST OF FIGURES

| | |
|---|----|
| Figure 1) SnapMirror data protection relationship. | 5 |
| Figure 2) Element SnapMirror replication to ONTAP. | 5 |
| Figure 3) Element DR to an ONTAP backup repository. | 9 |
| Figure 4) Element with NPS for Cloud. | 11 |
| Figure 5) Enable SnapMirror feature. | 19 |
| Figure 6) Create a SnapMirror endpoint. | 19 |
| Figure 7) Enable SnapMirror on an Element volume. | 21 |
| Figure 8) Snapshot copies created by SnapMirror. | 22 |
| Figure 9) Create Snapshot schedule. | 23 |
| Figure 10) SnapMirror replication from Element to ONTAP. | 25 |
| Figure 11) ONTAP SnapMirror failback to Element. | 25 |
| Figure 12) SnapMirror replication from Element to ONTAP. | 26 |
| Figure 13) SnapMirror volume disaster recovery workflow | 27 |

1 Executive Summary

Stored data is susceptible to disaster, through either hardware failure or environmental catastrophe. If something happens to the primary set of data, you can use mirroring technology to create an identical second set of data to replace the primary set.

NetApp® SolidFire® and NetApp HCI integration with NetApp SnapMirror® technology allows data mobility between NetApp Element® software and NetApp ONTAP® systems, enabling ONTAP customers to integrate Element into their existing data protection infrastructure. This integration builds on the NetApp Data Fabric and further connects Element into the broader data architecture that customers are building with NetApp's portfolio of products. The Data Fabric is the central tenet of NetApp's vision for data management, by which data in many forms with various requirements can be managed and migrated agilely as access and protection needs increase over time. SnapMirror integration also expands data protection and disaster recovery (DR) solutions for NetApp HCI and SolidFire customers by enabling NetApp AFF and FAS systems to serve as cost-effective DR targets for Element environments. The ability to use hybrid and disk-based FAS systems introduces new cost-effective DR options for all-flash, NetApp HCI and SolidFire products.

This document provides an architectural overview for enabling a collaborative replication and DR solution with SnapMirror between Element and ONTAP.

The Element and ONTAP teams jointly developed this architecture to enable SnapMirror deployments across heterogeneous storage architectures that provide superior data and application availability.

Mirroring is one of several methods for increasing data availability if hardware, software, or even site failures occur. SnapMirror technology offers a fast and flexible enterprise solution for mirroring or replicating data over LANs and WANs. SnapMirror is a key component in enterprise data protection strategies.

2 SnapMirror Technology

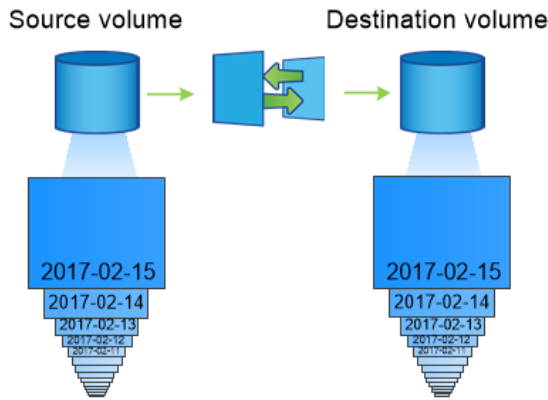
SnapMirror is a NetApp Snapshot™ replication technology that facilitates DR, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror technology creates a replica, or mirror, of the working data in secondary storage from which you can continue to serve data if an outage occurs at the primary site.

Data is mirrored at the volume level. The relationship between the source volume in primary storage and the destination volume in secondary storage is called a data protection relationship. The clusters (referred to as endpoints) in which the volumes reside and the volumes that contain the replicated data must be peered. A peer relationship enables clusters and volumes to exchange data securely.

SnapMirror runs natively on the NetApp ONTAP controllers and now is integrated into Element, which runs on NetApp HCI and SolidFire clusters. The logic to control SnapMirror resides in ONTAP software; therefore, all SnapMirror relationships must involve at least one ONTAP system to perform the coordination work. Users manage relationships between Element and ONTAP clusters primarily through the Element UI; however, some management tasks reside in NetApp OnCommand® System Manager. Users can also manage SnapMirror through the CLI and API, which are both available in ONTAP and Element.

Figure 1 illustrates the SnapMirror data protection relationship.

Figure 1) SnapMirror data protection relationship.



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

2.1 Components of a Mirror Relationship

In its simplest configuration, a mirror relationship is the relationship between a source volume and a destination volume. Data is replicated to the destination volume through NetApp Snapshot copies.

Typically, the source volume is a read/write volume that clients can access and modify. The destination volume is a read-only volume that can export a Snapshot copy to clients for read-only access.

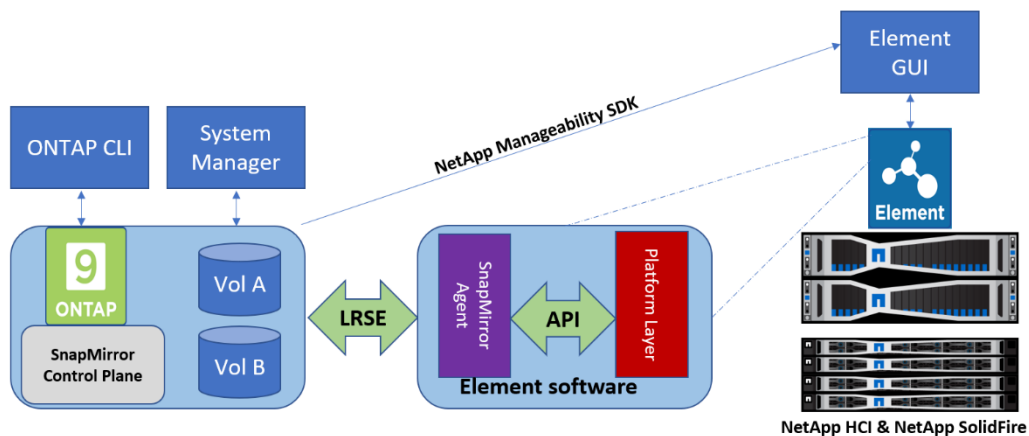
Snapshot copies are used by the source volume to update destination volumes. Snapshot copies are transferred from the source volume to the destination volume through an automated or manual schedule; therefore, mirror copies are updated asynchronously.

3 Architecture Overview

This section details the architecture of NetApp SnapMirror replication between NetApp Element and NetApp ONTAP.

Figure 2 illustrates the SnapMirror relationship between Element and ONTAP.

Figure 2) Element SnapMirror replication to ONTAP.



3.1 Functionality of Element SnapMirror Replication to ONTAP

As of Element 10.3 and ONTAP 9.4 software, Element SnapMirror replication to ONTAP supports the following functionalities:

Note: Applies to all Element-based products: NetApp HCI and SolidFire all-flash array.

- SnapMirror provides support for applications to fail over to a secondary volume and continue operating. It also can fail back to the primary location later. This capability is sometimes referred to as DR.
- Block Snapshot copies can be replicated from an Element source volume to an ONTAP destination volume and back.

Note: An ONTAP cluster is required as one of the endpoints.

- The following high-level features are supported:
 - Baseline and incremental transfer
 - Promotion of Element volumes to read/write to be usable on ONTAP as ONTAP logical unit numbers (LUNs)
 - CLI and API manageability through ONTAP CLI and Element API
 - GUI manageability through Element UI
 - Replication of Snapshot copies of a LUN created on an ONTAP node back to an Element system

Known Limitations

Using SnapMirror from Element to ONTAP has the following known limitations:

- No restore workflow (SnapMirror restore)
- No cascading from Element to ONTAP and ONTAP to ONTAP or NetApp Cloud Backup (formerly AltaVault™)
- No NetApp SnapCenter® orchestration
- No support for NetApp Cloud Volumes ONTAP

ONTAP 9.4 and Element 10.3 Features

ONTAP 9.4 and Element 10.3 provide the following features:

- DR from Element as a source to ONTAP as the target.
- Management of the following volume-level protection relationships:
 - Create, initialize, update, abort, modify, quiesce/resume, delete, and show
 - Mirror and vault policy
 - Asynchronous mirror policy
 - Schedule replication
 - Break or resynchronize
- ONTAP to Element (failover/failback use case):
 - Create, initialize, update, abort, modify, quiesce/resume, delete, and show
 - Asynchronous mirror policy
 - Break, and reverse resynchronize, and resynchronize
- For ONTAP to Element LUN migration (beginning with ONTAP 9.4 and Element 10.3), you can replicate Snapshot copies of a LUN created on an ONTAP node back to an Element system.
 - This migration is considered a one-time action. As a result, LUN migration is performed through the ONTAP CLI.

- After a relationship is created from the ONTAP side, the Element UI can be used to manage SnapMirror actions outlined in section 3.2, Management in the Element UI.
- Usable LUNs (by breaking mirror or by cloning Snapshot copies).
- IP redirection.

3.2 Management in the Element UI

Use the Element UI to manage the following tasks:

- Configure SnapMirror endpoints
- Set up DR replication:
 - Create and modify protection relationships
- Monitor DR replication:
 - View details of protection relationships
 - View details of individual transfers
- Control DR replication:
 - Initialize transfers
 - Update transfers
 - Pause and resume transfers
 - Break
 - Resynchronize
 - Reverse resynchronize

Note: Use the Element UI for SolidFire and NetApp HCI (different from primary NetApp HCI management tool).

3.3 Management in OnCommand System Manager

Use NetApp OnCommand System Manager software to manage the following tasks:

- Creation and management of SnapMirror policies and schedules
- SnapMirror break capability in ONTAP System Manager for a DR situation (SolidFire cluster is down)

3.4 Uses and Benefits of Element SnapMirror replication

Element SnapMirror replication use cases and benefits include:

- Integration of Element into the NetApp Data Fabric:
 - Make it easier for NetApp customers to incorporate the Element as part of their IT strategy.
 - Connect Element to customers' existing NetApp infrastructure
- Enhancing data protection options for Element customers with SnapMirror:
 - Provide lower-cost options for DR and disk-based backup.
 - Integrate with well-established NetApp tools to offer packaged data protection options.
- DR from Element to ONTAP:
 - Replicate from NetApp HCI in remote locations to AFF/FAS in a central data center.
 - Build lower-cost DR solutions from a FAS portfolio.
 - Use existing DR resources for newly added Element-based systems.
- Workload mobility and migration:
 - With the ability to send Snapshot copies between Element and ONTAP, customers can also move workloads (disruptively) between heterogeneous storage systems.

If you have both Element and ONTAP in your data center, you can move (block) volumes between them according to application need and storage resource availability to:

- Provide a bridge between ONTAP and Element.
- Provide tools to enable a better experience than off-the-shelf host-based migrations.
- Perform one-time migration of LUNs originating on ONTAP to Element (LUNs created either during DR outage or migrating to Element).

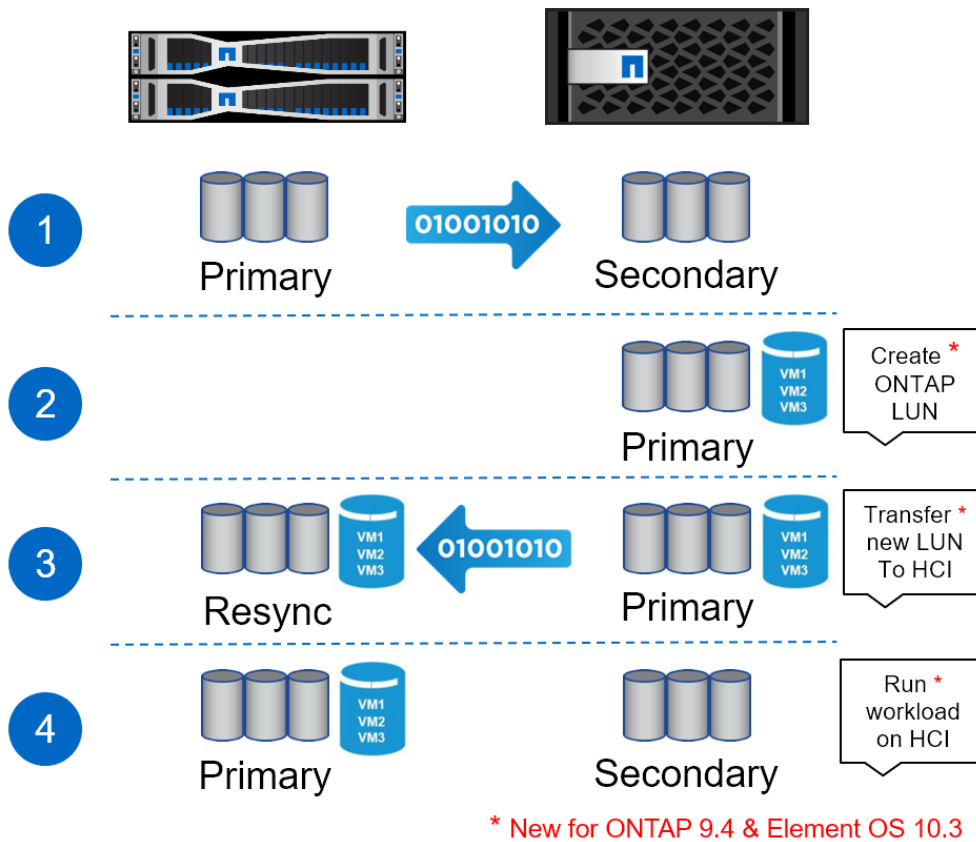
3.5 SnapMirror for Disaster Recovery

SnapMirror technology is an integral part of DR plans. If critical data is replicated to a different physical location, a serious disaster does not have to result in extended periods of unavailable data. Clients can access replicated data across the network until the damage caused by the disaster is repaired. Application servers at the recovery site can access replicated data to restore operations for business-critical applications for as long as necessary to recover the production site. Recovery might include recovery from corruption, natural disaster at the production site, accidental deletion, and so on.

If a disaster requires a failover and the primary storage is not completely lost, SnapMirror provides an efficient means of resynchronizing the primary and DR sites. When the primary site is back online, SnapMirror resynchronizes the two sites, transferring only changed or new data back to the primary site from the DR site by simply reversing the SnapMirror relationships. After the primary production site resumes normal application operations, SnapMirror transfers to the DR facility resume without requiring another complete data transfer.

Figure 3 illustrates Element Snapshot copies sent to an ONTAP destination for disaster recovery and fallback.

Figure 3) Element DR to an ONTAP backup repository.



1. Establish link and replicate.
2. Break mirror and promote ONTAP volumes.
3. Replicate back to Element.
4. Fail back to Element volumes.

3.6 Data Distribution and Remote Data Access

SnapMirror technology can be used to distribute large amounts of data throughout the enterprise, enabling access to data at remote locations. Remote data access provides faster access to data by clients in the remote locations. It also allows more efficient and predictable use of expensive network and server resources because WAN usage occurs at a predetermined replication time. Storage administrators can replicate production data at a specific time to minimize overall network utilization.

3.7 Data Copy Offloading and Remote Disk Archiving

SnapMirror technology can also be used for backup consolidation and for offloading disk backup overhead from production servers. This facilitates centralized backup operations, reducing backup administrative requirements at remote locations. Because NetApp Snapshot technology eliminates the traditional backup window on the primary storage system, offloading disk backup to a SnapMirror destination dramatically reduces the overhead of backup operations on production storage systems.

3.8 Architecture Flexibility

SnapMirror technology can be used between Element and ONTAP storage systems. This flexibility facilitates architectural design between systems with different performance characteristics and different costs, which can be deployed at the primary and DR sites. For example, depending on the capabilities required, the DR site might contain a lower-end platform or SATA disk versus solid-state drives (SSDs).

3.9 Application Testing and Development

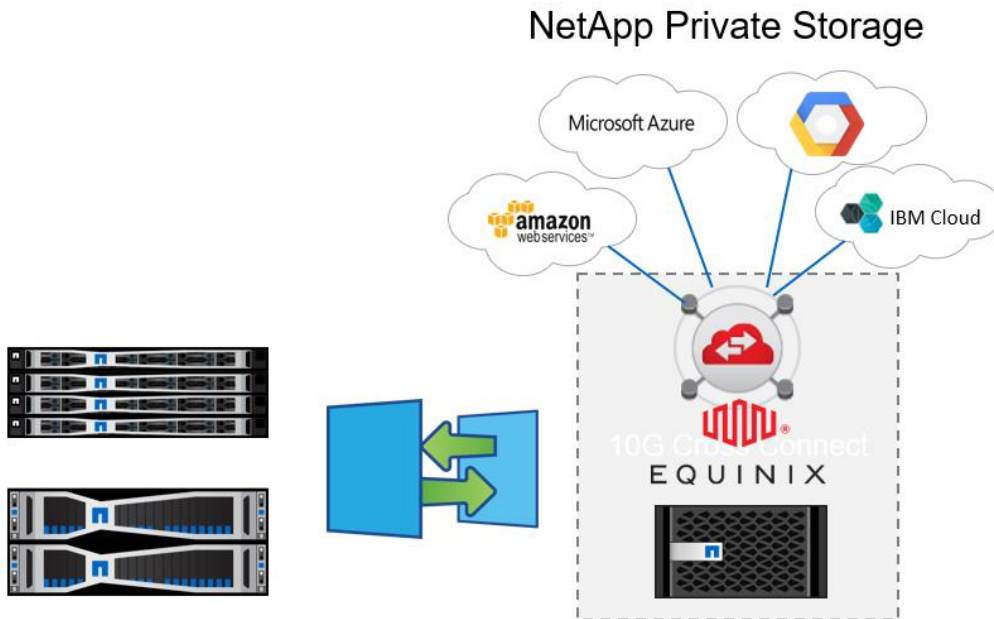
After SnapMirror has transferred data to an ONTAP system, NetApp FlexClone® technology can be used to quickly create a read/write copy of a SnapMirror destination NetApp FlexVol® volume, eliminating the need for additional copies of the data. For example, a 10GB FlexClone volume does not require another 10GB FlexClone volume; it requires only the metadata needed to define the FlexClone volume. FlexClone volumes only store data that is written or changed after a clone is created.

3.10 Element with NetApp Private Storage for Cloud

SnapMirror now enables replication of data from on-premises Element storage to an ONTAP NetApp Private Storage (NPS) solution at a colocation facility, as shown in Figure 4. Replication can also be performed between Element NPS storage and on-premises ONTAP clusters:

- Deliver cost-effective DR. Deploy cost-effective DR from premises-based workloads by activating cloud compute resources only in test and failover scenarios rather than making capital investments for compute resources.
- Use cloud resources for data center consolidation. To use colocation facilities and the public cloud as secondary and tertiary data center replacements, move workloads to NPS connected to cloud compute.
- Use cloud compute for any variable, bursty, or seasonal workload where there is also a need for data control. Match compute resources to utilization and avoid large capex investments required for peak, unforecasted, or seasonal workloads. You can meet short-term needs without overprovisioning. Pay by the hour and then turn off compute when you don't need it.
- Increase development and test agility. Use cloud compute; then run in the cloud you choose or redeploy (using SnapMirror) to your on-premises system.

Figure 4) Element with NPS for Cloud.



4 Replication Rules

An Element volume is roughly equivalent to a NetApp ONTAP LUN.

- ONTAP volumes that are replication targets for Element must contain a single LUN that serves as the container for the data being replicated from Element.
- An ONTAP volume can contain data from one Element volume only.
- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.
- For ONTAP 9.4 replication to an Element destination, the replication relationship must have a policy of type `async-mirror`. Policies of type `mirror-vault` are not supported.

Note: The `MirrorLatest` policy is not designed to support Element as a DR or backup target for ONTAP.

- An Element cluster might replicate to an ONTAP cluster through NetApp SnapMirror and other Element clusters by using the native replication features of Element. However, a specified volume might replicate to only a single endpoint (either ONTAP or Element).

4.1 Scale Support and Limitations

Scale support and limitations include the following:

- Element supports up to 30 Snapshot copies per volume for SnapMirror (the system limit is typically 32).
- ONTAP 9.3 supports up to 251 Snapshot copies (the system hard limit is 255).
- In ONTAP 9.4 and later, a destination volume can contain up to 1,019 Snapshot copies (the system hard limit is 1,023).
- SnapMirror supports a maximum of 500 protected volumes replicating from one Element cluster to ONTAP.

- SnapMirror supports a maximum of 32 SolidFire clusters replicating to a single ONTAP array. (Previously, support was 4:1.)
- SnapMirror supports a maximum of 2,000 volumes replicating to a single ONTAP array.
- You can have up to 100 concurrent transfers per SolidFire node.

5 Default Policies

The first time SnapMirror is invoked, it performs a baseline transfer from the source volume to the destination volume. You can use a default or custom policy when you create a replication relationship. The policy type determines which Snapshot copies to include and how many copies to retain. In all cases, SnapMirror creates a Snapshot copy of the source volume before initializing or updating the relationship.

Table 1 shows the default policies. Use the `MirrorLatest` policy to create a traditional DR relationship. Use the `MirrorAndVault` or `Unified7year` policy to create a unified replication relationship, in which DR and data archiving are configured on the same destination volume.

Table 1) SnapMirror policies and policy behavior.

| Policy | Policy Type | Initialization and Update Behavior |
|-----------------------------|---------------------------|--|
| <code>MirrorLatest</code> | <code>async-mirror</code> | Transfer only the Snapshot copy created by SnapMirror. |
| <code>MirrorAndVault</code> | <code>mirror-vault</code> | Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels <code>Daily</code> or <code>Weekly</code> . |
| <code>Unified7year</code> | <code>mirror-vault</code> | Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels <code>Daily</code> , <code>Weekly</code> , or <code>Monthly</code> . |

6 SnapMirror Labels

A SnapMirror label serves as a marker for transferring a specified Snapshot copy according to the retention rules of the relationship. Applying a label to a Snapshot copy marks it as a target for SnapMirror replication. The role of the relationship is to enforce the rules upon data transfer by selecting the matching labeled Snapshot copy, copying it to the destination volume, and making sure that the correct number of copies are kept. The label refers to the policy to determine the keep count and the retention period. The policy can have any number of rules, and each rule has a unique label. This label serves as the link between the Snapshot copy and the retention rule.

The SnapMirror label indicates which rule is applied for the selected Snapshot copy, group Snapshot copy, or schedule. Every policy with the `mirror-vault` policy type must have a rule that specifies which Snapshot copies to replicate. The rule `Daily`, for example, indicates that only Snapshot copies assigned the SnapMirror label `Daily` should be replicated. Assign the SnapMirror label when you configure SolidFire Snapshot copies.

7 Prerequisites for Element to ONTAP Replication

You must complete the following tasks before configuring an Element to ONTAP data protection relationship:

- NetApp SnapMirror must be licensed on the participating NetApp ONTAP cluster.
- All nodes on the Element cluster containing the volume to be replicated must be accessible to ONTAP over the network.

- The Element cluster must have the SnapMirror feature enabled.
- The Element volume must be enabled for SnapMirror replication.
- If you are using the `mirror-vault` policy type, a SnapMirror label must be configured for the Element Snapshot copies to be replicated.
- Make sure that port 5010 is available.

8 Support Details for Element to ONTAP Replication

Table 2 lists the support details for Element to ONTAP replication.

Table 2) Support details for Element to ONTAP replication.

| Resource or Feature | Support Details |
|----------------------------------|--|
| SnapMirror | <ul style="list-style-type: none"> • The SnapMirror restore feature is not supported. • The <code>MirrorAllSnapshots</code> and <code>XDPDefault</code> policies are not supported. • The <code>vault</code> policy type is not supported. • The system-defined rule <code>all_source_snapshots</code> is not supported. • The <code>mirror-vault</code> policy is supported only for replication from SolidFire to ONTAP. Use <code>async-mirror</code> for replication from ONTAP to SolidFire. • The <code>-schedule</code> and <code>-prefix</code> options for SnapMirror policy add-rule are not supported. • The <code>-preserve</code> and <code>-quick-resync</code> options for SnapMirror resynchronization are not supported. • Storage efficiency is not preserved. • Fan-out and cascade data protection deployments are not supported. |
| ONTAP | <ul style="list-style-type: none"> • Cloud Volumes ONTAP is not supported. • ONTAP Select is supported (ONTAP 9.4, Element 10.3). |
| Element | <ul style="list-style-type: none"> • Volume size limit is 8TiB. • Volume block size must be 512 bytes. A 4K byte block size is not supported for SnapMirror replication. • Volume size must be a multiple of 1MiB. • Volume attributes are not preserved. • Maximum number of Snapshot copies to be replicated is 30. |
| Network | <ul style="list-style-type: none"> • A single TCP connection is allowed per transfer. • The Element node must be specified as an IP address. DNS host name lookup is not supported. • IPspaces are not supported. |
| SnapLock | <ul style="list-style-type: none"> • NetApp SnapLock® volumes are not supported. |
| FlexGroup | <ul style="list-style-type: none"> • NetApp ONTAP FlexGroup volumes are not supported. |
| Storage virtual machine (SVM) DR | <ul style="list-style-type: none"> • ONTAP volumes in an SVM DR configuration are not supported. |

| Resource or Feature | Support Details |
|--|---|
| MetroCluster | <ul style="list-style-type: none"> NetApp MetroCluster™ is not supported as a target cluster configuration. |
| NetApp Cloud Backup (formerly AltaVault) | <ul style="list-style-type: none"> Element to ONTAP to Cloud Backup cascade relationships are not supported. Element direct replication to Cloud Backup is not supported. |

9 Support Details for ONTAP to Element Replication

Table 3 lists the support details for Element to ONTAP replication.

Table 3) Support details for ONTAP to Element replication.

| Resource or Feature | Support Details |
|------------------------|---|
| SnapMirror | <ul style="list-style-type: none"> MirrorLatest policy only |
| ONTAP | <ul style="list-style-type: none"> Cloud Volumes ONTAP is not supported. ONTAP Select is supported (ONTAP 9.4, Element 10.3). |
| Supported OS LUN types | <ul style="list-style-type: none"> VMware Linux Windows_2008 Windows_2016 Xen Hyper-V Transfer of any LUNs with unsupported OS types will fail |
| ONTAP LUN | <ul style="list-style-type: none"> ONTAP LUN must be in its own volume |
| Virtual Volumes (Wols) | <ul style="list-style-type: none"> Wols are not supported. LUN class must be set to regular. |

10 How Element SnapMirror Replication Works

10.1 Baseline Transfers

When SnapMirror is invoked the first time, it performs a baseline transfer from the source volume to the destination volume. The baseline transfer involves the following steps:

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

10.2 Incremental Transfers

After a baseline transfer is complete, SnapMirror transfers only new Snapshot copies to the mirror. After a new Snapshot copy is created on the source volume, the block-level difference between the new Snapshot copy and the last replication Snapshot copy is determined and then transferred to the

destination volume. This transfer includes other Snapshot copies that were created between the last replication Snapshot copy and the new one, if they are marked with the SnapMirror label.

Updates are asynchronous and follow the schedule configured in the SnapMirror policy. You can activate the destination volume with minimal disruption if a disaster occurs at the primary site and reactivate the source volume after service is restored.

Because SnapMirror transfers only Snapshot copies after the baseline is created, replication is fast and nondisruptive. As the failover use case implies, make sure that the FAS controllers on the NetApp ONTAP system are near-comparable equivalents to the primary Element-based system if comparable performance is the design objective.

10.3 Resynchronization

You can resynchronize data protection relationships in either direction after a failover without copying the entire volume again. If a relationship is resynchronized in the reverse direction, only new data written since the last successful synchronization Snapshot copy will be sent to the destination.

- If a common Snapshot copy (created by SnapMirror) exists between the two volumes, then it will be used for resynchronizing. (This is an incremental transfer.)
- If the baseline Snapshot copy is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume. (This is a full transfer.)

10.4 Workflow for SnapMirror Replication from Element to ONTAP

The Element SnapMirror to ONTAP workflow is as follows:

1. Write data to the Element LUN and create a Snapshot copy.
2. Do a baseline transfer to ONTAP (initialize).
3. Write more data to the Element LUN and create a Snapshot copy.
4. Do an incremental transfer to ONTAP.
5. Clone the Snapshot copies using NetApp FlexClone; mount and manually verify the contents.

10.5 Workflow for SnapMirror Replication from ONTAP to Element

Failback of Volume Originated on Element

The workflow for SnapMirror replication from ONTAP to Element is as follows:

1. Create a Snapshot copy of the ONTAP LUN.
2. Do an incremental transfer to Element.
3. Clone the Snapshot copy on Element; mount, and manually verify the contents.

Create New LUNs While Failed Over to ONTAP and Restore to Element on Failback

Starting with ONTAP 9.4, you can replicate Snapshot copies of a LUN created on an ONTAP system back to an Element volume. DR and backup with ONTAP as the source and Element as the target are not intended use cases of this solution. (Only the `MirrorLatest` policy is allowed). With the `MirrorLatest` policy, SnapMirror will copy and retain only the latest Snapshot copy from source to destination.

The following restrictions apply:

- If a SnapMirror relationship already exists between a SolidFire source and an ONTAP destination, a LUN created while you are serving data from the destination is automatically replicated when the source is reactivated.
- Otherwise, you must create and initialize a SnapMirror relationship between the ONTAP source and the SolidFire destination.

To migrate an ONTAP volume to Element through SnapMirror:

1. Create an ONTAP LUN.
2. Create a Snapshot copy of the ONTAP LUN.
3. Transfer to Element.
4. Clone the Snapshot copy on Element; mount, and manually verify its contents.

Creating a Relationship from an ONTAP Source to an Element Destination

Starting with ONTAP 9.4, you can use SnapMirror to replicate Snapshot copies of a LUN created on an ONTAP source back to an Element destination. You might be using the LUN to migrate data from ONTAP to Element.

Before You Begin

- The Element destination node must have been made accessible to ONTAP.
- The Element volume must have been enabled for SnapMirror replication.

About This Task

You must specify the Element destination path in the form `hostip:/lun/name`, where `lun` is the actual string "lun" and `name` is the name of the Element volume.

Replication rules are as follows:

- The replication relationship must have a policy of type `async-mirror`. You can use a default or custom policy.
- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

Step

1. Create a replication relationship from an ONTAP source to an Element destination:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -
destination-path hostip:/lun/name -type XDP -schedule schedule -policy
policy
```

Example

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

```
cluster_dst:> snapmirror create -source-path svm_1:volA_dst -
destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily -
policy MirrorLatest
```

Example

The following example creates a SnapMirror DR relationship using the custom `my_mirror` policy:

```
cluster_dst:> snapmirror create -source-path svm_1:volA_dst -
destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily -
policy my_mirror
```


After You Finish

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

Reactivating the Original Source Volume

Starting with ONTAP 9.4, Snapshot copies of a LUN created while you are serving data from the ONTAP destination are automatically replicated when the Element source is reactivated.

Replication rules are as follows:

- Only iSCSI LUNs are supported.
- You cannot replicate more than one LUN from an ONTAP volume to an Element volume.
- You cannot replicate a LUN from an ONTAP volume to multiple Element volumes.

Steps

1. Reverse the original data protection relationship:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume -  
destination-path hostip:/lun/name -policy policy
```

For complete command syntax, see the man page.

Although `resync` does not require a baseline transfer, it can be time consuming. You might want to run the resynchronization during off-peak hours.

Example

The following example reverses the relationship between the original source volume, `0005` at IP address `10.0.0.11`, 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 10.0.0.11:/lun/0005 -policy MirrorLatest
```

2. Update the reversed relationship:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume -  
destination-path hostip:/lun/name
```

For complete command syntax, see the man page.

The command fails if a common Snapshot copy does not exist on the source and destination. Use `snapmirror initialize` to reinitialize the relationship.

Example

The following example updates the relationship between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `0005` at IP address `10.0.0.11`:

```
cluster_src:> snapmirror update -source-path svm_backup:volA_dst -  
destination-path 10.0.0.11:/lun/0005
```

3. Stop scheduled transfers for the reversed relationship:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume -  
destination-path hostip:/lun/name
```

For complete command syntax, see the man page.

Example

The following example stops scheduled transfers between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `0005` at IP address `10.0.0.11`:

```
cluster_src:> snapmirror quiesce -source-path svm_backup:volA_dst -
```

```
destination-path 10.0.0.11:/lun/0005
```

4. Stop ongoing transfers for the reversed relationship:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume -  
destination-path hostip:/lun/name
```

For complete command syntax, see the man page.

Example

The following example stops ongoing transfers between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `0005` at IP address 10.0.0.11:

```
cluster_src:> snapmirror abort -source-path svm_backup:volA_dst -  
destination-path 10.0.0.11:/lun/0005
```

Break the reversed relationship:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume -  
destination-path hostip:/lun/name
```

For complete command syntax, see the man page.

Example

The following example breaks the relationship between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `0005` at IP address 10.0.0.11:

```
cluster_src:> snapmirror break -source-path svm_backup:volA_dst -  
destination-path 10.0.0.11:/lun/0005
```

5. Re-establish the original data protection relationship:

```
snapmirror resync -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

For complete command syntax, see the man page.

Example

The following example re-establishes the relationship between the original source volume, `0005` at IP address 10.0.0.11, and the original destination volume, `volA_dst` on `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path 10.0.0.11:/lun/0005 -  
destination-path svm_backup:volA_dst
```

After You Finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created. For complete command syntax, see the man page.

10.6 SnapMirror Configuration Options

This section describes the SnapMirror configuration options.

Setting Up the Cluster

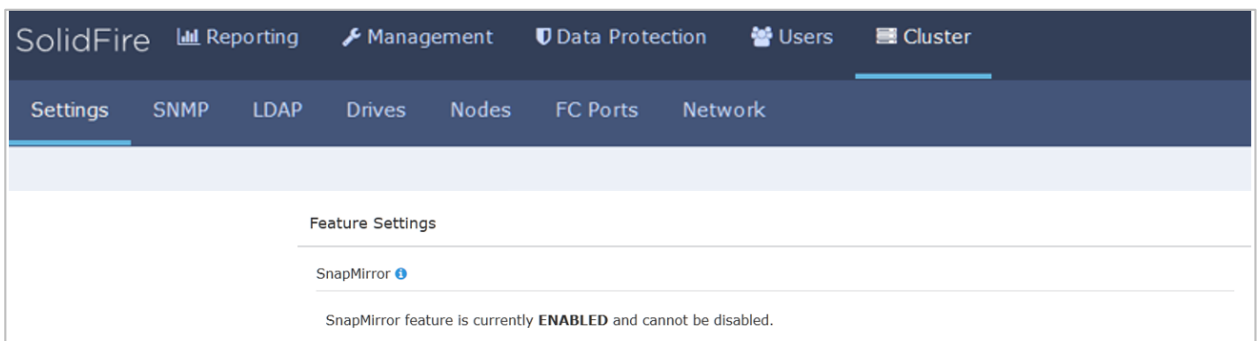
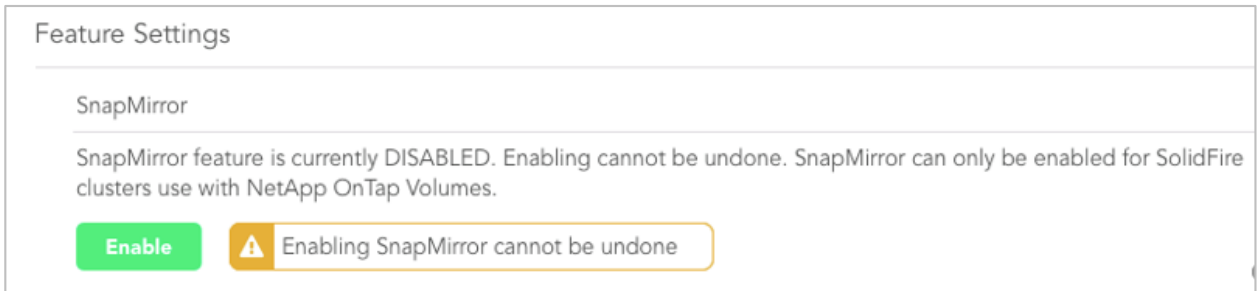
To create an Element cluster, complete the following steps:

1. Add all available drives from all nodes to the cluster.
2. Add an account.
3. If needed, get the account ID of the newly created account.
4. Create one or more volumes.

Enabling SnapMirror

1. Enable SnapMirror on the Feature Settings page.

Figure 5) Enable SnapMirror feature.



Configuring Access from the Remote ONTAP Cluster

Before any pairing can be attempted from the ONTAP cluster, Element must open its firewall to allow incoming connections on port 5010 from the ONTAP cluster's intercluster logical interfaces (LIFs).

1. Create a SnapMirror endpoint by using `CreateSnapMirrorEndpoint`.

The IP address list can be modified at any time (node removal or addition).

The Element cluster's administrator can prevent all future communication from an ONTAP cluster by deleting the endpoint.

Figure 6) Create a SnapMirror endpoint.



Create a New Endpoint
✕

Cluster Management IP

ONTAP Credentials

User Name

Password

Create Endpoint
Cancel

| ID | Cluster Name | Cluster Management IP | LIFs | Relationships | Status | Actions |
|----|--------------|-----------------------|--------------------------------|---------------|-----------|---------|
| 1 | RQD-Cluster1 | 10.117.65.205 | 10.117.81.206 10.117.81.207 | 8 | Connected | ⚙️ |

Showing 1 - 1 of 1 Snap Mirror Endpoints

Setting Up a Volume

For SnapMirror to take control of a volume (and for read/write access), the volume must be enabled for SnapMirror replication. All SnapMirror commands for a volume without SnapMirror replication enabled will fail.

Figure 7) Enable SnapMirror on an Element volume.

Create a New Volume ✕

Volume Details

Volume Name

Volume Size GB ▾ Block Size 512e 4k

Account
 ▾ [Create Account?](#)

Quality of Service

Policy
 ▾

Custom Settings

SnapMirror

Enabling SnapMirror allows the ability to replicate SolidFire data to specified ONTAP volumes.

Enable SnapMirror Mode

- You can set this property when creating a volume:
`enableSnapMirrorReplication=true`
- You can also set this property when cloning a volume:
`enableSnapMirrorReplication=true`
- You can also set this property when creating a relationship in the UI.
- A volume can be modified at any time to enable SnapMirror:
`enableSnapMirrorReplication=true`

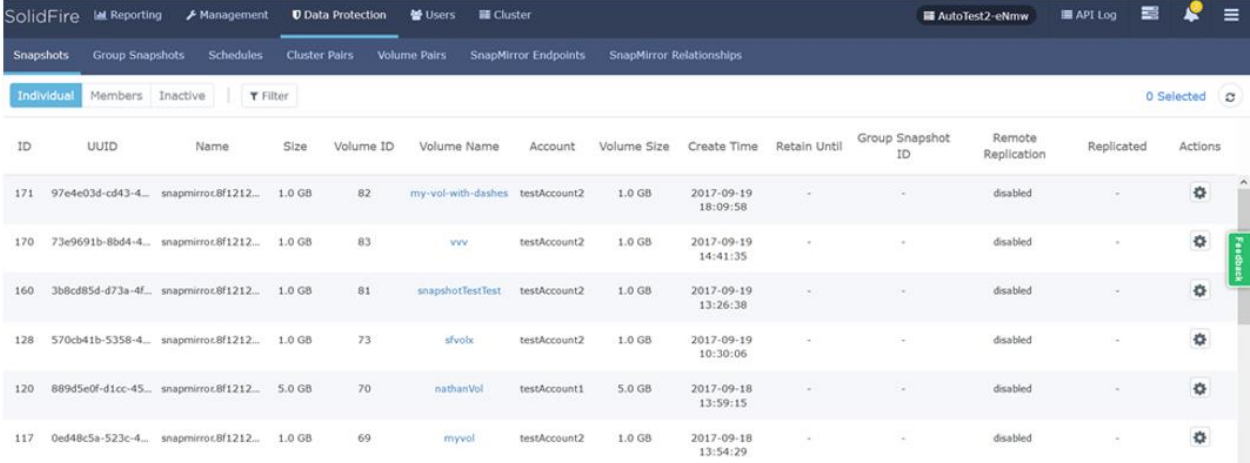
After the volume is configured to allow SnapMirror communication, use the SnapMirror CLI to create a relationship with this Element volume as the source:

```
> snapmirror create -source-path <Element SVIP>:/lun/1000 -destination-path vs1:vol2 -type xdp
```

Creating Snapshot Copies

After a relationship is established, you can assign existing policies or configure policies using NetApp OnCommand System Manager or the SnapMirror CLI. Regardless of the policy, each SnapMirror update command creates a Snapshot copy on Element to transfer to ONTAP. If the policy is a `mirror-vault` policy, you can also specify that Snapshot copies with particular labels be transferred to the ONTAP system.

Figure 8) Snapshot copies created by SnapMirror.



| ID | UUID | Name | Size | Volume ID | Volume Name | Account | Volume Size | Create Time | Retain Until | Group Snapshot ID | Remote Replication | Replicated | Actions |
|-----|---------------------|----------------------|--------|-----------|--------------------|--------------|-------------|---------------------|--------------|-------------------|--------------------|------------|---------|
| 171 | 97e4e03d-cd43-4... | snapmirror:8f1212... | 1.0 GB | 82 | my-vol-with-dashes | testAccount2 | 1.0 GB | 2017-09-19 18:09:58 | - | - | disabled | - | |
| 170 | 73e9691b-8b44-4... | snapmirror:8f1212... | 1.0 GB | 83 | vvv | testAccount2 | 1.0 GB | 2017-09-19 14:41:35 | - | - | disabled | - | |
| 160 | 3b8cd85d-473a-4f... | snapmirror:8f1212... | 1.0 GB | 81 | snapshotTestTest | testAccount2 | 1.0 GB | 2017-09-19 13:26:38 | - | - | disabled | - | |
| 128 | 570cb41b-5358-4... | snapmirror:8f1212... | 1.0 GB | 73 | sfvolx | testAccount2 | 1.0 GB | 2017-09-19 10:30:06 | - | - | disabled | - | |
| 120 | 88945e0f-d1cc-45... | snapmirror:8f1212... | 5.0 GB | 70 | nathanVol | testAccount1 | 5.0 GB | 2017-09-18 13:59:15 | - | - | disabled | - | |
| 117 | 0ed48c5a-523c-4... | snapmirror:8f1212... | 1.0 GB | 69 | myvol | testAccount2 | 1.0 GB | 2017-09-18 13:54:29 | - | - | disabled | - | |

Creating Snapshot Schedules

When combined with a `mirror-vault` policy, setting Snapshot schedules allows you to create regular Snapshot copies with a particular label. Scheduled Snapshot copies of Element volumes must be created through the Element UI or API.

Figure 9) Create Snapshot schedule.

| Frequency | Recurring | Manually Paused | Volume IDs | Last Run | Last Run Status | Actions |
|-------------|-----------|-----------------|--|----------|-----------------|---------|
| Once a Week | No | No | 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30 | - | Success | |

Create Schedule ✕

Volume IDs CSV

New Schedule Name

Schedule Type
 Recurring Schedule

Snapshot Details

New Snapshot Name

Include Snapshots in Replication When Paired

Snapshot Retention

Keep Forever
 Set Retention Period

SnapMirror

SnapMirror labels are added to mark which snapshots should be replicated in a SnapMirror relationship. Policy rules define which labels apply.

SnapMirror Label

Create Schedule ✕

Volume IDs CSV

New Schedule Name

Schedule Type
 Recurring Schedule

Snapshot Details

New Snapshot Name

Include Snapshots in Replication When Paired

Snapshot Retention

Keep Forever
 Set Retention Period

Retention Period
 Days Hours Minutes

SnapMirror

SnapMirror labels are added to mark which snapshots should be replicated in a SnapMirror relationship. Policy rules define which labels apply.

SnapMirror Label

Caution

The retention of Snapshot copies on Element cluster is completely independent of the deletion of Snapshot copies from ONTAP. The `mirror-vault` policy controls the Snapshot copy retention on ONTAP. Technically, the retention on Element only needs to be long enough for replication to DR to ONTAP to maintain a replica of that Snapshot copy. Of course, if you want to be able to restore to that Snapshot copy, it should be retained longer. Additionally, any Snapshot copies replicated to Element as part of DR failback will be controlled by the `mirror-vault` policy, because they will not have an Element retention set.

Cloning a Snapshot

You can clone Snapshot copies into new volumes by using the `CloneVolume` API method.

```
CloneVolume (volumeID=1, ...)
```

Force Snapshot Deletion

You can use the `DeleteSnapshot` method to forcefully delete a Snapshot copy that is prohibited from deletion due to the `Hold` attribute:

```
DeleteSnapshot(snapshotID=1, overrideSnapMirrorHold=true)
```

Breaking the SnapMirror Relationship

In any `SnapMirror` relationship, one volume is the source and the other is the destination. If the source volume becomes inaccessible, you might want to interrupt the transfer and make the destination volume readable and writable. To interrupt the transfer, use the break operation. If the ONTAP cluster is accessible, then the operation can be invoked with `SnapMirror` management software regardless of which side is the destination.

If an `Element` volume is the destination in a `SnapMirror` relationship and the ONTAP cluster becomes inaccessible, an `Element` administrator can break the relationship, roll back the volume to a Snapshot copy, and mount it by using the `BreakSnapMirrorVolume` method.

```
BreakSnapMirrorVolume(volumeID=1)
```

`SnapMirror` container attributes are cleared during the break operation. `SnapMirror` Snapshot attributes are not cleared.

Disabling SnapMirror Replication

At any time, an `Element` administrator can sever a `SnapMirror` relationship as long as the ONTAP system is available.

```
ModifyVolume(volumeID=1, enableSnapMirrorReplication=false)
```

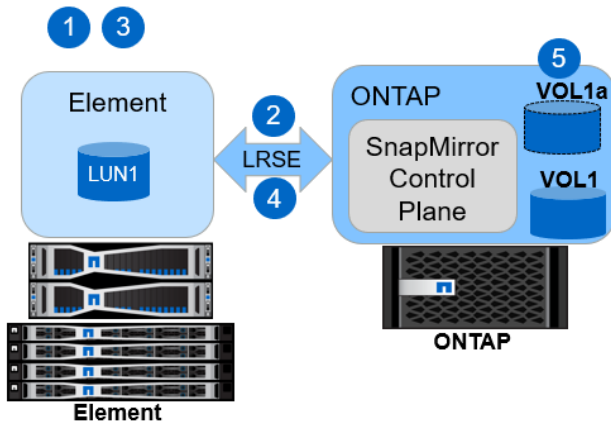
The `SnapMirror` container and Snapshot attributes are not cleared on the `Element` volume. You can resume replication by reenabling `enableSnapMirrorReplication`.

If the `Element` volume is the destination and the volume access mode is `snapMirrorTarget`, `ModifyVolume` cannot be used to make the volume read/write. You must issue `BreakSnapMirrorVolume` as described previously.

10.7 Transfer from Element to ONTAP

Figure 10 illustrates the `SnapMirror` transfers from `Element` to ONTAP.

Figure 10) SnapMirror replication from Element to ONTAP.

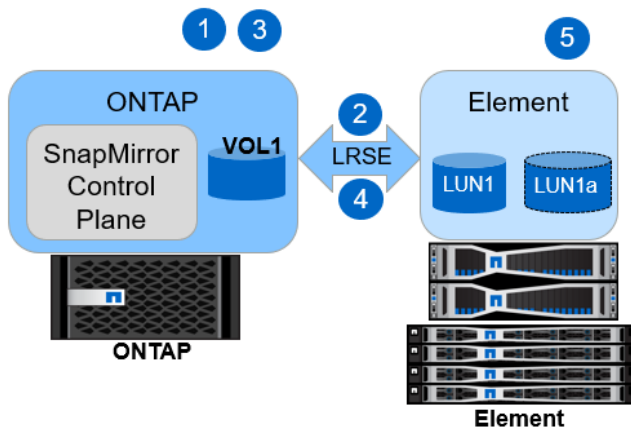


1. Write data to the Element LUN and create a Snapshot copy.
2. Perform a baseline transfer to ONTAP.
3. Write more data to the Element LUN and create another Snapshot copy.
4. Perform an incremental transfer to ONTAP.
5. Clone the Snapshot copy on ONTAP; mount and manually verify contents.

10.8 Transfer from ONTAP to Element

Figure 11 illustrates the SnapMirror transfers from ONTAP to Element.

Figure 11) ONTAP SnapMirror failback to Element.

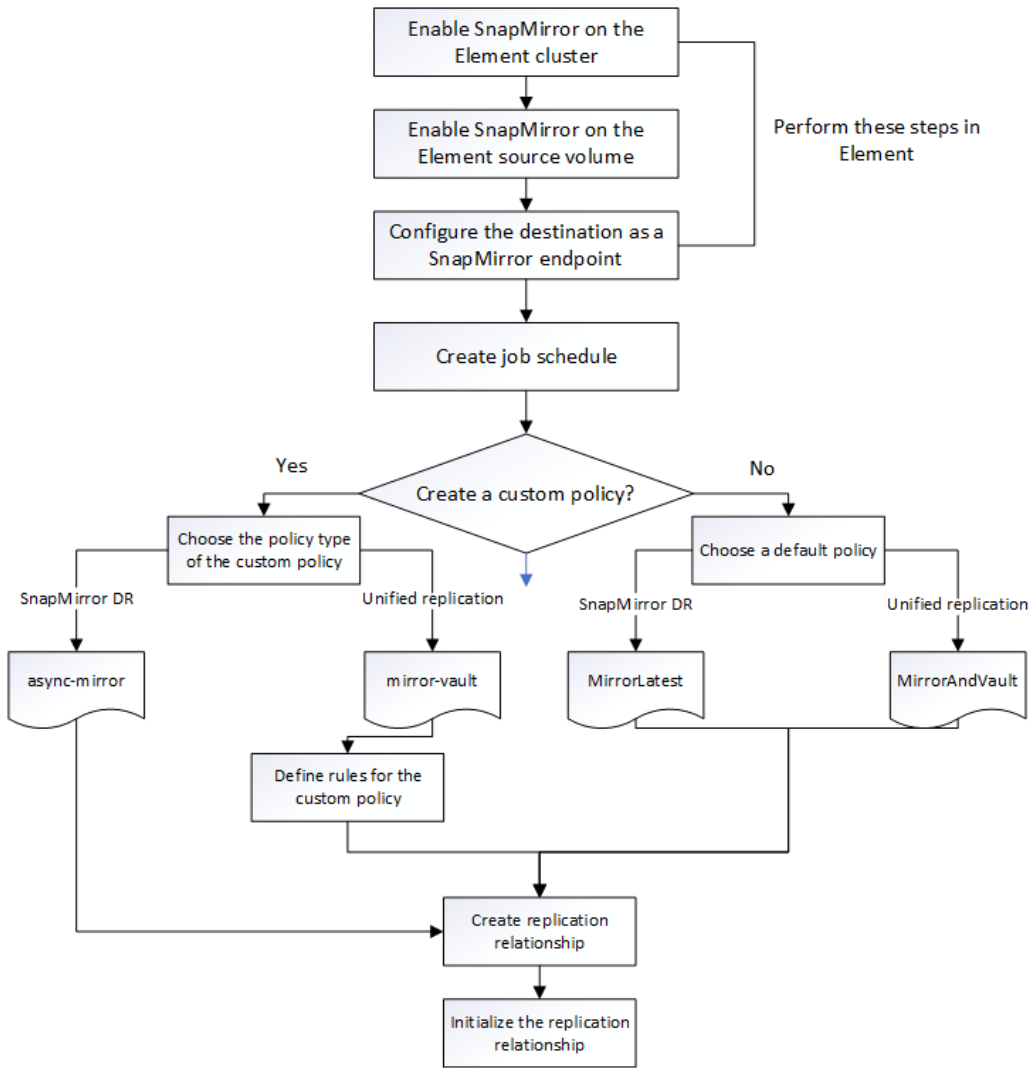


1. Write data to the ONTAP LUN and create a Snapshot copy.
2. Perform a baseline transfer to Element.
3. Write more data to the ONTAP LUN and create another Snapshot copy.
4. Perform an incremental transfer to Element.
5. Clone the Snapshot copy on Element; mount and manually verify contents.

11 Element to ONTAP Workflow

You can create a traditional DR relationship or a unified replication relationship. For each type of replication relationship, the basic workflow is the same: create a destination volume, create a job schedule, specify a policy, and create and initialize the relationship.

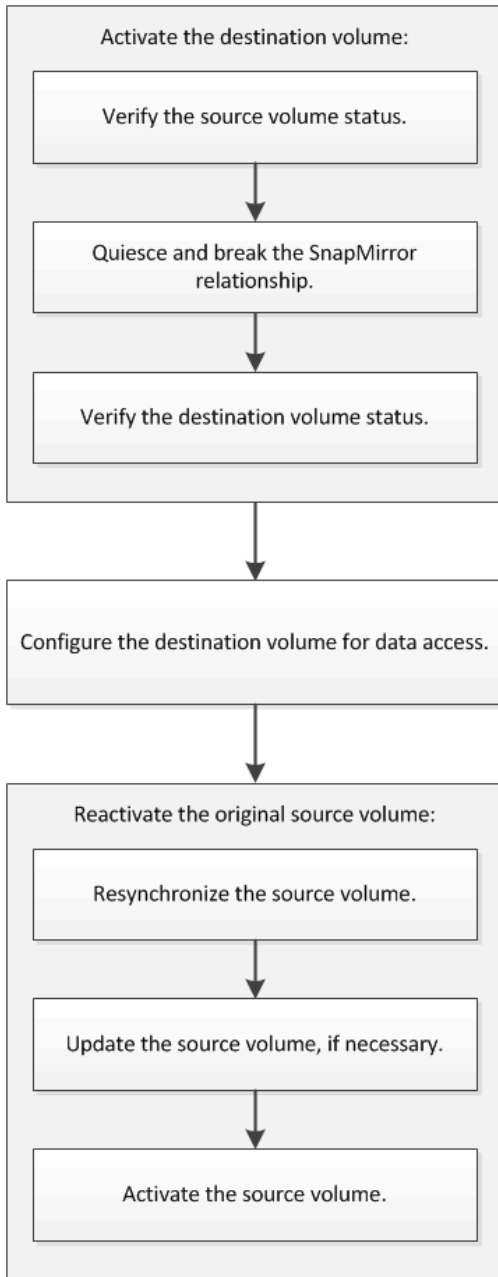
Figure 12) SnapMirror replication from Element to ONTAP.



11.1 Volume Disaster Recovery Workflow

The volume disaster recovery workflow includes activating the destination volume, configuring the destination volume for data access, and reactivating the original source volume.

Figure 13) SnapMirror volume disaster recovery workflow.



11.2 Reactivating the Original Source Volume

You can re-establish 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 following procedure assumes that the baseline in the original source volume is intact. If the baseline is not intact, before performing the procedure you must create and initialize the relationship between the volume you are serving data from and the original source volume.

You must specify the Element source path in the form *hostip:/lun/name*, where *lun* is the

actual string "lun" and *name* is the name of the Element volume.

Starting with ONTAP 9.4, if a SnapMirror relationship already exists between an Element source and an ONTAP destination, Snapshot copies of a LUN created while you are serving data from the ONTAP destination are automatically replicated when the Element source is reactivated.

12 Throttling SnapMirror Replication

Unless otherwise dictated by the user, NetApp SnapMirror consumes as much bandwidth as it can regardless of client I/O demands on the system. To limit the amount of performance resources consumed by SnapMirror, the throughput rate can be throttled at the relationship level.

12.1 Bandwidth Throttling

Bandwidth throttling can be implemented on a per-relationship basis. Throttling can be set in the Element UI or through the CLI and API. The maximum transfer rate setting controls the maximum amount of bandwidth that can be used by a given relationship. All SnapMirror reads and writes count against the allowed IOPS for an Element volume (QoS settings). If the `maxIOPS` value is exceeded, the QoS manager throttles transfers. However, it does not allow prioritization of client I/O over SnapMirror I/O. To limit the bandwidth consumed by SnapMirror transfers, you must set the `maxTransferRate` parameter on `SnapMirrorRelationship`.

You can also enable or disable throttling at the ONTAP node level to set the maximum bandwidth for outgoing transfers, the maximum bandwidth for incoming transfers, and the specified throttle value in Kbps. These options are enforced on each node in the cluster. For example, if the outgoing throttle bandwidth is set to 100Mbps for a given node, that node will have the outgoing bandwidth set to 100Mbps. When throttling is disabled, these transfers consume the entire usable bandwidth.

Table 4) ONTAP throttling.

| Type | Description |
|-------------------------------------|---|
| <code>maxTransferRate</code> | Specifies the upper bound, in Kbps, at which data is transferred. The default is unlimited (0), which permits the SnapMirror relationship to fully use the available network bandwidth. |
| <code>currentMaxTransferRate</code> | The upper bound, in Kbps, at which data is transferred for the current transfer. This value can be the same as <code>maxTransferRate</code> or different if overwritten when starting the transfer using the associated commands or APIs (<code>InitializeSnapMirrorRelationship</code> , <code>UpdateSnapMirrorRelationship</code> , <code>ModifySnapMirrorRelationship</code> , <code>ResyncSnapMirrorRelationship</code>). |

13 Scheduling

You can schedule replication hourly, daily, weekly, and monthly, and set time options to "month," "day," "day of the week," "week of the month," "hour," and "minute."

Table 5 describes the types of Snapshot copy schedules.

Table 5) Types of ONTAP Snapshot schedules.

| Type | Description |
|--------|---|
| Weekly | Weekly Snapshot copies are named weekly.n, where n is the date in year-month-day format followed by an underscore (_) and the time. For example, a weekly Snapshot copy created on 25 November 2012 is named weekly.2012-11-25_0015. |
| Daily | Daily Snapshot copies are named daily.n, where n is the date in year-month-day format followed by an underscore (_) and the time. For example, a daily Snapshot copy created on 4 December 2012 is named daily.2012-12-04_0010. |
| Hourly | Hourly Snapshot copies are named hourly.n, where n is the date in year-month-day format followed by an underscore (_) and the time. For example, an hourly Snapshot copy created on 4 December 2012 at 1:00 (1300) is named hourly.2012-12-04_1305. |

Updates are asynchronous and are based on Snapshot copies.

You can configure Snapshot replication as frequently as every 15 minutes, assuming the link to target and data change rates support this setting.

14 Basic Troubleshooting

14.1 Transfer Interruption

If a NetApp SnapMirror transfer is interrupted because of a network timeout, node failure, drive failure, or slice rebalance operation, then ONTAP restarts the transfer. There is currently no checkpointing of progress.

14.2 Connectivity Issues

If SnapMirror transfers aren't working because of connectivity problems, perform the following steps to debug:

1. Verify that you can ping each ONTAP storage LIF from each Element node and conversely.
2. If pings fail, verify the configuration.

The Element cluster uses the `SnapMirrorEndpoint` object to manage ONTAP IPs. An endpoint can be unmanaged or managed.

- **Managed.** You pass ONTAP management credentials to the `CreateSnapMirrorEndpoint` API command. The Element cluster autodiscovers ONTAP LIFs and allows them through the firewall. This mode also allows the Element web UI to perform management operations for SnapMirror workflows.
 - **Unmanaged.** You pass ONTAP LIFs to the `CreateSnapMirrorEndpoint` API command. The Element cluster opens the firewall for those IPs.
3. Run the following command on each Element node. The ONTAP LIFs should report as being allowed through the firewall. Verify that the IPs are correct.

```
u fw status
```

4. Verify that the SnapMirror agent is running and listening on the correct TCP port.

```
lsof | grep 5010
```

If the SnapMirror agent is not running, make sure that the SnapMirror feature has been enabled on the Element cluster.

<https://<MVIP>/json-rpc/10.0?method=EnableFeature&feature=SnapMirror>

`DisconnectedSnapMirrorEndpoint` is reported if any `SnapMirrorEndpoint` in the database is detected to have `isConnected` as `false`. This disconnection can be resolved by addressing the underlying connection issue with the remote cluster, or by deleting the `SnapMirrorEndpoint`.

14.3 Configuration Issues

- SnapMirror operations are blocked on the cluster until you enable the SnapMirror feature. You can enable this feature in the web UI or by using the `EnableFeature` API command.
- SnapMirror operations are blocked on a volume until you set the volume attribute `enableSnapMirrorReplication=true`. You can set this attribute with the web UI or by using the `ModifyVolume` or `CreateVolume` API command. To check if the attribute is enabled, send the API command `ListActiveVolumes`.
- Snapshot schedules and policies that use a SnapMirror label might not work properly if the attribute `snapMirrorLabel` is not set correctly on the Element Snapshot copy. This attribute can be set with the API commands `CreateSnapshot`, `ModifySnapshot`, `CreateSchedule`, and `ModifySchedule`. To check the current label, send the API command `ListSnapshots`.
- ONTAP does not allow duplicate Snapshot copy names in a container, but Element does. The following describes the behavior if there are duplicate Snapshot copy names:
 - If there are two Snapshot copies with the same name on the source (not possible on the ONTAP source):
 - All SnapMirror transfer commands return a user-friendly error explaining that duplicate Snapshot copy names on a volume are not allowed.
 - If the Snapshot copy about to be transferred has same name as a Snapshot copy on destination:
 - For Element to ONTAP transfers, existing logic is used.
 - For ONTAP to Element transfers, the existing SnapMirror logic to rename the older Snapshot copy is used, and the agent implements the renaming by using the new `Rename Snapshot` API.

15 Summary

NetApp SnapMirror functionality between Element and ONTAP extends the Data Fabric with this disaster recovery architecture, providing increased data protection options for Element while using the robust data management capabilities of ONTAP. You can also take advantage of these new data mobility options to enable centralized backup and analytics and maximize the value and flexibility of your critical data.

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and websites:

Refer to the following links for Element documentation:

- Element <https://mysupport.netapp.com/documentation/productlibrary/index.html?productID=62480>
- Element Resources <https://mysupport.netapp.com/info/web/ECMLP2740378.html>
- Element API Reference Guide https://library.netapp.com/ecm/ecm_download_file/ECMLP2839249

Refer to the following links for ONTAP SnapMirror replication documentation:

- Replication between Element and ONTAP https://library.netapp.com/ecm/ecm_download_file/ECMLP2834698

- Data Protection Power Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2811525
- SnapMirror guides
<https://mysupport.netapp.com/GPS/category/ECMLS2588167.html>

Version History

| Version | Date | Document Version History |
|---------------|----------------|---|
| Version 1.0 | December 2017 | Initial release |
| Version 1.0.1 | September 2018 | Updated to include additional feature functionality in Element 10.3 and ONTAP 9.4 |

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2018 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 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.

TR-4651-0918