Technical Report

NetApp SolidFire SnapMirror Architecture and Configuration

Erik Kemp, NetApp
December 2017 | TR-4651

Abstract

This document outlines the architecture and configuration of SnapMirror® technology when using NetApp® SolidFire® storage.

n NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1   Executive Summary

Stored data is susceptible to disaster, either through 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 SnapMirror technology allows data mobility between NetApp Element® OS and NetApp ONTAP®, allowing ONTAP customers to integrate SolidFire into their existing data protection infrastructure. This integration builds on the NetApp Data Fabric and further connects SolidFire 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 where data in many various forms with many various requirements can be managed and migrated agilely as customers evolve the need to access and protect their data over time. SnapMirror integration also expands data protection and disaster recovery (DR) solutions for SolidFire customers by enabling AFF and FAS systems to serve as cost-effective DR targets for NetApp SolidFire environments. The ability to use hybrid and disk-based FAS systems introduces new cost-effective DR options for all-flash, SolidFire, and HCI products.

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

SolidFire and ONTAP jointly developed this architecture to enable SnapMirror deployments across heterogeneous storage architectures. This architecture provides superior data and application availability.

Mirroring is one of several methods to increase data availability in the event of hardware, software, or even site failures. SnapMirror technology offers a fast and flexible enterprise solution for mirroring or replicating data over LANs and WANs. SnapMirror technology is a key component in enterprise data protection (DP) strategies.

1.1   Introduction

NetApp SolidFire and NetApp ONTAP jointly developed this architecture to enable successful SnapMirror deployments across heterogeneous storage architectures that provide superior data and application availability.

Mirroring is one of several approaches to increasing data availability in the face of hardware, software, or even site failures. NetApp 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 (DP) strategies.

2   SnapMirror Technology

SnapMirror is a Snapshot replication technology that enables DR, designed for fail over 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 in the event of a major or minor outage 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 ONTAP controllers and now is integrated into SolidFire Element OS, which runs on all SolidFire and hyper converged infrastructure (HCI) storage nodes. 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. User management of relationships between SolidFire and ONTAP clusters is performed primarily through the SolidFire Element UI; however, some

management tasks reside in NetApp OnCommand® System Manager. Users can also manage SnapMirror through CLI and API, which are both available in ONTAP and Element OS.

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.
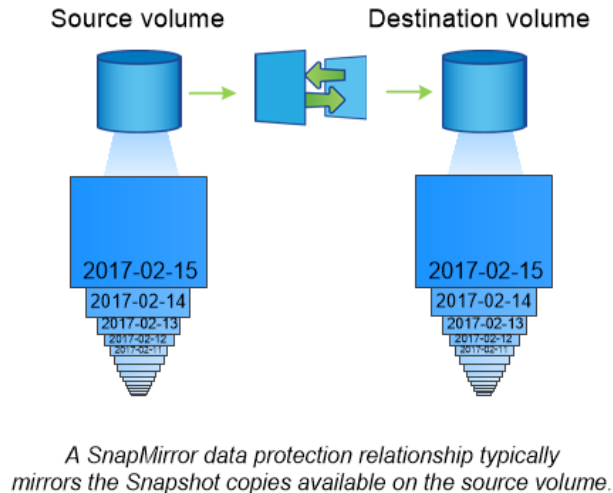
2.1   Components of a Mirror Relationship

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 by using 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 by using an automated or manual schedule; therefore, mirror copies are updated asynchronously.

3   Architecture Overview

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

Figure 2 illustrates the SnapMirror relationship between SolidFire and ONTAP.

Figure 2) SolidFire SnapMirror to ONTAP.
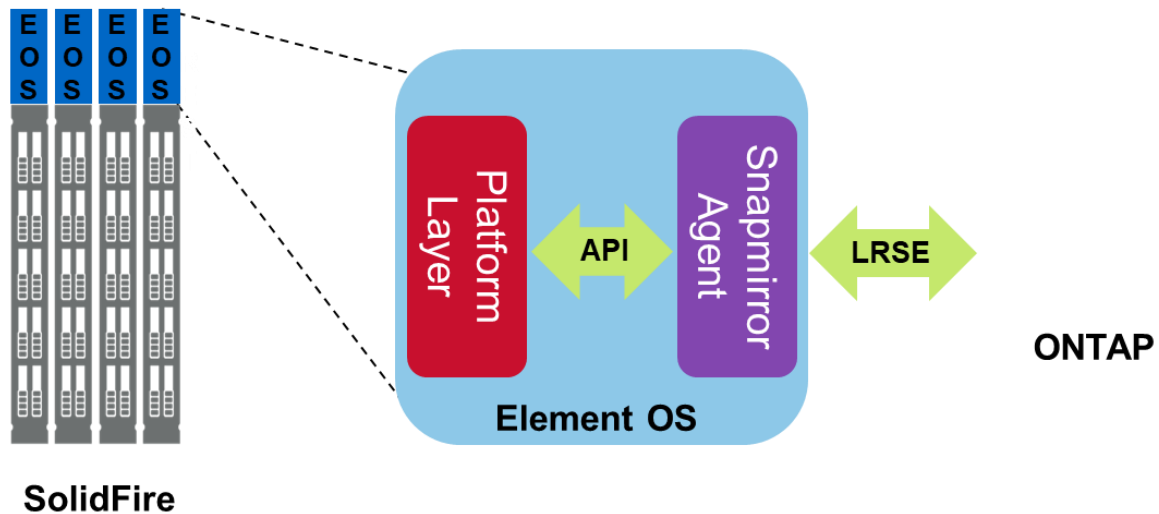
3.1 SolidFire SnapMirror to ONTAP Functionality

SolidFire SnapMirror to ONTAP supports the following functionalities (beginning with Element OS 10.1 and NetApp ONTAP 9.3 software):

Note: Applies to all Element OS-based products: SolidFire AFA, NetApp HCI, and FlexPod® SF.

- SnapMirror enables applications to fail over to a secondary volume and continue operating. It also has the capability to fail back to the primary location later. This capability is sometimes referred to as DR.
- Replicating block snapshots from a NetApp SolidFire source volume to a NetApp ONTAP destination volume and back.

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

- The following high-level features are supported:
  - Baseline and incremental transfer
  - SolidFire volumes can be promoted to read/write to be usable on ONTAP as ONTAP LUNs
  - CLI/API manageability through ONTAP CLI and SolidFire API
  - GUI manageability through SolidFire Element OS UI

Known Limitations

SolidFire SnapMirror to ONTAP has the following known limitations:

- No restore workflow (SnapMirror restore)
- No replication of LUNs originated from ONTAP to SolidFire
- No cascading from SolidFire to ONTAP and ONTAP to ONTAP or AltaVault
- No SnapCenter orchestration

ONTAP 9.3 and Element OS 10.1 Features

ONTAP 9.3 and Element OS 10.1 provide the following features:

- Bidirectional DR from NetApp SolidFire as a source to ONTAP as the target
- Manage 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/resync
- ONTAP to SolidFire (failover/failback use case):
    - Create, initialize, update, abort, modify, quiesce/resume, delete, and show
    - Async mirror policy
    - Break and resync/reverse and resync
- Usable LUNs (by breaking mirror or by cloning snapshots)
- IP redirection

3.2 Management in SolidFire Element UI

Use the SolidFire 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 transfer
    - Update transfer
    - Pause and resume transfer
    - Break
    - Resync

    Note: Use the Element OS UI for NetApp SolidFire, FlexPod SF, and NetApp HCI systems (different from primary NetApp HCI management tool).

3.3 Management in OnCommand System Manager

Use the OnCommand System Manager to manage the following tasks:

- Create and manage SnapMirror policies and schedules
- SnapMirror break capability in NetApp System Manager for a DR situation (SolidFire cluster is down)

Use Cases

3.4 NetApp SolidFire SnapMirror Replication Uses and Benefits

SolidFire SnapMirror Replication use cases and benefits include:

- Integrate SolidFire into the NetApp Data Fabric:
    - Make it easier for NetApp customers to incorporate SolidFire as part of their IT strategy
    - Connect SolidFire to customers' existing NetApp infrastructure
- Enhance data protection options for SolidFire 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 SolidFire to ONTAP:
  - Replicate from HCI in remote locations to AFF/FAS in central data center
  - Build lower-cost DR solutions from FAS portfolio
  - Use existing DR resources for newly added SolidFire systems
- Workload mobility and migration:
  - With the ability to send Snapshot copies between SolidFire and ONTAP, customers can also move workloads (disruptively) between heterogeneous storage systems

If you have both SolidFire and ONTAP in your data center and you can move (block) volumes between them based on application need and storage resource availability (SolidFire to ONTAP transfers only for first release) to:

- Provide bridge between ONTAP based and Element OS based products (including NetApp HCI)
- Provide tools to enable a better experience than off the shelf host-based migrations

## 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.

In cases in which a disaster requiring a failover occurs 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 newly created backups going to and from a SolidFire array for storage sent off the premises to an ONTAP backup repository to provide DR.

Figure 3) NetApp SolidFire DR to an ONTAP backup repository.
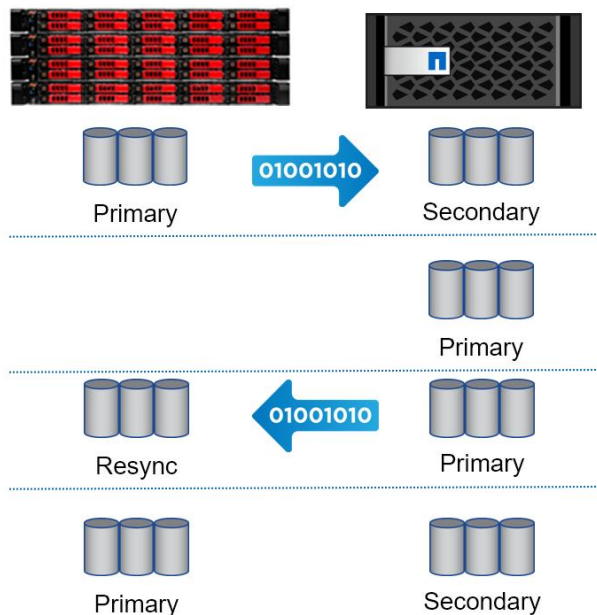
1. Establish link and replicate.
2. Break mirror/promote ONTAP volumes.
3. Replicate back to SolidFire.
4. Fail back to SolidFire volumes.

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 NetApp SolidFire and ONTAP storage systems. This flexibility allows for 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 SSDs.

3.9   Application Test/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 NetApp SolidFire – NetApp Private Storage (NPS) for Cloud

SnapMirror now enables replication of data from on-premises NetApp SolidFire storage to a NetApp ONTAP NetApp Private Storage (NPS) solution at a colocation facility, as shown Figure 4. Replication can also be performed between SolidFire 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.
- Leverage cloud resources for data center consolidation. Move workloads to NPS connected to cloud compute to use colocation facilities and public cloud as secondary and tertiary data center replacements.
- 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. Customers can meet short-term needs without overprovisioning. Pay by the hour and then turn off compute when you don't need it.
- Development and test agility. Leverage cloud compute, and, then, run in the cloud you choose or redeploy (SnapMirror) to on premises.

Figure 4) NetApp SolidFire: NPS for Cloud.
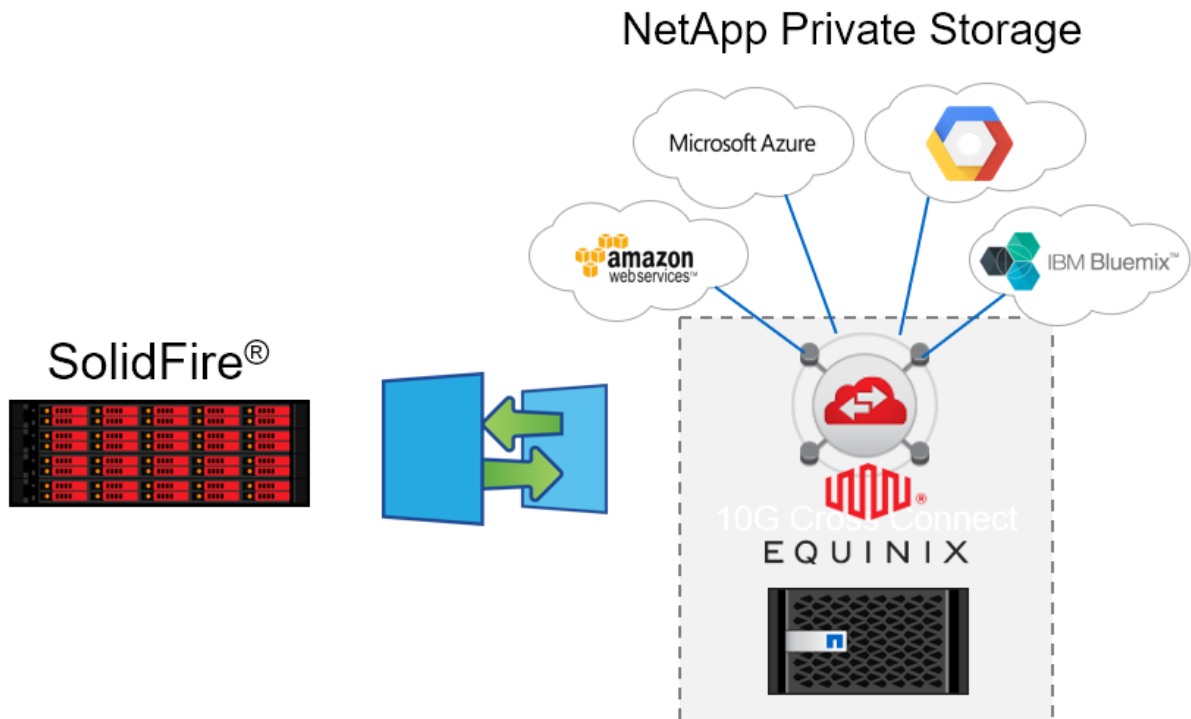
4 Replication Rules

A SolidFire volume is roughly equivalent to an ONTAP LUN.

- ONTAP volumes that are replication targets for SolidFire must contain a single LUN that serves as the container for the data being replicated from SolidFire.
- An ONTAP volume can contain data from one SolidFire volume only.
- If you replicate data from an ONTAP volume to a SolidFire volume, the data must have originated in the SolidFire volume, and the ONTAP volume must otherwise be empty.
- A SolidFire cluster might replicate to an ONTAP cluster through SnapMirror and other SolidFire clusters by using Native Replication feature of SolidFire. However, a specified volume might only replicate to a single endpoint (either ONTAP or SolidFire).

4.1 Scale Support and Limitations

Scale support and limitations include:

- SolidFire supports up to 30 snapshots per volume for SnapMirror (system limit is typically 32).
- ONTAP supports up to 251 Snapshot copies (system hard limit is 255).
- SnapMirror supports a maximum of 500 protected volumes replicating from one SolidFire cluster to ONTAP.
- SnapMirror supports a maximum of 4 SolidFire clusters replicating to a single ONTAP array.
- SnapMirror supports a maximum of 2000 volumes total (across 4 SolidFire clusters) replicating to a single ONTAP array.
- 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
MirrorLatest	async-mirror	Transfer only the Snapshot copy created by SnapMirror.
MirrorAndVault	mirror-vault	Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels Daily or Weekly.
Unified7year	mirror-vault	Transfer the Snapshot copy created by SnapMirror and any less recent Snapshot copies made since the last update, provided they have SnapMirror labels Daily, Weekly, or Monthly.

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. It 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 SolidFire-to-ONTAP Replication

You must complete the following tasks before configuring a SolidFire-to-ONTAP data protection relationship:

- SnapMirror must be licensed on the participating ONTAP cluster.
- All nodes on the SolidFire cluster containing the volume to be replicated must be accessible to ONTAP over the network.
- The SolidFire cluster must have the SnapMirror feature enabled.
- The SolidFire volume must be enabled for SnapMirror replication.
- If you are using the mirror-vault policy type, a SnapMirror label must be configured for the SolidFire snapshots to be replicated.
- Make sure that port 5010 is available.

8 Support Details SolidFire-to-ONTAP Replication

Table 2 lists the support details for SolidFire-to-ONTAP replication.

Table 2) Support details for SolidFire-to-ONTAP replication.

Resource or feature	Support details
SnapMirror	- The SnapMirror restore feature is not supported. - The `MirrorAllSnapshots` and `XDPDefault` policies are not supported. - The Vault policy type is not supported. - The system-defined rule "all_source_snapshots" is not supported. - The `Mirror-vault` policy is supported only for replication from SolidFire to ONTAP. Use `async-mirror` for replication from ONTAP to SolidFire. - The `-schedule` and `-prefix` options for SnapMirror policy add-rule are not supported. - The `-preserve` and `-quick-resync` options for SnapMirror resync are not supported. - Storage efficiency is not preserved.

Resource or feature	Support details
	• The SolidFire volume cannot be replicated to multiple ONTAP volumes (fan out).
SolidFire	• 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 snapshots to be replicated is 30.
Network	• A single TCP connection is allowed per transfer. • The SolidFire node must be specified as an IP address. DNS host name lookup is not supported. • IPspaces are not supported.
SnapLock®	• SnapLock volumes are not supported.
FlexGroup	• FlexGroup volumes are not supported.
Storage virtual machine (SVM) DR	• ONTAP volumes in an SVM DR configuration are not supported.
MetroCluster™	• MetroCluster is not supported as a target cluster config
AltaVault™	• SolidFire-to-ONTAP-to-AltaVault cascade relationships are not supported. • SolidFire direct replication to AltaVault is not supported.

9 How SnapMirror Works

9.1 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.

9.2 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 follows the schedule configured in the SnapMirror policy. You can activate the destination volume with minimal disruption in case of a disaster 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 ONTAP system

are near comparable equivalents to the primary SolidFire system if comparable performance is the design objective.

9.3   Resynchronization

Data protection relationships can be resynchronized 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.

9.4   SolidFire SnapMirror to ONTAP Workflow

The SolidFire SnapMirror to ONTAP workflow is as follows:

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

9.5   ONTAP SnapMirror to SolidFire Workflow

The ONTAP SnapMirror to SolidFire workflow is as follows. In this case, the volume must have originated on SolidFire.

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

9.6   SnapMirror Configuration Options

This section describes the SnapMirror configuration options.

Setting Up the Cluster

To create a SolidFire 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 AccountID of the newly created account.
4. Create one or more volumes.

Enabling SnapMirror

1. Enable SnapMirror in the Feature Settings page.

Figure 5) Enable SnapMirror feature.
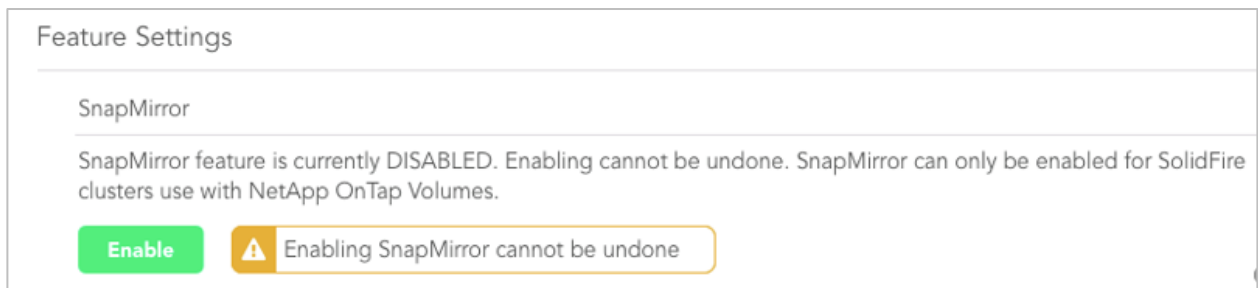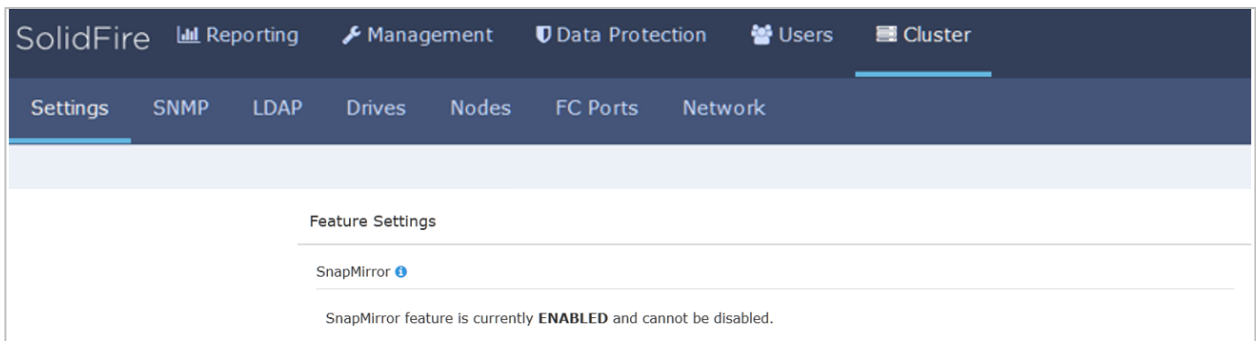
Configuring Access from Remote ONTAP Cluster

Before any pairing can be attempted from the ONTAP cluster, SolidFire must open its firewall to enable incoming connections on port 5010 from the ONTAP cluster's intercluster LIFs.

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

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

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

Figure 6) Create SnapMirror endpoint.

Setting Up a Volume

For SnapMirror to take control of a volume (and for read/write permission) 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 a SolidFire volume.

- 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
- And a volume can be modified at any time to enable SnapMirror as well:
  `enableSnapMirrorReplication=true`

After the volume is configured to enable SnapMirror communication, use the SnapMirror CLI to create a relationship with this SolidFire volume as the source:
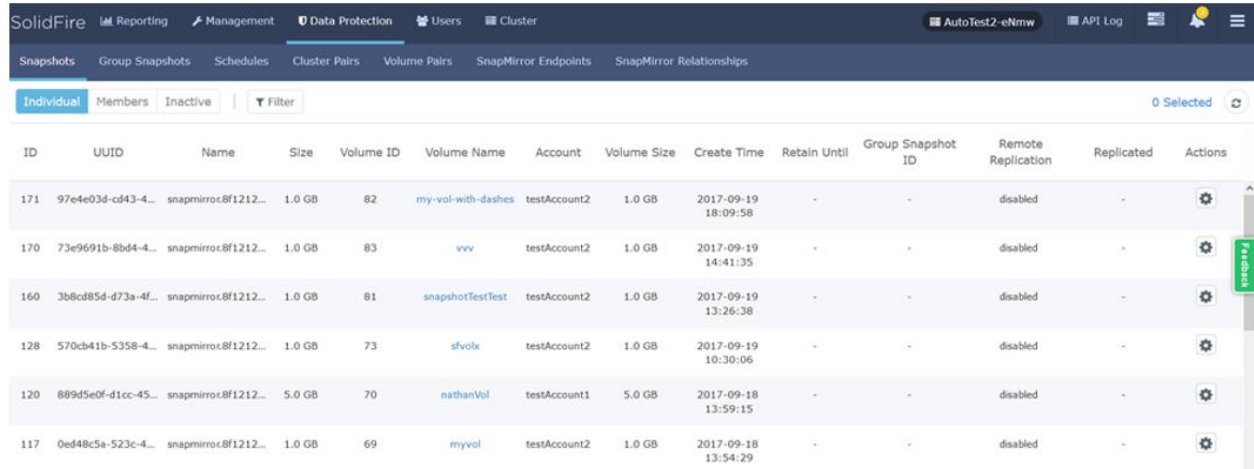
```
> snapmirror create -source-path <solidfire SVIP>:/lun/1000 -destination-path vs1:vol2 -type xdp
```

Creating Snapshots

After a relationship is established, you can assign existing policies or configure policies using OnCommand System Manager or the SnapMirror CLI. Regardless of the policy, each SnapMirror update command creates a snapshot on the SolidFire system to transfer to the ONTAP system (because we only support mirror relationships). If the policy is a mirror-vault policy, the user can also specify that snapshots with particular labels be transferred to the ONTAP system.

Figure 8) Snapshots created by SnapMirror.

Creating Snapshot Schedules

When combined with a mirror-vault policy, setting snapshot schedules, allows the user to create regular snapshots with a particular label. Scheduled snapshots of SolidFire volumes must be created using the SolidFire UI/API.

Figure 9) Create snapshot schedule.

<table>
<tr><td>equency</td><td>Recurring</td><td>Manually Paused</td><td>Volume IDs</td><td>Last Run</td><td>Last Run Status</td><td>Actions</td></tr>
<tr><td>rs Of Week</td><td>No</td><td>No</td><td>1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,
17,18,19,20,21,22,23,24,25,26,27,28,2
9,30</td><td>-</td><td>Success</td><td>⚙</td></tr>
</table>

Caution
The retention of snapshots on the SolidFire cluster is independent from when a Snapshot copy is deleted on the ONTAP system. The mirror-vault policy controls the Snapshot copy retention on the ONTAP system. Technically, the retention on the SolidFire system only needs to be long enough for replication to the DR ONTAP system to maintain a replica of that Snapshot copy. If you want to be able to restore to that snapshot then it should be retained longer. Also, any Snapshot copies replicated to the SolidFire cluster as part of DR failback will be controlled by the mirror-vault policy because they will not have a SolidFire retention set.

Cloning a Snapshot

Snapshots can be cloned 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 that is currently prohibited from deletion due to the Hold attribute:

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

Breaking the SnapMirror Relationship

If a SolidFire volume is the destination in a SnapMirror relationship and the ONTAP cluster becomes inaccessible, a SolidFire admin can break the relationship, rollback the volume to a snapshot, and mount it by using the `BreakSnapMirrorVolume` method.

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

SnapMirror container attributes will be cleared during the break operation. SnapMirror snapshot attributes will not be cleared.

Disabling SnapMirror Replication

The SnapMirror relationship can be disabled at any time by the SolidFire administrator; it is not dependent on the availability of the ONTAP system.

```
ModifyVolume(volumeID=1, enableSnapMirrorReplication=false)
```
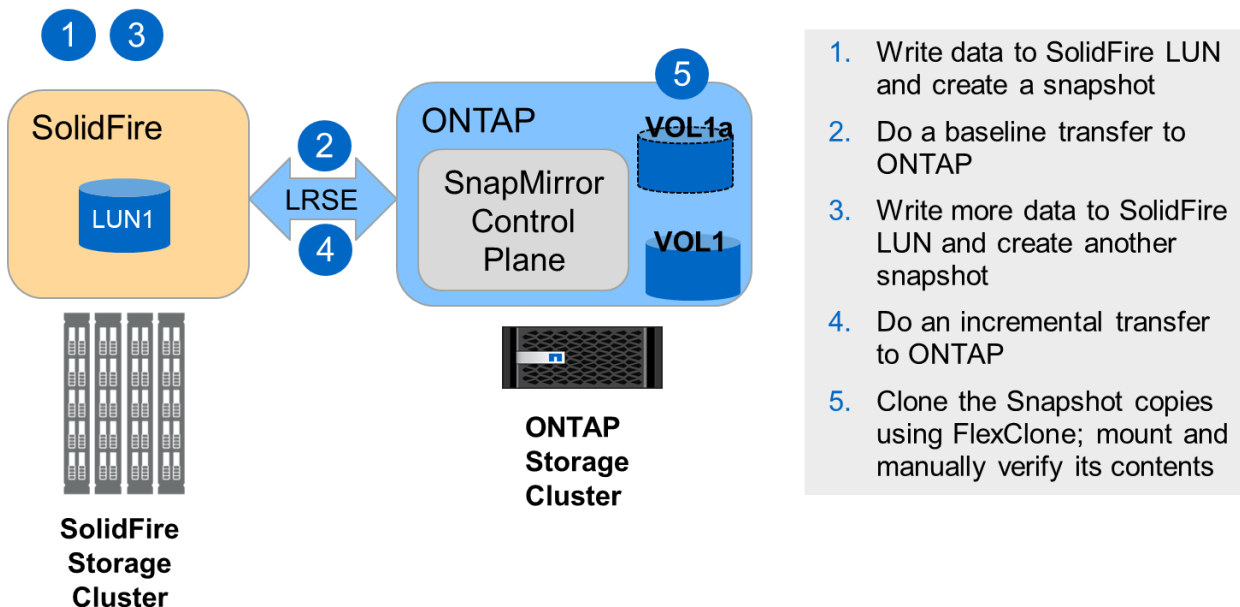
The SnapMirror container and snapshot attributes will not be cleared on the SolidFire volume. The user can resume replication by reenabling `enableSnapMirrorReplication`.

If the SolidFire volume is the destination and the volume access mode is snapMirrorTarget, `ModifyVolume` cannot be used to make the volume readWrite. The user must issue `BreakSnapMirrorVolume` as described previously.

9.7   Transfer from SolidFire to ONTAP

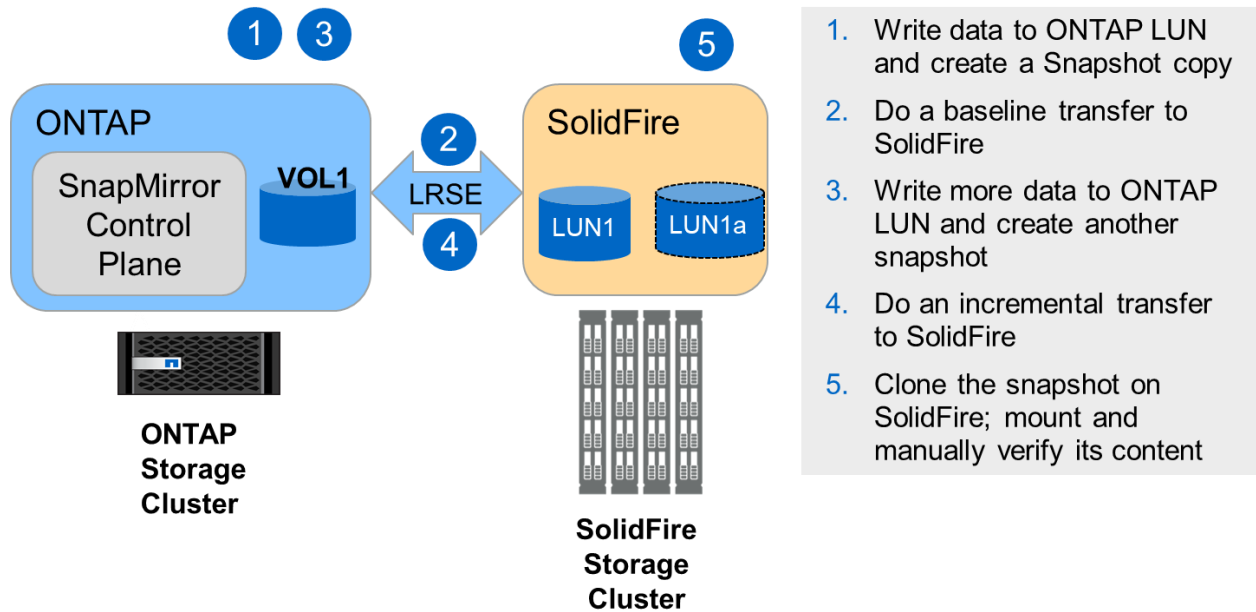Figure 10 illustrates the SnapMirror transfers from SolidFire to ONTAP.

Figure 10) SolidFire SnapMirror to ONTAP.

1. Write data to SolidFire LUN and create a snapshot
2. Do a baseline transfer to ONTAP
3. Write more data to SolidFire LUN and create another snapshot
4. Do an incremental transfer to ONTAP
5. Clone the Snapshot copies using FlexClone; mount and manually verify its contents

9.8 Transfer from ONTAP to SolidFire

Figure 11 illustrates the SnapMirror transfers from ONTAP to SolidFire.

**Figure 11) ONTAP SnapMirror failback to SolidFire.**

1. Write data to ONTAP LUN and create a Snapshot copy
2. Do a baseline transfer to SolidFire
3. Write more data to ONTAP LUN and create another snapshot
4. Do an incremental transfer to SolidFire
5. Clone the snapshot on SolidFire; mount and manually verify its content

10 SolidFire 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.
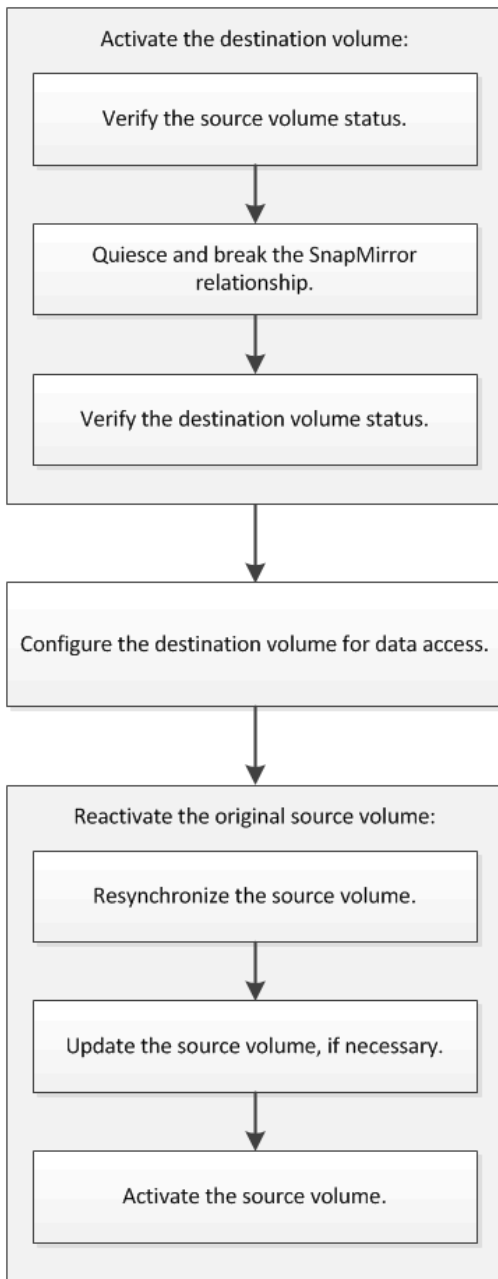
Figure 12) NetApp SolidFire SnapMirror to ONTAP.
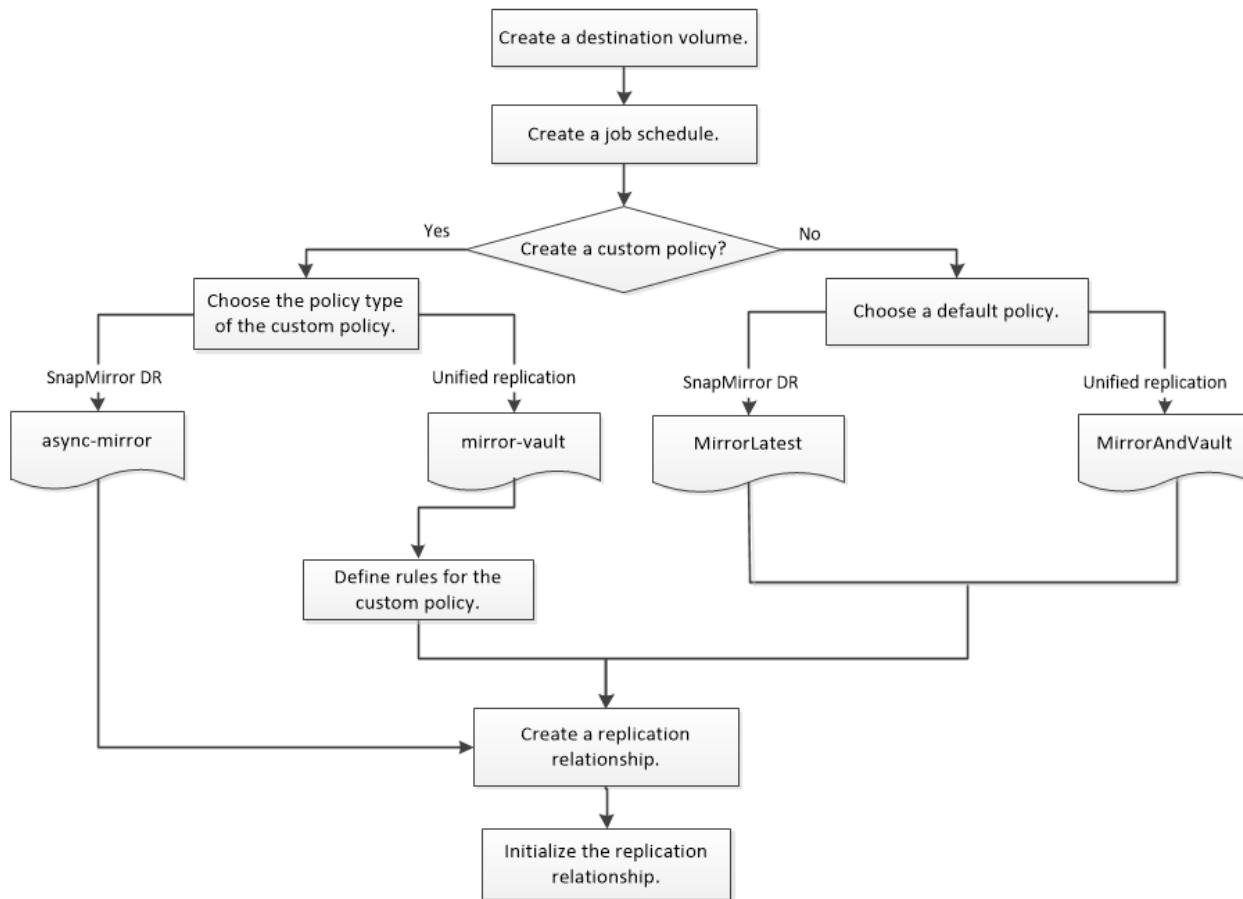
10.1 Volume Disaster Recovery Workflow

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 Throttling SnapMirror Replication

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

11.1 Bandwidth Throttling

Bandwidth throttling can be implemented on a per-relationship basis. This can be set in SolidFire UI or through CLI/API. The max transfer rate setting controls the maximum amount of bandwidth that can be utilized by a given relationship.

You can also enable or disable throttling at the ONTAP node level to set the maximum bandwidth for outgoing transfer, 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 3) ONTAP throttling.

Type	Description
maxTransferRate	Specifies the upper bound, in kilobytes per second, at which data is transferred. The default is unlimited (0), which permits the SnapMirror relationship to fully utilize the available network bandwidth.
currentMaxTransferRate	The upper bound, in kilobytes per second, at which data is transferred for the current transfer. This value can be the same as the `maxTransferRate` or different if overwritten when starting the transfer using the associated commands or APIs (`IntializeSnapMirrorRelationship`, `UpdateSnapMirrorRelationship`, `ModifySnapMirrorRelationship`, `ResyncSnapMirrorRelationship`).

12 Scheduling

Scheduling options include "hourly", "daily", "weekly", and "monthly" with time options of "month", "day", "day of the week", "month of the week", "hour", and "minute."

Table 4 describes the types of Snapshot copy schedules.

Table 4) 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.

A user can configure Snapshot copy replication as frequently as every 15 minutes with the assumption that the link to target and data change rates support this.

13 Basic Troubleshooting

13.1 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 SolidFire node and conversely.
2. If pings fail, then verify the configuration.
   - The SolidFire cluster uses the `SnapMirrorEndpoint` object to manage ONTAP IPs. An endpoint can be unmanaged or managed.
- Managed. The user passes ONTAP management credentials to `CreateSnapMirrorEndpoint` API command. SolidFire cluster automatically discovers ONTAP LIFs and allows them through the firewall. This mode also allows the SolidFire web UI to perform management operations for SnapMirror workflows.
- Unmanaged. The user passes ONTAP LIFs to `CreateSnapMirrorEndpoint` API command. SolidFire cluster opens the firewall for those IPs.

1. Run the following command on each SolidFire node. The ONTAP LIFs should report as being allowed through the firewall. Verify that the IPs are correct.

```
ufw status
```

2. 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 SolidFire cluster.

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

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

13.2 Configuration Issues

- SnapMirror operations are blocked on the cluster until the user enables the SnapMirror feature. This can be enabled in the web UI or by using the `EnableFeature` API command.
- SnapMirror operations are blocked on a volume until the user sets the volume attribute `enableSnapMirrorReplication=true`. This can be done 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 may not work properly if the attribute `snapMirrorLabel` is not set correctly on the SolidFire Snapshot copy. This 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 SolidFire 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:
       o This is not possible on ONTAP source
       o All SnapMirror transfer commands will return a user-friendly error explaining that duplicate Snapshot copy names on a volume are not allowed.
   - Snapshot copy about to be transferred has same name as Snapshot copy on destination:

- o For SolidFire to ONTAP transfers, existing logic will be used.
- o For ONTAP to SolidFire transfers, the existing SM logic to rename the older already existing snapshot will be used, and the new `RENAME SNAPSHOT` API is how the agent will implement this in the ONTAP->SF direction.

14 Summary

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

Where to Find Additional Information

To learn more about the information described in this document, see the following documents and/or websites:

See the following links for NetApp SolidFire documentation:

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

See the following links for ONTAP SnapMirror Replication documentation:

- SolidFire to ONTAP Backup Power Guide:
  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

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.

TR-4651-1217

n NetApp®