Technical Report

NetApp AltaVault Cloud-Integrated Storage Appliance

Solution Deployment: AltaVault with ONTAP Using SnapMirror

Mike Braden, NetApp
February 2018 | TR-4624

Abstract

This solution deployment guide outlines how easy it is to deploy and use a NetApp® AltaVault™ cloud-integrated storage appliance with NetApp ONTAP® using SnapMirror®. The AltaVault appliance provides a simple, efficient, and secure way to move data off site to either public or private cloud storage providers. Using advanced deduplication, compression, and encryption, AltaVault enables organizations to eliminate reliance on older, less reliable data protection solutions while improving backup windows and disaster recovery capabilities.

NetApp®

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 AltaVault Overview

1.1 Executive Overview

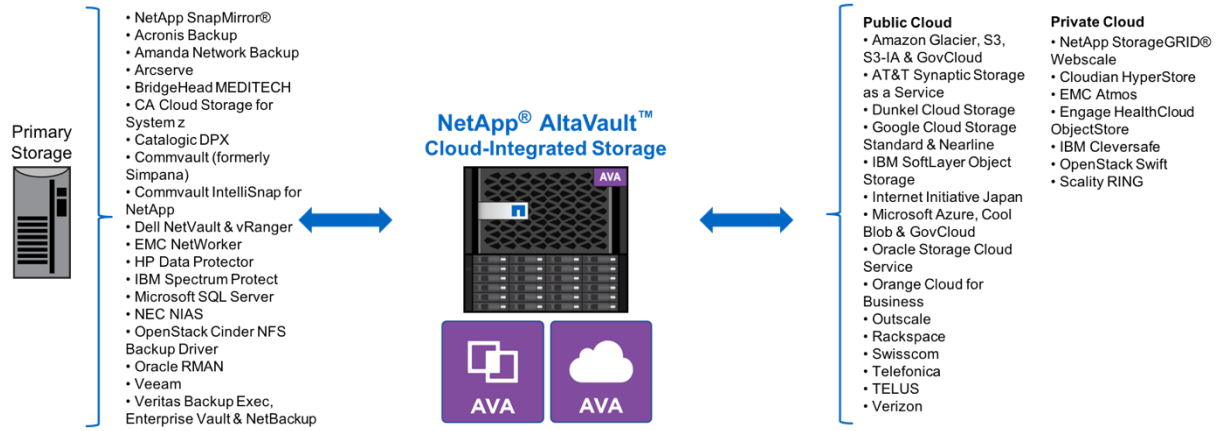
NetApp AltaVault storage enables customers to securely back up data to cloud at up to 90% less cost compared to that of on-premises solutions. AltaVault gives customers the power to tap into cloud economics while preserving investments in existing backup infrastructure and meeting backup and recovery SLAs. AltaVault appliances act as a NAS target within a backup infrastructure. Having this capability enables organizations to eliminate their reliance on tape infrastructure and all its associated capital and operational costs while improving backup windows and disaster recovery capabilities.

It is simple to set up the AltaVault appliance. You can start moving data to the cloud in as little as 30 minutes; setting up tape or other disk replication infrastructures can take days. By leveraging industry-leading deduplication, compression, and WAN optimization technologies, AltaVault appliances shrink dataset sizes by 10 to 30 times. They also substantially reduce cloud storage costs, accelerate data transfers, and store more data within the local cache, speeding recovery.

Security is provided by encrypting data on site, in flight, as well as in the cloud using 256-bit AES encryption and SSL v3/TLS v1. AltaVault appliances provide a dual layer of encryption that prevents any data moved into the cloud from being compromised, and it creates a complete end-to-end security solution for cloud storage.

Because an AltaVault appliance is an asymmetric, stateless appliance, no hardware is needed in the cloud. You can also recover the last known good state of a broken or destroyed AltaVault appliance to a new AltaVault appliance. AltaVault appliances provide flexibility to scale cloud object storage as business requirements change. Organizations avoid all the capital expenditure planning required with tape and disk replication–based solutions, saving up to 90%.

Figure 1) AltaVault ecosystem.



Note: Glacier is not supported for SnapMirror.

AltaVault SnapMirror stores Snapshot™ copies in the cloud for backup purposes. For disaster recovery of critical systems, the best level of protection is provided by using SnapMirror to replicate data to a secondary cluster. For long-term storage of Snapshot copies, the replication can also be performed to AltaVault, providing a complete solution for fast recovery of critical data in a disaster recovery as well as long-term off-site backups in cloud storage.

Benefits of using AltaVault for storing Snapshot copies in the cloud include:

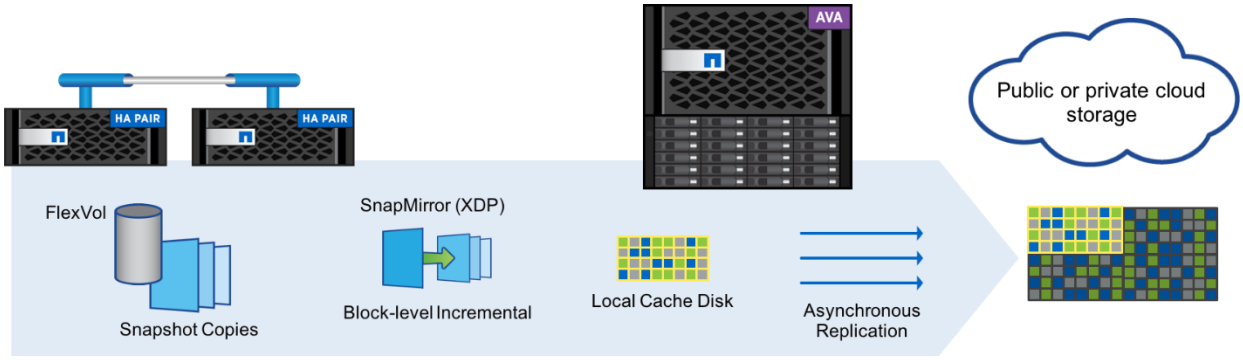
- Significant savings using AltaVault deduplication and compression
- Security with AltaVault data encryption for both local and cloud storage
- Support for a broad range of public and private cloud storage solutions
- AltaVault management of cloud storage services
- AltaVault migration capability for both longevity and investment protection

1.2 Solution Overview

Combining AltaVault with ONTAP 9 provides efficient and flexible backup to cloud storage. SnapMirror to AltaVault uses block-level incremental forever data transfers to protect data in Snapshot copies. AltaVault manages object storage with either a public cloud service or a private cloud object store.

Administrators have a wide range of choices for object storage using the AltaVault appliance. With services from hyperscalers or service providers, the AltaVault appliance manages cloud storage to provide the options for performance and space savings while maintaining security.

Figure 2) SnapMirror overview.



The AltaVault appliance shrinks data using deduplication with variable-length segmentation to provide a high level of storage optimization. The resulting data is further reduced with compression and is encrypted before being stored in a local cache. Sending data to the cloud is done using a high-performance asynchronous replication engine. As soon as data is packaged locally, replication to the cloud begins, with the goal of having all data in the cloud quickly. The cloud copy of the data becomes the off-site copy available for use when a local disaster makes a site unavailable.

1.3 Workflow Examples

Several use cases and workflows can be achieved by combining Data ONTAP and AltaVault in a solution using SnapMirror to replicate data:

- Back up volumes, configure Snapshot schedules, and define retention
- Restore individual files or LUNs
- Restore a whole volume
- Reestablish a replication relationship after a disaster recovery
- Manually delete Snapshot copies in either Data ONTAP or AltaVault

2 Design a Solution with AltaVault with SnapMirror

2.1 SnapMirror Overview: What About SnapVault?

Long-term ONTAP administrators know that SnapMirror is an industry-leading replication technology that was the original replication feature of ONTAP. SnapMirror has gone through a lot of changes across the many generations of ONTAP. Significant changes include moving from older 7-Mode systems to clustered ONTAP systems. The latest changes with SnapMirror include the addition of third-party endpoints with the introduction of SnapMirror for AltaVault.

In understanding SnapMirror for AltaVault, it is helpful to understand the history of SnapMirror, especially for long-term ONTAP administrators. In clustered ONTAP, SnapMirror is the name of the replication protocol or replication engine. In ONTAP 9, SnapMirror and SnapVault® are unified into a single internal engine referred to as unified replication. Administrators with experience recall that in previous generations of ONTAP, there were two different replication engines that served different purposes. These were called SnapMirror and SnapVault. One of the main differences between the two engines was the method of Snapshot retention. For SnapMirror, the source and destination had the same Snapshot copies creating a mirror image of the data in two locations. The primary use case for having the same Snapshot copies in two locations was for disaster recovery (DR) so that it was possible to move applications from the primary when there was an outage to use the secondary copy.

SnapVault differed in that it allowed the transfer of specific Snapshot copies so it was possible to have two locations for storing Snapshot copies, a source and a destination, yet the destination could have a different list of Snapshot copies than the primary. The primary use case for having different Snapshot copies was for data protection or backup. If there was a loss of data, such as an accidental deletion, if the Snapshot copy was no longer part of the source volume, the data could be recovered from the backup copy in the SnapVault destination. Having only specific Snapshot copies on the destination allowed for keeping Snapshot copies for a longer period. For example, the primary could retain many hourly and daily Snapshot copies, and the weekly Snapshot copies could be kept in the vault destination. This approach freed up Snapshot copies in the primary or source so that the most recent ones could be local, and the longer-term Snapshot copies would still be available for recovery if needed.

In newer versions of ONTAP, the replication engines were consolidated into a new replication engine referred to as unified replication. This new single replication engine allows the same type of Snapshot retentions by providing options to indicate the type of replication relationships. With the replication protocol becoming unified, the new protocol kept the SnapMirror name and offered both SnapMirror and SnapVault functionality in a more flexible and efficient way. The former SnapVault type of relationship, where only specific Snapshot copies are retained for backup purposes, is created using the XDP type. ONTAP Snapshot policies still refer to this retention as vault.

2.2 Hardware and Software Prerequisites

This guide describes the extra steps needed to configure SnapMirror. Utilize the product documentation to deploy and perform initial configuration of the systems.

Deploy an AltaVault appliance into a backup environment using the procedures from the installation section of the product documentation that matches the type of appliance (physical model or virtual model).

The solution should also be properly sized to meet capacity and network requirements. Use the sizing tools, including ONTAP SnapMirror sizing with SPM and the AltaVault sizing tool, available on the NetApp Field Portal.

2.3 Solution Requirements

The basic requirements provide for an ONTAP system to replicate with SnapMirror to an AltaVault appliance. Many more complex configurations are possible. The intention of this guide is to cover the

typical aspects and define the requirements and parameters to help design a solution across a wide range of organizations.

Supported Platforms

The initial release of SnapMirror for AltaVault is provided in ONTAP 9.1 and AltaVault software 4.3. For the initial release, there are some limitations on the platforms supported. Table 1 provides a high-level view of what is supported. See the Interoperability Matrix Tool (IMT) on the NetApp Support site for specific versions and platforms.

Table 1) Supported platforms for SnapMirror with AltaVault.

Platform	Replication Source	Replication Destination	Note
FAS	**Y**		
AFF	**Y**		
ONTAP Cloud	N		Not supported in initial release
ONTAP Select	N		Not supported in initial release
AltaVault 400/800	N	**Y**	
AltaVault Virtual	N	**Y**	
AltaVault Cloud	N	N	Not supported in initial release

Note: An AltaVault appliance offers two fundamental modes of operation known as backup mode and cold storage (archive) mode.

Note: SnapMirror for AltaVault does not support cold storage mode, only backup mode is supported.

Table 2) Software requirements.

Platform	Version
FAS/AFF	ONTAP 9.1 or later
AltaVault	AltaVault OS 4.3.1 or later

For a physical AltaVault appliance, such as AVA400, the license is built in for the operating system. No additional licenses are required.

For a virtual AltaVault appliance, a license key is provided with the purchase process. For a proof-of-concept (POC), the AltaVault virtual appliance includes a 90-day trial mode when no license is entered. When purchased, a license key is supplied as part of the purchase process.

AltaVault does not require additional licenses for SnapMirror or other protocols. Protocols are included with the AltaVault appliance software license.

Table 3) ONTAP license requirements.

License	System	Description
SnapMirror	Primary, secondary	SnapMirror license

License	System	Description
SnapRestore	Primary, secondary	SnapRestore® license needed for single-file SnapRestore restoration of data

Table 4) AltaVault license requirements.

License	Description
AVA OS license	AltaVault has an operating system license by platform. SnapMirror is included in the OS license (no separate license is required).

Review the product documentation on the NetApp Support site for information about hardware and software requirements for installation of virtual or physical appliances. This guide provides the additional requirements needed to implement the combined solution for SnapMirror between ONTAP and AltaVault appliances.

Note: For details about requirements for using SnapCenter to manage ONTAP SnapMirror to AltaVault, including NAS file catalog, refer to the Data Fabric workflow guide that is included in the SnapCenter product documentation or the Data Fabric resource page on the NetApp Support site.

SnapMirror Relationship Limits

Each AltaVault appliance can support several replication relationships from one or more ONTAP clusters. The actual SnapMirror relationships a given AltaVault appliance can support might also be dependent on other factors such as data transfer performance, cache capacity, or other sizing factors. Using the AltaVault sizing tool to estimate the practical limits of a configuration is recommended.

Table 5) AltaVault maximum SnapMirror relationships.

Platform	Version	Maximum SnapMirror Relationships
AltaVault 400/800	AltaVault OS 4.3.1	500
AltaVault virtual	AltaVault OS 4.3.1	500
AltaVault cloud	AltaVault OS 4.3.1	Not supported

SnapMirror Transfer Limits

A SnapMirror update performs a transfer of Snapshot blocks from the source to destination using an IPv4 TCP connection. Each relationship that gets updated uses a separate TCP connection to transfer the data. The session is referred to as a data transfer or simply a transfer. The transfer consists of all the changed blocks in the Snapshot copy that is part of the update.

An ONTAP cluster node can support up to 100 concurrent transfers. An AltaVault appliance also supports up to 100 concurrent SnapMirror transfers. The total of 100 concurrent transfers supported by the AltaVault appliance also applies to restore operations. This fact means that if 100 concurrent backups are running against a single AltaVault appliance, you cannot run any SnapMirror restores from the AltaVault appliance.

An ONTAP cluster automatically manages the number of updates from a single cluster to an AltaVault appliance to make sure that the 100-transfer limit is not exceeded. However, when using multiple clusters to an AltaVault appliance in a fan-in topology, the design should make sure that no more than 100 concurrent transfers occur because a single cluster is not aware of transfers from another cluster. Planning should consider the total number of transfers to make sure limits are not exceeded.

Planning concurrent transfer limits is especially important for cascade relationships. When designing cascade relationships such as ONTAP to ONTAP to AltaVault appliance topology, the second ONTAP node acts as a source and destination for SnapMirror transfers. In this configuration, if 100 ONTAP to ONTAP relationships are running concurrently, the ONTAP to AltaVault relationships are queued until the ONTAP to ONTAP transfers complete. If concurrent transfers between ONTAP to ONTAP and ONTAP to AltaVault are required, the relationship schedules must be configured such that the total number of relationships running concurrently doesn't exceed the limit.

Table 6) Maximum concurrent transfers

Platform	Version	Maximum Concurrent SnapMirror Transfers
FAS/AFF	ONTAP 9.1	100
FAS/AFF	ONTAP 9.2	100
AltaVault	AltaVault OS 4.3.1	100

Network Port Requirements

When creating cascade relationships between ONTAP clusters, the following ports need to be open between the systems if a firewall separates the systems. HTTPS is recommended when using OnCommand® System Manager; however, it is not required. ICMP should be allowed between the systems.

Table 7) ONTAP cluster network ports.

Port	IANA Service Name	Description
10000	ndmp	Network data management protocol
11104	netapp-icmgmt	NetApp intercluster management
11105	netapp-icdata	NetApp intercluster data

SnapMirror for AltaVault requires the following ports to be open between ONTAP and AltaVault systems.

Table 8) AltaVault network ports.

Port	Description
5010	SnapMirror data

A complete listing of ports and their use for AltaVault is available in TR-4405: AltaVault Security Overview Guide.

2.4 Time Synchronization

The use of Network Time Protocol (NTP) is recommended so that all the systems maintain correct time and are in sync with each other. AltaVault has NTP configured by default using ntp.org time servers. Time needs to be synchronized for authentication between systems to function properly, including cloud storage services, SMB, and Kerberos authentication. Data ONTAP should have NTP enabled and configured using either a preferred NTP server or the same default ntp.org servers that AltaVault uses.

Additional benefits are having log time stamps synchronized for troubleshooting.

2.5 Supported Topologies

Replication between storage systems can be set up in a variety of topologies depending on where the systems are located and how the data should be available. SnapMirror disaster recovery relationships can also differ from backup relationships, for example, when DR is configured for an application and the application needs access to both source and destination systems.

The supported topologies include:

- Cascade
- Fan-out of a volume
- Fan-in to one AltaVault appliance
- Fan-out from a cluster to multiple AltaVault appliances

Each volume in a source cluster can only replicate to one AltaVault share (endpoint). It is not possible to replicate a single volume to multiple AltaVault appliances. However, it is possible to fan out a source volume to multiple cluster endpoints and a single AltaVault endpoint or multiple volumes to multiple AltaVault appliances.

ONTAP systems and SnapMirror requirements should follow the guidelines described in the ONTAP product documentation for the version of ONTAP in use. Many combinations are possible, including cascade relationships. Cascade of FAS/AFF to FAS/AFF are all possible when doing SnapMirror to AltaVault. The ONTAP system that is in a SnapMirror relationship with an AltaVault appliance should meet the requirements shown in the previous section.

Note: Although ONTAP and AltaVault support many topologies, when using SnapCenter, the supported topologies are not the same. Refer to the SnapCenter product documentation for supported topologies.

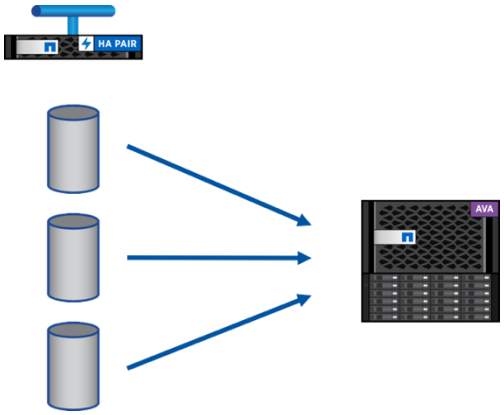
Deduplication for an AltaVault appliance is appliance-wide. All SnapMirror shares in an AltaVault appliance deduplicate data against each other as well as other types of shares on the same appliance.

Note: AltaVault does not provide a multitenant configuration. For solutions requiring separation of data, administration, multiple authentication, or multiple Microsoft Active Directory services, using one or more smaller appliances for each tenant is recommended.

Fan-in relationships are one possible topology when using ONTAP with an AltaVault appliance for backup. This topology allows for many volumes to be backed up by a single AltaVault appliance. When used with one ONTAP cluster, there are several advantages because the SnapMirror transfers are automatically managed within a single cluster providing the simplest design options.

Note: Fan-out is not supported from AltaVault. AltaVault is a destination or endpoint and cannot be a source of SnapMirror data.

Figure 3) Single-cluster multiple-volume fan-in to one AltaVault appliance.



Fan-in configurations are not limited to a single ONTAP cluster. It is possible to fan in volumes from more than one cluster to a single AltaVault appliance. Design and sizing of this type of topology are more complex than with a single ONTAP cluster. However, when designed within the limits described in this guide, this solution can offer an advantage for long-term backup to cloud storage with a single AltaVault appliance to manage.

Figure 4) Multiple-cluster multiple-volume fan-in to one AltaVault appliance.

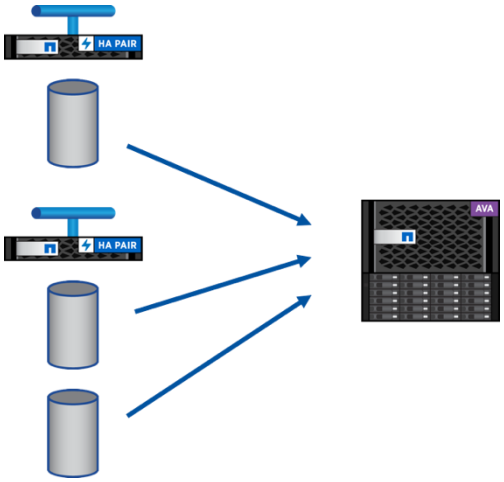


Figure 5) Volume fan-out to multiple AltaVault appliances.

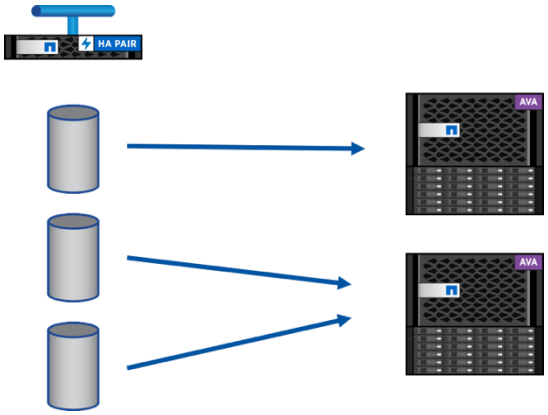


Figure 6) Fan-out of volume to secondary cluster and AltaVault appliance.

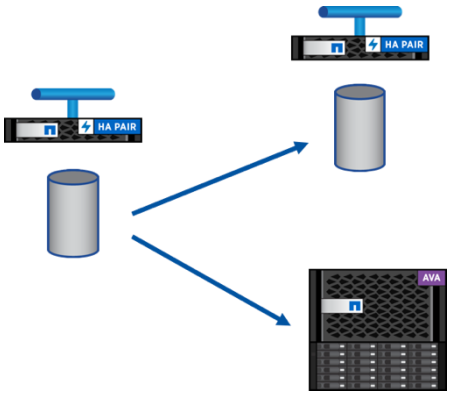
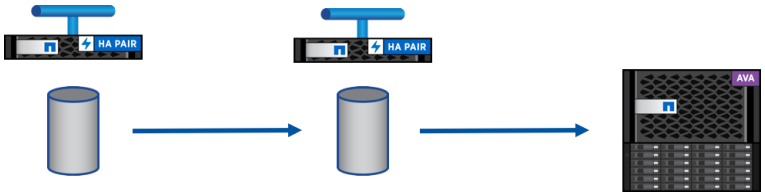
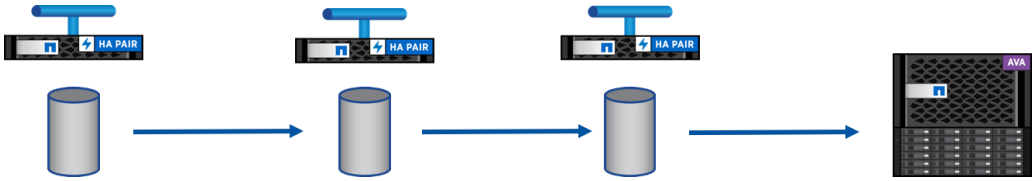


Figure 7) Volume cascade primary cluster to secondary cluster to AltaVault appliance.



Cascades are allowed if AltaVault is the endpoint of the cascade relationship. More complex cascade topologies are supported. The most common use case of cascades is to replicate volumes to a secondary FAS or AFF appliance that is used for failover in a disaster. One example is having a primary ONTAP system that provides storage for a hypervisor for virtual servers. The primary system would use SnapMirror to mirror the storage for the hypervisor to a secondary ONTAP system with the ability to fail over the virtual machines to the secondary ONTAP system in the event of a major outage. This approach would allow for business continuity. The same storage could be replicated to AltaVault for longer term backup using cloud storage.

Figure 8) Multiple cascade to AltaVault appliance.



2.6 SnapMirror Network Configuration

ONTAP requires SnapMirror traffic to use an intercluster (IC) logical interface (LIF). At least one intercluster LIF per cluster node must be configured. It is possible for an intercluster LIF to share the same port as a data or management interface. However, an intercluster LIF cannot share a port used for the cluster network. Each intercluster LIF requires an IP address.

Table 9) ONTAP networking terminology.

Terminology	Description
Cluster peering	The act of connecting two clusters to allow replication to occur between them.
Intercluster logical interfaces	Logical network interfaces used for intercluster communication.
Intercluster ports	Ports dedicated to intercluster replication.

For AltaVault, it is recommended that data interfaces are used for connections to back up data sources and restore traffic. This same recommendation also applies in the case of SnapMirror replication and is especially important for physical appliances where the data interfaces are often 10 Gb Ethernet. An AltaVault appliance supports using data interfaces directly or by combining one or more data interfaces into a bonded configuration. Bonded interfaces on an AltaVault appliance are called virtual interfaces, or VIFs. Each data interface or VIF requires an IP address.

Note: If a physical data interface port is configured in a VIF, the data port is not assigned an IP. Instead, it shares the IP address of the VIF with the other data interfaces defined in the VIF.

Note: When a data interface is part of a VIF, the data interface UI page might not show an accurate link state. The interface counters report shows an accurate link state.

AltaVault also supports use of VLAN tagging where each VLAN creates a logical subinterface. Refer to the AltaVault Administration Guide in the product documentation located on the NetApp Support site for more information.

SnapMirror Network Communication

SnapMirror transfers (updates or restores) from an ONTAP cluster use one TCP session for the life of the transfer. If multiple IC LIFs are configured, only one is used for a single transfer. Multiple transfers each use an IC LIF to distribute load across interfaces. There is no intelligent load balancing for use of multiple IC LIFs. Selection of a LIF does not depend on the latency of the connection.

ONTAP uses all the intercluster LIF interfaces to communicate SnapMirror traffic to and from the AltaVault appliance. The interfaces are selected based on the interface speed. A single interface is used for a single SnapMirror session. Multiple interfaces of the same speed are used round robin. SnapMirror to AltaVault uses a simple mechanism for load balancing. All intercluster LIFs need to be added to the AltaVault whitelist.

SnapMirror to AltaVault does not support checkpoint restarts. If a transfer fails, a restart of the transfer starts from the beginning.

3 Deploy AltaVault with SnapMirror

The overall process to deploy SnapMirror to AltaVault begins by configuring the feature on the AltaVault appliance and configuring access control.

The remaining steps are performed on the ONTAP cluster that does SnapMirror replication to the AltaVault appliance.

AltaVault steps:

1. Deploy and configure for cloud storage.
2. Enable SnapMirror shares.
3. Configure access control using whitelist.

ONTAP steps:

1. Configure policies:
   a. Schedule policy
   b. Snapshot policy
   c. Protection policy
2. Create and initialize a relationship.

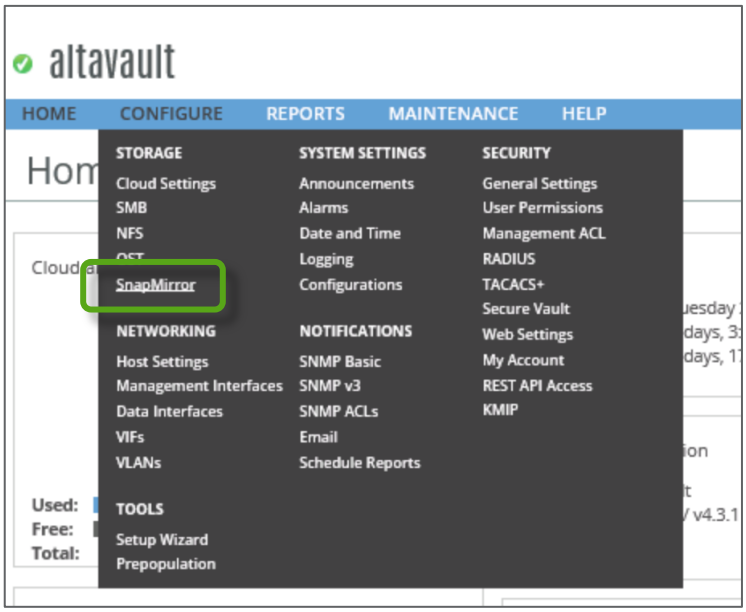
3.1 AltaVault Configuration

Deploy the AltaVault appliance and configure cloud storage according to the instructions in the AltaVault Administration Guide in the product documentation available on the NetApp Support site.

Enable SnapMirror

1. Choose SnapMirror from the Configure menu in the Storage section.

Figure 9) AltaVault SnapMirror configuration menu.

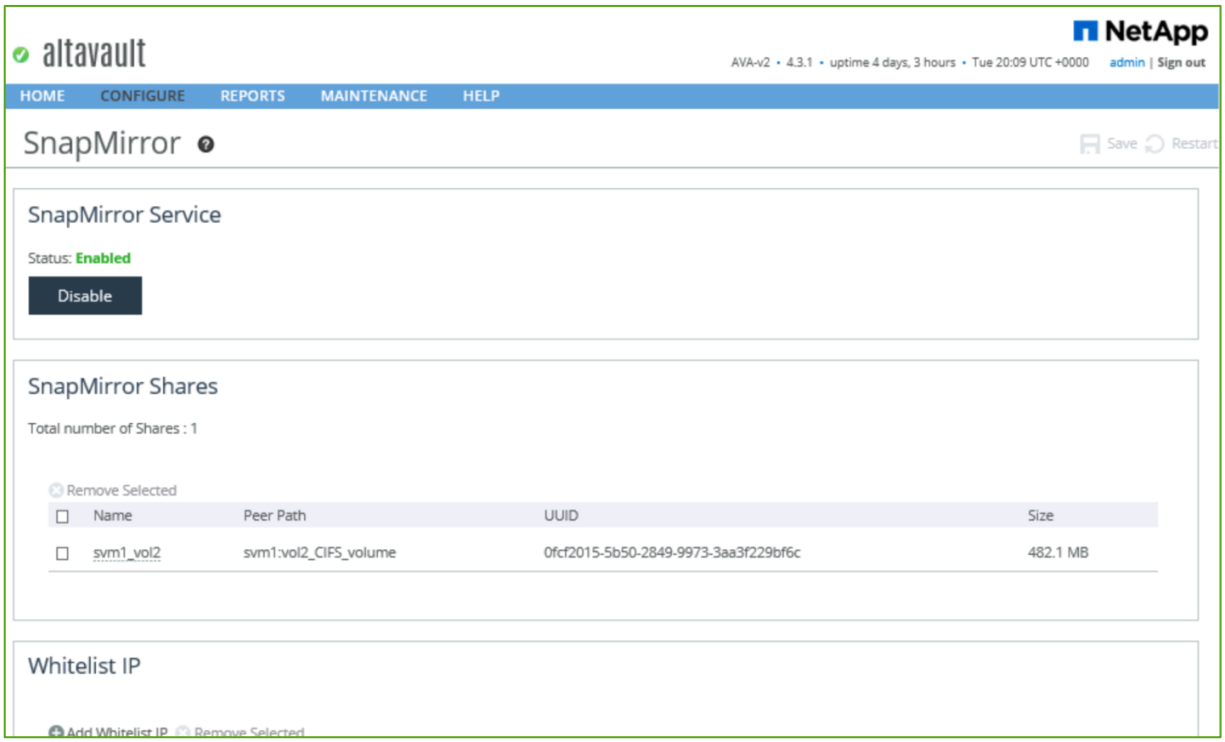


2. Click the enable button in the SnapMirror Service section.

3. Restart the optimization service using the restart button that is highlighted in the upper-right corner of the AltaVault admin UI. Optionally, you can choose Service in the Maintenance menu and click the restart button.

Note: Restarting the service affects any operations to other shares such as SMB, NFS, or OST. Make sure that no backups or restores are occurring (no reads or writes to any shares).

Figure 10) AltaVault SnapMirror service enabled.



Configure Whitelist IP

Access control between ONTAP clusters is done using the cluster peering procedure. The cluster peering procedure provides permissions for two clusters to share data using SnapMirror. This approach makes sure that the admin of each cluster has authenticated and allows the two clusters to exchange SnapMirror data.

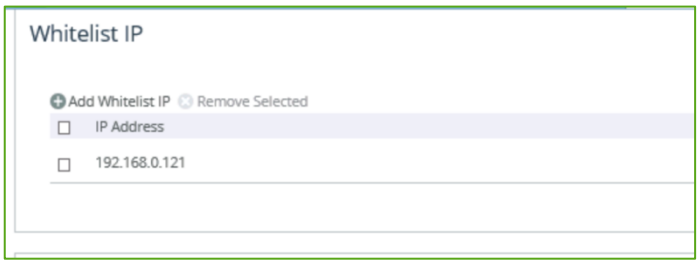
AltaVault does not use cluster peering to control access for SnapMirror. Access control is done using an IP whitelist. The IP addresses in the whitelist are the intercluster LIF IP addresses from the ONTAP cluster that perform SnapMirror backup and restore to the AltaVault appliance.

Note: Ping the IP addresses of the intercluster LIFs from the AltaVault CLI to make sure of connectivity of all interfaces.

Note: AltaVault currently only supports IPv4.

1. Choose SnapMirror from the Configure menu in the Storage section.
2. Click the button beside Add Whitelist IP.
3. Enter the IP address for an intercluster LIF interface from the cluster that uses SnapMirror with the AltaVault appliance.
4. Repeat steps 2 and 3 for all of the intercluster LIF interfaces on the cluster.

Figure 11) AltaVault SnapMirror whitelist.



Access control from the ONTAP or source side of the SnapMirror relationship is done automatically at the time a relationship is created. Instead of performing cluster peering to allow SnapMirror traffic from the cluster, peering is automatic to AltaVault. From the authentication standpoint, all the data transfer is initiated from the ONTAP cluster and requires authorization of the ONTAP user to initiate any relationships. Movement of data is always initiated from the ONTAP cluster and not from AltaVault.

From the AltaVault perspective, the preceding steps are all that are needed from the AltaVault configuration to begin using it as a destination for SnapMirror relationships.

3.2 ONTAP Policy Overview

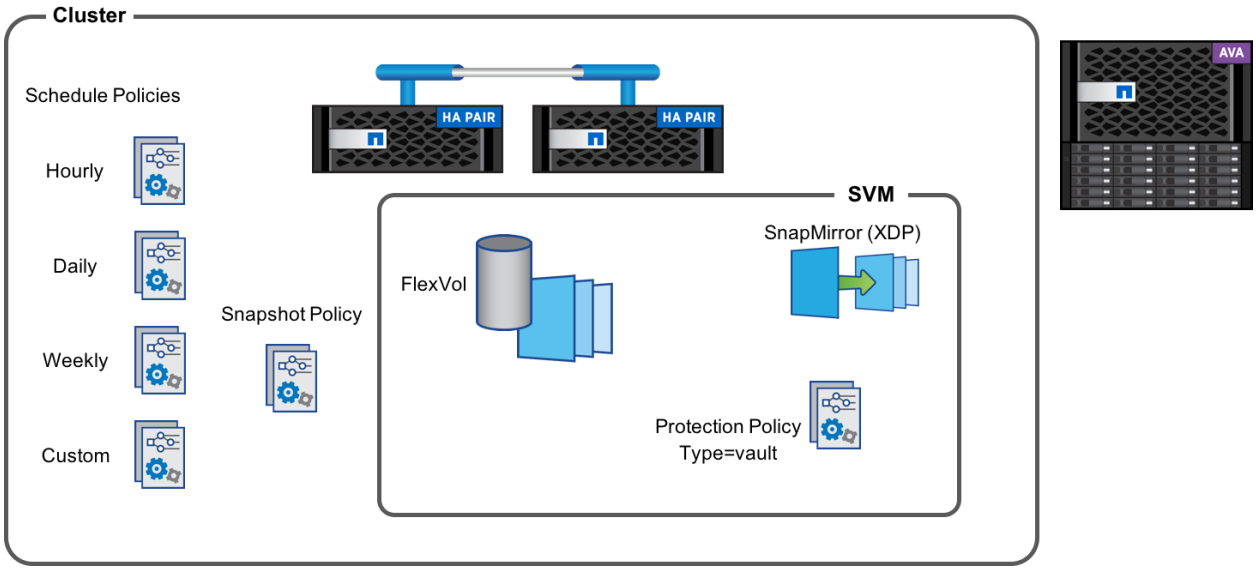
ONTAP policies are used to control schedules and retentions for Snapshot creation and replication to AltaVault as well as retention of Snapshot copies.

Several policy types work together to manage the various aspects of the solution:

- **Schedule policies.** Determine when Snapshot copies are created or when SnapMirror updates occur. They have a cluster-wide scope.
- **Snapshot policies.** Determine when Snapshot copies are created, labels applied, and retention of Snapshot copies on the primary volume. They have a cluster-wide scope.
- **Protection policies.** Determine the labels that are replicated and the retention of the secondary or backup copies. They have a storage virtual machine (SVM) scope.

Policies can be created using System Manager or using the ONTAP CLI.

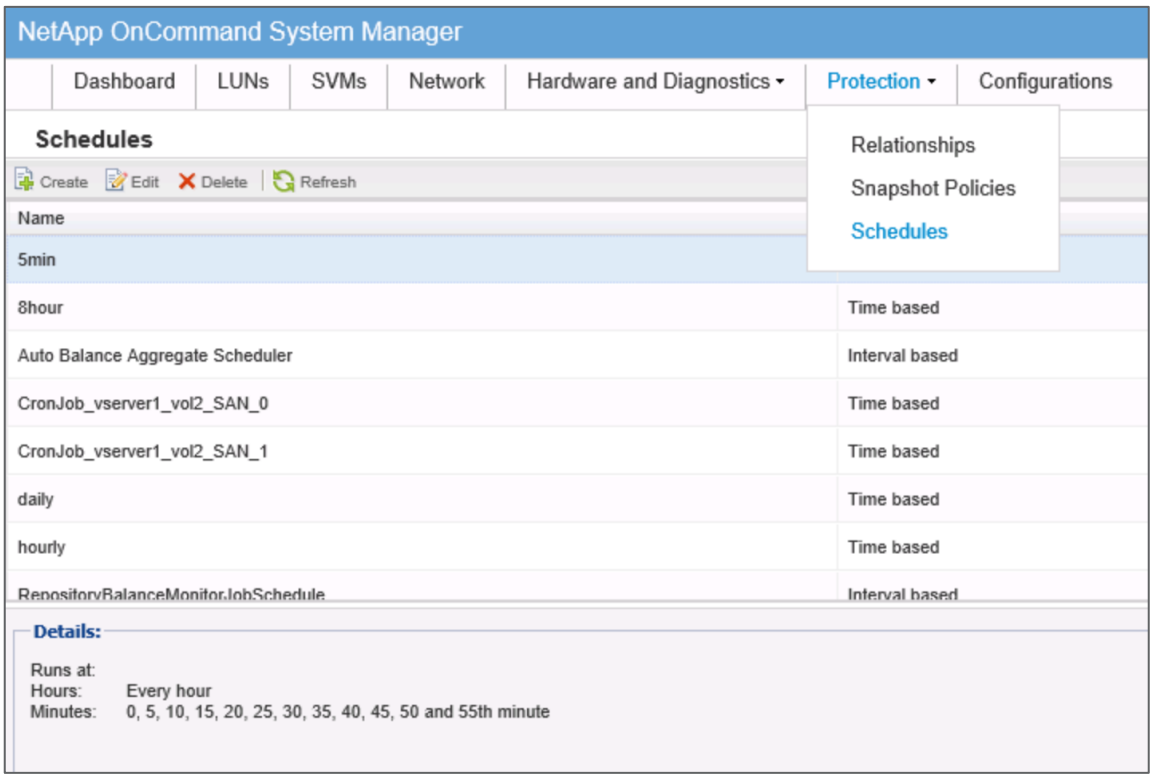
Figure 12) Policy relationship overview.



3.3 Schedule Policy

A schedule policy is an ONTAP policy that is assigned to a job to execute on a specific time interval. Schedule policies apply to the entire cluster.

Figure 13) Schedule policy example in System Manager.



A schedule policy is created either from the cluster CLI or using System Manager. The policy defines the time a job is executed as well as the frequency of the job.

In System Manager, the schedule policy is created with a cluster-wide scope from the Protection menu.

For most installations, the predefined ONTAP schedule policies are enough. If a custom policy is needed, consult the ONTAP product documentation for more information.

3.4 Snapshot Policy

A Snapshot policy can be configured in several ways. Overall, the functionality is to establish the schedule for performing Snapshot copies for a volume and the retention of the Snapshot copies. Snapshot policies also contain a SnapMirror label that is used to match a protection policy that is required to perform policy-based SnapMirror replication.

Create Snapshot policies using:

- System Manager:
  - Protection menu, Snapshot policies
  - Select an SVM: SVM settings menu, policies section, Snapshot policies
- Command line:
  - Snapshot policy create
  - Volume Snapshot policy create

Snapshot policies created using the Protection menu are assigned to the default SVM that represents the cluster.

Snapshot policies created from the SVM settings apply to that SVM.

When creating Snapshot policies on the command line, it is possible to specify the SVM to which the policy is assigned. This approach is most useful on a cluster that is multitenant and allows for the SVM administrator to manage those policies. If an SVM is not specified, the new policy uses the default SVM, as shown in the help syntax.

Snapshot Copies on Primary Volume

The primary volume is the originating source of the data that is replicated to AltaVault. The primary or source volume must have a Snapshot policy that determines when the Snapshot copies are created, label prefixes used for the Snapshot copies to use in a protection policy, and the retention of the Snapshot copies on the source volume.

Snapshot retentions are handled by various policies in ONTAP depending on the location of the Snapshot copies. For a primary volume, a Snapshot policy is created with a cluster-wide scope. This policy can be created from System Manager by selecting Protection from the main menu and choosing the Snapshot Policies menu.

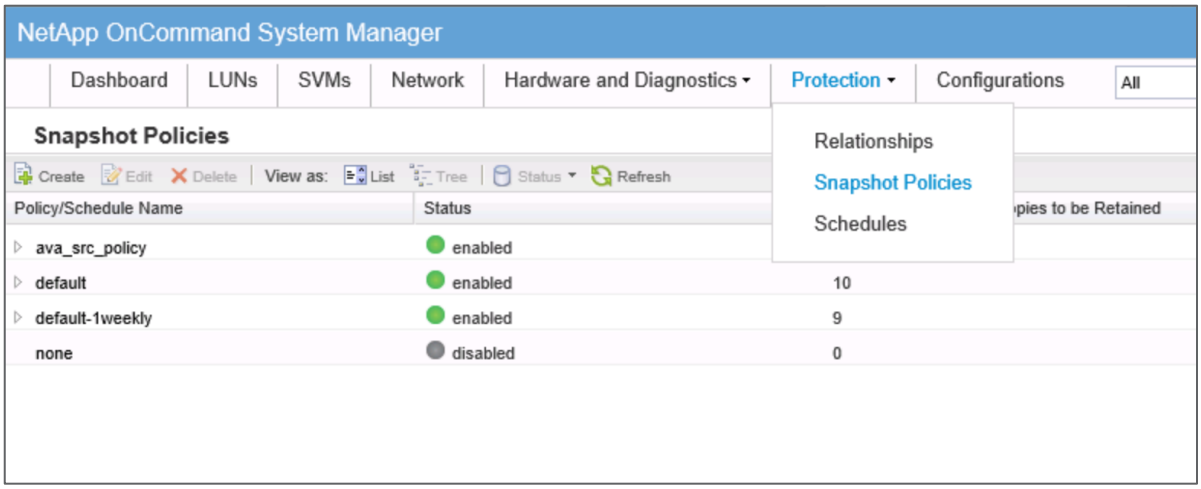
A Snapshot policy can automatically manage Snapshot copy schedules and retention on FlexVol® volumes. You must be a cluster administrator or storage virtual machine (SVM) administrator to perform most of the Snapshot policy commands.

Snapshot copy name settings are applied to a volume. The name setting determines the format of the Snapshot copy name. The format can use one of two name generation methods: ordinal or time stamp based. When a Snapshot copy is created by a Snapshot policy, the name typically consists of a prefix specified in the Snapshot policy combined with a time stamp. When manually creating Snapshot copies, it is also possible to specify a name for the Snapshot copy. Snapshot copy names have a limit of 255 characters.

Figure 14) Example: ordinal Snapshot name.

```
df1-cl1::> snap list
                                                              ---Blocks---
Vserver  Volume   Snapshot                                  Size Total% Used%
-------- -------- ------------------------------------ -------- ------ -----
df1-cl1-01
         vol0
                  hourly.0                                2.18MB     0%    1%

df1-cl1::>
```

Figure 15) System Manager Snapshot policies.



Snapshot Policy Create Syntax

The command line syntax to create a Snapshot policy includes the ability to specify multiple schedules. A total of five is possible. Each schedule specified includes a name, the number of Snapshot copies to retain for this schedule, a prefix for the Snapshot name, and a SnapMirror label.

```
snapshot policy create
  [ -vserver <vserver name> ]                Vserver Name (default: cluster1)
   [-policy] <snapshot policy>               Snapshot Policy Name
   [-enabled] {true|false}                   Snapshot Policy Enabled
  [ -comment <text> ]                        Comment
   [-schedule1] <text>                       Schedule1 Name
   [-count1] {0..255}                        Maximum Snapshot Copies for Schedule1
  [ -prefix1 <text> ]                        Snapshot Copy Name Prefix for Schedule1
  [ -snapmirror-label1 <text (size 0..31)> ] Label for SnapMirror Operations for Schedule1
  [ -schedule2 <text> ]                      Schedule2 Name
  [ -count2 {0..255} ]                       Maximum Snapshot Copies for Schedule2
  [ -prefix2 <text> ]                        Snapshot Copy Name Prefix for Schedule2
  [ -snapmirror-label2 <text (size 0..31)> ] Label for SnapMirror Operations for Schedule2
  [ -schedule3 <text> ]                      Schedule3 Name
  [ -count3 {0..255} ]                       Maximum Snapshot Copies for Schedule3
  [ -prefix3 <text> ]                        Snapshot Copy Name Prefix for Schedule3
  [ -snapmirror-label3 <text (size 0..31)> ] Label for SnapMirror Operations for Schedule3
  [ -schedule4 <text> ]                      Schedule4 Name
  [ -count4 {0..255} ]                       Maximum Snapshot Copies for Schedule4
  [ -prefix4 <text> ]                        Snapshot Copy Name Prefix for Schedule4
  [ -snapmirror-label4 <text (size 0..31)> ] Label for SnapMirror Operations for Schedule4
  [ -schedule5 <text> ]                      Schedule5 Name
  [ -count5 {0..255} ]                       Maximum Snapshot Copies for Schedule5
  [ -prefix5 <text> ]                        Snapshot Copy Name Prefix for Schedule5
  [ -snapmirror-label5 <text (size 0..31)> ] Label for SnapMirror Operations for Schedule5
```

Example of creating a Snapshot policy:

```
snapshot policy create -policy snap_policy1 -prefix1 hourly -snapmirror-
label1 ava_hourly -count1 24 -schedule1 hourly -prefix2 daily -snapmirror-
label2 ava_daily -count2 7 -schedule2 daily -prefix3 weekly -snapmirror-
label3 ava_weekly -count3 5 -schedule3 weekly -enabled true -comment "Source
Snapshot Policy"
```

Policies are viewed either in System Manager or using the Snapshot policy show command.

Example of Snapshot policy show:

```
cluster1::> snapshot policy show
Vserver: cluster1
Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
default                          3 true    Default policy with hourly, daily & weekly schedules.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     ----------------------- -------------------
    hourly                     6     hourly                -
    daily                      2     daily                 daily
    weekly                     2     weekly                weekly

default-1weekly                  3 true    Default policy with 6 hourly, 2 daily & 1 weekly
schedule.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     ----------------------- -------------------
    hourly                     6     hourly                -
    daily                      2     daily                 -
    weekly                     1     weekly                -

none                             0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     ----------------------- -------------------
    -                          -     -                     -

snap_policy1                     3 true    Source Snapshot Policy
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     ----------------------- -------------------
    hourly                    24     hourly                ava_hourly
    daily                      7     daily                 ava_daily
    weekly                     5     weekly                ava_weekly

4 entries were displayed.

cluster1::>
```

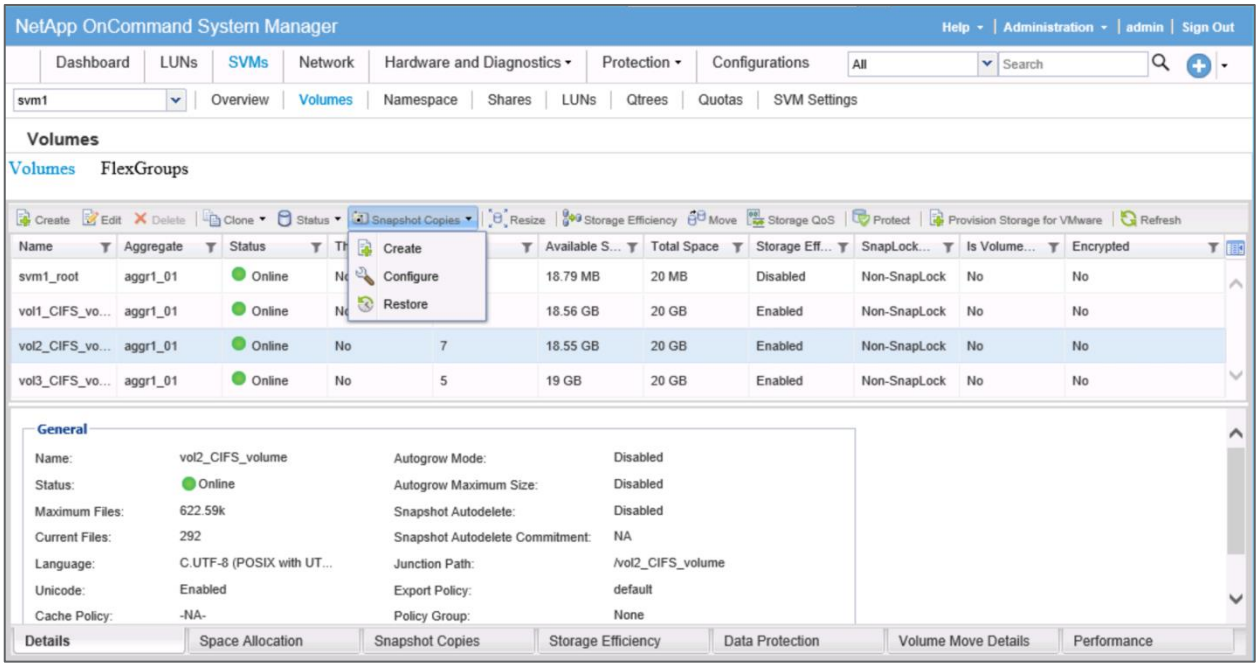
ONTAP has a default Snapshot policy that is included in a cluster installation. It is possible to modify the default policy to match specific needs. It is also possible to assign a policy to an SVM that applies to new volumes as part of the `vserver create` command or in the `vserver modify` command by specifying the policy name with the `-snapshot-policy` option.

Assign a Snapshot Policy to an Existing Volume

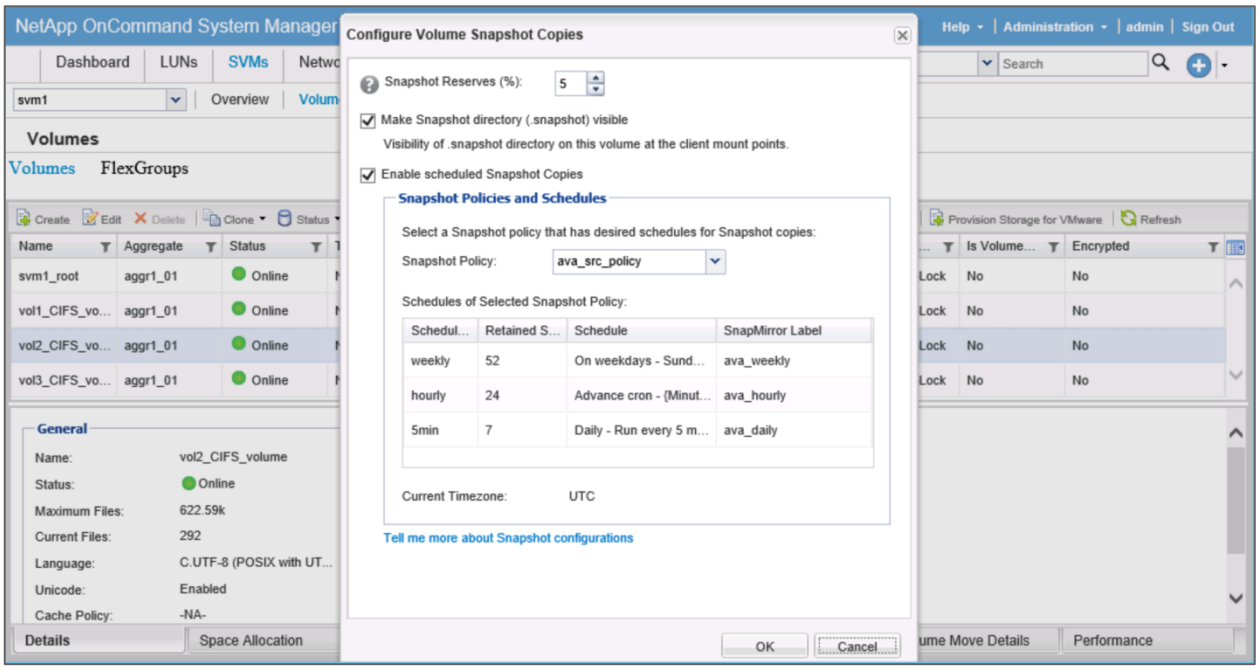
A policy must be assigned or associated to one or more volumes. The assignment can be performed in System Manager or using the command line on the cluster.

Assign a Snapshot creation policy in System Manager:

1. Log in to System Manager.
2. Choose the SVMs menu.
3. Select the SVM to manage.
4. Select the Volumes menu from the SVM menu.
5. Select the volume to modify from the list of volumes.
6. Select the Snapshot Copies drop-down menu.
7. Choose Configure to open the Snapshot configuration dialog box.



8. Check Enable Scheduled Snapshot Copies.
9. From the Snapshot Policy drop-down menu, select the name of the policy to assign.
10. Click OK to close the dialog box.



Example of assigning a Snapshot policy to a volume:

```
volume modify -vserver svm1 -volume vol2 -snapshot-policy snap_policy1
```

Note: If only one data vserver exists, -vserver can be omitted, and the data vserver is automatically selected.

Snapshot Policy Commands

Table 10) Snapshot policy-related commands.

Command	Description
volume snapshot policy show	Show information about a Snapshot policy for a volume.
volume snapshot policy create	Create a Snapshot policy.
volume snapshot policy add-schedule	Add a schedule to an existing Snapshot copy policy. A Snapshot policy can have up to five schedules.
volume snapshot policy remove-schedule	Remove a schedule from an existing Snapshot copy policy.
volume snapshot policy modify-schedule	Modify a schedule of an existing Snapshot copy policy.
volume snapshot policy modify	Modify the description of an existing Snapshot copy policy.
volume modify	Associate a Snapshot copy policy with a volume.
volume snapshot policy delete	Delete an existing Snapshot copy policy.
vserver modify	View or set the default Snapshot policy for an SVM.

For additional information, refer to the ONTAP 9 Data Protection Using SnapMirror and SnapVault guide in the product documentation.

3.5 Protection Policy

Managing Retention of SnapMirror Snapshot Copies on AltaVault

A protection policy is used to manage retention of Snapshot copies on an AltaVault appliance. The protection policy is part of the SVM configuration and is created on the cluster that is the source of SnapMirror replication. The policy contains rules that match a SnapMirror label. The matching rules define the Snapshot copies that are replicated to the AltaVault appliance as well as the retention.

AltaVault supports an extended retention for Snapshot copies, referred to as long-term retention in the AltaVault GUI. The extended retention mode should only be enabled when using an external system to manage Snapshot retention, such as SnapCenter. In a typical configuration with AltaVault and an ONTAP system, extended retention is not used. This approach allows an ONTAP protection policy to manage retention of the Snapshot copies on the AltaVault appliance. When an external system is configured to manage retentions, the extended retention can be used. This setting on the AltaVault appliance ignores Snapshot deletes from the source ONTAP system to allow up to the maximum retention on the AltaVault appliance. After the AltaVault appliance reaches the maximum of 3,700 Snapshot copies, the oldest is deleted as a new Snapshot copy is synced.

ONTAP 9.1 supports up to 251 Snapshot copies for a SnapMirror XDP endpoint. This amount is the maximum number of Snapshot copies that can be managed in an ONTAP protection policy of type vault.

Note: If a data protection vault policy is not specified when creating a relationship, the xdp default policy is assigned.

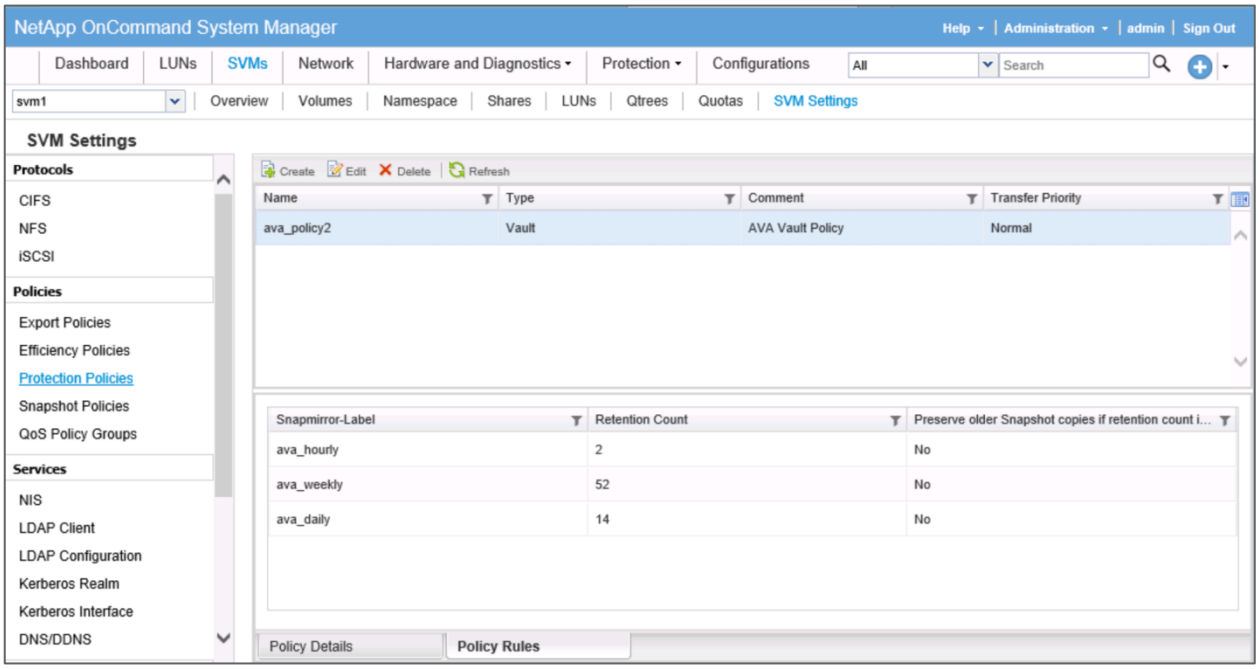
Note: The '-schedule' and '-prefix' options should not be set in rules for policies used for relationships between ONTAP and AltaVault. Rules that contain these options are ignored.

Example of a data protection vault policy:

```
snapmirror policy create ava_policy1 -vserver svm1 -type vault -comment "AVA
Vault Policy"

snapmirror policy add-rule -vserver svm1 ava_policy1 -snapmirror-label
ava_hourly 8

snapmirror policy add-rule -vserver svm1 ava_policy1 -snapmirror-label
ava_daily 100

snapmirror policy add-rule -vserver svm1 ava_policy1 -snapmirror-label
ava_weekly 50
```

In the previous example, a policy is created of type vault. Rules are assigned with labels that match labels specified in the Snapshot schedule. Any Snapshot copies created with the labels matching a rule are replicated to AltaVault. The policy also specifies the retention of Snapshot copies on AltaVault. In the preceding example, 8 hourly Snapshot copies, 100 daily Snapshot copies, and 50 weekly Snapshot copies are retained on the share of the AltaVault appliance.

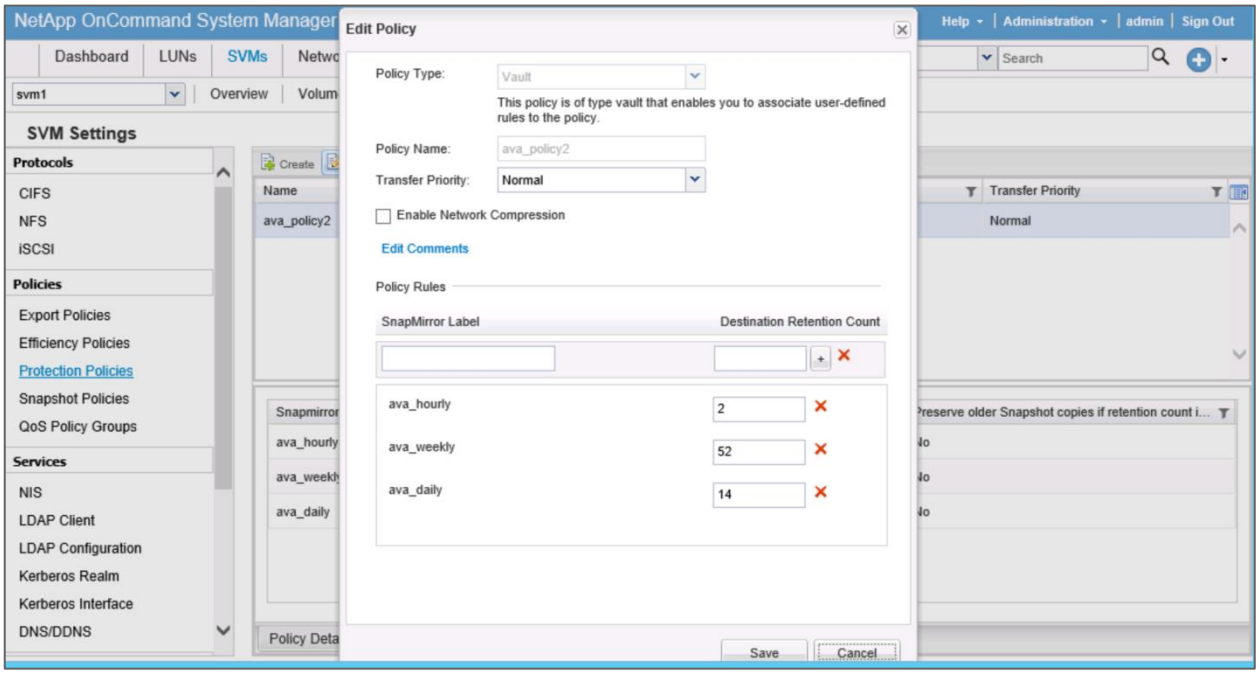
Figure 16) View a protection policy in System Manager.



Create a policy in System Manager:

1. Log in to System Manager.
2. Choose the SVMs menu.
3. Select the SVM to manage.
4. Select SVM Settings from the SVM menu.
5. Select Protection Policies from the Policies section on the left.
6. Click the Create button.
7. Select the vault policy type from the drop-down menu.
8. Enter a policy name.
9. Enter the first SnapMirror label to match (from a Snapshot policy).
10. Enter the number of Snapshot copies with this label to retain on AltaVault.
11. Click the add “+” button.
12. Repeat steps 9 to 11 as appropriate.
13. Click the Save button to save the new policy.

Figure 17) Create a protection policy in System Manager.



Note: Do not select Enable Network Compression. SnapMirror to AltaVault does not support compression.

3.6 Creating a Relationship

When creating SnapMirror relationships between two separate ONTAP clusters, the relationship is created on the destination cluster. When creating relationships with AltaVault, the process differs in that the creation takes place on the ONTAP cluster that is replicating to the AltaVault appliance. AltaVault endpoints for SnapMirror are created from the ONTAP cluster side because AltaVault does not have the functionality to create relationships.

Peering is another function that differs when using AltaVault as a SnapMirror target. Peering is a mechanism to provide permissions for performing SnapMirror transfers between systems. When AltaVault is an endpoint, the usual peering process is not used. Authentication from the AltaVault side is done using a whitelist of IP addresses. Because the commands are executed from the ONTAP cluster, peering is automatic from the source side. The only time peering is needed is when there is a cascade that requires two or more cluster ONTAP systems to replicate to each other.

An IP address used to identify the AltaVault appliance that is the destination for a replication relationship. DNS names are not supported for creating SnapMirror relationships with an AltaVault appliance.

Note: It is recommended to ping all the intercluster LIF IPs on the cluster from the AltaVault CLI before creating a relationship.

It is recommended to test and make sure all intercluster LIF IP addresses can communicate with the AltaVault appliance. The best way to check is to log in to the AltaVault appliance CLI using either the serial console or Secure Shell (SSH). If you perform the test from the ONTAP cluster, make sure that the ping syntax is using the actual IC LIF interfaces. Otherwise, the cluster management interface is used, and the check is invalid.

Note: A SnapMirror relationship to AltaVault must be created from the source ONTAP cluster using the CLI. System Manager does not currently support creating relationships that do not use ONTAP.

Example for creating a relationship:

```
snapmirror create -source-path svm1:/vol2 -destination-path
192.168.0.75:/share/svm1_vol2 -type XDP -policy ava_policy1 -schedule hourly
```

The example creates a relationship for `vol2` on `svm1`. The corresponding share name on the AltaVault appliance is `svm1_vol2`. The policy type `XDP` is required. The schedule `hourly` updates the SnapMirror relationship each hour as specified in the `hourly` schedule policy.

The SnapMirror create command is issued on the ONTAP cluster that contains vol2 and is the source of the replication to the AltaVault appliance.

```
snapmirror create -source-path <vserver>:/<volume> -destination-path
<IP_address>:/share/<share_name> -type XDP –policy <dp-policy> -schedule
```

```
snapmirror create -source-path svm1:vol2 -destination-path
192.168.0.75:/share/vol2 -type XDP
```

Note: For the ONTAP source volume path, /vol/ is optional. A path can be entered as either svm:/vol/myvol or svm:myvol, where svm is the name of the storage virtual machine, and myvol is the name of the source volume from that SVM.

```
cluster1::> vserver show
                                 Admin      Operational Root
Vserver     Type    Subtype      State      State       Volume     Aggregate
----------- ------- ---------- ---------- ----------- ---------- ----------
cluster1    admin   -          -          -           -          -
cluster1-01 node    -          -          -           -          -
svm1        data    default    running    running     svm1_root  aggr1_01
3 entries were displayed.

cluster1::>

cluster1::> snapmirror create -source-path svm1:/vol/vol2_CIFS_volume -destination-path
192.168.0.75:/share/svm1_vol2 -type XDP -policy ava_policy2 -schedule hourly
Operation succeeded: snapmirror create for the relationship with destination
"192.168.0.75:/share/svm1_vol2".


cluster1::> snapmirror show
                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
svm1:vol2_CIFS_volume
            XDP  192.168.0.75:/share/svm1_vol2
                             Uninitialized
                                     Idle           -         true    -

cluster1::>
```

Note: SnapLock® volumes are not supported.

Note: FlexGroups are not supported.

4 Backup and Restore

4.1 SnapMirror Initialize: First Backup

The first backup occurs after the SnapMirror relationship is initialized. This backup initiates a baseline transfer of the volume. The baseline transfer sends all of the existing data from the volume to the AltaVault appliance in a baseline Snapshot copy that is created by the initialize command. It is possible to specify a Snapshot copy using the `-source-snapshot` option of the `snapmirror initialize` command. Otherwise, a new Snapshot copy is created and used for the baseline transfer.

The baseline transfer sends only the Snapshot copy used for the initialize command. After the baseline transfer completes, additional Snapshot copies are sent in the next SnapMirror update using the DP policy settings. Snapshot copies can also be sent manually using the steps in the manual backup section.

```
snapmirror initialize -source-path <[vserver:][volume]> -destination-path
<hostip:/share/share-name> [-source-snapshot | -s <text>]

snapmirror initialize -source-path svm1:/vol2_CIFS_volume -destination-path
192.168.0.75:/share/svm1_vol2
```

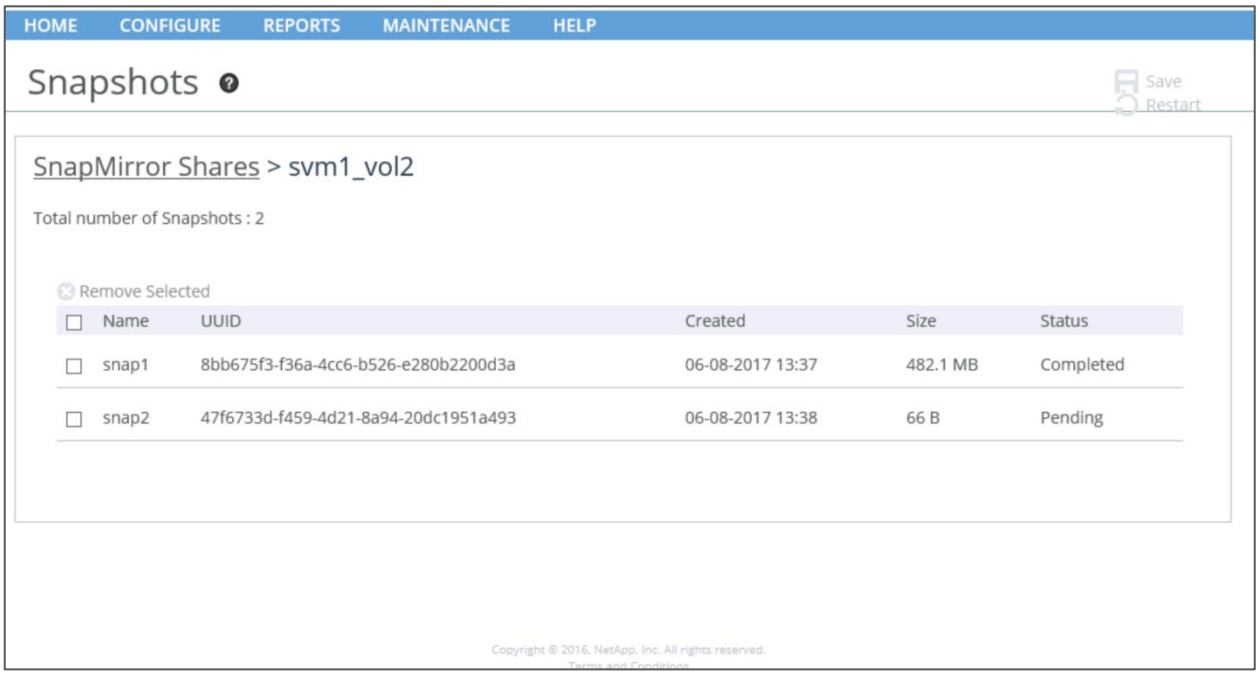
Checking the status of the baseline transfer can be done from the AltaVault appliance or from the ONTAP command line. Issuing the `snapmirror show` command displays the status for all relationships. It is possible to restrict the list by entering the source path, destination path, relationship type, or relationship status. See the ONTAP 9 Commands manual page reference for more information.

The following is an example of a SnapMirror show command with a relationship in the baseline transfer process. The state is uninitialized, and the status shows transferring. The progress indicates the amount of data sent.

```
cluster1::> snapmirror show
Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
svm1:vol2_CIFS_volume
            XDP  192.168.0.75:/share/svm1_vol2
                             Uninitialized
                                     Transferring   0B        true    06/03 02:20:07

cluster1::>
```

The following is an example of a SnapMirror show command with a relationship with the baseline transfer process completed. The state is now `SnapMirrored`, and the status is idle.

```
cluster1::> snapmirror show
                                                                    Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
svm1:vol2_CIFS_volume
            XDP  192.168.0.75:/share/svm1_vol2
                             Snapmirrored
                                     Idle           -         true    -

cluster1::>
```



4.2 Perform a Manual Backup

Occasionally it might be necessary to perform a manual backup of a volume. A manual backup consists of creating a named Snapshot copy and then manually initiating replication using a SnapMirror update.

Performing a backup of a volume is done using a snapshot create command on the ONTAP cluster that contains the source volume.

```
snapshot create -vserver svm1 -volume vol2_CIFS_volume -snapshot snap1
```

After the Snapshot copy is created, initiate replication using the following command. The Snapshot copy created in the previous step is specified using the `-s` option.

```
snapmirror update -source-path svm1:vol2_CIFS_volume -destination-path
192.168.0.75:/share/svm1_vol2 -s snap1
```

It is possible to view the status of the Snapshot transfer (update) from ONTAP or using the AltaVault web interface or CLI.

4.3 Overview of Restoring Data

Restoring data from a SnapMirror destination other than ONTAP differs from restoring data from an ONTAP destination. Similar to backup operations, the restore process is performed from the ONTAP system that is the location for the restore, which is typically the same ONTAP cluster that is the source of the backups. There are several things to consider when performing SnapMirror operations to an AltaVault appliance:

- AltaVault shows Snapshot names, but does not have a way to view Snapshot contents.
- AltaVault does not provide the .snapshot directory feature that is available in ONTAP.
- It is not possible to mount a Snapshot copy located on an AltaVault appliance.

Restoring data is performed using the SnapRestore feature of ONTAP by an administrator using the ONTAP CLI. Verify the ONTAP cluster is properly licensed for the SnapRestore feature for each cluster that is performing restores. It is possible to restore data to any cluster node that has access configured on the AltaVault appliance using the IP whitelist.

Note: System Manager does not currently support restore of data from a replication target other than ONTAP. It is possible to use System Manager to restore Snapshot copies that are located in the primary volume.

SnapMirror has a maximum number of transfers that can occur concurrently both for ONTAP and for the AltaVault appliance, as described in section 2 of this guide. Restore operations are considered regular SnapMirror transfers and count in the total of 100 concurrent transfers. For example, if 98 SnapMirror update transfers (backups) are in progress, 2 concurrent restore operations can be executed to reach the total maximum of 100 transfers. It should also be noted that each restore operation (command) entered counts as a single SnapMirror transfer even if the restore command includes more than one file.

Restore operations have a performance aspect related to the number of Snapshot copies retained. It is important to understand that due to the forever incremental backup model of SnapMirror, a restore operation iterates through each Snapshot copy to construct a restore stream. The restore process has optimizations when traversing older Snapshot copies that might reduce the effect. Iterating through a deep Snapshot list takes time, and restores are slower when performed on a share with large number of Snapshot copies, for example, 100 or more Snapshot copies, compared to a share with a small number of Snapshot copies.

Note: AltaVault SnapMirror shares are not mountable using NFS or SMB. SnapMirror shares can only transfer data using SnapMirror protocol. It is not possible to mount and browse a Snapshot copy on an AltaVault appliance.

4.4 File Restore

File restores are performed using SnapRestore incremental restore. This restore performs an incremental SnapRestore restoration of the files included in the command's file list from the Snapshot copy specified as the source Snapshot copy. The destination is the active file system on the volume indicated in the restore command.

When a file restore is performed, the data is restored to the file located in the active file system. Use caution when restoring files to the original location. After the operation is complete, the file is restored to the contents from the Snapshot copy specified, and any changes that have not been backed up are lost.

The following is an example of a restore command for a single file.

```
snapmirror restore -source-path 192.168.0.75:/share/svm1_vol2  -destination-
path svm1:vol2_CIFS_volume -source-snapshot snap1 -file-list /test1.txt
```

When using the –file-list option, a source Snapshot copy must be specified.

Note: AltaVault SnapMirror shares are not mountable using NFS or SMB. SnapMirror shares can only transfer data using SnapMirror protocol. It is not possible to mount and browse a Snapshot copy on an AltaVault appliance. Therefore, the exact name of a file and its path must be determined from ONTAP.

4.5 Multiple File Restore

Multiple files may be restored using the `-file-list` option of the `snapmirror restore` command. The syntax is similar to the single file restore and includes a comma-separated list of files.

Example syntax of a file list with multiple files:

```
-file-list /test1.txt,/dira/test2.txt,/myfile1.pptx
```

For more information, see the ONTAP 9 Commands manual page reference in the ONTAP 9 product documentation.

Multiple file restore limits vary by ONTAP and AltaVault version. The following table provides the limits for the versions used in this guide.

Table 11) Multiple file restore limits.

Version	Maximum Number of Files per Restore Operation
ONTAP 9.1	8
ONTAP 9.2	8
ONTAP 9.3	64
AltaVault OS 4.3	8
AltaVault OS 4.4	64

Note: ONTAP support for 64 files is only available when performing a restore from an AltaVault appliance.

4.6 Restoring a File to an Alternate Location

An alternate location restore can be accomplished in several ways. The intention is to not overwrite the source file and to place the restored data in a different location from the source data.

- Restore to a new location in the original source volume
- Create a new volume and restore to the new volume in the same cluster
- Create a new volume and restore to the new volume in a different cluster

It is possible to restore a file to a new location within the source volume by specifying an alternate path using the "`@`" syntax of the restore command. The syntax is to specify the file name, including path, as it existed in the original Snapshot copy, followed by "`, @`" and the new file name, including path.

When restoring a file to an alternate location, the path must exist before the restore command is executed. The restore command does not create a new path. The Snapshot copy must be specified, and the file must exist in that Snapshot copy. It is possible that a Snapshot copy that does not contain new data, for example, a 0-byte Snapshot copy, can be listed in the AltaVault appliance. However, the file exists in the Snapshot copy depending on when the file last changed.

Example syntax of a file list to restore to a different path:

```
-file-list /test1.txt,@/newdir/test1.txt
```

Example of restore to a different directory on the source volume using the same file name.

```
df1-cl2::> snapmirror restore -source-path 10.1.2.16:/share/df1-cl2-svm1_vol1  -destination-path
df1-cl2-svm1:vol1 -source-snapshot hourly.2017-09-05_1705 -file-list
/myfile1.txt,@/dir1/myfile1.txt
[Job 59] Job is queued: snapmirror restore from source "10.1.2.16:/share/df1-cl2-svm1_vol1" for
the snapshot hourly.2017-09-05_1705.

df1-cl2::>
```

```
df1-cl2::> snapmirror show
                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
10.1.2.16:/share/df1-cl2-svm1_vol1
            RST  df1-cl2-svm1:vol1
                             -       Idle           -         true    -
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                             Snapmirrored
                                     Idle           -         true    -
2 entries were displayed.

df1-cl2::> snapmirror show
                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                             Snapmirrored
                                     Idle           -         true    -

df1-cl2::>
```

Example of restore to a different directory on the source volume using a different file name.

```
df1-cl2::> snapmirror restore -source-path 10.1.2.16:/share/df1-cl2-svm1_vol1  -destination-path
df1-cl2-svm1:vol1 -source-snapshot hourly.2017-09-05_1805 -file-list /myfile2.txt,@/dir2/myfile2-
restored.txt
[Job 61] Job is queued: snapmirror restore from source "10.1.2.16:/share/df1-cl2-svm1_vol1" for
the snapshot hourly.2017-09-05_1805.

df1-cl2::> snapmirror show
                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
10.1.2.16:/share/df1-cl2-svm1_vol1
            RST  df1-cl2-svm1:vol1
                             -       Idle           -         true    -
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                             Snapmirrored
                                     Idle           -         true    -
2 entries were displayed.

df1-cl2::> snapmirror show
                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
```

```
----------- ---- ------------ ------- -------------- --------- ------- --------
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                                 Snapmirrored
                                         Idle           -         true    -

df1-cl2::>
```

Directory listing showing the restored file in the new location:

```
U:\>dir /s
 Volume in drive U is vol1
 Volume Serial Number is 806E-5180

 Directory of U:\

09/05/2017  06:09 PM    <DIR>          .
09/05/2017  06:09 PM    <DIR>          ..
06/02/2017  10:45 AM         1,130,328 ChromeSetup.exe
05/30/2017  04:47 PM        49,279,600 VMware-ClientIntegrationPlugin-5.5.0(1).e
xe
01/19/2017  04:14 PM         6,975,096 FileZilla_3.24.0_win64-setup.exe
12/13/2016  03:33 PM         1,159,168 altavault_ost_plug-in_1_1_n0.msi
09/05/2017  04:58 PM                37 myfile1.txt
09/05/2017  04:58 PM                19 myfile2.txt
09/05/2017  05:36 PM    <DIR>          dir1
09/05/2017  06:18 PM    <DIR>          dir2
               6 File(s)     58,544,248 bytes

 Directory of U:\dir1

09/05/2017  05:36 PM    <DIR>          .
09/05/2017  06:09 PM    <DIR>          ..
09/05/2017  05:36 PM                37 myfile1.txt
               1 File(s)             37 bytes

 Directory of U:\dir2

09/05/2017  06:18 PM    <DIR>          .
09/05/2017  06:09 PM    <DIR>          ..
09/05/2017  06:18 PM                19 myfile2-restored.txt
               1 File(s)             19 bytes

     Total Files Listed:
               8 File(s)     58,544,304 bytes
               8 Dir(s)     960,348,160 bytes free

U:\>
```

Restore Files to a Different Volume

A file can be restored to an alternate location by creating a new volume and restoring to the volume. The process is the same as the one described in the next section, “Restoring a Volume from a Snapshot Copy.” A volume is created, and the restore command is issued with the new volume as the destination. The files are specified with the new volume as the destination.

Note: The new volume is created as normal read/write type when restoring using –file-list.

Example commands to create a volume and restore two files:

```
volume create -vserver df1-cl2-svm1 -volume vol1_restore3 -aggregate agg1 -
size 1GB
```

```
snapmirror restore -source-path 10.1.2.16:/share/df1-cl2-svm1_vol1  -
destination-path df1-cl2-svm1:vol1_restore3 -source-snapshot hourly.2017-09-
06_0905 -file-list /myfile1.txt,/myfile2.txt
```

Example of using the previous commands to restore files to a new volume:

```
df1-cl2::> volume create -vserver df1-cl2-svm1 -volume vol1_restore3 -aggregate agg1 -size 1GB

Warning: The export-policy "default" has no rules in it. The volume will therefore be
inaccessible over NFS
         and CIFS protocol.
Do you want to continue? {y|n}: y
[Job 77] Job succeeded: Successful

df1-cl2::> volume show
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
df1-cl2-svm1
          df1cl2svm1_root
                       agg1         online     RW         20MB    18.73MB    6%
df1-cl2-svm1
          vol1         agg1         online     RW          1GB    915.6MB   10%
df1-cl2-svm1
          vol1_restore2
                       agg1         online     DP          1GB     1023MB    0%
df1-cl2-svm1
          vol1_restore3
                       agg1         online     RW          1GB    972.6MB    5%
df1-cl2-svm1
          vol_restore  agg1         online     RW          1GB    967.5MB    5%
df1-cl2_1 vol0         aggr0_df1_cl2_1_0
                                    online     RW          5GB     3.71GB   25%
6 entries were displayed.

df1-cl2::> snapmirror restore -source-path 10.1.2.16:/share/df1-cl2-svm1_vol1  -destination-path
df1-cl2-svm1:vol1_restore3 -source-snapshot hourly.2017-09-06_0905 -file-list
/myfile1.txt,/myfile2.txt
[Job 79] Job is queued: snapmirror restore from source "10.1.2.16:/share/df1-cl2-svm1_vol1" for
the snapshot hourly.2017-09-06_0905.

df1-cl2::> snapmirror show
Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
10.1.2.16:/share/df1-cl2-svm1_vol1
            RST  df1-cl2-svm1:vol1_restore3
                             -       Idle           -         true    -
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                             Snapmirrored
                                     Idle           -         true    -
2 entries were displayed.

df1-cl2::>

df1-cl2::> volume show
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
df1-cl2-svm1
          df1cl2svm1_root
                       agg1         online     RW         20MB    18.73MB    6%
df1-cl2-svm1
          vol1         agg1         online     RW          1GB    915.6MB   10%
df1-cl2-svm1
          vol1_restore2
                       agg1         online     DP          1GB     1023MB    0%
df1-cl2-svm1
```

```
          vol1_restore3
                       aggl         online     RW          1GB    972.5MB    5%
df1-cl2-svm1
          vol_restore  agg1         online     RW          1GB    967.5MB    5%
df1-cl2_1 vol0         aggr0_df1_cl2_1_0
                                    online     RW          5GB     3.71GB   25%
6 entries were displayed.

df1-cl2::>
```

```
X:\>net use
New connections will not be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           U:        \\df1-cl2-svm1\vol1
                                                 Microsoft Windows Network
OK           W:        \\df1-cl2-svm1\vol1_restore3
                                                 Microsoft Windows Network
OK           X:        \\df1-cl2-svm1\vol_restore
                                                 Microsoft Windows Network
The command completed successfully.


X:\>dir w:
 Volume in drive W is vol1_restore3
 Volume Serial Number is 806E-5183

 Directory of W:\

09/06/2017  10:00 AM    <DIR>          .
09/06/2017  10:00 AM    <DIR>          ..
09/06/2017  10:00 AM                37 myfile1.txt
09/06/2017  10:00 AM                19 myfile2.txt
               2 File(s)             56 bytes
               2 Dir(s)   1,019,744,256 bytes free

X:\>
```

4.7 Restoring a Volume from a Snapshot Copy

Restoring a volume is possible when restoring to a newly created volume of type DP. In this release, incremental restores are not supported from locations other than ONTAP. Incremental restores are required to restore a complete Snapshot copy to the source volume, which means that it is not possible to restore a complete Snapshot copy to the active file system of the original source volume. It is only possible to restore individual files using the procedures in the previous sections.

Note: Restore requires cluster administrator or SVM administrator privileges.

By default, the `snapmirror restore` copies the latest Snapshot copy from the source volume to the destination volume. A specific Snapshot copy can be selected with the `-source-snapshot` parameter.

The destination volume must be an empty data protection (DP) volume. The `snapmirror restore` command performs a baseline restore. For a baseline restore, the following steps are performed:

1. Create the RST SnapMirror relationship.
2. The entire contents of the Snapshot copy selected to be restored are copied to the active file system of the destination volume.
3. The destination volume is made read-write.

4. The RST SnapMirror relationship is deleted.

Note: Incremental restore from an endpoint other than Data ONTAP to a Data ONTAP volume is not supported.

Example of creating a new volume to use as a destination for a restore:

```
volume create -vserver df1-cl2-svm1 -volume vol_restore -aggregate agg1 -type
DP -size 1GB
```

Restore command example:

```
snapmirror restore -source-path 10.1.2.16:/share/df1-cl2-svm1_vol1  -
destination-path df1-cl2-svm1:vol_restore -source-snapshot hourly.2017-09-
06_0905
```

Example of performing a restore of a Snapshot copy to a new volume:

```
df1-cl2::> snapmirror restore -source-path 10.1.2.16:/share/df1-cl2-svm1_vol1  -destination-path
df1-cl2-svm1:vol_restore -source-snapshot hourly.2017-09-06_0905
[Job 67] Job is queued: snapmirror restore from source "10.1.2.16:/share/df1-cl2-svm1_vol1" for
the snapshot hourly.2017-09-06_0905.

df1-cl2::> snapmirror show
Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
10.1.2.16:/share/df1-cl2-svm1_vol1
            RST  df1-cl2-svm1:vol_restore
                              Snapmirrored
                                      Idle           -         true    -
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                              Snapmirrored
                                      Idle           -         true    -
2 entries were displayed.

df1-cl2::> snapmirror show
                                                                       Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
10.1.2.16:/share/df1-cl2-svm1_vol1
            RST  df1-cl2-svm1:vol_restore
                              Broken-off
                                      Idle           -         true    -
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                              Snapmirrored
                                      Idle           -         true    -
2 entries were displayed.

df1-cl2::>


df1-cl2::> volume show
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
df1-cl2-svm1
          df1cl2svm1_root
                       agg1         online     RW         20MB    18.77MB    6%
df1-cl2-svm1
          vol1         agg1         online     RW          1GB    915.7MB   10%
df1-cl2-svm1
```

```
          vol_restore  aggl         online     RW          1GB    967.5MB    5%
df1-cl2_1 vol0         aggr0_df1_cl2_1_0
                                    online     RW          5GB     3.74GB   25%
4 entries were displayed.

df1-cl2::>
```

Example of the directory after restoring from Windows:

```
X:\>dir
 Volume in drive X is vol_restore
 Volume Serial Number is 806E-5181

 Directory of X:\

09/05/2017  06:09 PM    <DIR>          .
09/05/2017  06:09 PM    <DIR>          ..
09/05/2017  06:18 PM    <DIR>          dir2
09/05/2017  05:36 PM    <DIR>          dir1
09/05/2017  04:58 PM                37 myfile1.txt
09/05/2017  04:58 PM                19 myfile2.txt
12/13/2016  03:33 PM         1,159,168 altavault_ost_plug-in_1_1_n0.msi
06/02/2017  10:45 AM         1,130,328 ChromeSetup.exe
01/19/2017  04:14 PM         6,975,096 FileZilla_3.24.0_win64-setup.exe
05/30/2017  04:47 PM        49,279,600 VMware-ClientIntegrationPlugin-5.5.0(1).e
xe
               6 File(s)     58,544,248 bytes
               4 Dir(s)   1,014,472,704 bytes free

X:\>net use
New connections will not be remembered.


Status       Local     Remote                    Network

-------------------------------------------------------------------------------
OK           U:        \\df1-cl2-svm1\vol1
                                                 Microsoft Windows Network
OK           X:        \\df1-cl2-svm1\vol_restore
                                                 Microsoft Windows Network

The command completed successfully.


X:\>
```

4.8 Monitoring Restore Operations

Monitoring the restore process and status is done from the ONTAP cluster on which the restore is being performed using `snapmirror show`. The event and job information in System Manager provides details about errors and a status for jobs.

Use the AltaVault appliance front-end report to see data transfers between ONTAP and the AltaVault appliance or the back-end report to see transfers between AltaVault and cloud object storage. In the case of errors, check for more details in the system log, available from the maintenance menu.

AutoSupport® allows for remote monitoring and troubleshooting for both ONTAP and AltaVault.

4.9 Clearing a Failed Restore Job

In the event that a restore request fails, it remains listed in the SnapMirror output until it is cleared. A failed restore request is listed in `snapmirror show` with a healthy status of false and a type of RST. Use the following option to clear a failed event.

```
-clean-up-failure true
```

Example showing a failed restore request:

```
df1-cl2::> snapmirror show
                                                                    Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
10.1.2.16:/share/df1-cl2-svm1_vol1
            RST  df1-cl2-svm1:vol1
                             -       Idle           -         false   -
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                             Snapmirrored
                                     Idle           -         true    -
2 entries were displayed.

df1-cl2::>
```

Repeat the restore request, appending the `-clean-up-failure` option to the restore with the source and destination paths. The job first changes healthy to true before it is removed from the `snapmirror show` output.

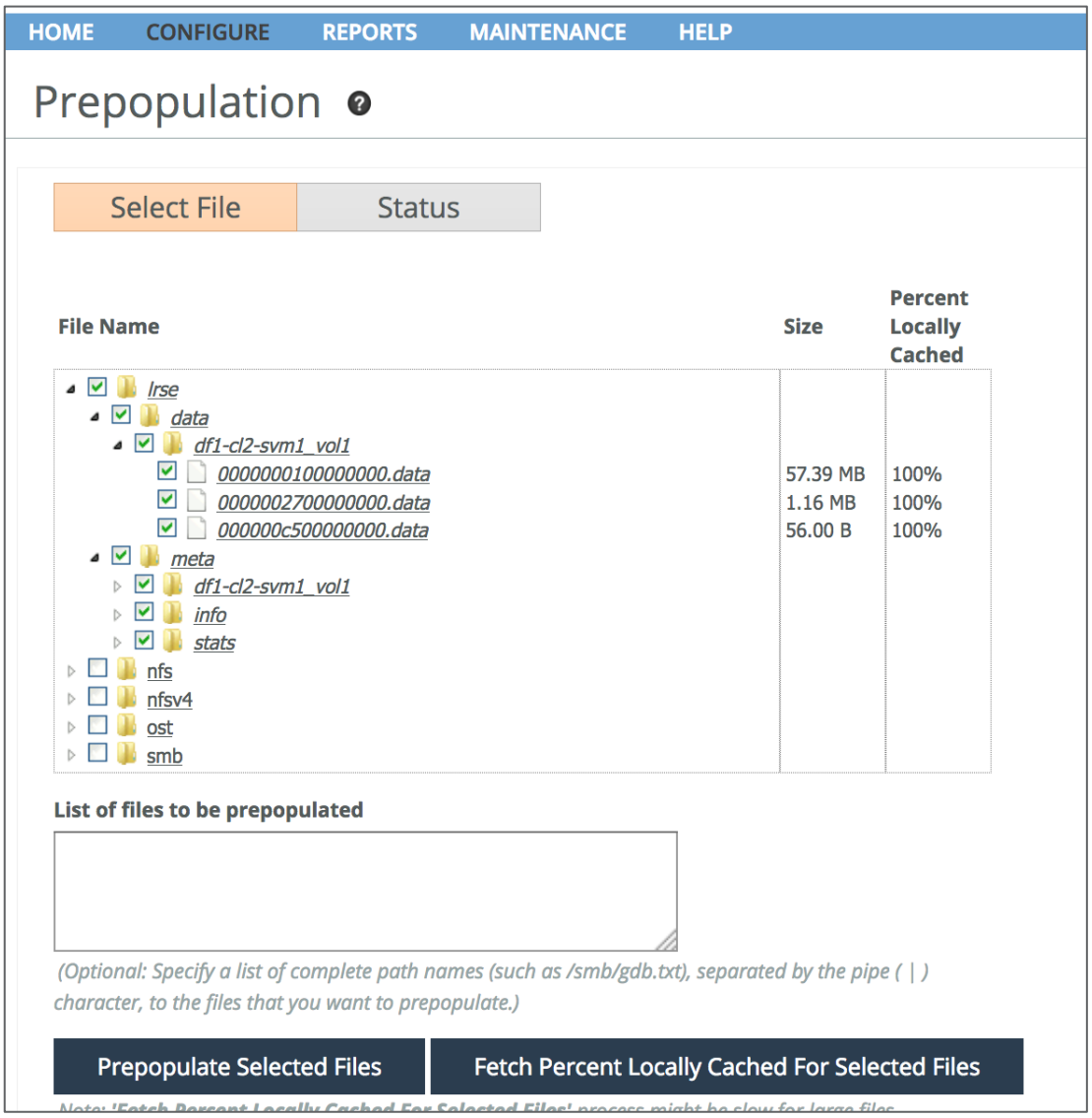
Example of using the `clean-up-failure` option and `snapmirror show` after the failed request is cleared:

```
df1-cl2::> snapmirror restore -source-path 10.1.2.16:/share/df1-cl2-svm1_vol1  -destination-path
df1-cl2-svm1:vol1 -clean-up-failure true
[Job 58] Job is queued: snapmirror restore from source "10.1.2.16:/share/df1-cl2-svm1_vol1".
df1-cl2::>

df1-cl2::> snapmirror show
                                                                    Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
df1-cl2-svm1:vol1
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                             Snapmirrored
                                     Idle           -         true    -

df1-cl2::>
```

4.10 Prepopulation of Snapshot Copies

Prepopulation of an individual Snapshot copy is not currently available. It is possible to do prepopulation for an entire SnapMirror share. SnapMirror shares are listed in the prepopulation section of the AltaVault GUI as in the LRSE directory.

Figure 18) Prepopulation using AltaVault GUI.

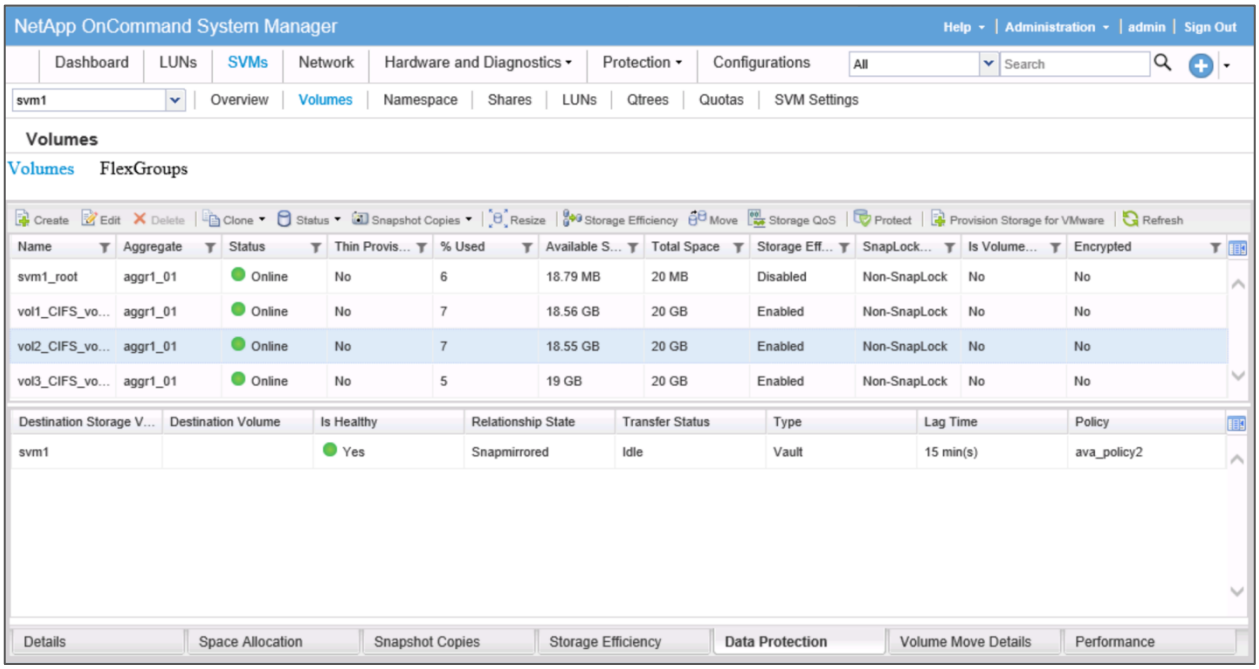


5 Managing SnapMirror Operations

5.1 Viewing SnapMirror Status

View status from ONTAP using `snapmirror show`. In System Manager, select the SVM's menu, then choose the SVM in the list. From there, choose the Volumes menu and select the volume to monitor. SnapMirror status is shown on the Data Protection tab and indicates the health and lag time in addition to other status information.

Figure 19) System Manager volume data protection status.

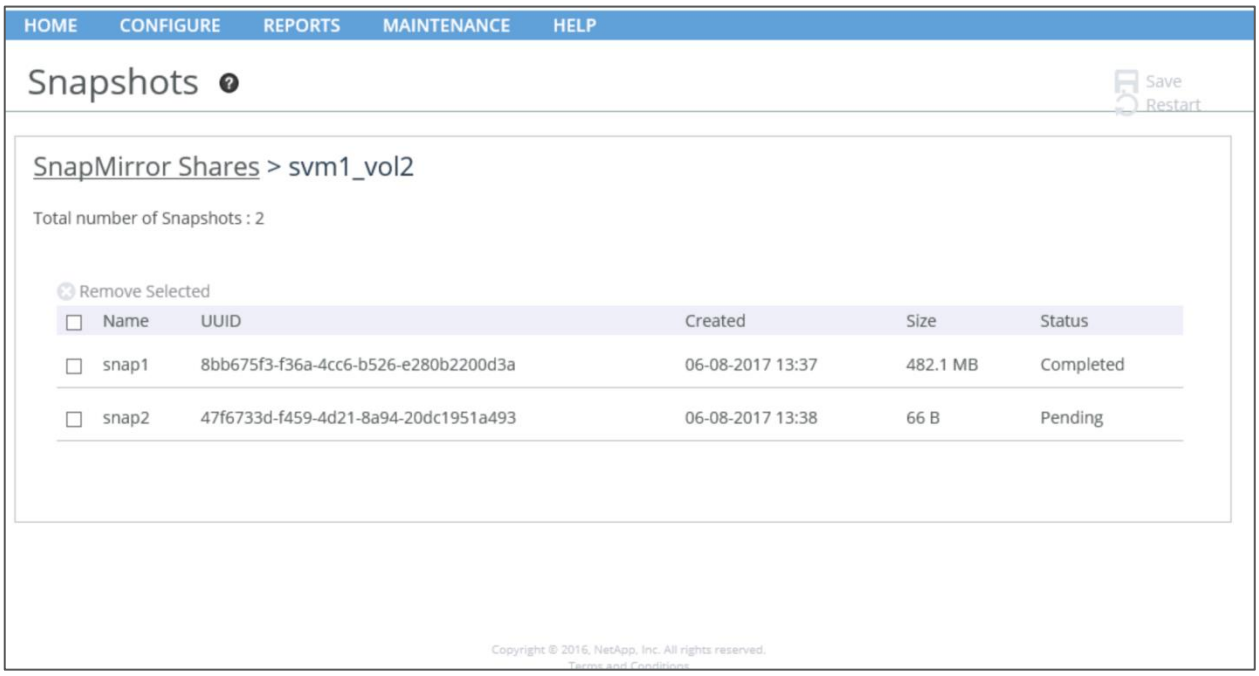


Example of SnapMirror show command with a relationship with the baseline transfer process completed. The state is SnapMirrored, and the status is Idle.

```
cluster1::> snapmirror show
                                                                    Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
svm1:vol2_CIFS_volume
            XDP  192.168.0.75:/share/svm1_vol2
                             Snapmirrored
                                     Idle           -         true    -

cluster1::>
```

It is also possible to see a status for the Snapshot transfer (`snapmirror update`) in the AltaVault web management interface. Choose SnapMirror from the configure menu, then click the name of the SnapMirror share to see a list of Snapshot copies and the transfer status.

Figure 20) AltaVault Snapshot status view.



The status from the AltaVault appliance can show:

- Pending
- Completed

The status indicates the progress of the replication to cloud object storage for the Snapshot data and metadata.

Viewing a Relationship in System Manager

System Manager does not currently support creation of SnapMirror relationships other than ONTAP. However, it is still possible to view the relationship status and details about it.

Figure 21) System Manager relationship details.

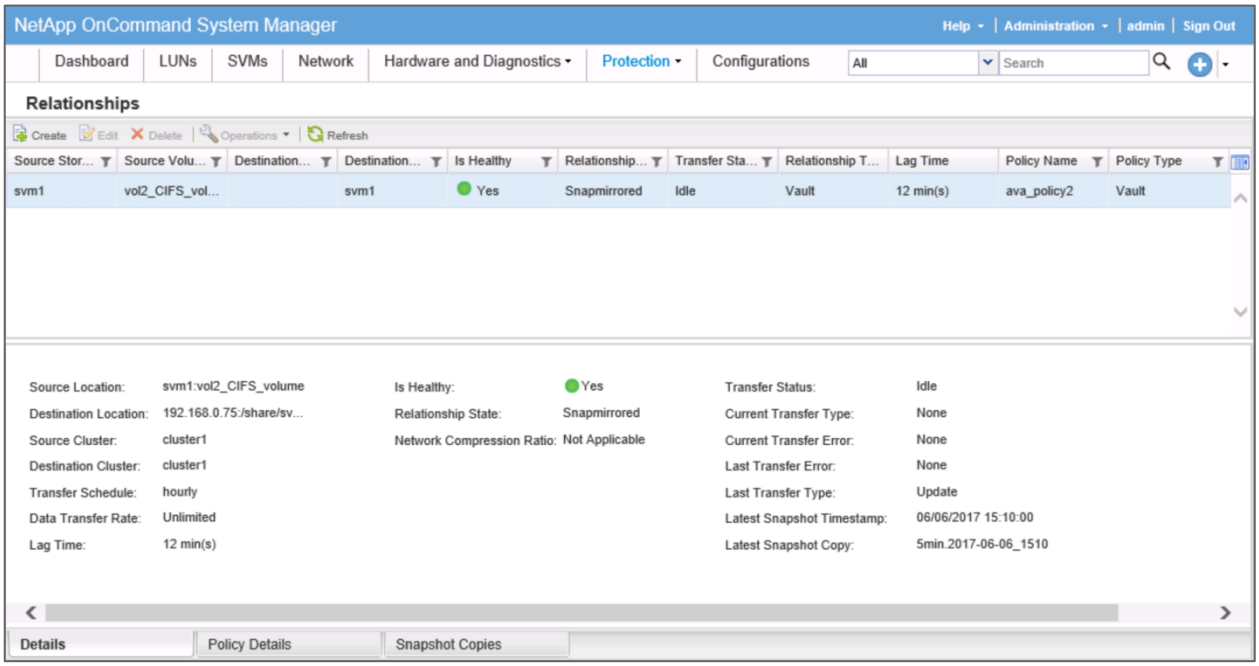
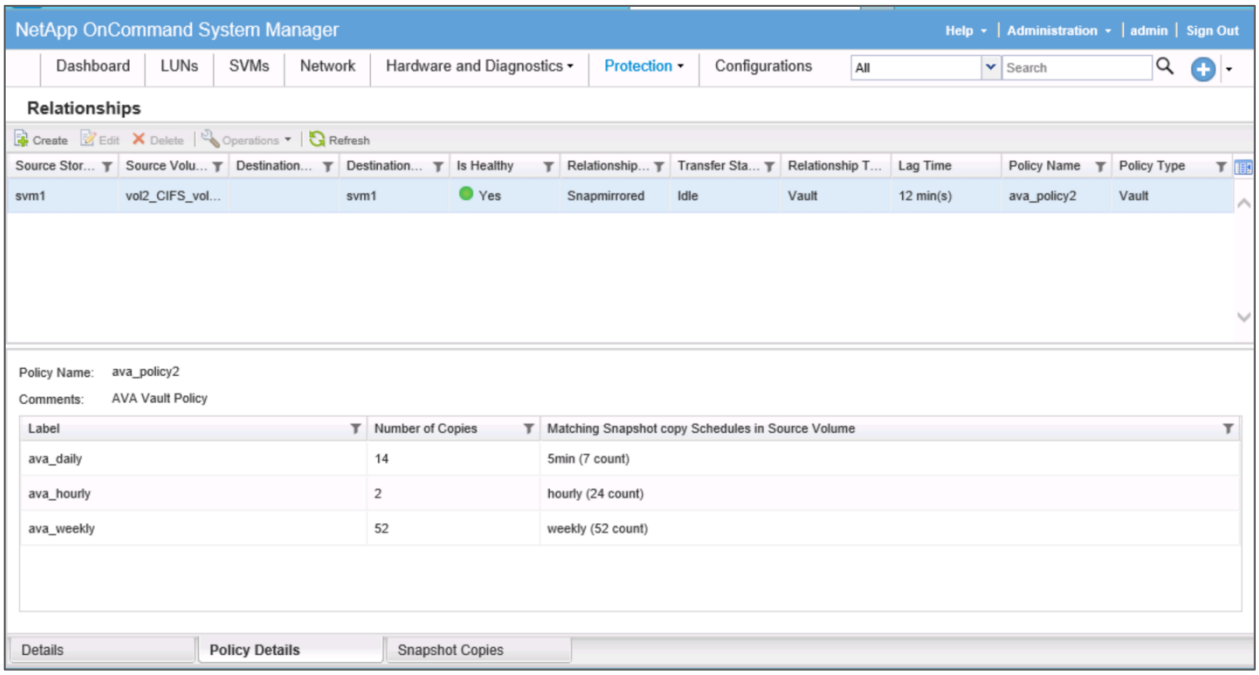


Figure 22) System Manager relationship policy details.



5.2 Managing SnapMirror Relationship

Updating a SnapMirror relationship sends any new Snapshot copies that have been created since the last update was performed. Normally, a vault policy triggers a job based on the schedule policy that was assigned to the vault policy when it was created. If there is a need to transfer new Snapshot copies before the schedule policy runs the update, this step can be performed manually using the `snapmirror update` command.

```
snapmirror update -destination-path 10.0.0.11:/share/dst_share

snapmirror update -source-path vs1:/vol/src_vol -destination-path
10.0.0.11:/share/dst_share
```

Note: Each SnapMirror update or data transfer operation uses a single TCP connection for the life of the transfer.

Example of manually transferring Snapshot copies with `snapmirror update`:

```
df1-cl2::> snapmirror update -source-vserver df1-cl2-svm1 -destination-path *
Operation is queued: snapmirror update of destination "10.1.2.16:/share/df1-cl2-svm1_vol1".
1 entry was acted on.

df1-cl2::>
```

To view the status of a SnapMirror operation from the AltaVault admin UI, click the share name on the SnapMirror configuration page.

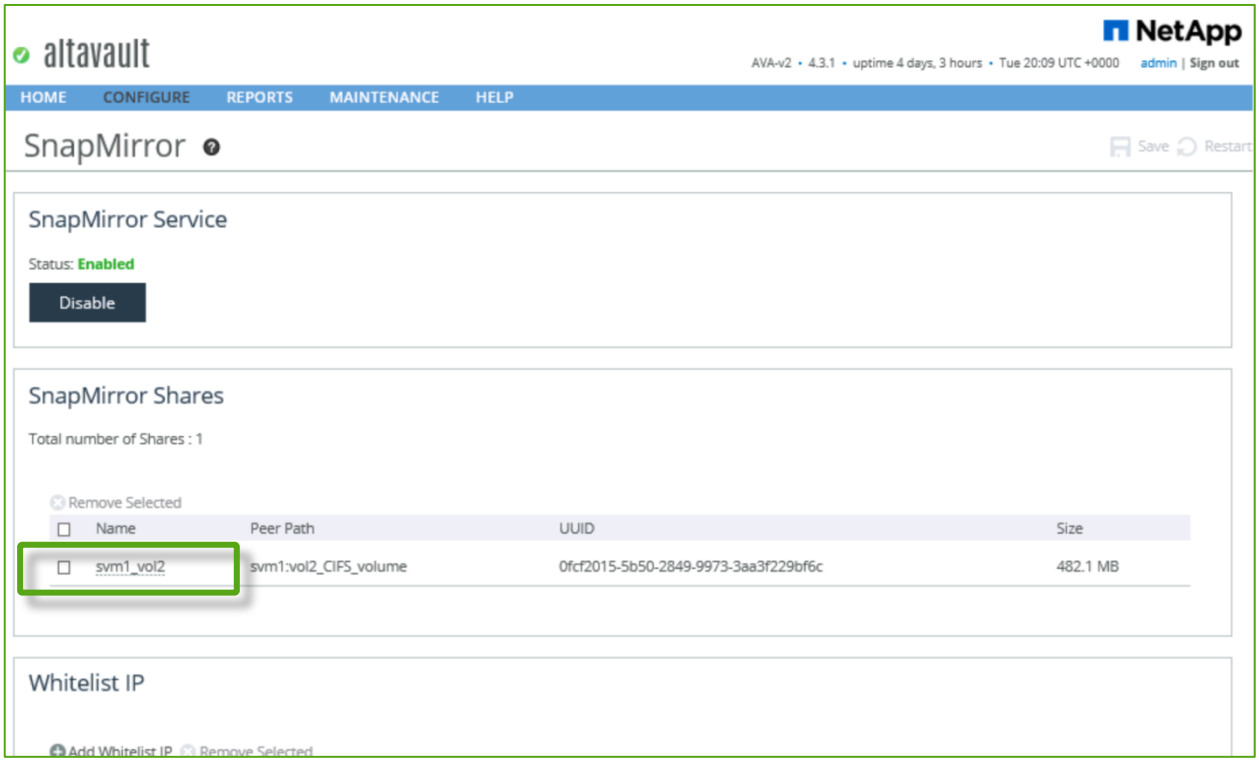
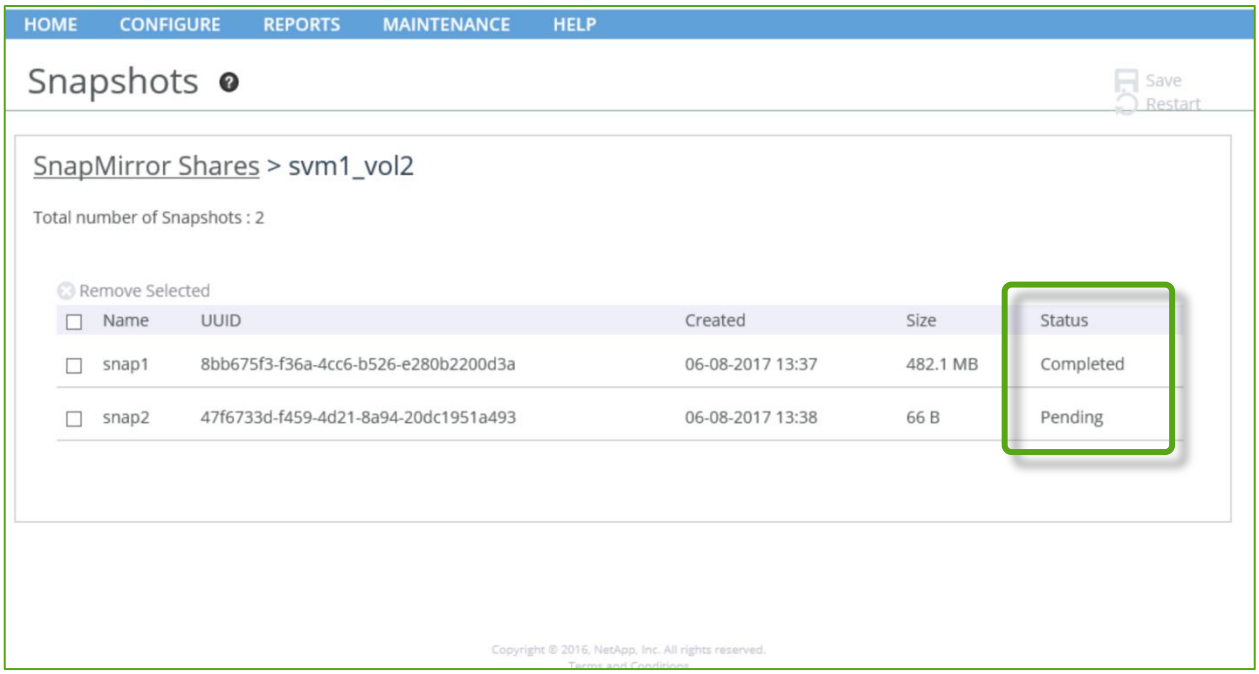


Figure 23) View status of SnapMirror update from AltaVault.



- **Snapshot name.** The name of the Snapshot copy assigned by the ONTAP administrator, ONTAP policy, or SnapCenter. The name is assigned when the Snapshot copy is taken.
- **UUID.** Specifies the unique identifier associated each Snapshot copy. The UUID value is generated by ONTAP.
- **Created.** The date and time when the Snapshot copy was created in ONTAP.
- **Size.** Size of the Snapshot copy.
- **Status.** Progress indicator for replication of the Snapshot copy to cloud storage can be one of two values:
  - **Pending.** Snapshot replication to cloud storage is in progress.
  - **Completed.** Snapshot replication to cloud storage was successful.

5.3 Remove a SnapMirror Relationship

Removing a SnapMirror relationship is the same as deleting a relationship when the destination is a system other than ONTAP. When a relationship is deleted, the data is retained in the shares on the AltaVault appliance. To remove the data on the AltaVault appliance, delete the Snapshot copies using the AltaVault UI or CLI and then delete the share established by the SnapMirror relationship. After Snapshot copies are deleted, the metadata is removed immediately. Freeing up data is done by asynchronous processes in the AltaVault appliance. Because the data is stored deduplicated, processes must run to determine the references to data, then perform a separate removal of unreferenced data in cache and a separate operation to clean up unreferenced data in cloud.

```
snapmirror delete [-source-path <vserver>:/vol/<volume>] -destination-path
<IP_address>:/share/<share_name>
```

```
snapmirror delete -source-path svm1:vol2 -destination-path
192.168.0.75:/share/vol2
```

or

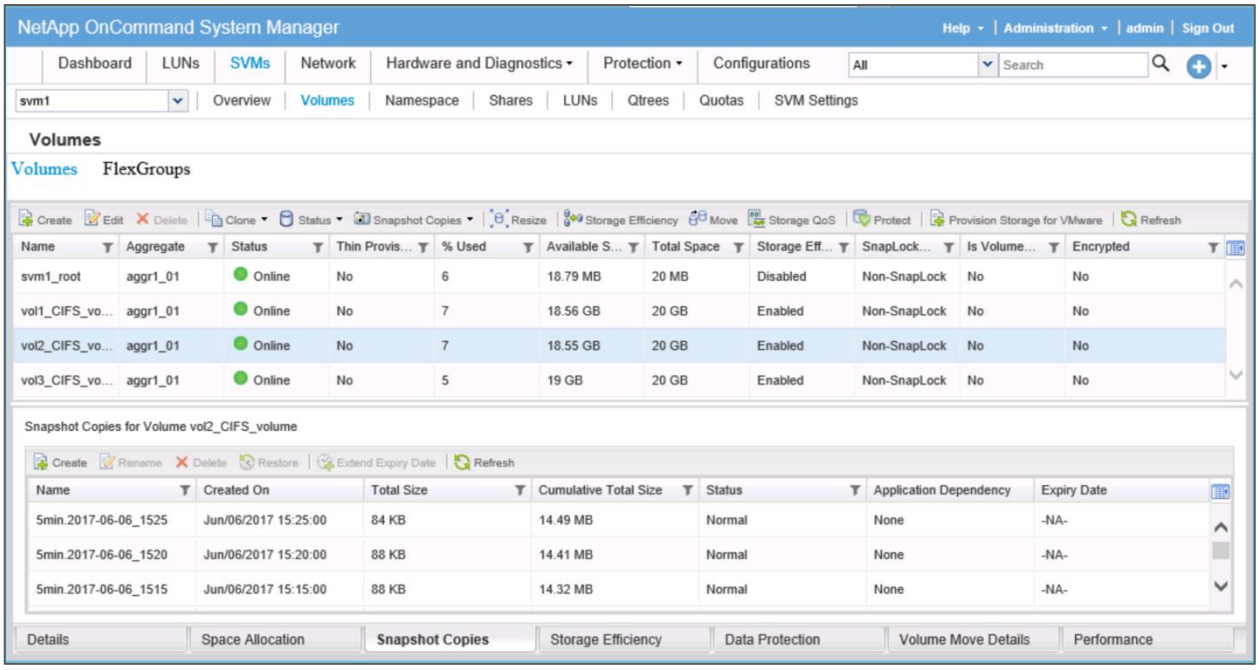
```
snapmirror delete -destination-path 192.168.0.75:/share/vol2
```

5.4 Managing Snapshot Copies on the Source Volume

It is possible to view and manage Snapshot copies on the source volume using System Manager or ONTAP commands.

In System Manager, Snapshot copies on the source volume are viewed by selecting the SVMs menu, clicking the name of the SVM to manage, then choosing the Volumes menu in the SVM section. Select the name of the volume to manage and choose the Snapshot Copies tab. From there it is possible to list and delete the Snapshot copies.

Figure 24) Source volume Snapshot list.



Managing Snapshot copies from the ONTAP command line is done using the snapshot command. Snapshot list provides details of all Snapshot copies on all volumes. The output can be restricted by specifying the vserver and/or volume name.

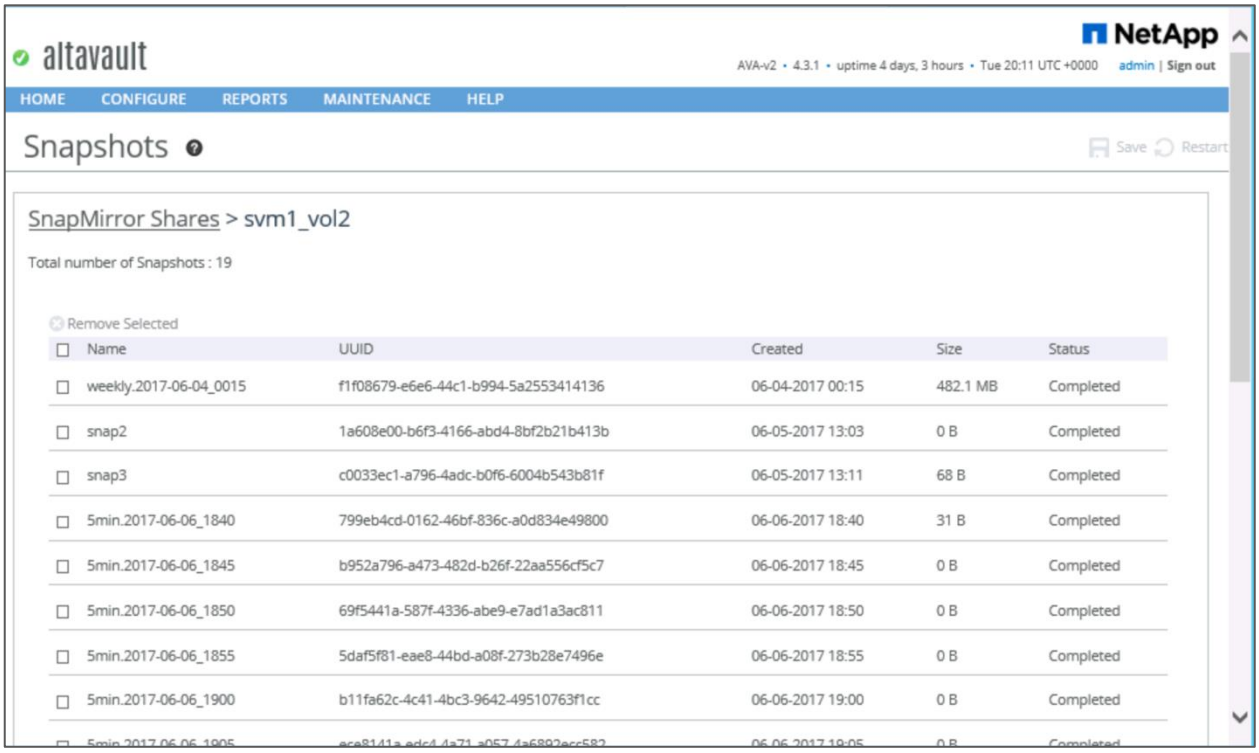
Example of snapshot list command:

```
df1-cl2::> snapshot list
                                                                  ---Blocks---
Vserver  Volume   Snapshot                                  Size Total% Used%
-------- -------- ------------------------------------ -------- ------ -----
df1-cl2-svm1
         vol1
                  daily.2017-08-31_0010                    456KB     0%    1%
                  daily.2017-09-01_0010                    556KB     0%    1%
                  daily.2017-09-02_0010                    644KB     0%    1%
                  weekly.2017-09-02_2015                   112KB     0%    0%
                  daily.2017-09-03_0010                     92KB     0%    0%
                  weekly.2017-09-03_0015                   772KB     0%    1%
                  daily.2017-09-04_0010                    788KB     0%    1%
                  daily.2017-09-05_0010                    792KB     0%    1%
                  hourly.2017-09-05_1405                   100KB     0%    0%
                  hourly.2017-09-05_1505                   100KB     0%    0%
                  hourly.2017-09-05_1605                   992KB     0%    2%
                  hourly.2017-09-05_1705                   148KB     0%    0%
                  hourly.2017-09-05_1805                   144KB     0%    0%
                  hourly.2017-09-05_1905                   100KB     0%    0%
                  hourly.2017-09-05_2005                   100KB     0%    0%
                  hourly.2017-09-05_2105                   100KB     0%    0%
                  hourly.2017-09-05_2205                   100KB     0%    0%
                  hourly.2017-09-05_2305                   100KB     0%    0%

                                                                  ---Blocks---
Vserver  Volume   Snapshot                                  Size Total% Used%
-------- -------- ------------------------------------ -------- ------ -----
df1-cl2-svm1
         vol1
                  hourly.2017-09-06_0005                    96KB     0%    0%
                  daily.2017-09-06_0010                    980KB     0%    2%
                  hourly.2017-09-06_0105                   100KB     0%    0%
                  hourly.2017-09-06_0205                   100KB     0%    0%
                  hourly.2017-09-06_0305                   100KB     0%    0%
                  hourly.2017-09-06_0405                   104KB     0%    0%
                  hourly.2017-09-06_0505                   100KB     0%    0%
                  hourly.2017-09-06_0605                   100KB     0%    0%
                  hourly.2017-09-06_0705                   100KB     0%    0%
                  hourly.2017-09-06_0805                   100KB     0%    0%
                  hourly.2017-09-06_0905                   124KB     0%    0%
                  hourly.2017-09-06_1005                   104KB     0%    0%
                  hourly.2017-09-06_1105                   948KB     0%    2%
                  hourly.2017-09-06_1205                   100KB     0%    0%
                  hourly.2017-09-06_1305                    92KB     0%    0%
         vol1_restore3
                  hourly.2017-09-06_1005                   192KB     0%   34%

                                                                  ---Blocks---
Vserver  Volume   Snapshot                                  Size Total% Used%
-------- -------- ------------------------------------ -------- ------ -----
df1-cl2-svm1
         vol1_restore3
                  hourly.2017-09-06_1105                    92KB     0%   20%
                  hourly.2017-09-06_1205                    92KB     0%   20%
                  hourly.2017-09-06_1305                    88KB     0%   19%
         vol_restore
                  hourly.2017-09-06_0905                 54.29MB     5%   96%
38 entries were displayed.

df1-cl2::>
```

5.5 Deleting Snapshot Copies from AltaVault

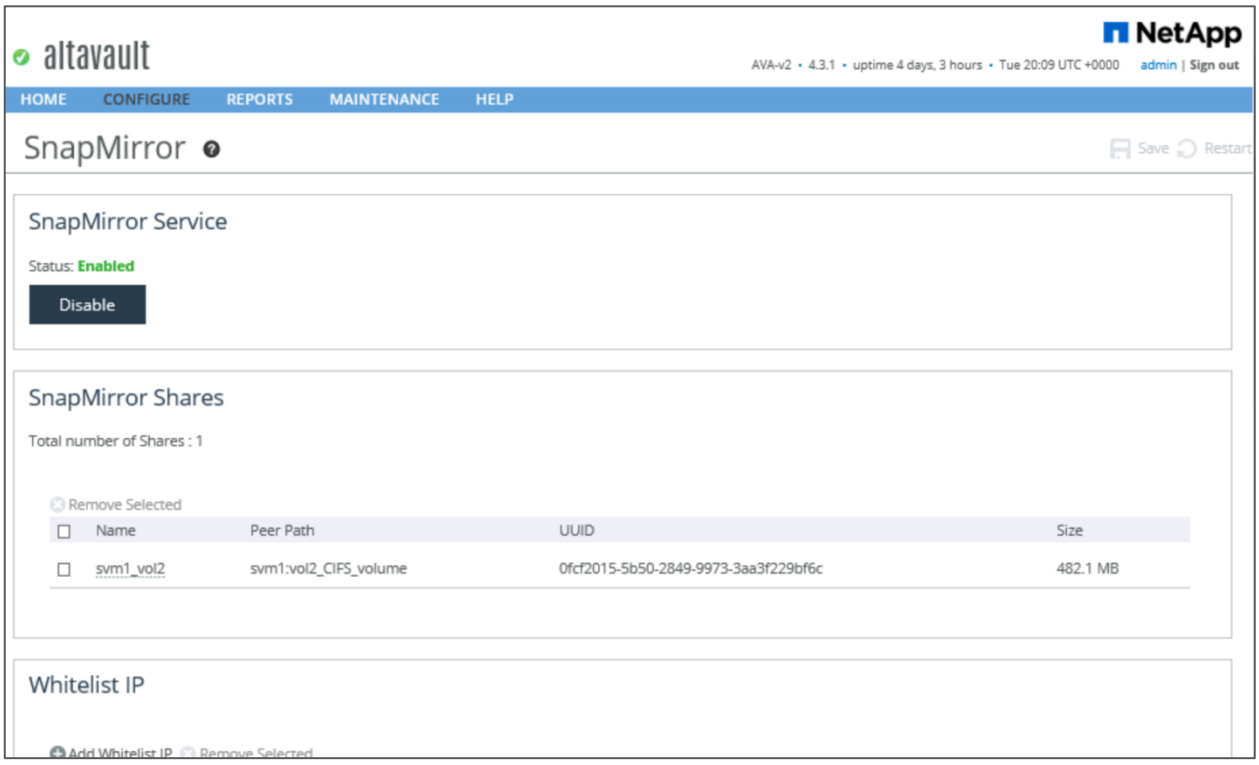
It is possible to manually delete Snapshot copies from the AltaVault appliance. This deletion is performed using the AltaVault web administration interface. From the Configure menu, choose SnapMirror. In the list of SnapMirror shares, select the share using the checkbox and click remove selected.

When a Snapshot copy is deleted, it is not possible to recover the Snapshot copy. The space is not immediately available. The processes that perform space recovery on AltaVault are asynchronous and go through several stages. This process is referred to as garbage collection, where initially the cache is checked and processed to free up space, followed by checking cloud object storage and freeing up data that is no longer referenced.



5.6 Deleting SnapMirror Shares from AltaVault

It is possible to delete an entire SnapMirror share that is no longer needed. The data is not recoverable. Similar to deleting Snapshot copies, the cleanup is a background process where space is not immediately available.



5.7 Volume Move

With relationships between ONTAP and AltaVault, if a volume move of a source volume is triggered while SnapMirror is transferring data, the volume move cutover is blocked until the SnapMirror transfer completes. If SnapMirror is not active and volume move is in cutover state, issuing a SnapMirror transfer now is blocked until the cutover is completed.

5.8 Disaster Recovery

Disaster recovery of an AltaVault appliance is described in the AltaVault administration guide in the product documentation located on the NetApp Support site.

Best practices for AltaVault disaster recovery are described in the following guide, available on the NetApp Field Portal: TR-4420: AltaVault Best Practices for DR.

Recovery of the AltaVault appliance is described in the AltaVault administration guide. The overall steps are:

1. Deploy an AltaVault appliance to use for the recovery.
2. Import the configuration of the AltaVault appliance that is being recovered.
3. Enable the AltaVault appliance for disaster recovery or disaster recovery test mode.
4. Allow the appliance to download the metadata from cloud.

After recovery of an AltaVault appliance and/or the clustered ONTAP systems, the next step is to restore any Snapshot copies. See the section on restores for more information.

After a volume has been recovered, the next process is to reestablish the SnapMirror relationship so that future backups continue. Reestablishing a relationship is done on the ONTAP system using SnapMirror resync. To reestablish a replication relationship, there needs to be a common Snapshot copy. Any newer

Snapshot copies, for example, if the restore of the volume did not use the latest Snapshot copy from AltaVault, are deleted.

After the volume has been restored, the Snapshot policy should be verified and modified to match the original source volume. After the resync is complete, the SnapMirror policy and schedule should also be checked and set to match the original source SnapMirror relationship.

Note: A disaster recovery plan should include plans to export the AltaVault configuration and store it in a secure location.

Example of a `snapmirror resync` command.

```
snapmirror resync -source-path df1-cl2-svm1:/vol/vol_restore -destination-
path 10.1.2.16:/share/df1-cl2-svm1_vol1 -type xdp
```

Example of resync for a SnapMirror relationship after restoring a Snapshot copy:

```
df1-cl2::> snapmirror resync -source-path df1-cl2-svm1:/vol/vol_restore -destination-path
10.1.2.16:/share/df1-cl2-svm1_vol1 -type xdp

Warning: All data newer than Snapshot copy hourly.2017-09-06_0905 on volume
         10.1.2.16:/share/df1-cl2-svm1_vol1 will be deleted.
Do you want to continue? {y|n}: y
Operation is queued: initiate snapmirror resync to destination "10.1.2.16:/share/df1-cl2-
svm1_vol1".

df1-cl2::> snapmirror show
Progress
Source            Destination Mirror  Relationship   Total             Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
df1-cl2-svm1:vol_restore
            XDP  10.1.2.16:/share/df1-cl2-svm1_vol1
                              Snapmirrored
                                      Idle           -         true    -

df1-cl2::>
```

Example of checking the policy and schedule:

```
df1-cl2::> snapmirror show -fields schedule,policy
source-path              destination-path                     schedule policy
------------------------ ------------------------------------ -------- ----------
df1-cl2-svm1:vol_restore 10.1.2.16:/share/df1-cl2-svm1_vol1 -        XDPDefault

df1-cl2::>
```

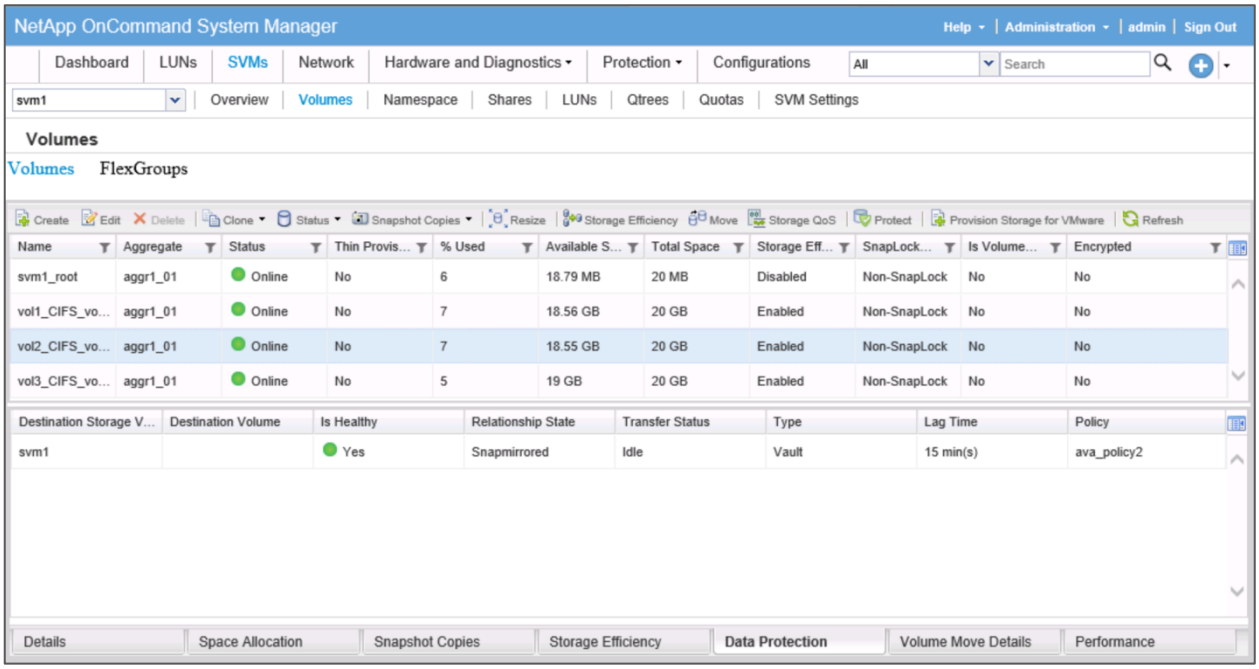
Example command to modify the policy and schedule to match the original source volume relationship:
`snapmirror modify -source-path df1-cl2-svm1:/vol/vol_restore -destination-path 10.1.2.16:/share/df1-cl2-svm1_vol1 -schedule hourly -policy ava_policy1`

Example of setting the policy and schedule:

```
df1-cl2::> snapmirror modify -source-path df1-cl2-svm1:/vol/vol_restore -destination-path
10.1.2.16:/share/df1-cl2-svm1_vol1 -schedule hourly -policy ava_policy1
Operation succeeded: snapmirror modify for the relationship with destination
"10.1.2.16:/share/df1-cl2-svm1_vol1".

df1-cl2::> snapmirror show -fields schedule,policy
source-path              destination-path                     schedule policy
------------------------ ------------------------------------ -------- -----------
df1-cl2-svm1:vol_restore 10.1.2.16:/share/df1-cl2-svm1_vol1 hourly   ava_policy1

df1-cl2::>
```

Viewing source volume Snapshot schedule assignment in System Manager is done from the Volumes section, available from the SVMs menu after selecting the name of the SVM to manage.

Figure 25) View source volume protection policy.



5.9 Supported SnapMirror Commands

When the endpoint of a SnapMirror relationship is an AltaVault appliance, the following SnapMirror commands are supported:

- abort
- create
- delete
- initialize
- modify
- quiesce/resume
- restore
- resync
- show
- update

Note: SnapMirror check command is not supported.

6 Troubleshooting

6.1 Failed Requests for a File Restore

Possible issue is the path, or the name of the file is not specified to match what exists on the volume.

The restore request shows a healthy status of false.

```
cluster1::> snapmirror show
                                                                    Progress
Source            Destination Mirror  Relationship   Total            Last
Path        Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
192.168.0.75:/share/svm1_vol2
            RST  svm1:vol2_CIFS_volume
                             -       Idle           -         false   -
```

Check to make sure the path and file name are correct. Use NFS or CIFS to view the exact name and path of the file on the primary volume. For CIFS shares, it is best to use a command window to perform a directory because Windows Explorer options do not always show the complete file name.

If it's not possible to view the primary volume share or there is still some question, it is possible to use the ONTAP CLI. The following example is for an instance when Windows Explorer was not displaying extensions and an extension was added to the file automatically in addition to one that was entered when creating the file.

```
cluster1::> set diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y

cluster1::*> run local ls -lr /vol/vol2_CIFS_volume
d777          64      3             4096         Fri Jun  2 20:50:52 UTC 2017     .
d777          64      3             4096         Fri Jun  2 20:50:52 UTC 2017     ..
d777          97      4             4096         Wed May 17 20:00:50 UTC 2017     BackupData
 10777      11620      1               68       Mon Jun  5 13:11:08 UTC 2017     test1.txt.txt

cluster1::*> set admin
```

6.2 Restore Operation Slow

When experiencing slow restore performance, it might be helpful to check some of the following areas:

- Check that the AltaVault appliance is not under excessive load using the CPU reports.
- Quiesce backups for the duration of restores.
- Keep number of concurrent restores less than 10.

Because of the forever incremental nature of Snapshot replication, along with some change rates, data might be spread across many Snapshot copies. Because older Snapshot copies need to be iterated to find valid data blocks, there might be processing overhead for Snapshot copies. This overhead could give an impression that restores are not occurring when the AltaVault appliance might be iterating through Snapshot copies.

Version History

Version	Date	Document Version History
Version 1.0	September 2017	Initial release.
Version 1.1	February 2018	Updated for AltaVault 4.4 release.

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.