Module 8
Data protection

About this module

This module focuses on enabling you to do the following:

- Manage Snapshot copies
- Restore data from Snapshot copies
- Back up and replicate data
- Use encryption to prevent unauthorized access to data

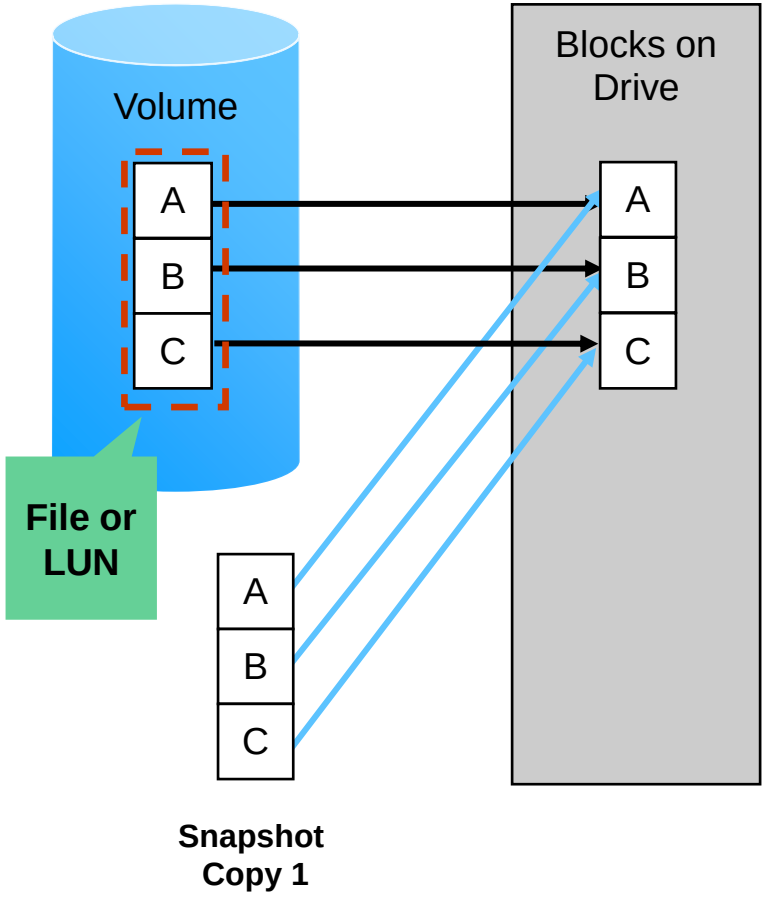
Lesson 1
Manage Snapshot copies

Snapshot copies

- A Snapshot copy is a read-only, point-in-time image of a FlexVol volume.
- The copy consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the most recent Snapshot copy was made.
- Snapshot copies owe their efficiency to the NetApp WAFL file system, which uses metadata to point to blocks on disk and writes to a new block rather than overwrite existing blocks.
- Instead of moving old blocks to a pool of space for Snapshot copies, old blocks remain in place. Only the pointers move from the active file system to the Snapshot copies.

Snapshot copy technology

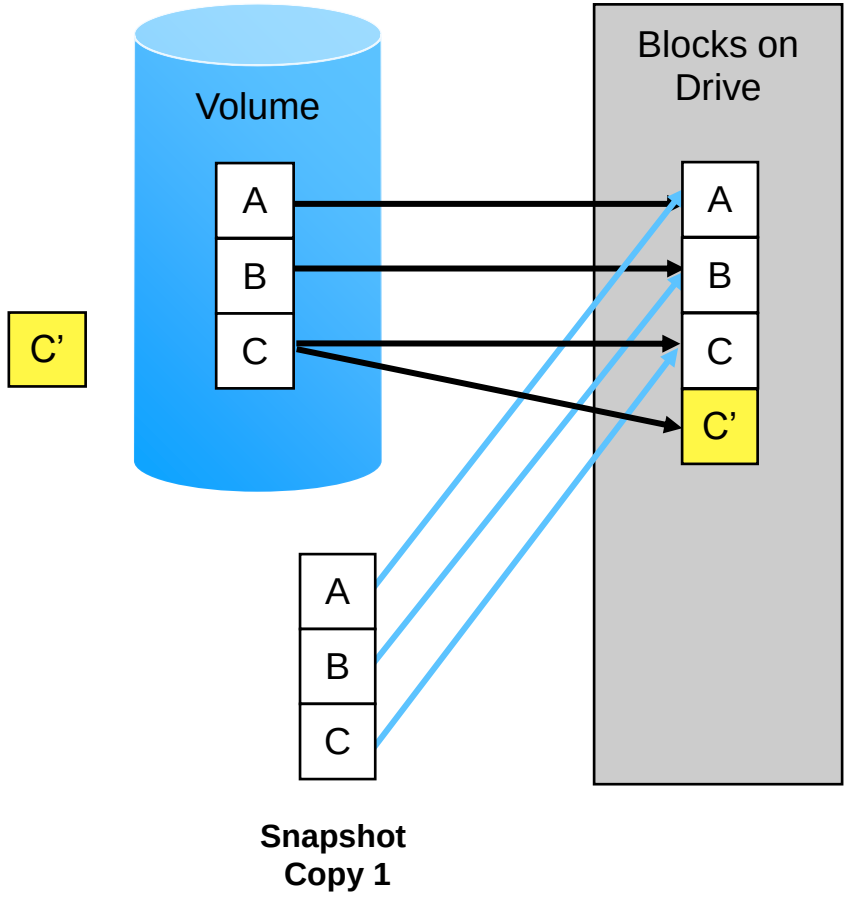
Create Snapshot copy 1



1. Create Snapshot copy 1: @9am
   - Pointers are copied.
   - No data is moved.

Snapshot copy technology

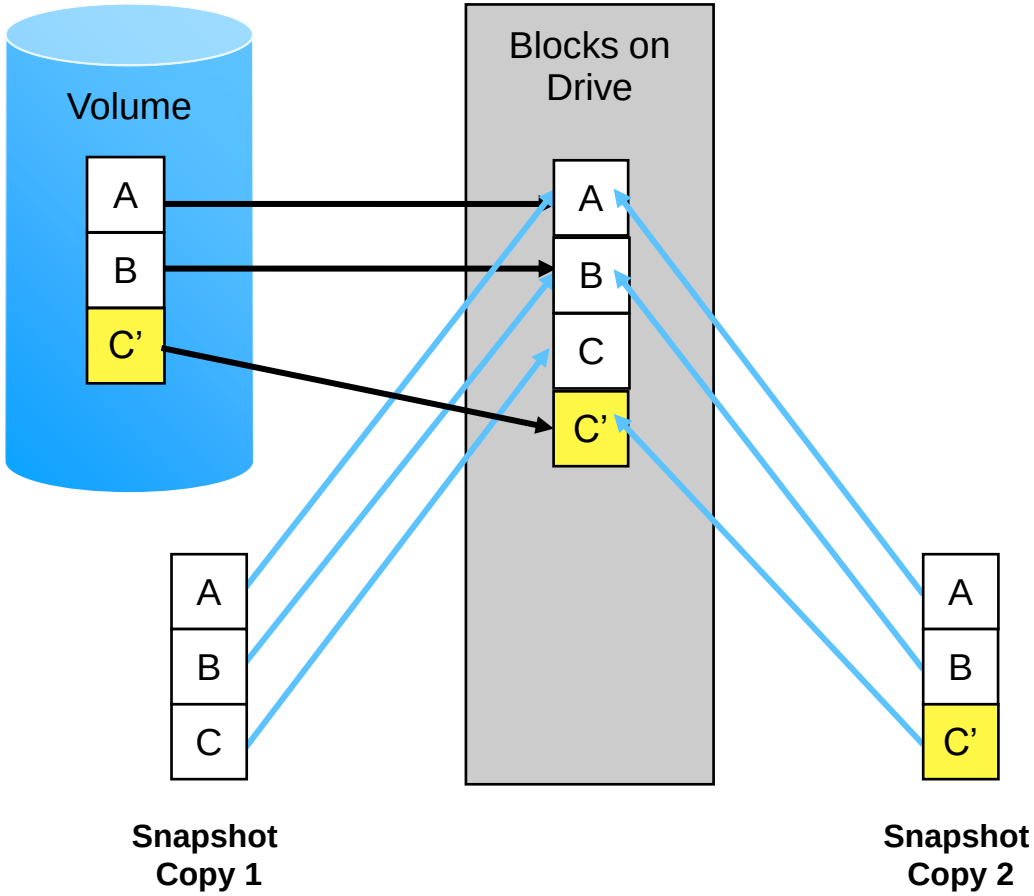
Continue writing data



1. Create Snapshot copy 1.
2. Continue writing data:
   - Data is written to a new location on the disk.
   - Pointers are updated.

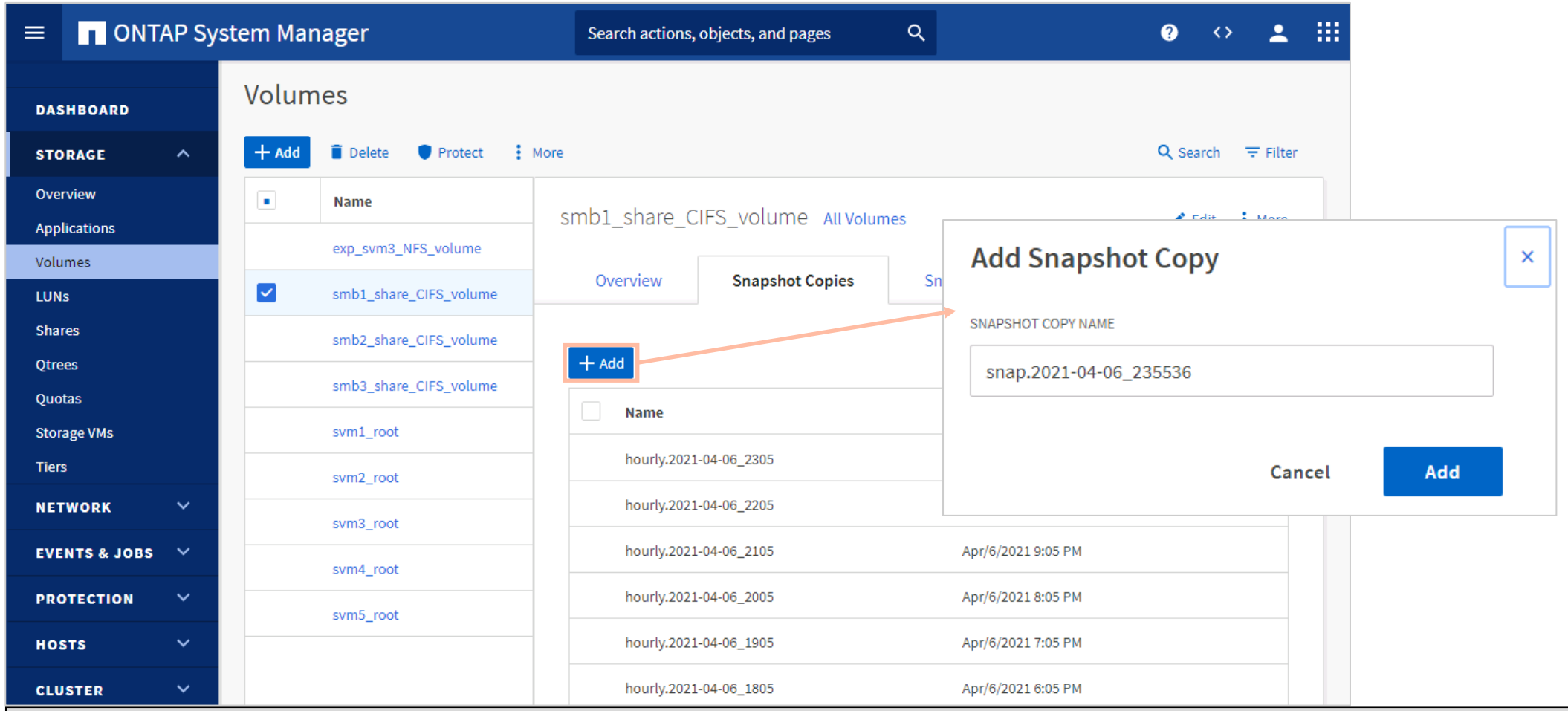
Snapshot copy technology

Create Snapshot copy 2



1. Create Snapshot copy 1.
2. Continue writing data.
3. Create Snapshot copy 2: @10am
   - Pointers are copied.
   - No data is moved.
   - Block C consumes Snapshot space because the active file system no longer references Block C.

Create a Snapshot copy




```
cluster1::> snapshot create -vserver svm4 -volume svm4_vol002
            -snapshot vol2-pre-app-upgrade
```

Snapshot copy design

Snapshot copies are the first line of defense against accidental data loss or inconsistency.

- Do not create more Snapshot copies than necessary.
- Check and adjust the volume Snapshot copy reserve defaults.
- To control storage consumption, configure Snapshot copy automatic deletion and volume automatic increase.
- Consult TR-4678 for guidance on planning Snapshot copies of NetApp FlexGroup volumes.

Naming conventions for Snapshot copies

- A Snapshot copy name can have a prefix or schedule name, timestamp, comment, and label:

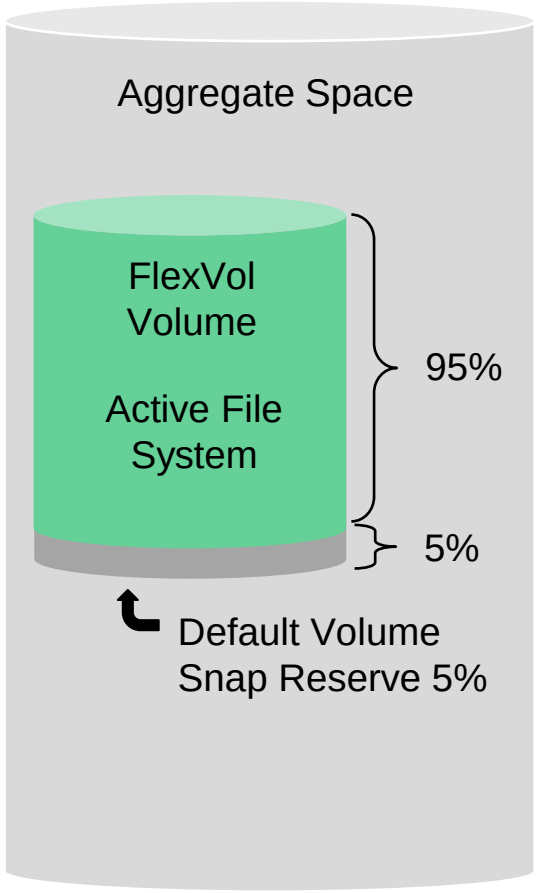
```
vserver         volume                  snapshot
-------         ----------------        ----------------------------
svm4            svm4_vol002             2HourSnapshot.2020-07-11_1030
```

(Prefix) (Timestamp)

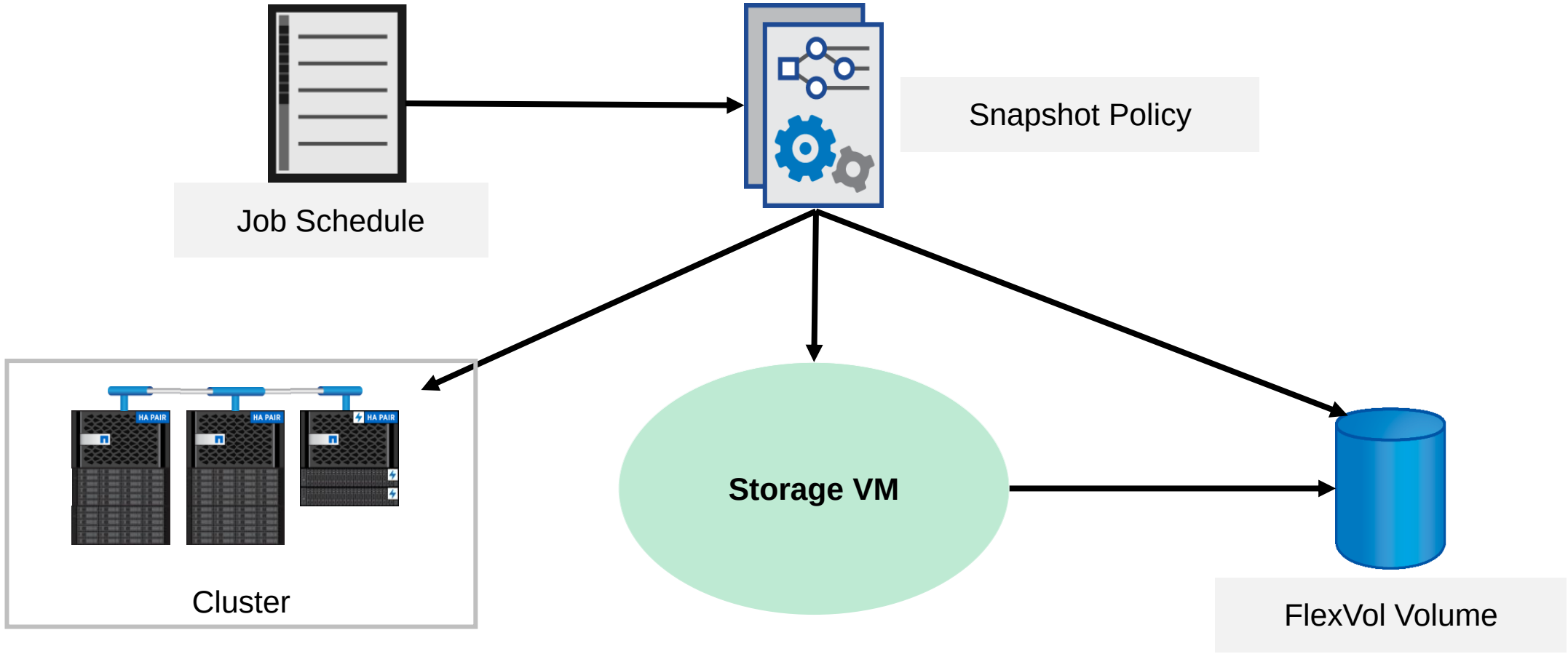
- Snapshot copy names cannot be longer than 255 characters.

The Snapshot copy reserve

- The Snapshot reserve is a storage space set aside inside a volume.
  - Often depicted as a partition
  - Actually a soft quota
- The reserve holds blocks that are no longer in the active file system but are still referenced by Snapshot copies.
- The reserve is not used for file system writes.
- The reserve can be increased or decreased.



The Snapshot policy

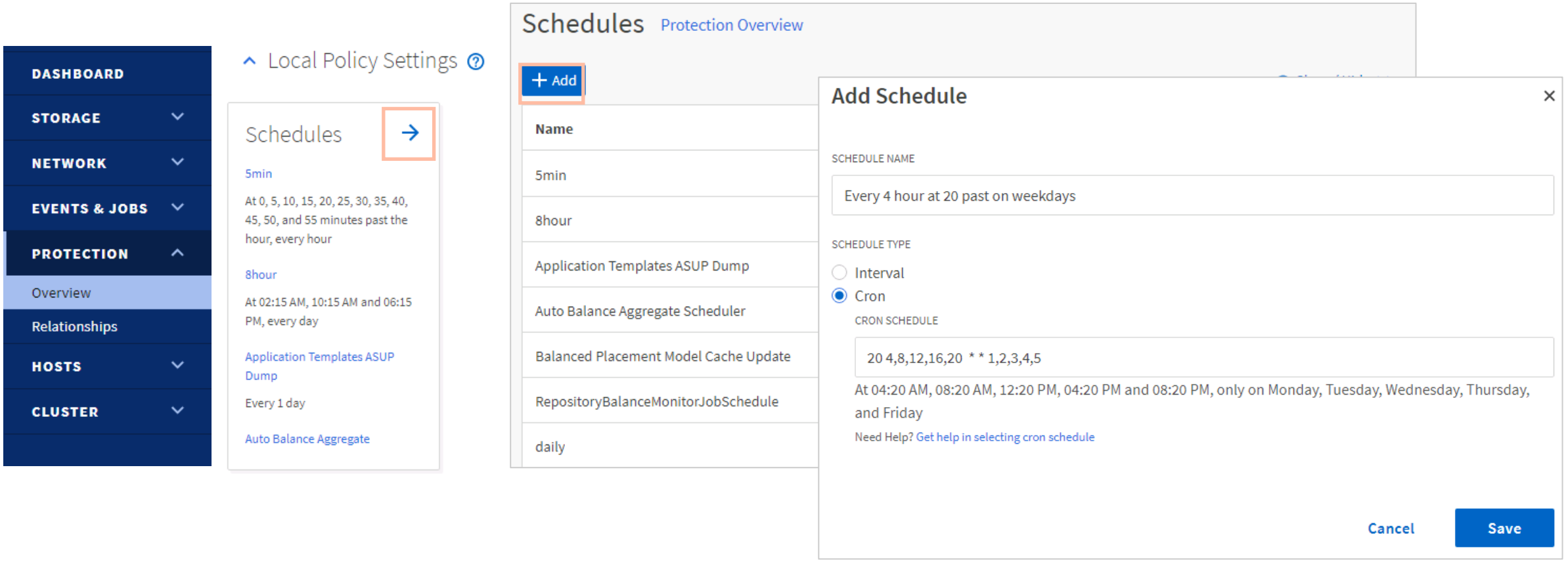


Storage VM = storage virtual machines, also known as SVM

Typical workflow

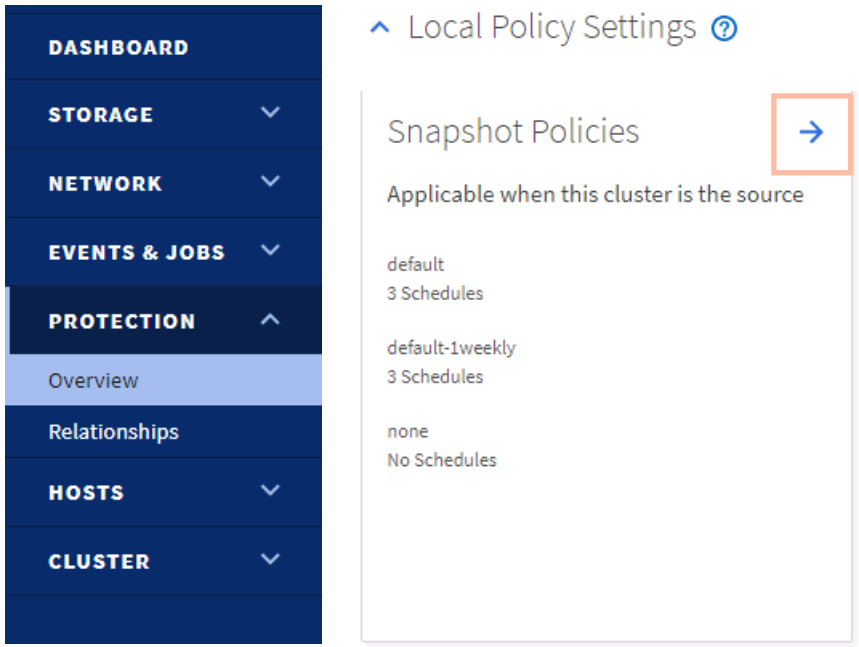
1. Create a job schedule, or use the default.
2. Create a Snapshot policy, and then specify the job schedule.
3. Assign the Snapshot policy to a FlexVol volume or SVM.

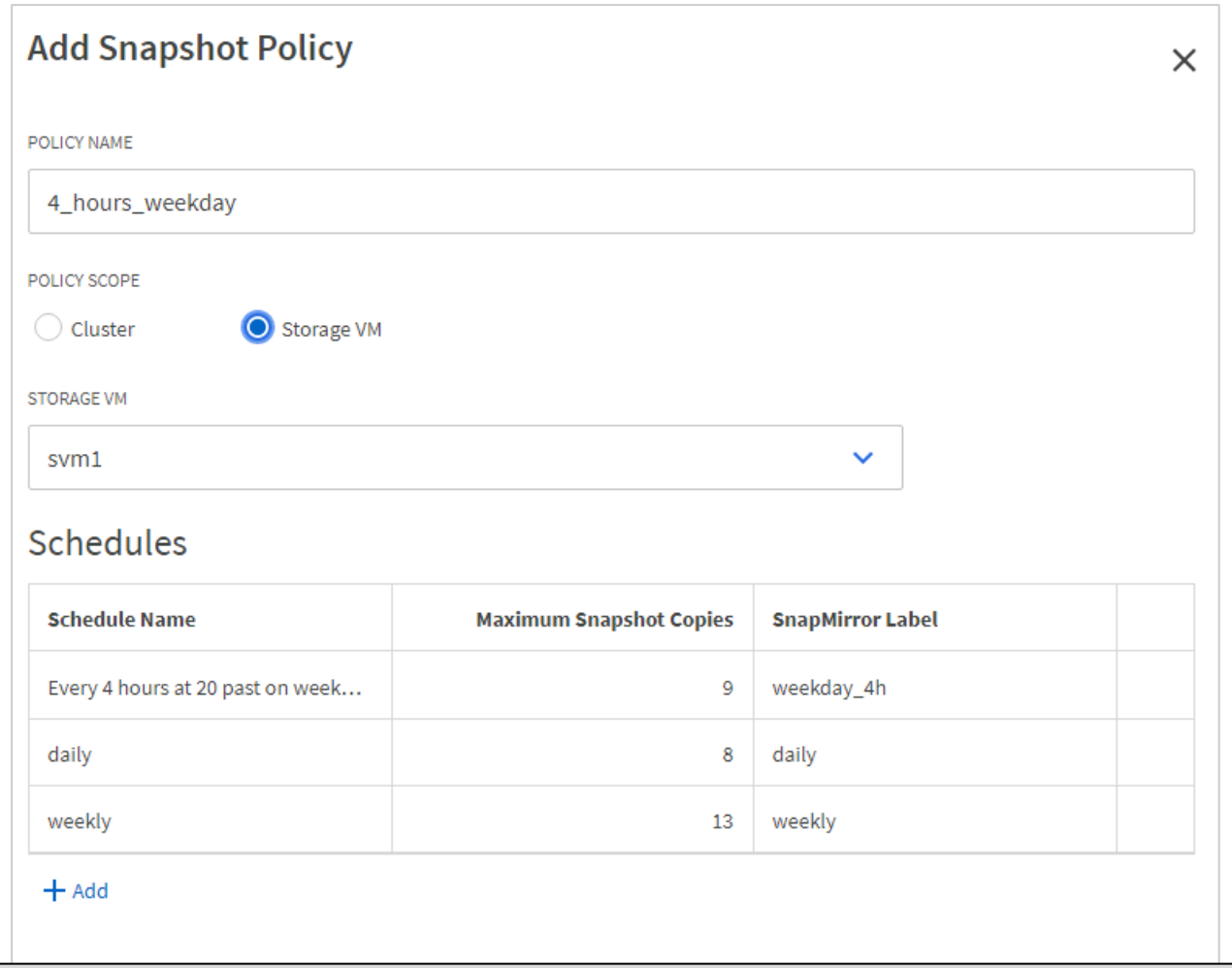
Create a job schedule




```
::> job schedule cron create -name 4hrs -hour 4,8,12,16,20 -minute 20
    -dayofweek Monday,Tuesday,Wednesday,Thursday,Friday
```

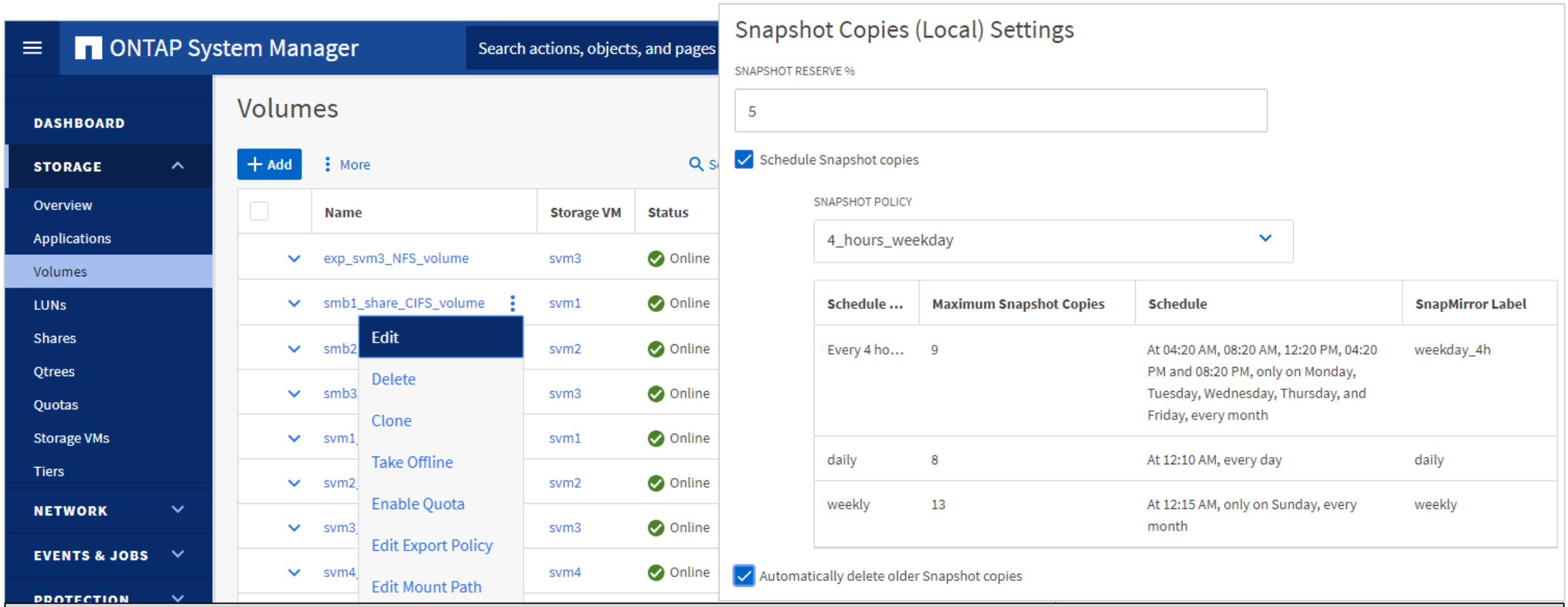

Create a Snapshot policy






```
::> volume snapshot policy create -vserver svm4 -policy sp_4hrs
    -schedule1 4hrs -count1 5 -prefix1 every_4_hrs -enabled true
```


Apply a Snapshot policy to a volume




```
::> vol modify -vserver svm4 -volume svm4_vol002 -snapshot-policy sp_4hrs
```


Topic for discussion

- Should all hourly Snapshot copies run on the hour?
- Why or why not?

Lesson 2
Restore data from a Snapshot copy

Recovering data

Recover Snapshot Data

- Copy data from Snapshot data.
- Use SnapRestore data recovery software.
- Use the Windows Previous Versions feature.

Copy from a Snapshot Copy

- Locate the Snapshot copy.
- Copy the file to the original location.
- Copy the file to a new location.

Use SnapRestore Technology

- Restore an entire volume.
- Quickly restore large files.

Snapshot visibility to clients

Snapshot directories are visible to NAS clients by default.

Use commands to hide the Snapshot directories at the volume level or share level.

Disable visibility of Snapshot directories for the volume:

```
::> vol modify -vserver svm4 -volume svm4_vol_002 -snapdir-access false
```

Disable visibility of Snapshot directories for an SMB share:

```
::> vserver cifs share properties remove -vserver svm4
    -share-name svm4_vol2 -share-properties showsnapshot
```

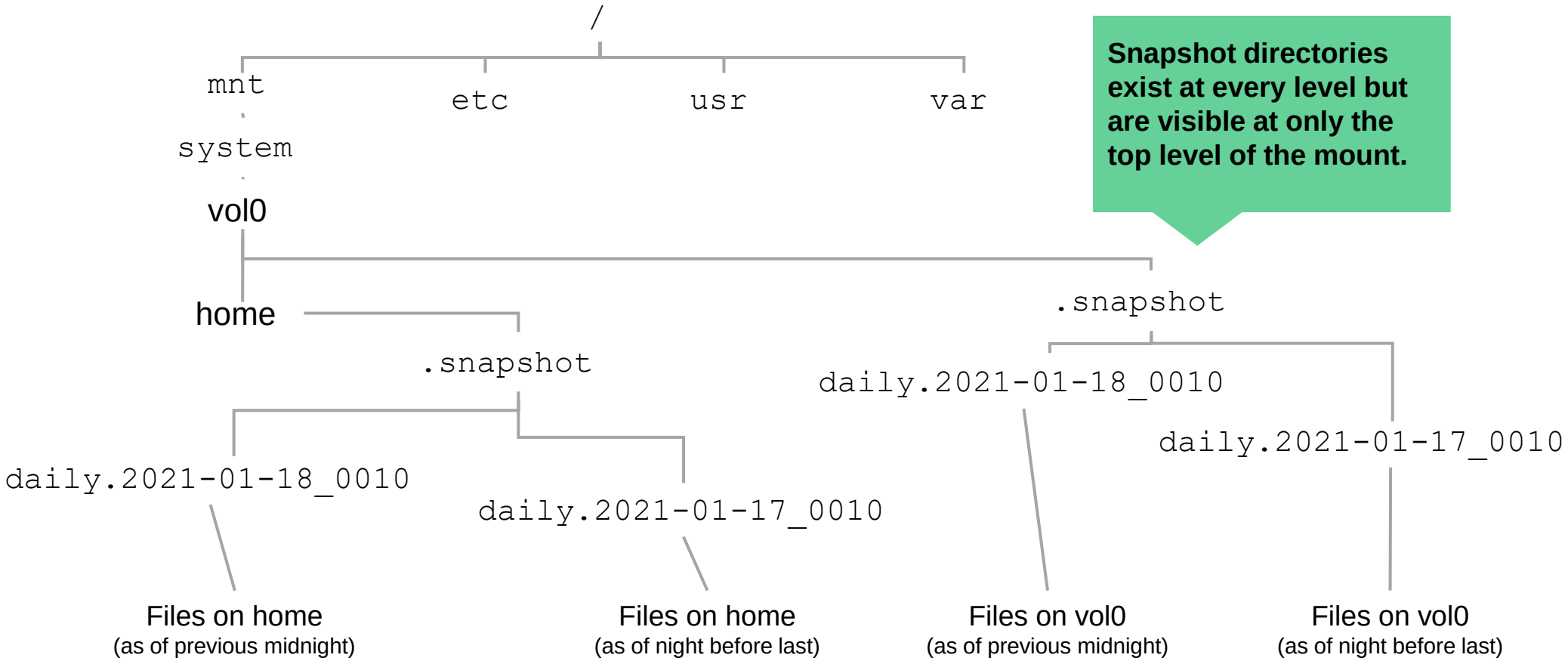

Topic for discussion

What are the advantages and disadvantages of enabling clients to restore their own data?

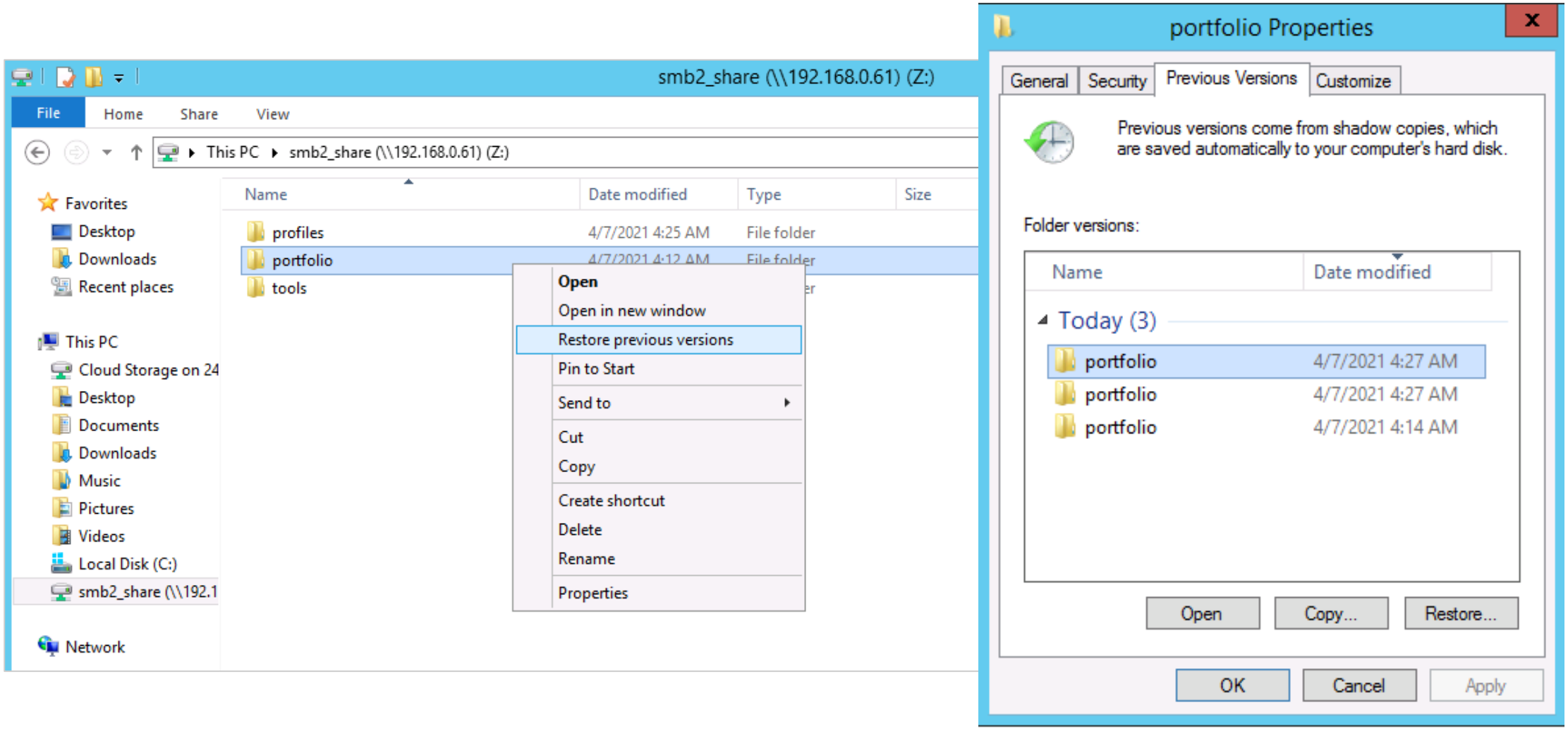
Snapshot view from a UNIX client

```
# ls /system/vol01/.snapshot

weekly.2021-01-15_0015  daily.2021-01-18_0010

daily.2021-01-19_0010   hourly.2021-01-19_0605

hourly.2021-01-19_0705  hourly.2021-01-19_0805

hourly.2021-01-19_0905  hourly.2021-01-19_1005

hourly.2021-01-19_1105  hourly.2021-01-19_1205

snapmirror.3_2147484677.2021-01-19_114126
```


Recovering files from the .snapshot directory of a UNIX host

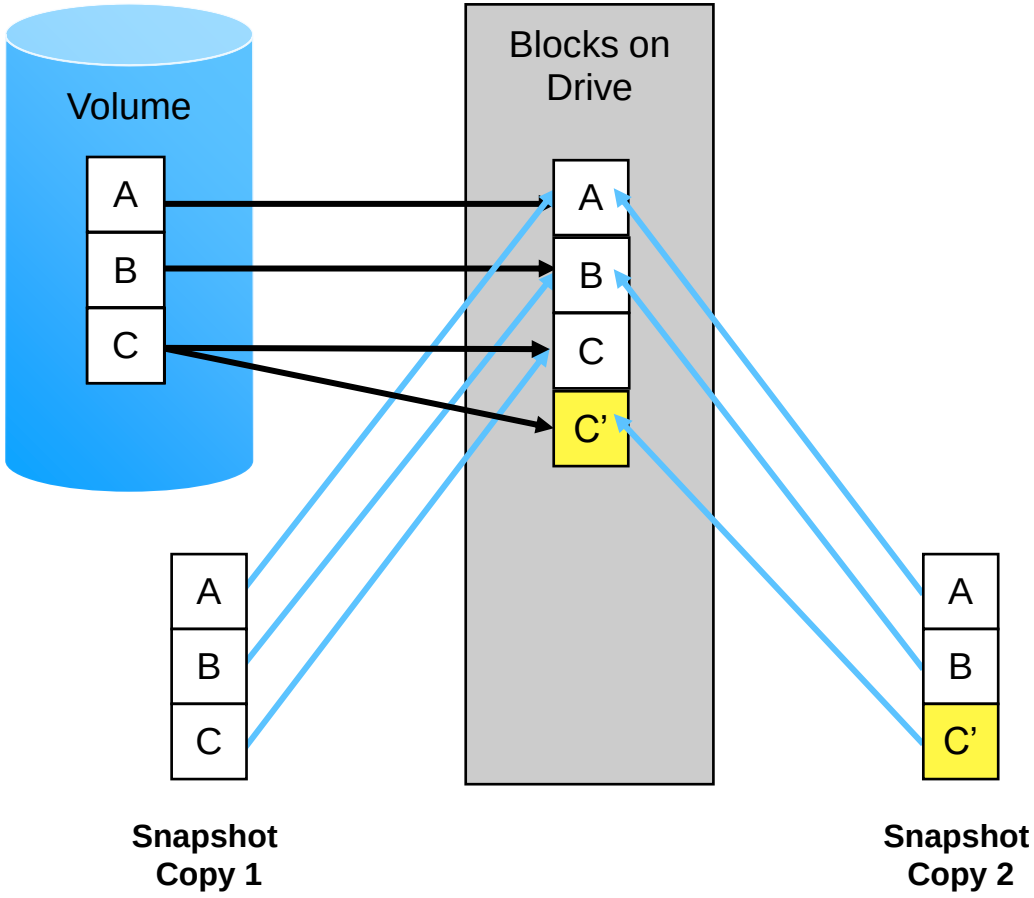


Restoring previous versions in Windows



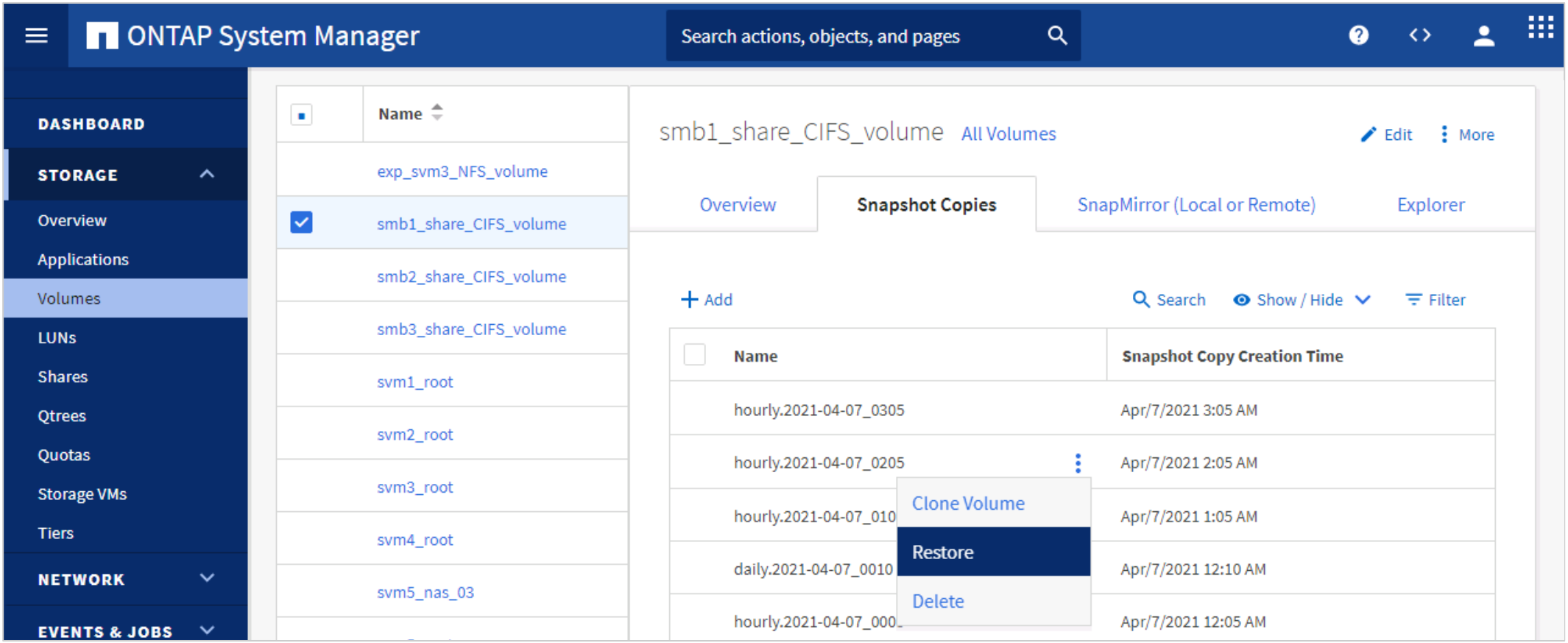
Snapshot copy technology

Restore from a Snapshot copy



- To restore a file or LUN from Snapshot copy 1, use SnapRestore data recovery software.
- Snapshot copies that were created after Snapshot copy 1 are deleted.
- Unused blocks on drives are made available as free space.

Reverting and restoring a volume




```
::> volume snapshot restore -vserver svm4 -volume svm4_vol_002
    -snapshot svm4_vol_002_snap
```


Reverting and restoring a file

1. Verify that the volume is online and writable.
2. List the Snapshot copies in the volume.

```
::> volume snapshot show –vserver svm4 –volume svm4_vol_002
```

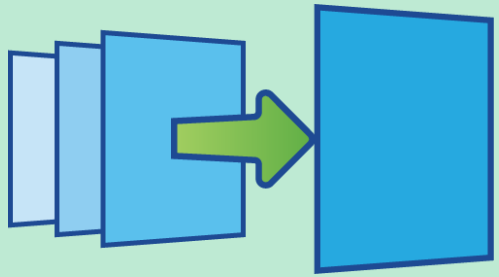
3. Notify network users about the reversion.
4. Identify the names of the Snapshot copy and the file to restore and initiate the reversion.

```
::> volume snapshot restore-file -vserver svm4 –volume svm4_vol_002
    -snapshot svm4_vol_002_snap –path /svm4_vol2/myfile.txt
```


SnapRestore technology versus copying

If a file is large (such as a database), you should use SnapRestore technology to revert instead of copying the file:

- Copying requires double the storage and time.
- Reverting saves time and reinstates the data.
- For reliability, NetApp recommends SnapRestore technology rather than alternative technologies.



Snapshot automatic delete

Use the **`volume snapshot autodelete modify`** command to modify the autodelete policy settings.

Enable automatic Snapshot copy deletion on a volume:

```
::> volume snapshot autodelete modify –vserver svm4 –volume svm4_vol_002
    –enabled true
```

Trigger automatic deletion of the oldest unlocked Snapshot copies when the volume threshold is exceeded:

```
::> volume snapshot autodelete modify -vserver svm4 -volume svm4_vol_002
    -trigger volume -commitment try -delete-order oldest_first
```


Lesson 3
Back up and replicate data

Disaster recovery and business continuance

There are two reasons for backing up and replicating data:

- **Disaster Recovery:** The ability to recover data that has been deleted, corrupted, infected by a virus, or physically lost due to a disaster
  - Network Data Management Protocol (NDMP) backup
  - SnapVault software
- **Business Continuance:** Using up-to-date replicas of data to keep a business operating despite a disaster
  - SnapMirror software
  - MetroCluster cluster configuration

Both reasons are constrained by Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

NDMP and SMTape backups

NDMP is the industry standard protocol that third-party backup applications use to back up data to physical or virtual tape devices.

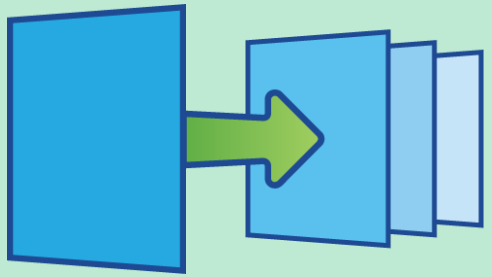
- Backup applications can use NDMP to perform a Snapshot copy-based backup of an entire volume, directory tree, or single file.
- NDMP supports baseline, differential, and incremental backups.

SMTape is a Snapshot copy-based solution that backs up volumes to tape.

- SMTape backs up and restores only entire volumes.
- SMTape is used primarily to back up Snapshot copies and to *seed* SnapMirror destination volumes.

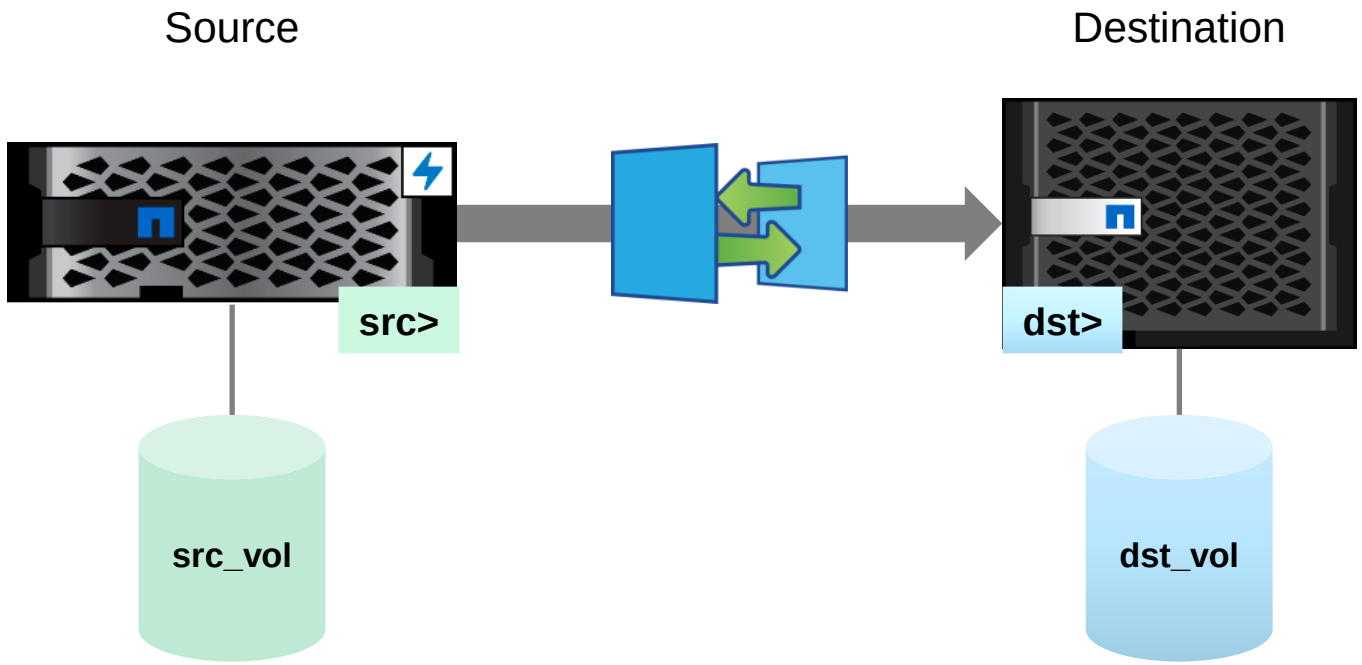
SnapVault software

- SnapVault software creates read-only backup copies on a destination volume.
- SnapVault software is frequently used to back up multiple production clusters to a few remote high-capacity disaster recovery clusters.
- Following are reasons for using SnapVault software instead of NDMP dump backups:
  - Data is stored on drives, so it is faster to access and to recover.
  - NDMP incrementals back up changed files. SnapVault software backs up only changed blocks.
  - SnapVault software can store hundreds of daily backups, often for lower costs than removable media.
  - SnapVault software provides efficient use of WAN resources for off-site backups.



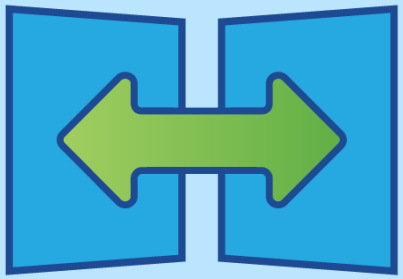
SnapMirror technology

SnapMirror technology enables the mirroring of volumes to other local or geographically remote systems.



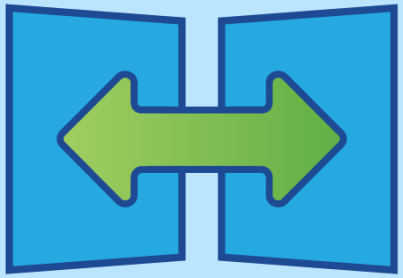
SnapMirror features and benefits

- The SnapMirror destination is a replica. Changes to the source are mirrored to the destination.
- Updates to the destination can be made frequently because only new and changed data blocks, rather than entire files, are sent.
- SnapMirror technology uses deduplication and compression and supports dual paths to keep latency low and network bandwidth needs to a minimum.
- For backup and recovery, NetApp SnapCenter software manages application-consistent and database-consistent backups, verification, cloning, and recovery.



SnapMirror foundational technology

- SnapMirror Asynchronous
- SnapMirror Synchronous
- SnapVault software
- SVM-DR
- SnapMirror Cloud
- SnapMirror Business Continuity

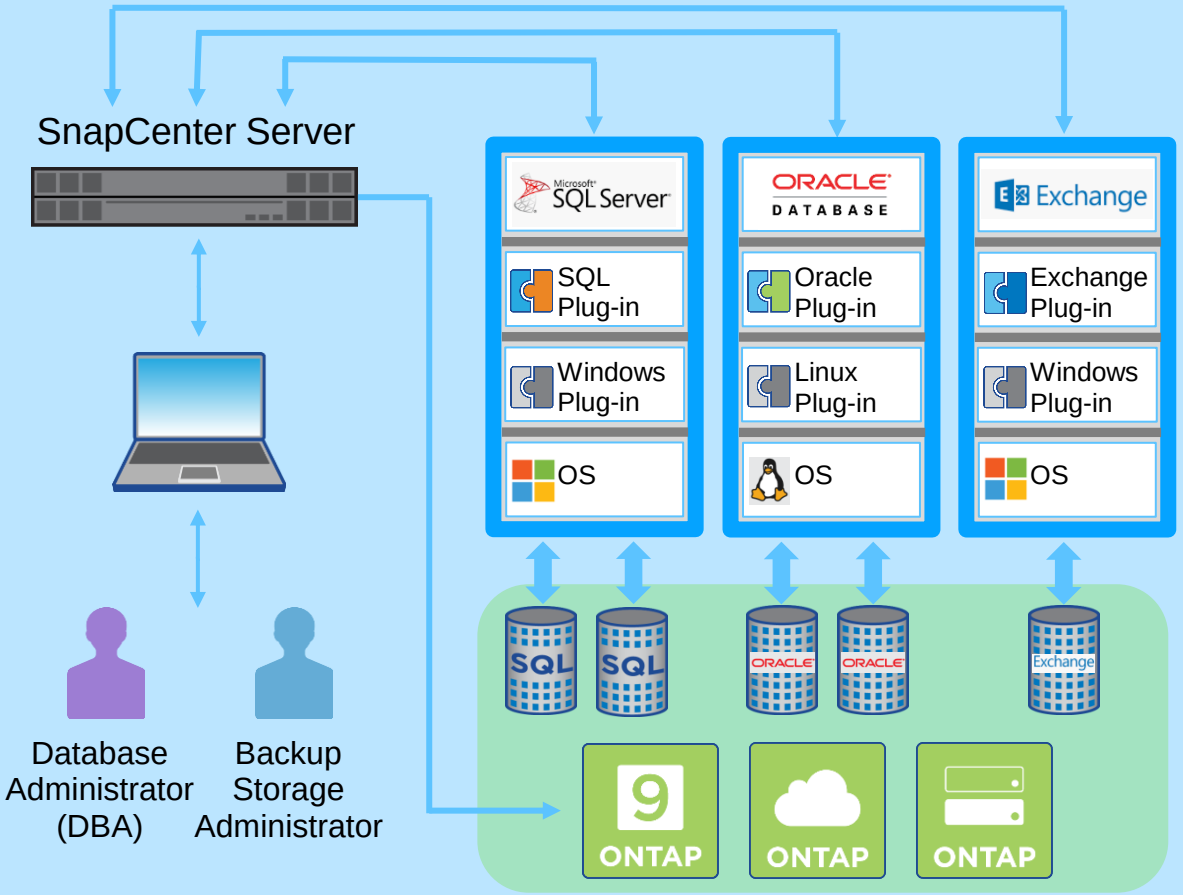


MetroCluster configuration

- A MetroCluster configuration geographically separates the partners in high-availability (HA) pairs.
- If a disaster damages the physical storage hardware or network access to the hardware, the cluster can continue to serve data.
- MetroCluster configuration is not an add-on feature or upgrade. Clusters must be physically installed and configured in a MetroCluster configuration.

SnapCenter

- Application-consistent data protection for applications, databases, host file systems, and VMs running on ONTAP systems anywhere in the hybrid cloud.
- Application plug-ins for:
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - Oracle databases on Linux
  - SAP HANA databases
  - VMware vSphere
- Sample custom plug-ins for other applications and databases available for download.



Lesson 4
Compliance

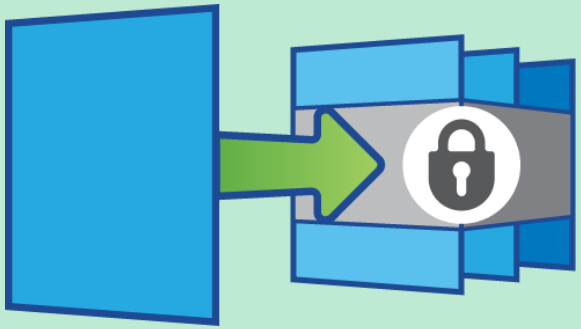
SnapLock

- SnapLock software is a high-performance compliance solution for organizations that use WORM storage to retain files in unmodified form for regulatory and governance purposes.
- Files are locked from modification for an administrator-defined length of time.

  Files in Snapshot copies and SnapMirror destinations are also locked until the time limit for all files expires.

  With SnapLock Enterprise administrators can delete files before the time limit expires.

  With SnapLock Compliance administrators can not delete files until after the time limit expires.
- SnapLock software requires a license.
- SnapLock software can be used in conjunction with storage encryption.

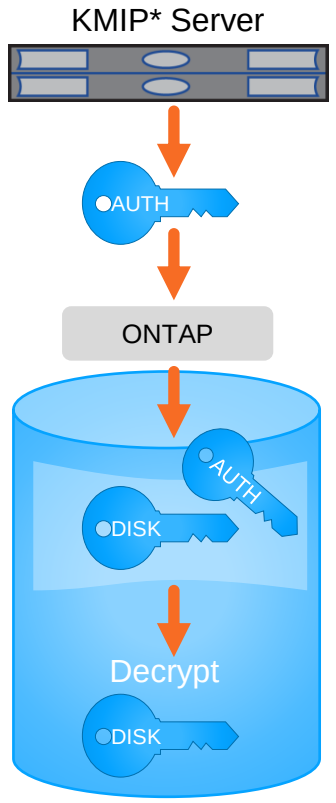


Recommended Practice: Learn and practice using SnapLock software on a simulator before implementing it because some mistakes are not reversible.

Lesson 5
Storage encryption

What is NetApp Storage Encryption?

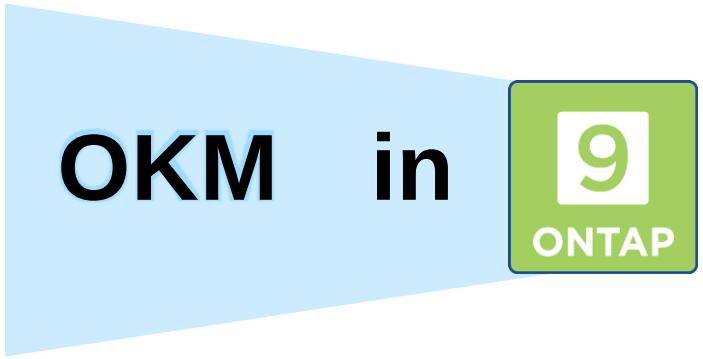
- NetApp Storage Encryption (NSE) is an ONTAP feature that provides support for self-encrypting drives (SEDs).
- SEDs protect data when it is at rest (when the drive is powered off).
- NSE manages the authorization process with a key management server to grant storage controllers access to the encrypted data on the drives.
- The encryption process is transparent to end users and has a minimal effect on performance.



* KMIP: Key Management Interoperability Protocol

Onboard key management

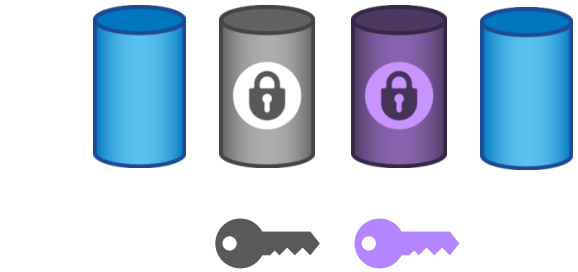
- The Onboard Key Manager (OKM) is a less expensive alternative to external KMIP servers. With onboard key management, the storage servers manage their own authentication to the NSE drives.
- You should not use OKM if any of the following conditions are true:
  - Your storage systems must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
  - You need a centralized, multicluster solution.
    OKM works only for the cluster that hosts the keys.
  - Your business requires the added security of storing authentication keys separately from the encrypted data.

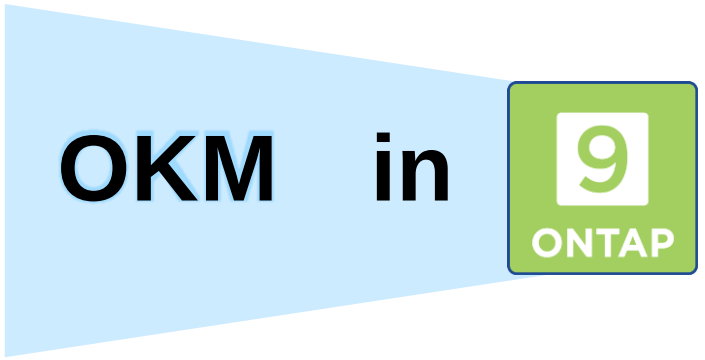


NetApp Volume Encryption

- NetApp Volume Encryption (NVE) is a software-based, data-at-rest encryption solution:
  - Encrypts sensitive data without relying on NSE drives
  - Uses Advanced Encryption Standard (AES)-256 encryption
  - Requires a license
- Each data volume has a unique encryption key:

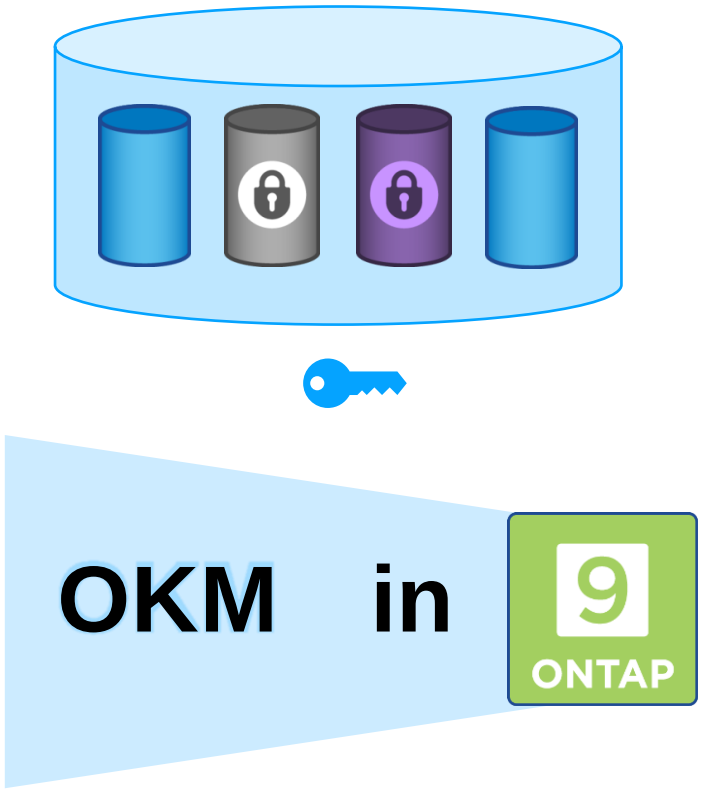
  Decide which volumes to encrypt and which to leave unencrypted.
- Encryption requires zero management:
  - Snapshot copies and FlexClone volumes are also encrypted.
  - If you are using a KMIP server, ONTAP automatically uploads the encryption key to the server when you encrypt a volume.





NetApp Aggregate Encryption

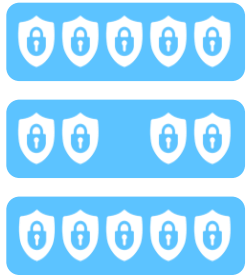
- You can use NetApp Aggregate Encryption (NAE) to assign encryption keys to the containing aggregate.
- Volumes that you create in the aggregate are encrypted by default by using the aggregate encryption keys.
- You can override the default encryption keys or disable encryption when you create the volume.



Additional storage security features

Use data encryption by default.

Data is encrypted automatically when key management is configured.

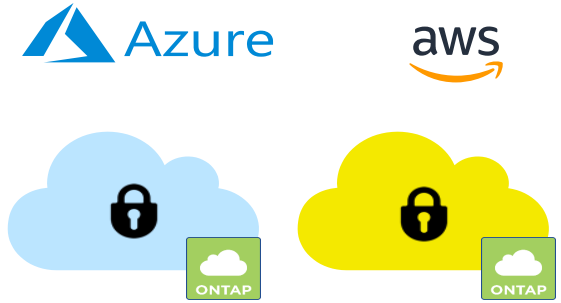


Honor “right to be forgotten.”

Manage new data-compliance regulations better with crypto-shredding of data through secure purge.

Protect systems in transit.

Protected controller reboot and secure Unified Extensible Firmware Interface (UEFI) boot prevent unwanted access of systems outside the data center.



Worry less about cloud security.

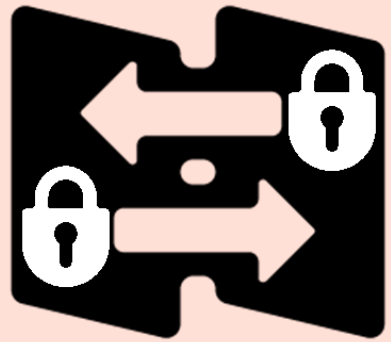
NVE support for NetApp Cloud Volumes ONTAP provides FIPS 140-2 certified encryption in the cloud.

? More info in Addendum

Securing in-flight data

Data traveling over a network to or from an ONTAP system is susceptible to interception and theft.

- All SnapMirror traffic between cluster peers is encrypted.
- Data accessed through the HTTPS protocol is encrypted.
- ONTAP 9.8 software includes the Internet Protocol security (IPsec) for encrypting IP traffic over Ethernet.
  - Uses a shared secret between the client and ONTAP software
  - Works with any client that supports Internet Key Exchange version 2



Knowledge check

Module 8: Data protection

Knowledge check

Data can be written to a Snapshot copy.

a. true

b. false

Knowledge check

Data can be written to a Snapshot copy.

a. true

b. false

Module summary

This module focused on enabling you to do the following:

- Manage Snapshot copies
- Restore data from Snapshot copies
- Back up and replicate data
- Use encryption to prevent unauthorized access to data

Additional data protection learning

Learn about advanced topics like configuration of intercluster replication, fan-in and fan-out strategies, and NetApp data-protection interfaces.

- *ONTAP Data Protection Fundamentals* (online course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000024323
- *ONTAP Data Protection Administration* (2-day instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022724
- *ONTAP Compliance Solutions Administration* (1-day instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000024832
- *ONTAP MetroCluster Installation* (2-day instructor-led course)
  https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/ledetail/cours000000000022663

References
Documentation

- ONTAP 9 Documentation Center: http://docs.netapp.com/ontap-9/index.jsp
  - *Logical Storage Management Guide*
  - *Data Protection Power Guide*
  - *Encryption Power Guide*
- *TR-4015 SnapMirror Configuration and Best Practices Guide*
- *TR-4678 Data Protection and Backup: NetApp FlexGroup Volumes*
- *Volume and Aggregate Encryption FAQ*

References
Videos

- NetApp SnapCenter Backup Management Software
  https://www.youtube.com/watch?v=ejsq7nNawI4
- ONTAP Data Security Overview
  https://www.youtube.com/watch?v=cY_iuayAL2M
- How to use the SnapLock feature in ONTAP 9
  https://www.youtube.com/watch?v=JUYtta3Ymdw

Complete an exercise

Module 8
Data protection

Managing Snapshot copies

- Access your lab equipment.
- Open your Exercise Guide, Module 8.
- Complete Exercise 1.
- Share your results.

This exercise requires approximately **30 minutes**.

Addendum
Secure purge and secure boot

Manage data spillage and right to erasure with secure purge

NVE for General Data Protection Regulation (GDPR) and US public sector

Immediate need to destroy data:

- When data with different classification levels accidentally ends up in the same volume
- To delete user data cryptographically to satisfy GDPR requirements

Cryptographically shred a single file from an encrypted volume when the file is not recoverable from the drives because the key has been deleted.

Protect systems in transit

Protected controller reboot

Passphrase required after reboot

Secure transport

Equipment return

Mission-forward deployments

Secure boot

Unified Extensible Firmware Interface

- Verifies that software is genuine NetApp ONTAP software during boot
- Prevents hacked or pre-release versions of ONTAP software anytime that the system boots
- Verifies signed ONTAP images by the boot loader