ONTAP cyber vault

NetApp Solutions

NetApp
September 14, 2024

Table of Contents

ONTAP cyber vault

ONTAP cyber vault overview

The primary driving threat that necessitates the implementation of cyber vaulting is the growing prevalence and evolving sophistication of cyber-attacks, particularly ransomware and data breaches. With a rise in phishing and ever more sophisticated methods of credential stealing, credentials used to begin a ransomware attack could then be used to access infrastructure systems. In these cases, even hardened infrastructure systems are at risk of attack. The only defense to a compromised system is to have your data protected and isolated in a cyber vault.

> Beginning in July 2024, content from technical reports previously published as PDFs has been integrated with ONTAP product documentation. In addition, new technical reports (TRs) such as this document will no longer be getting TR numbers.

What is cyber vaulting?

Cyber vaulting is a specific data protection technique that involves storing critical data in an isolated environment, separate from the primary IT infrastructure.

"Air gapped", **immutable** and **indelible** data repository that is immune to threats affecting the main network, such as malware, ransomware, or even insider threats. Cyber vaulting can be achieved with **immutable** and **indelible** snapshots.

Air-gapping backups that use traditional methods involve creating space and physically separating the primary and secondary media. By moving the media offsite and/or severing connectivity, bad actors have no access to the data. This protects the data but can lead to slower recovery times.

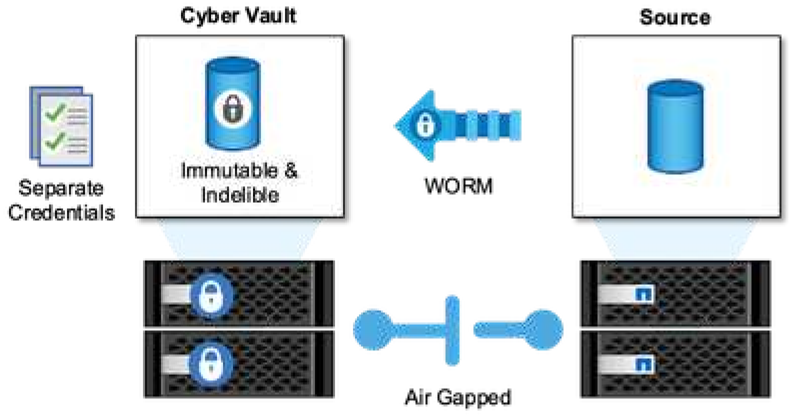
NetApp’s approach to cyber vaulting

Key features of NetApp reference architecture for cyber vaulting include:

- Secure, isolated storage infrastructure (e.g., air gapped storage systems)
- Copies of the data must be both **immutable** and **indelible** without exception
- Strict access controls and multi-factor authentication
- Rapid data restoration capabilities

You can use NetApp storage with ONTAP as an air-gapped cyber vault by leveraging SnapLock Compliance to WORM-protect Snapshot copies. You can perform all the basic SnapLock Compliance tasks on the Cyber vault. Once configured, Cyber vault volumes are automatically protected, eliminating the need to manually commit the Snapshot copies to WORM. More information on logical air-gapping can be found in this blog

SnapLock Compliance is used to comply with the Banking and Financial regulations SEC 70-a-4(f), FINRA 4511(c), and CFTC 1.31(c)-(d). It has been certified by Cohasset Associates to adhere to these regulations (audit report available upon request). By using SnapLock Compliance with this certification you get a hardened mechanism for air gapping of your data that is relied upon by the largest financial institutions in the world to ensure both retention and retrieval of banking records.



Cyber vault ONTAP terminology

These are the terms commonly used in cyber vault architectures.

Autonomous Ransomware Protection (ARP) - Autonomous Ransomware Protection (ARP) feature uses workload analysis in NAS (NFS and SMB) environments to proactively, and in real time, detect and warn about abnormal activity that might indicate a ransomware attack. When an attack is suspected, ARP also creates new Snapshot copies, in addition to existing protection from scheduled Snapshot copies. For more information, see the ONTAP documentation on Autonomous Ransomware Protection

Airgap (Logical) - You can configure NetApp storage with ONTAP as a logical air-gapped cyber vault by leveraging SnapLock Compliance to WORM-protect Snapshot copies

Airgap (Physical) - A physical airgapped system has no network connectivity to it. Using tape backups, you can move the images to another location. The SnapLock Compliance logical air gap is just as robust as a physical airgapped system.

Bastion host - A dedicated computer on an isolated network, configured to withstand attacks.

Immutable Snapshot copies - Snapshot copies that are not able to be modified, without exception (including a support organization or the ability to low level format the storage system).

Indelible Snapshot copies - Snapshot copies that are not able to be deleted, without exception (including a support organization or the ability to low level format the storage system).

Tamperproof Snapshot copies - Tamperproof Snapshot copies use the SnapLock Compliance clock feature to lock Snapshot copies for a specified period. These locked snapshots can not be deleted by any user or NetApp support. You can use locked Snapshot copies to recover data if a volume is compromised by a ransomware attack, malware, hacker, rogue administrator or accidental deletion. For more information, see the ONTAP documentation on Tamperproof Snapshot copies

SnapLock - SnapLock is a high-performance compliance solution for organizations that use WORM storage to retain files in unmodified form for regulatory and governance purposes. For more information, see the ONTAP documentation on SnapLock.

SnapMirror - SnapMirror is disaster recovery replication technology, designed to efficiently replicate data. SnapMirror can create a mirror (or exact copy of the data), vault (a copy of the data with longer Snapshot copy retention), or both to a secondary system, on premises or in the cloud. These copies can be used for many different purposes such as a disaster, bursting to the cloud, or a cyber vault (when using the vault policy and locking the vault). For more information, see the ONTAP documentation on SnapMirror

SnapVault - In ONTAP 9.3 SnapVault was deprecated in favor of configuring SnapMirror using the vault or mirror-vault policy. This is term, while still used, has been depreciated as well. For more information, see the ONTAP documentation on SnapVault.

Cyber vault sizing with ONTAP

Sizing a cyber vault requires understanding how much data that will need to be restored in a given Recovery Time Objective (RTO). Many factors play into properly designing a right sized cyber vault solution.

Sizing considerations

1. What are the source platform models (FAS v AFF A-Series v AFF C-Series)?
2. What is the bandwidth and latency between the source and cyber vault?
3. How large are the file sizes and how many files?
4. What is your recovery time objective?
5. How much data do you need to be recovered within the RTO?
6. How many SnapMirror fan-in relationships will the cyber vault be ingesting?
7. Will there be single or multiple recoveries happening at the same time?
8. Will those multiple recoveries be happening to the same primary?
9. Will SnapMirror be replicating to the vault during a recovery from a vault?

Creating a cyber vault with ONTAP

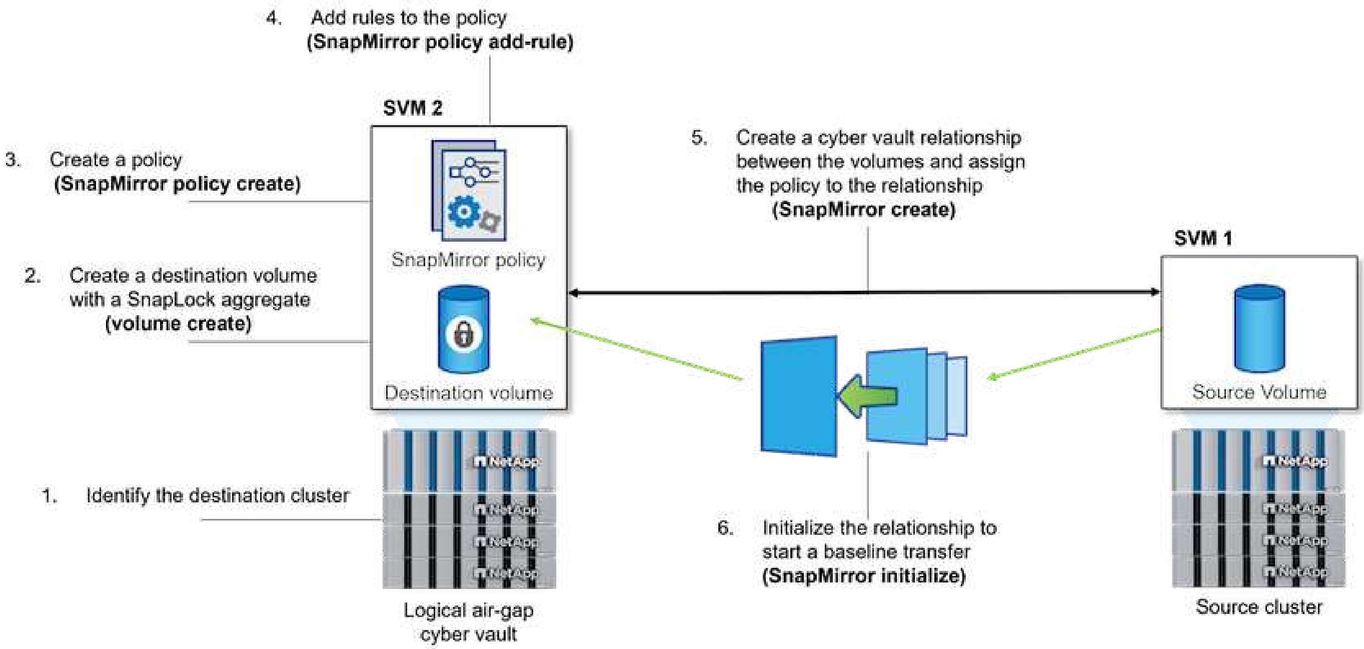
The steps below will assist with the creation of a cyber vault with ONTAP.

Before you begin

- The source cluster must be running ONTAP 9 or later.
- The source and destination aggregates must be 64-bit.
- The source and destination volumes must be created in peered clusters with peered SVMs. For more information, see Cluster Peering.
- If volume autogrow is disabled, the free space on the destination volume must be at least five percent more than the used space on the source volume.

About this task

The following illustration shows the procedure for initializing a SnapLock Compliance vault relationship:


4. Add rules to the policy (SnapMirror policy add-rule)
SVM 2
3. Create a policy (SnapMirror policy create)
SnapMirror policy
2. Create a destination volume with a SnapLock aggregate (volume create)
Destination volume
1. Identify the destination cluster
Logical air-gap cyber vault
5. Create a cyber vault relationship between the volumes and assign the policy to the relationship (SnapMirror create)
SVM 1
Source Volume
6. Initialize the relationship to start a baseline transfer (SnapMirror initialize)
Source cluster
NetApp

Steps

1. Identify the destination array to become the cyber vault to receive the air gapped data.
2. On the destination array, to prepare the cyber vault, install the ONTAP One license, initialize the Compliance Clock, and, if you are using an ONTAP release earlier than 9.10.1, create a SnapLock Compliance aggregate.
3. On the destination array, create a SnapLock Compliance destination volume of type DP:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name
   -snaplock-type compliance|enterprise -type DP -size size
   ```

4. Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate; therefore, you are no longer required to create a separate SnapLock aggregate if you are using ONTAP 9.10.1. You use the volume `-snaplock-type` option to specify a Compliance type. In ONTAP releases earlier than ONTAP 9.10.1, the SnapLock mode, Compliance is inherited from the aggregate. Version-flexible destination volumes are not supported. The language setting of the destination volume must match the language setting of the source volume.

   The following command creates a 2 GB SnapLock Compliance volume named `dstvolB` in `SVM2` on the aggregate `node01_aggr`:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate node01_aggr
   -snaplock-type compliance -type DP -size 2GG
   ```

5. On the destination cluster, to create the airgap, set the default retention period, as described in Set the default retention period.
   A SnapLock volume that is a vault destination has a default retention period assigned to it. The value for this period is initially set to a minimum of 0 years and maximum of 30 years for SnapLock Compliance volumes. Each NetApp Snapshot copy is committed with this default retention period at first. The default-retention-period must be changed. The retention period can be extended later, if needed, but never shortened. For more information, see Set retention time overview.
6. Create a new replication relationship between the non-SnapLock source and the new SnapLock destination you created in Step 3.

This example creates a new SnapMirror relationship with destination SnapLock volume dstvolB using a policy of XDPDefault to vault Snapshot copies labeled daily and weekly on an hourly schedule:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination-path
SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

Create a custom replication policy or a custom schedule if the available defaults are not suitable.

7. On the destination SVM, initialize the SnapVault relationship created in Step 5:

   ```
   snapmirror initialize -destination-path destination_path
   ```

8. The following command initializes the relationship between the source volume srcvolA on SVM1 and the destination volume dstvolB on SVM2:

   ```
   cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

9. After the relationship is initialized and idle, use the snapshot show command on the destination to verify the SnapLock expiry time applied to the replicated Snapshot copies.

   This example lists the Snapshot copies on volume dstvolB that have the SnapMirror label and the SnapLock expiration date:

   ```
   cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields snapmirror-
   label, snaplock-expiry-time
   ```

Cyber vault hardening

These are the additional recommendations to harden an ONTAP cyber vault. Please consult the ONTAP hardening guide below for more recommendations and procedures.

Cyber vault hardening recommendations

- Isolate the cyber vault’s management planes
- Do not enable data LIFs on the destination cluster as they are an additional attack vector
- On the destination cluster, limit intercluster LIF access to the source cluster with a service policy
- Segment the management LIF on the destination cluster for limited access with a service policy and a bastion host
- Restrict all data traffic from the source cluster to the cyber vault to allow only the ports required for SnapMirror traffic
- Where possible, disable any unneeded management access methods within ONTAP to decrease the attack surface
- Enable audit logging and remote log storage
- Enable multi-admin verification and require verification from an admin outside your regular storage administrators (e.g. CISO staff)
- Implement role-based access controls
- Require administrative multifactor authentication for System Manager and ssh
- Use token based authentication for scripts and REST API calls

Please refer to the ONTAP hardening guide, Multi-admin verification overview and ONTAP multifactor authentication guide for how to accomplish these hardening steps.

Cyber vault interoperability

ONTAP hardware and software can be used to create a cyber vault configuration.

ONTAP hardware recommendations

All ONTAP unified physical arrays can be used for a cyber vault implementation.

- FAS hybrid storage offers the most cost-efficient solution.
- AFF C-Series offers the most efficient power consumption and density.
- AFF A-Series is the highest performing platform offering the best RTO. With the recent announcement of our latest AFF A-Series, this platform will offer the best storage efficiency without performance compromise.

ONTAP software recommendations

Beginning with ONTAP 9.14.1, you can specify retention periods for specific SnapMirror labels in the SnapMirror policy of the SnapMirror relationship so that the replicated Snapshot copies from the source to the destination volume are retained for the retention-period specified in the rule. If no retention period is specified, the default-retention-period of the destination volume is used.

Beginning with ONTAP 9.13.1, you can instantaneously restore a locked Snapshot copy on the destination SnapLock volume of a SnapLock vault relationship by creating a FlexClone with the snaplock-type option set to "non-snaplock" and specifying the Snapshot copy as the "parent-snapshot" when executing the volume clone creation operation. Learn more about creating a FlexClone volume with a SnapLock type.

MetroCluster configuration

For MetroCluster configurations, you should be aware of the following:

- You can create a SnapVault relationship only between sync-source SVMs, not between a sync-source SVM and a sync-destination SVM.
- You can create a SnapVault relationship from a volume on a sync-source SVM to a data-serving SVM.
- You can create a SnapVault relationship from a volume on a data-serving SVM to a DP volume on a sync-source SVM.

Cyber vault resources

To learn more about the information described in this cyber vault information, refer to the following additional information and security concepts.

- NetApp Cyber vaulting: Multilayered Data Protection Solutions Brief
- NetApp Earns AAA Rating for Industry-First AI-Driven On-Box Ransomware Detection Solution
- Elevate cyber resilience with the most secure storage on the planet
- ONTAP security hardening guide

- NetApp Zero Trust
- NetApp Cyber Resilience
- NetApp Data Protection
- Cluster and SVM peering overview with the CLI
- SnapVault archiving