ONTAP® 9

Archive and Compliance Using SnapLock® Technology Power Guide

November 2020 | 215-11235_2020-11_en-us
doccomments@netapp.com

Updated for ONTAP 9.8

NetApp®

Contents

Deciding whether to use the Archive and Compliance Power Guide

This guide describes how to use NetApp SnapLock technology to retain files in unmodified form for regulatory and governance purposes. It shows you how to commit files and Snapshot copies to "write once, read many" (WORM) storage, and how to set retention periods for WORM-protected data.

You should use this guide if you want to work with SnapLock in the following ways:

- You want to use the ONTAP command-line interface (CLI), not ONTAP System Manager or an automated scripting tool.
  A limited but important set of SnapLock technology is available in System Manager. You can install SnapLock licenses, set the Compliance Clock, create SnapLock aggregates and volumes, and configure SnapLock volumes.
- You want to create Compliance or Enterprise aggregates to host SnapLock audit log volumes on MetroCluster configurations, with the following limitation:
  - SnapLock Enterprise is supported on mirrored and unmirrored aggregates.
  - SnapLock Compliance is supported on unmirrored aggregates only.

  All MetroCluster configurations support mirrored aggregates. See the ONTAP release notes to determine if your MetroCluster configuration supports unmirrored aggregates.
  ONTAP 9 Release Notes
- You want to use SnapLock Enterprise aggregates with FabricPool.
  Starting with ONTAP 9.8, SnapLock Enterprise aggregates are supported with FabricPool.
  Managing Storage Tiers By Using FabricPool
- You are not using SAN LUNs
  SAN LUNs are not supported on SnapLock volumes. Although it is possible to move SAN LUNs onto a SnapLock volume using legacy technology, this is not a supported operation, nor is any other operation involving SAN LUNs on a SnapLock volume.
- You are not using SMTape.
  SMTape is not supported by SnapLock.
- You are not creating Compliance aggregates for array LUNs.
  SnapLock Compliance aggregates do not support array LUNs.
- You are not creating Compliance aggregates with the SyncMirror option.
  SnapLock Compliance aggregates do not support SyncMirror plexes.

Note: SSDs and Flash Pool aggregates are supported by SnapLock starting with ONTAP 9.1.

The *Upgrade and Revert/Downgrade Guide* contains information about how to revert from ONTAP 9.1 to ONTAP 9.0 after you have created a SnapLock SSD or Flash Pool aggregate.

Upgrade, revert, or downgrade

If this guide is not suitable for your situation, you should see the following documentation instead:

- *ONTAP 9 commands*
- *Cluster management using System Manager*
- *NetApp Documentation: OnCommand Workflow Automation (current releases)*

What SnapLock is

SnapLock is a high-performance compliance solution for organizations that use WORM storage to retain files in unmodified form for regulatory and governance purposes. A single license entitles you to use SnapLock in strict *Compliance mode*, to satisfy external mandates like SEC Rule 17a-4, and a looser *Enterprise mode*, to meet internally mandated regulations for the protection of digital assets.

Differences between Compliance and Enterprise modes

SnapLock Compliance and Enterprise modes differ mainly in the level at which each mode protects WORM files:

- Compliance-mode WORM files are protected at the disk level.
  You cannot reinitialize a disk that contains Compliance-mode aggregates.
- Enterprise-mode WORM files are protected at the file level.

A related difference involves how strictly each mode manages file deletes:

- Compliance-mode WORM files cannot be deleted during the retention period.
- Enterprise-mode WORM files can be deleted during the retention period by the compliance administrator, using an audited *privileged delete* procedure.

After the retention period has elapsed, you are responsible for deleting any files you no longer need. Once a file has been committed to WORM, whether under Compliance or Enterprise mode, it cannot be modified, even after the retention period has expired.

You cannot move a WORM file during or after the retention period. You can copy a WORM file, but the copy will not retain its WORM characteristics.

The following table shows the differences between SnapLock Compliance and Enterprise modes:

Capability	SnapLock Compliance	SnapLock Enterprise
Privileged delete	No	Yes
Reinitialize disk	No	Yes
Destroy SnapLock aggregate and volume during retention period	No	Yes
Rename an aggregate or volume	No	Yes
Non-NetApp disks	No	Yes (with FlexArray Virtualization)
Use SnapLock volume for audit logging	Yes	Yes, starting with ONTAP 9.5
Single-file SnapRestore	No	Yes
SnapRestore	No	Yes
FlexClone	You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.	You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.
LUNs	No	No
SMTape	No	No

Capability	SnapLock Compliance	SnapLock Enterprise
MetroCluster configurations	SnapLock Compliance or Enterprise aggregates are supported to host SnapLock audit log volumes on MetroCluster configurations, with the following limitation: • SnapLock Enterprise is supported on mirrored and unmirrored aggregates. • SnapLock Compliance is supported only on unmirrored aggregates only. All MetroCluster configurations support mirrored aggregates. See the ONTAP release notes to determine if your MetroCluster configuration supports unmirrored aggregates. *ONTAP 9 Release Notes*	No
Support FabricPools on SnapLock aggregates	No	Yes, starting with ONTAP 9.8

MetroCluster configurations and compliance clocks

MetroCluster configurations use two compliance clock mechanisms, the Volume Compliance Clock (VCC) and the System Compliance Clock (SCC). The VCC and SCC are available to all SnapLock configurations. When you create a new volume on a node, its VCC is initialized with the current value of the SCC on that node. After the volume is created, the volume and file retention time is always tracked with the VCC.

When a volume is replicated to another site, its VCC is also replicated. When a volume switchover occurs, from Site A to Site B, for example, the VCC continues to be updated on Site B while the SCC on Site A halts when Site A goes offline.

When Site A is brought back online and the volume switchback is performed, the Site A SCC clock restarts while the VCC of the volume continues to be updated. Because the VCC is continuously updated, regardless of switchover and switchback operations, the file retention times do not depend on SCC clocks and do not stretch.

Committing files to WORM

You can use an application to commit files to WORM over NFS or CIFS, or use the SnapLock autocommit feature to commit files to WORM automatically. You can use a *WORM appendable file* to retain data that is written incrementally, like log information.

Data protection

SnapLock supports data protection methods that should satisfy most compliance requirements:

- You can use SnapLock for SnapVault to WORM-protect Snapshot copies on secondary storage.
- You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery.

7-Mode Transition

You can use the Copy-Based Transition (CBT) feature of the 7-Mode Transition Tool to migrate SnapLock volumes from 7-Mode to ONTAP. The SnapLock mode of the destination volume,

Compliance or Enterprise, must match the SnapLock mode of the source volume. You cannot use Copy-Free Transition (CFT) to migrate SnapLock volumes.

Encryption

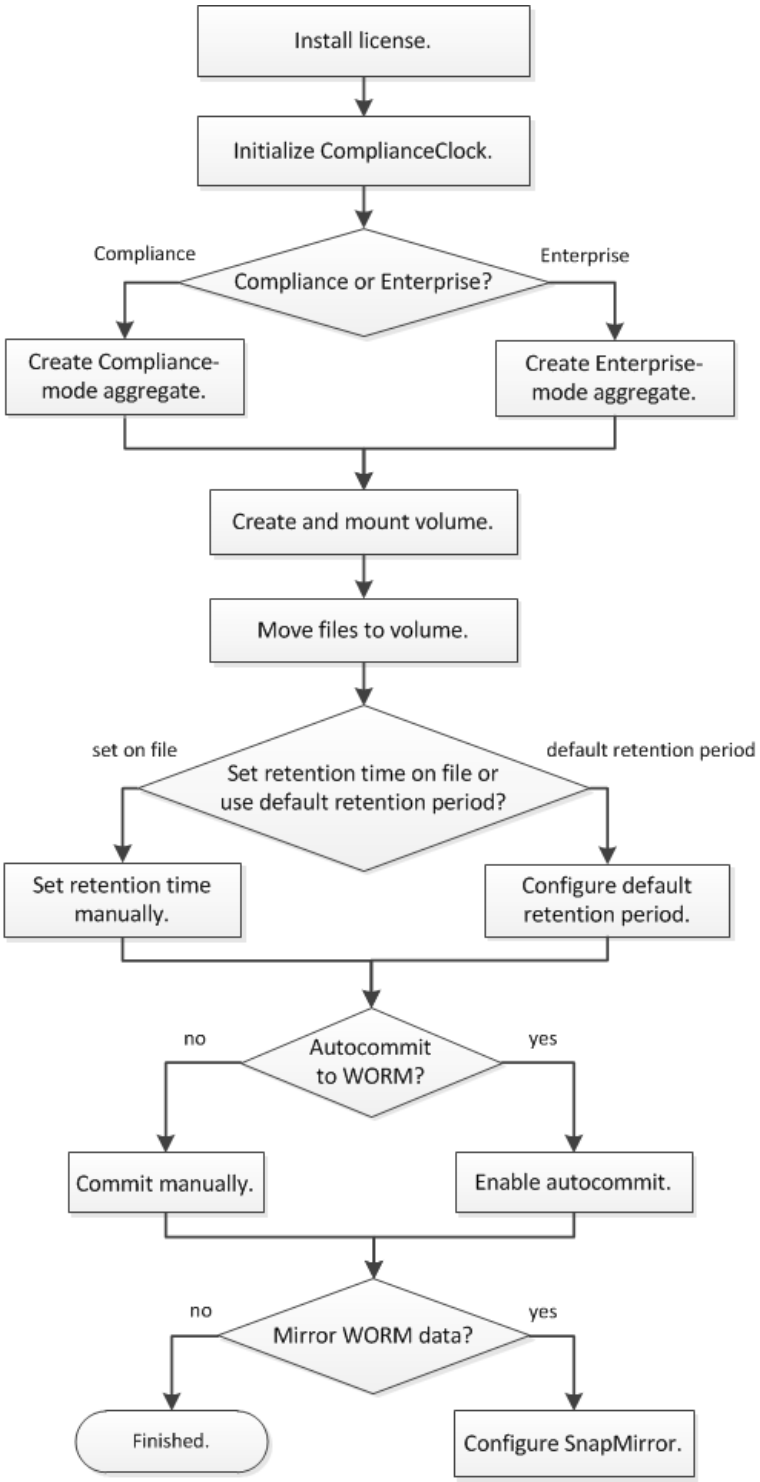
ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

Disclaimer: NetApp cannot guarantee that SnapLock-protected WORM files on self-encrypting drives or volumes will be retrievable if the authentication key is lost or if the number of failed authentication attempts exceeds the specified limit and results in the drive being permanently locked. You are responsible for ensuring against authentication failures.

Note: Starting with ONTAP 9.2, encrypted volumes are supported on SnapLock aggregates.

SnapLock workflow

You specify which SnapLock mode you want to use, Compliance or Enterprise, when you create a SnapLock aggregate. The SnapLock volume you create inherits the setting. You typically use a file archiving application to move files from primary storage to the SnapLock volume.



Configuring SnapLock

You must install the SnapLock license, initialize the ComplianceClock, create and configure a SnapLock aggregate and volume, and mount the volume before you can commit files to WORM.

Steps

Installing the license

A SnapLock license entitles you to use both SnapLock Compliance mode and SnapLock Enterprise mode. SnapLock licenses are issued on a per-node basis. You must install a license for each node that hosts a SnapLock aggregate.

Before you begin

You must be a cluster administrator to perform this task.

About this task

You should have received the SnapLock license keys from your sales representative.

Steps

1. Install the SnapLock license for a node:

   `system license add -license-code` *`license_key`*

   The following command installs the license with the key **`AAAAAAAAAAAAAAAAAAAAAAAAAAAA`**.

   ```
   cluster1::> system license add -license-code AAAAAAAAAAAAAAAAAAAAAAAAAAAA
   ```

2. Repeat the previous step for each node license.

Initializing the ComplianceClock

The SnapLock ComplianceClock ensures against tampering that might alter the retention period for WORM files. You must initialize the *system ComplianceClock* on each node that hosts a SnapLock aggregate. Once you initialize the ComplianceClock on a node, you cannot initialize it again.

Before you begin

- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.

About this task

The time on the system ComplianceClock is inherited by the *volume ComplianceClock*, which controls the retention period for WORM files on the volume. The volume ComplianceClock is initialized automatically when you create a new SnapLock volume.

Important: The initial setting of the ComplianceClock is based on the current system clock. For that reason, you should verify that the system time and time zone are correct before initializing the ComplianceClock. Once you initialize the ComplianceClock on a node, you cannot initialize it again.

Steps

1. Initialize the system ComplianceClock:

   snaplock compliance-clock initialize -node *node_name*

   The following command initializes the system ComplianceClock on **node1**:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

2. When prompted, confirm that the system clock is correct and that you want to initialize the ComplianceClock:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Repeat this procedure for each node that hosts a SnapLock aggregate.

Creating a SnapLock aggregate

You must create a SnapLock aggregate before creating a SnapLock volume. The Compliance or Enterprise SnapLock mode for the aggregate is inherited by the volumes in the aggregate.

Before you begin

- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.
- The ComplianceClock on the node must be initialized.
- If you have partitioned the disks as "root", "data1", and "data2", you must ensure that spare disks are available.

About this task

- You cannot create Compliance aggregates for array LUNs.
- You cannot create Compliance aggregates with the SyncMirror option.
- You can create Compliance or Enterprise aggregates in a MetroCluster configuration only if the aggregate is used to host SnapLock audit log volumes.

  Note: In a MetroCluster configuration, SnapLock Enterprise is supported on mirrored and unmirrored aggregates. SnapLock Compliance is supported only on unmirrored aggregates.

You can destroy or rename an Enterprise aggregate at any time. You cannot destroy a Compliance aggregate until the retention period has elapsed. Starting in ONTAP 9.8, you can rename a Compliance aggregate.

Step

Create a SnapLock aggregate:

storage aggregate create -aggregate *aggregate_name* -node *node_name* -diskcount *number_of_disks* -snaplock-type compliance|enterprise

The man page for the command contains a complete list of options.

The following command creates a SnapLock **Compliance** aggregate named **aggr1** with three disks on **node1**:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1 -diskcount 3 -snaplock-
type compliance
```

Creating a SnapLock volume

You must create a SnapLock volume for the files or Snapshot copies that you want to commit to the WORM state. The volume inherits the SnapLock mode—Compliance or Enterprise—from the SnapLock aggregate, and the ComplianceClock time from the node.

Before you begin

The SnapLock aggregate must be online.

About this task

You can destroy or rename an Enterprise volume at any time. You cannot destroy a Compliance volume until the retention period has elapsed. You can never rename a Compliance volume.

You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.

Note: LUNs are not supported on SnapLock volumes. Although it is possible to move LUNs onto a SnapLock volume using legacy technology, this is not a supported operation, nor is any other operation involving LUNs on a SnapLock volume.

Step

Create a SnapLock volume:

volume create -vserver *SVM_name* -volume *volume_name* -aggregate *aggregate_name*

For a complete list of options, see the man page for the command. The following options are not available for SnapLock volumes: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, and `vmalign`.

The following command creates a SnapLock **Compliance** volume named **vol1** on **aggr1** on **vs1**:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
```

Mounting a SnapLock volume

You can mount a SnapLock volume to a junction path in the SVM namespace for NAS client access.

Before you begin

The SnapLock volume must be online.

About this task

- You can mount a SnapLock volume only under the root of the SVM.
- You cannot mount a regular volume under a SnapLock volume.

Step

Mount a SnapLock volume:

volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*

For a complete list of options, see the man page for the command.

The following command mounts a SnapLock volume named **vol1** to the junction path **/sales** in the **vs1** namespace:

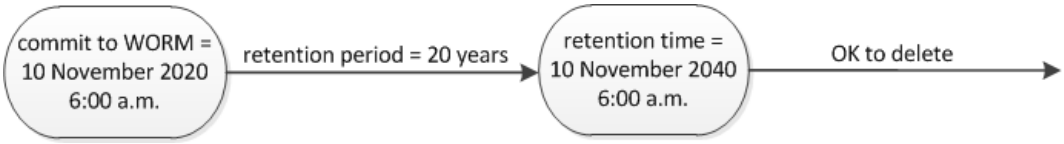
```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

Setting the retention time

You can set the retention time for a file explicitly, or you can use the default retention period for the volume to derive the retention time. Unless you set the retention time explicitly, SnapLock uses the default retention period to calculate the retention time.

Understanding retention period and retention time

The *retention period* for a WORM file specifies the length of time the file must be retained after it is committed to the WORM state. The *retention time* for a WORM file is the time after which the file no longer needs to be retained. A retention period of 20 years for a file committed to the WORM state on 10 November 2020 6:00 a.m., for example, would yield a retention time of 10 November 2040 6:00 a.m.



Note: Unless you set the default retention period to infinite, the maximum supported retention time is January 19 2071 (GMT).

Understanding the default retention periods

A SnapLock Compliance or Enterprise volume has four retention periods:

- Minimum retention period (**min**), with a default of 0
- Maximum retention period (**max**), with a default of 30 years
- Default retention period, with a default that depends on the mode:
  - For Compliance mode, the default is equal to **max**.
  - For Enterprise mode, the default is equal to **min**.
- Unspecified retention period.
  Starting in ONTAP 9.8, you can set the retention period on files in a volume to **unspecified**, to enable the file to be retained until you set an absolute retention time. You can set a file with absolute retention time to unspecified retention and back to absolute retention as long as the new absolute retention time is later than the absolute time you previously set.

So, if you do not set the retention time explicitly before committing a Compliance-mode file to the WORM state, and you do not modify the defaults, the file will be retained for 30 years. Similarly, if you do not set the retention time explicitly before committing an Enterprise-mode file to the WORM state, and you do not modify the defaults, the file will be retained for 0 years, or, effectively, not at all.

Choices

- *Setting the retention time for a file explicitly* on page 13
- *Setting the default retention period* on page 13

Setting the retention time for a file explicitly

You can set the retention time for a file explicitly by modifying its last access time. You can use any suitable command or program over NFS or CIFS to modify the last access time.

About this task

After a file has been committed to WORM, you can extend but not shorten the retention time. The retention time is stored in the `atime` field for the file.

Note: You cannot explicitly set the retention time of a file to **`infinite`**. That value is only available when you use the default retention period to calculate the retention time.

Step

Use a suitable command or program to modify the last access time for the file whose retention time you want to set.
In a UNIX shell, use the following command to set a retention time of 21 November 2020 6:00 a.m. on a file named `document.txt`:

```
touch -a -t 202011210600 document.txt
```

Note: You can use any suitable command or program to modify the last access time in Windows.

Setting the default retention period

You can use the `volume snaplock modify` command to set the default retention period for files on a SnapLock volume.

Before you begin

The SnapLock volume must be online.

About this task

The following table shows the possible values for the default retention period option:

Note: The default retention period must be greater than or equal to (>=) the minimum retention period and less than or equal to (<=) the maximum retention period.

Value	Unit	Notes
0 - 65535	seconds	
0 - 24	hours	
0 - 365	days	
0 - 12	months	
0 - 70	years	
max	-	Use the maximum retention period.
min	-	Use the minimum retention period.
infinite	-	Retain the files forever.
unspecified	-	Retain the files until an absolute retention period is set.

The values and ranges for the maximum and minimum retention periods are identical, except for **`max`** and **`min`**, which are not applicable. For more information about this task, see "Understanding the default retention period."

Understanding the default retention periods on page 12

You can use the `volume snaplock show` command to view the retention period settings for the volume. For more information, see the man page for the command.

Note: After a file has been committed to the WORM state, you can extend but not shorten the retention period.

Step

Set the default retention period for files on a SnapLock volume:

volume snaplock modify -vserver *SVM_name* -volume *volume_name* -default-retention-period *default_retention_period* -minimum-retention-period *min_retention_period* -maximum-retention-period *max_retention_period*

For a complete list of options, see the man page for the command.

Note: The following examples assume that the minimum and maximum retention periods have not been modified previously.

The following command sets the default retention period for a Compliance or Enterprise volume to 20 days:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default-retention-period
20days
```

The following command sets the default retention period for a Compliance volume to 70 years:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum-retention-period
70years
```

The following command sets the default retention period for an Enterprise volume to 10 years:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default-retention-period
max -maximum-retention-period 10years
```

The following commands set the default retention period for an Enterprise volume to 10 days:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum-retention-period
10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default-retention-period min
```

The following command sets the default retention period for a Compliance volume to infinite:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default-retention-period
infinite -maximum-retention-period infinite
```

Verifying SnapLock settings

You can use the `volume file fingerprint start` and `volume file fingerprint dump` commands to view key information about files and volumes, including the file type (regular, WORM, or WORM appendable), the volume expiration date, and so forth.

Steps

1. Generate a file fingerprint:

   volume file fingerprint start -vserver *SVM_name* -file *file_path*

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show -session-id
   16842791" to view the fingerprint session status.
   ```

   The command generates a session ID that you can use as input to the `volume file fingerprint dump` command.

Note: You can use the `volume file fingerprint show` command with the session ID to monitor the progress of the fingerprint operation. Make sure that the operation has completed before attempting to display the fingerprint.

2. Display the fingerprint for the file:

   `volume file fingerprint dump -session-id` *`session_ID`*

```
svm1::> volume file fingerprint dump -session-id 33619976
                                  Vserver:svm1
                               Session-ID:33619976
                                   Volume:slc_vol
                                     Path:/vol/slc_vol/f1
                         Data Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=
                     Metadata Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=
                    Fingerprint Algorithm:SHA256
                        Fingerprint Scope:data-and-metadata
                  Fingerprint Start Time:1460612586
          Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
                     Fingerprint Version:3
                        SnapLock License:available
                            Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
                             Volume MSID:2152884007
                             Volume DSID:1028
                                Hostname:my_host
                                Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
              Volume Containing Aggregate:slc_aggr1
                           Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
           SnapLock System ComplianceClock:1460610635
Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
                     Volume SnapLock Type:compliance
                    Volume ComplianceClock:1460610635
          Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
                       Volume Expiry Date:1465880998
          Is Volume Expiry Date Wraparound:false
              Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
                            Filesystem ID:1028
                                  File ID:96
                                File Type:worm
                                File Size:1048576
                            Creation Time:1460612515
                  Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
                        Modification Time:1460612515
               Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
                             Changed Time:1460610598
                Is Changed Time Wraparound:false
                    Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
                           Retention Time:1465880998
             Is Retention Time Wraparound:false
                 Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
                              Access Time:-
                    Formatted Access Time:-
                                 Owner ID:0
                                 Group ID:0
                                Owner SID:-
                     Fingerprint End Time:1460612586
           Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Resetting the ComplianceClock for an NTP-configured system

When the SnapLock secure clock daemon detects a skew beyond the threshold, the system time is used to reset both the system and volume ComplianceClocks.

Before you begin

- This feature is available only at the advanced privilege level.
- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.
- This feature is available only for Cloud Volumes ONTAP, ONTAP Select, and VSIM platforms.

About this task

When the SnapLock secure clock daemon detects a skew beyond the threshold, the system time is used to reset both the system and volume ComplianceClocks. A period of 24 hours is set as the

skew threshold. This means that the system ComplianceClock is synchronized to the system clock only if the skew is more than a day old.

The SnapLock secure clock daemon detects a skew and changes the ComplianceClock to the system time. Any attempt at modifying the system time to force the ComplianceClock to synchronize to the system time fails, since the ComplianceClock synchronizes to the system time only if the system time is synchronized with the NTP time.

Steps

1. Enable the SnapLock ComplianceClock time synchronization feature when an NTP server is configured:

   `snaplock compliance-clock ntp`

   The following command enables the system ComplianceClock time synchronization feature:

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

2. When prompted, confirm that the configured NTP servers are trusted and that the communications channel is secure to enable the feature:

   ```
   Warning: If Data ONTAP has been configured to use NTP server based system time, then
   this operation will
   make it possible for the SnapLock ComplianceClock to be synchronized to the system
   time. You must ensure that the
   configured NTP servers are trusted and the communication channel to them is secure.
   Failure to do this may result
   in SnapLock retention periods being compromised and compliance mandates being violated.

   Do you want to continue? {y|n}: y
   ```

3. Check that the feature is enabled:

   `snaplock compliance-clock ntp show`
   The following command checks that the system ComplianceClock time synchronization feature is enabled:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

Committing files to WORM

You can use a command or program to commit files to WORM manually, or use the SnapLock autocommit feature to commit files to WORM automatically.

Choices

Committing files to WORM manually

You commit a file to WORM manually by making the file read-only. You can use any suitable command or program over NFS or CIFS to change the read-write attribute of a file to read-only.

Before you begin

- The file you want to commit must reside on a SnapLock volume.
- The file must be writable.

About this task

The volume ComplianceClock time is written to the `ctime` field of the file when the command or program is executed. The ComplianceClock time determines when the retention time for the file has been reached.

Step

Use a suitable command or program to change the read-write attribute of a file to read-only.
In a UNIX shell, use the following command to make a file named **`document.txt`** read-only:

```
chmod -w document.txt
```

In a Windows shell, use the following command to make a file named **`document.txt`** read-only:

```
attrib +r document.txt
```

Autocommitting files to WORM

The SnapLock autocommit feature enables you to commit files to WORM automatically.

Before you begin

- The files you want to autocommit must reside on a SnapLock volume.
- The SnapLock volume must be online.
- The SnapLock volume must be a read-write volume.

Note: The SnapLock autocommit feature scans through all of the files in the volume and commits a file if it meets the autocommit requirement. There might be a time interval between when the file is ready for autocommit and when it is actually committed by the SnapLock autocommit scanner. However, the file is still protected from modifications and deletion by the file system as soon as it is eligible for autocommit.

About this task

The *autocommit period* specifies the amount of time that files must remain unchanged before they are autocommitted. Changing a file before the autocommit period has elapsed restarts the autocommit period for the file.

The following table shows the possible values for the autocommit period:

Value	Unit	Notes
none	-	The default.
5 - 5256000	minutes	-
1 - 87600	hours	-
1 - 3650	days	-
1 - 120	months	-
1 - 10	years	-

Note: The minimum value is 5 minutes and the maximum value is 10 years.

Step

Autocommit files on a SnapLock volume to WORM:

`volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-autocommit-period` *`autocommit_period`*

For a complete list of options, see the man page for the command.

The following command autocommits the files on volume **`vol1`** of SVM vs1, as long as the files remain unchanged for 5 hours:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit-period 5hours
```

Creating a WORM appendable file

A WORM appendable file retains data written incrementally, like log entries. You can use any suitable command or program to create a WORM appendable file, or you can use the SnapLock *volume append mode* feature to create WORM appendable files by default.

Using a command or program to create a WORM appendable file

You can use any suitable command or program over NFS or CIFS to create a WORM appendable file. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

Before you begin

The WORM appendable file must reside on a SnapLock volume.

About this task

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte n×256KB+1 of the file, the previous 256 KB segment becomes WORM-protected.

Steps

1. Use a suitable command or program to create a zero-length file with the desired retention time. In a UNIX shell, use the following command to set a retention time of 21 November 2020 6:00 a.m. on a zero-length file named **`document.txt`**:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. Use a suitable command or program to change the read-write attribute of the file to read-only. In a UNIX shell, use the following command to make a file named **`document.txt`** read-only:

```
chmod 444 document.txt
```

3. Use a suitable command or program to change the read-write attribute of the file back to writable.

   Note: This step is not deemed a compliance risk because there is no data in the file.

   In a UNIX shell, use the following command to make a file named **document.txt** writable:

```
chmod 777 document.txt
```

4. Use a suitable command or program to start writing data to the file.
   In a UNIX shell, use the following command to write data to **document.txt**:

```
echo test data >> document.txt
```

   Note: Change the file permissions back to read-only when you no longer need to append data to the file.

Using volume append mode to create WORM appendable files

Starting with ONTAP 9.3, you can use the SnapLock *volume append mode* (VAM) feature to create WORM appendable files by default. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

Before you begin

- The WORM appendable file must reside on a SnapLock volume.
- The SnapLock volume must be unmounted and empty of Snapshot copies and user-created files.

About this task

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte n×256KB+1 of the file, the previous 256 KB segment becomes WORM-protected.

If you specify an autocommit period for the volume, WORM appendable files that are not modified for a period greater than the autocommit period are committed to WORM.

Note: VAM is not supported on SnapLock audit log volumes.

Steps

1. Enable VAM:

   volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append-mode-enabled true|false

   For a complete list of options, see the man page for the command.

   The following command enables VAM on volume **vol1** of SVM **vs1**:

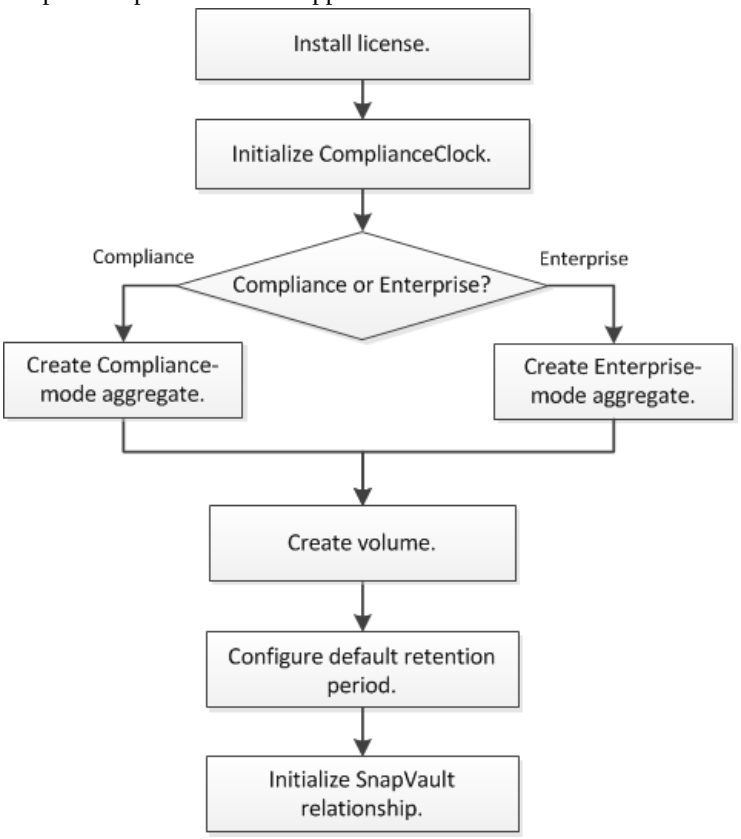
```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume-append-mode-
enabled true
```

2. Use a suitable command or program to create files with write permissions.

   The files are WORM appendable by default.

Committing Snapshot copies to WORM

You can use SnapLock for SnapVault to WORM-protect Snapshot copies on secondary storage. You perform all of the basic SnapLock tasks on the SnapVault destination. The destination volume is automatically mounted read-only, so there is no need to explicitly commit the Snapshot copies to WORM; therefore, creating scheduled Snapshot copies on the destination volume using SnapMirror policies is not supported.



Before you begin

- The source cluster must be running ONTAP 8.2.2 or later.
- The source and destination aggregates must be 64-bit.
- The source volume cannot be a SnapLock volume.
- The source and destination volumes must be created in peered clusters with peered SVMs.
  For more information, see the *Cluster Peering Express Guide*.
- 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 source volume can use NetApp or non-NetApp storage. For non-NetApp storage, you must use FlexArray Virtualization.

Note: You cannot rename a Snapshot copy that is committed to the WORM state.

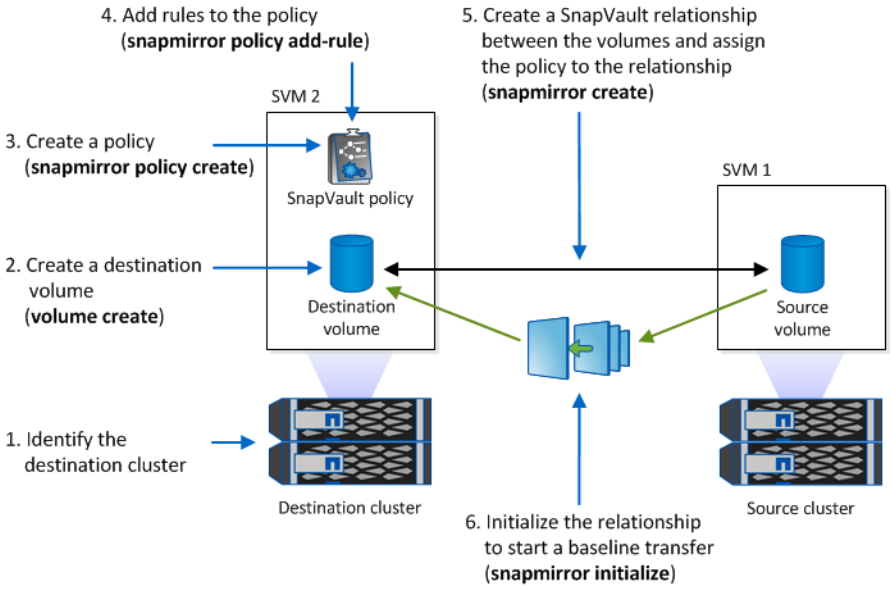
You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.

Note: LUNs are not supported on SnapLock volumes. Although it is possible to move LUNs onto a SnapLock volume using legacy technology, this is not a supported operation, nor is any other operation involving LUNs on a SnapLock volume.

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.

The following illustration shows the procedure for initializing a SnapVault relationship:



Steps

1. Identify the destination cluster.
2. On the destination cluster, install the SnapLock license, initialize the ComplianceClock, and create a SnapLock aggregate, as described in *Configuring SnapLock* on page 9.
3. On the destination cluster, create a SnapLock destination volume of type **DP** that is either the same or greater in size than the source volume:

   volume create -vserver *SVM_name* -volume *volume_name* -aggregate *aggregate_name* -type DP -size *size*

   Note: The SnapLock mode, Compliance or Enterprise, 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 -type
   DP -size 2GB
   ```

4. On the destination cluster, set the default retention period, as described in *Setting the default retention period* on page 13.

You can use the `snapshot extend-snapshot-retention` command to extend the retention period for Snapshot copies committed to WORM. For more information, see the man page for the command.

5. On the destination SVM, create a SnapVault policy:

   `snapmirror policy create -vserver` ***`SVM_name`*** **`-policy`** ***`policy_name`*** **`-type vault`**
   The following command creates the SVM-wide SnapVault policy **`SVM1-vault`**:

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-vault -type vault
   ```

6. Add rules to the policy that define Snapshot copy labels and the retention policy for each label:

   `snapmirror policy add-rule -vserver` ***`SVM_name`*** **`-policy`** ***`policy_name`*** **`-snapmirror-label`** ***`label`*** **`-keep`** ***`number_of_snapshot_copies_to_retain`***

   The following labels are available:

   - Daily
   - Weekly
   - Monthly
   - Hourly
   - Unlimited

   Note: The labels are case-sensitive.

   The following command adds a rule to the **`SVM1-vault`** policy that defines the **`Daily`** label and specifies that 30 Snapshot copies matching the label should be kept in the vault:

   ```
   SVM2::> snapmirror policy add-rule -vserver SVM2 -policy SVM1-vault
   -snapmirror-label Daily -keep 30
   ```

7. On the destination SVM, create a SnapVault schedule:

   `job schedule cron create -name` ***`schedule_name`*** **`-dayofweek`** ***`day_of_week`*** **`-hour`** ***`hour`*** **`-minute`** ***`minute`***
   The following command creates a SnapVault schedule named **`weekendcron`**:

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek "Saturday, Sunday" -hour
   3 -minute 0
   ```

8. On the destination SVM, create the SnapVault relationship and assign the SnapVault policy and schedule:

   `snapmirror create -source-path` ***`source_path`*** **`-destination-path`** ***`destination_path`*** **`-type XDP -policy`** ***`policy_name`*** **`-schedule`** ***`schedule_name`***
   The following command creates a SnapVault relationship between the source volume **`srcvolA`** on **`SVM1`** and the destination volume **`dstvolB`** on **`SVM2`**, and assigns the policy **`SVM1-vault`** and the schedule **`weekendcron`**:

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path SVM2:dstvolB -
   type XDP -policy SVM1-vault -schedule weekendcron
   ```

9. On the destination SVM, initialize the SnapVault relationship:

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

   The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all of the data blocks it references to the destination volume.

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

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

Related information

Cluster and SVM peering express configuration

Volume express backup using SnapVault

Mirroring WORM files

You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery and other purposes. Both the source volume and destination volume must be configured for SnapLock, and both volumes must have the same SnapLock mode, Compliance or Enterprise. All key SnapLock properties of the volume and files are replicated.

Before you begin

The source and destination volumes must be created in peered clusters with peered SVMs. For more information, see the *Cluster and SVM Peering Express Guide*.

About this task

- Starting with ONTAP 9.5, you can replicate WORM files with the XDP (extended data protection) type SnapMirror relationship rather than the DP (data protection) type relationship. XDP mode is ONTAP version-independent, and is able to differentiate files stored in the same block, making it much easier to resync replicated Compliance-mode volumes. For information on how to convert an existing DP-type relationship to an XDP-type relationship, see the *Data Protection Power Guide*.
- A resync operation on a DP type SnapMirror relationship fails for a Compliance-mode volume if SnapLock determines that it will result in a loss of data. If a resync operation fails, you can use the `volume clone create` command to make a clone of the destination volume. You can then resync the source volume with the clone.
- A SnapMirror relationship of type XDP between SnapLock compliant volumes supports a resync after a break even if data on the destination has diverged from the source post the break.

  On a resync, when data divergence is detected between the source the destination beyond the common snapshot, a new snapshot is cut on the destination to capture this divergence. The new snapshot and the common snapshot are both locked with a retention time as follows:

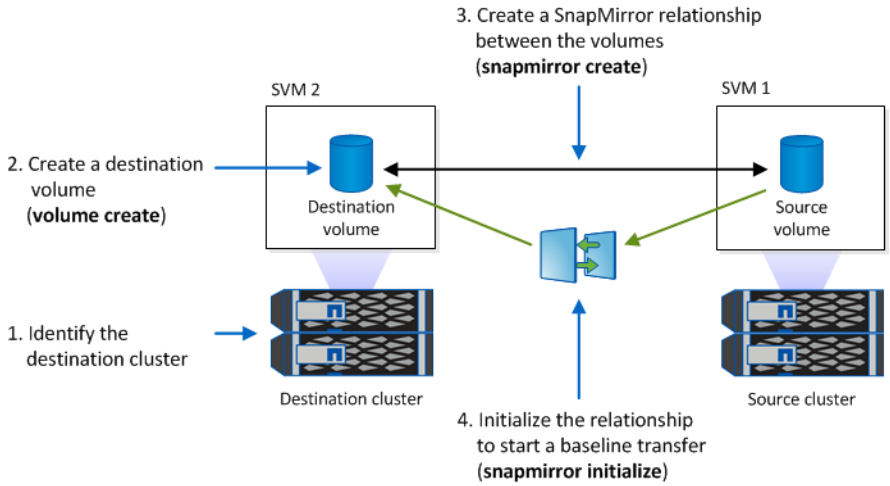
  - The volume expiry time of the destination
  - If the volume expiry time is in the past or has not been set, then the snapshot is locked for a period of 30 days
  - If the destination has legal-holds, the actual volume expiry period is masked and shows up as ‘indefinite’, however the snapshot is locked for the duration of the actual volume expiry period.

  If the destination volume has an expiry period that is later than the source, the destination expiry period is retained and will not be overwritten by the expiry period of the source volume post the resync.

  If the destination has legal-holds placed on it that differ from the source, a resync is not allowed. The source and destination must have identical legal-holds or all legal-holds on the destination must be released before a resync is attempted.

  A locked snapshot on the destination volume created to capture the divergent data can be copied to the source by running the `snapmirror update -s snapshot` command. The snapshot once copied will continue to be locked at the source as well.
- SVM data protection relationships are not supported.
- Load-sharing data protection relationships are not supported.

The following illustration shows the procedure for initializing a SnapMirror relationship:



Steps

1. Identify the destination cluster.
2. On the destination cluster, install the SnapLock license, initialize the ComplianceClock, and create a SnapLock aggregate.

   Configuring SnapLock on page 9
3. On the destination cluster, create a SnapLock destination volume of type **DP** that is either the same size as or greater in size than the source volume:

   volume create -vserver *SVM_name* -volume *volume_name* -aggregate *aggregate_name* -type DP -size *size*

   Note: The SnapLock mode—Compliance or Enterprise—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 -type
   DP -size 2GB
   ```
4. On the destination SVM, create a SnapMirror policy:

   snapmirror policy create -vserver *SVM_name* -policy *policy_name*
   The following command creates the SVM-wide policy **SVM1-mirror**:

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
   ```
5. On the destination SVM, create a SnapMirror schedule:

   job schedule cron create -name *schedule_name* -dayofweek *day_of_week* -hour *hour* -minute *minute*
   The following command creates a SnapMirror schedule named **weekendcron**:

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek "Saturday, Sunday" -hour
   3 -minute 0
   ```
6. On the destination SVM, create a SnapMirror relationship:

   snapmirror create -source-path *source_path* -destination-path *destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*
   The following command creates a SnapMirror relationship between the source volume **srcvolA** on **SVM1** and the destination volume **dstvolB** on **SVM2**, and assigns the policy **SVM1-mirror** and the schedule **weekendcron**:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination-path SVM2:dstvolB -
type XDP -policy SVM1-mirror -schedule weekendcron
```

Note: The XDP type is available in ONTAP 9.5 and later. You must use the DP type in ONTAP 9.4 and earlier.

7. On the destination SVM, initialize the SnapMirror relationship:

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

   The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a Snapshot copy of the source volume, then transfers the copy and all the data blocks that it references to the destination volume. It also transfers any other Snapshot copies on the source volume to the destination volume.

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

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

Related information

Cluster and SVM peering express configuration
Volume disaster recovery express preparation
Data protection

Creating an audit log

You must create a SnapLock-protected audit log before performing a privileged delete or SnapLock volume move. The audit log records the creation and deletion of SnapLock administrator accounts, modifications to the log volume, whether privileged delete is enabled, privileged delete operations, and SnapLock volume move operations.

Before you begin

You must be a cluster administrator to create a SnapLock aggregate.

About this task

You cannot delete an audit log until the log file retention period has elapsed. You cannot modify an audit log even after the retention period has elapsed.

Important: In ONTAP 9.4 and earlier, you cannot use a SnapLock Enterprise volume for audit logging. You must use a SnapLock Compliance volume. In ONTAP 9.5 and later, you can use either a SnapLock Enterprise volume or a SnapLock Compliance volume for audit logging.

In all cases, the audit log volume must be mounted at the junction path `/snaplock_audit_log`. No other volume can use this junction path.

You can find the SnapLock audit logs in the `/snaplock_log` directory under the root of the audit log volume, in subdirectories named `privdel_log` (privileged delete operations) and `system_log` (everything else). Audit log file names contain the timestamp of the first logged operation, making it easy to search for records by the approximate time that operations were executed.

- You can use the `snaplock log file show` command to view the log files on the audit log volume.
- You can use the `snaplock log file archive` command to archive the current log file and create a new one, which is useful in cases where you need to record audit log information in a separate file.

For more information, see the man pages for the commands.

Note: A data protection volume cannot be used as a SnapLock audit log volume.

Steps

1. Create a SnapLock aggregate.

   Creating a SnapLock aggregate on page 10

2. On the SVM that you want to configure for audit logging, create a SnapLock volume.

   Creating a SnapLock volume on page 11

3. Configure the SVM for audit logging:

   `snaplock log create -vserver` *`SVM_name`* `-volume` *`snaplock_volume_name`* `-max-file-size` *`size`* `-retention-period` *`default_retention_period`*

   Note: The minimum default retention period for audit log files is six months. If the retention period of an affected file is longer than the retention period of the audit log, the retention period of the log inherits the retention period of the file. So, if the retention period for a file deleted using privileged delete is 10 months, and the retention period of the audit log is 8 months, the retention period of the log is extended to 10 months.

   The following command configures the SVM **`SVM1`** for audit logging using the SnapLock volume **`logVol`**. The audit log has a maximum size of 20 GB and is retained for eight months.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-file-size 20GB -
retention-period 8months
```

4. On the SVM that you configured for audit logging, mount the SnapLock volume at the junction path `/snaplock_audit_log`.

Mounting a SnapLock volume on page 11

Using the privileged delete feature

You can use an audited *privileged delete* to delete Enterprise-mode WORM files during the retention period. You must be a SnapLock administrator to perform a privileged delete.

Steps

1. *Creating a SnapLock administrator account* on page 29
2. *Enabling the privileged delete feature* on page 29
3. *Deleting WORM files using privileged delete* on page 30

Creating a SnapLock administrator account

You must have SnapLock administrator privileges to perform a privileged delete. These privileges are defined in the vsadmin-snaplock role. If you have not already been assigned that role, you can ask your cluster administrator to create an SVM administrator account with the SnapLock administrator role.

Before you begin

- You must be a cluster administrator to perform this task.
- You must have logged in on a secure connection (SSH, console, or ZAPI).

Step

Create an SVM administrator account with the SnapLock administrator role:

`security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

The following command enables the SVM administrator account **`SnapLockAdmin`** with the predefined **`vsadmin-snaplock`** role to access the SVM **`SVM1`** using a password:

```
cluster1::> security login create -vserver SVM1 -user-or-group-name SnapLockAdmin -
application ssh -authmethod password -role vsadmin-snaplock
```

Enabling the privileged delete feature

You must explicitly enable the privileged delete feature on the Enterprise volume that contains the WORM files you want to delete.

About this task

The value of the `-privileged-delete` option determines whether privileged delete is enabled. Possible values are **`enabled`**, **`disabled`**, and **`permanently-disabled`**.

> **Note:** **`permanently-disabled`** is the terminal state. You cannot enable privileged delete on the volume after you set the state to **`permanently-disabled`**.

Step

Enable privileged delete for a SnapLock Enterprise volume:

`volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-privileged-delete disabled|enabled|permanently-disabled`

The following command enables the privileged delete feature for the Enterprise volume **`dataVol`** on the SVM **`SVM1`**:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged-delete enabled
```

Deleting WORM files using privileged delete

You can use the privileged delete feature to delete Enterprise-mode WORM files during the retention period.

Before you begin

- You must be a SnapLock administrator to perform this task.
- You must have created a SnapLock audit log and enabled the privileged delete feature on the Enterprise volume.

About this task

You cannot use a privileged delete operation to delete an expired WORM file. You can use the `volume file retention show` command to view the retention time of the WORM file that you want to delete. For more information, see the man page for the command.

Step

Delete a WORM file on an Enterprise volume:

`volume file privileged-delete -vserver` ***`SVM_name`*** **`-file`** ***`file_path`***

The following command deletes the file **`/vol/dataVol/f1`** on the SVM **`SVM1`**:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

Using the Legal Hold feature

Starting with ONTAP 9.3, you can use the *Legal Hold* feature to retain Compliance-mode WORM files for the duration of a litigation.

Before you begin

- You must be a SnapLock administrator to perform this task.
  Creating a SnapLock administrator account
- You must have logged in on a secure connection (SSH, console, or ZAPI).

About this task

A file under a Legal Hold behaves like a WORM file with an indefinite retention period. It is your responsibility to specify when the Legal Hold period ends.

The number of files you can place under a Legal Hold depends on the space available on the volume.

Steps

1. Start a Legal Hold:

   snaplock legal-hold begin -litigation-name *litigation_name* -volume *volume_name* -path *path_name*

   The following command starts a Legal Hold for all the files in **vol1**:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1 -volume vol1 -path /
   ```

2. End a Legal Hold:

   snaplock legal-hold end -litigation-name *litigation_name* -volume *volume_name* -path *path_name*

   The following command ends a Legal Hold for all the files in **vol1**:

   ```
   cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume vol1 -path /
   ```

Using the Event Based Retention (EBR) feature

Starting with ONTAP 9.3, you can use the SnapLock *Event Based Retention (EBR)* feature to define how long a file is retained after the occurrence of an event.

Before you begin

- You must be a SnapLock administrator to perform this task.
  Creating a SnapLock administrator account
- You must have logged in on a secure connection (SSH, console, or ZAPI).

About this task

The *event retention policy* defines the retention period for the file after the event occurs. The policy can be applied to a single file or all the files in a directory.

- If a file is not a WORM file, it will be committed to the WORM state for the retention period defined in the policy.
- If a file is a WORM file or a WORM appendable file, its retention period will be extended by the retention period defined in the policy.

You can use a Compliance-mode or Enterprise-mode volume.

Note: EBR policies cannot be applied to files under a Legal Hold.

For advanced usage, see *Compliant WORM Storage Using NetApp SnapLock*.

Compliant WORM Storage Using NetApp SnapLock

Using EBR to extend the retention period of already existing WORM files

EBR is convenient when you want to extend the retention period of already existing WORM files. For example, it might be your firm's policy to retain employee W-4 records in unmodified form for three years after the employee changes a withholding election. Another company policy might require that W-4 records be retained for five years after the employee is terminated.

In this situation, you could create an EBR policy with a five-year retention period. After the employee is terminated (the "event"), you would apply the EBR policy to the employee's W-4 record, causing its retention period to be extended. That will usually be easier than extending the retention period manually, particularly when a large number of files is involved.

Steps

1. Create an EBR policy:

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   The following command creates the EBR policy **`employee_exit`** on **`vs1`** with a retention period of ten years:

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name employee_exit -
   retention-period 10years
   ```

2. Apply an EBR policy:

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   The following command applies the EBR policy **`employee_exit`** on **`vs1`** to all the files in the directory **`d1`**:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name employee_exit -volume
vol1 -path /d1
```

Moving a SnapLock volume

Starting in ONTAP 9.8, you can move a SnapLock volume to a destination aggregate of the same type, either Enterprise to Enterprise, or Compliance to Compliance. You must be assigned the SnapLock security role to move a SnapLock volume.

Creating a SnapLock security administrator account

You must have SnapLock security administrator privileges to perform a SnapLock volume move. This privilege is granted to you with the *snaplock* role, introduced in ONTAP 9.8. If you have not already been assigned that role, you can ask your cluster administrator to create a SnapLock security user with this SnapLock security role.

Before you begin

- You must be a cluster administrator to perform this task.
- You must have logged in on a secure connection (SSH, console, or ZAPI).

About this task

The snaplock role is associated with the cluster SVM, unlike the vsadmin-snaplock role, which is associated with the data SVM.

Step

Create an SVM administrator account with the SnapLock administrator role:

security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

The following command enables the SVM administrator account **SnapLockAdmin** with the predefined **snaplock** role to access the SVM **SVM2** using a password:

```
cluster1::> security login create -vserver SVM2 -user-or-group-name SnapLockAdmin -
application ssh -authmethod password -role snaplock
```

Moving a SnapLock volume

You can use the `volume move` command to move a SnapLock volume to a destination aggregate.

Before you begin

- You must have created a SnapLock-protected audit log before performing SnapLock volume move.
  Creating an audit log on page 27
  .
- The destination aggregate must be the same SnapLock type as the SnapLock volume you want to move; either Compliance to Compliance or Enterprise to Enterprise.
- You must be a user with the SnapLock security snaplock role.

Steps

1. Using a secure connection, log in to the ONTAP cluster management LIF:

   ssh snaplock_user@node_mgmt_ip

2. Move a SnapLock volume:

   volume move start -vserver *SVM_name* -volume *SnapLock_volume_name* -destination-aggregate *destination_aggregate_name*

3. Check the status of the volume move operation:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
volume,phase,vserver
```

SnapLock APIs

You can use Zephyr APIs to integrate with SnapLock functionality in scripts or workflow automation. The APIs use XML messaging over HTTP, HTTPS, and Windows DCE/RPC.

file-fingerprint-abort

Abort a file fingerprint operation.

file-fingerprint-dump

Display file fingerprint information.

file-fingerprint-get-iter

Display the status of file fingerprint operations.

file-fingerprint-start

Generate a file fingerprint.

snaplock-archive-vserver-log

Archive the active audit log file.

snaplock-create-vserver-log

Create an audit log configuration for an SVM.

snaplock-delete-vserver-log

Delete an audit log configuration for an SVM.

snaplock-file-privileged-delete

Execute a privileged delete operation.

snaplock-get-file-retention

Get the retention period of a file.

snaplock-get-node-compliance-clock

Get the node ComplianceClock date and time.

snaplock-get-vserver-active-log-files-iter

Display the status of active log files.

snaplock-get-vserver-log-iter

Display the audit log configuration.

snaplock-modify-vserver-log

Modify the audit log configuration for an SVM.

snaplock-set-file-retention

Set the retention time for a file.

snaplock-set-node-compliance-clock

Set the node ComplianceClock date and time.

snaplock-volume-set-privileged-delete

Set the privileged-delete option on a SnapLock Enterprise volume.

volume-get-snaplock-attrs

Get the attributes of a SnapLock volume.

volume-set-snaplock-attrs

Set the attributes of a SnapLock volume.

Where to find additional information

You can learn more about the tasks described in this guide in NetApp's extensive documentation library.

- *ONTAP 9 commands*
  Describes SnapLock commands in reference format.
- *Cluster management using System Manager*
  Describes how to use ONTAP System Manager to install SnapLock licenses, set the Compliance Clock, create SnapLock aggregates and volumes, and configure SnapLock volumes.
- *NetApp Documentation: OnCommand Workflow Automation (current releases)*
  Describes how to use the OnCommand Workflow Automation scripting tool to perform SnapLock-related tasks.
- *Cluster and SVM peering express configuration*
  Describes how to quickly configure peer relationships between clusters and SVMs.
- *Volume express backup using SnapVault*
  Describes how to prepare volumes for SnapVault replication.
- *Volume disaster recovery express preparation*
  Describes how to prepare volumes for SnapMirror replication.
- *Volume disaster express recovery*
  Describes how to restore volumes after a disaster.

Copyright and trademark

Copyright

Trademark