Manage WORM files

ONTAP 9

NetApp
July 17, 2023

Table of Contents

Manage WORM files

Manage WORM files

You can manage WORM files in the following ways:

- Commit files to WORM
- Commit Snapshot copies to WORM on a vault destination
- Mirror WORM files for disaster recovery
- Retain WORM files during litigation
- Delete WORM files

Commit files to WORM

You can commit files to WORM (write once, read many) either manually or by committing them automatically. You can also create WORM appendable files.

Commit 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. You might choose to manually commit files if you want to ensure an application has finished writing to a file so that the file isn't committed prematurely or if there are scaling issues for the autocommit scanner because of a high number of volumes.

What you'll need

- 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.

Steps

1. 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
   ```

Commit files to WORM automatically

The SnapLock autocommit feature enables you to commit files to WORM automatically. The autocommit feature commits a file to WORM state on a SnapLock volume if the file did not change for the autocommit-period duration. The autocommit feature is disabled by default.

What you'll need

- 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.

> 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	-

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

Steps

1. 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
```

Create 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.

Use 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.

What you'll need

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.

   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
```

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

Use volume append mode to create WORM appendable files

Beginning 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.

What you'll need

- 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.

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.

Commit Snapshot copies to WORM on a vault destination

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 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 source volume can use NetApp or non-NetApp storage. For non-NetApp storage, you must use FlexArray Virtualization.

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.

LUNs are not supported in SnapLock volumes. LUNs are supported in SnapLock volumes only in scenarios where Snapshot copies created on a non-SnapLock volume are transferred to a SnapLock volume for protection as part of SnapLock vault relationship. LUNs are not supported in read/write SnapLock volumes. Tamperproof Snapshot copies however are supported on both SnapMirror source volumes and destination volumes that contain LUNs.

Beginning with ONTAP 9.13.1, you can instantaneously restore a locked Snapshot copy on the destination SnapLock volume of a SnapLock for SnapVault 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.

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, if you are using an ONTAP release earlier than 9.10.1, create a SnapLock aggregate, as described in SnapLock workflow.
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`* `-snaplock-type compliance|enterprise -type DP -size` *`size`*

   > 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 or Enterprise SnapLock volume type. In ONTAP releases earlier than ONTAP 9.10.1, 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 -snaplock-type compliance -type DP -size 2GB
   ```

4. On the destination cluster, 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 for SnapLock Enterprise volumes and a maximum of 30 years for SnapLock Compliance volumes. Each NetApp Snapshot copy is committed with this default retention period at first. The retention period can be extended later, if needed. For more information, see Set retention time overview.

5. 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.

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

snapmirror initialize -destination-path *destination_path*

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
```

7. After the relationship is initialized and idle, use the `snapshot show` command on the destination to verify 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
```

Related information

Cluster and SVM peering

Volume backup using SnapVault

Mirror WORM files for disaster recovery

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.

Prerequisites

The source and destination volumes must be created in peered clusters with peered SVMs. For more information, see Cluster and SVM peering.

About this task

- Beginning 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 Data Protection.
- 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 copy on the destination volume created to capture the divergent data can be copied to the source using the CLI 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:

System Manager

Beginning with ONTAP 9.12.1, you can use System Manager to set up SnapMirror replication of WORM files.

Steps

1. Navigate to **Storage > Volumes**.
2. Click **Show/Hide** and select **SnapLock Type** to display the column in the **Volumes** window.
3. Locate a SnapLock volume.
4. Click ⋮ and select **Protect**.
5. Choose the destination cluster and the destination storage VM.
6. Click **More Options**.
7. Select **Show legacy policies** and select **DPDefault (legacy)**.
8. In the **Destination Configuration details** section, select **Override transfer schedule** and select **hourly**.
9. Click **Save**.
10. To the left of the source volume name, click the arrow to expand the volume details, and on the right side of the page,review the remote SnapMirror protection details.
11. On the remote cluster, navigate to **Protection Relationships**.
12. Locate the relationship and click the destination volume name to view the relationship details.
13. Verify that the destination volume SnapLock type and other SnapLock information.

CLI

1. Identify the destination cluster.
2. On the destination cluster, install the SnapLock license, initialize the ComplianceClock, and, if you are using an ONTAP release earlier than 9.10.1, create a SnapLock aggregate.
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 -snaplock-type compliance|enterprise -type DP -size size
   ```

   > ⓘ 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 or Enterprise SnapLock volume type. In ONTAP releases earlier than ONTAP 9.10.1, 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 -snaplock-type compliance -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
   ```

   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

Volume disaster recovery preparation

Data protection

Retain WORM files during litigation using Legal Hold

Beginning with ONTAP 9.3, you can retain Compliance-mode WORM files for the duration of a litigation by using the *Legal Hold* feature.

What you'll need

- You must be a SnapLock administrator to perform this task.

  Create 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 /
```

Delete WORM files overview

You can delete Enterprise-mode WORM files during the retention period using the privileged delete feature. Before you can use this feature, you must create a SnapLock administrator account and then using the account, enable the feature.

Create 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.

What you'll need

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

Steps

1. 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 `SVM1` using a password:

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

Enable 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`.

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

Steps

1. 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 `SVM1`:

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

Delete Enterprise-mode WORM files

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

What you'll need

- 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

1. 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
   ```

Copyright information

Trademark information