Configure SnapLock

ONTAP 9

NetApp
December 04, 2021

Table of Contents

Configure SnapLock

Install 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.

What you'll need

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.

Initialize 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.

What you'll need

- 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.

> 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.

Create a SnapLock aggregate

You use the volume `-snaplock-type` option to specify a Compliance or Enterprise SnapLock volume type. For releases earlier than ONTAP 9.10.1, you must create a separate SnapLock aggregate. 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.

What you'll need

- 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.

Revert considerations

If you need to revert to an ONTAP version earlier than 9.10.1, you must move all SnapLock Compliance, SnapLock Enterprise, and SnapLock volumes to their own SnapLock aggregates.

About this task

- You cannot create Compliance aggregates for FlexArray LUNs, but SnapLock Compliance aggregates are supported with FlexArray LUNs.

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

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

Steps

1. 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
   ```

Create a SnapLock volume

You must create a SnapLock volume for the files or Snapshot copies that you want to commit to the WORM state. Beginning with ONTAP 9.10.1, any volume you create, regardless of the aggregate type, is created by default as a non-SnapLock volume. You must use the `-snaplock-type` option to explicitly create a SnapLock volume by specifying either Compliance or Enterprise as the SnapLock type. By default, the SnapLock type is set to `non-snaplock`.

What you'll need

- The SnapLock aggregate must be online.
- The SnapLock license must be installed on the node.
- The ComplianceClock on the node must be initialized.

About this task

With the proper SnapLock permissions, 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. The clone volume will be of the same SnapLock type as the parent volume.

> 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.

Steps

1. Create a SnapLock volume:

   volume create -vserver *SVM_name* -volume *volume_name* -aggregate *aggregate_name* -snaplock-type compliance|enterprise

   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
   -snaplock-type compliance
   ```

Mount a SnapLock volume

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

What you'll need

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.

Steps

1. 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
   ```

Set the retention time

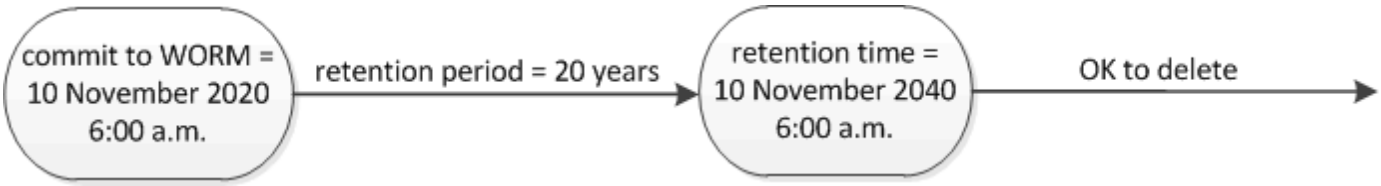
Set the retention time overview

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.

About 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.



Beginning with ONTAP 9.10.1, you can set a retention time up to October 26, 3058 and a retention period up to 100 years. When you extend retention dates, older policies are converted automatically. In ONTAP 9.9.1 and earlier releases, unless you set the default retention period to infinite, the maximum supported retention time is January 19 2071 (GMT).

Important revert considerations

ONTAP prevents you from reverting a cluster from ONTAP 9.10.1 to an earlier ONTAP version when there are any files with a retention period later than “January 19, 2071 8:44:07 AM”.

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 equal to `min` for both Compliance mode and Enterprise mode beginning with ONTAP 9.10.1. In ONTAP releases earlier than ONTAP 9.10.1, the default retention period 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.

Set 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.

> 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.

Steps

1. 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
   ```

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

Set the default retention period

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

What you'll need

The SnapLock volume must be online.

About this task

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

> 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	

Value	Unit	Notes
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 Set the retention time overview.

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.

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

Steps

1. 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.

   > 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
```

Verify 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.

   > 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
```

Reset 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.

What you'll need

- 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:
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
```