Tamperproof Snapshot copy locking

ONTAP 9

NetApp
December 01, 2022

Table of Contents

Tamperproof Snapshot copy locking

Tamperproof Snapshot copy locking overview

Beginning with ONTAP 9.12.1, you can lock a Snapshot copy on a non-SnapLock volume to provide protection from ransomware attacks. Locking Snapshot copies ensures that they can't be deleted accidentally or maliciously.

You use the SnapLock compliance clock feature to lock Snapshot copies for a specified period so that they cannot be deleted until the expiration time is reached. Locking Snapshot copies makes them tamperproof, protecting them from ransomware threats. You can use locked Snapshot copies to recover data if a volume is compromised by a ransomware attack.

Tamperproof Snapshot copy requirements and considerations

- All nodes in the cluster must be running ONTAP 9.12.1 or later.
- The SnapLock license must be installed on the cluster.

  For details, see Installing the SnapLock license
- The compliance clock on the cluster must be initialized.

  For details, see Initialize the Compliance Clock
- When Snapshot locking is enabled on a volume, you can upgrade the clusters to a version of ONTAP later than ONTAP 9.12.1; however, you cannot revert to an earlier version of ONTAP until all locked Snapshot copies have reached their expiration date and are deleted and Snapshot copy locking is disabled.
- When a Snapshot is locked, the volume expiry time is set to the expiry time of the Snapshot copy. If more than one Snapshot copy is locked, the volume expiry time reflects the largest expiry time among all Snapshot copies.
- The retention period for locked Snapshot copies takes precedence over the Snapshot copy keep count, which means the keep count limit is not honored if the Snapshot copy retention period for locked Snapshot copies has not expired.
- In a SnapMirror relationship, you can set a retention period on a mirror-vault policy rule, and the retention period is applied for Snapshot copies replicated to the destination if the destination volume has Snapshot copy locking enabled. The retention period takes precedence over keep count; for example, Snapshot copies that have not passed their expiry will be retained even if the keep count is exceeded.
- You can rename a Snapshot copy on a non-SnapLock volume. Snapshot rename operations on the primary volume of a SnapMirror relationship are reflected on the secondary volume only if the policy is MirrorAllSnapshots. For other policy types, the renamed Snapshot copy is not propagated during updates.
- You can restore a locked Snapshot copy with the `volume snapshot restore` command only if the locked Snapshot copy is the most recent. If there are any unexpired Snapshot copies later than the one being restored, the Snapshot copy restore operation fails.

Features supported with tamperproof Snapshot copies

- FlexGroup volumes

  Snapshot copy locking is supported on FlexGroup volumes. Snapshot locking occurs only on the root

constituent Snapshot copy. Deleting the FlexGroup volume is allowed only if the root constituent expiration time has passed.

- FlexVol to FlexGroup conversion

  You can convert a FlexVol volume with locked Snapshot copies to a FlexGroup volume. Snapshot copies remain locked after the conversion.

- FabricPool

  Snapshot copy locking is supported on FabricPool volumes only if the volume does not have any blocks tiered to the cloud and the tiering policy is set to “none”. When the Snapshot copy locking feature is enabled, setting the tiering policy on the volume to a policy other than “none” is not allowed.

Unsupported features

The following features currently are not supported with tamperproof Snapshot copies:

- Consistency groups
- FlexCache volumes
- SMtape
- SnapMirror Business Continuity (SM-BC)
- SnapMirror Synchronous

Enable Snapshot copy locking

Beginning with ONTAP 9.12.1, you can enable Snapshot copy locking when you create a new volume or when you modify an existing volume by using the `-snapshot-locking-enabled` option with the `volume create` and `volume modify` commands.

Enable Snapshot copy locking when creating a volume

1. To create a new volume and enable Snapshot copy locking, enter the following command:

   ```
   volume create -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

   The following command enables Snapshot copy locking on a new volume named vol1:

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked Snapshot copies
   are past their expiry time. A volume with unexpired locked Snapshot
   copies cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Enable Snapshot copy locking on an existing volume

1. To modify an existing volume to enable Snapshot copy locking, enter the following command:

   ```
   volume modify -vserver vserver_name -volume volume_name -snapshot-locking
   -enabled true
   ```

Create a locked Snapshot copy

Beginning with ONTAP 9.12.1, you can create Snapshot copy policies to apply a Snapshot copy retention period and apply the policy to a volume to lock Snapshot copies for the specified period. You can also lock a Snapshot copy by manually setting a retention period.

Create a Snapshot copy locking policy

1. To create a Snapshot copy policy, enter the following command:

   ```
   volume snapshot policy create -policy policy_name -enabled true -schedule1
   schedule1_name -count1 maximum_Snapshot_copies -retention-period1
   _retention_period
   ```

   The following command creates a Snapshot copy locking policy:

   ```
   cluster1> volume snapshot policy create -policy policy_name -enabled
   true -schedule1 5min -count1 5 -retention-period1 "1 months"
   ```

Apply a locking policy to a volume

1. To apply a Snapshot copy locking policy to an existing volume, enter the following command:

   ```
   volume modify -volume volume_name -vserver vserver_name -snapshot-policy
   policy_name
   ```

Apply retention period during manual Snapshot copy creation

1. To create a Snapshot copy manually and apply a locking retention period, enter the following command:

   ```
   volume snapshot create -volume volume_name -snapshot snapshot_copy_name
   -expiry-time expiration_date_time
   ```

   The following command creates a new Snapshot copy and sets the retention period:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Apply retention period to an existing Snapshot copy

1. To manually apply a retention period to an existing Snapshot copy, enter the following command:

   `volume snapshot modify-snaplock-expiry-time -volume` *`volume_name`* `-snapshot` *`snapshot_copy_name`* `-expiry-time` *`expiration_date_time`*

   The following example applies a retention period to an existing Snapshot copy:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

Copyright information

Trademark information