# Archivierung und Compliance mithilfe von SnapLock Technologie

ONTAP 9

NetApp
November 14, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/snaplock/index.html on November 14, 2026. Always check docs.netapp.com for the latest.

# Inhalt


Archivierung und Compliance mithilfe von SnapLock Technologie . . . 1
- Erfahren Sie mehr über ONTAP SnapLock . . . 1
  - Was Sie mit SnapLock machen können . . . 1
  - SnapLock Compliance- und Enterprise-Modi . . . 2
  - Unterstützte und nicht unterstützte Funktionen mit SnapLock . . . 3
  - FabricPool auf SnapLock Enterprise Aggregaten . . . 4
  - FlexGroup Volumes . . . 4
  - LUN-Unterstützung . . . 4
  - MetroCluster Unterstützung . . . 4
  - Unterstützung für die Multi-Admin-Verifizierung (MAV) . . . 5
  - Speichereffizienz . . . 5
  - Verschlüsselung . . . 5
- SnapLock konfigurieren . . . 6
  - ONTAP SnapLock Konfigurationsworkflow . . . 6
  - Initialisierung der ONTAP SnapLock Compliance Clock . . . 6
  - Ein ONTAP SnapLock Aggregat erstellen . . . 8
  - ONTAP SnapLock Volumes erstellen und einbinden . . . 10
  - Die ONTAP SnapLock Aufbewahrungszeit festlegen . . . 12
  - Ein ONTAP SnapLock-geschütztes Revisionsprotokoll erstellen . . . 17
  - ONTAP SnapLock Einstellungen überprüfen . . . 19
- WORM-Dateien verwalten . . . 20
  - WORM-Dateiverwaltung in ONTAP SnapLock . . . 20
  - Dateien mit ONTAP SnapLock auf WORM festschreiben . . . 21
  - Snapshots auf einem ONTAP SnapLock Vault-Ziel in WORM festschreiben . . . 25
  - WORM-Dateien mit ONTAP SnapMirror für die Notfallwiederherstellung spiegeln . . . 28
  - WORM-Dateien während eines Rechtsstreits mit ONTAP SnapLock Legal Hold aufbewahren . . . 32
  - WORM-Dateien mit ONTAP SnapLock löschen . . . 33
- Verschieben eines ONTAP SnapLock Volumes . . . 35
  - Ein SnapLock Sicherheitsadministratorkonto erstellen . . . 35
  - Ein SnapLock Volume verschieben . . . 36
- Einen ONTAP Snapshot zum Schutz vor Ransomware-Angriffen sperren . . . 37
  - Snapshot-Sperre beim Erstellen eines Volumes aktivieren . . . 39
  - Aktivieren der Snapshot-Sperre auf einem vorhandenen Volume . . . 39
  - Eine Richtlinie für gesperrte Snapshots erstellen und die Aufbewahrungsfrist anwenden . . . 40

# Archivierung und Compliance mithilfe von SnapLock Technologie

## Erfahren Sie mehr über ONTAP SnapLock

SnapLock ist eine leistungsstarke Compliance-Lösung für Organisationen, die WORM-Speicher verwenden, um Dateien für regulatorische und Governance-Zwecke unverändert aufzubewahren.

SnapLock hilft dabei, das Löschen, Ändern oder Umbenennen von Daten zu verhindern, um Vorschriften wie SEC 17a-4(f), HIPAA, FINRA, CFTC und DSGVO zu erfüllen. Mit SnapLock können spezielle Volumes erstellt werden, in denen Dateien gespeichert und entweder für einen festgelegten Aufbewahrungszeitraum oder unbegrenzt in einen nicht löschbaren, nicht beschreibbaren Zustand versetzt werden können. SnapLock ermöglicht diese Aufbewahrung auf Dateiebene über standardisierte offene Dateiprotokolle wie CIFS und NFS. Die unterstützten offenen Dateiprotokolle für SnapLock sind NFS (Versionen 2, 3 und 4) und CIFS (SMB 1.0, 2.0 und 3.0).

Mit SnapLock werden Dateien und Snapshots im WORM-Speicher abgelegt und Aufbewahrungsfristen für WORM-geschützte Daten festgelegt. SnapLock WORM-Speicher nutzt die NetApp Snapshot-Technologie und kann SnapMirror Replikation sowie SnapVault Backups als Basistechnologie für den Backup-Wiederherstellungsschutz von Daten nutzen. Weitere Informationen zu WORM-Speicher: "Konforme WORM-Speicherung mit NetApp SnapLock - TR-4526".

Eine Anwendung kann verwendet werden, um Dateien über NFS oder CIFS an WORM zu übergeben, oder die SnapLock Autocommit-Funktion kann genutzt werden, um Dateien automatisch an WORM zu übergeben. Eine *WORM-anhängbare Datei* kann verwendet werden, um inkrementell geschriebene Daten wie Protokollinformationen zu speichern. Weitere Informationen finden Sie unter "Den Volume-Append-Modus verwenden, um WORM-anhängbare Dateien zu erstellen".

SnapLock unterstützt Datenschutzmethoden, die die meisten Compliance-Anforderungen erfüllen sollten:

- Mit SnapLock für SnapVault lassen sich Snapshots auf sekundärem Speicher WORM-schützen. Siehe "Snapshots in WORM übernehmen".
- Mit SnapMirror können WORM-Dateien zur Notfallwiederherstellung an einen anderen geografischen Standort repliziert werden. Siehe "WORM-Dateien spiegeln".

SnapLock ist eine lizenzbasierte Funktion von ONTAP. Eine einzelne Lizenz berechtigt zur Nutzung von SnapLock im strikten Compliance-Modus, um externe Vorgaben wie SEC Rule 17a-4(f) zu erfüllen, sowie im weniger restriktiven Enterprise-Modus, um interne Vorschriften zum Schutz digitaler Assets einzuhalten. SnapLock-Lizenzen sind Bestandteil der "ONTAP One" Software-Suite.

SnapLock wird auf allen AFF und FAS Systemen sowie ONTAP Select unterstützt. SnapLock ist keine reine Softwarelösung, sondern eine integrierte Hardware- und Softwarelösung. Diese Unterscheidung ist wichtig für strenge WORM-Vorschriften wie SEC 17a-4(f), die eine integrierte Hardware- und Softwarelösung erfordern. Weitere Informationen finden sich unter "SEC-Leitfaden für Broker-Dealer zur Verwendung elektronischer Speichermedien".

### Was Sie mit SnapLock machen können

Nach der Konfiguration von SnapLock können die folgenden Aufgaben abgeschlossen werden:

- "Dateien in WORM übernehmen"
- "Snapshots für den Sekundärspeicher in WORM übernehmen"
- "WORM-Dateien für die Notfallwiederherstellung spiegeln"
- "WORM-Dateien während eines Rechtsstreits mit Legal Hold aufbewahren"
- "WORM-Dateien mit der Funktion „Privilegiertes Löschen“ entfernen"
- "Die Aufbewahrungsfrist für Dateien festlegen"
- "Ein SnapLock Volume verschieben"
- "Einen Snapshot zum Schutz vor Ransomware-Angriffen sperren"
- "Überprüfung der Nutzung von snapLock mit dem Revisionsprotokoll"
- "SnapLock APIs verwenden"

## SnapLock Compliance- und Enterprise-Modi

SnapLock Compliance- und Enterprise-Modi unterscheiden sich hauptsächlich darin, auf welcher Ebene jeder Modus WORM-Dateien schützt:

| SnapLock Modus | Schutzstufe | WORM-Dateilöschung während der Aufbewahrung |
|---|---|---|
| Konformitätsmodus | Auf der Festplattenebene | Kann nicht gelöscht werden |
| Enterprise-Modus | Auf Dateiebene | Kann vom Compliance-Administrator mithilfe eines protokollierten „privilegierten Löschvorgangs“ gelöscht werden |

Nach Ablauf der Aufbewahrungsfrist sind Sie für das Löschen aller Dateien verantwortlich, die Sie nicht mehr benötigen. Sobald eine Datei in WORM gespeichert wurde, unabhängig davon, ob im Compliance- oder Enterprise-Modus, kann sie nicht mehr geändert werden, auch nicht nach Ablauf der Aufbewahrungsfrist.

WORM-Dateien können weder während noch nach Ablauf der Aufbewahrungsfrist verschoben werden. Eine WORM-Datei kann kopiert werden, jedoch behält die Kopie ihre WORM-Eigenschaften nicht bei.

Die folgende Tabelle zeigt die Unterschiede in den von SnapLock Compliance und Enterprise Modi unterstützten Funktionen:

| Fähigkeit | SnapLock Compliance | SnapLock Enterprise |
|---|---|---|
| Dateien mit privilegiertem Löschen aktivieren und löschen | Nein | Ja |
| Festplatten neu initialisieren | Nein | Ja |
| Zerstörung von SnapLock Aggregaten und Volumes während der Aufbewahrungsfrist | Nein | Ja, mit Ausnahme des SnapLock Revisionsprotokoll-Volumes |
| Aggregate oder Volumes umbenennen | Nein | Ja |
| Nicht-NetApp-Datenträger verwenden | Nein | Nein |

| | | |
|---|---|---|
| Das SnapLock Volume für die Revisionsprotokollierung verwenden | Ja | Ja, beginnend mit ONTAP 9.5 |

## Unterstützte und nicht unterstützte Funktionen mit SnapLock

Die folgende Tabelle zeigt die Funktionen, die im SnapLock Compliance-Modus, im SnapLock Enterprise-Modus oder in beiden unterstützt werden:

| Funktion | Unterstützt mit SnapLock Compliance | Unterstützt mit SnapLock Enterprise |
|---|---|---|
| Konsistenzgruppen | Nein | Nein |
| Verschlüsselte Volumes | Ja, weitere Informationen zu Verschlüsselung und SnapLock. | Ja, weitere Informationen zu Verschlüsselung und SnapLock. |
| FabricPools auf SnapLock Aggregaten | Nein | Ja, beginnend mit ONTAP 9.8. Weitere Informationen zu FabricPool auf SnapLock Enterprise Aggregaten. |
| Flash Pool Aggregate | Ja. | Ja. |
| FlexClone | Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen. | Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen. |
| FlexGroup Volumes | Ja, beginnend mit ONTAP 9.11.1. Weitere Informationen zu FlexGroup Volumes. | Ja, beginnend mit ONTAP 9.11.1. Weitere Informationen zu FlexGroup Volumes. |
| LUNs | Nein. Weitere Informationen zu LUN-Unterstützung mit SnapLock. | Nein. Weitere Informationen zu LUN-Unterstützung mit SnapLock. |
| MetroCluster Konfigurationen | Ja, beginnend mit ONTAP 9.3. Weitere Informationen zu MetroCluster Unterstützung. | Ja, beginnend mit ONTAP 9.3. Weitere Informationen zu MetroCluster Unterstützung. |
| Multi-Admin-Verifizierung (MAV) | Ja, beginnend mit ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung. | Ja, beginnend mit ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung. |
| SAN | Nein | Nein |
| Single-File-SnapRestore | Nein | Ja |
| SnapMirror Active Sync | Nein | Nein |
| SnapRestore | Nein | Ja |
| SMTape | Nein | Nein |
| SnapMirror Synchronous | Nein | Nein |
| SSDs | Ja. | Ja. |
| Speichereffizienzfunktionen | Ja, beginnend mit ONTAP 9.9.1. Weitere Informationen zu Unterstützung der Speichereffizienz. | Ja, beginnend mit ONTAP 9.9.1. Weitere Informationen zu Unterstützung der Speichereffizienz. |

## FabricPool auf SnapLock Enterprise Aggregaten

FabricPools werden auf SnapLock Enterprise Aggregaten ab ONTAP 9.8 unterstützt. Allerdings muss Ihr Account-Team einen Antrag auf Produktabweichung stellen, in dem dokumentiert wird, dass Sie verstehen, dass FabricPool Daten, die in eine öffentliche oder private Cloud ausgelagert werden, nicht mehr durch SnapLock geschützt sind, da ein Cloud-Administrator diese Daten löschen kann.



Alle Daten, die FabricPool in eine öffentliche oder private Cloud auslagert, sind nicht mehr durch SnapLock geschützt, da diese Daten von einem Cloud-Administrator gelöscht werden können.

## FlexGroup Volumes

SnapLock unterstützt FlexGroup Volumes ab ONTAP 9.11.1; jedoch werden die folgenden Funktionen nicht unterstützt:

- Legal-Hold
- Ereignisbasierte Aufbewahrung
- SnapLock für SnapVault (unterstützt ab ONTAP 9.12.1)

Es ist außerdem auf die folgenden Verhaltensweisen zu achten:

- Die Volume Compliance Clock (VCC) eines FlexGroup Volumes wird durch die VCC der Root-Konstituente bestimmt. Alle nicht-Root-Konstituenten haben eine VCC, die eng mit der Root-VCC synchronisiert ist.
- Die SnapLock Konfigurationseigenschaften werden nur für das FlexGroup als Ganzes festgelegt. Einzelne Bestandteile können keine unterschiedlichen Konfigurationseigenschaften wie Standardaufbewahrungsdauer und Autocommit-Periode haben.

## LUN-Unterstützung

LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen Snapshots, die auf einem Nicht-SnapLock Volume erstellt wurden, auf ein SnapLock Volume zum Schutz im Rahmen einer SnapLock Vault-Beziehung übertragen werden. LUNs werden in lesen/schreiben SnapLock Volumes nicht unterstützt. Manipulationssichere Snapshots werden jedoch sowohl auf SnapMirror Quell-Volumes als auch auf Ziel-Volumes unterstützt, die LUNs enthalten.

## MetroCluster Unterstützung

SnapLock Unterstützung in MetroCluster Konfigurationen unterscheidet sich zwischen SnapLock Compliance-Modus und SnapLock Enterprise-Modus.

#### SnapLock Compliance

- Ab ONTAP 9.3 wird SnapLock Compliance auf nicht gespiegelten MetroCluster Aggregaten unterstützt.
- Ab ONTAP 9.3 wird SnapLock Compliance auf gespiegelten Aggregaten unterstützt, jedoch nur, wenn das Aggregat zum Hosten von SnapLock Revisionsprotokoll-Volumes verwendet wird.
- SVM-spezifische SnapLock Konfigurationen können mithilfe von MetroCluster auf primäre und sekundäre Standorte repliziert werden.

#### SnapLock Enterprise

- SnapLock Enterprise-Aggregate werden unterstützt.
- Ab ONTAP 9.3 werden SnapLock Enterprise-Aggregate mit privilegiertem Löschen unterstützt.

- SVM-spezifische SnapLock Konfigurationen können auf beiden Standorten mithilfe von MetroCluster repliziert werden.

**MetroCluster Konfigurationen und Konformitätsuhren**

MetroCluster Konfigurationen verwenden zwei Compliance-Uhren, die Volume Compliance Clock (VCC) und die System Compliance Clock (SCC). Die VCC und SCC stehen allen SnapLock Konfigurationen zur Verfügung. Wenn ein neues Volume auf einem Knoten erstellt wird, wird dessen VCC mit dem aktuellen Wert der SCC auf diesem Knoten initialisiert. Nach der Erstellung des Volumes wird die Aufbewahrungszeit von Volume und Dateien immer mit der VCC nachverfolgt.

Wird ein Volume an einen anderen Standort repliziert, wird auch dessen VCC repliziert. Bei einem Volume Switchover, beispielsweise von Standort A zu Standort B, wird die VCC an Standort B weiterhin aktualisiert, während die SCC an Standort A stoppt, sobald Standort A offline geht.

Sobald Standort A wieder online ist und die Volume-Rückschaltung durchgeführt wird, startet die SCC-Uhr von Standort A neu, während der VCC des Volumes weiterhin aktualisiert wird. Da der VCC unabhängig von Umschaltungs- und Rückschaltungsvorgängen kontinuierlich aktualisiert wird, hängen die Aufbewahrungszeiten der Dateien nicht von den SCC-Uhren ab und verlängern sich nicht.

## Unterstützung für die Multi-Admin-Verifizierung (MAV)

Ab ONTAP 9.13.1 kann ein Clusteradministrator die Multi-Admin-Verifizierung (MAV) explizit auf einem Cluster aktivieren, sodass für bestimmte SnapLock Operationen eine Quorum-Genehmigung erforderlich ist, bevor sie ausgeführt werden. Wenn MAV aktiviert ist, erfordern SnapLock Volume-Eigenschaften wie default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period und privileged-delete eine Quorum-Genehmigung. Weitere Informationen zu "MAV".

## Speichereffizienz

Ab ONTAP 9.9.1 unterstützt SnapLock Funktionen zur Speichereffizienz, wie Datenkompaktierung, volumenübergreifende Deduplizierung und adaptive Komprimierung für SnapLock Volumes und Aggregate. Weitere Informationen zur Speichereffizienz finden sich unter "ONTAP Speichereffizienz im Überblick".

## Verschlüsselung

ONTAP bietet sowohl software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Speichermedium umfunktioniert, zurückgegeben, verlegt oder gestohlen wird.

**Haftungsausschluss:** NetApp kann nicht garantieren, dass SnapLock-geschützte WORM-Dateien auf selbstverschlüsselnden Laufwerken oder Volumes wiederhergestellt werden können, wenn der Authentifizierungsschlüssel verloren geht oder die Anzahl fehlgeschlagener Authentifizierungsversuche das festgelegte Limit überschreitet und das Laufwerk dadurch dauerhaft gesperrt wird. Sie sind dafür verantwortlich, Authentifizierungsfehler zu vermeiden.

Verschlüsselte Volumes werden auf SnapLock Aggregaten unterstützt.

[[7-mode-transition]] == 7-Mode Transition

Sie können SnapLock Volumes von 7-Mode zu ONTAP migrieren, indem Sie die Funktion „Copy-Based Transition“ (CBT) des 7-Mode Transition Tool verwenden. Der SnapLock Modus des Ziel-Volumes, Compliance oder Enterprise, muss mit dem SnapLock Modus des Quell-Volumes übereinstimmen. Die Migration von SnapLock Volumes mit Copy-Free Transition (CFT) ist nicht möglich.

# SnapLock konfigurieren

## ONTAP SnapLock Konfigurationsworkflow

Bevor Sie SnapLock verwenden, ist es erforderlich, SnapLock zu konfigurieren, indem verschiedene Aufgaben ausgeführt werden, wie zum Beispiel "die SnapLock-Lizenz installieren" für jeden Knoten, der ein Aggregat mit einem SnapLock Volume hostet, die Initialisierung des "Compliance Clock", das Erstellen eines SnapLock Aggregats für Cluster, auf denen ONTAP Versionen vor ONTAP 9.10.1 ausgeführt werden, "Ein SnapLock Volume erstellen und einbinden" und weitere Aufgaben.

## Initialisierung der ONTAP SnapLock Compliance Clock

SnapLock verwendet die *Volume Compliance Clock*, um Manipulationen zu verhindern, die die Aufbewahrungsfrist für WORM-Dateien verändern könnten. Zunächst muss die *System ComplianceClock* auf jedem Knoten initialisiert werden, der ein SnapLock Aggregat hostet.

Ab ONTAP 9.14.1 können Sie die System Compliance Clock initialisieren oder neu initialisieren, wenn keine SnapLock-Volumes oder keine Volumes mit aktivierter Snapshot-Sperre vorhanden sind. Die Möglichkeit zur Neuinitialisierung ermöglicht es Systemadministratoren, die System Compliance Clock in Fällen zurückzusetzen, in denen sie möglicherweise falsch initialisiert wurde oder um eine Taktabweichung im System zu korrigieren. In ONTAP 9.13.1 und früheren Versionen können Sie die Compliance Clock nach der Initialisierung auf einem Node nicht erneut initialisieren.

### Bevor Sie beginnen

Um die Compliance-Uhr neu zu initialisieren:

- Alle Knoten im Cluster müssen sich im fehlerfreien Zustand befinden.
- Alle Volumes müssen online sein.
- In der Wiederherstellungswarteschlange dürfen keine Volumes vorhanden sein.
- Es dürfen keine SnapLock Volumes vorhanden sein.
- Es dürfen keine Volumes mit aktivierter Snapshot-Sperre vorhanden sein.

Allgemeine Anforderungen für die Initialisierung der Compliance Clock:

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- "Die SnapLock Lizenz muss auf dem Knoten installiert sein.".

### Über diese Aufgabe

Die Zeit auf der System-Compliance-Clock wird an die *Volume-Compliance-Clock* vererbt, wobei letztere den Aufbewahrungszeitraum für WORM-Dateien auf dem Volume steuert. Die Volume-Compliance-Clock wird automatisch initialisiert, wenn Sie ein neues SnapLock Volume erstellen.

> Die anfängliche Einstellung der System-Compliance-Uhr basiert auf der aktuellen Hardware-Systemuhr. Daher sollten Sie vor der Initialisierung der System-Compliance-Uhr auf jedem Knoten überprüfen, ob Systemzeit und Zeitzone korrekt sind. Nachdem Sie die System-Compliance-Uhr auf einem Knoten initialisiert haben, können Sie sie nicht erneut initialisieren,

wenn SnapLock-Volumes oder Volumes mit aktivierter Sperrung vorhanden sind.

**Schritte**

Die Compliance Clock kann über die ONTAP CLI initialisiert werden oder, ab ONTAP 9.12.1, über den System Manager.

**System Manager**

1. Zu **Cluster > Übersicht** navigieren.
2. Wählen Sie im Abschnitt **Knoten** die Option **SnapLock Compliance-Uhr initialisieren**.
3. Um die Spalte **Compliance Clock** anzuzeigen und zu überprüfen, ob die Compliance Clock initialisiert ist, wählen Sie im Abschnitt **Cluster > Übersicht > Knoten** die Option **Anzeigen/Ausblenden** und wählen Sie **SnapLock Compliance Clock**.

**CLI**

1. Initialisieren Sie die System-Compliance-Uhr:

   `snaplock compliance-clock initialize -node` *`node_name`*

   Der folgende Befehl initialisiert die System Compliance Clock `node1`:

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

   Weitere Informationen zu `snaplock compliance-clock initialize` finden sich in der "ONTAP-Befehlsreferenz".

2. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass die Systemuhr korrekt ist und dass Sie die Compliance-Uhr initialisieren möchten:

   ```
   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. Wiederholen Sie dieses Verfahren für jeden Knoten, der ein SnapLock Aggregat hostet.

### Compliance Clock-Resynchronisierung für ein NTP-konfiguriertes System aktivieren

Die SnapLock Compliance Clock-Synchronisierungsfunktion kann aktiviert werden, wenn ein NTP-Server konfiguriert ist.

**Bevor Sie beginnen**

- Diese Funktion ist nur auf der Stufe „Erweitert“ verfügbar.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- "Die SnapLock Lizenz muss auf dem Knoten installiert sein.".
- Diese Funktion ist nur für die Plattformen Cloud Volumes ONTAP, ONTAP Select und VSIM verfügbar.

**Über diese Aufgabe**

Wenn der SnapLock secure clock daemon eine Abweichung über dem Schwellenwert feststellt, verwendet ONTAP die Systemzeit, um sowohl die System- als auch die Volume Compliance Clocks zurückzusetzen. Ein Zeitraum von 24 Stunden ist als Schwellenwert für die Abweichung festgelegt. Die System Compliance Clock synchronisiert sich nur mit der Systemzeit, wenn die Abweichung mehr als einen Tag alt ist.

Der SnapLock Secure Clock Daemon erkennt eine Zeitabweichung und ändert die Compliance Clock auf die Systemzeit. Jeder Versuch, die Systemzeit zu ändern, um die Compliance Clock zur Synchronisierung mit der Systemzeit zu zwingen, schlägt fehl, da die Compliance Clock nur dann mit der Systemzeit synchronisiert wird, wenn die Systemzeit mit der NTP-Zeit synchronisiert ist.

**Schritte**

1. Die Funktion zur Synchronisierung der SnapLock Compliance Clock wird aktiviert, wenn ein NTP-Server konfiguriert ist:

   `snaplock compliance-clock ntp`

   Der folgende Befehl aktiviert die System-Compliance-Clock-Synchronisierungsfunktion:

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

   Weitere Informationen zu `snaplock compliance-clock ntp modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Bestätigen Sie bei entsprechender Aufforderung, dass die konfigurierten NTP-Server vertrauenswürdig sind und der Kommunikationskanal sicher ist, damit die Funktion aktiviert werden kann:
3. Überprüfen, ob die Funktion aktiviert ist:

   `snaplock compliance-clock ntp show`

   Der folgende Befehl prüft, ob die Systemfunktion zur Synchronisierung der Compliance Clock aktiviert ist:

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

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

   Weitere Informationen zu `snaplock compliance-clock ntp show` finden sich in der "ONTAP-Befehlsreferenz".

## Ein ONTAP SnapLock Aggregat erstellen

Die `-snaplock-type`Option „volume“ wird verwendet, um den Typ des SnapLock Volumes als Compliance oder Enterprise festzulegen. Für Versionen vor ONTAP 9.10.1 muss ein

separates SnapLock Aggregat erstellt werden. Ab ONTAP 9.10.1 können SnapLock- und Nicht-SnapLock-Volumes auf demselben Aggregate existieren, daher ist es nicht mehr erforderlich, ein separates SnapLock-Aggregate zu erstellen, wenn ONTAP 9.10.1 verwendet wird.

**Bevor Sie beginnen**

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die SnapLock "Lizenz muss installiert sein" auf dem Node. Diese Lizenz ist in "ONTAP One" enthalten.
- "Die Compliance-Uhr auf dem Knoten muss initialisiert sein.".
- Wenn Sie die Festplatten als “root”, “data1” und “data2” partitioniert haben, ist sicherzustellen, dass Ersatzfestplatten verfügbar sind.

**Upgrade-Überlegungen**

Beim Upgrade auf ONTAP 9.10.1 werden bestehende SnapLock und nicht-SnapLock Aggregate so aktualisiert, dass sowohl SnapLock als auch nicht-SnapLock Volumes unterstützt werden. Die bestehenden SnapLock Volume-Attribute werden jedoch nicht automatisch aktualisiert. Beispielsweise bleiben die Felder data-compaction, cross-volume-dedupe und cross-volume-background-dedupe unverändert. Neue SnapLock Volumes, die auf bestehenden Aggregaten erstellt werden, haben dieselben Standardwerte wie nicht-SnapLock Volumes, und die Standardwerte für neue Volumes und Aggregate sind plattformabhängig.

**Überlegungen zum Zurücksetzen**

Falls eine Rückkehr zu einer ONTAP Version vor 9.10.1 erforderlich ist, müssen alle SnapLock Compliance, SnapLock Enterprise und SnapLock Volumes auf eigene SnapLock Aggregate verschoben werden.

**Über diese Aufgabe**

- Compliance-Aggregate können mit der SyncMirror Option nicht erstellt werden.
- Gespiegelte Compliance Aggregate in einer MetroCluster Konfiguration können nur erstellt werden, wenn das Aggregat zum Hosten von SnapLock Revisionsprotokoll-Volumes verwendet wird.

> In einer MetroCluster Konfiguration wird SnapLock Enterprise sowohl auf gespiegelten als auch auf ungespiegelten Aggregaten unterstützt. SnapLock Compliance wird nur auf ungespiegelten Aggregaten unterstützt.

**Schritte**

1. Ein SnapLock Aggregat erstellen:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

Der folgende Befehl erstellt ein SnapLock `Compliance` Aggregat mit dem Namen `aggr1` mit drei Festplatten auf `node1`:

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

Weitere Informationen zu `storage aggregate create` finden sich in der "ONTAP-Befehlsreferenz".

## ONTAP SnapLock Volumes erstellen und einbinden

Sie müssen ein SnapLock Volume für die Dateien oder Snapshots erstellen, die Sie in den WORM-Status übernehmen möchten. Ab ONTAP 9.10.1 wird jedes Volume, das Sie erstellen, unabhängig vom Aggregattyp, standardmäßig als Nicht-SnapLock Volume erstellt. Die `-snaplock-type` Option muss verwendet werden, um explizit ein SnapLock Volume zu erstellen, indem entweder Compliance oder Enterprise als SnapLock Typ angegeben wird. Standardmäßig ist der SnapLock Typ auf `non-snaplock` eingestellt.

**Bevor Sie beginnen**

- Das SnapLock Aggregat muss online sein.
- Sie sollten "Es sollte überprüft werden, ob eine SnapLock-Lizenz installiert ist.". Wenn auf dem Knoten keine SnapLock-Lizenz installiert ist, muss "installieren" sie installiert werden. Diese Lizenz ist mit "ONTAP One" enthalten. Vor ONTAP One war die SnapLock-Lizenz im Security and Compliance Bundle enthalten. Das Security and Compliance Bundle wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl es derzeit nicht erforderlich ist, können bestehende Kunden sich dafür entscheiden, "Upgrade auf ONTAP One".
- "Die Compliance-Uhr auf dem Knoten muss initialisiert sein.".

**Über diese Aufgabe**

Mit den entsprechenden SnapLock-Berechtigungen ist es möglich, ein Enterprise Volume jederzeit zu zerstören oder umzubenennen. Ein Compliance Volume kann erst zerstört werden, nachdem die Aufbewahrungsfrist abgelaufen ist. Ein Compliance Volume kann niemals umbenannt werden.

Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen. Das geklonte Volume hat denselben SnapLock Typ wie das übergeordnete Volume.

> LUNs werden in SnapLock Volumes nicht unterstützt. LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen Snapshots, die auf einem Nicht-SnapLock Volume erstellt wurden, auf ein SnapLock Volume zum Schutz im Rahmen einer SnapLock Vault-Beziehung übertragen werden. LUNs werden in lesen/schreiben SnapLock Volumes nicht unterstützt. Manipulationssichere Snapshots werden jedoch sowohl auf SnapMirror Quell-Volumes als auch auf Ziel-Volumes unterstützt, die LUNs enthalten.

Diese Aufgabe kann mit ONTAP System Manager oder der ONTAP CLI ausgeführt werden.

**System Manager**

Ab ONTAP 9.12.1 ist es möglich, mit System Manager ein SnapLock Volume zu erstellen.

**Schritte**

1. Zu **Speicher > Volumes** navigieren und auf **Hinzufügen** klicken.
2. Im Fenster **Volume hinzufügen** auf **Weitere Optionen** klicken.
3. Geben Sie die neuen Volume-Informationen ein, einschließlich Name und Größe des Volumes.
4. **SnapLock aktivieren** auswählen und den SnapLock Typ, entweder Compliance oder Enterprise, wählen.
5. Im Abschnitt **Dateien automatisch übernehmen** ist **Geändert** auszuwählen und die Zeitspanne anzugeben, die eine Datei unverändert bleiben soll, bevor sie automatisch übernommen wird. Der Mindestwert beträgt 5 Minuten, der Höchstwert 10 Jahre.

6. Im Abschnitt **Datenaufbewahrung** sind die minimale und maximale Aufbewahrungsdauer auszuwählen.
7. Die Standardaufbewahrungsfrist auswählen.
8. Auf **Speichern** klicken.
9. Das neue Volume auf der Seite **Volumes** auswählen, um die SnapLock-Einstellungen zu überprüfen.

**CLI**

1. Ein SnapLock Volume erstellen:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz". Die folgenden Optionen sind für SnapLock Volumes nicht verfügbar: `-nvfail`, `-atime-update`, `-is -autobalance-eligible`, `-space-mgmt-try-first`, und `vmalign`.

Der folgende Befehl erstellt ein SnapLock `Compliance` Volume mit dem Namen `vol1` auf `aggr1` auf `vs1`:

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

### Ein SnapLock Volume einbinden

Ein SnapLock Volume kann an einem Verbindungspfad im SVM-Namespace für den Zugriff durch NAS-Clients eingebunden werden.

**Bevor Sie beginnen**

Das SnapLock Volume muss online sein.

**Über diese Aufgabe**

- Ein SnapLock Volume kann nur unter dem Stammverzeichnis der SVM eingebunden werden.
- Ein normales Volume kann nicht unter einem SnapLock Volume eingebunden werden.

**Schritte**

1. Ein SnapLock Volume einbinden:

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

Weitere Informationen zu `volume mount` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl bindet ein SnapLock Volume mit dem Namen `vol1` an den Verbindungspfad `/sales` im `vs1` Namespace ein:

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

## Die ONTAP SnapLock Aufbewahrungszeit festlegen

Sie können die Aufbewahrungsdauer für eine Datei explizit festlegen oder die Standardaufbewahrungsdauer für das Volume verwenden, um die Aufbewahrungsdauer abzuleiten. Sofern Sie die Aufbewahrungsdauer nicht explizit festlegen, verwendet SnapLock die Standardaufbewahrungsdauer zur Berechnung der Aufbewahrungsdauer. Die Dateiaufbewahrung kann auch nach einem Ereignis festgelegt werden.

#### Informationen zu Aufbewahrungsfrist und Aufbewahrungszeit

Die Aufbewahrungsfrist für eine WORM-Datei gibt an, wie lange die Datei nach dem Übergang in den WORM-Zustand aufbewahrt werden muss. Die Aufbewahrungsdauer einer WORM-Datei ist der Zeitpunkt, nach dem die Datei nicht mehr aufbewahrt werden muss. Eine Aufbewahrungsfrist von 20 Jahren für eine Datei, die am 10. November 2020 um 6:00 Uhr in den WORM-Zustand versetzt wurde, ergibt eine Aufbewahrungsdauer bis zum 10. November 2040 um 6:00 Uhr.




Ab ONTAP 9.10.1 kann eine Aufbewahrungsfrist bis zum 26. Oktober 3058 und eine Aufbewahrungsdauer von bis zu 100 Jahren festgelegt werden. Bei einer Verlängerung der Aufbewahrungsfristen werden ältere Richtlinien automatisch konvertiert. In ONTAP 9.9.1 und früheren Versionen beträgt die maximal unterstützte Aufbewahrungsfrist, sofern die Standardaufbewahrungsdauer nicht auf unbegrenzt gesetzt ist, den 19. Januar 2071 (GMT).

#### Wichtige Überlegungen zur Replikation

Wenn eine SnapMirror Beziehung mit einem SnapLock Quellvolume unter Verwendung eines Aufbewahrungsdatums nach dem 19. Januar 2071 (GMT) hergestellt wird, muss das Ziel-Cluster ONTAP 9.10.1 oder höher ausführen, andernfalls schlägt die SnapMirror Übertragung fehl.

#### Wichtige Überlegungen zur Rückführung

ONTAP verhindert, dass ein Cluster von ONTAP 9.10.1 auf eine frühere ONTAP Version zurückgesetzt werden kann, wenn Dateien mit einer Aufbewahrungsfrist nach „19. Januar 2071 8:44:07 Uhr“ vorhanden sind.

#### Aufbewahrungsfristen im Überblick

Ein SnapLock Compliance oder Enterprise Volume hat vier Aufbewahrungsfristen:

- Mindestaufbewahrungsdauer (`min`), mit einem Standardwert von 0
- Maximale Aufbewahrungsdauer (`max`), mit einem Standardwert von 30 Jahren
- Standardmäßige Aufbewahrungsfrist, mit einem Standardwert von `min` für sowohl den Compliance-Modus als auch den Enterprise-Modus ab ONTAP 9.10.1. In ONTAP Versionen vor ONTAP 9.10.1 hängt die standardmäßige Aufbewahrungsfrist vom Modus ab:
  - Im Compliance-Modus ist der Standardwert gleich `max`.

- Im Enterprise-Modus ist der Standardwert gleich `min`.

- Nicht spezifizierte Aufbewahrungsfrist.

> In ONTAP-Versionen vor ONTAP 9.10.1, wenn die Aufbewahrungsdauer nicht explizit festgelegt wurde, bevor eine Datei im Compliance-Modus in den WORM-Status überführt wird, und die Standardeinstellungen nicht geändert wurden, wird die Datei 30 Jahre lang aufbewahrt. Diese Änderung *kann* nicht rückgängig gemacht werden. Ebenso wird in ONTAP 9.10.1 und später, wenn die Aufbewahrungsdauer nicht explizit festgelegt wurde, bevor eine Datei im Enterprise-Modus in den WORM-Status überführt wird, und die Standardeinstellungen nicht geändert wurden, die Datei 0 Jahre lang aufbewahrt, also de facto gar nicht.

Ab ONTAP 9.8 kann die Aufbewahrungsdauer von Dateien in einem Volume auf `unspecified`unspezifiziert gesetzt werden, sodass die Datei bis zur Festlegung einer absoluten Aufbewahrungszeit aufbewahrt bleibt. Eine Datei mit absoluter Aufbewahrungszeit kann auf unspezifizierte Aufbewahrungsdauer und wieder zurück auf absolute Aufbewahrungszeit gesetzt werden, solange die neue absolute Aufbewahrungszeit später liegt als die zuvor festgelegte absolute Zeit.

Ab ONTAP 9.12.1 wird für WORM-Dateien mit der Aufbewahrungsdauer, die auf `unspecified` festgelegt ist, garantiert, dass die Aufbewahrungsdauer mindestens der für das SnapLock Volume konfigurierten Mindestaufbewahrungsdauer entspricht. Wenn die Aufbewahrungsdauer einer Datei von `unspecified` auf eine absolute Aufbewahrungszeit geändert wird, muss die neu angegebene Aufbewahrungszeit größer sein als die bereits für die Datei festgelegte Mindestaufbewahrungsdauer.

### Standardaufbewahrungsdauer festlegen

Sie können den `volume snaplock modify`Befehl verwenden, um die Standardaufbewahrungsdauer für Dateien auf einem SnapLock Volume festzulegen.

#### Bevor Sie beginnen

Das SnapLock Volume muss online sein.

#### Über diese Aufgabe

Die folgende Tabelle zeigt die möglichen Werte für die Option „Standardaufbewahrungsdauer“:

> Die Standardaufbewahrungsfrist muss größer oder gleich (>=) der minimalen Aufbewahrungsfrist und kleiner oder gleich (<=) der maximalen Aufbewahrungsfrist sein.

| Wert | Einheit | Hinweise |
|---|---|---|
| 0 - 65535 | Sekunden | |
| 0 - 60 | Minuten | |
| 0 - 24 | Stunden | |
| 0 - 36500 | Tage | |
| 0 - 1200 | Monate | |
| 0 - 100 | Jahre | Ab ONTAP 9.10.1. Bei früheren ONTAP Versionen liegt der Wert zwischen 0 und 70. |

| Wert | Einheit | Hinweise |
|---|---|---|
| max | - | Die maximale Aufbewahrungsfrist verwenden. |
| min | - | Die Mindestaufbewahrungsfrist verwenden. |
| unendlich | - | Die Dateien werden dauerhaft aufbewahrt. |
| nicht spezifiziert | - | Die Dateien bleiben erhalten, bis eine absolute Aufbewahrungsfrist festgelegt ist. |

Die Werte und Bereiche für die maximale und minimale Aufbewahrungsfrist sind identisch, mit Ausnahme von `max` und `min`, die nicht anwendbar sind. Weitere Informationen zu dieser Aufgabe finden sich unter "Übersicht zur Aufbewahrungszeit".

Sie können den `volume snaplock show` Befehl verwenden, um die Einstellungen für die Aufbewahrungsfrist des Volumes anzuzeigen. Weitere Informationen zu `volume snaplock show` finden sich in der "ONTAP-Befehlsreferenz".

Sobald eine Datei in den WORM-Status übertragen wurde, kann die Aufbewahrungsfrist verlängert, aber nicht verkürzt werden.

**Schritte**

1. Die Standardaufbewahrungsdauer für Dateien auf einem SnapLock Volume festlegen:

   **`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`***

   Weitere Informationen zu `volume snaplock modify` finden sich in der "ONTAP-Befehlsreferenz".

   Die folgenden Beispiele setzen voraus, dass die Mindest- und Höchstaufbewahrungsfristen zuvor nicht geändert wurden.

   Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Compliance oder Enterprise Volume auf 20 Tage fest:

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

   Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Compliance Volume auf 70 Jahre fest:

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

   Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Enterprise Volume auf 10 Jahre fest:

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

Die folgenden Befehle legen die Standardaufbewahrungsfrist für ein Enterprise-Volume auf 10 Tage fest:

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

Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Compliance Volume auf unendlich fest:

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

### Die Aufbewahrungszeit für eine Datei explizit festlegen

Sie können die Aufbewahrungsdauer einer Datei explizit festlegen, indem Sie deren letzten Zugriffszeitpunkt ändern. Sie können jeden geeigneten Befehl oder jedes geeignete Programm über NFS oder CIFS verwenden, um den letzten Zugriffszeitpunkt zu ändern.

#### Über diese Aufgabe

Nachdem eine Datei in WORM übertragen wurde, kann die Aufbewahrungszeit verlängert, aber nicht verkürzt werden. Die Aufbewahrungszeit wird im `atime` Feld für die Datei gespeichert.

> Die Aufbewahrungszeit einer Datei kann nicht explizit auf `infinite` gesetzt werden. Dieser Wert ist nur verfügbar, wenn die Aufbewahrungszeit anhand der Standardaufbewahrungsdauer berechnet wird.

#### Schritte

1. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um die letzte Zugriffszeit für die Datei zu ändern, deren Aufbewahrungszeit Sie festlegen möchten.

   In einer UNIX-Shell kann mit dem folgenden Befehl eine Aufbewahrungszeit von 21. November 2020, 6:00 Uhr, für eine Datei mit dem Namen `document.txt` festgelegt werden:

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

   > Es kann jeder geeignete Befehl oder jedes geeignete Programm verwendet werden, um die letzte Zugriffszeit in Windows zu ändern.

### Die Aufbewahrungsfrist für Dateien nach einem Ereignis festlegen

Ab ONTAP 9.3 kann mit der Funktion SnapLock *Event Based Retention (EBR)* festgelegt werden, wie lange eine Datei nach dem Eintreten eines Ereignisses aufbewahrt wird.

**Bevor Sie beginnen**

- Um diese Aufgabe auszuführen, sind SnapLock Administratorrechte erforderlich.

  "Ein SnapLock Administratorkonto erstellen"

- Eine Anmeldung über eine sichere Verbindung (SSH, Konsole oder ZAPI) muss erfolgt sein.

**Über diese Aufgabe**

Die *Ereignisaufbewahrungsrichtlinie* definiert die Aufbewahrungsdauer der Datei nach dem Eintreten des Ereignisses. Die Richtlinie kann auf eine einzelne Datei oder alle Dateien in einem Verzeichnis angewendet werden.

- Wenn es sich bei einer Datei nicht um eine WORM-Datei handelt, wird sie für die in der Richtlinie festgelegte Aufbewahrungsdauer in den WORM-Status übernommen.
- Wenn es sich bei einer Datei um eine WORM-Datei oder eine WORM-anhängbare Datei handelt, wird ihre Aufbewahrungsfrist um die in der Richtlinie festgelegte Aufbewahrungsfrist verlängert.

Es kann ein Volume im Compliance-Modus oder im Enterprise-Modus verwendet werden.

EBR-Richtlinien können nicht auf Dateien angewendet werden, die unter einer Legal Hold stehen.

Für fortgeschrittene Anwendungen siehe "Konforme WORM-Speicherung mit NetApp SnapLock".

| ***Verwendung von EBR zur Verlängerung der Aufbewahrungsfrist bereits vorhandener WORM-Dateien*** |
| --- |
| EBR ist praktisch, wenn die Aufbewahrungsfrist bereits vorhandener WORM-Dateien verlängert werden soll. Beispielsweise kann es eine Unternehmensrichtlinie sein, die W-4-Formulare von Mitarbeitern drei Jahre lang in unveränderter Form aufzubewahren, nachdem der Mitarbeiter eine Lohnsteuerabzugsoption geändert hat. Eine andere Unternehmensrichtlinie kann verlangen, dass die W-4-Formulare fünf Jahre nach Beendigung des Arbeitsverhältnisses aufbewahrt werden.<br><br>In diesem Fall könnte eine EBR-Richtlinie mit einer Aufbewahrungsfrist von fünf Jahren erstellt werden. Nach Beendigung des Arbeitsverhältnisses (dem „`event`“) wird die EBR-Richtlinie auf den W-4-Datensatz des Mitarbeiters angewendet, wodurch sich dessen Aufbewahrungsfrist verlängert. Das ist in der Regel einfacher als die manuelle Verlängerung der Aufbewahrungsfrist, insbesondere wenn eine große Anzahl von Dateien betroffen ist. |

**Schritte**

1. EBR-Richtlinie erstellen:

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

   Der folgende Befehl erstellt die EBR-Richtlinie `employee_exit` auf `vs1` mit einer Aufbewahrungsfrist von zehn Jahren:

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

2. Eine EBR-Richtlinie anwenden:

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

Der folgende Befehl wendet die EBR-Richtlinie `employee_exit` auf `vs1` alle Dateien im Verzeichnis `d1` an:

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

**Verwandte Informationen**

- "snaplock event-retention policy create"
- "snaplock event-retention apply"

## Ein ONTAP SnapLock-geschütztes Revisionsprotokoll erstellen

Bei Verwendung von ONTAP 9.9.1 oder älter ist zunächst ein SnapLock Aggregat zu erstellen und anschließend ein SnapLock-geschütztes Revisionsprotokoll, bevor ein privilegierter Löschvorgang oder eine SnapLock Volume-Verschiebung durchgeführt wird. Das Revisionsprotokoll zeichnet die Erstellung und Löschung von SnapLock Administratorkonten, Änderungen am Protokollvolume, ob privilegierter Löschvorgang aktiviert ist, privilegierte Löschvorgänge sowie SnapLock Volume-Verschiebungen auf.

Ab ONTAP 9.10.1 wird kein SnapLock Aggregat mehr erstellt. Die Option -snaplock-type muss verwendet werden, "explizit ein SnapLock Volume erstellen" indem entweder Compliance oder Enterprise als SnapLock Typ angegeben wird.

**Bevor Sie beginnen**

Wenn Sie ONTAP 9.9.1 oder eine frühere Version verwenden, ist die Rolle als Cluster-Administrator erforderlich, um ein SnapLock Aggregat zu erstellen.

**Über diese Aufgabe**

Ein Revisionsprotokoll kann erst nach Ablauf der Aufbewahrungsfrist gelöscht werden. Ein Revisionsprotokoll kann auch nach Ablauf der Aufbewahrungsfrist nicht mehr geändert werden. Dies gilt sowohl für den SnapLock Compliance- als auch für den Enterprise-Modus.

> In ONTAP 9.4 und früher kann ein SnapLock Enterprise Volume nicht für die Revisionsprotokollierung verwendet werden. Es muss ein SnapLock Compliance Volume verwendet werden. In ONTAP 9.5 und später kann entweder ein SnapLock Enterprise Volume oder ein SnapLock Compliance Volume für die Revisionsprotokollierung verwendet werden. In allen Fällen muss das Revisionsprotokoll-Volume am Verbindungspfad `/snaplock_audit_log` eingebunden sein. Kein anderes Volume kann diesen Verbindungspfad verwenden.

Die SnapLock Revisionsprotokolle befinden sich im `/snaplock_log` Verzeichnis unter dem Stammverzeichnis des Revisionsprotokoll-Volumes, in Unterverzeichnissen mit den Namen `privdel_log` (privilegierte Löschvorgänge) und `system_log` (alles andere). Die Dateinamen der Revisionsprotokolle enthalten den Zeitstempel des ersten protokollierten Vorgangs, was die Suche nach Einträgen anhand des ungefähren Ausführungszeitpunkts der Vorgänge erleichtert.

- Mit dem `snaplock log file show` Befehl lassen sich die Protokolldateien auf dem Revisionsprotokoll Volume anzeigen.
- Der `snaplock log file archive` Befehl kann verwendet werden, um die aktuelle Protokolldatei zu archivieren und eine neue zu erstellen, was in Fällen nützlich ist, in denen Revisionsprotokollinformationen in einer separaten Datei aufgezeichnet werden müssen.

Weitere Informationen zu `snaplock log file show` und `snaplock log file archive` finden sich in der "ONTAP-Befehlsreferenz".

Ein Datensicherungsvolume kann nicht als SnapLock Revisionsprotokollvolume verwendet werden.

**Schritte**

1. Ein SnapLock Aggregat erstellen.

   Ein SnapLock Aggregat erstellen

2. Erstellen Sie auf der SVM, die für die Revisionsprotokollierung konfiguriert werden soll, ein SnapLock Volume.

   Ein SnapLock Volume erstellen

3. Die SVM für die Revisionsprotokollierung konfigurieren:

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

   Die standardmäßige Mindestaufbewahrungsdauer für Revisionsprotokoll-Dateien beträgt sechs Monate. Ist die Aufbewahrungsdauer einer betroffenen Datei länger als die Aufbewahrungsdauer des Revisionsprotokolls, übernimmt die Aufbewahrungsdauer des Protokolls die Aufbewahrungsdauer der Datei. Wenn die Aufbewahrungsdauer einer mit privilegiertem Löschen entfernten Datei beispielsweise zehn Monate beträgt und die Aufbewahrungsdauer des Revisionsprotokolls acht Monate beträgt, wird die Aufbewahrungsdauer des Protokolls auf zehn Monate verlängert. Weitere Informationen zur Aufbewahrungszeit und zur standardmäßigen Aufbewahrungsdauer finden sich unter "Aufbewahrungszeit festlegen".

   Der folgende Befehl konfiguriert `SVM1` die Protokollierung mithilfe des SnapLock Volumes `logVol`. Das Revisionsprotokoll hat eine maximale Größe von 20 GB und wird acht Monate lang aufbewahrt.

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

   Weitere Informationen zu `snaplock log create` finden sich in der "ONTAP-Befehlsreferenz".

4. Auf der SVM, die für die Protokollierung konfiguriert wurde, das SnapLock-Volume am Verbindungspfad `/snaplock_audit_log` einbinden.

   Ein SnapLock Volume einbinden

## ONTAP SnapLock Einstellungen überprüfen

Sie können die `volume file fingerprint start` und `volume file fingerprint dump` Befehle verwenden, um wichtige Informationen über Dateien und Volumes anzuzeigen, einschließlich des Dateityps (regulär, WORM oder WORM-anhängbar), des Ablaufdatums des Volumes und so weiter.

**Schritte**

1. Dateifingerabdruck generieren:

   `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.
   ```

   Der Befehl generiert eine Sitzungs-ID, die Sie als Eingabe für den `volume file fingerprint dump` Befehl verwenden können.

   > Sie können den `volume file fingerprint show` Befehl mit der Sitzungs-ID verwenden, um den Fortschritt des Fingerabdruckvorgangs zu überwachen. Es sollte sichergestellt sein, dass der Vorgang abgeschlossen ist, bevor versucht wird, den Fingerabdruck anzuzeigen.

2. Der Fingerabdruck der Datei wird angezeigt:

   `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
```

# WORM-Dateien verwalten

## WORM-Dateiverwaltung in ONTAP SnapLock

Sie können WORM-Dateien auf folgende Weise verwalten:

- "Dateien in WORM übernehmen"
- "Snapshots auf einem WORM-Tresor-Ziel festschreiben"
- "WORM-Dateien für die Notfallwiederherstellung spiegeln"

- "WORM-Dateien während des Rechtsstreits aufbewahren"
- "WORM-Dateien löschen"

## Dateien mit ONTAP SnapLock auf WORM festschreiben

Sie können Dateien entweder manuell oder automatisch auf WORM (Write Once, Read Many) festschreiben. Es können auch WORM-anhängbare Dateien erstellt werden.

### Dateien manuell an WORM übergeben

Sie übertragen eine Datei manuell an WORM, indem Sie die Datei schreibgeschützt machen. Sie können über NFS oder CIFS jeden geeigneten Befehl oder jedes geeignete Programm verwenden, um das Lese-/Schreibattribut einer Datei auf schreibgeschützt zu ändern. Eine manuelle Übertragung von Dateien kann gewählt werden, wenn sichergestellt werden soll, dass eine Anwendung das Schreiben in eine Datei abgeschlossen hat, damit die Datei nicht vorzeitig übertragen wird, oder wenn aufgrund einer hohen Anzahl von Volumes Skalierungsprobleme beim Autocommit-Scanner bestehen.

#### Bevor Sie beginnen

- Die Datei, die Sie übertragen möchten, muss sich auf einem SnapLock Volume befinden.
- Die Datei muss beschreibbar sein.

#### Über diese Aufgabe

Die ComplianceClock-Zeit wird beim Ausführen des Befehls oder Programms in das `ctime` Feld der Datei geschrieben. Die ComplianceClock-Zeit bestimmt, wann die Aufbewahrungsfrist für die Datei erreicht ist.

#### Schritte

1. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um das Lese-/Schreibattribut einer Datei in schreibgeschützt zu ändern.

   In einer UNIX-Shell wird mit folgendem Befehl eine Datei mit dem Namen `document.txt` schreibgeschützt erstellt:

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

   In einer Windows-Shell wird mit dem folgenden Befehl eine Datei mit dem Namen `document.txt` schreibgeschützt erstellt:

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

### Dateien automatisch an WORM übergeben

Die SnapLock Autocommit-Funktion ermöglicht das automatische Übertragen von Dateien in den WORM-Status. Die Autocommit-Funktion überträgt eine Datei in den WORM-Status auf einem SnapLock Volume, wenn sie sich während der Autocommit-Periode nicht geändert hat. Die Autocommit-Funktion ist standardmäßig deaktiviert.

#### Bevor Sie beginnen

- Die Dateien, die Sie automatisch übertragen möchten, müssen sich auf einem SnapLock Volume befinden.

- Das SnapLock Volume muss online sein.
- Das SnapLock Volume muss ein Lese-/Schreib-Volume sein.

> Die SnapLock Autocommit-Funktion durchsucht alle Dateien im Volume und committet eine Datei, wenn sie die Autocommit-Anforderungen erfüllt. Zwischen dem Zeitpunkt, an dem die Datei für Autocommit bereit ist, und dem tatsächlichen Commit durch den SnapLock Autocommit-Scanner kann ein Zeitintervall liegen. Die Datei ist jedoch bereits ab dem Zeitpunkt, an dem sie für Autocommit geeignet ist, vor Änderungen und Löschung durch das Dateisystem geschützt.

**Über diese Aufgabe**

Die *Autocommit-Periode* gibt an, wie lange Dateien unverändert bleiben müssen, bevor sie automatisch übernommen werden. Wird eine Datei vor Ablauf der Autocommit-Periode geändert, beginnt die Autocommit-Periode für diese Datei von neuem.

Die folgende Tabelle zeigt die möglichen Werte für den Autocommit-Zeitraum:

| Wert | Einheit | Hinweise |
|---|---|---|
| keine | - | Die Standardeinstellung. |
| 5 - 5256000 | Minuten | - |
| 1 - 87600 | Stunden | - |
| 1 - 3650 | Tage | - |
| 1 - 120 | Monate | - |
| 1 - 10 | Jahre | - |

> Der Mindestwert beträgt 5 Minuten, der Höchstwert 10 Jahre.

**Schritte**

1. Automatisches Übertragen von Dateien auf einem SnapLock Volume auf WORM:

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

   Weitere Informationen zu `volume snaplock modify` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl speichert die Dateien auf dem Volume `vol1` von SVM vs1 automatisch, sofern die Dateien 5 Stunden lang unverändert bleiben:

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

### Eine WORM-anhängbare Datei erstellen

Eine WORM-anhängbare Datei speichert inkrementell geschriebene Daten, wie Protokolleinträge. Es kann jeder geeignete Befehl oder jedes geeignete Programm verwendet werden, um eine WORM-anhängbare Datei zu erstellen, oder die SnapLock *Volume-Append-Modus*-Funktion kann genutzt werden, um standardmäßig WORM-anhängbare Dateien zu erstellen.

### Einen Befehl oder ein Programm verwenden, um eine WORM-anhängbare Datei zu erstellen

Sie können über NFS oder CIFS jeden geeigneten Befehl oder jedes geeignete Programm verwenden, um eine WORM-anhängbare Datei zu erstellen. Eine WORM-anhängbare Datei speichert inkrementell geschriebene Daten, wie Protokolleinträge. Daten werden in 256-KB-Blöcken an die Datei angehängt. Sobald ein Block geschrieben wurde, wird der vorherige Block WORM-geschützt. Die Datei kann erst gelöscht werden, wenn die Aufbewahrungsfrist abgelaufen ist.

#### Bevor Sie beginnen

Die WORM-anhängbare Datei muss sich auf einem SnapLock Volume befinden.

#### Über diese Aufgabe

Daten müssen nicht sequenziell in den aktiven 256-KB-Block geschrieben werden. Wenn Daten in Byte n×256KB+1 der Datei geschrieben werden, wird das vorherige 256-KB-Segment WORM-geschützt.

Jegliche ungeordneten Schreibvorgänge, die über den aktuell aktiven 256 KB Chunk hinausgehen, führen dazu, dass der aktive 256 KB Chunk auf den letzten Offset zurückgesetzt wird und Schreibvorgänge auf ältere Offsets mit einem „Read Only File System (ROFS)“-Fehler fehlschlagen. Die Schreib-Offsets sind von der Client-Anwendung abhängig. Ein Client, der die WORM Append File Write Semantik nicht einhält, kann zu einem fehlerhaften Abschluss der Schreibinhalte führen. Es empfiehlt sich, entweder sicherzustellen, dass der Client die Offset-Beschränkungen für ungeordnete Schreibvorgänge einhält, oder synchrones Schreiben zu gewährleisten, indem das Dateisystem im synchronen Modus eingebunden wird.

#### Schritte

1. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um eine Datei mit null Länge und der gewünschten Aufbewahrungszeit zu erstellen.

   In einer UNIX-Shell kann mit dem folgenden Befehl für eine leere Datei mit dem Namen `document.txt` eine Aufbewahrungszeit bis zum 21. November 2020, 6:00 Uhr, festgelegt werden:

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

2. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um das Lese-/Schreibattribut der Datei in schreibgeschützt zu ändern.

   In einer UNIX-Shell wird mit folgendem Befehl eine Datei mit dem Namen `document.txt` schreibgeschützt erstellt:

   ```
   chmod 444 document.txt
   ```

3. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um das Lese-/Schreibattribut der Datei wieder auf beschreibbar zu ändern.

   Dieser Schritt stellt kein Compliance-Risiko dar, da sich keine Daten in der Datei befinden.

   In einer UNIX-Shell kann mit folgendem Befehl eine Datei mit dem Namen `document.txt` beschreibbar gemacht werden:

```
chmod 777 document.txt
```

4. Ein geeigneter Befehl oder ein geeignetes Programm kann verwendet werden, um mit dem Schreiben von Daten in die Datei zu beginnen.

   In einer UNIX-Shell kann mit dem folgenden Befehl Daten auf `document.txt` geschrieben werden:

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

   Die Dateiberechtigungen werden wieder auf schreibgeschützt gesetzt, wenn kein weiteres Anhängen von Daten an die Datei erforderlich ist.

**Den Volume-Append-Modus verwenden, um WORM-anhängbare Dateien zu erstellen**

Ab ONTAP 9.3 kann die SnapLock Volume Append Mode (VAM)-Funktion verwendet werden, um standardmäßig WORM-anhängbare Dateien zu erstellen. Eine WORM-anhängbare Datei speichert inkrementell geschriebene Daten, wie Protokolleinträge. Daten werden in 256-KB-Blöcken an die Datei angehängt. Sobald ein Block geschrieben wurde, wird der vorherige Block WORM-geschützt. Die Datei kann erst gelöscht werden, wenn die Aufbewahrungsfrist abgelaufen ist.

**Bevor Sie beginnen**

- Die WORM-anhängbare Datei muss sich auf einem SnapLock Volume befinden.
- Das SnapLock Volume muss ausgehängt und frei von Snapshots und benutzererstellten Dateien sein.

**Über diese Aufgabe**

Daten müssen nicht sequenziell in den aktiven 256-KB-Block geschrieben werden. Wenn Daten in Byte n×256KB+1 der Datei geschrieben werden, wird das vorherige 256-KB-Segment WORM-geschützt.

Wenn ein Autocommit-Zeitraum für das Volume festgelegt ist, werden WORM-anhängbare Dateien, die über einen Zeitraum, der länger als der Autocommit-Zeitraum ist, nicht geändert wurden, in WORM übernommen.

VAM wird auf SnapLock Revisionsprotokoll-Volumes nicht unterstützt.

**Schritte**

1. VAM aktivieren:

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

   Weitere Informationen zu `volume snaplock modify` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl aktiviert VAM auf dem Volume `vol1` der SVM`vs1`:

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

2. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um Dateien mit Schreibberechtigungen zu erstellen.

   Die Dateien sind standardmäßig WORM-anhängbar.

## Snapshots auf einem ONTAP SnapLock Vault-Ziel in WORM festschreiben

Mit SnapLock für SnapVault lassen sich Snapshots auf sekundärem Speicher WORM-schützen. Alle grundlegenden SnapLock-Aufgaben werden am Vault-Ziel durchgeführt. Das Ziel-Volume wird automatisch schreibgeschützt eingebunden, sodass ein explizites Commit der Snapshots in WORM nicht erforderlich ist.

**Bevor Sie beginnen**

- Wenn der System Manager zur Konfiguration der Beziehung verwendet werden soll, müssen sowohl der Quell- als auch der Ziel-Cluster ONTAP 9.15.1 oder höher ausführen.
- Auf dem Ziel-Cluster:
  - "Die SnapLock-Lizenz installieren".
  - "Die Compliance-Uhr initialisieren".
  - Wenn Sie die CLI mit einer ONTAP Version vor 9.10.1 verwenden, "ein SnapLock Aggregat erstellen".
- Die Datensicherungsstrategie muss vom Typ „vault“ sein.
- Die Quell- und Ziel-Aggregate müssen 64-Bit sein.
- Das Quellvolume darf kein SnapLock Volume sein.
- Wenn Sie die ONTAP CLI verwenden, müssen die Quell- und Ziel-Volumes in "verbundene Cluster" und "SVMs" erstellt werden.

**Über diese Aufgabe**

Das Quell-Volume kann NetApp- oder Storage anderer Anbieter (NetApp-fremd) verwenden.

> Ein Snapshot, der im WORM-Status festgeschrieben ist, kann nicht umbenannt werden.

Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen.

> LUNs werden in SnapLock Volumes nicht unterstützt. LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen Snapshots, die auf einem Nicht-SnapLock Volume erstellt wurden, auf ein SnapLock Volume zum Schutz im Rahmen einer SnapLock Vault-Beziehung übertragen werden. LUNs werden in lesen/schreiben SnapLock Volumes nicht unterstützt. Manipulationssichere Snapshots werden jedoch sowohl auf SnapMirror Quell-Volumes als auch auf Ziel-Volumes unterstützt, die LUNs enthalten.

Ab ONTAP 9.10.1 können SnapLock- und Nicht-SnapLock-Volumes auf demselben Aggregate existieren, daher ist es nicht mehr erforderlich, ein separates SnapLock-Aggregate zu erstellen, wenn ONTAP 9.10.1 verwendet wird. Die Volume-Option '-snaplock-type' wird verwendet, um einen Compliance- oder Enterprise-SnapLock-Volume-Typ anzugeben. In ONTAP-Versionen vor ONTAP 9.10.1 wird der SnapLock-Modus, Compliance oder Enterprise, vom Aggregate übernommen. Version-flexible Zielvolumes werden nicht unterstützt. Die Spracheinstellung des Ziel-Volumes muss mit der Spracheinstellung des Quell-Volumes übereinstimmen.

Ein SnapLock Volume, das als Vault-Ziel dient, hat eine standardmäßige Aufbewahrungsfrist zugewiesen. Der

Wert für diese Frist ist anfangs auf mindestens 0 Jahre für SnapLock Enterprise Volumes und maximal 30 Jahre für SnapLock Compliance Volumes festgelegt. Jeder NetApp Snapshot wird zunächst mit dieser standardmäßigen Aufbewahrungsfrist übernommen. Die Aufbewahrungsfrist kann bei Bedarf später verlängert werden. Weitere Informationen finden sich unter "Übersicht über die Aufbewahrungszeit festlegen".

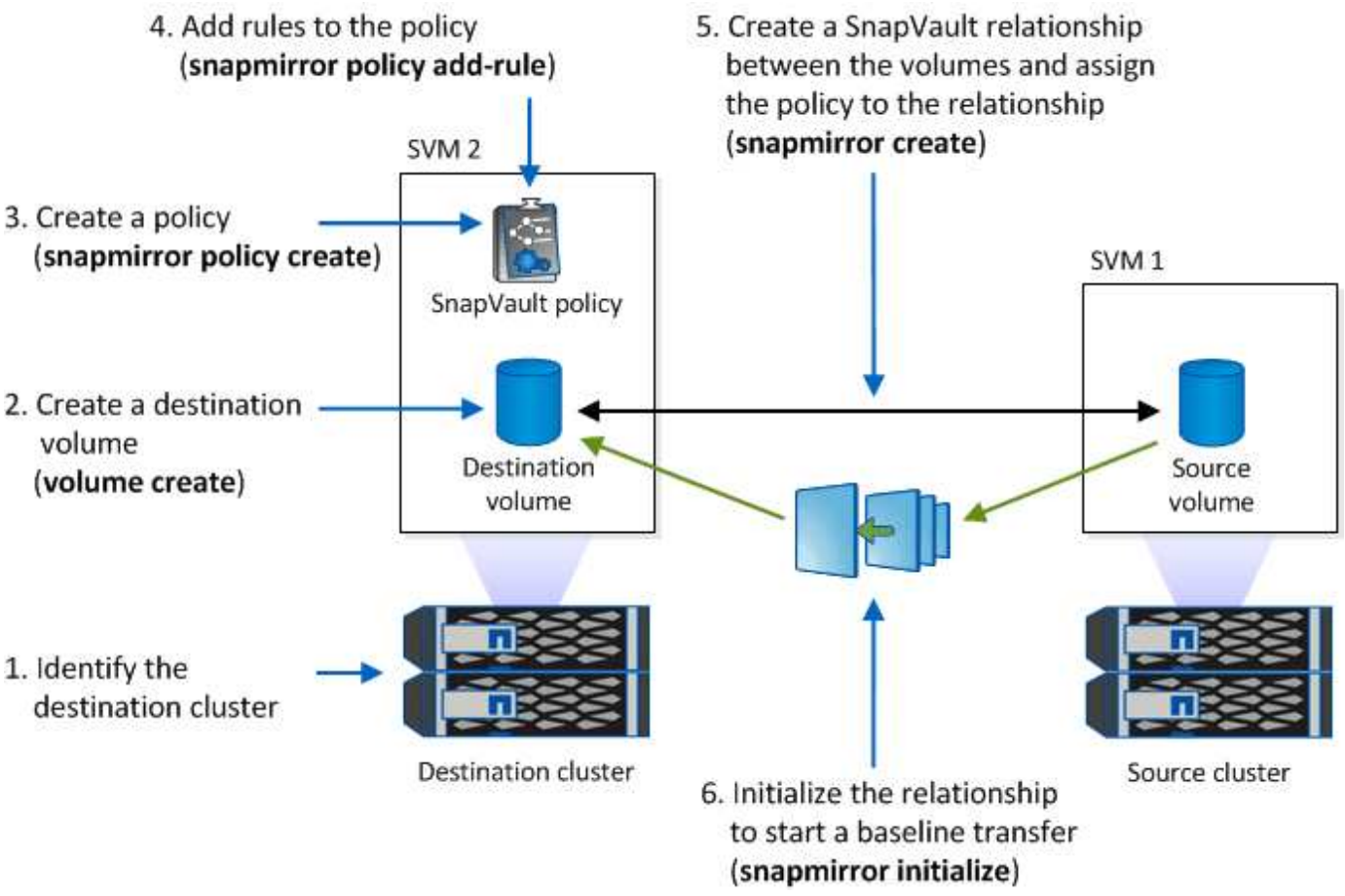
Ab ONTAP 9.14.1 können Aufbewahrungsfristen für bestimmte SnapMirror Labels in der SnapMirror Policy der SnapMirror Beziehung festgelegt werden, sodass die replizierten Snapshots vom Quell- zum Ziel-Volume für die in der Regel angegebene Aufbewahrungsfrist aufbewahrt werden. Wenn keine Aufbewahrungsfrist angegeben ist, wird die Standardaufbewahrungsfrist des Ziel-Volumes verwendet.

Ab ONTAP 9.13.1 ist es möglich, einen gesperrten Snapshot auf dem Ziel-SnapLock-Volume einer SnapLock Vault Beziehung sofort wiederherzustellen, indem eine FlexClone mit der `snaplock-type` Option auf `non-snaplock` erstellt und der Snapshot beim Ausführen der Volume-Klon-Erstellung als „parent-snapshot“ angegeben wird. Weitere Informationen zu "Erstellen eines FlexClone Volumens mit einem SnapLock Typ".

Für MetroCluster Konfigurationen gilt Folgendes:

- Eine SnapVault Beziehung kann nur zwischen Sync-Source-SVMs erstellt werden, nicht zwischen einer Sync-Source-SVM und einer Sync-Destination-SVM.
- Es ist möglich, eine SnapVault Beziehung von einem Volume auf einer Sync-Source-SVM zu einer Data-Serving-SVM zu erstellen.
- Es ist möglich, eine SnapVault Beziehung von einem Volume auf einer datenbereitstellenden SVM zu einem DP Volume auf einer Sync-Source-SVM zu erstellen.

Die folgende Abbildung zeigt das Vorgehen zum Initialisieren einer SnapLock Vault Beziehung:



**Schritte**

Mit der ONTAP CLI lässt sich eine SnapLock Vault Beziehung erstellen, ab ONTAP 9.15.1 ist dies auch mit dem System Manager möglich, um eine SnapLock Vault Beziehung zu erstellen.

**System Manager**

1. Falls das Volume noch nicht existiert, im Quell-Cluster zu **Speicher > Volumes** navigieren und **Hinzufügen** auswählen.
2. Im Fenster **Volume hinzufügen Weitere Optionen** auswählen.
3. Den Datenträgernamen, die Größe, die Exportrichtlinie und den Freigabenamen eingeben.
4. Speichern Sie Ihre Änderungen.
5. Im Ziel-Cluster zu **Schutz > Beziehungen** navigieren.
6. Oberhalb der Spalte **Quelle Schützen** auswählen und im Menü **Volumes** wählen.
7. Im Fenster **Volumes schützen Vault** als Datensicherungsstrategie auswählen.
8. Im Abschnitt **Quelle** sind der Cluster, die Storage-VM und das Volume auszuwählen, die geschützt werden sollen.
9. Im Abschnitt **Ziel** ist unter **Konfigurationsdetails** die Option **Ziel-Snapshots sperren** auszuwählen, anschließend **SnapLock für SnapVault** als Sperrmethode. **Sperrmethode** wird nicht angezeigt, wenn der ausgewählte Richtlinientyp nicht vom Typ `vault` ist, die SnapLock Lizenz nicht installiert ist oder die Compliance-Uhr nicht initialisiert wurde.
10. Falls diese Option noch nicht aktiviert ist, **SnapLock Compliance-Uhr initialisieren** auswählen.
11. Speichern Sie Ihre Änderungen.

**CLI**

1. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Zielvolume vom Typ `DP`, das entweder gleich groß oder größer als das Quellvolume ist:

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

   Der folgende Befehl erstellt ein 2GB SnapLock Compliance Volume mit dem Namen `dstvolB` in `SVM2` auf dem Aggregat `node01_aggr`:

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

2. Auf dem Ziel-Cluster "die Standard-Aufbewahrungsdauer festlegen".
3. "Eine neue Replikationsbeziehung erstellen" zwischen der non-SnapLock Quelle und dem neuen SnapLock Ziel, das erstellt wurde.

   Dieses Beispiel erstellt eine neue SnapMirror Beziehung mit Ziel-SnapLock Volume `dstvolB` unter Verwendung einer Strategie von `XDPDefault` zum Archivieren von Snapshots mit den Bezeichnungen täglich und wöchentlich nach einem stündlichen Zeitplan:

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

"Erstellen einer benutzerdefinierten Replikationsrichtlinie" oder ein "benutzerdefinierter Zeitplan", wenn die verfügbaren Standardeinstellungen nicht geeignet sind.

4. Auf der Ziel-SVM die erstellte SnapVault Beziehung initialisieren:

```
snapmirror initialize -destination-path <destination_path>
```

Der folgende Befehl initialisiert die Beziehung zwischen dem Quell-Volume `srcvolA` auf `SVM1` und dem Ziel-Volume `dstvolB` auf `SVM2`:

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

5. Nachdem die Beziehung initialisiert und im Leerlauf ist, kann mit dem `snapshot show` Befehl auf dem Ziel die für die replizierten Snapshots angewendete SnapLock Ablaufzeit überprüft werden.

Dieses Beispiel listet die Snapshots auf dem Volume `dstvolB` auf, die die SnapMirror Bezeichnung und das SnapLock Ablaufdatum haben:

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

**Verwandte Informationen**

- "Cluster- und SVM-Peering"
- "Volume Backup mit SnapVault"
- "snapmirror initialize"

## WORM-Dateien mit ONTAP SnapMirror für die Notfallwiederherstellung spiegeln

SnapMirror kann verwendet werden, um WORM-Dateien zur Notfallwiederherstellung und für andere Zwecke an einen anderen geografischen Standort zu replizieren. Sowohl das Quellvolume als auch das Zielvolume müssen für SnapLock konfiguriert sein, und beide Volumes müssen denselben SnapLock Modus (Compliance oder Enterprise) aufweisen. Alle wichtigen SnapLock Eigenschaften des Volumes und der Dateien werden repliziert.

**Voraussetzungen**

Die Quell- und Ziel-Volumes müssen in gepeerten Clustern mit gepeerten SVMs erstellt werden. Weitere Informationen finden sich unter "Cluster- und SVM-Peering".

**Über diese Aufgabe**

- Ab ONTAP 9.5 ist es möglich, WORM-Dateien mit der XDP (Extended Data Protection)-SnapMirror-Beziehung anstelle der DP (Data Protection)-Beziehung zu replizieren. Der XDP-Modus ist ONTAP versionsunabhängig und kann Dateien, die im selben Block gespeichert sind, unterscheiden, was die Resynchronisierung replizierter Compliance-Mode-Volumes erheblich erleichtert. Informationen zur Konvertierung einer bestehenden DP-Beziehung in eine XDP-Beziehung sind unter "Datensicherung" zu finden.
- Ein Resync-Vorgang für eine DP-Typ-SnapMirror Beziehung schlägt bei einem Compliance-Mode-Volume fehl, wenn SnapLock feststellt, dass dadurch ein Datenverlust entstehen würde. Wenn ein Resync-Vorgang fehlschlägt, kann mit dem `volume clone create` Befehl ein Klon des Ziel-Volumes erstellt werden. Anschließend lässt sich das Quell-Volume mit dem Klon erneut synchronisieren.
- Eine SnapMirror Beziehung eines SnapLock Volumes unterstützt ausschließlich die `MirrorAllSnapshots` Richtlinie vom Typ async-mirror. Die Aufbewahrungsdauer eines SnapLock Volumes wird durch die maximale Aufbewahrungsdauer aller darauf enthaltenen WORM-Dateien bestimmt. Da das Ziel eine DR-Kopie der Quelle ist, entspricht die Aufbewahrungsdauer des Ziel-SnapLock Volumes derjenigen der Quelle.
- Eine SnapMirror Beziehung vom Typ XDP zwischen SnapLock konformen Volumes unterstützt eine Resynchronisierung nach einer Unterbrechung, selbst wenn die Daten auf dem Ziel nach der Unterbrechung von den Daten auf der Quelle abgewichen sind.

  Bei einer Resynchronisierung wird, wenn zwischen Quelle und Ziel Datenabweichungen über den gemeinsamen Snapshot hinaus festgestellt werden, ein neuer Snapshot auf dem Ziel erstellt, um diese Abweichungen zu erfassen. Der neue Snapshot und der gemeinsame Snapshot werden beide mit einer Aufbewahrungszeit wie folgt gesperrt:

  - Die Ablaufzeit des Ziel-Volumes
  - Wenn die Ablaufzeit des Volumes in der Vergangenheit liegt oder nicht festgelegt wurde, ist der Snapshot für einen Zeitraum von 30 Tagen gesperrt.
  - Wenn das Zielsystem über rechtliche Sperren verfügt, wird die tatsächliche Ablaufzeit des Volumens ausgeblendet und als ‘indefinite’ angezeigt; der Snapshot ist jedoch für die Dauer der tatsächlichen Ablaufzeit des Volumens gesperrt.

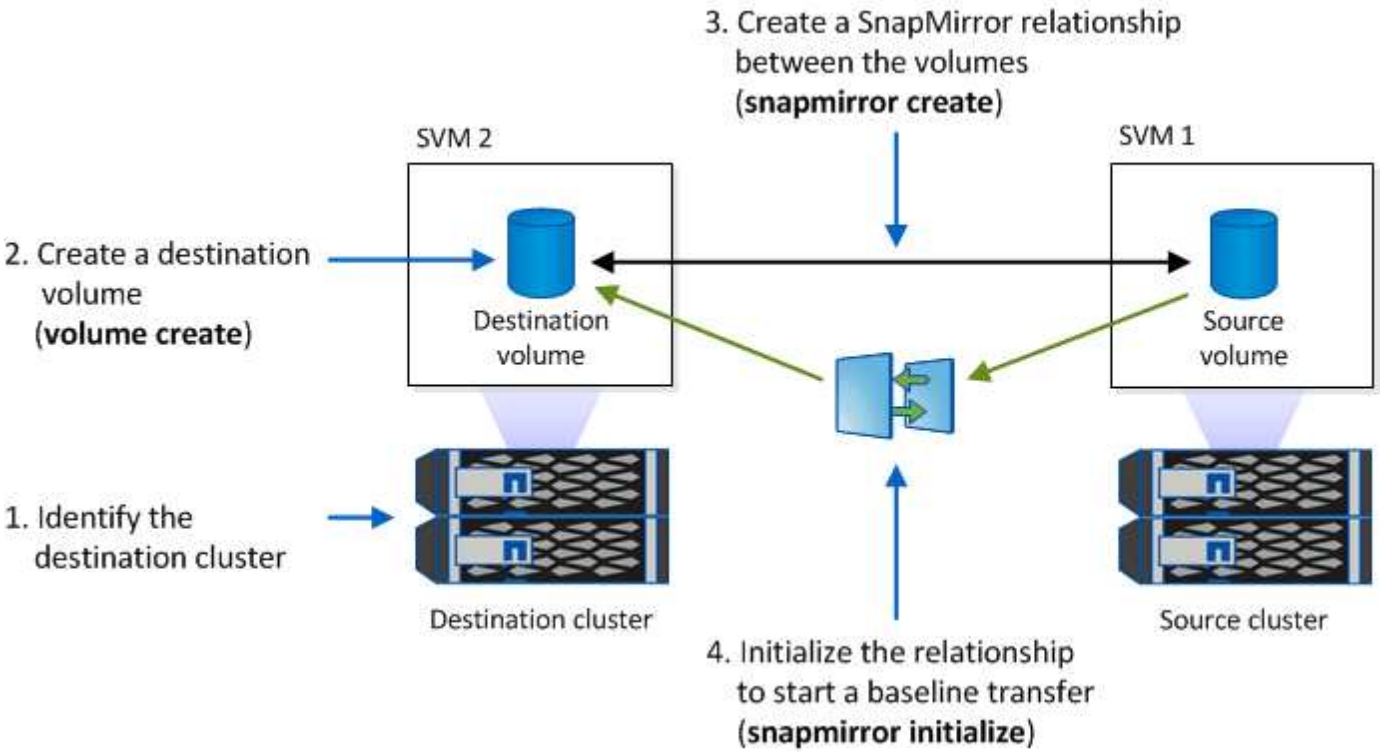
Wenn das Zielvolume eine Ablaufperiode hat, die später ist als die des Quellvolumes, bleibt die Ablaufperiode des Zielvolumes erhalten und wird nach der Resynchronisierung nicht durch die Ablaufperiode des Quellvolumes überschrieben.

Wenn auf dem Ziel rechtliche Sperren bestehen, die sich von denen auf der Quelle unterscheiden, ist eine erneute Synchronisierung nicht zulässig. Quelle und Ziel müssen identische rechtliche Sperren aufweisen oder alle rechtlichen Sperren auf dem Ziel müssen aufgehoben werden, bevor eine erneute Synchronisierung versucht wird.

Ein gesperrter Snapshot auf dem Zielvolume, der zur Erfassung der abweichenden Daten erstellt wurde, kann mithilfe der CLI durch Ausführen des `snapmirror update -s snapshot` Befehls auf das Quellvolume kopiert werden. Der Snapshot bleibt nach dem Kopieren auch auf dem Quellvolume gesperrt.

- SVM Datenschutzbeziehungen werden nicht unterstützt.
- Load-sharing-Datenschutzbeziehungen werden nicht unterstützt.

Die folgende Abbildung zeigt das Vorgehen zum Initialisieren einer SnapMirror Beziehung:




**System Manager**

Ab ONTAP 9.12.1 ist es möglich, mit System Manager die SnapMirror Replikation von WORM-Dateien einzurichten.

**Schritte**

1. Navigieren Sie zu **Storage > Volumes**.
2. Klicken Sie auf **Ein-/Ausblenden** und wählen Sie **SnapLock Type**, um die Spalte im Fenster **Volumes** anzuzeigen.
3. Ein SnapLock Volume lokalisieren.
4. Klicken Sie ⋮ und wählen Sie **Schützen**.
5. Den Ziel-Cluster und die Ziel-Speicher-VM auswählen.
6. Auf **Weitere Optionen** klicken.
7. **Legacy-Richtlinien anzeigen** und **DPDefault (legacy)** auswählen.
8. Im Abschnitt **Zielkonfigurationsdetails Übertragungsplan überschreiben** und **stündlich** auswählen.
9. Auf **Speichern** klicken.
10. Klicken Sie links neben dem Namen des Quellvolumes auf den Pfeil, um die Volume-Details zu erweitern, und überprüfen Sie auf der rechten Seite der Seite die Details zum Remote-SnapMirror-Schutz.
11. Im Remote-Cluster zu **Schutzbeziehungen** navigieren.
12. Die Beziehung kann gefunden werden, indem auf den Namen des Ziel-Volumes geklickt wird, wodurch die Details der Beziehung angezeigt werden.
13. Überprüfen Sie den SnapLock-Typ des Ziel-Volumes und weitere SnapLock-Informationen.

**CLI**

1. Der Ziel-Cluster wird identifiziert.
2. Auf dem Ziel-Cluster, "die SnapLock-Lizenz installieren", "Die Compliance-Uhr initialisieren" und, falls eine ONTAP Version vor 9.10.1 verwendet wird, "ein SnapLock Aggregat erstellen".
3. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Zielvolume vom Typ `DP`, das entweder die gleiche Größe wie das Quellvolume hat oder größer ist:

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

   > Ab ONTAP 9.10.1 können SnapLock- und Nicht-SnapLock-Volumes auf demselben Aggregate existieren, daher ist es nicht mehr erforderlich, ein separates SnapLock-Aggregate zu erstellen, wenn ONTAP 9.10.1 verwendet wird. Die Option volume -snaplock-type wird verwendet, um einen Compliance- oder Enterprise-SnapLock-Volume-Typ anzugeben. In ONTAP-Versionen vor ONTAP 9.10.1 wird der SnapLock-Modus (Compliance oder Enterprise) vom Aggregate übernommen. Die Spracheinstellung des Ziel-Volumes muss mit der Spracheinstellung des Quell-Volumes übereinstimmen.

   Der folgende Befehl erstellt ein 2 GB SnapLock `Compliance` Volume mit dem Namen `dstvolB` in `SVM2` auf dem Aggregat `node01_aggr`:

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

4. Auf der Ziel-SVM eine SnapMirror Richtlinie erstellen:

   `snapmirror policy create -vserver` *`SVM_name`* `-policy` *`policy_name`*

   Der folgende Befehl erstellt die SVM-weite Richtlinie `SVM1-mirror`:

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
   ```

5. Auf der Ziel-SVM einen SnapMirror Zeitplan erstellen:

   **`job schedule cron create -name` *`schedule_name`* `-dayofweek` *`day_of_week`* `-hour` *`hour`* `-minute` *`minute`***

   Der folgende Befehl erstellt einen SnapMirror Zeitplan mit dem Namen `weekendcron`:

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

6. Auf der Ziel-SVM eine SnapMirror Beziehung erstellen:

   `snapmirror create -source-path` *`source_path`* `-destination-path`

*destination_path* -type XDP|DP -policy *policy_name* -schedule *schedule_name*

Der folgende Befehl erstellt eine SnapMirror Beziehung zwischen dem Quellvolume `srcvolA` auf `SVM1` und dem Zielvolume `dstvolB` auf `SVM2`, und weist die Richtlinie `SVM1-mirror` und den Zeitplan `weekendcron` zu:

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

Der XDP Typ ist ab ONTAP 9.5 verfügbar. In ONTAP 9.4 und früher muss der DP Typ verwendet werden.

7. In der Ziel-SVM die SnapMirror Beziehung initialisieren:

   `snapmirror initialize -destination-path` *destination_path*

   Der Initialisierungsprozess führt einen Basistransfer auf das Ziel-Volume durch. SnapMirror erstellt einen Snapshot des Quell-Volumes und überträgt anschließend die Kopie sowie alle von ihr referenzierten Datenblöcke auf das Ziel-Volume. Es werden außerdem alle weiteren Snapshots des Quell-Volumes auf das Ziel-Volume übertragen.

   Der folgende Befehl initialisiert die Beziehung zwischen dem Quell-Volume `srcvolA` auf `SVM1` und dem Ziel-Volume `dstvolB` auf `SVM2`:

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

**Verwandte Informationen**

- "Cluster- und SVM-Peering"
- "Vorbereitung der Volume-Desaster-Recovery"
- "Datenschutz"
- "snapmirror create"
- "snapmirror initialize"
- "snapmirror policy create"

## WORM-Dateien während eines Rechtsstreits mit ONTAP SnapLock Legal Hold aufbewahren

Ab ONTAP 9.3 ist es möglich, WORM-Dateien im Compliance-Modus für die Dauer eines Rechtsstreits mithilfe der Funktion *Legal Hold* aufzubewahren.

**Bevor Sie beginnen**

- Um diese Aufgabe auszuführen, sind SnapLock Administratorrechte erforderlich.

  "Ein SnapLock Administratorkonto erstellen"

- Eine Anmeldung über eine sichere Verbindung (SSH, Konsole oder ZAPI) muss erfolgt sein.

**Über diese Aufgabe**

Eine unter Legal Hold stehende Datei verhält sich wie eine WORM-Datei mit unbestimmter Aufbewahrungsfrist. Es liegt in Ihrer Verantwortung, festzulegen, wann der Legal Hold Zeitraum endet.

Die Anzahl der Dateien, die Sie unter eine Legal Hold stellen können, hängt vom verfügbaren Speicherplatz auf dem Volume ab.

**Schritte**

1. Rechtliche Sicherung starten:

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   Der folgende Befehl startet eine rechtliche Sperre für alle Dateien in `vol1`:

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

2. Legal Hold beenden:

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   Der folgende Befehl beendet die rechtliche Sperre für alle Dateien in `vol1`:

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

**Verwandte Informationen**

- "snaplock legal-hold begin"
- "snaplock Legal-Hold Ende"

## WORM-Dateien mit ONTAP SnapLock löschen

Sie können WORM-Dateien im Enterprise-Modus während der Aufbewahrungsfrist mithilfe der Funktion „Privilegiertes Löschen“ löschen. Bevor diese Funktion genutzt werden kann, muss ein SnapLock Administratoraccount erstellt und anschließend mit diesem Konto die Funktion aktiviert werden.

### Ein SnapLock Administratorkonto erstellen

Sie müssen über SnapLock-Administratorrechte verfügen, um ein privilegiertes Löschen durchzuführen. Diese Berechtigungen sind in der Rolle vsadmin-snaplock definiert. Falls Ihnen diese Rolle noch nicht zugewiesen wurde, kann der Cluster-Administrator ein SVM-Administratorkonto mit der SnapLock-Administratorrolle erstellen.

**Bevor Sie beginnen**

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Eine Anmeldung über eine sichere Verbindung (SSH, Konsole oder ZAPI) muss erfolgt sein.

**Schritte**

1. Ein SVM-Administratorkonto mit der SnapLock Administratorrolle erstellen:

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

   Der folgende Befehl ermöglicht dem SVM-Administratorkonto `SnapLockAdmin` mit der vordefinierten `vsadmin-snaplock` Rolle den Zugriff `SVM1` mittels eines Passworts:

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

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

### Die Funktion zum privilegierten Löschen aktivieren

Sie müssen die Funktion zum privilegierten Löschen auf dem Enterprise Volume, das die zu löschenden WORM-Dateien enthält, explizit aktivieren.

**Über diese Aufgabe**

Der Wert der `-privileged-delete` Option bestimmt, ob privilegiertes Löschen aktiviert ist. Mögliche Werte sind `enabled`, `disabled` und `permanently-disabled`.

> `permanently-disabled` ist der Endzustand. Das privilegierte Löschen kann auf dem Volume nicht mehr aktiviert werden, nachdem der Zustand auf `permanently-disabled` gesetzt wurde.

**Schritte**

1. Privilegiertes Löschen für ein SnapLock Enterprise Volume aktivieren:

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

   Der folgende Befehl aktiviert die Funktion zum privilegierten Löschen für das Enterprise Volume `dataVol` auf `SVM1`:

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

### Enterprise-Modus WORM-Dateien löschen

Die Funktion „Privilegiertes Löschen“ ermöglicht das Löschen von WORM-Dateien im Enterprise-Modus während der Aufbewahrungsfrist.

#### Bevor Sie beginnen

- Um diese Aufgabe auszuführen, sind SnapLock Administratorrechte erforderlich.
- Ein SnapLock Revisionsprotokoll muss erstellt und die Funktion zum privilegierten Löschen auf dem Enterprise Volume aktiviert sein.

#### Über diese Aufgabe

Eine privilegierte Löschoperation kann nicht verwendet werden, um eine abgelaufene WORM-Datei zu löschen. Mit dem `volume file retention show` Befehl lässt sich die Aufbewahrungszeit der WORM-Datei anzeigen, die gelöscht werden soll. Weitere Informationen zu `volume file retention show` finden sich in der "ONTAP-Befehlsreferenz".

#### Schritt

1. Löschen einer WORM-Datei auf einem Enterprise Volume:

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

   Der folgende Befehl löscht die Datei `/vol/dataVol/f1` auf der SVM`SVM1`:

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

# Verschieben eines ONTAP SnapLock Volumes

Ab ONTAP 9.8 ist es möglich, ein SnapLock Volume in ein Zielaggregat desselben Typs zu verschieben, entweder von Enterprise zu Enterprise oder von Compliance zu Compliance. Die SnapLock Sicherheitsrolle muss zugewiesen sein, um ein SnapLock Volume zu verschieben.

## Ein SnapLock Sicherheitsadministratorkonto erstellen

Sie müssen über SnapLock Sicherheitsadministratorrechte verfügen, um eine SnapLock Volume-Verschiebung durchzuführen. Dieses Privileg wird Ihnen mit der Rolle *snaplock* gewährt, die in ONTAP 9.8 eingeführt wurde. Falls Ihnen diese Rolle noch nicht zugewiesen wurde, kann Ihr Cluster-Administrator einen SnapLock Sicherheitsbenutzer mit dieser SnapLock Sicherheitsrolle erstellen.

#### Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Eine Anmeldung über eine sichere Verbindung (SSH, Konsole oder ZAPI) muss erfolgt sein.

#### Über diese Aufgabe

Die SnapLock Rolle ist mit der Admin-SVM verknüpft, im Gegensatz zur vsadmin-snaplock Rolle, die mit der Daten-SVM verknüpft ist.

#### Schritt

1. Ein SVM-Administratorkonto mit der SnapLock Administratorrolle erstellen:

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

   Der folgende Befehl ermöglicht dem SVM-Administratorkonto `SnapLockAdmin` mit der vordefinierten `snaplock` Rolle den Zugriff auf die Admin SVM `cluster1` mit einem Passwort:

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

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

## Ein SnapLock Volume verschieben

Mit dem `volume move` Befehl lässt sich ein SnapLock Volume auf ein Zielaggregat verschieben.

**Bevor Sie beginnen**

- Vor der Durchführung einer SnapLock-geschützten Revisionsprotokollierung muss ein SnapLock-geschütztes Revisionsprotokoll erstellt worden sein.

  "Ein Revisionsprotokoll erstellen".

- Wenn eine Version von ONTAP vor ONTAP 9.10.1 verwendet wird, muss das Zielaggregat denselben SnapLock-Typ wie das SnapLock-Volume aufweisen, das verschoben werden soll; entweder Compliance zu Compliance oder Enterprise zu Enterprise. Ab ONTAP 9.10.1 entfällt diese Einschränkung und ein Aggregat kann sowohl Compliance als auch Enterprise SnapLock Volumes sowie Nicht-SnapLock Volumes enthalten.
- Sie müssen ein Benutzer mit der SnapLock Sicherheitsrolle sein.

**Schritte**

1. Über eine sichere Verbindung bei der ONTAP Cluster-Management-LIF anmelden:

   **ssh snaplock_user@cluster_mgmt_ip**

2. Ein SnapLock Volume verschieben:

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

3. Status des Volume-Verschiebungsvorgangs prüfen:

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

# Einen ONTAP Snapshot zum Schutz vor Ransomware-Angriffen sperren

Ab ONTAP 9.12.1 können Snapshots auf einem Nicht-SnapLock Volume gesperrt werden, um Schutz vor Ransomware-Angriffen zu bieten. Das Sperren von Snapshots stellt sicher, dass sie nicht versehentlich oder böswillig gelöscht werden können.

Die SnapLock compliance clock-Funktion wird verwendet, um Snapshots für einen festgelegten Zeitraum zu sperren, sodass sie erst nach Erreichen der Ablaufzeit gelöscht werden können. Das Sperren von Snapshots macht sie manipulationssicher und schützt sie vor Ransomware-Bedrohungen. Mit gesperrten Snapshots kann eine Datenwiederherstellung erfolgen, wenn ein Volume durch einen Ransomware-Angriff kompromittiert wurde.

Ab ONTAP 9.14.1 unterstützt die Snapshot-Sperre Snapshots mit langfristiger Aufbewahrung auf nicht-SnapLock Vault- und Mirror-Vault-SnapMirror Ziel-Volumes. Die Aktivierung der Snapshot-Sperre erfolgt durch Festlegen der Aufbewahrungsdauer mit SnapMirror Richtlinienregeln, die einem bestehende Richtlinienbezeichnung zugeordnet sind. Die Regel überschreibt die auf dem Volume festgelegte Standardaufbewahrungsdauer. Wenn dem SnapMirror Label keine Aufbewahrungsdauer zugeordnet ist, wird die Standardaufbewahrungsdauer des Volumes verwendet.

**Anforderungen und Überlegungen zu manipulationssicheren Snapshots**

- Wenn die ONTAP CLI verwendet wird, müssen alle Knoten im Cluster ONTAP 9.12.1 oder neuer ausführen. Wenn System Manager verwendet wird, müssen alle Knoten ONTAP 9.13.1 oder neuer ausführen.
- "Die SnapLock Lizenz muss auf dem Cluster installiert sein.". Diese Lizenz ist in "ONTAP One" enthalten.
- "Die Compliance-Uhr auf dem Cluster muss initialisiert sein.".
- Wenn die Snapshot-Sperre auf einem Volume aktiviert ist, können Sie die Cluster auf eine ONTAP Version aktualisieren, die nach ONTAP 9.12.1 liegt. Sie können jedoch erst dann auf eine frühere Version von ONTAP zurückkehren, wenn alle gesperrten Snapshots ihr Ablaufdatum erreicht haben, gelöscht wurden und die Snapshot-Sperre deaktiviert ist.
- Wenn ein Snapshot gesperrt ist, wird die Ablaufzeit des Volumes auf die Ablaufzeit des Snapshots gesetzt. Wenn mehr als ein Snapshot gesperrt ist, entspricht die Ablaufzeit des Volumes der größten Ablaufzeit aller Snapshots.
- Die Aufbewahrungsfrist für gesperrte Snapshots hat Vorrang vor der Snapshot-Aufbewahrungsanzahl, was bedeutet, dass die Begrenzung der Aufbewahrungsanzahl nicht berücksichtigt wird, wenn die Aufbewahrungsfrist für gesperrte Snapshots noch nicht abgelaufen ist.
- In einer SnapMirror Beziehung kann eine Aufbewahrungsdauer für eine Mirror-Vault-Richtlinienregel festgelegt werden, und die Aufbewahrungsdauer wird auf Snapshots angewendet, die auf das Ziel repliziert werden, wenn auf dem Zielvolume die Snapshot-Sperre aktiviert ist. Die Aufbewahrungsdauer hat Vorrang vor der Aufbewahrungsanzahl; beispielsweise werden Snapshots, deren Ablaufdatum noch nicht erreicht ist, auch dann aufbewahrt, wenn die Aufbewahrungsanzahl überschritten wurde.
- Sie können einen Snapshot auf einem Nicht-SnapLock Volume umbenennen. Snapshot-Umbenennungsvorgänge auf dem primären Volume einer SnapMirror Beziehung werden auf dem sekundären Volume nur dann widergespiegelt, wenn die Richtlinie MirrorAllSnapshots ist. Bei anderen Richtlinientypen wird der umbenannte Snapshot bei Aktualisierungen nicht übernommen.
- Wenn die ONTAP CLI verwendet wird, kann ein gesperrter Snapshot mit dem `volume snapshot restore` Befehl nur dann wiederhergestellt werden, wenn der gesperrte Snapshot der aktuellste ist. Wenn spätere, noch nicht abgelaufene Snapshots vorhanden sind, als der wiederherzustellende, schlägt die Snapshot-Wiederherstellung fehl.

**Funktionen, die mit manipulationssicheren Snapshots unterstützt werden**

- "Cloud Volumes ONTAP"
- FlexCache Ursprungs-Volumes

  Unterstützt ab ONTAP 9.16.1.

- FlexGroup Volumes

  Die Snapshot-Sperrung wird für FlexGroup Volumes unterstützt. Die Snapshot-Sperrung erfolgt nur beim Snapshot des Root-Bestandteils. Das Löschen des FlexGroup Volumes ist nur zulässig, wenn die Ablaufzeit des Root-Bestandteils abgelaufen ist.

- FlexVol zu FlexGroup Konvertierung

  Sie können ein FlexVol Volume mit gesperrten Snapshots in ein FlexGroup Volume konvertieren. Snapshots bleiben nach der Konvertierung gesperrt.

- SnapMirror Active Sync für NAS

  Ab ONTAP 9.20.1 können Sie manipulationssichere Snapshots auf SnapMirror active sync NAS FlexVol Volumes in SVM-Beziehungen erstellen.

- SnapMirror asynchron

  Die Compliance-Uhr muss sowohl auf dem Quell- als auch auf dem Zielsystem initialisiert werden.

- SnapMirror Richtlinienregeln mit dem `-schedule` Parameter
- SnapMirror synchron

  Ab ONTAP 9.19.1 kann die Ablaufzeit nur noch bei der Snapshot-Erstellung festgelegt werden. Sie können die Ablaufzeit für vorhandene Snapshots nicht festlegen oder verlängern.

- SVM Datenmobilität (wird für die Migration oder Verlagerung einer SVM von einem Quell-Cluster zu einem Ziel-Cluster verwendet)

  Unterstützt ab ONTAP 9.14.1.

- SVM DR

  Die Compliance-Uhr muss sowohl auf dem Quell- als auch auf dem Zielsystem initialisiert werden.

- Volume clone und Klon einer Datei

  Aus einem gesperrten Snapshot können Volume-Klone und Klone einer Datei erstellt werden.

**Nicht unterstützte Funktionen**

Manipulationssichere Snapshots unterstützen diese Funktionen nicht:

- Konsistenzgruppen
- "FabricPool"

  Manipulationssichere Snapshots bieten unveränderlichen Schutz, der nicht gelöscht werden kann. Da FabricPool die Möglichkeit zum Löschen von Daten benötigt, können FabricPool und Snapshot-Sperren nicht auf demselben Volume aktiviert werden.

- SMtape
- SnapMirror Active Sync für SAN

## Snapshot-Sperre beim Erstellen eines Volumes aktivieren

Ab ONTAP 9.12.1 kann die Snapshot-Sperre beim Erstellen eines neuen Volumes oder beim Ändern eines vorhandenen Volumes mithilfe der `-snapshot-locking-enabled` Option zusammen mit den `volume create` und `volume modify` Befehlen in der CLI aktiviert werden. Ab ONTAP 9.13.1 kann der System Manager verwendet werden, um die Snapshot-Sperre zu aktivieren.

**System Manager**

1. Navigieren Sie zu **Storage > Volumes** und wählen Sie **Add**.
2. Im Fenster **Volume hinzufügen Weitere Optionen** auswählen.
3. Den Datenträgernamen, die Größe, die Exportrichtlinie und den Freigabenamen eingeben.
4. **Snapshot-Sperre aktivieren** auswählen. Diese Auswahlmöglichkeit wird nicht angezeigt, wenn die SnapLock Lizenz nicht installiert ist.
5. Falls diese Option noch nicht aktiviert ist, **SnapLock Compliance-Uhr initialisieren** auswählen.
6. Speichern Sie Ihre Änderungen.
7. Im Fenster **Volumes** das aktualisierte Volume auswählen und **Übersicht** wählen.
8. Es wird geprüft, ob **SnapLock Snapshot Locking** als **Aktiviert** angezeigt wird.

**CLI**

1. Zum Erstellen eines neuen Volumes und Aktivieren der Snapshot-Sperre ist folgender Befehl einzugeben:

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

   Der folgende Befehl aktiviert die Snapshot-Sperre auf einem neuen Volume mit dem Namen vol1:

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

## Aktivieren der Snapshot-Sperre auf einem vorhandenen Volume

Ab ONTAP 9.12.1 ist es möglich, die Snapshot-Sperre für ein vorhandenes Volume mithilfe der ONTAP CLI zu aktivieren. Ab ONTAP 9.13.1 kann die Snapshot-Sperre für ein vorhandenes Volume mithilfe des System Manager aktiviert werden.

**System Manager**

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie ⋮ und dann **Bearbeiten > Volume**.
3. Im Fenster **Volume bearbeiten** befindet sich der Abschnitt Snapshots (Lokal) Einstellungen, dort kann **Snapshot-Sperre aktivieren** ausgewählt werden.

   Diese Auswahlmöglichkeit wird nicht angezeigt, wenn die SnapLock Lizenz nicht installiert ist.
4. Falls diese Option noch nicht aktiviert ist, **SnapLock Compliance-Uhr initialisieren** auswählen.
5. Speichern Sie Ihre Änderungen.
6. Im Fenster **Volumes** das aktualisierte Volume auswählen und **Übersicht** wählen.
7. Es wird geprüft, ob **SnapLock Snapshot-Sperrung** als **Aktiviert** angezeigt wird.

**CLI**

1. Um ein vorhandenes Volume zu modifizieren, um die Snapshot-Sperre zu aktivieren, ist folgender Befehl einzugeben:

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

## Eine Richtlinie für gesperrte Snapshots erstellen und die Aufbewahrungsfrist anwenden

Ab ONTAP 9.12.1 ist es möglich, Snapshot-Richtlinien zu erstellen, um eine Aufbewahrungsdauer für Snapshots festzulegen und die Richtlinie auf ein Volume anzuwenden, sodass Snapshots für den angegebenen Zeitraum gesperrt werden. Ein Snapshot kann auch durch das manuelle Festlegen einer Aufbewahrungsdauer gesperrt werden. Ab ONTAP 9.13.1 kann der System Manager verwendet werden, um Snapshot-Sperrrichtlinien zu erstellen und sie auf ein Volume anzuwenden.

### Erstellen einer Snapshot-Sperrrichtlinie

**System Manager**

1. Zu **Speicher > Speicher-VMs** navigieren und eine Speicher-VM auswählen.
2. **Einstellungen** auswählen.
3. **Snapshot-Richtlinien** suchen und → auswählen.
4. Im Fenster **Snapshot-Richtlinie hinzufügen** den Richtliniennamen eingeben.
5. Wählen Sie + Add .
6. Geben Sie die Details des Snapshot-Zeitplans an, einschließlich des Zeitplannamens, der maximalen Anzahl der aufzubewahrenden Snapshots und der SnapLock Aufbewahrungsdauer.
7. Geben Sie in der Spalte **SnapLock Aufbewahrungsdauer** die Anzahl der Stunden, Tage, Monate oder Jahre ein, für die die Snapshots aufbewahrt werden sollen. Beispielsweise sperrt eine Snapshot-Richtlinie mit einer Aufbewahrungsdauer von fünf Tagen einen Snapshot für fünf Tage ab dem Zeitpunkt seiner Erstellung; während dieser Zeit kann er nicht gelöscht werden. Folgende Aufbewahrungsdauerbereiche werden unterstützt:
   - Jahre: 0 - 100

- Monate: 0 - 1200
- Tage: 0 - 36500
- Stunden: 0 - 24

8. Speichern Sie Ihre Änderungen.

**CLI**

1. Zum Erstellen einer Snapshot-Richtlinie ist folgender Befehl einzugeben:

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   Der folgende Befehl erstellt eine Snapshot-Sperrrichtlinie:

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   Ein Snapshot wird nicht ersetzt, wenn er sich in aktiver Aufbewahrung befindet, das heißt, die Aufbewahrungsanzahl wird nicht berücksichtigt, wenn gesperrte Snapshots vorhanden sind, die noch nicht abgelaufen sind.

### Eine Sperrrichtlinie auf ein Volume anwenden

**System Manager**

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie ⋮ und dann **Bearbeiten > Volume**.
3. Im Fenster **Volume bearbeiten Snapshots planen** auswählen.
4. Die Richtlinie zum Sperren von Snapshots aus der Liste auswählen.
5. Falls die Snapshot-Sperre noch nicht aktiviert ist, **Snapshot-Sperre aktivieren** auswählen.
6. Speichern Sie Ihre Änderungen.

**CLI**

1. Um eine Snapshot-Sperrrichtlinie auf ein vorhandenes Volume anzuwenden, ist folgender Befehl einzugeben:

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

### Aufbewahrungsfrist bei manueller Snapshot-Erstellung anwenden

Sie können beim manuellen Erstellen eines Snapshots eine Aufbewahrungsdauer festlegen. Snapshot-Sperre muss für das Volume aktiviert sein, andernfalls wird die Einstellung der Aufbewahrungsdauer ignoriert.

**System Manager**

1. Zu **Speicher > Volumes** navigieren und ein Volume auswählen.
2. Auf der Seite mit den Volumendetails die Registerkarte **Snapshots** auswählen.
3. Wählen Sie + Add .
4. Geben Sie den Snapshot-Namen und die SnapLock Ablaufzeit ein. Es besteht die Möglichkeit, den Kalender auszuwählen, um das Ablaufdatum und die Uhrzeit der Aufbewahrung festzulegen.
5. Speichern Sie Ihre Änderungen.
6. Auf der Seite **Volumes > Snapshots Anzeigen/Ausblenden** auswählen und **SnapLock Expiration Time** wählen, um die Spalte **SnapLock Expiration Time** anzuzeigen und zu überprüfen, ob die Aufbewahrungszeit eingestellt ist.

**CLI**

1. Um einen Snapshot manuell zu erstellen und eine Sperr-Aufbewahrungsfrist anzuwenden, ist folgender Befehl einzugeben:

   ```
   volume snapshot create -volume <volume_name> -snapshot <snapshot name>
   -snaplock-expiry-time <expiration_date_time>
   ```

   Der folgende Befehl erstellt einen neuen Snapshot und legt die Aufbewahrungsdauer fest:

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

### Aufbewahrungszeitraum auf einen vorhandenen Snapshot anwenden

**System Manager**

1. Zu **Speicher > Volumes** navigieren und ein Volume auswählen.
2. Auf der Seite mit den Volumendetails die Registerkarte **Snapshots** auswählen.
3. Wählen Sie den Snapshot aus, wählen Sie ⋮ und dann **Modify SnapLock Expiration Time**. Es besteht die Möglichkeit, den Kalender auszuwählen, um das Ablaufdatum und die Uhrzeit der Aufbewahrung festzulegen.
4. Speichern Sie Ihre Änderungen.
5. Auf der Seite **Volumes > Snapshots Anzeigen/Ausblenden** auswählen und **SnapLock Expiration Time** wählen, um die Spalte **SnapLock Expiration Time** anzuzeigen und zu überprüfen, ob die Aufbewahrungszeit eingestellt ist.

**CLI**

1. Um einem vorhandenen Snapshot manuell eine Aufbewahrungsfrist zuzuweisen, ist folgender Befehl einzugeben:

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   Im folgenden Beispiel wird eine Aufbewahrungsfrist auf einen bestehenden Snapshot angewendet:

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

**Eine bestehende Richtlinie anpassen, um die langfristige Aufbewahrung anzuwenden.**

In einer SnapMirror Beziehung kann eine Aufbewahrungsdauer für eine Mirror-Vault-Richtlinienregel festgelegt werden, und die Aufbewahrungsdauer wird auf Snapshots angewendet, die auf das Ziel repliziert werden, wenn auf dem Zielvolume die Snapshot-Sperre aktiviert ist. Die Aufbewahrungsdauer hat Vorrang vor der Aufbewahrungsanzahl; beispielsweise werden Snapshots, deren Ablaufdatum noch nicht erreicht ist, auch dann aufbewahrt, wenn die Aufbewahrungsanzahl überschritten wurde.

Ab ONTAP 9.14.1 können Sie eine vorhandene SnapMirror Richtlinie ändern, indem Sie eine Regel hinzufügen, mit der die Langzeitaufbewahrung von Snapshots festgelegt wird. Die Regel überschreibt die standardmäßige Volume Aufbewahrungsdauer bei Nicht-SnapLock Vault- und Mirror-Vault-SnapMirror Ziel-Volumes.

1. Einer bestehenden SnapMirror Richtlinie eine Regel hinzufügen:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   Das folgende Beispiel erstellt eine Regel, die der bestehenden Richtlinie mit dem Namen „snapvault“ eine Aufbewahrungsfrist von 6 Monaten zuweist:

   ```
   snapmirror policy add-rule -vserver vs1 -policy snapvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

   Weitere Informationen zu `snapmirror policy add-rule` finden sich in der "ONTAP-Befehlsreferenz".

**Copyright-Informationen**

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

**Markeninformationen**

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.