Konfigurieren Sie SnapLock

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/snaplock/snaplock-config-overview-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren Sie SnapLock

Erfahren Sie mehr über die Konfiguration von ONTAP SnapLock

Bevor Sie SnapLock verwenden, müssen Sie SnapLock konfigurieren, indem Sie verschiedene Aufgaben durchführen, z. B. "Installieren Sie die SnapLock-Lizenz" für jeden Node, der ein Aggregat mit einem SnapLock-Volume hostet, initialisieren Sie den "Compliance-Uhr", erstellen Sie ein SnapLock-Aggregat für Cluster, auf denen ONTAP Versionen vor ONTAP 9.10.1 ausgeführt "Erstellen und Mounten eines SnapLock Volumes"werden, und mehr.

Initialisieren der ONTAP Compliance Clock

SnapLock verwendet die *Volume Compliance Clock*, um sicherzustellen, dass sich die Aufbewahrungsfrist für WORM-Dateien ändern kann. Sie müssen zuerst auf jedem Knoten, der ein SnapLock-Aggregat hostet, das *System ComplianceClock* initialisieren.

Ab ONTAP 9.14.1 können Sie die System-Compliance-Uhr initialisieren oder neu initialisieren, wenn keine SnapLock-Volumes oder keine Volumes mit aktivierter Snapshot-Sperrung vorhanden sind. Durch die Möglichkeit der Neuinitialisierung können Systemadministratoren die Compliance-Uhr des Systems in Fällen zurücksetzen, in denen sie möglicherweise falsch initialisiert wurde oder die Taktabweichung auf dem System korrigiert wurde. In ONTAP 9.13.1 und früheren Versionen können Sie die Compliance-Uhr nicht erneut initialisieren, sobald Sie die Compliance-Uhr auf einem Knoten initialisiert haben.

Bevor Sie beginnen

So initialisieren Sie die Compliance-Uhr neu:

- Alle Nodes im Cluster müssen sich in einem ordnungsgemäßen Zustand befinden.
- Alle Volumes müssen online sein.
- In der Wiederherstellungswarteschlange können keine Volumes vorhanden sein.
- Es können keine SnapLock Volumes vorhanden sein.
- Es können keine Volumes mit aktivierter Snapshot-Sperrung vorhanden sein.

Allgemeine Anforderungen für die Initialisierung der Compliance Clock:

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

Über diese Aufgabe

Die Zeit auf dem System Compliance Clock wird von der *Volume Compliance Clock* übernommen, von der Letzteres die Aufbewahrungsfrist für WORM-Dateien auf dem Volume steuert. Die Volume-Compliance-Uhr wird automatisch initialisiert, wenn Sie ein neues SnapLock-Volume erstellen.

Die anfängliche Einstellung der System-Compliance-Clock basiert auf der aktuellen Hardware-Systemuhr. Aus diesem Grund sollten Sie überprüfen, ob die Systemzeit und die Zeitzone korrekt sind, bevor Sie die System-Compliance-Uhr auf jedem Knoten initialisieren. Sobald Sie die Compliance-Uhr des Systems auf einem Node initialisiert haben, können Sie sie nicht erneut initialisieren, wenn SnapLock-Volumes oder Volumes mit aktivierter Sperrung vorhanden sind.

Schritte

Sie können die ONTAP-CLI verwenden, um die Compliance-Uhr zu initialisieren, oder Sie können ab ONTAP 9.12.1 die Compliance-Uhr mit dem System-Manager initialisieren.

System Manager

1. Navigieren Sie zu **Cluster > Übersicht**.
2. Klicken Sie im Abschnitt **Knoten** auf **SnapLock-Konformitätsuhr initialisieren**.
3. Um die Spalte **Compliance Clock** anzuzeigen und zu überprüfen, ob die Compliance Clock initialisiert ist, klicken Sie im Abschnitt **Cluster > Übersicht > Knoten** auf **Einblenden/Ausblenden** und wählen **SnapLock-Konformitätsuhr** aus.

CLI

1. Initialisieren Sie die System-Compliance-Uhr:

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

   Mit dem folgenden Befehl wird die Systemkonformität-Uhr initialisiert auf `node1`:

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

   Erfahren Sie mehr über `snaplock compliance-clock initialize` 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 diese Vorgehensweise für jeden Node, der ein SnapLock Aggregat hostet.

Aktivieren Sie die Neusynchronisierung der Compliance Clock für ein NTP-konfiguriertes System

Sie können die SnapLock Compliance Clock-Synchronisierungsfunktion aktivieren, wenn ein NTP-Server konfiguriert ist.

Bevor Sie beginnen

- Diese Funktion ist nur auf der erweiterten Berechtigungsebene verfügbar.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- "Die SnapLock-Lizenz muss auf dem Knoten installiert sein".
- Diese Funktion ist nur für Cloud Volumes ONTAP-, ONTAP Select- und VSIM-Plattformen verfügbar.

Über diese Aufgabe

Wenn der SnapLock Secure Clock Daemon eine Schräglage entdeckt, die über den Schwellenwert hinausgeht, verwendet ONTAP die Systemzeit, um die System- und Volume Compliance-Uhren zurückzusetzen. Als Schwellwert wird ein Zeitraum von 24 Stunden festgelegt. Das bedeutet, dass die System-Compliance-Uhr nur dann mit der Systemuhr synchronisiert wird, wenn die Schräglage älter als einen Tag ist.

Der SnapLock Secure Clock-Daemon erkennt einen Schräglauf und ändert die Compliance Clock in die Systemzeit. Jeder Versuch, die Systemzeit so zu ändern, dass die Compliance-Uhr mit der Systemzeit synchronisiert wird, schlägt fehl, da die Compliance-Uhr nur dann mit der Systemzeit synchronisiert wird, wenn die Systemzeit mit der NTP-Zeit synchronisiert ist.

Schritte

1. Aktivieren Sie die SnapLock Compliance Clock-Synchronisierungsfunktion, wenn ein NTP-Server konfiguriert ist:

   `snaplock compliance-clock ntp`

   Der folgende Befehl aktiviert die Synchronisierungsfunktion der Compliance Clock des Systems:

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

   Erfahren Sie mehr über `snaplock compliance-clock ntp modify` in der "ONTAP-Befehlsreferenz".

2. Bestätigen Sie bei der entsprechenden Aufforderung, dass die konfigurierten NTP-Server vertrauenswürdig sind und der Kommunikationskanal sicher ist, um die Funktion zu aktivieren:
3. Überprüfen Sie, ob die Funktion aktiviert ist:

   `snaplock compliance-clock ntp show`

   Der folgende Befehl überprüft, ob die Synchronisierungsfunktion der System-Compliance-Uhr aktiviert ist:

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

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

   Erfahren Sie mehr über `snaplock compliance-clock ntp show` in der "ONTAP-Befehlsreferenz".

Erstellen Sie ein ONTAP SnapLock -Aggregat

Sie verwenden die Volume- `-snaplock-type`Option, um einen Compliance- oder Enterprise SnapLock-Volume-Typ anzugeben. Bei älteren Versionen als ONTAP 9.10.1 müssen Sie ein separates SnapLock Aggregat erstellen. Ab ONTAP 9.10.1 können SnapLock- und nicht-SnapLock-Volumes auf demselben Aggregat vorhanden sein. Wenn Sie ONTAP 9.10.1 verwenden, sind Sie daher nicht mehr erforderlich, ein separates SnapLock Aggregat zu erstellen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Die SnapLock "Lizenz muss installiert sein"auf dem Node. Diese Lizenz ist in enthalten"ONTAP One".
- "Die Compliance Clock auf dem Knoten muss initialisiert werden".
- Wenn Sie die Festplatten mit „`root`“, „`data1`“ und „`data2`“ partitioniert haben, müssen Sie sicherstellen, dass Ersatzfestplatten verfügbar sind.

Upgrade-Überlegungen

Bei einem Upgrade auf ONTAP 9.10.1 werden vorhandene SnapLock und Aggregate anderer Anbieter aktualisiert, um sowohl SnapLock als auch nicht SnapLock Volumes zu unterstützen. Die vorhandenen SnapLock Volume-Attribute werden jedoch nicht automatisch aktualisiert. So bleiben beispielsweise Felder für Data-Compaction, Volume-übergreifende Deduplizierung und Volume-übergreifende Hintergrund-Deduplizierung unverändert. Neue SnapLock Volumes, die auf vorhandenen Aggregaten erstellt wurden, verfügen über dieselben Standardwerte wie nicht-SnapLock-Volumes, und die Standardwerte für neue Volumes und Aggregate sind plattformabhängig.

Überlegungen zurücksetzen

Wenn Sie auf eine ältere ONTAP Version als 9.10.1 zurücksetzen müssen, müssen Sie alle SnapLock-Compliance-, SnapLock Enterprise- und SnapLock-Volumes auf ihre eigenen SnapLock Aggregate verschieben.

Über diese Aufgabe

- Mit der Option SyncMirror können keine Compliance-Aggregate erstellt werden.
- Sie können gespiegelte Compliance-Aggregate in einer MetroCluster-Konfiguration nur dann erstellen, wenn das Aggregat SnapLock-Audit-Protokoll-Volumes hostet.

> In einer MetroCluster-Konfiguration wird SnapLock Enterprise auf gespiegelten und nicht gespiegelten Aggregaten unterstützt. SnapLock Compliance wird nur auf nicht gespiegelten Aggregaten unterstützt.

Schritte

1. Erstellung eines SnapLock Aggregats:

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

Mit dem folgenden Befehl wird ein SnapLock- `Compliance`Aggregat `erstellt, `aggr1` das mit drei Festplatten benannt `node1` ist:

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

Erfahren Sie mehr über `storage aggregate create` in der "ONTAP-Befehlsreferenz".

Erstellen und Mounten von ONTAP SnapLock -Volumes

Sie müssen für die Dateien oder Snapshots, die in den WORM-Status übergeben werden sollen, ein SnapLock Volume erstellen. Ab ONTAP 9.10.1 wird jedes der erstellten Volumes unabhängig vom Aggregattyp standardmäßig als nicht-SnapLock Volume erstellt. Sie müssen die `-snaplock-type` Option verwenden, um ein SnapLock-Volume explizit zu erstellen, indem Sie als SnapLock-Typ entweder Compliance oder Enterprise angeben. Standardmäßig ist der SnapLock-Typ auf eingestellt `non-snaplock`.

Bevor Sie beginnen

- Das SnapLock Aggregat muss online sein.
- Sie sollten "Vergewissern Sie sich, dass eine SnapLock-Lizenz installiert ist". Wenn auf dem Node keine SnapLock-Lizenz installiert ist, müssen Sie "Installieren"sie ausführen. Diese Lizenz ist in enthalten"ONTAP One". Vor ONTAP One war die SnapLock-Lizenz im Paket für Sicherheit und Compliance enthalten. Das Paket „Sicherheit und Compliance“ wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl derzeit nicht erforderlich, können Bestandskunden wählen"Upgrade auf ONTAP One".
- "Die Compliance Clock auf dem Knoten muss initialisiert werden".

Über diese Aufgabe

Mit den entsprechenden SnapLock Berechtigungen können Sie ein Enterprise-Volume jederzeit zerstören oder umbenennen. Sie können ein Compliance-Volumen erst zerstören, wenn der Aufbewahrungszeitraum abgelaufen ist. Ein Compliance-Volume kann nie umbenannt werden.

Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen. Das geklonte Volume hat den gleichen 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, zur Sicherung im Rahmen der SnapLock Vault-Beziehung auf ein SnapLock Volume übertragen werden. LUNs werden in SnapLock-Volumes mit Lese-/Schreibzugriff nicht unterstützt. Manipulationssichere Snapshots werden jedoch sowohl auf SnapMirror Quell-Volumes als auch auf Ziel-Volumes unterstützt, die LUNs enthalten.

Führen Sie diese Aufgabe über ONTAP System Manager oder die ONTAP-CLI aus.

System Manager

Ab ONTAP 9.12.1 können Sie mit System Manager ein SnapLock Volume erstellen.

Schritte

1. Navigieren Sie zu **Storage > Volumes** und klicken Sie auf **Hinzufügen**.
2. Klicken Sie im Fenster **Volume hinzufügen** auf **Weitere Optionen**.
3. Geben Sie die neuen Volume-Informationen ein, einschließlich Name und Größe des Volumes.
4. Wählen Sie **SnapLock aktivieren** und wählen Sie den SnapLock-Typ entweder Compliance oder Enterprise.
5. Wählen Sie im Abschnitt **Auto-Commit Files** die Option **Modified** aus und geben Sie den Zeitraum ein, in dem eine Datei unverändert bleiben soll, bevor sie automatisch aktiviert wird. Der Mindestwert beträgt 5 Minuten und der Höchstwert beträgt 10 Jahre.
6. Wählen Sie im Abschnitt **Datenspeicherung** den minimalen und maximalen Aufbewahrungszeitraum aus.
7. Wählen Sie den Standardaufbewahrungszeitraum aus.
8. Klicken Sie Auf **Speichern**.
9. Wählen Sie auf der Seite **Volumes** das neue Volume aus, um die SnapLock-Einstellungen zu überprüfen.

CLI

1. SnapLock Volume erstellen:

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

Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz". Für SnapLock-Volumes stehen folgende Optionen nicht zur Verfügung: `-nvfail`, `-atime-update`, , `-is-autobalance -eligible` `-space-mgmt-try-first` Und `vmalign`.

Mit dem folgenden Befehl wird ein SnapLock- `Compliance`Volume mit dem Namen `vol1` auf erstellt `aggr1` `vs1`:

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

Mounten Sie ein SnapLock Volume

Ein SnapLock Volume kann für den NAS-Client-Zugriff im SVM Namespace an einen Verbindungspfad gemountet werden.

Bevor Sie beginnen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

- Ein SnapLock Volume kann nur unter dem Root-Verzeichnis der SVM gemountet werden.
- Ein normales Volume kann nicht unter einem SnapLock Volume gemountet werden.

Schritte

1. Mounten eines SnapLock Volume:

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

   Erfahren Sie mehr über `volume mount` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird ein SnapLock Volume `vol1` mit dem Namen `/sales` im Verbindungspfad im `vs1` Namespace gemountet:

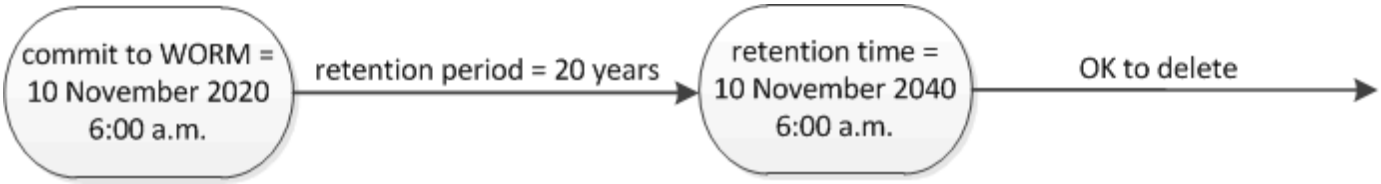
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Legen Sie die ONTAP SnapLock Aufbewahrungszeit fest

Sie können die Aufbewahrungszeit für eine Datei explizit festlegen oder den Standardaufbewahrungszeitraum für das Volume verwenden, um die Aufbewahrungszeit abzuleiten. Wenn Sie die Aufbewahrungszeit nicht explizit festlegen, verwendet SnapLock den Standardaufbewahrungszeitraum zur Berechnung der Aufbewahrungszeit. Sie können auch die Dateiaufbewahrung nach einem Ereignis festlegen.

Allgemeines zu Aufbewahrungszeitraum und Aufbewahrungszeit

Der_Aufbewahrungszeitraum_ für EINE WORM-Datei gibt die Zeitspanne an, die die Datei nach dem Festlegen des WORM-Status aufbewahrt werden muss. Die *Aufbewahrungszeit* für EINE WORM-Datei ist die Zeit, nach der die Datei nicht mehr aufbewahrt werden muss. Eine Aufbewahrungsfrist von 20 Jahren für eine Datei, die am 10. November 2020 6:00 Uhr im WORM-Zustand aufbewahrt wird, würde beispielsweise eine Aufbewahrungszeit vom 10. November 2040 6:00 Uhr erreichen



Ab ONTAP 9.10.1 können Sie eine Aufbewahrungszeit bis zum 26. Oktober 3058 und eine Aufbewahrungsfrist von bis zu 100 Jahren festlegen. Wenn Sie die Aufbewahrungszeiträume verlängern, werden ältere Richtlinien automatisch konvertiert. In ONTAP 9.9.1 und früheren Versionen, sofern Sie den Standard-Aufbewahrungszeitraum nicht auf unendlich eingestellt, ist die maximale unterstützte Aufbewahrungszeit Januar 19 2071 (GMT).

Wichtige Überlegungen zur Replizierung

Wenn Sie eine SnapMirror Beziehung mit einem SnapLock Quell-Volume unter Verwendung eines Aufbewahrungsdatums später als dem 19. Januar 2071 (GMT) aufbauen, muss das Ziel-Cluster ONTAP 9.10.1 oder höher ausführen. Sonst schlägt der SnapMirror Transfer fehl.

Wichtige Überlegungen zum Wechsel

ONTAP verhindert, dass Sie einen Cluster von ONTAP 9.10.1 auf eine frühere ONTAP -Version zurücksetzen, wenn Dateien mit einer Aufbewahrungsdauer nach „19. Januar 2071, 8:44:07 Uhr“ vorhanden sind.

Die Aufbewahrungsfristen verstehen

Ein SnapLock-Compliance- oder Enterprise-Volume hat vier Aufbewahrungszeiträume:

- Mindestaufbewahrungsdauer (`min`), mit einem Standardwert von 0
- Maximale Aufbewahrungsfrist (`max`), mit einem Verzug von 30 Jahren
- Standardaufbewahrungszeitraum, wobei der Standard `min` sowohl für den Compliance-Modus als auch für den Enterprise-Modus mit ONTAP 9.10.1 gleich ist. In älteren Versionen als ONTAP 9.10.1 von ONTAP hängt die standardmäßige Aufbewahrungsdauer von dem Modus ab:
  - Für den Compliance-Modus ist der Standardwert gleich `max` .
  - Für den Enterprise-Modus ist der Standardwert gleich `min` .
- Nicht festgelegte Aufbewahrungsdauer.

> In Versionen vor ONTAP 9.10.1 wird eine Datei im Compliance-Modus standardmäßig 30 Jahre lang aufbewahrt, wenn die Aufbewahrungszeit nicht explizit festgelegt wird, bevor sie in den WORM-Zustand versetzt wird, und wenn die Standardeinstellungen nicht geändert werden. Diese Änderung kann nicht rückgängig gemacht werden. In ähnlicher Weise wird in ONTAP 9.10.1 und späteren Versionen die Datei, wenn Sie die Aufbewahrungszeit nicht explizit festlegen, bevor Sie sie in den WORM-Zustand versetzen, und wenn Sie die Standardeinstellungen nicht ändern, 0 Jahre lang aufbewahrt, also effektiv gar nicht.

Ab ONTAP 9.8 können Sie die Aufbewahrungsfrist für Dateien in einem Volume auf `unspecified`, einstellen, damit die Datei beibehalten werden kann, bis Sie eine absolute Aufbewahrungszeit festlegen. Sie können eine Datei mit absoluter Aufbewahrungszeit auf unbestimmte Aufbewahrung und zurück zur absoluten Aufbewahrung setzen, solange die neue absolute Aufbewahrungszeit später ist als die zuvor festgelegte absolute Zeit.

Ab ONTAP 9.12.1 verfügen WORM-Dateien mit festgesetzten Aufbewahrungsfristen `unspecified` garantiert über einen Aufbewahrungszeitraum auf den für das SnapLock Volume konfigurierten Mindestaufbewahrungszeitraum. Wenn Sie die Aufbewahrungsdauer der Datei von `unspecified` in eine absolute Aufbewahrungszeit ändern, muss die neue angegebene Aufbewahrungszeit größer sein als die für die Datei bereits festgelegte Mindestaufbewahrungszeit.

Legen Sie den Standardaufbewahrungszeitraum fest

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

Bevor Sie beginnen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

In der folgenden Tabelle sind die möglichen Werte für die Option Standardaufbewahrungszeitraum aufgeführt:

Der Standardaufbewahrungszeitraum muss größer oder gleich (>=) dem Mindestaufbewahrungszeitraum und kleiner als oder gleich (<=) dem maximalen Aufbewahrungszeitraum sein.

Wert	Einheit	Hinweise
0–65535	Sekunden	
0–24	Stunden	
0–365	Tage	
0–12	Monaten	
0–100	Jahren	Ab ONTAP 9.10.1 Bei früheren Versionen von ONTAP beträgt der Wert 0 - 70.
maximale	-	Verwenden Sie den maximalen Aufbewahrungszeitraum.
Mindestens	-	Verwenden Sie den Mindestaufbewahrungszeitraum.
Skalierbar	-	Bewahren Sie die Dateien für immer auf.
Nicht angegeben	-	Bewahren Sie die Dateien so lange auf, bis ein absoluter Aufbewahrungszeitraum festgelegt ist.

Die Werte und Bereiche für die maximalen und minimalen Aufbewahrungsfristen sind identisch, mit Ausnahme von `max` und `min`, die nicht anwendbar sind. Weitere Informationen zu dieser Aufgabe finden Sie unter "Stellen Sie die Übersicht über die Aufbewahrungszeit ein".

Sie können mit dem `volume snaplock show` Befehl die Einstellungen für den Aufbewahrungszeitraum für das Volume anzeigen. Erfahren Sie mehr über `volume snaplock show` in der "ONTAP-Befehlsreferenz".

Nachdem eine Datei im WORM-Status übergeben wurde, können Sie den Aufbewahrungszeitraum verlängern, jedoch nicht verkürzen.

Schritte

1. Legen Sie den Standardaufbewahrungszeitraum für Dateien auf einem SnapLock-Volume fest:

```
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
```

Erfahren Sie mehr über `volume snaplock modify` in der "ONTAP-Befehlsreferenz".

> In den folgenden Beispielen wird davon ausgegangen, dass die minimalen und maximalen Aufbewahrungszeiträume zuvor nicht geändert wurden.

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für Compliance- oder Enterprise-Volumes auf 20 Tage festgelegt:

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

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für ein Compliance-Volume auf 70 Jahre festgelegt:

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

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für ein Enterprise-Volume auf 10 Jahre festgelegt:

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

Mit den folgenden Befehlen wird die Standardaufbewahrungsdauer für Enterprise-Volumes auf 10 Tage festgelegt:

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

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für ein Compliance-Volume auf „skalierbar“ gesetzt:

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

Legen Sie die Aufbewahrungszeit für eine Datei explizit fest

Sie können die Aufbewahrungszeit für eine Datei explizit festlegen, indem Sie die letzte Zugriffszeit ändern. Sie können jeden entsprechenden Befehl oder jedes Programm über NFS oder CIFS verwenden, um die Uhrzeit des letzten Zugriffs zu ändern.

Über diese Aufgabe

Nachdem eine Datei an WORM übergeben wurde, können Sie die Aufbewahrungszeit verlängern, aber nicht verkürzen. Die Aufbewahrungszeit wird im `atime` Feld für die Datei gespeichert.

> Sie können die Aufbewahrungszeit einer Datei nicht explizit auf einstellen `infinite`. Dieser Wert ist nur verfügbar, wenn Sie den Standardaufbewahrungszeitraum zur Berechnung der Aufbewahrungszeit verwenden.

Schritte

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

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Aufbewahrungszeit von 21. November 2020 6:00 Uhr für eine Datei mit dem Namen festzulegen `document.txt`:

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

   > Sie können alle geeigneten Befehle oder Programme verwenden, um die letzte Zugriffszeit in Windows zu ändern.

Legen Sie den Aufbewahrungszeitraum für die Datei nach einem Ereignis fest

Ab ONTAP 9.3 können Sie definieren, wie lange eine Datei nach einem Ereignis aufbewahrt wird, indem Sie die Funktion SnapLock *Event Based Retention (EBR)* verwenden.

Bevor Sie beginnen

- Sie müssen ein SnapLock-Administrator sein, um diese Aufgabe auszuführen.

  "Erstellen Sie ein SnapLock-Administratorkonto"

- Sie müssen sich mit einer sicheren Verbindung (SSH, Konsole oder ZAPI) angemeldet haben.

Über diese Aufgabe

Die Richtlinie_Event Retention_ definiert den Aufbewahrungszeitraum für die Datei nach dem Ereignis. Die Richtlinie kann auf eine einzelne Datei oder alle Dateien in einem Verzeichnis angewendet werden.

- Handelt es sich bei einer Datei nicht um EINE WORM-Datei, wird sie im IN der Richtlinie definierten Aufbewahrungszeitraum im WORM-Status versetzt.
- Wenn es sich bei einer Datei um EINE WORM-Datei oder EINE WORM-Dateien handelt, verlängert sich deren Aufbewahrungszeitraum um den in der Richtlinie definierten Aufbewahrungszeitraum.

Es können ein Compliance-Modus oder ein Enterprise-Mode Volume verwendet werden.

> EBR-Richtlinien können nicht auf Dateien angewendet werden, die sich in einer Legal Hold befinden.

Für erweiterte Verwendung siehe "Worm-Speicherung gemäß NetApp SnapLock".

Verwendung von EBR, um den Aufbewahrungszeitraum bereits vorhandener WORM-Dateien zu verlängern
EBR ist praktisch, wenn Sie den Aufbewahrungszeitraum bereits vorhandener WORM-Dateien verlängern möchten. So könnte es z. B. sein, dass Ihr Unternehmen die Richtlinie hat, W-4-Datensätze von Mitarbeitern in unveränderter Form für drei Jahre zu speichern, nachdem der Mitarbeiter eine Quellwahl geändert hat. Eine andere Unternehmensrichtlinie kann verlangen, dass W-4-Datensätze fünf Jahre nach Beendigung des Mitarbeiters aufbewahrt werden. In diesem Fall könnten Sie eine EBR-Richtlinie mit einer Aufbewahrungsfrist von fünf Jahren erstellen. Nach Beendigung des Mitarbeiters (das „`Event`“) wenden Sie die EBR-Richtlinie auf den W-4-Datensatz des Mitarbeiters an, wodurch die Aufbewahrungsfrist verlängert wird. Das ist in der Regel einfacher als die manuelle Verlängerung des Aufbewahrungszeitraums, insbesondere dann, wenn eine große Anzahl von Dateien beteiligt ist.

Schritte

1. EBR-Richtlinie erstellen:

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

   Mit dem folgenden Befehl wird die EBR-Richtlinie `employee_exit` für `vs1` mit einer Aufbewahrungsfrist von zehn Jahren erstellt:

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

2. Anwenden einer EBR-Richtlinie:

   `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 an `d1`:

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

Verwandte Informationen

- "Snaplock-Ereignisaufbewahrungsrichtlinie erstellen"
- "Snaplock-Ereignisaufbewahrung anwenden"

Erstellen Sie ein ONTAP SnapLock-geschütztes Audit-Protokoll

Bei Nutzung von ONTAP 9.9.1 oder einer älteren Version müssen Sie zunächst ein

SnapLock Aggregat erstellen und anschließend ein SnapLock geschütztes Revisionsprotokoll erstellen, bevor Sie eine privilegierte Löschung oder SnapLock-Volume-Verschiebung durchführen. Das Revisionsprotokoll erfasst die Erstellung und Löschung von SnapLock-Administratorkonten, Änderungen an dem Protokoll-Volume, die Aktivierung und das Löschen privilegierter Vorgänge sowie die Verschiebung von SnapLock Volumes.

Ab ONTAP 9.10.1 erstellen Sie kein SnapLock Aggregat mehr. Sie müssen die Option -SnapLock-type für verwenden"Explizit ein SnapLock Volume erstellen", indem Sie entweder Compliance oder Enterprise als SnapLock-Typ angeben.

Bevor Sie beginnen

Wenn Sie ONTAP 9.9.1 oder eine frühere Version verwenden, müssen Sie zum Erstellen eines SnapLock Aggregats Cluster-Administrator sein.

Über diese Aufgabe

Sie können ein Überwachungsprotokoll erst löschen, wenn der Aufbewahrungszeitraum für die Protokolldatei abgelaufen ist. Sie können ein Überwachungsprotokoll auch nach Ablauf des Aufbewahrungszeitraums nicht ändern. Dies gilt sowohl für SnapLock Compliance als auch für den Enterprise-Modus.

> In ONTAP 9.4 und früher können Sie ein SnapLock Enterprise Volume nicht zur Audit-Protokollierung verwenden. Sie müssen ein SnapLock-Compliance-Volume verwenden. In ONTAP 9.5 und höher können Sie entweder ein SnapLock Enterprise Volume oder ein SnapLock Compliance Volume zur Audit-Protokollierung verwenden. In allen Fällen muss das Audit-Log-Volume am Verbindungspfad gemountet werden `/snaplock_audit_log`. Kein anderes Volume kann diesen Verbindungspfad verwenden.

Sie finden die SnapLock-Prüfprotokolle im `/snaplock_log` Verzeichnis unter dem Stammverzeichnis des Audit-Log-Volumes, in Unterverzeichnissen mit den Namen `privdel_log` (privilegierte Löschvorgänge) und `system_log` (alles andere). Die Namen von Audit-Log-Dateien enthalten den Zeitstempel der ersten protokollierten Operation und erleichtern so die Suche nach Datensätzen bis zu dem Zeitpunkt, zu dem die Vorgänge durchgeführt wurden.

- Sie können den `snaplock log file show` Befehl verwenden, um die Protokolldateien auf dem Überwachungsprotokoll-Volume anzuzeigen.
- Sie können den `snaplock log file archive` Befehl verwenden, um die aktuelle Protokolldatei zu archivieren und eine neue zu erstellen, was in Fällen nützlich ist, in denen Sie Überwachungsprotokollinformationen in einer separaten Datei aufzeichnen müssen.

Erfahren Sie mehr über `snaplock log file show` und `snaplock log file archive` in der "ONTAP-Befehlsreferenz".

> Ein Datensicherungs-Volume kann nicht als SnapLock-Audit-Protokoll-Volume verwendet werden.

Schritte

1. Erstellen Sie ein SnapLock Aggregat.

   Erstellen Sie ein SnapLock Aggregat

2. Erstellen Sie für die SVM, die Sie für die Audit-Protokollierung konfigurieren möchten, ein SnapLock

Volume.

SnapLock Volume erstellen

3. SVM für Audit-Protokollierung konfigurieren:

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

> Die Mindestaufbewahrungsdauer für Audit-Log-Dateien beträgt sechs Monate. Wenn die Aufbewahrungsfrist einer betroffenen Datei länger als die Aufbewahrungsfrist des Prüfprotokolls ist, erbt die Aufbewahrungsfrist des Protokolls die Aufbewahrungsfrist der Datei. Wenn also die Aufbewahrungsfrist für eine mit privilegierter Löschung gelöschte Datei 10 Monate beträgt und die Aufbewahrungsdauer des Prüfprotokolls 8 Monate beträgt, verlängert sich die Aufbewahrungsfrist des Protokolls auf 10 Monate. Weitere Informationen zur Aufbewahrungszeit und zum Standardaufbewahrungszeitraum finden Sie unter "Aufbewahrungszeit einstellen".

Mit dem folgenden Befehl wird `SVM1` die Audit-Protokollierung mit dem SnapLock-Volume konfiguriert `logVol`. Das Prüfprotokoll 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
```

Erfahren Sie mehr über `snaplock log create` in der "ONTAP-Befehlsreferenz".

4. Mounten Sie auf der für die Audit-Protokollierung konfigurierten SVM das SnapLock-Volume im Verbindungspfad `/snaplock_audit_log`.

Mounten Sie ein SnapLock Volume

Überprüfen der ONTAP SnapLock -Einstellungen

Mit den `volume file fingerprint start` `volume file fingerprint dump` Befehlen und lassen sich wichtige Informationen über Dateien und Volumes einschließlich des Dateityps (normal, WORM oder WORM ANZEIGEFÄHIG), des Ablaufdatums des Volumes und so weiter anzeigen.

Schritte

1. Generieren eines Dateiprints:

```
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 Session ID, die Sie als Eingabe für den `volume file fingerprint dump` Befehl verwenden können.

> Sie können den `volume file fingerprint show` Befehl mit dem Session ID verwenden, um den Fortschritt des Fingerabdruckvorgangs zu überwachen. Vergewissern Sie sich, dass der Vorgang abgeschlossen ist, bevor Sie versuchen, den Fingerabdruck anzuzeigen.

2. Zeigen Sie den Fingerabdruck für die Datei an:

   `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
```

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.