SnapLock konfigurieren

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/snaplock/snaplock-config-overview-concept.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

SnapLock konfigurieren . . . 1
ONTAP SnapLock Konfigurationsworkflow . . . 1
Initialisierung der ONTAP SnapLock Compliance Clock . . . 1
Compliance Clock-Resynchronisierung für ein NTP-konfiguriertes System aktivieren . . . 2
Ein ONTAP SnapLock Aggregat erstellen . . . 4
ONTAP SnapLock Volumes erstellen und einbinden . . . 5
Ein SnapLock Volume einbinden . . . 6
Die ONTAP SnapLock Aufbewahrungszeit festlegen . . . 7
Standardaufbewahrungsdauer festlegen . . . 8
Die Aufbewahrungszeit für eine Datei explizit festlegen . . . 10
Die Aufbewahrungsfrist für Dateien nach einem Ereignis festlegen . . . 11
Ein ONTAP SnapLock-geschütztes Revisionsprotokoll erstellen . . . 12
ONTAP SnapLock Einstellungen überprüfen . . . 14

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	

Wert	Einheit	Hinweise
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.
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. 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
```

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.