Konfigurieren Sie SnapLock

ONTAP 9

NetApp
March 24, 2023

Inhaltsverzeichnis

Konfigurieren Sie SnapLock

Konfigurieren Sie SnapLock

Bevor Sie SnapLock verwenden, müssen Sie SnapLock konfigurieren, indem Sie verschiedene Aufgaben ausführen, wie z. B. die Installation der SnapLock-Lizenz, die Initialisierung der Compliance-Uhr, die Erstellung eines SnapLock-Aggregats und mehr.

Installieren Sie die Lizenz

Eine SnapLock Lizenz berechtigt Sie sowohl zum SnapLock-Compliance-Modus als auch zum SnapLock-Enterprise-Modus. SnapLock-Lizenzen werden auf Node-Basis ausgestellt. Sie müssen eine Lizenz für jeden Node installieren, der ein SnapLock Aggregat hostet.

Weitere Informationen zum Compliance-Modus und zum Enterprise-Modus finden Sie unter "Was ist SnapLock".

Was Sie benötigen

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

Über diese Aufgabe

Sie sollten die SnapLock Lizenzschlüssel von Ihrem Vertriebsrepräsentant erhalten haben.

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

System Manager

1. Navigieren Sie zu **Cluster > Einstellungen > Lizenzen > Lizenz hinzufügen**.
2. Klicken Sie Auf **+Hinzufügen**.
3. Klicken Sie auf **Durchsuchen** und suchen Sie die NetApp Lizenzdatei.
4. Klicken Sie Auf **Hinzufügen**.

CLI

1. Installieren Sie die SnapLock Lizenz für einen Node:

   `system license add -license-code` *`license_key`*

   Mit dem folgenden Befehl wird die Lizenz mit dem Schlüssel installiert `AAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

   ```
   cluster1::> system license add -license-code
   AAAAAAAAAAAAAAAAAAAAAAAAAAAA
   ```

2. Wiederholen Sie den vorherigen Schritt für jede Node-Lizenz.

Initialisieren Sie die ComplianceClock

Die SnapLock ComplianceClock sorgt für Manipulationen, die die Aufbewahrungsfrist für WORM-Dateien ändern können. Sie müssen auf jedem Knoten, der ein SnapLock-Aggregat hostet, die ComplexClock *System ComplianceClock* initialisieren. Sobald Sie die ComplexClock auf einem Knoten initialisiert haben, können Sie sie nicht erneut initialisieren.

Was Sie benötigen

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

Über diese Aufgabe

Die Zeit auf dem System ComplexanceClock wird durch das *Volume ComplexanceClock* geerbt, welches die Aufbewahrungsfrist für WORM-Dateien auf dem Volume steuert. Der Datenträger ComplexanceClock wird automatisch initialisiert, wenn Sie ein neues SnapLock Volume erstellen.

> Die Ersteinstellung der ComplexanceClock basiert auf der aktuellen Systemuhr. Aus diesem Grund sollten Sie überprüfen, ob die Systemzeit und die Zeitzone korrekt sind, bevor Sie die ComplianceClock initialisieren. Sobald Sie die ComplexClock auf einem Knoten initialisiert haben, können Sie sie nicht erneut initialisieren.

System Manager

Ab ONTAP 9.12.1 können Sie mit System Manager die SnapLock-Compliance-Uhr initialisieren.

Schritte

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 **ein-/Ausblenden** und wählen Sie **SnapLock Compliance Clock**.

CLI

1. Initialisieren Sie das System ComplianceClock:

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

   Mit dem folgenden Befehl wird das System ComplianceClock ON initialisiert `node1`:

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

2. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass die Systemuhr korrekt ist und Sie die ComplianceClock 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 Resynchronisierung der ComplianceClock-Synchronisierung für ein NTP-konfiguriertes System

Wenn ein NTP-Server konfiguriert ist, können Sie die SnapLock CommianceClock-Zeitsynchronisation aktivieren.

Was Sie benötigen

- 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 Node 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 über den Schwellenwert hinaus erkennt, verwendet ONTAP die Systemzeit, um sowohl das System als auch die Complexe des Volumes zurückzusetzen. Als Schwellwert wird ein Zeitraum von 24 Stunden festgelegt. Das bedeutet, dass das System ComplexClock nur dann mit der Systemuhr synchronisiert wird, wenn die Skew mehr als einen Tag alt ist.

Der SnapLock Secure Clock Daemon erkennt eine Schräglage und ändert die ComplexanceClock in die Systemzeit. Jeder Versuch, die Systemzeit zu ändern, um die ComplexceClock zu zwingen, mit der Systemzeit zu synchronisieren, schlägt fehl, da die CommianceClock nur dann mit der Systemzeit synchronisiert wird, wenn die Systemzeit mit der NTP-Zeit synchronisiert wird.

Schritte

1. Aktivieren Sie die SnapLock ComplianceClock-Zeitsynchronisierung, wenn ein NTP-Server konfiguriert ist:

   `snaplock compliance-clock ntp`

   Mit dem folgenden Befehl wird die Systemfunktion CommianceClock Time synchronisiert:

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

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`

   Mit dem folgenden Befehl wird überprüft, ob die Funktion zur Synchronisierung der Systemzeit CommianceClock aktiviert ist:

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

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

Erstellen Sie ein SnapLock Aggregat

Sie verwenden die Lautstärke `-snaplock-type` Option zum Festlegen eines Volume-Typs für Compliance oder Enterprise SnapLock. 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.

Was Sie benötigen

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

- Die SnapLock-Lizenz muss auf dem Node installiert sein.
- Die ComlianceClock 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

- Sie können keine Compliance-Aggregate für FlexArray LUNs erstellen, doch SnapLock-Compliance-Aggregate werden mit FlexArray LUNs unterstützt.
- 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`

   Die man-Page für den Befehl enthält eine vollständige Liste der Optionen.

   Mit dem folgenden Befehl wird eine SnapLock erstellt `Compliance` Aggregat mit dem Namen `aggr1` Mit drei Festplatten auf `node1`:

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

SnapLock Volumes erstellen und mounten

Sie müssen ein SnapLock-Volume für die Dateien oder Snapshot-Kopien erstellen, die

Sie in DEN WORM-Zustand versetzen möchten. Ab ONTAP 9.10.1 wird jedes der erstellten Volumes unabhängig vom Aggregattyp standardmäßig als nicht-SnapLock Volume erstellt. Sie müssen den verwenden `-snaplock-type` Option zum explizit Erstellen eines SnapLock-Volumes, indem entweder Compliance oder Enterprise als SnapLock-Typ angegeben werden. Standardmäßig ist der SnapLock-Typ auf festgelegt `non-snaplock`.

Was Sie benötigen

- Das SnapLock Aggregat muss online sein.
- Die SnapLock-Lizenz muss auf dem Node installiert sein.
- Die ComlianceClock 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 auf SnapLock Volumes nicht unterstützt. Obwohl es möglich ist, LUNs mithilfe älterer Technologie auf ein SnapLock Volume zu verschieben, ist dies kein unterstützter Vorgang und auch kein anderer Vorgang, der LUNs auf einem SnapLock Volume betrifft.

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`

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl. Die folgenden Optionen sind für SnapLock Volumes nicht verfügbar: `-nvfail`, `-atime-update`, `-is -autobalance-eligible`, `-space-mgmt-try-first`, und `vmalign`.

   Mit dem folgenden Befehl wird eine SnapLock erstellt `Compliance` Volume mit Namen `vol1` Ein `aggr1` Ein `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.

Was Sie benötigen

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*`

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

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

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

Aufbewahrungszeit einstellen

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 es Dateien mit einer Aufbewahrungsfrist später als „Januar 19, 2071 8:44:07“ gibt.

Allgemeines zu den Standardaufbewahrungszeiten

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

- Mindestaufbewahrungszeitraum (`min`), mit einem Standardwert von 0
- Maximale Aufbewahrungsfrist (`max`), mit einem Standardwert von 30 Jahren
- Standardaufbewahrungszeitraum: Standardmäßig ist dieser Wert identisch `min` Sowohl im Compliance-Modus als auch im Enterprise-Modus ab ONTAP 9.10.1. In älteren Versionen als ONTAP 9.10.1 von ONTAP hängt die standardmäßige Aufbewahrungsdauer von dem Modus ab:
  - Für den Compliance-Modus ist die Standardeinstellung gleich `max`.
  - Im Enterprise-Modus ist die Standardeinstellung gleich `min`.
- Nicht festgelegte Aufbewahrungsdauer.

  Ab ONTAP 9.8 können Sie die Aufbewahrungsfrist für Dateien in einem Volume auf einstellen `unspecified`, Um die Datei so lange zu speichern, bis Sie eine absolute Aufbewahrungszeit festgelegt haben. 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 SIND WORM-Dateien, deren Aufbewahrungszeitraum auf festgelegt ist `unspecified` Sie haben für das SnapLock Volume eine Aufbewahrungsfrist festgelegt, die auf der für das Mindestaufbewahrungszeitraum konfiguriert ist. Wenn Sie den Aufbewahrungszeitraum für die Datei von ändern `unspecified` Um eine absolute Aufbewahrungszeit zu erreichen, muss die angegebene neue Aufbewahrungszeit größer sein als die für die Datei bereits festgelegte Mindestaufbewahrungszeit.

Wenn Sie also die Aufbewahrungszeit nicht explizit festlegen, bevor Sie eine Compliance-Modus-Datei in DEN WORM-Status überführen, und Sie die Standardeinstellungen nicht ändern, wird die Datei 30 Jahre lang aufbewahrt. Gleiches gilt, wenn Sie die Aufbewahrungszeit nicht explizit festlegen, bevor Sie eine Enterprise-Modus-Datei in DEN WORM-Status überführen, und Sie die Standardeinstellungen nicht ändern, wird die Datei 0 Jahre lang aufbewahrt oder, effektiv, überhaupt nicht.

Legen Sie den Standardaufbewahrungszeitraum fest

Sie können das verwenden `volume snaplock modify` Befehl zum Festlegen des Standardaufbewahrungszeitraums für Dateien auf einem SnapLock Volume

Was Sie benötigen

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 bis 65535	Sekunden	
0 bis 24	Stunden	
0 bis 365	Tage	
0 bis 12	Monaten	
0 bis 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 maximale und minimale Aufbewahrungsdauer 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 das verwenden `volume snaplock show` Befehl zum Anzeigen der Einstellungen für den Aufbewahrungszeitraum für das Volume. Weitere Informationen finden Sie auf der man-Page für den Befehl.

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*

   Eine vollständige Liste der Optionen finden Sie auf der man-Page für den Befehl.

   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 gespeichert `atime` Feld für die Datei.

Sie können die Aufbewahrungszeit einer Datei nicht explizit auf festlegen `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 vom 21. November 2020 6:00 Uhr festzulegen In einer Datei mit dem Namen `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.

Was Sie benötigen

- 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.

Weitere Informationen zur erweiterten Verwendung finden Sie unter "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 erstellt `employee_exit` Ein `vs1` Mit einer Aufbewahrungsfrist von zehn Jahren:

   ```
   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 an `employee_exit` Ein `vs1` Zu allen Dateien im Verzeichnis `d1`:

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

Erstellen eines Prüfprotokolls

Sie müssen ein SnapLock-geschütztes Prüfprotokoll erstellen, bevor Sie ein privilegiertes Löschen 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.

Was Sie benötigen

Zum Erstellen eines SnapLock Aggregats müssen Sie ein 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 Protokoll-Volume am Verbindungspfad angehängt werden `/snaplock_audit_log`. Kein anderes Volume kann diesen Verbindungspfad verwenden.

Die SnapLock-Prüfprotokolle finden Sie im `/snaplock_log` Verzeichnis unter dem Stammverzeichnis des Audit-Log-Volumes, in Unterverzeichnissen mit 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 das verwenden `snaplock log file show` Befehl zum Anzeigen der Protokolldateien auf dem Audit-Protokoll-Volume.
- Sie können das verwenden `snaplock log file archive` Befehl, um die aktuelle Protokolldatei zu archivieren und eine neue zu erstellen, was in Fällen nützlich ist, in denen Audit-Log-Informationen in einer separaten Datei aufgezeichnet werden müssen.

Weitere Informationen finden Sie auf den man-Pages für die Befehle.

> 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-file -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".

Die Konfiguration mit dem folgenden Befehl wird konfiguriert `SVM1` Für die Audit-Protokollierung mit dem SnapLock Volume `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-file-size
20GB -retention-period 8months
```

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

   Mounten Sie ein SnapLock Volume

Überprüfen Sie die SnapLock-Einstellungen

Sie können das verwenden `volume file fingerprint start` Und `volume file fingerprint dump` Befehle, um wichtige Informationen zu Dateien und Volumes anzuzeigen, einschließlich Dateityp (regulär, WORM oder WORM appensible), Ablaufdatum des Volumes usw.

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 Eingaben in den verwenden können `volume file fingerprint dump` Befehl.

   > Sie können das verwenden `volume file fingerprint show` Befehl mit der Session-ID zum Überwachen des Fortschritts des Fingerabdruckvorgangs. 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
```