MANAGEN von WORM-Dateien

ONTAP 9

NetApp
March 21, 2023

Inhaltsverzeichnis

MANAGEN von WORM-Dateien

MANAGEN von WORM-Dateien

ES gibt folgende Möglichkeiten, WORM-Dateien zu verwalten:

- "Übertragung von Dateien an DIE WORM-Funktion"
- "Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel"
- "SPIEGELN VON WORM-Dateien für das Disaster Recovery"
- "Aufbewahrung VON WORM-Dateien bei Gerichtsverfahren"
- "LÖSCHEN SIE WORM-Dateien"

Übertragung von Dateien an DIE WORM-Funktion

Dateien können entweder manuell oder automatisch in DEN WORM-Modus verschoben werden (einmal schreiben, viele lesen). Sie können auch ANGEHÄNGBARE WORM-Dateien erstellen.

Manuelles Versetzen von Dateien in DIE WORM-FUNKTION

Sie übergeben eine Datei manuell in WORM, indem Sie die Datei schreibgeschützt machen. Sie können jeden geeigneten Befehl oder jedes Programm über NFS oder CIFS verwenden, um das Lese-/Schreibattribut einer Datei in schreibgeschützt zu ändern. Sie können Dateien manuell übergeben, wenn Sie sicherstellen möchten, dass eine Anwendung das Schreiben in eine Datei abgeschlossen hat, damit die Datei nicht vorzeitig beendet wird oder wenn aufgrund einer hohen Anzahl von Volumes Skalierungsprobleme für den Autocommit-Scanner auftreten.

Was Sie benötigen

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

Über diese Aufgabe

Der Band ComplexanceClock Time wird in geschrieben `ctime` Feld der Datei, wenn der Befehl oder das Programm ausgeführt wird. Die ComlianceClock-Zeit bestimmt, wann die Aufbewahrungszeit für die Datei erreicht wurde.

Schritte

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

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Datei mit dem Namen zu erstellen `document.txt` Schreibgeschützt:

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

   Verwenden Sie in einer Windows-Shell den folgenden Befehl, um eine Datei mit dem Namen zu erstellen

`document.txt` Schreibgeschützt:

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

Automatisches Versetzen von Dateien in DIE WORM-FUNKTION

Mit der Funktion für automatische Verschiebungsfunktion von SnapLock können Sie Dateien automatisch in DIE WORM-FUNKTION übertragen. Die Funktion Autocommit begeht eine Datei in DEN WORM-Status auf einem SnapLock Volume, wenn sich die Datei während der Dauer des automatischen Commit-Zeitraums nicht geändert hat. Die Funktion Autocommit ist standardmäßig deaktiviert.

Was Sie benötigen

- Die Dateien, die automatisch übertragen werden sollen, müssen auf einem SnapLock-Volume gespeichert sein.
- Das SnapLock Volume muss online sein.
- Das SnapLock Volume muss ein Lese- und Schreib-Volume sein.

Die Funktion Autocommit von SnapLock scannt alle Dateien auf dem Volume und begeht eine Datei, wenn sie die Anforderung für automatische Übertragung erfüllt. Es kann ein Zeitintervall zwischen dem Zeitpunkt geben, in dem die Datei für die automatische Übergabe bereit ist und dem SnapLock-Lesegerät für die automatische Übertragung tatsächlich gesetzt wird. Die Datei ist jedoch weiterhin vor Änderungen und Löschung durch das Dateisystem geschützt, sobald sie für die automatische Übertragung geeignet ist.

Über diese Aufgabe

Der Zeitraum *autocommit* gibt an, wie lange Dateien vor der automatischen Übergabe unverändert bleiben müssen. Durch Ändern einer Datei vor Ablauf des automatischen Verschiebungszeitraums wird der Zeitraum für die automatische Übertragung der Datei neu gestartet.

In der folgenden Tabelle sind die möglichen Werte für den automatischen Commit-Zeitraum aufgeführt:

Wert	Einheit	Hinweise
Keine	-	Der Standardwert.
5 - 5256000	Minuten	-
1 - 87600	Stunden	-
1 - 3650	Tage	-
1 - 120	Monaten	-
1 - 10	Jahren	-

Der Mindestwert beträgt 5 Minuten und der Höchstwert beträgt 10 Jahre.

Schritte

1. Automatisches Versetzen von Dateien auf einem SnapLock Volume in DIE WORM-FUNKTION:

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

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

   Mit dem folgenden Befehl werden die Dateien auf dem Volume automatisch festgeschrieben `vol1` Der SVM vs1, sofern die Dateien 5 Stunden lang unverändert bleiben:

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

ERSTELLEN einer ANGEHÄNGBAREN WORM-Datei

In einer ANGEHÄNGBAREN WORM-Datei werden die Daten, die inkrementell geschrieben werden, wie Protokolleinträge. Sie können einen beliebigen geeigneten Befehl oder ein geeignetes Programm verwenden, um eine WORM-Datei zu erstellen, oder Sie können die Funktion SnapLock_Volume append Mode_ verwenden, um STANDARDMÄSSIG WORM-Dateien zu erstellen.

Verwenden Sie einen Befehl oder ein Programm, um eine WORM-Datei zu erstellen

Sie können jeden entsprechenden Befehl oder Programm über NFS oder CIFS verwenden, um eine WORM-Datei zu erstellen. In einer ANGEHÄNGBAREN WORM-Datei werden die Daten, die inkrementell geschrieben werden, wie Protokolleinträge. Die Daten werden in 256-KB-Blöcken an die Datei angehängt. Wenn jeder Datenblock geschrieben wird, wird der vorherige Datenblock ALS WORM-geschützt. Sie können die Datei erst löschen, wenn der Aufbewahrungszeitraum abgelaufen ist.

Was Sie benötigen

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

Über diese Aufgabe

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

Schritte

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

   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 Null-Länge `document.txt`:

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

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

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Datei mit dem Namen zu erstellen

`document.txt` Schreibgeschützt:

```
chmod 444 document.txt
```

3. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um das Lese-Schreib-Attribut der Datei wieder in beschreibbar zu ändern.

   Dieser Schritt gilt nicht als Compliance-Risiko, da sich keine Daten in der Datei befinden.

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Datei mit dem Namen zu erstellen `document.txt` Beschreibbar:

   ```
   chmod 777 document.txt
   ```

4. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um mit dem Schreiben von Daten in die Datei zu beginnen.

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um Daten in zu schreiben `document.txt`:

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

   Ändern Sie die Dateiberechtigungen zurück in den schreibgeschützten Bereich, wenn Sie keine Daten mehr an die Datei anhängen müssen.

Verwenden Sie den Volume Appendable-Modus, um WORM-Dateien zu erstellen

Ab ONTAP 9.3 können Sie MIT der Funktion SnapLock_Volume Append Mode_ (VAM) STANDARDMÄSSIG WORM-Dateien erstellen. In einer ANGEHÄNGBAREN WORM-Datei werden die Daten, die inkrementell geschrieben werden, wie Protokolleinträge. Die Daten werden in 256-KB-Blöcken an die Datei angehängt. Wenn jeder Datenblock geschrieben wird, wird der vorherige Datenblock ALS WORM-geschützt. Sie können die Datei erst löschen, wenn der Aufbewahrungszeitraum abgelaufen ist.

Was Sie benötigen

- Die angehängbare WORM-Datei muss sich auf einem SnapLock Volume befinden.
- Das SnapLock Volume muss abgehängt und leer werden, ohne dass Snapshot Kopien und vom Benutzer erstellte Dateien enthalten sind.

Über diese Aufgabe

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

Wenn Sie einen automatischen Commit-Zeitraum für das Volume angeben, werden WORM-Dateien, die für einen Zeitraum größer als der automatische Verschiebungszeitraum nicht geändert werden, in DEN WORM-CODE übernommen.

VAM wird auf SnapLock-Audit-Protokoll-Volumes nicht unterstützt.

Schritte

1. VAM aktivieren:

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

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

   Mit dem folgenden Befehl wird VAM auf dem Volume aktiviert `vol1` Der SVM`vs1`:

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

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

   Die Dateien sind standardmäßig WORM-appensible.

Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel

Mit SnapLock für SnapVault können Snapshot Kopien IM Sekundärspeicher GESICHERT WERDEN. Sie führen alle grundlegenden SnapLock-Aufgaben auf dem SnapVault Ziel aus. Das Ziel-Volume wird automatisch schreibgeschützt gemountet, sodass die Snapshot Kopien nicht explizit in WORM festgeschrieben werden müssen. Somit werden geplante Snapshot Kopien auf dem Ziel-Volume mithilfe von SnapMirror Richtlinien nicht unterstützt.

Bevor Sie beginnen

- Der Quell-Cluster muss ONTAP 8.2.2 oder höher ausführen.
- Die Quell- und Zielaggregate müssen 64 Bit sein.
- Das Quell-Volume kann kein SnapLock Volume sein.
- Die Quell- und Ziel-Volumes müssen in Peering-Clustern mit Peering SVMs erstellt werden.

  Weitere Informationen finden Sie unter "Cluster-Peering".

- Wenn Autogrow-Volume deaktiviert ist, muss der freie Speicherplatz auf dem Ziel-Volume mindestens fünf Prozent mehr als der verwendete Speicherplatz auf dem Quell-Volume sein.

Über diese Aufgabe

Das Quell-Volume kann Storage von NetApp oder anderen Herstellern verwenden. Für Storage anderer Anbieter als NetApp müssen Sie die FlexArray-Virtualisierung verwenden.

Sie können eine Snapshot Kopie, die im WORM-Status übergeben ist, nicht umbenennen.

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

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. Ab ONTAP 9.9 werden LUNs auf einem SnapLock Volume in SnapLock *nur* für SnapVault Beziehungen unterstützt, bei denen eine Snapshot Kopie eines nicht-SnapLock Quell-Volume repliziert und an einem SnapLock Ziel gesperrt wird. Diese Snapshot Kopien können LUNs enthalten.

Bei MetroCluster Konfigurationen sollten Sie die folgenden Aspekte beachten:

- Sie können eine SnapVault-Beziehung nur zwischen den synchronen Quell-SVMs und nicht zwischen einer SVM mit Sync-Source-Synchronisierung und einer SVM erstellen.
- Sie können eine SnapVault-Beziehung von einem Volume auf einer Quell-SVM zu einer datenServing-SVM erstellen.
- Es ist möglich, eine SnapVault-Beziehung zwischen einem Volume auf einer Datenservice-SVM und einem DP-Volume auf einer SVM mit synchronem Quell-Volume zu erstellen.

Die folgende Abbildung zeigt das Verfahren zur Initialisierung einer SnapVault Beziehung:

Schritte

1. Ermitteln des Ziel-Clusters
2. Installieren Sie auf dem Ziel-Cluster die SnapLock Lizenz, initialisieren Sie die ComplianceClock und erstellen Sie, wenn Sie eine ONTAP Version vor 9.10.1 verwenden, ein SnapLock-Aggregat, wie in beschrieben SnapLock-Workflow.
3. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Ziel-Volume des Typs `DP` Das ist entweder die gleiche oder größer als das Quellvolumen:

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

   Ab ONTAP 9.10.1 können SnapLock- und nicht-SnapLock-Volumes auf demselben Aggregat vorhanden sein. Wenn Sie ONTAP 9.10.1 verwenden, sind Sie daher nicht mehr erforderlich, ein separates SnapLock Aggregat zu erstellen. Mithilfe der Option Volume -snaplock-TYPE können Sie einen Compliance- oder Enterprise SnapLock Volume-Typ festlegen. Bei älteren Versionen als ONTAP ONTAP 9.10.1 wird der SnapLock-Modus, Compliance oder Enterprise, vom Aggregat übernommen. Versionsflexible Ziel-Volumes werden nicht unterstützt. Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

   Mit dem folgenden Befehl wird eine 2-GB-SnapLock erstellt `Compliance` Volume mit Namen `dstvolB` In `SVM2` Auf dem Aggregat `node01_aggr`:

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

4. Legen Sie auf dem Ziel-Cluster den Standardaufbewahrungszeitraum fest, wie in beschrieben Legen Sie den Standardaufbewahrungszeitraum fest.

Einem SnapLock-Volume, das ein Vault-Ziel ist, ist ein Standardaufbewahrungszeitraum zugewiesen. Der Wert für diesen Zeitraum wird zunächst auf mindestens 0 Jahre für SnapLock Enterprise Volumes und maximal 30 Jahre für SnapLock Compliance Volumes festgelegt. Jede NetApp Snapshot-Kopie wird zunächst mit diesem standardmäßigen Aufbewahrungszeitraum festgelegt. Die Aufbewahrungsfrist kann bei Bedarf später verlängert werden. Weitere Informationen finden Sie unter Aufbewahrungszeit einstellen.

5. Erstellen einer neuen Replikationsbeziehung Zwischen der nicht-SnapLock-Quelle und dem neuen SnapLock-Ziel, den Sie in Schritt 3 erstellt haben.

   Dieses Beispiel erstellt eine neue SnapMirror Beziehung mit dem Ziel-SnapLock Volume `dstvolB` Verwenden einer Richtlinie von `XDPDefault` So speichern Sie Snapshot-Kopien, die täglich und wöchentlich nach einem stündlichen Zeitplan gekennzeichnet sind:

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

   Erstellen Sie eine benutzerdefinierte Replikationsrichtlinie Oder A Benutzerdefinierter Zeitplan Wenn die verfügbaren Standardeinstellungen nicht geeignet sind.

6. Initialisieren Sie auf der Ziel-SVM die SnapVault-Beziehung, die in Schritt 5 erstellt wurde:

   `snapmirror initialize -destination-path` *`destination_path`*

   Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume initialisiert `srcvolA` Ein `SVM1` Und dem Ziel-Volume `dstvolB` Ein `SVM2`:

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

7. Nachdem die Beziehung initialisiert und inaktiv ist, verwenden Sie den `snapshot show` Befehl auf dem Ziel, um zu überprüfen, ob die SnapLock-Ablaufzeit auf die replizierten Snapshot Kopien angewendet wurde.

   Dieses Beispiel führt die Snapshot Kopien auf dem Volume auf `dstvolB` Die über das SnapMirror-Etikett und das SnapLock-Ablaufdatum verfügen:

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

Verwandte Informationen

"Cluster- und SVM-Peering"

"Volume Backup mit SnapVault"

SPIEGELN VON WORM-Dateien für das Disaster Recovery

AUSSERDEM KÖNNEN WORM-Dateien zur Disaster Recovery und zu anderen Zwecken an einem anderen geografischen Standort repliziert werden. Das Quell-Volume und das Ziel-Volume müssen für SnapLock konfiguriert werden. Dabei müssen beide Volumes denselben SnapLock-Modus, dieselbe Konformität oder ein Enterprise aufweisen. Alle wichtigen SnapLock Eigenschaften des Volume und der Dateien werden repliziert.

Voraussetzungen

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

Über diese Aufgabe

- Ab ONTAP 9.5 können Sie WORM-Dateien mit dem XDP-Typ (erweiterte Datensicherung) SnapMirror Beziehung replizieren, anstatt die DP-Beziehung (Datenschutz) zu verwenden. XDP-Modus ist unabhängig von der ONTAP-Version und ist in der Lage, Dateien im selben Block zu differenzieren, was die Resynchronisierung replizierter Compliance-Modus-Volumes erheblich erleichtert. Informationen zum Konvertieren einer bestehenden DP-Typ-Beziehung in eine XDP-Beziehung finden Sie unter "Datensicherung".
- Resync-Vorgang auf einer DP-Typ SnapMirror-Beziehung schlägt für ein Compliance-Modus-Volume fehl, wenn SnapLock feststellt, dass es zu einem Datenverlust führt. Falls ein Resynchronisierungsvorgang fehlschlägt, können Sie das verwenden `volume clone create` Befehl, um einen Klon des Ziel-Volume zu erstellen. Sie können dann das Quell-Volume mit dem Klon neu synchronisieren.
- Eine SnapMirror-Beziehung des Typs XDP zwischen SnapLock-konformen Volumes unterstützt eine Resynchronisierung nach einer Pause, auch wenn Daten auf dem Ziel von der Quelle nach der Pause umgeleitet wurden.

  Wenn bei einer Resynchronisierung Datendivergenz zwischen der Quelle, dem Ziel über den gemeinsamen Snapshot hinaus erkannt wird, wird ein neuer Snapshot auf das Ziel geschnitten, um diese Divergenz zu erfassen. Der neue Snapshot und der gemeinsame Snapshot sind mit einer Aufbewahrungszeit wie folgt gesperrt:

  - Die Verfallszeit des Zieldatums
  - Wenn die Ablaufzeit des Datenträgers in der Vergangenheit liegt oder noch nicht eingestellt wurde, wird der Snapshot für einen Zeitraum von 30 Tagen gesperrt
  - Wenn das Ziel gesetzliche Aufbewahrungspflichten hat, wird die tatsächliche Verfallszeit des Volumens maskiert und zeigt sich als ‘undefined’ an, der Snapshot ist jedoch für die Dauer des tatsächlichen Verfallszeitraums des Volumens gesperrt.

Wenn das Ziellaufwerk eine Ablauffrist hat, die später als das Quellvolumen ist, wird die Gültigkeitsdauer des Zieldatums beibehalten und wird nach der Resynchronisierung nicht durch den Ablaufzeitraum des Quellvolumens überschrieben.

Wenn auf dem Ziel gesetzliche Aufbewahrungspflichten liegen, die sich von der Quelle unterscheiden, ist eine Resynchronisierung nicht zulässig. Quelle und Ziel müssen identische gesetzlichen Aufbewahrungspflichten haben oder alle gesetzlichen Aufbewahrungspflichten auf dem Ziel müssen vor Beginn einer Neusynchronisierung freigegeben werden.

Eine gesperrte Snapshot Kopie auf dem Ziel-Volume, das zum Erfassen der divergenten Daten erstellt wurde, kann mithilfe der CLI auf die Quelle kopiert werden `snapmirror update -s snapshot` Befehl. Der nach

dem Kopieren kopierte Snapshot wird weiterhin an der Quelle gesperrt.

- SVM-Datensicherungsbeziehungen werden nicht unterstützt.
- Beziehungen zur Lastverteilung für Daten werden nicht unterstützt.

Die folgende Abbildung zeigt das Verfahren zur Initialisierung einer SnapMirror Beziehung:

System Manager

Ab ONTAP 9.12.1 kann mit System Manager die SnapMirror Replizierung von WORM-Dateien eingerichtet werden.

Schritte

1. Navigieren Sie zu **Storage > Volumes**.
2. Klicken Sie auf **ein-/Ausblenden** und wählen Sie **SnapLock-Typ**, um die Spalte im Fenster **Volumen** anzuzeigen.
3. Suchen Sie ein SnapLock Volume.
4. Klicken Sie Auf ⋮ Und wählen Sie **Protect**.
5. Auswahl des Ziel-Clusters und der Ziel-Storage-VM
6. Klicken Sie Auf **Weitere Optionen**.
7. Wählen Sie **Legacy-Richtlinien anzeigen** und wählen Sie **DPDefault (Legacy)**.
8. Wählen Sie im Abschnitt **Zielkonfigurationsdetails** die Option **Transferzeitplan überschreiben** aus und wählen Sie **stündlich** aus.
9. Klicken Sie Auf **Speichern**.
10. Klicken Sie links vom Namen des Quell-Volumes auf den Pfeil, um die Volume-Details zu erweitern, und rechts auf der Seite sehen Sie die Remote SnapMirror Sicherungsdetails.
11. Navigieren Sie auf dem Remote-Cluster zu **Protection Relationships**.
12. Suchen Sie die Beziehung, und klicken Sie auf den Namen des Zielvolumes, um die Beziehungsdetails anzuzeigen.
13. Überprüfen Sie, ob der SnapLock-Typ des Ziel-Volumes und andere SnapLock-Informationen verwendet werden.

CLI

1. Ermitteln des Ziel-Clusters
2. Installieren Sie auf dem Ziel-Cluster die SnapLock Lizenz, initialisieren Sie die ComplianceClock und erstellen Sie, wenn Sie eine ONTAP Version vor 9.10.1 verwenden, ein SnapLock-Aggregat.
3. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Ziel-Volume des Typs `DP` Das ist entweder die gleiche Größe wie oder größer als das Quellvolumen:

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

   > Ab ONTAP 9.10.1 können SnapLock- und nicht-SnapLock-Volumes auf demselben Aggregat vorhanden sein. Wenn Sie ONTAP 9.10.1 verwenden, sind Sie daher nicht mehr erforderlich, ein separates SnapLock Aggregat zu erstellen. Mithilfe der Option Volume -snaplock-TYPE können Sie einen Compliance- oder Enterprise SnapLock Volume-Typ festlegen. In älteren Versionen als ONTAP ONTAP 9.10.1 übernimmt der SnapLock-Modus – Compliance oder Enterprise – das Aggregat. Versionsflexible Ziel-Volumes werden nicht unterstützt. Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

   Mit dem folgenden Befehl wird eine 2-GB-SnapLock erstellt `Compliance` Volume mit Namen `dstvolB` In `SVM2` Auf dem Aggregat `node01_aggr`:

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

4. Erstellen Sie auf der Ziel-SVM eine SnapMirror Richtlinie:

   `snapmirror policy create -vserver SVM_name -policy policy_name`

   Mit dem folgenden Befehl wird die SVM-weite Richtlinie erstellt `SVM1-mirror`:

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

5. Erstellen Sie auf der Ziel-SVM einen SnapMirror Zeitplan:

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

   Mit dem folgenden Befehl wird ein SnapMirror Zeitplan mit dem Namen erstellt `weekendcron`:

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

6. Erstellen Sie auf der Ziel-SVM eine SnapMirror Beziehung:

   `snapmirror create -source-path source_path -destination-path destination_path -type XDP|DP -policy policy_name -schedule schedule_name`

   Mit dem folgenden Befehl wird eine SnapMirror Beziehung zwischen dem Quell-Volume erstellt `srcvolA` Ein `SVM1` Und dem Ziel-Volume `dstvolB` Ein `SVM2`, Und weist die Richtlinie zu `SVM1-mirror` Und Zeitplan `weekendcron`:

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

   > Der XDP-Typ ist in ONTAP 9.5 und höher erhältlich. Sie müssen den DP-Typ in ONTAP 9.4 und früher verwenden.

7. Initialisieren Sie auf der Ziel-SVM die SnapMirror-Beziehung:

   `snapmirror initialize -destination-path destination_path`

   Der Initialisierungsvorgang führt einen *Baseline Transfer* zum Ziel-Volume durch. SnapMirror erstellt eine Snapshot-Kopie des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die er auf das Ziel-Volume verweist. Sie überträgt zudem alle anderen Snapshot Kopien auf dem Quell-Volume auf das Ziel-Volume.

Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume initialisiert `srcvolA` Ein `SVM1` Und dem Ziel-Volume `dstvolB` Ein `SVM2`:

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

Verwandte Informationen

"Cluster- und SVM-Peering"

"Vorbereitung der Volume Disaster Recovery"

"Datensicherung"

BEWAHREN SIE WORM-Dateien bei Rechtsstreitigkeiten mithilfe der gesetzlichen Aufbewahrung auf

Ab ONTAP 9.3 können Sie WORM-Dateien im Compliance-Modus während der Dauer eines Rechtsstreits mithilfe der Funktion *Legal Hold* aufbewahren.

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

Eine Datei unter einer gesetzlichen Aufbewahrungspflichten, verhält sich wie EINE WORM-Datei mit einer unbestimmten Aufbewahrungsfrist. Es liegt in Ihrer Verantwortung anzugeben, wann die gesetzliche Haltefrist endet.

Die Anzahl der Dateien, die Sie unter einem Legal Hold platzieren können, hängt von dem verfügbaren Speicherplatz des Volume ab.

Schritte

1. Gesetzliche Aufbewahrungspflichten starten:

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

   Mit dem folgenden Befehl wird ein Legal Hold für alle Dateien in gestartet `vol1`:

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

2. Beenden einer gesetzlichen Aufbewahrungspflichten:

   `snaplock legal-hold end -litigation-name` *`litigation_name`* `-volume` *`volume_name`*

-path *path_name*

Mit dem folgenden Befehl wird ein Legal Hold für alle Dateien in beendet `vol1`:

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

ÜBERSICHT ZU WORM-Dateien löschen

SIE können WORM-Dateien im Enterprise-Modus während des Aufbewahrungszeitraums mit der Funktion Privileged delete löschen. Bevor Sie diese Funktion verwenden können, müssen Sie ein SnapLock-Administratorkonto erstellen und dann die Funktion mit dem Konto aktivieren.

Erstellen Sie ein SnapLock-Administratorkonto

Sie benötigen Administratorrechte von SnapLock, um ein privilegiertes Löschen durchführen zu können. Diese Berechtigungen werden in der Rolle vsadmin-snaplock definiert. Wenn Sie dieser Rolle noch nicht zugewiesen haben, können Sie den Cluster-Administrator bitten, ein SVM-Administratorkonto mit der SnapLock-Administratorrolle zu erstellen.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen sich mit einer sicheren Verbindung (SSH, Konsole oder ZAPI) angemeldet haben.

Schritte

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

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

   Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `SnapLockAdmin` Mit dem vordefinierten `vsadmin-snaplock` Rolle für den Zugriff `SVM1` Verwenden eines Passworts:

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

Aktivieren Sie die Funktion „privilegiertes Löschen“

Sie müssen das Priviledged delete-Feature auf dem Enterprise Volume, das die ZU löschenden WORM-Dateien enthält, explizit aktivieren.

Über diese Aufgabe

Der Wert des `-privileged-delete` Mit dieser Option wird festgelegt, ob das privilegierte Löschen aktiviert

ist. Mögliche Werte sind `enabled`, `disabled`, und `permanently-disabled`.

> `permanently-disabled` Ist der Terminalstatus. Sie können das privilegierte Löschen auf dem Volume nicht aktivieren, nachdem Sie den Status auf festgelegt haben `permanently-disabled`.

Schritte

1. Privilegiertes Löschen für ein SnapLock Enterprise Volume aktivieren:

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

   Mit dem folgenden Befehl wird die Privileged delete-Funktion für das Enterprise Volume aktiviert `dataVol` Ein `SVM1`:

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

LÖSCHEN SIE WORM-Dateien im Enterprise-Modus

Mit der Funktion Priviledged delete können SIE WORM-Dateien im Enterprise-Modus während des Aufbewahrungszeitraums löschen.

Was Sie benötigen

- Sie müssen ein SnapLock-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen ein SnapLock-Auditprotokoll erstellt und die Funktion zum Löschen von Berechtigungen auf dem Enterprise Volume aktiviert haben.

Über diese Aufgabe

Sie können eine abgelaufene WORM-Datei nicht mit einem privilegierten Löschvorgang löschen. Sie können das verwenden `volume file retention show` Befehl zum Anzeigen der Aufbewahrungszeit der WORM-Datei, die Sie löschen möchten. Weitere Informationen finden Sie auf der man-Page für den Befehl.

Schritt

1. LÖSCHEN EINER WORM-Datei auf einem Enterprise Volume:

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

   Mit dem folgenden Befehl wird die Datei gelöscht `/vol/dataVol/f1` Auf der SVM`SVM1`:

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