MANAGEN von WORM-Dateien

ONTAP 9

NetApp
February 12, 2026

Inhalt

MANAGEN von WORM-Dateien

Verwalten Sie WORM-Dateien mit ONTAP SnapLock

ES gibt folgende Möglichkeiten, WORM-Dateien zu verwalten:

- "Übertragung von Dateien an DIE WORM-Funktion"
- "Setzen Sie Snapshots auf WORM auf einem Vault-Ziel"
- "SPIEGELN VON WORM-Dateien für das Disaster Recovery"
- "Aufbewahrung VON WORM-Dateien bei Gerichtsverfahren"
- "LÖSCHEN SIE WORM-Dateien"

Übertragen Sie Dateien mit ONTAP SnapLock in WORM

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.

Bevor Sie beginnen

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

Über diese Aufgabe

Die Volume ComplianceClock Time wird in das `ctime` Feld der Datei geschrieben, 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 `document.txt` schreibgeschützt zu erstellen:

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

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

`document.txt` schreibgeschützt zu erstellen:

```
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.

Bevor Sie beginnen

- 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`*

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

   Mit dem folgenden Befehl werden die Dateien auf dem `vol1` SVM vs1-Volume automatisch übertragen, 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.

Bevor Sie beginnen

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.

Alle ungeordneten Schreibvorgänge, die über den aktuellen aktiven 256-KB-Block hinausgehen, führen dazu, dass der aktive 256-KB-Block auf den letzten Offset zurückgesetzt wird und dass Schreibvorgänge auf ältere Offsets mit einem Fehler „Read Only File System (ROFS)“ fehlschlagen. Die Schreiboffsets sind abhängig von der Client-Anwendung. Ein Client, der nicht der Schreibsemantik der WORM-Datei mit angehangenen Dateien entspricht, kann zu einer falschen Beendigung der Schreibinhalte führen. Es wird daher empfohlen, entweder sicherzustellen, dass der Client die Offset-Beschränkungen für ungeordnete Schreibvorgänge befolgt, oder um synchrone Schreibvorgänge sicherzustellen, indem das Dateisystem im synchronen Modus gemountet wird.

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 von 21. November 2020 6:00 Uhr auf einer Datei mit der Nulllänge festzulegen `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 `document.txt` schreibgeschützt zu erstellen:

```
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 `document.txt` beschreibbar zu machen:

```
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 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.

Bevor Sie beginnen

- Die angehängbare WORM-Datei muss sich auf einem SnapLock Volume befinden.
- Das SnapLock-Volume muss abgehängt werden und darf keine Snapshots und vom Benutzer erstellten Dateien enthalten.

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`

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

   Mit dem folgenden Befehl wird VAM auf Volume `vol1` der SVM aktiviert`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.

Übertragen Sie Snapshots an WORM auf einem ONTAP Vault-Ziel

Sie können SnapLock für SnapVault verwenden, um WORM-gesicherte Snapshots auf dem Sekundärspeicher zu erstellen. Sie führen alle grundlegenden SnapLock-Aufgaben auf dem Vault-Ziel aus. Das Ziel-Volume wird automatisch schreibgeschützt gemountet, sodass die Snapshots nicht explizit auf WORM übergeben werden müssen.

Bevor Sie beginnen

- Wenn Sie System Manager zum Konfigurieren der Beziehung verwenden möchten, müssen auf dem Quell- und Ziel-Cluster ONTAP 9.15.1 oder höher ausgeführt werden.
- Auf dem Ziel-Cluster:
  - "Installieren Sie die SnapLock Lizenz".
  - "Initialisieren Sie die Compliance-Uhr".
  - Wenn Sie die CLI mit einer ONTAP Version vor 9.10.1 verwenden, "Erstellung eines SnapLock Aggregats".
- Die Schutzrichtlinie muss vom Typ „Vault“ sein.
- Die Quell- und Zielaggregate müssen 64 Bit sein.
- Das Quell-Volume kann kein SnapLock Volume sein.

- Wenn Sie die ONTAP-CLI verwenden, müssen die Quell- und Zielvolumes in "Peering-Cluster" und erstellt werden"SVMs".

Über diese Aufgabe

Das Quellvolume kann NetApp oder Nicht- NetApp -Speicher verwenden.

Sie können einen Snapshot, der in den WORM-Status versetzt wird, nicht umbenennen.

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

LUNs werden in SnapLock Volumes nicht unterstützt. LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen Snapshots, die auf einem nicht-SnapLock Volume erstellt wurden, zur Sicherung im Rahmen der SnapLock Vault-Beziehung auf ein SnapLock Volume übertragen werden. LUNs werden in SnapLock-Volumes mit Lese-/Schreibzugriff nicht unterstützt. Manipulationssichere Snapshots werden jedoch sowohl auf SnapMirror Quell-Volumes als auch auf Ziel-Volumes unterstützt, die LUNs enthalten.

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. Sie verwenden die Option „-snaplock-type“ des Volumes, um einen Compliance- oder Enterprise SnapLock Volume-Typ anzugeben. 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.

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. Jeder NetApp-Snapshot wird zunächst mit diesem Standardaufbewahrungszeitraum festgeschrieben. Die Aufbewahrungsfrist kann bei Bedarf später verlängert werden. Weitere Informationen finden Sie unter "Aufbewahrungszeit einstellen".

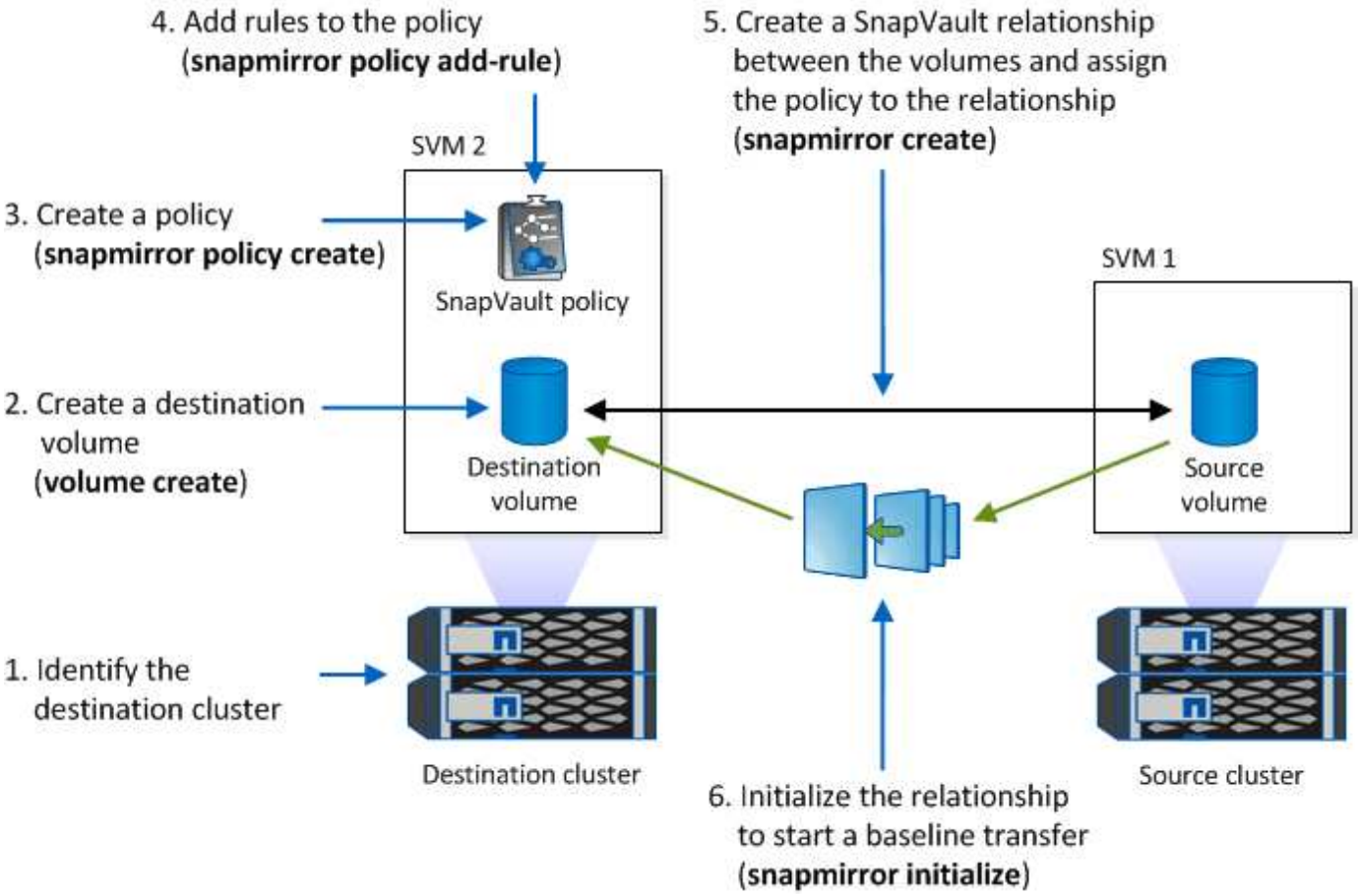
Ab ONTAP 9.14.1 können Sie in der SnapMirror-Richtlinie der SnapMirror-Beziehung Aufbewahrungszeiträume für bestimmte SnapMirror-Labels festlegen, sodass die replizierten Snapshots vom Quell- zum Ziel-Volume für den in der Regel festgelegten Aufbewahrungszeitraum beibehalten werden. Wenn kein Aufbewahrungszeitraum angegeben wird, wird die Standardaufbewahrungsfrist des Ziel-Volume verwendet.

Ab ONTAP 9.13.1 können Sie sofort einen gesperrten Snapshot auf dem Ziel-SnapLock Volume einer SnapLock Vault-Beziehung wiederherstellen, indem Sie einen FlexClone erstellen, bei dem `snaplock-type` die Option auf gesetzt `non-snaplock` ist und den Snapshot bei der Ausführung des Volume-Klonerstellungsvorgangs als „Parent-Snapshot“ angeben. Erfahren Sie mehr über "Erstellung eines FlexClone Volume mit einem SnapLock-Typ".

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.

In der folgenden Abbildung wird das Verfahren zum Initialisieren einer SnapLock Vault-Beziehung gezeigt:



Schritte

Sie können die ONTAP CLI zum Erstellen einer SnapLock Vault-Beziehung oder ab ONTAP 9.15.1 mit System Manager eine SnapLock Vault-Beziehung erstellen.

System Manager

1. Wenn das Volume noch nicht vorhanden ist, navigieren Sie auf dem Quellcluster zu **Speicher > Volumes** und wählen Sie **Hinzufügen**.
2. Wählen Sie im Fenster **Volume hinzufügen Weitere Optionen**.
3. Geben Sie den Namen, die Größe, die Exportrichtlinie und den Freigabenamen des Volumes ein.
4. Speichern Sie die Änderungen.
5. Navigieren Sie auf dem Zielcluster zu **Schutz > Beziehungen**.
6. Wählen Sie über der Spalte **Source Protect** und wählen Sie **Volumes** aus dem Menü.
7. Wählen Sie im Fenster **Volumes schützen** als Schutzrichtlinie **Vault** aus.
8. Wählen Sie im Abschnitt **Source** den Cluster, die Speicher-VM und das Volume aus, das Sie schützen möchten.
9. Wählen Sie im Abschnitt **Ziel** unter **Konfigurationsdetails Zielabzüge sperren** aus und wählen Sie dann **SnapLock für SnapVault** als Sperrmethode. **Sperrmethode** wird nicht angezeigt, wenn der ausgewählte Richtlinientyp nicht vom Typ ist `vault`, wenn die SnapLock-Lizenz nicht installiert ist oder wenn die Konformitätsuhr nicht initialisiert ist.
10. Wenn sie noch nicht aktiviert ist, wählen Sie **SnapLock-Compliance-Uhr initialisieren** aus.
11. Speichern Sie die Änderungen.

CLI

1. Erstellen Sie auf dem Ziel-Cluster ein SnapLock-Ziel-Volume des Typs `DP`, das entweder gleich oder größer ist als das Quell-Volume:

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

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

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

2. Auf dem Zielcluster, "Legen Sie den Standardaufbewahrungszeitraum fest".
3. "Erstellen einer neuen Replikationsbeziehung" Zwischen der nicht-SnapLock-Quelle und dem neuen SnapLock-Ziel, das Sie erstellt haben.

   Dieses Beispiel erstellt eine neue SnapMirror-Beziehung mit dem Ziel-SnapLock-Volume `dstvolB` unter Verwendung einer Richtlinie `XDPDefault`, täglich und wöchentlich markierte Snapshots nach einem stündlichen Zeitplan zu archivieren:

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

"Erstellen Sie eine benutzerdefinierte Replikationsrichtlinie" Oder ein"Benutzerdefinierter Zeitplan", wenn die verfügbaren Standardeinstellungen nicht geeignet sind.

4. Initialisieren Sie auf der Ziel-SVM die erstellte SnapVault Beziehung:

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

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

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

5. Nachdem die Beziehung initialisiert und inaktiv wurde, überprüfen Sie mit dem `snapshot show` Befehl auf dem Ziel die SnapLock-Verfallszeit, die auf die replizierten Snapshots angewendet wird.

Im folgenden Beispiel werden die Snapshots auf einem Volume mit dem SnapMirror-Label und dem SnapLock-Ablaufdatum aufgelistet `dstvolB`:

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

Verwandte Informationen

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

Spiegeln Sie WORM-Dateien mit ONTAP SnapMirror für die Notfallwiederherstellung

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 vorhandenen DP-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. Wenn eine Neusynchronisierung fehlschlägt, können Sie den `volume clone create` Befehl verwenden, um einen Klon des Ziel-Volume zu erstellen. Sie können dann das Quell-Volume mit dem Klon neu synchronisieren.
- Eine SnapMirror -Beziehung eines SnapLock -Volumes unterstützt nur die `MirrorAllSnapshots` Richtlinie vom Typ „Async-Mirror“. Die Aufbewahrungsdauer eines SnapLock -Volumes wird durch die maximale Aufbewahrungsdauer aller darin enthaltenen WORM-Dateien bestimmt. Da es sich beim Ziel um eine DR-Kopie der Quelle handelt, ist die Aufbewahrungsdauer des Ziel- SnapLock -Volumes dieselbe wie die der Quelle.
- 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 legal-holds hat, wird die tatsächliche Gültigkeitsdauer des Volumes maskiert und als ‘unbestimmt’ angezeigt. Der Snapshot wird jedoch für die Dauer der tatsächlichen Gültigkeitsdauer des Volumes gesperrt.

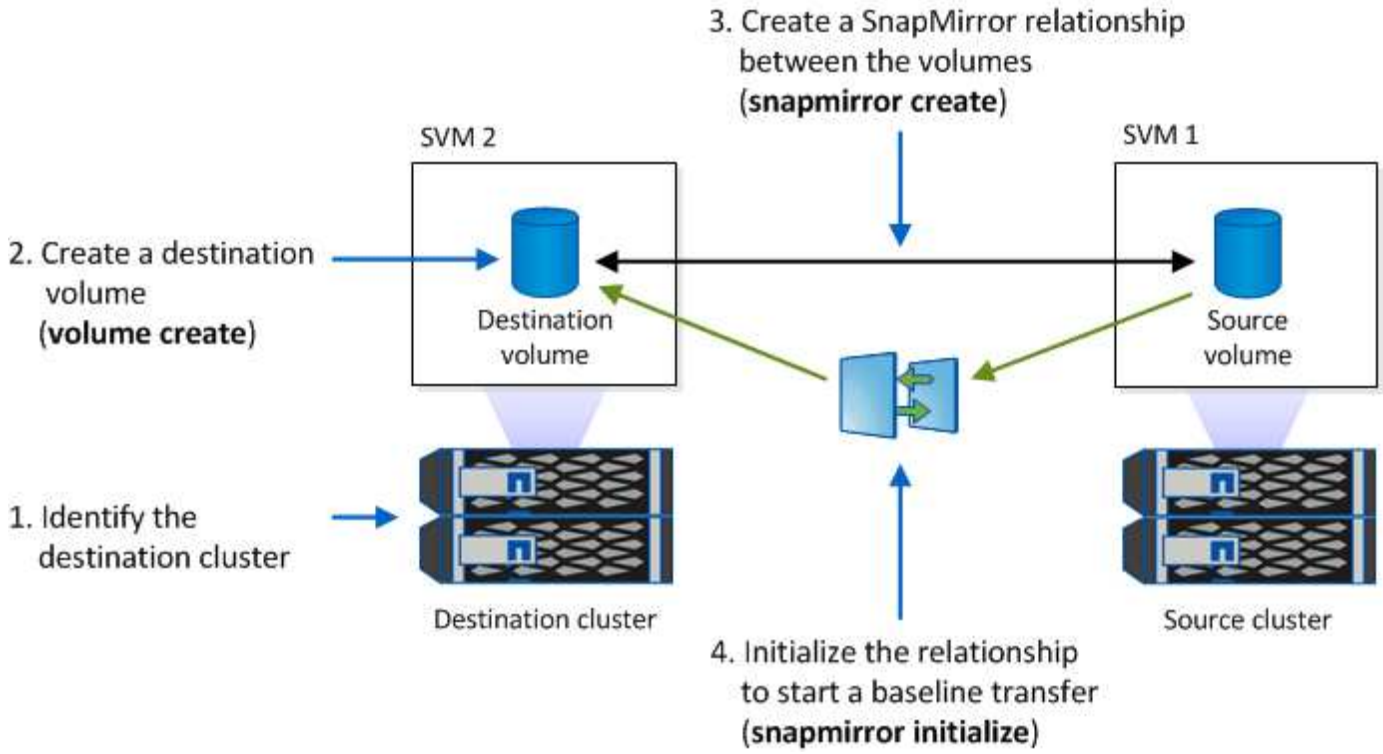
Wenn das Ziellaufwerk eine Ablauffrist hat, die später als das Quellvolumen ist, wird die Gültigkeitsdauer des Zieldatums beibehalten und wird nach der Resynchronisierung nicht durch den Ablaufzeitraum des Quellvolumens überschrieben.

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.

Ein gesperrter Snapshot auf dem Ziellaufwerk, der zur Erfassung der divergierenden Daten erstellt wurde, kann mithilfe der CLI durch Ausführen des Befehls auf die Quelle kopiert werden `snapmirror update -s snapshot`. 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:


3. Create a SnapMirror relationship between the volumes (**snapmirror create**)
SVM 2
SVM 1
2. Create a destination volume (**volume create**)
Destination volume
Source volume
1. Identify the destination cluster
Destination cluster
Source cluster
4. Initialize the relationship to start a baseline transfer (**snapmirror initialize**)

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 **Schutz**.
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. Auf dem Ziel-Cluster, "Installieren Sie die SnapLock-Lizenz", "Initialisieren Sie die Compliance Clock"und, wenn Sie eine ONTAP-Version vor 9.10.1 verwenden, "Erstellung eines SnapLock Aggregats".
3. Erstellen Sie auf dem Ziel-Cluster ein SnapLock-Ziel-Volume des Typs `DP`, das entweder dieselbe oder eine größere Größe als das Quell-Volume hat:

   ```
   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. Daher müssen Sie bei Verwendung von ONTAP 9.10.1 kein separates SnapLock -Aggregat mehr erstellen. Mit der Option „Volume -Snaplock -Type“ geben Sie einen Compliance- oder Enterprise- SnapLock -Volumetyp an. In ONTAP -Versionen vor ONTAP 9.10.1 wird der SnapLock -Modus – Compliance oder Enterprise – vom Aggregat übernommen. Die Spracheinstellung des Zielvolumes muss mit der Spracheinstellung des Quellvolumes übereinstimmen.

   Mit dem folgenden Befehl wird ein 2 GB SnapLock- `Compliance`Volume erstellt, das `dstvolB` im `SVM2` Aggregat genannt `node01_aggr` wird:

```
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 `weekendcron` dem Namen erstellt:

   ```
   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 `srcvolA` `SVM1` `dstvolB` auf und dem Ziel-Volume auf erstellt `SVM2` und die Policy `SVM1-mirror` und den Zeitplan zugewiesen `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 einen Snapshot des Quell-Volume, überträgt dann die Kopie und alle Datenblöcke, die es auf das Ziel-Volume verweist. Außerdem werden alle anderen Snapshots auf dem Quell-Volume an das Ziel-Volume übertragen.

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

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

Verwandte Informationen

- "Cluster- und SVM-Peering"
- "Vorbereitung der Volume Disaster Recovery"
- "Datensicherung"
- "snapmirror erstellen"
- "snapmirror Initialisierung"
- "Snapmirror-Richtlinie erstellen"

Bewahren Sie WORM-Dateien während eines Rechtsstreits mit ONTAP SnapLock Legal Hold auf

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

Bevor Sie beginnen

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

  "Erstellen Sie ein SnapLock-Administratorkonto"

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

Über diese Aufgabe

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 /
   ```

Verwandte Informationen

- "Snaplock Legal-Hold-Beginn"
- "Snaplock Legal-Hold-Ende"

Löschen Sie WORM-Dateien mit ONTAP SnapLock

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.

Bevor Sie beginnen

- 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 `SnapLockAdmin` `vsadmin-snaplock` kann das SVM-Administratorkonto mit der vordefinierten Rolle `SVM1` über ein Passwort darauf zugreifen:

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

Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

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

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

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 privilegierte Löschfunktion für das Enterprise-Volume aktiviert `dataVol` `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.

Bevor Sie beginnen

- 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 mit dem `volume file retention show` Befehl die Aufbewahrungszeit der WORM-Datei anzeigen, die Sie löschen möchten. Erfahren Sie mehr über `volume file retention show` in der "ONTAP-Befehlsreferenz".

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 `/vol/dataVol/f1` auf der SVM gelöscht`SVM1`:

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