WORM-Dateien verwalten

ONTAP 9

NetApp
November 10, 2026

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

Inhalt

WORM-Dateien verwalten . . . 1
- WORM-Dateiverwaltung in ONTAP SnapLock . . . 1
- Dateien mit ONTAP SnapLock auf WORM festschreiben . . . 1
  - Dateien manuell an WORM übergeben . . . 1
  - Dateien automatisch an WORM übergeben . . . 2
  - Eine WORM-anhängbare Datei erstellen . . . 3
  - Einen Befehl oder ein Programm verwenden, um eine WORM-anhängbare Datei zu erstellen . . . 3
  - Den Volume-Append-Modus verwenden, um WORM-anhängbare Dateien zu erstellen . . . 4
- Snapshots auf einem ONTAP SnapLock Vault-Ziel in WORM festschreiben . . . 5
- WORM-Dateien mit ONTAP SnapMirror für die Notfallwiederherstellung spiegeln . . . 9
- WORM-Dateien während eines Rechtsstreits mit ONTAP SnapLock Legal Hold aufbewahren . . . 13
- WORM-Dateien mit ONTAP SnapLock löschen . . . 14
  - Ein SnapLock Administratorkonto erstellen . . . 14
  - Die Funktion zum privilegierten Löschen aktivieren . . . 15
  - Enterprise-Modus WORM-Dateien löschen . . . 15

WORM-Dateien verwalten

WORM-Dateiverwaltung in ONTAP SnapLock

Sie können WORM-Dateien auf folgende Weise verwalten:

- "Dateien in WORM übernehmen"
- "Snapshots auf einem WORM-Tresor-Ziel festschreiben"
- "WORM-Dateien für die Notfallwiederherstellung spiegeln"
- "WORM-Dateien während des Rechtsstreits aufbewahren"
- "WORM-Dateien löschen"

Dateien mit ONTAP SnapLock auf WORM festschreiben

Sie können Dateien entweder manuell oder automatisch auf WORM (Write Once, Read Many) festschreiben. Es können auch WORM-anhängbare Dateien erstellt werden.

Dateien manuell an WORM übergeben

Sie übertragen eine Datei manuell an WORM, indem Sie die Datei schreibgeschützt machen. Sie können über NFS oder CIFS jeden geeigneten Befehl oder jedes geeignete Programm verwenden, um das Lese-/Schreibattribut einer Datei auf schreibgeschützt zu ändern. Eine manuelle Übertragung von Dateien kann gewählt werden, wenn sichergestellt werden soll, dass eine Anwendung das Schreiben in eine Datei abgeschlossen hat, damit die Datei nicht vorzeitig übertragen wird, oder wenn aufgrund einer hohen Anzahl von Volumes Skalierungsprobleme beim Autocommit-Scanner bestehen.

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 ComplianceClock-Zeit wird beim Ausführen des Befehls oder Programms in das `ctime` Feld der Datei geschrieben. Die ComplianceClock-Zeit bestimmt, wann die Aufbewahrungsfrist für die Datei erreicht ist.

Schritte

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

   In einer UNIX-Shell wird mit folgendem Befehl eine Datei mit dem Namen `document.txt` schreibgeschützt erstellt:

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

   In einer Windows-Shell wird mit dem folgenden Befehl eine Datei mit dem Namen `document.txt` schreibgeschützt erstellt:

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

Dateien automatisch an WORM übergeben

Die SnapLock Autocommit-Funktion ermöglicht das automatische Übertragen von Dateien in den WORM-Status. Die Autocommit-Funktion überträgt eine Datei in den WORM-Status auf einem SnapLock Volume, wenn sie sich während der Autocommit-Periode nicht geändert hat. Die Autocommit-Funktion ist standardmäßig deaktiviert.

Bevor Sie beginnen

- Die Dateien, die Sie automatisch übertragen möchten, müssen sich auf einem SnapLock Volume befinden.
- Das SnapLock Volume muss online sein.
- Das SnapLock Volume muss ein Lese-/Schreib-Volume sein.

> Die SnapLock Autocommit-Funktion durchsucht alle Dateien im Volume und committet eine Datei, wenn sie die Autocommit-Anforderungen erfüllt. Zwischen dem Zeitpunkt, an dem die Datei für Autocommit bereit ist, und dem tatsächlichen Commit durch den SnapLock Autocommit-Scanner kann ein Zeitintervall liegen. Die Datei ist jedoch bereits ab dem Zeitpunkt, an dem sie für Autocommit geeignet ist, vor Änderungen und Löschung durch das Dateisystem geschützt.

Über diese Aufgabe

Die *Autocommit-Periode* gibt an, wie lange Dateien unverändert bleiben müssen, bevor sie automatisch übernommen werden. Wird eine Datei vor Ablauf der Autocommit-Periode geändert, beginnt die Autocommit-Periode für diese Datei von neuem.

Die folgende Tabelle zeigt die möglichen Werte für den Autocommit-Zeitraum:

Wert	Einheit	Hinweise
keine	-	Die Standardeinstellung.
5 - 5256000	Minuten	-
1 - 87600	Stunden	-
1 - 3650	Tage	-
1 - 120	Monate	-
1 - 10	Jahre	-

> Der Mindestwert beträgt 5 Minuten, der Höchstwert 10 Jahre.

Schritte

1. Automatisches Übertragen von Dateien auf einem SnapLock Volume auf WORM:

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

   Weitere Informationen zu `volume snaplock modify` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl speichert die Dateien auf dem Volume `vol1` von SVM vs1 automatisch, sofern die Dateien 5 Stunden lang unverändert bleiben:

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

Eine WORM-anhängbare Datei erstellen

Eine WORM-anhängbare Datei speichert inkrementell geschriebene Daten, wie Protokolleinträge. Es kann jeder geeignete Befehl oder jedes geeignete Programm verwendet werden, um eine WORM-anhängbare Datei zu erstellen, oder die SnapLock *Volume-Append-Modus*-Funktion kann genutzt werden, um standardmäßig WORM-anhängbare Dateien zu erstellen.

Einen Befehl oder ein Programm verwenden, um eine WORM-anhängbare Datei zu erstellen

Sie können über NFS oder CIFS jeden geeigneten Befehl oder jedes geeignete Programm verwenden, um eine WORM-anhängbare Datei zu erstellen. Eine WORM-anhängbare Datei speichert inkrementell geschriebene Daten, wie Protokolleinträge. Daten werden in 256-KB-Blöcken an die Datei angehängt. Sobald ein Block geschrieben wurde, wird der vorherige Block WORM-geschützt. Die Datei kann erst gelöscht werden, wenn die Aufbewahrungsfrist abgelaufen ist.

Bevor Sie beginnen

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

Über diese Aufgabe

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

Jegliche ungeordneten Schreibvorgänge, die über den aktuell aktiven 256 KB Chunk hinausgehen, führen dazu, dass der aktive 256 KB Chunk auf den letzten Offset zurückgesetzt wird und Schreibvorgänge auf ältere Offsets mit einem „Read Only File System (ROFS)“-Fehler fehlschlagen. Die Schreib-Offsets sind von der Client-Anwendung abhängig. Ein Client, der die WORM Append File Write Semantik nicht einhält, kann zu einem fehlerhaften Abschluss der Schreibinhalte führen. Es empfiehlt sich, entweder sicherzustellen, dass der Client die Offset-Beschränkungen für ungeordnete Schreibvorgänge einhält, oder synchrones Schreiben zu gewährleisten, indem das Dateisystem im synchronen Modus eingebunden wird.

Schritte

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

   In einer UNIX-Shell kann mit dem folgenden Befehl für eine leere Datei mit dem Namen `document.txt` eine Aufbewahrungszeit bis zum 21. November 2020, 6:00 Uhr, festgelegt werden:

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

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

In einer UNIX-Shell wird mit folgendem Befehl eine Datei mit dem Namen `document.txt` schreibgeschützt erstellt:

```
chmod 444 document.txt
```

3. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um das Lese-/Schreibattribut der Datei wieder auf beschreibbar zu ändern.

   Dieser Schritt stellt kein Compliance-Risiko dar, da sich keine Daten in der Datei befinden.

   In einer UNIX-Shell kann mit folgendem Befehl eine Datei mit dem Namen `document.txt` beschreibbar gemacht werden:

   ```
   chmod 777 document.txt
   ```

4. Ein geeigneter Befehl oder ein geeignetes Programm kann verwendet werden, um mit dem Schreiben von Daten in die Datei zu beginnen.

   In einer UNIX-Shell kann mit dem folgenden Befehl Daten auf `document.txt` geschrieben werden:

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

   Die Dateiberechtigungen werden wieder auf schreibgeschützt gesetzt, wenn kein weiteres Anhängen von Daten an die Datei erforderlich ist.

Den Volume-Append-Modus verwenden, um WORM-anhängbare Dateien zu erstellen

Ab ONTAP 9.3 kann die SnapLock Volume Append Mode (VAM)-Funktion verwendet werden, um standardmäßig WORM-anhängbare Dateien zu erstellen. Eine WORM-anhängbare Datei speichert inkrementell geschriebene Daten, wie Protokolleinträge. Daten werden in 256-KB-Blöcken an die Datei angehängt. Sobald ein Block geschrieben wurde, wird der vorherige Block WORM-geschützt. Die Datei kann erst gelöscht werden, wenn die Aufbewahrungsfrist abgelaufen ist.

Bevor Sie beginnen

- Die WORM-anhängbare Datei muss sich auf einem SnapLock Volume befinden.
- Das SnapLock Volume muss ausgehängt und frei von Snapshots und benutzererstellten Dateien sein.

Über diese Aufgabe

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

Wenn ein Autocommit-Zeitraum für das Volume festgelegt ist, werden WORM-anhängbare Dateien, die über einen Zeitraum, der länger als der Autocommit-Zeitraum ist, nicht geändert wurden, in WORM übernommen.

VAM wird auf SnapLock Revisionsprotokoll-Volumes nicht unterstützt.

Schritte

1. VAM aktivieren:

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

   Weitere Informationen zu `volume snaplock modify` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl aktiviert VAM auf dem Volume `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-anhängbar.

Snapshots auf einem ONTAP SnapLock Vault-Ziel in WORM festschreiben

Mit SnapLock für SnapVault lassen sich Snapshots auf sekundärem Speicher WORM-schützen. Alle grundlegenden SnapLock-Aufgaben werden am Vault-Ziel durchgeführt. Das Ziel-Volume wird automatisch schreibgeschützt eingebunden, sodass ein explizites Commit der Snapshots in WORM nicht erforderlich ist.

Bevor Sie beginnen

- Wenn der System Manager zur Konfiguration der Beziehung verwendet werden soll, müssen sowohl der Quell- als auch der Ziel-Cluster ONTAP 9.15.1 oder höher ausführen.
- Auf dem Ziel-Cluster:
  - "Die SnapLock-Lizenz installieren".
  - "Die Compliance-Uhr initialisieren".
  - Wenn Sie die CLI mit einer ONTAP Version vor 9.10.1 verwenden, "ein SnapLock Aggregat erstellen".
- Die Datensicherungsstrategie muss vom Typ „vault“ sein.
- Die Quell- und Ziel-Aggregate müssen 64-Bit sein.
- Das Quellvolume darf kein SnapLock Volume sein.
- Wenn Sie die ONTAP CLI verwenden, müssen die Quell- und Ziel-Volumes in "verbundene Cluster" und "SVMs" erstellt werden.

Über diese Aufgabe

Das Quell-Volume kann NetApp- oder Storage anderer Anbieter (NetApp-fremd) verwenden.

> Ein Snapshot, der im WORM-Status festgeschrieben ist, kann nicht umbenannt werden.

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, auf ein SnapLock Volume zum Schutz im Rahmen einer SnapLock Vault-Beziehung übertragen werden. LUNs werden in lesen/schreiben SnapLock Volumes nicht unterstützt. Manipulationssichere Snapshots werden jedoch sowohl auf SnapMirror Quell-Volumes als auch auf Ziel-Volumes unterstützt, die LUNs enthalten.

Ab ONTAP 9.10.1 können SnapLock- und Nicht-SnapLock-Volumes auf demselben Aggregate existieren, daher ist es nicht mehr erforderlich, ein separates SnapLock-Aggregate zu erstellen, wenn ONTAP 9.10.1 verwendet wird. Die Volume-Option '-snaplock-type' wird verwendet, um einen Compliance- oder Enterprise-SnapLock-Volume-Typ anzugeben. In ONTAP-Versionen vor ONTAP 9.10.1 wird der SnapLock-Modus, Compliance oder Enterprise, vom Aggregate übernommen. Version-flexible Zielvolumes werden nicht unterstützt. Die Spracheinstellung des Ziel-Volumes muss mit der Spracheinstellung des Quell-Volumes übereinstimmen.

Ein SnapLock Volume, das als Vault-Ziel dient, hat eine standardmäßige Aufbewahrungsfrist zugewiesen. Der Wert für diese Frist ist anfangs auf mindestens 0 Jahre für SnapLock Enterprise Volumes und maximal 30 Jahre für SnapLock Compliance Volumes festgelegt. Jeder NetApp Snapshot wird zunächst mit dieser standardmäßigen Aufbewahrungsfrist übernommen. Die Aufbewahrungsfrist kann bei Bedarf später verlängert werden. Weitere Informationen finden sich unter "Übersicht über die Aufbewahrungszeit festlegen".

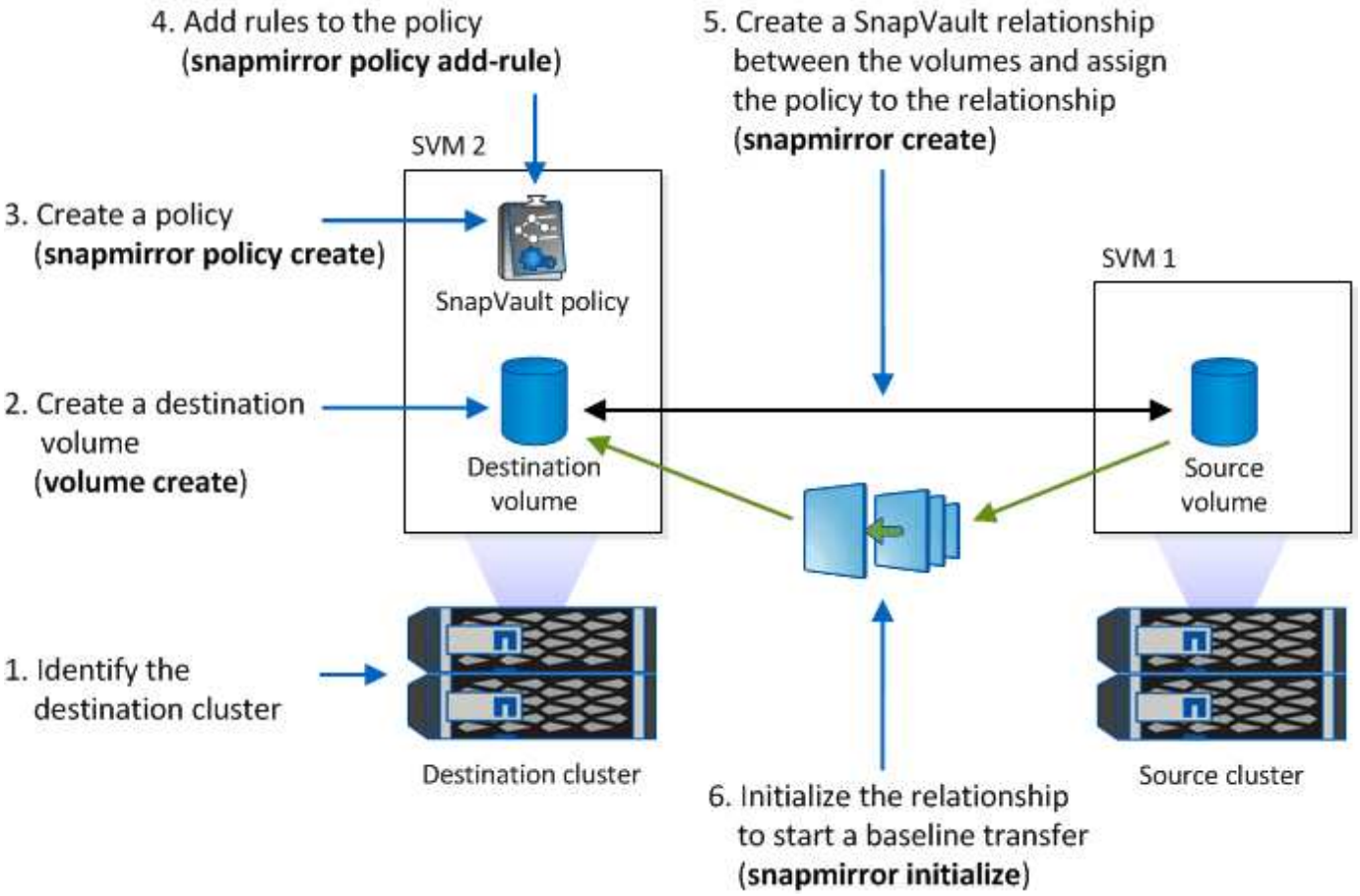
Ab ONTAP 9.14.1 können Aufbewahrungsfristen für bestimmte SnapMirror Labels in der SnapMirror Policy der SnapMirror Beziehung festgelegt werden, sodass die replizierten Snapshots vom Quell- zum Ziel-Volume für die in der Regel angegebene Aufbewahrungsfrist aufbewahrt werden. Wenn keine Aufbewahrungsfrist angegeben ist, wird die Standardaufbewahrungsfrist des Ziel-Volumes verwendet.

Ab ONTAP 9.13.1 ist es möglich, einen gesperrten Snapshot auf dem Ziel-SnapLock-Volume einer SnapLock Vault Beziehung sofort wiederherzustellen, indem eine FlexClone mit der `snaplock-type` Option auf `non-snaplock` erstellt und der Snapshot beim Ausführen der Volume-Klon-Erstellung als „parent-snapshot“ angegeben wird. Weitere Informationen zu "Erstellen eines FlexClone Volumens mit einem SnapLock Typ".

Für MetroCluster Konfigurationen gilt Folgendes:

- Eine SnapVault Beziehung kann nur zwischen Sync-Source-SVMs erstellt werden, nicht zwischen einer Sync-Source-SVM und einer Sync-Destination-SVM.
- Es ist möglich, eine SnapVault Beziehung von einem Volume auf einer Sync-Source-SVM zu einer Data-Serving-SVM zu erstellen.
- Es ist möglich, eine SnapVault Beziehung von einem Volume auf einer datenbereitstellenden SVM zu einem DP Volume auf einer Sync-Source-SVM zu erstellen.

Die folgende Abbildung zeigt das Vorgehen zum Initialisieren einer SnapLock Vault Beziehung:



Schritte

Mit der ONTAP CLI lässt sich eine SnapLock Vault Beziehung erstellen, ab ONTAP 9.15.1 ist dies auch mit dem System Manager möglich, um eine SnapLock Vault Beziehung zu erstellen.

System Manager

1. Falls das Volume noch nicht existiert, im Quell-Cluster zu **Speicher > Volumes** navigieren und **Hinzufügen** auswählen.
2. Im Fenster **Volume hinzufügen Weitere Optionen** auswählen.
3. Den Datenträgernamen, die Größe, die Exportrichtlinie und den Freigabenamen eingeben.
4. Speichern Sie Ihre Änderungen.
5. Im Ziel-Cluster zu **Schutz > Beziehungen** navigieren.
6. Oberhalb der Spalte **Quelle Schützen** auswählen und im Menü **Volumes** wählen.
7. Im Fenster **Volumes schützen Vault** als Datensicherungsstrategie auswählen.
8. Im Abschnitt **Quelle** sind der Cluster, die Storage-VM und das Volume auszuwählen, die geschützt werden sollen.
9. Im Abschnitt **Ziel** ist unter **Konfigurationsdetails** die Option **Ziel-Snapshots sperren** auszuwählen, anschließend **SnapLock für SnapVault** als Sperrmethode. **Sperrmethode** wird nicht angezeigt, wenn der ausgewählte Richtlinientyp nicht vom Typ `vault` ist, die SnapLock Lizenz nicht installiert ist oder die Compliance-Uhr nicht initialisiert wurde.
10. Falls diese Option noch nicht aktiviert ist, **SnapLock Compliance-Uhr initialisieren** auswählen.

11. Speichern Sie Ihre Änderungen.

CLI

1. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Zielvolume vom Typ `DP`, das entweder gleich groß oder größer als das Quellvolume ist:

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

   Der folgende Befehl erstellt ein 2GB SnapLock Compliance Volume mit dem 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
```

2. Auf dem Ziel-Cluster "die Standard-Aufbewahrungsdauer festlegen".
3. "Eine neue Replikationsbeziehung erstellen" zwischen der non-SnapLock Quelle und dem neuen SnapLock Ziel, das erstellt wurde.

   Dieses Beispiel erstellt eine neue SnapMirror Beziehung mit Ziel-SnapLock Volume `dstvolB` unter Verwendung einer Strategie von `XDPDefault` zum Archivieren von Snapshots mit den Bezeichnungen täglich und wöchentlich nach einem stündlichen Zeitplan:

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

   > "Erstellen einer benutzerdefinierten Replikationsrichtlinie" oder ein "benutzerdefinierter Zeitplan", wenn die verfügbaren Standardeinstellungen nicht geeignet sind.

4. Auf der Ziel-SVM die erstellte SnapVault Beziehung initialisieren:

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

   Der folgende Befehl initialisiert die Beziehung zwischen dem Quell-Volume `srcvolA` auf `SVM1` und dem Ziel-Volume `dstvolB` auf `SVM2`:

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

5. Nachdem die Beziehung initialisiert und im Leerlauf ist, kann mit dem `snapshot show` Befehl auf dem Ziel die für die replizierten Snapshots angewendete SnapLock Ablaufzeit überprüft werden.

   Dieses Beispiel listet die Snapshots auf dem Volume `dstvolB` auf, die die SnapMirror Bezeichnung

und das SnapLock Ablaufdatum haben:

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

Verwandte Informationen

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

WORM-Dateien mit ONTAP SnapMirror für die Notfallwiederherstellung spiegeln

SnapMirror kann verwendet werden, um WORM-Dateien zur Notfallwiederherstellung und für andere Zwecke an einen anderen geografischen Standort zu replizieren. Sowohl das Quellvolume als auch das Zielvolume müssen für SnapLock konfiguriert sein, und beide Volumes müssen denselben SnapLock Modus (Compliance oder Enterprise) aufweisen. Alle wichtigen SnapLock Eigenschaften des Volumes und der Dateien werden repliziert.

Voraussetzungen

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

Über diese Aufgabe

- Ab ONTAP 9.5 ist es möglich, WORM-Dateien mit der XDP (Extended Data Protection)-SnapMirror-Beziehung anstelle der DP (Data Protection)-Beziehung zu replizieren. Der XDP-Modus ist ONTAP versionsunabhängig und kann Dateien, die im selben Block gespeichert sind, unterscheiden, was die Resynchronisierung replizierter Compliance-Mode-Volumes erheblich erleichtert. Informationen zur Konvertierung einer bestehenden DP-Beziehung in eine XDP-Beziehung sind unter "Datensicherung" zu finden.
- Ein Resync-Vorgang für eine DP-Typ-SnapMirror Beziehung schlägt bei einem Compliance-Mode-Volume fehl, wenn SnapLock feststellt, dass dadurch ein Datenverlust entstehen würde. Wenn ein Resync-Vorgang fehlschlägt, kann mit dem `volume clone create` Befehl ein Klon des Ziel-Volumes erstellt werden. Anschließend lässt sich das Quell-Volume mit dem Klon erneut synchronisieren.
- Eine SnapMirror Beziehung eines SnapLock Volumes unterstützt ausschließlich die `MirrorAllSnapshots` Richtlinie vom Typ async-mirror. Die Aufbewahrungsdauer eines SnapLock Volumes wird durch die maximale Aufbewahrungsdauer aller darauf enthaltenen WORM-Dateien bestimmt. Da das Ziel eine DR-Kopie der Quelle ist, entspricht die Aufbewahrungsdauer des Ziel-SnapLock Volumes derjenigen der Quelle.
- Eine SnapMirror Beziehung vom Typ XDP zwischen SnapLock konformen Volumes unterstützt eine Resynchronisierung nach einer Unterbrechung, selbst wenn die Daten auf dem Ziel nach der Unterbrechung von den Daten auf der Quelle abgewichen sind.

  Bei einer Resynchronisierung wird, wenn zwischen Quelle und Ziel Datenabweichungen über den gemeinsamen Snapshot hinaus festgestellt werden, ein neuer Snapshot auf dem Ziel erstellt, um diese

Abweichungen zu erfassen. Der neue Snapshot und der gemeinsame Snapshot werden beide mit einer Aufbewahrungszeit wie folgt gesperrt:

- Die Ablaufzeit des Ziel-Volumes
- Wenn die Ablaufzeit des Volumes in der Vergangenheit liegt oder nicht festgelegt wurde, ist der Snapshot für einen Zeitraum von 30 Tagen gesperrt.
- Wenn das Zielsystem über rechtliche Sperren verfügt, wird die tatsächliche Ablaufzeit des Volumens ausgeblendet und als 'indefinite' angezeigt; der Snapshot ist jedoch für die Dauer der tatsächlichen Ablaufzeit des Volumens gesperrt.

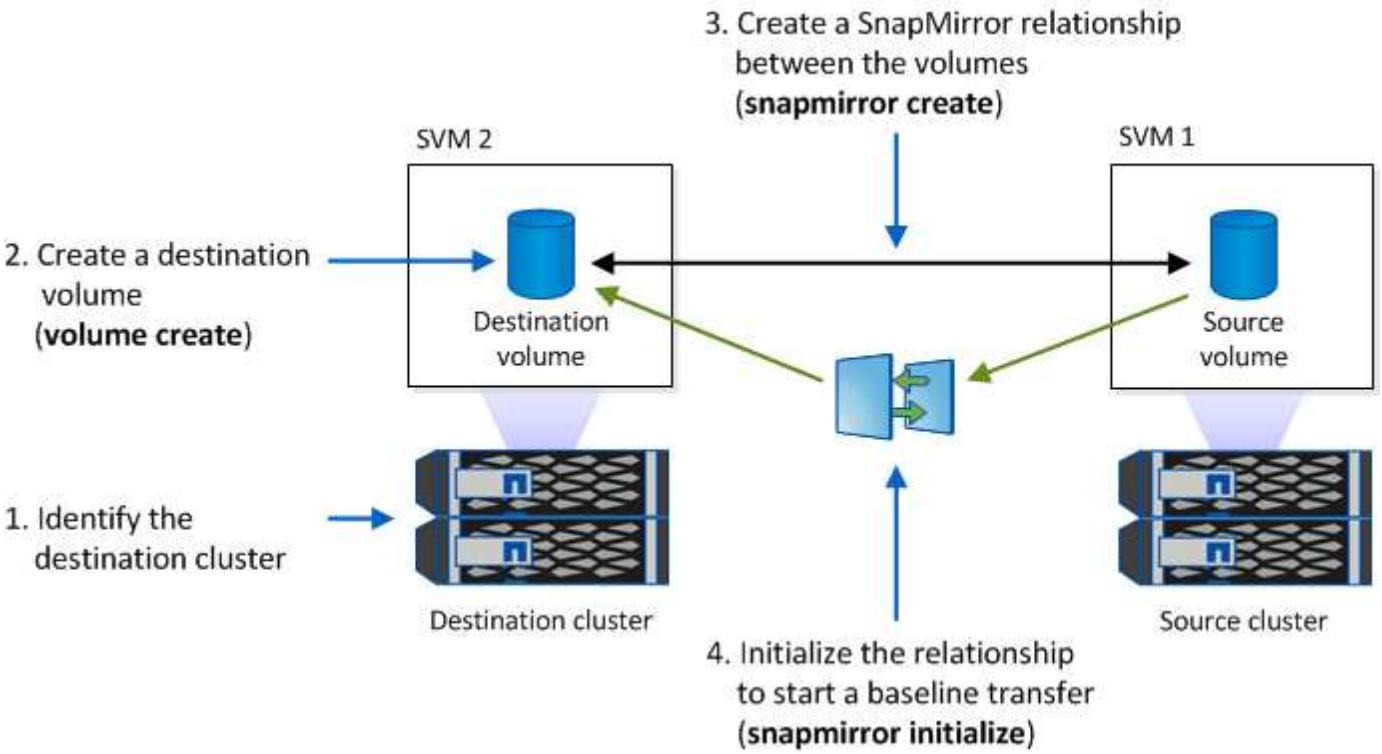
Wenn das Zielvolume eine Ablaufperiode hat, die später ist als die des Quellvolumes, bleibt die Ablaufperiode des Zielvolumes erhalten und wird nach der Resynchronisierung nicht durch die Ablaufperiode des Quellvolumes überschrieben.

Wenn auf dem Ziel rechtliche Sperren bestehen, die sich von denen auf der Quelle unterscheiden, ist eine erneute Synchronisierung nicht zulässig. Quelle und Ziel müssen identische rechtliche Sperren aufweisen oder alle rechtlichen Sperren auf dem Ziel müssen aufgehoben werden, bevor eine erneute Synchronisierung versucht wird.

Ein gesperrter Snapshot auf dem Zielvolume, der zur Erfassung der abweichenden Daten erstellt wurde, kann mithilfe der CLI durch Ausführen des `snapmirror update -s snapshot` Befehls auf das Quellvolume kopiert werden. Der Snapshot bleibt nach dem Kopieren auch auf dem Quellvolume gesperrt.

- SVM Datenschutzbeziehungen werden nicht unterstützt.
- Load-sharing-Datenschutzbeziehungen werden nicht unterstützt.

Die folgende Abbildung zeigt das Vorgehen zum Initialisieren einer SnapMirror Beziehung:



System Manager

Ab ONTAP 9.12.1 ist es möglich, mit System Manager die SnapMirror Replikation von WORM-Dateien einzurichten.

Schritte

1. Navigieren Sie zu **Storage > Volumes**.
2. Klicken Sie auf **Ein-/Ausblenden** und wählen Sie **SnapLock Type**, um die Spalte im Fenster **Volumes** anzuzeigen.
3. Ein SnapLock Volume lokalisieren.
4. Klicken Sie ⋮ und wählen Sie **Schützen**.
5. Den Ziel-Cluster und die Ziel-Speicher-VM auswählen.
6. Auf **Weitere Optionen** klicken.
7. **Legacy-Richtlinien anzeigen** und **DPDefault (legacy)** auswählen.
8. Im Abschnitt **Zielkonfigurationsdetails Übertragungsplan überschreiben** und **stündlich** auswählen.
9. Auf **Speichern** klicken.
10. Klicken Sie links neben dem Namen des Quellvolumes auf den Pfeil, um die Volume-Details zu erweitern, und überprüfen Sie auf der rechten Seite der Seite die Details zum Remote-SnapMirror-Schutz.
11. Im Remote-Cluster zu **Schutzbeziehungen** navigieren.
12. Die Beziehung kann gefunden werden, indem auf den Namen des Ziel-Volumes geklickt wird, wodurch die Details der Beziehung angezeigt werden.
13. Überprüfen Sie den SnapLock-Typ des Ziel-Volumes und weitere SnapLock-Informationen.

CLI

1. Der Ziel-Cluster wird identifiziert.
2. Auf dem Ziel-Cluster, "die SnapLock-Lizenz installieren", "Die Compliance-Uhr initialisieren" und, falls eine ONTAP Version vor 9.10.1 verwendet wird, "ein SnapLock Aggregat erstellen".
3. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Zielvolume vom Typ `DP`, das entweder die gleiche Größe wie das Quellvolume hat oder größer ist:

   ```
   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 Aggregate existieren, daher ist es nicht mehr erforderlich, ein separates SnapLock-Aggregate zu erstellen, wenn ONTAP 9.10.1 verwendet wird. Die Option volume -snaplock-type wird verwendet, um einen Compliance- oder Enterprise-SnapLock-Volume-Typ anzugeben. In ONTAP-Versionen vor ONTAP 9.10.1 wird der SnapLock-Modus (Compliance oder Enterprise) vom Aggregate übernommen. Die Spracheinstellung des Ziel-Volumes muss mit der Spracheinstellung des Quell-Volumes übereinstimmen.

   Der folgende Befehl erstellt ein 2 GB SnapLock `Compliance` Volume mit dem 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. Auf der Ziel-SVM eine SnapMirror Richtlinie erstellen:

   `snapmirror policy create -vserver` *`SVM_name`* `-policy` *`policy_name`*

   Der folgende Befehl erstellt die SVM-weite Richtlinie `SVM1-mirror`:

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

5. Auf der Ziel-SVM einen SnapMirror Zeitplan erstellen:

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

   Der folgende Befehl erstellt einen SnapMirror Zeitplan mit dem Namen `weekendcron`:

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

6. Auf der Ziel-SVM eine SnapMirror Beziehung erstellen:

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

   Der folgende Befehl erstellt eine SnapMirror Beziehung zwischen dem Quellvolume `srcvolA` auf `SVM1` und dem Zielvolume `dstvolB` auf `SVM2`, und weist die Richtlinie `SVM1-mirror` und den Zeitplan `weekendcron` zu:

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

   Der XDP Typ ist ab ONTAP 9.5 verfügbar. In ONTAP 9.4 und früher muss der DP Typ verwendet werden.

7. In der Ziel-SVM die SnapMirror Beziehung initialisieren:

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

   Der Initialisierungsprozess führt einen Basistransfer auf das Ziel-Volume durch. SnapMirror erstellt einen Snapshot des Quell-Volumes und überträgt anschließend die Kopie sowie alle von ihr referenzierten Datenblöcke auf das Ziel-Volume. Es werden außerdem alle weiteren Snapshots des Quell-Volumes auf das Ziel-Volume übertragen.

Der folgende Befehl initialisiert die Beziehung zwischen dem Quell-Volume `srcvolA` auf `SVM1` und dem Ziel-Volume `dstvolB` auf `SVM2`:

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

Verwandte Informationen

- "Cluster- und SVM-Peering"
- "Vorbereitung der Volume-Desaster-Recovery"
- "Datenschutz"
- "snapmirror create"
- "snapmirror initialize"
- "snapmirror policy create"

WORM-Dateien während eines Rechtsstreits mit ONTAP SnapLock Legal Hold aufbewahren

Ab ONTAP 9.3 ist es möglich, WORM-Dateien im Compliance-Modus für die Dauer eines Rechtsstreits mithilfe der Funktion *Legal Hold* aufzubewahren.

Bevor Sie beginnen

- Um diese Aufgabe auszuführen, sind SnapLock Administratorrechte erforderlich.

  "Ein SnapLock Administratorkonto erstellen"

- Eine Anmeldung über eine sichere Verbindung (SSH, Konsole oder ZAPI) muss erfolgt sein.

Über diese Aufgabe

Eine unter Legal Hold stehende Datei verhält sich wie eine WORM-Datei mit unbestimmter Aufbewahrungsfrist. Es liegt in Ihrer Verantwortung, festzulegen, wann der Legal Hold Zeitraum endet.

Die Anzahl der Dateien, die Sie unter eine Legal Hold stellen können, hängt vom verfügbaren Speicherplatz auf dem Volume ab.

Schritte

1. Rechtliche Sicherung starten:

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

   Der folgende Befehl startet eine rechtliche Sperre für alle Dateien in `vol1`:

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

2. Legal Hold beenden:

```
snaplock legal-hold end -litigation-name <litigation_name> -volume
<volume_name> -path <path_name>
```

Der folgende Befehl beendet die rechtliche Sperre für alle Dateien in `vol1`:

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

Verwandte Informationen

- "snaplock legal-hold begin"
- "snaplock Legal-Hold Ende"

WORM-Dateien mit ONTAP SnapLock löschen

Sie können WORM-Dateien im Enterprise-Modus während der Aufbewahrungsfrist mithilfe der Funktion „Privilegiertes Löschen“ löschen. Bevor diese Funktion genutzt werden kann, muss ein SnapLock Administratoraccount erstellt und anschließend mit diesem Konto die Funktion aktiviert werden.

Ein SnapLock Administratorkonto erstellen

Sie müssen über SnapLock-Administratorrechte verfügen, um ein privilegiertes Löschen durchzuführen. Diese Berechtigungen sind in der Rolle vsadmin-snaplock definiert. Falls Ihnen diese Rolle noch nicht zugewiesen wurde, kann der Cluster-Administrator ein SVM-Administratorkonto mit der SnapLock-Administratorrolle erstellen.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Eine Anmeldung über eine sichere Verbindung (SSH, Konsole oder ZAPI) muss erfolgt sein.

Schritte

1. Ein 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

   Der folgende Befehl ermöglicht dem SVM-Administratorkonto `SnapLockAdmin` mit der vordefinierten `vsadmin-snaplock` Rolle den Zugriff `SVM1` mittels eines Passworts:

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

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

Die Funktion zum privilegierten Löschen aktivieren

Sie müssen die Funktion zum privilegierten Löschen auf dem Enterprise Volume, das die zu löschenden WORM-Dateien enthält, explizit aktivieren.

Über diese Aufgabe

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

> `permanently-disabled` ist der Endzustand. Das privilegierte Löschen kann auf dem Volume nicht mehr aktiviert werden, nachdem der Zustand auf `permanently-disabled` gesetzt wurde.

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

   Der folgende Befehl aktiviert die Funktion zum privilegierten Löschen für das Enterprise Volume `dataVol` auf `SVM1`:

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

Enterprise-Modus WORM-Dateien löschen

Die Funktion „Privilegiertes Löschen“ ermöglicht das Löschen von WORM-Dateien im Enterprise-Modus während der Aufbewahrungsfrist.

Bevor Sie beginnen

- Um diese Aufgabe auszuführen, sind SnapLock Administratorrechte erforderlich.
- Ein SnapLock Revisionsprotokoll muss erstellt und die Funktion zum privilegierten Löschen auf dem Enterprise Volume aktiviert sein.

Über diese Aufgabe

Eine privilegierte Löschoperation kann nicht verwendet werden, um eine abgelaufene WORM-Datei zu löschen. Mit dem `volume file retention show` Befehl lässt sich die Aufbewahrungszeit der WORM-Datei anzeigen, die gelöscht werden soll. Weitere Informationen zu `volume file retention show` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Löschen einer WORM-Datei auf einem Enterprise Volume:

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

   Der folgende Befehl löscht die Datei `/vol/dataVol/f1` auf der SVM`SVM1`:

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.