



Archivierung und Compliance mit SnapLock Technologie

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Archivierung und Compliance mit SnapLock Technologie 1
 - Was ist SnapLock. 1
 - Konfigurieren Sie SnapLock. 6
 - MANAGEN von WORM-Dateien 22
 - SnapLock Volumes werden verschoben 35
 - Sperrern einer Snapshot Kopie zum Schutz vor Ransomware-Angriffen 37
 - SnapLock APIs 45

Archivierung und Compliance mit SnapLock Technologie

Was ist SnapLock

SnapLock ist eine hochperformante Compliance-Lösung für Unternehmen, die WORM-Storage verwenden, um Dateien zu gesetzlichen Vorschriften und zu Governance-Zwecken in unveränderter Form aufzubewahren.

SnapLock hilft dabei, das Löschen, Ändern oder Umbenennen von Daten zu vermeiden, um gesetzliche Vorgaben wie SEC 17a-4, HIPAA, FINRA, CFTC und GDPR zu erfüllen. Mit SnapLock können Sie spezielle Volumes erstellen, in denen Dateien gespeichert und nicht löschbar, nicht beschreibbar sind – entweder für einen festgelegten Aufbewahrungszeitraum oder für unbegrenzte Zeit. SnapLock ermöglicht diese Aufbewahrung auf Dateiebene mithilfe von standardmäßigen offenen Dateiprotokollen wie CIFS und NFS. Die unterstützten Open-File-Protokolle für SnapLock sind NFS (Versionen 2, 3 und 4) und CIFS (SMB 1.0, 2.0 und 3.0).

Mithilfe von SnapLock können Sie Dateien und Snapshot-Kopien in WORM-Storage übergeben und Aufbewahrungszeiträume für WORM-gesicherte Daten festlegen. SnapLock WORM Storage nutzt NetApp Snapshot-Technologie und kann SnapMirror Replizierung, und SnapVault Backups als Basistechnologie für Backup Recovery-Sicherung von Daten nutzen. Erfahren Sie mehr über WORM Storage: "[Worm-Speicherung gemäß NetApp SnapLock - TR-4526](#)".

Mit einer Applikation LASSEN sich Dateien über NFS oder CIFS in WORM-FORMAT übersenden oder die automatische Verfestigungsfunktion von SnapLock verwenden, um Dateien automatisch in DEN WORM-SPEICHER zu übertragen. Sie können eine appendable Datei *WORM* verwenden, um Daten, die inkrementell geschrieben werden, wie Protokollinformationen, aufzubewahren. Weitere Informationen finden Sie unter "[Verwenden Sie den Volume Appendable-Modus, um WORM-Dateien zu erstellen](#)".

SnapLock unterstützt Datensicherungsmethoden, die die meisten Compliance-Anforderungen erfüllen:

- Mit SnapLock für SnapVault können Snapshot Kopien IM Sekundärspeicher GESICHERT WERDEN. Siehe "[Übertragung von Snapshot Kopien an WORM](#)".
- WORM-Dateien können zur Disaster Recovery an einen anderen geografischen Standort repliziert werden. Siehe "[Spiegelung VON WORM-Dateien](#)".

SnapLock ist eine lizenzbasierte Funktion des NetApp ONTAP. Eine einzige Lizenz berechtigt Sie zur Verwendung von SnapLock im strengen Compliance-Modus, zur Erfüllung externer Vorgaben wie SEC Rule 17a-4 und einem gelockerten Enterprise-Modus, um die intern vorgeschriebenen Vorschriften zum Schutz digitaler Assets zu erfüllen. SnapLock-Lizenzen sind Teil des "[ONTAP One](#)" Softwaresuite:

SnapLock wird auf allen AFF und FAS Systemen sowie auf ONTAP Select unterstützt. SnapLock ist keine rein softwarebasierte Lösung, sondern eine integrierte Hardware- und Softwarelösung. Diese Auszeichnung ist wichtig für strenge WORM-Vorgaben wie SEC 17a-4, die eine integrierte Hardware- und Softwarelösung erfordert. Weitere Informationen finden Sie unter "[SEC-Interpretation: Elektronische Speicherung von Broker-Dealer Records](#)".

Ihre Möglichkeiten mit SnapLock

Nachdem Sie SnapLock konfiguriert haben, können Sie die folgenden Aufgaben ausführen:

- "Übertragung von Dateien an DIE WORM-Funktion"
- "Versetzen von Snapshot Kopien in WORM für Sekundärspeicher"
- "SPIEGELN VON WORM-Dateien für das Disaster Recovery"
- "BEWAHREN SIE WORM-Dateien bei Rechtsstreitigkeiten mithilfe der gesetzlichen Aufbewahrung auf"
- "LÖSCHEN SIE WORM-Dateien mit der Funktion „privilegiertes Löschen“"
- "Legen Sie den Aufbewahrungszeitraum für Dateien fest"
- "SnapLock Volumes werden verschoben"
- "Sperren einer Snapshot Kopie zum Schutz vor Ransomware-Angriffen"
- "Prüfen der Verwendung von SnapLock mit dem Überwachungsprotokoll"
- "Verwenden Sie SnapLock-APIs"

SnapLock Compliance und Enterprise Modi

Die SnapLock Compliance- und Enterprise-Modi unterscheiden sich hauptsächlich dadurch, wie der jeweilige Modus WORM-Dateien schützt:

SnapLock-Modus	Sicherungsstufe	WORM-Datei wird während der Aufbewahrung gelöscht
Compliance-Modus	Auf Dateiebene	Kann nicht gelöscht werden
Enterprise-Modus	Auf Festplattenebene	Kann vom Compliance-Administrator mit einem geprüften „privilegierten Löschen“ Verfahren gelöscht werden

Nach Ablauf des Aufbewahrungszeitraums sind Sie für das Löschen aller Dateien verantwortlich, die Sie nicht mehr benötigen. Sobald eine Datei im WORM-Modus oder im Enterprise-Modus versetzt wurde, kann sie auch nach dem Ablauf des Aufbewahrungszeitraums nicht mehr verändert werden.

SIE können EINE WORM-Datei nicht während oder nach dem Aufbewahrungszeitraum verschieben. Sie können eine WORM-Datei kopieren, die Kopie behält jedoch ihre WORM-Merkmale nicht bei.

Die folgende Tabelle zeigt die Unterschiede in den von SnapLock Compliance und Enterprise-Modi unterstützten Funktionen:

Dar	SnapLock-Compliance	SnapLock Enterprise
Aktivieren und löschen Sie Dateien mit privilegierter Löschung	Nein	Ja.
Festplatten neu initialisieren	Nein	Ja.
Zerstören Sie SnapLock Aggregate und Volumes während der Aufbewahrungsdauer	Nein	Ja, mit Ausnahme des SnapLock Revisionsprotokoll-Volumes

Benennen Sie Aggregate oder Volumes um	Nein	Ja.
Verwenden Sie nicht NetApp Festplatten	Nein	Ja (mit "FlexArray Virtualisierung")
Verwenden Sie das SnapLock Volume zur Audit-Protokollierung	Ja.	Ja, ab ONTAP 9.5

Unterstützte und nicht unterstützte Funktionen in SnapLock

Die folgende Tabelle zeigt die Funktionen, die von SnapLock Compliance-Modus, SnapLock Enterprise-Modus oder beiden unterstützt werden:

Merkmal	Unterstützt durch SnapLock Compliance	Unterstützt durch SnapLock Enterprise
Konsistenzgruppen	Nein	Nein
Verschlüsselte Volumes	Ja, ab ONTAP 9.2. Weitere Informationen zu Verschlüsselung und SnapLock .	Ja, ab ONTAP 9.2. Weitere Informationen zu Verschlüsselung und SnapLock .
FabricPool auf SnapLock Aggregaten	Nein	Ja, ab ONTAP 9.8. Weitere Informationen zu FabricPool auf SnapLock Enterprise-Aggregaten .
Flash Pool-Aggregate	Ja, ab ONTAP 9.1.	Ja, ab ONTAP 9.1.
FlexClone	Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen.	Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen.
FlexGroup Volumes	Ja, ab ONTAP 9.11.1. Weitere Informationen zu [flexgroup] .	Ja, ab ONTAP 9.11.1. Weitere Informationen zu [flexgroup] .
LUNs	Nein Weitere Informationen zu LUN-Unterstützung Mit SnapLock.	Nein Weitere Informationen zu LUN-Unterstützung Mit SnapLock.
MetroCluster Konfigurationen	Ja, ab ONTAP 9.3. Weitere Informationen zu MetroCluster Support .	Ja, ab ONTAP 9.3. Weitere Informationen zu MetroCluster Support .
Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV)	Ja, ab ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung .	Ja, ab ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung .

San	Nein	Nein
SnapRestore mit einer Datei	Nein	Ja.
SnapMirror Business Continuity	Nein	Nein
SnapRestore	Nein	Ja.
SMTape	Nein	Nein
SnapMirror Synchronous	Nein	Nein
SSDs	Ja, ab ONTAP 9.1.	Ja, ab ONTAP 9.1.
Funktionen für effizienteren Storage	Ja, ab ONTAP 9.9.1. Weitere Informationen zu Support für Storage-Effizienz .	Ja, ab ONTAP 9.9.1. Weitere Informationen zu Support für Storage-Effizienz .

FabricPool auf SnapLock Enterprise-Aggregaten

FabricPool werden ab ONTAP 9.8 auf SnapLock Enterprise Aggregaten unterstützt. Ihr Account-Team muss jedoch eine Anfrage zu Produktabweichungen stellen, die Ihnen dokumentieren, dass FabricPool Daten zu einer Public oder Private Cloud nicht mehr durch SnapLock geschützt sind, da ein Cloud-Administrator diese Daten löschen kann.



Daten, die FabricPool-Tiers in eine Public oder Private Cloud übertragen, werden von SnapLock nicht mehr geschützt, da diese Daten von einem Cloud-Administrator gelöscht werden können.

FlexGroup Volumes

SnapLock unterstützt FlexGroup Volumes ab ONTAP 9.11.1. Die folgenden Funktionen werden jedoch nicht unterstützt:

- Gesetzliche Aufbewahrungspflichten
- Ereignisbasierte Aufbewahrung
- SnapLock for SnapVault (unterstützt ab ONTAP 9.12.1)

Sie sollten auch die folgenden Verhaltensweisen beachten:

- Die Volume Compliance-Uhr (VCC) eines FlexGroup-Volumes wird durch den VCC der Root-Komponente bestimmt. Alle nicht-Root-Bestandteile werden ihren VCC eng mit dem Root-VCC synchronisiert.
- Die SnapLock-Konfigurationseigenschaften werden nur auf der gesamten FlexGroup festgelegt. Einzelne Komponenten können nicht über unterschiedliche Konfigurationseigenschaften verfügen, z. B. Standardaufbewahrungszeit und automatische Verschiebungszeit.

LUN-Unterstützung

LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen auf einem nicht-SnapLock Volume erstellte Snapshot Kopien 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 Snapshot Kopien werden jedoch auf SnapMirror Quell-Volumes und Ziel-Volumes unterstützt, die LUNs enthalten.

MetroCluster Support

Die SnapLock-Unterstützung in MetroCluster Konfigurationen unterscheidet sich zwischen dem SnapLock-Compliance-Modus und dem SnapLock Enterprise-Modus.

SnapLock-Compliance

- Ab ONTAP 9.3 wird SnapLock Compliance auf nicht gespiegelten MetroCluster-Aggregaten unterstützt.
- Ab ONTAP 9.3 wird SnapLock Compliance auf gespiegelten Aggregaten unterstützt, allerdings nur, wenn das Aggregat SnapLock-Audit-Protokoll-Volumes hostet.
- SVM-spezifische SnapLock-Konfigurationen können mit MetroCluster auf primäre und sekundäre Standorte repliziert werden.

SnapLock Enterprise

- Ab ONTAP 9 werden SnapLock Enterprise Aggregate unterstützt.
- Ab ONTAP 9.3 werden SnapLock Enterprise-Aggregate mit privilegierten Löschen unterstützt.
- SVM-spezifische SnapLock-Konfigurationen können mithilfe von MetroCluster zu beiden Standorten repliziert werden.

MetroCluster-Konfigurationen und Compliance-Uhren

Bei MetroCluster-Konfigurationen werden zwei Compliance-Takt-Mechanismen zum Einsatz kommen, Volume Compliance Clock (VCC) und System Compliance Clock (SCC). Das VCC und das SCC sind für alle SnapLock-Konfigurationen verfügbar. Wenn Sie ein neues Volume auf einem Node erstellen, wird sein VCC mit dem aktuellen Wert des SCC auf diesem Node initialisiert. Nach der Erstellung des Volumes wird die Aufbewahrungszeit für Volumes und Dateien immer mit dem VCC verfolgt.

Wenn ein Volume an einen anderen Standort repliziert wird, wird auch dessen VCC repliziert. Wenn eine Volume-Umschaltung stattfindet, wird z. B. von Standort A nach Standort B der VCC weiterhin an Standort B aktualisiert, während der SCC an Standort A stoppt, wenn Standort A offline geht.

Wenn Standort A wieder online geschaltet wird und das Volume zurückgeschaltet wird, startet die SCC-Uhr des Standorts A neu, während der VCC des Volumes weiterhin aktualisiert wird. Da der VCC kontinuierlich aktualisiert wird, unabhängig von Umschalttakten und Switchback-Vorgängen, hängen die Aufbewahrungszeiten der Dateien nicht von SCC-Uhren ab und dehnen sich nicht aus.

Unterstützung für die Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV)

Ab ONTAP 9.13.1 kann ein Cluster-Administrator die Verifizierung mehrerer Administratoren auf einem Cluster explizit aktivieren, sodass vor der Ausführung einiger SnapLock-Vorgänge eine Quorumgenehmigung erforderlich ist. Wenn die MAV aktiviert ist, müssen SnapLock Volume-Eigenschaften wie Default-Retention-Time, Minimum-Retention-Time, Maximum-Retention-Time, Volume-Append-Mode, Autocommit-Period und Privileged-delete genehmigt werden. Weitere Informationen zu ["MAV"](#).

Storage-Effizienz

Ab ONTAP 9.9 unterstützt SnapLock Storage-Effizienzfunktionen wie Data-Compaction, Volume-übergreifende Deduplizierung und die anpassungsfähige Komprimierung für SnapLock Volumes und Aggregate. Weitere Informationen zur Storage-Effizienz finden Sie unter ["Logisches Storage-Management – Übersicht mit der CLI"](#).

Verschlüsselung

ONTAP bietet sowohl Software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Storage-Medium neu verwendet, zurückgegeben, verloren gegangen oder gestohlen wird.

Haftungsausschluss: NetApp kann nicht garantieren, dass SnapLock-geschützte WORM-Dateien auf selbstverschlüsselnden Laufwerken oder Volumes abgerufen werden können, wenn der Authentifizierungsschlüssel verloren geht oder die Anzahl fehlgeschlagener Authentifizierungsversuche das festgelegte Limit überschreitet und eine dauerhafte Sperrung des Laufwerks zur Folge hat. Sie sind für die Gewährleistung gegen Authentifizierungsfehler verantwortlich.



Ab ONTAP 9.2 werden verschlüsselte Volumes von SnapLock Aggregaten unterstützt.

Umstieg Von 7-Mode

Sie können SnapLock Volumes von 7-Mode auf ONTAP migrieren, indem Sie die Copy-Based Transition (CBT)-Funktion des 7-Mode Transition Tools verwenden. Der SnapLock-Modus des Ziel-Volume, Compliance oder Enterprise, muss dem SnapLock-Modus des Quell-Volume entsprechen. Sie können SnapLock Volumes nicht mit Copy-Free Transition (CFT) migrieren.

Konfigurieren Sie SnapLock

Konfigurieren Sie SnapLock

Bevor Sie SnapLock verwenden, müssen Sie SnapLock konfigurieren, indem Sie verschiedene Aufgaben wie ausführen ["Installieren Sie die SnapLock-Lizenz"](#) Initialisieren Sie für jeden Node, der ein Aggregat mit einem SnapLock Volume hostet, das ["Compliance-Uhr"](#), Ein SnapLock-Aggregat für Cluster erstellen, auf denen ONTAP-Versionen vor ONTAP 9.10.1 laufen, ["Erstellen und Mounten eines SnapLock Volumes"](#), Und vieles mehr.

Initialisieren Sie die Compliance-Uhr

SnapLock verwendet die *Volume Compliance Clock*, um sicherzustellen, dass sich die Aufbewahrungsfrist für WORM-Dateien ändern kann. Sie müssen zuerst auf jedem Knoten, der ein SnapLock-Aggregat hostet, das *System ComplianceClock* initialisieren.

Ab ONTAP 9.14.1 können Sie die System-Compliance-Uhr initialisieren oder neu initialisieren, wenn keine SnapLock-Volumes oder keine Volumes vorhanden sind, für die Snapshot-Kopie gesperrt ist. Durch die Möglichkeit der Neuinitialisierung können Systemadministratoren die Compliance-Uhr des Systems in Fällen zurücksetzen, in denen sie möglicherweise falsch initialisiert wurde oder die Taktabweichung auf dem System korrigiert wurde. In ONTAP 9.13.1 und früheren Versionen können Sie die Compliance-Uhr nicht erneut

initialisieren, sobald Sie die Compliance-Uhr auf einem Knoten initialisiert haben.

Bevor Sie beginnen

So initialisieren Sie die Compliance-Uhr neu:

- Alle Nodes im Cluster müssen sich in einem ordnungsgemäßen Zustand befinden.
- Alle Volumes müssen online sein.
- In der Wiederherstellungswarteschlange können keine Volumes vorhanden sein.
- Es können keine SnapLock Volumes vorhanden sein.
- Es können keine Volumes mit aktivierter Snapshot-Kopiersperrung vorhanden sein.

Allgemeine Anforderungen für die Initialisierung der Compliance Clock:

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- ["Die SnapLock-Lizenz muss auf dem Knoten installiert sein"](#).

Über diese Aufgabe

Die Zeit auf dem System Compliance Clock wird von der *Volume Compliance Clock* übernommen, von der Letzteres die Aufbewahrungsfrist für WORM-Dateien auf dem Volume steuert. Die Volume-Compliance-Uhr wird automatisch initialisiert, wenn Sie ein neues SnapLock-Volume erstellen.



Die anfängliche Einstellung der System-Compliance-Clock basiert auf der aktuellen Hardware-Systemuhr. Aus diesem Grund sollten Sie überprüfen, ob die Systemzeit und die Zeitzone korrekt sind, bevor Sie die System-Compliance-Uhr auf jedem Knoten initialisieren. Sobald Sie die Compliance-Uhr des Systems auf einem Node initialisiert haben, können Sie sie nicht erneut initialisieren, wenn SnapLock-Volumes oder Volumes mit aktivierter Sperrung vorhanden sind.

Schritte

Sie können die ONTAP-CLI verwenden, um die Compliance-Uhr zu initialisieren, oder Sie können ab ONTAP 9.12.1 die Compliance-Uhr mit dem System-Manager initialisieren.

System Manager

1. Navigieren Sie zu **Cluster > Übersicht**.
2. Klicken Sie im Abschnitt **Knoten** auf **SnapLock-Konformitätsuhr initialisieren**.
3. Um die Spalte **Compliance Clock** anzuzeigen und zu überprüfen, ob die Compliance Clock initialisiert ist, klicken Sie im Abschnitt **Cluster > Übersicht > Knoten** auf **Einblenden/Ausblenden** und wählen **SnapLock-Konformitätsuhr** aus.

CLI

1. Initialisieren Sie die System-Compliance-Uhr:

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

Mit dem folgenden Befehl wird die Systemkonformität-Uhr auf initialisiert node1:

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

2. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass die Systemuhr korrekt ist und dass Sie die Compliance-Uhr initialisieren möchten:

```
Warning: You are about to initialize the secure ComplianceClock of  
the node "node1" to the current value of the node's system clock.  
This procedure can be performed only once on a given node, so you  
should ensure that the system time is set correctly before  
proceeding.
```

```
The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016
```

```
Do you want to continue? (y|n): y
```

3. Wiederholen Sie diese Vorgehensweise für jeden Node, der ein SnapLock Aggregat hostet.

Aktivieren Sie die Neusynchronisierung der Compliance Clock für ein NTP-konfiguriertes System

Sie können die SnapLock-Funktion zur Zeitsynchronisierung aktivieren, wenn ein NTP-Server konfiguriert ist.

Was Sie benötigen

- Diese Funktion ist nur auf der erweiterten Berechtigungsebene verfügbar.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- ["Die SnapLock-Lizenz muss auf dem Knoten installiert sein"](#).
- Diese Funktion ist nur für Cloud Volumes ONTAP-, ONTAP Select- und VSIM-Plattformen verfügbar.

Über diese Aufgabe

Wenn der SnapLock Secure Clock Daemon eine Schräglage entdeckt, die über den Schwellenwert hinausgeht, verwendet ONTAP die Systemzeit, um die System- und Volume Compliance-Uhren

zurückzusetzen. Als Schwellwert wird ein Zeitraum von 24 Stunden festgelegt. Das bedeutet, dass die System-Compliance-Uhr nur dann mit der Systemuhr synchronisiert wird, wenn die Schräglage älter als einen Tag ist.

Der SnapLock Secure Clock-Daemon erkennt einen Schräglauf und ändert die Compliance Clock in die Systemzeit. Jeder Versuch, die Systemzeit so zu ändern, dass die Compliance-Uhr mit der Systemzeit synchronisiert wird, schlägt fehl, da die Compliance-Uhr nur dann mit der Systemzeit synchronisiert wird, wenn die Systemzeit mit der NTP-Zeit synchronisiert ist.

Schritte

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

```
snaplock compliance-clock ntp
```

Mit dem folgenden Befehl wird die Funktion zur Synchronisierung der Systemkonformität-Uhrzeit aktiviert:

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

2. Bestätigen Sie bei der entsprechenden Aufforderung, dass die konfigurierten NTP-Server vertrauenswürdig sind und der Kommunikationskanal sicher ist, um die Funktion zu aktivieren:
3. Überprüfen Sie, ob die Funktion aktiviert ist:

```
snaplock compliance-clock ntp show
```

Mit dem folgenden Befehl wird überprüft, ob die Funktion zur Synchronisierung der Systemkonformität-Zeituhr aktiviert ist:

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

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

Erstellen Sie ein SnapLock Aggregat

Sie verwenden die Lautstärke `-snaplock-type` Option zum Festlegen eines Volume-Typs für Compliance oder Enterprise SnapLock. Bei älteren Versionen als ONTAP 9.10.1 müssen Sie ein separates SnapLock Aggregat erstellen. Ab ONTAP 9.10.1 können SnapLock- und nicht-SnapLock-Volumes auf demselben Aggregat vorhanden sein. Wenn Sie ONTAP 9.10.1 verwenden, sind Sie daher nicht mehr erforderlich, ein separates SnapLock Aggregat zu erstellen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Das SnapLock ["Lizenz muss installiert sein"](#) Auf dem Node. Diese Lizenz ist in enthalten ["ONTAP One"](#).
- ["Die Compliance Clock auf dem Knoten muss initialisiert werden"](#).
- Wenn Sie die Festplatten mit „root“, „data1“ und „data2“ partitioniert haben, müssen Sie sicherstellen, dass Ersatzfestplatten verfügbar sind.

Upgrade-Überlegungen

Bei einem Upgrade auf ONTAP 9.10.1 werden vorhandene SnapLock und Aggregate anderer Anbieter aktualisiert, um sowohl SnapLock als auch nicht SnapLock Volumes zu unterstützen. Die vorhandenen SnapLock Volume-Attribute werden jedoch nicht automatisch aktualisiert. So bleiben beispielsweise Felder für Data-Compaction, Volume-übergreifende Deduplizierung und Volume-übergreifende Hintergrund-Deduplizierung unverändert. Neue SnapLock Volumes, die auf vorhandenen Aggregaten erstellt wurden, verfügen über dieselben Standardwerte wie nicht-SnapLock-Volumes, und die Standardwerte für neue Volumes und Aggregate sind plattformabhängig.

Überlegungen zurücksetzen

Wenn Sie auf eine ältere ONTAP Version als 9.10.1 zurücksetzen müssen, müssen Sie alle SnapLock-Compliance-, SnapLock Enterprise- und SnapLock-Volumes auf ihre eigenen SnapLock Aggregate verschieben.

Über diese Aufgabe

- Sie können keine Compliance-Aggregate für FlexArray LUNs erstellen, doch SnapLock-Compliance-Aggregate werden mit FlexArray LUNs unterstützt.
- Mit der Option SyncMirror können keine Compliance-Aggregate erstellt werden.
- Sie können gespiegelte Compliance-Aggregate in einer MetroCluster-Konfiguration nur dann erstellen, wenn das Aggregat SnapLock-Audit-Protokoll-Volumes hostet.



In einer MetroCluster-Konfiguration wird SnapLock Enterprise auf gespiegelten und nicht gespiegelten Aggregaten unterstützt. SnapLock Compliance wird nur auf nicht gespiegelten Aggregaten unterstützt.

Schritte

1. Erstellung eines SnapLock Aggregats:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>  
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

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

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

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

SnapLock Volumes erstellen und mounten

Sie müssen ein SnapLock-Volume für die Dateien oder Snapshot-Kopien erstellen, die Sie in DEN WORM-Zustand versetzen möchten. Ab ONTAP 9.10.1 wird jedes der erstellten Volumes unabhängig vom Aggregattyp standardmäßig als nicht-SnapLock Volume erstellt. Sie müssen den verwenden `-snaplock-type` Option zum explizit Erstellen eines SnapLock-Volumes, indem entweder Compliance oder Enterprise als

SnapLock-Typ angegeben werden. Standardmäßig ist der SnapLock-Typ auf festgelegt `non-snaplock`.

Bevor Sie beginnen

- Das SnapLock Aggregat muss online sein.
- Sollten Sie "[Vergewissern Sie sich, dass eine SnapLock-Lizenz installiert ist](#)". Wenn auf dem Node keine SnapLock-Lizenz installiert ist, müssen Sie diese ausführen "[Installieren](#)". Es. Diese Lizenz ist in enthalten "[ONTAP One](#)". Vor ONTAP One war die SnapLock-Lizenz im Paket für Sicherheit und Compliance enthalten. Das Paket „Sicherheit und Compliance“ wird nicht mehr angeboten, ist aber weiterhin gültig. Bestehende Kunden können diese Option wählen, obwohl sie derzeit nicht benötigt werden "[Upgrade auf ONTAP One](#)".
- "[Die Compliance Clock auf dem Knoten muss initialisiert werden](#)".

Über diese Aufgabe

Mit den entsprechenden SnapLock Berechtigungen können Sie ein Enterprise-Volume jederzeit zerstören oder umbenennen. Sie können ein Compliance-Volumen erst zerstören, wenn der Aufbewahrungszeitraum abgelaufen ist. Ein Compliance-Volume kann nie umbenannt werden.

Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen. Das geklonte Volume hat den gleichen SnapLock-Typ wie das übergeordnete Volume.



LUNs werden in SnapLock Volumes nicht unterstützt. LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen auf einem nicht-SnapLock Volume erstellte Snapshot Kopien 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 Snapshot Kopien werden jedoch auf SnapMirror Quell-Volumes und Ziel-Volumes unterstützt, die LUNs enthalten.

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

System Manager

Ab ONTAP 9.12.1 können Sie mit System Manager ein SnapLock Volume erstellen.

Schritte

1. Navigieren Sie zu **Storage > Volumes** und klicken Sie auf **Hinzufügen**.
2. Klicken Sie im Fenster **Volume hinzufügen** auf **Weitere Optionen**.
3. Geben Sie die neuen Volume-Informationen ein, einschließlich Name und Größe des Volumes.
4. Wählen Sie **SnapLock aktivieren** und wählen Sie den SnapLock-Typ entweder Compliance oder Enterprise.
5. Wählen Sie im Abschnitt **Auto-Commit Files** die Option **Modified** aus und geben Sie den Zeitraum ein, in dem eine Datei unverändert bleiben soll, bevor sie automatisch aktiviert wird. Der Mindestwert beträgt 5 Minuten und der Höchstwert beträgt 10 Jahre.
6. Wählen Sie im Abschnitt **Datenspeicherung** den minimalen und maximalen Aufbewahrungszeitraum aus.
7. Wählen Sie den Standardaufbewahrungszeitraum aus.
8. Klicken Sie Auf **Speichern**.
9. Wählen Sie auf der Seite **Volumes** das neue Volume aus, um die SnapLock-Einstellungen zu überprüfen.

CLI

1. SnapLock Volume erstellen:

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

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

Mit dem folgenden Befehl wird eine SnapLock erstellt Compliance Volume mit Namen `vol1` Ein `aggr1` Ein `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1  
-snaplock-type compliance
```

Mounten Sie ein SnapLock Volume

Ein SnapLock Volume kann für den NAS-Client-Zugriff im SVM Namespace an einen Verbindungspfad gemountet werden.

Was Sie benötigen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

- Ein SnapLock Volume kann nur unter dem Root-Verzeichnis der SVM gemountet werden.
- Ein normales Volume kann nicht unter einem SnapLock Volume gemountet werden.

Schritte

1. Mounten eines SnapLock Volume:

```
volume mount -vserver SVM_name -volume volume_name -junction-path path
```

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

Mit dem folgenden Befehl wird ein SnapLock-Volume mit dem Namen `vol1` zum Verbindungspfad `/sales` im `vs1` Namespace:

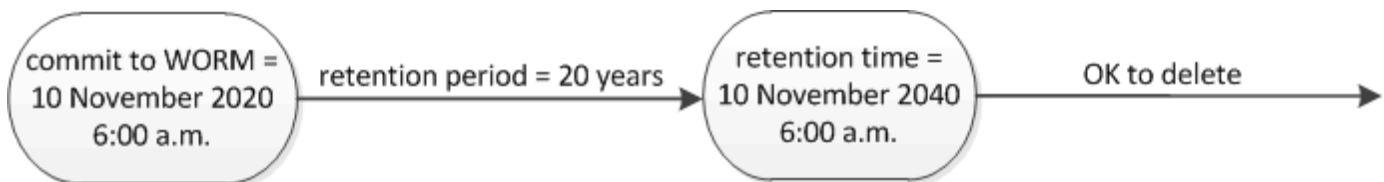
```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

Aufbewahrungszeit einstellen

Sie können die Aufbewahrungszeit für eine Datei explizit festlegen oder den Standardaufbewahrungszeitraum für das Volume verwenden, um die Aufbewahrungszeit abzuleiten. Wenn Sie die Aufbewahrungszeit nicht explizit festlegen, verwendet SnapLock den Standardaufbewahrungszeitraum zur Berechnung der Aufbewahrungszeit. Sie können auch die Dateiaufbewahrung nach einem Ereignis festlegen.

Allgemeines zu Aufbewahrungszeitraum und Aufbewahrungszeit

Der `_Aufbewahrungszeitraum_` für EINE WORM-Datei gibt die Zeitspanne an, die die Datei nach dem Festlegen des WORM-Status aufbewahrt werden muss. Die *Aufbewahrungszeit* für EINE WORM-Datei ist die Zeit, nach der die Datei nicht mehr aufbewahrt werden muss. Eine Aufbewahrungsfrist von 20 Jahren für eine Datei, die am 10. November 2020 6:00 Uhr im WORM-Zustand aufbewahrt wird, würde beispielsweise eine Aufbewahrungszeit vom 10. November 2040 6:00 Uhr erreichen



Ab ONTAP 9.10.1 können Sie eine Aufbewahrungszeit bis zum 26. Oktober 3058 und eine Aufbewahrungsfrist von bis zu 100 Jahren festlegen. Wenn Sie die Aufbewahrungszeiträume verlängern, werden ältere Richtlinien automatisch konvertiert. In ONTAP 9.9.1 und früheren Versionen, sofern Sie den Standard-Aufbewahrungszeitraum nicht auf unendlich eingestellt, ist die maximale unterstützte Aufbewahrungszeit Januar 19 2071 (GMT).

Wichtige Überlegungen zur Replizierung

Wenn Sie eine SnapMirror Beziehung mit einem SnapLock Quell-Volume unter Verwendung eines Aufbewahrungsdatums später als dem 19. Januar 2071 (GMT) aufbauen, muss das Ziel-Cluster ONTAP 9.10.1 oder höher ausführen. Sonst schlägt der SnapMirror Transfer fehl.

Wichtige Überlegungen zum Wechsel

ONTAP verhindert, dass Sie einen Cluster von ONTAP 9.10.1 auf eine frühere ONTAP-Version zurücksetzen, wenn es Dateien mit einer Aufbewahrungsfrist später als „Januar 19, 2071 8:44:07“ gibt.

Die Aufbewahrungsfristen verstehen

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

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

Ab ONTAP 9.8 können Sie die Aufbewahrungsfrist für Dateien in einem Volume auf einstellen `unspecified`. Um die Datei so lange zu speichern, bis Sie eine absolute Aufbewahrungszeit festgelegt haben. Sie können eine Datei mit absoluter Aufbewahrungszeit auf unbestimmte Aufbewahrung und zurück zur absoluten Aufbewahrung setzen, solange die neue absolute Aufbewahrungszeit später ist als die zuvor festgelegte absolute Zeit.

Ab ONTAP 9.12.1 SIND WORM-Dateien, deren Aufbewahrungszeitraum auf festgelegt ist `unspecified`. Sie haben für das SnapLock Volume eine Aufbewahrungsfrist festgelegt, die auf der für das Mindestaufbewahrungszeitraum konfiguriert ist. Wenn Sie den Aufbewahrungszeitraum für die Datei von `unspecified` Um eine absolute Aufbewahrungszeit zu erreichen, muss die angegebene neue Aufbewahrungszeit größer sein als die für die Datei bereits festgelegte Mindestaufbewahrungszeit.

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

Legen Sie den Standardaufbewahrungszeitraum fest

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

Was Sie benötigen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

In der folgenden Tabelle sind die möglichen Werte für die Option Standardaufbewahrungszeitraum aufgeführt:



Der Standardaufbewahrungszeitraum muss größer oder gleich (\geq) dem Mindestaufbewahrungszeitraum und kleiner als oder gleich (\leq) dem maximalen Aufbewahrungszeitraum sein.

Wert	Einheit	Hinweise
0 bis 65535	Sekunden	
0 bis 24	Stunden	
0 bis 365	Tage	
0 bis 12	Monaten	
0 bis 100	Jahren	Ab ONTAP 9.10.1 Bei früheren Versionen von ONTAP beträgt der Wert 0 - 70.
maximale	-	Verwenden Sie den maximalen Aufbewahrungszeitraum.
Mindestens	-	Verwenden Sie den Mindestaufbewahrungszeitraum.
Skalierbar	-	Bewahren Sie die Dateien für immer auf.
Nicht angegeben	-	Bewahren Sie die Dateien so lange auf, bis ein absoluter Aufbewahrungszeitraum festgelegt ist.

Die Werte und Bereiche für die maximale und minimale Aufbewahrungsdauer sind identisch, mit Ausnahme von `max` und `min`, die nicht anwendbar sind. Weitere Informationen zu dieser Aufgabe finden Sie unter ["Stellen Sie die Übersicht über die Aufbewahrungszeit ein"](#).

Sie können das `volume snaplock show` Befehl zum Anzeigen der Einstellungen für den Aufbewahrungszeitraum für das Volume. Weitere Informationen finden Sie auf der man-Page für den Befehl.



Nachdem eine Datei im WORM-Status übergeben wurde, können Sie den Aufbewahrungszeitraum verlängern, jedoch nicht verkürzen.

Schritte

1. Legen Sie den Standardaufbewahrungszeitraum für Dateien auf einem SnapLock-Volume fest:

```
volume snaplock modify -vserver SVM_name -volume volume_name -default  
-retention-period default_retention_period -minimum-retention-period  
min_retention_period -maximum-retention-period max_retention_period
```

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



In den folgenden Beispielen wird davon ausgegangen, dass die minimalen und maximalen Aufbewahrungszeiträume zuvor nicht geändert wurden.

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für Compliance- oder Enterprise-Volumes auf 20 Tage festgelegt:

```
cluster1::> volume snaplock modify -vserver vs1 -volume voll1 -default  
-retention-period 20days
```

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für ein Compliance-Volume auf 70 Jahre festgelegt:

```
cluster1::> volume snaplock modify -vserver vs1 -volume voll1 -maximum  
-retention-period 70years
```

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für ein Enterprise-Volume auf 10 Jahre festgelegt:

```
cluster1::> volume snaplock modify -vserver vs1 -volume voll1 -default  
-retention-period max -maximum-retention-period 10years
```

Mit den folgenden Befehlen wird die Standardaufbewahrungsdauer für Enterprise-Volumes auf 10 Tage festgelegt:

```
cluster1::> volume snaplock modify -vserver vs1 -volume voll1 -minimum  
-retention-period 10days  
cluster1::> volume snaplock modify -vserver vs1 -volume voll1 -default  
-retention-period min
```

Mit dem folgenden Befehl wird die Standardaufbewahrungsdauer für ein Compliance-Volume auf „skalierbar“ gesetzt:

```
cluster1::> volume snaplock modify -vserver vs1 -volume voll1 -default  
-retention-period infinite -maximum-retention-period infinite
```

Legen Sie die Aufbewahrungszeit für eine Datei explizit fest

Sie können die Aufbewahrungszeit für eine Datei explizit festlegen, indem Sie die letzte Zugriffszeit ändern. Sie können jeden entsprechenden Befehl oder jedes Programm über NFS oder CIFS verwenden, um die Uhrzeit des letzten Zugriffs zu ändern.

Über diese Aufgabe

Nachdem eine Datei an WORM übergeben wurde, können Sie die Aufbewahrungszeit verlängern, aber nicht verkürzen. Die Aufbewahrungszeit wird im gespeichert `atime` Feld für die Datei.



Sie können die Aufbewahrungszeit einer Datei nicht explizit auf festlegen *infinite*. Dieser Wert ist nur verfügbar, wenn Sie den Standardaufbewahrungszeitraum zur Berechnung der Aufbewahrungszeit verwenden.

Schritte

1. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um die letzte Zugriffszeit für die Datei zu ändern, deren Aufbewahrungszeit Sie einstellen möchten.

Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Aufbewahrungszeit vom 21. November 2020 6:00 Uhr festzulegen In einer Datei mit dem Namen `document.txt`:

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



Sie können alle geeigneten Befehle oder Programme verwenden, um die letzte Zugriffszeit in Windows zu ändern.

Legen Sie den Aufbewahrungszeitraum für die Datei nach einem Ereignis fest

Ab ONTAP 9.3 können Sie definieren, wie lange eine Datei nach einem Ereignis aufbewahrt wird, indem Sie die Funktion *SnapLock Event Based Retention (EBR)* verwenden.

Was Sie benötigen

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

["Erstellen Sie ein SnapLock-Administratorkonto"](#)

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

Über diese Aufgabe

Die Richtlinie `_Event Retention_` definiert den Aufbewahrungszeitraum für die Datei nach dem Ereignis. Die Richtlinie kann auf eine einzelne Datei oder alle Dateien in einem Verzeichnis angewendet werden.

- Handelt es sich bei einer Datei nicht um EINE WORM-Datei, wird sie im IN der Richtlinie definierten Aufbewahrungszeitraum im WORM-Status versetzt.
- Wenn es sich bei einer Datei um EINE WORM-Datei oder EINE WORM-Dateien handelt, verlängert sich deren Aufbewahrungszeitraum um den in der Richtlinie definierten Aufbewahrungszeitraum.

Es können ein Compliance-Modus oder ein Enterprise-Mode Volume verwendet werden.



EBR-Richtlinien können nicht auf Dateien angewendet werden, die sich in einer Legal Hold befinden.

Weitere Informationen zur erweiterten Verwendung finden Sie unter ["Worm-Speicherung gemäß NetApp SnapLock"](#).

Verwendung von EBR, um den Aufbewahrungszeitraum bereits vorhandener WORM-Dateien zu verlängern

EBR ist praktisch, wenn Sie den Aufbewahrungszeitraum bereits vorhandener WORM-Dateien verlängern möchten. So könnte es z. B. sein, dass Ihr Unternehmen die Richtlinie hat, W-4-Datensätze von Mitarbeitern in unveränderter Form für drei Jahre zu speichern, nachdem der Mitarbeiter eine Quellwahl geändert hat. Eine andere Unternehmensrichtlinie kann verlangen, dass W-4-Datensätze fünf Jahre nach Beendigung des Mitarbeiters aufbewahrt werden.

In diesem Fall könnten Sie eine EBR-Richtlinie mit einer Aufbewahrungsfrist von fünf Jahren erstellen. Nach Beendigung des Mitarbeiters (das „Event“) wenden Sie die EBR-Richtlinie auf den W-4-Datensatz des Mitarbeiters an, wodurch die Aufbewahrungsfrist verlängert wird. Das ist in der Regel einfacher als die manuelle Verlängerung des Aufbewahrungszeitraums, insbesondere dann, wenn eine große Anzahl von Dateien beteiligt ist.

Schritte

1. EBR-Richtlinie erstellen:

```
snaplock event-retention policy create -vserver SVM_name -name policy_name -retention-period retention_period
```

Mit dem folgenden Befehl wird die EBR-Richtlinie erstellt `employee_exit` Ein `vs1` Mit einer Aufbewahrungsfrist von zehn Jahren:

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name employee_exit -retention-period 10years
```

2. Anwenden einer EBR-Richtlinie:

```
snaplock event-retention apply -vserver SVM_name -name policy_name -volume volume_name -path path_name
```

Der folgende Befehl wendet die EBR-Richtlinie an `employee_exit` Ein `vs1` Zu allen Dateien im Verzeichnis `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name employee_exit -volume voll1 -path /d1
```

Erstellen eines Prüfprotokolls

Bei Nutzung von ONTAP 9.9.1 oder einer älteren Version müssen Sie zunächst ein SnapLock Aggregat erstellen und anschließend ein SnapLock geschütztes Revisionsprotokoll erstellen, bevor Sie eine privilegierte Löschung oder SnapLock-Volume-Verschiebung durchführen. Das Revisionsprotokoll erfasst die Erstellung und Löschung von SnapLock-Administratorkonten, Änderungen an dem Protokoll-Volume, die Aktivierung und das Löschen privilegierter Vorgänge sowie die Verschiebung von SnapLock Volumes.

Ab ONTAP 9.10.1 erstellen Sie kein SnapLock Aggregat mehr. Sie müssen für die Option `-snaplock-type`

verwenden ["Explizit ein SnapLock Volume erstellen"](#) Indem Sie als SnapLock-Typ entweder Compliance oder Enterprise angeben.

Bevor Sie beginnen

Wenn Sie ONTAP 9.9.1 oder eine frühere Version verwenden, müssen Sie zum Erstellen eines SnapLock Aggregats Cluster-Administrator sein.

Über diese Aufgabe

Sie können ein Überwachungsprotokoll erst löschen, wenn der Aufbewahrungszeitraum für die Protokolldatei abgelaufen ist. Sie können ein Überwachungsprotokoll auch nach Ablauf des Aufbewahrungszeitraums nicht ändern. Dies gilt sowohl für SnapLock Compliance als auch für den Enterprise-Modus.



In ONTAP 9.4 und früher können Sie ein SnapLock Enterprise Volume nicht zur Audit-Protokollierung verwenden. Sie müssen ein SnapLock-Compliance-Volume verwenden. In ONTAP 9.5 und höher können Sie entweder ein SnapLock Enterprise Volume oder ein SnapLock Compliance Volume zur Audit-Protokollierung verwenden. In allen Fällen muss das Protokoll-Volume am Verbindungspfad angehängt werden `/snaplock_audit_log`. Kein anderes Volume kann diesen Verbindungspfad verwenden.

Die SnapLock-Prüfprotokolle finden Sie im `/snaplock_log` Verzeichnis unter dem Stammverzeichnis des Audit-Log-Volumes, in Unterverzeichnissen mit Namen `privdel_log` (Privilegierte Löschvorgänge) und `system_log` (Alles andere). Die Namen von Audit-Log-Dateien enthalten den Zeitstempel der ersten protokollierten Operation und erleichtern so die Suche nach Datensätzen bis zu dem Zeitpunkt, zu dem die Vorgänge durchgeführt wurden.

- Sie können das verwenden `snaplock log file show` Befehl zum Anzeigen der Protokolldateien auf dem Audit-Protokoll-Volume.
- Sie können das verwenden `snaplock log file archive` Befehl, um die aktuelle Protokolldatei zu archivieren und eine neue zu erstellen, was in Fällen nützlich ist, in denen Audit-Log-Informationen in einer separaten Datei aufgezeichnet werden müssen.

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



Ein Datensicherungs-Volume kann nicht als SnapLock-Audit-Protokoll-Volume verwendet werden.

Schritte

1. Erstellen Sie ein SnapLock Aggregat.

[Erstellen Sie ein SnapLock Aggregat](#)

2. Erstellen Sie für die SVM, die Sie für die Audit-Protokollierung konfigurieren möchten, ein SnapLock Volume.

[SnapLock Volume erstellen](#)

3. SVM für Audit-Protokollierung konfigurieren:

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
-size size -retention-period default_retention_period
```



Die Mindestaufbewahrungsdauer für Audit-Log-Dateien beträgt sechs Monate. Wenn die Aufbewahrungsfrist einer betroffenen Datei länger als die Aufbewahrungsfrist des Prüfprotokolls ist, erbt die Aufbewahrungsfrist des Protokolls die Aufbewahrungsfrist der Datei. Wenn also die Aufbewahrungsfrist für eine mit privilegierter Löschung gelöschte Datei 10 Monate beträgt und die Aufbewahrungsdauer des Prüfprotokolls 8 Monate beträgt, verlängert sich die Aufbewahrungsfrist des Protokolls auf 10 Monate. Weitere Informationen zur Aufbewahrungszeit und zum Standardaufbewahrungszeitraum finden Sie unter ["Aufbewahrungszeit einstellen"](#).

Die Konfiguration mit dem folgenden Befehl wird konfiguriert SVM1 Für die Audit-Protokollierung mit dem SnapLock Volume logVol. Das Prüfprotokoll hat eine maximale Größe von 20 GB und wird acht Monate lang aufbewahrt.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size 20GB -retention-period 8months
```

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

[Mounten Sie ein SnapLock Volume](#)

Überprüfen Sie die SnapLock-Einstellungen

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

Schritte

1. Generieren eines Dateiprints:

```
volume file fingerprint start -vserver SVM_name -file file_path
```

```
svml1::> volume file fingerprint start -vserver svml -file /vol/sle/vol/fl  
File fingerprint operation is queued. Run "volume file fingerprint show -session-id 16842791" to view the fingerprint session status.
```

Der Befehl generiert eine Session-ID, die Sie als Eingaben in den verwenden können `volume file fingerprint dump` Befehl.



Sie können das verwenden `volume file fingerprint show` Befehl mit der Session-ID zum Überwachen des Fortschritts des Fingerabdruckvorgangs. Vergewissern Sie sich, dass der Vorgang abgeschlossen ist, bevor Sie versuchen, den Fingerabdruck anzuzeigen.

2. Zeigen Sie den Fingerabdruck für die Datei an:

volume file fingerprint dump -session-id *session_ID*

```
svml:> volume file fingerprint dump -session-id 33619976
Vserver:svml
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/fl
Data
Fingerprint:MOFJVEvxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfylg=Metadata

Fingerprint:8iMjqJXiNcggXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
    Fingerprint Scope:data-and-metadata
    Fingerprint Start Time:1460612586
    Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
    Fingerprint Version:3
    **SnapLock License:available**
    Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
    Volume MSID:2152884007
    Volume DSID:1028
    Hostname:my_host
    Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
    Volume Containing Aggregate:slc_aggr1
    Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
    **SnapLock System ComplianceClock:1460610635
    Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
    Volume SnapLock Type:compliance
    Volume ComplianceClock:1460610635
    Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
    Volume Expiry Date:1465880998**
    Is Volume Expiry Date Wraparound:false
    Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
    Filesystem ID:1028
    File ID:96
    File Type:worm
    File Size:1048576
    Creation Time:1460612515
    Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
    Modification Time:1460612515
    Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
    Changed Time:1460610598
    Is Changed Time Wraparound:false
    Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
    Retention Time:1465880998
    Is Retention Time Wraparound:false
```

```
Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
Access Time:-
Formatted Access Time:-
Owner ID:0
Group ID:0
Owner SID:-
Fingerprint End Time:1460612586
Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

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 ComplianceClock Time wird in geschrieben `ctime` Feld der Datei, wenn der Befehl oder das Programm ausgeführt wird. Die ComplianceClock-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	-

Wert	Einheit	Hinweise
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 $n \times 256 \text{ KB} + 1$ 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 Vault-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 in SnapLock Volumes nicht unterstützt. LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen auf einem nicht-SnapLock Volume erstellte Snapshot Kopien 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 Snapshot Kopien werden jedoch auf SnapMirror Quell-Volumes und Ziel-Volumes unterstützt, die LUNs enthalten.

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

Ab ONTAP 9.13.1 können Sie sofort eine gesperrte Snapshot Kopie auf dem Ziel-SnapLock Volume einer SnapLock Vault-Beziehung wiederherstellen, indem Sie einen FlexClone mit dem erstellen `snaplock-type` Option auf „nicht-snaplock“ gesetzt und die Snapshot Kopie als „Parent-Snapshot“ bei der Ausführung des Volume-Klonerstellungsvorgangs angeben. Weitere Informationen zu ["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

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 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 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. 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 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 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 dstvol1B 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 voll1:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume  
voll1 -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 Privileged 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 Privileged 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 SVMsVM1:

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

SnapLock Volumes werden verschoben

Ab ONTAP 9.8 können Sie ein SnapLock Volume zu einem Zielaggregat desselben Typs verschieben: Von Enterprise zu Enterprise oder Compliance zu Compliance. Zum

Verschieben eines SnapLock Volumes muss Ihnen die SnapLock-Sicherheitsrolle zugewiesen werden.

Erstellen Sie ein SnapLock-Sicherheitsadministratorkonto

Zum Verschieben eines SnapLock Volumes müssen Sie über SnapLock-Sicherheitsadministratorrechte verfügen. Dieses Privileg wird Ihnen mit der im ONTAP 9.8 eingeführten *SnapLock*-Rolle gewährt. Wenn Sie dieser Rolle noch nicht zugewiesen wurden, können Sie den Cluster-Administrator bitten, einen SnapLock-Sicherheitsbenutzer mit dieser SnapLock-Sicherheitsrolle 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.

Über diese Aufgabe

die SnapLock-Rolle ist mit der Admin-SVM verbunden – im Gegensatz zur vsadmin-snaplock-Rolle, die mit der Daten-SVM verknüpft ist.

Schritt

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 snaplock Rolle für den Zugriff auf Admin-SVM cluster1 Verwenden eines Passworts:

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

SnapLock Volumes werden verschoben

Sie können das verwenden `volume move` Befehl zum Verschieben eines SnapLock Volume in ein Zielaggregat.

Was Sie benötigen

- Vor der Verschiebung eines SnapLock Volumes müssen Sie ein SnapLock-geschütztes Prüfprotokoll erstellt haben.

["Erstellen eines Prüfprotokolls"](#).

- Wenn Sie eine ältere Version von ONTAP als ONTAP 9.10.1 verwenden, muss das Zielaggregat den gleichen SnapLock-Typ sein wie das SnapLock Volume, das Sie verschieben möchten: Compliance zu Compliance oder Enterprise zu Enterprise. Ab ONTAP 9.10.1 wurde diese Einschränkung entfernt und ein Aggregat kann sowohl Compliance- als auch Enterprise SnapLock Volumes enthalten, die nicht von SnapLock stammen.
- Sie müssen ein Benutzer mit der Sicherheitsrolle „SnapLock“ sein.

Schritte

1. Melden Sie sich über eine sichere Verbindung bei der ONTAP Cluster-Management-LIF an:

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Verschieben eines SnapLock Volumes:

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination  
-aggregate destination_aggregate_name
```

3. Prüfen Sie den Status der Volume-Verschiebung:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields  
volume,phase,vserver
```

Sperrern einer Snapshot Kopie zum Schutz vor Ransomware-Angriffen

Ab ONTAP 9.12.1 können Sie eine Snapshot-Kopie auf einem nicht-SnapLock-Volume sperren, um vor Ransomware-Angriffen zu schützen. Das Sperren von Snapshot-Kopien sorgt dafür, dass sie nicht versehentlich oder versehentlich gelöscht werden können.

Mithilfe der SnapLock-Funktion für Compliance-Uhren können Sie Snapshot-Kopien für einen bestimmten Zeitraum sperren, damit sie bis zum Erreichen der Verfallszeit nicht gelöscht werden können. Durch das Sperren von Snapshot-Kopien sind sie vor Ransomware-Bedrohungen geschützt. Mit gesperrten Snapshot-Kopien können Daten wiederhergestellt werden, falls ein Volume durch einen Ransomware-Angriff kompromittiert wird.

Ab ONTAP 9.14.1 unterstützt die Sperrung von Snapshot Kopien zur langfristigen Aufbewahrung von Snapshot Kopien auf SnapLock Vault-Zielen und auf nicht-SnapLock SnapMirror Ziel-Volumes. Die Sperrung von Snapshot Kopien wird aktiviert, indem die Aufbewahrungsfrist mithilfe von SnapMirror Richtlinien festgelegt wird, die mit einem verknüpft sind [Vorhandene Richtlinienbezeichnung](#). Die Regel überschreibt den auf dem Volume festgelegten Standardaufbewahrungszeitraum. Wenn dem SnapMirror-Label keine Aufbewahrungsfrist zugeordnet ist, wird die Standardaufbewahrungsdauer des Volume verwendet.

Überlegungen und Überlegungen zu Snapshot Kopien vor Manipulationen

- Wenn Sie die ONTAP-CLI verwenden, muss auf allen Nodes im Cluster ONTAP 9.12.1 oder höher ausgeführt werden. Wenn Sie System Manager verwenden, muss auf allen Nodes ONTAP 9.13.1 oder höher ausgeführt werden.
- ["Die SnapLock-Lizenz muss auf dem Cluster installiert sein"](#). Diese Lizenz ist in enthalten ["ONTAP One"](#).
- ["Die Compliance-Uhr auf dem Cluster muss initialisiert werden"](#).
- Wenn die Snapshot-Sperrung auf einem Volume aktiviert ist, können Sie die Cluster auf eine ONTAP Version später als ONTAP 9.12.1 aktualisieren. Sie können jedoch nicht auf eine frühere Version von ONTAP zurücksetzen, bis alle gesperrten Snapshot Kopien ihr Ablaufdatum erreicht haben und gelöscht werden und das Sperren von Snapshot Kopien deaktiviert ist.
- Wenn ein Snapshot gesperrt ist, wird die Ablaufzeit des Volumes auf die Ablaufzeit der Snapshot Kopie festgelegt. Wenn mehr als eine Snapshot Kopie gesperrt ist, gibt die Ablaufzeit des Volumes unter allen Snapshot Kopien die höchste Ablaufzeit wieder.
- Der Aufbewahrungszeitraum für gesperrte Snapshot Kopien hat Vorrang vor der Anzahl der Snapshots.

Dies bedeutet, dass die zulässige Anzahl von Kopien nicht beachtet wird, wenn der Aufbewahrungszeitraum für gesperrte Snapshot Kopien nicht abgelaufen ist.

- In einer SnapMirror Beziehung können Sie einen Aufbewahrungszeitraum für eine Richtlinie mit Spiegelungs-Vault festlegen. Der Aufbewahrungszeitraum wird für Snapshot Kopien, die auf dem Ziel-Volume repliziert werden, angewendet, wenn die Sperrung der Snapshot Kopien aktiviert ist. Der Aufbewahrungszeitraum hat Vorrang vor der Datenanzahl. Beispielsweise werden Snapshot Kopien, die ihren Ablaufdatum nicht bestanden haben, auch dann beibehalten, wenn die behalten wird.
- Sie können eine Snapshot-Kopie auf einem nicht-SnapLock-Volume umbenennen. Umbenennungsvorgänge für Snapshots auf dem primären Volume einer SnapMirror-Beziehung werden nur auf dem sekundären Volume wiedergegeben, wenn die Richtlinie MirrorAllSnapshots ist. Bei anderen Richtlinien wird die umbenannte Snapshot Kopie während Updates nicht propagiert.
- Wenn Sie die ONTAP CLI verwenden, können Sie eine gesperrte Snapshot Kopie mit dem wiederherstellen `volume snapshot restore` Befehl nur, wenn die gesperrte Snapshot Kopie das aktuellste ist. Wenn später noch nicht abgelaufene Snapshot Kopien als der wiederherzustellende Snapshot Kopie vorhanden sind, schlägt der Wiederherstellungsvorgang für die Snapshot Kopie fehl.

Funktionen, die durch manipulationssichere Snapshot Kopien unterstützt werden

- FlexGroup Volumes

Die Sperrung von Snapshot Kopien wird auf FlexGroup Volumes unterstützt. Das Sperren von Snapshots erfolgt nur auf der Snapshot-Kopie der Root-Komponente. Das Löschen des FlexGroup-Volume ist nur zulässig, wenn die Ablaufzeit der Root-Komponente abgelaufen ist.

- Konvertierung von FlexVol zu FlexGroup

Sie können ein FlexVol Volume mit gesperrten Snapshot Kopien in ein FlexGroup Volume konvertieren. Snapshot-Kopien bleiben nach der Konvertierung gesperrt.

- Volume-Klon und Dateiklon

Sie können Volume-Klone und Dateiklone aus einer gesperrten Snapshot Kopie erstellen.

Nicht unterstützte Funktionen

Die folgenden Funktionen werden derzeit nicht durch manipulationssichere Snapshot Kopien unterstützt:

- Cloud Volumes ONTAP
- Konsistenzgruppen
- FabricPool
- FlexCache Volumes
- SMTape
- SnapMirror Business Continuity (SM-BC)
- SnapMirror Richtlinie regeln mithilfe der `-schedule` Parameter
- SnapMirror Synchronous
- SVM-Datenmobilität (verwendet für die Migration oder Verschiebung einer SVM von einem Quell-Cluster zu einem Ziel-Cluster)

Aktivieren Sie die Sperrung von Snapshot Kopien bei der Erstellung eines Volume

Ab ONTAP 9.12.1 können Sie die Sperrung von Snapshot Kopien aktivieren, wenn Sie ein neues Volume erstellen oder ein vorhandenes Volume mithilfe von ändern `-snapshot-locking-enabled` Option mit dem `volume create` Und `volume modify` Befehle in der CLI. Ab ONTAP 9.13.1 können Sie System Manager verwenden, um die Sperrung von Snapshot Kopien zu aktivieren.

System Manager

1. Navigieren Sie zu **Storage > Volumes** und wählen Sie **Add**.
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. Wählen Sie **Snapshot sperren aktivieren**. Diese Auswahl wird nicht angezeigt, wenn die SnapLock-Lizenz nicht installiert ist.
5. Wenn sie noch nicht aktiviert ist, wählen Sie **SnapLock-Compliance-Uhr initialisieren** aus.
6. Speichern Sie die Änderungen.
7. Wählen Sie im Fenster **Volumes** das Volume aus, das Sie aktualisiert haben, und wählen Sie **Übersicht**.
8. Vergewissern Sie sich, dass **SnapLock Snapshot Copy Locking** als **aktiviert** angezeigt wird.

CLI

1. Geben Sie den folgenden Befehl ein, um ein neues Volume zu erstellen und das Sperren von Snapshot Kopien zu aktivieren:

```
volume create -vserver vs1 -volume vol1 -snapshot-locking-enabled true
```


Mit dem folgenden Befehl wird das Sperren von Snapshot Kopien auf einem neuen Volume namens vol1 aktiviert:

```
> volume create -volume voll1 -aggregate aggr1 -size 100m -snapshot-locking-enabled true
Warning: Snapshot copy locking is being enabled on volume "voll1" in Vserver "vs1". It cannot be disabled until all locked Snapshot copies are past their expiry time. A volume with unexpired locked Snapshot copies cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

Aktivieren Sie die Sperrung von Snapshot Kopien auf einem vorhandenen Volume

Ab ONTAP 9.12.1 können Sie die Sperre von Snapshot Kopien auf einem vorhandenen Volume mithilfe der ONTAP CLI aktivieren. Ab ONTAP 9.13.1 können Sie System Manager verwenden, um die Sperrung von Snapshot Kopien für ein vorhandenes Volume zu aktivieren.

System Manager

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie  Und wählen Sie **Bearbeiten > Lautstärke**.
3. Suchen Sie im Fenster **Volume bearbeiten** den Abschnitt Snapshot-Kopien (Lokal) Einstellungen und wählen Sie **Snapshot-Sperrung aktivieren** aus.

Diese Auswahl wird nicht angezeigt, wenn die SnapLock-Lizenz nicht installiert ist.

4. Wenn sie noch nicht aktiviert ist, wählen Sie **SnapLock-Compliance-Uhr initialisieren** aus.
5. Speichern Sie die Änderungen.
6. Wählen Sie im Fenster **Volumes** das Volume aus, das Sie aktualisiert haben, und wählen Sie **Übersicht**.
7. Vergewissern Sie sich, dass **SnapLock Snapshot Copy Locking** als **aktiviert** angezeigt wird.

CLI

1. Geben Sie den folgenden Befehl ein, um ein vorhandenes Volume zu ändern, um das Sperren von Snapshot Kopien zu aktivieren:

```
volume modify -vserver vserver_name -volume volume_name -snapshot-locking  
-enabled true
```

Erstellen Sie eine Richtlinie für gesperrte Snapshot Kopien und wenden Sie die Aufbewahrung an

Ab ONTAP 9.12.1 können Sie Richtlinien für Snapshot Kopien erstellen, um eine Aufbewahrungsdauer für Snapshot Kopien anzuwenden und die Richtlinie auf ein Volume anzuwenden, um Snapshot Kopien für den angegebenen Zeitraum zu sperren. Sie können eine Snapshot-Kopie auch sperren, indem Sie manuell einen Aufbewahrungszeitraum festlegen. Ab ONTAP 9.13.1 können Sie mit System Manager Sperrrichtlinien für Snapshot Kopien erstellen und diese auf ein Volume anwenden.

Erstellen Sie eine Sperrrichtlinie für Snapshot Kopien

System Manager

1. Navigieren Sie zu **Storage > Storage VMs** und wählen Sie eine Storage VM aus.
2. Wählen Sie **Einstellungen**.
3. Suchen Sie **Snapshot Policies** und wählen Sie aus ➔.
4. Geben Sie im Fenster **Add Snapshot Policy** den Richtliniennamen ein.
5. Wählen Sie **+ Add**.
6. Geben Sie die Planungsdetails für Snapshot Kopien an, einschließlich des Planungsnamens, der maximalen Anzahl der zu haltenden Snapshot-Kopien und der Aufbewahrungsdauer von SnapLock.
7. Geben Sie in der Spalte **SnapLock Aufbewahrungsfrist** die Anzahl der Stunden, Tage, Monate oder Jahre ein, die die Snapshot Kopien behalten sollen. Eine Richtlinie für Snapshot Kopien beispielsweise mit einer Aufbewahrungsfrist von 5 Tagen sperrt eine Snapshot Kopie 5 Tage nach dem Erstellen und kann in dieser Zeit nicht gelöscht werden. Folgende Aufbewahrungszeiträume werden unterstützt:
 - Jahre: 0 - 100
 - Monate: 0 - 1200
 - Tage: 0 - 36500
 - Öffnungszeiten: 0 - 24
8. Speichern Sie die Änderungen.

CLI

1. Geben Sie den folgenden Befehl ein, um eine Snapshot Kopie-Richtlinie zu erstellen:

```
volume snapshot policy create -policy policy_name -enabled true -schedule1  
schedule1_name -count1 maximum_Snapshot_copies -retention-period1  
_retention_period
```


Mit dem folgenden Befehl wird eine Sperrrichtlinie für Snapshot-Kopien erstellt:

```
cluster1> volume snapshot policy create -policy policy_name -enabled  
true -schedule1 hourly -count1 24 -retention-period1 "1 days"
```

Eine Snapshot-Kopie wird nicht ersetzt, wenn sie unter aktiver Aufbewahrung liegt. Das heißt, die Aufbewahrungszahl wird nicht gewürdigt, wenn gesperrte Snapshot-Kopien noch nicht abgelaufen sind.

Wenden Sie eine Sperrrichtlinie auf ein Volume an

System Manager

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie  Und wählen Sie **Bearbeiten > Lautstärke**.
3. Wählen Sie im Fenster **Volume bearbeiten** die Option **Snapshot-Kopien planen** aus.
4. Wählen Sie in der Liste die Richtlinie zum Sperren von Snapshot Kopien aus.
5. Falls die Snapshot Kopie-Sperrung noch nicht aktiviert ist, wählen Sie **Snapshot-Sperrung aktivieren** aus.
6. Speichern Sie die Änderungen.

CLI

1. Geben Sie den folgenden Befehl ein, um eine Sperrrichtlinie für Snapshot Kopien auf ein vorhandenes Volume anzuwenden:

```
volume modify -volume volume_name -vserver vserver_name -snapshot-policy policy_name
```

Wenden Sie den Aufbewahrungszeitraum während der Erstellung manueller Snapshot Kopien an

Sie können einen Aufbewahrungszeitraum für Snapshot Kopien anwenden, wenn Sie manuell eine Snapshot Kopie erstellen. Die Sperrung der Snapshot Kopie muss auf dem Volume aktiviert sein, anderenfalls wird die Einstellung für den Aufbewahrungszeitraum ignoriert.

System Manager

1. Navigieren Sie zu **Speicher > Volumes** und wählen Sie ein Volume aus.
2. Wählen Sie auf der Seite Volume Details die Registerkarte **Snapshot Copies** aus.
3. Wählen Sie **+ Add**.
4. Geben Sie den Namen der Snapshot Kopie und die SnapLock Ablaufzeit ein. Sie können den Kalender auswählen, um das Ablaufdatum und die Uhrzeit für die Aufbewahrung auszuwählen.
5. Speichern Sie die Änderungen.
6. Wählen Sie auf der Seite **Volumes > Snapshot-Kopien ein-/Ausblenden** und wählen Sie **SnapLock-Ablaufzeit**, um die Spalte **SnapLock-Ablaufzeit** anzuzeigen und zu überprüfen, ob die Aufbewahrungszeit eingestellt ist.

CLI

1. Geben Sie den folgenden Befehl ein, um eine Snapshot Kopie manuell zu erstellen und einen Aufbewahrungszeitraum für Sperrungen anzuwenden:


```
volume snapshot create -volume volume_name -snapshot snapshot_copy_name  
-snaplock-expiry-time expiration_date_time
```

Mit dem folgenden Befehl wird eine neue Snapshot Kopie erstellt und der Aufbewahrungszeitraum festgelegt:

```
cluster1> volume snapshot create -vserver vs1 -volume voll -snapshot  
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

Wenden Sie den Aufbewahrungszeitraum auf eine vorhandene Snapshot Kopie an

System Manager

1. Navigieren Sie zu **Speicher > Volumes** und wählen Sie ein Volume aus.
2. Wählen Sie auf der Seite Volume Details die Registerkarte **Snapshot Copies** aus.
3. Wählen Sie die Snapshot Kopie aus und wählen Sie aus , Und wählen Sie **SnapLock-Ablaufzeit ändern**. Sie können den Kalender auswählen, um das Ablaufdatum und die Uhrzeit für die Aufbewahrung auszuwählen.
4. Speichern Sie die Änderungen.
5. Wählen Sie auf der Seite **Volumes > Snapshot-Kopien ein-/Ausblenden** und wählen Sie **SnapLock-Ablaufzeit**, um die Spalte **SnapLock-Ablaufzeit** anzuzeigen und zu überprüfen, ob die Aufbewahrungszeit eingestellt ist.

CLI

1. Geben Sie den folgenden Befehl ein, um einen Aufbewahrungszeitraum manuell auf eine vorhandene Snapshot Kopie anzuwenden:

```
volume snapshot modify-snaplock-expiry-time -volume volume_name -snapshot snapshot_copy_name -expiry-time expiration_date_time
```

Im folgenden Beispiel wird ein Aufbewahrungszeitraum für eine vorhandene Snapshot Kopie angewendet:

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume voll1 -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
```

Ändern Sie eine vorhandene Richtlinie, um die langfristige Aufbewahrung anzuwenden

Ab ONTAP 9.14.1 können Sie eine vorhandene SnapMirror Richtlinie ändern, indem Sie eine Regel hinzufügen, um die langfristige Aufbewahrung von Snapshot-Kopien festzulegen. Die Regel wird verwendet, um den Standardaufbewahrungszeitraum des Volumes auf SnapLock Vault-Zielen und auf nicht-SnapLock SnapMirror Ziel-Volumes außer Kraft zu setzen.

1. Fügen Sie einer vorhandenen SnapMirror-Richtlinie eine Regel hinzu:

```
snapmirror policy add-rule -vserver <SVM name> -policy <policy name> -snapmirror-label <label name> -keep <number of Snapshot copies> -retention-period [<integer> days|months|years]
```

Im folgenden Beispiel wird eine Regel erstellt, die eine Aufbewahrungsfrist von 6 Monaten auf die vorhandene Richtlinie namens „lockvault“ anwendet:

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror-label test1 -keep 10 -retention-period "6 months"
```

SnapLock APIs

Zephyr-APIs lassen sich in SnapLock-Funktionen in Skripten oder in die Workflow-Automatisierung integrieren. Die APIs verwenden XML-Messaging über HTTP, HTTPS und Windows DCE/RPC. Weitere Informationen finden Sie unter ["Dokumentation zur ONTAP-Automatisierung"](#).

Datei-Fingerabdruck-Abbruch

Abbrechen eines Fingerabdruckvorgangs für die Datei.

Datei-Fingerabdruck-Dump

Anzeigen von Fingerabdruckinformationen für Dateien

Datei-Fingerabdruck-get-iter

Zeigt den Status von Datei-Fingerabdruckoperationen an.

Starten von Datei-Fingerabdruck

Generieren eines DateiFingerabdrucks.

snaplock-ArchivvServer-Protokoll

Archivieren Sie die aktive Audit-Log-Datei.

snaplock-create-vserver-log

Erstellen einer Auditprotokollkonfiguration für eine SVM

snaplock-delete-vServer-Protokoll

Löschen einer Audit-Protokollkonfiguration für eine SVM

snaplock-Datei mit Privileged-delete

Führen Sie einen privilegierten Löschvorgang aus.

snaplock-Get-Retention

Erhalten Sie den Aufbewahrungszeitraum einer Datei.

snaplock-get-Node-Compliance-Clock

Abrufen des Knotens ComplianceClock Datum und Uhrzeit.

snaplock-get-vserver-aktiv-log-files-iter

Zeigt den Status der aktiven Protokolldateien an.

snaplock-get-vserver-log-iter

Zeigt die Konfiguration des Prüfprotokolls an.

snaplock-modify-vserver-log

Ändern der Konfiguration des Prüfprotokolls für eine SVM

snaplock-Set-file-Retention

Aufbewahrungszeit für eine Datei festlegen.

snaplock-Set-Node-Compliance-Clock

Stellen Sie das Datum und die Uhrzeit des Knotens ComplianceClock ein.

snaplock-Volume-set-privilegiert-delete

Legen Sie die Option Privileged-delete für ein SnapLock Enterprise Volume fest.

Volume-get-snaplock-attrs

Erhalten Sie die Attribute eines SnapLock Volume.

Volume-Set-snaplock-attrs

Legen Sie die Attribute eines SnapLock-Volumes fest.

Copyright-Informationen

Copyright © 2024 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 IRGEND EINER 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.