Datenschutz und Notfallwiederherstellung

ONTAP 9

NetApp
November 14, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/peering/index.html on November 14, 2026. Always check docs.netapp.com for the latest.

Inhalt

Datenschutz und Notfallwiederherstellung . . . 1
- Cluster- und SVM-Peering . . . 1
  - Informationen zu ONTAP Cluster und SVM Peering . . . 1
  - Vorbereitung auf Cluster- und SVM-Peering . . . 1
  - Intercluster-LIFs konfigurieren . . . 5
  - Peer-Beziehungen konfigurieren . . . 17
  - ONTAP Cluster Peer-Verschlüsselung für Peer-Beziehungen aktivieren . . . 25
  - ONTAP Cluster-Peering-Verschlüsselung aus den Peer-Beziehungen entfernen . . . 25
- Lokale Snapshots verwalten . . . 26
  - Informationen zur Verwaltung lokaler ONTAP Snapshots . . . 27
  - Informationen zu ONTAP Langzeitaufbewahrungs-Snapshots . . . 27
  - Benutzerdefinierte Snapshot-Richtlinien konfigurieren . . . 28
  - Snapshots manuell verwalten . . . 31
  - Snapshot Reserve verwalten . . . 34
  - Dateien aus Snapshots wiederherstellen . . . 38
- SnapMirror Volume-Replikation . . . 43
  - Informationen zur SnapMirror Volumenreplikation . . . 44
  - Konfiguration der SnapMirror Volume-Replikation . . . 74
  - Konfiguration Ihres ONTAP Systems für die Backend-Replizierung über FC . . . 94
  - Replikation von SnapMirror Volumes verwalten . . . 98
- SVM-Replikation von SnapMirror verwalten . . . 127
  - Informationen zu ONTAP SnapMirror SVM-Replizierung . . . 127
  - SVM Konfigurationen replizieren . . . 133
  - Daten von einem SnapMirror SVM DR Ziel bereitstellen . . . 146
  - Die SnapMirror Quelle-SVM reaktivieren . . . 150
  - Konvertieren einer ONTAP SnapMirror Volumenbeziehung zu einer SVM-Beziehung . . . 163
  - Ändern der Zielvolumenkapazität in einer ONTAP SVM DR Beziehung . . . 164
  - Löschen einer ONTAP SnapMirror SVM-Replikationsbeziehung . . . 165
- Replikation des SnapMirror Stammvolumes verwalten . . . 167
  - Informationen zur Replikation des ONTAP SnapMirror Root-Volumes . . . 167
  - ONTAP Load-Sharing Mirror-Beziehungen erstellen und initialisieren . . . 167
  - Aktualisierung einer ONTAP Load-Sharing Mirror Beziehung . . . 169
  - Eine ONTAP Load-Sharing Mirror befördern . . . 169
- In die Cloud sichern . . . 171
  - Installation einer ONTAP SnapMirror Cloud-Lizenz . . . 171
  - Daten in der Cloud mit ONTAP SnapMirror Cloud sichern . . . 172
  - Sicherung von ONTAP Daten mit NetApp Backup and Recovery . . . 175
- Archivierung und Compliance mithilfe von SnapLock Technologie . . . 176
  - Erfahren Sie mehr über ONTAP SnapLock . . . 176
  - SnapLock konfigurieren . . . 181
  - WORM-Dateien verwalten . . . 195
  - Verschieben eines ONTAP SnapLock Volumes . . . 211
  - Einen ONTAP Snapshot zum Schutz vor Ransomware-Angriffen sperren . . . 212

Konsistenzgruppen . . . 219
Informationen zu ONTAP Konsistenzgruppen . . . 219
Objektgrenzen für ONTAP Konsistenzgruppen . . . 225
Eine einzelne ONTAP Konsistenzgruppe konfigurieren . . . 227
Eine hierarchische ONTAP Konsistenzgruppe konfigurieren . . . 230
ONTAP Konsistenzgruppen schützen . . . 233
Mitgliedsvolumes in einer ONTAP Konsistenzgruppe ändern . . . 243
ONTAP Konsistenzgruppen-Geometrie ändern . . . 248
ONTAP Konsistenzgruppe: Anwendungs- und Komponententags bearbeiten . . . 253
Klonen einer ONTAP Konsistenzgruppe . . . 254
Löschen einer ONTAP Konsistenzgruppe . . . 256
SnapMirror Active Sync . . . 257
Einführung . . . 257
Planen . . . 272
Konfigurieren . . . 283
Aktive Synchronisierung von SnapMirror verwalten und Daten schützen . . . 327
Fehlerbehebung . . . 345
Informationen zu ONTAP Mediator für MetroCluster IP und SnapMirror active sync . . . 355
Informationen zur MetroCluster IP-Standortverwaltung mit ONTAP System Manager . . . 355
Datensicherung mit Tape-Backup . . . 356
Informationen zum Tape-Backup von ONTAP FlexVol Volumes . . . 356
ONTAP Tape-Backup und Wiederherstellungs-Workflow . . . 357
Anwendungsfälle für ONTAP SMTape und Dump Backup Engines . . . 358
Tape-Laufwerke verwalten . . . 358
Über Tape-Laufwerke . . . 363
Daten zwischen Speichersystemen übertragen . . . 372
NDMP für FlexVol Volumes . . . 376
Informationen zur NDMP-Unterstützung mit ONTAP FlexGroup Volumes . . . 401
Informationen zu NDMP mit ONTAP SnapLock Volumes . . . 402
Knotenbezogenen NDMP-Modus für FlexVol Volumes verwalten . . . 402
NDMP-Modus mit SVM-Umfang für FlexVol Volumes verwalten . . . 404
Über die Dump-Engine für FlexVol Volumes . . . 410
Informationen zur SMTape Engine für FlexVol Volumes . . . 422
Tape-Backup- und Wiederherstellungsvorgänge für FlexVol Volumes überwachen . . . 426
Fehlermeldungen für Tape-Backup und Wiederherstellung von FlexVol Volumes . . . 430
NDMP-Konfiguration . . . 450
Erfahren Sie mehr über die ONTAP NDMP-Konfiguration . . . 450
Informationen zum ONTAP NDMP Konfigurationsworkflow . . . 450
ONTAP NDMP-Konfigurationen vorbereiten . . . 451
Verbindungen von ONTAP NDMP Tape-Geräten überprüfen . . . 454
Bandreservierungen für ONTAP NDMP-Backup-Vorgänge aktivieren . . . 455
SVM-bezogenes NDMP konfigurieren . . . 455
Node-spezifisches NDMP konfigurieren . . . 464
Backup-Anwendungen für ONTAP NDMP Konfiguration konfigurieren . . . 469
Informationen zur Replikation zwischen NetApp Element software und ONTAP . . . 469

Datenschutz und Notfallwiederherstellung

Cluster- und SVM-Peering

Informationen zu ONTAP Cluster und SVM Peering

Sie können Peer-Beziehungen zwischen Quell- und Ziel-Cluster sowie zwischen Quell- und Ziel-Storage-VMs (Storage Virtual Machines) erstellen. Peer-Beziehungen zwischen diesen Entitäten müssen erstellt werden, bevor Snapshots mit SnapMirror repliziert werden können.

ONTAP 9.3 bietet Verbesserungen, die die Konfiguration von Peer-Beziehungen zwischen Clustern und SVMs vereinfachen. Die Verfahren zum Peering von Clustern und SVMs sind für alle ONTAP 9 Versionen verfügbar. Das jeweils passende Verfahren für Ihre ONTAP Version sollte verwendet werden.

Die Prozeduren werden über die Befehlszeilenschnittstelle (CLI) durchgeführt, nicht über System Manager oder ein automatisiertes Scripting-Tool.

Vorbereitung auf Cluster- und SVM-Peering

Grundlagen des ONTAP Peerings

Peer-Beziehungen zwischen Quell- und Ziel-Cluster sowie zwischen Quell- und Ziel-SVMs müssen erstellt werden, bevor Snapshots mithilfe von SnapMirror repliziert werden können. Eine Peer-Beziehung definiert Netzwerkverbindungen, die den sicheren Datenaustausch zwischen Clustern und SVMs ermöglichen.

Cluster und SVMs in Peer-Beziehungen kommunizieren über das Intercluster-Netzwerk mithilfe von *logischen Intercluster-Schnittstellen (LIFs).* Eine Intercluster-LIF ist eine LIF, die den Netzwerkschnittstellendienst „intercluster-core“ unterstützt und typischerweise mit der Netzwerkschnittstellendienstrichtlinie „default-intercluster“ erstellt wird. Intercluster-LIFs sind auf jedem Node der zu peerenden Cluster zu erstellen.

Intercluster-LIFs verwenden Routen, die zur System-SVM gehören, der sie zugewiesen sind. ONTAP erstellt automatisch eine System-SVM für Cluster-Kommunikation innerhalb eines IPspace.

Sowohl Fan-out- als auch Kaskadentopologien werden unterstützt. In einer Kaskadentopologie ist es nur erforderlich, Intercluster-Netzwerke zwischen dem primären und dem sekundären Cluster sowie zwischen dem sekundären und dem tertiären Cluster zu erstellen. Ein Intercluster-Netzwerk zwischen dem primären und dem tertiären Cluster ist nicht erforderlich.

> Es ist möglich (aber nicht empfehlenswert), dass ein Administrator den intercluster-core Service aus der default-intercluster Service-Richtlinie entfernt. Falls dies geschieht, sind mit „default-intercluster“ erstellte LIFs tatsächlich keine Intercluster-LIFs. Zur Bestätigung, dass die default-intercluster Service-Richtlinie den intercluster-core Service enthält, kann folgender Befehl verwendet werden:
>
> `network interface service-policy show -policy default-intercluster`
>
> Weitere Informationen zu `network interface service-policy show` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Voraussetzungen für ONTAP Peering

Bevor Sie Cluster-Peering einrichten, sollten Sie sicherstellen, dass die Anforderungen an Konnektivität, Port, IP-Adresse, Subnetz, Firewall und Cluster erfüllt sind.

Ab ONTAP 9.6 bietet Cluster Peering standardmäßig Unterstützung für TLS 1.2 AES-256 GCM-Verschlüsselung bei der Datenreplizierung. Die standardmäßigen Sicherheitsverschlüsselungsverfahren („PSK-AES256-GCM-SHA384“) sind für die Funktion von Cluster Peering erforderlich, selbst wenn die Verschlüsselung deaktiviert ist.

Ab ONTAP 9.11.1 sind DHE-PSK Sicherheitsverschlüsselungsverfahren standardmäßig verfügbar.

Ab ONTAP 9.15.1 bietet Cluster Peering standardmäßig Unterstützung für TLS 1.3-Verschlüsselung bei der Datenreplizierung.

Konnektivitätsanforderungen

Jede Intercluster-LIF auf dem lokalen Cluster muss mit jeder Intercluster-LIF auf dem Remote-Cluster kommunizieren können.

Obwohl es nicht zwingend erforderlich ist, ist es in der Regel einfacher, die für die Intercluster-LIFs verwendeten IP-Adressen im selben Subnetz zu konfigurieren. Die IP-Adressen können sich im selben Subnetz wie die Daten-LIFs oder in einem anderen Subnetz befinden. Das in jedem Cluster verwendete Subnetz muss die folgenden Anforderungen erfüllen:

- Das Subnetz muss zur Broadcast-Domäne gehören, die die Ports enthält, die für die Intercluster-Verbindung verwendet werden.
- Das Subnetz muss über genügend verfügbare IP-Adressen verfügen, um einer Intercluster-LIF pro Knoten eine Adresse zuzuweisen.

  Beispielsweise muss in einem Cluster mit vier Knoten das für die Intercluster-Verbindung verwendete Subnetz über vier verfügbare IP-Adressen verfügen.

Jeder Knoten muss über eine Intercluster-LIF mit einer IP-Adresse im Intercluster-Netzwerk verfügen.

Intercluster LIFs können eine IPv4-Adresse oder eine IPv6-Adresse haben.

ONTAP ermöglicht die Migration Ihrer Peering-Netzwerke von IPv4 zu IPv6, indem optional beide Protokolle gleichzeitig auf den Intercluster-LIFs vorhanden sein können. In früheren Versionen waren alle Intercluster-Beziehungen eines gesamten Clusters entweder IPv4 oder IPv6. Dies bedeutete, dass ein Protokollwechsel potenziell zu Unterbrechungen führen konnte.

Port-Anforderungen

Sie können dedizierte Ports für die Intercluster-Verbindung verwenden oder Ports gemeinsam nutzen, die vom Datennetzwerk verwendet werden. Ports müssen die folgenden Anforderungen erfüllen:

- Alle Ports, die zur Kommunikation mit einem bestimmten Remote-Cluster verwendet werden, müssen sich im selben IPspace befinden.

  Sie können mehrere IPspaces verwenden, um mit mehreren Clustern ein Peering herzustellen. Eine paarweise vollständige Mesh-Konnektivität ist nur innerhalb eines IPspaces erforderlich.

- Die Broadcast-Domäne, die für die Intercluster-Verbindung verwendet wird, muss mindestens zwei Ports pro Knoten umfassen, damit die Intercluster-Verbindung von einem Port auf einen anderen umgeschaltet werden kann.

  Ports, die zu einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Schnittstellengruppen (ifgrps) sein.

- Alle Anschlüsse müssen verkabelt sein.
- Alle Ports müssen in einem einwandfreien Zustand sein.
- Die MTU-Einstellungen der Ports müssen einheitlich sein.

Firewall-Anforderungen

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für LIFs konfigurieren".

Firewalls und die Intercluster-Firewall-Richtlinie müssen die folgenden Protokolle zulassen:

- Bidirektionaler ICMP-Verkehr
- Bidirektionaler initiierter TCP-Verkehr zu den IP-Adressen aller Intercluster-LIFs über die Ports 11104 und 11105
- Bidirektionales HTTPS zwischen den Intercluster-LIFs

  Obwohl HTTPS bei der Einrichtung des Cluster-Peerings über die CLI nicht erforderlich ist, ist HTTPS später erforderlich, wenn der System Manager zur Konfiguration des Datenschutzes verwendet wird.

Die Standard `intercluster`-Firewallrichtlinie erlaubt den Zugriff über das HTTPS-Protokoll und von allen IP-Adressen (0.0.0.0/0). Die Richtlinie kann bei Bedarf geändert oder ersetzt werden.

Cluster-Peer-Limits

Die unterstützte Anzahl von Cluster-Peers hängt von der ONTAP Version ab:

- ONTAP 9.14.1 und höher: Es werden bis zu 400 Cluster-Peers unterstützt.
- Frühere ONTAP Releases: Es werden bis zu 255 Cluster-Peers unterstützt.

```
[NOTE]
These values represent supported and validated limits. There is no
strictly enforced maximum cluster peer limit.
```

Gemeinsam genutzte oder dedizierte ONTAP Ports verwenden

Sie können dedizierte Ports für die Intercluster-Verbindung verwenden oder Ports gemeinsam nutzen, die vom Datennetzwerk verwendet werden. Bei der Entscheidung, ob Ports gemeinsam genutzt werden, sind die Netzwerkbandbreite, das Replikationsintervall und die Portverfügbarkeit zu berücksichtigen.

Ports können auf einem Peered-Cluster gemeinsam genutzt werden, während auf dem anderen

dedizierte Ports verwendet werden.

Netzwerkbandbreite

Bei einem Hochgeschwindigkeitsnetzwerk wie beispielsweise 10 GbE steht möglicherweise genügend lokale LAN-Bandbreite zur Verfügung, um die Replikation über dieselben 10 GbE Ports durchzuführen, die auch für den Datenzugriff verwendet werden.

Auch dann sollte die verfügbare WAN-Bandbreite mit der LAN-Bandbreite verglichen werden. Liegt die verfügbare WAN-Bandbreite deutlich unter 10 GbE, kann der Einsatz dedizierter Ports erforderlich sein.

Eine Ausnahme von dieser Regel könnte bestehen, wenn alle oder viele Knoten im Cluster Daten replizieren, in diesem Fall wird die Bandbreitennutzung typischerweise auf die Knoten verteilt.

Wenn Sie keine dedizierten Ports verwenden, sollte die maximale Übertragungseinheit (MTU) des Replikationsnetzwerks typischerweise der MTU des Datennetzwerks entsprechen.

Replikationsintervall

Wenn die Replikation außerhalb der Spitzenzeiten erfolgt, sollte es möglich sein, die Datenports auch ohne 10-GbE-LAN-Verbindung für die Replikation zu verwenden.

Erfolgt die Datenreplizierung während der regulären Geschäftszeiten, ist die Menge der zu replizierenden Daten sowie die Frage zu berücksichtigen, ob dafür so viel Bandbreite benötigt wird, dass es zu Konflikten mit den Datenprotokollen kommen könnte. Liegt die Netzwerkauslastung durch Datenprotokolle (SMB, NFS, iSCSI) über 50 %, empfiehlt sich die Nutzung dedizierter Ports für die Intercluster-Verbindung, um eine nicht beeinträchtigte Performance im Falle eines Knotenausfalls zu ermöglichen.

Portverfügbarkeit

Wenn Sie feststellen, dass der Replikationsverkehr den Datenverkehr beeinträchtigt, können Intercluster-LIFs auf einen beliebigen anderen Intercluster-fähigen gemeinsam genutzten Port auf demselben Knoten migriert werden.

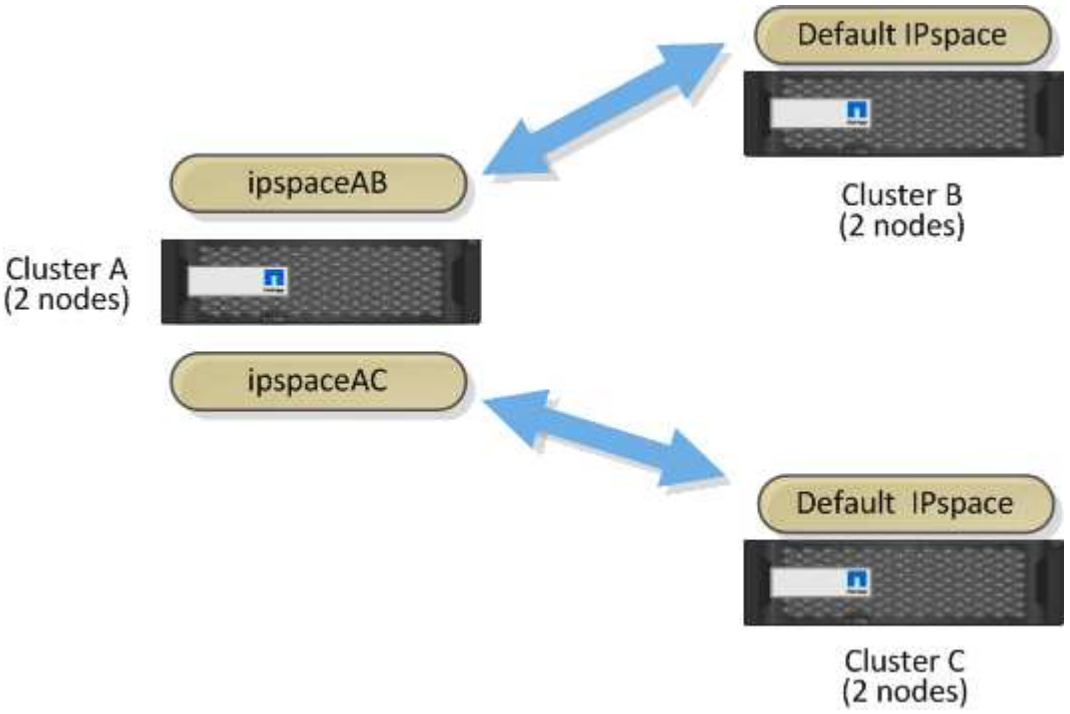
Sie können auch VLAN-Ports für die Replikation reservieren. Die Bandbreite des Ports wird zwischen allen VLANs und dem Basis-Port gemeinsam genutzt.

Benutzerdefinierte ONTAP IPspaces ermöglichen die Isolierung des Replikationsverkehrs.

Mithilfe benutzerdefinierter IPspaces lassen sich die Interaktionen eines Clusters mit seinen Peers trennen. Diese als *designated intercluster connectivity* bezeichnete Konfiguration ermöglicht es Dienstanbietern, den Replikationsverkehr in mandantenfähigen Umgebungen zu isolieren.

Angenommen, Sie möchten beispielsweise den Replikationsverkehr zwischen Cluster A und Cluster B vom Replikationsverkehr zwischen Cluster A und Cluster C trennen. Zu diesem Zweck können zwei IPspaces auf Cluster A erstellt werden.

Ein IPspace enthält die Intercluster-LIFs, die Sie zur Kommunikation mit Cluster B verwenden. Der andere enthält die Intercluster-LIFs, die Sie zur Kommunikation mit Cluster C verwenden, wie in der folgenden Abbildung zu sehen ist.



Verwandte Informationen

- "Informationen zur ONTAP IPspace Konfiguration"

Intercluster-LIFs konfigurieren

ONTAP Intercluster-LIFs auf gemeinsam genutzten Datenports konfigurieren

Intercluster-LIFs können auf Ports konfiguriert werden, die mit dem Datennetzwerk gemeinsam genutzt werden. Dadurch wird die Anzahl der für die Intercluster-Vernetzung benötigten Ports reduziert.

Schritte

1. Die Ports im Cluster werden aufgelistet:

   `network port show`

   Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Netzwerkanschlüsse in `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
```

```
        e0c       Default      Default          up     1500   auto/1000
        e0d       Default      Default          up     1500   auto/1000
cluster01-02
        e0a       Cluster      Cluster          up     1500   auto/1000
        e0b       Cluster      Cluster          up     1500   auto/1000
        e0c       Default      Default          up     1500   auto/1000
        e0d       Default      Default          up     1500   auto/1000
```

2. Intercluster-LIFs können entweder auf einer Admin-SVM (Default-IPspace) oder einer System-SVM (benutzerdefinierter IPspace) erstellt werden:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 und früher:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel erstellt Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Es sollte überprüft werden, ob die Intercluster-LIFs erstellt wurden:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface show -service-policy default-intercluster`

Option	Beschreibung
In ONTAP 9.5 und früher:	`network interface show -role intercluster`

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Es sollte sichergestellt werden, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:	`network interface show -role intercluster -failover`

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, dass die Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02` auf dem `e0c` Port auf den `e0d` Port übergehen.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
```

```
          cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

ONTAP Intercluster-LIFs auf dedizierten Ports konfigurieren

Sie können Intercluster-LIFs auf dedizierten Ports konfigurieren. Dadurch erhöht sich in der Regel die verfügbare Bandbreite für Replikationsverkehr.

Schritte

1. Die Ports im Cluster werden aufgelistet:

   `network port show`

   Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Netzwerkanschlüsse in `cluster01`:

```
cluster01::> network port show
                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Ermitteln, welche Ports für die Intercluster-Verbindung zur Verfügung stehen:

   `network interface show -fields home-port,curr-port`

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, dass Ports `e0e` und `e0f` keine LIFs zugewiesen wurden:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Eine Failover-Gruppe für die dedizierten Ports erstellen:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical _or_logical_ports`*

   Das folgende Beispiel weist Ports `e0e` und `e0f` der Failover-Gruppe `intercluster01` auf der System-SVM `cluster01` zu:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Es sollte überprüft werden, ob die Failover-Gruppe erstellt wurde:

   `network interface failover-groups show`

   Weitere Informationen zu `network interface failover-groups show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
```

```
cluster01
                  Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                  intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Intercluster-LIFs auf der System-SVM erstellen und der Failover-Gruppe zuweisen.

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home- port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover -group` *`failover_group`*
In ONTAP 9.5 und früher:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover-group` *`failover_group`*

Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel erstellt Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02` in der Failover-Gruppe `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Es sollte überprüft werden, ob die Intercluster-LIFs erstellt wurden:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:	`network interface show -role intercluster`

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Es sollte sichergestellt werden, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:	`network interface show -role intercluster -failover`

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, dass die Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02` auf dem SVM`e0e` Port auf den `e0f` Port übergehen.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
```

```
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

ONTAP Intercluster-LIFs in benutzerdefinierten IPspaces konfigurieren

Sie können Intercluster-LIFs in benutzerdefinierten IPspaces konfigurieren. Dadurch lässt sich der Replikationsverkehr in mandantenfähigen Umgebungen isolieren.

Wenn ein benutzerdefiniertes IPspace erstellt wird, erstellt das System eine systemeigene Storage Virtual Machine (SVM), die als Container für die Systemobjekte in diesem IPspace dient. Die neue SVM kann als Container für beliebige Intercluster-LIFs im neuen IPspace verwendet werden. Die neue SVM hat denselben Namen wie das benutzerdefinierte IPspace.

Schritte

1. Die Ports im Cluster werden aufgelistet:

   `network port show`

   Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Netzwerkanschlüsse in `cluster01`:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Benutzerdefinierte IPspaces auf dem Cluster erstellen:

   `network ipspace create -ipspace ipspace`

   Das folgende Beispiel erstellt den benutzerdefinierten IPspace `ipspace-IC1`:

   ```
   cluster01::> network ipspace create -ipspace ipspace-IC1
   ```

   Weitere Informationen zu `network ipspace create` finden sich in der "ONTAP-Befehlsreferenz".

3. Ermitteln, welche Ports für die Intercluster-Verbindung zur Verfügung stehen:

   `network interface show -fields home-port,curr-port`

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt, dass Ports `e0e` und `e0f` keine LIFs zugewiesen wurden:

   ```
   cluster01::> network interface show -fields home-port,curr-port
   vserver lif                  home-port curr-port
   ------- -------------------- --------- ---------
   Cluster cluster01_clus1   e0a       e0a
   Cluster cluster01_clus2   e0b       e0b
   Cluster cluster02_clus1   e0a       e0a
   Cluster cluster02_clus2   e0b       e0b
   cluster01
           cluster_mgmt         e0c       e0c
   cluster01
           cluster01-01_mgmt1   e0c       e0c
   cluster01
           cluster01-02_mgmt1   e0c       e0c
   ```

4. Die verfügbaren Ports aus der Standard Broadcast-Domäne entfernen:

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Ein Port kann nicht gleichzeitig in mehr als einer Broadcast-Domäne sein. Weitere Informationen zu `network port broadcast-domain remove-ports` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel entfernt Ports `e0e` und `e0f` aus der Standard-Broadcast-Domäne:

   ```
   cluster01::> network port broadcast-domain remove-ports -broadcast
   -domain Default -ports
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

5. Es sollte überprüft werden, ob die Ports aus der Standard Broadcast-Domäne entfernt wurden:

   `network port show`

   Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt, dass Ports `e0e` und `e0f` aus der Standard-Broadcast-Domäne entfernt wurden:

```
cluster01::> network port show
                                                      Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Eine Broadcast-Domäne im benutzerdefinierten IPspace erstellen:

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   Das folgende Beispiel erstellt die Broadcast-Domäne `ipspace-IC1-bd` im IPspace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Es sollte überprüft werden, ob die Broadcast-Domäne erstellt wurde:

   `network port broadcast-domain show`

Weitere Informationen zu `network port broadcast-domain show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  ---------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a             complete
                            cluster01-01:e0b             complete
                            cluster01-02:e0a             complete
                            cluster01-02:e0b             complete
Default Default       1500
                            cluster01-01:e0c             complete
                            cluster01-01:e0d             complete
                            cluster01-01:e0f             complete
                            cluster01-01:e0g             complete
                            cluster01-02:e0c             complete
                            cluster01-02:e0d             complete
                            cluster01-02:e0f             complete
                            cluster01-02:e0g             complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e             complete
                            cluster01-01:e0f             complete
                            cluster01-02:e0e             complete
                            cluster01-02:e0f             complete
```

8. Intercluster-LIFs auf der System-SVM erstellen und der Broadcast-Domäne zuweisen:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 und früher:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Die LIF wird in der Broadcast-Domäne erstellt, der der Home-Port zugewiesen ist. Die Broadcast-Domäne verfügt über eine Standard Failover-Gruppe mit demselben Namen wie die Broadcast-Domäne. Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel erstellt Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02` in der Broadcast-Domäne `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Es sollte überprüft werden, ob die Intercluster-LIFs erstellt wurden:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 und früher:	`network interface show -role intercluster`

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

10. Es sollte sichergestellt werden, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
In ONTAP 9.6 und höher:	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 und früher:	`network interface show -role intercluster -failover`

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, dass die Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02` auf dem SVM `e0e`-Port auf den `e0f`-Port umschalten:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Peer-Beziehungen konfigurieren

ONTAP Cluster Peer-Beziehungen erstellen

Bevor Sie Ihre Daten durch Replikation auf einen Remote-Cluster zu Zwecken der Datensicherung und Notfallwiederherstellung schützen können, sollte eine Cluster Peer-Beziehung zwischen dem lokalen und dem Remote-Cluster erstellt werden.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu folgen, um die Snapshot-Replikation einzurichten. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Es stehen mehrere Standard-Schutzrichtlinien zur Verfügung. Eigene Schutzrichtlinien müssen erstellt worden sein, wenn benutzerdefinierte Richtlinien verwendet werden sollen.

Bevor Sie beginnen

Wenn Sie die ONTAP CLI verwenden, müssen auf jedem Knoten in den zu verbindenden Clustern Intercluster-LIFs mit einer der folgenden Methoden erstellt worden sein:

- "Intercluster-LIFs auf gemeinsam genutzten Datenports konfigurieren"
- "Intercluster-LIFs auf dedizierten Daten-Ports konfigurieren"
- "Intercluster-LIFs in benutzerdefinierten IPspaces konfigurieren"

Schritte

Diese Aufgabe kann mit ONTAP System Manager oder der ONTAP CLI ausgeführt werden.

System Manager

1. Im lokalen Cluster auf **Cluster > Einstellungen** klicken.
2. Im Abschnitt **Intercluster-Einstellungen** auf **Netzwerkschnittstellen hinzufügen** klicken und die IP-Adresse sowie die Subnetzmaske eingeben, um Intercluster-Netzwerkschnittstellen für den Cluster hinzuzufügen.

   Dieser Schritt ist auf dem Remote-Cluster zu wiederholen.
3. Im Remote-Cluster auf **Cluster > Einstellungen** klicken.
4. Auf ⋮ im Abschnitt **Cluster Peers** klicken und **Passphrase generieren** auswählen.
5. Die Version des Remote ONTAP Clusters auswählen.
6. Die generierte Passphrase kopieren.
7. Im lokalen Cluster unter **Cluster Peer** auf ⋮ klicken und **Peer-Cluster** auswählen.
8. Im Fenster **Peer-Cluster** die Passphrase einfügen und auf **Cluster-Peering initiieren** klicken.

CLI

1. Auf dem Ziel-Cluster eine Peer-Beziehung mit dem Quell-Cluster erstellen:

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
   <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
   <ipspace>
   ```

   Wenn Sie sowohl `-generate-passphrase` als auch `-peer-addrs` angeben, kann nur der Cluster, dessen Intercluster-LIFs in `-peer-addrs` angegeben sind, das generierte Passwort verwenden.

   Sie können die `-ipspace` Option ignorieren, wenn Sie keinen benutzerdefinierten IPspace verwenden. Weitere Informationen zu `cluster peer create` finden sich in der "ONTAP-Befehlsreferenz".

   Wenn die Peering-Beziehung in ONTAP 9.6 oder höher erstellt wird und keine Verschlüsselung der Intercluster-Peering-Kommunikation gewünscht ist, muss die `-encryption-protocol-proposed none` Option zur Deaktivierung der Verschlüsselung verwendet werden.

   Das folgende Beispiel erstellt eine Cluster Peer-Beziehung mit einem nicht näher spezifizierten Remote-Cluster und autorisiert vorab Peer-Beziehungen mit SVMs `vs1` und `vs2` auf dem lokalen Cluster:

   ```
   cluster02::> cluster peer create -generate-passphrase -offer
   ```

```
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

Das folgende Beispiel erstellt eine Cluster Peer-Beziehung mit dem Remote-Cluster an den Intercluster-LIF-IP-Adressen 192.140.112.103 und 192.140.112.104 und autorisiert vorab eine Peer-Beziehung mit einer beliebigen SVM auf dem lokalen Cluster:

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

Das folgende Beispiel erstellt eine Cluster Peer-Beziehung mit einem nicht näher spezifizierten Remote-Cluster und autorisiert vorab Peer-Beziehungen mit SVMs`vs1` und `vs2` auf dem lokalen Cluster:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. Im Quell-Cluster wird der Quell-Cluster gegenüber dem Ziel-Cluster authentifiziert:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Weitere Informationen zu `cluster peer create` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel authentifiziert das lokale Cluster beim Remote-Cluster an den Intercluster-LIF-IP-Adressen 192.140.112.101 und 192.140.112.102:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Geben Sie die Passphrase für die Peer-Beziehung ein, wenn Sie dazu aufgefordert werden.

3. Es sollte überprüft werden, ob die Cluster Peer-Beziehung erstellt wurde:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
                Availability of the Remote Cluster: Available
                               Remote Cluster Name: cluster2
                               Active IP Addresses: 192.140.112.101,
192.140.112.102
                             Cluster Serial Number: 1-80-123456
                    Address Family of Relationship: ipv4
                Authentication Status Administrative: no-authentication
                   Authentication Status Operational: absent
                                   Last Update Time: 02/05 21:05:41
                      IPspace for the Relationship: Default
```

4. Die Konnektivität und der Status der Knoten in der Peer-Beziehung können überprüft werden:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgaben mit… auszuführen	Diesen Inhalt ansehen…
System Manager Classic (verfügbar mit ONTAP 9.7 und früher)	"Überblick über die Vorbereitung der Volume-Desaster-Recovery"

Erstellen von ONTAP Intercluster SVM Peer-Beziehungen

Mit dem `vserver peer create` Befehl lässt sich eine Peer-Beziehung zwischen SVMs auf lokalen und entfernten Clustern erstellen.

Bevor Sie beginnen

- Die Quell- und Zielcluster müssen per Peering verbunden sein.
- Sie benötigen "vorautorisierte" Peer-Beziehungen für die SVMs auf dem Remote-Cluster.

Weitere Informationen finden sich unter "Erstellung einer Cluster Peer-Beziehung".

Über diese Aufgabe

Sie können Peer-Beziehungen für mehrere SVMs „vorautorisieren“, indem Sie die SVMs in der `-initial-allowed-vserver` Option angeben, wenn Sie eine Cluster Peer-Beziehung erstellen. Weitere Informationen finden sich unter "Erstellung einer Cluster Peer-Beziehung".

Schritte

1. Im Ziel-Cluster für den Datenschutz werden die SVMs angezeigt, die für das Peering vorautorisiert sind:

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. Auf dem Quell-Cluster für den Datenschutz eine Peer-Beziehung zu einer vorautorisierten SVM auf dem Ziel-Cluster für den Datenschutz erstellen:

   `vserver peer create -vserver` *`local_SVM`* `-peer-cluster` *`peer_cluster`* `-peer-vserver` *`remote_SVM`* `-application` *`application`*

   Weitere Informationen zu `vserver peer create` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel erstellt eine Peer-Beziehung zwischen der lokalen SVM `pvs1` und der vorautorisierten Remote-SVM `vs1`:

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-cluster cluster02
   -peer-vserver vs1 -application snapmirror
   ```

3. Die SVM Peer-Beziehung überprüfen:

   `vserver peer show`

   ```
   cluster01::> vserver peer show
               Peer        Peer                           Peering
   Remote
   Vserver     Vserver     State        Peer Cluster      Applications
   Vserver
   ----------- ----------- ------------ ----------------- --------------
   ---------
   pvs1        vs1         peered       cluster02         snapmirror
   vs1
   ```

ONTAP Intercluster SVM Peer-Beziehungen hinzufügen

Wenn eine SVM nach der Konfiguration einer Cluster Peer-Beziehung erstellt wird, muss die Peer-Beziehung für die SVM manuell hinzugefügt werden. Mit dem `vserver peer create` Befehl kann eine Peer-Beziehung zwischen SVMs erstellt werden. Nachdem die Peer-Beziehung erstellt wurde, kann `vserver peer accept` auf dem Remote-Cluster ausgeführt werden, um die Peer-Beziehung zu autorisieren.

Bevor Sie beginnen

Die Quell- und Zielcluster müssen per Peering verbunden sein.

Über diese Aufgabe

Es können Peer-Beziehungen zwischen SVMs im selben Cluster für die lokale Datensicherung erstellt werden. Weitere Informationen zu `vserver peer create` finden sich in der "ONTAP-Befehlsreferenz".

Administratoren verwenden gelegentlich den `vserver peer reject` Befehl, um eine vorgeschlagene SVM Peer-Beziehung abzulehnen. Befindet sich die Beziehung zwischen SVMs im `rejected` Status, muss die Beziehung gelöscht werden, bevor eine neue erstellt werden kann. Weitere Informationen zu `vserver peer reject` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie auf dem Quell-Cluster für die Datensicherung eine Peer-Beziehung zu einer SVM auf dem Ziel-Cluster:

   `vserver peer create -vserver local_SVM -peer-vserver remote_SVM -applications snapmirror|file-copy|lun-copy -peer-cluster remote_cluster`

   Das folgende Beispiel erstellt eine Peer-Beziehung zwischen der lokalen SVM`pvs1` und der Remote-SVM`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Wenn die lokalen und entfernten SVMs denselben Namen haben, muss ein *lokaler Name* verwendet werden, um die SVM Peer-Beziehung zu erstellen:

   ```
   cluster01::> vserver peer create -vserver vs1 -peer-vserver
   vs1 -applications snapmirror -peer-cluster cluster01
   -local-name cluster1vs1LocallyUniqueName
   ```

2. Auf dem Datensicherungs-Quell-Cluster überprüfen, ob die Peer-Beziehung initiiert wurde:

   `vserver peer show-all`

   Weitere Informationen zu `vserver peer show-all` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt, dass die Peer-Beziehung zwischen SVM`pvs1` und SVM`vs1` initiiert wurde:

```
cluster01::> vserver peer show-all
            Peer        Peer                        Peering
Vserver     Vserver     State      Peer Cluster     Applications
--------    --------    ---------  -------------    ------------
pvs1        vs1         initiated   Cluster02         snapmirror
```

3. Im Ziel-Cluster für den Datenschutz die ausstehende SVM Peer-Beziehung anzeigen:

   `vserver peer show`

   Weitere Informationen zu `vserver peer show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel listet die ausstehenden Peer-Beziehungen für `cluster02` auf:

```
cluster02::> vserver peer show

                  Peer               Peer
Vserver           Vserver            State
-----------       -----------        ------------
vs1               pvs1               pending
```

4. Auf dem Ziel-Cluster für den Datenschutz die ausstehende Peer-Beziehung autorisieren:

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Weitere Informationen zu `vserver peer accept` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel autorisiert die Peer-Beziehung zwischen der lokalen SVM `vs1` und der Remote-SVM `pvs1`:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Die SVM Peer-Beziehung überprüfen:

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
```

```
vs1
```

ONTAP Cluster Peer-Verschlüsselung für Peer-Beziehungen aktivieren

Ab ONTAP 9.6 ist die Cluster Peering-Verschlüsselung standardmäßig für alle neu erstellten Cluster Peer-Beziehungen aktiviert. Die Cluster Peering-Verschlüsselung verwendet einen vorab vereinbarten Schlüssel (PSK) und die Transport Security Layer (TLS), um die clusterübergreifende Peer-Kommunikation abzusichern. Dadurch entsteht eine zusätzliche Sicherheitsebene zwischen den verbundenen Clustern.

Über diese Aufgabe

Wenn Sie peered Cluster auf ONTAP 9.6 oder höher aktualisieren und die Peer-Beziehung in ONTAP 9.5 oder früher erstellt wurde, muss die Cluster Peer-Verschlüsselung nach dem Upgrade manuell aktiviert werden. Beide Cluster in der Peer-Beziehung müssen ONTAP 9.6 oder höher ausführen, damit die Cluster Peer-Verschlüsselung aktiviert werden kann.

Schritte

1. Auf dem Ziel-Cluster die Verschlüsselung für die Kommunikation mit dem Quell-Cluster aktivieren:

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Bei Aufforderung ist eine Passphrase einzugeben.
3. Auf dem Datensicherungs-Quell-Cluster die Verschlüsselung für die Kommunikation mit dem Datensicherungs-Ziel-Cluster aktivieren:

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Bei entsprechender Aufforderung ist dieselbe Passphrase einzugeben, die auf dem Ziel-Cluster verwendet wurde.

Weitere Informationen zu `cluster peer modify` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "TLS-Hardware-Offload konfigurieren"

ONTAP Cluster-Peering-Verschlüsselung aus den Peer-Beziehungen entfernen

Standardmäßig ist die Cluster-Peering-Verschlüsselung für alle Peer-Beziehungen aktiviert, die in ONTAP 9.6 oder höher erstellt wurden. Wenn keine Verschlüsselung für die clusterübergreifende Peering-Kommunikation gewünscht ist, besteht die Möglichkeit, sie zu deaktivieren.

Schritte

1. Im Ziel-Cluster die Kommunikation mit dem Quell-Cluster so anpassen, dass die Verwendung der Cluster-Peering-Verschlüsselung eingestellt wird:
   - Um die Verschlüsselung zu entfernen, aber die Authentifizierung beizubehalten, Folgendes eingeben:

```
cluster peer modify <source_cluster> -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

- So werden Verschlüsselung und Authentifizierung entfernt:
  i. Die Cluster-Peering-Richtlinie wird so geändert, dass nicht authentifizierter Zugriff möglich ist:

  ```
  cluster peer policy modify -is-unauthenticated-access-permitted
  true
  ```

  ii. Zugriff auf Verschlüsselung und Authentifizierung ändern:

  ```
  cluster peer modify <source_cluster> -auth-status no-
  authentication
  ```

2. Bei Aufforderung die Passphrase eingeben.
3. Die Passphrase wird bestätigt, indem sie erneut eingegeben wird.
4. Auf dem Quell-Cluster die Verschlüsselung für die Kommunikation mit dem Ziel-Cluster deaktivieren:
   - Um die Verschlüsselung zu entfernen, aber die Authentifizierung beizubehalten, Folgendes eingeben:

   ```
   cluster peer modify <destination_cluster> -auth-status-admin use-
   authentication -encryption-protocol-proposed none
   ```

   - So werden Verschlüsselung und Authentifizierung entfernt:
     i. Die Cluster-Peering-Richtlinie wird so geändert, dass nicht authentifizierter Zugriff möglich ist:

     ```
     cluster peer policy modify -is-unauthenticated-access-permitted
     true
     ```

     ii. Zugriff auf Verschlüsselung und Authentifizierung ändern:

     ```
     cluster peer modify <destination_cluster> -auth-status no-
     authentication
     ```

5. Bei Aufforderung ist die gleiche Passphrase einzugeben und erneut einzugeben, die auf dem Ziel-Cluster verwendet wurde.

Lokale Snapshots verwalten

Informationen zur Verwaltung lokaler ONTAP Snapshots

Ein Snapshot ist ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes. Das Image benötigt minimalen Speicherplatz und verursacht einen vernachlässigbaren Performance-Overhead, da nur die Änderungen an Dateien seit dem letzten Snapshot aufgezeichnet werden.

Mithilfe eines Snapshots kann der gesamte Inhalt eines Volumes oder einzelne Dateien oder LUNs wiederhergestellt werden. Snapshots werden im Verzeichnis `.snapshot` auf dem Volume gespeichert.

In ONTAP 9.4 und höher kann ein FlexVol Volume bis zu 1023 Snapshots enthalten. In ONTAP 9.3 und früher kann ein Volume bis zu 255 Snapshots enthalten.

Ab ONTAP 9.8 können FlexGroup Volumes 1023 Snapshots enthalten. Weitere Informationen finden sich unter "Schutz von FlexGroup Volumes mithilfe von Snapshots".

Es gibt mehrere gängige ONTAP Snapshot-Typen:

- `sched_created`: Snapshots, die automatisch von einer ONTAP-Snapshot-Richtlinie auf Basis vordefinierter Zeitpläne (zum Beispiel stündlich, täglich, wöchentlich oder monatlich) erstellt werden.
- `sm_created`: Automatische Snapshots, die im Zuge von SnapMirror-Replikationsübertragungen (Aktualisierungs- oder Initialisierungsvorgängen) erstellt werden.
- `application_created`: Snapshots, die von Integrationssoftware auf Host- oder Datenbankebene wie SnapCenter oder SnapDrive generiert werden.
- `user_created`: Snapshots, die manuell von einem Administrator entweder über die ONTAP CLI oder den System Manager ausgelöst werden.
- `sv_created`: Snapshots, die automatisch während Cluster-Operationen erstellt werden, wie zum Beispiel bei Storage Virtual Machine (SVM) DR oder bestimmten Schutz-Workflows.
- `luns_created`: Snapshots, die erstellt wurden, um den Zustand von LUN- oder NVMe-Namespace-Klonen zu sichern oder zu erfassen.

Informationen zu ONTAP Langzeitaufbewahrungs-Snapshots

SnapMirror Beziehungen mit einem Richtlinientyp von entweder „vault“ oder „mirror-vault“ ermöglichen die direkte Erstellung von Snapshots auf dem sekundären Volume der SnapMirror Beziehung. Diese Snapshots werden auf dem Ziel als Backups aufbewahrt. Diese Snapshots werden häufig für die langfristige Aufbewahrung erstellt und als Snapshots zur langfristigen Aufbewahrung bezeichnet.

Ein Langzeit-Aufbewahrungs-Snapshot wird erstellt, indem in der SnapMirror Richtlinienregel ein Zeitplan für die Snapshot-Erstellung, das Snapshot-Namenspräfix, das SnapMirror Label und die Aufbewahrungsanzahl angegeben werden. Dieser Snapshot bleibt auf dem SnapMirror Ziel-Volume erhalten, unabhängig von den Aufbewahrungsregeln auf der Quelle.

Langzeitaufbewahrungs-Snapshots sind nur für FlexVol SnapMirror Konfigurationen verfügbar. Langzeitaufbewahrungs-Snapshots können für FlexGroup SnapMirror Konfigurationen nicht erstellt werden.

In einer SnapMirror Kaskadenbeziehung können Langzeit-Snapshots nur auf dem letzten Volume der Kaskade erstellt werden.

Verwandte Informationen

- "Informationen darüber, wie Kaskadenbereitstellungen funktionieren"
- "Einen ONTAP SnapMirror Zeitplan definieren, um eine lokale Kopie auf dem Ziel zu erstellen"

Benutzerdefinierte Snapshot-Richtlinien konfigurieren

Informationen zu benutzerdefinierten ONTAP Snapshot-Richtlinien

Eine Snapshot-Richtlinie definiert, wie das System Snapshots erstellt. Die Richtlinie legt fest, wann Snapshots erstellt werden, wie viele Kopien aufbewahrt werden und wie diese benannt werden. Beispielsweise könnte ein System täglich um 0:10 Uhr einen Snapshot erstellen, die beiden aktuellsten Kopien aufbewahren und die Kopien „daily.`timestamp`“ nennen.

Die Standardrichtlinie für ein Volume erstellt automatisch Snapshots nach folgendem Zeitplan, wobei die ältesten Snapshots gelöscht werden, um Platz für neuere Kopien zu schaffen:

- Maximal sechs stündliche Momentaufnahmen, die fünf Minuten nach der vollen Stunde erstellt werden.
- Maximal zwei tägliche Schnappschüsse, aufgenommen von Montag bis Samstag jeweils 10 Minuten nach Mitternacht.
- Maximal zwei wöchentliche Snapshots, die jeden Sonntag um 0:15 Uhr erstellt werden.

Sofern beim Erstellen eines Volumes keine Snapshot-Richtlinie angegeben wird, übernimmt das Volume die Snapshot-Richtlinie der zugehörigen Storage Virtual Machine (SVM).

Wann eine benutzerdefinierte ONTAP Snapshot-Richtlinie konfiguriert werden sollte

Wenn die Standard-Snapshot-Richtlinie für ein Volume nicht geeignet ist, kann eine benutzerdefinierte Richtlinie konfiguriert werden, die Häufigkeit, Aufbewahrungsdauer und Namen der Snapshots anpasst. Der Zeitplan wird hauptsächlich durch die Änderungsrate des aktiven Dateisystems bestimmt.

Ein stark frequentiertes Dateisystem wie eine Datenbank wird beispielsweise stündlich gesichert, während selten genutzte Dateien einmal täglich gesichert werden. Selbst bei einer Datenbank erfolgt üblicherweise ein- bis zweimal täglich eine vollständige Sicherung, während die Transaktionsprotokolle stündlich gesichert werden.

Weitere Faktoren sind die Bedeutung der Dateien für Ihr Unternehmen, Ihre Service Level Agreement (SLA), Ihr Recovery Point Objective (RPO) und Ihr Recovery Time Objective (RTO). Im Allgemeinen sollten nur so viele Snapshots aufbewahrt werden, wie unbedingt erforderlich sind.

Erstellen eines ONTAP Snapshot Jobplans

Eine Snapshot-Richtlinie erfordert mindestens einen Snapshot-Auftragsplan. Es besteht die Möglichkeit, System Manager oder den `job schedule cron create` Befehl zu verwenden, um einen Auftragsplan zu erstellen. Weitere Informationen zu `job schedule cron create` finden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu folgen, um einen Snapshot-Jobzeitplan zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Standardmäßig bildet ONTAP die Namen von Snapshots, indem an den Jobplannamen ein Zeitstempel angehängt wird.

Wenn Sie sowohl den Tag des Monats als auch den Wochentag angeben, werden die Werte unabhängig voneinander betrachtet. Beispielsweise wird ein Cron-Schedule mit der Tag-Spezifikation `Friday` und der Tag-des-Monats-Spezifikation `13`jeden Freitag und am 13. Tag jedes Monats ausgeführt, nicht nur an jedem Freitag, der auf den 13. fällt.

Beispiel 1. Schritte

System Manager

1. Navigieren Sie zu **Schutz > Übersicht** und erweitern Sie **Lokale Richtlinieneinstellungen**.
2. Im Bereich **Zeitpläne** auf → klicken.
3. Im Fenster **Zeitpläne** auf + Add klicken.
4. Im Fenster **Zeitplan hinzufügen** den Namen des Zeitplans eingeben sowie den Kontext und den Zeitplantyp auswählen.
5. Auf **Speichern** klicken.

CLI

1. Einen Arbeitszeitplan erstellen:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Für `-month`, `-dayofweek` und `-hour` kann `all` angegeben werden, damit der Job jeden Monat, an jedem Wochentag bzw. zu jeder Stunde ausgeführt wird.

Ab ONTAP 9.10.1 kann der Vserver in den Jobplan einbezogen werden:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

Das folgende Beispiel erstellt einen Jobplan mit dem Namen `myweekly`, der samstags um 3:00 Uhr morgens ausgeführt wird:

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Das folgende Beispiel erstellt einen Zeitplan mit dem Namen `myweeklymulti`, der mehrere Tage, Stunden und Minuten angibt:

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

Erstellen einer ONTAP Snapshot-Richtlinie

Eine Snapshot-Richtlinie legt fest, wann Snapshots erstellt werden, wie viele Kopien aufbewahrt werden und wie diese benannt werden. Beispielsweise kann ein System täglich um 0:10 Uhr einen Snapshot erstellen, die beiden aktuellsten Kopien aufbewahren und sie „daily.*timestamp*.“ nennen. Eine Snapshot-Richtlinie kann bis zu fünf Auftragspläne enthalten.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu befolgen, um eine Snapshot Policy zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Standardmäßig bildet ONTAP die Namen von Snapshots, indem dem Namen des Jobplans ein Zeitstempel angehängt wird:

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Es kann ein Präfix anstelle des Auftragsplannamens verwendet werden, falls gewünscht.

Die `snapmirror-label` Option ist für die SnapMirror Replikation. Weitere Informationen finden sich unter "Definieren einer Regel für eine Richtlinie".

Schritte

Sie können eine Snapshot-Richtlinie mithilfe von System Manager oder der ONTAP CLI erstellen. Das Verfahren erstellt eine Snapshot-Richtlinie nur auf dem lokalen Cluster.

System Manager

1. Navigieren Sie zu **Schutz > Übersicht** und erweitern Sie **Lokale Richtlinieneinstellungen**.
2. Im Bereich **Snapshot-Richtlinien** auf → klicken.
3. Im Tab **Snapshot-Richtlinien** auf + Add klicken.
4. Im Fenster **Snapshot-Richtlinie hinzufügen** den Richtliniennamen eingeben und den Geltungsbereich auswählen.
5. Klicken Sie + Add .
6. Um einen Zeitplan auszuwählen, auf den aktuell angezeigten Zeitplannamen klicken, auf ⌄ klicken und einen anderen Zeitplan auswählen.
7. Geben Sie die maximale Anzahl der aufzubewahrenden Snapshots ein und, falls erforderlich, die SnapMirror-Bezeichnung und die SnapLock-Aufbewahrungsdauer.

8. Auf **Speichern** klicken.

CLI

1. Erstellen einer Snapshot-Richtlinie:

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

Das folgende Beispiel erstellt eine Snapshot-Richtlinie mit dem Namen `snap_policy_daily`, die nach einem `daily` Zeitplan ausgeführt wird. Die Richtlinie hat maximal fünf Snapshots, jeweils mit dem Namen `daily.`*`timestamp`* und dem SnapMirror-Label `daily`:

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

Snapshots manuell verwalten

ONTAP Snapshots manuell erstellen und löschen

Sie können Snapshots manuell erstellen, wenn Sie nicht auf die Erstellung eines geplanten Snapshots warten können, und Sie können Snapshots löschen, wenn sie nicht mehr benötigt werden.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu befolgen, um einen On-Demand Snapshot zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Snapshot manuell erstellen

Sie können manuell einen Snapshot mit System Manager oder der ONTAP CLI erstellen.

System Manager

Schritte

1. Zu **Speicher > Volumes** navigieren und die Registerkarte **Snapshots** auswählen.
2. Klicken Sie + Add .
3. Im Fenster **Snapshot hinzufügen** lässt sich der Standard-Snapshot-Name übernehmen oder bei Bedarf bearbeiten.

4. **Optional**: Eine SnapMirror Beschriftung kann hinzugefügt werden.
5. Klicken Sie auf **Add**.

CLI

1. Snapshot erstellen:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Snapshots manuell löschen

Sie können einen Snapshot manuell über den System Manager oder die ONTAP CLI löschen.

System Manager

Schritte

1. Navigieren Sie zu **Speicher > Volumes** und wählen Sie die Registerkarte **Snapshot copies** aus.
2. Den Snapshot, den Sie löschen möchten, suchen, auf ⋮ klicken und **Löschen** auswählen.
3. Im Fenster **Snapshot löschen** wird **Snapshot löschen** ausgewählt.
4. Klicken Sie auf **Delete**.

CLI

1. Mit dem `volume snapshot show` Befehl lässt sich überprüfen, welche Snapshots gelöscht werden sollen.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

In diesem Beispiel zeigt der Befehl die Snapshots auf dem Volume vol3 in der SVM vs3 an.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
```

```
                  snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. Einen Snapshot löschen:

Wenn Sie möchten…	Geben Sie diesen Befehl ein…
Einen einzelnen Snapshot löschen	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`
Mehrere Snapshots löschen	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
Alle Snapshots löschen	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

Berechnung des zurückgewinnbaren Speicherplatzes vor dem Löschen von ONTAP Snapshots

Sie können Snapshots auswählen, die Sie löschen möchten, und den zurückgewinnbaren Speicherplatz berechnen, bevor Sie sie löschen.

In Releases vor ONTAP 9.20.1 wird die Berechnung des freigebbaren Speicherplatzes auf FlexVol Volumes unterstützt, und für FlexGroup Volumes ist eine manuelle Zusammenführung der Snapshot-Nutzung über die einzelnen FlexGroup Teil-Volumes erforderlich. Ab ONTAP 9.20.1 kann der freigebbare Speicherplatz für Snapshots in FlexGroup Volumes berechnet werden.

Schritte

Diese Aufgabe kann über den System Manager oder die ONTAP CLI ausgeführt werden.

System Manager

1. **Speicher > Volumes** auswählen.
2. Das Volume auswählen, von dem Snapshots gelöscht werden sollen.
3. **Schnappschüsse** auswählen.
4. Einen oder mehrere Schnappschüsse auswählen.
5. Auf **Wiederverwertbarer Speicherplatz berechnen** klicken.

CLI

1. Berechnung des zurückgewinnbaren Speicherplatzes:

```
volume snapshot compute-reclaimable -vserver <svm_name> -volume
<volume_name> -snapshots <snap1,snap2,snap3>
```

Snapshot Reserve verwalten

Informationen zur Verwaltung des ONTAP Snapshot Reserve

Die Snapshot-Reserve reserviert einen bestimmten Prozentsatz des Speicherplatzes für Snapshots, standardmäßig fünf Prozent. Da Snapshots Speicherplatz im aktiven Dateisystem belegen, wenn die Snapshot-Reserve erschöpft ist, kann es sinnvoll sein, die Snapshot-Reserve bei Bedarf zu erhöhen. Alternativ ist es möglich, Snapshots automatisch zu löschen, wenn die Reserve voll ist.

Wann die Snapshot-Reserve erhöht werden sollte

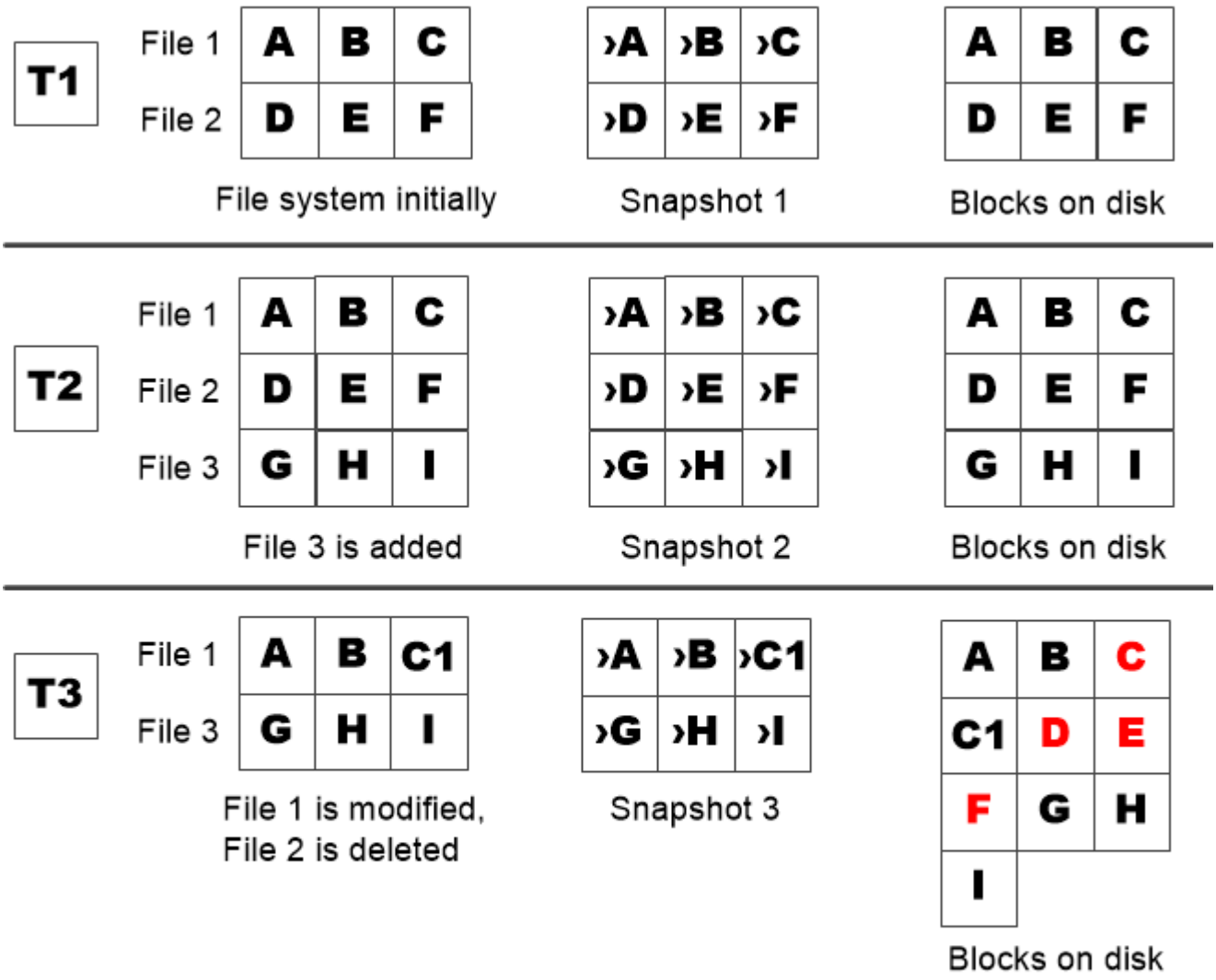
Bei der Entscheidung, ob die Snapshot-Reserve erhöht werden soll, ist zu beachten, dass ein Snapshot nur die Änderungen an Dateien seit der letzten Snapshot-Erstellung aufzeichnet. Er belegt nur dann Speicherplatz, wenn Blöcke im aktiven Dateisystem geändert oder gelöscht werden.

Das bedeutet, dass die Änderungsrate des Dateisystems der entscheidende Faktor für den von Snapshots belegten Speicherplatz ist. Unabhängig davon, wie viele Snapshots erstellt werden, wird kein Speicherplatz belegt, wenn sich das aktive Dateisystem nicht geändert hat.

Ein FlexVol volume, das beispielsweise Datenbanktransaktionsprotokolle enthält, könnte eine Snapshot-Reserve von bis zu 20 % aufweisen, um der höheren Änderungsrate Rechnung zu tragen. Es empfiehlt sich, mehr Snapshots zu erstellen, um die häufigeren Aktualisierungen der Datenbank zu erfassen, und zudem eine größere Snapshot-Reserve vorzusehen, um den zusätzlichen Speicherplatzbedarf der Snapshots abzudecken.



Ein Snapshot besteht aus Zeigern auf Blöcke, nicht aus Kopien der Blöcke. Ein Zeiger kann als ein „Anspruch“ auf einen Block betrachtet werden: ONTAP „hält“ den Block, bis der Snapshot gelöscht wird.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

Wie das Löschen geschützter Dateien zu weniger Speicherplatz als erwartet führen kann

Ein Snapshot verweist auch dann noch auf einen Speicherblock, nachdem Sie die Datei gelöscht haben, die diesen Block verwendet hat. Dies erklärt, warum ein erschöpfter Snapshot Reserve zu dem kontraintuitiven Ergebnis führen kann, dass nach dem Löschen eines gesamten Dateisystems weniger Speicherplatz verfügbar ist, als das Dateisystem belegt hat.

Betrachten Sie folgendes Beispiel. Bevor Dateien gelöscht werden, ist die Ausgabe des `df` Befehls wie folgt:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

Nach dem Löschen des gesamten Dateisystems und dem Erstellen eines Snapshots des Volumes erzeugt der `df` Befehl die folgende Ausgabe:

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

Wie die Ausgabe zeigt, werden die gesamten 3 GB, die zuvor vom aktiven Dateisystem genutzt wurden, nun von Snapshots belegt, zusätzlich zu den 0,5 GB, die vor dem Löschen verwendet wurden.

Da der von den Snapshots belegte Speicherplatz nun die Snapshot-Reserve übersteigt, fließt der Überschuss von 2,5 GB in den für aktive Dateien reservierten Speicherplatz, sodass Ihnen 0,5 GB freier Speicherplatz für Dateien bleiben, wo Sie vernünftigerweise 3 GB erwartet hätten.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

ONTAP Snapshot-Speicherverbrauch überwachen

Sie können die Speichernutzung von Snapshots mithilfe des `df` Befehls überwachen. Der Befehl zeigt den freien Speicherplatz im aktiven Dateisystem und die Snapshot-Reserve an.

Schritt

1. Anzeige des Snapshot-Speicherverbrauchs: `df`

   Das folgende Beispiel zeigt den Festplattenverbrauch von Snapshots:

   ```
   cluster1::> df
   Filesystem           kbytes  used    avail  capacity
   /vol/vol0/           3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Verfügbare ONTAP Snapshot-Reserve auf einem Volume prüfen

Es kann sinnvoll sein zu prüfen, wie viel Snapshot-Reserve auf einem Volume verfügbar ist, indem der `snapshot-reserve-available` Parameter mit dem `volume show` Befehl verwendet wird. Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Die auf einem Volume verfügbare Snapshot-Reserve prüfen:

   `vol show -vserver` *`SVM`* `-volume` *`volume`* `-fields snapshot-reserve-available`

   Das folgende Beispiel zeigt die verfügbare Snapshot-Reserve für `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

Die ONTAP Snapshot Reserve anpassen

Es kann sinnvoll sein, eine größere Snapshot-Reserve zu konfigurieren, um zu verhindern, dass Snapshots Speicherplatz belegen, der für das aktive Dateisystem reserviert ist. Die Snapshot-Reserve kann verringert werden, wenn nicht mehr so viel Speicherplatz für Snapshots benötigt wird.

Schritt

1. Die Snapshot-Reserve ändern:

   `volume modify -vserver` *SVM* `-volume` *volume* `-percent-snapshot-space` *snap_reserve*

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

   Im folgenden Beispiel wird die Snapshot-Reserve für `vol1` auf 10 Prozent festgelegt:

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

Automatisches Löschen von ONTAP Snapshots

Sie können den `volume snapshot autodelete modify` Befehl verwenden, um die automatische Löschung von Snapshots auszulösen, wenn der Snapshot-Reserve überschritten wird. Standardmäßig werden die ältesten Snapshots zuerst gelöscht. Weitere Informationen zu `volume snapshot autodelete modify` finden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

LUN- und Dateiklone werden gelöscht, wenn keine Snapshots mehr gelöscht werden müssen.

Schritt

1. Automatisches Löschen von Snapshots:

   `volume snapshot autodelete modify -vserver` *SVM* `-volume` *volume* `-enabled true|false -trigger volume|snap_reserve`

   Das folgende Beispiel löscht Snapshots für `vol1` automatisch, wenn der Snapshot-Reserve erschöpft ist:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Dateien aus Snapshots wiederherstellen

Wie NFS- und SMB-Clients Dateien aus ONTAP Snapshots wiederherstellen

Ein Benutzer auf einem NFS- oder SMB-Client kann eine Datei direkt aus einem Snapshot wiederherstellen, ohne dass ein Systemadministrator des Speichersystems eingreifen muss.

Jedes Verzeichnis im Dateisystem enthält ein Unterverzeichnis mit dem Namen `.snapshot` , das für NFS- und SMB-Benutzer zugänglich ist. Das `.snapshot` Unterverzeichnis enthält Unterverzeichnisse, die den Snapshots des Volumes entsprechen:

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Bei NFSv4 wird das `ls` Kommando das `.snapshot` Verzeichnis nicht anzeigen, es bleibt jedoch für den Client zum Wiederherstellen von Dateien zugänglich.

Jedes Unterverzeichnis enthält die im Snapshot referenzierten Dateien. Wenn Benutzer versehentlich eine Datei löschen oder überschreiben, kann die Datei im übergeordneten Lese-/Schreibverzeichnis wiederhergestellt werden, indem die Datei aus dem Snapshot-Unterverzeichnis in das Lese-/Schreibverzeichnis kopiert wird:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Aktivieren und Deaktivieren des NFS- und SMB-Clientzugriffs auf das ONTAP Snapshot-Verzeichnis

Sie können den Zugriff auf das Snapshot-Verzeichnis mithilfe der ONTAP CLI `-snapdir -access` Option des `volume modify` Befehls aktivieren und deaktivieren, und ab

ONTAP 9.10.1 besteht die Möglichkeit, mit System Manager den Zugriff von Clientsystemen auf ein Snapshot-Verzeichnis auf einem Volume zu aktivieren oder zu deaktivieren. Durch die Aktivierung des Zugriffs wird das Snapshot-Verzeichnis für Clients sichtbar, und Windows-Clients können ein Laufwerk mit dem Snapshot-Verzeichnis verbinden, um dessen Inhalt anzuzeigen und darauf zuzugreifen. NFS- und SMB-Clients können dann eine Datei oder LUN aus einem Snapshot wiederherstellen.

Sie können den Zugriff auf das Snapshot-Verzeichnis eines Volumes aktivieren oder deaktivieren, indem die Volume-Einstellungen oder die Freigabeeinstellungen des Volumes bearbeitet werden.

Clientzugriff auf das Snapshot-Verzeichnis durch Bearbeiten eines Volumes aktivieren oder deaktivieren

Schritte

Sie können den Zugriff auf das Client-Snapshot-Verzeichnis mithilfe von ONTAP System Manager oder der ONTAP CLI aktivieren und deaktivieren. Das Snapshot-Verzeichnis auf einem Volume ist standardmäßig für Clients zugänglich.

System Manager

1. **Speicher > Volumes** auswählen.
2. Wählen Sie das Volume aus, das das Snapshots-Verzeichnis enthält, das entweder angezeigt oder ausgeblendet werden soll.
3. Klicken Sie ⋮ und wählen Sie **Bearbeiten**.
4. Im Abschnitt **Snapshot (Lokale) Einstellungen** wird **Snapshot-Verzeichnis für Clients anzeigen** ausgewählt oder abgewählt.
5. Auf **Speichern** klicken.

CLI

1. Status des Zugriffs auf das Snapshot-Verzeichnis prüfen:

   ```
   volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
   access
   ```

   Beispiel:

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
   access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

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

2. Der Zugriff auf das Snapshot-Verzeichnis kann aktiviert oder deaktiviert werden:

```
volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
<true|false>
```

Das folgende Beispiel ermöglicht den Zugriff auf das Snapshot-Verzeichnis auf vol1:

```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
true
Volume modify successful on volume vol1 of Vserver vs0.
```

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

Clientzugriff auf das Snapshot-Verzeichnis kann durch Bearbeiten einer Freigabe aktiviert oder deaktiviert werden.

Das Snapshot-Verzeichnis auf einem Volume ist standardmäßig für Clients zugänglich.

Schritte

1. **Speicher > Freigaben** auswählen.
2. Wählen Sie das Volume aus, das das Snapshots-Verzeichnis enthält, das entweder angezeigt oder ausgeblendet werden soll.
3. Klicken Sie ⋮ und wählen Sie **Bearbeiten**.
4. Im Abschnitt **Freigabeeigenschaften** wird die Option **Clients den Zugriff auf das Snapshot-Verzeichnis erlauben** ausgewählt oder abgewählt.
5. Auf **Speichern** klicken.

Eine einzelne Datei aus einem ONTAP Snapshot wiederherstellen

Sie können den `volume snapshot restore-file` Befehl verwenden, um eine einzelne Datei oder LUN aus einem Snapshot wiederherzustellen. Die Datei kann an einem anderen Speicherort im übergeordneten lesen/schreiben-Volume wiederhergestellt werden, wenn keine vorhandene Datei ersetzt werden soll.

Über diese Aufgabe

Wenn eine vorhandene LUN wiederhergestellt wird, wird ein LUN-Klon erstellt und in Form eines Snapshots gesichert. Während des Wiederherstellungsvorgangs ist lesen und schreiben auf die LUN möglich.

Dateien mit Streams werden standardmäßig wiederhergestellt.

Schritte

1. Snapshots in einem Volume auflisten:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Weitere Informationen zu `volume snapshot show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Momentaufnahmen in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Eine Datei aus einem Snapshot wiederherstellen:

   `volume snapshot restore-file -vserver` *SVM* `-volume` *volume* `-snapshot` *snapshot* `-path` *file_path* `-restore-path` *destination_path*

   Weitere Informationen zu `volume snapshot restore-file` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel stellt die Datei `myfile.txt` wieder her:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Einen Teil einer Datei aus einem ONTAP Snapshot wiederherstellen

Sie können den `volume snapshot partial-restore-file` Befehl verwenden, um einen Datenbereich aus einem Snapshot auf eine LUN oder in eine NFS- oder SMB-Containerdatei wiederherzustellen, sofern der Startbyte-Offset der Daten und die Byte-Anzahl bekannt sind. Dieser Befehl kann beispielsweise genutzt werden, um eine der Datenbanken auf einem Host wiederherzustellen, der mehrere Datenbanken in derselben LUN speichert.

Ab ONTAP 9.12.1 ist die teilweise Wiederherstellung für Volumes mit SnapMirror Active Sync verfügbar.

Schritte

1. Snapshots in einem Volume auflisten:

   `volume snapshot show -vserver` *SVM* `-volume` *volume*

   Weitere Informationen zu `volume snapshot show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Momentaufnahmen in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Einen Teil einer Datei aus einem Snapshot wiederherstellen:

   `volume snapshot partial-restore-file -vserver` *SVM* `-volume` *volume* `-snapshot` *snapshot* `-path` *file_path* `-start-byte` *starting_byte* `-byte-count` *byte_count*

   Der Startbyte-Offset und die Byteanzahl müssen Vielfache von 4.096 sein.

   Das folgende Beispiel stellt die ersten 4096 Bytes der Datei `myfile.txt` wieder her:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Wiederherstellung des Inhalts eines Volumes aus einem ONTAP Snapshot

Ein Volume kann auf einen früheren Zeitpunkt zurückgesetzt werden, indem es aus einem Snapshot wiederhergestellt wird. Mit System Manager oder dem `volume snapshot restore` Befehl lässt sich der Inhalt eines Volumes aus einem Snapshot wiederherstellen. Weitere Informationen zu `volume snapshot restore` finden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Wenn das Volume SnapMirror Beziehungen aufweist, sollten alle Spiegelkopien des Volumes unmittelbar nach der Wiederherstellung aus einem Snapshot manuell repliziert werden. Andernfalls können unbrauchbare Spiegelkopien entstehen, die gelöscht und neu erstellt werden müssen.

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um aus einem früheren Snapshot wiederherzustellen.

System Manager

1. Auf **Speicher** klicken und ein Volume auswählen.
2. Unter **Snapshot-Kopien** auf ⋮ neben dem Snapshot, den Sie wiederherstellen möchten, klicken und **Wiederherstellen** auswählen.

CLI

1. Snapshots in einem Volume auflisten:

```
volume snapshot show -vserver <svm> -volume <volume>
```

Das folgende Beispiel zeigt die Momentaufnahme in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Den Inhalt eines Volumes aus einem Snapshot wiederherstellen:

```
volume snapshot restore -vserver <svm> -volume <volume> -snapshot
<snapshot>
```

Das folgende Beispiel stellt den Inhalt von `vol1` wieder her:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

SnapMirror Volume-Replikation

Informationen zur SnapMirror Volumenreplikation

Informationen zu ONTAP SnapMirror asynchroner Disaster Recovery

SnapMirror ist eine Technologie zur Notfallwiederherstellung, die für die Ausfallsicherung von primärem Speicher auf sekundären Speicher an einem geografisch entfernten Standort entwickelt wurde. Wie der Name schon sagt, erstellt SnapMirror eine Replik, also einen Spiegel, Ihrer Arbeitsdaten im sekundären Speicher, von dem aus im Katastrophenfall am primären Standort weiterhin Daten bereitgestellt werden können.

Wenn der primäre Standort weiterhin Daten bereitstellen kann, können die benötigten Daten einfach dorthin zurückübertragen werden, und es erfolgt keine Client-Bedienung mehr vom Spiegel. Wie der Failover-Anwendungsfall impliziert, sollten die Controller des sekundären Systems den Controllern des primären Systems gleichwertig oder nahezu gleichwertig sein, um Daten effizient vom gespiegelten Speicher bereitzustellen.

Ab ONTAP 9.20.1 können Sie "Konfiguration der asynchronen SnapMirror Replizierung über bestehende Fibre Channel (FC) Fabrics". Dadurch entfällt die in ONTAP 9.19.1 und früheren Versionen bestehende Anforderung an Backend-IP-Netzwerke, Firewall-Ausnahmen oder eine Netzwerk-Rearchitektur zwischen Standorten.

Informationen zu "Konfiguration Ihres ONTAP Systems für die Backend-Replikation über FC".

Datensicherungsbeziehungen

Die Daten werden auf Volume-Ebene gespiegelt. Die Beziehung zwischen dem Quell-Volume im Primärspeicher und dem Ziel-Volume im Sekundärspeicher wird als *Data Protection Relationship* bezeichnet. Die Cluster, in denen sich die Volumes befinden, und die SVMs, die Daten von den Volumes bereitstellen, müssen "gepeert" sein. Eine Peer-Beziehung ermöglicht den sicheren Austausch von Daten zwischen Clustern und SVMs.

Diese Abbildung veranschaulicht SnapMirror Datenschutzbeziehungen:



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

Umfang der Datenschutzbeziehungen

Sie können eine Datensicherungsbeziehung direkt zwischen Volumes oder zwischen den SVMs, denen die Volumes gehören, erstellen. In einer SVM-Datensicherungsbeziehung werden die gesamte oder ein Teil der SVM-Konfiguration, von NFS-Exporten und SMB-Freigaben bis zu RBAC, sowie die Daten in den Volumes, die der SVM gehören, repliziert.

SnapMirror kann auch für spezielle Datenschutzanwendungen verwendet werden:

- Eine *Load-Sharing Mirror*-Kopie des SVM-Root-Volumes stellt sicher, dass die Daten im Falle eines Node-Ausfalls oder Failover zugänglich bleiben.
- Eine Datenschutzbeziehung zwischen *SnapLock Volumes* ermöglicht die Replikation von WORM-Dateien auf Sekundärspeicher.

  "Archivierung und Compliance mithilfe von SnapLock Technologie"

- Ab ONTAP 9.13.1 kann SnapMirror asynchron zum Schutz Konsistenzgruppen verwendet werden. Ab ONTAP 9.14.1 kann SnapMirror asynchron genutzt werden, um volume-granulare Snapshots mithilfe der Konsistenzgruppe an das Ziel-Cluster zu replizieren. Weitere Informationen finden sich unter Asynchrone SnapMirror Sicherung konfigurieren.

Wie SnapMirror Datenschutzbeziehungen initialisiert werden

Beim ersten Aufruf von SnapMirror erfolgt ein *Basistransfer* vom Quell-Volume zum Ziel-Volume. Die *SnapMirror Richtlinie* für die Beziehung definiert den Inhalt des Basistransfers und alle Aktualisierungen.

Ein Basistransfer gemäß der Standardrichtlinie SnapMirror `MirrorAllSnapshots` umfasst die folgenden Schritte:

- Eine Momentaufnahme des Quellvolumes erstellen.
- Der Snapshot und alle von ihm referenzierten Datenblöcke werden auf das Zielvolume übertragen.
- Die verbleibenden, weniger aktuellen Snapshots auf dem Quellvolume werden auf das Zielvolume übertragen, damit sie im Falle einer Beschädigung des “aktiven” Spiegels verwendet werden können.

Wie SnapMirror Datenschutzbeziehungen aktualisiert werden

Aktualisierungen erfolgen asynchron gemäß dem von Ihnen konfigurierten Zeitplan. Die Aufbewahrung entspricht der Snapshot-Richtlinie auf der Quelle.

Bei jeder Aktualisierung unter der `MirrorAllSnapshots` Richtlinie erstellt SnapMirror einen Snapshot des Quell-Volumes und überträgt diesen Snapshot sowie alle Snapshots, die seit der letzten Aktualisierung erstellt wurden. In der folgenden Ausgabe des Befehls für die `snapmirror policy show` Richtlinie `MirrorAllSnapshots` ist Folgendes zu beachten:

- `Create Snapshot` ist “true”, was bedeutet, dass `MirrorAllSnapshots` einen Snapshot erstellt, wenn SnapMirror die Beziehung aktualisiert.
- `MirrorAllSnapshots` verfügt über die Regeln “sm_created” und “all_source_snapshots”, die darauf hinweisen, dass sowohl der von SnapMirror erstellte Snapshot als auch alle seit der letzten Aktualisierung erstellten Snapshots übertragen werden, wenn SnapMirror die Beziehung aktualisiert.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance
```

```
                    Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

MirrorLatest Richtlinie

Die vorkonfigurierte `MirrorLatest`Richtlinie funktioniert genau wie `MirrorAllSnapshots`, mit der Ausnahme, dass bei der Initialisierung und Aktualisierung nur der von SnapMirror erstellte Snapshot übertragen wird.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

Verwandte Informationen

- "snapmirror policy show"

Informationen zu ONTAP SnapMirror synchroner Disaster Recovery

Ab ONTAP 9.5 wird SnapMirror synchron (SM-S) Technologie auf allen FAS und AFF Plattformen mit mindestens 16 GB Arbeitsspeicher sowie auf allen ONTAP Select Plattformen unterstützt. Die SnapMirror synchron Technologie ist eine lizenzpflichtige Funktion pro Node, die synchrone Datenreplizierung auf Volume-Ebene bereitstellt.

Diese Funktionalität erfüllt die regulatorischen und nationalen Vorgaben für synchrone Replizierung im Finanzwesen, im Gesundheitswesen und anderen regulierten Branchen, in denen kein Datenverlust zulässig ist.

SnapMirror synchron Operationen zulässig

Das Limit für die Anzahl der SnapMirror synchronen Replizierungsvorgänge pro HA-Paar hängt vom Controller-Modell ab.

Die folgende Tabelle listet die Anzahl der SnapMirror synchronen Operationen auf, die pro HA-Paar je nach Plattformtyp und ONTAP Version zulässig sind.

Plattform	ONTAP 9.20.1 und höher	ONTAP 9.11.1 bis ONTAP 9.19.1	ONTAP 9.10.1	ONTAP 9.9.1	Versionen vor ONTAP 9.9.1
AFF	600	400	200	160	80
ASA	400	400	200	160	80
FAS	80	80	80	80	40
ONTAP Select	40	40	40	40	20

Unterstützte Funktionen

Die folgende Tabelle zeigt die mit SnapMirror synchron unterstützten Funktionen und die ONTAP Versionen, in denen diese Unterstützung verfügbar ist.

Funktion	Erste unterstützte Release	Weitere Informationen
Antivirus auf dem primären Volume der SnapMirror synchronen Beziehung	ONTAP 9.6	
Replikation von anwendungserstellten Snapshots	ONTAP 9.7	Wenn ein Snapshot zum Zeitpunkt der `snapshot create` Operation über die CLI oder die ONTAP API mit dem entsprechenden Label versehen wird, repliziert SnapMirror synchron die Snapshots – sowohl benutzererstellte als auch solche, die mit externen Skripten erstellt wurden – nach dem Quiescing der Anwendungen. Ab ONTAP 9.14.1 ist die Label-Anforderung für die Replikation von anwendungserstellten Snapshots nicht mehr erforderlich. Weitere Informationen zur Replikation von anwendungserstellten Snapshots finden Sie unter "NetApp Knowledge Base: Wie sich von Anwendungen erstellte Snapshots mit SnapMirror synchron replizieren lassen".
Autonomer Ransomware-Schutz	ONTAP 9.19.1	
Automatisches Löschen von Klonen	ONTAP 9.6	

FabricPool Aggregate mit den Tiering-Richtlinien Keine, Snapshot oder Auto werden mit SnapMirror synchronem Quell- und Ziel-Cluster unterstützt.	ONTAP 9.5	Das Zielvolumen in einem FabricPool Aggregat kann nicht auf die Tiering-Policy „All“ eingestellt werden.
FC	ONTAP 9.5	Über alle Netzwerke, bei denen die Latenz 10 ms nicht überschreitet
FC-NVMe	ONTAP 9.7	
Dateiklone	ONTAP 9.7	
FPolicy auf dem primären Volume der SnapMirror synchronen Beziehung	ONTAP 9.6	
Harte und weiche Quoten für das primäre Volumen der SnapMirror synchronen Beziehung	ONTAP 9.6	Die Quotenregeln werden nicht an den Ziel-Cluster repliziert; daher wird die Quoten-Datenbank nicht an den Ziel-Cluster repliziert.
Intracluster synchron Beziehungen	ONTAP 9.14.1	Hochverfügbarkeit wird gewährleistet, wenn Quell- und Ziel-Volumes auf unterschiedlichen HA-Paaren platziert werden. Wenn der gesamte Cluster ausfällt, ist der Zugriff auf die Volumes erst nach der Wiederherstellung des Clusters wieder möglich. Intra-Cluster-SnapMirror-synchrone Beziehungen tragen zur Gesamtgrenze der gleichzeitigen Beziehungen pro HA Paar bei.
iSCSI	ONTAP 9.5	
LUN-Klone und NVMe-Namespace-Klone	ONTAP 9.7	
LUN-Klone, die durch von Anwendungen erstellte Snapshots unterstützt werden	ONTAP 9.7	
Zugriff über gemischte Protokolle (NFS v3 und SMB)	ONTAP 9.6	
NDMP/NDMP Wiederherstellung	ONTAP 9.13.1	Sowohl der Quell- als auch der Ziel-Cluster müssen ONTAP 9.13.1 oder höher ausführen, um ein Dump- oder SMTape-basiertes NDMP-Backup von SnapMirror synchronen Volumes durchzuführen. NDMP-Wiederherstellungen, egal ob Dump- oder SMTape-basiert, werden für Ziel-Volumes in einer SnapMirror active sync- oder SnapMirror synchronen Beziehung nicht unterstützt.
Unterbrechungsfreie SnapMirror synchron Operationen (NDO) nur auf AFF/ASA-Plattformen.	ONTAP 9.12.1	Die Unterstützung unterbrechungsfreier Betriebsabläufe ermöglicht die Durchführung vieler gängiger Wartungsaufgaben ohne geplante Ausfallzeiten. Zu den unterstützten Vorgängen gehören Takeover und Giveback sowie Volume Move, vorausgesetzt, dass in jedem der beiden Cluster mindestens ein Node aktiv ist.
NFS v4.2	ONTAP 9.10.1	

NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/TCP	9.10.1	
Aufhebung der Beschränkung der hohen Metadaten-Operationsfrequenz	ONTAP 9.6	
Replikation von Snapshot-Verwaltungsvorgängen	ONTAP 9.19.1	Ab ONTAP 9.19.1 werden die Snapshot-Management-Operationen `snapshot delete`, `snapshot rename` und `snapshot modify` auf den sekundären Cluster repliziert.
Geplante Snapshot-Replikation	ONTAP 9.19.1	Ab ONTAP 9.19.1 können Sie die Replikation geplanter Snapshots mithilfe einer SnapMirror-Richtlinie aktivieren. In Versionen vor ONTAP 9.19.1 werden geplante Snapshots, die mithilfe einer Snapshot-Richtlinie erstellt wurden, nicht repliziert.
Sicherheit für sensible Daten während der Übertragung mit TLS 1.2 Verschlüsselung	ONTAP 9.6	
Wiederherstellung einzelner Dateien und teilweiser Dateiinhalte	ONTAP 9.13.1	
SMB 2.0 oder höher	ONTAP 9.6	
SnapMirror synchron Spiegel-Spiegel-Kaskade	ONTAP 9.6	Die Beziehung vom Ziel-Volume der SnapMirror synchronen Beziehung muss eine SnapMirror asynchrone Beziehung sein.
SVM Disaster Recovery	ONTAP 9.6	• Eine SnapMirror synchron Quelle kann auch eine SVM Disaster Recovery Quelle sein, zum Beispiel eine Fan-Out-Konfiguration mit SnapMirror synchron als einem Zweig und SVM Disaster Recovery als dem anderen. • Eine SnapMirror synchron Quelle kann nicht als SVM Disaster Recovery Ziel dienen, da SnapMirror synchron die Kaskadierung einer Datensicherungsquelle nicht unterstützt. Die synchron Beziehung muss aufgehoben werden, bevor eine SVM Disaster Recovery Flip Resynchronisierung im Ziel-Cluster durchgeführt wird. • Ein SnapMirror synchrones Ziel kann keine SVM-Disaster-Recovery-Quelle sein, da die SVM-Disaster-Recovery die Replikation von DP Volumes nicht unterstützt. Eine Flip-Resynchronisierung der synchronen Quelle hätte zur Folge, dass die SVM-Disaster-Recovery das DP Volume im Ziel-Cluster ausschließt.

"Manipulationssichere Schnappschüsse"	ONTAP 9.19.1	Die Ablaufzeit kann nur bei der Erstellung von Snapshots festgelegt werden. Sie können die Ablaufzeit für vorhandene Snapshots nicht festlegen oder verlängern.
Bandbasierte Wiederherstellung auf das Quellvolume	ONTAP 9.13.1	
Zeitstempelparität zwischen Quell- und Ziel-Volumes für NAS	ONTAP 9.6	Wenn Sie von ONTAP 9.5 auf ONTAP 9.6 aktualisiert haben, wird der Zeitstempel nur für neue und geänderte Dateien im Quell-Volume repliziert. Der Zeitstempel bereits vorhandener Dateien im Quell-Volume wird nicht synchronisiert.

Nicht unterstützte Funktionen

Folgende Funktionen werden bei SnapMirror synchronen Beziehungen nicht unterstützt:

- Konsistenzgruppen
- DP_Optimized (DPO) Systeme
- FlexGroup Volumes
- FlexCache Volumes
- Globale Drosselung
- In einer Fan-Out-Konfiguration kann nur eine Beziehung eine SnapMirror synchron Beziehung sein, alle anderen Beziehungen vom Quellvolume müssen SnapMirror asynchron Beziehungen sein.
- LUN-Verschiebung
- MetroCluster Konfigurationen
- Gemischte SAN- und NVMe-Zugriffs-LUNs und NVMe-Namespaces werden auf demselben Volume oder derselben SVM nicht unterstützt.
- SnapCenter
- SnapLock Volumes
- Dump- oder SMTape-basierte NDMP-Wiederherstellung auf Ziel-Volumes in einer SnapMirror active sync- oder SnapMirror synchronen Beziehung
- Mindestdurchsatz (QoS Min) für Quellvolumes
- Volume SnapRestore
- VVol

Betriebsarten

SnapMirror synchron verfügt über zwei Betriebsmodi, basierend auf der Art der verwendeten SnapMirror Richtlinie:

- **Synchronmodus** Im Synchronmodus werden die E/A-Operationen der Anwendung parallel an das primäre und sekundäre Speichersystem gesendet. Wenn der Schreibvorgang auf dem sekundären Speicher aus irgendeinem Grund nicht abgeschlossen wird, kann die Anwendung weiterhin auf den primären Speicher schreiben. Wenn der Fehlerzustand behoben ist, synchronisiert die SnapMirror synchron Technologie sich automatisch mit dem sekundären Speicher und setzt die Replizierung vom primären zum sekundären Speicher im synchronen Modus fort. Im Synchronmodus gilt RPO=0 und RTO ist sehr niedrig, bis ein

Fehler bei der sekundären Replizierung auftritt. Zu diesem Zeitpunkt sind RPO und RTO unbestimmt, entsprechen jedoch der Zeit, die zur Behebung des Problems, das zum Ausfall der sekundären Replizierung geführt hat, und zum Abschluss der Resynchronisierung benötigt wird.

- **StrictSync-Modus** SnapMirror synchron kann optional im StrictSync-Modus betrieben werden. Wenn der Schreibvorgang auf den Sekundärspeicher aus irgendeinem Grund nicht abgeschlossen wird, schlägt die Anwendungs-I/O fehl, wodurch sichergestellt wird, dass Primär- und Sekundärspeicher identisch sind. Die Anwendungs-I/O auf dem Primärspeicher wird erst wieder aufgenommen, nachdem die SnapMirror Beziehung wieder den `InSync` Status erreicht hat. Wenn der Primärspeicher ausfällt, kann die Anwendungs-I/O nach dem Failover auf dem Sekundärspeicher ohne Datenverlust fortgesetzt werden. Im StrictSync-Modus ist RPO immer null und RTO sehr niedrig.

Beziehungsstatus

Der Status einer SnapMirror synchronen Beziehung ist während des Normalbetriebs immer im `InSync` Status. Wenn die SnapMirror Übertragung aus irgendeinem Grund fehlschlägt, ist das Ziel nicht mit der Quelle synchron und kann in den `OutofSync` Status wechseln.

Bei SnapMirror synchronen Beziehungen prüft das System den Beziehungsstatus automatisch `InSync` oder `OutofSync` in einem festgelegten Intervall. Ist der Beziehungsstatus `OutofSync`, löst ONTAP automatisch den Auto-Resync-Prozess aus, um die Beziehung wieder in den `InSync` Status zu versetzen. Die automatische Resynchronisierung wird nur ausgelöst, wenn die Übertragung aufgrund eines Vorgangs fehlschlägt, wie etwa eines ungeplanten Storage-Failovers am Quell- oder Ziel-Cluster oder eines Netzwerkausfalls. Benutzerinitiierte Vorgänge wie `snapmirror quiesce` und `snapmirror break` lösen keine automatische Resynchronisierung aus.

Wenn der Beziehungsstatus `OutofSync` für eine SnapMirror synchrone Beziehung im StrictSync-Modus erreicht wird, werden alle I/O-Operationen auf dem primären Volume gestoppt. Der `OutofSync`-Zustand für eine SnapMirror synchrone Beziehung im Sync-Modus ist für das primäre Volume nicht störend, und I/O-Operationen sind auf dem primären Volume zulässig.

Geplante Snapshot-Replikation

Ab ONTAP 9.19.1 können Sie den SnapMirror Policy-Parameter `-sync-snapshot-replication-mode` im erweiterten Berechtigungsmodus verwenden, um geplante Snapshots zum SnapMirror Ziel zu replizieren. Die Replikation geplanter Snapshots bietet Symmetrie zwischen den primären und sekundären Volumes in einer SnapsMirror synchronen Beziehung.

Voraussetzungen

- Sie müssen Cluster- oder SVM-Administrator sein
- Sie müssen sich im erweiterten Berechtigungsmodus befinden
- Sie müssen eine benutzerdefinierte SnapMirror-Richtlinie konfigurieren, die den Parameter `-sync -snapshot-replication-mode` verwendet und die Option `sched_created` enthält.
  - Systemdefinierte Richtlinien können nicht geändert werden. Sie müssen eine neue Richtlinie erstellen und die Beziehung neu herstellen.
  - Änderungen an benutzerdefinierten Richtlinien erfordern eine Resynchronisierung (Quiesce gefolgt von Resume), um bei bestehenden Beziehungen wirksam zu werden.

Der Parameter akzeptiert folgende Optionen:

- `none`- Deaktiviert die Replikation von nicht-SnapMirror synchronen Snapshots
- `application_created`- repliziert von der Anwendung erstellte Snapshots

- `sched_created` - repliziert geplante Snapshots
- `sm_created` - repliziert von SnapMirror asynchron (Fanout-Leg) erstellte Snapshots
- Eine durch Kommas getrennte Liste von Typen: `application_created`, `sched_created` und `sm_created`.

Der Parameter wird erst wirksam, wenn der Beziehungsstatus `InSync` ist. Nicht aufgeführte Snapshot-Typen werden nur auf dem primären Volume gespeichert.

Ab ONTAP 9.19.1, `snapmirror initialize` werden alle Snapshots auf den sekundären Cluster repliziert, während `snapmirror resync` nur neue Snapshots repliziert werden, die nach dem letzten gemeinsamen Snapshot erstellt wurden. Bei einer Resynchronisierung werden nicht replizierte Snapshots, die als primary-only gekennzeichnet sind, wenn der Beziehungsstatus `InSync` ist, nicht auf den sekundären Cluster repliziert, und diese Snapshots bleiben nach einer Flip-Resynchronisierung im neuen sekundären Cluster erhalten.

> Das Erstellen von Snapshots auf SnapMirror synchronen Volumes kann die Benutzer-I/O-Latenz erhöhen. Es wird empfohlen, Snapshot-Zeitpläne mit einer Frequenz von mehr als 30 Minuten zu verwenden.

Verwandte Informationen

- "NetApp Technical Report 4733: SnapMirror synchron Konfiguration und bewährte Verfahren"
- "Volume-Snapshot erstellen"
- "Volume-Snapshot löschen"
- "Volume Snapshot ändern"
- "Volume-Snapshot umbenennen"
- "snapmirror break"
- "snapmirror quiesce"

Standardmäßige ONTAP Datenschutzrichtlinien

ONTAP umfasst standardmäßige Datensicherungsstrategien, die für Ihre Datensicherungsbeziehungen verwendet werden können. Die verwendete Richtlinie hängt vom Typ der Datensicherungsbeziehung ab.

Ab ONTAP 9.20.1 können Sie "Konfiguration der asynchronen Backend-SnapMirror Replizierung über bestehende FC-Fabrics" mithilfe einer unterstützten asynchronen Datensicherungsstrategie. Die folgenden Standard-Datensicherungsstrategien unterstützen die Backend-FC-Replizierung:

- asynchron
- MirrorAllSnapshots
- MirrorAndVault
- XDPDefault

Wenn die Standardrichtlinien Ihren Anforderungen an Datenschutzbeziehungen nicht entsprechen, können Sie "eine benutzerdefinierte Richtlinie erstellen".

Liste der Standard-Schutzrichtlinien und Beschreibungen

Standard-Schutzrichtlinien und die zugehörigen Richtlinientypen sind nachfolgend beschrieben.

Name	Beschreibung	Richtlinientyp
asynchron	Eine einheitliche SnapMirror asynchrone und Vault-Richtlinie zur Spiegelung des zuletzt aktiven Dateisystems sowie täglicher und wöchentlicher Snapshots mit einem stündlichen Übertragungsplan.	asynchron
AutomatedFailOver	Richtlinie für SnapMirror synchron mit Null-RTO-Garantie, bei der die Client-I/O bei Replikationsfehlern nicht unterbrochen wird.	Synchron
AutomatedFailOverDuplex	Richtlinie für SnapMirror synchron mit Null-RTO-Garantie und bidirektionaler synchroner Replikation.	Synchron
CloudBackupDefault	Vault-Richtlinie mit täglicher Regel.	asynchron
Kontinuierlich	Richtlinie für die Spiegelung von S3-Bucket.	Kontinuierlich
DailyBackup	Vault-Richtlinie mit einer täglichen Regel und einem täglichen Übertragungsplan.	asynchron
DPDefault	SnapMirror asynchrone Richtlinie zum Spiegeln aller Snapshots und des zuletzt aktiven Dateisystems.	asynchron
MirrorAllSnapshots	SnapMirror asynchrone Richtlinie zum Spiegeln aller Snapshots und des zuletzt aktiven Dateisystems.	asynchron
MirrorAllSnapshotsDiscardNetwork	SnapMirror asynchrone Richtlinie zum Spiegeln aller Snapshots und des zuletzt aktiven Dateisystems unter Ausschluss der Netzwerkkonfigurationen.	asynchron
MirrorAndVault	Eine einheitliche SnapMirror asynchrone und Vault-Richtlinie zur Spiegelung des zuletzt aktiven Dateisystems sowie täglicher und wöchentlicher Snapshots.	asynchron
MirrorAndVaultDiscardNetwork	Eine einheitliche SnapMirror asynchrone und Vault-Richtlinie zur Spiegelung des zuletzt aktiven Dateisystems sowie täglicher und wöchentlicher Snapshots, wobei die Netzwerkkonfigurationen ausgenommen sind.	asynchron
MirrorLatest	SnapMirror asynchrone Richtlinie zum Spiegeln des zuletzt aktiven Dateisystems.	asynchron
SnapCenterSync	Richtlinie für SnapMirror synchron für SnapCenter mit Application Created Snapshot Konfiguration.	Synchron
StrictSync	Richtlinie für SnapMirror synchron, bei der der Clientzugriff bei einem Replikationsfehler unterbrochen wird.	Synchron

Name	Beschreibung	Richtlinientyp
Synchronisieren	Richtlinie für SnapMirror synchron, bei der der Clientzugriff bei einem Replikationsfehler nicht unterbrochen wird.	Synchron
Unified7year	Einheitliche SnapMirror Richtlinie mit 7-jähriger Aufbewahrungsfrist.	asynchron
XDPDefault	Vault-Richtlinie mit täglichen und wöchentlichen Regeln.	asynchron

Von ONTAP StrictSync und Synchronisierungsrichtlinien unterstützte Workloads

StrictSync und Synchronisierungsrichtlinien unterstützen alle LUN-basierten Anwendungen mit den Protokollen FC, iSCSI und FC-NVMe sowie die Protokolle NFSv3 und NFSv4 für Unternehmensanwendungen wie Datenbanken, VMWare, Quota, SMB und so weiter. Ab ONTAP 9.6 kann SnapMirror synchron für Unternehmensdateidienste wie Electronic Design Automation (EDA), Home-Verzeichnisse und Software-Build-Workloads verwendet werden.

In ONTAP 9.5 sind bei der Auswahl von NFSv3- oder NFSv4-Workloads für eine Sync-Richtlinie einige wichtige Aspekte zu beachten. Die Menge der Lese- oder Schreibvorgänge der Workloads ist dabei unerheblich, da die Sync-Richtlinie auch hohe Lese- oder Schreib-IO-Workloads verarbeiten kann. In ONTAP 9.5 sind Workloads mit übermäßiger Dateierstellung, Verzeichniserstellung, Änderungen von Dateiberechtigungen oder Verzeichnisberechtigungen möglicherweise nicht geeignet (diese werden als Workloads mit hohem Metadatenaufkommen bezeichnet). Ein typisches Beispiel für einen solchen High-Metadaten-Workload ist ein DevOps-Workload, bei dem mehrere Testdateien erstellt, Automatisierungen ausgeführt und die Dateien gelöscht werden. Ein weiteres Beispiel ist ein paralleler Build-Workload, bei dem während der Kompilierung mehrere temporäre Dateien erzeugt werden. Die Auswirkung einer hohen Rate an Schreib-Metadatenaktivität besteht darin, dass die Synchronisierung zwischen den Spiegeln vorübergehend unterbrochen werden kann, was dazu führt, dass Lese- und Schreib-IOs vom Client angehalten werden.

Ab ONTAP 9.6 werden diese Einschränkungen aufgehoben, und SnapMirror synchron kann für Workloads von Unternehmensdateidiensten verwendet werden, die Mehrbenutzerumgebungen umfassen, wie etwa Home-Verzeichnisse und Software-Build-Workloads.

Verwandte Informationen

"SnapMirror synchron Konfiguration und bewährte Verfahren"

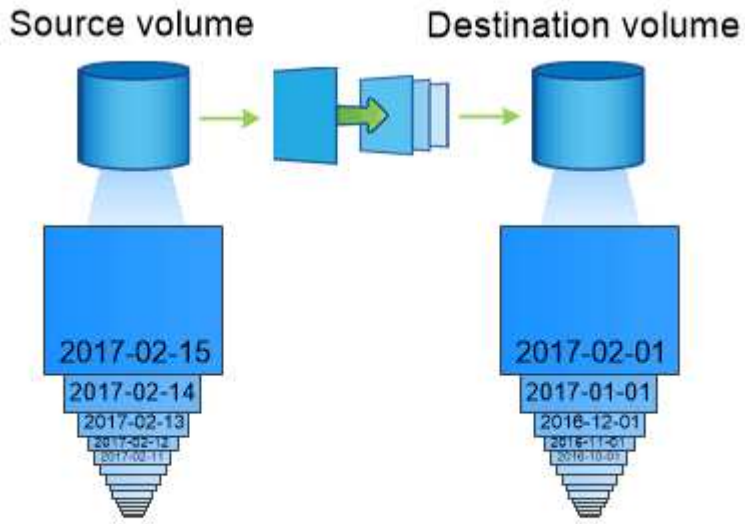
Informationen zur Vault-Archivierung mit ONTAP SnapMirror Technologie

SnapMirror Vault-Richtlinien ersetzen die SnapVault Technologie in ONTAP 9.3 und höher. Eine SnapMirror Vault-Richtlinie wird für die Festplatten-zu-Festplatten-Snapshot-Replikation zur Einhaltung von Standards und für andere Governance-bezogene Zwecke verwendet. Im Gegensatz zu einer SnapMirror Beziehung, bei der das Ziel in der Regel nur die aktuell im Quellvolume vorhandenen Snapshots enthält, bewahrt ein Vault-Ziel typischerweise zeitpunktgenaue Snapshots auf, die über einen deutlich längeren Zeitraum erstellt wurden.

Beispielsweise könnten Sie monatliche Snapshots Ihrer Daten über einen Zeitraum von 20 Jahren

aufbewahren, um die gesetzlichen Buchführungsvorschriften für Ihr Unternehmen einzuhalten. Da keine Anforderung besteht, Daten aus dem Vault-Speicher bereitzustellen, können auf dem Zielsystem langsamere, kostengünstigere Festplatten verwendet werden.

Die folgende Abbildung veranschaulicht SnapMirror Vault-Datenschutzbeziehungen.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Wie Vault-Datenschutzbeziehungen initialisiert werden

Die SnapMirror Richtlinie für die Beziehung definiert den Inhalt des Basistransfers und aller Aktualisierungen.

Ein Basistransfer unter der Standard-Vault-Richtlinie `XDPDefault` erstellt einen Snapshot des Quellvolumes und überträgt anschließend diese Kopie sowie die von ihr referenzierten Datenblöcke auf das Zielvolume. Im Gegensatz zu SnapMirror Beziehungen sind bei einer Vault-Sicherung ältere Snapshots nicht in der Baseline enthalten.

Wie Vault-Datenschutzbeziehungen aktualisiert werden

Aktualisierungen erfolgen asynchron gemäß dem von Ihnen konfigurierten Zeitplan. Die in der Richtlinie für die SnapMirror Beziehung definierten Regeln legen fest, welche neuen Snapshots in Aktualisierungen einbezogen werden und wie viele Kopien beibehalten werden. Die in der Richtlinie definierten Labels („monthly“ zum Beispiel) müssen mit einem oder mehreren Labels übereinstimmen, die in der Snapshot-Richtlinie auf der Quelle definiert sind. Andernfalls schlägt die Replikation fehl.

Bei jeder Aktualisierung unter der `XDPDefault` Richtlinie werden von SnapMirror Snapshots übertragen, die seit der letzten Aktualisierung erstellt wurden, sofern ihre Bezeichnungen mit den in den Richtlinienregeln definierten Bezeichnungen übereinstimmen. In der folgenden Ausgabe des Befehls für die `snapmirror policy show` Richtlinie `XDPDefault` ist Folgendes zu beachten:

- `Create Snapshot` ist “false”, was bedeutet, dass `XDPDefault` beim Aktualisieren der SnapMirror Beziehung keinen Snapshot erstellt.
- `XDPDefault` verfügt über die Regeln “daily” und “weekly”, die angeben, dass alle Snapshots mit übereinstimmenden Bezeichnungen auf der Quelle übertragen werden, wenn SnapMirror die Beziehung

aktualisiert.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                       Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Verwandte Informationen

- "snapmirror policy show"

Informationen zur einheitlichen Replizierung von ONTAP SnapMirror

SnapMirror *einheitliche Replikation* ermöglicht die Konfiguration von Notfallwiederherstellung und Archivierung auf demselben Ziel-Volume. Wenn einheitliche Replikation angebracht ist, ergeben sich Vorteile durch den geringeren Bedarf an Sekundärspeicher, die Begrenzung der Anzahl von Basistransfers und die Verringerung des Netzwerkverkehrs.

Wie einheitliche Datenschutzbeziehungen initialisiert werden

Wie bei SnapMirror führt die einheitliche Datensicherung beim ersten Aufruf einen Basistransfer durch. Die SnapMirror Richtlinie für die Beziehung definiert den Inhalt des Basistransfers und aller Aktualisierungen.

Ein Basistransfer unter der standardmäßigen einheitlichen Datensicherungsstrategie `MirrorAndVault` erstellt eine Snapshot-Kopie des Quellvolumes und überträgt diese Kopie sowie die von ihr referenzierten Datenblöcke auf das Ziel-Volume. Wie bei der Vault-Archivierung sind ältere Snapshots beim einheitlichen

Datenschutz nicht im Basistransfer enthalten.

Wie einheitliche Datenschutzbeziehungen aktualisiert werden

Bei jeder Aktualisierung unter der `MirrorAndVault` Richtlinie erstellt SnapMirror einen Snapshot des Quellvolumes und überträgt diesen Snapshot sowie alle Snapshots, die seit der letzten Aktualisierung erstellt wurden, sofern deren Bezeichnungen mit den in den Snapshot-Richtlinienregeln definierten Bezeichnungen übereinstimmen. In der folgenden Ausgabe des Befehls für die `snapmirror policy show` Richtlinie `MirrorAndVault` ist Folgendes zu beachten:

- `Create Snapshot` ist “true”, was bedeutet, dass `MirrorAndVault` einen Snapshot erstellt, wenn SnapMirror die Beziehung aktualisiert.
- `MirrorAndVault` verfügt über die Regeln “sm_created”, “daily” und “weekly”, was darauf hinweist, dass sowohl der von SnapMirror erstellte Snapshot als auch die Snapshots mit übereinstimmenden Bezeichnungen auf der Quelle übertragen werden, wenn SnapMirror die Beziehung aktualisiert.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Einheitliche 7-Jahres-Richtlinie

Die vorkonfigurierte `Unified7year` Richtlinie funktioniert genau wie `MirrorAndVault`, außer dass eine vierte Regel monatliche Snapshots überträgt und diese sieben Jahre lang aufbewahrt.

```
                           Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                                  ----------------     ----  -------- ----
--------- ------
                                  sm_created              1  false       0 -
-
                                  daily                   7  false       0 -
-
                                  weekly                 52  false       0 -
-
                                  monthly                84  false       0 -
-
```

Schutz vor möglicher Datenbeschädigung

Die einheitliche Datenreplizierung beschränkt den Inhalt des Basistransfers auf den Snapshot, der bei der Initialisierung von SnapMirror erstellt wurde. Bei jeder Aktualisierung erstellt SnapMirror einen weiteren Snapshot der Quelle und überträgt diesen Snapshot sowie alle neuen Snapshots, deren Bezeichnungen mit den in den Snapshot-Richtlinienregeln definierten Bezeichnungen übereinstimmen.

Sie können sich vor der Möglichkeit schützen, dass ein aktualisierter Snapshot beschädigt wird, indem Sie eine Kopie des zuletzt übertragenen Snapshots auf dem Ziel erstellen. Diese „lokale Kopie“ bleibt unabhängig von den Aufbewahrungsregeln auf der Quelle erhalten, sodass selbst dann, wenn der ursprünglich von SnapMirror übertragene Snapshot auf der Quelle nicht mehr verfügbar ist, eine Kopie davon auf dem Ziel verfügbar ist.

Wann die einheitliche Datenreplizierung verwendet wird

Sie müssen den Nutzen der Aufrechterhaltung eines vollständigen Spiegels gegen die Vorteile der einheitlichen Datenreplizierung abwägen, die die Reduzierung des Bedarfs an sekundärem Storage, die Begrenzung der Anzahl von Basistransfers und die Verringerung des Netzwerkverkehrs mit sich bringt.

Der entscheidende Faktor für die Eignung einer einheitlichen Replikation ist die Änderungsrate des aktiven Dateisystems. Ein herkömmlicher Spiegel eignet sich beispielsweise besser für ein Volume, das stündliche Snapshots von Datenbanktransaktionsprotokollen enthält.

Verwandte Informationen

- "snapmirror policy show"

Wie ONTAP Datensicherungsziel-Volumes automatisch wachsen

Während einer Spiegelübertragung zum Datenschutz wächst das Ziel-Volume automatisch, wenn das Quell-Volume gewachsen ist, vorausgesetzt, im Aggregat, das das Volume enthält, ist noch Speicherplatz verfügbar.

Dieses Verhalten tritt unabhängig von jeglichen Einstellungen für automatisches Wachstum am Ziel auf. Das Wachstum des Volumes kann nicht begrenzt werden, und ONTAP kann nicht daran gehindert werden, es zu vergrößern.

Standardmäßig sind Datensicherungsvolumes auf den `grow_shrink` automatische Größenanpassung-Modus eingestellt, wodurch das Volume je nach belegtem Speicherplatz wächst oder schrumpft. Die maximale automatische Größenanpassung für Datensicherungsvolumes entspricht der maximalen FlexVol-Größe und ist plattformabhängig. Beispiel:

- FAS8200, Standard-DP Volume maximale automatische Größenanpassung = 100TB

Weitere Informationen finden sich unter "NetApp Hardware Universe".

Informationen zu ONTAP Datenschutz Fan-Out und Kaskadenbereitstellungen

Eine *fan-out* Bereitstellung kann verwendet werden, um den Datenschutz auf mehrere sekundäre Systeme auszuweiten. Eine *cascade* Bereitstellung kann verwendet werden, um den Datenschutz auf tertiäre Systeme auszuweiten.

Sowohl Fan-Out- als auch Kaskadenbereitstellungen unterstützen beliebige Kombinationen aus SnapMirror DR, SnapVault oder einheitlicher Replikation. Ab ONTAP 9.5 unterstützen SnapMirror synchron Beziehungen Fan-Out-Bereitstellungen mit einer oder mehreren SnapMirror asynchron Beziehungen. Nur eine Beziehung in der Fan-Out-Konfiguration darf eine SnapMirror synchron Beziehung sein, alle anderen Beziehungen vom Quellvolume müssen SnapMirror asynchron Beziehungen sein. SnapMirror synchron Beziehungen unterstützen auch Kaskadenbereitstellungen (ab ONTAP 9.6); die Beziehung vom Zielvolume der SnapMirror synchron Beziehung muss jedoch eine SnapMirror asynchron Beziehung sein. SnapMirror Active Sync (unterstützt ab ONTAP 9.13.1) unterstützt ebenfalls Fan-Out-Konfigurationen.

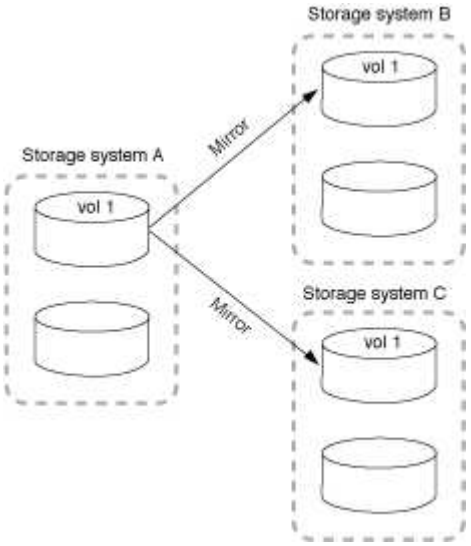
> Mithilfe einer Fan-in-Bereitstellung lassen sich Datensicherungsbeziehungen zwischen mehreren primären Systemen und einem einzelnen sekundären System erstellen. Jede Beziehung muss ein anderes Volume auf dem sekundären System verwenden.

> Es sollte beachtet werden, dass Volumes, die Teil einer Fan-Out- oder Kaskadenkonfiguration sind, länger für die Resynchronisierung benötigen können. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „preparing“ über einen längeren Zeitraum meldet.

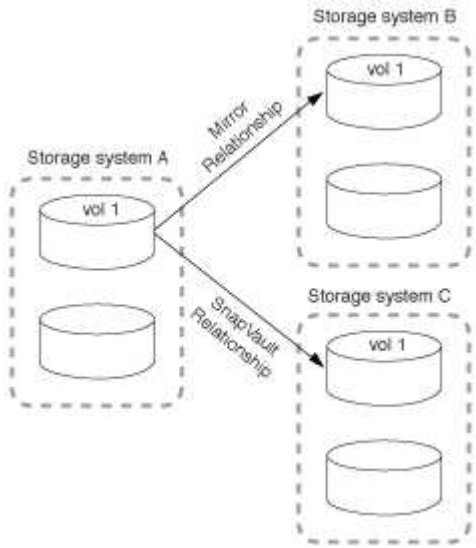
Funktionsweise von Fan-Out-Bereitstellungen

SnapMirror unterstützt *multiple-mirrors* und *mirror-vault* Fan-Out-Bereitstellungen.

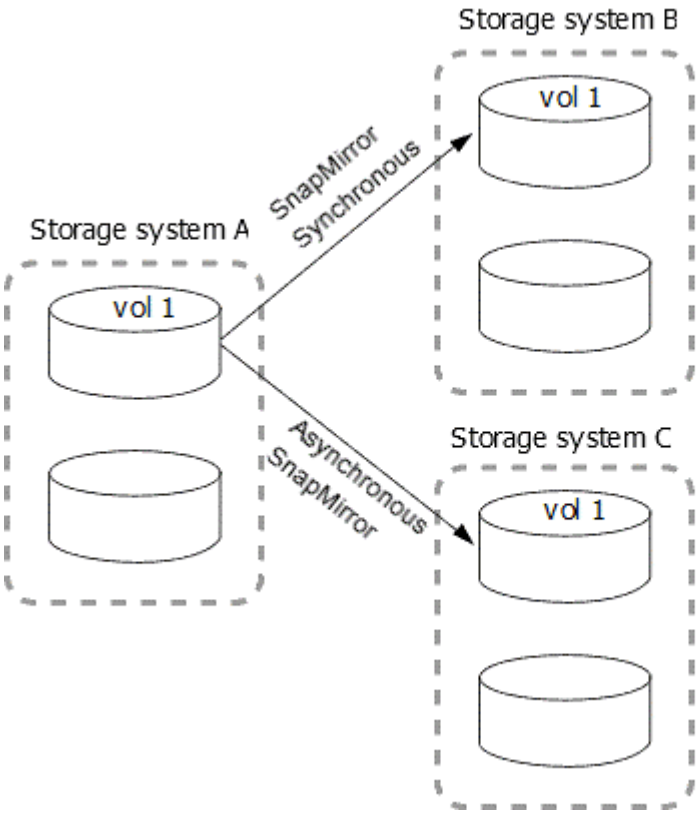
Eine Multiple-Mirrors-Fan-Out-Bereitstellung besteht aus einem Quellvolume, das eine Spiegelbeziehung zu mehreren sekundären Volumes aufweist.



Eine Mirror Vault Fan Out Bereitstellung besteht aus einem Quellvolume, das eine Spiegelbeziehung zu einem sekundären Volume und eine SnapVault Beziehung zu einem anderen sekundären Volume hat.



Ab ONTAP 9.5 sind Fan-out-Bereitstellungen mit SnapMirror synchronen Beziehungen möglich; jedoch darf nur eine Beziehung in der Fan-out-Konfiguration eine SnapMirror synchron Beziehung sein, alle anderen Beziehungen vom Quellvolume müssen SnapMirror asynchron Beziehungen sein.



Wie Kaskadenbereitstellungen funktionieren

SnapMirror unterstützt kaskadierende Bereitstellungen von *mirror-mirror*, *mirror-vault*, *vault-mirror* und *vault-vault*.

Eine Mirror-Mirror-Kaskadenbereitstellung besteht aus einer Kette von Beziehungen, in der ein Quellvolume auf ein sekundäres Volume gespiegelt wird und das sekundäre Volume auf ein tertiäres Volume gespiegelt wird. Wenn das sekundäre Volume nicht verfügbar ist, lässt sich die Beziehung zwischen dem primären und dem tertiären Volume synchronisieren, ohne einen neuen Basistransfer durchzuführen.

In einer Beziehung von kaskadierten Volumes werden Langzeitaufbewahrungs-Snapshots nur auf dem finalen SnapMirror Ziel-Volume der Kaskade in allen Versionen von ONTAP 9 unterstützt. Die Aktivierung von Langzeitaufbewahrungs-Snapshots auf einem beliebigen Zwischen-Volume in der Kaskade führt zu fehlenden Backups und Snapshots. Wenn eine nicht unterstützte Konfiguration vorliegt, bei der Langzeitaufbewahrungs-Snapshots auf einem beliebigen Zwischen-Volume einer Kaskade aktiviert wurden, sollte der technische Support kontaktiert und auf die "NetApp Knowledge Base: Das Kaskadieren eines Volumes mit aktivierten Langzeitaufbewahrungs-Snapshots (LTR) wird nicht unterstützt." verwiesen werden.

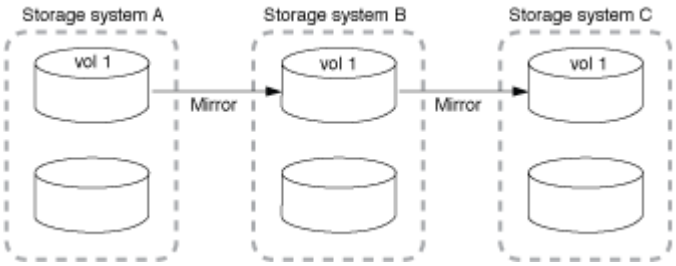
Die folgenden ONTAP Versionen erlauben es nicht, Langzeit-Snapshots auf einem beliebigen Volume in einer Kaskade zu aktivieren, außer auf dem endgültigen SnapMirror Zielvolume.

- 9.15.1 und später
- 9.14.1P2 und P4 bis P14
- 9.13.1P9 bis P17
- 9.12.1 P12 bis P19
- 9.11.1P15 bis P20
- 9.10.1P18 bis P20

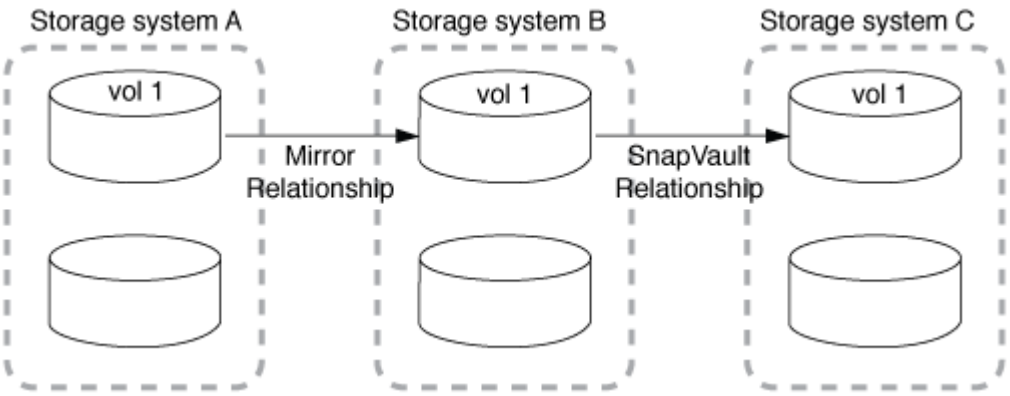
- 9.9.1P20

Weitere Informationen zu "Langzeitaufbewahrungs-Snapshots".

Ab ONTAP 9.6 werden SnapMirror synchron Beziehungen in einer Mirror-Mirror-Kaskadenbereitstellung unterstützt. Nur die primären und sekundären Volumes können sich in einer SnapMirror synchron Beziehung befinden. Die Beziehung zwischen den sekundären und tertiären Volumes muss asynchron sein.



Eine Mirror-Vault-Kaskadenimplementierung besteht aus einer Kette von Beziehungen, in der ein Quellvolume auf ein sekundäres Volume gespiegelt wird und das sekundäre Volume auf ein tertiäres Volume übertragen wird.



Vault Mirror und Vault Vault Kaskadenbereitstellungen werden ebenfalls unterstützt:

- Eine Vault-Mirror-Kaskadenimplementierung besteht aus einer Kette von Beziehungen, in der ein Quellvolume auf ein sekundäres Volume gesichert wird und das sekundäre Volume auf ein Tertiärvolume gespiegelt wird.
- Eine Vault-Vault-Kaskadenbereitstellung besteht aus einer Kette von Beziehungen, in der ein Quellvolume in ein sekundäres Volume repliziert wird und das sekundäre Volume in ein tertiäres Volume repliziert wird.

Verwandte Informationen

- Wiederaufnahme des Schutzes in einer Fan-out-Konfiguration mit SnapMirror active sync

Informationen zur ONTAP SnapMirror Lizenzierung

Ab ONTAP 9.3 ist die Lizenzierung für die Replikation zwischen ONTAP Instanzen vereinfacht. In ONTAP 9 Releases unterstützt die SnapMirror Lizenz sowohl Vault- als auch Mirror-Beziehungen. Mit einer SnapMirror Lizenz kann die ONTAP Replizierung sowohl für Backup- als auch für Disaster Recovery Anwendungsfälle unterstützt werden.

Vor der Einführung von ONTAP 9.3 war eine separate SnapVault Lizenz erforderlich, um *Vault*-Beziehungen zwischen ONTAP Instanzen zu konfigurieren, wobei die DP-Instanz eine höhere Anzahl von Snapshots

behalten konnte, um Backup-Anwendungsfälle mit längeren Aufbewahrungszeiten zu unterstützen. Eine SnapMirror Lizenz war erforderlich, um *Mirror*-Beziehungen zwischen ONTAP Instanzen zu konfigurieren, bei denen jede ONTAP Instanz die gleiche Anzahl von Snapshots (also ein *Mirror*-Abbild) behielt, um Disaster-Recovery-Anwendungsfälle zu unterstützen und Cluster-Failover zu ermöglichen. Sowohl SnapMirror als auch SnapVault Lizenzen werden weiterhin für ONTAP 8.x und 9.x Releases verwendet und unterstützt.

Während SnapVault Lizenzen weiterhin funktionieren und sowohl für ONTAP 8.x als auch für 9.x unterstützt werden, kann die SnapMirror Lizenz anstelle einer SnapVault Lizenz verwendet werden und kann sowohl für Mirror- als auch für Vault-Konfigurationen eingesetzt werden.

Für die ONTAP asynchrone Replizierung wird ab ONTAP 9.3 eine einheitliche Replikations-Engine verwendet, um Richtlinien für den erweiterten Datenschutzmodus (XDP) zu konfigurieren, wobei die SnapMirror Lizenz für eine Spiegelrichtlinie, eine Vault-Richtlinie oder eine Spiegel-Vault-Richtlinie konfiguriert werden kann. Eine SnapMirror Lizenz ist sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster erforderlich. Eine SnapVault Lizenz ist nicht erforderlich, wenn bereits eine SnapMirror Lizenz installiert ist. Die SnapMirror asynchron unbefristete Lizenz ist in der ONTAP One Software Suite enthalten, die auf neuen AFF und FAS Systemen installiert ist.

Die Konfigurationsgrenzen für den Datenschutz werden anhand verschiedener Faktoren bestimmt, darunter Ihre ONTAP Version, die Hardwareplattform und die installierten Lizenzen. Weitere Informationen finden sich unter "Hardware Universe".

SnapMirror synchron Lizenz

Ab ONTAP 9.5 werden SnapMirror synchron Beziehungen unterstützt. Für die Erstellung einer SnapMirror synchron Beziehung sind die folgenden Lizenzen erforderlich:

- Die SnapMirror synchron Lizenz ist sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster erforderlich.

  Die SnapMirror synchron Lizenz ist Teil der "ONTAP One Lizenzpaket".

  Wenn Ihr System vor Juni 2019 mit einem Premium oder Flash Bundle erworben wurde, kann ein NetApp Lizenzschlüssel heruntergeladen werden, um die erforderliche SnapMirror synchron Lizenz von der NetApp Support Site zu erhalten: "Lizenzschlüssel".

- Die SnapMirror Lizenz ist sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster erforderlich.

SnapMirror Cloud-Lizenz

Ab ONTAP 9.8 bietet die SnapMirror Cloud-Lizenz asynchrone Replizierung von Snapshots von ONTAP Instanzen zu Objektspeicher-Endpunkten. Replikationsziele können sowohl mit lokalen Objektspeichern als auch mit S3 und S3-kompatiblen öffentlichen Cloud Objektspeicherdiensten konfiguriert werden. SnapMirror Cloud-Beziehungen von ONTAP Systemen zu vorqualifizierten Objektspeicherzielen werden unterstützt.

SnapMirror cloud ist nicht als Einzellizenz erhältlich. Es wird nur eine Lizenz pro ONTAP Cluster benötigt. Zusätzlich zu einer SnapMirror cloud Lizenz ist auch die SnapMirror asynchron Lizenz erforderlich.

Für die Erstellung einer SnapMirror Cloud-Beziehung sind die folgenden Lizenzen erforderlich:

- Sowohl eine SnapMirror Lizenz als auch eine SnapMirror Cloud-Lizenz für die Replikation direkt zum Objektspeicher-Endpunkt.
- Bei der Konfiguration eines Replikationsworkflows mit mehreren Richtlinien (z. B. Disk-to-Disk-to-Cloud) ist eine SnapMirror Lizenz auf allen ONTAP Instanzen erforderlich, während die SnapMirror Cloud-Lizenz nur für den Quell-Cluster erforderlich ist, der direkt zum Objektspeicher-Endpunkt repliziert.

Ab ONTAP 9.9.1 ist es möglich, "System Manager für SnapMirror Cloud-Replikation verwenden".

Eine Liste der autorisierten SnapMirror Cloud-Drittanbieteranwendungen ist auf der NetApp Website veröffentlicht.

Data Protection Optimized Lizenz

Data Protection Optimized (DPO) Lizenzen werden nicht mehr verkauft, und DPO wird auf aktuellen Plattformen nicht unterstützt; wenn jedoch eine DPO Lizenz auf einer unterstützten Plattform installiert ist, bietet NetApp weiterhin Support bis zum Ende der Verfügbarkeit dieser Plattform.

DPO ist nicht im ONTAP One Lizenzpaket enthalten, und ein Upgrade auf das ONTAP One Lizenzpaket ist nicht möglich, wenn die DPO Lizenz auf einem System installiert ist.

Informationen zu den unterstützten Plattformen sind unter "Hardware Universe" zu finden.

Funktionserweiterungen von ONTAP DPO-Systemen

Ab ONTAP 9.6 erhöht sich die maximale Anzahl unterstützter FlexVol Volumes, wenn die DP_Optimized (DPO) Lizenz installiert ist. Ab ONTAP 9.4 unterstützen Systeme mit der DPO Lizenz SnapMirror Backoff, volumenübergreifende Hintergrunddeduplizierung, die Verwendung von Snapshot-Blöcken als Donoren und Kompaktierung.

Ab ONTAP 9.6 wurde die maximal unterstützte Anzahl von FlexVol Volumes auf sekundären oder Datensicherungssystemen erhöht, sodass eine Skalierung auf bis zu 2.500 FlexVol Volumes pro Knoten oder bis zu 5.000 im Failover-Modus möglich ist. Die Erhöhung der FlexVol Volumes wird mit dem "DP_Optimized (DPO) Lizenz" ermöglicht. Ein "SnapMirror Lizenz" ist weiterhin sowohl auf dem Quell- als auch auf dem Zielknoten erforderlich.

Ab ONTAP 9.4 sind die folgenden Funktionserweiterungen für DPO-Systeme verfügbar:

- SnapMirror backoff: In DPO-Systemen erhält der Replikationsverkehr die gleiche Priorität wie die Client-Workloads.

  SnapMirror Backoff ist auf DPO-Systemen standardmäßig deaktiviert.

- Volume Hintergrunddeduplizierung und volumeübergreifende Hintergrunddeduplizierung: Volume Hintergrunddeduplizierung und volumeübergreifende Hintergrunddeduplizierung sind in DPO Systemen aktiviert.

  Sie können den `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` Befehl ausführen, um die vorhandenen Daten zu deduplizieren. Die empfohlene Vorgehensweise ist, den Befehl außerhalb der Spitzenzeiten auszuführen, um die Auswirkungen auf die Leistung zu verringern.

  Weitere Informationen zu `storage aggregate efficiency cross-volume-dedupe start` finden sich in der "ONTAP-Befehlsreferenz".

- Erhöhte Einsparungen durch die Verwendung von Snapshot-Blöcken als Spender: Die Datenblöcke, die im aktiven Dateisystem nicht verfügbar sind, aber in Snapshots gespeichert sind, werden als Spender für die Volume-Deduplizierung verwendet.

  Die neuen Daten können mit den in Snapshots gespeicherten Daten dedupliziert werden, wodurch die Snapshot-Blöcke effektiv gemeinsam genutzt werden. Der vergrößerte freie Speicherplatz führt zu weiteren

Einsparungen, insbesondere wenn das Volume eine große Anzahl von Snapshots enthält.

- Compaction: Die Datenkompaktierung ist auf DPO-Volumes standardmäßig aktiviert.

Informationen zur Mustererkennung von Pfadnamen in ONTAP SnapMirror Befehlen

Mithilfe von Mustervergleich können Sie die Quell- und Zielpfade in `snapmirror` Befehlen angeben.

```
`snapmirror`Befehle verwenden vollqualifizierte Pfadnamen im folgenden
Format: `vserver:volume`. Der Pfadname kann abgekürzt werden, wenn der
SVM-Name nicht eingegeben wird. Wenn dies erfolgt, nimmt der  `snapmirror`
Befehl den lokalen SVM-Kontext des Benutzers an.
```

Unter der Annahme, dass die SVM “vserver1” heißt und das Volume “vol1” heißt, lautet der vollqualifizierte Pfadname `vserver1:vol1`.

Sie können das Sternchen (*) in Pfaden als Platzhalter verwenden, um übereinstimmende, vollqualifizierte Pfadnamen auszuwählen. Die folgende Tabelle enthält Beispiele für die Verwendung des Platzhalters zur Auswahl eines Bereichs von Volumes.

`*`	Entspricht allen Pfaden.
`vs*`	Findet alle SVMs und Volumes, deren SVM-Namen mit `vs` beginnen.
`:*src`	Findet alle SVMs mit Volumennamen, die den `src` Text enthalten.
`:vol`	Findet alle SVMs mit Volumennamen, die mit `vol` beginnen.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------ ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                 Snapmirrored  Idle           -
true    -
```

Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

Anwenden erweiterter Abfragen auf ONTAP SnapMirror Beziehungen

Sie können erweiterte Abfragen verwenden, um SnapMirror Operationen an mehreren SnapMirror Beziehungen gleichzeitig durchzuführen. Beispielsweise kann es mehrere nicht initialisierte SnapMirror Beziehungen geben, die mit einem einzigen Befehl initialisiert werden sollen.

Über diese Aufgabe

Es besteht die Möglichkeit, erweiterte Abfragen auf die folgenden SnapMirror Operationen anzuwenden:

- Initialisierung nicht initialisierter Beziehungen
- Wiederaufnahme ruhender Beziehungen
- Resynchronisierung unterbrochener Beziehungen
- Aktualisierung inaktiver Beziehungen
- Abbruch von Beziehungsdatenübertragungen

Schritt

1. Eine SnapMirror Operation auf vielen Beziehungen durchführen:

   `snapmirror command` `{-state state } *`

   Der folgende Befehl initialisiert SnapMirror Beziehungen, die sich in einem `Uninitialized` Zustand befinden:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

   Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

Kompatible ONTAP Versionen für SnapMirror Beziehungen

Die Quell- und Zielvolumes müssen kompatible ONTAP Versionen ausführen, bevor eine SnapMirror Datenschutzbeziehung erstellt wird. Vor einem ONTAP Upgrade sollte überprüft werden, ob die aktuelle ONTAP Version mit der Ziel-ONTAP Version für SnapMirror Beziehungen kompatibel ist.

Vereinheitlichte Replikationsbeziehungen

Für SnapMirror Beziehungen vom Typ “XDP”, bei Verwendung von lokalen oder Cloud Volumes ONTAP Versionen:

Ab ONTAP 9.9.0:

- ONTAP 9.x.0 Releases sind ausschließlich für die Cloud verfügbar und unterstützen Cloud Volumes ONTAP Systeme. Das Sternchen (*) nach der Versionsnummer kennzeichnet eine reine Cloud-Version.

  ONTAP 9.16.0 bildet eine Ausnahme von der Cloud-only-Regel, da es Unterstützung für "ASA r2-Systeme" bietet. Das Pluszeichen (+) nach der Release-Version zeigt sowohl eine ASA r2- als auch eine Cloud-unterstützte Version an. ASA r2-Systeme unterstützen

SnapMirror-Beziehungen nur zu anderen ASA r2-Systemen.

- ONTAP 9.x.1 Releases sind allgemeine Releases und unterstützen sowohl On-Premises als auch Cloud Volumes ONTAP Systeme.

Wenn "fortschrittlicher Kapazitätsausgleich" auf Volumes in Clustern aktiviert ist, auf denen ONTAP 9.16.1 oder höher ausgeführt wird, werden SnapMirror-Übertragungen zu Clustern, auf denen ONTAP Versionen vor ONTAP 9.16.1 ausgeführt werden, nicht unterstützt.

Interoperabilität ist bidirektional.

Interoperabilität für ONTAP Version 9.5 und höher

ONTAP Version …	**Ist mit diesen früheren ONTAP Versionen kompatibel…**																					
	9.19.1	9.18.1	9.17.1	9.16.1	9.16.0+	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9,8	9,7	9,6	9,5
9.19.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.18.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.17.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.16.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.16.0+	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.15.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein
9.15.0*	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein	Nein	Nein
9.14.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein
9.14.0*	Nein	Nein	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein	Nein	Nein
9.13.1	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein

ONTAP Version …	Ist mit diesen früheren ONTAP Versionen kompatibel…																						
9.13.0*	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein
9.12.1	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.12.0*	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	Nein	Nein
9.11.1	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein
9.11.0*	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein
9.10.1	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9.10.0*	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**
9.9.1	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9.9.0*	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,8	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,7	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,6	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**

SnapMirror synchron Beziehungen

SnapMirror synchron wird für ONTAP Cloud Instanzen nicht unterstützt.

ONTAP Version…	Ist mit diesen früheren ONTAP Versionen kompatibel…														
	9.19.1	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5
9.19.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.18.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.17.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.16.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein
9.15.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein
9.14.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.13.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.12.1	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.11.1	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein
9.10.1	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.9.1	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9,8	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein
9,7	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9,6	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**
9,5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**

SnapMirror SVM-Beziehungen zur Katastrophenwiederherstellung

- Diese Matrix gilt für die SVM Datenmobilität Migrationsfunktion ab ONTAP 9.10.1.
- Sie können SVM DR verwenden, um eine SVM zu migrieren, die die für "SVM Migration (SVM Datenmobilität)" angegebenen Einschränkungen nicht erfüllt.
- In beiden Fällen dürfen maximal 2 **neuere** Hauptversionen von ONTAP zwischen Quell- und Ziel-Cluster liegen, wobei die Zielversion die gleiche oder eine neuere ONTAP Version als die Quellversion sein muss.

Für SVM-Notfallwiederherstellungsdaten und SVM-Schutz:

Die SVM-Notfallwiederherstellung wird nur zwischen Clustern unterstützt, auf denen dieselbe Version von

ONTAP ausgeführt wird. **Versionsunabhängigkeit wird für die SVM-Replikation nicht unterstützt**.

Für die SVM-Notfallwiederherstellung bei der SVM-Migration:

- Die Replikation wird in eine Richtung unterstützt, von einer früheren Version von ONTAP auf dem Quell-Cluster zur gleichen oder einer späteren Version von ONTAP auf dem Ziel-Cluster.
- Die ONTAP Version auf dem Ziel-Cluster darf höchstens zwei Hauptversionen der lokalen Version oder zwei Hauptversionen der Cloud-Version neuer sein (beginnend mit ONTAP 9.9.0), wie in der folgenden Tabelle gezeigt.
  - Die Replikation wird für Anwendungsfälle des langfristigen Datenschutzes nicht unterstützt.

Das Sternchen (*) nach der Versionsnummer kennzeichnet eine reine Cloud-Version.

Zur Ermittlung der Unterstützung befindet sich die Quellversion in der linken Tabellenspalte, die Zielversion in der obersten Zeile (DR/Migration für gleichartige Versionen und nur Migration für neuere Versionen).

Wenn Sie ONTAP 9.10.1 oder höher verwenden, kann die "SVM Datenmobilität" Funktion anstelle von SVM DR verwendet werden, um SVMs von einem Cluster auf einen anderen zu migrieren.

Quelle	**Ziel**																				
	9,5	9,6	9,7	9,8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1	9.19.1
9,5	DR/Migration nur	nur Migration	nur Migration																				
9,6		DR/Migration nur	nur Migration	nur Migration																			
9,7			DR/Migration nur	nur Migration	nur Migration																		
9,8				DR/Migration nur	Migration	Migration		Migration															

Quelle	Ziel																					
9.9.0*					DR/Migration	Migration	Migration	Migration	Migration	Migration												
9.9.1						DR/Migration	Migration	Migration	Migration	Migration												
9.10.0*							DR/Migration	Migration	Migration	Migration	Migration	Migration										
9.10.1								DR/Migration	Migration	Migration	Migration	Migration										
9.11.0*									DR/Migration	Migration	Migration	Migration	Migration	Migration								
9.11.1										DR/Migration	Migration	Migration	Migration	Migration								
9.12.0*											DR/Migration	Migration	Migration	Migration	Migration	Migration						
9.12.1												DR/Migration	Migration	Migration	Migration	Migration						
9.13.0*													DR/Migration	Migration	Migration	Migration	Migration	Migration				

Quelle	Ziel																				
9.13.1														DR/Migration	Migration	Migration	Migration	Migration					
9.14.0*															DR/Migration	Migration	Migration	Migration	Migration	Migration	Migration			
9.14.1																DR/Migration	Migration	Migration	Migration	Migration	Migration			
9.15.0*																	DR/Migration	Migration	Migration	Migration	Migration	Migration		
9.15.1																		DR/Migration	Migration	Migration	Migration	Migration		
9.16.0																			DR/Migration	Migration	Migration	Migration	Migration	
9.16.1																				DR/Migration	Migration	Migration	Migration	
9.17.1																					DR/Migration	Migration	Migration	Migration
9.18.1																						DR/Migration	Migration	

Quelle	Ziel																				
9.19.1																					DR/Migration

SnapMirror Disaster-Recovery-Beziehungen

Für SnapMirror Beziehungen vom Typ “DP” und Richtlinientyp “async-mirror”:

DP-Typ-Spiegel können ab ONTAP 9.11.1 nicht mehr initialisiert werden und sind in ONTAP 9.12.1 vollständig veraltet. Weitere Informationen finden sich unter "Abschaffung von Datenschutz-SnapMirror-Beziehungen".

In der folgenden Tabelle gibt die Spalte links die ONTAP Version auf dem Quellvolume an, und die oberste Zeile gibt die ONTAP Versionen an, die auf dem Zielvolume vorhanden sein können.

Quelle	Ziel								
	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5	9,4	9,3
9.11.1	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.10.1	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.9.1	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein	Nein
9,8	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein	Nein
9,7	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein	Nein
9,6	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein	Nein
9,5	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein	Nein
9,4	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja	Nein
9,3	Nein	Nein	Nein	Nein	Nein	Nein	Ja	Ja	Ja

Interoperabilität ist nicht bidirektional.

ONTAP SnapMirror Beschränkungen

Es ist wichtig, sich der grundlegenden SnapMirror Einschränkungen bewusst zu sein, bevor eine Datenschutzbeziehung erstellt wird.

- Ein Zielvolume kann nur ein Quellvolume haben.

Ein Quellvolume kann mehrere Zielvolumes haben. Das Zielvolume kann für jede Art von SnapMirror Replikationsbeziehung als Quellvolume dienen.

- Je nach Array-Modell können maximal acht oder sechzehn Zielvolumes von einem einzelnen Quellvolume aus verteilt werden. Siehe "Hardware Universe" für Details zu Ihrer spezifischen Konfiguration.
- Dateien können nicht am Zielort einer SnapMirror DR-Beziehung wiederhergestellt werden.
- Quell- oder Ziel-SnapVault Volumes dürfen nicht 32-Bit sein.
- Das Quell-Volume für eine SnapVault Beziehung sollte kein FlexClone Volume sein.

> Die Beziehung wird funktionieren, aber die durch FlexClone Volumes gebotene Effizienz wird nicht erhalten bleiben.

Konfiguration der SnapMirror Volume-Replikation

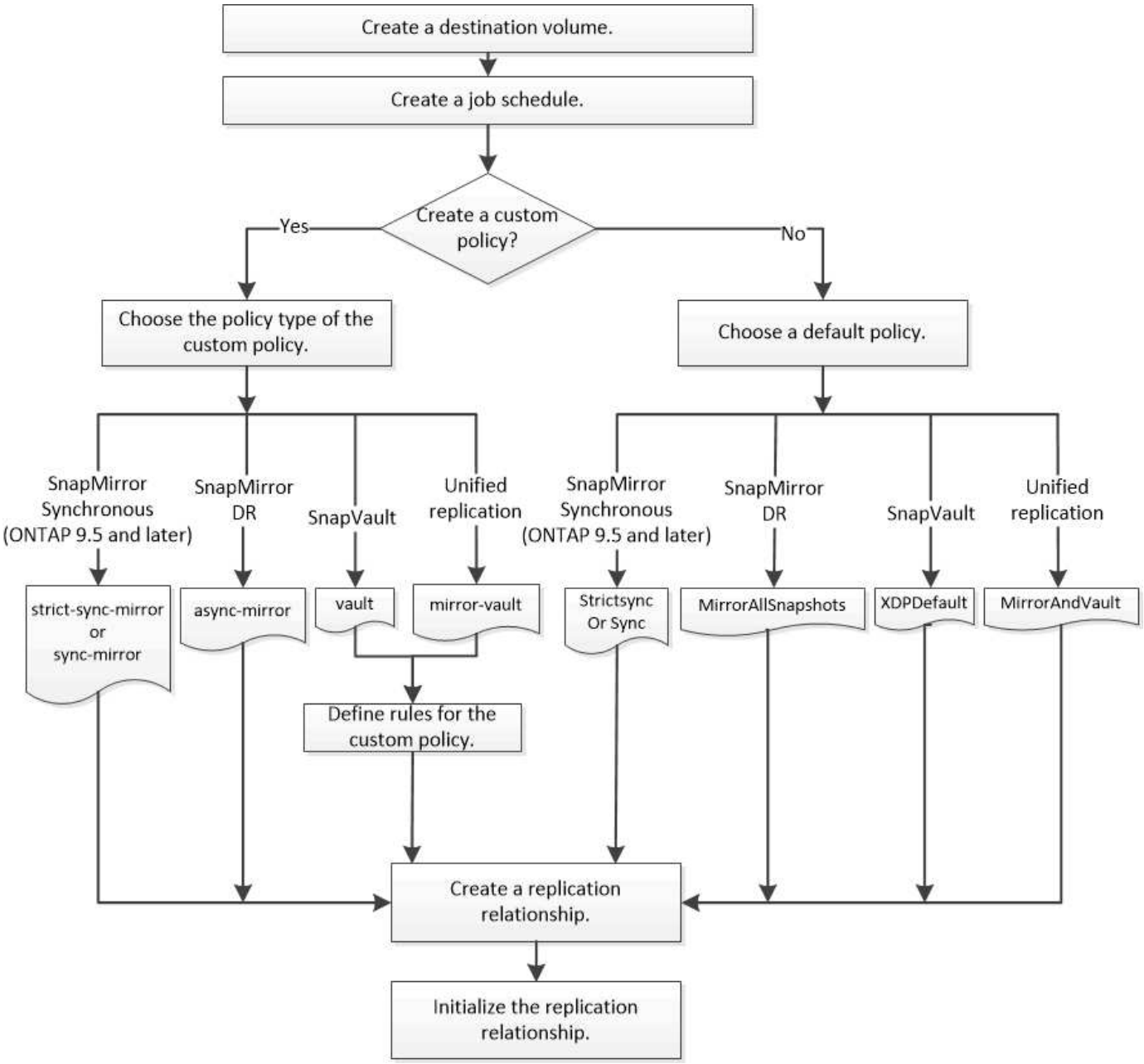
ONTAP SnapMirror Replikationsworkflow

SnapMirror bietet drei Arten von Datenschutzbeziehungen: SnapMirror DR, Archiv (früher bekannt als SnapVault), und einheitliche Replizierung. Für jede Art der Beziehung kann derselbe grundlegende Arbeitsablauf verwendet werden.

Ab der allgemeinen Verfügbarkeit in ONTAP 9.9.1 "SnapMirror Active Sync" bietet Zero Recovery Time Objective (Zero RTO) oder Transparent Application Failover (TAF) die Möglichkeit, ein automatisches Failover geschäftskritischer Anwendungen in SAN-Umgebungen zu ermöglichen.

Für jede Art von SnapMirror Datensicherungsbeziehung ist der Arbeitsablauf derselbe: Zielvolume erstellen, Jobzeitplan erstellen, Richtlinie festlegen, Beziehung erstellen und initialisieren.

Ab ONTAP 9.3 kann mit dem `snapmirror protect` Befehl eine Datensicherungsbeziehung in einem einzigen Schritt konfiguriert werden. Auch wenn `snapmirror protect` verwendet wird, ist das Verständnis jedes einzelnen Schritts im Arbeitsablauf erforderlich.



Verwandte Informationen

- "snapmirror protect"

Konfiguration einer ONTAP SnapMirror Replikationsbeziehung in einem Schritt

Sie können den `snapmirror protect` Befehl verwenden, um eine Datensicherungsbeziehung in einem einzigen Schritt zu konfigurieren. Sie geben eine Liste der zu replizierenden Volumes, eine SVM im Ziel-Cluster, einen Jobzeitplan und eine SnapMirror Richtlinie an. `snapmirror protect` übernimmt den Rest.

Bevor Sie beginnen

- Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

  "Cluster- und SVM-Peering"

- Die Sprache auf dem Ziel-Volume muss mit der Sprache auf dem Quell-Volume übereinstimmen.
- Ab ONTAP 9.20.1 können Sie die Backend-SnapMirror asynchrone Replizierung über bestehende FC-Fabrics konfigurieren. Dafür muss das Backend Ihres ONTAP Systems für die FC-Replizierung konfiguriert sein, und sowohl die FC-Fabric als auch das Intercluster-IP-Netzwerk müssen betriebsbereit sein. Replizierungsdaten können über die FC-Fabric übertragen werden, das Intercluster-IP-Netzwerk ist jedoch für die Clusterkommunikation und die Funktionen zur Replizierungsverwaltung erforderlich. Direkt angeschlossene FC-Konfigurationen werden für die Backend-FC-Replizierung nicht unterstützt. "Informationen zur Konfiguration des Backends Ihres ONTAP Systems für die FC-Replikation"
  - Wenn Sie eine asynchrone SnapMirror Beziehung für die Verwendung von FC als Transportprotokoll konfigurieren, muss in einer MetroCluster Konfiguration der für das MetroCluster verwendete Storage-Initiator von dem für die Replizierung über FC verwendeten Initiator getrennt sein. Die gemeinsame Nutzung des Initiator-Storage zwischen den beiden wird nicht unterstützt.

Über diese Aufgabe

Der `snapmirror protect` Befehl wählt ein Aggregat aus, das der angegebenen SVM zugeordnet ist. Wenn kein Aggregat der SVM zugeordnet ist, erfolgt die Auswahl aus allen Aggregaten im Cluster. Die Auswahl des Aggregats basiert auf dem verfügbaren Speicherplatz und der Anzahl der Volumes auf dem Aggregat.

Der `snapmirror protect` Befehl führt dann die folgenden Schritte aus:

- Erstellt ein Zielvolume mit dem passenden Typ und der passenden Menge an reserviertem Speicherplatz für jedes Volume in der Liste der zu replizierenden Volumes.

  Der Name des Zielvolumens hat die Form *`source_volume_name_dst`*. Bei einem Konflikt mit einem bestehenden Namen fügt der Befehl dem Volumennamen eine Zahl hinzu. Ein Präfix und/oder Suffix kann in den Befehlsoptionen angegeben werden. Das Suffix ersetzt das vom System bereitgestellte `dst` Suffix.

  Ein Zielvolume kann bis zu 1019 Snapshots enthalten.

- Konfiguriert eine Replikationsbeziehung, die für die von Ihnen angegebene Richtlinie geeignet ist.
- Initialisiert die Beziehung.

> Die Initialisierung kann zeitaufwändig sein. `snapmirror protect` wartet nicht darauf, dass die Initialisierung abgeschlossen ist, bevor der Job beendet wird. Aus diesem Grund empfiehlt sich die Verwendung des `snapmirror show` Befehls anstelle des `job show` Befehls, um festzustellen, wann die Initialisierung abgeschlossen ist.

- Ab ONTAP 9.20.1 erfolgt die Replizierung über Ihr FC-Fabric beim Erstellen Ihrer SnapMirror Beziehung mit einer unterstützten asynchronen Datensicherungsstrategie und der `-transport fc` Option. Die Backend-Replizierung verwendet standardmäßig das IP-Protokoll. "Welche standardmäßigen asynchronen Datenschutzrichtlinien die Backend FC Replikation unterstützt".

> Um das ausgewählte Transportprotokoll nach dem Erstellen einer SnapMirror Replikationsbeziehung zu ändern, müssen Sie die Beziehung löschen und neu erstellen.

Schritt

1. Eine Replikationsbeziehung in einem Schritt erstellen und initialisieren:

   Vor dem Ausführen dieses Befehls sind die Variablen in spitzen Klammern durch die erforderlichen Werte zu ersetzen.

```
snapmirror protect -path-list <SVM:volume> -destination-vserver
<destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
<true|false> -destination-volume-prefix <prefix> -destination-volume
-suffix <suffix>
```

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden. Die `-auto-initialize`Option ist standardmäßig auf “true” gesetzt.

Das folgende Beispiel erstellt und initialisiert eine SnapMirror DR-Beziehung unter Verwendung der `MirrorAllSnapshots`Standardrichtlinie und des FC-Transportprotokolls:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily -transport fc
```

Es kann auch eine benutzerdefinierte Richtlinie verwendet werden. Weitere Informationen finden sich unter "Erstellen einer benutzerdefinierten Replikationsrichtlinie".

Das folgende Beispiel erstellt und initialisiert eine SnapVault Beziehung mit der Standard `XDPDefault`Datensicherungsstrategie:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

Das folgende Beispiel erstellt und initialisiert eine einheitliche Replikationsbeziehung mithilfe der Standard `MirrorAndVault`richtlinie:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

Das folgende Beispiel erstellt und initialisiert eine SnapMirror synchron Beziehung mit der Standard `Sync`richtlinie:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

Für SnapVault und einheitliche Replikationsrichtlinien kann es hilfreich sein, einen Zeitplan für die Erstellung einer Kopie des zuletzt übertragenen Snapshots auf dem Ziel zu definieren. Weitere Informationen finden sich unter "Festlegen eines Zeitplans für die Erstellung einer lokalen Kopie auf dem Ziel".

Nachdem Sie fertig sind

Mit dem `snapmirror show`Befehl lässt sich überprüfen, ob die SnapMirror Beziehung erstellt wurde.

Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Job anzeigen"

Eine Replikationsbeziehung Schritt für Schritt konfigurieren

Ein ONTAP SnapMirror Zielvolume erstellen

Der `volume create`-Befehl kann auf dem Zielsystem verwendet werden, um ein Zielvolume zu erstellen. Das Zielvolume sollte genauso groß oder größer als das Quellvolume sein. Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Zielvolume erstellen:

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

   Das folgende Beispiel erstellt ein 2-GB-Zielvolume mit dem Namen `volA_dst`:

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

Erstellung eines ONTAP SnapMirror Replikationsauftragszeitplans

Der Jobplan legt fest, wann SnapMirror die Datensicherungsbeziehung, der der Plan zugewiesen ist, automatisch aktualisiert. Es besteht die Möglichkeit, den System Manager oder den `job schedule cron create` Befehl zu verwenden, um einen Replikationsjobplan zu erstellen. Weitere Informationen zu `job schedule cron create` finden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Sie weisen einen Jobplan zu, wenn Sie eine Datenschutzbeziehung erstellen. Wenn Sie keinen Jobplan zuweisen, muss die Beziehung manuell aktualisiert werden.

Schritte

Ein Replikationsauftragsplan kann mit System Manager oder der ONTAP CLI erstellt werden.

System Manager

1. Zu **Schutz > Übersicht** navigieren und **Lokale Richtlinieneinstellungen** erweitern.
2. Im Bereich **Zeitpläne** auf → klicken.

3. Im Fenster **Zeitpläne** auf + Add klicken.
4. Im Fenster **Zeitplan hinzufügen** den Namen des Zeitplans eingeben sowie den Kontext und den Zeitplantyp auswählen.
5. Auf **Speichern** klicken.

CLI

1. Einen Arbeitszeitplan erstellen:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Für `-month`, `-dayofweek` und `-hour` kann `all` angegeben werden, damit der Job jeden Monat, an jedem Wochentag bzw. zu jeder Stunde ausgeführt wird.

Ab ONTAP 9.10.1 kann der Vserver in den Jobplan einbezogen werden:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

Der minimal unterstützte Zeitplan (RPO) für FlexVol Volumes in einer Volume SnapMirror Beziehung beträgt 5 Minuten. Der minimal unterstützte Zeitplan (RPO) für FlexGroup Volumes in einer Volume SnapMirror Beziehung beträgt 30 Minuten.

Das folgende Beispiel erstellt einen Jobplan mit dem Namen `my_weekly`, der samstags um 3:00 Uhr morgens ausgeführt wird:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Erstellen einer benutzerdefinierten ONTAP SnapMirror Replikationsrichtlinie

Sie können eine benutzerdefinierte Replikationsrichtlinie erstellen, wenn die Standardrichtlinie für eine Beziehung nicht geeignet ist. Beispielsweise kann es sinnvoll sein, Daten bei einer Netzwerkübertragung zu komprimieren oder die Anzahl der Versuche zu ändern, die SnapMirror zum Übertragen von Snapshots unternimmt.

Es kann beim Erstellen einer Replikationsbeziehung eine Standard- oder eine benutzerdefinierte Richtlinie verwendet werden. Für eine benutzerdefinierte Archivierungsrichtlinie (früher SnapVault) oder eine einheitliche Replikationsrichtlinie ist es erforderlich, eine oder mehrere *Regeln* zu definieren, die festlegen, welche Snapshots während der Initialisierung und Aktualisierung übertragen werden. Es kann außerdem ein Zeitplan für die Erstellung lokaler Snapshots auf dem Ziel-Cluster definiert werden.

Der *Richtlinientyp* der Replikationsrichtlinie bestimmt die Art der Beziehung, die sie unterstützt. Die folgende Tabelle zeigt die verfügbaren Richtlinientypen.

Richtlinientyp	Beziehungstyp
async-mirror	SnapMirror DR
Vault	SnapVault
mirror-vault	Einheitliche Replikation
strict-sync-mirror	SnapMirror synchron im StrictSync Modus (unterstützt ab ONTAP 9.5)
Sync Mirror	SnapMirror synchron im Sync Modus (unterstützt ab ONTAP 9.5)

Wenn Sie eine benutzerdefinierte Replikationsrichtlinie erstellen, ist es ratsam, die Richtlinie an einer Standardrichtlinie zu orientieren.

Schritte

Sie können benutzerdefinierte Datenschutzrichtlinien mit System Manager oder der ONTAP CLI erstellen. Ab ONTAP 9.11.1 ist es möglich, mit System Manager benutzerdefinierte Mirror- und Vault-Richtlinien zu erstellen sowie ältere Richtlinien anzuzeigen und auszuwählen. Diese Funktion ist auch in ONTAP 9.8P12 und späteren Patches von ONTAP 9.8 verfügbar.

Benutzerdefinierte Schutzrichtlinien sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster erstellen.

System Manager

1. Klicken Sie auf **Schutz > Übersicht > Lokale Richtlinieneinstellungen**.
2. Unter **Schutzrichtlinien** auf → klicken.
3. Im Bereich **Schutzrichtlinien** auf + Add klicken.
4. Geben Sie den Namen der neuen Richtlinie ein und wählen Sie den Geltungsbereich der Richtlinie aus.
5. Wählen Sie einen Richtlinientyp aus. Zum Hinzufügen einer reinen Vault- oder Mirror-Richtlinie **Asynchron** auswählen und auf **Legacy-Richtlinientyp verwenden** klicken.
6. Die Pflichtfelder ausfüllen.
7. Auf **Speichern** klicken.
8. Diese Schritte sind auf dem anderen Cluster zu wiederholen.

CLI

1. Erstellen einer benutzerdefinierten Replikationsrichtlinie:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

Ab ONTAP 9.5 kann der Zeitplan für die Erstellung eines gemeinsamen Snapshot-Zeitplans für SnapMirror synchron Beziehungen mithilfe des `-common-snapshot-schedule` Parameters festgelegt werden. Standardmäßig beträgt der gemeinsame Snapshot-Zeitplan für SnapMirror synchron Beziehungen eine Stunde. Für den Snapshot-Zeitplan für SnapMirror synchron

Beziehungen kann ein Wert zwischen 30 Minuten und zwei Stunden angegeben werden.

Das folgende Beispiel erstellt eine benutzerdefinierte Replikationsrichtlinie für SnapMirror DR, die die Netzwerkkomprimierung für Datenübertragungen aktiviert:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

Das folgende Beispiel erstellt eine benutzerdefinierte Replikationsrichtlinie für SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

Das folgende Beispiel erstellt eine benutzerdefinierte Replikationsrichtlinie für die einheitliche Replikation:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

Das folgende Beispiel erstellt eine benutzerdefinierte Replikationsrichtlinie für eine SnapMirror synchron Beziehung im StrictSync Modus:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Weitere Informationen zu `snapmirror policy create` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Für die Richtlinientypen “vault” und “mirror-vault” sind Regeln zu definieren, die festlegen, welche Snapshots während der Initialisierung und Aktualisierung übertragen werden.

Mit dem `snapmirror policy show` Befehl lässt sich überprüfen, ob die SnapMirror Richtlinie erstellt wurde.

Weitere Informationen zu `snapmirror policy show` finden sich in der "ONTAP-Befehlsreferenz".

Eine Regel für eine ONTAP SnapMirror Richtlinie definieren

Für benutzerdefinierte Richtlinien mit dem `vault` oder `mirror-vault` Richtlinientyp muss mindestens eine Regel definiert werden, die festlegt, welche Snapshots während der Initialisierung und Aktualisierung übertragen werden. Es können auch Regeln für

Standardrichtlinien mit dem `vault` oder `mirror-vault` Richtlinientyp definiert werden.

Über diese Aufgabe

Jede Richtlinie mit dem `vault` oder `mirror-vault`-Richtlinientyp muss eine Regel enthalten, die angibt, welche Snapshots repliziert werden. Die Regel `bi-monthly` gibt beispielsweise an, dass nur Snapshots mit dem SnapMirror-Label `bi-monthly` repliziert werden. Das SnapMirror-Label wird bei der Konfiguration der Snapshot-Richtlinie auf der Quelle angegeben.

Jedem Richtlinientyp sind eine oder mehrere systemdefinierte Regeln zugeordnet. Diese Regeln werden einer Richtlinie automatisch zugewiesen, wenn deren Richtlinientyp angegeben wird. Die folgende Tabelle zeigt die systemdefinierten Regeln.

Systemdefinierte Regel	Wird in Richtlinientypen verwendet	Ergebnis
sm_created	async-mirror, mirror-vault, Sync, StrictSync	Ein von SnapMirror erstellter Snapshot wird bei der Initialisierung und Aktualisierung übertragen.
all_source_snapshots	async-mirror	Neue Snapshots auf der Quelle werden bei Initialisierung und Aktualisierung übertragen.
täglich	Vault, Mirror-Vault	Neue Snapshots auf dem Quell-Cluster mit dem SnapMirror-Label `daily` werden bei Initialisierung und Aktualisierung übertragen.
wöchentlich	Vault, Mirror-Vault	Neue Snapshots auf dem Quell-Cluster mit dem SnapMirror-Label `weekly` werden bei Initialisierung und Aktualisierung übertragen.
monatlich	mirror-vault	Neue Snapshots auf dem Quell-Cluster mit dem SnapMirror-Label `monthly` werden bei Initialisierung und Aktualisierung übertragen.
app_consistent	Sync, StrictSync	Snapshots mit dem SnapMirror-Label `app_consistent` auf der Quelle werden synchron zum Ziel repliziert. Unterstützt ab ONTAP 9.7.

Mit Ausnahme des Richtlinientyps „`async-mirror`“ lassen sich bei Bedarf zusätzliche Regeln für Standard- oder benutzerdefinierte Richtlinien angeben. Beispiel:

- Für die `MirrorAndVault`Standardrichtlinie könnte eine Regel mit dem Namen `bi-monthly` erstellt werden, um Snapshots auf dem Quell-System mit dem `bi-monthly` SnapMirror Label abzugleichen.
- Für eine benutzerdefinierte Richtlinie mit dem `mirror-vault` Richtlinientyp könnte eine Regel mit dem Namen `bi-weekly` erstellt werden, um Snapshots auf dem Quell-Cluster mit dem `bi-weekly` SnapMirror Label abzugleichen.

Schritt

1. Eine Regel für eine Richtlinie definieren:

`snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror -label snapmirror-label -keep retention_count`

Das folgende Beispiel fügt eine Regel mit der Bezeichnung SnapMirror `bi-monthly` zur Standard `MirrorAndVault`richtlinie hinzu:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

Das folgende Beispiel fügt eine Regel mit der Bezeichnung SnapMirror `bi-weekly` zur benutzerdefinierten `my_snapvault` Richtlinie hinzu:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

Das folgende Beispiel fügt eine Regel mit der Bezeichnung SnapMirror `app_consistent` zur benutzerdefinierten `Sync` Richtlinie hinzu:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Weitere Informationen zu `snapmirror policy add-rule` finden sich in der "ONTAP-Befehlsreferenz".

Anschließend können Snapshots aus dem Quell-Cluster repliziert werden, die diesem SnapMirror-Label entsprechen:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Erstellung eines lokalen Kopierplans für ein ONTAP SnapMirror Ziel

Für SnapVault und einheitliche Replikationsbeziehungen besteht Schutz vor der Möglichkeit, dass ein aktualisierter Snapshot beschädigt ist, indem eine Kopie des zuletzt übertragenen Snapshots auf dem Ziel erstellt wird. Diese „lokale Kopie“ bleibt unabhängig von den Aufbewahrungsregeln auf dem Quell-Cluster erhalten, sodass selbst wenn der ursprünglich von SnapMirror übertragene Snapshot auf dem Quell-Cluster nicht mehr verfügbar ist, eine Kopie davon auf dem Ziel vorhanden ist.

Über diese Aufgabe

Den Zeitplan für die Erstellung einer lokalen Kopie geben Sie in der `-schedule` Option des `snapmirror policy add-rule` Befehls an.

Schritt

1. Ein Zeitplan für die Erstellung einer lokalen Kopie auf dem Zielsystem wird definiert:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -schedule schedule
```

Ein Beispiel für die Erstellung eines Arbeitsplans ist unter "Erstellen eines Replikationsjob-Zeitplans" zu finden.

Das folgende Beispiel fügt der Standard `MirrorAndVault`richtlinie einen Zeitplan für die Erstellung einer lokalen Kopie hinzu:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

Das folgende Beispiel fügt der benutzerdefinierten `my_unified` Policy einen Zeitplan für die Erstellung einer lokalen Kopie hinzu:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

Weitere Informationen zu `snapmirror policy add-rule` finden sich in der "ONTAP-Befehlsreferenz".

Erstellung einer ONTAP SnapMirror Replikationsbeziehung

Die Beziehung zwischen dem Quell-Volume im Primärspeicher und dem Ziel-Volume im Sekundärspeicher wird als *Datensicherungsbeziehung* bezeichnet. Mit dem `snapmirror create` Befehl lassen sich SnapMirror DR-, SnapVault- oder Unified Replication Datensicherungsbeziehungen erstellen.

Über diese Aufgabe

- Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu folgen, um eine Replikationsbeziehung zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.
- Ab ONTAP 9.20.1 kann die Backend-SnapMirror asynchrone Replizierung so konfiguriert werden, dass entweder IP- oder FC-Transport verwendet wird. Standardmäßig verwendet die Backend-Replikation das IP-Netzwerk. Für die Replizierung über Ihr FC-Fabric werden beim Erstellen Ihrer SnapMirror Beziehung eine unterstützte asynchrone Datensicherungsstrategie und die `-transport fc` Option verwendet. "Welche standardmäßigen asynchronen Datenschutzrichtlinien die Backend FC Replikation unterstützt".
  - Um das ausgewählte Transportprotokoll nach dem Erstellen einer SnapMirror Replikationsbeziehung zu ändern, müssen Sie die Beziehung löschen und neu erstellen.
  - Direkt angeschlossene FC-Konfigurationen werden für die Backend FC-Replikation nicht unterstützt.
- Ab ONTAP 9.11.1 kann im System Manager die Auswahl von vordefinierten und benutzerdefinierten Mirror- und Vault-Richtlinien erfolgen, die Anzeige und Auswahl von älteren Richtlinien sowie das Überschreiben der in einer Datensicherungsstrategie definierten Übertragungszeitpläne beim Schutz von Volumes und Storage-VMs. Diese Funktion ist auch in ONTAP 9.8P12 und späteren Patches von ONTAP 9.8 verfügbar.

> Wenn Sie ONTAP 9.8P12 oder eine spätere ONTAP 9.8 Patch-Version verwenden und SnapMirror mit System Manager konfiguriert haben, sollten Sie ONTAP 9.9.1P13 oder eine

spätere sowie ONTAP 9.10.1P10 oder eine spätere Patch-Version verwenden, falls ein Upgrade auf ONTAP 9.9.1 oder ONTAP 9.10.1 Releases vorgesehen ist.

Bevor Sie beginnen

- In ONTAP 9.20.1 und späteren Versionen gilt: Wenn Sie eine SnapMirror asynchrone Beziehung für die Verwendung von FC als Transportprotokoll konfigurieren:
  - Ihr ONTAP System-Backend muss für die FC-Replikation konfiguriert sein, und sowohl das FC Fabric als auch das Intercluster-IP-Netzwerk müssen betriebsbereit sein. Replikationsdaten können über das FC Fabric übertragen werden, das Intercluster-IP-Netzwerk ist jedoch für die Clusterkommunikation und die Replikationsverwaltungsfunktionen erforderlich. "Informationen zur Konfiguration des Backends Ihres ONTAP Systems für die FC-Replikation".
  - In einer MetroCluster Konfiguration muss der für MetroCluster verwendete Storage-Initiator von dem für die Replizierung über FC verwendeten Initiator getrennt sein. Die gemeinsame Nutzung von Initiator-Storage zwischen beiden wird nicht unterstützt.
- Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

  "Cluster- und SVM-Peering"

- Die Sprache auf dem Ziel-Volume muss mit der Sprache auf dem Quell-Volume übereinstimmen.

Über diese Aufgabe

Bis ONTAP 9.3 verwendeten SnapMirror im DP-Modus und SnapMirror im XDP-Modus unterschiedliche Replikations-Engines mit unterschiedlichen Ansätzen zur Versionsabhängigkeit:

- SnapMirror im DP-Modus verwendete eine versionsabhängige Replikations-Engine, bei der die ONTAP Version auf dem primären und sekundären Speicher identisch sein musste:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror im XDP-Modus verwendete eine versionsflexible Replikations-Engine, die unterschiedliche ONTAP Versionen auf primärem und sekundärem Speicher unterstützte:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Mit Leistungsverbesserungen überwiegen die signifikanten Vorteile des versionsflexiblen SnapMirror den leichten Vorteil im Replikationsdurchsatz, der mit dem versionsabhängigen Modus erzielt wird. Aus diesem Grund ist ab ONTAP 9.3 der XDP Modus der neue Standard, und alle Aufrufe des DP Modus in der Befehlszeile oder in neuen oder bestehenden Skripten werden automatisch in den XDP Modus umgewandelt.

Bestehende Beziehungen bleiben unberührt. Wenn eine Beziehung bereits vom Typ DP ist, bleibt sie vom Typ DP. Die folgende Tabelle zeigt das zu erwartende Verhalten.

Wenn Sie angeben…	Der Typ ist…	Die Standardrichtlinie (wenn Sie keine Richtlinie angeben) ist…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)

Nichts	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	XDPDefault (SnapVault)

Siehe auch die Beispiele im nachfolgenden Verfahren.

Die einzigen Ausnahmen von der Umwandlung sind wie folgt:

- SVM-Datensicherungsbeziehungen bleiben weiterhin standardmäßig im DP-Modus.

  XDP muss explizit angegeben werden, um den XDP-Modus mit der Standard `MirrorAllSnapshots`Richtlinie zu erhalten.

- Lastverteilende Datenschutzbeziehungen verwenden weiterhin standardmäßig den DP-Modus.
- SnapLock Datenschutzbeziehungen verbleiben weiterhin standardmäßig im DP-Modus.
- Explizite Aufrufe von DP verwenden weiterhin standardmäßig den DP-Modus, wenn die folgende clusterweite Option festgelegt ist:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Diese Option wird ignoriert, wenn DP nicht explizit aufgerufen wird.

Ab ONTAP 9.14.1 wird die `-backoff-level` Option zu den `snapmirror create`, `snapmirror modify` und `snapmirror restore` Befehlen hinzugefügt, sodass das Backoff-Level pro Beziehung angegeben werden kann. Die Option wird nur bei FlexVol SnapMirror Beziehungen unterstützt. Der optionale Befehl legt das SnapMirror Backoff-Level aufgrund von Client-Operationen fest. Backoff-Werte können hoch, mittel oder keine sein. Der Standardwert ist hoch.

Ab ONTAP 9.5 werden SnapMirror synchron Beziehungen unterstützt.

In ONTAP 9.4 und höher kann ein Zielvolume bis zu 1019 Snapshots enthalten. In ONTAP 9.3 und früher kann ein Zielvolume bis zu 251 Snapshots enthalten.

Schritte

Mit dem System Manager oder der ONTAP CLI lässt sich eine Replikationsbeziehung erstellen.

System Manager

1. Das zu schützende Volume oder die LUN auswählen: **Speicher > Volumes** oder **Speicher > LUNs** auswählen und dann auf den gewünschten Volume- oder LUN-Namen klicken.
2. Klicken Sie Protect.
3. Den Ziel-Cluster und die Storage-VM auswählen.
4. Die asynchron Datensicherungsstrategie ist standardmäßig ausgewählt. Eine synchron Datensicherungsstrategie kann über **Weitere Optionen** ausgewählt werden.
5. Auf **Schützen** klicken.
6. Klicken Sie auf die Registerkarte **SnapMirror (Lokal oder Remote)** für das ausgewählte Volume oder die LUN, um zu überprüfen, ob der Schutz korrekt eingerichtet ist.

CLI

1. Vom Ziel-Cluster aus eine Replikationsbeziehung erstellen:

   Vor dem Ausführen dieses Befehls sind die Variablen in spitzen Klammern durch die erforderlichen Werte zu ersetzen.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   Der `schedule`Parameter ist bei der Erstellung SnapMirror synchroner Beziehungen nicht anwendbar.

   Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung unter Verwendung der Standard `MirrorLatest`richtlinie:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   Das folgende Beispiel erstellt eine SnapVault Beziehung mit der Standard `XDPDefault`richtlinie:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   Das folgende Beispiel erstellt eine einheitliche Replikationsbeziehung unter Verwendung der standardmäßigen `MirrorAndVault` asynchronen Richtlinie und des `fc` Transportprotokolls:

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorAndVault -transport fc
   ```

   Das folgende Beispiel erstellt eine einheitliche Replikationsbeziehung mithilfe der benutzerdefinierten `my_unified` Richtlinie:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   my_unified
   ```

   Das folgende Beispiel erstellt eine SnapMirror synchron Beziehung mit der Standard `Sync`richtlinie:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   ```

```
-path svm_backup:volA_dst -type XDP -policy Sync
```

Das folgende Beispiel erstellt eine SnapMirror synchron Beziehung mit der Standard `StrictSync`richtlinie:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung. Mit der automatischen Konvertierung des DP-Typs in XDP und ohne Angabe einer Richtlinie wird standardmäßig die `MirrorAllSnapshots` Richtlinie verwendet:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung. Wenn kein Typ oder keine Richtlinie angegeben ist, wird standardmäßig die `MirrorAllSnapshots` Richtlinie verwendet:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung. Wenn keine Richtlinie angegeben ist, wird die Richtlinie standardmäßig auf die `XDPDefault` Richtlinie gesetzt:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

Das folgende Beispiel erstellt eine SnapMirror synchron Beziehung mit der vordefinierten Richtlinie `SnapCenterSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

Die vordefinierte Richtlinie `SnapCenterSync` ist vom Typ `Sync`. Diese Richtlinie repliziert jeden Snapshot, der mit dem `snapmirror-label` Parameter "app_consistent" erstellt wurde.

Nachdem Sie fertig sind

Mit dem `snapmirror show`Befehl lässt sich überprüfen, ob die SnapMirror Beziehung erstellt wurde.

Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "SnapMirror Failover-Testvolumes erstellen und löschen".

Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgaben mit… auszuführen	Diesen Inhalt ansehen…
System Manager Classic (verfügbar mit ONTAP 9.7 und früher)	"Volume-Sicherung mit SnapVault Übersicht"

Verwandte Informationen

- "snapmirror create"

Initialisierung einer ONTAP SnapMirror Replikationsbeziehung

Bei allen Beziehungstypen führt die Initialisierung eine Basisübertragung durch: Dabei wird ein Snapshot des Quell-Volumes erstellt und anschließend diese Kopie zusammen mit allen darin referenzierten Datenblöcken auf das Ziel-Volume übertragen. Andernfalls hängt der Inhalt der Übertragung von der Richtlinie ab.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

"Cluster- und SVM-Peering"

Über diese Aufgabe

Die Initialisierung kann zeitaufwändig sein. Es empfiehlt sich, den Basistransfer außerhalb der Spitzenzeiten durchzuführen.

Ab ONTAP 9.5 werden SnapMirror synchron Beziehungen unterstützt.

Es ist zu beachten, dass die Initialisierung nicht automatisch fortgesetzt wird, wenn ein Dateisystem aus irgendeinem Grund, wie etwa einem Neustart des Knotens, einer Übernahme/Rückgabe oder einem Systemabsturz, neu gestartet wird. In diesem Fall muss die Initialisierung manuell neu gestartet werden.

Schritt

1. Eine Replikationsbeziehung initialisieren:

   ```
   snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

   Das folgende Beispiel initialisiert die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

Sie können den `snapmirror snapshot-owner create` Befehl verwenden, um einen gekennzeichneten Snapshot auf dem sekundären System in einer Mirror-Vault-Bereitstellung zu erhalten. Dadurch wird sichergestellt, dass ein gemeinsamer Snapshot für die Aktualisierung der Vault-Beziehung vorhanden ist.

Über diese Aufgabe

Bei Verwendung einer kombinierten Mirror-Vault-Fan-Out- oder Kaskadenbereitstellung ist zu beachten, dass Aktualisierungen fehlschlagen, wenn auf den Quell- und Ziel-Volumes kein gemeinsamer Snapshot vorhanden ist.

Dies stellt bei der Spiegelbeziehung in einer Mirror-Vault-Fan-Out- oder Kaskadenbereitstellung niemals ein Problem dar, da SnapMirror immer einen Snapshot des Quellvolumes erstellt, bevor die Aktualisierung durchgeführt wird.

Dies könnte jedoch ein Problem für die Vault-Beziehung darstellen, da SnapMirror beim Aktualisieren einer Vault-Beziehung keinen Snapshot des Quell-Volumes erstellt. Es ist erforderlich, das `snapmirror snapshot-owner create` zu verwenden, um sicherzustellen, dass mindestens ein gemeinsamer Snapshot sowohl auf dem Quell- als auch auf dem Ziel-Volume der Vault-Beziehung vorhanden ist. "Weitere Informationen zu Fan-out- und Kaskadierungsbereitstellungen für den Datenschutz".

Schritte

1. Weisen Sie auf dem Quell-Volume dem gekennzeichneten Snapshot, den Sie beibehalten möchten, einen Besitzer zu:

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   Im folgenden Beispiel wird `ApplicationA` als Eigentümer des `snap1` Snapshots zugewiesen:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   Weitere Informationen zu `snapmirror snapshot-owner create` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Spiegelbeziehung wird aktualisiert, wie in "Manuelles Aktualisieren einer Replikationsbeziehung" beschrieben.

   Alternativ ist es möglich, auf die planmäßige Aktualisierung der Spiegelbeziehung zu warten.

3. Den beschrifteten Snapshot an das Tresorziel übertragen:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot
   ```

   Das folgende Beispiel überträgt den `snap1` Snapshot

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   ```

```
-source-snapshot snap1
```

Der gekennzeichnete Snapshot bleibt erhalten, wenn die Vault-Beziehung aktualisiert wird.

Weitere Informationen zu `snapmirror update` finden sich in der "ONTAP-Befehlsreferenz".

4. Auf dem Quellvolume den Besitzer aus dem gekennzeichneten Snapshot entfernen:

`snapmirror snapshot-owner delete -vserver` *SVM* `-volume` *volume* `-snapshot` *snapshot* `-owner` *owner*

Die folgenden Beispiele entfernen `ApplicationA` als Eigentümer des `snap1` Snapshots:

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

Weitere Informationen zu `snapmirror snapshot-owner delete` finden sich in der "ONTAP-Befehlsreferenz".

Konfiguration einer ONTAP SnapMirror Vault-Vault-Kaskade

Anhand eines Beispiels wird konkret veranschaulicht, wie Replikationsbeziehungen Schritt für Schritt konfiguriert werden können. Mithilfe der im Beispiel konfigurierten vault-vault Kaskadenbereitstellung können mehr als 251 Snapshots mit der Bezeichnung `my-weekly` aufbewahrt werden.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

Über diese Aufgabe

Das Beispiel setzt Folgendes voraus:

- Snapshots wurden auf dem Quell-Cluster mit den SnapMirror Labels `my-daily`, `my-weekly` und `my-monthly` konfiguriert.
- Sie haben Ziel-Volumes mit dem Namen `volA` auf den sekundären und tertiären Ziel-Clustern konfiguriert.
- Sie haben Replikationsjob-Zeitpläne mit dem Namen `my_snapvault` auf den sekundären und tertiären Ziel-Cluster konfiguriert.

Das Beispiel zeigt, wie Replikationsbeziehungen auf Basis zweier benutzerdefinierter Richtlinien erstellt werden:

- Die `snapvault_secondary`Richtlinie speichert 7 tägliche, 52 wöchentliche und 180 monatliche Snapshots auf dem sekundären Ziel-Cluster.
- Der `snapvault_tertiary policy` speichert 250 wöchentliche Snapshots auf dem tertiären Ziel-Cluster.

Schritte

1. Erstellen Sie auf dem sekundären Ziel-Cluster die `snapvault_secondary`Richtlinie:

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver
svm_secondary
```

2. Definieren Sie auf dem sekundären Ziel-Cluster die `my-daily`Regel für die Richtlinie:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. Definieren Sie auf dem sekundären Ziel-Cluster die `my-weekly`Regel für die Richtlinie:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. Definieren Sie auf dem sekundären Ziel-Cluster die `my-monthly`Regel für die Richtlinie:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. Auf dem sekundären Ziel-Cluster die Richtlinie überprüfen:

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily               7  false       0 -
-
                              my-weekly             52  false       0 -
-
                              my-monthly           180  false       0 -
-
```

6. Auf dem sekundären Ziel-Cluster die Beziehung zum Quell-Cluster erstellen:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. Auf dem sekundären Ziel-Cluster die Beziehung zum Quell-Cluster initialisieren:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. Auf dem tertiären Ziel-Cluster die `snapvault_tertiary`Richtlinie erstellen:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. Definieren Sie auf dem tertiären Ziel-Cluster die `my-weekly`Regel für die Richtlinie:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. Auf dem tertiären Ziel-Cluster die Richtlinie überprüfen:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                    Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
            Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. Erstellen Sie auf dem tertiären Ziel-Cluster die Beziehung zum sekundären Cluster:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. Auf dem tertiären Ziel-Cluster die Beziehung zum sekundären Cluster initialisieren:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

Verwandte Informationen

- "snapmirror create"
- "snapmirror initialize"
- "snapmirror policy add-rule"
- "snapmirror policy create"
- "snapmirror policy show"

Konfiguration Ihres ONTAP Systems für die Backend-Replizierung über FC

Ab ONTAP 9.20.1 können Sie die asynchrone Replizierung im Backend mit SnapMirror und SnapLock für SnapVault über vorhandene Fibre-Channel-Netzwerke (FC) konfigurieren. Für die Aktivierung der Datenreplizierung über FC muss die Backend FC-Replizierung konfiguriert sein.

> Bei der Konfiguration der Backend-Replikation über FC müssen sowohl das FC-Fabric als auch das Intercluster-IP-Netzwerk betriebsbereit sein. Replikationsdaten können über das FC-Fabric übertragen werden, das Intercluster-IP-Netzwerk ist jedoch für die Clusterkommunikation und Funktionen der Replikationsverwaltung erforderlich.

Über diese Aufgabe

Für die Backend-Replizierung über FC werden direkt angeschlossene FC-Konfigurationen und Konfigurationen mit automatischer Fabric-Zonierung nicht unterstützt.

Bevor Sie beginnen

Die Knoten in Ihren Quell- und Ziel-Clustern müssen die folgenden Konfigurationsanforderungen erfüllen:

- Mindestens vier Storage-Knoten müssen an der Replikationsbeziehung beteiligt sein: zwei Knoten im Quell-Cluster und zwei Knoten im Ziel-Cluster.
- Jeder Knoten muss mit mindestens den folgenden Ports konfiguriert sein:
  - 2 dedizierte FC-Initiatoranschlüsse
  - 2 FC-Zielports für FC-Frontend-Konnektivität
  - 2 FC Zielports für FC Backend-Konnektivität
- Die Switch-Fabric, die den Quell-Cluster und den Ziel-Cluster verbindet, muss über mindestens 16 verfügbare Ports mit passenden SFPs verfügen, die für den Backend-Datenverkehr reserviert sind. Weitere Informationen zu "Bewährte Verfahren für die FC Fabric Konfiguration".
- Alle HBAs, SFPs und Switch-Ports im Replikationspfad sollten mit derselben festen Geschwindigkeit arbeiten, um die Verbindungsstabilität zu gewährleisten.

Schritte

1. Die FC-Netzwerkadapter im Quell- und Ziel-Cluster, die als Backend-Initiatoren verwendet werden sollen, sind zu identifizieren:

```
network fcp adapter show
```

In den folgenden Beispielen ist ssan-a50-06a-06b der Quell-Cluster und ssan-a50-07a-07b der Ziel-Cluster. Die Beispielausgabe für den Quell-Cluster lautet wie folgt:

```
ssan-a50-06a-06b::*>network fcp adapter show
                  Connection  Port    Admin    Operational
Node         Adapter  Established Address Status   Status
------------ -------- ----------- ------- -------- ---------------
ssan-a50-06a 3a       false       0       up       link not connected
ssan-a50-06a 3b       false       0       up       link not connected
ssan-a50-06a 3c       false       0       up       link not connected
ssan-a50-06a 3d       false       0       up       link not connected
ssan-a50-06b 3a       false       0       up       link not connected
ssan-a50-06b 3b       false       0       up       link not connected
ssan-a50-06b 3c       false       0       up       link not connected
ssan-a50-06b 3d       false       0       up       link not connected
```

Die Beispielausgabe für den Ziel-Cluster sieht wie folgt aus:

```
ssan-a50-07a-07b::*>network fcp adapter show
ssan-a50-07a 3a       false       0       up       link not connected
ssan-a50-07a 3b       false       0       up       link not connected
ssan-a50-07a 3c       false       0       up       link not connected
ssan-a50-07a 3d       false       0       up       link not connected
ssan-a50-07b 3a       false       0       up       link not connected
ssan-a50-07b 3b       false       0       up       link not connected
ssan-a50-07b 3c       false       0       up       link not connected
ssan-a50-07b 3d       false       0       up       link not connected
```

2. Für den Initiatormodus sind auf jedem Knoten in der Replikationsbeziehung sowohl im Quell- als auch im Ziel-Cluster 2 Ports zu konfigurieren:

   a. Den Adapter offline schalten:

```
network fcp adapter modify -node <node_name> -adapter <adapter>
-status-admin down
```

   Im folgenden Beispiel wird Port 3c offline gesetzt.

```
network fcp adapter modify -node ssan-a50-06a -adapter 3c -status-admin
down
```

a. Konfiguration des Adapters für den Initiatormodus:

```
system hardware unified-connect modify -t initiator <adapter_port>
```

Der Node sollte zum Anwenden der Adapteränderung nicht neu gestartet werden. Nach der Konfiguration aller erforderlichen Adapter und ihrer erneuten Online-Schaltung erfolgt für jeden Node ein Storage Failover, damit die Änderungen unterbrechungsfrei wirksam werden.

b. Den Adapter online schalten:

```
network fcp adapter modify -node <node_name> -adapter <adapter>
-status-admin up
```

c. Die Schritte sind für jeden Port zu wiederholen, der für den Initiatormodus konfiguriert werden muss.

d. Zu überprüfen ist, ob alle Ports online und als Initiatoren konfiguriert sind:

```
network fcp adapter show
```

3. Auf jedem HA-Paar, das für die FC-Replikation konfiguriert wird, erfolgt ein manuelles Storage Failover.

Das Storage Failover ermöglicht den Abschluss der Adaptermodifikationen ohne einen störenden Neustart des Knotens.

a. Storage Failover für den ersten Knoten in einem HA-Paar ausführen:

```
storage failover takeover
```

b. Zu prüfen ist, ob das Storage Failover erfolgreich war:

```
storage failover show-takeover
```

Die automatische Rückgabe ist standardmäßig aktiviert. Nachdem ein Knoten übernommen wurde und den Neustart abgeschlossen hat, initiiert der Partnerknoten automatisch eine Rückgabe.

c. Nach Abschluss der automatischen Rückgabe des ersten Knotens erfolgt auf dem zweiten Knoten im HA-Paar ein Storage Failover.

d. Für jedes HA-Paar, das für die FC-Replikation konfiguriert wird, ist eine Wiederholung der Storage Failover Schritte erforderlich.

4. Sicherzustellen ist, dass die Netzwerk-FC-Ports auf allen Knoten, die für die FC-Replizierung konfiguriert

werden, online und als Initiatoren konfiguriert sind:

```
system hardware unified-connect show
```

5. Es ist sicherzustellen, dass die FC-Adapter Ihres Onboard-Systems als Ziele konfiguriert sind:

```
network fcp adapter show
```

Onboard-Systemadapter sind standardmäßig als Ziele konfiguriert.

6. Anhand des empfohlenen Verkabelungsdiagramms lässt sich die FC-Verkabelung zwischen den FC-Zielports und den Initiatorports vervollständigen.
7. Nach der Verkabelung erfolgt die Zonierung der FC-Ziel- und Initiator-Ports für jedes HA-Paar.

Jede Zone darf nur einen Initiator und ein Ziel haben.

Im Folgenden finden Sie ein Beispiel für Zonen, die zwischen den Knoten san-a50-06a/6b und san-a50-07a/7b erstellt wurden:

```
zone-6a-7a-1 → Ports san-a50-06a:3c & san-a50-07a:3a
zone-6a-7a-2 → Ports san-a50-06a:3d & san-a50-07a:3a
zone-6a-7a-3 → Ports san-a50-06a:3c & san-a50-07a:3b
zone-6a-7a-4 → Ports san-a50-06a:3d & san-a50-07a:3b
zone-6b-7a-1 → Ports san-a50-06b:3c & san-a50-07a:3a
zone-6b-7a-2 → Ports san-a50-06b:3d & san-a50-07a:3a
zone-6b-7a-3 → Ports san-a50-06b:3c & san-a50-07a:3b
zone-6b-7a-4 → Ports san-a50-06b:3d & san-a50-07a:3b
zone-6a-7b-1 → Ports san-a50-06a:3c & san-a50-07b:3a
zone-6a-7b-2 → Ports san-a50-06a:3d & san-a50-07b:3a
zone-6a-7b-3 → Ports san-a50-06a:3c & san-a50-07b:3b
zone-6a-7b-4 → Ports san-a50-06a:3d & san-a50-07b:3b
zone-6b-7b-1 → Ports san-a50-06b:3c & san-a50-07b:3a
zone-6b-7b-2 → Ports san-a50-06b:3d & san-a50-07b:3a
zone-6b-7b-3 → Ports san-a50-06b:3c & san-a50-07b:3b
zone-6b-7b-4 → Ports san-a50-06b:3d & san-a50-07b:3b
```

8. Die Erstellung der Backend-FC-Zielnetzwerkschnittstellen (LIFs) erfolgt zunächst auf dem Quell-Cluster und anschließend auf dem Ziel-Cluster:

```
network interface create -vserver <SVM> -lif <fcp_backend_target_lif>
-data-protocol fcp -home-node <home_node> -home-port <home_port> -status
-admin up
```

Im folgenden Beispiel werden Backend FC LIFs auf Cluster A erstellt: ssan-a50-06a.

```
network interface create -vserver ssan-a50-06a -lif
fcp_backend_target_lif_1 -data-protocol fcp -home-node ssan-a50-06a
-home-port 3a -status-admin up
network interface create -vserver ssan-a50-06a -lif
fcp_backend_target_lif_2 -data-protocol fcp -home-node ssan-a50-06a
-home-port 3b -status-admin up
network interface create -vserver ssan-a50-06b -lif
fcp_backend_target_lif_1 -data-protocol fcp -home-node ssan-a50-06b
-home-port 3a -status-admin up
network interface create -vserver ssan-a50-06b -lif
fcp_backend_target_lif_2 -data-protocol fcp -home-node ssan-a50-06b
-home-port 3b -status-admin up
```

Im folgenden Beispiel werden Backend FC LIFs auf Cluster B erstellt: ssan-a50-07a

```
network interface create -vserver ssan-a50-07a -lif
fcp_backend_target_lif_1 -data-protocol fcp -home-node ssan-a50-07a
-home-port 3a -status-admin up
network interface create -vserver ssan-a50-07a -lif
fcp_backend_target_lif_2 -data-protocol fcp -home-node ssan-a50-07a
-home-port 3b -status-admin up
network interface create -vserver ssan-a50-07b -lif
fcp_backend_target_lif_1 -data-protocol fcp -home-node ssan-a50-07b
-home-port 3a -status-admin up
network interface create -vserver ssan-a50-07b -lif
fcp_backend_target_lif_2 -data-protocol fcp -home-node ssan-a50-07b
-home-port 3b -status-admin up
```

9. Überprüfung, ob die LIFs erstellt wurden:

```
network interface show -vserver <SVM>
```

Was kommt als Nächstes?

Sie sind bereit, "SnapMirror Replikation konfigurieren" FC als Backend-Transportprotokoll zu verwenden.

Replikation von SnapMirror Volumes verwalten

Konvertieren einer bestehenden ONTAP SnapMirror DP-Beziehung in XDP

Wenn Sie auf ONTAP 9.12.1 oder höher aktualisieren, müssen DP-Typ-Beziehungen vor dem Upgrade in XDP konvertiert werden. ONTAP 9.12.1 und höher unterstützt keine DP-Typ-Beziehungen. Eine bestehende DP-Typ-Beziehung kann einfach in XDP konvertiert werden, um die versionsflexible SnapMirror Funktionalität zu nutzen.

Vor dem Upgrade auf ONTAP 9.12.1 müssen bestehende DP-Beziehungen in XDP konvertiert werden, bevor ein Upgrade auf ONTAP 9.12.1 und spätere Versionen möglich ist.

Über diese Aufgabe

- SnapMirror konvertiert bestehende DP-Beziehungen nicht automatisch in XDP-Beziehungen. Für die Konvertierung der Beziehung ist es erforderlich, die bestehende Beziehung zu unterbrechen und zu löschen, eine neue XDP-Beziehung zu erstellen und die Beziehung erneut zu synchronisieren.
- Bei der Planung Ihrer Umstellung sollten Sie beachten, dass die Vorbereitung im Hintergrund und die Datenspeicherungsphase einer XDP SnapMirror Beziehung viel Zeit in Anspruch nehmen können. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „preparing“ über einen längeren Zeitraum meldet.

> Nach der Konvertierung eines SnapMirror Beziehungstyps von DP zu XDP werden speicherbezogene Einstellungen, wie automatische Größenanpassung und Speicherplatzzusage, nicht mehr an das Ziel repliziert.

Schritte

1. Im Ziel-Cluster ist sicherzustellen, dass die SnapMirror Beziehung vom Typ DP ist, der Spiegelungsstatus SnapMirrored ist, der Beziehungsstatus auf Idle steht und die Beziehung fehlerfrei ist:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   Das folgende Beispiel zeigt die Ausgabe des `snapmirror show` Befehls:

   ```
   cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

   Source Path: svm1:volA
   Destination Path: svm_backup:volA_dst
   Relationship Type: DP
   SnapMirror Schedule: -
   Tries Limit: -
   Throttle (KB/sec): unlimited
   Mirror State: Snapmirrored
   Relationship Status: Idle
   Transfer Snapshot: -
   Snapshot Progress: -
   Total Progress: -
   Snapshot Checkpoint: -
   Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
   123478563412_2147484682.2014-06-27_100026
   Newest Snapshot Timestamp: 06/27 10:00:55
   Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
   123478563412_2147484682.2014-06-27_100026
   Exported Snapshot Timestamp: 06/27 10:00:55
   Healthy: true
   ```

Es kann hilfreich sein, eine Kopie der `snapmirror show` Befehlsausgabe aufzubewahren, um die bestehenden Beziehungseinstellungen nachzuverfolgen. Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

2. Anhand der Quell- und Ziel-Volumes ist sicherzustellen, dass beide Volumes über einen gemeinsamen Snapshot verfügen:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Das folgende Beispiel zeigt die `volume snapshot show` Ausgabe für die Quell- und Ziel-Volumes:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
```

```
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Um sicherzustellen, dass geplante Aktualisierungen während der Konvertierung nicht ausgeführt werden, die bestehende DP-Typ-Beziehung in einen inaktiven Zustand versetzen:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel versetzt die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup` in den Ruhezustand:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror quiesce` finden sich in der "ONTAP-Befehlsreferenz".

4. Die bestehende DP-Beziehung auflösen:

```
snapmirror break -destination-path <SVM:volume>
```

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel unterbricht die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

5. Wenn die automatische Löschung von Snapshots auf dem Zielvolume aktiviert ist, sollte sie deaktiviert werden:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

Das folgende Beispiel deaktiviert die automatische Löschung von Snapshots auf dem Zielvolume

volA_dst:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Die bestehende DP-Beziehung löschen:

```
snapmirror delete -destination-path <SVM:volume>
```

Weitere Informationen zu `snapmirror-delete` finden sich in der "ONTAP-Befehlsreferenz".

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel löscht die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Die ursprüngliche SVM Disaster Recovery Beziehung auf dem Quell-Cluster freigeben:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

Das folgende Beispiel gibt die SVM Disaster Recovery Beziehung frei:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

Weitere Informationen zu `snapmirror release` finden sich in der "ONTAP-Befehlsreferenz".

8. Sie können die Ausgabe, die Sie vom `snapmirror show` Befehl behalten haben, verwenden, um die neue XDP Typ Beziehung zu erstellen:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

Die neue Beziehung muss dasselbe Quell- und Zielvolume verwenden. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel erstellt eine SnapMirror Disaster-Recovery-Beziehung zwischen dem Quell-Volume

`volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf `svm_backup` unter Verwendung der Standard `MirrorAllSnapshots`-Richtlinie:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Die Quell- und Ziel-Volumes werden erneut synchronisiert:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Um die Resynchronisierungszeit zu verbessern, können Sie die `-quick-resync` Option verwenden, sollten sich aber darüber im Klaren sein, dass Einsparungen bei der Speichereffizienz verloren gehen können.

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden. Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden.

Das folgende Beispiel synchronisiert die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror resync` finden sich in der "ONTAP-Befehlsreferenz".

10. Falls die automatische Löschung von Snapshots deaktiviert wurde, sollte sie wieder aktiviert werden:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Nachdem Sie fertig sind

1. Mit dem `snapmirror show`Befehl lässt sich überprüfen, ob die SnapMirror Beziehung erstellt wurde.

   Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

2. Sobald das SnapMirror XDP-Zielvolume mit der Aktualisierung von Snapshots gemäß der SnapMirror Richtlinie beginnt, kann mit der Ausgabe des `snapmirror list-destinations` Befehls aus dem Quell-Cluster die neue SnapMirror XDP-Beziehung angezeigt werden.

Zusätzliche Informationen zu DP-Beziehungen

Ab ONTAP 9.3 ist der XDP Modus standardmäßig aktiviert, und alle Aufrufe des DP Modus in der Befehlszeile oder in neuen oder bestehenden Skripten werden automatisch in den XDP Modus konvertiert.

Bestehende Beziehungen bleiben unberührt. Wenn eine Beziehung bereits vom Typ DP ist, bleibt sie vom Typ DP. Ab ONTAP 9.5 ist MirrorAndVault die Standardrichtlinie, wenn kein Datenschutzmodus angegeben ist oder wenn der XDP-Modus als Beziehungstyp festgelegt wurde. Die folgende Tabelle zeigt das erwartete Verhalten.

Wenn Sie angeben…	Der Typ ist…	Die Standardrichtlinie (wenn Sie keine Richtlinie angeben) ist…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nichts	XDP	MirrorAndVault (einheitliche Replikation)
XDP	XDP	MirrorAndVault (einheitliche Replikation)

Wie die Tabelle zeigt, gewährleisten die unter verschiedenen Umständen XDP zugewiesenen Standardrichtlinien, dass die Konvertierung die funktionale Äquivalenz der vorherigen Typen beibehält. Es können selbstverständlich auch andere Richtlinien verwendet werden, einschließlich Richtlinien für die einheitliche Replikation.

Wenn Sie angeben…	Und die Richtlinie lautet…	Das Ergebnis ist…
DP	MirrorAllSnapshots	SnapMirror DR
XDPDefault	SnapVault	MirrorAndVault
Einheitliche Replikation	XDP	MirrorAllSnapshots
SnapMirror DR	XDPDefault	SnapVault

Die einzigen Ausnahmen von der Umwandlung sind wie folgt:

- SVM-Datensicherungsbeziehungen sind in ONTAP 9.3 und früher weiterhin standardmäßig im DP-Modus.

  Ab ONTAP 9.4 sind SVM-Datensicherungsbeziehungen standardmäßig im XDP-Modus.

- Die Load-Sharing-Datenschutzbeziehungen des Root-Volumes verbleiben weiterhin standardmäßig im DP-Modus.
- SnapLock Datenschutzbeziehungen verbleiben in ONTAP 9.4 und früher weiterhin standardmäßig im DP-Modus.

  Ab ONTAP 9.5 werden SnapLock Datenschutzbeziehungen standardmäßig im XDP-Modus hergestellt.

- Explizite Aufrufe von DP verwenden weiterhin standardmäßig den DP-Modus, wenn die folgende clusterweite Option festgelegt ist:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Diese Option wird ignoriert, wenn DP nicht explizit aufgerufen wird.

Verwandte Informationen

- "snapmirror create"
- "snapmirror delete"

- "snapmirror quiesce"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"

Den Typ einer ONTAP SnapMirror Beziehung konvertieren

Ab ONTAP 9.5 wird SnapMirror synchron unterstützt. Eine SnapMirror asynchron Beziehung kann in eine SnapMirror synchron Beziehung oder umgekehrt umgewandelt werden, ohne dass ein Basistransfer erforderlich ist.

Über diese Aufgabe

Sie können eine SnapMirror asynchron Beziehung nicht durch Ändern der SnapMirror Richtlinie in eine SnapMirror synchron Beziehung oder umgekehrt umwandeln.

Schritte

- **Umwandlung einer SnapMirror asynchronen Beziehung in eine SnapMirror synchronen Beziehung**

  a. Vom Ziel-Cluster aus die SnapMirror asynchrone Beziehung löschen:

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. Vom Quell-Cluster die SnapMirror Beziehung freigeben, ohne die gemeinsamen Snapshots zu löschen:

  ```
  snapmirror release -relationship-info-only true -destination-path
  <destination_SVM>:<destination_volume>
  ```

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  c. Vom Ziel-Cluster aus eine SnapMirror synchron Beziehung erstellen:

  ```
  snapmirror create -source-path src_SVM:src_volume -destination-path
  <destination_SVM>:<destination_volume> -policy sync-mirror
  ```

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  d. Die SnapMirror synchron Beziehung erneut synchronisieren:

  ```
  snapmirror resync -destination-path <destination_SVM:destination_volume>
  ```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- **Umwandlung einer SnapMirror synchronen Beziehung in eine SnapMirror asynchrone Beziehung**

  a. Vom Ziel-Cluster die bestehende SnapMirror synchron Beziehung stilllegen:

  `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

  ```
  cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
  ```

  b. Vom Ziel-Cluster aus die SnapMirror asynchrone Beziehung löschen:

  `snapmirror delete -destination-path <SVM:volume>`

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  c. Vom Quell-Cluster die SnapMirror Beziehung freigeben, ohne die gemeinsamen Snapshots zu löschen:

  `snapmirror release -relationship-info-only true -destination-path <destination_SVM:destination_volume>`

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  d. Vom Ziel-Cluster aus eine SnapMirror asynchrone Beziehung erstellen:

  `snapmirror create -source-path src_SVM:src_volume -destination-path <destination_SVM:destination_volume> -policy MirrorAllSnapshots`

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  e. Die SnapMirror synchron Beziehung erneut synchronisieren:

  `snapmirror resync -destination-path <destination_SVM:destination_volume>`

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Verwandte Informationen

- "snapmirror create"
- "snapmirror delete"
- "snapmirror quiesce"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"

Den Modus einer ONTAP SnapMirror synchronen Beziehung konvertieren

Ab ONTAP 9.5 werden SnapMirror synchron Beziehungen unterstützt. Der Modus einer SnapMirror synchron Beziehung kann von StrictSync auf Sync oder umgekehrt geändert werden.

Über diese Aufgabe

Die Richtlinie einer SnapMirror synchronen Beziehung kann nicht geändert werden, um deren Modus zu konvertieren.

Schritte

1. Vom Ziel-Cluster die bestehende SnapMirror synchron Beziehung stilllegen:

   ```
   snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
   ```

   ```
   cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
   ```

2. Vom Ziel-Cluster aus die bestehende SnapMirror synchron Beziehung löschen:

   ```
   snapmirror delete -destination-path <destination_SVM>:<destination_volume>
   ```

   ```
   cluster2::> snapmirror delete -destination-path vs1_dr:vol1
   ```

3. Vom Quell-Cluster die SnapMirror Beziehung freigeben, ohne die gemeinsamen Snapshots zu löschen:

   ```
   snapmirror release -relationship-info-only true -destination-path
   <destination_SVM>:<destination_volume>
   ```

   ```
   cluster1::> snapmirror release -relationship-info-only true -destination
   -path vs1_dr:vol1
   ```

4. Vom Ziel-Cluster aus eine SnapMirror synchron Beziehung erstellen, indem der Modus angegeben wird, in den die SnapMirror synchron Beziehung konvertiert werden soll:

   ```
   snapmirror create -source-path vs1:vol1 -destination-path
   <destination_SVM>:<destination_volume> -policy Sync|StrictSync
   ```

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. Vom Ziel-Cluster aus die SnapMirror Beziehung neu synchronisieren:

   ```
   snapmirror resync -destination-path <destination_SVM>:<destination_volume>
   ```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

Verwandte Informationen

- "snapmirror create"
- "snapmirror delete"
- "snapmirror quiesce"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"

ONTAP SnapMirror Failover-Testvolumes erstellen und löschen

Ab ONTAP 9.14.1 kann mit System Manager ein Volume-Klon erstellt werden, um das SnapMirror Failover und die Disaster Recovery zu testen, ohne die aktive SnapMirror Beziehung zu unterbrechen. Nach Abschluss der Tests können die zugehörigen Daten bereinigt und das Testvolume gelöscht werden.

Ein SnapMirror Failover-Testvolume erstellen

Über diese Aufgabe

- Failover-Tests können für synchrone und SnapMirror asynchrone Beziehungen durchgeführt werden.
- Ein Volume-Klon wird erstellt, um den Disaster-Recovery-Test durchzuführen.
- Das Klon-Volume wird auf derselben Storage-VM wie das SnapMirror Ziel erstellt.
- Sie können FlexVol und FlexGroup SnapMirror-Beziehungen verwenden.
- Wenn für die ausgewählte Beziehung bereits ein Testklon existiert, kann kein weiterer Klon für diese Beziehung erstellt werden.
- SnapLock Vault-Beziehungen werden nicht unterstützt.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein.
- Die SnapMirror Lizenz muss auf dem Quell-Cluster und dem Ziel-Cluster installiert sein.

Schritte

1. Im Ziel-Cluster **Schutz > Beziehungen** auswählen.
2. Wählen Sie ⋮ neben der Beziehungsquelle die Option **Test Failover**.
3. Im Fenster **Test Failover** die Option **Test Failover** auswählen.
4. **Speicher > Volumes** auswählen und überprüfen, ob das Test-Failover-Volume aufgeführt ist.
5. **Speicher > Freigaben** auswählen.
6. Wählen Sie + Add und dann **Teilen** aus.
7. Im Fenster **Freigabe hinzufügen** im Feld **Freigabename** einen Namen für die Freigabe eingeben.
8. Im Feld **Ordner Durchsuchen** auswählen, das Test-Klon-Volume auswählen und **Speichern**.
9. Unten im Fenster **Freigabe hinzufügen** die Option **Speichern** auswählen.

10. Im Bereich **Speicher > Freigaben** die erstellte Freigabe suchen und ⌄ auswählen, um die Freigabeinformationen anzuzeigen.
11. Unter **SMB/CIFS-Zugriff** den Zugriffspfad für die Freigabe kopieren oder notieren, zum Beispiel `\\123.456.7.890\failover_test`.
12. Verwenden Sie den SMB-Zugriffspfad, um die Freigabe auf dem Client zu öffnen und zu überprüfen, ob das Testvolume über Lese- und Schreibfunktionen verfügt.

Failover-Daten bereinigen und das Testvolume löschen

Nach Abschluss der Failover-Tests können alle mit dem Testvolume verbundenen Daten bereinigt und das Testvolume gelöscht werden.

Schritte

1. Im Ziel-Cluster **Schutz > Beziehungen** auswählen.
2. Wählen Sie ⋮ neben der Beziehungsquelle die Option **Test-Failover bereinigen**.
3. Im Fenster **Clean Up Test Failover** die Option **Clean Up** auswählen.
4. **Storage > Volumes** auswählen und überprüfen, ob das Testvolume gelöscht wurde.

Daten von einem SnapMirror DR-Zielvolume bereitstellen

Das ONTAP SnapMirror Zielvolume beschreibbar machen

Das Zielvolume muss beschreibbar gemacht werden, bevor Daten von diesem Volume an Clients ausgeliefert werden können. Um Daten von einem SnapMirror Ziel bereitzustellen, wenn eine Quelle nicht verfügbar ist, werden die geplanten Übertragungen zum Ziel gestoppt und anschließend die SnapMirror Beziehung getrennt, um das Ziel beschreibbar zu machen.

Über diese Aufgabe

Diese Aufgabe muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um ein Zielvolume beschreibbar zu machen.

System Manager

1. Die Schutzbeziehung wird ausgewählt, indem auf **Schutz > Beziehungen** und dann auf den gewünschten Volume-Namen geklickt wird.
2. Klicken Sie ⋮.
3. Geplante Übertragungen anhalten: **Pause** auswählen.
4. Das Ziel beschreibbar machen: Auf **Break** klicken.
5. Auf der Hauptseite **Beziehungen** lässt sich überprüfen, ob der Beziehungsstatus als "abgebrochen" angezeigt wird.

Nächste Schritte

Sie müssen "die Replikationsbeziehung rückwärts resynchronisieren" ausführen, nachdem das Zielvolume beschreibbar gemacht wurde.

Wenn das deaktivierte Quellvolume wieder verfügbar ist, sollte die Beziehung erneut rücksynchronisiert werden, um die aktuellen Daten auf das ursprüngliche Quellvolume zu kopieren.

CLI

1. Geplante Transfers zum Ziel-Cluster anhalten:

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Das folgende Beispiel stoppt geplante Übertragungen zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror quiesce` finden sich in der "ONTAP-Befehlsreferenz".

2. Laufende Transfers zum Ziel-Cluster beenden:

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Dieser Schritt ist für SnapMirror synchron Beziehungen nicht erforderlich (unterstützt ab ONTAP 9.5).

Das folgende Beispiel stoppt laufende Übertragungen zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror abort` finden sich in der "ONTAP-Befehlsreferenz".

3. Die SnapMirror DR-Beziehung beenden:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Das folgende Beispiel unterbricht die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
```

```
-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

Nächste Schritte

Sie müssen "die Replikationsbeziehung resynchronisieren" ausführen, nachdem das Zielvolume beschreibbar gemacht wurde.

Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgaben mit… auszuführen	Diesen Inhalt ansehen…
System Manager Classic (verfügbar mit ONTAP 9.7 und früher)	"Überblick über die Volume-Desaster-Recovery"

Das ONTAP SnapMirror Zielvolume für den Datenzugriff konfigurieren

Nachdem das Zielvolume beschreibbar gemacht wurde, muss das Volume für den Datenzugriff konfiguriert werden. NAS-Clients, NVMe-Subsystem und SAN-Hosts können auf die Daten des Zielvolumes zugreifen, bis das Quellvolume reaktiviert wird.

NAS Umgebung:

1. Das NAS-Volume wird in den Namespace eingebunden, wobei derselbe Verbindungspfad verwendet wird, an den das Quell-Volume im Quell-SVM eingebunden war.
2. Die entsprechenden ACLs werden auf die SMB-Freigaben am Zielvolume angewendet.
3. Die NFS-Exportrichtlinien werden dem Zielvolume zugewiesen.
4. Die Quotenregeln werden auf das Zielvolume angewendet.
5. Clients werden zum Zielvolume umgeleitet.
6. Die NFS- und SMB-Freigaben auf den Clients erneut einbinden.

SAN Umgebung:

1. Die LUNs im Volume werden der entsprechenden Initiatorgruppe zugeordnet.
2. Für iSCSI werden iSCSI-Sitzungen von den SAN-Host-Initiatoren zu den SAN LIFs erstellt.
3. Auf dem SAN-Client ist ein erneuter Speicherscan erforderlich, damit die angeschlossenen LUNs erkannt werden.

Informationen zur NVMe-Umgebung sind unter "SAN Verwaltung" verfügbar.

Das ursprüngliche ONTAP SnapMirror Quellvolume wird reaktiviert

Sie können die ursprüngliche Datensicherungsbeziehung zwischen Quell- und Zielvolume wiederherstellen, wenn keine Daten mehr vom Zielvolume bereitgestellt werden müssen.

Über diese Aufgabe

- Das folgende Verfahren setzt voraus, dass die Baseline im ursprünglichen Quellvolume intakt ist. Falls die Baseline nicht intakt ist, muss die Beziehung zwischen dem Volume, von dem Daten bereitgestellt werden, und dem ursprünglichen Quellvolume erstellt und initialisiert werden, bevor das Verfahren durchgeführt wird.
- Die Hintergrundvorbereitung und die Data-Warehousing-Phase einer XDP SnapMirror Beziehung können viel Zeit in Anspruch nehmen. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „preparing“ über einen längeren Zeitraum meldet.

Schritte

1. Die ursprüngliche Datensicherungsbeziehung umkehren:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Weitere Informationen zu `snapmirror resync` finden sich in der "ONTAP-Befehlsreferenz".

   > Dieser Befehl muss von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden. Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden. Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein gemeinsamer Snapshot vorhanden ist. Mit `snapmirror initialize` kann die Beziehung neu initialisiert werden. Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel kehrt die Beziehung zwischen dem ursprünglichen Quellvolume, `volA` auf `svm1`, und dem Volume, von dem Daten bereitgestellt werden, `volA_dst` auf `svm_backup` um:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. Wenn Sie bereit sind, den Datenzugriff auf die ursprüngliche Quelle wiederherzustellen, beenden Sie den Zugriff auf das ursprüngliche Zielvolume. Eine Möglichkeit hierfür ist das Stoppen der ursprünglichen Ziel-SVM:

   `vserver stop -vserver` *`SVM`*

   > Dieser Befehl muss von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster ausgeführt werden. Dieser Befehl unterbindet den Benutzerzugriff auf die gesamte ursprüngliche Ziel-SVM. Es besteht die Möglichkeit, den Zugriff auf das ursprüngliche Ziel-Volume mit anderen Methoden zu unterbinden.

   Das folgende Beispiel stoppt die ursprüngliche Ziel-SVM:

   ```
   cluster_dst::> vserver stop svm_backup
   ```

   Weitere Informationen zu `vserver stop` finden sich in der "ONTAP-Befehlsreferenz".

3. Die umgekehrte Beziehung aktualisieren:

`snapmirror update -source-path SVM:volume -destination-path SVM:volume`

> Dieser Befehl muss von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden.

Das folgende Beispiel aktualisiert die Beziehung zwischen dem Volume, von dem Daten bereitgestellt werden, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quellvolume, `volA` auf `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Weitere Informationen zu `snapmirror update` finden sich in der "ONTAP-Befehlsreferenz".

4. Vom ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster geplante Übertragungen für die umgekehrte Beziehung anhalten:

`snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

> Dieser Befehl muss von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden.

Das folgende Beispiel stoppt geplante Übertragungen zwischen dem ursprünglichen Zielvolume, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quellvolume, `volA` auf `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Weitere Informationen zu `snapmirror quiesce` finden sich in der "ONTAP-Befehlsreferenz".

5. Wenn das letzte Update abgeschlossen ist und die Beziehung den Status „Quiesced“ anzeigt, kann der folgende Befehl auf der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden, um die umgekehrte Beziehung aufzuheben:

`snapmirror break -source-path SVM:volume -destination-path SVM:volume`

> Dieser Befehl muss von der ursprünglichen Quell-SVM oder dem Quell-Cluster ausgeführt werden.

Das folgende Beispiel unterbricht die Beziehung zwischen dem ursprünglichen Zielvolume, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quellvolume, `volA` auf `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

6. Aus der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster die umgekehrte Datensicherungsbeziehung löschen:

   `snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

   > Dieser Befehl muss von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden.

   Das folgende Beispiel löscht die umgekehrte Beziehung zwischen dem ursprünglichen Quellvolume, `volA` auf `svm1`, und dem Volume, von dem Daten bereitgestellt werden, `volA_dst` auf `svm_backup`:

   ```
   cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Weitere Informationen zu `snapmirror delete` finden sich in der "ONTAP-Befehlsreferenz".

7. Die umgekehrte Beziehung vom ursprünglichen Ziel-SVM oder vom ursprünglichen Ziel-Cluster aufheben.

   `snapmirror release -source-path SVM:volume -destination-path SVM:volume`

   > Dieser Befehl muss von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster ausgeführt werden.

   Das folgende Beispiel hebt die umgekehrte Beziehung zwischen dem ursprünglichen Zielvolume, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quellvolume, `volA` auf `svm1`, auf:

   ```
   cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Weitere Informationen zu `snapmirror release` finden sich in der "ONTAP-Befehlsreferenz".

8. Die ursprüngliche Datensicherungsbeziehung vom ursprünglichen Ziel-Cluster wiederherstellen:

   `snapmirror resync -source-path SVM:volume -destination-path SVM:volume`

   Das folgende Beispiel stellt die Beziehung zwischen dem ursprünglichen Quellvolume, `volA` auf `svm1`, und dem ursprünglichen Zielvolume, `volA_dst` auf `svm_backup`, wieder her:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   Weitere Informationen zu `snapmirror resync` finden sich in der "ONTAP-Befehlsreferenz".

9. Gegebenenfalls die ursprüngliche Ziel-SVM starten:

   `vserver start -vserver SVM`

Das folgende Beispiel startet die ursprüngliche Ziel-SVM:

```
cluster_dst::> vserver start svm_backup
```

Weitere Informationen zu `vserver start` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Mit dem `snapmirror show`Befehl lässt sich überprüfen, ob die SnapMirror Beziehung erstellt wurde.

Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

Dateien von einem SnapMirror Zielvolume wiederherstellen

Wiederherstellung einer Datei, LUN oder eines NVMe-Namensraums von einem ONTAP SnapMirror Ziel

Sie können eine einzelne Datei, LUN, eine Gruppe von Dateien oder LUNs aus einem Snapshot oder einen NVMe-Namensraum von einem SnapMirror Ziel-Volume wiederherstellen. Ab ONTAP 9.7 ist auch die Wiederherstellung von NVMe-Namensräumen von einem SnapMirror synchron Ziel möglich. Dateien können auf dem ursprünglichen Quell-Volume oder auf einem anderen Volume wiederhergestellt werden.

Bevor Sie beginnen

Um eine Datei oder LUN von einem SnapMirror synchronen Ziel wiederherzustellen (unterstützt ab ONTAP 9.5), muss zuerst die Beziehung gelöscht und freigegeben werden.

Über diese Aufgabe

Das Volume, auf dem Sie Dateien oder LUNs wiederherstellen (das Zielvolume), muss ein Lese-/Schreibvolume sein:

- SnapMirror führt eine *inkrementelle Wiederherstellung* durch, wenn Quell- und Zielvolume einen gemeinsamen Snapshot haben (was typischerweise der Fall ist, wenn auf das ursprüngliche Quellvolume wiederhergestellt wird).
- Andernfalls führt SnapMirror eine *Basistransfer-Wiederherstellung* durch, bei der der angegebene Snapshot und alle von ihm referenzierten Datenblöcke auf das Ziel-Volume übertragen werden.

Schritte

1. Die Snapshots im Ziel-Volume auflisten:

   ```
   volume snapshot show -vserver <SVM> -volume volume
   ```

   Weitere Informationen zu `volume snapshot show` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Momentaufnahmen auf dem `vserverB:secondary1` Ziel-Cluster:

   ```
   cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

   Vserver     Volume      Snapshot                  State    Size  Total%
   Used%
   ```

```
-------     ------      ---------- ---------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Eine einzelne Datei oder LUN oder ein Satz von Dateien oder LUNs aus einem Snapshot in einem SnapMirror Ziel-Volume wiederherstellen:

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot -file-list <source_file_path,@destination_file_path>
   ```

   Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

   Der folgende Befehl stellt die Dateien `file1` und `file2` aus dem Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` an derselben Stelle im aktiven Dateisystem des ursprünglichen Quellvolumes `primary1` wieder her:

   ```
   cluster_dst::> snapmirror restore -source-path vserverB:secondary1
   -destination-path vserverA:primary1 -source-snapshot daily.2013-01-
   25_0010 -file-list /dir1/file1,/dir2/file2

   [Job 3479] Job is queued: snapmirror restore for the relationship with
   destination vserverA:primary1
   ```

   Der folgende Befehl stellt die Dateien `file1` und `file2` aus dem Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` an einem anderen Ort im aktiven Dateisystem des ursprünglichen Quellvolumes `primary1` wieder her.

   Der Zieldateipfad beginnt mit dem @-Symbol, gefolgt vom Pfad der Datei ausgehend vom Stammverzeichnis des ursprünglichen Quell-Volumes. In diesem Beispiel wird `file1` auf `/dir1/file1.new` wiederhergestellt und file2 auf `/dir2.new/file2` auf `primary1` wiederhergestellt:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Der folgende Befehl stellt die Dateien `file1` und `file3` aus dem Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` an verschiedenen Orten im aktiven Dateisystem des ursprünglichen Quellvolumes `primary1` wieder her und stellt `file2` von `snap1` am selben Ort im aktiven Dateisystem von `primary1` wieder her.

In diesem Beispiel wird die Datei `file1` wiederhergestellt zu `/dir1/file1.new` und `file3` wird wiederhergestellt zu `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Verwandte Informationen

- "SnapMirror Restore"

Wiederherstellung von Volumeninhalten aus einem ONTAP SnapMirror Ziel

Sie können den Inhalt eines gesamten Volumes aus einem Snapshot in einem SnapMirror Ziel-Volume wiederherstellen. Der Inhalt des Volumes kann auf das ursprüngliche Quell-Volume oder auf ein anderes Volume wiederhergestellt werden.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zum Wiederherstellen von Daten zu verwenden. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Das Zielvolume für den Wiederherstellungsvorgang muss eines der folgenden sein:

- Ein lesen/schreiben Volume, in diesem Fall führt SnapMirror eine inkrementelle Wiederherstellung durch, vorausgesetzt, dass Quell- und Ziel-Volume über einen gemeinsamen Snapshot verfügen (was typischerweise der Fall ist, wenn auf das ursprüngliche Quell-Volume wiederhergestellt wird).

  Der Befehl schlägt fehl, wenn kein gemeinsamer Snapshot vorhanden ist. Der Inhalt eines Volumes kann nicht auf einem leeren lesen/schreiben-Volume wiederhergestellt werden.

- Ein leeres Datensicherungsvolume, in diesem Fall führt SnapMirror eine *Baseline-Wiederherstellung* durch, bei der der angegebene Snapshot und alle von ihm referenzierten Datenblöcke auf das Quellvolume übertragen werden.

Das Wiederherstellen des Inhalts eines Volumes ist ein unterbrechender Vorgang. SMB-Datenverkehr darf auf dem SnapVault primären Volume nicht ausgeführt werden, wenn ein Wiederherstellungsvorgang läuft.

Wenn auf dem Zielvolume für die Wiederherstellung die Komprimierung aktiviert ist und auf dem Quellvolume die Komprimierung nicht aktiviert ist, sollte die Komprimierung auf dem Zielvolume deaktiviert werden. Die Komprimierung muss nach Abschluss der Wiederherstellung wieder aktiviert werden.

Alle für das Zielvolume definierten Kontingentregeln werden vor der Wiederherstellung deaktiviert. Mit dem `volume quota modify` Befehl lassen sich die Kontingentregeln nach Abschluss der Wiederherstellung wieder aktivieren.

Wenn Daten in einem Volume verloren gehen oder beschädigt werden, kann eine Wiederherstellung durch das Zurücksetzen auf einen früheren Snapshot erfolgen.

Dieses Verfahren ersetzt die aktuellen Daten auf dem Quellvolume durch Daten aus einer früheren Snapshot-Version. Diese Aufgabe ist auf dem Ziel-Cluster durchzuführen.

Schritte

Der Inhalt eines Volumes kann mithilfe von System Manager oder der ONTAP CLI wiederhergestellt werden.

System Manager

1. **Schutz > Beziehungen** auswählen und anschließend den Namen des Quellvolumes anklicken.
2. Klicken Sie ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle** ist standardmäßig das Quellvolume ausgewählt. **Anderes Volume** kann ausgewählt werden, wenn ein anderes Volume als das Quellvolume gewählt werden soll.
4. Unter **Ziel** den Snapshot auswählen, der wiederhergestellt werden soll.
5. Wenn sich Quelle und Ziel auf unterschiedlichen Clustern befinden, im Remote-Cluster unter **Schutz > Beziehungen** den Wiederherstellungsfortschritt überwachen.

CLI

1. Die Snapshots im Ziel-Volume auflisten:

   ```
   volume snapshot show -vserver <SVM> -volume <volume>
   ```

   Das folgende Beispiel zeigt die Momentaufnahmen auf dem `vserverB:secondary1` Ziel-Cluster:

   ```
   cluster_dst::> volume snapshot show -vserver vserverB -volume
   secondary1

   Vserver     Volume      Snapshot                State    Size
   Total% Used%
   -------     ------      ---------- ----------- ------   -----
   ------ -----
   ```

```
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Den Inhalt eines Volumes aus einem Snapshot in einem SnapMirror Ziel-Volume wiederherstellen:

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
   <snapshot>
   ```

   Dieser Befehl muss von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden.

   Der folgende Befehl stellt den Inhalt des ursprünglichen Quellvolumes `primary1` aus dem Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` wieder her:

   ```
   cluster_src::> snapmirror restore -source-path vserverB:secondary1
   -destination-path vserverA:primary1 -source-snapshot daily.2013-01-
   25_0010

   Warning: All data newer than snapshot daily.2013-01-25_0010 on
   volume vserverA:primary1 will be deleted.

   Do you want to continue? {y|n}: y

   [Job 34] Job is queued: snapmirror restore from source
   vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
   ```

3. Das wiederhergestellte Volume erneut einbinden und alle Anwendungen, die das Volume verwenden, neu starten.

Weitere Möglichkeiten, dies in ONTAP zu tun

Um diese Aufgaben mit… auszuführen	Diesen Inhalt ansehen…
System Manager Classic (verfügbar mit ONTAP 9.7 und früher)	"Volumenwiederherstellung mit SnapVault Übersicht"

Verwandte Informationen

- "SnapMirror Restore"
- "volume snapshot show"

Eine ONTAP SnapMirror Replikationsbeziehung manuell aktualisieren

Möglicherweise ist eine manuelle Aktualisierung einer Replikationsbeziehung erforderlich, wenn eine Aktualisierung fehlschlägt, weil das Quellvolume verschoben wurde.

Über diese Aufgabe

SnapMirror bricht alle Übertragungen von einem verschobenen Quellvolume ab, bis die Replikationsbeziehung manuell aktualisiert wird.

Ab ONTAP 9.5 werden SnapMirror synchron Beziehungen unterstützt. Obwohl Quell- und Zielvolume in diesen Beziehungen stets synchron sind, wird die Ansicht vom sekundären Cluster nur stündlich mit dem primären synchronisiert. Wenn die zeitpunktgenauen Daten am Ziel angezeigt werden sollen, ist eine manuelle Aktualisierung durch Ausführen des `snapmirror update` Befehls erforderlich.

Schritt

1. Eine Replikationsbeziehung manuell aktualisieren:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

> Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden. Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein gemeinsamer Snapshot vorhanden ist. Mit `snapmirror initialize` kann die Beziehung neu initialisiert werden. Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel aktualisiert die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror update` finden sich in der "ONTAP-Befehlsreferenz".

Eine ONTAP SnapMirror Replikationsbeziehung neu synchronisieren

Eine Replikationsbeziehung muss neu synchronisiert werden, nachdem ein Zielvolume beschreibbar gemacht wurde, nachdem ein Update fehlgeschlagen ist, weil kein gemeinsamer Snapshot auf dem Quell- und Zielvolume vorhanden ist, oder wenn die

Replikationsrichtlinie für die Beziehung geändert werden soll.

Ab ONTAP 9.8 kann mit System Manager eine umgekehrte Resynchronisierung durchgeführt werden, um eine bestehende Schutzbeziehung zu löschen und die Funktionen der Quell- und Zielvolumes umzukehren. Anschließend wird das Zielvolume zur Datenbereitstellung verwendet, während das Quellvolume repariert oder ersetzt, aktualisiert und die ursprüngliche Systemkonfiguration wiederhergestellt wird.

> System Manager unterstützt keine umgekehrte Resynchronisierung mit Intracluster-Beziehungen. Mit der ONTAP CLI lassen sich umgekehrte Resynchronisierungsvorgänge mit Intracluster-Beziehungen durchführen.

Über diese Aufgabe

- Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden.
- Volumes, die Teil einer Fan-Out- oder Kaskadenkonfiguration sind, können länger für die Resynchronisierung benötigen. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „preparing“ über einen längeren Zeitraum meldet.
- Ab ONTAP 9.13.1 versucht ONTAP standardmäßig, die Schnellsynchronisierung zu nutzen, um die Synchronisierungszeit zu verkürzen. Die folgenden Bedingungen müssen erfüllt sein, damit die Schnellsynchronisierung standardmäßig verwendet wird:
  - FlexVol Volumes enthalten keine Klone auf dem Volume
  - Bei Verwendung der MirrorAllSnapshots Richtlinie

> Die Verwendung von `-quick-resync` kann aufgrund der Entfernung der Speichereffizienz bei übertragenen Datenblöcken zusätzlichen Speicherplatz auf dem Resync-Ziel-Volume beanspruchen. Dieser zusätzliche Speicherplatz wird im Rahmen der Inline- oder Post-Replikations-Speichereffizienzanwendung auf dem Resync-Ziel wiederhergestellt.

  Der `-quick-resync` Parameter ist optional. Die Schnell-Resynchronisierung kann durch Verwendung des `-quick-resync true|false` Parameters mit dem `snapmirror resync` Befehl aktiviert oder deaktiviert werden.

  Weitere Informationen zu `-quick-resync` finden sich unter "ONTAP-Befehlsreferenz".

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um diese Aufgabe auszuführen. Bei Verwendung der ONTAP CLI ist das Verfahren unabhängig davon gleich, ob ein Ziel-Volume beschreibbar gemacht oder die Replikationsbeziehung aktualisiert wird.

System Manager Reverse-Resynchronisierung

Nachdem Sie "eine Beziehung beenden" ein Ziel beschreibbar gemacht haben, wird die Beziehung durch Rücksynchronisierung umgekehrt:

1. Im Ziel-Cluster auf **Schutz > Beziehungen** klicken.
2. Fahren Sie mit dem Mauszeiger über die abgebrochene Beziehung, klicken Sie auf ⋮ und wählen Sie **Reverse Resync** aus.
3. Im Fenster **Umgekehrte Resynchronisierungsbeziehung** auf **Umgekehrte Resynchronisierung** klicken.

4. Unter **Beziehungen** lässt sich der Fortschritt der umgekehrten Resynchronisierung überwachen, indem **Übertragungsstatus** für die Beziehung angezeigt wird.

Nächste Schritte

Wenn die ursprüngliche Quelle wieder verfügbar ist, kann die ursprüngliche Beziehung wiederhergestellt werden, indem die umgekehrte Beziehung aufgehoben und eine weitere Reverse-Resync-Operation durchgeführt wird. Der Reverse-Resync-Prozess kopiert alle Änderungen von der Seite, die die Daten bereitstellt, auf die ursprüngliche Quelle und macht die ursprüngliche Quelle wieder lesen/schreiben-fähig.

System Manager Resynchronisierung

1. **Schutz > Beziehungen** auswählen.
2. Bewegen Sie den Mauszeiger über die Beziehung, die Sie neu synchronisieren möchten, und klicken Sie auf ⋮ und wählen Sie dann **Trennen**.
3. Wenn der Beziehungsstatus „Abgebrochen“ angezeigt wird, ⋮ und anschließend **Neu synchronisieren** ausgewählt wird.
4. Unter **Beziehungen** lässt sich der Fortschritt der Resynchronisierung überwachen, indem der Beziehungsstatus überprüft wird. Der Status ändert sich zu „Gespiegelt“, wenn die Resynchronisierung abgeschlossen ist.

CLI

1. Die Quell- und Ziel-Volumes werden erneut synchronisiert:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

ⓘ Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel resynchronisiert die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror resync` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Die Daten auf einer ONTAP SnapMirror Ziel-SVM werden erneut synchronisiert"

Löschen einer ONTAP SnapMirror Volume-Replikationsbeziehung

Sie können die `snapmirror delete` und `snapmirror release` Befehle verwenden, um eine Volume-Replikationsbeziehung zu löschen. Anschließend können nicht mehr benötigte Ziel-Volumes manuell gelöscht werden.

Über diese Aufgabe

Der `snapmirror release`Befehl löscht alle von SnapMirror erstellten Snapshots aus der Quelle. Mit der `-relationship-info-only`Option besteht die Möglichkeit, die Snapshots zu erhalten.

Schritte

1. Die Replikationsbeziehung anhalten:

   `snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>`

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   Weitere Informationen zu `snapmirror quiesce` finden sich in der "ONTAP-Befehlsreferenz".

2. (Optional) Trennen der Replikationsbeziehung, wenn das Ziel-Volume ein lesen/schreiben-Volume sein muss. Sie können diesen Schritt überspringen, wenn Sie das Ziel-Volume löschen möchten oder das Volume nicht für lesen/schreiben benötigt wird:

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path svm_backup:volA_dst
   ```

   Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

3. Die Replikationsbeziehung löschen:

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   Dieser Befehl muss vom Ziel-Cluster oder der Ziel-SVM ausgeführt werden.

   Das folgende Beispiel löscht die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination -path svm_backup:volA_dst
   ```

   Weitere Informationen zu `snapmirror delete` finden sich in der "ONTAP-Befehlsreferenz".

4. Informationen zur Replikationsbeziehung aus der Quell-SVM freigeben:

   `snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   Dieser Befehl muss vom Quell-Cluster oder der Quell-SVM ausgeführt werden.

Das folgende Beispiel gibt Informationen für die angegebene Replikationsbeziehung von der Quell-SVM `svm1` frei:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Weitere Informationen zu `snapmirror release` finden sich in der "ONTAP-Befehlsreferenz".

Speichereffizienz auf ONTAP SnapMirror Volumes verwalten

SnapMirror bewahrt die Speichereffizienz auf dem Quell- und Zielvolume, außer wenn die nachträgliche Datenkomprimierung auf dem Zielvolume aktiviert ist. In diesem Fall geht die gesamte Speichereffizienz auf dem Zielvolume verloren. Zur Behebung dieses Problems ist die nachträgliche Datenkomprimierung auf dem Zielvolume zu deaktivieren, die Beziehung manuell zu aktualisieren und die Speichereffizienz erneut zu aktivieren.

Über diese Aufgabe

Sie können den `volume efficiency show` Befehl verwenden, um festzustellen, ob die Effizienz auf einem Volume aktiviert ist. Weitere Informationen zu `volume efficiency show` finden sich in der "ONTAP-Befehlsreferenz".

Es kann überprüft werden, ob SnapMirror die Speichereffizienz beibehält, indem die SnapMirror Audit-Protokolle angezeigt und die Übertragungsbeschreibung gesucht wird. Wenn in der Übertragungsbeschreibung `transfer_desc=Logical Transfer with Storage Efficiency` angezeigt wird, behält SnapMirror die Speichereffizienz bei. Wenn in der Übertragungsbeschreibung `transfer_desc=Logical Transfer` angezeigt wird, behält SnapMirror die Speichereffizienz nicht bei. Beispiel:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Bevor Sie beginnen

- Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

  "Cluster- und SVM-Peering"

- Die Nachbearbeitungskomprimierung muss auf dem Zielvolume deaktiviert werden.
- Logische Übertragung mit Speicher: Ab ONTAP 9.3 ist keine manuelle Aktualisierung mehr erforderlich, um die Speichereffizienz wieder zu aktivieren. Wenn SnapMirror erkennt, dass die Nachbearbeitungskomprimierung deaktiviert wurde, wird die Speichereffizienz beim nächsten geplanten Update automatisch wieder aktiviert. Sowohl das Quell- als auch das Zielsystem müssen ONTAP 9.3 ausführen.
- Ab ONTAP 9.3 verwalten AFF Systeme die Einstellungen zur Speichereffizienz anders als FAS Systeme,

nachdem ein Zielvolume beschreibbar gemacht wurde:

- Nachdem ein Zielvolume mit dem `snapmirror break` Befehl beschreibbar gemacht wurde, wird die Caching-Richtlinie für das Volume automatisch auf `auto` (die Standardeinstellung) gesetzt.

  Dieses Verhalten gilt nur für FlexVol Volumen und nicht für FlexGroup Volumen.

  Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

- Bei der erneuten Synchronisierung wird die Caching-Richtlinie automatisch auf `none` gesetzt, und Deduplizierung sowie Inline-Komprimierung werden automatisch deaktiviert, unabhängig von Ihren ursprünglichen Einstellungen. Die Einstellungen sind bei Bedarf manuell anzupassen.

Manuelle Aktualisierungen mit aktivierter Speichereffizienz können zeitaufwändig sein. Es kann sinnvoll sein, den Vorgang außerhalb der Stoßzeiten auszuführen.

Schritte

1. Eine Replikationsbeziehung aktualisieren und die Speichereffizienz wieder aktivieren:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden. Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein gemeinsamer Snapshot vorhanden ist. Mit `snapmirror initialize` kann die Beziehung neu initialisiert werden. Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel aktualisiert die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA_dst` auf `svm_backup`, und aktiviert die Speichereffizienz wieder:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

Weitere Informationen zu `snapmirror update` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SnapMirror globale Drosselung verwenden

Globale Netzwerkdrosselung ist für alle SnapMirror- und SnapVault-Übertragungen auf Knotenebene verfügbar.

Über diese Aufgabe

SnapMirror globale Drosselung beschränkt die Bandbreite, die für eingehende und/oder ausgehende SnapMirror und SnapVault Transfers verwendet wird. Die Beschränkung wird clusterweit auf allen Knoten im Cluster durchgesetzt.

Wenn beispielsweise die ausgehende Bandbreite auf 100 MBps begrenzt ist, beträgt die ausgehende Bandbreite auf jedem Knoten im Cluster 100 MBps. Wenn die globale Begrenzung deaktiviert ist, ist sie auf

allen Knoten deaktiviert.

Obwohl Datentransferraten oft in Bit pro Sekunde (bps) angegeben werden, müssen die Drosselungswerte in Kilobyte pro Sekunde (KBps) eingegeben werden.

> In ONTAP 9.9.1 und früheren Versionen hat die Drosselung keine Auswirkung auf `volume move` Übertragungen oder Load-Sharing Mirror Übertragungen. Ab ONTAP 9.10.0 kann eine Option zur Drosselung eines Volume Move Vorgangs angegeben werden. Weitere Details finden sich unter "Drosselung der Volume-Verschiebung in ONTAP 9.10 und neueren Versionen".

Die globale Drosselung funktioniert zusammen mit der Drosselungsfunktion pro Beziehung für SnapMirror und SnapVault Transfers. Die Drosselung pro Beziehung wird so lange angewendet, bis die kombinierte Bandbreite der pro-Beziehung-Transfers den Wert der globalen Drosselung überschreitet, danach wird die globale Drosselung angewendet. Ein Drosselungswert `0`bedeutet, dass die globale Drosselung deaktiviert ist.

> SnapMirror globale Drosselung hat keine Auswirkung auf SnapMirror synchron Beziehungen, wenn sie In-Sync sind. Die Drosselung wirkt sich jedoch auf SnapMirror synchron Beziehungen aus, wenn sie eine asynchrone Übertragungsphase wie eine Initialisierungsoperation oder nach einem Out Of Sync-Ereignis durchführen. Aus diesem Grund wird die Aktivierung der globalen Drosselung bei SnapMirror synchron Beziehungen nicht empfohlen.

Schritte

1. Globale Drosselung aktivieren:

   ```
   options -option-name replication.throttle.enable on|off
   ```

   Das folgende Beispiel zeigt, wie die globale Drosselung von SnapMirror aktiviert wird `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Die maximale Gesamtbandbreite, die von eingehenden Übertragungen auf dem Ziel-Cluster verwendet wird, angeben:

   ```
   options -option-name replication.throttle.incoming.max_kbs <KBps>
   ```

   Die empfohlene minimale Bandbreite beträgt 4 Kilobyte pro Sekunde (KBps), die maximale bis zu 2 Terabyte pro Sekunde (TBps). Der Standardwert für diese Option ist `unlimited`, was bedeutet, dass es keine Begrenzung für die insgesamt genutzte Bandbreite gibt.

   Das folgende Beispiel zeigt, wie die maximale gesamte Bandbreite für eingehende Übertragungen auf 100 Megabit pro Sekunde (Mbit/s) festgelegt wird:

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 Megabit pro Sekunde (Mbps) = 12500 Kilobyte pro Sekunde (KBps)

3. Die maximale Gesamtbandbreite, die von ausgehenden Übertragungen auf dem Quell-Cluster verwendet wird, angeben:

```
options -option-name replication.throttle.outgoing.max_kbs <KBps>
```

Die empfohlene minimale Bandbreite beträgt 4 KBps, die maximale bis zu 2 TBps. Der Standardwert für diese Option ist `unlimited`, was bedeutet, dass es keine Begrenzung für die insgesamt genutzte Bandbreite gibt. Die Parameterwerte werden in Kilobyte pro Sekunde (KBps) angegeben.

Das folgende Beispiel zeigt, wie die maximale Gesamtbandbreite für ausgehende Übertragungen auf 100 Mbit/s festgelegt wird:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

SVM-Replikation von SnapMirror verwalten

Informationen zu ONTAP SnapMirror SVM-Replizierung

Mit SnapMirror lässt sich eine Datensicherungsbeziehung zwischen SVMs erstellen. Bei dieser Art von Datensicherungsbeziehung werden die gesamte oder ein Teil der SVM-Konfiguration, von NFS-Exporten und SMB-Freigaben bis hin zu RBAC, sowie die Daten in den Volumes, die der SVM gehören, repliziert.

Unterstützte Beziehungstypen

Nur datenliefernde SVMs können repliziert werden. Die folgenden Datensicherungsbeziehungstypen werden unterstützt:

- *SnapMirror DR,* wobei das Ziel typischerweise nur die Snapshots enthält, die sich aktuell auf dem Quell-Cluster befinden.

  Ab ONTAP 9.9.1 ändert sich dieses Verhalten bei Verwendung der Mirror-Vault-Richtlinie. Ab ONTAP 9.9.1 ist es möglich, unterschiedliche Snapshot-Richtlinien auf dem Quell-Cluster und dem Ziel-Cluster zu erstellen, und die Snapshots auf dem Ziel-Cluster werden nicht durch Snapshots auf dem Quell-Cluster überschrieben:

  - Sie werden während normaler geplanter Vorgänge, Aktualisierungen und Resynchronisierungen nicht von der Quelle auf das Ziel überschrieben.
  - Sie werden während Pausenvorgängen nicht gelöscht.
  - Sie werden bei Flip-Resync-Vorgängen nicht gelöscht. Bei der Konfiguration einer SVM-Notfallbeziehung mit der Mirror-Vault-Richtlinie unter ONTAP 9.9.1 und höher verhält sich die Richtlinie wie folgt:
  - Benutzerdefinierte Snapshot-Richtlinien am Quell-Cluster werden nicht auf das Ziel-Cluster kopiert.
  - Systemdefinierte Snapshot-Richtlinien werden nicht auf das Ziel kopiert.
  - Die Zuordnung von Volumes zu benutzerdefinierten und systemdefinierten Snapshot-Richtlinien wird nicht auf die Ziel-SVM kopiert.
- *SnapMirror Unified Replication*, bei der das Ziel sowohl für Disaster Recovery als auch für die Langzeitaufbewahrung konfiguriert ist.

Weitere Informationen zur einheitlichen SnapMirror Replikation finden sich unter "SnapMirror Grundlagen der

einheitlichen Replikation".

Der *Richtlinientyp* der Replikationsrichtlinie bestimmt die Art der Beziehung, die sie unterstützt. Die folgende Tabelle zeigt die verfügbaren Richtlinientypen.

Richtlinientyp	Beziehungstyp
async-mirror	SnapMirror DR
mirror-vault	Einheitliche Replikation

XDP ersetzt DP als Standard-SVM-Replikationsverfahren in ONTAP 9.4

Ab ONTAP 9.4 sind SVM-Datensicherungsbeziehungen standardmäßig im XDP-Modus. SVM-Datensicherungsbeziehungen sind in ONTAP 9.3 und früher weiterhin standardmäßig im DP-Modus.

Bestehende Beziehungen sind von der XDP-Standardeinstellung nicht betroffen. Wenn eine Beziehung bereits vom Typ DP ist, bleibt sie vom Typ DP. Die folgende Tabelle zeigt das zu erwartende Verhalten.

Wenn Sie angeben…	Der Typ ist…	Die Standardrichtlinie (wenn Sie keine Richtlinie angeben) ist…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nichts	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	MirrorAndVault (Vereinheitlichte Replikation)

Informationen zur Konvertierung von DP-Beziehungen in XDP-Beziehungen und weitere Details sind hier zu finden: "Konvertieren einer bestehenden ONTAP DP-Beziehung in XDP".

> Versionsunabhängigkeit wird für die SVM-Replizierung nicht unterstützt. In einer SVM-Disaster-Recovery-Konfiguration muss sich die Ziel-SVM auf einem Cluster befinden, der dieselbe ONTAP Version wie der Quell-SVM-Cluster ausführt, um Failover und Failback Vorgänge zu unterstützen.

"Kompatible ONTAP Versionen für SnapMirror Beziehungen"

Wie SVM Konfigurationen repliziert werden

Der Inhalt einer SVM-Replikationsbeziehung wird durch das Zusammenspiel der folgenden Felder bestimmt:

- Die `-identity-preserve true` Option des `snapmirror create` Befehls repliziert die gesamte SVM-Konfiguration.

  Die `-identity-preserve false` Option repliziert lediglich die Volumes sowie die Authentifizierungs- und Autorisierungskonfigurationen der SVM und die Protokoll- und Namensdiensteinstellungen, die in "Konfigurationen, die in SVM Disaster Recovery-Beziehungen repliziert werden" aufgeführt sind.

- Die `-discard-configs network` Option des `snapmirror policy create` Befehls schließt LIFs und zugehörige Netzwerkeinstellungen von der SVM-Replikation aus, für Fälle, in denen sich Quell- und Ziel-SVMs in unterschiedlichen Subnetzen befinden.

- Die `-vserver-dr-protection unprotected`Option des `volume modify`Befehls schließt das angegebene Volume von der SVM-Replikation aus.

Ansonsten ist die SVM-Replikation nahezu identisch mit der Volume-Replikation. Für die SVM-Replikation kann praktisch derselbe Workflow wie für die Volume-Replikation verwendet werden.

Supportdetails

Die folgende Tabelle zeigt Unterstützungsdetails für die SnapMirror SVM-Replikation.

Ressource oder Funktion	Supportdetails
Bereitstellungsarten	• Eine Quelle zu einem einzigen Ziel • Ab ONTAP 9.4 ist Fan-Out verfügbar. Es kann ein Fan-Out auf nur zwei Ziele erfolgen. Standardmäßig ist pro Quell-SVM nur eine -identity-preserve true Beziehung zulässig.
Beziehungstypen	• SnapMirror Katastrophenwiederherstellung • SnapMirror einheitliche Replikation
Replikationsbereich	Nur zwischen Clustern möglich. SVMs können nicht im selben Cluster repliziert werden.
Autonomous Ransomware Protection	• Unterstützt ab ONTAP 9.12.1. Weitere Informationen finden sich unter "Autonomous Ransomware Protection".
Asynchrone Unterstützung für Konsistenzgruppen	Ab ONTAP 9.14.1 werden maximal 32 SVM Disaster Recovery-Beziehungen unterstützt, wenn Konsistenzgruppen vorhanden sind. Siehe "Eine Konsistenzgruppe schützen" und "Konsistenzgruppenlimits" für weitere Informationen.
FabricPool	Ab ONTAP 9.6 wird die SnapMirror SVM-Replikation mit FabricPool unterstützt. Bei einer SVM DR-Beziehung müssen Quell- und Ziel-Volumes keine FabricPool Aggregate verwenden, sie müssen jedoch dieselbe Tiering-Richtlinie nutzen. Ab ONTAP 9.12.1 wird die SnapMirror SVM-Replikation mit FabricPool und FlexGroup Volumes unterstützt, die gemeinsam arbeiten. Vor Version 9.12.1 funktionierten jeweils zwei dieser Funktionen zusammen, jedoch nicht alle drei gleichzeitig.
IPsec aktivieren	Ab ONTAP 9.19.1 nicht unterstützt.

MetroCluster	Ab ONTAP 9.11.1 können beide Seiten einer SVM-Notfallwiederherstellungsbeziehung innerhalb einer MetroCluster Konfiguration als Quelle für zusätzliche SVM-Notfallwiederherstellungskonfigurationen dienen. Ab ONTAP 9.5 wird die SnapMirror SVM-Replikation auf MetroCluster Konfigurationen unterstützt. • In Versionen vor ONTAP 9.10.X kann eine MetroCluster Konfiguration nicht das Ziel einer SVM-Notfallwiederherstellungsbeziehung sein. • In ONTAP 9.10.1 und späteren Versionen kann eine MetroCluster Konfiguration ausschließlich zu Migrationszwecken das Ziel einer SVM-Disaster-Recovery-Beziehung sein und muss alle notwendigen Anforderungen erfüllen, die in "TR-4966: Migration einer SVM in eine MetroCluster Lösung" beschrieben sind. • Nur eine aktive SVM innerhalb einer MetroCluster Konfiguration kann die Quelle einer SVM-Notfallwiederherstellungsbeziehung sein. Eine Quelle kann vor dem Switchover eine Sync-Source SVM oder nach dem Switchover eine Sync-Destination SVM sein. • Wenn sich eine MetroCluster Konfiguration im stabilen Zustand befindet, kann die MetroCluster Sync-Destination-SVM nicht die Quelle einer SVM-Disaster-Recovery-Beziehung sein, da die Volumes nicht online sind. • Wenn die Sync-Source-SVM die Quelle einer SVM Disaster-Recovery-Beziehung ist, werden die Informationen zur Quell-SVM Disaster-Recovery-Beziehung an den MetroCluster Partner repliziert. • Während der Umschaltungs- und Rückschaltungsprozesse kann die Replikation zum SVM-Disaster-Recovery-Ziel fehlschlagen. Nach Abschluss des Umschaltungs- oder Rückschaltungsprozesses werden die nächsten geplanten Updates der SVM-Disaster Recovery erfolgreich durchgeführt.
ONTAP S3	Wird bei SVM-Disaster Recovery nicht unterstützt.
SnapMirror Cloud	Wird bei SVM-Disaster Recovery nicht unterstützt.
SnapMirror Synchronous	Wird bei SVM-Disaster Recovery nicht unterstützt.
Versionsunabhängigkeit	Nicht unterstützt.

Volumenverschlüsselung	• Verschlüsselte Datenträger auf dem Quellsystem sind auch auf dem Zielsystem verschlüsselt. • Auf dem Zielsystem müssen Onboard Key Manager oder KMIP-Server konfiguriert sein. • Am Zielort werden neue Verschlüsselungsschlüssel generiert. • Wenn das Ziel keinen Knoten enthält, der volume .encryption unterstützt, ist die Replikation zwar erfolgreich, aber die Zielvolumes sind nicht verschlüsselt.

Konfigurationen, die in SVM Disaster Recovery-Beziehungen repliziert werden

Die folgende Tabelle zeigt die Wechselwirkung der `snapmirror create -identity-preserve` Option und der `snapmirror policy create -discard-configs network` Option:

Konfiguration repliziert		**`-identity-preserve true`**		**`-identity-preserve false`**
		Richtlinie ohne `-discard-configs network` Festlegung	**Richtlinie mit `-discard-configs network` set**	
Netzwerk	NAS-LIFs	Ja	Nein	Nein
LIF Kerberos Konfiguration	Ja	Nein	Nein	SAN-LIFs
Nein	Nein	Nein	Firewall-Richtlinien	Ja
Ja	Nein	Servicerichtlinien	Ja	Ja
Nein	Routen	Ja	Nein	Nein
Broadcast-Domain	Nein	Nein	Nein	Subnetz
Nein	Nein	Nein	IPspace	Nein
Nein	Nein	SMB	SMB-Server	Ja
Ja	Nein	Lokale Gruppen und lokale Nutzer	Ja	Ja
Ja	Privileg	Ja	Ja	Ja
Schattenkopie	Ja	Ja	Ja	BranchCache
Ja	Ja	Ja	Serveroptionen	Ja
Ja	Ja	Serversicherheit	Ja	Ja
Nein	Home-Verzeichnis, Freigabe	Ja	Ja	Ja
Symlink	Ja	Ja	Ja	Fpolicy policy, Fsecurity policy und Fsecurity NTFS

Ja	Ja	Ja	Namenszuordnung und Gruppenzuordnung	Ja
Ja	Ja	Auditinformationen	Ja	Ja
Ja	NFS	Export-Richtlinien	Ja	Ja
Nein	Exportrichtlinienregeln	Ja	Ja	Nein
NFS-Server	Ja	Ja	Nein	RBAC
Sicherheitszertifikate	Ja	Ja	Nein	Benutzername, öffentlicher Schlüssel, Rolle und Rollenkonfiguration
Ja	Ja	Ja	SSL	Ja
Ja	Nein	Namensdienste	DNS und DNS-Hosts	Ja
Ja	Nein	UNIX-Benutzer und UNIX-Gruppe	Ja	Ja
Ja	Kerberos Realm und Kerberos Keyblocks	Ja	Ja	Nein
LDAP und LDAP-Client	Ja	Ja	Nein	Netgroup
Ja	Ja	Nein	NIS	Ja
Ja	Nein	Web und Webzugriff	Ja	Ja
Nein	Volumen	Objekt	Ja	Ja
Ja	Snapshots und Snapshot-Richtlinie	Ja	Ja	Ja
Richtlinie zum automatischen Löschen	Nein	Nein	Nein	Effizienzrichtlinie
Ja	Ja	Ja	Quota-Policy und Quota-Policy-Regel	Ja
Ja	Ja	Wiederherstellungswarteschlange	Ja	Ja
Ja	Root Volume	Namensraum	Ja	Ja
Ja	Nutzerdaten	Nein	Nein	Nein
Qtrees	Nein	Nein	Nein	Kontingente
Nein	Nein	Nein	QoS auf Dateiebene	Nein

Nein	Nein	Attribute: Status des Root-Volumes, Speicherplatzzusage, Größe, automatische Größenanpassung und Gesamtanzahl der Dateien	Nein	Nein
Nein	Storage QoS	QoS Richtliniengruppe	Ja	Ja
Ja	Fibre Channel (FC)	Nein	Nein	Nein
iSCSI	Nein	Nein	Nein	LUNs
Objekt	Ja	Ja	Ja	igroups
Nein	Nein	Nein	Portsets	Nein
Nein	Nein	Seriennummern	Nein	Nein
Nein	SNMP	v3 Benutzer	Ja	Ja

Storage-Grenzen für die SVM-Notfallwiederherstellung

Die folgende Tabelle zeigt die empfohlene maximale Anzahl an Volumes und SVM-Disaster-Recovery-Beziehungen pro Speicherobjekt. Es ist zu beachten, dass die Grenzwerte häufig plattformabhängig sind. In der "Hardware Universe" sind die Grenzwerte für Ihre spezifische Konfiguration aufgeführt.

Speicherobjekt	Limit
SVM	300 Flexible Volumes
HA-Paar	1.000 Flexible Volumes
Cluster	128 SVM Katastrophenbeziehungen

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"

SVM Konfigurationen replizieren

ONTAP SnapMirror SVM-Replikationsworkflow

SnapMirror SVM-Replikation umfasst das Erstellen der Ziel-SVM, das Erstellen eines Replikationsjob-Zeitplans und das Erstellen und Initialisieren einer SnapMirror Beziehung.

Es empfiehlt sich zu ermitteln, welcher Replikationsworkflow am besten zu Ihren Anforderungen passt:

- "Eine vollständige SVM-Konfiguration replizieren"
- "LIFs und zugehörige Netzwerkeinstellungen von der SVM-Replizierung ausschließen"
- "Netzwerk-, Namensdienst- und andere Einstellungen von der SVM-Konfiguration ausschließen"

Kriterien für die Platzierung von Volumes auf ONTAP SnapMirror Ziel-SVMs

Beim Replizieren von Volumes von der Quell-SVM zur Ziel-SVM ist es wichtig, die Kriterien für die Auswahl der Aggregate zu kennen.

Die Auswahl der Aggregate erfolgt anhand der folgenden Kriterien:

- Volumes werden immer auf Nicht-Root-Aggregaten platziert.
- Nicht-Root-Aggregate werden basierend auf dem verfügbaren freien Speicherplatz und der Anzahl der bereits auf dem Aggregat gehosteten Volumes ausgewählt.

  Aggregate mit mehr freiem Speicherplatz und weniger Volumes erhalten Priorität. Das Aggregat mit der höchsten Priorität wird ausgewählt.

- Quellvolumina auf FabricPool Aggregaten werden auf FabricPool Aggregaten am Ziel mit derselben Tiering-Policy platziert.
- Wenn sich ein Volume auf der Quell-SVM in einem Flash Pool Aggregat befindet, wird das Volume in einem Flash Pool Aggregat auf der Ziel-SVM platziert, sofern ein solches Aggregat existiert und über genügend freien Speicherplatz verfügt.
- Wenn die `-space-guarantee` Option des zu replizierenden Volumes auf `volume` gesetzt ist, werden nur Aggregate berücksichtigt, deren freier Speicherplatz größer als die Volume-Größe ist.
- Die Volume-Größe wächst während der Replikation auf dem Ziel-SVM automatisch basierend auf der Quell-Volume-Größe.

  Wenn Sie die Größe auf der Ziel-SVM vorab reservieren möchten, müssen Sie das Volume anpassen. Die Volume-Größe wird auf der Ziel-SVM nicht automatisch basierend auf der Quell-SVM verkleinert.

Wenn ein Volume von einem Aggregat auf ein anderes verschoben werden soll, kann der `volume move` Befehl auf der Ziel-SVM verwendet werden.

Eine vollständige ONTAP SVM Konfiguration replizieren

Es kann eine SVM Disaster Recovery (SVM DR) Beziehung erstellt werden, um eine SVM Konfiguration auf eine andere zu replizieren. Bei einem Ausfall am primären Standort lässt sich die Ziel-SVM schnell aktivieren.

Bevor Sie beginnen

- Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

  Weitere Informationen finden Sie unter "Erstellen einer Cluster Peer-Beziehung" und "Erstellen einer SVM Intercluster Peer-Beziehung".

- Ab ONTAP 9.19.1 wird die Aktivierung von IPsec auf SVMs, die für SVM DR konfiguriert sind, nicht unterstützt. Wenn Sie IPsec verwenden, muss es deaktiviert werden oder eine andere SVM für die Konfiguration einer SVM DR Beziehung ausgewählt werden. Eine Fehlermeldung erscheint, wenn ONTAP 9.19.1 oder höher verwendet wird und versucht wird, IPsec auf einer für SVM DR konfigurierten SVM zu aktivieren.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Dieser Workflow setzt voraus, dass Sie bereits eine Standardrichtlinie oder eine benutzerdefinierte Replikationsrichtlinie verwenden.

Ab ONTAP 9.9.1 ist es bei Verwendung der mirror-vault Richtlinie möglich, unterschiedliche Snapshot-Richtlinien auf der Quell- und Ziel-SVM zu erstellen, wobei die Snapshots auf dem Ziel nicht durch Snapshots auf der Quelle überschrieben werden. Weitere Informationen finden sich unter "Überblick über die SnapMirror SVM-Replikation".

Diese Prozedur ist vom Ziel aus durchzuführen. Falls eine neue Datensicherungsstrategie erforderlich ist, zum Beispiel wenn die Quell-Speicher-VM mit SMB konfiguriert ist, sollte die Strategie erstellt und die Option **Identity preserve** verwendet werden. Weitere Informationen finden sich unter "Benutzerdefinierte Datensicherungsstrategien erstellen".

Schritte

Diese Aufgabe kann über den System Manager oder die ONTAP CLI ausgeführt werden.

System Manager

1. Im Ziel-Cluster auf **Schutz > Beziehungen** klicken.
2. Unter **Beziehungen** auf **Schützen** klicken und **Storage VMs (DR)** auswählen.
3. Wählen Sie eine Datensicherungsstrategie. Wenn Sie eine benutzerdefinierte Datensicherungsstrategie erstellt haben, wählen Sie diese aus und anschließend den Quell-Cluster sowie die Speicher-VM, die repliziert werden soll. Es besteht auch die Möglichkeit, eine neue Ziel-Speicher-VM zu erstellen, indem ein neuer Name für die Speicher-VM eingegeben wird.
4. Bei Bedarf lassen sich die Zieleinstellungen ändern, um die Identitätsbeibehaltung zu überschreiben sowie Netzwerkschnittstellen und Protokolle ein- oder auszuschließen.
5. Auf **Speichern** klicken.

CLI

1. Erstellen einer Ziel-SVM:

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   Der SVM-Name muss sowohl im Quell-Cluster als auch im Ziel-Cluster eindeutig sein.

   Das folgende Beispiel erstellt eine Ziel-SVM mit dem Namen `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

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

2. Vom Quell-Cluster aus eine SVM Peer-Beziehung mit dem `vserver peer create` Befehl erstellen.

   Weitere Informationen finden sich unter "Erstellen einer SVM Intercluster Peer-Beziehung".

   Weitere Informationen zu `vserver peer create` finden sich in der "ONTAP-Befehlsreferenz".

3. Erstellen eines Replikationsauftragszeitplans:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Für `-month`, `-dayofweek` und `-hour` kann `all` angegeben werden, damit der Job jeden Monat, an jedem Wochentag bzw. zu jeder Stunde ausgeführt wird.

> Der minimal unterstützte Zeitplan (RPO) für FlexVol Volumes in einer SVM SnapMirror Beziehung beträgt 15 Minuten. Der minimal unterstützte Zeitplan (RPO) für FlexGroup Volumes in einer SVM SnapMirror Beziehung beträgt 30 Minuten.

Das folgende Beispiel erstellt einen Jobplan mit dem Namen `my_weekly`, der samstags um 3:00 Uhr morgens ausgeführt wird:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

Weitere Informationen zu `job schedule cron create` finden sich in der "ONTAP-Befehlsreferenz".

4. Vom Ziel-SVM oder Ziel-Cluster aus eine Replikationsbeziehung erstellen:

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination -path` Optionen einen Doppelpunkt (:) eingeben.

Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung unter Verwendung der Standard `MirrorAllSnapshots`richtlinie:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

Das folgende Beispiel erstellt eine einheitliche Replikationsbeziehung mit der Standard `MirrorAndVault`richtlinie:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp `async-mirror` erstellt, erstellt das folgende Beispiel eine SnapMirror DR-Beziehung:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp `mirror-vault` erstellt, erzeugt das folgende Beispiel eine einheitliche Replikationsbeziehung:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

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

5. Die Ziel-SVM anhalten:

```
vserver stop -vserver <SVM_name>
```

Das folgende Beispiel stoppt eine Ziel-SVM mit dem Namen svm_backup:

```
cluster_dst::> vserver stop -vserver svm_backup
```

Weitere Informationen zu `vserver stop` finden sich in der "ONTAP-Befehlsreferenz".

6. Vom Ziel-SVM oder Ziel-Cluster aus die SVM-Replikationsbeziehung initialisieren:

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination -path` Optionen einen Doppelpunkt (:) eingeben.

Das folgende Beispiel initialisiert die Beziehung zwischen der Quell-SVM, `svm1`, und der Ziel-SVM, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

LIFs und Netzwerkeinstellungen von ONTAP SnapMirror SVM-Replikation ausschließen

Wenn sich Quell- und Ziel-SVMs in unterschiedlichen Subnetzen befinden, kann die `-discard-configs network` Option des `snapmirror policy create` Befehls verwendet werden, um LIFs und zugehörige Netzwerkeinstellungen von der SVM-Replikation auszuschließen.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

Weitere Informationen finden Sie unter "Erstellen einer Cluster Peer-Beziehung" und "Erstellen einer SVM Intercluster Peer-Beziehung".

Über diese Aufgabe

Die `-identity-preserve`Option des `snapmirror create`Befehls muss auf `true`gesetzt werden, wenn die SVM-Replikationsbeziehung erstellt wird.

Schritte

1. Erstellen einer Ziel-SVM:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

   Der SVM-Name muss sowohl im Quell-Cluster als auch im Ziel-Cluster eindeutig sein.

   Das folgende Beispiel erstellt eine Ziel-SVM mit dem Namen `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Vom Ziel-Cluster aus eine SVM Peer-Beziehung mit dem `vserver peer create` Befehl erstellen.

   Weitere Informationen finden sich unter "Erstellen einer SVM Intercluster Peer-Beziehung".

   Weitere Informationen zu `vserver peer create` finden sich in der "ONTAP-Befehlsreferenz".

3. Einen Arbeitszeitplan erstellen:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Für `-month`, `-dayofweek` und `-hour` kann `all` angegeben werden, damit der Job jeden Monat, an jedem Wochentag bzw. zu jeder Stunde ausgeführt wird.

   > Der minimal unterstützte Zeitplan (RPO) für FlexVol Volumes in einer SVM SnapMirror Beziehung beträgt 15 Minuten. Der minimal unterstützte Zeitplan (RPO) für FlexGroup Volumes in einer SVM SnapMirror Beziehung beträgt 30 Minuten.

   Das folgende Beispiel erstellt einen Jobplan mit dem Namen `my_weekly`, der samstags um 3:00 Uhr morgens ausgeführt wird:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   ```

```
"Saturday" -hour 3 -minute 0
```

4. Erstellen einer benutzerdefinierten Replikationsrichtlinie:

   `snapmirror policy create -vserver SVM -policy policy -type async-mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

   Das folgende Beispiel erstellt eine benutzerdefinierte Replikationsrichtlinie für SnapMirror DR, die LIFs ausschließt:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_exclude_LIFs -type async-mirror -discard-configs network
   ```

   Das folgende Beispiel erstellt eine benutzerdefinierte Replikationsrichtlinie für die einheitliche Replikation, die LIFs ausschließt:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   unified_exclude_LIFs -type mirror-vault -discard-configs network
   ```

   > Es empfiehlt sich, dieselbe benutzerdefinierte SnapMirror-Richtlinie auf dem Quell-Cluster für zukünftige Failover- und Failback-Szenarien zu erstellen.

   Weitere Informationen zu `snapmirror policy create` finden sich in der "ONTAP-Befehlsreferenz".

5. Von der Ziel-SVM oder dem Ziel-Cluster aus den folgenden Befehl ausführen, um eine Replikationsbeziehung zu erstellen:

   `snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve true|false -discard -configs true|false`

   > Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Die folgenden Beispiele veranschaulichen dies.

   Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung, die LIFs ausschließt:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
   -identity-preserve true
   ```

   Das folgende Beispiel erstellt eine SnapMirror einheitliche Replikationsbeziehung, die LIFs ausschließt:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   ```

```
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
-identity-preserve true -discard-configs true
```

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

6. Die Ziel-SVM anhalten:

   `vserver stop`

   `SVM name`

   Das folgende Beispiel stoppt die Ziel-SVM mit dem Namen svm_backup:

```
cluster_dst::> vserver stop -vserver svm_backup
```

7. Vom Ziel-SVM oder Ziel-Cluster aus eine Replikationsbeziehung initialisieren:

   `snapmirror initialize -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Das folgende Beispiel initialisiert die Beziehung zwischen der Quelle, `svm1` und dem Ziel, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

   Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Das Netzwerk und die Protokolle auf der Ziel-SVM sind für den Datenzugriff im Katastrophenfall zu konfigurieren.

Verwandte Informationen

- "Eine ONTAP SnapMirror SVM-Replikationsbeziehung kann so umgewandelt werden, dass SVM-Konfigurationsinformationen einbezogen werden."
- "snapmirror create"
- "snapmirror initialize"
- "snapmirror policy create"

Netzwerk- und Namensdiensteinstellungen von der ONTAP SVM Replikation ausschließen

Es kann sinnvoll sein, Netzwerk-, Namensdienst- und andere Einstellungen von einer SVM-Replikationsbeziehung auszuschließen, um Konflikte oder Konfigurationsunterschiede mit der Ziel-SVM zu vermeiden.

Die `-identity-preserve false` Option des `snapmirror create` Befehls ermöglicht die Replikation ausschließlich der Volume- und Sicherheitskonfigurationen einer SVM. Einige Protokoll- und Namensdiensteinstellungen werden ebenfalls beibehalten.

Über diese Aufgabe

Eine Liste der gespeicherten Protokoll- und Namensdiensteinstellungen ist unter "Konfigurationen, die in SVM DR-Beziehungen repliziert werden" zu finden.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster sowie die SVMs müssen miteinander verbunden sein.

Weitere Informationen finden Sie unter "Erstellen einer Cluster Peer-Beziehung" und "Erstellen einer SVM Intercluster Peer-Beziehung".

Schritte

1. Erstellen einer Ziel-SVM:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

   Der SVM-Name muss sowohl im Quell-Cluster als auch im Ziel-Cluster eindeutig sein.

   Das folgende Beispiel erstellt eine Ziel-SVM mit dem Namen `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Vom Ziel-Cluster aus eine SVM Peer-Beziehung mit dem `vserver peer create` Befehl erstellen.

   Weitere Informationen finden sich unter "Erstellen einer SVM Intercluster Peer-Beziehung".

   Weitere Informationen zu `vserver peer create` finden sich in der "ONTAP-Befehlsreferenz".

3. Erstellen eines Replikationsauftragszeitplans:

   `job schedule cron create -name` *`job_name`* `-month` *`month`* `-dayofweek` *`day_of_week`* `-day` *`day_of_month`* `-hour` *`hour`* `-minute` *`minute`*

   Für `-month`, `-dayofweek` und `-hour` kann `all` angegeben werden, damit der Job jeden Monat, an jedem Wochentag bzw. zu jeder Stunde ausgeführt wird.

   > Der minimal unterstützte Zeitplan (RPO) für FlexVol Volumes in einer SVM SnapMirror Beziehung beträgt 15 Minuten. Der minimal unterstützte Zeitplan (RPO) für FlexGroup Volumes in einer SVM SnapMirror Beziehung beträgt 30 Minuten.

   Das folgende Beispiel erstellt einen Jobplan mit dem Namen `my_weekly`, der samstags um 3:00 Uhr morgens ausgeführt wird:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Eine Replikationsbeziehung erstellen, die Netzwerk-, Namensdienst- und andere Konfigurationseinstellungen ausschließt:

   `snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP`

```
-schedule schedule -policy policy -identity-preserve false
```

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Die folgenden Beispiele veranschaulichen dies. Dieser Befehl muss von der Ziel-SVM oder dem Ziel-Cluster ausgeführt werden.

Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung mithilfe der Standard `MirrorAllSnapshots`richtlinie. Die Beziehung schließt Netzwerk-, Namensdienst- und andere Konfigurationseinstellungen von der SVM-Replikation aus:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

Das folgende Beispiel erstellt eine einheitliche Replikationsbeziehung mithilfe der Standard `MirrorAndVault`richtlinie. Die Beziehung schließt Netzwerk-, Namensdienst- und andere Konfigurationseinstellungen aus:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp `async-mirror` erstellt, erstellt das folgende Beispiel eine SnapMirror DR-Beziehung. Die Beziehung schließt Netzwerk-, Namensdienst- und andere Konfigurationseinstellungen von der SVM-Replikation aus:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp `mirror-vault` erstellt, erstellt das folgende Beispiel eine einheitliche Replikationsbeziehung. Die Beziehung schließt Netzwerk-, Namensdienst- und andere Konfigurationseinstellungen von der SVM-Replikation aus:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

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

5. Die Ziel-SVM anhalten:

   `vserver stop`

   SVM name

Das folgende Beispiel stoppt eine Ziel-SVM namens dvs1:

```
destination_cluster::> vserver stop -vserver dvs1
```

6. Wenn Sie SMB verwenden, muss auch ein SMB-Server konfiguriert werden.

   Siehe "Nur SMB: Erstellen eines SMB-Servers".

7. Vom Ziel-SVM oder Ziel-Cluster aus die SVM-Replikationsbeziehung initialisieren:

   `snapmirror initialize -source-path SVM_name: -destination-path SVM_name:`

   Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Das Netzwerk und die Protokolle auf der Ziel-SVM sind für den Datenzugriff im Katastrophenfall zu konfigurieren.

Konvertierung einer ONTAP SnapMirror SVM-Beziehung zur Einbeziehung von SVM-Einstellungen

Sie können eine SVM DR-Beziehung, die SVM-Konfigurationsinformationen während der Replikation ausschließt, mithilfe des `-identity-preserve true` Parameters in eine Beziehung umwandeln, die die Konfigurationsinformationen repliziert.

Bevor Sie beginnen

Wenn derzeit SnapMirror-Transfers laufen, entweder abwarten, bis diese abgeschlossen sind, oder sie abbrechen.

Schritte

1. Vom Ziel-Cluster aus die Beziehung stilllegen:

   `snapmirror quiesce -destination-path <destination_svm>:`

2. Wenn der Beziehungsstatus auf „ruhend“ gesetzt ist, löschen Sie die Beziehung vom Ziel-Cluster aus:

   `snapmirror delete -destination-path <destination_svm>:`

3. Vom Quell-Cluster die Beziehung freigeben, ohne SnapMirror Snapshot-Informationen zu löschen:

   ```
   snapmirror release -destination-path <destination_svm>: -relationship-info
   -only true
   ```

4. Vom Ziel aus die Replikationsbeziehung mit `-identity-preserve true` erneut erstellen:

   ```
   snapmirror create -source-path <source_svm>: -destination-path
   <destination_svm>: -policy <policy> -schedule <schedule> -identity-preserve
   true
   ```

5. Vom Ziel-Cluster aus die SnapMirror Beziehung neu synchronisieren:

   `snapmirror resync -destination-path <destination_svm>:`

Lokale Ebenen zur Verwendung für ONTAP SnapMirror SVM DR-Beziehungen angeben

Nachdem eine SVM für die Notfallwiederherstellung erstellt wurde, kann mit der `aggr-list` Option des `vserver modify` Befehls eingeschränkt werden, welche lokalen Tiers zum Hosten der SVM DR Ziel-Volumes verwendet werden.

Schritte

1. Erstellen einer Ziel-SVM:

   ```
   vserver create -vserver SVM -subtype dp-destination
   ```

2. Die aggr-list der Disaster-Recovery-SVM wird angepasst, um die lokalen Tiers einzuschränken, die zum Hosten des Volumes der Disaster-Recovery-SVM verwendet werden:

   ```
   cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
   ```

Erstellung eines SMB-Servers für eine ONTAP SnapMirror Ziel-SVM

Wenn die Quell-SVM über eine SMB-Konfiguration verfügt und Sie `identity-preserve` auf `false` gesetzt haben, ist ein SMB-Server für die Ziel-SVM zu erstellen. Ein SMB-Server ist für einige SMB-Konfigurationen erforderlich, beispielsweise für Freigaben während der Initialisierung der SnapMirror Beziehung.

Schritte

1. Die Ziel-SVM wird mit dem `vserver start` Befehl gestartet.

   ```
   destination_cluster::> vserver start -vserver dvs1
   [Job 30] Job succeeded: DONE
   ```

   Weitere Informationen zu `vserver start` finden sich in der "ONTAP-Befehlsreferenz".

2. Es sollte überprüft werden, ob sich die Ziel-SVM im `running` Zustand befindet und der Subtyp `dp-destination` ist, indem der `vserver show` Befehl verwendet wird.

   ```
   destination_cluster::> vserver show
                                       Admin      Operational Root
   Vserver  Type    Subtype            State      State       Volume
   Aggregate
   -------- ------- ----------       ---------- ----------- ----------
   ----------
   dvs1     data    dp-destination    running    running       -         -
   ```

   Weitere Informationen zu `vserver show` finden sich in der "ONTAP-Befehlsreferenz".

3. Eine LIF wird mit dem `network interface create` Befehl erstellt.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

4. Eine Route kann mithilfe des `network route create` Befehls erstellt werden.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Netzwerkmanagement"

Weitere Informationen zu `network route create` finden sich in der "ONTAP-Befehlsreferenz".

5. DNS kann mithilfe des `vserver services dns create` Befehls konfiguriert werden.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

Weitere Informationen zu `vserver services dns create` finden sich in der "ONTAP-Befehlsreferenz".

6. Der bevorzugte Domänencontroller wird mit dem `vserver cifs domain preferred-dc add` Befehl hinzugefügt.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

Weitere Informationen zu `vserver cifs domain preferred-dc add` finden sich in der "ONTAP-Befehlsreferenz".

7. Der SMB-Server wird mit dem `vserver cifs create` Befehl erstellt.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

Weitere Informationen zu `vserver cifs create` finden sich in der "ONTAP-Befehlsreferenz".

8. Die Ziel-SVM wird mit dem `vserver stop` Befehl angehalten.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Weitere Informationen zu `vserver stop` finden sich in der "ONTAP-Befehlsreferenz".

Ausschließen von Volumes aus einer ONTAP SnapMirror SVM DR-Beziehung

Standardmäßig werden alle RW-Datenvolumes der Quell-SVM repliziert. Wenn nicht alle Volumes der Quell-SVM geschützt werden sollen, kann die `-vserver-dr-protection unprotected` Option des `volume modify` Befehls verwendet werden, um Volumes von der SVM-Replikation auszuschließen.

Schritte

1. Ein Volume von der SVM-Replikation ausschließen:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

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

   Im folgenden Beispiel wird das Volume `volA_src` von der SVM-Replikation ausgeschlossen:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

   Wenn Sie später ein Volume in die SVM-Replikation einbeziehen möchten, das Sie ursprünglich ausgeschlossen haben, führen Sie den folgenden Befehl aus:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection protected`

   Das folgende Beispiel beinhaltet das Volumen `volA_src` in der SVM-Replikation:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

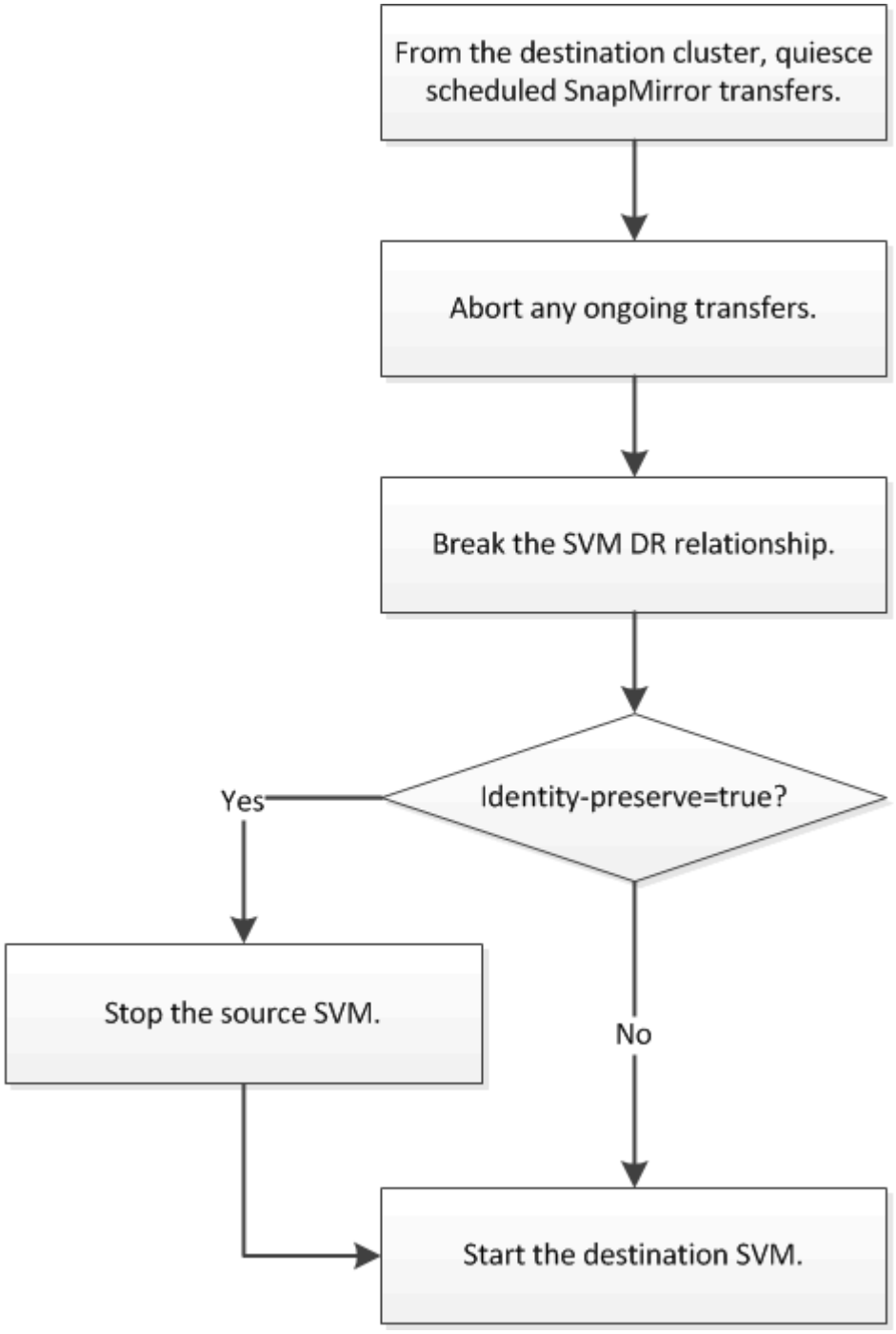
2. Die SVM-Replikationsbeziehung wird erstellt und initialisiert, wie in "Replikation einer gesamten SVM-Konfiguration" beschrieben.

Daten von einem SnapMirror SVM DR Ziel bereitstellen

ONTAP SnapMirror SVM-Workflow zur Notfallwiederherstellung

Um sich von einem Ausfall zu erholen und Daten vom Ziel-SVM bereitzustellen, muss das Ziel-SVM aktiviert werden. Die Aktivierung des Ziel-SVM umfasst das Stoppen geplanter SnapMirror-Transfers, das Abbrechen laufender SnapMirror-Transfers, das

Aufheben der Replikationsbeziehung, das Stoppen des Quell-SVM und das Starten des Ziel-SVM.



Das ONTAP SnapMirror SVM Zielvolume als beschreibbar konfigurieren

Die SVM-Zielvolumes müssen beschreibbar sein, bevor Daten an Clients bereitgestellt werden können.

Das Verfahren ist weitgehend identisch mit dem Verfahren für die Volume-Replikation, mit einer Ausnahme. Wenn `-identity-preserve true` beim Erstellen der SVM-Replikationsbeziehung gesetzt wurde, muss die Quell-SVM gestoppt werden, bevor die Ziel-SVM aktiviert wird.

Über diese Aufgabe

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

> In einem Disaster-Recovery-Szenario kann kein SnapMirror Update von der Quell-SVM zur Disaster-Recovery-Ziel-SVM durchgeführt werden, da Ihre Quell-SVM und deren Daten nicht zugänglich sind und Updates seit der letzten Resynchronisierung möglicherweise fehlerhaft oder beschädigt sind.

Ab ONTAP 9.8 kann mit dem System Manager eine Ziel-Storage-VM nach einem Ausfall aktiviert werden. Durch die Aktivierung der Ziel-Storage-VM werden die SVM-Zielvolumes beschreibbar und ermöglichen die Bereitstellung von Daten für Clients.

Schritte

Diese Aufgabe kann über den System Manager oder die ONTAP CLI ausgeführt werden.

System Manager

1. Wenn der Quell-Cluster erreichbar ist, lässt sich überprüfen, ob die SVM gestoppt ist: Unter **Storage > Storage VMs** in der Spalte **State** für die SVM nachsehen.
2. Wenn der Status der Quell-SVM „Running“ ist, diese anhalten: ⋮ und **Stop** auswählen.
3. Im Ziel-Cluster die gewünschte Schutzbeziehung suchen: **Schutz > Beziehungen** auswählen.
4. Fahren Sie mit dem Mauszeiger über den gewünschten Namen der Quell-Speicher-VM, klicken Sie auf ⋮ und wählen Sie **Ziel-Speicher-VM aktivieren**.
5. Im Fenster **Ziel-Speicher-VM aktivieren** die Option **Ziel-Speicher-VM aktivieren und Beziehung aufheben** auswählen.
6. Auf **Aktivieren** klicken.

CLI

1. Vom Ziel-SVM oder Ziel-Cluster aus den SVM in den Ruhezustand versetzen, um geplante Übertragungen zum Ziel zu stoppen:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination -path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel stoppt geplante Übertragungen zwischen der Quell-SVM `svm1` und der Ziel-SVM `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

Weitere Informationen zu `snapmirror quiesce` finden sich in der "ONTAP-Befehlsreferenz".

2. Vom Ziel-SVM oder Ziel-Cluster aus laufende Übertragungen zum Ziel anhalten:

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel stoppt laufende Übertragungen zwischen der Quell-SVM `svm1` und der Ziel-SVM `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

Weitere Informationen zu `snapmirror abort` finden sich in der "ONTAP-Befehlsreferenz".

3. Von der Ziel-SVM oder dem Ziel-Cluster aus die Replikationsbeziehung aufheben:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel unterbricht die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

4. Wenn `-identity-preserve true` beim Erstellen der SVM-Replikationsbeziehung festgelegt wurde, sollte die Quell-SVM gestoppt werden:

```
vserver stop -vserver <SVM>
```

Das folgende Beispiel stoppt die Quell-SVM `svm1`:

```
cluster_src::> vserver stop svm1
```

5. Die Ziel-SVM wird gestartet:

```
vserver start -vserver <SVM>
```

Das folgende Beispiel startet die Ziel-SVM `svm_backup`:

```
cluster_dst::> vserver start svm_backup
```

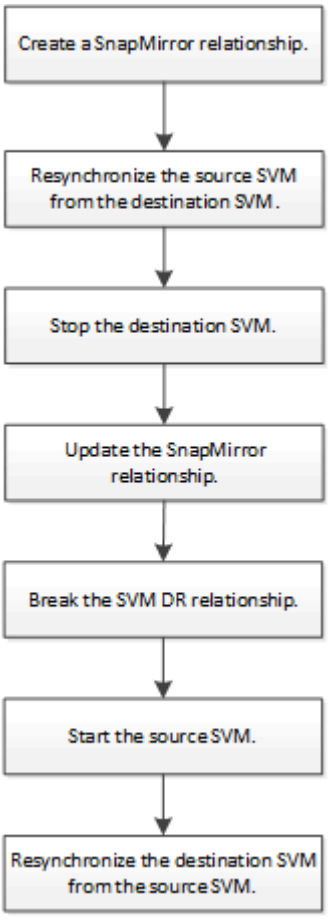
Nachdem Sie fertig sind

SVM Ziel-Volumes für den Datenzugriff konfigurieren, wie in "Konfiguration des Zielvolumes für den Datenzugriff" beschrieben.

Die SnapMirror Quelle-SVM reaktivieren

ONTAP SnapMirror Quelle SVM Reaktivierungs-Workflow

Wenn die Quell-SVM nach einem Katastrophenfall noch existiert, kann sie reaktiviert und geschützt werden, indem die SVM-Katastrophenwiederherstellungsbeziehung wiederhergestellt wird.



Die ursprüngliche ONTAP SnapMirror Quelle-SVM reaktivieren

Sie können die ursprüngliche Datensicherungsbeziehung zwischen Quell-SVM und Ziel-SVM wiederherstellen, wenn keine Daten mehr vom Ziel-SVM bereitgestellt werden müssen. Das Verfahren ist weitgehend identisch mit dem Verfahren für die Volume-Replikation, mit einer Ausnahme. Der Ziel-SVM muss gestoppt werden, bevor der Quell-SVM reaktiviert wird.

Bevor Sie beginnen

- Wenn Sie die Größe des Ziel-Volumes erhöht haben, während Sie davon Daten bereitgestellt haben, sollten Sie max-autosize auf dem ursprünglichen Quell-Volume manuell erhöhen, bevor Sie das Quell-Volume reaktivieren, damit es ausreichend wachsen kann.

"Wenn ein Zielvolumen automatisch wächst"

> Zur Vermeidung von Datenverlust sollten die Clientanwendungen angehalten werden, bevor die ursprüngliche Quelle reaktiviert wird. Wenn die Ziel-SVM gestoppt wird, kommt es bei den Clientanwendungen zu einer E/A-Unterbrechung, bis die Quell-SVM wieder aktiviert wird.

Über diese Aufgabe

Ab ONTAP 9.11.1 können Sie die Resynchronisierungszeit während einer Disaster-Recovery-Probe verkürzen, indem Sie die CLI `-quick-resync true` Option des `snapmirror resync` Befehls bei einer umgekehrten Resynchronisierung einer SVM DR Beziehung verwenden. Eine schnelle Resynchronisierung kann die Zeit bis zur Rückkehr in den Produktivbetrieb verkürzen, indem die Vorgänge für Neuaufbau und Wiederherstellung des Data Warehouse umgangen werden. Weitere Informationen zu `snapmirror resync` finden Sie im "ONTAP-Befehlsreferenz".

> Die schnelle Resynchronisierung erhält die Speichereffizienz der Ziel-Volumes nicht. Durch Aktivieren der schnellen Resynchronisierung kann sich der von den Ziel-Volumes belegte Speicherplatz erhöhen.

Dieses Verfahren setzt voraus, dass die Baseline im ursprünglichen Quell-Volume intakt ist. Falls die Baseline nicht intakt ist, muss die Beziehung zwischen dem Volume, von dem Daten bereitgestellt werden, und dem ursprünglichen Quellvolume erstellt und initialisiert werden, bevor das Verfahren durchgeführt wird.

Ab ONTAP 9.8 ist es möglich, mit System Manager eine Quell-Storage-VM nach einem Ausfall zu reaktivieren.

Schritte

Diese Aufgabe kann mit dem System Manager oder der ONTAP CLI ausgeführt werden.

System Manager ONTAP 9.17.1 und höher

1. Auf dem Ziel-Cluster steht die gewünschte Schutzbeziehung unter **Schutz > Replikation** zur Auswahl.
2. Wenn Sie den Mauszeiger über den Quellnamen bewegen, können Sie ⋮ und anschließend **Resynchronisierung umkehren** auswählen.
3. Im Fenster **Umgekehrte Resynchronisierungsbeziehung** wird **Umgekehrte Resynchronisierung** ausgewählt.

   Die Beziehung verschwindet aus der **Replikationstabelle** und wird nun vom ursprünglichen Quell-Cluster verwaltet.

4. Auf dem ursprünglichen Quell-Cluster ist unter **Protection > Replication** erkennbar, ob die umgekehrte Resynchronisierung abgeschlossen ist; der Status muss **Mirrored** anzeigen.
5. Im ursprünglichen Ziel-Cluster zu **Cluster > Storage VMs** navigieren.
6. Nachdem Sie die Storage VM lokalisiert haben, bewegen Sie den Mauszeiger über den Namen der Storage VM, wählen ⋮ und anschließend **Stop**.
7. Im Fenster **Stop storage VM** erfolgt die Auswahl von **Stop**.
8. Auf dem Quell-Cluster unter **Protection > Replication** die Storage VM suchen, die reaktiviert werden soll, den Mauszeiger über den Namen der Storage VM bewegen, ⋮ auswählen und anschließend **Activate destination storage VM** auswählen.
9. Im Fenster **Ziel-Storage-VM aktivieren** wird zunächst **Ziel-Storage-VM aktivieren und Beziehung aufheben** und anschließend **Aktivieren** ausgewählt.
10. Wenn Sie zur Seite **Replikation** zurückkehren, bewegen Sie den Mauszeiger erneut über den Namen der Storage-VM, wählen Sie ⋮ und anschließend **Umgekehrte Resynchronisierung** aus.

System Manager ONTAP 9.16.1 und früher

1. Auf dem Ziel-Cluster lässt sich die gewünschte Schutzbeziehung über **Schutz > Beziehungen** auswählen.
2. Wenn Sie den Mauszeiger über den Quellnamen bewegen, können Sie ⋮ und anschließend **Resynchronisierung umkehren** auswählen.
3. Im Fenster **Umgekehrte Resynchronisierungsbeziehung** wird **Umgekehrte Resynchronisierung** ausgewählt.

   Die Beziehung verschwindet aus der Tabelle **Relationships**, da sie nun vom ursprünglichen Quell-Cluster verwaltet wird.

4. Wählen Sie im ursprünglichen Quell-Cluster **Schutz > Beziehungen** aus, und vergewissern Sie sich, dass die umgekehrte Resynchronisierung abgeschlossen ist, indem Sie prüfen, ob der Status als **Gespiegelt** angezeigt wird.
5. Navigieren Sie im ursprünglichen Ziel-Cluster zu **Storage > Storage VMs**.
6. Nachdem Sie die Storage VM lokalisiert haben, bewegen Sie den Mauszeiger über den Namen der Storage VM, wählen ⋮ und anschließend **Stop**.
7. Im Fenster **Stop storage VM** erfolgt die Auswahl von **Stop**.
8. Auf dem Quell-Cluster ist die Storage VM zu lokalisieren, die nun die Quell-SVM der umgekehrten Beziehung ist. Der Cursor ist über den SVM-Namen zu bewegen, ⋮ ist auszuwählen, und **Activate destination storage VM** ist auszuwählen.
9. Im Fenster **Ziel-Storage-VM aktivieren** erfolgt die Auswahl von **Ziel-Storage-VM aktivieren und Beziehung aufheben** und anschließend von **Aktivieren**.
10. Nach der Rückkehr zur Seite **Beziehungen** den Mauszeiger erneut auf den Namen der Storage VM bewegen, ⋮ auswählen und anschließend **Umgekehrte Resynchronisierung** auswählen.

CLI

1. Ausgehend von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster wird eine umgekehrte SVM DR-Beziehung mit derselben Konfiguration, Richtlinie und Einstellung zur Identitätserhaltung wie bei der ursprünglichen SVM DR-Beziehung erstellt:

   ```
   snapmirror create -source-path <SVM>: -destination-path <SVM>:
   ```

Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel stellt eine Beziehung zwischen der SVM, von der Sie Daten bereitstellen, `svm_backup`, und der ursprünglichen Quell-SVM, `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

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

2. Vom ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster aus wird der folgende Befehl ausgeführt, um die Datenschutzbeziehung umzukehren:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden.

Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein gemeinsamer Snapshot vorhanden ist. `snapmirror initialize` kann verwendet werden, um die Beziehung neu zu initialisieren.

Das folgende Beispiel kehrt die Beziehung zwischen der ursprünglichen Quell-SVM, `svm1`, und der SVM, von der Daten bereitgestellt werden, `svm_backup` um:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

Beispiel für die Verwendung der Option -quick-resync:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. Wenn der Datenzugriff auf die ursprüngliche Quell-SVM wiederhergestellt werden soll, wird die ursprüngliche Ziel-SVM gestoppt, um alle derzeit mit der ursprünglichen Ziel-SVM verbundenen Clients zu trennen.

```
vserver stop -vserver <SVM>
```

Das folgende Beispiel stoppt die ursprüngliche Ziel-SVM, die aktuell Daten bereitstellt:

```
cluster_dst::> vserver stop svm_backup
```

4. Es sollte mithilfe des `vserver show` Befehls überprüft werden, ob sich die ursprüngliche Ziel-SVM im gestoppten Zustand befindet.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- --------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. Vom ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster aus wird der folgende Befehl ausgeführt, um die endgültige Aktualisierung der umgekehrten Beziehung durchzuführen und alle Änderungen vom ursprünglichen Ziel-SVM auf den ursprünglichen Quell-SVM zu übertragen:

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination -path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel aktualisiert die Beziehung zwischen der ursprünglichen Ziel-SVM, über die Sie Daten bereitstellen, `svm_backup`, und der ursprünglichen Quell-SVM, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

Weitere Informationen zu `snapmirror update` finden sich in der "ONTAP-Befehlsreferenz".

6. Führen Sie auf der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster den folgenden Befehl aus, um geplante Übertragungen für die umgekehrte Beziehung zu stoppen:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel stoppt geplante Übertragungen zwischen der SVM, von der Sie Daten bereitstellen, `svm_backup`, und der ursprünglichen SVM, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. Wenn das letzte Update abgeschlossen ist und die Beziehung den Beziehungsstatus „Quiesced“ anzeigt, muss der folgende Befehl auf der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden, um die umgekehrte Beziehung aufzuheben:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel unterbricht die Beziehung zwischen dem ursprünglichen Ziel-SVM, von dem Sie Daten bereitgestellt haben, `svm_backup`, und dem ursprünglichen Quell-SVM, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

8. Falls die ursprüngliche Quell-SVM zuvor gestoppt wurde, starten Sie die ursprüngliche Quell-SVM vom ursprünglichen Quell-Cluster aus:

```
vserver start -vserver <SVM>
```

Das folgende Beispiel startet die ursprüngliche Quell-SVM:

```
cluster_src::> vserver start svm1
```

9. Vom ursprünglichen Ziel-SVM oder vom ursprünglichen Ziel-Cluster wird die ursprüngliche Datensicherungsbeziehung wiederhergestellt:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel stellt die Beziehung zwischen der ursprünglichen Quell-SVM, `svm1`, und der ursprünglichen Ziel-SVM, `svm_backup` wieder her:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. Führen Sie auf der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster den folgenden Befehl aus, um die umgekehrte Datensicherungsbeziehung zu löschen:

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel löscht die umgekehrte Beziehung zwischen der ursprünglichen Ziel-SVM, `svm_backup`, und der ursprünglichen Quell-SVM, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. Vom ursprünglichen Ziel-SVM oder vom ursprünglichen Ziel-Cluster die umgekehrte Datensicherungsbeziehung freigeben:

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel hebt die umgekehrte Beziehung zwischen der ursprünglichen Ziel-SVM, `svm_backup`, und der ursprünglichen Quell-SVM, `svm1` auf.

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

Was kommt als Nächstes

- Mit dem `snapmirror show`Befehl lässt sich überprüfen, ob die SnapMirror Beziehung erstellt wurde.

  Weitere Informationen zu `snapmirror show` finden sich in der "ONTAP-Befehlsreferenz".

- Die Schreibvorgänge von Ihrem Client zur ursprünglichen Quell-SVM werden wieder aufgenommen.

Verwandte Informationen

- "snapmirror create"
- "snapmirror delete"
- "snapmirror initialize"
- "snapmirror quiesce"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"

Die ursprüngliche ONTAP SnapMirror Quelle-SVM für FlexGroup Volumes wird reaktiviert

Sie können die ursprüngliche Datensicherungsbeziehung zwischen Quell-SVM und Ziel-SVM wiederherstellen, wenn keine Daten mehr vom Ziel-SVM bereitgestellt werden müssen. Um die ursprüngliche Quell-SVM bei Verwendung von FlexGroup Volumes zu reaktivieren, sind zusätzliche Schritte erforderlich, einschließlich des Löschens der ursprünglichen SVM DR-Beziehung und des Freigebens der ursprünglichen Beziehung, bevor die Beziehung umgekehrt wird. Auch die umgekehrte Beziehung muss freigegeben und die ursprüngliche Beziehung wiederhergestellt werden, bevor geplante Übertragungen gestoppt werden.

Schritte

1. Vom ursprünglichen Ziel-SVM oder vom ursprünglichen Ziel-Cluster die ursprüngliche SVM-DR-Beziehung löschen:

   ```
   snapmirror delete -source-path SVM: -destination-path SVM:
   ```

   > Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

   Das folgende Beispiel löscht die ursprüngliche Beziehung zwischen der ursprünglichen Quell-SVM, svm1, und der ursprünglichen Ziel-SVM, `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. Vom ursprünglichen Quell-SVM oder vom ursprünglichen Quell-Cluster wird die ursprüngliche Beziehung freigegeben, wobei die Snapshots intakt bleiben:

   ```
   snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
   -only true
   ```

   > Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path`

Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel gibt die ursprüngliche Beziehung zwischen der ursprünglichen Quell-SVM, svm1, und der ursprünglichen Ziel-SVM `svm_backup` frei.

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. Ausgehend von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster wird eine umgekehrte SVM DR-Beziehung mit derselben Konfiguration, Richtlinie und Einstellung zur Identitätserhaltung wie bei der ursprünglichen SVM DR-Beziehung erstellt:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

   Das folgende Beispiel stellt eine Beziehung zwischen der SVM, von der Sie Daten bereitstellen, `svm_backup`, und der ursprünglichen Quell-SVM, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

4. Vom ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster aus wird der folgende Befehl ausgeführt, um die Datenschutzbeziehung umzukehren:

   `snapmirror resync -source-path SVM: -destination-path SVM:`

   Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

   Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden.

   Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein gemeinsamer Snapshot vorhanden ist. `snapmirror initialize` kann verwendet werden, um die Beziehung neu zu initialisieren.

   Das folgende Beispiel kehrt die Beziehung zwischen der ursprünglichen Quell-SVM, `svm1`, und der SVM, von der Daten bereitgestellt werden, `svm_backup` um:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

5. Wenn der Datenzugriff auf die ursprüngliche Quell-SVM wiederhergestellt werden soll, wird die ursprüngliche Ziel-SVM gestoppt, um alle derzeit mit der ursprünglichen Ziel-SVM verbundenen Clients zu

trennen.

`vserver stop -vserver SVM`

Das folgende Beispiel stoppt die ursprüngliche Ziel-SVM, die aktuell Daten bereitstellt:

```
cluster_dst::> vserver stop svm_backup
```

6. Es sollte mithilfe des `vserver show` Befehls überprüft werden, ob sich die ursprüngliche Ziel-SVM im gestoppten Zustand befindet.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

7. Vom ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster aus wird der folgende Befehl ausgeführt, um die endgültige Aktualisierung der umgekehrten Beziehung durchzuführen und alle Änderungen vom ursprünglichen Ziel-SVM auf den ursprünglichen Quell-SVM zu übertragen:

`snapmirror update -source-path SVM: -destination-path SVM:`

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel aktualisiert die Beziehung zwischen der ursprünglichen Ziel-SVM, von der Sie Daten bereitstellen ,`svm_backup`, und der ursprünglichen Quell-SVM, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

Weitere Informationen zu `snapmirror update` finden sich in der "ONTAP-Befehlsreferenz".

8. Führen Sie auf der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster den folgenden Befehl aus, um geplante Übertragungen für die umgekehrte Beziehung zu stoppen:

`snapmirror quiesce -source-path SVM: -destination-path SVM:`

> Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

Das folgende Beispiel stoppt geplante Übertragungen zwischen der SVM, von der Sie Daten bereitstellen,

`svm_backup`, und der ursprünglichen SVM, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

Weitere Informationen zu `snapmirror quiesce` finden sich in der "ONTAP-Befehlsreferenz".

9. Wenn das letzte Update abgeschlossen ist und die Beziehung den Beziehungsstatus „Quiesced“ anzeigt, muss der folgende Befehl auf der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausgeführt werden, um die umgekehrte Beziehung aufzuheben:

   `snapmirror break -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

   Das folgende Beispiel unterbricht die Beziehung zwischen dem ursprünglichen Ziel-SVM, von dem Sie Daten bereitgestellt haben, `svm_backup`, und dem ursprünglichen Quell-SVM, `svm1`:

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

   Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

10. Falls die ursprüngliche Quell-SVM zuvor gestoppt wurde, starten Sie die ursprüngliche Quell-SVM vom ursprünglichen Quell-Cluster aus:

    `vserver start -vserver` *`SVM`*

    Das folgende Beispiel startet die ursprüngliche Quell-SVM:

    ```
    cluster_src::> vserver start svm1
    ```

11. Löschen Sie von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster die umgekehrte SVM DR-Beziehung:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

    Das folgende Beispiel löscht die umgekehrte Beziehung zwischen der ursprünglichen Ziel-SVM, svm_backup, und der ursprünglichen Quell-SVM, `svm1`:

    ```
    cluster_src::> snapmirror delete -source-path svm_backup: -destination
    ```

```
-path svm1:
```

12. Vom ursprünglichen Ziel-SVM oder vom ursprünglichen Ziel-Cluster die umgekehrte Beziehung freigeben, wobei die Snapshots intakt bleiben:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

    Das folgende Beispiel löst die umgekehrte Beziehung zwischen der ursprünglichen Ziel-SVM, svm_backup, und der ursprünglichen Quell-SVM, svm1, auf:

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1: -relationship-info-only true
    ```

13. Stellen Sie vom ursprünglichen Ziel-SVM oder vom ursprünglichen Ziel-Cluster aus die ursprüngliche Beziehung wieder her. Es wird dieselbe Konfiguration, Richtlinie und Einstellung zur Identitätsbeibehaltung wie bei der ursprünglichen SVM DR-Beziehung verwendet.

    `snapmirror create -source-path SVM: -destination-path SVM:`

    Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

    Das folgende Beispiel stellt eine Beziehung zwischen der ursprünglichen Quell-SVM, `svm1`, und der ursprünglichen Ziel-SVM, `svm_backup` her:

    ```
    cluster_dst::> snapmirror create -source-path svm1: -destination-path
    svm_backup:
    ```

14. Vom ursprünglichen Ziel-SVM oder vom ursprünglichen Ziel-Cluster wird die ursprüngliche Datensicherungsbeziehung wiederhergestellt:

    `snapmirror resync -source-path *SVM*: -destination-path *SVM*:`

    Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

    Das folgende Beispiel stellt die Beziehung zwischen der ursprünglichen Quell-SVM, `svm1`, und der ursprünglichen Ziel-SVM, `svm_backup` wieder her:

    ```
    cluster_dst::> snapmirror resync -source-path svm1: -destination-path
    svm_backup:
    ```

Verwandte Informationen

- "snapmirror create"
- "snapmirror delete"
- "snapmirror initialize"
- "snapmirror quiesce"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"

Die Daten auf einer ONTAP SnapMirror Ziel-SVM werden erneut synchronisiert

Sie können die Daten und Konfigurationsdetails von der Quell Storage VM zur Ziel Storage VM in einer unterbrochenen Schutzbeziehung resynchronisieren und die Beziehung wiederherstellen.

ONTAP 9.11.1 bietet die Möglichkeit, bei einer Notfallwiederherstellungsübung den kompletten Neuaufbau des Data Warehouse zu umgehen, sodass eine schnellere Rückkehr zur Produktion möglich ist.

Ab ONTAP 9.20.1 können Sie in der ONTAP CLI mit FlexGroup Bestandteilen in SVM-DR-Beziehungen die `quick-resync` Option verwenden. ONTAP System Manager bietet keine quick resync option für reverse resync.

Die Resynchronisierung wird nur vom Ziel der ursprünglichen Beziehung aus durchgeführt. Dabei werden alle Daten in der Ziel-Speicher-VM gelöscht, die neuer sind als die Daten in der Quell-Speicher-VM.

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um diese Aufgabe auszuführen.

System Manager

1. Im Ziel-Cluster die gewünschte Schutzbeziehung auswählen: **Schutz > Beziehungen** anklicken.
2. Optional kann **Schnelle Resynchronisierung durchführen** ausgewählt werden, um einen vollständigen Neuaufbau des Data Warehouse während einer Notfallwiederherstellungsübung zu umgehen.
3. Klicken Sie auf ⋮ und dann auf **Neu synchronisieren**.
4. Unter **Beziehungen** lässt sich der Fortschritt der Resynchronisierung überwachen, indem der **Übertragungsstatus** für die Beziehung angezeigt wird.

CLI

1. Vom Ziel-Cluster aus die Beziehung neu synchronisieren:

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

Verwandte Informationen

- "SnapMirror Resynchronisierung"

Konvertieren einer ONTAP SnapMirror Volumenbeziehung zu einer SVM-Beziehung

Es ist möglich, Replikationsbeziehungen zwischen Volumes in eine Replikationsbeziehung zwischen den Storage Virtual Machines (SVMs), denen die Volumes gehören, zu konvertieren, sofern jedes Volume auf dem Quell-Cluster (außer dem Root-Volume) repliziert wird und jedes Volume auf dem Quell-Cluster (einschließlich des Root-Volumes) denselben Namen wie das Volume auf dem Ziel-Cluster hat.

Über diese Aufgabe

Der `volume rename` Befehl kann verwendet werden, wenn die SnapMirror Beziehung inaktiv ist, um Ziel-Volumes bei Bedarf umzubenennen. Weitere Informationen zu `volume rename` finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Von der Ziel-SVM oder dem Ziel-Cluster aus den folgenden Befehl ausführen, um die Quell- und Ziel-Volumes neu zu synchronisieren:

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

   Weitere Informationen zu `snapmirror resync` finden sich in der "ONTAP-Befehlsreferenz".

   > Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden.

   Das folgende Beispiel synchronisiert die Beziehung zwischen dem Quellvolume `volA` auf `svm1` und dem Zielvolume `volA` auf `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. Eine SVM-Replikationsbeziehung zwischen der Quell-SVM und der Ziel-SVM wird erstellt, wie in "Replikation von SVM Konfigurationen" beschrieben.

   Sie müssen die `-identity-preserve true` Option des `snapmirror create` Befehls verwenden, wenn Sie Ihre Replikationsbeziehung erstellen.

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

3. Die Ziel-SVM anhalten:

   ```
   vserver stop -vserver SVM
   ```

   Weitere Informationen zu `vserver stop` finden sich in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel stoppt die Ziel-SVM `svm_backup`:

```
cluster_dst::> vserver stop svm_backup
```

4. Von der Ziel-SVM oder dem Ziel-Cluster aus den folgenden Befehl ausführen, um die Quell- und Ziel-SVMs neu zu synchronisieren:

   `snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP -policy <policy>`

   > Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.
   >
   > Obwohl für die Resynchronisierung kein Basistransfer erforderlich ist, kann sie zeitaufwändig sein. Die Resynchronisierung kann außerhalb der Spitzenzeiten durchgeführt werden.

   Das folgende Beispiel synchronisiert die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Verwandte Informationen

- "snapmirror create"
- "SnapMirror Resynchronisierung"

Ändern der Zielvolumenkapazität in einer ONTAP SVM DR Beziehung

Ab ONTAP 9.20.1 können Storage-Administratoren und Datensicherungsadministratoren einige Volumenkapazitätsattribute auf einem SVM DR Zielvolume anpassen, um die Grenzen der automatischen Größenanpassung des Ziels an das Wachstum der Quelle anzupassen, die Snapshot-Reserve für die Aufbewahrung des Ziels zu erhöhen, und Serviceprovider-Administratoren können mandantenfähige DR-Kunden auf der Grundlage der Zielkapazität präzise managen.

Anpassen der maximalen Größe, auf die SVM DR Ziel-Volumes automatisch anwachsen können

Schritte

1. Um den maximalen Wert der automatischen Größenanpassung des Volumes zu ändern, wird der folgende Befehl eingegeben:

   `volume modify -vserver <dest svm name> -volume <vol name> -max-autosize <integer>`

   Beispiel:

```
volume modify -vserver svmdr_dst -volume vol1 -max-autosize 10TB
```

Anpassen der Mindestgröße, auf die SVM DR Volumes automatisch verkleinert werden können

1. Zum Ändern des Mindestwerts der automatischen Größenanpassung eines Volumes ist der folgende Befehl einzugeben:

   ```
   volume modify -vserver <dest svm name> -volume vol1 -min-autosize <integer>
   ```

   Beispiel:

   ```
   volume modify -vserver svmdr_dst -volume vol1 -min-autosize 1TB
   ```

Modus der automatischen Größenanpassung des Volume ändern

1. Zum Ändern des Modus für die automatische Größenanpassung dient der folgende Befehl:

   ```
   volume modify -vserver svmdr_dst -volume vol1 -autosize-mode
   ```

   Beispiel:

   ```
   volume modify -vserver svmdr_dst -volume vol1 -autosize-mode grow
   ```

Anpassung des für Snapshots reservierten Speicherplatzes

1. Zum Ändern des Prozentsatzes des für Snapshots reservierten Speicherplatzes dient der folgende Befehl:

   ```
   volume modify -vserver <dest svm name> -volume <vol name> -percent-snapshot
   -space <integer>
   ```

   Beispiel:

   ```
   volume modify -vserver svmdr_dst -volume vol1 -percent-snapshot-space 25
   ```

Löschen einer ONTAP SnapMirror SVM-Replikationsbeziehung

Sie können die `snapmirror delete` und `snapmirror release` Befehle verwenden, um eine SVM-Replikationsbeziehung zu löschen. Anschließend können nicht mehr benötigte Ziel-Volumes manuell gelöscht werden. Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Der `snapmirror release`Befehl löscht alle von SnapMirror erstellten Snapshots aus der Quelle. Mit der `-relationship-info-only`Option besteht die Möglichkeit, die Snapshots zu erhalten.

Schritte

1. Der folgende Befehl ist auf der Ziel-SVM oder dem Ziel-Cluster auszuführen, um die Replikationsbeziehung zu unterbrechen:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

   Das folgende Beispiel unterbricht die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM `svm_backup`:

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

   Weitere Informationen zu `snapmirror break` finden sich in der "ONTAP-Befehlsreferenz".

2. Der folgende Befehl ist auf der Ziel-SVM oder dem Ziel-Cluster auszuführen, um die Replikationsbeziehung zu löschen:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

   Das folgende Beispiel löscht die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

   Weitere Informationen zu `snapmirror delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Der folgende Befehl wird auf dem Quell-Cluster oder der Quell-SVM ausgeführt, um die Replikationsbeziehungsinformationen von der Quell-SVM zu lösen:

   `snapmirror release -source-path SVM: -destination-path SVM:`

   > Sie müssen nach dem SVM-Namen in den `-source-path` und `-destination-path` Optionen einen Doppelpunkt (:) eingeben. Das folgende Beispiel verdeutlicht dies.

   Das folgende Beispiel gibt Informationen für die angegebene Replikationsbeziehung von der Quell-SVM `svm1` frei:

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

Weitere Informationen zu `snapmirror release` finden sich in der "ONTAP-Befehlsreferenz".

Replikation des SnapMirror Stammvolumes verwalten

Informationen zur Replikation des ONTAP SnapMirror Root-Volumes

Jede SVM in einer NAS-Umgebung verfügt über einen eindeutigen Namensraum. Das SVM-Root-Volume ist der Einstiegspunkt in diese Namensraumhierarchie. Bei Clustern mit zwei oder mehr HA-Paaren sollten Sie Load-Sharing Mirrors (LSMs) des SVM-Root-Volumes in Betracht ziehen, um sicherzustellen, dass der Namensraum für Clients auch dann zugänglich bleibt, wenn beide Knoten eines HA-Paares ausfallen. Load-Sharing Mirrors sind nicht für Cluster mit nur einem HA-Paar geeignet und sind nicht für eine MetroCluster-Umgebung geeignet.

- Ab ONTAP 9.1 sind Load-Sharing-Mirrors für Datavolumes veraltet und werden nur noch für SVM-Root-Volumes unterstützt.
- SnapMirror Load-Sharing-Mirror sind nur in der Lage, NAS-Clients (CIFS/NFSv3) zu unterstützen. Load-Sharing-Mirror unterstützen keine NFSv4-Clients oder SAN-Client-Protokollverbindungen (FC, FCoE oder iSCSI). NFSv4 und Load-Sharing-Mirror können jedoch in derselben Umgebung koexistieren.

ONTAP Load-Sharing Mirror-Beziehungen erstellen und initialisieren

Für jedes SVM Root Volume, das NAS-Daten im Cluster bereitstellt, sollte ein Load-Sharing Mirror (LSM) erstellt werden. Bei Clustern, die aus zwei oder mehr HA-Paaren bestehen, empfiehlt sich die Verwendung von Load-Sharing Mirrors der SVM Root Volumes, damit der Namespace für Clients auch dann zugänglich bleibt, wenn beide Nodes eines HA-Paares ausfallen. Load-Sharing Mirrors sind für Cluster, die nur aus einem HA-Paar bestehen, nicht geeignet.

Bevor Sie beginnen

Ab ONTAP 9.16.1 kann beim Erstellen einer Load-Sharing-Mirror-Beziehung für die Ziel-SVM kein Speicherlimit aktiviert sein.

Über diese Aufgabe

Wenn Sie ein LSM auf demselben Knoten erstellen und dieser Knoten nicht verfügbar ist, entsteht ein Single Point of Failure, und es gibt keine zweite Kopie, um die Daten für Clients weiterhin zugänglich zu halten. Wenn das LSM jedoch auf einem anderen Knoten als dem mit dem Root Volume oder auf einem anderen HA-Paar erstellt wird, sind die Daten auch im Falle eines Ausfalls weiterhin zugänglich.

Beispielsweise in einem Vier-Node-Cluster mit einem Root-Volume auf drei Knoten:

- Für das Root-Volume auf HA 1 Knoten 1 das LSM auf HA 2 Knoten 1 oder HA 2 Knoten 2 erstellen.
- Für das Root-Volume auf HA 1 Knoten 2 ist das LSM auf HA 2 Knoten 1 oder HA 2 Knoten 2 zu erstellen.
- Für das Root-Volume auf HA 2 Knoten 1 ist das LSM auf HA 1 Knoten 1 oder HA 1 Knoten 2 zu erstellen.

Schritte

1. Ein Ziel-Volume für den LSM erstellen:

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

Das Zielvolume sollte mindestens so groß sein wie das Stammvolume.

Es ist eine Best Practice, das Root- und das Ziel-Volume mit Suffixen wie `_root` und `_m1` zu benennen.

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

Das folgende Beispiel erstellt ein Load-Sharing Mirror Volume für das Root-Volume `svm1_root` in `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Einen Replikationsauftragszeitplan erstellen".
3. Eine Load-Sharing-Mirror-Beziehung zwischen dem SVM-Root-Volume und dem Ziel-Volume für das LSM erstellen:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

Das folgende Beispiel erstellt eine Load-Sharing-Mirror-Beziehung zwischen dem Root-Volume `svm1_root` und dem Load-Sharing-Mirror-Volume `svm1_m1`:

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

Das Attribut „type“ des Load-Sharing-Mirrors ändert sich von `DP` zu `LS`.

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

4. Den Load-Sharing-Spiegel initialisieren:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

Das folgende Beispiel initialisiert den Load-Sharing Mirror für das Root-Volume `svm1_root`:

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

Weitere Informationen zu `snapmirror initialize` finden sich in der "ONTAP-Befehlsreferenz".

Aktualisierung einer ONTAP Load-Sharing Mirror Beziehung

Load-sharing Mirror (LSM) Beziehungen werden für SVM Root Volumes automatisch aktualisiert, nachdem ein Volume in der SVM eingebunden oder ausgehängt wurde, und während `volume create` Vorgängen, die die `junction-path` Option enthalten. Eine LSM Beziehung kann manuell aktualisiert werden, wenn eine Aktualisierung vor dem nächsten geplanten Update gewünscht ist.

Lastverteilungs-Spiegelbeziehungen werden in den folgenden Fällen automatisch aktualisiert:

- Es ist Zeit für ein planmäßiges Update
- Ein Mount- oder Unmount-Vorgang wird auf einem Volume im SVM Root-Volume durchgeführt.
- Ein `volume create` Befehl wird ausgeführt, der die `junction-path` Option enthält

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

Schritt

1. Eine Load-Sharing Mirror Beziehung manuell aktualisieren:

   Vor dem Ausführen dieses Befehls sind die Variablen in spitzen Klammern durch die erforderlichen Werte zu ersetzen.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   Das folgende Beispiel aktualisiert die Load-Sharing Mirror Beziehung für das Root-Volume `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

   Weitere Informationen zu `snapmirror update` finden sich in der "ONTAP-Befehlsreferenz".

Eine ONTAP Load-Sharing Mirror befördern

Wenn ein Root-Volume dauerhaft nicht verfügbar ist, kann das Load-Sharing Mirror (LSM) Volume hochgestuft werden, um Schreibzugriff auf die Daten des Root-Volumes bereitzustellen.

Bevor Sie beginnen

Für diese Aufgabe müssen Sie Befehle auf dem erweiterten Berechtigungsniveau verwenden.

Schritte

1. Wechsel zum erweiterten Berechtigungslevel:

   ```
   set -privilege advanced
   ```

2. Ein LSM-Volumen promoten:

Vor dem Ausführen dieses Befehls sind die Variablen in spitzen Klammern durch die erforderlichen Werte zu ersetzen.

```
snapmirror promote -destination-path <SVM:volume>
```

Im folgenden Beispiel wird das Volume `svm1_m2` als neues SVM Root Volume festgelegt:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Drücken Sie `y`. ONTAP macht das LSM-Volume zu einem lesen/schreiben-Volume und löscht das ursprüngliche Root-Volume, falls dieses zugänglich ist.

> Das neu hochgestufte Root-Volume enthält möglicherweise nicht alle Daten, die sich im ursprünglichen Root-Volume befanden, wenn die letzte Aktualisierung nicht kürzlich erfolgte.

Weitere Informationen zu `snapmirror promote` finden sich in der "ONTAP-Befehlsreferenz".

3. Zurück zur Administrator-Berechtigungsebene:

```
set -privilege admin
```

4. Das hochgestufte Volume ist gemäß der Namenskonvention umzubenennen, die für das Root-Volume verwendet wurde:

   Vor dem Ausführen dieses Befehls sind die Variablen in spitzen Klammern durch die erforderlichen Werte zu ersetzen.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   Im folgenden Beispiel wird das hochgestufte Volume `svm1_m2` mit dem Namen `svm1_root` umbenannt:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Das umbenannte Root-Volume wird geschützt, wie in Schritt 3 bis Schritt 4 in "Erstellen und Initialisieren von Load-Sharing Mirror-Beziehungen" beschrieben.

In die Cloud sichern

Installation einer ONTAP SnapMirror Cloud-Lizenz

SnapMirror Cloud-Beziehungen können mithilfe vorqualifizierter Backup-Anwendungen von Drittanbietern orchestriert werden. Ab ONTAP 9.9.1 ist es auch möglich, die SnapMirror Cloud-Replikation mit System Manager zu orchestrieren. Sowohl SnapMirror- als auch SnapMirror Cloud-Kapazitätslizenzen sind erforderlich, wenn mit System Manager On-Premises ONTAP-Backups auf Objektspeicher orchestriert werden. Außerdem ist es notwendig, die SnapMirror Cloud-API-Lizenz anzufordern und zu installieren.

Über diese Aufgabe

Die SnapMirror cloud- und SnapMirror S3-Lizenzen sind Clusterlizenzen, keine Node-Lizenzen, daher werden sie nicht mit dem ONTAP One Lizenzbundle geliefert. Diese Lizenzen sind im separaten ONTAP One Compatibility Bundle enthalten. Für die Aktivierung von SnapMirror cloud ist die Anforderung dieses Bundles erforderlich.

Zusätzlich erfordert die System Manager Orchestrierung von SnapMirror Cloud-Backups in Objektspeicher einen SnapMirror Cloud-API-Schlüssel. Diese API-Lizenz ist eine clusterweite Einzelinstanzlizenz, das bedeutet, sie muss nicht auf jedem Knoten im Cluster installiert werden.

Schritte

Es ist erforderlich, das ONTAP One Kompatibilitätspaket und die SnapMirror Cloud-API-Lizenz anzufordern und herunterzuladen und diese anschließend mit System Manager zu installieren.

1. Die Cluster-UUID für den Cluster, der lizenziert werden soll, ermitteln und notieren.

   Die Cluster-UUID wird benötigt, wenn Sie Ihre Anfrage zur Bestellung des ONTAP One Compatibility bundle für Ihren Cluster einreichen.

2. Das NetApp Vertriebsteam kann kontaktiert werden, um das ONTAP One Kompatibilitätspaket anzufordern.
3. Die SnapMirror Cloud-API-Lizenz kann gemäß den Anweisungen auf der NetApp Support Site angefordert werden.

   "Lizenzschlüssel für die SnapMirror Cloud-API anfordern"

4. Nachdem Sie die Lizenzdateien erhalten und heruntergeladen haben, kann der System Manager verwendet werden, um die ONTAP Cloud Compatibility NLF und die SnapMirror cloud API NLF in den Cluster hochzuladen:
   a. **Cluster > Einstellungen** auswählen.
   b. Im Fenster **Einstellungen** auf **Lizenzen** klicken.
   c. Im Fenster **Lizenzen** auf + Add klicken.
   d. Im Dialogfeld **Lizenz hinzufügen** auf **Durchsuchen** klicken, um die heruntergeladene NLF auszuwählen, und anschließend auf **Hinzufügen** klicken, um die Datei in den Cluster hochzuladen.

Verwandte Informationen

"Daten mit SnapMirror in der Cloud sichern"

"NetApp Softwarelizenzsuche"

Daten in der Cloud mit ONTAP SnapMirror Cloud sichern

SnapMirror Cloud bietet ONTAP Replikation auf Objektspeicherziele. Dies ermöglicht es Ihnen, ältere Backup-to-Tape-Architekturen durch Objektspeicher für die langfristige Datenaufbewahrung und Archivierung zu ersetzen. Sie können Anbieter wie Amazon S3, Alibaba Cloud, Azure Blob, Google Cloud Storage, IBM Cloud Object Storage, NetApp StorageGRID oder ONTAP S3 als Ihren Cloud-Objektspeicher verwenden.

SnapMirror Cloud-Replikation, die von System Manager verwaltet wird, unterstützt ausschließlich StorageGrid und ONTAP S3 als Objektspeicherziel. Andere Anbieter werden nicht unterstützt.

Die Unterstützung für SnapMirror Cloud-Replikation zu anderen Objektspeicheranbietern mit anderen Backup und Recovery-Produkten variiert. Informationen zu den Supportrichtlinien erhalten Sie von Ihrem Drittanbieter.

Die Nutzung der SnapMirror Cloud-APIs ist grundsätzlich auf Backup-Partner beschränkt. Kunden, die eigene API-basierte Lösungen entwickeln möchten, erhalten Informationen zu den Lizenzbedingungen über ihr NetApp Account-Team.

Ab ONTAP 9.20.1:

- Ab ONTAP 9.20.1 unterstützt SnapMirror cloud Wiederherstellung vor Ort für FlexVol Volumes, wodurch die direkte Wiederherstellung eines Cloud-Snapshots auf das ursprüngliche Quell-Volume möglich ist. ONTAP wählt automatisch den neuesten gemeinsamen Snapshot aus und überträgt nur das Delta vom Objektspeicher auf den angeforderten Ziel-Snapshot, wodurch eine vollständige Baseline-Wiederherstellung vermieden wird.

Ab ONTAP 9.19.1:

- SnapMirror Cloud erhöht die Anzahl der pro Cluster unterstützten S3-Objektspeicher-Buckets von 6 auf 100. Diese Begrenzung gilt für die Gesamtzahl der Objektspeicher, die über alle SnapMirror Cloud Objektspeicher-Endpunkte auf einem ONTAP Cluster konfiguriert sind. Bei der Nutzung dieser Funktion sind folgende Aspekte zu berücksichtigen:
  - Wenn Sie mehr als 6 Buckets pro Cluster verwenden, sollten Sie die Virtual-Hosted-Style-URL-Konfiguration für Anbieter nutzen, die dies unterstützen, einschließlich AWS S3, Alibaba Cloud, StorageGrid, Google Cloud Storage, IBM Cloud Object Storage, ONTAP S3 und andere S3-kompatible Anbieter. Diese Konfiguration wird empfohlen, um eine skalierbare Adressierung des Objektspeichers zu ermöglichen und zugrunde liegende Einschränkungen zu vermeiden.
  - Die Wiederherstellung bei Bedarf ist standardmäßig aktiviert.
  - Die Latenz von Lesevorgängen während bedarfsgesteuerter Wiederherstellungen kann höher sein, je nachdem, wie viele gleichzeitige Wiederherstellungen im System aktiv sind.

Ab ONTAP 9.18.1:

- SnapMirror Cloud unterstützt Backup- und Recovery-Operationen für FlexGroup Volumes auf MetroCluster Konfigurationen unter Verwendung des bestehenden "ONTAP REST-APIs". Diese Funktionalität ermöglicht die Erstellung von SnapMirror Cloud-Beziehungen für FlexGroup Volumes auf MetroCluster

Konfigurationen, die nach einem Switchover und Switchback vom Partnerstandort aus verwaltet werden.

Vor der Nutzung der SnapMirror Cloud-Funktion empfiehlt es sich, einen SnapMirror Cloud-API-Lizenzschlüssel von der NetApp Support Site anzufordern: "Lizenzschlüssel für die SnapMirror Cloud API anfordern".

Gemäß den Anweisungen ist eine kurze Beschreibung Ihres Geschäftsvorhabens bereitzustellen und der API-Schlüssel durch eine E-Mail an die angegebene Adresse anzufordern. Innerhalb von 24 Stunden sollte eine E-Mail-Antwort mit weiteren Anweisungen zum Erwerb des API-Schlüssels eingehen.

Sie benötigen möglicherweise sowohl einen SnapMirror Cloud Lizenzschlüssel als auch einen API-Schlüssel. ONTAP One enthält zwar die SnapMirror Cloud Lizenz selbst, der Lizenzschlüssel ist jedoch erforderlich, um die SnapMirror Cloud Funktion zu aktivieren. Der Lizenzschlüssel muss gegebenenfalls separat generiert und installiert werden.

Einen Cloud-Objektspeicher hinzufügen

Bevor Sie SnapMirror Cloud-Backups konfigurieren, müssen Sie einen StorageGRID oder ONTAP S3 Cloud-Objektspeicher hinzufügen.

Schritte

1. **Schutz > Übersicht > Cloud-Objektspeicher** auswählen.
2. Klicken Sie + Add .

Sicherung mit der Standardrichtlinie

Sie können schnell ein SnapMirror Cloud-Backup für ein vorhandenes Volume mit der standardmäßigen Cloud-Datensicherungsstrategie, DailyBackup, konfigurieren.

Schritte

1. **Schutz > Übersicht** auswählen und **Volumes in der Cloud sichern** wählen.
2. Wenn Sie zum ersten Mal ein Backup in der Cloud erstellen, geben Sie Ihren SnapMirror Cloud-API-Lizenzschlüssel wie angegeben in das Lizenzfeld ein.
3. **Authentifizieren und fortfahren** auswählen.
4. Wählen Sie ein Quellvolume aus.
5. Einen Cloud Objektspeicher auswählen.
6. Auf **Speichern** klicken.

Erstellen einer benutzerdefinierten Cloud Backup-Richtlinie

Wenn Sie nicht die Standard-Cloud-Richtlinie DailyBackup für Ihre SnapMirror Cloud-Backups verwenden möchten, kann eine eigene Richtlinie erstellt werden.

Schritte

1. **Schutz > Übersicht > Lokale Richtlinieneinstellungen** auswählen und **Schutzrichtlinien** selektieren.
2. Auf **Hinzufügen** klicken und die Details der neuen Richtlinie eingeben.
3. Im Abschnitt **Richtlinientyp In der Cloud sichern** auswählen, um anzugeben, dass eine Cloud-Richtlinie erstellt wird.
4. Auf **Speichern** klicken.

Eine Sicherung kann auf der Seite Volumes erstellt werden.

Die Seite **Volumes** im System Manager kann verwendet werden, wenn Cloud-Backups für mehrere Volumes gleichzeitig ausgewählt und erstellt werden sollen oder wenn eine benutzerdefinierte Datensicherungsstrategie genutzt wird.

Schritte

1. **Speicher > Volumes** auswählen.
2. Wählen Sie die Volumes aus, die Sie in der Cloud sichern möchten, und klicken Sie auf **Protect**.
3. Im Fenster **Volume schützen** auf **Weitere Optionen** klicken.
4. Eine Richtlinie auswählen.

   Sie können die Standardrichtlinie DailyBackup oder eine von Ihnen erstellte benutzerdefinierte Cloud-Richtlinie auswählen.

5. Einen Cloud Objektspeicher auswählen.
6. Auf **Speichern** klicken.

Wiederherstellung aus der Cloud

Mit dem System Manager ist es möglich, gesicherte Daten aus dem Cloud-Speicher auf ein anderes Volume im Quell-Cluster wiederherzustellen.

> Wenn Sie ONTAP 9.16.1 oder höher verwenden und eine SnapMirror Cloud-Einzeldateiwiederherstellung auf ein FlexGroup Volume durchführen, sollten Dateien nur in ein neues Verzeichnis im FlexGroup Volume wiederhergestellt werden, und Granulare Daten muss auf `advanced` auf dem Ziel-FlexGroup Volume gesetzt sein. Weitere Informationen zum Festlegen der `-granular-data advanced` Option finden sich unter "Erweiterten Kapazitätsausgleich auf ONTAP FlexGroup Volumes aktivieren".

Schritte

1. Im Quell-Cluster einer SnapMirror-to-Cloud-Beziehung auf **Storage > Volumes** klicken.
2. Wählen Sie das Volume aus, das Sie wiederherstellen möchten.
3. Die Registerkarte **In der Cloud sichern** auswählen.
4. Klicken Sie ⋮ neben das Quellvolume, das Sie wiederherstellen möchten, um das Menü anzuzeigen, und wählen Sie **Wiederherstellen**.
5. Unter **Quelle** eine Storage-VM auswählen und anschließend den Namen des Volumes eingeben, auf das die Daten wiederhergestellt werden sollen.
6. Unter **Ziel** den Snapshot auswählen, der wiederhergestellt werden soll.
7. Auf **Speichern** klicken.

Eine SnapMirror Cloud-Beziehung löschen

Mit dem System Manager lässt sich eine Cloud-Beziehung löschen.

Schritte

1. Klicken Sie auf **Speicher > Volumes** und wählen Sie das Volume aus, das Sie löschen möchten.
2. Klicken Sie ⋮ neben das Quellvolume und wählen Sie **Löschen**.

3. **Cloud Objektspeicher-Endpunkt löschen (optional)** kann ausgewählt werden, wenn der Cloud Objektspeicher-Endpunkt gelöscht werden soll.
4. Klicken Sie auf **Delete**.

Entfernen eines Cloud-Objektspeichers

Sie können den System Manager verwenden, um einen Cloud Objektspeicher zu entfernen, sofern dieser nicht Teil einer Cloud Backup Beziehung ist. Wenn ein Cloud Objektspeicher Teil einer Cloud Backup Beziehung ist, kann er nicht gelöscht werden.

Schritte

1. **Schutz > Übersicht > Cloud-Objektspeicher** auswählen.
2. Wählen Sie den Objektspeicher, den Sie löschen möchten, klicken Sie auf ⋮ und wählen Sie **Löschen**.

Sicherung von ONTAP Daten mit NetApp Backup and Recovery

Ab ONTAP 9.19.1 unterstützt System Manager die Datensicherung in der Cloud mit dem NetApp Backup and Recovery Service nicht mehr. Stattdessen müssen Sie die NetApp Console verwenden, um den NetApp Backup and Recovery Service zu konfigurieren und eine SnapMirror Beziehung zu einem Cloud-Ziel herzustellen.

Backup and Recovery unterstützt FlexVol Read-Write-Volumes und Data-Protection-Volumes (DP-Volumes). Ab ONTAP 9.12.1 unterstützt Backup and Recovery FlexGroup Volumes und SnapLock Volumes.

Weitere Informationen zu "NetApp Backup and Recovery".

Bevor Sie beginnen

Sie sollten die folgenden Verfahren durchführen, um ein Konto in der NetApp Console einzurichten. Für das Dienstkonto ist die Rolle „Account Admin“ zu erstellen.

1. "Ein Konto in der NetApp Console erstellen".
2. "Einen Console-Agenten in der NetApp Console erstellen" mit einem der folgenden Cloud-Anbieter:
   - Microsoft Azure
   - Amazon Web Services (AWS)
   - Google Cloud Platform (GCP)
   - StorageGRID (ONTAP 9.10.1)

   > ⓘ Ab ONTAP 9.10.1 kann StorageGRID als Cloud-Backup-Anbieter ausgewählt werden, jedoch nur, wenn die NetApp Console lokal bereitgestellt ist. Der Console-Agent muss lokal installiert und über die NetApp Console Software-as-a-Service (SaaS) Anwendung verfügbar sein.

3. "NetApp Backup and Recovery in der NetApp Console abonnieren" (erfordert die entsprechende Lizenz).
4. "Einen Zugriffsschlüssel und einen geheimen Schlüssel mithilfe der NetApp Console generieren".

Verwenden Sie NetApp Console und NetApp Backup and Recovery, um ONTAP-Backups zu verwalten.

Ab ONTAP 9.19.1 unterstützt System Manager NetApp Backup and Recovery nicht mehr. Siehe "Verwalten Sie Backups für Ihre ONTAP-Systeme mit NetApp Backup and Recovery" für weitere Informationen zur

Verwendung von NetApp Backup and Recovery mit NetApp Console.

Daten aus Sicherungsdateien wiederherstellen

Sie können Backup-Management-Vorgänge wie das Wiederherstellen von Daten, das Aktualisieren von Beziehungen und das Löschen von Beziehungen nur bei Verwendung der NetApp Console durchführen. Weitere Informationen finden Sie unter "Wiederherstellen von Daten aus Sicherungsdateien".

Archivierung und Compliance mithilfe von SnapLock Technologie

Erfahren Sie mehr über ONTAP SnapLock

SnapLock ist eine leistungsstarke Compliance-Lösung für Organisationen, die WORM-Speicher verwenden, um Dateien für regulatorische und Governance-Zwecke unverändert aufzubewahren.

SnapLock hilft dabei, das Löschen, Ändern oder Umbenennen von Daten zu verhindern, um Vorschriften wie SEC 17a-4(f), HIPAA, FINRA, CFTC und DSGVO zu erfüllen. Mit SnapLock können spezielle Volumes erstellt werden, in denen Dateien gespeichert und entweder für einen festgelegten Aufbewahrungszeitraum oder unbegrenzt in einen nicht löschbaren, nicht beschreibbaren Zustand versetzt werden können. SnapLock ermöglicht diese Aufbewahrung auf Dateiebene über standardisierte offene Dateiprotokolle wie CIFS und NFS. Die unterstützten offenen Dateiprotokolle für SnapLock sind NFS (Versionen 2, 3 und 4) und CIFS (SMB 1.0, 2.0 und 3.0).

Mit SnapLock werden Dateien und Snapshots im WORM-Speicher abgelegt und Aufbewahrungsfristen für WORM-geschützte Daten festgelegt. SnapLock WORM-Speicher nutzt die NetApp Snapshot-Technologie und kann SnapMirror Replikation sowie SnapVault Backups als Basistechnologie für den Backup-Wiederherstellungsschutz von Daten nutzen. Weitere Informationen zu WORM-Speicher: "Konforme WORM-Speicherung mit NetApp SnapLock - TR-4526".

Eine Anwendung kann verwendet werden, um Dateien über NFS oder CIFS an WORM zu übergeben, oder die SnapLock Autocommit-Funktion kann genutzt werden, um Dateien automatisch an WORM zu übergeben. Eine *WORM-anhängbare Datei* kann verwendet werden, um inkrementell geschriebene Daten wie Protokollinformationen zu speichern. Weitere Informationen finden Sie unter "Den Volume-Append-Modus verwenden, um WORM-anhängbare Dateien zu erstellen".

SnapLock unterstützt Datenschutzmethoden, die die meisten Compliance-Anforderungen erfüllen sollten:

- Mit SnapLock für SnapVault lassen sich Snapshots auf sekundärem Speicher WORM-schützen. Siehe "Snapshots in WORM übernehmen".
- Mit SnapMirror können WORM-Dateien zur Notfallwiederherstellung an einen anderen geografischen Standort repliziert werden. Siehe "WORM-Dateien spiegeln".

SnapLock ist eine lizenzbasierte Funktion von ONTAP. Eine einzelne Lizenz berechtigt zur Nutzung von SnapLock im strikten Compliance-Modus, um externe Vorgaben wie SEC Rule 17a-4(f) zu erfüllen, sowie im weniger restriktiven Enterprise-Modus, um interne Vorschriften zum Schutz digitaler Assets einzuhalten. SnapLock-Lizenzen sind Bestandteil der "ONTAP One" Software-Suite.

SnapLock wird auf allen AFF und FAS Systemen sowie ONTAP Select unterstützt. SnapLock ist keine reine Softwarelösung, sondern eine integrierte Hardware- und Softwarelösung. Diese Unterscheidung ist wichtig für strenge WORM-Vorschriften wie SEC 17a-4(f), die eine integrierte Hardware- und Softwarelösung erfordern.

Weitere Informationen finden sich unter "SEC-Leitfaden für Broker-Dealer zur Verwendung elektronischer Speichermedien".

Was Sie mit SnapLock machen können

Nach der Konfiguration von SnapLock können die folgenden Aufgaben abgeschlossen werden:

- "Dateien in WORM übernehmen"
- "Snapshots für den Sekundärspeicher in WORM übernehmen"
- "WORM-Dateien für die Notfallwiederherstellung spiegeln"
- "WORM-Dateien während eines Rechtsstreits mit Legal Hold aufbewahren"
- "WORM-Dateien mit der Funktion „Privilegiertes Löschen“ entfernen"
- "Die Aufbewahrungsfrist für Dateien festlegen"
- "Ein SnapLock Volume verschieben"
- "Einen Snapshot zum Schutz vor Ransomware-Angriffen sperren"
- "Überprüfung der Nutzung von snapLock mit dem Revisionsprotokoll"
- "SnapLock APIs verwenden"

SnapLock Compliance- und Enterprise-Modi

SnapLock Compliance- und Enterprise-Modi unterscheiden sich hauptsächlich darin, auf welcher Ebene jeder Modus WORM-Dateien schützt:

SnapLock Modus	Schutzstufe	WORM-Dateilöschung während der Aufbewahrung
Konformitätsmodus	Auf der Festplattenebene	Kann nicht gelöscht werden
Enterprise-Modus	Auf Dateiebene	Kann vom Compliance-Administrator mithilfe eines protokollierten „privilegierten Löschvorgangs“ gelöscht werden

Nach Ablauf der Aufbewahrungsfrist sind Sie für das Löschen aller Dateien verantwortlich, die Sie nicht mehr benötigen. Sobald eine Datei in WORM gespeichert wurde, unabhängig davon, ob im Compliance- oder Enterprise-Modus, kann sie nicht mehr geändert werden, auch nicht nach Ablauf der Aufbewahrungsfrist.

WORM-Dateien können weder während noch nach Ablauf der Aufbewahrungsfrist verschoben werden. Eine WORM-Datei kann kopiert werden, jedoch behält die Kopie ihre WORM-Eigenschaften nicht bei.

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

Fähigkeit	SnapLock Compliance	SnapLock Enterprise
Dateien mit privilegiertem Löschen aktivieren und löschen	Nein	Ja
Festplatten neu initialisieren	Nein	Ja

Zerstörung von SnapLock Aggregaten und Volumes während der Aufbewahrungsfrist	Nein	Ja, mit Ausnahme des SnapLock Revisionsprotokoll-Volumes
Aggregate oder Volumes umbenennen	Nein	Ja
Nicht-NetApp-Datenträger verwenden	Nein	Nein
Das SnapLock Volume für die Revisionsprotokollierung verwenden	Ja	Ja, beginnend mit ONTAP 9.5

Unterstützte und nicht unterstützte Funktionen mit SnapLock

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

Funktion	Unterstützt mit SnapLock Compliance	Unterstützt mit SnapLock Enterprise
Konsistenzgruppen	Nein	Nein
Verschlüsselte Volumes	Ja, weitere Informationen zu Verschlüsselung und SnapLock.	Ja, weitere Informationen zu Verschlüsselung und SnapLock.
FabricPools auf SnapLock Aggregaten	Nein	Ja, beginnend mit ONTAP 9.8. Weitere Informationen zu FabricPool auf SnapLock Enterprise Aggregaten.
Flash Pool Aggregate	Ja.	Ja.
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, beginnend mit ONTAP 9.11.1. Weitere Informationen zu FlexGroup Volumes.	Ja, beginnend mit ONTAP 9.11.1. Weitere Informationen zu FlexGroup Volumes.
LUNs	Nein. Weitere Informationen zu LUN-Unterstützung mit SnapLock.	Nein. Weitere Informationen zu LUN-Unterstützung mit SnapLock.
MetroCluster Konfigurationen	Ja, beginnend mit ONTAP 9.3. Weitere Informationen zu MetroCluster Unterstützung.	Ja, beginnend mit ONTAP 9.3. Weitere Informationen zu MetroCluster Unterstützung.
Multi-Admin-Verifizierung (MAV)	Ja, beginnend mit ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung.	Ja, beginnend mit ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung.
SAN	Nein	Nein
Single-File-SnapRestore	Nein	Ja
SnapMirror Active Sync	Nein	Nein
SnapRestore	Nein	Ja

SMTape	Nein	Nein
SnapMirror Synchronous	Nein	Nein
SSDs	Ja.	Ja.
Speichereffizienzfunktionen	Ja, beginnend mit ONTAP 9.9.1. Weitere Informationen zu Unterstützung der Speichereffizienz.	Ja, beginnend mit ONTAP 9.9.1. Weitere Informationen zu Unterstützung der Speichereffizienz.

FabricPool auf SnapLock Enterprise Aggregaten

FabricPools werden auf SnapLock Enterprise Aggregaten ab ONTAP 9.8 unterstützt. Allerdings muss Ihr Account-Team einen Antrag auf Produktabweichung stellen, in dem dokumentiert wird, dass Sie verstehen, dass FabricPool Daten, die in eine öffentliche oder private Cloud ausgelagert werden, nicht mehr durch SnapLock geschützt sind, da ein Cloud-Administrator diese Daten löschen kann.

Alle Daten, die FabricPool in eine öffentliche oder private Cloud auslagert, sind nicht mehr durch SnapLock geschützt, da diese Daten von einem Cloud-Administrator gelöscht werden können.

FlexGroup Volumes

SnapLock unterstützt FlexGroup Volumes ab ONTAP 9.11.1; jedoch werden die folgenden Funktionen nicht unterstützt:

- Legal-Hold
- Ereignisbasierte Aufbewahrung
- SnapLock für SnapVault (unterstützt ab ONTAP 9.12.1)

Es ist außerdem auf die folgenden Verhaltensweisen zu achten:

- Die Volume Compliance Clock (VCC) eines FlexGroup Volumes wird durch die VCC der Root-Konstituente bestimmt. Alle nicht-Root-Konstituenten haben eine VCC, die eng mit der Root-VCC synchronisiert ist.
- Die SnapLock Konfigurationseigenschaften werden nur für das FlexGroup als Ganzes festgelegt. Einzelne Bestandteile können keine unterschiedlichen Konfigurationseigenschaften wie Standardaufbewahrungsdauer und Autocommit-Periode haben.

LUN-Unterstützung

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

MetroCluster Unterstützung

SnapLock Unterstützung in MetroCluster Konfigurationen unterscheidet sich zwischen SnapLock Compliance-Modus und 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, jedoch nur, wenn das Aggregat zum Hosten von SnapLock Revisionsprotokoll-Volumes verwendet wird.
- SVM-spezifische SnapLock Konfigurationen können mithilfe von MetroCluster auf primäre und sekundäre Standorte repliziert werden.

SnapLock Enterprise

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

MetroCluster Konfigurationen und Konformitätsuhren

MetroCluster Konfigurationen verwenden zwei Compliance-Uhren, die Volume Compliance Clock (VCC) und die System Compliance Clock (SCC). Die VCC und SCC stehen allen SnapLock Konfigurationen zur Verfügung. Wenn ein neues Volume auf einem Knoten erstellt wird, wird dessen VCC mit dem aktuellen Wert der SCC auf diesem Knoten initialisiert. Nach der Erstellung des Volumes wird die Aufbewahrungszeit von Volume und Dateien immer mit der VCC nachverfolgt.

Wird ein Volume an einen anderen Standort repliziert, wird auch dessen VCC repliziert. Bei einem Volume Switchover, beispielsweise von Standort A zu Standort B, wird die VCC an Standort B weiterhin aktualisiert, während die SCC an Standort A stoppt, sobald Standort A offline geht.

Sobald Standort A wieder online ist und die Volume-Rückschaltung durchgeführt wird, startet die SCC-Uhr von Standort A neu, während der VCC des Volumes weiterhin aktualisiert wird. Da der VCC unabhängig von Umschaltungs- und Rückschaltungsvorgängen kontinuierlich aktualisiert wird, hängen die Aufbewahrungszeiten der Dateien nicht von den SCC-Uhren ab und verlängern sich nicht.

Unterstützung für die Multi-Admin-Verifizierung (MAV)

Ab ONTAP 9.13.1 kann ein Clusteradministrator die Multi-Admin-Verifizierung (MAV) explizit auf einem Cluster aktivieren, sodass für bestimmte SnapLock Operationen eine Quorum-Genehmigung erforderlich ist, bevor sie ausgeführt werden. Wenn MAV aktiviert ist, erfordern SnapLock Volume-Eigenschaften wie default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period und privileged-delete eine Quorum-Genehmigung. Weitere Informationen zu "MAV".

Speichereffizienz

Ab ONTAP 9.9.1 unterstützt SnapLock Funktionen zur Speichereffizienz, wie Datenkompaktierung, volumenübergreifende Deduplizierung und adaptive Komprimierung für SnapLock Volumes und Aggregate. Weitere Informationen zur Speichereffizienz finden sich unter "ONTAP Speichereffizienz im Überblick".

Verschlüsselung

ONTAP bietet sowohl software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Speichermedium umfunktioniert, zurückgegeben, verlegt oder gestohlen wird.

Haftungsausschluss: NetApp kann nicht garantieren, dass SnapLock-geschützte WORM-Dateien auf selbstverschlüsselnden Laufwerken oder Volumes wiederhergestellt werden können, wenn der Authentifizierungsschlüssel verloren geht oder die Anzahl fehlgeschlagener Authentifizierungsversuche das festgelegte Limit überschreitet und das Laufwerk dadurch dauerhaft gesperrt wird. Sie sind dafür verantwortlich, Authentifizierungsfehler zu vermeiden.

Verschlüsselte Volumes werden auf SnapLock Aggregaten unterstützt.

[[7-mode-transition]]
== 7-Mode Transition

Sie können SnapLock Volumes von 7-Mode zu ONTAP migrieren, indem Sie die Funktion „Copy-Based Transition“ (CBT) des 7-Mode Transition Tool verwenden. Der SnapLock Modus des Ziel-Volumes, Compliance oder Enterprise, muss mit dem SnapLock Modus des Quell-Volumes übereinstimmen. Die Migration von SnapLock Volumes mit Copy-Free Transition (CFT) ist nicht möglich.

SnapLock konfigurieren

ONTAP SnapLock Konfigurationsworkflow

Bevor Sie SnapLock verwenden, ist es erforderlich, SnapLock zu konfigurieren, indem verschiedene Aufgaben ausgeführt werden, wie zum Beispiel "die SnapLock-Lizenz installieren" für jeden Knoten, der ein Aggregat mit einem SnapLock Volume hostet, die Initialisierung des "Compliance Clock", das Erstellen eines SnapLock Aggregats für Cluster, auf denen ONTAP Versionen vor ONTAP 9.10.1 ausgeführt werden, "Ein SnapLock Volume erstellen und einbinden" und weitere Aufgaben.

Initialisierung der ONTAP SnapLock Compliance Clock

SnapLock verwendet die *Volume Compliance Clock*, um Manipulationen zu verhindern, die die Aufbewahrungsfrist für WORM-Dateien verändern könnten. Zunächst muss die *System ComplianceClock* auf jedem Knoten initialisiert werden, der ein SnapLock Aggregat hostet.

Ab ONTAP 9.14.1 können Sie die System Compliance Clock initialisieren oder neu initialisieren, wenn keine SnapLock-Volumes oder keine Volumes mit aktivierter Snapshot-Sperre vorhanden sind. Die Möglichkeit zur Neuinitialisierung ermöglicht es Systemadministratoren, die System Compliance Clock in Fällen zurückzusetzen, in denen sie möglicherweise falsch initialisiert wurde oder um eine Taktabweichung im System zu korrigieren. In ONTAP 9.13.1 und früheren Versionen können Sie die Compliance Clock nach der Initialisierung auf einem Node nicht erneut initialisieren.

Bevor Sie beginnen

Um die Compliance-Uhr neu zu initialisieren:

- Alle Knoten im Cluster müssen sich im fehlerfreien Zustand befinden.
- Alle Volumes müssen online sein.
- In der Wiederherstellungswarteschlange dürfen keine Volumes vorhanden sein.
- Es dürfen keine SnapLock Volumes vorhanden sein.
- Es dürfen keine Volumes mit aktivierter Snapshot-Sperre vorhanden sein.

Allgemeine Anforderungen für die Initialisierung der Compliance Clock:

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- "Die SnapLock Lizenz muss auf dem Knoten installiert sein.".

Über diese Aufgabe

Die Zeit auf der System-Compliance-Clock wird an die *Volume-Compliance-Clock* vererbt, wobei letztere den Aufbewahrungszeitraum für WORM-Dateien auf dem Volume steuert. Die Volume-Compliance-Clock wird automatisch initialisiert, wenn Sie ein neues SnapLock Volume erstellen.

> ⓘ Die anfängliche Einstellung der System-Compliance-Uhr basiert auf der aktuellen Hardware-Systemuhr. Daher sollten Sie vor der Initialisierung der System-Compliance-Uhr auf jedem Knoten überprüfen, ob Systemzeit und Zeitzone korrekt sind. Nachdem Sie die System-Compliance-Uhr auf einem Knoten initialisiert haben, können Sie sie nicht erneut initialisieren, wenn SnapLock-Volumes oder Volumes mit aktivierter Sperrung vorhanden sind.

Schritte

Die Compliance Clock kann über die ONTAP CLI initialisiert werden oder, ab ONTAP 9.12.1, über den System Manager.

System Manager

1. Zu **Cluster > Übersicht** navigieren.
2. Wählen Sie im Abschnitt **Knoten** die Option **SnapLock Compliance-Uhr initialisieren**.
3. Um die Spalte **Compliance Clock** anzuzeigen und zu überprüfen, ob die Compliance Clock initialisiert ist, wählen Sie im Abschnitt **Cluster > Übersicht > Knoten** die Option **Anzeigen/Ausblenden** und wählen Sie **SnapLock Compliance Clock**.

CLI

1. Initialisieren Sie die System-Compliance-Uhr:

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

   Der folgende Befehl initialisiert die System Compliance Clock `node1`:

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

   Weitere Informationen zu `snaplock compliance-clock initialize` finden sich in der "ONTAP-Befehlsreferenz".

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 dieses Verfahren für jeden Knoten, der ein SnapLock Aggregat hostet.

Compliance Clock-Resynchronisierung für ein NTP-konfiguriertes System aktivieren

Die SnapLock Compliance Clock-Synchronisierungsfunktion kann aktiviert werden, wenn ein NTP-Server konfiguriert ist.

Bevor Sie beginnen

- Diese Funktion ist nur auf der Stufe „Erweitert“ verfügbar.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- "Die SnapLock Lizenz muss auf dem Knoten installiert sein.".
- Diese Funktion ist nur für die Plattformen Cloud Volumes ONTAP, ONTAP Select und VSIM verfügbar.

Über diese Aufgabe

Wenn der SnapLock secure clock daemon eine Abweichung über dem Schwellenwert feststellt, verwendet ONTAP die Systemzeit, um sowohl die System- als auch die Volume Compliance Clocks zurückzusetzen. Ein Zeitraum von 24 Stunden ist als Schwellenwert für die Abweichung festgelegt. Die System Compliance Clock synchronisiert sich nur mit der Systemzeit, wenn die Abweichung mehr als einen Tag alt ist.

Der SnapLock Secure Clock Daemon erkennt eine Zeitabweichung und ändert die Compliance Clock auf die Systemzeit. Jeder Versuch, die Systemzeit zu ändern, um die Compliance Clock zur Synchronisierung mit der Systemzeit zu zwingen, schlägt fehl, da die Compliance Clock nur dann mit der Systemzeit synchronisiert wird, wenn die Systemzeit mit der NTP-Zeit synchronisiert ist.

Schritte

1. Die Funktion zur Synchronisierung der SnapLock Compliance Clock wird aktiviert, wenn ein NTP-Server konfiguriert ist:

   `snaplock compliance-clock ntp`

   Der folgende Befehl aktiviert die System-Compliance-Clock-Synchronisierungsfunktion:

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

   Weitere Informationen zu `snaplock compliance-clock ntp modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Bestätigen Sie bei entsprechender Aufforderung, dass die konfigurierten NTP-Server vertrauenswürdig sind und der Kommunikationskanal sicher ist, damit die Funktion aktiviert werden kann:
3. Überprüfen, ob die Funktion aktiviert ist:

   `snaplock compliance-clock ntp show`

   Der folgende Befehl prüft, ob die Systemfunktion zur Synchronisierung der Compliance Clock aktiviert ist:

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

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

Weitere Informationen zu `snaplock compliance-clock ntp show` finden sich in der "ONTAP-Befehlsreferenz".

Ein ONTAP SnapLock Aggregat erstellen

Die `-snaplock-type`Option „volume“ wird verwendet, um den Typ des SnapLock Volumes als Compliance oder Enterprise festzulegen. Für Versionen vor ONTAP 9.10.1 muss ein separates SnapLock Aggregat erstellt werden. Ab ONTAP 9.10.1 können SnapLock- und Nicht-SnapLock-Volumes auf demselben Aggregate existieren, daher ist es nicht mehr erforderlich, ein separates SnapLock-Aggregate zu erstellen, wenn ONTAP 9.10.1 verwendet wird.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die SnapLock "Lizenz muss installiert sein" auf dem Node. Diese Lizenz ist in "ONTAP One" enthalten.
- "Die Compliance-Uhr auf dem Knoten muss initialisiert sein.".
- Wenn Sie die Festplatten als “root”, “data1” und “data2” partitioniert haben, ist sicherzustellen, dass Ersatzfestplatten verfügbar sind.

Upgrade-Überlegungen

Beim Upgrade auf ONTAP 9.10.1 werden bestehende SnapLock und nicht-SnapLock Aggregate so aktualisiert, dass sowohl SnapLock als auch nicht-SnapLock Volumes unterstützt werden. Die bestehenden SnapLock Volume-Attribute werden jedoch nicht automatisch aktualisiert. Beispielsweise bleiben die Felder data-compaction, cross-volume-dedupe und cross-volume-background-dedupe unverändert. Neue SnapLock Volumes, die auf bestehenden Aggregaten erstellt werden, haben dieselben Standardwerte wie nicht-SnapLock Volumes, und die Standardwerte für neue Volumes und Aggregate sind plattformabhängig.

Überlegungen zum Zurücksetzen

Falls eine Rückkehr zu einer ONTAP Version vor 9.10.1 erforderlich ist, müssen alle SnapLock Compliance, SnapLock Enterprise und SnapLock Volumes auf eigene SnapLock Aggregate verschoben werden.

Über diese Aufgabe

- Compliance-Aggregate können mit der SyncMirror Option nicht erstellt werden.
- Gespiegelte Compliance Aggregate in einer MetroCluster Konfiguration können nur erstellt werden, wenn das Aggregat zum Hosten von SnapLock Revisionsprotokoll-Volumes verwendet wird.

> ⓘ In einer MetroCluster Konfiguration wird SnapLock Enterprise sowohl auf gespiegelten als auch auf ungespiegelten Aggregaten unterstützt. SnapLock Compliance wird nur auf ungespiegelten Aggregaten unterstützt.

Schritte

1. Ein SnapLock Aggregat erstellen:

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

Der folgende Befehl erstellt ein SnapLock `Compliance` Aggregat mit dem Namen `aggr1` mit drei Festplatten auf `node1`:

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

Weitere Informationen zu `storage aggregate create` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SnapLock Volumes erstellen und einbinden

Sie müssen ein SnapLock Volume für die Dateien oder Snapshots erstellen, die Sie in den WORM-Status übernehmen möchten. Ab ONTAP 9.10.1 wird jedes Volume, das Sie erstellen, unabhängig vom Aggregattyp, standardmäßig als Nicht-SnapLock Volume erstellt. Die `-snaplock-type` Option muss verwendet werden, um explizit ein SnapLock Volume zu erstellen, indem entweder Compliance oder Enterprise als SnapLock Typ angegeben wird. Standardmäßig ist der SnapLock Typ auf `non-snaplock` eingestellt.

Bevor Sie beginnen

- Das SnapLock Aggregat muss online sein.
- Sie sollten "Es sollte überprüft werden, ob eine SnapLock-Lizenz installiert ist.". Wenn auf dem Knoten keine SnapLock-Lizenz installiert ist, muss "installieren" sie installiert werden. Diese Lizenz ist mit "ONTAP One" enthalten. Vor ONTAP One war die SnapLock-Lizenz im Security and Compliance Bundle enthalten. Das Security and Compliance Bundle wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl es derzeit nicht erforderlich ist, können bestehende Kunden sich dafür entscheiden, "Upgrade auf ONTAP One".
- "Die Compliance-Uhr auf dem Knoten muss initialisiert sein.".

Über diese Aufgabe

Mit den entsprechenden SnapLock-Berechtigungen ist es möglich, ein Enterprise Volume jederzeit zu zerstören oder umzubenennen. Ein Compliance Volume kann erst zerstört werden, nachdem die Aufbewahrungsfrist abgelaufen ist. Ein Compliance Volume kann niemals umbenannt werden.

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

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

Diese Aufgabe kann mit ONTAP System Manager oder der ONTAP CLI ausgeführt werden.

System Manager

Ab ONTAP 9.12.1 ist es möglich, mit System Manager ein SnapLock Volume zu erstellen.

Schritte

1. Zu **Speicher > Volumes** navigieren und auf **Hinzufügen** klicken.
2. Im Fenster **Volume hinzufügen** auf **Weitere Optionen** klicken.
3. Geben Sie die neuen Volume-Informationen ein, einschließlich Name und Größe des Volumes.
4. **SnapLock aktivieren** auswählen und den SnapLock Typ, entweder Compliance oder Enterprise, wählen.
5. Im Abschnitt **Dateien automatisch übernehmen** ist **Geändert** auszuwählen und die Zeitspanne anzugeben, die eine Datei unverändert bleiben soll, bevor sie automatisch übernommen wird. Der Mindestwert beträgt 5 Minuten, der Höchstwert 10 Jahre.
6. Im Abschnitt **Datenaufbewahrung** sind die minimale und maximale Aufbewahrungsdauer auszuwählen.
7. Die Standardaufbewahrungsfrist auswählen.
8. Auf **Speichern** klicken.
9. Das neue Volume auf der Seite **Volumes** auswählen, um die SnapLock-Einstellungen zu überprüfen.

CLI

1. Ein SnapLock Volume erstellen:

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

Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz". Die folgenden Optionen sind für SnapLock Volumes nicht verfügbar: `-nvfail`, `-atime-update`, `-is -autobalance-eligible`, `-space-mgmt-try-first`, und `vmalign`.

Der folgende Befehl erstellt ein SnapLock `Compliance` Volume mit dem Namen `vol1` auf `aggr1` auf `vs1`:

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

Ein SnapLock Volume einbinden

Ein SnapLock Volume kann an einem Verbindungspfad im SVM-Namespace für den Zugriff durch NAS-Clients eingebunden werden.

Bevor Sie beginnen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

- Ein SnapLock Volume kann nur unter dem Stammverzeichnis der SVM eingebunden werden.
- Ein normales Volume kann nicht unter einem SnapLock Volume eingebunden werden.

Schritte

1. Ein SnapLock Volume einbinden:

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

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

Der folgende Befehl bindet ein SnapLock Volume mit dem Namen `vol1` an den Verbindungspfad `/sales` im `vs1` Namespace ein:

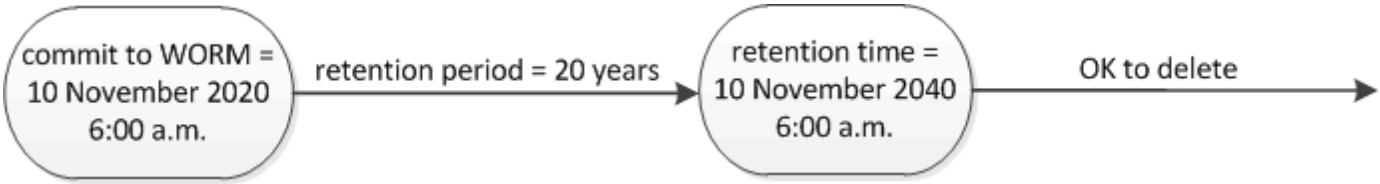
```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

Die ONTAP SnapLock Aufbewahrungszeit festlegen

Sie können die Aufbewahrungsdauer für eine Datei explizit festlegen oder die Standardaufbewahrungsdauer für das Volume verwenden, um die Aufbewahrungsdauer abzuleiten. Sofern Sie die Aufbewahrungsdauer nicht explizit festlegen, verwendet SnapLock die Standardaufbewahrungsdauer zur Berechnung der Aufbewahrungsdauer. Die Dateiaufbewahrung kann auch nach einem Ereignis festgelegt werden.

Informationen zu Aufbewahrungsfrist und Aufbewahrungszeit

Die Aufbewahrungsfrist für eine WORM-Datei gibt an, wie lange die Datei nach dem Übergang in den WORM-Zustand aufbewahrt werden muss. Die Aufbewahrungsdauer einer WORM-Datei ist der Zeitpunkt, nach dem die Datei nicht mehr aufbewahrt werden muss. Eine Aufbewahrungsfrist von 20 Jahren für eine Datei, die am 10. November 2020 um 6:00 Uhr in den WORM-Zustand versetzt wurde, ergibt eine Aufbewahrungsdauer bis zum 10. November 2040 um 6:00 Uhr.



Ab ONTAP 9.10.1 kann eine Aufbewahrungsfrist bis zum 26. Oktober 3058 und eine Aufbewahrungsdauer von bis zu 100 Jahren festgelegt werden. Bei einer Verlängerung der Aufbewahrungsfristen werden ältere Richtlinien automatisch konvertiert. In ONTAP 9.9.1 und früheren Versionen beträgt die maximal unterstützte Aufbewahrungsfrist, sofern die Standardaufbewahrungsdauer nicht auf unbegrenzt gesetzt ist, den 19. Januar 2071 (GMT).

Wichtige Überlegungen zur Replikation

Wenn eine SnapMirror Beziehung mit einem SnapLock Quellvolume unter Verwendung eines Aufbewahrungsdatums nach dem 19. Januar 2071 (GMT) hergestellt wird, muss das Ziel-Cluster ONTAP 9.10.1 oder höher ausführen, andernfalls schlägt die SnapMirror Übertragung fehl.

Wichtige Überlegungen zur Rückführung

ONTAP verhindert, dass ein Cluster von ONTAP 9.10.1 auf eine frühere ONTAP Version zurückgesetzt werden kann, wenn Dateien mit einer Aufbewahrungsfrist nach „19. Januar 2071 8:44:07 Uhr“ vorhanden sind.

Aufbewahrungsfristen im Überblick

Ein SnapLock Compliance oder Enterprise Volume hat vier Aufbewahrungsfristen:

- Mindestaufbewahrungsdauer (`min`), mit einem Standardwert von 0

- Maximale Aufbewahrungsdauer (`max`), mit einem Standardwert von 30 Jahren
- Standardmäßige Aufbewahrungsfrist, mit einem Standardwert von `min` für sowohl den Compliance-Modus als auch den Enterprise-Modus ab ONTAP 9.10.1. In ONTAP Versionen vor ONTAP 9.10.1 hängt die standardmäßige Aufbewahrungsfrist vom Modus ab:
  - Im Compliance-Modus ist der Standardwert gleich `max`.
  - Im Enterprise-Modus ist der Standardwert gleich `min`.
- Nicht spezifizierte Aufbewahrungsfrist.

> In ONTAP-Versionen vor ONTAP 9.10.1, wenn die Aufbewahrungsdauer nicht explizit festgelegt wurde, bevor eine Datei im Compliance-Modus in den WORM-Status überführt wird, und die Standardeinstellungen nicht geändert wurden, wird die Datei 30 Jahre lang aufbewahrt. Diese Änderung *kann* nicht rückgängig gemacht werden. Ebenso wird in ONTAP 9.10.1 und später, wenn die Aufbewahrungsdauer nicht explizit festgelegt wurde, bevor eine Datei im Enterprise-Modus in den WORM-Status überführt wird, und die Standardeinstellungen nicht geändert wurden, die Datei 0 Jahre lang aufbewahrt, also de facto gar nicht.

Ab ONTAP 9.8 kann die Aufbewahrungsdauer von Dateien in einem Volume auf `unspecified`unspezifiziert gesetzt werden, sodass die Datei bis zur Festlegung einer absoluten Aufbewahrungszeit aufbewahrt bleibt. Eine Datei mit absoluter Aufbewahrungszeit kann auf unspezifizierte Aufbewahrungsdauer und wieder zurück auf absolute Aufbewahrungszeit gesetzt werden, solange die neue absolute Aufbewahrungszeit später liegt als die zuvor festgelegte absolute Zeit.

Ab ONTAP 9.12.1 wird für WORM-Dateien mit der Aufbewahrungsdauer, die auf `unspecified` festgelegt ist, garantiert, dass die Aufbewahrungsdauer mindestens der für das SnapLock Volume konfigurierten Mindestaufbewahrungsdauer entspricht. Wenn die Aufbewahrungsdauer einer Datei von `unspecified` auf eine absolute Aufbewahrungszeit geändert wird, muss die neu angegebene Aufbewahrungszeit größer sein als die bereits für die Datei festgelegte Mindestaufbewahrungsdauer.

Standardaufbewahrungsdauer festlegen

Sie können den `volume snaplock modify`Befehl verwenden, um die Standardaufbewahrungsdauer für Dateien auf einem SnapLock Volume festzulegen.

Bevor Sie beginnen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

Die folgende Tabelle zeigt die möglichen Werte für die Option „Standardaufbewahrungsdauer“:

> Die Standardaufbewahrungsfrist muss größer oder gleich (>=) der minimalen Aufbewahrungsfrist und kleiner oder gleich (<=) der maximalen Aufbewahrungsfrist sein.

Wert	Einheit	Hinweise
0 - 65535	Sekunden	
0 - 60	Minuten	
0 - 24	Stunden	
0 - 36500	Tage	

Wert	Einheit	Hinweise
0 - 1200	Monate	
0 - 100	Jahre	Ab ONTAP 9.10.1. Bei früheren ONTAP Versionen liegt der Wert zwischen 0 und 70.
max	-	Die maximale Aufbewahrungsfrist verwenden.
min	-	Die Mindestaufbewahrungsfrist verwenden.
unendlich	-	Die Dateien werden dauerhaft aufbewahrt.
nicht spezifiziert	-	Die Dateien bleiben erhalten, bis eine absolute Aufbewahrungsfrist festgelegt ist.

Die Werte und Bereiche für die maximale und minimale Aufbewahrungsfrist sind identisch, mit Ausnahme von `max` und `min`, die nicht anwendbar sind. Weitere Informationen zu dieser Aufgabe finden sich unter "Übersicht zur Aufbewahrungszeit".

Sie können den `volume snaplock show` Befehl verwenden, um die Einstellungen für die Aufbewahrungsfrist des Volumes anzuzeigen. Weitere Informationen zu `volume snaplock show` finden sich in der "ONTAP-Befehlsreferenz".

Sobald eine Datei in den WORM-Status übertragen wurde, kann die Aufbewahrungsfrist verlängert, aber nicht verkürzt werden.

Schritte

1. Die Standardaufbewahrungsdauer für Dateien auf einem SnapLock Volume festlegen:

   `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`*

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

   Die folgenden Beispiele setzen voraus, dass die Mindest- und Höchstaufbewahrungsfristen zuvor nicht geändert wurden.

   Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Compliance oder Enterprise Volume auf 20 Tage fest:

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

   Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Compliance Volume auf 70 Jahre fest:

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
   ```

```
-retention-period 70years
```

Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Enterprise Volume auf 10 Jahre fest:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Die folgenden Befehle legen die Standardaufbewahrungsfrist für ein Enterprise-Volume auf 10 Tage fest:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

Der folgende Befehl legt die Standardaufbewahrungsfrist für ein Compliance Volume auf unendlich fest:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Die Aufbewahrungszeit für eine Datei explizit festlegen

Sie können die Aufbewahrungsdauer einer Datei explizit festlegen, indem Sie deren letzten Zugriffszeitpunkt ändern. Sie können jeden geeigneten Befehl oder jedes geeignete Programm über NFS oder CIFS verwenden, um den letzten Zugriffszeitpunkt zu ändern.

Über diese Aufgabe

Nachdem eine Datei in WORM übertragen wurde, kann die Aufbewahrungszeit verlängert, aber nicht verkürzt werden. Die Aufbewahrungszeit wird im `atime` Feld für die Datei gespeichert.

> Die Aufbewahrungszeit einer Datei kann nicht explizit auf `infinite` gesetzt werden. Dieser Wert ist nur verfügbar, wenn die Aufbewahrungszeit anhand der Standardaufbewahrungsdauer berechnet wird.

Schritte

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

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

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

   > Es kann jeder geeignete Befehl oder jedes geeignete Programm verwendet werden, um die letzte Zugriffszeit in Windows zu ändern.

Die Aufbewahrungsfrist für Dateien nach einem Ereignis festlegen

Ab ONTAP 9.3 kann mit der Funktion SnapLock *Event Based Retention (EBR)* festgelegt werden, wie lange eine Datei nach dem Eintreten eines Ereignisses aufbewahrt wird.

Bevor Sie beginnen

- Um diese Aufgabe auszuführen, sind SnapLock Administratorrechte erforderlich.

  "Ein SnapLock Administratorkonto erstellen"

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

Über diese Aufgabe

Die *Ereignisaufbewahrungsrichtlinie* definiert die Aufbewahrungsdauer der Datei nach dem Eintreten des Ereignisses. Die Richtlinie kann auf eine einzelne Datei oder alle Dateien in einem Verzeichnis angewendet werden.

- Wenn es sich bei einer Datei nicht um eine WORM-Datei handelt, wird sie für die in der Richtlinie festgelegte Aufbewahrungsdauer in den WORM-Status übernommen.
- Wenn es sich bei einer Datei um eine WORM-Datei oder eine WORM-anhängbare Datei handelt, wird ihre Aufbewahrungsfrist um die in der Richtlinie festgelegte Aufbewahrungsfrist verlängert.

Es kann ein Volume im Compliance-Modus oder im Enterprise-Modus verwendet werden.

> EBR-Richtlinien können nicht auf Dateien angewendet werden, die unter einer Legal Hold stehen.

Für fortgeschrittene Anwendungen siehe "Konforme WORM-Speicherung mit NetApp SnapLock".

Verwendung von EBR zur Verlängerung der Aufbewahrungsfrist bereits vorhandener WORM-Dateien
EBR ist praktisch, wenn die Aufbewahrungsfrist bereits vorhandener WORM-Dateien verlängert werden soll. Beispielsweise kann es eine Unternehmensrichtlinie sein, die W-4-Formulare von Mitarbeitern drei Jahre lang in unveränderter Form aufzubewahren, nachdem der Mitarbeiter eine Lohnsteuerabzugsoption geändert hat. Eine andere Unternehmensrichtlinie kann verlangen, dass die W-4-Formulare fünf Jahre nach Beendigung des Arbeitsverhältnisses aufbewahrt werden. In diesem Fall könnte eine EBR-Richtlinie mit einer Aufbewahrungsfrist von fünf Jahren erstellt werden. Nach Beendigung des Arbeitsverhältnisses (dem „`event`“) wird die EBR-Richtlinie auf den W-4-Datensatz des Mitarbeiters angewendet, wodurch sich dessen Aufbewahrungsfrist verlängert. Das ist in der Regel einfacher als die manuelle Verlängerung der Aufbewahrungsfrist, insbesondere wenn eine große Anzahl von Dateien betroffen ist.

Schritte

1. EBR-Richtlinie erstellen:

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

   Der folgende Befehl erstellt die EBR-Richtlinie `employee_exit` auf `vs1` mit einer Aufbewahrungsfrist von zehn Jahren:

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   ```

```
employee_exit -retention-period 10years
```

2. Eine EBR-Richtlinie anwenden:

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

   Der folgende Befehl wendet die EBR-Richtlinie `employee_exit` auf `vs1` alle Dateien im Verzeichnis `d1` an:

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

Verwandte Informationen

- "snaplock event-retention policy create"
- "snaplock event-retention apply"

Ein ONTAP SnapLock-geschütztes Revisionsprotokoll erstellen

Bei Verwendung von ONTAP 9.9.1 oder älter ist zunächst ein SnapLock Aggregat zu erstellen und anschließend ein SnapLock-geschütztes Revisionsprotokoll, bevor ein privilegierter Löschvorgang oder eine SnapLock Volume-Verschiebung durchgeführt wird. Das Revisionsprotokoll zeichnet die Erstellung und Löschung von SnapLock Administratorkonten, Änderungen am Protokollvolume, ob privilegierter Löschvorgang aktiviert ist, privilegierte Löschvorgänge sowie SnapLock Volume-Verschiebungen auf.

Ab ONTAP 9.10.1 wird kein SnapLock Aggregat mehr erstellt. Die Option -snaplock-type muss verwendet werden, "explizit ein SnapLock Volume erstellen" indem entweder Compliance oder Enterprise als SnapLock Typ angegeben wird.

Bevor Sie beginnen

Wenn Sie ONTAP 9.9.1 oder eine frühere Version verwenden, ist die Rolle als Cluster-Administrator erforderlich, um ein SnapLock Aggregat zu erstellen.

Über diese Aufgabe

Ein Revisionsprotokoll kann erst nach Ablauf der Aufbewahrungsfrist gelöscht werden. Ein Revisionsprotokoll kann auch nach Ablauf der Aufbewahrungsfrist nicht mehr geändert werden. Dies gilt sowohl für den SnapLock Compliance- als auch für den Enterprise-Modus.

> In ONTAP 9.4 und früher kann ein SnapLock Enterprise Volume nicht für die Revisionsprotokollierung verwendet werden. Es muss ein SnapLock Compliance Volume verwendet werden. In ONTAP 9.5 und später kann entweder ein SnapLock Enterprise Volume oder ein SnapLock Compliance Volume für die Revisionsprotokollierung verwendet werden. In allen Fällen muss das Revisionsprotokoll-Volume am Verbindungspfad `/snaplock_audit_log` eingebunden sein. Kein anderes Volume kann diesen Verbindungspfad verwenden.

Die SnapLock Revisionsprotokolle befinden sich im `/snaplock_log` Verzeichnis unter dem

Stammverzeichnis des Revisionsprotokoll-Volumes, in Unterverzeichnissen mit den Namen `privdel_log` (privilegierte Löschvorgänge) und `system_log` (alles andere). Die Dateinamen der Revisionsprotokolle enthalten den Zeitstempel des ersten protokollierten Vorgangs, was die Suche nach Einträgen anhand des ungefähren Ausführungszeitpunkts der Vorgänge erleichtert.

- Mit dem `snaplock log file show` Befehl lassen sich die Protokolldateien auf dem Revisionsprotokoll Volume anzeigen.
- Der `snaplock log file archive` Befehl kann verwendet werden, um die aktuelle Protokolldatei zu archivieren und eine neue zu erstellen, was in Fällen nützlich ist, in denen Revisionsprotokollinformationen in einer separaten Datei aufgezeichnet werden müssen.

Weitere Informationen zu `snaplock log file show` und `snaplock log file archive` finden sich in der "ONTAP-Befehlsreferenz".

Ein Datensicherungsvolume kann nicht als SnapLock Revisionsprotokollvolume verwendet werden.

Schritte

1. Ein SnapLock Aggregat erstellen.

   Ein SnapLock Aggregat erstellen

2. Erstellen Sie auf der SVM, die für die Revisionsprotokollierung konfiguriert werden soll, ein SnapLock Volume.

   Ein SnapLock Volume erstellen

3. Die SVM für die Revisionsprotokollierung konfigurieren:

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

   Die standardmäßige Mindestaufbewahrungsdauer für Revisionsprotokoll-Dateien beträgt sechs Monate. Ist die Aufbewahrungsdauer einer betroffenen Datei länger als die Aufbewahrungsdauer des Revisionsprotokolls, übernimmt die Aufbewahrungsdauer des Protokolls die Aufbewahrungsdauer der Datei. Wenn die Aufbewahrungsdauer einer mit privilegiertem Löschen entfernten Datei beispielsweise zehn Monate beträgt und die Aufbewahrungsdauer des Revisionsprotokolls acht Monate beträgt, wird die Aufbewahrungsdauer des Protokolls auf zehn Monate verlängert. Weitere Informationen zur Aufbewahrungszeit und zur standardmäßigen Aufbewahrungsdauer finden sich unter "Aufbewahrungszeit festlegen".

   Der folgende Befehl konfiguriert `SVM1` die Protokollierung mithilfe des SnapLock Volumes `logVol`. Das Revisionsprotokoll 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
   ```

   Weitere Informationen zu `snaplock log create` finden sich in der "ONTAP-Befehlsreferenz".

4. Auf der SVM, die für die Protokollierung konfiguriert wurde, das SnapLock-Volume am Verbindungspfad `/snaplock_audit_log` einbinden.

   Ein SnapLock Volume einbinden

ONTAP SnapLock Einstellungen überprüfen

Sie können die `volume file fingerprint start` und `volume file fingerprint dump` Befehle verwenden, um wichtige Informationen über Dateien und Volumes anzuzeigen, einschließlich des Dateityps (regulär, WORM oder WORM-anhängbar), des Ablaufdatums des Volumes und so weiter.

Schritte

1. Dateifingerabdruck generieren:

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

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   Der Befehl generiert eine Sitzungs-ID, die Sie als Eingabe für den `volume file fingerprint dump` Befehl verwenden können.

   > Sie können den `volume file fingerprint show` Befehl mit der Sitzungs-ID verwenden, um den Fortschritt des Fingerabdruckvorgangs zu überwachen. Es sollte sichergestellt sein, dass der Vorgang abgeschlossen ist, bevor versucht wird, den Fingerabdruck anzuzeigen.

2. Der Fingerabdruck der Datei wird angezeigt:

   ```
   volume file fingerprint dump -session-id <session_ID>
   ```

   ```
   svm1::> volume file fingerprint dump -session-id 33619976
           Vserver:svm1
           Session-ID:33619976
           Volume:slc_vol
           Path:/vol/slc_vol/f1
           Data
   Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

   Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
   Algorithm:SHA256
           Fingerprint Scope:data-and-metadata
           Fingerprint Start Time:1460612586
           Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
   ```

```
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

WORM-Dateien verwalten

WORM-Dateiverwaltung in ONTAP SnapLock

Sie können WORM-Dateien auf folgende Weise verwalten:

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

Dateien mit ONTAP SnapLock auf WORM festschreiben

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

Dateien manuell an WORM übergeben

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

Dateien automatisch an WORM übergeben

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

standardmäßig deaktiviert.

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

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

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

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

Eine WORM-anhängbare Datei erstellen

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

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

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

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

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

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

   ```
   chmod 444 document.txt
   ```

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

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

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

```
chmod 777 document.txt
```

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

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

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

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

VAM wird auf SnapLock Revisionsprotokoll-Volumes nicht unterstützt.

Schritte

1. VAM aktivieren:

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

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

   Der folgende Befehl aktiviert VAM auf dem Volume `vol1` der SVM`vs1`:

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

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

   Die Dateien sind standardmäßig WORM-anhängbar.

Snapshots auf einem ONTAP SnapLock Vault-Ziel in WORM festschreiben

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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

Ab ONTAP 9.10.1 können SnapLock- und Nicht-SnapLock-Volumes auf demselben Aggregate existieren, daher ist es nicht mehr erforderlich, ein separates SnapLock-Aggregate zu erstellen, wenn ONTAP 9.10.1 verwendet wird. Die Volume-Option '-snaplock-type' wird verwendet, um einen Compliance- oder Enterprise-SnapLock-Volume-Typ anzugeben. In ONTAP-Versionen vor ONTAP 9.10.1 wird der SnapLock-Modus,

Compliance oder Enterprise, vom Aggregate übernommen. Version-flexible Zielvolumes werden nicht unterstützt. Die Spracheinstellung des Ziel-Volumes muss mit der Spracheinstellung des Quell-Volumes übereinstimmen.

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

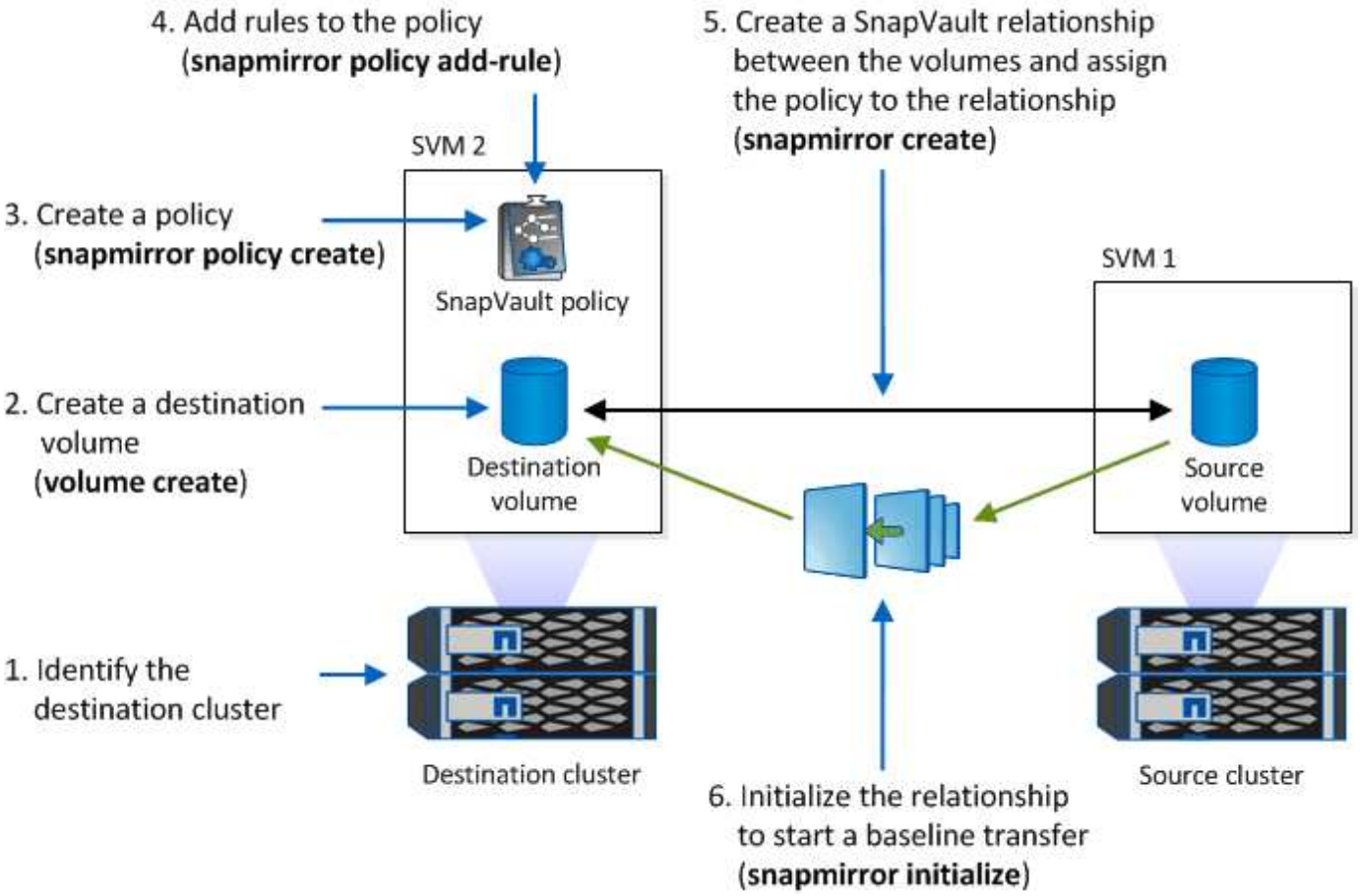
Ab ONTAP 9.14.1 können Aufbewahrungsfristen für bestimmte SnapMirror Labels in der SnapMirror Policy der SnapMirror Beziehung festgelegt werden, sodass die replizierten Snapshots vom Quell- zum Ziel-Volume für die in der Regel angegebene Aufbewahrungsfrist aufbewahrt werden. Wenn keine Aufbewahrungsfrist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

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

Für MetroCluster Konfigurationen gilt Folgendes:

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

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



Schritte

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

System Manager

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

11. Speichern Sie Ihre Änderungen.

CLI

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

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

   Der folgende Befehl erstellt ein 2GB SnapLock Compliance Volume mit dem Namen `dstvolB` in `SVM2` auf dem Aggregat `node01_aggr`:

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

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

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

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

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

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

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

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

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

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

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

und das SnapLock Ablaufdatum haben:

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

Verwandte Informationen

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

WORM-Dateien mit ONTAP SnapMirror für die Notfallwiederherstellung spiegeln

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

Voraussetzungen

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

Über diese Aufgabe

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

  Bei einer Resynchronisierung wird, wenn zwischen Quelle und Ziel Datenabweichungen über den gemeinsamen Snapshot hinaus festgestellt werden, ein neuer Snapshot auf dem Ziel erstellt, um diese Abweichungen zu erfassen. Der neue Snapshot und der gemeinsame Snapshot werden beide mit einer Aufbewahrungszeit wie folgt gesperrt:

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

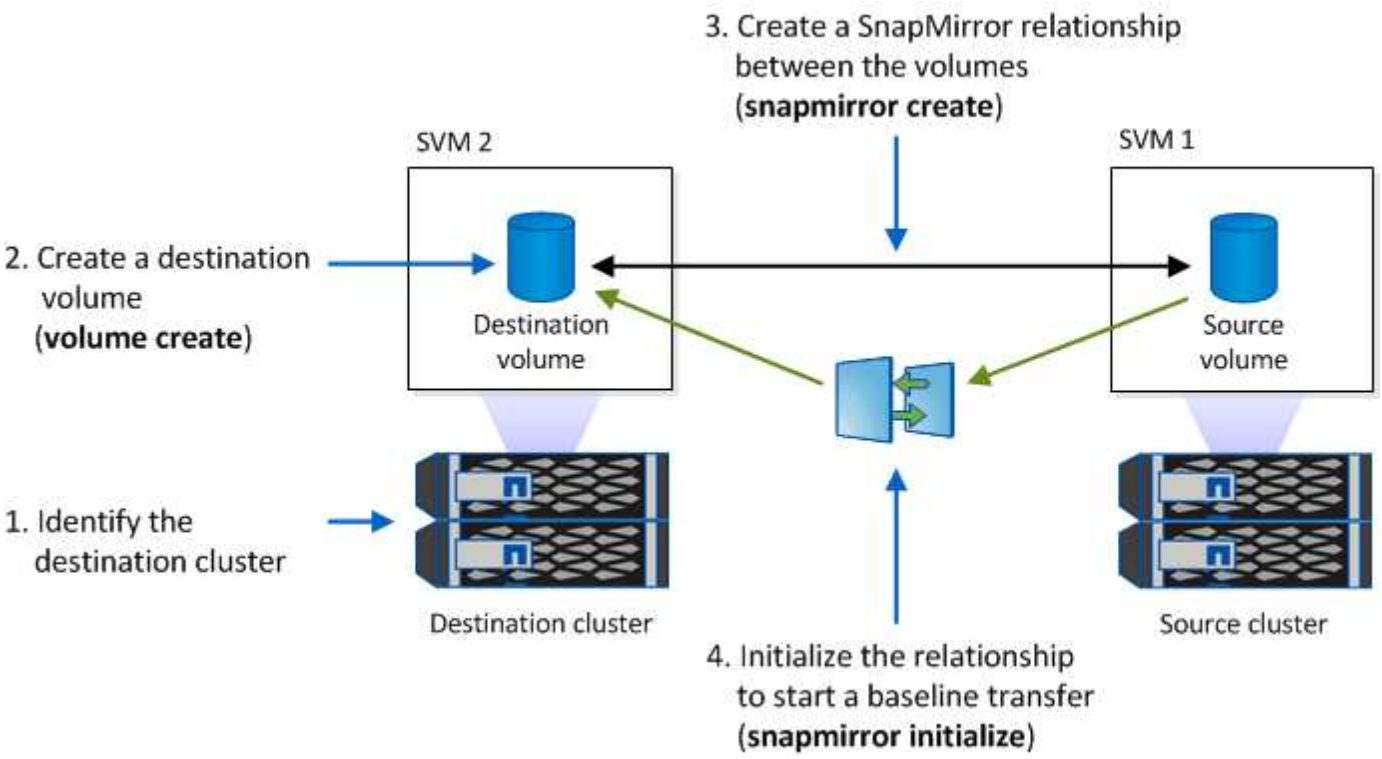
Wenn das Zielvolume eine Ablaufperiode hat, die später ist als die des Quellvolumes, bleibt die Ablaufperiode des Zielvolumes erhalten und wird nach der Resynchronisierung nicht durch die Ablaufperiode des Quellvolumes überschrieben.

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

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

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

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



System Manager

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

Schritte

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

CLI

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

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

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

   Der folgende Befehl erstellt ein 2 GB SnapLock `Compliance` Volume mit dem Namen `dstvolB` in `SVM2` auf dem Aggregat `node01_aggr`:

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

4. Auf der Ziel-SVM eine SnapMirror Richtlinie erstellen:

   `snapmirror policy create -vserver SVM_name -policy policy_name`

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

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

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

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

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

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

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

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

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

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

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

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

   `snapmirror initialize -destination-path destination_path`

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

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

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

Verwandte Informationen

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

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

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

Bevor Sie beginnen

- Um diese Aufgabe auszuführen, sind SnapLock Administratorrechte erforderlich.

  "Ein SnapLock Administratorkonto erstellen"

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

Über diese Aufgabe

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

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

Schritte

1. Rechtliche Sicherung starten:

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

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

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

2. Legal Hold beenden:

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

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

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

Verwandte Informationen

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

WORM-Dateien mit ONTAP SnapLock löschen

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

Ein SnapLock Administratorkonto erstellen

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

Bevor Sie beginnen

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

Schritte

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

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

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

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

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

Die Funktion zum privilegierten Löschen aktivieren

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

Über diese Aufgabe

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

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

Schritte

1. Privilegiertes Löschen für ein SnapLock Enterprise Volume aktivieren:

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

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

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

Enterprise-Modus WORM-Dateien löschen

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritt

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

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

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

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

Verschieben eines ONTAP SnapLock Volumes

Ab ONTAP 9.8 ist es möglich, ein SnapLock Volume in ein Zielaggregat desselben Typs zu verschieben, entweder von Enterprise zu Enterprise oder von Compliance zu Compliance. Die SnapLock Sicherheitsrolle muss zugewiesen sein, um ein SnapLock Volume zu verschieben.

Ein SnapLock Sicherheitsadministratorkonto erstellen

Sie müssen über SnapLock Sicherheitsadministratorrechte verfügen, um eine SnapLock Volume-Verschiebung durchzuführen. Dieses Privileg wird Ihnen mit der Rolle *snaplock* gewährt, die in ONTAP 9.8 eingeführt wurde. Falls Ihnen diese Rolle noch nicht zugewiesen wurde, kann Ihr Cluster-Administrator einen SnapLock Sicherheitsbenutzer mit dieser SnapLock Sicherheitsrolle erstellen.

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritt

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

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

   Der folgende Befehl ermöglicht dem SVM-Administratorkonto `SnapLockAdmin` mit der vordefinierten `snaplock` Rolle den Zugriff auf die Admin SVM `cluster1` mit einem Passwort:

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

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

Ein SnapLock Volume verschieben

Mit dem `volume move` Befehl lässt sich ein SnapLock Volume auf ein Zielaggregat verschieben.

Bevor Sie beginnen

- Vor der Durchführung einer SnapLock-geschützten Revisionsprotokollierung muss ein SnapLock-geschütztes Revisionsprotokoll erstellt worden sein.

  "Ein Revisionsprotokoll erstellen".

- Wenn eine Version von ONTAP vor ONTAP 9.10.1 verwendet wird, muss das Zielaggregat denselben SnapLock-Typ wie das SnapLock-Volume aufweisen, das verschoben werden soll; entweder Compliance zu Compliance oder Enterprise zu Enterprise. Ab ONTAP 9.10.1 entfällt diese Einschränkung und ein

Aggregat kann sowohl Compliance als auch Enterprise SnapLock Volumes sowie Nicht-SnapLock Volumes enthalten.

- Sie müssen ein Benutzer mit der SnapLock Sicherheitsrolle sein.

Schritte

1. Über eine sichere Verbindung bei der ONTAP Cluster-Management-LIF anmelden:

   ```
   ssh snaplock_user@cluster_mgmt_ip
   ```

2. Ein SnapLock Volume verschieben:

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

3. Status des Volume-Verschiebungsvorgangs prüfen:

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

Einen ONTAP Snapshot zum Schutz vor Ransomware-Angriffen sperren

Ab ONTAP 9.12.1 können Snapshots auf einem Nicht-SnapLock Volume gesperrt werden, um Schutz vor Ransomware-Angriffen zu bieten. Das Sperren von Snapshots stellt sicher, dass sie nicht versehentlich oder böswillig gelöscht werden können.

Die SnapLock compliance clock-Funktion wird verwendet, um Snapshots für einen festgelegten Zeitraum zu sperren, sodass sie erst nach Erreichen der Ablaufzeit gelöscht werden können. Das Sperren von Snapshots macht sie manipulationssicher und schützt sie vor Ransomware-Bedrohungen. Mit gesperrten Snapshots kann eine Datenwiederherstellung erfolgen, wenn ein Volume durch einen Ransomware-Angriff kompromittiert wurde.

Ab ONTAP 9.14.1 unterstützt die Snapshot-Sperre Snapshots mit langfristiger Aufbewahrung auf nicht-SnapLock Vault- und Mirror-Vault-SnapMirror Ziel-Volumes. Die Aktivierung der Snapshot-Sperre erfolgt durch Festlegen der Aufbewahrungsdauer mit SnapMirror Richtlinienregeln, die einem bestehende Richtlinienbezeichnung zugeordnet sind. Die Regel überschreibt die auf dem Volume festgelegte Standardaufbewahrungsdauer. Wenn dem SnapMirror Label keine Aufbewahrungsdauer zugeordnet ist, wird die Standardaufbewahrungsdauer des Volumes verwendet.

Anforderungen und Überlegungen zu manipulationssicheren Snapshots

- Wenn die ONTAP CLI verwendet wird, müssen alle Knoten im Cluster ONTAP 9.12.1 oder neuer ausführen. Wenn System Manager verwendet wird, müssen alle Knoten ONTAP 9.13.1 oder neuer ausführen.
- "Die SnapLock Lizenz muss auf dem Cluster installiert sein.". Diese Lizenz ist in "ONTAP One" enthalten.
- "Die Compliance-Uhr auf dem Cluster muss initialisiert sein.".
- Wenn die Snapshot-Sperre auf einem Volume aktiviert ist, können Sie die Cluster auf eine ONTAP Version aktualisieren, die nach ONTAP 9.12.1 liegt. Sie können jedoch erst dann auf eine frühere Version von ONTAP zurückkehren, wenn alle gesperrten Snapshots ihr Ablaufdatum erreicht haben, gelöscht wurden und die Snapshot-Sperre deaktiviert ist.
- Wenn ein Snapshot gesperrt ist, wird die Ablaufzeit des Volumes auf die Ablaufzeit des Snapshots gesetzt. Wenn mehr als ein Snapshot gesperrt ist, entspricht die Ablaufzeit des Volumes der größten Ablaufzeit aller Snapshots.

- Die Aufbewahrungsfrist für gesperrte Snapshots hat Vorrang vor der Snapshot-Aufbewahrungsanzahl, was bedeutet, dass die Begrenzung der Aufbewahrungsanzahl nicht berücksichtigt wird, wenn die Aufbewahrungsfrist für gesperrte Snapshots noch nicht abgelaufen ist.
- In einer SnapMirror Beziehung kann eine Aufbewahrungsdauer für eine Mirror-Vault-Richtlinienregel festgelegt werden, und die Aufbewahrungsdauer wird auf Snapshots angewendet, die auf das Ziel repliziert werden, wenn auf dem Zielvolume die Snapshot-Sperre aktiviert ist. Die Aufbewahrungsdauer hat Vorrang vor der Aufbewahrungsanzahl; beispielsweise werden Snapshots, deren Ablaufdatum noch nicht erreicht ist, auch dann aufbewahrt, wenn die Aufbewahrungsanzahl überschritten wurde.
- Sie können einen Snapshot auf einem Nicht-SnapLock Volume umbenennen. Snapshot-Umbenennungsvorgänge auf dem primären Volume einer SnapMirror Beziehung werden auf dem sekundären Volume nur dann widergespiegelt, wenn die Richtlinie MirrorAllSnapshots ist. Bei anderen Richtlinientypen wird der umbenannte Snapshot bei Aktualisierungen nicht übernommen.
- Wenn die ONTAP CLI verwendet wird, kann ein gesperrter Snapshot mit dem `volume snapshot restore` Befehl nur dann wiederhergestellt werden, wenn der gesperrte Snapshot der aktuellste ist. Wenn spätere, noch nicht abgelaufene Snapshots vorhanden sind, als der wiederherzustellende, schlägt die Snapshot-Wiederherstellung fehl.

Funktionen, die mit manipulationssicheren Snapshots unterstützt werden

- "Cloud Volumes ONTAP"
- FlexCache Ursprungs-Volumes

  Unterstützt ab ONTAP 9.16.1.

- FlexGroup Volumes

  Die Snapshot-Sperrung wird für FlexGroup Volumes unterstützt. Die Snapshot-Sperrung erfolgt nur beim Snapshot des Root-Bestandteils. Das Löschen des FlexGroup Volumes ist nur zulässig, wenn die Ablaufzeit des Root-Bestandteils abgelaufen ist.

- FlexVol zu FlexGroup Konvertierung

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

- SnapMirror Active Sync für NAS

  Ab ONTAP 9.20.1 können Sie manipulationssichere Snapshots auf SnapMirror active sync NAS FlexVol Volumes in SVM-Beziehungen erstellen.

- SnapMirror asynchron

  Die Compliance-Uhr muss sowohl auf dem Quell- als auch auf dem Zielsystem initialisiert werden.

- SnapMirror Richtlinienregeln mit dem `-schedule` Parameter
- SnapMirror synchron

  Ab ONTAP 9.19.1 kann die Ablaufzeit nur noch bei der Snapshot-Erstellung festgelegt werden. Sie können die Ablaufzeit für vorhandene Snapshots nicht festlegen oder verlängern.

- SVM Datenmobilität (wird für die Migration oder Verlagerung einer SVM von einem Quell-Cluster zu einem Ziel-Cluster verwendet)

Unterstützt ab ONTAP 9.14.1.

- SVM DR

  Die Compliance-Uhr muss sowohl auf dem Quell- als auch auf dem Zielsystem initialisiert werden.

- Volume clone und Klon einer Datei

  Aus einem gesperrten Snapshot können Volume-Klone und Klone einer Datei erstellt werden.

Nicht unterstützte Funktionen

Manipulationssichere Snapshots unterstützen diese Funktionen nicht:

- Konsistenzgruppen
- "FabricPool"

  Manipulationssichere Snapshots bieten unveränderlichen Schutz, der nicht gelöscht werden kann. Da FabricPool die Möglichkeit zum Löschen von Daten benötigt, können FabricPool und Snapshot-Sperren nicht auf demselben Volume aktiviert werden.

- SMtape
- SnapMirror Active Sync für SAN

Snapshot-Sperre beim Erstellen eines Volumes aktivieren

Ab ONTAP 9.12.1 kann die Snapshot-Sperre beim Erstellen eines neuen Volumes oder beim Ändern eines vorhandenen Volumes mithilfe der `-snapshot-locking-enabled` Option zusammen mit den `volume create` und `volume modify` Befehlen in der CLI aktiviert werden. Ab ONTAP 9.13.1 kann der System Manager verwendet werden, um die Snapshot-Sperre zu aktivieren.

System Manager

1. Navigieren Sie zu **Storage > Volumes** und wählen Sie **Add**.
2. Im Fenster **Volume hinzufügen Weitere Optionen** auswählen.
3. Den Datenträgernamen, die Größe, die Exportrichtlinie und den Freigabenamen eingeben.
4. **Snapshot-Sperre aktivieren** auswählen. Diese Auswahlmöglichkeit wird nicht angezeigt, wenn die SnapLock Lizenz nicht installiert ist.
5. Falls diese Option noch nicht aktiviert ist, **SnapLock Compliance-Uhr initialisieren** auswählen.
6. Speichern Sie Ihre Änderungen.
7. Im Fenster **Volumes** das aktualisierte Volume auswählen und **Übersicht** wählen.
8. Es wird geprüft, ob **SnapLock Snapshot Locking** als **Aktiviert** angezeigt wird.

CLI

1. Zum Erstellen eines neuen Volumes und Aktivieren der Snapshot-Sperre ist folgender Befehl einzugeben:

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   Der folgende Befehl aktiviert die Snapshot-Sperre auf einem neuen Volume mit dem Namen vol1:

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
-locking-enabled true
Warning: snapshot locking is being enabled on volume "vol1" in
Vserver "vs1". It cannot be disabled until all locked snapshots are
past their expiry time. A volume with unexpired locked snapshots
cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

Aktivieren der Snapshot-Sperre auf einem vorhandenen Volume

Ab ONTAP 9.12.1 ist es möglich, die Snapshot-Sperre für ein vorhandenes Volume mithilfe der ONTAP CLI zu aktivieren. Ab ONTAP 9.13.1 kann die Snapshot-Sperre für ein vorhandenes Volume mithilfe des System Manager aktiviert werden.

System Manager

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie ⋮ und dann **Bearbeiten > Volume**.
3. Im Fenster **Volume bearbeiten** befindet sich der Abschnitt Snapshots (Lokal) Einstellungen, dort kann **Snapshot-Sperre aktivieren** ausgewählt werden.

   Diese Auswahlmöglichkeit wird nicht angezeigt, wenn die SnapLock Lizenz nicht installiert ist.
4. Falls diese Option noch nicht aktiviert ist, **SnapLock Compliance-Uhr initialisieren** auswählen.
5. Speichern Sie Ihre Änderungen.
6. Im Fenster **Volumes** das aktualisierte Volume auswählen und **Übersicht** wählen.
7. Es wird geprüft, ob **SnapLock Snapshot-Sperrung** als **Aktiviert** angezeigt wird.

CLI

1. Um ein vorhandenes Volume zu modifizieren, um die Snapshot-Sperre zu aktivieren, ist folgender Befehl einzugeben:

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

Eine Richtlinie für gesperrte Snapshots erstellen und die Aufbewahrungsfrist anwenden

Ab ONTAP 9.12.1 ist es möglich, Snapshot-Richtlinien zu erstellen, um eine Aufbewahrungsdauer für Snapshots festzulegen und die Richtlinie auf ein Volume anzuwenden, sodass Snapshots für den angegebenen Zeitraum gesperrt werden. Ein Snapshot kann auch durch das manuelle Festlegen einer Aufbewahrungsdauer gesperrt werden. Ab ONTAP 9.13.1 kann der System Manager verwendet werden, um Snapshot-Sperrrichtlinien zu erstellen und sie auf ein Volume anzuwenden.

Erstellen einer Snapshot-Sperrrichtlinie

System Manager

1. Zu **Speicher > Speicher-VMs** navigieren und eine Speicher-VM auswählen.
2. **Einstellungen** auswählen.
3. **Snapshot-Richtlinien** suchen und → auswählen.
4. Im Fenster **Snapshot-Richtlinie hinzufügen** den Richtliniennamen eingeben.
5. Wählen Sie + Add .
6. Geben Sie die Details des Snapshot-Zeitplans an, einschließlich des Zeitplannamens, der maximalen Anzahl der aufzubewahrenden Snapshots und der SnapLock Aufbewahrungsdauer.
7. Geben Sie in der Spalte **SnapLock Aufbewahrungsdauer** die Anzahl der Stunden, Tage, Monate oder Jahre ein, für die die Snapshots aufbewahrt werden sollen. Beispielsweise sperrt eine Snapshot-Richtlinie mit einer Aufbewahrungsdauer von fünf Tagen einen Snapshot für fünf Tage ab dem Zeitpunkt seiner Erstellung; während dieser Zeit kann er nicht gelöscht werden. Folgende Aufbewahrungsdauerbereiche werden unterstützt:
   - Jahre: 0 - 100
   - Monate: 0 - 1200
   - Tage: 0 - 36500
   - Stunden: 0 - 24
8. Speichern Sie Ihre Änderungen.

CLI

1. Zum Erstellen einer Snapshot-Richtlinie ist folgender Befehl einzugeben:

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   Der folgende Befehl erstellt eine Snapshot-Sperrrichtlinie:

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

   Ein Snapshot wird nicht ersetzt, wenn er sich in aktiver Aufbewahrung befindet, das heißt, die Aufbewahrungsanzahl wird nicht berücksichtigt, wenn gesperrte Snapshots vorhanden sind, die noch nicht abgelaufen sind.

Eine Sperrrichtlinie auf ein Volume anwenden

System Manager

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie ⋮ und dann **Bearbeiten > Volume**.
3. Im Fenster **Volume bearbeiten Snapshots planen** auswählen.

4. Die Richtlinie zum Sperren von Snapshots aus der Liste auswählen.
5. Falls die Snapshot-Sperre noch nicht aktiviert ist, **Snapshot-Sperre aktivieren** auswählen.
6. Speichern Sie Ihre Änderungen.

CLI

1. Um eine Snapshot-Sperrrichtlinie auf ein vorhandenes Volume anzuwenden, ist folgender Befehl einzugeben:

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

Aufbewahrungsfrist bei manueller Snapshot-Erstellung anwenden

Sie können beim manuellen Erstellen eines Snapshots eine Aufbewahrungsdauer festlegen. Snapshot-Sperre muss für das Volume aktiviert sein, andernfalls wird die Einstellung der Aufbewahrungsdauer ignoriert.

System Manager

1. Zu **Speicher > Volumes** navigieren und ein Volume auswählen.
2. Auf der Seite mit den Volumendetails die Registerkarte **Snapshots** auswählen.
3. Wählen Sie + Add .
4. Geben Sie den Snapshot-Namen und die SnapLock Ablaufzeit ein. Es besteht die Möglichkeit, den Kalender auszuwählen, um das Ablaufdatum und die Uhrzeit der Aufbewahrung festzulegen.
5. Speichern Sie Ihre Änderungen.
6. Auf der Seite **Volumes > Snapshots Anzeigen/Ausblenden** auswählen und **SnapLock Expiration Time** wählen, um die Spalte **SnapLock Expiration Time** anzuzeigen und zu überprüfen, ob die Aufbewahrungszeit eingestellt ist.

CLI

1. Um einen Snapshot manuell zu erstellen und eine Sperr-Aufbewahrungsfrist anzuwenden, ist folgender Befehl einzugeben:

   ```
   volume snapshot create -volume <volume_name> -snapshot <snapshot name>
   -snaplock-expiry-time <expiration_date_time>
   ```

   Der folgende Befehl erstellt einen neuen Snapshot und legt die Aufbewahrungsdauer fest:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Aufbewahrungszeitraum auf einen vorhandenen Snapshot anwenden

System Manager

1. Zu **Speicher > Volumes** navigieren und ein Volume auswählen.
2. Auf der Seite mit den Volumendetails die Registerkarte **Snapshots** auswählen.

3. Wählen Sie den Snapshot aus, wählen Sie ⋮ und dann **Modify SnapLock Expiration Time**. Es besteht die Möglichkeit, den Kalender auszuwählen, um das Ablaufdatum und die Uhrzeit der Aufbewahrung festzulegen.
4. Speichern Sie Ihre Änderungen.
5. Auf der Seite **Volumes > Snapshots Anzeigen/Ausblenden** auswählen und **SnapLock Expiration Time** wählen, um die Spalte **SnapLock Expiration Time** anzuzeigen und zu überprüfen, ob die Aufbewahrungszeit eingestellt ist.

CLI

1. Um einem vorhandenen Snapshot manuell eine Aufbewahrungsfrist zuzuweisen, ist folgender Befehl einzugeben:

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   Im folgenden Beispiel wird eine Aufbewahrungsfrist auf einen bestehenden Snapshot angewendet:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Eine bestehende Richtlinie anpassen, um die langfristige Aufbewahrung anzuwenden.

In einer SnapMirror Beziehung kann eine Aufbewahrungsdauer für eine Mirror-Vault-Richtlinienregel festgelegt werden, und die Aufbewahrungsdauer wird auf Snapshots angewendet, die auf das Ziel repliziert werden, wenn auf dem Zielvolume die Snapshot-Sperre aktiviert ist. Die Aufbewahrungsdauer hat Vorrang vor der Aufbewahrungsanzahl; beispielsweise werden Snapshots, deren Ablaufdatum noch nicht erreicht ist, auch dann aufbewahrt, wenn die Aufbewahrungsanzahl überschritten wurde.

Ab ONTAP 9.14.1 können Sie eine vorhandene SnapMirror Richtlinie ändern, indem Sie eine Regel hinzufügen, mit der die Langzeitaufbewahrung von Snapshots festgelegt wird. Die Regel überschreibt die standardmäßige Volume Aufbewahrungsdauer bei Nicht-SnapLock Vault- und Mirror-Vault-SnapMirror Ziel-Volumes.

1. Einer bestehenden SnapMirror Richtlinie eine Regel hinzufügen:

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

   Das folgende Beispiel erstellt eine Regel, die der bestehenden Richtlinie mit dem Namen „snapvault“ eine Aufbewahrungsfrist von 6 Monaten zuweist:

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

   Weitere Informationen zu `snapmirror policy add-rule` finden sich in der "ONTAP-Befehlsreferenz".

Konsistenzgruppen

Informationen zu ONTAP Konsistenzgruppen

Eine Konsistenzgruppe ist eine Sammlung von Volumes, die als eine Einheit verwaltet werden. In ONTAP ermöglichen Konsistenzgruppen eine einfache Verwaltung und gewährleisten den Schutz von Anwendungsworkloads, die sich über mehrere Volumes erstrecken.

Sie können Konsistenzgruppen verwenden, um Ihre Speicherverwaltung zu vereinfachen. Stellen Sie sich vor, Sie haben eine wichtige Datenbank, die sich über zwanzig LUNs erstreckt. Die LUNs könnten einzeln verwaltet oder als ein einziger Datensatz behandelt und in einer einzigen Konsistenzgruppe organisiert werden.

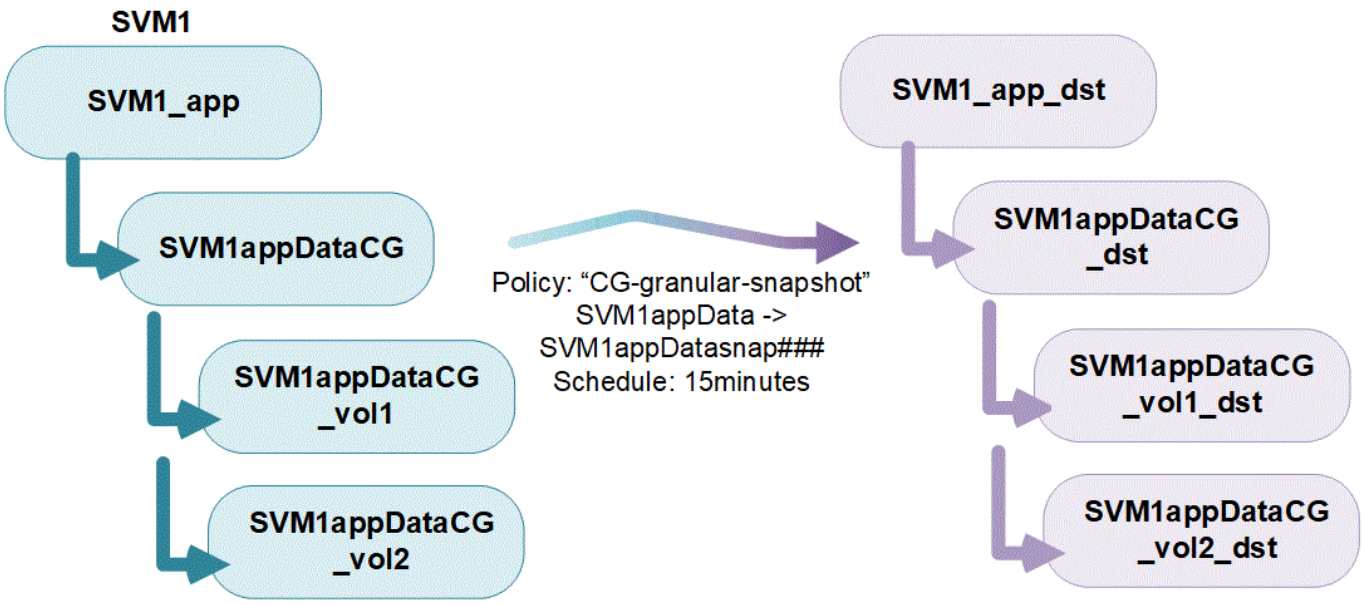
Konsistenzgruppen erleichtern das Management von Anwendungsworkloads, indem sie einfach konfigurierbare lokale und Remote-Datensicherungsstrategien sowie gleichzeitige absturzkonsistente oder applikationskonsistente Snapshots einer Sammlung von Volumes zu einem bestimmten Zeitpunkt bereitstellen. Snapshots einer Konsistenzgruppe ermöglichen die Wiederherstellung eines gesamten Anwendungsworkloads.

Informationen zu Konsistenzgruppen

Konsistenzgruppen unterstützen beliebige FlexVol volume unabhängig vom Protokoll (NAS, SAN oder NVMe) und können über die ONTAP REST API oder im System Manager unter dem Menüpunkt **Storage > Consistency Groups** verwaltet werden. Ab ONTAP 9.14.1 können Konsistenzgruppen mit der ONTAP CLI verwaltet werden.

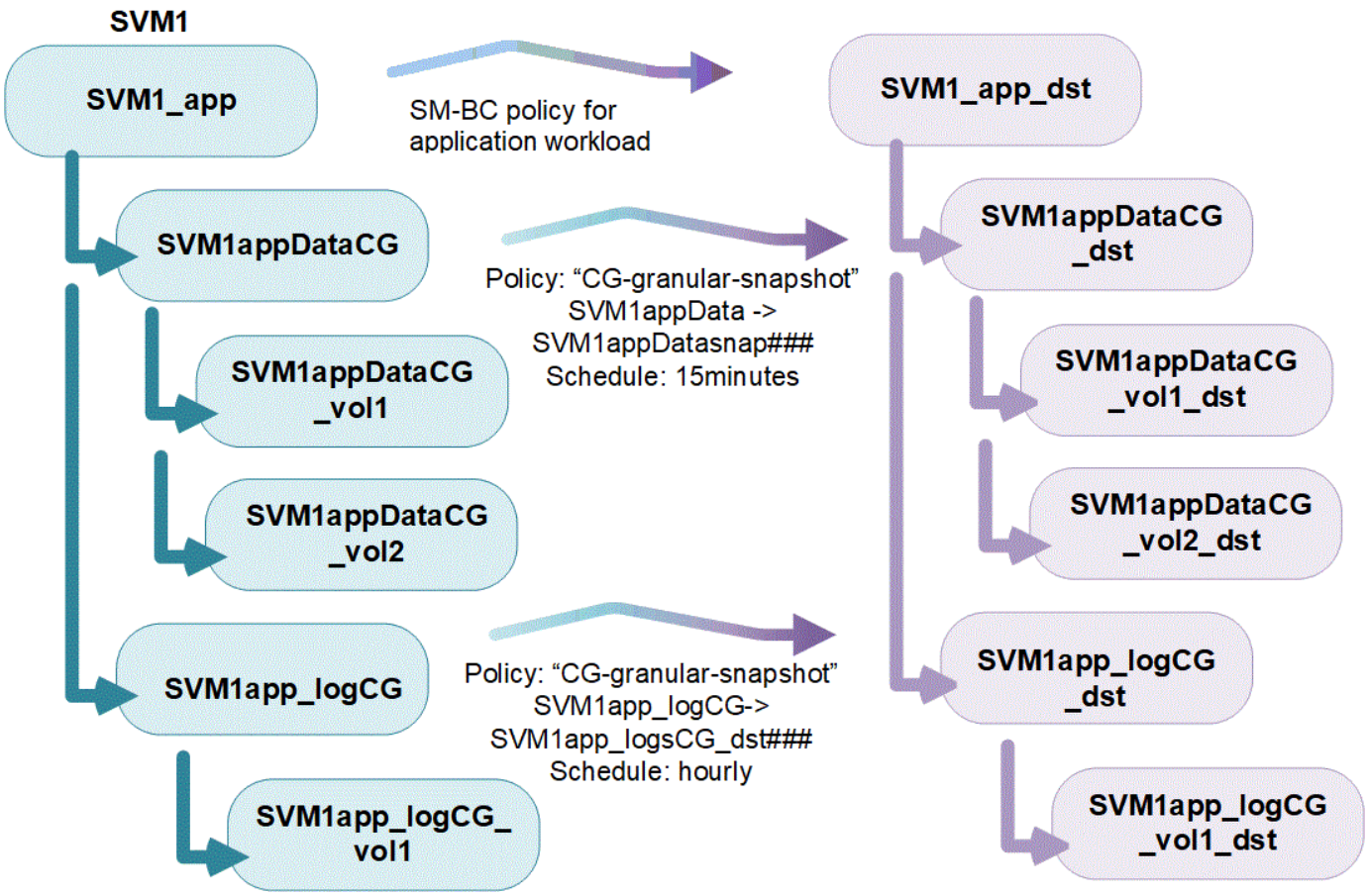
Konsistenzgruppen können als einzelne Einheiten, als Sammlung von Volumes, oder in einer hierarchischen Beziehung existieren, die aus anderen Konsistenzgruppen besteht. Einzelne Volumes können über eine eigene volume-granulare Snapshot-Policy verfügen. Zusätzlich kann eine Konsistenzgruppen-weite Snapshot-Policy vorhanden sein. Die Konsistenzgruppe kann nur eine SnapMirror active sync Beziehung und eine gemeinsame SnapMirror Policy haben, mit der die gesamte Konsistenzgruppe wiederhergestellt werden kann.

Das folgende Diagramm veranschaulicht, wie eine einzelne Konsistenzgruppe verwendet werden kann. Die Daten für eine Anwendung, die auf `SVM1` gehostet wird, erstrecken sich über zwei Volumes: `vol1` und `vol2`. Eine Snapshot-Richtlinie für die Konsistenzgruppe erfasst alle 15 Minuten Snapshots der Daten.



Größere Anwendungsworkloads erfordern möglicherweise mehrere Konsistenzgruppen. In solchen Situationen können hierarchische Konsistenzgruppen erstellt werden, wobei eine einzelne Konsistenzgruppe die untergeordneten Komponenten einer übergeordneten Konsistenzgruppe bildet. Die übergeordnete Konsistenzgruppe kann bis zu fünf untergeordnete Konsistenzgruppen enthalten. Wie bei einzelnen Konsistenzgruppen kann eine Remote SnapMirror active sync Datensicherungsstrategie auf die gesamte Konfiguration der Konsistenzgruppen (übergeordnete und untergeordnete) angewendet werden, um den Anwendungsworkload wiederherzustellen.

Im folgenden Beispiel wird eine Anwendung auf `SVM1` gehostet. Der Administrator hat eine übergeordnete Konsistenzgruppe erstellt, `SVM1_app`, die zwei untergeordnete Konsistenzgruppen umfasst: `SVM1appDataCG` für die Daten und `SVM1app_logCG` für die Protokolle. Jede untergeordnete Konsistenzgruppe verfügt über eine eigene Snapshot-Strategie. Snapshots der Volumes in `SVM1appDataCG` werden alle 15 Minuten erstellt. Snapshots von `SVM1app_logCG` werden stündlich erstellt. Die übergeordnete Konsistenzgruppe `SVM1_app` verfügt über eine SnapMirror active sync-Strategie, die die Daten repliziert, um die fortlaufende Bereitstellung im Katastrophenfall sicherzustellen.



Ab ONTAP 9.12.1 unterstützen Konsistenzgruppen Klonen und die Änderung der Mitglieder der Konsistenzgruppe durch Hinzufügen oder Entfernen von Volumes sowohl im System Manager als auch in der ONTAP REST API. Ab ONTAP 9.12.1 unterstützt die ONTAP REST API außerdem:

- Erstellen von Konsistenzgruppen mit neuen NFS- oder SMB-Volumes oder NVMe-Namespaces.
- Hinzufügen neuer oder vorhandener NFS- oder SMB-Volumes oder NVMe-Namespaces zu bestehenden Konsistenzgruppen.

Weitere Informationen zur ONTAP REST API finden Sie unter "ONTAP REST API Referenzdokumentation".

Konsistenzgruppen überwachen

Ab ONTAP 9.13.1 bieten Konsistenzgruppen Echtzeit- und historische Kapazitäts- und Leistungsüberwachung und ermöglichen Einblicke in die Performance von Anwendungen und einzelnen Konsistenzgruppen.

Die Überwachungsdaten werden alle fünf Minuten aktualisiert und bis zu einem Jahr lang gespeichert. Es lassen sich Kennzahlen für Folgendes nachverfolgen:

- Leistung: IOPS, Latenz und Durchsatz
- Kapazität: Größe, logisch verwendet, verfügbar

Überwachungsdaten sind auf der Registerkarte **Übersicht** im Konsistenzgruppen-Menü des System Managers oder über die ONTAP REST API abrufbar. Ab ONTAP 9.14.1 lassen sich Konsistenzgruppenmetriken mit der ONTAP CLI über den `consistency-group metrics show` Befehl anzeigen. Weitere Informationen zu `consistency-group metrics show` finden sich in der "ONTAP-Befehlsreferenz".

In ONTAP 9.13.1 können historische Metriken nur über die ONTAP REST API abgerufen werden. Ab ONTAP 9.14.1 sind historische Metriken auch im System Manager verfügbar.

Konsistenzgruppen schützen

Konsistenzgruppen bieten applikationskonsistente Schutzmechanismen und gewährleisten die Konsistenz Ihrer Daten über mehrere Volumes oder LIFs hinweg. Beim Erstellen eines Snapshots einer Konsistenzgruppe wird ein „Fence“ auf der Konsistenzgruppe gesetzt. Der Fence initiiert eine Warteschlange für Ein-/Ausgabe, bis der Snapshot-Vorgang abgeschlossen ist, und stellt so die zeitpunktgenaue Konsistenz der Daten über alle Entitäten in der Konsistenzgruppe sicher. Der Fence kann während Snapshot-Erstellungsvorgängen, wie etwa einer geplanten Snapshot-Richtlinie oder der Erstellung eines Snapshots mit System Manager, zu einem vorübergehenden Anstieg der Latenz führen.

Die Art des für Konsistenzgruppen verfügbaren Datenschutzes variiert je nach Ihrer ONTAP Version.

Verfügbar ab ONTAP…	Datensicherung für Konsistenzgruppen
9.20.1	"SnapLock für SnapVault aus nicht-SnapLock Volumes"
9.14.1	"SVM Disaster Recovery"
9.13.1	SnapMirror asynchron
9.10.1	• Snapshot Richtlinien • SnapMirror Active Sync

Das Erstellen einer Konsistenzgruppe aktiviert den Schutz nicht automatisch. Lokale und Remote-Datensicherungsstrategien können beim Erstellen oder nach dem Erstellen einer Konsistenzgruppe festgelegt werden.

Zum Konfigurieren des Schutzes einer Konsistenzgruppe siehe "Eine Konsistenzgruppe schützen".

Um Fernschutz nutzen zu können, müssen die Voraussetzungen für SnapMirror Active Sync erfüllt sein.

SnapMirror active sync-Beziehungen können auf Volumes, die für den NAS-Zugriff eingebunden sind, nicht hergestellt werden.

Unterstützung der Multi-Admin-Verifizierung für Konsistenzgruppen

Ab ONTAP 9.16.1 kann die Multi-Admin-Verifizierung (MAV) mit Konsistenzgruppen verwendet werden, um sicherzustellen, dass bestimmte Vorgänge, wie das Erstellen, Ändern oder Löschen von Konsistenzgruppen, nur nach Genehmigung durch die zuständigen Administratoren ausgeführt werden können. Dadurch wird verhindert, dass kompromittierte, böswillige oder unerfahrene Administratoren unerwünschte Änderungen an bestehenden Konfigurationen vornehmen.

"Mehr erfahren"

Konsistenzgruppen in MetroCluster Konfigurationen

Ab ONTAP 9.11.1 ist die Bereitstellung von Konsistenzgruppen mit neuen Volumes auf einem Cluster innerhalb einer MetroCluster Konfiguration möglich. Diese Volumes werden auf gespiegelten Aggregaten bereitgestellt.

Nach der Bereitstellung können Volumes, die Konsistenzgruppen zugeordnet sind, zwischen gespiegelten und

ungespiegelten Aggregaten verschoben werden. Daher können Volumes, die Konsistenzgruppen zugeordnet sind, auf gespiegelten Aggregaten, ungespiegelten Aggregaten oder auf beiden liegen. Gespiegelte Aggregate, die Volumes enthalten, die Konsistenzgruppen zugeordnet sind, können in ungespiegelte Aggregate umgewandelt werden. Ebenso können ungespiegelte Aggregate, die Volumes enthalten, die Konsistenzgruppen zugeordnet sind, für die Spiegelung aktiviert werden.

Volumes und Snapshots, die Konsistenzgruppen auf gespiegelten Aggregaten zugeordnet sind, werden an den Remote-Standort (Standort B) repliziert. Die Inhalte der Volumes an Standort B gewährleisten die Schreibreihenfolge für die Konsistenzgruppe, sodass im Katastrophenfall eine Wiederherstellung von Standort B möglich ist. Auf Snapshots von Konsistenzgruppen kann mit der Konsistenzgruppe über die ONTAP REST API und den System Manager auf Clustern mit ONTAP 9.11.1 oder neuer zugegriffen werden. Ab ONTAP 9.14.1 ist auch der Zugriff auf Snapshots mit der ONTAP CLI möglich.

Wenn sich einige oder alle Volumes, die einer Konsistenzgruppe zugeordnet sind, auf nicht gespiegelten Aggregaten befinden, auf die derzeit nicht zugegriffen werden kann, verhalten sich GET- oder DELETE-Operationen auf der Konsistenzgruppe so, als wären die lokalen Volumes oder die hostenden Aggregate offline.

Konsistenzgruppenkonfigurationen für die Replikation

Wenn auf Standort B ONTAP 9.10.1 oder eine ältere Version ausgeführt wird, werden nur die Volumes, die den auf gespiegelten Aggregaten befindlichen Konsistenzgruppen zugeordnet sind, auf Standort B repliziert. Die Konsistenzgruppen-Konfigurationen werden nur auf Standort B repliziert, wenn auf beiden Standorten ONTAP 9.11.1 oder eine neuere Version ausgeführt wird. Nach dem Upgrade von Standort B auf ONTAP 9.11.1 werden die Daten der Konsistenzgruppen auf Standort A, deren zugehörige Volumes vollständig auf gespiegelten Aggregaten liegen, auf Standort B repliziert.

> Es wird empfohlen, für gespiegelte Aggregate mindestens 20 % freien Speicherplatz vorzuhalten, um optimale Speicherleistung und Verfügbarkeit zu gewährleisten. Obwohl für nicht gespiegelte Aggregate 10 % empfohlen werden, kann das Dateisystem die zusätzlichen 10 % des Speicherplatzes nutzen, um inkrementelle Änderungen aufzufangen. Inkrementelle Änderungen erhöhen die Speicherauslastung gespiegelter Aggregate aufgrund der Redirect-on-Write-Snapshot-basierten Architektur von ONTAP. Die Nichtbeachtung dieser Best Practices kann sich negativ auf die Leistung auswirken.

Upgrade-Überlegungen

Beim Upgrade auf ONTAP 9.10.1 oder höher werden Konsistenzgruppen, die in ONTAP 9.8 und 9.9.1 mit SnapMirror active sync (früher als SnapMirror Business Continuity bezeichnet) erstellt wurden, automatisch aktualisiert und können anschließend in System Manager oder in der ONTAP REST API unter **Storage > Consistency Groups** verwaltet werden. Weitere Informationen zum Upgrade von ONTAP 9.8 oder 9.9.1 enthält "SnapMirror Überlegungen zum Upgrade und zur Rücksetzung von active sync".

> Snapshots, die mit den ONTAPI-Befehlen `cg-start` und `cg-commit` erstellt wurden, werden nicht als Konsistenzgruppe-Snapshots erkannt und können daher weder über die Konsistenzgruppe-Oberfläche des System Manager noch über die Konsistenzgruppe-Endpunkte in der ONTAP REST API verwaltet werden. Ab ONTAP 9.14.1 können diese Snapshots auf das Zielvolume gespiegelt werden, wenn eine SnapMirror asynchron Richtlinie verwendet wird. Weitere Informationen finden sich unter Asynchrones SnapMirror konfigurieren.

Unterstützte Funktionen nach Version

Beginnend mit ONTAP…	Unterstützte Funktionen
9.20.1	SnapLock für SnapVault Schutz auf Sekundärsystemen
9.16.1	Multi-Admin-Verifizierung
9.14.1	• SVM Disaster Recovery (nur einzelne Konsistenzgruppe) • CLI-Unterstützung
9.13.1	• Volumes zwischen untergeordneten Konsistenzgruppen verschieben • Konsistenzgruppe Geometrie ändern • Überwachung • SnapMirror asynchron (nur einzelne Konsistenzgruppen)
9.12.1	• Volumes hinzufügen und entfernen • Anwendungs- und Komponententags • Konsistenzgruppen klonen • Erstellen von CGs mit neuen NAS Volumes (nur REST API) • Erstellen von CGs mit NVMe Namespaces (nur REST API)
9.11.1	• MetroCluster Konfigurationen • Zwei-Phasen-Commits (nur REST API)
9.10.1	• Hierarchische Konsistenzgruppen • Lokaler Schutz mit Snapshots • SnapMirror Active Sync

Weitere Informationen zu Konsistenzgruppen



Verwandte Informationen

- "ONTAP Automatisierungsdokumentation"
- SnapMirror Active Sync
- SnapMirror asynchrone Grundlagen der Notfallwiederherstellung
- "MetroCluster Dokumentation"
- "Multi-Admin-Verifizierung"
- "ONTAP-Befehlsreferenz"

Objektgrenzen für ONTAP Konsistenzgruppen

Bei der Planung und Verwaltung Ihrer Konsistenzgruppen sind die Objektgrenzen sowohl auf Clusterebene als auch auf Ebene der übergeordneten oder untergeordneten Konsistenzgruppe zu berücksichtigen.

Durchgesetzte Grenzwerte

Die folgende Tabelle enthält die Grenzwerte für Konsistenzgruppen. Für Konsistenzgruppen, die SnapMirror active sync verwenden, gelten separate Grenzwerte. Weitere Informationen finden sich unter "SnapMirror active sync-Grenzen".

Limit	Umfang	Minimum	Maximal

Anzahl der Konsistenzgruppen	Cluster	0	• Wenn SnapMirror active sync nicht aktiviert ist, gilt dasselbe wie die maximale Volume-Anzahl im Cluster • Wenn die aktive Synchronisierung von SnapMirror aktiviert ist, 50 Konsistenzgruppen
Anzahl der übergeordneten Konsistenzgruppen	Cluster	0	Entspricht der maximalen Volume-Anzahl im Cluster
Anzahl der individuellen und übergeordneten Konsistenzgruppen	Cluster	0	Entspricht der maximalen Volume-Anzahl im Cluster
Anzahl der Volumes in einer Konsistenzgruppe	Einzelne Konsistenzgruppe	1 Volume	• In ONTAP 9.20.1 und höher: 256 Volumes • In ONTAP 9.19.1 und früheren Versionen: 80 Volumes
Anzahl der Volumes in einer Konsistenzgruppe mit SnapMirror asynchron	Einzelne Konsistenzgruppe	1 Volume	• In ONTAP 9.15.1 und höher: 80 Volumes • In ONTAP 9.13.1 und 9.14.1: 16 Volumes
Anzahl der Volumes im untergeordneten Element einer übergeordneten Konsistenzgruppe	Übergeordnete Konsistenzgruppe	1 Volume	• In ONTAP 9.20.1 und höher: 256 Volumes • In ONTAP 9.19.1 und früheren Versionen: 80 Volumes
Anzahl der Volumes in einer untergeordneten Konsistenzgruppe	Untergeordnete Konsistenzgruppe	1 Volume	• In ONTAP 9.20.1 und höher: 256 Volumes • In ONTAP 9.19.1 und früheren Versionen: 80 Volumes
Anzahl der Kind-Konsistenzgruppen in einer Eltern Konsistenzgruppe	Übergeordnete Konsistenzgruppe	1 Konsistenzgruppe	• In ONTAP 9.20.1 und höher: 64 Konsistenzgruppen • In ONTAP 9.19.1 und früheren Versionen: 5 Konsistenzgruppen

Anzahl der SVM Notfallwiederherstellungsbeziehungen, bei denen eine Konsistenzgruppe existiert (verfügbar ab ONTAP 9.14.1)	Cluster	0	32

Nicht durchgesetzte Beschränkungen

Der minimal unterstützte Snapshot-Zeitplan für Konsistenzgruppen beträgt 30 Minuten. Dies basiert auf "Tests für FlexGroup Volumes", die dieselbe Snapshot-Infrastruktur wie Konsistenzgruppen verwenden.

Eine einzelne ONTAP Konsistenzgruppe konfigurieren

Konsistenzgruppen können mit bestehenden Volumes oder neuen LUNs oder Volumes erstellt werden (abhängig von der Version von ONTAP). Ein Volume oder eine LUN kann jeweils nur einer Konsistenzgruppe zugeordnet sein.

Über diese Aufgabe

- In ONTAP 9.10.1 bis 9.11.1 wird das Ändern der Mitgliedsvolumes einer Konsistenzgruppe nach deren Erstellung nicht unterstützt.

  Ab ONTAP 9.12.1 ist es möglich, die Mitgliedsvolumes einer Konsistenzgruppe zu ändern. Weitere Informationen zu diesem Vorgang finden sich unter Eine Konsistenzgruppe ändern.

- Ab ONTAP 9.17.1 kann das NVMe-Protokoll ausgewählt werden, um einen Host einem NVMe-Subsystem für VMware-Workloads in einer SnapMirror active sync Konfiguration zuzuordnen.

Eine Konsistenzgruppe mit neuen LUNs oder Volumes erstellen

In ONTAP 9.10.1 bis 9.12.1 kann eine Konsistenzgruppe mit neuen LUNs erstellt werden. Ab ONTAP 9.13.1 unterstützt System Manager auch das Erstellen einer Konsistenzgruppe mit neuen NVMe Namespaces oder neuen NAS Volumes. (Dies wird in der ONTAP REST API ab ONTAP 9.12.1 ebenfalls unterstützt.)

System Manager (ONTAP 9.16.1 und früher)

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. **+Hinzufügen** auswählen und anschließend das Protokoll für das Speicherobjekt wählen.

   In ONTAP 9.10.1 bis 9.12.1 ist die einzige Option für ein neues Speicherobjekt **Using new LUNs**. Ab ONTAP 9.13.1 unterstützt System Manager das Erstellen von Konsistenzgruppen mit neuen NVMe-Namespaces und neuen NAS-Volumes.

3. Die Konsistenzgruppe benennen. Die Anzahl der Volumes oder LUNs und die Kapazität pro Volume oder LUN angeben.
   a. **Anwendungstyp**: Bei Verwendung von ONTAP 9.12.1 oder höher kann ein Anwendungstyp ausgewählt werden. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ **Sonstige** zugewiesen. Weitere Informationen zur Kennzeichnung der Konsistenz sind in Anwendungs- und Komponententags verfügbar. Wenn eine Konsistenzgruppe mit einer Remote Datensicherungsstrategie erstellt werden soll, ist **Sonstige** zu verwenden.

b. Für **neue LUNs**: Das Host-Betriebssystem und das LUN-Format auswählen. Die Host-Initiatorinformationen eingeben.

c. Für **neue NAS-Volumes** sollte die passende Exportoption (NFS oder SMB/CIFS) entsprechend der NAS-Konfiguration Ihrer SVM gewählt werden.

d. Für **neue NVMe Namespaces**: Das Host-Betriebssystem und das NVMe Subsystem auswählen.

4. Zum Konfigurieren von Datensicherungsstrategien, Hinzufügen einer untergeordneten Konsistenzgruppe oder Festlegen von Zugriffsberechtigungen steht **Weitere Optionen** zur Verfügung.
5. **Speichern** auswählen.
6. Die Erstellung der Konsistenzgruppe lässt sich bestätigen, indem zum Hauptmenü der Konsistenzgruppe zurückgekehrt wird, wo sie nach Abschluss des Vorgangs angezeigt wird. Wurde eine Datensicherungsstrategie festgelegt, ist deren Anwendung an einem grünen Schild unter der entsprechenden Richtlinie, remote oder lokal, zu erkennen.

System Manager (ONTAP 9.17.1 und höher)

Schritte

1. **Schutz > Konsistenzgruppen** auswählen.
2. **+Hinzufügen** auswählen und anschließend das Protokoll für das Speicherobjekt wählen.
3. Die Konsistenzgruppe benennen. Die Anzahl der Volumes oder LUNs und die Kapazität pro Volume oder LUN angeben. **Anwendungstyp**: Einen Anwendungstyp auswählen. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ **Sonstige** zugewiesen. Weitere Informationen zur Kennzeichnung der Konsistenz sind in Anwendungs- und Komponententags verfügbar. Wenn eine Konsistenzgruppe mit einer Remote Datensicherungsstrategie erstellt werden soll, ist **Sonstige** zu verwenden.

   a. Für **neue LUNs**: Das Host-Betriebssystem und das LUN-Format auswählen. Die Host-Initiatorinformationen eingeben.

   b. Für **neue NAS-Volumes** sollte die passende Exportoption (NFS oder SMB/CIFS) entsprechend der NAS-Konfiguration Ihrer SVM gewählt werden.

   c. Für **neue NVMe Namespaces**: Das Host-Betriebssystem und das NVMe Subsystem auswählen.

4. Zum Konfigurieren von Datensicherungsstrategien, Hinzufügen einer untergeordneten Konsistenzgruppe oder Festlegen von Zugriffsberechtigungen steht **Weitere Optionen** zur Verfügung.
5. **Speichern** auswählen.
6. Die Erstellung der Konsistenzgruppe lässt sich bestätigen, indem zum Hauptmenü der Konsistenzgruppe zurückgekehrt wird, wo sie nach Abschluss des Vorgangs angezeigt wird. Wurde eine Datensicherungsstrategie festgelegt, ist deren Anwendung an einem grünen Schild unter der entsprechenden Richtlinie, remote oder lokal, zu erkennen.

CLI

Ab ONTAP 9.14.1 kann eine neue Konsistenzgruppe mit neuen Volumes mithilfe der ONTAP CLI erstellt werden. Die spezifischen Parameter hängen davon ab, ob die Volumes SAN, NVMe oder NFS sind.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine Konsistenzgruppe mit NFS-Volumes erstellen

1. Konsistenzgruppe erstellen:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

Eine Konsistenzgruppe mit SAN-Volumes erstellen

1. Konsistenzgruppe erstellen:

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
   -lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
   ```

Eine Konsistenzgruppe mit NVMe-Namespaces erstellen

1. Konsistenzgruppe erstellen:

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency_group_name> -namespace <namespace_name> -volume-count <number>
   -namespace-count <number> -size <size> -subsystem <subsystem_name>
   ```

   Weitere Informationen zu `consistency-group create` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

1. Bestätigen Sie, dass Ihre Konsistenzgruppe mit dem `consistency-group show` Befehl erstellt wurde.

   Weitere Informationen zu `consistency-group show` finden sich in der "ONTAP-Befehlsreferenz".

Eine Konsistenzgruppe mit vorhandenen Volumes erstellen

Vorhandene Volumes können zur Erstellung einer Konsistenzgruppe verwendet werden.

System Manager (ONTAP 9.16.1 und früher)

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. **+Hinzufügen** und dann **Vorhandene Volumes verwenden** auswählen.
3. Die Konsistenzgruppe benennen und die Storage-VM auswählen.
   a. **Anwendungstyp**: Bei Verwendung von ONTAP 9.12.1 oder höher kann ein Anwendungstyp ausgewählt werden. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ **Sonstige** zugewiesen. Weitere Informationen zur Kennzeichnung der Konsistenz sind in Anwendungs- und Komponententags verfügbar. Wenn die Konsistenzgruppe eine SnapMirror active sync-Beziehung aufweist, ist **Sonstige** zu verwenden.

   > In Versionen von ONTAP vor ONTAP 9.15.1 wird SnapMirror active sync als SnapMirror Business Continuity bezeichnet.

4. Wählen Sie die vorhandenen Volumes aus, die einbezogen werden sollen. Nur Volumes, die noch keiner Konsistenzgruppe angehören, stehen zur Auswahl.

   > Wenn eine Konsistenzgruppe mit vorhandenen Volumes erstellt wird, unterstützt die

Konsistenzgruppe FlexVol Volumes. Volumes mit SnapMirror synchronen oder SnapMirror asynchronen Beziehungen können zu Konsistenzgruppen hinzugefügt werden, sind jedoch nicht konsistenzgruppenfähig. Konsistenzgruppen unterstützen keine S3 Buckets oder Storage-VMs mit SVMDR-Beziehungen.

5. **Speichern** auswählen.
6. Die Erstellung der Konsistenzgruppe lässt sich bestätigen, indem nach Abschluss des ONTAP-Jobs zum Hauptmenü der Konsistenzgruppe zurückgekehrt wird, wo sie erscheint. Falls eine Datensicherungsstrategie gewählt wurde, lässt sich deren korrekte Einstellung durch Auswahl der Konsistenzgruppe im Menü bestätigen. Wenn eine Datensicherungsstrategie festgelegt wurde, ist deren Anwendung daran zu erkennen, dass unter der entsprechenden Richtlinie, remote oder lokal, ein grünes Schild angezeigt wird.

CLI

Ab ONTAP 9.14.1 ist es möglich, eine Konsistenzgruppe mit vorhandenen Volumes mithilfe der ONTAP CLI zu erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Schritte

1. Den `consistency-group create`Befehl ausgeben. Der `-volumes` Parameter akzeptiert eine durch Kommas getrennte Liste von Volume-Namen.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

   Weitere Informationen zu `consistency-group create` finden sich in der "ONTAP-Befehlsreferenz".

2. Die Konsistenzgruppe kann mit dem `consistency-group show` Befehl angezeigt werden.

   Weitere Informationen zu `consistency-group show` finden sich in der "ONTAP-Befehlsreferenz".

Nächste Schritte

- Eine Konsistenzgruppe schützen
- Eine Konsistenzgruppe ändern
- Eine Konsistenzgruppe klonen

Eine hierarchische ONTAP Konsistenzgruppe konfigurieren

Hierarchische Konsistenzgruppen ermöglichen die Verwaltung großer Arbeitslasten, die sich über mehrere Volumes erstrecken, indem eine übergeordnete Konsistenzgruppe erstellt wird, die als Dach für untergeordnete Konsistenzgruppen dient.

Hierarchische Konsistenzgruppen haben ein übergeordnetes Element, das bis zu fünf einzelne Konsistenzgruppen enthalten kann. Hierarchische Konsistenzgruppen können unterschiedliche lokale

Snapshot-Richtlinien für verschiedene Konsistenzgruppen oder einzelne Volumes unterstützen. Wird eine Remote-Datensicherungsstrategie verwendet, gilt diese für die gesamte hierarchische Konsistenzgruppe (übergeordnetes Element und untergeordnete Elemente).

Ab ONTAP 9.13.1 ist es möglich, die Geometrie Ihrer Konsistenzgruppen ändern und Volumes zwischen untergeordneten Konsistenzgruppen verschieben.

Informationen zu Objektbeschränkungen für Konsistenzgruppen sind unter Objektgrenzen für Konsistenzgruppen zu finden.

Eine hierarchische Konsistenzgruppe mit neuen LUNs oder Volumes erstellen

Beim Erstellen einer hierarchischen Konsistenzgruppe kann sie mit neuen LUNs gefüllt werden. Ab ONTAP 9.13.1 können auch neue NVMe Namespaces und NAS Volumes verwendet werden.

System Manager

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. **+Hinzufügen** auswählen und anschließend das Protokoll für das Speicherobjekt wählen.

   In ONTAP 9.10.1 bis 9.12.1 ist die einzige Option für ein neues Speicherobjekt **Using new LUNs**. Ab ONTAP 9.13.1 unterstützt System Manager das Erstellen von Konsistenzgruppen mit neuen NVMe-Namespaces und neuen NAS-Volumes.

3. Die Konsistenzgruppe benennen. Die Anzahl der Volumes oder LUNs und die Kapazität pro Volume oder LUN angeben.
   a. **Anwendungstyp**: Bei Verwendung von ONTAP 9.12.1 oder höher kann ein Anwendungstyp ausgewählt werden. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ **Sonstige** zugewiesen. Weitere Informationen zur Kennzeichnung der Konsistenz sind in Anwendungs- und Komponententags verfügbar. Wenn eine Remote Datensicherungsstrategie verwendet werden soll, ist **Other** auszuwählen.
4. Das Host-Betriebssystem und das LUN-Format auswählen. Die Host-Initiatorinformationen eingeben.
   a. Für **neue LUNs**: Das Host-Betriebssystem und das LUN-Format auswählen. Die Host-Initiatorinformationen eingeben.
   b. Für **neue NAS-Volumes** sollte die passende Exportoption (NFS oder SMB/CIFS) entsprechend der NAS-Konfiguration Ihrer SVM gewählt werden.
   c. Für **neue NVMe Namespaces**: Das Host-Betriebssystem und das NVMe Subsystem auswählen.
5. Zum Hinzufügen einer untergeordneten Konsistenzgruppe **Weitere Optionen** auswählen und dann **+Untergeordnete Konsistenzgruppe hinzufügen** wählen.
6. Die Leistungsstufe, die Anzahl der LUNs oder Volumes sowie die Kapazität pro LUN oder Volume auswählen. Die entsprechenden Exportkonfigurationen oder Betriebssysteminformationen je nach verwendetem Protokoll angeben.
7. Optional kann eine lokale Snapshot-Richtlinie ausgewählt und die Zugriffsberechtigungen festgelegt werden.
8. Für bis zu fünf untergeordnete Konsistenzgruppen wiederholen.
9. **Speichern** auswählen.
10. Bestätigen Sie, dass Ihre Konsistenzgruppe erstellt wurde, indem Sie zum Hauptmenü der Konsistenzgruppen zurückkehren, wo sie angezeigt wird, sobald der ONTAP Job abgeschlossen ist.

Falls eine Datensicherungsstrategie festgelegt wurde, ist unter der entsprechenden Strategie, remote oder lokal, nachzusehen; dort sollte ein grünes Schild mit einem Häkchen angezeigt werden.

CLI

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Beim Erstellen einer hierarchischen Konsistenzgruppe in der CLI mit neuen Volumes ist jede untergeordnete Konsistenzgruppe einzeln zu erstellen.

Schritt

1. Die neue Konsistenzgruppe wird mit dem `consistency-group create` Befehl erstellt.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
   -count <number_of_volumes> -size <size>
   ```

2. Wenn Sie von der CLI dazu aufgefordert werden, bestätigen Sie, dass Sie die neue übergeordnete Konsistenzgruppe erstellen möchten. Drücken Sie `y`.
3. Optional kann Schritt 1 wiederholt werden, um weitere untergeordnete Konsistenzgruppen zu erstellen.

   Weitere Informationen zu `consistency-group create` finden sich in der "ONTAP-Befehlsreferenz".

Eine hierarchische Konsistenzgruppe mit vorhandenen Volumes erstellen

Bestehende Volumes lassen sich in einer hierarchischen Konsistenzgruppe organisieren.

System Manager

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. **+Hinzufügen** und dann **Vorhandene Volumes verwenden** auswählen.
3. Die Storage-VM auswählen.
4. Wählen Sie die vorhandenen Volumes aus, die einbezogen werden sollen. Nur Volumes, die noch keiner Konsistenzgruppe angehören, stehen zur Auswahl.
5. Um eine untergeordnete Konsistenzgruppe hinzuzufügen, **+Untergeordnete Konsistenzgruppe hinzufügen** auswählen. Die erforderlichen Konsistenzgruppen werden erstellt und automatisch benannt.
   a. **Komponententyp**: Wenn Sie ONTAP 9.12.1 oder höher verwenden, kann als Komponententyp „data“, „logs“ oder „other“ ausgewählt werden. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ **Sonstige** zugewiesen. Weitere Informationen zur Kennzeichnung der Konsistenz sind in Anwendungs- und Komponententags verfügbar. Bei Verwendung einer Remote Datensicherungsstrategie muss **Other** verwendet werden.

6. Vorhandene Volumes werden jeder Konsistenzgruppe zugewiesen.
7. Optional kann eine lokale Snapshot-Richtlinie ausgewählt werden.
8. Für bis zu fünf untergeordnete Konsistenzgruppen wiederholen.
9. **Speichern** auswählen.
10. Bestätigen Sie, dass Ihre Konsistenzgruppe erstellt wurde, indem Sie zum Hauptmenü der Konsistenzgruppen zurückkehren, wo sie angezeigt wird, sobald der ONTAP Job abgeschlossen ist. Falls eine Datensicherungsstrategie ausgewählt wurde, lässt sich deren korrekte Einstellung bestätigen, indem im Menü die entsprechende Konsistenzgruppe ausgewählt wird; unter dem passenden Richtlinientyp erscheint ein grünes Schild mit einem Häkchen.

CLI

Ab ONTAP 9.14.1 ist es möglich, eine hierarchische Konsistenzgruppe mithilfe der CLI zu erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Schritte

1. Eine neue übergeordnete Konsistenzgruppe bereitstellen und Volumes einer neuen untergeordneten Konsistenzgruppe zuweisen:

   ```
   consistency-group create -vserver <svm_name> -consistency-group
   <child_consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volumes <volume_names>
   ```

2. Geben Sie `y` ein, um zu bestätigen, dass Sie eine neue übergeordnete und untergeordnete Konsistenzgruppe erstellen möchten.

   Weitere Informationen zu `consistency-group create` finden sich in der "ONTAP-Befehlsreferenz".

Nächste Schritte

- Die Geometrie einer Konsistenzgruppe ändern
- Eine Konsistenzgruppe ändern
- Eine Konsistenzgruppe schützen

ONTAP Konsistenzgruppen schützen

Konsistenzgruppen bieten einfach zu verwaltenden lokalen und Remote-Schutz für SAN, NAS und NVMe-Anwendungen, die sich über mehrere Volumes erstrecken.

Das Erstellen einer Konsistenzgruppe aktiviert den Schutz nicht automatisch. Datensicherungsstrategien können zum Zeitpunkt der Erstellung oder nach dem Erstellen Ihrer Konsistenzgruppe festgelegt werden.

Die Art des für Konsistenzgruppen verfügbaren Datenschutzes variiert je nach Ihrer ONTAP Version.

Verfügbar ab ONTAP…	Datensicherung für Konsistenzgruppen
9.20.1	SnapLock für SnapVault aus nicht-SnapLock Volumes
9.14.1	SVM Disaster Recovery
9.13.1	SnapMirror asynchron
9.11.1	Konsistenzgruppen bieten Zwei-Phasen-Konsistenzgruppen-Snapshot-Erstellung. Der zweiphasige Snapshot-Vorgang führt eine Vorprüfung durch, um sicherzustellen, dass der Snapshot erfolgreich erfasst wird.
9.10.1	• Snapshot Richtlinien • SnapMirror Active Sync

Wenn Sie verschachtelte Konsistenzgruppen verwenden, können Sie unterschiedliche Datensicherungsstrategien für die übergeordnete und die untergeordnete Konsistenzgruppe festlegen.

Die Wiederherstellung kann für eine gesamte Konsistenzgruppe, eine einzelne Konsistenzgruppe in einer hierarchischen Konfiguration oder für einzelne Volumes innerhalb der Konsistenzgruppe erfolgen. Die Wiederherstellung erfolgt durch Auswahl der Konsistenzgruppe, die wiederhergestellt werden soll, Auswahl des Snapshot-Typs und anschließender Identifizierung des Snapshots, auf dem die Wiederherstellung basieren soll. Weitere Informationen zu diesem Prozess finden sich unter "Ein Volume aus einem früheren Snapshot wiederherstellen".

Eine lokale Snapshot-Richtlinie konfigurieren

Das Festlegen einer lokalen Snapshot Datensicherungsstrategie ermöglicht das Erstellen einer Richtlinie, die alle Volumes in einer Konsistenzgruppe umfasst.

Über diese Aufgabe

Der minimal unterstützte Snapshot-Zeitplan für Konsistenzgruppen beträgt 30 Minuten. Dies basiert auf "Tests für FlexGroup Volumes", die dieselbe Snapshot-Infrastruktur wie Konsistenzgruppen verwenden.

System Manager

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die von Ihnen erstellte Konsistenzgruppe im Menü „Konsistenzgruppe“ aus.
3. Oben rechts auf der Übersichtsseite für die Konsistenzgruppe die Option **Bearbeiten** auswählen.
4. Das Kontrollkästchen neben **Snapshots planen (lokal)** ist zu aktivieren.
5. Wählen Sie eine Snapshot-Richtlinie aus. Zum Konfigurieren einer neuen, benutzerdefinierten Richtlinie siehe "Eine benutzerdefinierte Datensicherungsstrategie erstellen".
6. **Speichern** auswählen.
7. Zurück zum Konsistenzgruppe Übersichtsmenü. In der linken Spalte unter **Snapshots (Lokal)** wird der Status als geschützt neben  angezeigt.

CLI

Ab ONTAP 9.14.1 lässt sich die Datensicherungsstrategie einer Konsistenzgruppe mithilfe der CLI ändern.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Schritt

1. Der folgende Befehl dient zum Festlegen oder Ändern der Datensicherungsstrategie:

   Wenn Sie die Datensicherungsstrategie einer untergeordneten Konsistenz ändern, müssen Sie die übergeordnete Konsistenzgruppe mithilfe des `-parent-consistency-group` *`parent_consistency_group_name`* Parameters identifizieren.

   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group_name`* `-snapshot-policy` *`policy_name`*

Erstellen Sie einen On-Demand-Snapshot

Falls Sie außerhalb einer regulären Datensicherungsstrategie eine Momentaufnahme Ihrer Konsistenzgruppe erstellen müssen, kann eine solche Momentaufnahme bei Bedarf erstellt werden.

System Manager

Schritte

1. Zu **Speicher** > **Konsistenzgruppen** navigieren.
2. Wählen Sie die Konsistenzgruppe aus, für die ein On-Demand-Snapshot erstellt werden soll.
3. Zum Tab **Snapshot copies** wechseln und anschließend **+Add** auswählen.
4. Geben Sie einen **Namen** und eine **SnapMirror Bezeichnung** an. Im Dropdown-Menü für **Konsistenz** steht **Anwendungskonsistent** oder **Absturzkonsistent** zur Auswahl.
5. **Speichern** auswählen.

CLI

Ab ONTAP 9.14.1 ist es möglich, mithilfe der CLI einen On-Demand-Snapshot einer Konsistenzgruppe zu erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Schritt

1. Snapshot erstellen:

   Standardmäßig ist der Snapshot-Typ absturzkonsistent. Der Snapshot-Typ kann mit dem optionalen `-type` Parameter geändert werden.

   `consistency-group snapshot create -vserver` *`svm_name`* `-consistency-group` *`consistency_group_name`* `-snapshot` *`snapshot_name`*

Snapshots von Zwei-Phasen-Konsistenzgruppen erstellen

Ab ONTAP 9.11.1 unterstützen Konsistenzgruppen zweiphasige Commits für die Erstellung von Konsistenzgruppen-Snapshots (CG-Snapshots), wobei vor dem Commit des Snapshots eine Vorprüfung durchgeführt wird. Diese Funktion ist nur mit der ONTAP REST API verfügbar.

Die zweiphasige Erstellung von CG-Snapshots ist nur für die Snapshot-Erstellung verfügbar, nicht für die Bereitstellung von Konsistenzgruppen oder die Wiederherstellung von Konsistenzgruppen.

Ein zweiphasiger CG-Snapshot unterteilt den Snapshot-Erstellungsprozess in zwei Phasen:

1. In der ersten Phase führt die API Vorabprüfungen durch und initiiert die Snapshot-Erstellung. Die erste Phase beinhaltet einen Zeitüberschreitung Parameter, der die Zeitspanne für die erfolgreiche Speicherung des Snapshots festlegt.
2. Wenn die Anfrage in Phase eins erfolgreich abgeschlossen wird, kann die zweite Phase innerhalb des festgelegten Intervalls nach der ersten Phase aufgerufen werden, wodurch der Snapshot an den entsprechenden Endpunkt übertragen wird.

Bevor Sie beginnen

- Um die Erstellung von CG-Snapshots in zwei Phasen zu nutzen, müssen alle Knoten im Cluster mit ONTAP 9.11.1 oder höher ausgeführt werden.
- Es wird jeweils nur ein aktiver Aufruf einer Snapshot-Operation für eine Konsistenzgruppe pro Konsistenzgruppeninstanz unterstützt, unabhängig davon, ob es sich um eine ein- oder zweiphasige Operation handelt. Der Versuch, eine Snapshot-Operation aufzurufen, während eine andere bereits ausgeführt wird, führt zu einem Fehler.
- Beim Aufruf der Snapshot-Erstellung kann optional ein Zeitüberschreitung Wert zwischen 5 und 120 Sekunden festgelegt werden. Wird kein Zeitüberschreitung Wert angegeben, tritt nach dem Standardwert von 7 Sekunden eine Zeitüberschreitung auf. In der ONTAP REST API wird der Zeitüberschreitung Wert mit dem `action_timeout` Parameter festgelegt. In der ONTAP CLI wird das `-timeout` Flag verwendet.

Schritte

Ein zweiphasiger Snapshot kann mit der ONTAP REST API oder, beginnend mit ONTAP 9.14.1, mit der ONTAP CLI abgeschlossen werden. Diese Operation wird im System Manager nicht unterstützt.

> Wenn Sie die Snapshot-Erstellung mit der ONTAP REST API aufrufen, muss der Snapshot mit der ONTAP REST API gespeichert werden. Wenn Sie die Snapshot-Erstellung mit der ONTAP CLI aufrufen, muss der Snapshot mit der ONTAP CLI gespeichert werden. Die Kombination verschiedener Methoden wird nicht unterstützt.

CLI

Ab ONTAP 9.14.1 ist es möglich, mit der CLI einen zweiphasigen Snapshot zu erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Schritte

1. Snapshot initiieren:

```
consistency-group snapshot start -vserver svm_name -consistency-group
consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
-write-fence {true|false}]
```

2. Es wird überprüft, ob die Momentaufnahme erstellt wurde:

```
consistency-group snapshot show
```

3. Snapshot übernehmen:

```
consistency-group snapshot commit svm_name -consistency-group
consistency_group_name -snapshot snapshot_name
```

API

1. Die Snapshot-Erstellung wird ausgelöst. Eine POST-Anfrage wird an den Konsistenzgruppe-Endpunkt mit dem `action=start` Parameter gesendet.

```
curl -k -X POST 'https://<IP_address>/application/consistency-
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
"accept: application/hal+json" -H "content-type: application/json"
-d '
{
  "name": "<snapshot_name>",
  "consistency_type": "crash",
  "comment": "<comment>",
  "snapmirror_label": "<SnapMirror_label>"
}'
```

2. Wenn die POST-Anfrage erfolgreich ist, enthält die Ausgabe eine Snapshot-UUID. Mit dieser UUID kann eine PATCH-Anfrage gesendet werden, um den Snapshot zu committen.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Remote-Schutz für eine Konsistenzgruppe festlegen

Je nach Ihrer ONTAP Version bieten Konsistenzgruppen Remote-Schutz durch SnapMirror active sync, SnapMirror asynchron und SnapLock für SnapVault Beziehungen.

Ab ONTAP 9.20.1 ist SnapLock für SnapVault Schutz verfügbar. Ab ONTAP 9.13.1 ist SnapMirror asynchroner Schutz verfügbar.

Bevor Sie beginnen

- Sie müssen "eine Cluster Peer-Beziehung erstellen".
- Sie müssen "Erstellen einer Intercluster-SVM Peer-Beziehung".

Schutz mit SnapMirror active sync konfigurieren

Mit SnapMirror active sync kann sichergestellt werden, dass Snapshots von Konsistenzgruppen, die auf Ihrer Konsistenzgruppe erstellt wurden, an das Ziel kopiert werden. Weitere Informationen zu SnapMirror active sync oder zur Konfiguration von SnapMirror active sync über die CLI finden sich unter Schutz für die Geschäftskontinuität konfigurieren.

Bevor Sie beginnen

- SnapMirror active sync-Beziehungen können auf Volumes, die für den NAS-Zugriff eingebunden sind, nicht hergestellt werden.
- Die Richtlinienbezeichnungen im Quell- und Ziel-Cluster müssen übereinstimmen.
- SnapMirror active sync repliziert Snapshots standardmäßig nicht, es sei denn, der vordefinierten `AutomatedFailOver` Richtlinie wird eine Regel mit einem SnapMirror Label hinzugefügt und die Snapshots werden mit diesem Label erstellt.

  Weitere Informationen zu diesem Prozess finden Sie unter "Mit SnapMirror active sync schützen".
- Kaskadierte Bereitstellungen werden mit SnapMirror active sync nicht unterstützt.
- Ab ONTAP 9.13.1 ist es möglich, Volumes zu einer Konsistenzgruppe hinzufügen unterbrechungsfrei mit einer aktiven SnapMirror active sync Beziehung zu arbeiten. Alle anderen Änderungen an einer Konsistenzgruppe erfordern das Aufheben der SnapMirror active sync Beziehung, die Modifikation der Konsistenzgruppe sowie das anschließende Wiederherstellen und Resynchronisieren der Beziehung.

> Zur Konfiguration von SnapMirror Active Sync mit der CLI siehe Mit SnapMirror active sync schützen.

Schritte für System Manager

1. Stellen Sie sicher, dass Sie die "Voraussetzungen für die Verwendung von SnapMirror Active Sync" erfüllt haben.
2. **Speicher > Konsistenzgruppen** auswählen.
3. Wählen Sie die von Ihnen erstellte Konsistenzgruppe im Menü „Konsistenzgruppe“ aus.
4. Oben rechts auf der Übersichtsseite **Mehr** und dann **Schützen** auswählen.
5. System Manager füllt die Quellseiteninformationen automatisch aus. Der passende Cluster und die passende Storage-VM für das Ziel sind auszuwählen. Wählen Sie eine Datensicherungsstrategie. Es ist sicherzustellen, dass **Beziehung initialisieren** aktiviert ist.
6. **Speichern** auswählen.
7. Die Konsistenzgruppe muss initialisiert und synchronisiert werden. Die erfolgreiche Synchronisierung lässt sich durch Rückkehr zum Menü **Konsistenzgruppe** bestätigen. Der Status **SnapMirror (Remote)** wird `Protected` neben angezeigt.

Asynchrones SnapMirror konfigurieren

Ab ONTAP 9.13.1 ist es möglich, SnapMirror asynchrone Datensicherung für eine einzelne Konsistenzgruppe zu konfigurieren. Ab ONTAP 9.14.1 kann SnapMirror asynchron genutzt werden, um volume-granulare Snapshots mithilfe der Konsistenzgruppe an das Ziel-Cluster zu replizieren.

Über diese Aufgabe

Um volume-granulare Snapshots zu replizieren, muss ONTAP 9.14.1 oder höher ausgeführt werden. Für MirrorAndVault und Vault Richtlinien muss das SnapMirror Label der volume-granularen Snapshot-Richtlinie mit der SnapMirror Richtlinienregel der Konsistenzgruppe übereinstimmen. Volume-granulare Snapshots richten sich nach dem Aufbewahrungswert der SnapMirror Richtlinie der Konsistenzgruppe, der unabhängig von den Konsistenzgruppen-Snapshots berechnet wird. Wenn beispielsweise eine Richtlinie zum Aufbewahren von zwei Snapshots auf dem Ziel-Cluster besteht, können zwei volume-granulare Snapshots und zwei Konsistenzgruppen-Snapshots vorhanden sein.

Beim Resynchronisieren der SnapMirror Beziehung mit volume-granularen Snapshots können volume-granulare Snapshots mit dem `-preserve` Flag beibehalten werden. Volume-granulare Snapshots, die neuer als Konsistenzgruppe-Snapshots sind, werden beibehalten. Wenn keine Konsistenzgruppe-Snapshot vorhanden ist, können bei der Resynchronisierung keine volume-granularen Snapshots übertragen werden.

Bevor Sie beginnen

- Ab ONTAP 9.20.1 können Sie die Backend SnapMirror Replikation über bestehende FC-Fabrics konfigurieren. Wenn Sie die FC-Fabric für die Replikation verwenden möchten, müssen Sie "Konfiguration Ihres Systems für die Backend-FC-Replikation". Sie müssen außerdem:
  - Bei der Erstellung Ihrer asynchronen SnapMirror Beziehung für die Replikation über Ihr FC-Fabric erfolgt die Auswahl von FC als Transportprotokoll. Die Backend-Replikation verwendet standardmäßig das IP-Protokoll.
  - Voraussetzung ist eine unterstützte asynchrone Datensicherungsstrategie "Welche standardmäßigen asynchronen Datenschutzrichtlinien die Backend FC Replikation unterstützt".
- SnapMirror asynchroner Schutz ist nur für eine einzelne Konsistenzgruppe verfügbar. Er wird für hierarchische Konsistenzgruppen nicht unterstützt. Zur Umwandlung einer hierarchischen Konsistenzgruppe in eine einzelne Konsistenzgruppe siehe Konsistenzgruppenarchitektur ändern.
- Die Richtlinienbezeichnungen im Quell- und Ziel-Cluster müssen übereinstimmen.
- Eine unterbrechungsfreie Volumes zu einer Konsistenzgruppe hinzufügen ist mit einer aktiven SnapMirror asynchronen Beziehung möglich. Alle anderen Änderungen an einer Konsistenzgruppe erfordern das Aufheben der SnapMirror Beziehung, das Modifizieren der Konsistenzgruppe sowie das anschließende Wiederherstellen und Resynchronisieren der Beziehung.
- Konsistenzgruppen, die für den Schutz mit SnapMirror asynchron aktiviert sind, haben unterschiedliche Grenzwerte. Weitere Informationen finden sich unter Konsistenzgruppenlimits.
- Wenn Sie eine asynchrone SnapMirror Schutzbeziehung für mehrere einzelne Volumes konfiguriert haben, können diese Volumes in eine Konsistenzgruppe umgewandelt werden, wobei die vorhandenen Snapshots erhalten bleiben. Für eine erfolgreiche Konvertierung der Volumes gilt Folgendes:
  - Es muss eine gemeinsame Snapshot-Kopie der Volumes vorhanden sein.
  - Sie müssen die bestehende SnapMirror Beziehung unterbrechen, die Volumes zu einer einzigen Konsistenzgruppe hinzufügen, dann die Beziehung mithilfe des folgenden Workflows erneut synchronisieren.

Schritte

1. Im Ziel-Cluster **Speicher > Konsistenzgruppen** auswählen.

2. Wählen Sie die von Ihnen erstellte Konsistenzgruppe im Menü „Konsistenzgruppe“ aus.
3. Oben rechts auf der Übersichtsseite **Mehr** und dann **Schützen** auswählen.
4. System Manager füllt die Quellseiteninformationen automatisch aus. Der passende Cluster und die passende Storage-VM für das Ziel sind auszuwählen. Wählen Sie eine Datensicherungsstrategie. Es ist sicherzustellen, dass **Beziehung initialisieren** aktiviert ist.

   Bei Auswahl einer asynchronen Richtlinie besteht die Möglichkeit, den **Übertragungsplan zu überschreiben**.

   Der minimal unterstützte Zeitplan (Recovery Point Objective, RPO) für Konsistenzgruppen mit SnapMirror asynchron beträgt 30 Minuten.

5. **Speichern** auswählen.
6. Die Konsistenzgruppe muss initialisiert und synchronisiert werden. Die erfolgreiche Synchronisierung lässt sich durch Rückkehr zum Menü **Konsistenzgruppe** bestätigen. Der Status **SnapMirror (Remote)** wird `Protected` neben angezeigt.

Konfigurieren von SnapLock für SnapVault Replikation aus einer Nicht-SnapLock Quelle

Ab ONTAP 9.20.1 können Sie eine Konsistenzgruppe von einem Nicht-SnapLock Quellvolume auf ein SnapLock für SnapVault Zielvolume replizieren. Snapshots, die auf dem Zielvolume durch SnapLock für SnapVault geschützt sind, können weder versehentlich noch böswillig gelöscht werden.

Bevor Sie beginnen

- Sie sollten "Es sollte überprüft werden, ob eine SnapLock-Lizenz installiert ist.". Wenn auf dem Knoten keine SnapLock Lizenz installiert ist, müssen Sie "es installieren". Diese Lizenz ist im Lieferumfang von "ONTAP One" enthalten.
- Das "Die Compliance-Uhr muss initialisiert werden" auf beiden Clusterknoten.
- Sie können Backend SnapLock für SnapVault über bestehende FC-Fabrics für die Replikation konfigurieren. Wenn Sie die FC-Fabric für die Replikation nutzen möchten, müssen Sie "Konfiguration Ihres Systems für die Backend-FC-Replikation". Außerdem ist Folgendes erforderlich:
  - Beim Erstellen Ihrer SnapLock für SnapVault Beziehung zur Replizierung über Ihr FC-Fabric ist als Transportprotokoll FC zu verwenden. Die Backend-Replizierung verwendet standardmäßig das IP-Protokoll.
  - Dabei kommt die MirrorAndVault asynchrone Datensicherungsstrategie zum Einsatz..

Schritte

System Manager oder die CLI dienen zur Konfiguration Ihrer SnapLock für SnapVault Replizierungsbeziehung

System Manager

Die Aktivierung von SnapLock für SnapVault in System Manager erfolgt durch die Auswahl einer *vault* -Replikationsrichtlinie und anschließend der Option zum Sperren der Ziel-Snapshots.

1. In System Manager befindet sich dies unter **Schutz > Konsistenzgruppen**.
2. Anschließend erfolgt die Auswahl einer Konsistenzgruppe und dann von **Protect**.

   System Manager füllt die Quellseiteninformationen automatisch aus.

3. Den Ziel-Cluster und die Storage-VM auswählen.
4. Wählen Sie eine Datensicherungsstrategie.

   Sie müssen eine *vault*-Replikationsrichtlinie auswählen, die mit Aufbewahrungsregeln konfiguriert ist. In ONTAP 9.20.1 und höher müssen Sie für die Backend-FC-Replikation die Richtlinie *MirrorAndVault* auswählen.

5. Hier wird die Option **Ziel-Konsistenzgruppen sperren** ausgewählt.
6. Es muss **Beziehung initialisieren** ausgewählt sein.
7. **Speichern** auswählen.

CLI

1. Erstellung eines SnapLock Ziel-Volumes für die Quell-Konsistenzgruppe:

   ```
   volume create -vserver <dst_svm> -volume <dst_vol> -aggregate <aggr>
   -size <size> -type DP -snaplock-type enterprise
   ```

2. Erstellen einer SnapMirror Vault-Richtlinie:

   ```
   snapmirror policy create -vserver <dst_svm> -policy <policy_name>
   -type vault
   ```

3. Der Richtlinie werden Aufbewahrungsregeln hinzugefügt:

   ```
   snapmirror policy add-rule -vserver <dst_svm> -policy <policy_name>
   -snapmirror-label daily -keep <retention_length> -retention-period
   <retention_period>
   ```

   Im folgenden Beispiel ist die Aufbewahrungsfrist auf 1 Jahr festgelegt:

   ```
   snapmirror policy add-rule -vserver svm1 -policy vault -snapmirror-label
   monthly -keep 12 -retention-period "1 years"
   ```

   Im folgenden Beispiel ist die Aufbewahrungsfrist auf 30 Tage festgelegt:

   ```
   snapmirror policy add-rule -vserver svm1 -policy vault -snapmirror-label
   daily -keep 30 -retention-period "30 days"
   ```

4. Erstellung der SnapLock für SnapVault Beziehung:

   ```
   snapmirror create -source-path <src_svm>:/cg/<src_cg> -destination
   -path <dst_svm>:/cg/<dst_cg> -policy <policy_name>
   ```

5. Initialisierung der Beziehung:

```
snapmirror initialize -destination-path <dst_svm>:<dst_vol>
```

6. Überprüfung, ob die Beziehung hergestellt wurde:

```
snapmirror show -destination-path <dst_svm>:<dst_vol> -fields
policy,status,state
```

7. Überprüfen, ob die Snapshots am Ziel gesperrt sind:

```
volume snapshot show -vserver <dst_svm> -volume <dst_vol> -fields
snapshot,snaplock-expiry-time,is-snaplock-expiry-locked
```

SVM-Notfallwiederherstellung konfigurieren

Ab ONTAP 9.14.1 SVM Disaster Recovery werden Konsistenzgruppen unterstützt, sodass Konsistenzgruppeninformationen vom Quell-Cluster auf den Ziel-Cluster gespiegelt werden können.

Wenn die SVM-Notfallwiederherstellung auf einer SVM aktiviert wird, die bereits eine Konsistenzgruppe enthält, sollten die SVM-Konfigurationsworkflows für System Manager oder die ONTAP CLI beachtet werden.

Wenn einer SVM, die sich in einer aktiven und fehlerfreien SVM-Disaster-Recovery-Beziehung befindet, eine Konsistenzgruppe hinzugefügt wird, muss die SVM-Disaster-Recovery-Beziehung vom Ziel-Cluster aus aktualisiert werden. Weitere Informationen finden sich unter Eine Replikationsbeziehung manuell aktualisieren. Die Beziehung muss jedes Mal aktualisiert werden, wenn die Konsistenzgruppe erweitert wird.

Einschränkungen

- Die SVM-Notfallwiederherstellung unterstützt keine hierarchischen Konsistenzgruppen.
- Die SVM-Notfallwiederherstellung unterstützt keine Konsistenzgruppen, die mit SnapMirror asynchron geschützt sind. Die SnapMirror Beziehung muss aufgehoben werden, bevor die SVM-Notfallwiederherstellung konfiguriert wird.
- Beide Cluster müssen mit ONTAP 9.14.1 oder höher betrieben werden.
- Fan-out-Beziehungen werden für SVM-Disaster-Recovery-Konfigurationen, die Konsistenzgruppen enthalten, nicht unterstützt.
- Weitere Grenzwerte sind unter Konsistenzgruppe Grenzen aufgeführt.

Beziehungen visualisieren

System Manager visualisiert LUN-Zuordnungen unter dem Menüpunkt **Schutz > Beziehungen**. Bei Auswahl einer Quellbeziehung zeigt System Manager eine Visualisierung der Quell-Beziehungen an. Durch Auswahl eines Volumes ist eine detaillierte Analyse dieser Beziehungen möglich, einschließlich einer Liste der enthaltenen LUNs und der Initiatorgruppen-Beziehungen. Diese Informationen können aus der Ansicht des einzelnen Volumes als Excel-Arbeitsmappe heruntergeladen werden; der Downloadvorgang läuft im Hintergrund.

Verwandte Informationen

- "Eine Konsistenzgruppe klonen"
- "Snapshots konfigurieren"
- "Benutzerdefinierte Datensicherungsstrategien erstellen"
- "Wiederherstellung aus Snapshots"
- "Ein Volume aus einem früheren Snapshot wiederherstellen"
- "SnapMirror active sync Übersicht"
- "ONTAP Automatisierungsdokumentation"
- SnapMirror asynchrone Grundlagen der Notfallwiederherstellung

Mitgliedsvolumes in einer ONTAP Konsistenzgruppe ändern

Ab ONTAP 9.12.1 ist es möglich, eine Konsistenzgruppe zu ändern, indem Volumes entfernt oder hinzugefügt werden (Erweiterung der Konsistenzgruppe). Ab ONTAP 9.13.1 ist es möglich, Volumes zwischen untergeordneten Konsistenzgruppen zu verschieben, sofern diese eine gemeinsame übergeordnete Gruppe haben.

Volumes zu einer Konsistenzgruppe hinzufügen

Ab ONTAP 9.12.1 ist es möglich, Volumes unterbrechungsfrei zu einer Konsistenzgruppe hinzuzufügen.

Über diese Aufgabe

- Sie können keine Volumes hinzufügen, die mit einer anderen Konsistenzgruppe verknüpft sind.
- Konsistenzgruppen unterstützen NAS, SAN und NVMe-Protokolle.
- Sie können bis zu 16 Bände gleichzeitig zu einer Konsistenzgruppe hinzufügen, sofern die Anpassungen innerhalb des Gesamtbereichs Konsistenzgruppe Grenzen liegen.
- Ab ONTAP 9.13.1 ist es möglich, Volumes unterbrechungsfrei zu einer Konsistenzgruppe mit einer aktiven SnapMirror active sync- oder SnapMirror asynchronen Datensicherungsstrategie hinzuzufügen.
- Wenn Volumes zu einer durch SnapMirror active sync geschützten Konsistenzgruppe hinzugefügt werden, ändert sich der Status der SnapMirror active sync-Beziehung zu „Wird erweitert“, bis Spiegelung und Schutz für das neue Volume konfiguriert sind. Falls auf dem primären Cluster ein Ausfall auftritt, bevor dieser Vorgang abgeschlossen ist, wird die Konsistenzgruppe im Rahmen des Failover-Vorgangs auf ihre ursprüngliche Zusammensetzung zurückgesetzt.
- In ONTAP 9.12.1 und früher können Volumes nicht zu einer Konsistenzgruppe in einer SnapMirror active sync-Beziehung hinzugefügt werden. Zuerst muss die SnapMirror active sync-Beziehung gelöscht, die Konsistenzgruppe geändert und anschließend der Schutz mit SnapMirror active sync wiederhergestellt werden.
- Ab ONTAP 9.12.1 unterstützt die ONTAP REST API das Hinzufügen neuer oder vorhandener Volumes zu einer Konsistenzgruppe. Weitere Informationen zur ONTAP REST API sind unter "ONTAP REST API Referenzdokumentation" verfügbar.

  Ab ONTAP 9.13.1 ist diese Funktionalität im System Manager verfügbar.

- Beim Erweitern einer Konsistenzgruppe werden Snapshots der Konsistenzgruppe, die vor der Änderung erstellt wurden, als partiell betrachtet. Jede Wiederherstellung, die auf einem solchen Snapshot basiert, gibt die Konsistenzgruppe zum Zeitpunkt des Snapshots wieder.
- Wenn Sie ONTAP 9.10.1 bis 9.11.1 verwenden, kann eine Konsistenzgruppe nicht geändert werden. Um die Konfiguration einer Konsistenzgruppe in ONTAP 9.10.1 oder 9.11.1 zu ändern, muss die

Konsistenzgruppe gelöscht und anschließend eine neue Konsistenzgruppe mit den gewünschten Volumes erstellt werden.

- Ab ONTAP 9.14.1 können volume-granulare Snapshots zum Ziel-Cluster repliziert werden, wenn SnapMirror asynchron verwendet wird. Beim Erweitern einer Konsistenzgruppe mit SnapMirror asynchron werden volume-granulare Snapshots erst nach der Erweiterung der Konsistenzgruppe repliziert, wenn die SnapMirror Richtlinie MirrorAll oder MirrorAndVault ist. Es werden nur volume-granulare Snapshots repliziert, die neuer als der Basis-Snapshot der Konsistenzgruppe sind.
- Wenn Volumes zu einer Konsistenzgruppe in einer SVM-Disaster-Recovery-Beziehung hinzugefügt werden (unterstützt ab ONTAP 9.14.1), muss die SVM-Disaster-Recovery-Beziehung nach der Erweiterung der Konsistenzgruppe vom Ziel-Cluster aus aktualisiert werden. Weitere Informationen finden sich unter Eine Replikationsbeziehung manuell aktualisieren.
- Wenn NVMe mit ONTAP 9.17.1 verwendet wird, kann eine Konsistenzgruppe nicht geändert werden.

Beispiel 2. Schritte

System Manager

Ab ONTAP 9.12.1 ist diese Operation mit System Manager möglich.

1. **Speicher > Konsistenzgruppen** auswählen.
2. Die Konsistenzgruppe, die geändert werden soll, auswählen.
3. Wenn Sie eine einzelne Konsistenzgruppe bearbeiten, wählen Sie oben im Menü **Volumes** die Option **More** und dann **Expand**, um ein Volume hinzuzufügen.

   Wenn eine untergeordnete Konsistenzgruppe bearbeitet wird, ist die übergeordnete Konsistenzgruppe zu identifizieren, die bearbeitet werden soll. Die Schaltfläche **>** zeigt die untergeordneten Konsistenzgruppen an, anschließend ⋮ neben dem Namen der untergeordneten Konsistenzgruppe auswählen, die bearbeitet werden soll. Im daraufhin angezeigten Menü die Option **Erweitern** auswählen.

4. Bis zu 16 Volumes können zur Konsistenzgruppe hinzugefügt werden.
5. **Speichern** auswählen. Nach Abschluss des Vorgangs sind die neu hinzugefügten Volumes im Menü **Volumes** der Konsistenzgruppe sichtbar.

CLI

Ab ONTAP 9.14.1 ist es möglich, Volumes mithilfe der ONTAP CLI zu einer Konsistenzgruppe hinzuzufügen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Vorhandene Volumes hinzufügen

1. Führen Sie den folgenden Befehl aus. Der `-volumes`Parameter akzeptiert eine durch Kommas getrennte Liste von Volumes.

   ⓘ Den `-parent-consistency-group` Parameter nur einbeziehen, wenn die Konsistenzgruppe in einer hierarchischen Beziehung steht.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   ```

```
consistency_group_name -parent-consistency-group parent_consistency_group
-volume volumes
```

Neue Volumes hinzufügen

Die Vorgehensweise zum Hinzufügen neuer Volumes hängt vom verwendeten Protokoll ab.

> Der `-parent-consistency-group` Parameter ist nur einzubeziehen, wenn die Konsistenzgruppe in einer hierarchischen Beziehung steht.

- Neue Volumes können hinzugefügt werden, ohne sie zu exportieren:

```
consistency-group volume create -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group existingParentCg -volume
volume_name -size size
```

- Neue NFS-Volumes hinzufügen:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- Neue SAN-Volumes hinzufügen:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- Neue NVMe-Namensräume hinzufügen:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

Volumes aus einer Konsistenzgruppe entfernen

Volumes, die aus einer Konsistenzgruppe entfernt werden, werden nicht gelöscht. Sie bleiben im Cluster aktiv.

Über diese Aufgabe

- Sie können keine Volumes aus einer Konsistenzgruppe in einer SnapMirror active sync- oder SVM-Disaster-Recovery-Beziehung entfernen. Zunächst muss die SnapMirror active sync-Beziehung gelöscht werden, um die Konsistenzgruppe zu ändern, und anschließend die Beziehung wiederhergestellt werden.
- Wenn eine Konsistenzgruppe nach dem Löschvorgang keine Volumes mehr enthält, wird die Konsistenzgruppe gelöscht.
- Wenn ein Volume aus einer Konsistenzgruppe entfernt wird, bleiben vorhandene Snapshots der Konsistenzgruppe erhalten, gelten jedoch als ungültig. Die vorhandenen Snapshots können nicht zur Wiederherstellung des Inhalts der Konsistenzgruppe verwendet werden. Volume-spezifische Snapshots bleiben gültig.
- Wenn ein Volume aus dem Cluster gelöscht wird, wird es automatisch aus der Konsistenzgruppe entfernt.
- Um die Konfiguration einer Konsistenzgruppe in ONTAP 9.10.1 oder 9.11.1 zu ändern, muss die Konsistenzgruppe gelöscht und anschließend eine neue Konsistenzgruppe mit den gewünschten

Mitgliedsvolumes erstellt werden.

- Das Löschen eines Volumes aus dem Cluster entfernt es automatisch auch aus der Konsistenzgruppe.

System Manager

Ab ONTAP 9.12.1 ist diese Operation mit System Manager möglich.

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. Die einzelne oder untergeordnete Konsistenzgruppe, die geändert werden soll, auswählen.
3. Im Menü **Volumes** die Kontrollkästchen neben den einzelnen Volumes auswählen, die aus der Konsistenzgruppe entfernt werden sollen.
4. **Volumes aus der Konsistenzgruppe entfernen** auswählen.
5. Bestätigen Sie, dass Sie verstehen, dass durch das Entfernen der Volumes alle Snapshots der Konsistenzgruppe ungültig werden und wählen Sie **Entfernen**.

CLI

Ab ONTAP 9.14.1 ist es möglich, Volumes aus einer Konsistenzgruppe mithilfe der CLI zu entfernen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Schritt

1. Die Volumes werden entfernt. Der `-volumes`Parameter akzeptiert eine durch Kommas getrennte Liste von Volumes.

   Den `-parent-consistency-group` Parameter nur einbeziehen, wenn die Konsistenzgruppe in einer hierarchischen Beziehung steht.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Volumes zwischen Konsistenzgruppen verschieben

Ab ONTAP 9.13.1 ist es möglich, Volumes zwischen untergeordneten Konsistenzgruppen zu verschieben, die ein gemeinsames übergeordnetes Element haben.

Über diese Aufgabe

- Volumes können nur zwischen Konsistenzgruppen verschoben werden, die unter derselben übergeordneten Konsistenzgruppe verschachtelt sind.
- Vorhandene Konsistenzgruppen-Snapshots werden ungültig und sind nicht mehr als Konsistenzgruppen-Snapshots zugänglich. Einzelne Volume-Snapshots bleiben gültig.
- Momentaufnahmen der übergeordneten Konsistenzgruppe bleiben gültig.
- Wenn alle Volumes aus einer untergeordneten Konsistenzgruppe verschoben werden, wird diese Konsistenzgruppe gelöscht.

- Änderungen an einer Konsistenzgruppe müssen Konsistenzgruppe Grenzen entsprechen.

System Manager

Ab ONTAP 9.12.1 ist diese Operation mit System Manager möglich.

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die übergeordnete Konsistenzgruppe aus, die die Volumes enthält, die Sie verschieben möchten. Suchen Sie die untergeordnete Konsistenzgruppe und erweitern Sie anschließend das Menü **Volumes**. Wählen Sie die Volumes aus, die Sie verschieben möchten.
3. **Verschieben** auswählen.
4. Wählen Sie aus, ob die Volumes in eine neue Konsistenzgruppe oder in eine bestehende Gruppe verschoben werden sollen.
   a. Um zu einer bestehenden Konsistenzgruppe zu wechseln, **Bestehende untergeordnete Konsistenzgruppe** auswählen und dann den Namen der Konsistenzgruppe aus dem Dropdown-Menü wählen.
   b. Zum Wechsel in eine neue Konsistenzgruppe die Option **Neue untergeordnete Konsistenzgruppe** auswählen. Einen Namen für die neue untergeordnete Konsistenzgruppe eingeben und einen Komponententyp auswählen.
5. **Verschieben** auswählen.

CLI

Ab ONTAP 9.14.1 ist es möglich, Volumes mithilfe der ONTAP CLI zwischen Konsistenzgruppen zu verschieben.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Volumes in eine neue untergeordnete Konsistenzgruppe verschieben

1. Der folgende Befehl erstellt eine neue untergeordnete Konsistenzgruppe, die die angegebenen Volumes enthält.

   Beim Erstellen der neuen Konsistenzgruppe können neue Snapshot-, QoS- und Tiering-Richtlinien festgelegt werden.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Volumes in eine bestehende untergeordnete Konsistenzgruppe verschieben

1. Weisen Sie die Volumes neu zu. Der `-volumes` Parameter akzeptiert eine durch Kommas getrennte Liste von Volume-Namen.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   ```

```
parent_consistency_group -volume volumes -to-consistency-group
target_consistency_group
```

Verwandte Informationen

- Konsistenzgruppenlimits
- Eine Konsistenzgruppe klonen

ONTAP Konsistenzgruppen-Geometrie ändern

Ab ONTAP 9.13.1 kann die Geometrie einer Konsistenzgruppe geändert werden. Das Ändern der Geometrie einer Konsistenzgruppe ermöglicht eine Anpassung der Konfiguration von untergeordneten oder übergeordneten Konsistenzgruppen, ohne laufende E/A-Operationen zu unterbrechen.

Das Ändern der Geometrie einer Konsistenzgruppe wirkt sich auf bestehende Snapshots der Konsistenzgruppe aus. Einzelheiten finden sich bei der jeweiligen Geometrieänderung, die durchgeführt werden soll.

Die Geometrie einer Konsistenzgruppe, die mit einer Remote Datensicherungsstrategie konfiguriert ist, kann nicht geändert werden. Zuerst muss die Schutzbeziehung aufgehoben, dann die Geometrie geändert und anschließend der Remote-Schutz wiederhergestellt werden.

Eine neue untergeordnete Konsistenzgruppe hinzufügen

Ab ONTAP 9.13.1 ist es möglich, einer bestehenden übergeordneten Konsistenzgruppe eine neue untergeordnete Konsistenzgruppe hinzuzufügen.

Über diese Aufgabe

- Eine übergeordnete Konsistenzgruppe kann maximal fünf untergeordnete Konsistenzgruppen enthalten. Siehe Konsistenzgruppe Grenzen für weitere Einschränkungen.
- Sie können einer einzelnen Konsistenzgruppe keine untergeordnete Konsistenzgruppe hinzufügen. Zuerst muss die Konsistenzgruppe [promoten] werden, danach kann eine untergeordnete Konsistenzgruppe hinzugefügt werden.
- Vorhandene Snapshots der Konsistenzgruppe, die vor der Erweiterungsoperation erstellt wurden, werden als partiell betrachtet. Jede Wiederherstellung, die auf einem solchen Snapshot basiert, gibt die Konsistenzgruppe zum Zeitpunkt des Snapshots wieder.

Beispiel 3. Schritte

System Manager

Ab ONTAP 9.13.1 ist es möglich, diese Operation mit System Manager durchzuführen.

Eine neue untergeordnete Konsistenzgruppe hinzufügen

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die übergeordnete Konsistenzgruppe aus, zu der Sie eine untergeordnete Konsistenzgruppe hinzufügen möchten.
3. Neben dem Namen der übergeordneten Konsistenzgruppe **Mehr** und dann **Neue untergeordnete Konsistenzgruppe** auswählen.

4. Ein Name für Ihre Konsistenzgruppe wird eingegeben.
5. Wählen Sie aus, ob neue oder bereits vorhandene Volumes hinzugefügt werden sollen.
   a. Wenn Sie bereits vorhandene Volumes hinzufügen, **Vorhandene Volumes** auswählen und anschließend die gewünschten Volumes aus dem Dropdown-Menü wählen.
   b. Wenn Sie neue Volumes hinzufügen, wählen Sie **Neue Volumes** aus und geben Sie anschließend die Anzahl der Volumes und deren Größe an.
6. Wählen Sie **Hinzufügen**.

CLI

Ab ONTAP 9.14.1 ist es möglich, mithilfe der ONTAP CLI eine untergeordnete Konsistenzgruppe hinzuzufügen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine untergeordnete Konsistenzgruppe mit neuen Volumes hinzufügen

1. Die neue Konsistenzgruppe wird erstellt. Werte für den Namen der Konsistenzgruppe, das Volume-Präfix, die Volume-Anzahl, die Volume-Größe, den Storage-Service und den Namen der Export-Policy werden angegeben:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

Eine untergeordnete Konsistenzgruppe mit vorhandenen Volumes hinzufügen

1. Die neue Konsistenzgruppe wird erstellt. Der `volumes` Parameter akzeptiert eine durch Kommas getrennte Liste von Volume-Namen.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

Eine untergeordnete Konsistenzgruppe trennen

Ab ONTAP 9.13.1 ist es möglich, eine untergeordnete Konsistenzgruppe von ihrer übergeordneten Gruppe zu entfernen, wodurch sie in eine eigenständige Konsistenzgruppe umgewandelt wird.

Über diese Aufgabe

- Das Trennen einer untergeordneten Konsistenzgruppe führt dazu, dass die Snapshots der übergeordneten Konsistenzgruppe ungültig und nicht mehr zugänglich werden. Volume-granulare Snapshots bleiben gültig.
- Vorhandene zeitpunktgenaue Kopien der einzelnen Konsistenzgruppe bleiben gültig.
- Dieser Vorgang schlägt fehl, wenn bereits eine einzelne Konsistenzgruppe mit demselben Namen wie die untergeordnete Konsistenzgruppe, die Sie trennen möchten, existiert. In diesem Fall muss die Konsistenzgruppe beim Trennen umbenannt werden.

Beispiel 4. Schritte

System Manager

Ab ONTAP 9.13.1 ist es möglich, diese Operation mit System Manager durchzuführen.

Eine untergeordnete Konsistenzgruppe trennen

1. **Speicher > Konsistenzgruppen** auswählen.
2. Die übergeordnete Konsistenzgruppe auswählen, die das untergeordnete Element enthält, das abgetrennt werden soll.
3. Wählen Sie neben der untergeordneten Konsistenzgruppe, die Sie abtrennen möchten, **Mehr** und dann **Vom übergeordneten Element abtrennen**.
4. Optional kann die Konsistenzgruppe umbenannt und ein Anwendungstyp ausgewählt werden.
5. **Trennen** auswählen.

CLI

Ab ONTAP 9.14.1 ist das Trennen einer untergeordneten Konsistenzgruppe mithilfe der ONTAP CLI möglich.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine untergeordnete Konsistenzgruppe trennen

1. Die Konsistenzgruppe wird getrennt. Optional kann die getrennte Konsistenzgruppe mit dem `-new -name` Parameter umbenannt werden.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Eine bestehende einzelne Konsistenzgruppe unter eine übergeordnete Konsistenzgruppe verschieben

Ab ONTAP 9.13.1 ist es möglich, eine bestehende einzelne Konsistenzgruppe in eine untergeordnete Konsistenzgruppe umzuwandeln. Die Konsistenzgruppe kann entweder unter eine bestehende übergeordnete Konsistenzgruppe verschoben oder während des Verschiebevorgangs eine neue übergeordnete Konsistenzgruppe erstellt werden.

Über diese Aufgabe

- Die übergeordnete Konsistenzgruppe darf höchstens vier untergeordnete Konsistenzgruppen haben. Eine übergeordnete Konsistenzgruppe kann maximal fünf untergeordnete Konsistenzgruppen enthalten. Siehe Konsistenzgruppe Grenzen für weitere Einschränkungen.
- Vor diesem Vorgang erstellte Snapshots der übergeordneten Konsistenzgruppe gelten als partiell. Jede Wiederherstellung, die auf einem dieser Snapshots basiert, spiegelt die Konsistenzgruppe zum Zeitpunkt des Snapshots wider.
- Vorhandene Snapshots der einzelnen Konsistenzgruppe bleiben gültig.

Beispiel 5. Schritte

System Manager

Ab ONTAP 9.13.1 ist es möglich, diese Operation mit System Manager durchzuführen.

Eine bestehende einzelne Konsistenzgruppe unter eine übergeordnete Konsistenzgruppe verschieben

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die Konsistenzgruppe aus, die Sie konvertieren möchten.
3. **Mehr** und dann **Unter andere Konsistenzgruppe** auswählen.
4. Optional kann ein neuer Name für die Konsistenzgruppe eingegeben und ein Komponententyp ausgewählt werden. Standardmäßig ist der Komponententyp Sonstige.
5. Wählen Sie aus, ob Sie zu einer bestehenden übergeordneten Konsistenzgruppe migrieren oder eine neue übergeordnete Konsistenzgruppe erstellen möchten:
   a. Um zu einer bestehenden übergeordneten Konsistenzgruppe zu migrieren, **Bestehende Konsistenzgruppe** auswählen und anschließend die Konsistenzgruppe aus dem Dropdown-Menü wählen.
   b. Zum Erstellen einer neuen übergeordneten Konsistenzgruppe **Neue Konsistenzgruppe** auswählen und anschließend einen Namen für die neue Konsistenzgruppe angeben.
6. **Verschieben** auswählen.

CLI

Ab ONTAP 9.14.1 ist es möglich, eine einzelne Konsistenzgruppe mithilfe der ONTAP CLI unter eine übergeordnete Konsistenzgruppe zu verschieben.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine Konsistenzgruppe unter eine neue übergeordnete Konsistenzgruppe verschieben

1. Die neue übergeordnete Konsistenzgruppe wird erstellt. Der `-consistency-groups` Parameter migriert alle vorhandenen Konsistenzgruppen zur neuen übergeordneten Konsistenzgruppe.

   ```
   consistency-group attach -vserver svm_name -consistency-group
   parent_consistency_group -consistency-groups child_consistency_group
   ```

Eine Konsistenzgruppe unter eine bestehende Konsistenzgruppe verschieben

1. Die Konsistenzgruppe verschieben:

   ```
   consistency-group add -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   ```

Eine untergeordnete Konsistenzgruppe hochstufen

Ab ONTAP 9.13.1 ist es möglich, eine einzelne Konsistenzgruppe zu einer übergeordneten Konsistenzgruppe zu machen. Wird die einzelne Konsistenzgruppe zu einer übergeordneten Konsistenzgruppe gemacht, entsteht gleichzeitig eine neue untergeordnete Konsistenzgruppe, die alle Volumes der ursprünglichen einzelnen Konsistenzgruppe übernimmt.

Über diese Aufgabe

- Wenn eine untergeordnete Konsistenzgruppe in eine übergeordnete Konsistenzgruppe umgewandelt werden soll, muss zunächst Eine untergeordnete Konsistenzgruppe trennen die untergeordnete Konsistenzgruppe erstellt und anschließend dieses Verfahren angewendet werden.
- Vorhandene Snapshots der Konsistenzgruppe bleiben auch nach der Heraufstufung der Konsistenzgruppe gültig.

System Manager

Ab ONTAP 9.13.1 ist es möglich, diese Operation mit System Manager durchzuführen.

Eine untergeordnete Konsistenzgruppe hochstufen

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die Konsistenzgruppe aus, die Sie promoten möchten.
3. **Mehr** und dann **Zu übergeordneter Konsistenzgruppe hochstufen** auswählen.
4. Einen **Namen** eingeben und einen **Komponententyp** für die untergeordnete Konsistenzgruppe auswählen.
5. **Befördern** auswählen.

CLI

Ab ONTAP 9.14.1 ist es möglich, eine einzelne Konsistenzgruppe mithilfe der ONTAP CLI unter eine übergeordnete Konsistenzgruppe zu verschieben.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine untergeordnete Konsistenzgruppe hochstufen

1. Die Konsistenzgruppe wird hochgestuft. Dieser Befehl erstellt eine übergeordnete und eine untergeordnete Konsistenzgruppe.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

Ein übergeordnetes Element zu einer einzelnen Konsistenzgruppe herabstufen

Ab ONTAP 9.13.1 ist es möglich, eine übergeordnete Konsistenzgruppe in eine einzelne Konsistenzgruppe herabzustufen. Durch das Herabstufen der übergeordneten Konsistenzgruppe wird die Hierarchie der Konsistenzgruppe aufgehoben und alle zugehörigen untergeordneten Konsistenzgruppen werden entfernt. Alle Volumes in der Konsistenzgruppe verbleiben unter der neuen, einzelnen Konsistenzgruppe.

Über diese Aufgabe

- Vorhandene Snapshots der *übergeordneten* Konsistenzgruppe bleiben nach der Herabstufung zu einer einzelnen Konsistenz gültig. Vorhandene Snapshots aller zugehörigen *untergeordneten* Konsistenzgruppen dieser übergeordneten Gruppe werden bei der Herabstufung ungültig. Die einzelnen Volume-Snapshots innerhalb der untergeordneten Konsistenzgruppe bleiben weiterhin als volume-granulare Snapshots zugänglich.

Beispiel 6. Schritte

System Manager

Ab ONTAP 9.13.1 ist es möglich, diese Operation mit System Manager durchzuführen.

Eine Konsistenzgruppe herabstufen

1. **Speicher > Konsistenzgruppen** auswählen.
2. Die übergeordnete Konsistenzgruppe auswählen, die herabgestuft werden soll.
3. **Mehr** und dann **Zu einzelner Konsistenzgruppe herabstufen** auswählen.
4. Eine Warnung weist darauf hin, dass alle zugehörigen untergeordneten Konsistenzgruppen gelöscht werden und deren Volumes unter die neue einzelne Konsistenzgruppe verschoben werden. Mit **Herabstufen** wird bestätigt, dass die Auswirkungen verstanden wurden.

CLI

Ab ONTAP 9.14.1 ist es möglich, eine Konsistenzgruppe mithilfe der ONTAP CLI herabzustufen.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine Konsistenzgruppe herabstufen

1. Die Konsistenzgruppe herabstufen. Mit dem optionalen `-new-name` Parameter kann die Konsistenzgruppe umbenannt werden.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

ONTAP Konsistenzgruppe: Anwendungs- und Komponententags bearbeiten

Ab ONTAP 9.12.1 unterstützen Konsistenzgruppen die Kennzeichnung von Komponenten und Anwendungen. Anwendungs- und Komponentenkennzeichnungen dienen als Verwaltungswerkzeug, mit dem verschiedene Workloads in Konsistenzgruppen gefiltert und identifiziert werden können.

Über diese Aufgabe

Konsistenzgruppen bieten zwei Arten von Tags:

- **Anwendungstags**: Diese gelten für einzelne und übergeordnete Konsistenzgruppen. Anwendungstags bieten eine Kennzeichnung für Workloads wie MongoDB, Oracle oder SQL Server. Der Standard-Anwendungstag für Konsistenzgruppen ist Other.
- **Komponenten-Tags**: Untergeordnete Elemente in hierarchischen Konsistenzgruppen haben Komponenten-Tags anstelle von Anwendungs-Tags. Die Optionen für Komponenten-Tags sind „data“, „logs“ oder „other“. Der Standardwert ist „other“.

Tags können beim Erstellen von Konsistenzgruppen oder nachdem die Konsistenzgruppen erstellt wurden, angewendet werden.

Wenn die Konsistenzgruppe eine SnapMirror active sync-Beziehung aufweist, ist **Other** als Anwendungs- oder Komponententag zu verwenden.

Schritte

Ab ONTAP 9.12.1 ist es möglich, Anwendungs- und Komponententags mit System Manager zu ändern. Ab ONTAP 9.14.1 ist es möglich, die Anwendungs- und Komponententags mit der ONTAP CLI zu ändern.

System Manager

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die Konsistenzgruppe aus, deren Tag Sie ändern möchten. Wählen Sie das ⋮ neben dem Namen der Konsistenzgruppe und dann **Bearbeiten**.
3. Im Dropdown-Menü das passende Anwendungs- oder Komponenten-Tag auswählen.
4. **Speichern** auswählen.

CLI

Ab ONTAP 9.14.1 lässt sich das Anwendungs- oder Komponenten-Tag einer bestehenden Konsistenzgruppe mithilfe der ONTAP CLI ändern.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Das Anwendungs-Tag ändern

1. Anwendungstags akzeptieren nur eine begrenzte Anzahl vordefinierter Zeichenketten. Die Liste der zulässigen Zeichenketten kann mit folgendem Befehl angezeigt werden:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Wählen Sie die passende Zeichenkette aus der Ausgabe aus, und ändern Sie die Konsistenzgruppe:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Das Komponenten-Tag ändern

1. Den Komponententyp ändern. Der Komponententyp kann Daten, Protokolle oder Sonstige sein. Wenn SnapMirror active sync verwendet wird, muss „Sonstige“ ausgewählt sein.
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

Klonen einer ONTAP Konsistenzgruppe

Ab ONTAP 9.12.1 ist das Klonen einer Konsistenzgruppe möglich, um eine Kopie der Konsistenzgruppe und ihres Inhalts zu erstellen. Das Klonen einer Konsistenzgruppe erstellt eine Kopie der Konsistenzgruppen-Konfiguration, ihrer Metadaten wie Anwendungstyp sowie aller Volumes und deren Inhalte wie Dateien, Verzeichnisse, LUNs oder NVMe-Namespaces.

Über diese Aufgabe

Beim Klonen einer Konsistenzgruppe kann diese mit ihrer aktuellen Konfiguration geklont werden, wobei der Inhalt des Volumes entweder wie er ist übernommen wird oder auf einem vorhandenen Snapshot der Konsistenzgruppe basiert.

Das Klonen einer Konsistenzgruppe wird nur für die gesamte Konsistenzgruppe unterstützt. Es ist nicht möglich, eine einzelne untergeordnete Konsistenzgruppe in einer hierarchischen Beziehung zu klonen; nur die vollständige Konfiguration der Konsistenzgruppe kann geklont werden.

Beim Klonen einer Konsistenzgruppe werden die folgenden Komponenten nicht geklont:

- iGroups
- LUN-Zuordnungen
- NVMe Subsysteme
- NVMe Namespace Subsystem-Zuordnungen

Bevor Sie beginnen

- Beim Klonen einer Konsistenzgruppe erstellt ONTAP keine SMB-Freigaben für die geklonten Volumes, wenn kein Freigabename angegeben ist. * Geklonte Konsistenzgruppen werden nicht eingebunden, wenn kein Verbindungspfad angegeben ist.
- Wenn versucht wird, eine Konsistenzgruppe auf Basis eines Snapshots zu klonen, der die aktuellen Bestandteile der Konsistenzgruppe nicht widerspiegelt, schlägt der Vorgang fehl.
- Nach dem Klonen einer Konsistenzgruppe ist die entsprechende Zuordnungsoperation erforderlich.

  Weitere Informationen sind unter Igroups mehreren LUNs zuordnen oder Einem NVMe-Namensraum einem Subsystem zuordnen verfügbar.

- Das Klonen einer Konsistenzgruppe wird für eine Konsistenzgruppe in einer SnapMirror active sync-Beziehung oder mit zugehörigen DP Volumes nicht unterstützt.

System Manager

Schritte

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die Konsistenzgruppe aus, die Sie aus dem Menü **Konsistenzgruppe** klonen möchten.
3. Oben rechts auf der Übersichtsseite für die Konsistenzgruppe die Option **Klonen** auswählen.
4. Geben Sie einen Namen für die neue, geklonte Konsistenzgruppe ein oder übernehmen Sie den Standardnamen.
   a. Wählen Sie aus, ob Sie "**Thin Provisioning**" aktivieren möchten.
   b. **Split Clone** sollte ausgewählt werden, wenn die Konsistenzgruppe von ihrer Quelle getrennt und zusätzlicher Speicherplatz für die geklonte Konsistenzgruppe bereitgestellt werden soll.
5. Um die Konsistenzgruppe in ihrem aktuellen Zustand zu klonen, **Neuen Snapshot hinzufügen** auswählen.

   Um die Konsistenzgruppe anhand eines Snapshots zu klonen, die Option **Vorhandenen Snapshot verwenden** auswählen. Bei Auswahl dieser Option öffnet sich ein neues Untermenü. Den Snapshot auswählen, der als Grundlage für den Klonvorgang verwendet werden soll.

6. Wählen Sie **Clone** aus.

7. Zum Menü **Konsistenzgruppe** zurückkehren, um zu bestätigen, dass die Konsistenzgruppe geklont wurde.

CLI

Ab ONTAP 9.14.1 ist das Klonen einer Konsistenzgruppe mithilfe der CLI mit Cluster-Administratorrechten möglich.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine Konsistenzgruppe klonen

1. Der `consistency-group clone create`Befehl klont die Konsistenzgruppe in ihrem aktuellen zeitpunktgenauen Status. Um den Klonvorgang auf einem Snapshot zu basieren, ist der `-source-snapshot`Parameter einzuschließen.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

   Weitere Informationen zu `consistency-group clone create` finden sich in der "ONTAP-Befehlsreferenz".

Nächste Schritte

- Igroups mehreren LUNs zuordnen
- Einem NVMe-Namensraum einem Subsystem zuordnen

Löschen einer ONTAP Konsistenzgruppe

Wenn Sie feststellen, dass Sie eine Konsistenzgruppe nicht mehr benötigen, können Sie sie löschen.

Über diese Aufgabe

- Das Löschen einer Konsistenzgruppe löscht die Instanz der Konsistenzgruppe und hat keine Auswirkungen auf die zugehörigen Volumes oder LUNs. Das Löschen einer Konsistenzgruppe führt nicht zur Löschung der auf den einzelnen Volumes vorhandenen Snapshots, diese sind jedoch nicht mehr als Konsistenzgruppen-Snapshots zugänglich. Die Snapshots können jedoch weiterhin als gewöhnliche, granulare Volume-Snapshots verwaltet werden.
- ONTAP löscht eine Konsistenzgruppe automatisch, wenn alle Volumes in der Konsistenzgruppe gelöscht wurden.
- Das Löschen einer übergeordneten Konsistenzgruppe führt zum Löschen aller zugehörigen untergeordneten Konsistenzgruppen.
- Wenn eine Version von ONTAP zwischen 9.10.1 und 9.12.0 verwendet wird, können Volumes nur dann aus einer Konsistenzgruppe entfernt werden, wenn das Volume selbst gelöscht wird. In diesem Fall wird das Volume automatisch aus der Konsistenzgruppe entfernt. Ab ONTAP 9.12.1 ist es möglich, Volumes aus einer Konsistenzgruppe zu entfernen, ohne die Konsistenzgruppe zu löschen. Weitere Informationen zu diesem Vorgang finden sich unter Eine Konsistenzgruppe ändern.

Beispiel 7. Schritte

System Manager

1. **Speicher > Konsistenzgruppen** auswählen.
2. Wählen Sie die Konsistenzgruppe aus, die Sie löschen möchten.
3. Wählen Sie neben dem Namen der Konsistenzgruppe ⋮ dann **Löschen** aus.

CLI

Ab ONTAP 9.14.1 ist das Löschen einer Konsistenzgruppe über die CLI möglich.

Bevor Sie beginnen

- Sie müssen sich auf der Administrator-Ebene befinden, um diese Aufgabe auszuführen.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 ist es erforderlich, Cluster- oder SVM-Administrator zu sein, um diese Aufgabe auszuführen.

Eine Konsistenzgruppe löschen

1. Die Konsistenzgruppe löschen:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror Active Sync

Einführung

Informationen zu ONTAP SnapMirror Active Sync

SnapMirror active sync (vor ONTAP 9.15.1 als SnapMirror Business Continuity bezeichnet) ermöglicht die Fortführung von Geschäftsservices im Falle eines vollständigen Standortausfalls. Diese Technologie ermöglicht Anwendungen, nahtlos auf eine sekundäre Kopie umzuschalten, ohne manuelle Eingriffe oder benutzerdefinierte Skripte.

SnapMirror active sync (SM-as) ist als granularerer, kostengünstigerer und benutzerfreundlicherer Anwendungsschutz auf Applikationsebene mit automatischem Failover konzipiert. Mit SnapMirror active sync können mehrere Volumes einer Anwendung synchron zwischen Standorten an geografisch verteilten Orten repliziert werden. Im Falle einer Störung des primären Systems kann automatisch auf die sekundäre Kopie umgeschaltet werden, wodurch die Geschäftskontinuität für Tier-1-Anwendungen ermöglicht wird.

Die Vorschriften für Finanzinstitute in einigen Ländern verpflichten Unternehmen, regelmäßig über ihre sekundären Rechenzentren erreichbar zu sein. SnapMirror active sync ermöglicht mit seinen hochverfügbaren Clustern diese Rechenzentrumswechsel zur Sicherstellung der Geschäftskontinuität.

SnapMirror active sync wird auf AFF, ASA und ASA r2 Clustern unterstützt. Der primäre und der sekundäre Cluster müssen vom selben Typ sein: entweder AFF, ASA oder ASA r2. SnapMirror active sync schützt Applikationen mit iSCSI oder FCP LUNs oder NVMe Namespaces.

Ab Juli 2024 wurden Inhalte aus zuvor als PDFs veröffentlichten technischen Berichten in die ONTAP Produktdokumentation integriert. Die ONTAP SnapMirror active sync Dokumentation

> enthält nun Inhalte aus *TR-4878: SnapMirror active sync*.

Vorteile

SnapMirror active sync bietet folgende Vorteile:

- Kontinuierliche Verfügbarkeit für geschäftskritische Anwendungen.
- Fähigkeit, geschäftskritische Anwendungen abwechselnd von primären und sekundären Standorten aus zu hosten.
- Vereinfachtes Anwendungsmanagement mit Konsistenzgruppen für abhängige Schreibreihenfolgekonsistenz.
- Die Möglichkeit, das Failover für jede Anwendung zu testen.
- Sofortige Erstellung von Spiegelklonen ohne Beeinträchtigung der Anwendungsverfügbarkeit.
- Die Möglichkeit, geschützte und ungeschützte Workloads im selben ONTAP Cluster bereitzustellen.
- Die LUN-, NVMe-Namespace-, NVMe-Subsystem- oder Speichereinheitsidentität für SAN-Konfigurationen und die Volumenidentität für NAS-Konfigurationen bleiben gleich, sodass die Anwendung sie als ein gemeinsam genutztes virtuelles Gerät erkennt.
- Die Möglichkeit, sekundäre Cluster flexibel wiederzuverwenden, um sofortige Klone für die Anwendungsnutzung zu erstellen, beispielsweise für Entwicklungs-, Test-, UAT- oder Berichtszwecke, ohne die Anwendungsleistung oder Verfügbarkeit zu beeinträchtigen.

SnapMirror active sync ermöglicht den Schutz Ihrer Daten-LUNs oder NVMe-Namespaces in SAN-Konfigurationen sowie Volumes in NAS-Konfigurationen, wodurch Anwendungen im Falle einer Katastrophe transparent auf ein anderes System umschalten können, um die Geschäftskontinuität sicherzustellen. Weitere Informationen finden sich unter "Anwendungsfälle".

Schlüsselkonzepte

SnapMirror active sync verwendet Konsistenzgruppen in SAN-Konfigurationen und SVMs in NAS-Konfigurationen, um die Replizierung Ihrer Daten sicherzustellen. SnapMirror active sync verwendet den ONTAP Mediator oder, beginnend mit ONTAP 9.17.1, den Cloud Mediator für automatisches Failover, wodurch sichergestellt wird, dass die Daten im Katastrophenfall bereitgestellt werden. Bei der Planung Ihrer SnapMirror active sync-Bereitstellung ist es wichtig, die grundlegenden Konzepte von SnapMirror active sync und dessen Architektur zu verstehen.

Asymmetrie und Symmetrie

In symmetrischen Aktiv/Aktiv-SAN-Clusterkonfigurationen können beide Standorte für aktive E/A auf den lokalen Speicher zugreifen. Symmetrische Aktiv/Aktiv-Konfigurationen sind für Clusteranwendungen wie VMware vMSC, Windows Failover Cluster mit SQL und Oracle RAC optimiert.

In asymmetrischen Aktiv/Aktiv SAN-Konfigurationen werden Daten am sekundären Standort an eine LUN, einen Namespace oder eine Speichereinheit weitergeleitet.

Weitere Informationen finden sich unter SnapMirror Active Sync-Architektur.

In NAS-Konfigurationen gibt es keinen Proxy und die sekundäre SVM ist inaktiv, aber die Volumes können auf eine andere SVM geklont werden, um Zugriff darauf bereitzustellen.

Konsistenzgruppe (nur SAN)

Für AFF und ASA Systeme ist eine "Konsistenzgruppe"Konsistenzgruppe eine Sammlung von FlexVol Volumes, die eine Konsistenzgarantie für die Anwendungs-Workload bieten, die zum Schutz der

Geschäftskontinuität erforderlich ist. In ASA r2 Systemen ist eine Konsistenzgruppe eine Sammlung von Speichereinheiten.

Der Zweck einer Konsistenzgruppe besteht darin, gleichzeitig Snapshot-Kopien einer Sammlung von Volumes oder Speichereinheiten zu erstellen und so absturzkonsistente Kopien der Sammlung zu einem bestimmten Zeitpunkt zu gewährleisten. Eine Konsistenzgruppe stellt sicher, dass alle Volumes eines Datasets in den Ruhezustand versetzt und dann exakt zum selben Zeitpunkt gesichert werden. Dies bietet einen datenkonsistenten Wiederherstellungspunkt über alle Volumes oder Speichereinheiten hinweg, die das Dataset unterstützen. Eine Konsistenzgruppe stellt dabei die Konsistenz der abhängigen Schreibreihenfolge sicher. Soll Anwendungen für die Geschäftskontinuität Schutz geboten werden, muss die Gruppe der dieser Anwendung entsprechenden Volumes oder Speichereinheiten einer Konsistenzgruppe hinzugefügt werden, sodass eine Datensicherungsbeziehung zwischen einer Quell- und einer Ziel-Konsistenzgruppe besteht. Die Quell- und die Ziel-Konsistenzgruppe müssen die gleiche Anzahl und den gleichen Typ von Volumes enthalten.

SVM- und FlexVol-Unterstützung (SnapMirror active sync für NAS)

In ONTAP 9.19.1 unterstützt SnapMirror active sync für NAS den Schutz von SVMs, die FlexVol Volumes enthalten. Konsistenzgruppen oder FlexGroup Volumes innerhalb einer SVM werden von SnapMirror active sync in NAS-Konfigurationen nicht unterstützt.

Bestandteil

In einer SAN-Konfiguration ist ein Bestandteil ein einzelnes Volume, eine LUN oder ein NVMe-Namespace (beginnend mit ONTAP 9.17.1), das Teil der Konsistenzgruppe ist, die in der SnapMirror active sync-Beziehung geschützt ist.

In einer NAS-Konfiguration ist ein Bestandteil ein Volume, und die enthaltende SVM ist die Entität, die in der SnapMirror active sync-Beziehung geschützt wird.

ONTAP Mediator

Der "ONTAP Mediator" empfängt Statusinformationen über verbundene ONTAP Cluster und Knoten, koordiniert zwischen beiden und ermittelt, ob jeder Knoten bzw. Cluster betriebsbereit ist. ONTAP Mediator liefert Statusinformationen über:

- Peer ONTAP Cluster
- Peer ONTAP Clusterknoten
- Failover-Einheiten (die Konsistenzgruppen in einer SnapMirror Aktiv/Synchronisierung-für-SAN-Beziehung und SVMs in einer SnapMirror Aktiv/Synchronisierung-für-NAS-Beziehung entsprechen); für jede Failover-Einheit sind die folgenden Informationen angegeben:
  - Replikationsstatus: Nicht initialisiert, Synchron, oder Nicht synchron
  - Welcher Cluster hostet die primäre Kopie
  - Betriebskontext (wird für geplanten Failover verwendet)

Mit diesen ONTAP Mediator-Gesundheitsinformationen können Cluster zwischen verschiedenen Fehlertypen unterscheiden und feststellen, ob ein automatisches Failover durchgeführt werden soll. ONTAP Mediator ist neben beiden ONTAP Clustern (primär und sekundär) eine der drei Parteien im SnapMirror Aktiv-Sync-Quorum. Um einen Konsens zu erreichen, müssen mindestens zwei Parteien im Quorum einer bestimmten Operation zustimmen.



Ab ONTAP 9.15.1 zeigt der System Manager den Status Ihrer SnapMirror Active Sync-Beziehung von beiden Clustern aus an. Auch der Status des ONTAP Mediators kann im System Manager von beiden Clustern aus überwacht werden. In früheren Versionen von ONTAP zeigt System Manager den Status von SnapMirror Aktiv/Aktiv-Synchronisierungsbeziehungen vom

Quell-Cluster an.

ONTAP Cloud Mediator

ONTAP Cloud Mediator ist ab ONTAP 9.17.1 verfügbar. ONTAP Cloud Mediator bietet die gleichen Dienste wie ONTAP Mediator, wird jedoch in der Cloud über die NetApp Console gehostet.

Geplantes Failover

Ein manueller Vorgang zum Ändern der Rollen von Kopien in einer SnapMirror Aktiv/Aktiv-Synchronisierungsbeziehung. Der primäre Standort wird zum sekundären und der sekundäre zum primären.

Automatisches ungeplantes Failover (AUFO)

Ein automatischer Vorgang zur Durchführung eines Failovers auf die Spiegelkopie. Der Vorgang erfordert die Unterstützung des ONTAP Mediators, um zu erkennen, dass die primäre Kopie nicht verfügbar ist.

Primärwahl und Primär-Bias

SnapMirror active sync verwendet das Prinzip „Primär zuerst“, das der primären Kopie Vorrang bei der Bedienung von E/A-Vorgängen im Falle einer Netzwerkpartition einräumt.

Primär-Bias ist eine spezielle Quorum-Implementierung, die die Verfügbarkeit eines durch SnapMirror active sync geschützten Datensatzes verbessert. Wenn die primäre Kopie verfügbar ist, tritt Primär-Bias in Kraft, wenn der ONTAP Mediator von beiden Clustern aus nicht erreichbar ist.

Primary-first und Primary Bias werden in SnapMirror Aktiv/Sync SAN-Konfigurationen ab ONTAP 9.11.1 unterstützt. Primäre Kopien werden im System Manager festgelegt und mit der REST API und CLI ausgegeben.

Nicht synchronisiert (OOS)

Wenn die Anwendungs-E/A nicht auf das sekundäre Speichersystem repliziert wird, wird dies als **nicht synchron** gemeldet. Ein „nicht synchron“-Status bedeutet, dass die sekundären Volumes nicht mit dem primären (Quell-)Volume synchronisiert sind und dass die SnapMirror Replizierung nicht erfolgt.

Wenn der Spiegelungsstatus `Snapmirrored` ist, bedeutet dies, dass eine SnapMirror Beziehung hergestellt wurde und der Datentransfer abgeschlossen ist, das heißt, das Zielvolume ist auf dem neuesten Stand mit dem Quellvolume.

SnapMirror active sync unterstützt die automatische Resynchronisierung, sodass Kopien wieder in den InSync-Zustand versetzt werden können.

Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync "automatische Rekonfiguration in Fan-Out Konfigurationen".

Uniforme und nicht-uniforme Konfiguration

- **Einheitlicher Hostzugriff** bedeutet, dass Hosts beider Standorte mit allen Pfaden zu den Speicherclustern beider Standorte verbunden sind. Standortübergreifende Pfade werden über Entfernungen hinweg genutzt. Einheitlicher Hostzugriff gilt nur für SAN Konfigurationen.
- **Nicht-uniformer Hostzugriff** bedeutet, dass Hosts von jedem Standort nur mit dem Cluster am selben Standort verbunden sind. Standortübergreifende Pfade und gestreckte Pfade sind nicht verbunden.



Einheitlicher Hostzugriff wird für jede SnapMirror active sync-Bereitstellung unterstützt, nicht-einheitlicher Hostzugriff wird nur für symmetrische Aktiv/Aktiv-Bereitstellungen unterstützt.

Zero RPO

RPO steht für Recovery Point Objective, also das Maß an Datenverlust, das innerhalb eines bestimmten Zeitraums als akzeptabel gilt. Ein RPO von Null bedeutet, dass kein Datenverlust akzeptabel ist.

Zero RTO

RTO steht für Recovery Time Objective, also das Wiederherstellungszeitziel, und bezeichnet die Zeitspanne, die als akzeptabel gilt, damit eine Anwendung nach einem Ausfall, Fehler oder einem anderen Datenverlustereignis unterbrechungsfrei wieder zum Normalbetrieb zurückkehrt. Zero RTO bedeutet, dass keinerlei Ausfallzeit akzeptabel ist.

SnapMirror Aktiv/Aktiv-Synchronisierungs-Konfigurationsunterstützung nach ONTAP Version

Die von SnapMirror active sync unterstützten Clustertypen, Protokolle und Konfigurationen variieren je nach Ihrer ONTAP Version. Die Tabelle zeigt die ONTAP Version, in der die Aktualisierungen hinzugefügt wurden, sowie die Konfigurationen, die diese Aktualisierungen unterstützen.

Beginnend mit ONTAP…	SnapMirror active sync unterstützt
9.19.1	NAS-Workloads auf SVM-Ebene • Unterstützte Protokolle: NFS (v3 und v4) und SMB (2.x oder höher) • Unterstützte Clustertypen: AFF (nur 2-Knoten) oder AFX (nur 4-Knoten) • Unterstützung für lesen/schreiben-Zugriff nur auf dem primären System. Die sekundäre SVM und die darin enthaltenen Volumes sind über NAS-Protokolle nicht zugänglich, aber Sie können die sekundären Volumes in eine andere SVM klonen, um den Zugriff darauf bereitzustellen.
9.17.1	NVMe für VMware Host-Workloads
9.16.1	• ASA r2, nur 2-Knoten-Cluster • AFF und ASA symmetrische Aktiv/Aktiv 4-Node auf 4-Node Clustern Symmetrische Aktiv/Aktiv Konfigurationen unterstützen in ONTAP 9.16.1 und späteren Versionen neben 2-Knoten-zu-2-Knoten-Clustern auch 4-Knoten-zu-4-Knoten-Cluster. Für ASA r2 werden nur 2-Node-zu-2-Node-Cluster unterstützt.
9.15.1	Der folgende Konfigurationstyp: • Symmetrische Aktiv/Aktiv Konfigurationen nur auf 2-Knoten-Clustern Symmetrische Aktiv/Aktiv Konfigurationen ermöglichen es beiden Kopien einer geschützten LUN, lesen/schreiben E/A-Vorgänge mit bidirektionaler synchroner Replizierung auszuführen, sodass jede LUN-Kopie lokale E/A-Anforderungen bedienen kann.

Beginnend mit ONTAP…	SnapMirror active sync unterstützt
9.9.1	Systeme * AFF * ASA (nur C-Serie) Protokolle: • iSCSI • FC (nur Frontend-Unterstützung) Konfigurationstypen: • Asymmetrisch Aktiv/Aktiv

Primäre und sekundäre Cluster müssen vom gleichen Typ sein: entweder "ASA", "ASA r2" oder AFF.

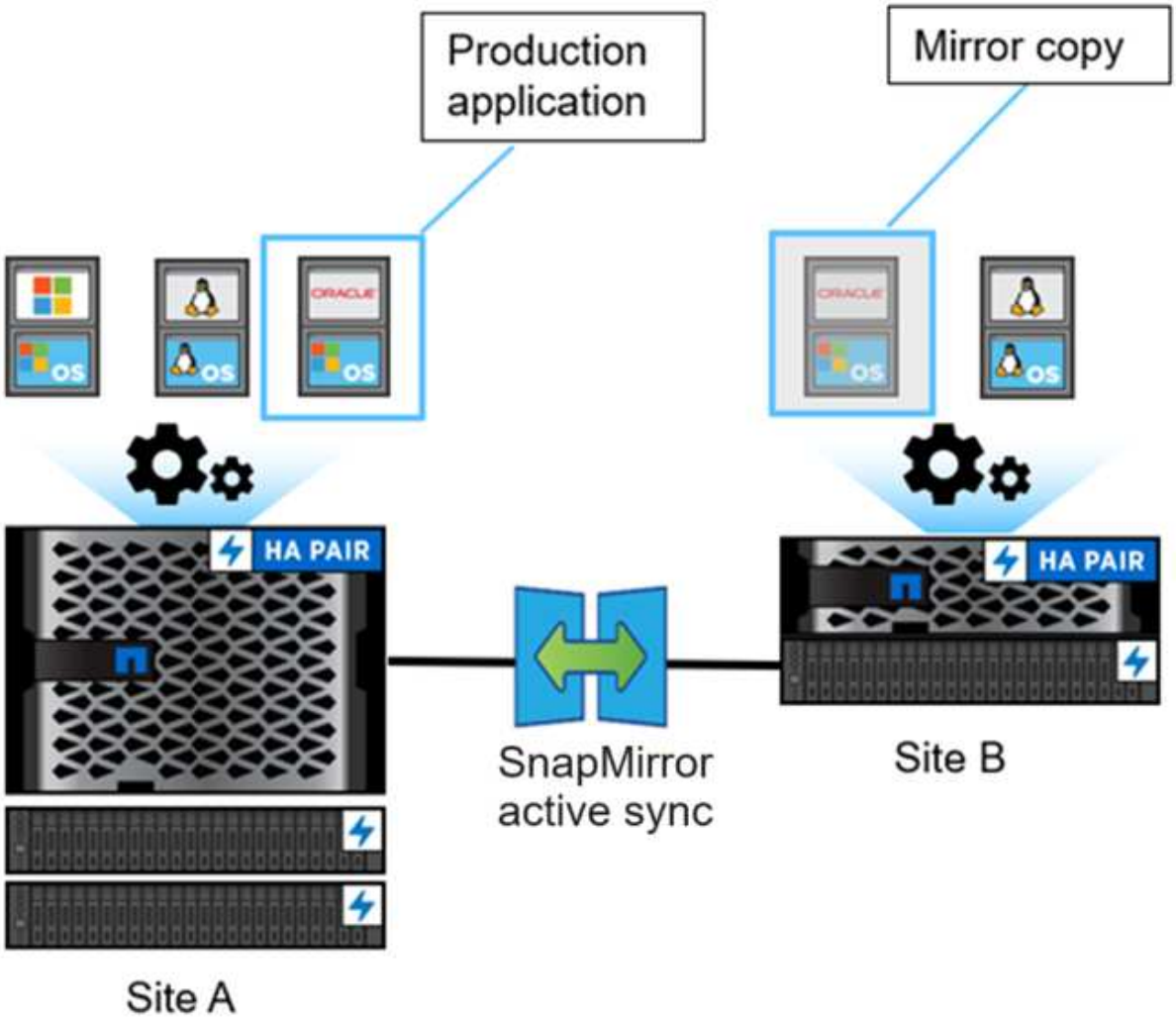
Weitere Konfigurationsinformationen sind verfügbar unter:

- "SnapMirror Active Sync-Voraussetzungen"
- "SnapMirror Active Sync-Objektbeschränkungen"

ONTAP SnapMirror Active Sync-Architektur

Die SnapMirror active sync Architektur ermöglicht aktive Workloads auf beiden Clustern, wobei primäre Workloads gleichzeitig von beiden Clustern bereitgestellt werden können. Vorschriften für Finanzinstitute in einigen Ländern verlangen, dass Unternehmen regelmäßig auch von ihren sekundären Rechenzentren aus bedient werden können, sogenannte „Tick-Tock“-Bereitstellungen, die durch SnapMirror active sync ermöglicht werden.

In einer SAN-Konfiguration wird die Datensicherungsbeziehung zum Schutz der Geschäftskontinuität zwischen Quell-Storage-System und Ziel-Storage-System hergestellt, indem die anwendungsspezifischen LUNs oder NVMe-Namespaces aus verschiedenen Volumes innerhalb einer Storage Virtual Machine (SVM) zur Konsistenzgruppe hinzugefügt werden. Im Normalbetrieb schreibt die Unternehmensanwendung in die primäre Konsistenzgruppe, die diese E/A synchron in die Spiegel-Konsistenzgruppe repliziert.



Obwohl in der Datensicherungsbeziehung zwei separate Datenkopien existieren, sieht der Anwendungshost dies als ein gemeinsam genutztes virtuelles Gerät mit mehreren Pfaden, da SnapMirror active sync in einer SAN-Konfiguration dieselbe LUN- oder NVMe-Namespace-Identität und in einer NAS-Konfiguration dieselben Volumes in einer SVM beibehält, während jeweils nur auf eine LUN-, NVMe-Namespace- oder Volume-Kopie geschrieben wird. Wenn ein Ausfall das primäres Storage-System offline nimmt, erkennt ONTAP diesen Ausfall und verwendet den Mediator zur erneuten Bestätigung; können weder ONTAP noch der Mediator den primären Standort anpingen, führt ONTAP den automatischen Failover-Vorgang durch. Durch diesen Prozess wird nur eine bestimmte Anwendung per Failover umgeschaltet, ohne dass manuelle Eingriffe oder Skripte erforderlich sind, wie sie zuvor für das Failover notwendig waren.

Weitere zu berücksichtigende Punkte:

- Nicht gespiegelte Volumes, die außerhalb des Schutzes für Geschäftskontinuität existieren, werden unterstützt.
- Eine einzelne SnapMirror asynchrone Fan-Out-Beziehung wird für Volumes unterstützt, die für Geschäftskontinuität geschützt werden. In NAS-Konfigurationen wird ausschließlich eine volumebasierte asynchrone Beziehung unterstützt. Asynchrone Beziehungen für SVMs oder Konsistenzgruppen werden nicht unterstützt.
- Kaskadentopologien werden mit Schutz für die Geschäftskontinuität nicht unterstützt.

Die Rolle der Mediatoren

SnapMirror active sync verwendet einen Mediator als passiven Zeugen für SnapMirror active sync Kopien. Im Falle einer Netzwerkpartition oder der Nichtverfügbarkeit einer Kopie nutzt SnapMirror active sync den Mediator, um zu bestimmen, welche Kopie weiterhin E/A bedient, während die E/A auf der anderen Kopie eingestellt wird. Zusätzlich zum lokalen ONTAP Mediator kann ab ONTAP 9.17.1 der ONTAP Cloud Mediator installiert werden, um dieselbe Funktionalität in einer Cloud-Bereitstellung bereitzustellen. Es kann entweder der ONTAP Mediator oder der ONTAP Cloud Mediator verwendet werden, jedoch nicht beide gleichzeitig.

Der Mediator spielt in SnapMirror active sync Konfigurationen eine entscheidende Rolle als passiver Quorum-Zeuge, gewährleistet die Quorum-Aufrechterhaltung und ermöglicht den Datenzugriff bei Ausfällen. Er fungiert als Ping-Proxy für Controller, um die Verfügbarkeit von Peer-Controllern zu ermitteln. Obwohl der Mediator keine Switchover-Operationen aktiv auslöst, erfüllt er eine wichtige Funktion, indem er dem verbleibenden Knoten ermöglicht, den Status seines Partners bei Netzwerkkommunikationsproblemen zu überprüfen. In seiner Rolle als Quorum-Zeuge stellt der ONTAP Mediator einen alternativen Pfad bereit (und dient somit effektiv als Proxy) zum Peer-Cluster.

Darüber hinaus ermöglicht es Clustern, diese Informationen im Rahmen des Quorum-Prozesses zu erhalten. Es werden die Node-Management-LIF und die Cluster-Management-LIF für Kommunikationszwecke verwendet. Es werden redundante Verbindungen über mehrere Pfade hergestellt, um zwischen Standortausfall und InterSwitch Link (ISL)-Ausfall zu unterscheiden. Wenn ein Cluster aufgrund eines Ereignisses die Verbindung zur Mediator-Software und zu allen seinen Nodes verliert, gilt es als nicht erreichbar. Dies löst eine Warnung aus und ermöglicht ein automatisiertes Failover zur Spiegel-Konsistenzgruppe am sekundären Standort, wodurch eine unterbrechungsfreie I/O für den Client sichergestellt wird. Der Replikations-Datenpfad basiert auf einem Heartbeat-Mechanismus, und wenn eine Netzwerkstörung oder ein Ereignis länger als einen bestimmten Zeitraum andauert, kann dies zu Heartbeat-Ausfällen führen, wodurch die Beziehung aus dem Synchronisationszustand gerät. Das Vorhandensein redundanter Pfade, wie etwa ein LIF-Failover auf einen anderen Port, kann jedoch den Heartbeat aufrechterhalten und solche Störungen verhindern.

ONTAP Mediator

ONTAP Mediator ist in einer dritten Ausfalldomäne installiert, die von den beiden ONTAP-Clustern, die er überwacht, getrennt ist. In dieser Konfiguration gibt es drei Hauptkomponenten:

SAN Konfigurationen

- Primärer ONTAP Cluster, der die SnapMirror Aktiv-Sync primäre Konsistenzgruppe hostet
- Sekundärer ONTAP Cluster, der die Spiegel-Konsistenzgruppe hostet
- ONTAP Mediator

NAS Konfigurationen

- Primärer ONTAP Cluster, der die SnapMirror Aktiv-Sync primäre SVM hostet
- Sekundärer ONTAP Cluster, der die Spiegel-SVM hostet
- ONTAP Mediator

ONTAP Mediator wird für folgende Zwecke verwendet:

- Feststellung der Beschlussfähigkeit
- Kontinuierliche Verfügbarkeit durch automatisches Failover (AUFO)
- Geplante Failover (PFO)

Wenn der ONTAP Mediator nicht verfügbar ist, können geplante oder automatisierte Failover

nicht durchgeführt werden. Die Anwendungsdaten werden weiterhin synchron und ohne Unterbrechung repliziert, sodass kein Datenverlust auftritt.

Weitere Informationen finden Sie in "ONTAP Mediator Dokumentation".

ONTAP Cloud Mediator

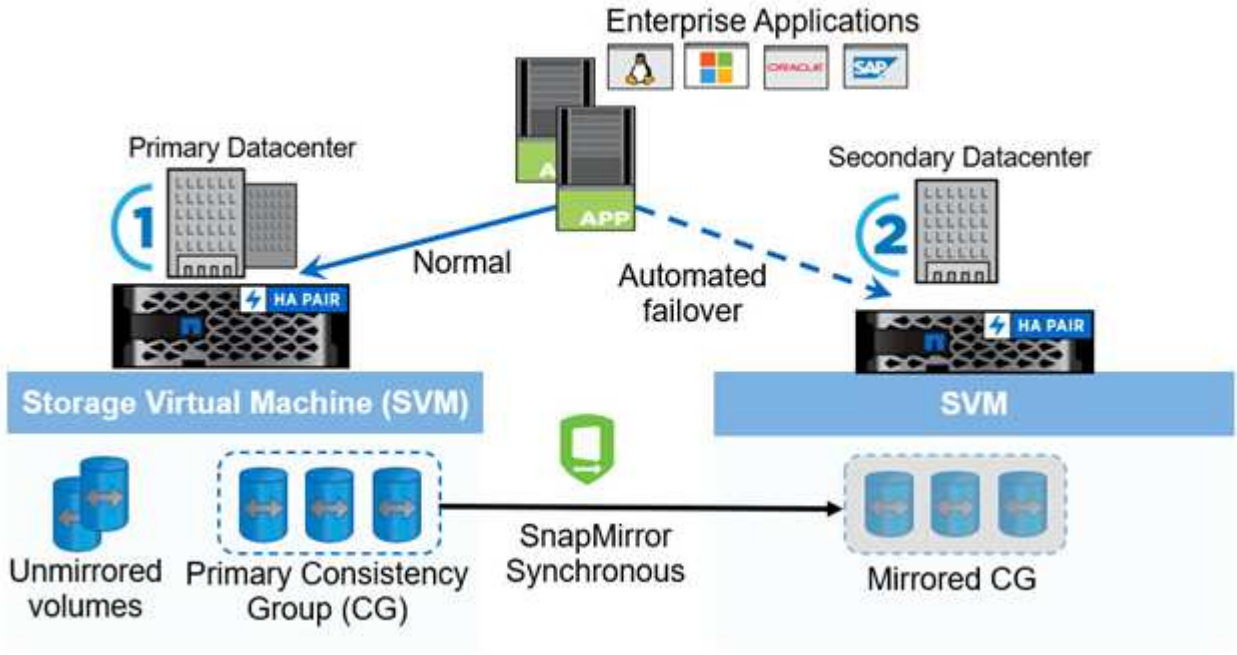
Ab ONTAP 9.17.1 ist ONTAP Cloud Mediator als Cloud-basierter Dienst in der NetApp Console für die Verwendung mit SnapMirror active sync verfügbar. Ähnlich wie ONTAP Mediator bietet ONTAP Cloud Mediator die folgende Funktionalität in einer SnapMirror active sync Beziehung:

- Bietet einen persistenten und abgeschotteten Speicher für HA- oder SnapMirror active sync-Metadaten.
- Dient als Ping-Proxy für die Controller-Lebendigkeit.
- Stellt eine synchrone Abfragefunktion für den Zustand von Knoten bereit, um die Quorumbestimmung zu unterstützen.

Der ONTAP Cloud Mediator vereinfacht die Bereitstellung von SnapMirror Active Sync, indem der NetApp Console Cloud-Service als dritter Standort genutzt wird, der nicht verwaltet werden muss. Der ONTAP Cloud Mediator Service bietet die gleiche Funktionalität wie der lokale ONTAP Mediator, jedoch reduziert der ONTAP Cloud Mediator die betriebliche Komplexität bei der Wartung eines dritten Standorts. Im Gegensatz dazu ist der ONTAP Mediator als Paket verfügbar und muss auf einem Linux-Host an einem dritten Standort mit unabhängiger Strom- und Netzwerkinfrastruktur für seinen Betrieb installiert werden.

SnapMirror Active Sync-Operationsworkflow für SAN-Konfigurationen

Die folgende Abbildung veranschaulicht das Design der SnapMirror Active Sync in SAN-Konfiguration auf hoher Ebene.



Das Diagramm zeigt eine Unternehmensanwendung, die auf einer Storage-VM (SVM) im primären Rechenzentrum gehostet wird. Die SVM enthält fünf Volumes, von denen drei Teil einer Konsistenzgruppe sind. Die drei Volumes in der Konsistenzgruppe werden in ein sekundäres Rechenzentrum gespiegelt. Unter normalen Umständen werden alle Schreibvorgänge im primären Rechenzentrum ausgeführt, sodass dieses Rechenzentrum als Quelle für E/A-Operationen dient, während das sekundäre Rechenzentrum als Ziel dient.

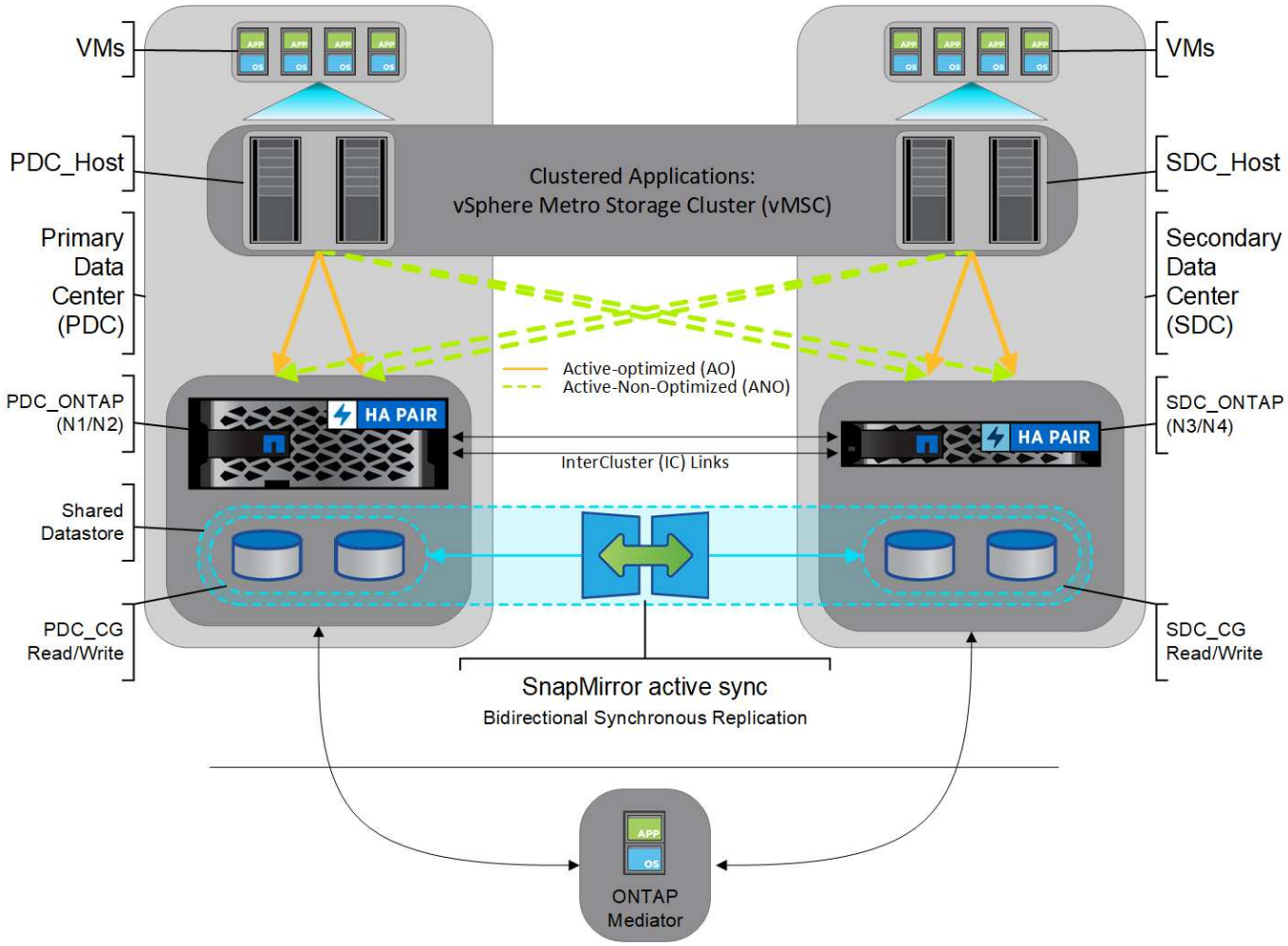
Im Katastrophenfall im primären Rechenzentrum weist ONTAP das sekundäre Rechenzentrum an, als primäres zu fungieren und alle I/O-Operationen auszuführen. Nur die Volumes, die in der Konsistenzgruppe gespiegelt sind, werden bedient. Alle Operationen, die die anderen beiden Volumes auf der SVM betreffen, sind von dem Katastrophenereignis betroffen.

Symmetrisch Aktiv/Aktiv

SnapMirror active sync bietet asymmetrische und symmetrische Lösungen für SAN-Konfigurationen.

In asymmetrischen Konfigurationen stellt die primäre Speicherkopie einen aktiv optimierten Pfad bereit und bedient aktiv die Client-I/O. Der sekundäre Standort verwendet einen Remote-Pfad für die I/O. Die Speicherpfade des sekundären Standorts gelten als aktiv-nicht-optimiert. Der Zugriff auf die Schreib-LUN wird vom sekundären Standort aus weitergeleitet. NVMe-Protokoll wird in asymmetrischen Konfigurationen nicht unterstützt.

In symmetrischen Aktiv/Aktiv-Konfigurationen werden aktiv-optimierte Pfade an beiden Standorten bereitgestellt, sind hostspezifisch und konfigurierbar, was bedeutet, dass Hosts auf beiden Seiten für aktive E/A auf den lokalen Speicher zugreifen können. Ab ONTAP 9.16.1 wird die symmetrische Aktiv/Aktiv-Konfiguration auf 2-Node-Clustern und auf 4-Node-Clustern unterstützt. SnapMirror active sync unterstützt 2-Node-Cluster-zu-2-Node-Cluster-Konfigurationen und 4-Node-Cluster-zu-4-Node-Cluster-Konfigurationen. Konfigurationen von 4-Node-Cluster zu 2-Node-Cluster oder von 2-Node-Cluster zu 4-Node-Cluster werden nicht unterstützt. Ab ONTAP 9.17.1 unterstützen symmetrische Aktiv/Aktiv-Konfigurationen das NVMe-Protokoll auf 2-Node-Clustern.

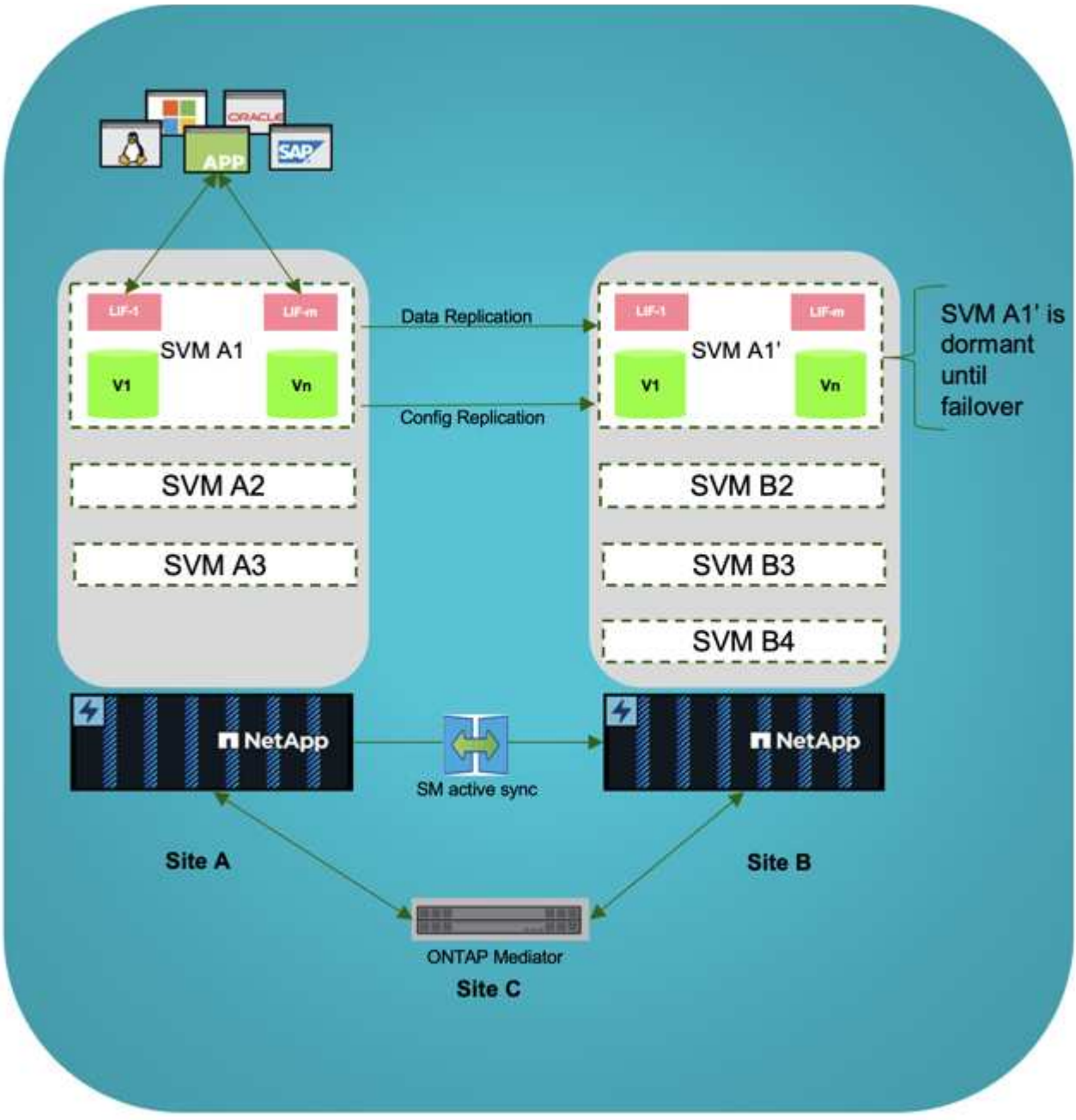


Symmetrisches Aktiv/Aktiv ist für Clusteranwendungen wie VMware Metro Storage Cluster, Oracle RAC und

Windows Failover Clustering mit SQL vorgesehen.

SnapMirror Active Sync-Operationsworkflow für NAS-Konfigurationen

Ab ONTAP 9.19.1 bietet SnapMirror active sync Schutz für NAS-Workloads auf SVM-Ebene. In einer NAS-Konfiguration bleibt die Ziel-SVM (sekundäre SVM) im Ruhezustand, bis ein Failover-Ereignis eintritt. Um einen unterbrechungsfreien Failover zu ermöglichen, müssen die Netzwerkidentität und die Protokollkonfigurationen, einschließlich der IP-Adressen, auf der primären und der sekundären SVM identisch sein. Diese Konfigurationen werden automatisch auf den sekundären Cluster repliziert, wodurch konsistente IP-Adressierung und Protokolleinstellungen in beiden Clustern sichergestellt werden. Die folgende Abbildung zeigt das Design von SnapMirror active sync in einer NAS-Konfiguration auf hoher Ebene.



In ONTAP 9.19.1 werden nur FlexVol Volumes unterstützt. Konsistenzgruppen werden nicht unterstützt. Bei ausschließlicher FlexVol Unterstützung gewährleistet der sekundäre Cluster keine konsistente Schreibreihenfolge über Volumes hinweg. In der Abbildung werden Daten und Konfigurationsinformationen von

SVM A1 im Quell-Cluster auf die inaktive SVM, SVM A1', im Ziel-Cluster repliziert.

Anwendungsfälle für ONTAP SnapMirror Active Sync

Die Anforderungen eines global vernetzten Geschäftsumfelds erfordern eine schnelle Wiederherstellung geschäftskritischer Applikationsdaten ohne Datenverlust im Falle von Störungen wie Cyberangriffen, Stromausfällen oder Naturkatastrophen. Diese Anforderungen sind in Bereichen wie dem Finanzsektor und bei Unternehmen, die regulatorischen Vorgaben wie der General Data Protection Regulation (GDPR) unterliegen, besonders hoch.

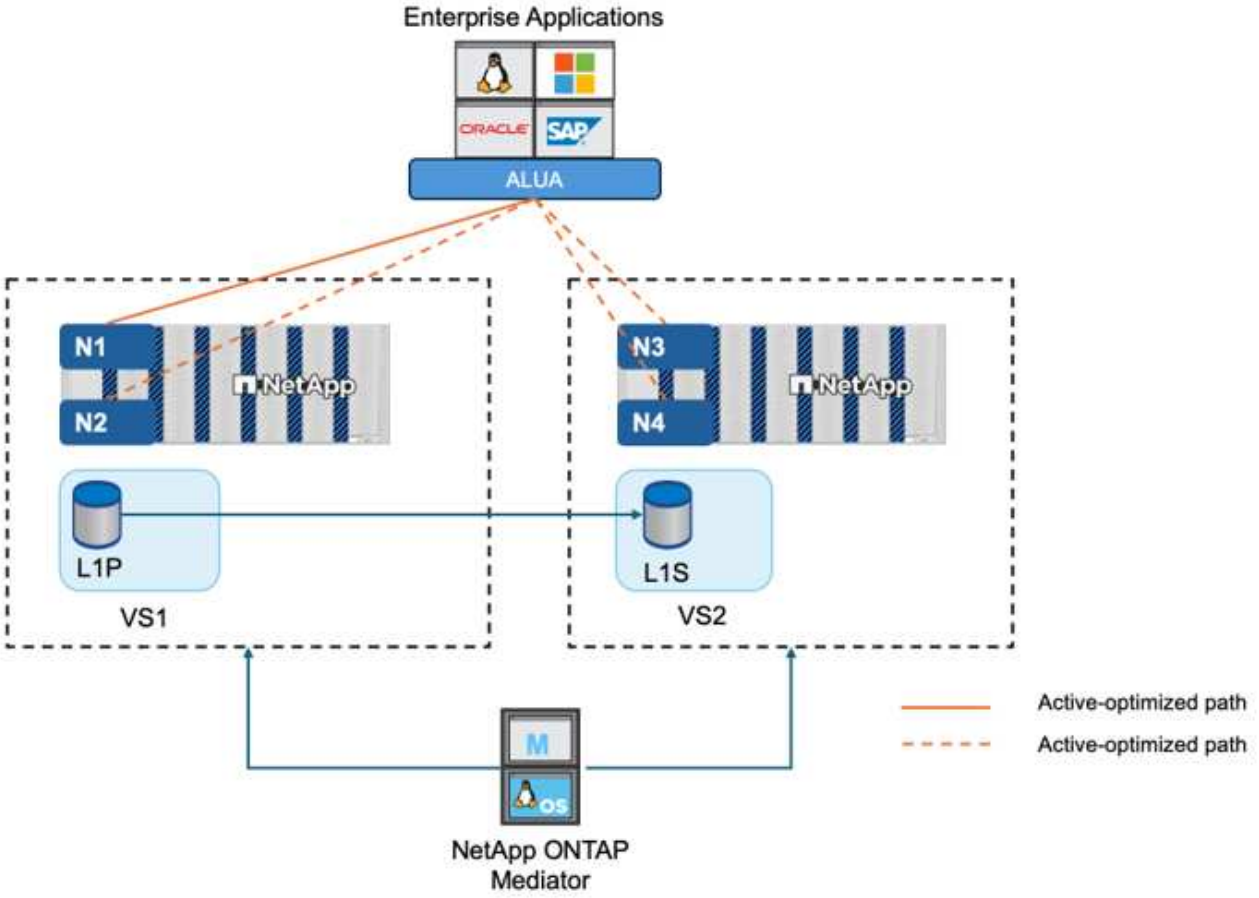
SnapMirror active sync bietet folgende Anwendungsfälle:

Anwendungsbereitstellung für ein Recovery Time Objective (RTO) von null

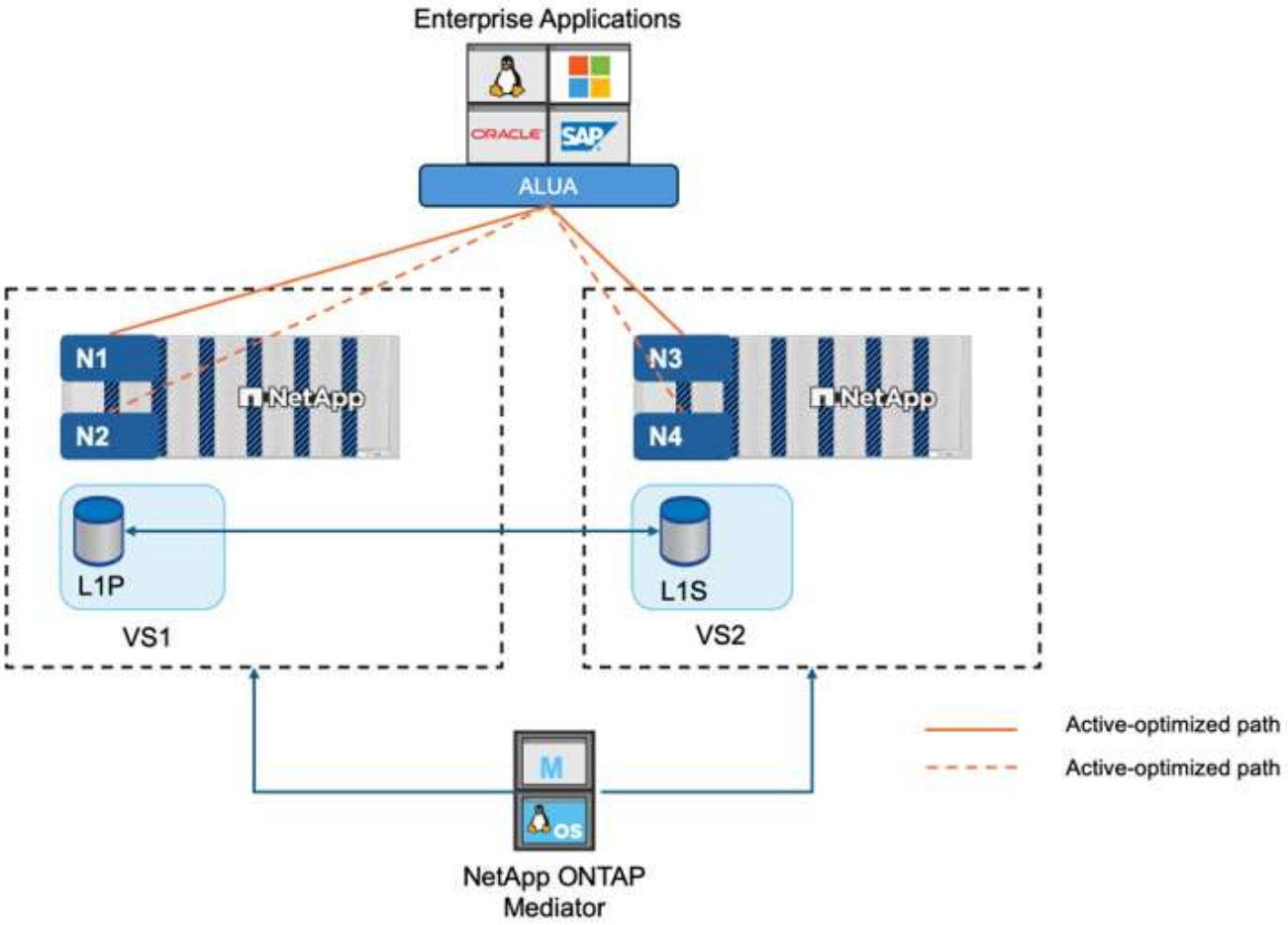
In einer SnapMirror active sync-Umgebung gibt es einen primären und einen sekundären Cluster. Eine LUN im primären Cluster `L1P` hat ein Spiegelbild `L1S` im sekundären Cluster; beide LUNs verwenden dieselbe serielle ID und werden dem Host als Lese-/Schreib-LUNs gemeldet. In asymmetrischen Konfigurationen werden Lese- und Schreibvorgänge jedoch nur auf der primären LUN ausgeführt `L1P`. Schreibvorgänge auf das Spiegelbild `L1S` werden über einen Proxy abgewickelt.

Anwendungsbereitstellung für null RTO oder transparentes Anwendungs-Failover (TAF)

TAF basiert auf dem softwarebasierten Pfad-Failover der Host-MPIO-Software, um einen unterbrechungsfreien Zugriff auf den Speicher zu ermöglichen. Beide LUN Kopien, beispielsweise die primäre (L1P) und die Spiegelkopie (L1S), besitzen dieselbe Identität (Seriennummer) und werden dem Host als lese- und schreibbar gemeldet. In asymmetrischen Konfigurationen werden Lese- und Schreibvorgänge jedoch ausschließlich vom primären Volume ausgeführt. E/A-Vorgänge, die an die Spiegelkopie gerichtet sind, werden an die primäre Kopie weitergeleitet. Der bevorzugte Pfad des Hosts zu L1 ist VS1:N1, basierend auf dem ALUA-Zugriffsstatus Aktiv Optimiert (A/O). ONTAP Mediator ist für die Bereitstellung erforderlich, hauptsächlich um das Failover (geplant oder ungeplant) im Falle eines Speicherausfalls auf dem primären Volume durchzuführen.



TAF arbeitet in zwei Modi: Automatisches Failover und Automatisches Failover Duplex. Bei Automatischem Failover werden Lese- und Schreibvorgänge ausschließlich vom primären Volume verarbeitet, daher werden IOs, die an die Spiegelkopie (die selbst keine Schreibvorgänge ausführen kann) gerichtet sind, an die primäre Kopie weitergeleitet. Bei Automatischem Failover Duplex können sowohl die primäre als auch die sekundäre Kopie IOs verarbeiten, sodass kein Proxy erforderlich ist.



Wenn Sie NVMe für den Hostzugriff mit ONTAP 9.17.1 verwenden, wird nur die AutomatedFailoverDuplex Richtlinie unterstützt.

SnapMirror active sync verwendet ALUA, einen Mechanismus, der es einem Anwendungshost ermöglicht, Multipathing-Software mit Pfaden zu nutzen, die mit Prioritäten und Zugriffsverfügbarkeit für die Kommunikation des Anwendungshosts mit dem Storage-Array angekündigt werden. ALUA kennzeichnet aktive optimierte Pfade zu den Controllern, denen die LUN gehört, und andere als aktive nicht optimierte Pfade, die nur verwendet werden, wenn der primäre Pfad ausfällt.

SnapMirror active sync mit NVMe-Protokoll verwendet Asymmetric Namespace Access (ANA), wodurch Anwendungshosts optimierte und nicht optimierte Pfade zu geschützten NVMe-Namespaces ermitteln können. Das ONTAP NVMe Target veröffentlicht die entsprechenden Pfadzustände, sodass Anwendungshosts den optimalen Pfad für einen geschützten NVMe-Namespace nutzen können.

Clusteranwendungen

Clusterbasierte Applikationen, einschließlich VMware Metro Storage Cluster, Oracle RAC und Windows Failover Clustering mit SQL, erfordern simultanen Zugriff, sodass die VMs ohne Leistungseinbußen auf einen anderen Standort überführt werden können. SnapMirror active sync Symmetric Aktiv/Aktiv bedient IO lokal mit bidirektionaler Replizierung, um die Anforderungen clusterbasierter Applikationen zu erfüllen. Ab ONTAP 9.16.1 wird Symmetric Aktiv/Aktiv in einer Konfiguration mit vier Node Clustern unterstützt, wodurch die Zwei-Node-Cluster-Beschränkung in ONTAP 9.15.1 erweitert wird.

Katastrophenszenario

Mehrere Volumes einer Anwendung lassen sich synchron zwischen geografisch verteilten Standorten replizieren. Bei einer Störung des primären Clusters kann automatisch auf die sekundäre Kopie umgeschaltet

werden, wodurch die Geschäftskontinuität für Tier-1-Applikationen gewährleistet wird. Wenn der Standort, an dem sich das primäre Cluster befindet, von einer Katastrophe betroffen ist, markiert die Multipathing-Software des Hosts alle Pfade durch das Cluster als ausgefallen und verwendet die Pfade des sekundären Clusters. Das Ergebnis ist ein unterbrechungsfreies Failover auf die Spiegelkopie, ermöglicht durch ONTAP Mediator.

Erweiterte Anwendungsunterstützung

SnapMirror active sync bietet Flexibilität mit einfach zu verwendender, applikationsspezifischer Granularität und automatischem Failover. SnapMirror active sync verwendet die bewährte SnapMirror synchrone Replizierung über ein IP-Netzwerk, um Daten mit hoher Geschwindigkeit über LAN oder WAN zu replizieren, sodass eine hohe Datenverfügbarkeit und schnelle Datenreplizierung für geschäftskritische Applikationen wie Oracle, Microsoft SQL Server und andere sowohl in virtuellen als auch in physischen Umgebungen erreicht werden.

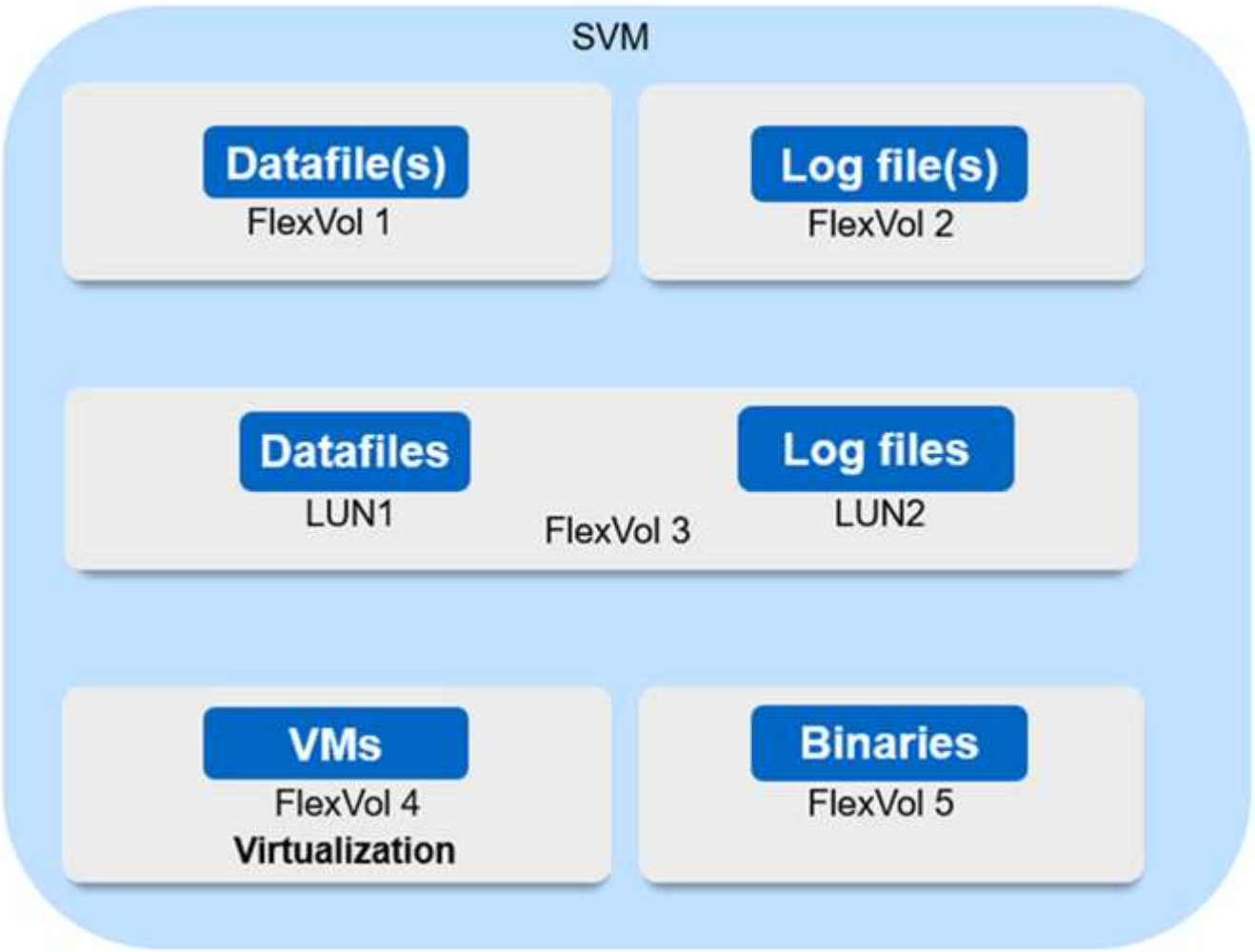
SnapMirror active sync ermöglicht, dass geschäftskritische Business-Services auch bei einem vollständigen Standortausfall mit TAF auf die sekundäre Kopie weiter betrieben werden können. Für dieses Failover sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich.

Bereitstellungsstrategie und Best Practices für ONTAP SnapMirror active sync

Es ist wichtig, dass Ihre Datenschutzstrategie die Workloads, die für die Geschäftskontinuität geschützt werden müssen, klar identifiziert. Der kritischste Schritt in Ihrer Datenschutzstrategie ist es, Klarheit über das Datenlayout Ihrer Unternehmensanwendungen zu haben, damit Sie entscheiden können, wie Sie die Volumes verteilen und die Geschäftskontinuität schützen. Da das Failover auf Konsistenzgruppenebene pro Anwendung erfolgt, sollten die erforderlichen Daten-Volumes der Konsistenzgruppe hinzugefügt werden.

SVM-Konfiguration

Das Diagramm zeigt eine empfohlene Storage VM (SVM) Konfiguration für SnapMirror active sync.



- Für Datavolumes:
  - Zufällige Lesevorgänge sind von sequenziellen Schreibvorgängen isoliert, daher werden die Daten- und Protokolldateien je nach Größe der Datenbank typischerweise auf separaten Volumes abgelegt.
    - Bei großen kritischen Datenbanken befindet sich die einzelne Datendatei auf FlexVol 1 und die zugehörige Protokolldatei auf FlexVol 2.
    - Zur besseren Konsolidierung werden kleine bis mittelgroße, nicht kritische Datenbanken so gruppiert, dass sich alle Datendateien auf FlexVol 1 und die zugehörigen Protokolldateien auf FlexVol 2 befinden. Durch diese Gruppierung geht jedoch die Granularität auf Anwendungsebene verloren.
  - Eine weitere Variante besteht darin, alle Dateien innerhalb desselben FlexVol 3 zu haben, wobei sich die Datendateien in LUN1 und die Protokolldateien in LUN2 befinden.
- Wenn Ihre Umgebung virtualisiert ist, befinden sich alle VMs für verschiedene Unternehmensanwendungen in einem gemeinsamen Datenspeicher. Typischerweise werden die VMs und Anwendungsbinärdateien asynchron mithilfe von SnapMirror repliziert.

Planen

Voraussetzungen für ONTAP SnapMirror active sync

Bei der Planung Ihrer SnapMirror Active Sync-Implementierung ist sicherzustellen, dass

die verschiedenen Hardware-, Software- und Systemkonfigurationsanforderungen erfüllt sind.

Hardware

SAN-Unterstützung

Die folgende Tabelle gibt einen Überblick über die unterstützten NetApp Clusterkonfigurationen.

Clustertyp	Unterstützte Modelle	Unterstützte Funktionen	Maximal unterstützte Cluster-Nodes
AFF	A-Series, C-Series	Automated Failover Duplex (symmetrisch Aktiv/Aktiv), Automated Failover (asymmetrisch Aktiv/Passiv)	• 2 (ONTAP 9.9.1 oder höher) • 4 (ONTAP 9.16.1 mit symmetrischen Aktiv/Aktiv Konfigurationen)
ASA	A-Series, C-Series	Automated Failover Duplex (symmetrisch Aktiv/Aktiv), Automated Failover (asymmetrisch Aktiv/Passiv)	• 2 (ONTAP 9.9.1 oder höher • 4 (ONTAP 9.16.1 mit symmetrischen Aktiv/Aktiv Konfigurationen)
ASA r2	Alle	Automatisiertes Failover Duplex (symmetrisch Aktiv/Aktiv)	• 2 (ONTAP 9.17.1 oder früher) • 4 (ONTAP 9.18.1 oder höher)

NAS-Unterstützung

Die folgende Tabelle gibt einen Überblick über die unterstützten NetApp Clusterkonfigurationen.

Clustertyp	**Unterstützte Modelle**	**Unterstützte Funktionen**	**Maximal unterstützte Cluster-Nodes**
AFF	A-Series, C-Series	Asymmetrisches Aktiv/Passiv (Automatisches Failover)	2 (ONTAP 9.19.1 oder höher)
AFX	Alle	Asymmetrisches Aktiv/Passiv (Automatisches Failover)	4 (ONTAP 9.19.1 oder höher)

Plattformübergreifende Replikation

Die folgende Tabelle gibt einen Überblick über die Replikationsmöglichkeiten zwischen Clustertypen.

Clustertyp 1	Clustertyp 2	Wird Replikation unterstützt?
AFF A-Series	AFF C-Series	Ja
AFF	AFX	Nein
ASA r2 A-Series	ASA r2 C-Series	Ja

AFF	ASA	Nein
ASA	ASA r2	Nein

Software

- ONTAP 9.9.1 oder höher
- ONTAP Mediator 1.2 oder höher
- Ein Linux-Server oder eine virtuelle Maschine für ONTAP Mediator, auf der ein unterstütztes Betriebssystem ausgeführt wird. Weitere Informationen finden Sie in der "ONTAP Mediator Unterstützungsmatrix".

Lizenzierung

Folgende SnapMirror Lizenzen sind im Rahmen der ONTAP One Lizenzsuite verfügbar und müssen auf beiden Clustern angewendet werden:

- SnapMirror synchron
- SnapMirror

> Wenn Ihre ONTAP Speichersysteme vor Juni 2019 erworben wurden, siehe "ONTAP Lizenzschlüssel" für den erforderlichen SnapMirror synchron Lizenzschlüssel.

- Für vSphere Metro Storage Cluster (vMSC) ist eine VMware vSphere-Lizenz erforderlich.

Netzwerkumgebung

- Die Latenzzeit für die Hin- und Rückübertragung (Round Trip Time, RTT) zwischen den Clustern muss weniger als 10 Millisekunden betragen.
- Ab ONTAP 9.14.1 "SCSI-3 persistente Reservierungen" werden SnapMirror active sync unterstützt.

Unterstützte Protokolle

SnapMirror Active Sync unterstützt die folgenden SAN-Protokolle.

- Die FC- und iSCSI-Protokolle werden ab ONTAP 9.9.1 unterstützt.
- Das NVMe-Protokoll wird mit VMware-Workloads ab ONTAP 9.17.1 unterstützt.

  SnapMirror active sync unterstützt mit dem NVMe-Protokoll Folgendes nicht:

  - 4-Knoten symmetrische Aktiv/Aktiv-Konfigurationen
  - Asymmetrische Aktiv/Passiv-Konfigurationen
  - Änderungen der Konsistenzgruppengröße

    Sie können eine Konsistenzgruppe nicht unterbrechungsfrei erweitern oder verkleinern, wenn Sie das NVMe-Protokoll mit SnapMirror Active Sync verwenden. Das Erweitern und Verkleinern einer Konsistenzgruppe ist unterbrechend, wenn das NVMe-Protokoll mit SnapMirror Active Sync verwendet wird.

  - Koexistenz von LUNs und Namensräumen in derselben Konsistenzgruppe.

Ab ONTAP 9.19.1 unterstützt SnapMirror Active Sync die folgenden NAS-Protokolle.

- NFSv3 und später

  Unterbrechungsfreies Failover wird für NFSv3 und höher unterstützt.

- SMB
  - Für SMB 3 CA-Freigaben wird ein unterbrechungsfreies Failover unterstützt.
  - Ein unterbrechender Failover (bei dem jedoch ein RPO von null aufrechterhalten wird) wird für SMB2- und SMB3-Freigaben ohne CA unterstützt.
  - SMB1 wird nicht unterstützt.

NAS-Cluster benötigen dieselbe IP-Adresse und Protokollkonfiguration auf dem primären und sekundären Cluster, um ein unterbrechungsfreies Failover zu ermöglichen. Da SVMs mit derselben IP-Adresse und denselben Protokollen konfiguriert werden können, unterstützt SnapMirror active sync NAS-Konfigurationen auf SVM-Ebene; jedoch bleibt die sekundäre SVM inaktiv (nicht aktiv), da die LIFs bis zum Failover deaktiviert bleiben müssen, um eine IP-Kollision mit der primären SVM zu verhindern.

IPspace

Der Standard-IPspace ist für SnapMirror active sync für Cluster-Peer-Beziehungen erforderlich. Benutzerdefinierte IPspaces werden nicht unterstützt.

Mit SnapMirror active sync für NAS können sich primäre und sekundäre SVMs in unterschiedlichen IPspaces befinden.

NTFS-Sicherheitsstil

NTFS-Sicherheitsstil wird auf SnapMirror active sync Volumes für SAN **nicht** unterstützt. NTFS-Sicherheitsstil wird mit SnapMirror active sync für NAS unterstützt.

ONTAP Mediator

- ONTAP Mediator muss extern bereitgestellt und an ONTAP angebunden werden, um ein transparentes Anwendungs-Failover zu ermöglichen.
- Um voll funktionsfähig zu sein und ein automatisches ungeplantes Failover zu ermöglichen, sollte der externe ONTAP Mediator mit ONTAP Clustern bereitgestellt und konfiguriert werden.
- ONTAP Mediator muss in einer dritten Ausfalldomäne installiert sein, die von den beiden ONTAP Clustern getrennt ist.
- Bei der Installation von ONTAP Mediator sollte das selbstsignierte Zertifikat durch ein gültiges Zertifikat ersetzt werden, das von einer etablierten und zuverlässigen Zertifizierungsstelle signiert wurde.

Weitere Informationen zu ONTAP Mediator sind unter "ONTAP Mediator Dokumentation" verfügbar.

Weitere Voraussetzungen

- In Versionen vor ONTAP 9.15.1 werden SnapMirror Aktiv-Sync-Beziehungen auf Lese/Schreib-Ziel-Volumes (Volumes, die aus DP in einer asymmetrischen Aktiv/Passiv-Konfiguration in Lese/Schreib konvertiert wurden) nicht unterstützt. Bevor ein Lese/Schreib-Volume verwendet werden kann, muss es durch Erstellen einer Volume-basierten SnapMirror Beziehung (entweder asynchron oder synchron) und anschließendes Löschen der Beziehung in ein DP-Volume konvertiert werden. Weitere Details finden sich unter "Eine bestehende SnapMirror-Beziehung in SnapMirror active sync umwandeln".
- Storage-VMs, die SnapMirror active sync verwenden, können nicht als Clientcomputer in Active Directory eingebunden werden.

Weitere Informationen

- "Hardware Universe"
- "ONTAP Mediator Dokumentation"

ONTAP SnapMirror Active Sync Interoperabilität

SnapMirror Active Sync ist mit zahlreichen Betriebssystemen, Anwendungshosts und anderen Funktionen in ONTAP kompatibel.

Weitere Informationen zur Supportfähigkeit von NAS Konfigurationen sind unter "Mit ONTAP SnapMirror Active Sync für NAS schützen" zu finden.

Für spezifische Supportfähigkeit und Interoperabilität Details, die hier nicht behandelt werden, kann das Interoperabilitätsmatrix-Tool ("IMT" konsultiert werden.

Anwendungshosts

SnapMirror active sync unterstützt Hypervisoren wie Hyper-V, ESXi, Betriebssysteme wie Red Hat Enterprise Linux (RHEL), Windows Server und Clustering-Lösungen wie vSphere Metro Storage Cluster (vMSC) sowie ab ONTAP 9.14.1 auch Windows Server Failover Cluster.

Betriebssysteme

SnapMirror Active Sync wird mit zahlreichen Betriebssystemen unterstützt, darunter:

- AIX
  - Ab ONTAP 9.19.1 wird Transparent Application Failover (TAF) mit symmetrischen Aktiv/Aktiv-Konfigurationen unterstützt. Kein PVR ist erforderlich.
  - Ab ONTAP 9.11.1 bis ONTAP 9.18.1 wird AIX nur noch von PVR für automatisches Failover mit symmetrischen Aktiv/Aktiv-Konfigurationen unterstützt.
- HP-UX (ab ONTAP 9.10.1)
- Solaris 11.4 (ab ONTAP 9.10.1)

AIX

Ab ONTAP 9.19.1 wird Transparent Application Failover für AIX mit SnapMirror active sync in symmetrischen Aktiv/Aktiv-Konfigurationen unterstützt. Sie können System Manager oder die ONTAP CLI verwenden, um eine AIX LUN zu erstellen. Um transparentes Failover zu gewährleisten, müssen Sie bei Verwendung der ONTAP CLI die Option access-mode local mit dem Befehl lun create oder lun modify angeben. Standardmäßig ist der Zugriffsmodus auf global eingestellt. Wenn Sie System Manager verwenden, wählen Sie AIX als Host und local als Zugriffsmodus. Weitere Informationen zum Erstellen einer LUN finden Sie unter "SAN-Speicher bereitstellen". Weitere Informationen zur Unterstützung von AIX finden Sie im NetApp Knowledge Base Artikel: "SnapMirror active sync-Unterstützung für AIX: Verhalten je nach ONTAP Release und Migrationshinweise".

Wenn Sie ONTAP 9.11.1 bis ONTAP 9.18.1 verwenden, wird AIX mit SnapMirror active sync über einen standardmäßigen Engineering Feature Policy Variance Request (FPVR) unterstützt, vorausgesetzt, die folgenden Bestimmungen werden verstanden:

- SnapMirror active sync kann einen RPO von null für den Datenschutz bieten, jedoch erfordert der Failover-Prozess mit AIX zusätzliche Schritte, um die Pfadänderung zu erkennen. LUNs, die nicht Teil einer Root-Volume-Gruppe sind, erleben eine I/O-Pause, bis ein `cfgmgr` Befehl ausgeführt wird. Dies kann

automatisiert werden, und die meisten Anwendungen setzen den Betrieb ohne weitere Unterbrechung fort.

- LUNs, die Teil einer Root-Volume-Gruppe sind, sollten generell nicht mit SnapMirror active sync geschützt werden. Es ist nicht möglich, den `cfgmgr` Befehl nach einem Failover auszuführen, was bedeutet, dass ein Neustart erforderlich ist, um die Änderungen in den SAN-Pfaden zu erkennen. Ein RPO-Null-Datenschutz der Root-Volume-Gruppe ist weiterhin möglich, jedoch ist das Failover mit Unterbrechungen verbunden.

Für weitere Informationen zu SnapMirror active sync mit AIX steht Ihnen Ihr NetApp Account-Team zur Verfügung.

HP-UX

Ab ONTAP 9.10.1 wird SnapMirror Active Sync für HP-UX unterstützt.

Automatisches ungeplantes Failover mit HP-UX

Ein automatisches ungeplantes Failover (AUFO) auf dem isolierten primären Cluster kann durch einen doppelten Ereignisausfall verursacht werden, wenn die Verbindung zwischen dem primären und dem sekundären Cluster verloren geht und auch die Verbindung zwischen dem primären Cluster und dem Mediator verloren geht. Dies gilt als seltenes Ereignis, im Gegensatz zu anderen AUFO-Ereignissen.

- In diesem Szenario kann es mehr als 120 Sekunden dauern, bis die E/A auf dem HP-UX Host wieder aufgenommen wird. Abhängig von den ausgeführten Anwendungen kann dies zu keiner E/A-Unterbrechung oder Fehlermeldung führen.
- Zur Behebung des Problems ist ein Neustart der Anwendungen auf dem HP-UX-Host erforderlich, deren Ausfalltoleranz weniger als 120 Sekunden beträgt.

Solaris

Ab ONTAP 9.10.1 unterstützt SnapMirror Aktiv Sync Solaris 11.4.

Um sicherzustellen, dass Solaris-Clientanwendungen bei einem ungeplanten Standort-Switchover in einer SnapMirror Aktiv/Aktiv-Sync-Umgebung unterbrechungsfrei weiterlaufen, sollten die Standardeinstellungen des Solaris-Betriebssystems angepasst werden. Zur Konfiguration von Solaris mit den empfohlenen Einstellungen siehe "NetApp Knowledge Base: Solaris Host-Unterstützung empfohlene Einstellungen in SnapMirror Aktiv/Aktiv-Synchronisierung".

ONTAP Interoperabilität

SnapMirror active sync integriert sich mit Komponenten von ONTAP, um dessen Datensicherungsfunktionen zu erweitern.

Autonomous Ransomware Protection

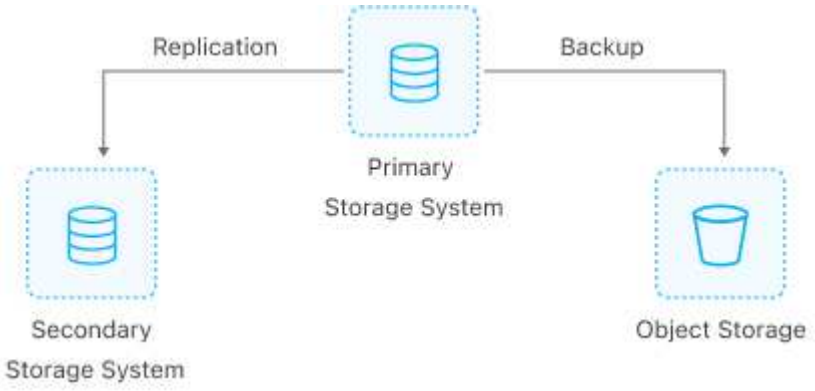
Ab ONTAP 9.19.1 unterstützt ARP/AI primäre Volumes, die an SnapMirror Aktiv Sync SAN-Beziehungen teilnehmen. Weitere Informationen finden Sie unter "Anwendungsfälle und Überlegungen zum autonomen Ransomware-Schutz".

FabricPool

SnapMirror active sync unterstützt Quell- und Ziel-Volumes auf FabricPool Aggregaten mit den Tiering-Richtlinien None, Snapshot oder Auto. SnapMirror active sync unterstützt keine FabricPool Aggregate mit der Tiering-Richtlinie All.

Fan-out Konfigurationen

In Fan-Out Konfigurationen dieser Konfiguration kann Ihr Quellvolume auf einen SnapMirror Aktiv/Aktiv-Zielendpunkt und auf eine SnapMirror asynchrone Beziehung gespiegelt werden.



SnapMirror active sync für SAN unterstützt Fan-Out Konfigurationen mit der `MirrorAllSnapshots` Richtlinie und ab ONTAP 9.11.1 die `MirrorAndVault` Richtlinie. Fan-out-Konfigurationen werden in SnapMirror active sync mit der `XDPDefault` Richtlinie nicht unterstützt.

Ab ONTAP 9.15.1 unterstützt SnapMirror active sync die automatische Neukonfiguration im Fan-Out-Bein nach einem Failover-Ereignis. Wenn das Failover vom primären zum sekundären Standort erfolgreich war, wird die Neukonfiguration der Fan-Out-Beziehung beim nächsten geplanten Update des asynchronen Fan-Out-Beins initiiert. Sie wird nicht unmittelbar nach dem SnapMirror active sync Failover ausgelöst. Das asynchrone Fan-Out-Bein kann eine Konsistenzgruppenbeziehung in einer SAN-Konfiguration oder eine unabhängige Volume-Beziehung sein. Die Neukonfiguration funktioniert in beiden Fällen. Sie wird sowohl durch ein geplantes als auch durch ein ungeplantes Failover ausgelöst. Auch beim Failback zum primären Standort erfolgt eine Neukonfiguration.

Informationen zur Verwaltung Ihrer Fan-Out-Konfiguration in früheren Versionen von ONTAP sind unter Schutzfortsetzung in der Fan-Out-Konfiguration zu finden.

NDMP Wiederherstellung

Ab ONTAP 9.13.1 kann NDMP zum Kopieren und Wiederherstellen von Daten mit SnapMirror Aktiv Sync verwendet werden. Mit NDMP lässt sich die Datenverschiebung auf die SnapMirror Aktiv Sync Quelle durchführen, sodass eine Wiederherstellung abgeschlossen werden kann, ohne den Schutz zu unterbrechen. Dies ist besonders in Fan-out-Konfigurationen hilfreich.

SnapCenter

SnapMirror active sync wird ab SnapCenter "SnapCenter 5.0" unterstützt. SnapCenter ermöglicht die Erstellung von Snapshots, die zum Schutz und zur Wiederherstellung von Anwendungen und virtuellen Maschinen verwendet werden können, wodurch stets verfügbare Speicherlösungen mit Granularität auf Anwendungsebene ermöglicht werden.

SnapRestore

SnapMirror Active Sync unterstützt die teilweise und Einzeldatei SnapRestore.

Einzeldatei SnapRestore

Ab ONTAP 9.11.1 Einzeldatei SnapRestore wird SnapMirror Aktiv-Sync-Volumes unterstützt. Es ist möglich, eine einzelne Datei aus einem Snapshot wiederherzustellen, der von der SnapMirror Aktiv-Sync-Quelle zum

Ziel repliziert wurde. Da Volumes eine oder mehrere LUNs enthalten können, unterstützt diese Funktion eine weniger störende Wiederherstellung, indem eine einzelne LUN granular wiederhergestellt wird, ohne die anderen LUNs zu beeinträchtigen. Einzeldatei SnapRestore bietet zwei Optionen: In-Place und Out-of-Place.

Teildatei SnapRestore

Ab ONTAP 9.12.1 wird "partielle LUN Wiederherstellung" für SnapMirror Aktiv/Sync-Volumes unterstützt. Eine Wiederherstellung von Daten aus anwendungserstellten Snapshots, die zwischen dem SnapMirror Aktiv/Sync-Quellvolume (Volume) und den Ziel- (Snapshot-)Volumes repliziert wurden, ist möglich. Eine partielle LUN- oder Dateiwiederherstellung kann erforderlich sein, wenn eine Datenbank auf einem Host wiederhergestellt werden muss, der mehrere Datenbanken auf derselben LUN speichert. Für die Nutzung dieser Funktionalität sind der Startbyte-Offset der Daten und die Byteanzahl erforderlich.

Manipulationssichere Schnappschüsse

Ab ONTAP 9.20.1 werden in Beziehungen auf SVM-Ebene manipulationssichere Snapshots mit SnapMirror active sync NAS FlexVol Volumes unterstützt. Weitere Informationen zu manipulationssicheren Snapshots sind unter "Einen ONTAP Snapshot zum Schutz vor Ransomware-Angriffen sperren" verfügbar.

Große LUNs und große Volumes

Die Unterstützung für große LUNs und große Volumes (größer als 100 TB) hängt von der verwendeten ONTAP-Version und Ihrer Plattform ab.

ONTAP 9.12.1P2 und höher

- Ab ONTAP 9.12.1 P2 und höher unterstützt SnapMirror Aktiv/Aktiv große LUNs und große Volumes über 100 TB auf ASA und AFF (A-Series und C-Series). Primäre und sekundäre Cluster müssen vom gleichen Typ sein: entweder ASA oder AFF. Die Replikation von AFF A-Series zu AFF C-Series und umgekehrt wird unterstützt.

> Für ONTAP Releases 9.12.1P2 und höher ist sicherzustellen, dass sowohl der primäre als auch der sekundäre Cluster entweder All-Flash SAN Arrays (ASA) oder All Flash Array (AFF) sind und dass auf beiden ONTAP 9.12.1P2 oder höher installiert ist. Wenn auf dem sekundären Cluster eine Version älter als ONTAP 9.12.1P2 ausgeführt wird oder der Array-Typ nicht mit dem des primären Clusters übereinstimmt, kann die synchrone Beziehung aus dem Gleichgewicht geraten, wenn das primäre Volume größer als 100 TB wird.

ONTAP 9.9.1 – 9.12.1P1

- Für ONTAP-Versionen zwischen ONTAP 9.9.1 und 9.12.1 P1 (einschließlich) werden große LUNs und große Volumes über 100 TB nur auf All-Flash SAN Arrays unterstützt. Die Replikation von AFF A-Series zu AFF C-Series und umgekehrt wird unterstützt.

> Für ONTAP-Versionen zwischen ONTAP 9.9.1 und 9.12.1 P2 muss sichergestellt sein, dass sowohl der primäre als auch der sekundäre Cluster All-Flash SAN Arrays sind und auf beiden ONTAP 9.9.1 oder eine neuere Version installiert ist. Wenn auf dem sekundären Cluster eine Version älter als ONTAP 9.9.1 ausgeführt wird oder es sich nicht um ein All-Flash SAN Array handelt, kann die synchrone Beziehung aus dem Gleichgewicht geraten, wenn das primäre Volume größer als 100 TB wird.

Weitere Informationen

- "Konfiguration eines AIX-Hosts für SnapMirror Active Sync"

Anforderungen an Netzwerkports für ONTAP SnapMirror active sync

SnapMirror active sync-Replikation hat mehrere Netzwerkport-Anforderungen.

Beispielsweise muss jeder an der Replikation beteiligte Knoten den Zustand seiner Partnerknoten überwachen, die Replikationsaktivität steuern und die Daten selbst replizieren. Darüber hinaus muss der ONTAP Mediator bzw. ONTAP Cloud Mediator mit allen Knoten kommunizieren, um Quorumdienste bereitzustellen und beim Failover zu unterstützen. Alle diese Funktionen haben unterschiedliche Anforderungen an Endpunkte und Ports.

In den meisten Fällen wird die SnapMirror Active Sync-Replikation in einem internen Netzwerk ohne Port- oder Ziel-beschränkungen betrieben. Wenn der IP-Verkehr durch Firewalls, Router, Netzwerktopologie oder andere Mechanismen eingeschränkt ist, sollten die folgenden Konnektivitätsanforderungen überprüft werden.

Kommunikation zwischen Knoten über Intercluster-/Peer-Verbindungen

Port	Quelle	Richtung	Ziel	Zweck
3260/tcp	Intercluster-LIFs	Beide	Intercluster-LIFs	LUN-Konsens
11104/tcp + 11105/tcp	Intercluster-LIFs	Beide	Intercluster-LIFs	Kommunikation zwischen Clustern SnapMirror Datentransfer
443/tcp (HTTPS)	Intercluster-LIFs	Beide	Intercluster-LIFs	Intercluster-Management
10000/tcp	Cluster-Management-LIFs + Knoten-Management-LIFs	Beide	Optional	Kommunikation mit Active IQ Unified Manager

Kommunikation zwischen Mediator und Clusterknoten

Port	Quelle	Richtung	Ziel	Zweck
22/tcp (SSH)	Management-Host(s)	Eingehend	ONTAP Mediator	ONTAP Mediator-Management
31784/tcp (HTTPS)	Cluster-Management-LIFs	Eingehend	ONTAP Mediator Webserver	REST API
31784/tcp	Node-Management-LIFs	Eingehend	ONTAP Mediator Webserver	Quorum-Dienst

Objektbeschränkungen für ONTAP SnapMirror active sync

Bei der Vorbereitung der Verwendung von SnapMirror Active Sync sind die folgenden Objektbeschränkungen zu beachten.

Konsistenzgruppen in einem Cluster

Die Konsistenzgruppen-Grenzwerte für einen Cluster mit einer SnapMirror Aktiv/Aktiv SAN-Konfiguration werden auf Basis von Beziehungen berechnet und hängen von der verwendeten ONTAP-Version ab. Die

Grenzwerte sind plattformunabhängig.

ONTAP Version	Maximale Anzahl von Beziehungen
ONTAP 9.11.1 und höher	50*
ONTAP 9.10.1	20
ONTAP 9.9.1	5

*Ab ONTAP 9.16.1 unterstützt SnapMirror Active Sync Vier-Knoten-Cluster in symmetrischen Aktiv/Aktiv Konfigurationen. In einem Vier-Knoten-Cluster werden 100 Konsistenzgruppen unterstützt.

Volumes pro Konsistenzgruppe

Die maximale Anzahl von Volumes pro Konsistenzgruppe mit SnapMirror active sync für SAN-Konfigurationen ist plattformunabhängig.

ONTAP Version	Maximale Anzahl von Volumes, die in einer Konsistenzgruppenbeziehung unterstützt werden
ONTAP 9.15.1 und höher	80
ONTAP 9.10.1-9.14.1	16
ONTAP 9.9.1	12

Volumes

Die Volumenbegrenzungen in SnapMirror active sync für SAN-Konfigurationen werden anhand der Anzahl der Endpunkte und nicht der Anzahl der Beziehungen berechnet. Eine Konsistenzgruppe mit 12 Volumes trägt sowohl im primären als auch im sekundären Cluster 12 Endpunkte bei. Sowohl SnapMirror active sync als auch SnapMirror synchron Beziehungen tragen zur Gesamtzahl der Endpunkte bei.

Diese Grenzwerte gelten für AFF und ASA Systeme. Für ASA r2 Systeme (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20) siehe "ASA r2 Dokumentation".

Die maximale Anzahl an Endpunkten pro Plattform ist in der folgenden Tabelle aufgeführt.

Plattform	Endpunkte pro HA für SnapMirror Active Sync				Gesamte Synchronisierungs- und SnapMirror Aktiv-Sync-Endpunkte pro HA			
	ONTAP 9.20.1	ONTAP 9.11.1 und höher	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.20.1	ONTAP 9.11.1 und höher	ONTAP 9.10.1	ONTAP 9.9.1
AFF	600*	400*	200	60	600	400	200	80
ASA	600*	400*	200	60	600	400	200	80

* Ab ONTAP 9.16.1 unterstützt SnapMirror active sync Vier-Knoten-Cluster in symmetrischen Aktiv/Aktiv Konfigurationen. Die Gesamtgrenze für einen Vier-Knoten-Cluster beträgt 800 Endpunkte. Ab ONTAP 9.20.1 beträgt die Gesamtgrenze für einen Vier-Knoten-Cluster 1200 Endpunkte.

SAN Objektbeschränkungen

Die Grenzwerte für SAN-Objekte sind in der folgenden Tabelle aufgeführt. Die Grenzwerte gelten plattformunabhängig.

Objekte in einer SnapMirror Aktivsynchronisierungsbeziehung	Anzahl
LUNs pro Volume	• 256 (ONTAP 9.9.1 - ONTAP 9.15.0) • 512 (ONTAP 9.15.1 und höher)
SCSI-3 Registrierungen persistenter Reservierungen pro LUN	• 182 (ONTAP 9.9.1 – ONTAP 9.19.1) • 256 (ONTAP 9.20.1 und höher)
Anzahl eindeutiger LUNs, Namensräume oder Speichereinheiten pro 2 x 2 SnapMirror Aktiv/Aktiv-Sync-Lösung	4.096
Anzahl eindeutiger LUNs, Namensräume oder Speichereinheiten pro 4 x 4 SnapMirror active sync Lösung (verfügbar ab ONTAP 9.16.1)	6.144
LIFs pro SVM (mit mindestens einem Volumen in einer SnapMirror Aktiv/Aktiv-Synchronisierungsbeziehung)	256
Intercluster LIFs pro Knoten	4
Intercluster-LIFs pro Cluster	8

NAS Objektbeschränkungen

Ab ONTAP 9.19.1 unterstützt SnapMirror Active Sync NAS-Protokolle. Die Grenzwerte für NAS-Objekte sind in der folgenden Tabelle aufgeführt.

Maximale Anzahl an Objekten in einer SnapMirror Aktiv/Aktiv-Synchronisierungsbeziehung	Anzahl
Anzahl der Failover-Einheiten pro HA-Paar	50
Anzahl der NAS SVMs pro HA-Paar	50
Anzahl der Volumina pro SVM	80
Anzahl der Anwendungskonsistenzgruppen pro HA-Paar	Nicht unterstützt
Anzahl der Volumina pro Konsistenzgruppe	Nicht zutreffend
Anzahl der Volumina pro HA Paar	• 400 (ONTAP 9.19.1) • 600 (ONTAP 9.20.1 und höher)
Cluster-Paare, die von einem einzelnen Mediator verwaltet werden können	10
Anzahl der Knoten in einem Cluster	2 (nur AFF Cluster) 4 (nur AFX Cluster)

NVMe Objektbeschränkungen

Ab ONTAP 9.17.1 unterstützt SnapMirror Aktiv Sync das NVMe-Protokoll. NVMe-Objektgrenzen sind in der folgenden Tabelle enthalten.

Maximale Anzahl an Objekten in einer SnapMirror Aktiv/Aktiv-Synchronisierungsbeziehung	Anzahl
Anzahl der Namespace-Zuordnungen pro Knoten	4K
Clustergröße	2 Knoten
Anzahl der Konsistenzgruppen pro HA-Paar	50
Anzahl der Volumes in einer einzelnen NVMe SnapMirror Aktiv Sync Konsistenzgruppe	80
Anzahl der Volumina in einem HA-Paar	400
NVMe Subsysteme pro Konsistenzgruppe	16
Namensraumzuordnungen pro Konsistenzgruppe	256

Verwandte Informationen

- "Hardware Universe"
- "Konsistenzgruppenlimits"

Konfigurieren

ONTAP Cluster für SnapMirror Active Sync konfigurieren

SnapMirror active sync verwendet gekoppelte Cluster, um Ihre Daten im Falle eines Failover-Szenarios zu schützen. Vor der Konfiguration von ONTAP Mediator oder ONTAP Cloud Mediator für SnapMirror active sync muss zunächst sichergestellt werden, dass der Cluster korrekt konfiguriert ist.

Bevor Sie beginnen

Bevor Sie ONTAP Mediator oder ONTAP Cloud Mediator konfigurieren, sollten Sie Folgendes überprüfen:

1. Zwischen den Clustern besteht eine Cluster Peer-Beziehung.

   > Der Standard-IPspace ist für SnapMirror active sync für Cluster-Peer-Beziehungen erforderlich. Ein benutzerdefinierter IPspace wird nicht unterstützt.

   "Erstellung einer Cluster Peer-Beziehung"

2. Die SVMs werden auf jedem Cluster erstellt.

   "Erstellen einer SVM"

3. Eine Peer-Beziehung besteht zwischen den SVMs in jedem Cluster.

   "Erstellen einer SVM Peer-Beziehung"

4. Die Volumes existieren für Ihre LUNs.

"Erstellen eines Volumens"

5. Auf jedem Knoten beider Cluster wird mindestens ein SAN LIF (entweder FC oder iSCSI, je nach Anwendbarkeit) für Ihre SAN-Konfiguration erstellt, oder auf jedem Knoten im primären Cluster wird mindestens ein NAS LIF (entweder NFS oder SMB, je nach Anwendbarkeit) für die Replikation in den sekundären Cluster erstellt.

   "Überlegungen zu LIFs in einer Cluster-SAN-Umgebung"

   "Erstellung eines LIF"

   "Informationen zur NFS Konfiguration"

   "Informationen zur SMB Konfiguration"

6. Nur SAN: Die erforderlichen LUNs werden erstellt und einer Initiatorgruppe zugeordnet, die dazu dient, LUNs dem Initiator auf dem Anwendungshost zuzuordnen.

   "LUNs erstellen und Initiatorgruppen zuordnen"

7. Der Anwendungshost wird erneut gescannt, damit neue LUNs oder Volumes erkannt werden.

Den ONTAP Mediator für SnapMirror Active Sync konfigurieren

SnapMirror active sync verwendet gekoppelte Cluster, um Ihre Daten im Falle eines Failover-Szenarios zu schützen. ONTAP Mediator ist eine zentrale Ressource, die die Geschäftskontinuität ermöglicht, indem sie den Zustand jedes Clusters überwacht. Um SnapMirror active sync zu konfigurieren, muss zunächst ONTAP Mediator installiert und überprüft werden, ob die primären und sekundären Cluster korrekt konfiguriert sind.

Sobald Sie den ONTAP Mediator installiert und Ihre Cluster konfiguriert haben, ONTAP Mediator für SnapMirror Aktiv Sync mit selbstsignierten Zertifikaten initialisieren. Sie müssen dann Konsistenzgruppe für SnapMirror Active Sync erstellen, initialisieren und zuordnen.

ONTAP Mediator

ONTAP Mediator stellt einen persistenten und geschützten Speicher für Hochverfügbarkeits-(HA)-Metadaten bereit, die von den ONTAP Clustern in einer SnapMirror active sync Beziehung verwendet werden. Zusätzlich bietet ONTAP Mediator eine synchrone Funktion zur Abfrage des Knotenzustands zur Unterstützung der Quorumbestimmung und dient als Ping-Proxy zur Erkennung der Controller-Lebendigkeit.

Jede Cluster Peer-Beziehung kann nur einer einzigen ONTAP Mediator Instanz zugeordnet werden. HA Mediator Instanzen werden nicht unterstützt. Wenn ein Cluster in mehreren Peer-Beziehungen mit anderen Clustern steht, stehen die folgenden ONTAP Mediator Optionen zur Verfügung:

- Wenn SnapMirror active sync für jede Beziehung konfiguriert ist, kann jede Cluster Peer-Beziehung über eine eigene ONTAP Mediator Instanz verfügen.
- Der Cluster kann für alle Peer-Beziehungen dieselbe ONTAP Mediator-Instanz verwenden.

Wenn beispielsweise Cluster B eine Peer-Beziehung zu Cluster A, Cluster C und Cluster D hat, kann jede dieser drei Cluster Peer-Beziehungen eine eindeutige zugeordnete ONTAP Mediator Instanz haben, wenn SnapMirror active sync für jede Beziehung konfiguriert ist. Alternativ kann Cluster B für alle drei Peer-Beziehungen dieselbe ONTAP Mediator Instanz verwenden. In diesem Szenario wird dieselbe Instanz von ONTAP Mediator dreimal für den Cluster aufgeführt.

Ab ONTAP 9.19.1 und ONTAP Mediator 1.12 kann dieselbe ONTAP Mediator Instanz verwendet werden, um eine vierknoten MetroCluster IP Konfiguration und eine SnapMirror Aktiv-Sync Cluster Peer-Beziehung gleichzeitig zu überwachen. Die Konfiguration muss die folgenden Anforderungen erfüllen:

- ONTAP Mediator 1.12.1 oder höher ist auf einem Host mit einer 2-Kern-CPU installiert.
- Die ONTAP Mediator Instanz ist mit dem HTTPS-Protokoll konfiguriert.

> Es kann nur eine Vier-Knoten-MetroCluster-IP-Konfiguration und eine SnapMirror Active Sync Peer-Beziehung mit derselben ONTAP Mediator Instanz überwacht werden.

Ab ONTAP 9.17.1 kann "ONTAP Cloud Mediator" zur Überwachung des Zustands Ihres Clusters in einer SnapMirror active sync Konfiguration konfiguriert werden, jedoch können nicht beide Mediatoren gleichzeitig verwendet werden.

> Wenn Sie SnapMirror active sync und ONTAP Mediator oder ONTAP Cloud Mediator mit ONTAP 9.17.1 verwenden, sollten Sie die **Bekannten Probleme und Einschränkungen** in der "ONTAP Versionshinweise" überprüfen, um wichtige Informationen zu diesen Konfigurationen zu erhalten.

Voraussetzungen für ONTAP Mediator

- ONTAP Mediator hat eigene Voraussetzungen. Diese Voraussetzungen müssen vor der Installation von ONTAP Mediator erfüllt sein.

  Weitere Informationen finden Sie unter "Vorbereitung der Installation des ONTAP Mediators".

- Standardmäßig stellt der ONTAP Mediator seine Dienste über TCP-Port 31784 bereit. Es sollte sichergestellt werden, dass Port 31784 zwischen den ONTAP Clustern und dem ONTAP Mediator geöffnet und verfügbar ist.

ONTAP Mediator installieren und die Cluster-Konfiguration bestätigen

Führen Sie die folgenden Schritte aus, um ONTAP Mediator zu installieren und die Cluster-Konfiguration zu überprüfen. Nach jedem Schritt sollte bestätigt werden, dass die jeweilige Konfiguration durchgeführt wurde. Jeder Schritt enthält einen Link zur jeweiligen Vorgehensweise, die befolgt werden muss.

Schritte

1. ONTAP Mediator ist vor der Überprüfung zu installieren, ob Quell- und Ziel-Cluster korrekt konfiguriert sind.

   "Installieren Sie ONTAP Mediator".

2. Bestätigen Sie, dass zwischen den Clustern eine Cluster Peer-Beziehung besteht.

   > Der Standard-IPspace ist für SnapMirror active sync für Cluster-Peer-Beziehungen erforderlich. Ein benutzerdefinierter IPspace wird nicht unterstützt.

   "ONTAP Cluster für SnapMirror Active Sync konfigurieren"

Initialisierung des ONTAP Mediators für SnapMirror active sync unter Verwendung selbstsignierter Zertifikate

Nachdem Sie ONTAP Mediator installiert und Ihre Cluster-Konfiguration bestätigt haben, muss ONTAP Mediator für die Cluster-Überwachung initialisiert werden. ONTAP Mediator kann mit dem System Manager oder der ONTAP CLI initialisiert werden.

System Manager

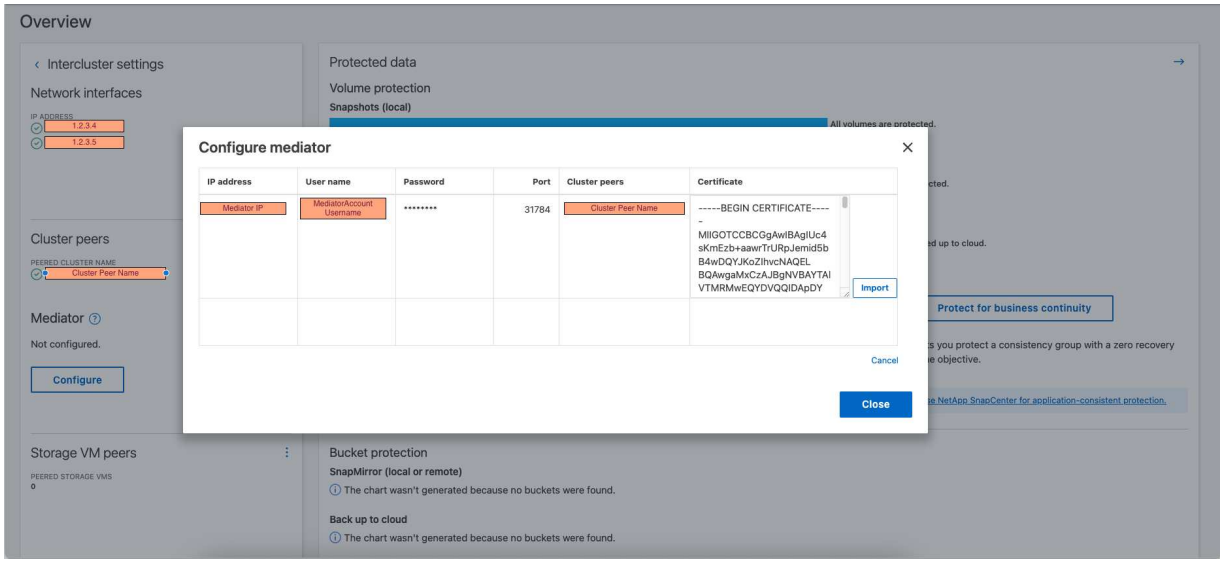
Mit System Manager kann ONTAP Mediator für automatisches Failover konfiguriert werden. Es besteht außerdem die Möglichkeit, das selbstsignierte SSL-Zertifikat und die Zertifizierungsstelle durch das von einem Drittanbieter validierte SSL-Zertifikat und die Zertifizierungsstelle zu ersetzen, sofern dies noch nicht erfolgt ist.

Von ONTAP 9.8 bis ONTAP 9.14.1 wird SnapMirror active sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

ONTAP Mediator 1.9 und höher

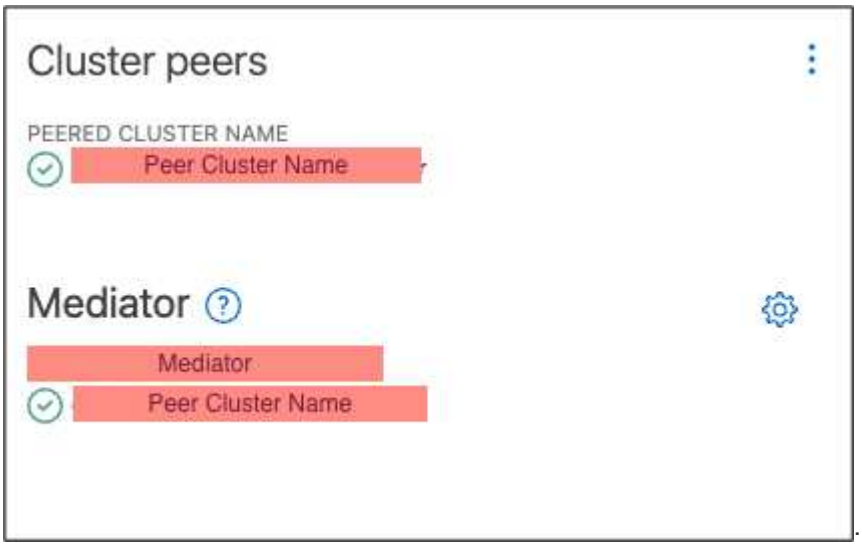
1. Wechseln Sie zu **Schutz > Übersicht > Mediator > Konfigurieren**.
2. **Hinzufügen** auswählen und die folgenden ONTAP Mediator Informationen eingeben:
   - IPv4-Adresse
   - Benutzername
   - Passwort
   - Zertifikat
3. Die Zertifikatseingabe kann auf zwei Arten erfolgen:
   - **Option (a)**: Wählen Sie **Import**, um zur `intermediate.crt` Datei zu navigieren und sie zu importieren.
   - **Option (b)**: Den Inhalt der `intermediate.crt` Datei kopieren und in das Feld **Zertifikat** einfügen.

     Wenn alle Details korrekt eingegeben wurden, wird das bereitgestellte Zertifikat auf allen Peer-Clustern installiert.



Nach Abschluss des Hinzufügens des Zertifikats wird ONTAP Mediator dem ONTAP Cluster hinzugefügt.

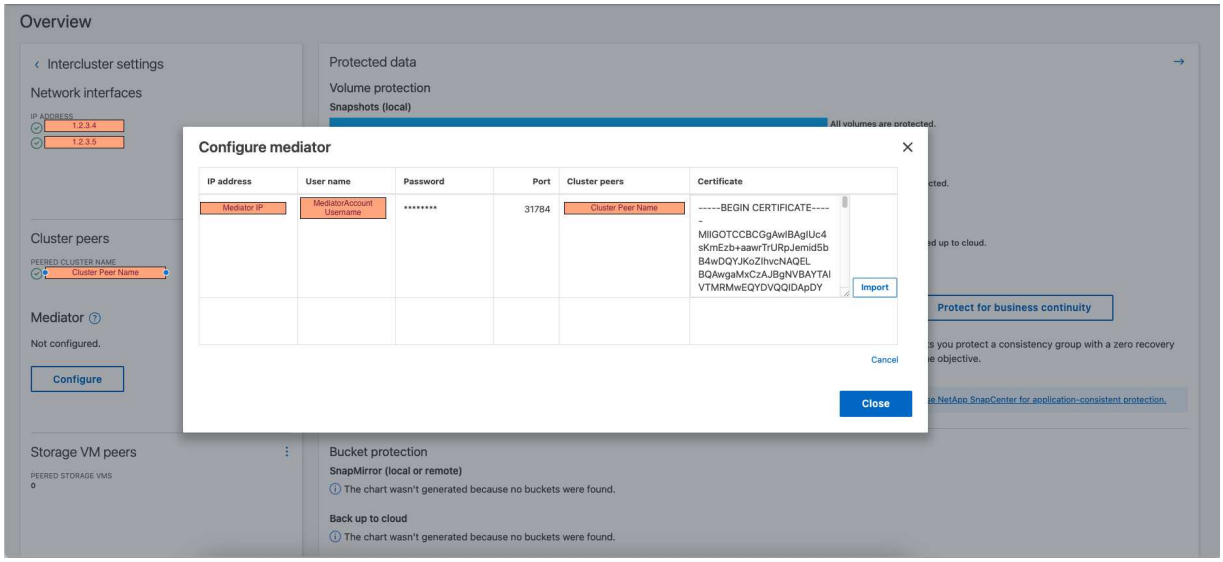
Das folgende Bild zeigt eine erfolgreiche ONTAP Mediator Konfiguration:



ONTAP Mediator 1.8 und früher

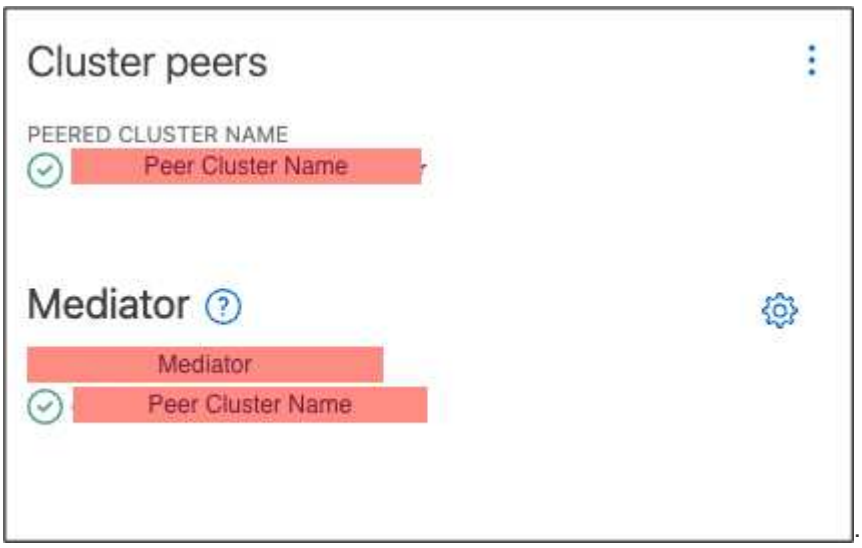
1. Wechseln Sie zu **Schutz > Übersicht > Mediator > Konfigurieren**.
2. **Hinzufügen** auswählen und die folgenden ONTAP Mediator Informationen eingeben:
   - IPv4-Adresse
   - Benutzername
   - Passwort
   - Zertifikat
3. Die Zertifikatseingabe kann auf zwei Arten erfolgen:
   - **Option (a)**: Wählen Sie **Import**, um zur `ca.crt` Datei zu navigieren und sie zu importieren.
   - **Option (b)**: Den Inhalt der `ca.crt` Datei kopieren und in das Feld **Zertifikat** einfügen.

     Wenn alle Details korrekt eingegeben wurden, wird das bereitgestellte Zertifikat auf allen Peer-Clustern installiert.



Nach Abschluss des Hinzufügens des Zertifikats wird ONTAP Mediator dem ONTAP Cluster hinzugefügt.

Das folgende Bild zeigt eine erfolgreiche ONTAP Mediator Konfiguration:



CLI

Sie können ONTAP Mediator entweder vom primären oder vom sekundären Cluster aus mit der ONTAP CLI initialisieren. Wenn der `mediator add` Befehl auf einem Cluster ausgeführt wird, wird ONTAP Mediator automatisch auch auf dem anderen Cluster hinzugefügt.

Wenn Sie ONTAP Mediator zur Überwachung einer SnapMirror active sync-Beziehung verwenden, kann ONTAP Mediator in ONTAP nicht ohne ein gültiges selbstsigniertes Zertifikat oder ein Zertifikat einer Zertifizierungsstelle (CA) initialisiert werden. Sie fügen dem Zertifikatsspeicher für verbundene Cluster ein gültiges Zertifikat hinzu.

ONTAP Mediator 1.9 und höher

1. Suchen Sie die ONTAP Mediator CA-Zertifikate im Installationsverzeichnis der ONTAP Mediator Linux VM/Host-Software:

   ```
   [root@ontap-mediator ~] cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
   ```

   Sie sollten eine Ausgabe sehen, die dem folgenden Beispiel ähnelt:

   ```
   1-ontap-mediator.rules  intermediate.crt   make_self_signed_certs.sh
   ontap_mediator_server_chain.crt  ontap_mediator.user_config.yaml
   root_ca.crt
   config_migration        intermediate.key   netapp_sudoers
   ontap_mediator_server.crt        openssl_ca.cnf
   root_ca.key
   config.pyc              intermediate.srl
   ontap_mediator.config.yaml     ontap_mediator_server.csr
   openssl_intermediate.cnf
   __init__.pyc            logging.conf.yaml
   ontap_mediator.constants.yaml  ontap_mediator_server.key
   ```

```
openssl_server.cnf
```

2. Zeigen Sie den Inhalt des Stammzertifikats der Zertifizierungsstelle an:

```
[root@ontap-mediator ~] cat root_ca.crt
```

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. Zeigen Sie den Inhalt des Zwischenzertifikats der Zertifizierungsstelle an:

```
[root@ontap-mediator ~] cat intermediate.crt
```

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

4. Installieren Sie die Root- und Zwischenzertifizierungsstellenzertifikate auf dem primären oder sekundären Cluster:

   a. Installieren Sie das Root-CA-Zertifikat:

      ```
      security certificate install -type server-ca -vserver <vserver_name>
      ```

      Geben Sie die `root.crt` ein, wenn Sie dazu aufgefordert werden, wie im folgenden Beispiel gezeigt:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Enter certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: <serial_value>

The certificate's generated name for reference: ONTAPMediatorCA
```

```
C1_test_cluster::*>
```

5. Installieren Sie das Zwischenzertifikat der Zertifizierungsstelle:

   `security certificate install -type server-ca -vserver <vserver_name>`

   Geben Sie die `intermediate.crt` ein, wenn Sie dazu aufgefordert werden, wie im folgenden Beispiel gezeigt:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Enter certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: <serial_value>

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Wiederholen Sie den vorherigen Schritt, um die Root- und Zwischenzertifikate der Zertifizierungsstelle auf dem verbundenen Cluster zu installieren.
7. Zeigen Sie die installierten selbstsignierten CA-Zertifikate mit dem generierten Namen des Zertifikats an:

   `security certificate show -common-name <common_name>`

   Beispiel:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver         Serial Number   Certificate Name
Type
----------      ---------------
------------------------------------ ------------
C1_test_cluster <serial_number> ONTAPMediatorCA
```

```
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Nov 28 05:26:07 2030

C1_test_cluster <serial_number> ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Nov 28 05:26:07 2030

2 entries were displayed.
```

8. ONTAP Mediator wird auf einem der Cluster initialisiert. ONTAP Mediator wird für das andere Cluster automatisch hinzugefügt.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

9. Optional kann der Job-ID-Status `job show -id` überprüft werden, um festzustellen, ob der Befehl SnapMirror Mediator hinzufügen erfolgreich war.

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued
```

```
C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

10. Status der ONTAP Mediator Konfiguration prüfen:

    `snapmirror mediator show`

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

    `Quorum Status` gibt an, ob die SnapMirror Konsistenzgruppenbeziehungen mit ONTAP Mediator synchronisiert sind; ein Status von `true` zeigt eine erfolgreiche Synchronisierung an.

ONTAP Mediator 1.8 und früher

1. Das ONTAP Mediator CA-Zertifikat befindet sich am Installationsort der ONTAP Mediator Linux VM/Host-Software `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Dem Zertifikatsspeicher des verbundenen Clusters wird eine gültige Zertifizierungsstelle hinzugefügt.

   Beispiel:

```
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. Fügen Sie das ONTAP Mediator CA-Zertifikat zu einem ONTAP Cluster hinzu. Wenn Sie dazu aufgefordert werden, das vom ONTAP Mediator erhaltene CA-Zertifikat einfügen. Die Schritte sind auf allen Peer-Clustern zu wiederholen.

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   Beispiel:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

   ```
   C1_test_cluster::*> security certificate install -type server-ca
   -vserver C1_test_cluster

   Please enter Certificate: Press when done
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----

   You should keep a copy of the CA-signed digital certificate for
   future reference.

   The installed certificate's CA and serial number for reference:
   CA: ONTAP Mediator CA
   serial: D86D8E4E87142XXX

   The certificate's generated name for reference: ONTAPMediatorCA

   C1_test_cluster::*>
   ```

4. Das selbstsignierte CA-Zertifikat, das mit dem generierten Namen des Zertifikats installiert wurde, kann angezeigt werden:

   ```
   security certificate show -common-name <common_name>
   ```

Beispiel:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. ONTAP Mediator wird auf einem der Cluster initialisiert. ONTAP Mediator wird für das andere Cluster automatisch hinzugefügt.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Optional kann der Job-ID-Status `job show -id` überprüft werden, um festzustellen, ob der Befehl SnapMirror Mediator hinzufügen erfolgreich war.

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.
```

```
Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------- ----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------- ----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. Status der ONTAP Mediator Konfiguration prüfen:

   `snapmirror mediator show`

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

   `Quorum Status` gibt an, ob die SnapMirror Konsistenzgruppenbeziehungen mit ONTAP Mediator synchronisiert sind; ein Status von `true` zeigt eine erfolgreiche Synchronisierung an.

ONTAP Mediator mit Zertifikaten von Drittanbietern neu initialisieren

Möglicherweise muss ONTAP Mediator neu initialisiert werden. Es kann Situationen geben, die eine erneute Initialisierung von ONTAP Mediator erfordern, wie zum Beispiel eine Änderung der ONTAP Mediator-IP-Adresse, ein Zertifikatsablauf und Ähnliches.

Das folgende Verfahren veranschaulicht die Reinitialisierung des ONTAP Mediator für einen konkreten Fall, in dem ein selbstsigniertes Zertifikat durch ein Zertifikat eines Drittanbieters ersetzt werden muss.

Über diese Aufgabe

Es ist erforderlich, die selbstsignierten Zertifikate des SnapMirror Active Sync Clusters durch Zertifikate von Drittanbietern zu ersetzen, die ONTAP Mediator Konfiguration aus ONTAP zu entfernen und anschließend ONTAP Mediator hinzuzufügen.

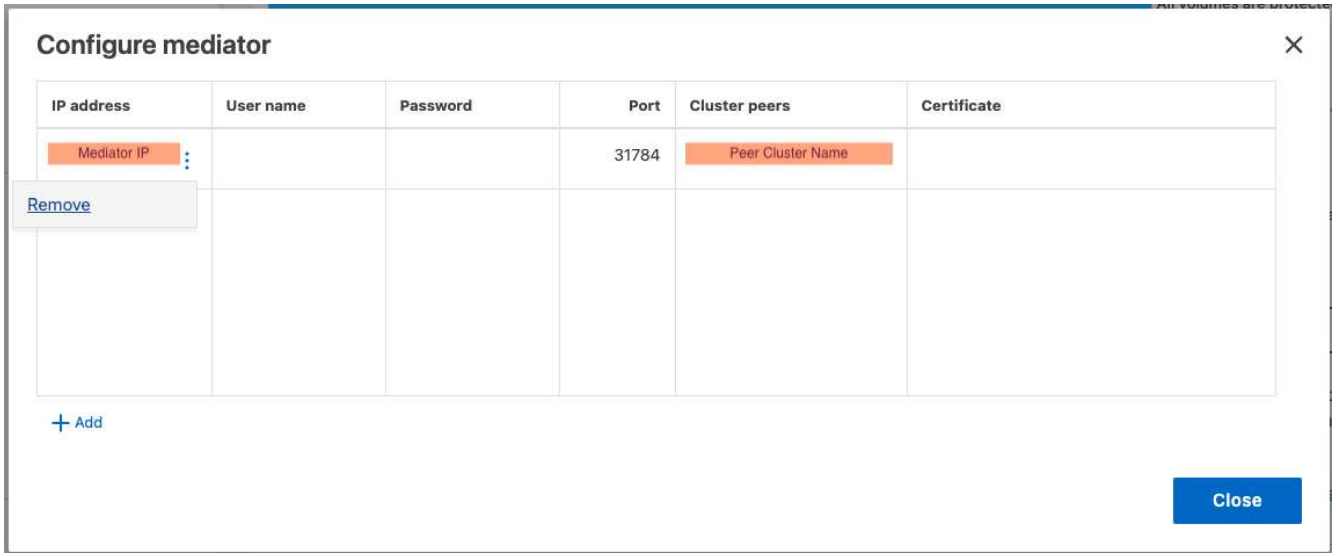
System Manager

Mit System Manager ist die mit dem alten selbstsignierten Zertifikat konfigurierte ONTAP Mediator-Version aus dem ONTAP Cluster zu entfernen und der ONTAP Cluster mit dem neuen Drittanbieterzertifikat neu zu konfigurieren.

Schritte

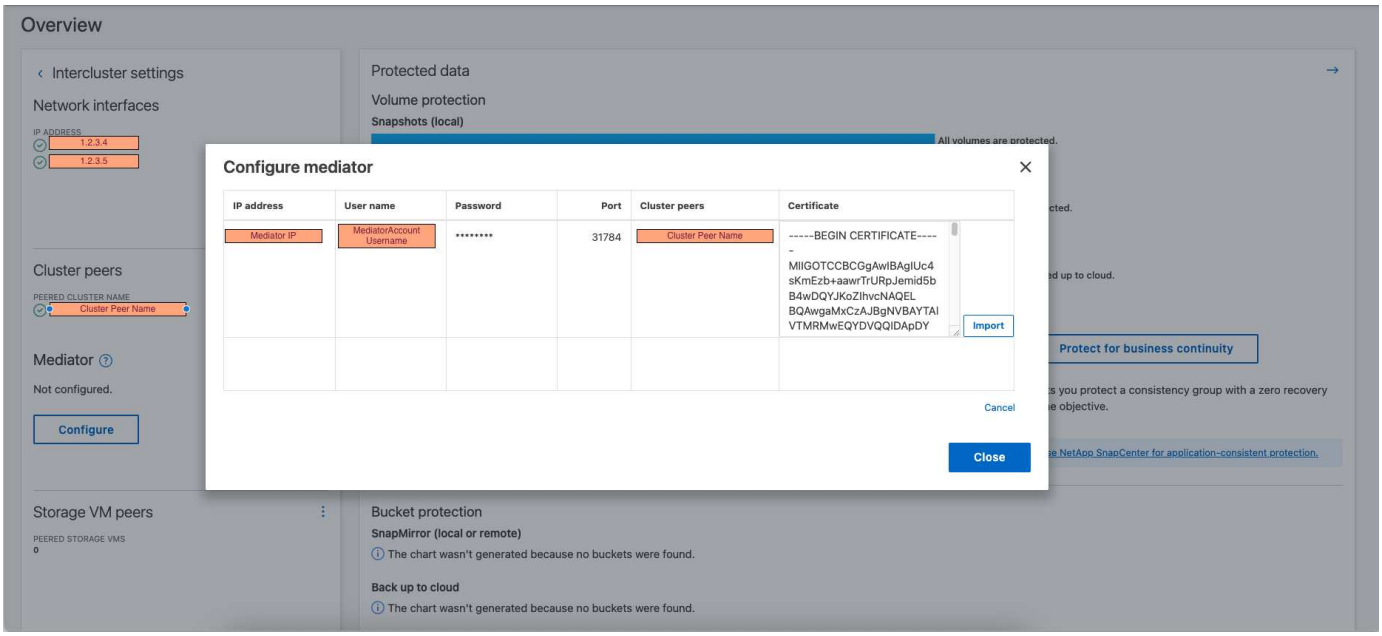
1. Das Menüsymbol auswählen und **Entfernen** wählen, um ONTAP Mediator zu entfernen.

> Dieser Schritt entfernt das selbstsignierte Server-CA-Zertifikat nicht aus dem ONTAP Cluster. NetApp empfiehlt, zum Tab **Zertifikat** zu navigieren und es manuell zu entfernen, bevor der nächste Schritt zum Hinzufügen eines Drittanbieterzertifikats durchgeführt wird:



2. ONTAP Mediator erneut mit dem korrekten Zertifikat hinzufügen.

ONTAP Mediator ist jetzt mit dem neuen selbstsignierten Zertifikat eines Drittanbieters konfiguriert.



CLI

ONTAP Mediator kann entweder vom primären oder vom sekundären Cluster aus mithilfe der ONTAP CLI neu initialisiert werden, um das selbstsignierte Zertifikat durch das Zertifikat eines Drittanbieters zu ersetzen.

ONTAP Mediator 1.9 und höher

1. Entfernen Sie das zuvor installierte selbstsignierte `intermediate.crt` Zertifikat, das verwendet wurde, als für alle Cluster selbstsignierte Zertifikate genutzt wurden. Im folgenden Beispiel gibt es zwei Cluster:

   Beispiel:

   ```
    C1_test_cluster::*> security certificate delete -vserver
   C1_test_cluster -common-name ONTAPMediatorCA
    2 entries were deleted.

    C2_test_cluster::*> security certificate delete -vserver
   C2_test_cluster -common-name ONTAPMediatorCA *
    2 entries were deleted.
   ```

2. Den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror active sync Cluster mit `-force true` entfernen:

   Beispiel:

   ```
   C1_test_cluster::*> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   1.2.3.4          C2_test_cluster   connected         true
   ```

```
C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Die in "Selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen" beschriebenen Schritte enthalten Anweisungen zum Erhalt von Zertifikaten von einer untergeordneten CA, bezeichnet als `intermediate.crt`. Selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen

   Das `intermediate.crt` verfügt über bestimmte Eigenschaften, die aus der Anfrage abgeleitet werden und an die PKI-Behörde gesendet werden müssen, wie in der Datei `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf` definiert.

4. Fügen Sie das neue Drittanbieter ONTAP Mediator CA-Zertifikat `intermediate.crt` aus dem Installationsverzeichnis der ONTAP Mediator Linux VM/Host-Software hinzu:

   Beispiel:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Die `intermediate.crt` Datei zum Peered-Cluster hinzufügen. Dieser Schritt ist für alle Peer-Cluster zu wiederholen:

   Beispiel:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster
```

```
Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror active sync Cluster entfernen:

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator erneut hinzufügen:

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:
```

```
Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

`Quorum Status`gibt an, ob die SnapMirror Konsistenzgruppen-Beziehungen mit dem Mediator synchronisiert sind; ein Status von `true`zeigt eine erfolgreiche Synchronisierung an.

ONTAP Mediator 1.8 und früher

1. Entfernen Sie das zuvor installierte selbstsignierte `ca.crt` Zertifikat, das verwendet wurde, als für alle Cluster selbstsignierte Zertifikate genutzt wurden. Im folgenden Beispiel gibt es zwei Cluster:

   Beispiel:

   ```
    C1_test_cluster::*> security certificate delete -vserver
   C1_test_cluster -common-name ONTAPMediatorCA
    2 entries were deleted.

    C2_test_cluster::*> security certificate delete -vserver
   C2_test_cluster -common-name ONTAPMediatorCA *
    2 entries were deleted.
   ```

2. Den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror active sync Cluster mit `-force true` entfernen:

   Beispiel:

   ```
   C1_test_cluster::*> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   1.2.3.4          C2_test_cluster   connected         true

   C1_test_cluster::*> snapmirror mediator remove -mediator-address
   1.2.3.4 -peer-cluster C2_test_cluster -force true

   Warning: You are trying to remove the ONTAP Mediator configuration
   with force. If this configuration exists on the peer cluster, it
   could lead to failure of a SnapMirror failover operation. Check if
   this configuration
            exists on the peer cluster C2_test_cluster and remove it as
   well.
   Do you want to continue? {y|n}: y

   Info: [Job 136] 'mediator remove' job queued
   ```

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Die in "Selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen" beschriebenen Schritte enthalten Anweisungen zum Erhalt von Zertifikaten von einer untergeordneten CA, bezeichnet als `ca.crt`. Selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen

   Das `ca.crt` verfügt über bestimmte Eigenschaften, die aus der Anfrage abgeleitet werden und an die PKI-Behörde gesendet werden müssen, wie in der Datei `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf` definiert.

4. Fügen Sie das neue Drittanbieter ONTAP Mediator CA-Zertifikat `ca.crt` aus dem Installationsverzeichnis der ONTAP Mediator Linux VM/Host-Software hinzu:

   Beispiel:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Die `intermediate.crt` Datei zum Peered-Cluster hinzufügen. Dieser Schritt ist für alle Peer-Cluster zu wiederholen:

   Beispiel:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX
```

```
The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror active sync Cluster entfernen:

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. ONTAP Mediator erneut hinzufügen:

   Beispiel:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status`gibt an, ob die SnapMirror Konsistenzgruppen-Beziehungen mit dem Mediator synchronisiert sind; ein Status von `true`zeigt eine erfolgreiche Synchronisierung an.

Verwandte Informationen

- "ONTAP Mediator Dokumentation"

- "Job anzeigen"
- "Sicherheitszertifikat löschen"
- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "snapmirror mediator add"
- "SnapMirror Mediator entfernen"
- "snapmirror mediator show"

Anforderungen für die Konfiguration des ONTAP Cloud Mediators

Bevor Sie "ONTAP Cloud Mediator konfigurieren" beginnen, muss sichergestellt sein, dass die Voraussetzungen erfüllt sind.

Firewall-Anforderungen

Die Firewall-Einstellungen auf dem Domänencontroller müssen HTTPS-Datenverkehr `api.bluexp.netapp.com` von beiden Clustern zulassen.

Anforderungen an den Proxyserver

Wenn Sie Proxyserver für SnapMirror Active Sync verwenden, ist sicherzustellen, dass die Proxyserver erstellt wurden und folgende Proxyserver-Informationen vorliegen:

- HTTPS Proxy-IP
- Port
- Benutzername
- Passwort

Latenz

Die empfohlene Ping-Latenz zwischen dem NetApp Console Cloud-Server und SnapMirror Aktiv/Synchron-Cluster-Peers beträgt weniger als 200 ms.

Root CA-Zertifikate

Der Cluster wird auf Zertifikate überprüft.

ONTAP wird mit vorinstallierten, bekannten Stammzertifizierungsstellenzertifikaten ausgeliefert, sodass in den meisten Fällen das Stammzertifizierungsstellenzertifikat des NetApp Console Servers nicht installiert werden muss. Vor Beginn der ONTAP Cloud Mediator Konfiguration kann der Cluster überprüft werden, um zu verifizieren, dass die Zertifikate vorhanden sind.

Beispiel:

```
C1_cluster% openssl s_client -showcerts -connect api.bluexp.netapp.com:443
-servername api.bluexp.netapp.com | egrep "s:|i:"

depth=4 C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited,
CN=AAA Certificate Services
```

```
verify error:num=19:self-signed certificate in certificate chain
verify return:1
depth=4 C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited,
CN=AAA Certificate Services
verify return:1
depth=3 C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network,
CN=USERTrust RSA Certification Authority
verify return:1
depth=2 C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication
Root R46
verify return:1
depth=1 C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication
CA OV R36
verify return:1
depth=0 C=US, ST=California, O=NetApp, Inc., CN=cloud.netapp.com
verify return:1
 0 s:C=US, ST=California, O=NetApp, Inc., CN=cloud.netapp.com
   i:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA
OV R36
 1 s:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA
OV R36
   i:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root
R46
 2 s:C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication Root
R46
   i:C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network,
CN=USERTrust RSA Certification Authority
 3 s:C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network,
CN=USERTrust RSA Certification Authority
   i:C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA
Certificate Services
 4 s:C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA
Certificate Services
   i:C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA
Certificate Services

C1_cluster::> security certificate show -common-name
Sectigo*|USERTrust*|AAA*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
C1_sti245-vsim-ocvs024k_1775534714 42F2CCDA1B6937445F15FE752810B8F4
SectigoPublicServerAuthenticationRootE46 server-ca
    Certificate Authority: Sectigo Public Server Authentication Root E46
          Expiration Date: Wed Mar 21 19:59:59 2046
```

```
C1_sti245-vsim-ocvs024k_1775534714 758DFD8BAE7C0700FAA925A7E1C7AD14
SectigoPublicServerAuthenticationRootR46 server-ca
    Certificate Authority: Sectigo Public Server Authentication Root R46
          Expiration Date: Wed Mar 21 19:59:59 2046

C1_sti245-vsim-ocvs024k_1775534714 5C8B99C55A94C5D27156DECD8980CC26
USERTrustECCCertificationAuthority server-ca
    Certificate Authority: USERTrust ECC Certification Authority
          Expiration Date: Mon Jan 18 18:59:59 2038

C1_sti245-vsim-ocvs024k_1775534714 01FD6D30FCA3CA51A81BBC640E35032D
USERTrustRSACertificationAuthority server-ca
    Certificate Authority: USERTrust RSA Certification Authority
          Expiration Date: Mon Jan 18 18:59:59 2038
```

Proxyserver auf installierte Zertifikate prüfen

Wenn Sie einen Proxy verwenden, um eine Verbindung zum ONTAP Cloud Mediator Service in der NetApp Console herzustellen, ist sicherzustellen, dass die Root-CA-Zertifikate des Proxyservers in ONTAP installiert sind:

Beispiel:

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 -servername api.bluexp.netapp.com |egrep "s:|i:"
```

Das CA-Zertifikat herunterladen:

Bei Bedarf können die Root-CA-Zertifikate von der Website der Zertifizierungsstelle heruntergeladen und auf den Clustern installiert werden.

Beispiel:

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

Der ONTAP Cloud Mediator für SnapMirror Aktiv-Sync wird konfiguriert

Ab ONTAP 9.17.1 kann mit ONTAP Cloud Mediator die Geschäftskontinuität gewährleistet werden, indem der Zustand jedes Clusters überwacht wird. ONTAP Cloud Mediator ist ein Cloud-basierter Dienst. Bei der Verwendung von ONTAP Cloud Mediator mit SnapMirror active sync ist zunächst zu bestätigen, dass die NetApp Console-Dienste und Clientinformationen konfiguriert sind und ein korrektes Cluster-Peering besteht.

Wie beim ONTAP Mediator bietet auch ONTAP Cloud Mediator einen persistenten und geschützten Speicher für Hochverfügbarkeits-(HA)-Metadaten, die von den ONTAP Clustern in einer SnapMirror Aktiv/Aktiv-Synchronisierungsbeziehung verwendet werden. ONTAP Cloud Mediator bietet eine synchrone Funktion zur Abfrage des Knotenzustands zur Unterstützung der Quorumbestimmung und dient als Ping-Proxyserver zur Erkennung der Controller-Lebendigkeit.

> Wenn Sie SnapMirror active sync und ONTAP Mediator oder ONTAP Cloud Mediator mit ONTAP 9.17.1 verwenden, sollten Sie die **Bekannten Probleme und Einschränkungen** in der "ONTAP Versionshinweise" überprüfen, um wichtige Informationen zu diesen Konfigurationen zu erhalten.

Bevor Sie beginnen

Bevor Sie ONTAP Cloud Mediator konfigurieren, sollten die folgenden Informationen bestätigt werden:

- Der Cluster ist konfiguriert.

  "ONTAP Cluster für SnapMirror Active Sync konfigurieren"

- Sie haben Ihre NetApp Console-Organisations-ID aus der NetApp Console kopiert und ein Console-Mitgliedsservicekonto erstellt, das bei der Konfiguration von ONTAP Cloud Mediator verwendet wird. Beim Erstellen des Servicekontos muss die Organisation auf das Abonnement festgelegt werden, in dem der ONTAP Cloud Mediator konfiguriert wurde. Die Kategorie muss auf **Application** und der Rollentyp auf **ONTAP Mediator Setup Role** gesetzt werden. Die Client-ID und das Client Secret müssen beim Erstellen der Rolle gespeichert werden.

  "Mitglieder der NetApp Console und Servicekonten hinzufügen"

Schritte

ONTAP Cloud Mediator kann über den System Manager oder die ONTAP CLI hinzugefügt werden.

System Manager

1. Zu **Schutz > Übersicht > Mediator** navigieren und **Hinzufügen** auswählen.
2. Im Fenster **Mediator hinzufügen** ist als Mediatortyp **Cloud** auszuwählen und die folgenden Informationen sind einzugeben:
   - NetApp Console Organisations-ID
   - NetApp Console Client-ID
   - NetApp Console-Client-Geheimnis
3. Den Cluster-Peer auswählen.
4. Falls ein HTTP-Proxy verwendet wird und dieser noch nicht konfiguriert ist, sind die HTTP-Proxy-Informationen für den lokalen und den Remote-Host einzugeben.

   Es wird empfohlen, für jeden Cluster-Peer einen anderen Proxyserver zu verwenden.

5. Optional: Falls ein Root-CA-Zertifikat in ONTAP installiert werden muss, insbesondere bei Verwendung eines Proxyserver, das Zertifikat in das dafür vorgesehene Textfeld einfügen.
6. Wählen Sie **Add**.
7. Navigieren Sie zu **Schutz > Übersicht** und prüfen Sie den Status der Beziehung zwischen den SnapMirror Aktiv/Aktiv-Clustern und ONTAP Cloud Mediator.

CLI

1. ONTAP Cloud Mediator konfigurieren:
   ```
   snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp
   -org-id <NetApp Console Organization ID> -service-account-client-id
   <Service Account Client ID> -use-http-proxy-local <true|false> -use-http
   -proxy-remote <true|false>
   ```
2. ONTAP Cloud Mediator Status prüfen:
   ```
   snapmirror mediator show
   ```

   Beispiel:

   ```
   C1_cluster::> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   Type
   ---------------- ---------------- ----------------- -------------
   -------
   0.0.0.0          C2_cluster       connected         true
   cloud
   ```

Mit ONTAP SnapMirror Active Sync für SAN schützen

SnapMirror active sync bietet asymmetrischen Schutz und ab ONTAP 9.15.1 auch symmetrischen Aktiv/Aktiv-Schutz.

Asymmetrischen Schutz konfigurieren

Die Konfiguration des asymmetrischen Schutzes für SAN-Konfigurationen mit SnapMirror active sync umfasst die Auswahl von LUNs im ONTAP Quell-Cluster und deren Hinzufügen zu einer Konsistenzgruppe.

Bevor Sie beginnen

- Sie benötigen eine SnapMirror Synchronous-Lizenz.
- Sie müssen Administrator eines Clusters oder einer Storage-VM sein.
- Alle Bestandteile einer Konsistenzgruppe müssen sich in einer einzigen Storage VM (SVM) befinden.
  - LUNs können auf verschiedenen Volumes liegen.
- Quell- und Ziel-Cluster dürfen nicht identisch sein.
- Es kann keine SnapMirror Aktiv-Sync-Konsistenzgruppenbeziehung zwischen ASA Clustern und Nicht-ASA-Clustern hergestellt werden.
- Der Standard-IPspace ist für SnapMirror active sync für Cluster-Peer-Beziehungen erforderlich. Benutzerdefinierte IPspaces werden nicht unterstützt.
- Der Name der Konsistenzgruppe muss eindeutig sein.
- Die Volumes auf dem sekundären (Ziel-Cluster) müssen vom Typ DP sein.
- Die primäre und die sekundäre SVM müssen in einer Peering-Beziehung stehen.
- Der Quell- und Ziel-Cluster dürfen nicht Teil einer MetroCluster Konfiguration sein.

Schritte

Eine Konsistenzgruppe lässt sich mithilfe der ONTAP CLI oder des System Manager konfigurieren.

Ab ONTAP 9.10.1 bietet ONTAP im System Manager einen Endpunkt und ein Menü für Konsistenzgruppen mit zusätzlichen Verwaltungsfunktionen. Wenn ONTAP 9.10.1 oder höher verwendet wird, siehe "Eine Konsistenzgruppe konfigurieren" dann "Schutz konfigurieren" zur Erstellung einer SnapMirror Aktiv Sync-Beziehung.

Von ONTAP 9.8 bis ONTAP 9.14.1 wird SnapMirror active sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

System Manager

1. Im primären Cluster zu **Schutz > Übersicht > Schutz für Geschäftskontinuität > LUNs schützen** navigieren.
2. Wählen Sie die LUNs aus, die Sie schützen möchten, und fügen Sie sie einer Schutzgruppe hinzu.
3. Den Ziel-Cluster und die SVM auswählen.
4. **Beziehung initialisieren** ist standardmäßig ausgewählt. Mit **Speichern** beginnt der Schutz.
5. **Dashboard > Leistung** zeigt die IOPS-Aktivität für die LUNs an.
6. Auf dem Ziel-Cluster kann im System Manager überprüft werden, ob die Beziehung für den Schutz der Geschäftskontinuität synchron ist: **Schutz > Beziehungen**.

CLI

1. Eine Konsistenzgruppenbeziehung vom Ziel-Cluster aus erstellen.
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   Sie können bis zu 12 Teil-Volumes mit dem `cg-item-mappings`-Parameter im `snapmirror create`-Befehl zuordnen.

   Das folgende Beispiel erstellt zwei Konsistenzgruppen: `cg_src_ on the source with `vol1` und `vol2` und eine gespiegelte Ziel-Konsistenzgruppe, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOverDuplex
   ```

2. Vom Ziel-Cluster aus die Konsistenzgruppe initialisieren.

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. Bestätigen Sie, dass die Initialisierung erfolgreich abgeschlossen wurde. Der Status sollte `InSync` sein.

   ```
   snapmirror show
   ```

4. Auf jedem Cluster eine Initiatorgruppe erstellen, damit LUNs dem Initiator auf dem Anwendungshost zugeordnet werden können.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator`

initiator_name

Weitere Informationen zu `lun igroup create` finden sich in der "ONTAP-Befehlsreferenz".

5. Auf jedem Cluster die LUNs der Initiatorgruppe zuordnen:

   `lun map -path path_name -igroup igroup_name`

6. Die erfolgreiche Ausführung der LUN-Zuordnung lässt sich mit dem `lun map` Befehl überprüfen. Anschließend ist es möglich, die neuen LUNs auf dem Anwendungshost zu erkennen.

Symmetrischer Aktiv/Aktiv-Schutz konfigurieren

Sie können einen symmetrischen Schutz für SAN-Konfigurationen mithilfe des System Manager oder der ONTAP CLI einrichten. In beiden Schnittstellen sind unterschiedliche Schritte für einheitliche und nicht einheitliche Konfigurationen erforderlich.

Bevor Sie beginnen

- Beide Cluster müssen ONTAP 9.15.1 oder höher ausführen.
- Symmetrische Aktiv/Aktiv Konfigurationen erfordern die `AutomatedFailoverDuplex` Datensicherungsstrategie. Alternativ ist es möglich, eine benutzerdefinierte SnapMirror Richtlinie erstellen sofern die `-type automated-failover-duplex` erfüllt ist.
- In ONTAP 9.15.1 wird symmetrisches Aktiv/Aktiv nur auf Zwei-Node-Clustern unterstützt.
- Ab ONTAP 9.16.1 GA unterstützt SnapMirror Active Sync symmetrische Aktiv/Aktiv-Konfigurationen auf Vier-Node-Clustern.
  - Um SnapMirror active sync auf einem Vier-Node-Cluster zu verwenden, muss ONTAP 9.16.1 GA oder neuer ausgeführt werden.
  - Vor der Bereitstellung einer Vier-Node-Konfiguration ist Folgendes zu beachten eine Cluster Peer-Beziehung erstellen.
  - Die Informationen Grenzen für Vier-Node-Cluster werden angezeigt.
  - Wenn Sie zu einem Zwei-Node-Cluster zurückkehren, müssen Sie die SnapMirror Active Sync-Beziehungen aus dem Cluster entfernen, bevor Sie zurückkehren.
  - Die Vier-Node-Konfiguration kann verwendet werden, um Speicher und Controller zu aktualisieren. Dieser Vorgang ist unterbrechungsfrei und erweitert den Cluster, während Volumes in die neuen Nodes verschoben werden. Weitere Informationen finden sich unter "einen Cluster aktualisieren".
- Ab ONTAP 9.17.1 kann der symmetrische Aktiv/Aktiv-Schutz auf NVMe-Namespaces nur konfiguriert werden, wenn beide Cluster ONTAP 9.17.1 oder höher ausführen.

Symmetrischer Aktiv/Aktiv-Schutz mit einer SCSI SnapMirror active sync Konfiguration

Schritte

Mit dem System Manager oder der ONTAP CLI lässt sich ein symmetrischer Aktiv/Aktiv-Schutz mithilfe von SCSI-Protokoll-Hostzuordnungen konfigurieren.

System Manager

Schritte für eine einheitliche Konfiguration

1. Auf der Hauptseite, "Erstellen einer Konsistenzgruppe unter Verwendung neuer LUNs".

a. Beim Erstellen der Konsistenzgruppe Host-Initiatoren angeben, um Initiatorgruppen zu erstellen.

b. Das Kontrollkästchen zum **Aktivieren von SnapMirror** auswählen und anschließend die `AutomatedFailoverDuplex` Richtlinie wählen.

c. Im daraufhin angezeigten Dialogfeld das Kontrollkästchen **Initiatorgruppen replizieren** aktivieren, um Initiatorgruppen zu replizieren. In **Proximity-Einstellungen bearbeiten** proximale SVMs für die Hosts festlegen.

d. **Speichern** auswählen.

Schritte für eine nicht einheitliche Konfiguration

1. Auf der Hauptseite, "Erstellen einer Konsistenzgruppe unter Verwendung neuer LUNs".
   a. Beim Erstellen der Konsistenzgruppe Host-Initiatoren angeben, um Initiatorgruppen zu erstellen.
   b. Das Kontrollkästchen zum **Aktivieren von SnapMirror** auswählen und anschließend die `AutomatedFailoverDuplex` Richtlinie wählen.
   c. **Speichern** auswählen, um die LUNs, Konsistenzgruppe, Initiatorgruppe, SnapMirror Beziehung und Initiatorgruppen-Zuordnung zu erstellen.
2. Am sekundären Standort wird eine Initiatorgruppe erstellt und die LUNs werden zugeordnet.
   a. Zu **Hosts** > **SAN Initiatorgruppen** navigieren.
   b. **+Hinzufügen** auswählen, um eine neue Initiatorgruppe zu erstellen.
   c. Einen **Namen** angeben, das **Host-Betriebssystem** auswählen und anschließend die **Mitglieder der Initiatorgruppe** wählen.
   d. **Speichern** auswählen, um die Beziehung zu initialisieren.
3. Die neue Initiatorgruppe wird den Ziel-LUNs zugeordnet.
   a. Zu **Speicher** > **LUNs** navigieren.
   b. Alle LUNs auswählen, die der Initiatorgruppe zugeordnet werden sollen.
   c. **Mehr** und dann **Initiatorgruppen zuordnen** auswählen.

CLI

Schritte für eine einheitliche Konfiguration

1. Eine neue SnapMirror Beziehung erstellen, die alle Volumes in der Anwendung gruppiert. Dabei ist die `AutomatedFailOverDuplex` Richtlinie zur Einrichtung der bidirektionalen synchronen Replikation zu bestimmen.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Beispiel: Das folgende Beispiel erstellt zwei Konsistenzgruppen: cg_src auf der Quelle mit vol1 und vol2 sowie eine gespiegelte Konsistenzgruppe auf dem Ziel, cg_dst.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
   AutomatedFailOverDuplex
   ```

2. Die SnapMirror Beziehung initialisieren:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. Der erfolgreiche Abschluss des Vorgangs lässt sich bestätigen, indem abgewartet wird, bis das `Mirrored State` als `SnapMirrored` und das `Relationship Status` als `Insync` angezeigt wird.

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

4. Auf Ihrem Host wird die Host-Konnektivität mit Zugriff auf jeden Cluster entsprechend Ihren Anforderungen konfiguriert.
5. Die Initiatorgruppe-Konfiguration wird eingerichtet. Die bevorzugten Pfade für Initiatoren im lokalen Cluster werden festgelegt. Die Option, die Konfiguration für inverse Affinität auf den Peer-Cluster zu replizieren, wird angegeben.

   ```
   SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
   <igroup_name> -replication-peer <peer_svm_name> -initiator <host>
   ```

   Ab ONTAP 9.16.1 ist der `-proximal-vserver local` Parameter in diesem Befehl zu verwenden.

   ```
   SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
   <os_type> -initiator <host>
   ```

   Ab ONTAP 9.16.1 ist der `-proximal-vserver peer` Parameter in diesem Befehl zu verwenden.

6. Vom Host aus werden die Pfade ermittelt und es wird überprüft, ob die Hosts über einen aktiven/optimierten Pfad zum Storage-LUN vom bevorzugten Cluster verfügen.
7. Die Anwendung wird bereitgestellt und die VM-Workloads werden auf die Cluster verteilt, sodass der erforderliche Lastausgleich erreicht wird.

Schritte für eine nicht einheitliche Konfiguration

1. Eine neue SnapMirror Beziehung erstellen, die alle Volumes in der Anwendung gruppiert. Dabei ist die `AutomatedFailOverDuplex` Richtlinie zur Einrichtung der bidirektionalen synchronen Replikation zu bestimmen.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Beispiel: Das folgende Beispiel erstellt zwei Konsistenzgruppen: cg_src auf der Quelle mit vol1 und vol2 sowie eine gespiegelte Konsistenzgruppe auf dem Ziel, cg_dst.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
   AutomatedFailOverDuplex
   ```

2. Die SnapMirror Beziehung initialisieren:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. Der erfolgreiche Abschluss des Vorgangs lässt sich bestätigen, indem abgewartet wird, bis das `Mirrored State` als `SnapMirrored` und das `Relationship Status` als `Insync` angezeigt wird.

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

4. Auf Ihrem Host wird die Host-Konnektivität mit Zugriff auf jeden Cluster entsprechend Ihren Anforderungen konfiguriert.
5. Die Initiatorgruppen-Konfigurationen sind sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster zu erstellen.

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```

6. Vom Host aus werden die Pfade ermittelt und es wird überprüft, ob die Hosts über einen aktiven/optimierten Pfad zum Storage-LUN vom bevorzugten Cluster verfügen.
7. Die Anwendung wird bereitgestellt und die VM-Workloads werden auf die Cluster verteilt, sodass der erforderliche Lastausgleich erreicht wird.

Symmetrischer Aktiv/Aktiv-Schutz mit einer NVMe SnapMirror active sync Konfiguration

Bevor Sie beginnen

Zusätzlich zu den Anforderungen für die Konfiguration des symmetrischen Aktiv/Aktiv-Schutzes ist es wichtig, die unterstützten und nicht unterstützten Konfigurationen bei der Verwendung des NVMe-Protokolls zu kennen.

- Konsistenzgruppen können ein oder mehrere Subsysteme enthalten.
- Volumes innerhalb der Konsistenzgruppe können Namespace-Zuordnungen aus mehreren Subsystemen aufweisen.
- Subsysteme dürfen keine Namespace-Maps haben, die zu mehr als einer Konsistenzgruppe gehören.
- Subsysteme können nicht einige Namespace-Maps haben, die zu einer Konsistenzgruppe gehören, und einige Namespace-Maps, die nicht zu einer Konsistenzgruppe gehören.
- Subsysteme müssen Namespace-Maps haben, die Teil derselben Konsistenzgruppe sind.

Schritte

Ab ONTAP 9.17.1 ist es möglich, mit System Manager oder der ONTAP CLI eine Konsistenzgruppe zu erstellen und einen symmetrischen Aktiv/Aktiv-Schutz mithilfe von NVMe-Protokoll-Hostzuordnungen zu konfigurieren.

System Manager

1. Auf der Hauptseite, "Erstellen einer Konsistenzgruppe mithilfe neuer Volumes oder NVMe-Namespaces".

2. **+Hinzufügen** auswählen und **Neue NVMe-Namespaces verwenden** wählen.
3. Den Namen der Konsistenzgruppe eingeben.
4. **Mehr** auswählen.
5. Im Abschnitt **Schutz Aktivieren SnapMirror** auswählen und dann die `AutomatedFailoverDuplex` Richtlinie wählen.
6. Im Abschnitt **Host-Zuordnung** entweder **Vorhandenes NVMe-Subsystem** oder **Neues NVMe-Subsystem** auswählen.
7. **In der Nähe von** auswählen, um die proximale SVM zu ändern. Die Quell-SVM ist standardmäßig ausgewählt.
8. Gegebenenfalls kann ein weiteres NVMe Subsystem hinzugefügt werden.

CLI

1. Eine neue SnapMirror Beziehung erstellen, die alle Volumes gruppiert, die sämtliche von der Anwendung verwendeten NVMe-Namespaces enthalten. Dabei ist die `AutomatedFailOverDuplex` Richtlinie zur Einrichtung der bidirektionalen synchronen Replikation zu bestimmen.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Beispiel:

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. Die SnapMirror Beziehung initialisieren:
   `snapmirror initialize -destination-path <destination-consistency-group>`

   Beispiel:

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. Der erfolgreiche Abschluss des Vorgangs lässt sich bestätigen, indem abgewartet wird, bis das `Mirrored State` als `SnapMirrored` und das `Relationship Status` als `Insync` angezeigt wird.

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

   Die NVMe-Subsysteme, die den NVMe-Namespaces in den primären Volumes zugeordnet sind, werden automatisch auf den sekundären Cluster repliziert.

4. Auf Ihrem Host wird die Host-Konnektivität mit Zugriff auf jeden Cluster entsprechend Ihren Anforderungen konfiguriert.
5. Geben Sie die SVM an, die sich in der Nähe jedes Ihrer Hosts befindet. Dadurch erhalten die Hosts Zugriff auf den NVMe-Namensraum über einen Pfad vom bevorzugten Cluster. Dies kann die SVM im

primären Cluster oder die SVM im DR Cluster sein.

Der folgende Befehl gibt an, dass SVM VS_A dem Host H1 nahe ist und VS_A als proximale SVM festgelegt ist:

```
SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
-proximal-vservers <VS_A>
```

Der folgende Befehl zeigt an, dass SVM VS_B dem Host H2 nahe ist und VS_B als proximale SVM festgelegt wird:

```
SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
-proximal-vservers <VS_B>
```

6. Vom Host aus lassen sich die Pfade ermitteln und es kann überprüft werden, ob die Hosts über einen Aktiv/optimiert-Pfad zum Speicher vom bevorzugten Cluster verfügen.
7. Die Anwendung wird bereitgestellt und die VM-Workloads werden auf die Cluster verteilt, sodass der erforderliche Lastausgleich erreicht wird.

Verwandte Informationen

- "snapmirror create"
- "snapmirror initialize"
- "snapmirror show"

Mit ONTAP SnapMirror Active Sync für NAS schützen

Konfiguration der SnapMirror active sync für NAS

Ab ONTAP 9.19.1 ist die Konfiguration von SnapMirror Active Sync für NAS Konfigurationen möglich.

Bevor Sie beginnen

- Beide Cluster in der SnapMirror Aktiv Sync-Beziehung müssen mit ONTAP 9.19.1 oder höher betrieben werden.
- Sie müssen Cluster-Administrator sein.
- ONTAP Mediator oder ONTAP Cloud Mediator muss konfiguriert sein.
- Die Quell- und Zielcluster müssen per Peering verbunden sein.

ONTAP unterstützte und nicht unterstützte Funktionen mit SnapMirror active sync für NAS

Die folgende Tabelle beschreibt die unterstützten und nicht unterstützten ONTAP-Funktionen mit SnapMirror active sync für NAS.

ONTAP Funktion	Unterstützt durch SnapMirror active sync	Weitere Informationen
Konsistenzgruppen für Anwendungen	Nein	
Prüfung	Ja	Nur die konsolidierten Protokolle in der SVM werden repliziert.
DP-Volumes	Nein	

ONTAP Funktion	Unterstützt durch SnapMirror active sync	Weitere Informationen
FabricPool	Teilweise	Die `all`Tiering-Richtlinie ist auf SnapMirror active sync NAS-Volumes nicht zulässig.
Dateisystemanalyse	Teilweise	Auf der sekundären SVM ist die Dateisystemanalyse standardmäßig auf `Off` gesetzt und muss nach einem Failover manuell auf `On` gesetzt werden.
FlexCache Volume	Nein	
FlexGroup-Volume	Nein	
Fpolicy und Antivirus-Scan	Ja	
Load-sharing-Spiegel	Nein	In ONTAP 9.19.1 unterstützt SnapMirror Active Sync für NAS nur 2 Knoten in einem AFF Cluster.
MetroCluster Konfiguration	Nein	
Multi Admin Verify für NAS-Befehle	Nein	
S3 NAS	Nein	
SAN-Volumes in einer SnapMirror active sync NAS-geschützten SVM	Nein	SnapMirror Active Sync für die NAS-Initialisierung schlägt fehl, wenn Volumes, die LUNs hosten, in der SVM vorhanden sind.
SnapLock	Nein	
SnapMirror to Cloud	Nein	
SVM Migration	Nein	

Über diese Aufgabe

Um SnapMirror active sync für NAS zu aktivieren, wird eine Ziel-SVM erstellt. Die Ziel-SVM bleibt inaktiv, bis ein Failover auftritt.

Schritte

Sie können den System Manager oder die ONTAP CLI verwenden, um SnapMirror active sync für NAS zu konfigurieren.

System Manager

1. Im Quell-Cluster zu Cluster > Storage-VMs navigieren.
2. Klicken Sie ⋮ neben dem Namen der SVM, die Sie konfigurieren möchten, und wählen Sie **Schützen** aus.
3. Im Fenster **Speicher-VM schützen** das Ziel-Cluster auswählen.
4. Wählen Sie `AutomatedFailOver` als Replikationsrichtlinie.
5. Geben Sie einen Namen für die Speicher-VM ein, die auf dem Ziel erstellt wird.

6. Wählen Sie die zu schützenden Volumes aus:
   a. **Alle Volumes schützen** – standardmäßig sind alle Volumes geschützt
   b. **Zu schützende Volumes auswählen** - nur die ausgewählten Volumes sind geschützt
   c. **Auszuschließende Volumes auswählen** – die ausgewählten Volumes sind vom Schutz ausgeschlossen
7. Auf **Beziehung initialisieren** klicken.
8. Auf **Speichern** klicken.
9. Im Fenster **Storage VM schützen** lässt sich der SVM-Schutzstatus in der Spalte **Schutz** überprüfen.

CLI

1. Im Ziel-Cluster eine SVM vom Typ dp-destination erstellen:

   ```
   vserver create -vserver <SVM name> -sub-type dp-destination
   ```

   Beispiel:

   ```
   destination::> vserver create -vserver vs_b -sub-type dp-destination
   ```

2. Eine SVM Peer-Beziehung zur Quell-SVM erstellen:

   ```
   vserver peer create -vserver <destination SVM> -peer-vserver <souce SVM>
   -peer-cluster <source cluster> -applications snapmirror
   ```

   Beispiel:

   ```
   destination::> vserver peer create -vserver vs_b -peer-vserver vs_a
   -peer-cluster SiteA -applications snapmirror
   ```

3. Auf dem Quell-SVM die Peer-Anfrage akzeptieren:

   ```
   vserver peer accept -vserver <source SVM name> -peer-vserver <destination
   SVM name>vserver peer accept -vserver <source SVM name> -peer-vserver
   <destination SVM name>
   ```

   Beispiel:

   ```
   source::> vserver peer accept -vserver vs_a -peer-vserver vs_b
   ```

4. Die SnapMirror Beziehung erstellen:

   ```
   snapmirror create -source-path <source SVM name>: -destination-path
   <destination SVM name>: -policy AutomatedFailOver
   ```

   Beispiel:

```
destination::> snapmirror create -source-path vs_a: -destination
-path vs_b: -policy AutomatedFailOver
```

5. Überprüfung, ob die Beziehung erstellt wurde, und Statuskontrolle:

   'snapmirror show'

   Beispiel:

```
destination::> snapmirror show
Progress
    Source            Destination Mirror        Relationship   Total
Last
    Path        Type  Path        State         Status
Progress  Healthy Updated
    ----------- ---- ------------ -------       --------------
--------- ------- --------
    vs_a:       XDP  vs_b:        Uninitialized Idle           -
true    -
```

6. Auf der Ziel-SVM die Beziehung initialisieren:

   `snapmirror initialize -destination-path <SVM name>:`

   Beispiel:

```
destination::> snapmirror initialize -destination-path vs_b:
```

7. Initialisierungsstatus prüfen:

   `snapmirror show`

   Beispiel:

```
    destination::> snapmirror show

Progress
    Source            Destination Mirror        Relationship   Total
Last
    Path        Type  Path        State         Status
Progress  Healthy Updated
    ----------- ---- ------------ -------       --------------
--------- ------- --------
    vs_a:       XDP  vs_b:        Snapmirrored  InSync         -
```

```
true    -
```

Ein ungeschütztes Volume in einer SnapMirror active sync NAS Konfiguration erstellen

Sie können Volumes von SnapMirror active sync ausschließen, wenn kein Schutz erforderlich ist, zum Beispiel beim Erstellen eines FlexClone Volume für Entwicklungstests.

Schritt

Sie können den System Manager oder die ONTAP CLI verwenden, um ein geklontes Volume von SnapMirror active sync für NAS auszuschließen.

System Manager

1. Im Quell-Cluster zu **Storage > Volumes** navigieren.
2. In der Liste der Volumes ⋮ neben dem Namen des Volumes, das geklont werden soll, **Klonen** auswählen.
3. Im Fenster **Volume klonen** sollte sichergestellt sein, dass **Klon in den Schutz für Geschäftskontinuität einbeziehen** deaktiviert ist.
4. Auf **Klonen** klicken.

CLI

1. Vom Quell-Cluster aus ein ungeschütztes Volume zu einer bestehenden SnapMirror active sync Konfiguration hinzufügen:

```
volume clone create -vserver <SVM name> -flexclone <clone vol name> -parent
-vserver <SVM name> -parent-volume <vol name> -parent-snapshot <snapshot
name>
volume add -vserver <SVM name> -volume <volume name> -smas-protection
unprotected
```

Verwenden Sie die ONTAP CLI, um ein Volume aus einer SnapMirror Active Sync NAS-Konfiguration auszuschließen.

Sie können ein Volume aus einer SnapMirror active sync NAS-Konfiguration ausschließen, wenn der Schutz nicht mehr benötigt wird oder wenn das Volume gelöscht werden soll.

ⓘ Das Aufheben des Schutzes eines aktuell geschützten Volumes löst eine Verkleinerungsoperation an der SnapMirror active sync Beziehung aus. Die Verkleinerungsoperation löscht SnapMirror Einträge für das Volume sowohl auf dem Quell- als auch auf dem Zielsystem.

ⓘ Das Markieren eines Volumes als ungeschützt löscht das Volume nicht automatisch in der primären oder sekundären Beziehung. Soll das Volume gelöscht werden, ist eine manuelle Löschung sowohl auf der primären als auch auf der sekundären SVM möglich.

Schritt

1. Entfernen eines Volumes aus dem aktiven NAS-Schutz von SnapMirror:

```
volume modify -vserver <SVM name> -volume <volume name> -smas-protection
```

```
unprotected
```

Konvertieren einer SVM-DR-Beziehung in eine SnapMirror active sync-Beziehung

In ONTAP 9.19.1 ist es nicht möglich, eine SVM DR-Beziehung direkt in eine SnapMirror active sync for NAS Beziehung umzuwandeln. Stattdessen ist die SVM DR-Beziehung zu löschen, eine neue Ziel-SVM zu erstellen, eine neue SnapMirror active sync Beziehung zu etablieren und die Beziehung zu initialisieren.

Der `snapmirror resync`Befehl wird derzeit nicht unterstützt.

1. Im Ziel-Cluster die SnapMirror Beziehung löschen:

   ```
   snapmirror delete -destination-path
   ```

2. Auf dem primären Cluster die Beziehungsinformationen freigeben:

   ```
   snapmirror release -relationship-info-only true
   ```

3. Im Ziel-Cluster eine SVM mit dem Subtyp dp-destination erstellen:

   ```
   vserver create -vserver <SVM name> -sub-type dp-destination
   ```

4. Erstellen Sie auf dem Ziel-Cluster die SnapMirror Beziehung mithilfe der `AutomatedFailover` Richtlinie:

   ```
   snapmirror create -source-path <source SVM name> -destination-path
   <destination SVM name> -policy AutomatedFailOver
   ```

5. Im Ziel-Cluster die Beziehung initialisieren:

   ```
   snapmirror initialize -destination-path <SVM name>
   ```

Verwandte Informationen

- "snapmirror create"
- "snapmirror initialize"
- "snapmirror show"

Konvertierung einer bestehenden ONTAP SnapMirror SAN Beziehung in SnapMirror active sync

Wenn SnapMirror-Schutz konfiguriert wurde, kann eine SAN-Beziehung in SnapMirror active sync für SAN umgewandelt werden. Ab ONTAP 9.15.1 kann die Beziehung so umgestellt werden, dass symmetrischer Aktiv/Aktiv-Schutz verwendet wird.

Informationen zur Umwandlung einer SVM-DR-Beziehung in eine SnapMirror active sync for NAS-Beziehung sind unter "Konvertieren einer SVM-DR-Beziehung in eine SnapMirror active sync-Beziehung" zu finden.

Eine bestehende iSCSI oder FC SnapMirror Beziehung in eine asymmetrische SnapMirror Active Sync Beziehung umwandeln

Wenn bereits eine iSCSI- oder FC-SnapMirror-synchron Beziehung zwischen einem Quell- und einem Ziel-Cluster besteht, kann diese in eine asymmetrische SnapMirror Active Sync-Beziehung umgewandelt werden. Dadurch ist es möglich, die gespiegelten Volumes einer Konsistenzgruppe zuzuordnen, was einen RPO von null über einen Workload mit mehreren Volumes sicherstellt. Zudem können vorhandene SnapMirror-

Snapshots beibehalten werden, falls auf einen Zeitpunkt vor dem Einrichten der SnapMirror Active Sync-Beziehung zurückgegriffen werden muss.

Über diese Aufgabe

- Sie sind als Cluster- und SVM-Administrator auf dem primären und sekundären Cluster erforderlich.
- Sie können eine Zero-RPO- in eine Zero-RTO-Synchronisierung nicht durch Ändern der SnapMirror-Richtlinie umwandeln.
- Es ist sicherzustellen, dass die LUNs nicht zugeordnet sind, bevor der `snapmirror create` Befehl ausgeführt wird.

  Wenn vorhandene LUNs auf dem sekundären Volume zugeordnet sind und die `AutomatedFailover` Richtlinie konfiguriert ist, löst der `snapmirror create` Befehl einen Fehler aus.

Bevor Sie beginnen

- Eine SnapMirror synchron Beziehung mit einem RPO von Null muss zwischen dem primären und dem sekundären Cluster bestehen.
- Alle LUNs auf dem Ziel-Volume müssen unzugeordnet werden, bevor die Zero RTO SnapMirror Beziehung erstellt werden kann.
- "ONTAP Mediator"muss für SnapMirror active sync konfiguriert sein.

Schritte

1. Im sekundären Cluster eine SnapMirror-Aktualisierung der bestehenden Beziehung durchführen:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Überprüfen Sie, ob das SnapMirror Update erfolgreich abgeschlossen wurde:

   ```
   SiteB::>snapmirror show
   ```

3. Jede der synchronen Beziehungen mit RPO Null unterbrechen:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Jede der synchronen Beziehungen mit RPO Null löschen:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Die SnapMirror Beziehung der Quelle wird freigegeben, die gemeinsamen Snapshots bleiben jedoch erhalten:

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Erstellung einer SnapMirror synchronen Beziehung mit null RTO:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailover
```

7. Die Konsistenzgruppe erneut synchronisieren:

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Die Host-LUN-I/O-Pfade werden erneut gescannt, um alle Pfade zu den LUNs wiederherzustellen.

Eine bestehende iSCSI oder FC SnapMirror Beziehung in eine symmetrische Aktiv/Aktiv umwandeln

Ab ONTAP 9.15.1 ist es möglich, eine bestehende iSCSI oder FC SnapMirror Beziehung in eine SnapMirror active sync symmetrische Aktiv/Aktiv Beziehung zu konvertieren.

Bevor Sie beginnen

- ONTAP 9.15.1 oder höher muss ausgeführt werden.
- Eine SnapMirror synchrone Beziehung mit null RPO muss zwischen dem primären und dem sekundären Cluster bestehen.
- Alle LUNs auf dem Ziel-Volume müssen unzugeordnet werden, bevor die Zero RTO SnapMirror Beziehung erstellt werden kann.
- SnapMirror active sync unterstützt ausschließlich SAN-Protokolle (nicht NFS/CIFS). Es ist sicherzustellen, dass kein Bestandteil der Konsistenzgruppe für den NAS-Zugriff eingebunden ist.
- "ONTAP Mediator"muss für SnapMirror active sync konfiguriert sein.

Schritte

1. Im sekundären Cluster eine SnapMirror-Aktualisierung der bestehenden Beziehung durchführen:

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. Überprüfen Sie, ob das SnapMirror Update erfolgreich abgeschlossen wurde:

```
SiteB::>snapmirror show
```

3. Jede der synchronen Beziehungen mit RPO Null unterbrechen:

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Jede der synchronen Beziehungen mit RPO Null löschen:

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Die SnapMirror Beziehung der Quelle wird freigegeben, die gemeinsamen Snapshots bleiben jedoch erhalten:

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1
```

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. Eine Zero-RTO-SnapMirror synchron Beziehung mit der AutomatedFailoverDuplex Richtlinie erstellen:

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. Wenn sich die vorhandenen Hosts lokal im primären Cluster befinden, sollte der Host dem sekundären Cluster hinzugefügt und die Konnektivität mit entsprechendem Zugriff auf jeden Cluster hergestellt werden.
8. Am sekundären Standort die LUN-Zuordnungen auf den Initiatorgruppen löschen, die mit Remote-Hosts verknüpft sind.

> Es ist sicherzustellen, dass die Initiatorgruppe keine Zuordnungen für nicht replizierte LUNs enthält.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. Am primären Standort wird die Initiatorkonfiguration für bestehende Hosts angepasst, sodass der proximale Pfad für Initiatoren im lokalen Cluster festgelegt ist.

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
<host> -proximal-vserver <server>
```

10. Fügen Sie eine neue Initiatorgruppe (igroup) und einen Initiator für die neuen Hosts hinzu und legen Sie die Host-Nähe für die Host-Affinität auf den lokalen Standort fest. Aktivieren Sie die igroup Replikation, um die Konfiguration zu replizieren und die Host-Lokalität auf dem Remote-Cluster umzukehren.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. Ermitteln Sie die Pfade auf den Hosts und überprüfen Sie, ob die Hosts über einen Aktiv/Optimiert-Pfad zum Speicher-LUN vom bevorzugten Cluster verfügen.
12. Die Anwendung wird bereitgestellt und die VM-Workloads werden auf die Cluster verteilt.
13. Die Konsistenzgruppe erneut synchronisieren:

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. Die Host-LUN-I/O-Pfade werden erneut gescannt, um alle Pfade zu den LUNs wiederherzustellen.

Verwandte Informationen

- "ONTAP Mediator Dokumentation"
- "snapmirror create"
- "snapmirror delete"
- "snapmirror quiesce"
- "SnapMirror Release"

- "SnapMirror Resynchronisierung"
- "snapmirror show"

ONTAP SnapMirror Active Sync Beziehungstyp konvertieren

Ab ONTAP 9.15.1 ist eine Konvertierung zwischen den Typen des SnapMirror Active Sync-Schutzes möglich: von asymmetrisch zu symmetrisch Aktiv/Aktiv und umgekehrt.

In eine symmetrische Aktiv/Aktiv-Beziehung umwandeln

Eine iSCSI- oder FC-SnapMirror Active Sync-Beziehung mit asymmetrischem Schutz kann in eine symmetrische Aktiv/Aktiv-Beziehung umgewandelt werden.

Bevor Sie beginnen

- Beide Cluster müssen ONTAP 9.15.1 oder höher ausführen.
- Symmetrische Aktiv/Aktiv Konfigurationen erfordern die `AutomatedFailoverDuplex` Datensicherungsstrategie. Alternativ ist es möglich, eine benutzerdefinierte SnapMirror Richtlinie erstellen sofern die `-type automated-failover-duplex` erfüllt ist.

System Manager

Schritte für eine einheitliche Konfiguration

1. Die Ziel-Initiatorgruppe entfernen:
   a. Im Ziel-Cluster zu **Hosts** > **SAN Initiatorgruppen** navigieren.
   b. Die Initiatorgruppe mit der SnapMirror Beziehung auswählen und anschließend **Löschen** wählen.
   c. Im Dialogfeld das Kontrollkästchen **Zugehörige LUNs aufheben** auswählen und dann **Löschen**.
2. Die SnapMirror Active Sync-Beziehung bearbeiten.
   a. Zu **Schutz** > **Beziehungen** navigieren.
   b. Das Kebab-Menü neben der Beziehung, die geändert werden soll, auswählen und anschließend auf **Bearbeiten** gehen.
   c. Die **Datensicherungsstrategie** wird auf AutomatedFailoverDuplex geändert.
   d. Durch Auswahl `AutoMatedFailoverDuplex` wird ein Dialogfeld zur Änderung der Host-Näheeinstellungen geöffnet. Für die Initiatoren ist die passende Option für **Initiator in der Nähe von** auszuwählen und anschließend **Speichern**.
   e. **Speichern** auswählen.
3. Im Menü **Schutz** wird der erfolgreiche Abschluss des Vorgangs bestätigt, wenn die Beziehung als `InSync` angezeigt wird.

Schritte für eine nicht einheitliche Konfiguration

1. Die Ziel-Initiatorgruppe entfernen:
   a. Auf der sekundären Website zu **Hosts** > **SAN Initiatorgruppen** navigieren.
   b. Die Initiatorgruppe mit der SnapMirror Beziehung auswählen und anschließend **Löschen** wählen.
   c. Im Dialogfeld das Kontrollkästchen **Zugehörige LUNs aufheben** auswählen und dann **Löschen**.
2. Neue Initiatorgruppe erstellen:
   a. Im Menü **SAN Initiator Groups** auf der Zielseite **Hinzufügen** auswählen.

b. Einen **Namen** angeben, das **Host-Betriebssystem** auswählen und anschließend die **Mitglieder der Initiatorgruppe** wählen.

c. **Speichern** auswählen.

3. Die neue Initiatorgruppe wird den Ziel-LUNs zugeordnet.

a. Zu **Speicher** > **LUNs** navigieren.

b. Alle LUNs auswählen, die der Initiatorgruppe zugeordnet werden sollen.

c. **Mehr** und dann **Initiatorgruppen zuordnen** auswählen.

4. Die SnapMirror Active Sync-Beziehung bearbeiten.

a. Zu **Schutz** > **Beziehungen** navigieren.

b. Das Kebab-Menü neben der Beziehung, die geändert werden soll, auswählen und anschließend auf **Bearbeiten** gehen.

c. Die **Datensicherungsstrategie** wird auf AutomatedFailoverDuplex geändert.

d. Die Auswahl von AutoMatedFailoverDuplex initiiert die Möglichkeit, die Einstellungen für die Hostnähe zu ändern. Für die Initiatoren ist die passende Option für **Initiator in der Nähe von** auszuwählen und anschließend **Speichern**.

e. **Speichern** auswählen.

5. Im Menü **Schutz** wird der erfolgreiche Abschluss des Vorgangs bestätigt, wenn die Beziehung als `InSync` angezeigt wird.

CLI

Schritte für eine einheitliche Konfiguration

1. Die SnapMirror Richtlinie wird von `AutomatedFailover` auf `AutomatedFailoverDuplex` geändert:

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. Durch die Änderung der Richtlinie wird eine erneute Synchronisierung ausgelöst. Warten Sie, bis die erneute Synchronisierung abgeschlossen ist, und bestätigen Sie, dass die Beziehung `Insync`:

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

3. Wenn sich die vorhandenen Hosts lokal im primären Cluster befinden, ist der Host dem zweiten Cluster hinzuzufügen und die Konnektivität mit entsprechendem Zugriff auf jeden Cluster herzustellen.

4. Am sekundären Standort die LUN-Zuordnungen auf den Initiatorgruppen löschen, die mit Remote-Hosts verknüpft sind.

> Es ist sicherzustellen, dass die Initiatorgruppe keine Zuordnungen für nicht replizierte LUNs enthält.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

5. Am primären Standort die Berechtigungsstufe auf `advanced` setzen:

```
SiteA::> set -privilege advanced
```

6. Die Initiatorkonfiguration für bestehende Hosts wird angepasst, sodass der proximale Pfad für Initiatoren auf dem lokalen Cluster festgelegt ist.

```
SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
-initiator <host> -proximal-vserver <server>
```

> Die Berechtigungsstufe kann nach Abschluss dieses Schritts wieder auf Administrator gesetzt werden.

7. Fügen Sie eine neue Initiatorgruppe (igroup) und einen Initiator für die neuen Hosts hinzu und legen Sie die Host-Nähe für die Host-Affinität auf den lokalen Standort fest. Aktivieren Sie die igroup Replikation, um die Konfiguration zu replizieren und die Host-Lokalität auf dem Remote-Cluster umzukehren.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
host2 -proximal-vserver vsB
```

8. Ermitteln Sie die Pfade auf den Hosts und überprüfen Sie, ob die Hosts über einen Aktiv/Optimiert-Pfad zum Speicher-LUN vom bevorzugten Cluster verfügen.
9. Die Anwendung wird bereitgestellt und die VM-Workloads werden auf die Cluster verteilt.

Schritte für eine nicht einheitliche Konfiguration

1. Die SnapMirror Richtlinie wird von `AutomatedFailover` auf `AutomatedFailoverDuplex` geändert:

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. Durch die Änderung der Richtlinie wird eine erneute Synchronisierung ausgelöst. Warten Sie, bis die erneute Synchronisierung abgeschlossen ist, und bestätigen Sie, dass die Beziehung `Insync`:

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

3. Wenn sich die vorhandenen Hosts lokal beim primären Cluster befinden, ist der Host dem zweiten Cluster hinzuzufügen und die Konnektivität mit entsprechendem Zugriff auf jeden Cluster herzustellen.
4. Am sekundären Standort eine neue Initiatorgruppe (igroup) und einen Initiator für die neuen Hosts hinzufügen und die Host-Nähe für die Host-Affinität auf den lokalen Standort setzen. Die LUNs der Initiatorgruppe (igroup) zuordnen.

```
SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
<host_name>
SiteB::> lun mapping create -igroup <igroup> -path <path_name>
```

5. Ermitteln Sie die Pfade auf den Hosts und überprüfen Sie, ob die Hosts über einen Aktiv/Optimiert-Pfad zum Speicher-LUN vom bevorzugten Cluster verfügen.

6. Die Anwendung wird bereitgestellt und die VM-Workloads werden auf die Cluster verteilt.

Konvertierung von einer symmetrischen Aktiv/Aktiv- in eine asymmetrische iSCSI- oder FC-Beziehung

Wenn Sie einen symmetrischen Aktiv/Aktiv-Schutz mit iSCSI oder FC konfiguriert haben, kann die Beziehung mithilfe der ONTAP CLI in einen asymmetrischen Schutz umgewandelt werden.

Schritte

1. Alle VM-Workloads werden auf den Host verschoben, der sich lokal beim Quell-Cluster befindet.
2. Die Initiatorgruppe-Konfiguration für die Hosts, die die VM-Instanzen nicht verwalten, wird entfernt, anschließend wird die Initiatorgruppe-Konfiguration geändert, um die Initiatorgruppe-Replikation zu beenden.

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. Am sekundären Standort die Zuordnung der LUNs aufheben.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. Am sekundären Standort die symmetrische Aktiv/Aktiv Beziehung löschen.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. Am primären Standort die symmetrische Aktiv/Aktiv Beziehung freigeben.
   `SiteA::> snapmirror release -destination-path <destination_path> -relationship -info-only true`
6. Vom sekundären Standort aus eine Beziehung zum gleichen Satz von Volumes mit der `AutomatedFailover`Richtlinie erstellen, um die Beziehung zu resynchronisieren.

   ```
   SiteB::> snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source:@destination> -policy
   AutomatedFailover
   SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
   <policy_type>
   ```

   > Die Konsistenzgruppe am sekundären Standort benötigt "zu löschen" vor der erneuten Erstellung der Beziehung. Die Ziel-Volumes "muss in den Typ DP konvertiert werden". Um die Volumes in DP zu konvertieren, wird der `snapmirror resync`-Befehl mit einer nicht-`AutomatedFailover`-Strategie ausgeführt: `MirrorAndVault`, `MirrorAllSnapshots` oder `Sync`.

7. Bestätigen, dass der Mirror State der Beziehung `Snapmirrored` und der Relationship Status `Insync` ist.

   ```
   snapmirror show -destination-path destination_path
   ```

8. Die Pfade vom Host erneut erkennen.

Verwandte Informationen

- "snapmirror delete"
- "snapmirror modify"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"
- "snapmirror show"

Aktive Synchronisierung von SnapMirror verwalten und Daten schützen

Einen gemeinsamen Snapshot zwischen ONTAP Konsistenzgruppen oder NAS SVMs erstellen

Zusätzlich zu den regelmäßig geplanten Snapshot-Operationen kann eine gemeinsame "Schnappschuss" zwischen den Volumes in der primären SnapMirror Konsistenzgruppe und den Volumes in der sekundären SnapMirror Konsistenzgruppe in einer SAN-Konfiguration oder auf SVM-Ebene bei NAS-Konfigurationen manuell erstellt werden.

Über diese Aufgabe

Das geplante Snapshot-Erstellungsintervall beträgt 12 Stunden für die Richtlinie Automated Failover und 3 Stunden für die Richtlinie Automated Failover Duplex.

Bevor Sie beginnen

- Die SnapMirror Gruppenbeziehung muss synchron sein.

Schritte

Sie können einen gemeinsamen Snapshot mit System Manager oder der ONTAP CLI erstellen.

System Manager

1. Im Ziel-Cluster zu **Schutz > Replikation** navigieren.
2. Die Beziehungsquelle suchen, ⋮ auswählen und **Aktualisieren** wählen.
3. **Gemäß Richtlinie** oder **Snapshot auswählen** kann gewählt werden, um einen vorhandenen Snapshot auszuwählen.
4. Wählen Sie **Aktualisieren**.

CLI

1. Vom Zielstandort aus einen gemeinsamen Snapshot erstellen:

   ```
   snapmirror update -destination-path <destination path>
   ```

   Beispiel für eine SAN Konfiguration:

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

   Beispiel für eine NAS Konfiguration:

   ```
   snapmirror update -destination-path vs_b:
   ```

2. Der Fortschritt des Updates kann überwacht werden:

```
destination::>snapmirror show -fields newest-snapshot
```

Verwandte Informationen

- "snapmirror show"

Ein geplantes Failover in ONTAP SnapMirror active sync durchführen

Bei einem geplanten Failover von ONTAP Clustern in einer SnapMirror active sync Beziehung werden die Rollen des primären und sekundären Clusters getauscht, sodass der sekundäre Cluster die Aufgaben des primären Clusters übernimmt. Während eines Failovers verarbeitet der normalerweise sekundäre Cluster Ein- und Ausgabeanforderungen lokal, ohne den Clientbetrieb zu unterbrechen.

Ein geplantes Failover kann durchgeführt werden, um die Funktionsfähigkeit der Disaster-Recovery-Konfiguration zu testen oder Wartungsarbeiten am primären Cluster vorzunehmen.

Über diese Aufgabe

Ein geplanter Failover wird vom Administrator des sekundären Clusters initiiert. Der Vorgang erfordert das Tauschen der primären und sekundären Rollen, sodass der sekundäre Cluster die Aufgaben des primären Clusters übernimmt. Der neue primäre Cluster kann dann die Verarbeitung von Ein- und Ausgabeanfragen lokal aufnehmen, ohne den Clientbetrieb zu unterbrechen.

Bevor Sie beginnen

- Die SnapMirror active sync-Beziehung muss synchron sein.
- Ein geplanter Failover kann nicht eingeleitet werden, wenn ein unterbrechungsfreier Vorgang ausgeführt wird. Unterbrechungsfreie Vorgänge umfassen Volume-Verschiebungen, Aggregat-Relokationen und Storage Failover.
- Der ONTAP Mediator muss konfiguriert, verbunden und im Quorum sein.

Schritte

Ein geplantes Failover kann mithilfe der ONTAP CLI oder des System Manager durchgeführt werden.

System Manager

Von ONTAP 9.8 bis ONTAP 9.14.1 wird SnapMirror active sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

1. Im System Manager **Schutz > Übersicht > Beziehungen** auswählen.
2. Identifizieren Sie die SnapMirror Active Sync-Beziehung, für die ein Failover durchgeführt werden soll. Neben dem Namen der Beziehung das … auswählen und anschließend **Failover** wählen.
3. Zum Überwachen des Status des Failovers kann der `snapmirror failover show` Befehl in der ONTAP CLI genutzt werden.

CLI

1. Vom Ziel-Cluster aus den Failover-Vorgang einleiten:

```
snapmirror failover start -destination-path <path>
```

Beispiel für das Failover einer SAN-Konfiguration:

```
destination::>snapmirror failover start -destination-path vs1_dst:/cg/cg_dst
```

Beispiel für das Failover einer NAS-Konfiguration:

```
destination::>snapmirror failover start -destination-path vs_b:
```

2. Vom Ziel aus lässt sich der Fortschritt des Failovers überwachen:

```
snapmirror failover show
```

3. Nach Abschluss des Failover-Vorgangs kann der Status der SnapMirror synchronen Schutzbeziehung vom Ziel-Cluster aus überwacht werden:

```
snapmirror show
```

Verwandte Informationen

- "snapmirror failover show"
- "SnapMirror Failover Start"
- "snapmirror show"

Wiederherstellung nach automatischen ungeplanten ONTAP Cluster Failover-Operationen

Ein automatischer ungeplanter Failover (AUFO) erfolgt, wenn der primäre Cluster ausfällt oder isoliert ist. SnapMirror active sync erkennt solche Fehler und initiiert einen automatischen ungeplanten Failover auf den sekundären Cluster. Der sekundäre Cluster wird in den primären (bevorzugten) Cluster umgewandelt und beginnt mit der Bedienung der Clients. Zu beachten ist, dass die Fehlererkennung und die Failover-Verarbeitung nur mit Unterstützung des ONTAP Mediators durchgeführt werden können.

Nach dem automatischen ungeplanten Failover ist es wichtig, die Hostpfade erneut zu scannen, damit kein Verlust von E/A-Pfaden auftritt.

Die Schutzbeziehung nach einem ungeplanten Failover wiederherstellen

Sobald der ursprüngliche primäre Cluster, beispielsweise Cluster A, wiederhergestellt ist, stellt SnapMirror active sync den Schutz automatisch in umgekehrter Richtung her. Wenn der ursprüngliche Zustand wiederhergestellt werden soll und Cluster A wieder der primäre, bevorzugte Cluster sein soll, ist ein manuelles Failback möglich, indem ein geplanter Failover-Vorgang über System Manager oder die ONTAP CLI initiiert wird.

System Manager

Schritte

Von ONTAP 9.8 bis ONTAP 9.14.1 wird SnapMirror active sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

1. Zu **Schutz > Beziehungen** navigieren und abwarten, bis der Beziehungsstatus "InSync" angezeigt wird.
2. Um ein Failback durchzuführen und den Betrieb auf dem ursprünglichen Quell-Cluster fortzusetzen, ⋮ und **Failover** auswählen.

CLI

Der Status des automatischen ungeplanten Failovers kann mit dem `snapmirror failover show` Befehl überwacht werden.

Beispiel:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Den Status der umgekehrten Schutzbeziehung können Sie mit dem `snapmirror show`-Befehl auf dem ursprünglichen primären Cluster überwachen.

Beispiel:

```
ClusterA::> snapmirror show

Progress
Source             Destination  Mirror        Relationship   Total
Last
Path         Type  Path         State         Status         Progress
Healthy Updated
-----------  ----  ------------ -------       -------------- ---------
------- --------
vs3:/cg/dcg3 XDP   vs1:/cg/scg3 Snapmirrored  InSync          -
true    -
```

Ein Failback zum ursprünglichen primären Cluster kann mit dem `snapmirror failover start` Befehl durchgeführt werden.

Beispiel:

```
ClusterA::> snapmirror failover start -destination-path vs1:/cg/scg3
```

In der "EMS-Referenz" finden sich Informationen zu Ereignismeldungen und Korrekturmaßnahmen.

Wiederaufnahme des Schutzes in einer Fan-Out-Konfiguration nach einem Failover

Ab ONTAP 9.15.1 unterstützt SnapMirror active sync die automatische Neukonfiguration im Fan-Out-Bein nach einem Failover-Ereignis in einer SAN-Beziehung. In einer NAS-Konfiguration ist die Schutzbeziehung nach einem SnapMirror active sync Failover manuell neu zu konfigurieren. Das asynchrone Fan-Out-Bein kann eine Konsistenzgruppenbeziehung oder eine unabhängige Volume-Beziehung sein. Weitere Informationen finden sich unter "Fan-Out Konfigurationen".

Wenn ONTAP 9.14.1 oder eine frühere Version verwendet wird und ein Failover auf dem sekundären Cluster in der SnapMirror Aktiv/Aktiv-Sync-Beziehung auftritt, wird das SnapMirror asynchrone Ziel-Cluster fehlerhaft. Der Schutz muss manuell wiederhergestellt werden, indem die Beziehung mit dem SnapMirror asynchronen Endpunkt gelöscht und neu erstellt wird.

Schritte

1. Es wird überprüft, ob das Failover erfolgreich abgeschlossen wurde:
   `snapmirror failover show`
2. Am SnapMirror asynchronen Endpunkt den Fan-Out-Endpunkt löschen:
   `snapmirror delete -destination-path` *`destination_path`*
3. Am dritten Standort wird eine SnapMirror asynchrone Beziehung zwischen dem neuen SnapMirror Active Sync-Primärvolume und dem asynchronen Fan-Out-Zielvolume erstellt:
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*
4. Die Beziehung neu synchronisieren:
   `snapmirror resync -destination-path` *`destination_path`*
5. Beziehungsstatus und Zustand der Beziehung prüfen:
   `snapmirror show`

Verwandte Informationen

- "snapmirror create"
- "snapmirror delete"
- "snapmirror failover show"
- "SnapMirror Resynchronisierung"
- "snapmirror show"

ONTAP SnapMirror Active Sync-Vorgänge überwachen

Sie können die folgenden SnapMirror active sync-Vorgänge überwachen, um den Zustand Ihrer SnapMirror active sync-Konfiguration sicherzustellen:

- ONTAP Mediator
- Geplante Failover-Vorgänge

- Automatische ungeplante Failover Operationen
- SnapMirror Active Sync-Verfügbarkeit

> Ab ONTAP 9.15.1 zeigt der System Manager den Status Ihrer SnapMirror Active Sync-Beziehung von beiden Clustern aus an. Auch der Status des ONTAP Mediators kann im System Manager von beiden Clustern aus überwacht werden.

ONTAP Mediator

Während des normalen Betriebs sollte der ONTAP Mediator den Status „Verbunden“ aufweisen. Befindet er sich in einem anderen Status, kann dies auf eine Fehlerbedingung hinweisen. Die "Meldungen des Event Management System (EMS)" kann überprüft werden, um den Fehler und geeignete Korrekturmaßnahmen zu bestimmen.

Geplante Failover-Vorgänge

Status und Fortschritt eines geplanten Failover-Vorgangs lassen sich mit dem `snapmirror failover show` Befehl überwachen. Beispielsweise in einer SAN-Konfiguration:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Sobald der Failover-Vorgang abgeschlossen ist, kann der SnapMirror-Schutzstatus vom neuen Ziel-Cluster aus überwacht werden. Beispiel:

```
ClusterA::> snapmirror show
```

In der "EMS-Referenz" finden sich Informationen zu Ereignismeldungen und Korrekturmaßnahmen.

Automatische ungeplante Failover Operationen

Während eines ungeplanten automatischen Failovers kann der Status des Vorgangs mit dem `snapmirror failover show` Befehl überwacht werden.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

In der "EMS-Referenz" finden sich Informationen zu Ereignismeldungen und Korrekturmaßnahmen.

SnapMirror Active Sync-Verfügbarkeit

Die Verfügbarkeit der SnapMirror active sync-Beziehung lässt sich mithilfe einer Reihe von Befehlen entweder auf dem primären Cluster, dem sekundären Cluster oder auf beiden prüfen.

Zu den verwendeten Befehlen gehören der `snapmirror mediator show` Befehl auf dem primären und sekundären Cluster, um den Verbindungs- und Quorumstatus zu überprüfen, der `snapmirror show` Befehl und der `volume show` Befehl. Beispiel:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                    Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                     No-consensus
```

Verwandte Informationen

- "snapmirror failover show"

- "SnapMirror Failover Start"
- "snapmirror mediator show"

Hinzufügen oder Entfernen von Volumes in einer ONTAP Konsistenzgruppe

Wenn sich die Anforderungen Ihrer Anwendungs-Workloads ändern, kann es erforderlich sein, Volumes zu einer Konsistenzgruppe hinzuzufügen oder daraus zu entfernen, um die Geschäftskontinuität in Ihrer SAN-Konfiguration sicherzustellen. Der Prozess zum Hinzufügen und Entfernen von Volumes in einer aktiven SnapMirror active sync-Beziehung hängt von der verwendeten ONTAP-Version ab.

In den meisten Fällen handelt es sich um einen disruptiven Prozess, bei dem die SnapMirror Beziehung gelöscht, die Konsistenzgruppe geändert und anschließend der Schutz wieder aufgenommen werden muss. Ab ONTAP 9.13.1 ist das Hinzufügen von Volumes zu einer Konsistenzgruppe mit einer aktiven SnapMirror Beziehung ein nicht-disruptiver Vorgang.

Über diese Aufgabe

- In ONTAP 9.9.1 können Volumes mithilfe der ONTAP CLI zu einer Konsistenzgruppe hinzugefügt oder daraus entfernt werden.
- Ab ONTAP 9.10.1 wird empfohlen, "Konsistenzgruppen" über den System Manager oder mit der ONTAP REST API zu verwalten.

  Wenn Sie die Zusammensetzung der Konsistenzgruppe durch Hinzufügen oder Entfernen eines Volumes ändern möchten, muss zunächst die ursprüngliche Beziehung gelöscht und anschließend die Konsistenzgruppe mit der neuen Zusammensetzung erneut erstellt werden.

- Ab ONTAP 9.13.1 ist es möglich, Volumes ohne Unterbrechung zu einer Konsistenzgruppe mit einer aktiven SnapMirror Beziehung vom Quell- oder Zielsystem hinzuzufügen. Diese Aktion wird mit dem NVMe-Protokoll nicht unterstützt.

  Das Entfernen von Volumes ist ein störender Vorgang. Die SnapMirror Beziehung muss gelöscht werden, bevor Volumes entfernt werden.

ONTAP 9.9.1-9.13.0

Bevor Sie beginnen

- Die Konsistenzgruppe kann nicht geändert werden, solange sie sich im `InSync` Zustand befindet.
- Das Zielvolume sollte vom Typ DP sein.
- Das neue Volume, das zur Erweiterung der Konsistenzgruppe hinzugefügt wird, muss über ein Paar gemeinsamer Snapshots zwischen dem Quell- und dem Zielvolume verfügen.

Schritte

Die Beispiele werden in zwei Volumenzuordnungen gezeigt: `vol_src1` ←→ `vol_dst1` und `vol_src2` ←→ `vol_dst2`, in einer Konsistenzgruppenbeziehung zwischen den Endpunkten `vs1_src:/cg/cg_src` und `vs1_dst:/cg/cg_dst`.

1. Auf den Quell- und Ziel-Clustern lässt sich mit dem Befehl überprüfen, ob ein gemeinsamer Snapshot zwischen den Quell- und Ziel-Clustern vorhanden ist. `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
snapmirror*

destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
snapmirror*
```

2. Falls kein gemeinsamer Snapshot existiert, eine FlexVol SnapMirror Beziehung erstellen und initialisieren:

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3
-destination-path vs1_dst:vol_dst3
```

3. Die Konsistenzgruppenbeziehung löschen:

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

4. Die Quell-SnapMirror Beziehung aufheben und die gemeinsamen Snapshots beibehalten:

```
source::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol_dst3
```

5. Die LUNs aufheben und die bestehende Konsistenzgruppenbeziehung löschen:

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
<igroup_name>
```

> Die Ziel-LUNs sind nicht zugeordnet, während die LUNs auf der primären Kopie weiterhin die Host-I/O bedienen.

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
-relationship-info-only true
```

6. **Wenn Sie ONTAP 9.10.1 bis 9.13.0 verwenden,** die Konsistenzgruppe auf der Quelle mit der korrekten Zusammensetzung löschen und neu erstellen. Die Schritte in "Eine Konsistenzgruppe löschen" und dann "Eine einzelne Konsistenzgruppe konfigurieren" sind zu befolgen. In ONTAP 9.10.1 und höher müssen die Lösch- und Erstellungsvorgänge im System Manager oder mit der ONTAP REST API durchgeführt werden; es gibt kein CLI-Verfahren.

   Wenn Sie ONTAP 9.9.1 verwenden, zum nächsten Schritt wechseln.

7. Die neue Konsistenzgruppe wird auf dem Ziel mit der neuen Zusammensetzung erstellt:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Die Zero-RTO-Konsistenzgruppe-Beziehung wird resynchronisiert, um sicherzustellen, dass sie synchron ist:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Ordnen Sie die in Schritt 5 aufgehobenen LUNs wieder zu:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Die Host-LUN-I/O-Pfade werden erneut gescannt, um alle Pfade zu den LUNs wiederherzustellen.

ONTAP 9.13.1 und höher

Ab ONTAP 9.13.1 ist es möglich, Volumes unterbrechungsfrei zu einer Konsistenzgruppe mit einer aktiven SnapMirror active sync Beziehung hinzuzufügen. SnapMirror active sync unterstützt das Hinzufügen von Volumes sowohl vom Quell- als auch vom Zielsystem.

> Von ONTAP 9.8 bis ONTAP 9.14.1 wird SnapMirror active sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

Weitere Informationen zum Hinzufügen von Volumes aus der Konsistenzgruppe finden Sie unter Eine Konsistenzgruppe ändern.

Ein Volume aus dem Ziel-Cluster hinzufügen

1. Im Ziel-Cluster **Schutz** > **Beziehungen** auswählen.
2. Suchen Sie die SnapMirror Konfiguration, zu der Sie Volumes hinzufügen möchten. Wählen Sie ⋮ und anschließend **Erweitern**.
3. Wählen Sie die Volumenbeziehungen aus, deren Volumes zur Konsistenzgruppe hinzugefügt werden sollen
4. **Erweitern** auswählen.

Verwandte Informationen

- "snapmirror delete"
- "snapmirror initialize"
- "SnapMirror Release"
- "SnapMirror Resynchronisierung"

Upgrade und Rücksetzung mit ONTAP SnapMirror active sync

SnapMirror active sync wird ab ONTAP 9.9.1 unterstützt. Das Aktualisieren und Zurücksetzen Ihres ONTAP Clusters oder Ihrer Controller hat Auswirkungen auf Ihre SnapMirror active sync Beziehungen, abhängig von der ONTAP Version, auf die Sie aktualisieren oder zurücksetzen.

Cluster aktualisieren

Ab ONTAP 9.16.1 unterstützt SnapMirror Active Sync Vier-Knoten-Cluster in symmetrischen Aktiv/Aktiv-Konfigurationen. Mit dem Vier-Knoten-Cluster ist ein Upgrade von Controllern und Speicher möglich.

Bevor Sie beginnen

- Lesen Sie die "Anforderungen für Vier-Knoten-Cluster".
- Während des Technologieaktualisierung-Prozesses können asymmetrische Konfigurationen erstellt werden; nach Abschluss der Aktualisierung sollte jedoch zu einer symmetrischen Konfiguration zurückgekehrt werden.

- Diese Anweisungen gelten für eine bestehende Vier-Knoten-Konfiguration mit 50 oder weniger Konsistenzgruppen und 400 oder weniger Volume-Endpunkten.

Schritte

1. "Alle SnapMirror active sync Volumes auf ein einziges Hochverfügbarkeitspaar (HA) verschieben".
2. "Nicht verwendete Knoten aus dem Cluster entfernen".
3. "Die neuen Knoten werden dem Cluster hinzugefügt.".
4. "Alle Volumes verschieben" in die neuen Knoten.
5. "Nicht verwendete Knoten aus dem Cluster entfernen"dann werden sie "mit den neuen Knoten" ersetzt.

ONTAP mit SnapMirror Active Sync aktualisieren

Um SnapMirror active sync zu verwenden, müssen auf allen Knoten der Quell- und Ziel-Cluster ONTAP 9.9.1 oder höher ausgeführt werden.

Bei der Aktualisierung von ONTAP mit Aktiv/Aktiv-SnapMirror active sync-Beziehungen empfiehlt sich die Verwendung von automatisiertes unterbrechungsfreies Upgrade (ANDU). Durch die Nutzung von ANDU bleibt gewährleistet, dass Ihre Aktiv/Aktiv-SnapMirror active sync-Beziehungen während des Upgrade-Prozesses synchron und fehlerfrei sind.

Für SnapMirror Aktiv/Aktiv-Synchronisierungsbereitstellungen sind keine Konfigurationsschritte zur Vorbereitung auf ONTAP Upgrades erforderlich. Es wird jedoch empfohlen, vor und nach dem Upgrade Folgendes zu überprüfen:

- SnapMirror Active Sync-Beziehungen sind synchron.
- Im Ereignisprotokoll sind keine Fehler im Zusammenhang mit SnapMirror verzeichnet.
- Der Mediator ist online und in beiden Clustern funktionsfähig.
- Alle Hosts können alle Pfade ordnungsgemäß sehen, um LUNs zu schützen.

> Wenn Cluster von ONTAP 9.9.1 oder 9.9.1 auf ONTAP 9.10.1 und höher aktualisiert werden, erstellt ONTAP neue Konsistenzgruppen auf sowohl Quell- als auch Ziel-Clustern für SnapMirror active sync Beziehungen, die mit System Manager konfiguriert werden können.

> Die `snapmirror quiesce` und `snampirror resume` Befehle werden mit SnapMirror active sync nicht unterstützt.

Zurück zu ONTAP 9.9.1 von ONTAP 9.10.1

Um Beziehungen von 9.10.1 auf 9.9.1 zurückzusetzen, müssen SnapMirror active sync-Beziehungen gelöscht werden, gefolgt von der 9.10.1 Konsistenzgruppeninstanz. Konsistenzgruppen mit einer aktiven SnapMirror active sync-Beziehung können nicht gelöscht werden. Alle FlexVol Volumes, die auf 9.10.1 aktualisiert wurden und zuvor in 9.9.1 oder früher mit einem anderen Smart Container oder einer Enterprise App verknüpft waren, sind nach dem Zurücksetzen nicht mehr verknüpft. Das Löschen von Konsistenzgruppen löscht weder die zugehörigen Volumes noch die Volume-Granularitäts-Snapshots. Weitere Informationen zu dieser Aufgabe in ONTAP 9.10.1 und höher enthält "Eine Konsistenzgruppe löschen".

Zurücksetzen von ONTAP 9.9.1

> SnapMirror active sync wird bei gemischten ONTAP Clustern, die Versionen vor ONTAP 9.9.1 enthalten, nicht unterstützt.

Beim Zurücksetzen von ONTAP 9.9.1 auf eine frühere Version von ONTAP ist Folgendes zu beachten:

- Wenn der Cluster ein SnapMirror Active Sync-Ziel hostet, ist ein Downgrade auf ONTAP 9.8 oder früher erst zulässig, wenn die Beziehung getrennt und gelöscht wurde.
- Wenn der Cluster eine SnapMirror Aktiv-Sync-Quelle hostet, ist ein Zurücksetzen auf ONTAP 9.8 oder früher erst zulässig, nachdem die Beziehung freigegeben wurde.
- Alle vom Benutzer erstellten benutzerdefinierten SnapMirror Active Sync-Richtlinien müssen gelöscht werden, bevor auf ONTAP 9.8 oder eine frühere Version zurückgegriffen wird.

Um diese Anforderungen zu erfüllen, siehe "Entfernen einer SnapMirror Active Sync Konfiguration".

Schritte

1. Bestätigen Sie Ihre Bereitschaft zum Zurücksetzen, indem Sie den folgenden Befehl von einem der Cluster in der SnapMirror active sync-Beziehung eingeben:

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   Die folgende Beispielausgabe zeigt einen Cluster, der nicht bereit ist, zurückgesetzt zu werden, mit Anweisungen zur Bereinigung.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
      wait for the Relationship Status to be Quiesced.
       Command to quiesce a SnapMirror relationship: snapmirror quiesce
       Command to abort transfers on a SnapMirror relationship: snapmirror
   ```

```
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. Sobald Sie die Anforderungen der Rücksetzprüfung erfüllt haben, siehe "ONTAP zurücksetzen".

Verwandte Informationen

- "Netzwerkschnittstelle"
- "snapmirror break"
- "snapmirror policy delete"
- "snapmirror policy show"
- "snapmirror quiesce"
- "snapmirror show"

Entfernen einer ONTAP SnapMirror Active Sync-Konfiguration

Wenn kein Zero-RTO-SnapMirror-synchroner Schutz mehr erforderlich ist, kann die SnapMirror active sync Beziehung gelöscht werden.

Zuordnung der LUNs auf dem Ziel-Cluster aufheben

Über diese Aufgabe

- Bevor die SnapMirror active sync SAN-Beziehung gelöscht wird, müssen alle LUNs im Ziel-Cluster aus der Zuordnung entfernt werden.
- Nachdem die LUNs entfernt und der Host neu gescannt wurden, benachrichtigt das SCSI-Ziel die Hosts, dass sich das LUN-Inventar geändert hat. Die vorhandenen LUNs auf den Zero RTO sekundären Volumes ändern ihre Identität, nachdem die Zero RTO Beziehung gelöscht wurde. Die Hosts erkennen die sekundären Volume LUNs als neue LUNs, die keine Beziehung zu den Quell-Volume LUNs haben.
- Die sekundären Volumes bleiben auch nach dem Löschen der Beziehung DP-Volumes. Mit dem `snapmirror break` Befehl ist eine Umwandlung in lesen/schreiben möglich.
- Das Löschen der Beziehung ist im Failover-Zustand nicht zulässig, wenn die Beziehung nicht umgekehrt ist.

Schritte

Vor dem Löschen einer SnapMirror active sync SAN Beziehung müssen Sie auf dem Ziel-Cluster die Zuordnung aller LUNs aufheben, die Teil der Beziehung sind. Vor dem Löschen einer asymmetrischen SAN-Konfiguration sind die folgenden Schritte erforderlich.

1. Wenn eine Ziel-LUN über eine replizierte Initiatorgruppe zugeordnet ist, müssen Sie die Replikation der Initiatorgruppe im Quell-Cluster prüfen und entfernen, bevor Sie die LUN-Zuordnung im Ziel-Cluster löschen können:

   ```
   SiteB::> igroup show -igroup <igroup_name> -vserver <vserver_name> -fields
   replication-peer
   ```

2. Wenn die Initiatorgruppe repliziert wird, ist die Replikations-Peer-Zuordnung aus dem Quell-Cluster zu entfernen:

   ```
   SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -replication
   -peer "-"
   ```

3. Überprüfung, ob die Initiatorgruppe nicht mehr repliziert wird:

   ```
   SiteB::> igroup show -igroup <igroup_name> -vserver <vserver_name> -fields
   replication-peer
   ```

4. Löschen der LUN-Zuordnung auf der Zielseite:

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
   <lun_path>
   ```

5. Sind der Initiatorgruppe keine weiteren LUNs zugeordnet, kann die Initiatorgruppe gelöscht werden:

   ```
   SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
   ```

Löschen der SnapMirror active sync SAN Beziehung

Nach dem Aufheben der Zuordnung der LUNs wird die SnapMirror Active Sync Beziehung gelöscht.

Schritte

1. Vom sekundären Cluster aus die SnapMirror Aktiv Sync Konsistenzgruppenbeziehung zwischen Quell-Endpunkt und Ziel-Endpunkt entfernen:

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. Vom primären Cluster aus die Konsistenzgruppenbeziehung und die für die Beziehung erstellten Snapshots freigeben:

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Ein erneuter Host-Scan aktualisiert das LUN-Inventar.
4. Ab ONTAP 9.10.1 wird beim Löschen der SnapMirror Beziehung die Konsistenzgruppe nicht gelöscht. Zum Löschen der Konsistenzgruppe ist die Verwendung von System Manager oder der ONTAP REST API erforderlich. Siehe Eine Konsistenzgruppe löschen für weitere Informationen.

Symmetrische Aktiv/Aktiv-Konfiguration für iSCSI oder FC entfernen

Sie können eine symmetrische Konfiguration mithilfe von System Manager oder der ONTAP CLI entfernen. In beiden Schnittstellen sind unterschiedliche Schritte für einheitliche und nicht einheitliche Konfigurationen erforderlich.

System Manager

Schritte für eine einheitliche Konfiguration

1. Am primären Standort die Remote-Hosts aus der Initiatorgruppe entfernen und die Replikation beenden.
   a. Zu **Hosts** > **SAN Initiatorgruppen** navigieren.
   b. Die zu ändernde Initiatorgruppe auswählen und anschließend **Bearbeiten** wählen.
   c. Den Remote-Initiator entfernen und die Initiatorgruppe-Replikation beenden. **Speichern** auswählen.
2. Am sekundären Standort die replizierte Beziehung durch Aufheben der Zuordnung der LUNs löschen.
   a. Zu **Hosts** > **SAN Initiatorgruppen** navigieren.
   b. Die Initiatorgruppe mit der SnapMirror Beziehung auswählen und anschließend **Löschen** wählen.
   c. Im Dialogfeld das Kontrollkästchen **Zugehörige LUNs aufheben** auswählen und dann **Löschen**.
   d. Zu **Schutz** > **Beziehungen** navigieren.
   e. Die SnapMirror Aktiv-Sync-Beziehung auswählen und anschließend **Release** verwenden, um die Beziehungen zu löschen.

Schritte für eine nicht einheitliche Konfiguration

1. Am primären Standort die Remote-Hosts aus der Initiatorgruppe entfernen und die Replikation beenden.
   a. Zu **Hosts** > **SAN Initiatorgruppen** navigieren.
   b. Die zu ändernde Initiatorgruppe auswählen und anschließend **Bearbeiten** wählen.
   c. Den Remote-Initiator entfernen und die Initiatorgruppe-Replikation beenden. **Speichern** auswählen.
2. Am sekundären Standort die SnapMirror active sync Beziehung entfernen.
   a. Zu **Schutz** > **Beziehungen** navigieren.

b. Die SnapMirror Aktiv-Sync-Beziehung auswählen und anschließend **Release** verwenden, um die Beziehungen zu löschen.

CLI

Schritte für eine einheitliche Konfiguration

1. Alle VM-Workloads werden auf den Host verschoben, der sich lokal zum Quell-Cluster von SnapMirror active sync befindet.
2. Auf dem Quell-Cluster die Initiatoren aus der Initiatorgruppe entfernen und die Initiatorgruppe-Konfiguration ändern, um die Initiatorgruppe-Replikation zu beenden.

   ```
   SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
   <os_type> -initiator <host2>
   SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
   <os_type> -replication-peer "-"
   ```

3. Am sekundären Standort die LUN-Zuordnung löschen und die Initiatorgruppen-Konfiguration entfernen:

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
   <>
   SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
   ```

4. Am sekundären Standort die SnapMirror active sync Beziehung löschen.

   ```
   SiteB::> snapmirror delete -destination-path destination_path
   ```

5. Am primären Standort die SnapMirror Active Sync-Beziehung vom primären Standort aufheben.

   ```
   SiteA::> snapmirror release -destination-path <destination_path>
   ```

6. Die Pfade werden erneut ermittelt, um zu überprüfen, dass dem Host nur der lokale Pfad zur Verfügung steht.

Schritte für eine nicht einheitliche Konfiguration

1. Alle VM-Workloads werden auf den Host verschoben, der sich lokal zum Quell-Cluster von SnapMirror active sync befindet.
2. Auf dem Quell-Cluster die Initiatoren aus der Initiatorgruppe entfernen.

   ```
   SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
   <host2>
   ```

3. Am sekundären Standort die LUN-Zuordnung löschen und die Initiatorgruppen-Konfiguration entfernen:

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
   <>
   SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
   ```

4. Am sekundären Standort die SnapMirror active sync Beziehung löschen.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. Am primären Standort die SnapMirror Active Sync-Beziehung vom primären Standort aufheben.

   ```
   SiteA::> snapmirror release -destination-path <destination_path>
   ```

6. Die Pfade werden erneut ermittelt, um zu überprüfen, dass dem Host nur der lokale Pfad zur Verfügung steht.

Entfernen einer symmetrischen NVMe Aktiv/Aktiv-Konfiguration

System Manager

Schritte

1. Im Quell-Cluster zu **Schutz > Replikation** navigieren.
2. Suchen Sie die Beziehung, die entfernt werden soll, wählen Sie ⋮ und wählen Sie **Löschen** aus.
3. Im Fenster **Replikationskonfiguration löschen** die Option **Quell-Volume-Basis-Snapshots freigeben.** auswählen und **Löschen** wählen.

CLI

1. Vom Ziel-Cluster aus die SnapMirror Active Sync-Beziehung löschen.

   ```
   snapmirror delete -destination-path <destination_path> -unmap-namespace
   true
   ```

   Beispiel:

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   Das Subsystem und seine Namensräume werden aus dem sekundären Cluster entfernt.

2. Vom Quell-Cluster die SnapMirror Active Sync-Beziehung vom primären Standort freigeben.

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

   Beispiel:

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. Die Pfade werden erneut ermittelt, um zu überprüfen, dass dem Host nur der lokale Pfad zur Verfügung steht.

Entfernen einer NAS-Konfiguration

System Manager

Schritte

1. Im Quell-Cluster zu **Schutz > Replikation** navigieren.

2. Suchen Sie die Beziehung, die entfernt werden soll, wählen Sie ⋮ und wählen Sie **Löschen** aus.
3. Im Fenster **Replikationskonfiguration löschen** die Option **Basis-Snapshots der Quell-Speicher-VM freigeben** aktivieren und **Löschen** auswählen.

CLI

1. Vom Ziel-Cluster aus die SnapMirror Active Sync-Beziehung löschen.

   `snapmirror delete -destination-path <destination_path>`

   Beispiel:

   ```
   DST::> snapmirror delete -destination-path vs_b:
   ```

   Die SVM und ihre Volumes werden aus dem sekundären Cluster entfernt.

2. Vom Quell-Cluster die SnapMirror Active Sync-Beziehung vom primären Standort freigeben.

   `snapmirror release -destination-path <destination_path>`

   Beispiel:

   ```
   SRC::> snapmirror release -destination-path vs_b:
   ```

3. Die Pfade werden erneut ermittelt, um zu überprüfen, dass dem Host nur der lokale Pfad zur Verfügung steht.

Verwandte Informationen

- "snapmirror break"
- "snapmirror delete"
- "SnapMirror Release"

ONTAP Mediator oder ONTAP Cloud Mediator entfernen

Wenn eine bestehende ONTAP Mediator oder ONTAP Cloud Mediator Konfiguration aus den ONTAP Clustern entfernt werden soll, ist dies mit dem `snapmirror mediator remove` Befehl möglich. Es kann jeweils nur ein Typ von Mediator verwendet werden, daher muss eine Instanz entfernt werden, bevor die andere installiert wird.

Schritte

ONTAP Mediator oder ONTAP Cloud Mediator kann entfernt werden, indem einer der folgenden Schritte abgeschlossen wird.

ONTAP Mediator

1. ONTAP Mediator entfernen:

   `snapmirror mediator remove -mediator-address <address> -peer-cluster`

<peerClusterName>

Beispiel:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer
-cluster cluster_xyz
```

ONTAP Cloud Mediator

1. ONTAP Cloud Mediator entfernen:

   `snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud`

   Beispiel:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Verwandte Informationen

- "SnapMirror Mediator entfernen"

Fehlerbehebung

ONTAP SnapMirror Löschvorgang schlägt im Übernahmezustand fehl

Die folgenden Informationen sind relevant, wenn der `snapmirror delete` Befehl fehlschlägt, wenn sich eine SnapMirror active sync Konsistenzgruppe Beziehung im Übernahmezustand befindet.

Problem:

Wenn ONTAP 9.9.1 auf einem Cluster installiert ist, schlägt die Ausführung des `snapmirror delete` Befehls fehl, wenn sich eine SnapMirror Aktiv Sync Konsistenzgruppenbeziehung im Übernahmezustand befindet.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Lösung

Wenn sich die Knoten in einer SnapMirror Aktiv Sync-Beziehung im Übernahmezustand befinden, ist der SnapMirror Lösch- und Freigabevorgang mit der Option "-force" auf true auszuführen.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
```

```
          Consistency Group might not be made writable, deletable, or
modifiable
          after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Verwandte Informationen

- "snapmirror delete"

Fehler beim Erstellen einer ONTAP SnapMirror Beziehung und beim Initialisieren der Konsistenzgruppe

Die folgenden Informationen sind relevant, wenn die Erstellung einer SnapMirror Beziehung und die Initialisierung einer Konsistenzgruppe fehlschlagen.

Problem:

Erstellung der SnapMirror Beziehung und Initialisierung der Konsistenzgruppe schlägt fehl.

Lösung:

Stellen Sie sicher, dass Sie die maximale Anzahl an Konsistenzgruppen pro Cluster nicht überschritten haben. Die Grenzwerte für Konsistenzgruppen in SnapMirror active sync sind plattformunabhängig und unterscheiden sich je nach Version von ONTAP. Siehe "Objektgrenzen" für Hinweise, die speziell für Ihre ONTAP Version gelten.

Fehler:

Wenn die Konsistenzgruppe beim Initialisieren hängen bleibt, kann der Status der Konsistenzgruppen-Initialisierungen mit der ONTAP REST API, dem System Manager oder dem Befehl `sn show -expand` überprüft werden.

Von ONTAP 9.8 bis ONTAP 9.14.1 wird SnapMirror active sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

Lösung:

Wenn die Initialisierung von Konsistenzgruppen fehlschlägt, sollte die SnapMirror active sync Beziehung entfernt, die Konsistenzgruppe gelöscht und anschließend die Beziehung neu erstellt und initialisiert werden. Dieser Ablauf unterscheidet sich je nach verwendeter ONTAP-Version.

Wenn Sie ONTAP 9.9.1 verwenden	Wenn Sie ONTAP 9.10.1 oder höher verwenden
1. "Die SnapMirror Active Sync-Konfiguration entfernen" 2. "Eine Konsistenzgruppenbeziehung erstellen und anschließend die Konsistenzgruppenbeziehung initialisieren"	1. Unter **Schutz > Beziehungen** befindet sich die SnapMirror Aktiv/Aktiv-Beziehung in der Konsistenzgruppe. Mit ⋮ und anschließend **Löschen** wird die SnapMirror Aktiv/Aktiv-Beziehung entfernt. 2. "Konsistenzgruppe löschen" 3. "Die Konsistenzgruppe konfigurieren"

Geplantes ONTAP Cluster Failover fehlgeschlagen

Die folgenden Informationen sind relevant, falls die geplante Failover-Operation fehlschlägt.

Problem:

Nach Ausführung des `snapmirror failover start` Befehls wird in der Ausgabe des `snapmirror failover show` Befehls eine Meldung angezeigt, die darauf hinweist, dass ein unterbrechungsfreier Vorgang im Gange ist.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                              08:35:04
08:35:04
```

Ursache:

Ein geplanter Failover kann nicht gestartet werden, wenn ein unterbrechungsfreier Vorgang im Gange ist, einschließlich Volume Move, Aggregat-Relocation und Storage Failover.

Lösung:

Warten Sie, bis der unterbrechungsfreie Vorgang abgeschlossen ist, und versuchen Sie den Failover-Vorgang erneut.

Verwandte Informationen

- "snapmirror failover show"
- "SnapMirror Failover Start"

ONTAP Mediator oder ONTAP Cloud Mediator nicht erreichbar oder Mediator-Quorumstatus ist falsch

Die folgenden Informationen gelten, wenn der ONTAP Mediator oder ONTAP Cloud Mediator nicht erreichbar ist oder der Quorumstatus des Mediators auf „false“ steht.

Problem:

Nach Ausführung des `snapmirror failover start` Befehls wird in der Ausgabe für den `snapmirror failover show` Befehl eine Meldung angezeigt, die darauf hinweist, dass entweder der ONTAP Mediator oder ONTAP Cloud Mediator nicht konfiguriert ist.

Siehe "Den ONTAP Mediator und die Cluster für SnapMirror active sync konfigurieren" oder "Der ONTAP Cloud Mediator für SnapMirror Aktiv-Sync wird konfiguriert".

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
```

```
-------- ---------- -------- -------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Ursache:

Mediator ist nicht konfiguriert oder es bestehen Probleme mit der Netzwerkverbindung.

Lösung:

Wenn der ONTAP Mediator nicht konfiguriert ist, muss der ONTAP Mediator konfiguriert werden, bevor eine SnapMirror active sync-Beziehung hergestellt werden kann. Etwaige Netzwerkverbindungsprobleme beheben. Sicherstellen, dass der Mediator verbunden ist und der Quorum-Status sowohl auf der Quell- als auch auf der Zielseite mit dem Befehl snapmirror mediator show auf true steht. Weitere Informationen finden sich unter "Den ONTAP Mediator konfigurieren".

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Verwandte Informationen

- "snapmirror failover show"
- "SnapMirror Failover Start"
- "snapmirror mediator show"

ONTAP Cloud Mediator ist erreichbar, reagiert aber langsam

Die folgenden Informationen sind relevant, wenn der ONTAP Cloud Mediator mit einer Fehlermeldung ausfällt, die besagt, dass die Ping-Latenz höher als die empfohlene Latenz ist.

Problem:

System Manager: Der Cloud Mediator Service ist erreichbar, reagiert aber langsam.

CLI: Der `mediator add` Befehl schlägt mit dem Fehler fehl:
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms which is higher than twice the recommended latency of 200 ms.`

Ursache:

Die Cluster befinden sich möglicherweise nicht in unmittelbarer Nähe der NetApp Console Cloud oder es bestehen Engpässe im Netzwerkpfad.

Lösung:

- Den geografischen Standort und die Nähe zur NetApp Console Cloud (US East) prüfen.
- Netzwerkpfad optimieren oder Engpässe adressieren.

- Die Round-Trip-Time (RTT) kann mit Netzwerktools gemessen und die Latenz auf die empfohlenen Grenzwerte reduziert werden.
- Ein HTTP-Proxy kann zur Leistungsverbesserung beitragen.

Siehe "Den ONTAP Cloud Mediator und die Cluster für SnapMirror Active Sync konfigurieren".

Automatisches ungeplantes Failover wird an Standort B nicht ausgelöst.

Die folgenden Informationen gelten, wenn ein Ausfall an Standort A keinen ungeplanten Failover an Standort B auslöst.

Problem:

Ein Ausfall an Standort A löst keinen ungeplanten Failover an Standort B aus.

Mögliche Ursache Nr. 1:

Der ONTAP Mediator oder der ONTAP Cloud Mediator ist nicht konfiguriert. Um festzustellen, ob dies die Ursache ist, kann der `snapmirror mediator show` Befehl auf dem Cluster von Standort B ausgeführt werden.

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

Dieses Beispiel zeigt, dass der Mediator auf Standort B nicht konfiguriert ist.

Lösung:

Es muss sichergestellt sein, dass der Mediator auf beiden Clustern konfiguriert ist, der Status auf „Verbunden“ steht und das Quorum auf „True“ gesetzt ist.

Mögliche Ursache Nr. 2:

SnapMirror Konsistenzgruppe ist nicht synchron. Zur Feststellung, ob dies die Ursache ist, kann das Ereignisprotokoll eingesehen werden, um zu prüfen, ob die Konsistenzgruppe zum Zeitpunkt des Ausfalls von Site A synchron war.

```
cluster::> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Lösung:

Die folgenden Schritte sind erforderlich, um ein erzwungenes Failover auf Standort B durchzuführen.

1. Alle LUNs, die zur Konsistenzgruppe gehören, vom Standort B unzuordnen.
2. Die SnapMirror Konsistenzgruppenbeziehung wird mit der `force` Option gelöscht.
3. Den `snapmirror break` Befehl auf den Konsistenzgruppen-Bestandteilen ausführen, um Volumes von DP auf R/W zu konvertieren und I/O von Site B zu ermöglichen.
4. Die Knoten von Standort A werden gestartet, um eine Zero-RTO-Beziehung von Standort B zu Standort A zu erstellen.
5. Die Konsistenzgruppe wird mit `relationship-info-only` auf Standort A freigegeben, um einen gemeinsamen Snapshot beizubehalten und die zugehörigen LUNs der Konsistenzgruppe zu entkoppeln.
6. Die Volumes am Standort A werden von R/W auf DP konvertiert, indem auf Volume-Ebene eine Beziehung mithilfe der Sync-Richtlinie oder der Async-Richtlinie eingerichtet wird.
7. Den Befehl `snapmirror resync` ausgeben, um die Beziehungen zu synchronisieren.
8. Die SnapMirror Beziehungen mit der Sync-Richtlinie auf Standort A löschen.
9. Die SnapMirror Beziehungen mit Sync-Richtlinie werden mithilfe von `relationship-info-only true` auf Standort B freigegeben.
10. Eine Konsistenzgruppen-Beziehung von Standort B zu Standort A erstellen.
11. Eine Konsistenzgruppe-Resynchronisierung von Standort A aus durchführen und anschließend überprüfen, ob die Konsistenzgruppe synchron ist.
12. Die Host-LUN-I/O-Pfade werden erneut gescannt, um alle Pfade zu den LUNs wiederherzustellen.

Verwandte Informationen

- "snapmirror break"
- "snapmirror mediator show"
- "SnapMirror Resynchronisierung"

Verbindung zwischen Standort B und ONTAP Mediator unterbrochen und Standort A ausgefallen

Zur Überprüfung der Verbindung des ONTAP Mediator oder des ONTAP Cloud Mediator kann der `snapmirror mediator show` Befehl verwendet werden. Wenn der Verbindungsstatus „Nicht erreichbar“ ist und Site B Site A nicht erreichen kann, erscheint eine ähnliche Ausgabe wie unten gezeigt. In der Lösung sind die Schritte zur Wiederherstellung der Verbindung aufgeführt.

Beispiel:

Mit der ONTAP Cloud Mediator-Ausgabe des Befehls `snapmirror mediator show`:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
---------------- ---------------- ----------------- ------------- -------
0.0.0.0          C1_cluster       unreachable       true          cloud
```

Verwendung der ONTAP Mediator-Ausgabe mit dem Befehl `snapmirror mediator show`:

```
cluster::> snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Lösung

Ein Failover wird erzwungen, um die E/A von Standort B zu ermöglichen, und anschließend wird eine Zero-RTO-Beziehung von Standort B zu Standort A hergestellt. Die folgenden Schritte beschreiben das Vorgehen für ein erzwungenes Failover an Standort B.

1. Alle LUNs, die zur Konsistenzgruppe von Standort B gehören, ausbinden. Dies schlägt fehl, daher muss zunächst die Initiatorgruppe geändert werden, um die Replikations-Peer-SVM zu entfernen, und anschließend die LUN-Zuordnung gelöscht werden.

Beispiel:

```
C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
```

```
vs0        /vol/cg1_lun/lun_1                          igroup1       0
mixed
vs0        /vol/cg1_lun/lun_2                          igroup1       1
mixed
2 entries were displayed.

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_5 -igroup igroup1
Error: command failed: The peer cluster is unreachable and a SnapMirror
       Mediator is not configured. The configuration is locked for
replicated
       objects in this Vserver peer relationship on both clusters. The
only
       supported configuration change is to manually disable replication
on
       both sides of the relationship, after which configuration changes
are
       supported.
C1_cluster::> igroup modify -igroup igroup1 -replication-peer -

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_1 -igroup igroup1

C1_cluster::> lun mapping show
Vserver    Path                                        Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_2                          igroup1       1
mixed
1 entries were displayed.
```

1. Die SnapMirror Konsistenzgruppenbeziehung wird mit der Option „Erzwingen“ gelöscht.
2. Den SnapMirror break-Befehl (`snapmirror break -destination_path` *svm*`:_volume_` auf den Konsistenzgruppe-Teil-Volumes eingeben, um Volumes von DP auf RW umzuwandeln und I/O von Site B zu ermöglichen.

   Sie müssen den SnapMirror break-Befehl für jede Beziehung in der Konsistenzgruppe ausführen. Wenn die Konsistenzgruppe drei Volumes enthält, wird der Befehl für jedes Volume ausgeführt.

3. Die Knoten von Standort A werden gestartet, um eine Zero-RTO-Beziehung von Standort B zu Standort A zu erstellen.
4. Die Konsistenzgruppe mit der Option "relationship-info-only" auf Site A freigeben, um den gemeinsamen Snapshot beizubehalten und die zugehörigen LUNs der Konsistenzgruppe aufzuheben.
5. Die Volumes am Standort A werden von RW zu DP konvertiert, indem auf Volume-Ebene eine Beziehung mit entweder einer Sync-Policy oder einer Async-Policy eingerichtet wird.
6. Der `snapmirror resync`Befehl wird verwendet, um die Beziehungen zu synchronisieren.
7. Die SnapMirror-Beziehungen mit Sync-Richtlinie auf Standort A löschen.

8. Die SnapMirror-Beziehungen mit der Sync-Richtlinie auf Site B unter Verwendung von relationship-info-only true aufheben.
9. Eine Konsistenzgruppenbeziehung zwischen Standort B und Standort A erstellen.
10. Von dem Quell-Cluster aus die Konsistenzgruppe erneut synchronisieren. Überprüfen, ob der Status der Konsistenzgruppe synchron ist.
11. Die Host-LUN-I/O-Pfade werden erneut gescannt, sodass alle Pfade zu den LUNs wiederhergestellt werden.

Verwandte Informationen

- "snapmirror break"
- "snapmirror mediator show"
- "SnapMirror Resynchronisierung"
- "snapmirror show"

Verbindung zwischen Standort A und ONTAP Mediator unterbrochen und Standort B ausgefallen

Bei Verwendung von SnapMirror active sync kann die Verbindung zwischen dem ONTAP Mediator oder Ihren Peered-Clustern verloren gehen. Das Problem lässt sich diagnostizieren, indem der Verbindungs-, Verfügbarkeits- und Konsensstatus der verschiedenen Teile der SnapMirror active sync-Beziehung überprüft und anschließend die Verbindung gezielt wiederhergestellt wird.

Was überprüft werden sollte	CLI Befehl	Indikator
Mediator von Standort A	`snapmirror mediator show`	Der Verbindungsstatus wird angezeigt als `unreachable`
Standort B Konnektivität	`cluster peer show`	Die Verfügbarkeit wird angezeigt als `unavailable`
Konsensstatus des SnapMirror Aktiv Sync-Volumes	`volume show` *`volume_name`* `-fields smbc-consensus`	Das `sm-bc consensus`Feld zeigt `Awaiting-consensus`

Weitere Informationen zur Diagnose und Behebung dieses Problems sind in der "NetApp Knowledge Base: Verbindung zwischen Standort A und Mediator ausgefallen und Standort B ausgefallen bei Verwendung von SnapMirror active sync" zu finden.

Verwandte Informationen

- "cluster peer show"
- "snapmirror mediator show"

ONTAP SnapMirror Löschvorgang schlägt fehl, wenn auf dem Zielvolume eine Sperre eingerichtet ist

Die folgenden Informationen sind relevant, wenn der SnapMirror Löschvorgang fehlschlägt, weil auf einem der Ziel-Volumes eine Umleitungssperre gesetzt ist.

Problem:

SnapMirror Löschvorgang schlägt fehl, wenn für eines der Ziel-Volumes eine Umleitungssperre gesetzt ist.

Lösung

Die folgenden Vorgänge werden ausgeführt, um die Umleitung erneut zu versuchen und die Sperre vom Ziel-Volume zu entfernen.

- SnapMirror Resynchronisierung
- SnapMirror Aktualisierung

Die Volume-Verschiebungsoperation bleibt hängen, wenn der ONTAP Primärserver ausgefallen ist.

Die folgenden Informationen sind relevant, wenn ein Volume-Verschiebungsvorgang im Status „Cutover Deferred“ auf unbestimmte Zeit festhängt, weil der primäre Standort in einer SnapMirror active sync Beziehung ausgefallen ist.

Problem:

Ein Volume-Verschiebungsvorgang bleibt im Status „Aufgeschobene Umschaltung“ dauerhaft hängen, wenn der primäre Standort in einer SnapMirror active sync Beziehung ausgefallen ist. Wenn der primäre Standort ausgefallen ist, führt der sekundäre Standort ein automatisches ungeplantes Failover (AUFO) durch. Wenn ein Volume-Verschiebungsvorgang in Bearbeitung ist, wenn das AUFO ausgelöst wird, bleibt der Volume-Verschiebungsvorgang hängen.

Lösung:

Die festhängende Volume-Verschiebungsinstanz wird abgebrochen und der Volume-Verschiebungsvorgang neu gestartet.

ONTAP SnapMirror Freigabe schlägt fehl, wenn der Snapshot nicht gelöscht werden kann.

Die folgenden Informationen sind relevant, wenn der SnapMirror Freigabevorgang fehlschlägt, weil der Snapshot nicht gelöscht werden kann.

Problem:

Der SnapMirror Freigabevorgang schlägt fehl, wenn der Snapshot nicht gelöscht werden kann.

Lösung:

Der Snapshot enthält ein temporäres Tag. Mit dem `snapshot delete` Befehl und der `-ignore-owners` Option lässt sich der temporäre Snapshot entfernen.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Den `snapmirror release`Befehl erneut versuchen.

Verwandte Informationen

- "SnapMirror Release"

Der Referenz-Snapshot für die Volumenverschiebung wird als der neueste für die ONTAP SnapMirror Beziehung angezeigt.

Die folgenden Informationen gelten, wenn der Referenz-Snapshot der Volume-Verschiebung nach einer Volume-Verschiebung als der neueste für die SnapMirror Beziehung angezeigt wird.

Problem:

Nach der Durchführung einer Volume-Verschiebung auf einem Konsistenzgruppe-Volume kann der Referenz-

Snapshot der Volume-Verschiebung fälschlicherweise als der neueste für die SnapMirror Beziehung angezeigt werden.

Der neueste Snapshot kann mit folgendem Befehl angezeigt werden:

```
snapmirror show -fields newest-snapshot status -expand
```

Lösung:

Manuell eine `snapmirror resync`durchführen oder auf die nächste automatische Resynchronisierung nach Abschluss des Volume-Verschiebungsvorgangs warten.

Verwandte Informationen

- "SnapMirror Resynchronisierung"
- "snapmirror show"

Informationen zu ONTAP Mediator für MetroCluster IP und SnapMirror active sync

ONTAP Mediator unterstützt SnapMirror active sync und MetroCluster IP, indem ein persistenter und geschützter Speicher für Metadaten zur Hochverfügbarkeit (HA) bereitgestellt wird, eine synchrone Abfrage des Node-Systemstatus zur Unterstützung der Quorumbestimmung erfolgt und ein Ping-Proxy für die Controller-Verfügbarkeit bereitgestellt wird.

ONTAP Mediator läuft auf einem Linux-Host in einer dritten Ausfalldomäne, getrennt von Ihren ONTAP Clustern, und stellt dort einen persistenten, geschützten Speicher für HA-Metadaten bereit. ONTAP nutzt diesen Speicher zusammen mit der Systemstatusabfrage und den Ping Proxy Funktionen des Mediators, um SnapMirror Active Sync Beziehungen und MetroCluster IP Konfigurationen zu überwachen.

- ONTAP Mediator nutzt die Knotenverwaltungs-LIF und die Clusterverwaltungs-LIF, um über mehrere redundante Pfade mit jedem Cluster zu kommunizieren. Dadurch kann ONTAP zwischen einem vollständigen Standortausfall und dem Ausfall einer einzelnen InterSwitch Link (ISL) unterscheiden.
- Bei SnapMirror active sync behandelt ONTAP den Peer als nicht erreichbar, wenn ein Cluster die Verbindung sowohl zu seinem Peer als auch zu ONTAP Mediator verliert, und kann automatisch auf die verbleibende Kopie umschalten.
- In MetroCluster IP-Konfigurationen unterstützt ONTAP Mediator einen Mediator-gestützten automatischen ungeplanten Switchover (MAUSO), indem er Statusinformationen über die MetroCluster Knoten speichert und dabei hilft, im Fehlerfall die geeignete Vorgehensweise zu bestimmen.

Informationen zur Installation oder Aktualisierung der On-Premises Version von ONTAP Mediator finden Sie in der "ONTAP Mediator Dokumentation"

Informationen zum ONTAP Cloud Mediator, der ab ONTAP 9.17.1 verfügbar ist, bietet die "SnapMirror active sync Dokumentation".

Informationen zur MetroCluster IP-Standortverwaltung mit ONTAP System Manager

MetroCluster Konfigurationen spiegeln Daten und Konfigurationen zwischen zwei ONTAP

Clustern an unterschiedlichen Standorten synchron wider. Ab ONTAP 9.8 kann der System Manager als vereinfachte Oberfläche für die Verwaltung einer MetroCluster IP Konfiguration verwendet werden.

> Mit dem System Manager können MetroCluster-Operationen nur in einer MetroCluster IP-Konfiguration durchgeführt werden. In einer MetroCluster FC-Konfiguration ist die Verwaltung der einzelnen Knoten in Ihrer MetroCluster Konfiguration weiterhin mit dem System Manager möglich, jedoch können keine MetroCluster-spezifischen Operationen durchgeführt werden.

Typischerweise werden Cluster in einer MetroCluster Konfiguration an zwei geografisch getrennten Standorten eingerichtet und konfiguriert. Anschließend wird ein Peering zwischen den Clustern eingerichtet, sodass sie synchronisiert werden und Daten gemeinsam nutzen. Die beiden Cluster im Peering-Netzwerk bieten eine bidirektionale Notfallwiederherstellung (Disaster Recovery, DR), wobei jeder Cluster sowohl Quelle als auch Backup des anderen Clusters sein kann. In MetroCluster IP Konfigurationen mit acht oder vier Knoten besteht jeder Standort aus Speicherkontrollern, die als ein oder zwei Hochverfügbarkeitspaare (High Availability, HA) konfiguriert sind.

Sie können "ONTAP Mediator installieren" an einem dritten Standort verwenden, um den Status der Knoten und ihrer DR-Partner zu überwachen. ONTAP Mediator kann im Katastrophenfall eine Mediator-assisted unplanned switchover (MAUSO) implementieren.

Es besteht auch die Möglichkeit, eine vereinbarte Umschaltung durchzuführen, um einen der Cluster für geplante Wartungsarbeiten außer Betrieb zu nehmen. Der Partnercluster übernimmt alle Daten-I/O-Operationen für beide Cluster, bis der Cluster, an dem die Wartung durchgeführt wurde, wieder in Betrieb genommen wird und eine Rückschaltung erfolgt.

Verfahren zum Einrichten und Verwalten einer MetroCluster IP Konfiguration mit System Manager sind im "MetroCluster Dokumentation" zu finden.

Datensicherung mit Tape-Backup

Informationen zum Tape-Backup von ONTAP FlexVol Volumes

ONTAP unterstützt Tape-Backup und Wiederherstellung über das Network Data Management Protocol (NDMP). NDMP ermöglicht die Sicherung von Daten in Speichersystemen direkt auf Band, was zu einer effizienten Nutzung der Bandbreite führt. ONTAP unterstützt sowohl Dump- als auch SMTape-Engines für Tape-Backup.

Ein Dump- oder SMTape-Backup oder eine Wiederherstellung kann mithilfe von NDMP-kompatiblen Backup-Anwendungen durchgeführt werden. Es wird nur NDMP Version 4 unterstützt.

Tape-Backup mit Dump

Dump ist eine Snapshot-basierte Datensicherung, bei der Ihre Dateisystemdaten auf Band gesichert werden. Die ONTAP Dump-Engine sichert Dateien, Verzeichnisse und die zugehörige Zugriffssteuerungsliste (ACL) auf Band. Es ist möglich, ein gesamtes Volume, einen gesamten Qtree oder einen Teilbaum zu sichern, der kein gesamtes Volume oder kein gesamter Qtree ist. Dump unterstützt Baseline-, Differenzial- und inkrementelle Backups.

Tape-Backup mit SMTape

SMTape ist eine Snapshot-basierte Disaster-Recovery-Lösung von ONTAP, die Datenblöcke auf Band sichert. Mit SMTape lassen sich Volume-Backups auf Tape durchführen. Ein Backup auf Qtree- oder Subtree-Ebene ist jedoch nicht möglich. SMTape unterstützt Baseline-, Differenzial- und inkrementelle Backups.

Ab ONTAP 9.13.1 wird Tape-Backup mit SMTape unterstützt SnapMirror Active Sync.

ONTAP Tape-Backup und Wiederherstellungs-Workflow

Tape-Backup- und Wiederherstellungsvorgänge sind mit einer NDMP-fähigen Sicherungsanwendung möglich.

Über diese Aufgabe

Der Tape-Backup und Restore-Workflow bietet einen Überblick über die Aufgaben, die bei der Durchführung von Tape-Backup und Restore-Operationen anfallen. Detaillierte Informationen zur Durchführung eines Backup- und Restore-Vorgangs enthält die Dokumentation der Backup-Anwendung.

Schritte

1. Eine Tape-Bibliothek Konfiguration wird eingerichtet, indem eine NDMP-unterstützte Tape-Topologie ausgewählt wird.
2. NDMP-Dienste auf dem Speichersystem aktivieren.

   Sie können die NDMP-Dienste entweder auf Knotenebene oder auf Ebene der Storage Virtual Machine (SVM) aktivieren. Dies hängt vom NDMP-Modus ab, in dem die Tape-Backup- und Wiederherstellungsoperation durchgeführt wird.

3. NDMP-Optionen dienen zur Verwaltung von NDMP auf dem Speichersystem.

   Sie können NDMP-Optionen entweder auf Knotenebene oder auf SVM-Ebene verwenden. Dies hängt vom NDMP-Modus ab, in dem die Tape-Backup- und Wiederherstellungsoperation durchgeführt wird.

   Sie können die NDMP-Optionen auf Knotenebene mit dem `system services ndmp modify` Befehl und auf SVM-Ebene mit dem `vserver services ndmp modify` Befehl ändern. Weitere Informationen zu `system services ndmp modify` und `vserver services ndmp modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Eine Tape-Backup- oder Wiederherstellungsoperation kann mit einer NDMP-fähigen Sicherungsanwendung durchgeführt werden.

   ONTAP unterstützt sowohl Dump als auch SMTape Engines für Tape-Backup und Wiederherstellung.

   Weitere Informationen zur Verwendung der Backup-Anwendung (auch *Datenverwaltungsanwendungen* oder *DMAs* genannt) für Sicherungs- oder Wiederherstellungsvorgänge enthält die Dokumentation Ihrer Backup-Anwendung.

Verwandte Informationen

Gängige NDMP Tape-Backup-Bandsicherungstopologien

Überblick über die Dump-Engine für FlexVol Volumes

Anwendungsfälle für ONTAP SMTape und Dump Backup Engines

ONTAP unterstützt zwei Backup-Engines: SMTape und dump. Die Anwendungsfälle der SMTape- und dump-Backup-Engines sind zu berücksichtigen, um die geeignete Backup-Engine für Tape-Backup- und Wiederherstellungsvorgänge auszuwählen.

Dump kann in folgenden Fällen verwendet werden:

- Direkte Wiederherstellung (DAR) von Dateien und Verzeichnissen
- Sicherung einer Teilmenge von Unterverzeichnissen oder Dateien in einem bestimmten Pfad
- Bestimmte Dateien und Verzeichnisse während der Datensicherung ausschließen
- Langzeitarchivierung von Backups

SMTape kann in folgenden Fällen verwendet werden:

- Lösung zur Notfallwiederherstellung
- Beibehalten der Deduplizierungseinsparungen und Deduplizierungseinstellungen der gesicherten Daten während eines Wiederherstellungsvorgangs
- Sicherung großer Datenmengen

Tape-Laufwerke verwalten

Informationen zur Verwaltung von ONTAP Tape-Laufwerken

Sie können die Verbindungen der Tape-Bibliothek überprüfen und Informationen zum Tape-Laufwerk anzeigen, bevor ein Tape-Backup oder eine Wiederherstellung durchgeführt wird. Ein nicht qualifiziertes Tape-Laufwerk kann verwendet werden, indem es als qualifiziertes Tape-Laufwerk emuliert wird. Zusätzlich können Tape-Aliase zugewiesen und entfernt sowie vorhandene Aliase angezeigt werden.

Beim Sichern von Daten auf Band werden diese in Banddateien gespeichert. Dateimarken trennen die Banddateien, und die Dateien haben keine Namen. Eine Banddatei wird über ihre Position auf dem Band angegeben. Eine Banddatei wird mit einem Tape-Gerät geschrieben. Beim Lesen der Banddatei muss ein Gerät mit demselben Komprimierungstyp verwendet werden, der auch beim Schreiben dieser Banddatei verwendet wurde.

ONTAP Befehle zur Verwaltung von Tape-Laufwerken, Medienwechslern und Tape-Laufwerk-Operationen

Es gibt Befehle zum Anzeigen von Informationen über Tape-Laufwerke und Medienwechsler in einem Cluster, zum Online- und Offline-Schalten eines Tape-Laufwerks, zum Ändern der Tape-Laufwerk-Kassettenposition, zum Festlegen und Löschen des Tape-Laufwerk-Aliasnamens sowie zum Zurücksetzen eines Tape-Laufwerks. Auch Tape-Laufwerk-Statistiken können angezeigt und zurückgesetzt werden.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Ein Tape-Laufwerk online schalten	`storage tape online`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Aliasnamen für Tape-Laufwerk oder Medienwechsler löschen	`storage tape alias clear`
Aktivieren oder Deaktivieren einer Tape-Trace-Operation für ein Tape-Laufwerk	`storage tape trace`
Die Position der Tape-Laufwerk-Kassette ändern	`storage tape position`
Tape-Laufwerk zurücksetzen	`storage tape reset` Dieser Befehl ist nur auf der Stufe „Erweitert“ verfügbar.
Einen Aliasnamen für das Tape-Laufwerk oder den Medienwechsler festlegen	`storage tape alias set`
Ein Tape-Laufwerk offline schalten	`storage tape offline`
Informationen zu allen Tape-Laufwerken und Medienwechslern	`storage tape show`
Informationen zu den an den Cluster angeschlossenen Tape-Laufwerken	• `storage tape show-tape-drive` • `system node hardware tape drive show`
Informationen zu Medienwechslern, die an den Cluster angeschlossen sind	`storage tape show-media-changer`
Fehlerinformationen zu den an den Cluster angeschlossenen Tape-Laufwerken anzeigen	`storage tape show-errors`
Alle qualifizierten und unterstützten ONTAP Tape-Laufwerke, die an jeden Node im Cluster angeschlossen sind, werden angezeigt.	`storage tape show-supported-status`
Aliase aller Tape-Laufwerke und Medienwechsler anzeigen, die an jeden Node im Cluster angeschlossen sind	`storage tape alias show`
Die Statistiken eines Tape-Laufwerks auf Null zurücksetzen	`storage stats tape zero tape_name` Dieser Befehl ist in der Nodeshell zu verwenden.
Von ONTAP unterstützte Tape-Laufwerke anzeigen	`storage show tape supported [-v]` Dieser Befehl ist in der Nodeshell zu verwenden. Mit der `-v` Option lassen sich weitere Details zu jedem Tape-Laufwerk anzeigen.
Tape-Gerät Statistiken bieten Einblick in die Tape-Performance und das Nutzungsmuster.	`storage stats tape tape_name` Dieser Befehl ist in der Nodeshell zu verwenden.

Verwandte Informationen

- "Storage-Tape"
- "storage tape show"
- "storage tape show-supported-status"

- "storage tape show-tape-drive"
- "Storage Tape-Alias löschen"
- "Storage-Tape-Alias-Set"
- "storage tape Alias anzeigen"
- "Storage Tape-Trace"

Ein nicht qualifiziertes Tape-Laufwerk für ONTAP Tape-Backup verwenden

Sie können ein nicht qualifiziertes Tape-Laufwerk in einem Speichersystem verwenden, wenn es ein qualifiziertes Tape-Laufwerk emulieren kann. Es wird dann wie ein qualifiziertes Tape-Laufwerk behandelt. Um ein nicht qualifiziertes Tape-Laufwerk zu verwenden, muss zunächst festgestellt werden, ob es eines der qualifizierten Tape-Laufwerke emuliert.

Über diese Aufgabe

Ein nicht qualifiziertes Tape-Laufwerk ist ein Laufwerk, das an das Speichersystem angeschlossen ist, aber von ONTAP nicht unterstützt oder erkannt wird.

Schritte

1. Die nicht qualifizierten Tape-Laufwerke, die an ein Speichersystem angeschlossen sind, werden mit dem `storage tape show-supported-status` Befehl angezeigt.

   Der folgende Befehl zeigt die an das Speichersystem angeschlossenen Tape-Laufwerke sowie den Unterstützungs- und Qualifizierungsstatus jedes einzelnen Tape-Laufwerks an. Nicht qualifizierte Tape-Laufwerke werden ebenfalls aufgeführt. `tape_drive_vendor_name` ist ein nicht qualifiziertes Tape-Laufwerk, das an das Speichersystem angeschlossen ist, aber von ONTAP nicht unterstützt wird.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. Das qualifizierte Tape-Laufwerk emulieren.

   "NetApp Downloads: Konfigurationsdateien für Tape-Geräte"

Verwandte Informationen

- Was qualifizierte Tape-Laufwerke sind
- "storage tape show-supported-status"

Tape-Aliase einem Tape-Laufwerk oder Medienwechsler für ONTAP Tape-Backup zuweisen

Zur einfachen Geräteidentifizierung kann einem Tape-Laufwerk oder Medienwechsler ein Tape-Alias zugewiesen werden. Aliase stellen eine Entsprechung zwischen den logischen Namen der Backup-Geräte und einem dauerhaft zugewiesenen Namen für das Tape-Laufwerk oder den Medienwechsler her.

Schritte

1. Einem Tape-Laufwerk oder einem Medium-Changer kann ein Alias mit dem `storage tape alias set` Befehl zugewiesen werden.

   Weitere Informationen zu `storage tape alias set` finden sich in der "ONTAP-Befehlsreferenz".

   Sie können die Seriennummerninformationen (SN) der Tape-Laufwerke mit dem `system node hardware tape drive show` Befehl und die Informationen zu Tape-Bibliotheken mit den `system node hardware tape library show` Befehlen anzeigen.

   Der folgende Befehl weist einem Tape-Laufwerk mit der Seriennummer SN[123456]L4, das an den Knoten cluster1-01 angeschlossen ist, einen Aliasnamen zu:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name st3
   -mapping SN[123456]L4
   ```

   Der folgende Befehl weist einem Medienwechsler mit der Seriennummer SN[65432], der an den Knoten cluster1-01 angeschlossen ist, einen Aliasnamen zu:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name mc1
   -mapping SN[65432]
   ```

Verwandte Informationen

- Was Tape-Aliasing ist
- Entfernen von Tape-Aliasen
- "Storage-Tape-Alias-Set"

Bandaliase für ein Tape-Laufwerk oder einen Medienwechsler bei ONTAP Tape-Backup entfernen

Aliase können mit dem `storage tape alias clear` Befehl entfernt werden, wenn persistente Aliase für ein Tape-Laufwerk oder einen Medium-Changer nicht mehr erforderlich sind.

Schritte

1. Ein Alias kann von einem Tape-Laufwerk oder Medienwechsler mit dem `storage tape alias clear`

Befehl entfernt werden.

Weitere Informationen zu `storage tape alias clear` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl entfernt die Aliase aller Tape-Laufwerke, indem der Umfang der Alias-Löschoperation auf `tape` festgelegt wird:

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

Nachdem Sie fertig sind

Wenn eine Tape-Backup- oder Wiederherstellungsoperation mit NDMP durchgeführt wird, muss nach dem Entfernen eines Alias von einem Tape-Laufwerk oder Medienwechsler dem Tape-Laufwerk oder Medienwechsler ein neuer Aliasname zugewiesen werden, um weiterhin Zugriff auf das Tape-Gerät zu haben.

Verwandte Informationen

- Was Tape-Aliasing ist
- Zuweisung von Tape-Aliasen
- "Storage Tape-Alias löschen"

ONTAP Bandreservierungen aktivieren oder deaktivieren

Sie können steuern, wie ONTAP Tape-Gerät-Reservierungen verwaltet, indem Sie die `tape.reservations` Option verwenden. Standardmäßig ist die Tape-Reservierung deaktiviert.

Über diese Aufgabe

Die Aktivierung der Bandreservierungsoption kann Probleme verursachen, wenn Bandlaufwerke, Medienwechsler, Bridges oder Bibliotheken nicht ordnungsgemäß funktionieren. Wenn Bandbefehle melden, dass das Gerät reserviert ist, obwohl kein anderes Speichersystem das Gerät verwendet, sollte diese Option deaktiviert werden.

Schritte

1. Um entweder den SCSI Reserve/Release-Mechanismus oder SCSI Persistent Reservations zu verwenden oder Tape-Reservierungen zu deaktivieren, ist folgender Befehl in der Clustershell einzugeben:

   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi`Wählt den SCSI Reserve/Release-Mechanismus aus.

   `persistent` SCSI Persistent Reservations wird ausgewählt.

   `off`deaktiviert Tape-Reservierungen.

Verwandte Informationen

Was Bandreservierungen sind

ONTAP Befehle zur Überprüfung der Tape-Bibliothek-Verbindungen

Sie können Informationen zum Verbindungspfad zwischen einem Speichersystem und

einer an das Speichersystem angeschlossenen Tape-Bibliothek anzeigen. Diese Informationen können zur Überprüfung des Verbindungspfads zur Tape-Bibliothek oder zur Fehlerbehebung bei Problemen im Zusammenhang mit den Verbindungspfaden verwendet werden.

Die folgenden Tape-Bibliothek-Details können angezeigt werden, um die Tape-Bibliothek-Verbindungen nach dem Hinzufügen oder Erstellen einer neuen Tape-Bibliothek oder nach der Wiederherstellung eines ausgefallenen Pfads bei Einzelpfad- oder Mehrpfadzugriff auf eine Tape-Bibliothek zu überprüfen. Diese Informationen sind auch bei der Fehlerbehebung von pfadbezogenen Fehlern oder bei einem Zugriffsfehler auf eine Tape-Bibliothek hilfreich.

- Knoten, an dem die Tape-Bibliothek angeschlossen ist
- Geräte-ID
- NDMP Pfad
- Tape-Bibliothek Name
- Zielport- und Initiatorport-IDs
- Single-Path- oder Multipath-Zugriff auf eine Tape-Bibliothek für jeden Ziel- oder FC-Initiatorport
- Details zur Datenintegrität im Zusammenhang mit Pfaden, wie „`Path Errors`“ und „`Path Qual`“
- LUN-Gruppen und LUN-Anzahlen

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen zu einer Tape-Bibliothek in einem Cluster	`system node hardware tape library show`
Pfadinformationen für eine Tape-Bibliothek anzeigen	`storage tape library path show`
Pfadinformationen für eine Tape-Bibliothek für jeden Initiatorport	`storage tape library path show-by-initiator`
Verbindungsinformationen zwischen einer Tape-Bibliothek und einem Cluster anzeigen	`storage tape library config show`

Verwandte Informationen

- "Tape-Bibliothek Konfiguration anzeigen"
- "system node hardware Tape-Bibliothek show"
- "storage Tape-Bibliothek Pfad anzeigen"
- "Tape-Bibliothek-Pfad anzeigen nach Initiator"

Über Tape-Laufwerke

Informationen zu qualifizierten ONTAP Tape-Laufwerken

Sie müssen ein qualifiziertes Tape-Laufwerk verwenden, das getestet wurde und auf einem Speichersystem einwandfrei funktioniert. Tape-Aliasing kann verwendet und Tape-Reservierungen aktiviert werden, um sicherzustellen, dass jeweils nur ein Speichersystem auf ein Tape-Laufwerk zugreift.

Ein qualifiziertes Tape-Laufwerk ist ein Tape-Laufwerk, das getestet wurde und auf Speichersystemen

ordnungsgemäß funktioniert. Tape-Laufwerke können für bestehende ONTAP Versionen mithilfe der Konfigurationsdatei qualifiziert werden.

Format der ONTAP Konfigurationsdatei

Das Format der Konfigurationsdatei für Tapes besteht aus Feldern wie Hersteller-ID, Produkt-ID und Details zu den Kompressionstypen für ein Tape-Laufwerk. Diese Datei enthält außerdem optionale Felder zum Aktivieren der Autoload-Funktion eines Tape-Laufwerks und zum Ändern der Befehls-Zeitüberschreitungswerte eines Tape-Laufwerks.

Die folgende Tabelle zeigt das Format der Tape-Konfigurationsdatei:

Artikel	Größe	Beschreibung
`vendor_id` (Zeichenkette)	bis zu 8 Bytes	Die vom `SCSI Inquiry` Befehl gemeldete Vendor-ID.
`product_id`(Zeichenkette)	bis zu 16 Bytes	Die Produkt-ID, wie sie vom `SCSI Inquiry` Befehl gemeldet wird.
`id_match_size`(Nummer)		Die Anzahl der Bytes der Produkt-ID, die für den Abgleich verwendet werden, um das zu identifizierende Tape-Laufwerk zu erkennen, beginnend mit dem ersten Zeichen der Produkt-ID in den Inquiry-Daten.
`vendor_pretty` (Zeichenkette)	bis zu 16 Bytes	Wenn dieser Parameter vorhanden ist, wird er durch die vom Befehl angezeigte Zeichenkette `storage tape show -device-names` angegeben; andernfalls wird INQ_VENDOR_ID angezeigt.
`product_pretty`(Zeichenkette)	bis zu 16 Bytes	Wenn dieser Parameter vorhanden ist, wird er durch die vom Befehl angezeigte Zeichenkette `storage tape show -device-names` angegeben; andernfalls wird INQ_PRODUCT_ID angezeigt.

Die `vendor_pretty` und `product_pretty` Felder sind optional, aber wenn eines dieser Felder einen Wert hat, muss auch das andere einen Wert haben.

Die folgende Tabelle erläutert die Beschreibung, den Dichtecode und den Komprimierungsalgorithmus für die verschiedenen Komprimierungstypen, wie `l`, `m`, `h` und `a`:

Artikel	Größe	Beschreibung
`{l	m	h

Artikel	Größe	Beschreibung
a}_description=(string)`	bis zu 24 Bytes	Die Zeichenkette, die für den nodeshell Befehl ausgegeben wird `sysconfig -t`, die die Eigenschaften der jeweiligen Dichteeinstellung beschreibt.
`{l	m	h
a}_density=(hex codes)`		Der Dichtecode, der im SCSI-Modus-Seitenblockdeskriptor entsprechend dem gewünschten Dichtecode für l, m, h oder a festgelegt wird.
`{l	m	h
a}_algorithm=(hex codes)`		Der Komprimierungsalgorithmus, der auf der SCSI Compression Mode Page entsprechend dem Dichtecode und der gewünschten Dichtecharakteristik eingestellt werden soll.

Die folgende Tabelle beschreibt die optionalen Felder, die in der Tape-Konfigurationsdatei verfügbar sind:

Feld	Beschreibung
`autoload=(Boolean yes/no)`	Dieses Feld ist auf `yes` gesetzt, wenn das Tape-Laufwerk über eine automatische Ladefunktion verfügt; das heißt, nachdem die Bandkassette eingelegt wurde, ist das Tape-Laufwerk betriebsbereit, ohne dass ein `SCSI load` (Start/Stop-Einheit) Befehl ausgeführt werden muss. Der Standardwert für dieses Feld ist `no`.
`cmd_timeout_0x`	Individueller Zeitüberschreitungswert. Dieses Feld sollte nur verwendet werden, wenn ein anderer Zeitüberschreitungswert als der vom Tape-Laufwerk standardmäßig verwendete Wert angegeben werden soll. Die Beispieldatei listet die vom Tape-Laufwerk verwendeten Standardwerte für die SCSI-Befehlszeitüberschreitung auf. Der Zeitüberschreitungswert kann in Minuten (m), Sekunden (s) oder Millisekunden (ms) angegeben werden. Dieses Feld sollten Sie nicht ändern.

Die Konfigurationsdatei für das Tape kann von der NetApp Support Site heruntergeladen und angezeigt werden.

Beispiel eines Tape-Konfigurationsdateiformats

Das Format der Konfigurationsdatei für das HP LTO5 ULTRIUM Tape-Laufwerk ist wie folgt:

```
vendor_id="HP"

product_id="Ultrium 5-SCSI"

id_match_size=9

vendor_pretty="Hewlett-Packard"

product_pretty="LTO-5"

l_description="LTO-3(ro)/4 4/800GB"

l_density=0x00

l_algorithm=0x00

m_description="LTO-3(ro)/4 8/1600GB cmp"

m_density=0x00

m_algorithm=0x01

h_description="LTO-5 1600GB"

h_density=0x58

h_algorithm=0x00

a_description="LTO-5 3200GB cmp"

a_density=0x58

a_algorithm=0x01

autoload="yes"
```

Verwandte Informationen

- "NetApp Tools: Konfigurationsdateien für Tape-Geräte"
- "storage tape show"

Wie das ONTAP Speichersystem ein Tape-Laufwerk dynamisch qualifiziert

Das Speichersystem qualifiziert ein Tape-Laufwerk dynamisch, indem es dessen Hersteller-ID und Produkt-ID mit den Informationen in der Tape-Qualifizierungstabelle abgleicht.

Wenn ein Tape-Laufwerk an das Speichersystem angeschlossen wird, sucht das System nach einer Übereinstimmung der Hersteller-ID und Produkt-ID zwischen den während der Banderkennung erhaltenen Informationen und den Informationen in der internen Tape-Qualifizierungstabelle. Wird eine Übereinstimmung gefunden, kennzeichnet das Speichersystem das Tape-Laufwerk als qualifiziert und kann auf das Tape-Laufwerk zugreifen. Kann das Speichersystem keine Übereinstimmung finden, bleibt das Tape-Laufwerk im

nicht qualifizierten Zustand und wird nicht verwendet.

Übersicht über Bandgeräte

Informationen zu ONTAP Tape-Geräten

Ein Tape-Gerät ist eine Darstellung eines Tape-Laufwerks. Es ist eine spezifische Kombination aus Rückspultyp und Kompressionsfähigkeit eines Tape-Laufwerks.

Ein Tape-Gerät wird für jede Kombination aus Rückspultyp und Komprimierungsfähigkeit erstellt. Daher kann ein Tape-Laufwerk oder eine Tape-Bibliothek mehrere zugeordnete Tape-Geräte haben. Ein Tape-Gerät muss angegeben werden, um Bänder zu verschieben, zu beschreiben oder zu lesen.

Wenn ein Tape-Laufwerk oder eine Tape-Bibliothek in ein Speichersystem installiert wird, erstellt ONTAP Tape-Geräte, die dem Tape-Laufwerk oder der Tape-Bibliothek zugeordnet sind.

ONTAP erkennt Tape-Laufwerke und Tape-Bibliotheken und weist ihnen logische Nummern und Tape-Geräte zu. ONTAP erkennt die Fibre Channel-, SAS- und parallelen SCSI Tape-Laufwerke und Tape-Bibliotheken, wenn sie an die Schnittstellen-Ports angeschlossen sind. ONTAP erkennt diese Laufwerke, wenn deren Schnittstellen aktiviert sind.

Format eines ONTAP Tape-Gerät Namens

Jedes Tape-Gerät hat einen zugehörigen Namen, der in einem definierten Format erscheint. Das Format enthält Informationen über den Gerätetyp, den Rückspultyp, den Alias und den Komprimierungstyp.

Das Format eines Tape-Gerät-Namens ist wie folgt:

`rewind_type st alias_number compression_type`

`rewind_type` ist vom Typ „Zurückspulen“.

Die folgende Liste beschreibt die verschiedenen Rückspultyp-Werte:

- **r**

  ONTAP spult das Band zurück, nachdem das Schreiben der Banddatei abgeschlossen ist.

- **nr**

  ONTAP spult das Band nach dem Beschreiben der Banddatei nicht zurück. Diese Rückspulart muss verwendet werden, wenn mehrere Banddateien auf dasselbe Band geschrieben werden sollen.

- **ur**

  Dies ist der Rückspultyp „Entladen/Laden“. Bei diesem Rückspultyp entlädt die Tape-Bibliothek das Band, sobald das Ende einer Banddatei erreicht ist, und lädt anschließend das nächste Band, sofern eines vorhanden ist.

  Diese Rückspulart darf nur unter folgenden Umständen verwendet werden:

  - Das mit diesem Gerät verbundene Tape-Laufwerk befindet sich in einer Tape-Bibliothek oder in einem Medienwechsler, der sich im Bibliotheksmodus befindet.

- Das mit diesem Gerät verbundene Tape-Laufwerk ist an ein Speichersystem angeschlossen.
- Für den von Ihnen durchgeführten Vorgang sind ausreichend Tapes in der für dieses Tape-Laufwerk definierten Tape-Bibliothekssequenz verfügbar.

> Wenn ein Tape mit einem No-Rewind-Gerät beschrieben wird, muss das Tape vor dem Auslesen zurückgespult werden.

`st` ist die Standardbezeichnung für ein Tape-Laufwerk.

`alias_number` ist der Alias, den ONTAP dem Tape-Laufwerk zuweist. Wenn ONTAP ein neues Tape-Laufwerk erkennt, weist ONTAP dem Tape-Laufwerk einen Alias zu.

`compression_type` ist ein laufwerkspezifischer Code für die Datendichte auf dem Band und die Art der Komprimierung.

Die folgende Liste beschreibt die verschiedenen Werte für `compression_type`:

- **a**

  Höchste Kompression

- **h**

  Hohe Kompression

- **m**

  Mittlere Kompression

- **l**

  Niedrige Kompression

Beispiele

`nrst0a`Gibt ein No-Rewind-Gerät auf Tape-Laufwerk 0 mit der höchsten Komprimierung an.

Beispiel einer Auflistung von Tape-Geräten

Das folgende Beispiel zeigt die mit HP Ultrium 2-SCSI verbundenen Tape-Geräte:

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,        format is: HP (200GB)
nrst0l -  no rewind device,     format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,        format is: HP (200GB)
nrst0m -  no rewind device,     format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,        format is: HP (200GB)
nrst0h -  no rewind device,     format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,        format is: HP (400GB w/comp)
```

```
    nrst0a -  no rewind device,     format is: HP (400GB w/comp)
    urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

Die folgende Liste beschreibt die Abkürzungen im vorhergehenden Beispiel:

- GB – Gigabyte; dies ist die Kapazität des Tape.
- w/comp, mit Kompression; dies zeigt die Bandkapazität mit Kompression.

Unterstützte Anzahl gleichzeitiger ONTAP Tape-Geräte

ONTAP unterstützt maximal 64 gleichzeitige Tape-Laufwerk-Verbindungen, 16 Medienwechsler und 16 Bridge- oder Router-Geräte pro Speichersystem (pro Knoten) in beliebiger Kombination von Fibre Channel-, SCSI- oder SAS-Anschlüssen.

Tape-Laufwerke oder Medienwechsler können Geräte in physischen oder virtuellen Tape-Bibliotheken oder Standalone-Geräte sein.

> Obwohl ein Speichersystem 64 Tape-Laufwerk-Verbindungen erkennen kann, hängt die maximale Anzahl gleichzeitig durchführbarer Sicherungs- und Wiederherstellungssitzungen von den Skalierbarkeitsgrenzen der Sicherungs-Engine ab.

Verwandte Informationen

Skalierbarkeitsgrenzen für Dump-Backup und Wiederherstellungssitzungen

Bandaliasing

Tape-Aliasing Übersicht

Die Aliasvergabe vereinfacht die Geräteidentifizierung. Die Aliasvergabe verknüpft einen physischen Pfadnamen (PPN) oder eine Seriennummer (SN) eines Bandes oder Medienwechslers mit einem permanenten, aber veränderbaren Aliasnamen.

Die folgende Tabelle beschreibt, wie die Verwendung von Bandaliasen sicherstellt, dass ein Tape-Laufwerk (oder eine Tape-Bibliothek oder ein Medienwechsler) immer mit einem einzigen Aliasnamen verknüpft ist:

Szenario	Neuzuweisung des Alias
Wenn das System neu startet	Das Tape-Laufwerk erhält automatisch seinen vorherigen Alias zurück.
Wenn ein Tape-Gerät zu einem anderen Port wechselt	Der Alias kann so angepasst werden, dass er auf die neue Adresse verweist.
Wenn mehr als ein System ein bestimmtes Tape-Gerät verwendet	Der Benutzer kann den Alias so einstellen, dass er für alle Systeme gleich ist.

Durch die Vergabe von Bandaliasen entsteht eine Entsprechung zwischen den logischen Namen von Sicherungsgeräten (zum Beispiel st0 oder mc1) und einem Namen, der dauerhaft einem Port, einem Tape-Laufwerk oder einem Medium Changer zugewiesen ist.

> st0 und st00 sind unterschiedliche logische Namen.

Logische Namen und Seriennummern werden nur für den Zugriff auf ein Gerät verwendet. Nach dem Zugriff gibt das Gerät alle Fehlermeldungen über den physischen Pfadnamen zurück.

Für die Aliasvergabe stehen zwei Arten von Namen zur Verfügung: physischer Pfadname und Seriennummer.

Informationen zu physischen Wegnamen

Physische Pfadnamen (PPNs) sind die numerischen Adresssequenzen, die ONTAP Tape-Laufwerken und Tape-Bibliotheken basierend auf dem SCSI-2/3-Adapter oder Switch (genauer Standort) zuweist, mit dem sie mit dem Speichersystem verbunden sind. PPNs werden auch als elektrische Namen bezeichnet.

Die PPNs von direkt angeschlossenen Geräten verwenden folgendes Format: `host_adapter.device_id_lun`

Der LUN-Wert wird nur für Tape- und Medium-Changer-Geräte angezeigt, deren LUN-Werte nicht null sind; das heißt, wenn der LUN-Wert null ist, wird der `lun` Teil des PPN nicht angezeigt.

Beispielsweise gibt PPN 8.6 an, dass die Host-Adapter-Nummer 8, die Geräte-ID 6 und die logische Einheitennummer (LUN) 0 ist.

SAS Tape-Geräte sind ebenfalls direkt angeschlossene Geräte. Beispielsweise gibt die PPN 5c.4 an, dass in einem Speichersystem der SAS HBA in Steckplatz 5 angeschlossen ist, SAS Tape an Port C des SAS HBA angeschlossen ist und die Geräte-ID 4 ist.

PPNs von Fibre Channel Switch-attached Devices verwenden das folgende Format: `switch:port_id.device_id_lun`

Beispielsweise zeigt der PPN MY_SWITCH:5.3L2, dass das an Port 5 eines Switches namens MY_SWITCH angeschlossene Tape-Laufwerk die Geräte-ID 3 und die LUN 2 hat.

Die LUN (logische Einheitennummer) wird vom Laufwerk bestimmt. Fibre Channel, SCSI Tape-Laufwerke und Tape-Bibliotheken sowie Festplatten verfügen über PPNs.

Die PPNs von Tape-Laufwerken und Tape-Bibliotheken ändern sich nicht, es sei denn, der Name des Switches ändert sich, das Tape-Laufwerk oder die Tape-Bibliothek wird verschoben oder das Tape-Laufwerk bzw. die Tape-Bibliothek wird neu konfiguriert. Die PPNs bleiben nach einem Neustart unverändert. Wenn zum Beispiel ein Tape-Laufwerk mit dem Namen MY_SWITCH:5.3L2 entfernt und ein neues Tape-Laufwerk mit derselben Geräte-ID und LUN an Port 5 des Switches MY_SWITCH angeschlossen wird, ist das neue Tape-Laufwerk über MY_SWITCH:5.3L2 erreichbar.

Informationen zu Seriennummern

Eine Seriennummer (SN) ist eine eindeutige Kennung für ein Tape-Laufwerk oder einen Medienwechsler. ONTAP generiert Aliase basierend auf der SN anstelle der WWN.

Da die Seriennummer (SN) eine eindeutige Kennung für ein Tape-Laufwerk oder einen Medienwechsler ist, bleibt der Alias unabhängig von den verschiedenen Verbindungspfaden zum Tape-Laufwerk oder Medienwechsler gleich. Dies ermöglicht es Speichersystemen, dasselbe Tape-Laufwerk oder denselben Medienwechsler in einer Tape-Bibliothek-Konfiguration nachzuverfolgen.

Die SN eines Tape-Laufwerks oder eines Medium Changers ändert sich nicht, selbst wenn der Fibre Channel Switch, an den das Tape-Laufwerk oder der Medium Changer angeschlossen ist, umbenannt wird. In einer

Tape-Bibliothek werden jedoch, wenn ein vorhandenes Tape-Laufwerk durch ein neues ersetzt wird, von ONTAP neue Aliase generiert, da sich die SN des Tape-Laufwerks ändert. Wenn ein vorhandenes Tape-Laufwerk in einen neuen Steckplatz in einer Tape-Bibliothek verschoben oder die LUN des Tape-Laufwerks neu zugeordnet wird, generiert ONTAP ebenfalls einen neuen Alias für dieses Tape-Laufwerk.

Die Backup-Anwendungen sind mit den neu generierten Aliasen zu aktualisieren.

Die Seriennummer eines Tape-Geräts verwendet folgendes Format: `SN[xxxxxxxxxx]L[X]`

`x` ist ein alphanumerisches Zeichen und L`X` ist die LUN des Tape-Geräts. Wenn die LUN 0 ist, wird der L`X`-Teil der Zeichenkette nicht angezeigt.

Jede Seriennummer besteht aus bis zu 32 Zeichen; das Format der Seriennummer ist nicht case-sensitiv.

Überlegungen bei der Konfiguration des ONTAP Multipath-Tape-Zugriffs

Es können zwei Pfade vom Speichersystem konfiguriert werden, um auf die Tape-Laufwerke in einer Tape-Bibliothek zuzugreifen. Wenn ein Pfad ausfällt, kann das Speichersystem die anderen Pfade nutzen, um auf die Tape-Laufwerke zuzugreifen, ohne den ausgefallenen Pfad sofort reparieren zu müssen. So wird sichergestellt, dass Tape-Operationen neu gestartet werden können.

Bei der Konfiguration des Multipath-Tape-Zugriffs von Ihrem Speichersystem sind die folgenden Punkte zu berücksichtigen:

- In Tape-Bibliotheken, die LUN-Mapping unterstützen, muss das LUN-Mapping für den Mehrwegezugriff auf eine LUN-Gruppe auf jedem Pfad symmetrisch sein.

  Tape-Laufwerke und Medienwechsler werden in einer Tape-Bibliothek LUN-Gruppen (einem Satz von LUNs, die denselben Initiator-Pfad-Satz gemeinsam nutzen) zugewiesen. Alle Tape-Laufwerke einer LUN-Gruppe müssen für Sicherungs- und Wiederherstellungsvorgänge auf allen Pfaden verfügbar sein.

- Es können maximal zwei Pfade vom Speichersystem zur Nutzung der Tape-Laufwerke in einer Tape-Bibliothek konfiguriert werden.
- Multipath-Tape-Zugriff unterstützt Lastverteilung. Lastverteilung ist standardmäßig deaktiviert.

Im folgenden Beispiel greift das Speichersystem über zwei Initiatorpfade, 0b und 0d, auf die LUN-Gruppe 0 zu. In beiden Pfaden hat die LUN-Gruppe dieselbe LUN-Nummer, 0, und dieselbe LUN-Anzahl, 5. Das Speichersystem greift auf die LUN-Gruppe 1 nur über einen Initiatorpfad, 3d, zu.

```
STSW-3070-2_cluster::> storage tape library config show

Node                    LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
```

```
                                1       2          IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Verwandte Informationen

- "Tape-Bibliothek Konfiguration anzeigen"

Informationen zum Hinzufügen von Tape-Laufwerken und Tape-Bibliotheken zu ONTAP Speichersystemen

Sie können Tape-Laufwerke und Tape-Bibliotheken dynamisch zum Speichersystem hinzufügen (ohne das Speichersystem offline zu nehmen).

Wenn ein neuer Medienwechsler hinzugefügt wird, erkennt das Speichersystem dessen Vorhandensein und fügt ihn der Konfiguration hinzu. Wenn der Medienwechsler bereits in den Aliasinformationen referenziert ist, werden keine neuen logischen Namen erstellt. Wenn die Bibliothek nicht referenziert ist, erstellt das Speichersystem einen neuen Alias für den Medienwechsler.

In einer Tape-Bibliothek-Konfiguration muss ein Tape-Laufwerk oder ein Medium-Changer auf LUN 0 eines Zielports konfiguriert werden, damit ONTAP alle Medium-Changer und Tape-Laufwerke an diesem Zielport erkennt.

Informationen zu ONTAP Tape-Reservierungen

Mehrere Speichersysteme können gemeinsam auf Tape-Laufwerke, Medienwechsler, Bridges oder Tape-Bibliotheken zugreifen. Tape-Reservierungen gewährleisten, dass jeweils nur ein Speichersystem auf ein Gerät zugreift, indem entweder der SCSI Reserve/Release-Mechanismus oder SCSI Persistent Reservations für alle Tape-Laufwerke, Medienwechsler, Bridges und Tape-Bibliotheken aktiviert werden.

> Alle Systeme, die Geräte in einer Bibliothek gemeinsam nutzen, unabhängig davon, ob Switches beteiligt sind oder nicht, müssen die gleiche Reservierungsmethode verwenden.

Der SCSI Reserve/Release-Mechanismus zur Reservierung von Geräten funktioniert unter normalen Bedingungen einwandfrei. Während Fehlerbehebungsverfahren an der Schnittstelle können Reservierungen jedoch verloren gehen. Falls dies geschieht, können Initiatoren, die nicht der reservierende Eigentümer sind, auf das Gerät zugreifen.

Reservierungen, die mit SCSI Persistent Reservations vorgenommen werden, sind von Fehlerkorrekturmechanismen wie Loop Reset oder Target Reset nicht betroffen, allerdings implementieren nicht alle Geräte SCSI Persistent Reservations korrekt.

Daten zwischen Speichersystemen übertragen

ONTAP Daten mit ndmpcopy übertragen

Der `ndmpcopy`nodeshell-Befehl überträgt Daten zwischen Storage-Systemen, die NDMP v4 unterstützen. Sowohl vollständige als auch inkrementelle Datentransfers sind möglich. Vollständige oder teilweise Volumes, Qtrees, Verzeichnisse oder einzelne

Dateien können übertragen werden.

Über diese Aufgabe

Bei ONTAP 8.x und früheren Versionen sind inkrementelle Übertragungen auf maximal zwei Ebenen beschränkt (eine vollständige und bis zu zwei inkrementelle Sicherungen).

Ab ONTAP 9.0 und späteren Versionen sind inkrementelle Übertragungen auf maximal neun Ebenen beschränkt (eine vollständige und bis zu neun inkrementelle Backups).

Der Befehl `ndmpcopy` kann an der nodeshell Befehlszeile des Quell- und Ziel-Storage-Systems oder eines Storage-Systems ausgeführt werden, das weder das Quell- noch das Zielsystem des Datentransfers ist. Der Befehl `ndmpcopy` kann auch auf einem einzelnen Storage-System ausgeführt werden, das sowohl das Quell- als auch das Zielsystem des Datentransfers ist.

Sie können die IPv4- oder IPv6-Adressen der Quell- und Ziel-Storage-Systeme im `ndmpcopy` Befehl verwenden. Das Pfadformat ist `/vserver_name/volume_name \[path\]`.

Schritte

1. NDMP-Service auf den Quell- und Ziel-Storage-Systemen aktivieren:

Wenn Sie den Datentransfer am Quell- oder Zielsystem durchführen…	Der folgende Befehl kann verwendet werden…
SVM-basierter NDMP-Modus	`vserver services ndmp on` Für die NDMP-Authentifizierung in der Admin-SVM ist das Benutzerkonto `admin` und die Benutzerrolle `admin` oder `backup`. In der Daten-SVM ist das Benutzerkonto `vsadmin` und die Benutzerrolle `vsadmin` oder `vsadmin-backup`-Rolle.
Knotenbezogener NDMP-Modus	`system services ndmp on`

2. Daten innerhalb eines Speichersystems oder zwischen Speichersystemen mit dem `ndmpcopy` Befehl an der Nodeshell übertragen:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

DNS-Namen werden in ndmpcopy nicht unterstützt. Die IP-Adresse des Quell- und des Zielsystems muss angegeben werden. Die Loopback-Adresse (127.0.0.1) wird weder als Quell-IP-Adresse noch als Ziel-IP-Adresse unterstützt.

   - Der `ndmpcopy` Befehl bestimmt den Adressierungsmodus für Steuerverbindungen wie folgt:
     - Der Adressmodus für die Steuerverbindung entspricht der angegebenen IP-Adresse.
     - Sie können diese Regeln mit den `-mcs`- und `-mcd`-Optionen außer Kraft setzen.

- Wenn das Quell- oder das Zielsystem das ONTAP System ist, sollte je nach NDMP-Modus (node-scoped oder SVM-scoped) eine IP-Adresse verwendet werden, die den Zugriff auf das Ziel-Volume ermöglicht.
- `source_path` und `destination_path` sind die absoluten Pfadnamen bis hin zur granularen Ebene von Volume, Qtree, Verzeichnis oder Datei.
- `-mcs` gibt den bevorzugten Adressierungsmodus für die Steuerverbindung zum Quell-Storage-System an.

  `inet` gibt einen IPv4-Adressmodus an und `inet6` gibt einen IPv6-Adressmodus an.
- `-mcd`legt den bevorzugten Adressierungsmodus für die Steuerverbindung zum Ziel-Storage-System fest.

  `inet` gibt einen IPv4-Adressmodus an und `inet6` gibt einen IPv6-Adressmodus an.
- `-md` gibt den bevorzugten Adressierungsmodus für Datentransfers zwischen dem Quell- und dem Ziel-Storage-System an.

  `inet` gibt einen IPv4-Adressmodus an und `inet6` gibt einen IPv6-Adressmodus an.

  Wenn die Option `-md` im Befehl `ndmpcopy` nicht verwendet wird, wird der Adressierungsmodus für die Datenverbindung wie folgt bestimmt:

  - Wenn eine der für die Steuerverbindungen angegebenen Adressen eine IPv6-Adresse ist, ist der Adressmodus für die Datenverbindung IPv6.
  - Wenn beide für die Steuerverbindungen angegebenen Adressen IPv4-Adressen sind, versucht der `ndmpcopy`Befehl zunächst, für die Datenverbindung einen IPv6-Adressmodus zu verwenden.

    Falls das fehlschlägt, verwendet der Befehl den IPv4-Adressmodus.

    Eine IPv6-Adresse muss, sofern angegeben, in eckige Klammern gesetzt werden.

  Dieser Beispielbefehl migriert Daten von einem Quellpfad (`source_path`) zu einem Zielpfad (`destination_path`).

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
Dieser Beispielbefehl legt explizit fest, dass die Steuerverbindungen und die Datenverbindung den IPv6-Adressmodus verwenden:

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-

Befehlsreferenz".

Optionen für den Befehl ndmpcopy

Sie sollten die für den `ndmpcopy`nodeshell Befehl verfügbaren Optionen verstehen, um "Daten übertragen"erfolgreich auszuführen.

Die folgende Tabelle listet die verfügbaren Optionen auf.

Option	Beschreibung
`-sa username:[password]`	Diese Option legt den Authentifizierungs-Benutzernamen und das Passwort für die Verbindung mit dem Quell-Storage-System fest. Diese Option ist obligatorisch. Für Benutzer ohne Administratorrechte muss das systemgenerierte, NDMP-spezifische Passwort des Benutzers angegeben werden. Das systemgenerierte Passwort ist sowohl für Administratoren als auch für Benutzer ohne Administratorrechte obligatorisch.
`-da username:[password]`	Diese Option legt den Authentifizierungs-Benutzernamen und das Passwort für die Verbindung mit dem Ziel-Storage-System fest. Diese Option ist obligatorisch.
`-st {md5`	`text}`
Diese Option legt den Quell-Authentifizierungstyp fest, der beim Verbinden mit dem Quell-Storage-System verwendet wird. Dies ist eine obligatorische Option, daher sollte entweder die `text`- oder die `md5` -Option angegeben werden.	`-dt {md5`
`text}`	Mit dieser Option wird der Authentifizierungstyp für die Verbindung zum Ziel-Storage-System festgelegt.
`-l`	Diese Option legt die für den Datentransfer verwendete Sicherungsebene auf den angegebenen Wert von level fest. Gültige Werte sind `0`, `1`, bis `9`, wobei `0` eine vollständige Übertragung und `1` bis `9` eine inkrementelle Übertragung angeben. Der Standardwert ist `0`.
`-d`	Diese Option ermöglicht die Generierung von ndmpcopy-Debug-Protokollmeldungen. Die ndmpcopy-Debug-Protokolldateien befinden sich im `/mroot/etc/log` Stammverzeichnis. Die Dateinamen der ndmpcopy-Debug-Protokolldateien sind im `ndmpcopy.yyyymmdd` Format.
`-f`	Diese Option aktiviert den erzwungenen Modus. Dieser Modus ermöglicht das Überschreiben von Systemdateien im `/etc` Verzeichnis auf dem Root des 7-Mode-Volumes.
`-h`	Diese Option gibt die Hilfemeldung aus.

Option	Beschreibung
`-p`	Diese Option fordert zur Eingabe des Passworts für die Quell- und Zielautorisierung auf. Dieses Passwort überschreibt das für `-sa` und `-da` angegebene Passwort. Diese Option kann nur verwendet werden, wenn der Befehl in einer interaktiven Konsole ausgeführt wird.
`-exclude`	Diese Option schließt bestimmte Dateien oder Verzeichnisse vom angegebenen Pfad für den Datentransfer aus. Der Wert kann eine durch Kommas getrennte Liste von Verzeichnis- oder Dateinamen sein, wie zum Beispiel **`.pst`** `oder.txt`. Die maximale Anzahl unterstützter Ausschlussmuster beträgt 32 und die maximale Anzahl unterstützter Zeichen beträgt 255.

NDMP für FlexVol Volumes

Informationen zu NDMP für ONTAP FlexVol Volumes

Das Network Data Management Protocol (NDMP) ist ein standardisiertes Protokoll zur Steuerung von Backup, Wiederherstellung und anderen Arten des Datentransfers zwischen primären und sekundären Speichergeräten, wie zum Beispiel Speichersystemen und Tape Libraries.

Durch die Aktivierung der NDMP-Unterstützung auf einem Speichersystem wird diesem die Kommunikation mit NDMP-fähigen, netzwerkgebundenen Backup-Anwendungen (auch *Data Management Applications* oder *DMAs* genannt), Datenservern und Tape-Servern ermöglicht, die an Backup- oder Wiederherstellungsvorgängen beteiligt sind. Die gesamte Netzwerkkommunikation erfolgt über TCPIP oder TCP/IPv6-Netzwerk. NDMP bietet außerdem eine Steuerung von Tape-Laufwerken und Medienwechslern auf niedriger Ebene.

Tape-Backup- und Wiederherstellungsvorgänge sind entweder im Node-scoped NDMP-Modus oder im Storage Virtual Machine (SVM)-scoped NDMP-Modus möglich.

Es sind die bei der Verwendung von NDMP zu berücksichtigenden Aspekte, die Liste der Umgebungsvariablen und die unterstützten NDMP Tape-Backup-Topologien zu beachten. Die erweiterte DAR-Funktionalität kann ebenfalls aktiviert oder deaktiviert werden. Die beiden von ONTAP unterstützten Authentifizierungsmethoden zur Authentifizierung des NDMP-Zugriffs auf ein Speichersystem sind: Klartext und Challenge.

Verwandte Informationen

Von ONTAP unterstützte Umgebungsvariablen

Informationen zu den Betriebsmodi von NDMP

Informationen zu den Betriebsmodi von ONTAP NDMP

Sie können Tape-Backup- und Wiederherstellungsvorgänge entweder auf Knotenebene oder auf Ebene der Storage Virtual Machine (SVM) durchführen. Damit diese Vorgänge

auf SVM-Ebene erfolgreich durchgeführt werden können, muss der NDMP-Service auf der SVM aktiviert sein.

Um Tape-Backup- und Wiederherstellungsvorgänge im node-scoped NDMP-Modus durchzuführen, muss der node-scoped NDMP-Modus explizit aktiviert werden.

Informationen zum knotenbezogenen ONTAP NDMP-Betriebsmodus

Im knotenbezogenen NDMP-Modus können Tape-Backup- und Wiederherstellungsvorgänge auf Knotenebene durchgeführt werden.

Im knotenbezogenen NDMP-Modus können Tape-Backup- und Wiederherstellungsvorgänge auf einem Knoten durchgeführt werden, dem das Volume gehört. Für diese Vorgänge müssen NDMP-Steuerungsverbindungen auf einem LIF eingerichtet werden, das auf dem Knoten gehostet wird, dem das Volume oder die Tape-Geräte gehören.

Dieser Modus ist veraltet und wird in einer zukünftigen Hauptversion entfernt.

Informationen zum SVM-basierten ONTAP NDMP-Modus

Tape-Backup- und Wiederherstellungsvorgänge auf Ebene der Storage Virtual Machine (SVM) sind erfolgreich möglich, wenn der NDMP-Service auf der SVM aktiviert ist. Alle Volumes, die auf verschiedenen Knoten in der SVM eines Clusters gehostet werden, können gesichert und wiederhergestellt werden, sofern die Sicherungsanwendung die CAB-Erweiterung unterstützt.

Eine NDMP-Steuerungsverbindung kann auf verschiedenen LIF-Typen hergestellt werden. Im SVM-bezogenen NDMP-Modus gehören diese LIFs entweder zur Daten-SVM oder zur Admin-SVM. Die Verbindung kann nur auf einem LIF hergestellt werden, wenn der NDMP-Service auf der SVM aktiviert ist, der dieses LIF gehört.

Ein Daten-LIF gehört zum Daten-SVM und der Intercluster-LIF, der Node-Management-LIF und der Cluster-Management-LIF gehören zum Admin-SVM.

Im SVM-basierten NDMP-Modus hängt die Verfügbarkeit von Volumes und Tape-Geräten für Backup- und Restore-Vorgänge vom LIF-Typ ab, auf dem die NDMP-Steuerverbindung hergestellt wird, sowie vom Status der CAB-Erweiterung. Wenn die Backup-Anwendung die CAB-Erweiterung unterstützt und ein Volume und das Tape-Gerät dieselbe Affinität aufweisen, kann die Backup-Anwendung eine lokale Backup- oder Restore-Operation anstelle einer Drei-Wege-Backup- oder Restore-Operation ausführen.

Verwandte Informationen

Befehle zur Verwaltung des node-scoped NDMP-Modus

Zu beachtende Punkte bei der Nutzung des ONTAP NDMP-Service

Beim Starten des NDMP-Service auf Ihrem Speichersystem sind eine Reihe von Aspekten zu berücksichtigen.

- Jeder Knoten unterstützt maximal 16 gleichzeitige Backups, Wiederherstellungen oder eine Kombination aus beidem unter Verwendung angeschlossener Bandlaufwerke.
- NDMP-Dienste können auf Anfrage von NDMP-Backup-Anwendungen Dateiverlaufsdaten generieren.

  Die Dateiversionshistorie wird von Backup-Anwendungen genutzt, um die optimierte Wiederherstellung ausgewählter Datenteilmengen aus einem Backup-Image zu ermöglichen. Die Generierung und

Verarbeitung der Dateiversionshistorie kann sowohl für das Speichersystem als auch für die Backup-Anwendung zeitaufwändig und CPU-intensiv sein.

SMTape unterstützt keinen Dateiverlauf.

Wenn Ihre Datensicherung für die Notfallwiederherstellung konfiguriert ist, bei der das gesamte Backup-Image wiederhergestellt wird, kann die Dateiverlaufsgenerierung deaktiviert werden, um die Backup-Zeit zu verkürzen. In der Dokumentation der Backup-Anwendung ist ersichtlich, ob die NDMP-Dateiverlaufsgenerierung deaktiviert werden kann.

- Die Firewall-Richtlinie für NDMP ist standardmäßig auf allen LIF-Typen aktiviert.
- Im knotenbezogenen NDMP-Modus ist zum Sichern eines FlexVol volume erforderlich, dass die Sicherungsanwendung verwendet wird, um eine Sicherung auf einem Knoten zu initiieren, dem das Volume gehört.

  Ein Backup des Root-Volumes eines Knotens ist jedoch nicht möglich.

- NDMP-Backup kann von jedem LIF aus durchgeführt werden, sofern dies durch die Firewall-Richtlinien zulässig ist.

  Wenn ein Daten-LIF verwendet wird, muss ein LIF ausgewählt werden, das nicht für Failover konfiguriert ist. Wenn ein Daten-LIF während eines NDMP-Vorgangs ein Failover durchführt, schlägt der NDMP-Vorgang fehl und muss erneut ausgeführt werden.

- Im node-scoped NDMP-Modus und im Storage Virtual Machine (SVM) scoped NDMP-Modus ohne CAB-Erweiterungsunterstützung verwendet die NDMP-Datenverbindung die gleiche LIF wie die NDMP-Steuerverbindung.
- Während der LIF-Migration werden laufende Backup- und Wiederherstellungsvorgänge unterbrochen.

  Die Sicherungs- und Wiederherstellungsvorgänge sind nach der LIF-Migration zu initiieren.

- Der NDMP-Backup-Pfad hat das Format *`/vserver_name/volume_name/path_name`*.

  `path_name` ist optional und gibt den Pfad des Verzeichnisses, der Datei oder des Snapshots an.

- Wenn ein SnapMirror Ziel mithilfe der Dump-Engine auf Band gesichert wird, werden nur die Daten im Volume gesichert.

  Wenn jedoch ein SnapMirror Ziel mit SMTape auf Band gesichert wird, werden auch die Metadaten gesichert. Die SnapMirror Beziehungen und die zugehörigen Metadaten werden nicht auf Band gesichert. Daher wird bei der Wiederherstellung nur die Daten auf diesem Volume wiederhergestellt, die zugehörigen SnapMirror Beziehungen werden jedoch nicht wiederhergestellt.

Verwandte Informationen

Was die Cluster Aware Backup Erweiterung leistet

"Systemadministration"

Umgebungsvariable

Unterstützte Umgebungsvariablen für ONTAP NDMP

Umgebungsvariablen werden verwendet, um Informationen über einen Backup- oder

Wiederherstellungsvorgang zwischen einer NDMP-fähigen Backup-Anwendung und einem Speichersystem auszutauschen.

Wenn ein Benutzer beispielsweise angibt, dass eine Backup-Anwendung ein Backup erstellen soll `/vserver1/vol1/dir1`, setzt die Backup-Anwendung die Umgebungsvariable FILESYSTEM auf `/vserver1/vol1/dir1`. Ebenso setzt die Backup-Anwendung die Umgebungsvariable LEVEL auf 1 (eins), wenn ein Benutzer angibt, dass es sich um ein Backup der Stufe 1 handeln soll.

Das Festlegen und Prüfen von Umgebungsvariablen erfolgt in der Regel transparent für Backup-Administratoren; das heißt, die Backup-Anwendung legt sie automatisch fest.

Ein Backup-Administrator legt Umgebungsvariablen selten fest; es kann jedoch erforderlich sein, den Wert einer Umgebungsvariablen gegenüber dem von der Backup-Anwendung festgelegten Wert zu ändern, um ein Funktions- oder Leistungsproblem zu charakterisieren oder zu umgehen. Beispielsweise könnte ein Administrator die Generierung des Dateiverlaufs vorübergehend deaktivieren, um festzustellen, ob die Verarbeitung von Dateiverlaufsinformationen durch die Backup-Anwendung zu Leistungsproblemen oder Funktionsproblemen beiträgt.

Viele Backup-Anwendungen bieten die Möglichkeit, Umgebungsvariablen zu überschreiben oder zu ändern oder zusätzliche Umgebungsvariablen anzugeben. Informationen dazu enthält die Dokumentation der jeweiligen Backup-Anwendung.

Von ONTAP unterstützte Umgebungsvariablen

ONTAP unterstützt Umgebungsvariablen, die jeweils einen zugeordneten Standardwert haben. Diese Standardwerte können jedoch manuell geändert werden.

Wenn Sie die von der Backup-Anwendung festgelegten Werte manuell ändern, kann sich die Anwendung unvorhersehbar verhalten. Dies liegt daran, dass die Backup- oder Wiederherstellungsvorgänge möglicherweise nicht das tun, was die Backup-Anwendung erwartet. In manchen Fällen kann eine gezielte Änderung jedoch helfen, Probleme zu identifizieren oder zu umgehen.

Die folgenden Tabellen listen die Umgebungsvariablen auf, deren Verhalten für dump und SMTape identisch ist, sowie diejenigen Variablen, die nur für dump beziehungsweise nur für SMTape unterstützt werden. Diese Tabellen enthalten außerdem Beschreibungen, wie die von ONTAP unterstützten Umgebungsvariablen funktionieren, falls diese verwendet werden:

In den meisten Fällen akzeptieren Variablen, die den Wert `Y` haben, auch `T` und `N` akzeptieren auch `F`.

Unterstützte Umgebungsvariablen für Dump und SMTape

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
DEBUG	`Y` oder `N`	`N`	Gibt an, dass Debugging-Informationen ausgegeben werden.
DATEISYSTEM	`string`	`none`	Gibt den Pfadnamen des Stammverzeichnisses der zu sichernden Daten an.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
NDMP_VERSION	`return_only`	`none`	Die Variable NDMP_VERSION sollte nicht verändert werden. Die Variable NDMP_VERSION wird vom Backup-Vorgang erstellt und gibt die NDMP-Version zurück. ONTAP setzt die Variable NDMP_VERSION während eines Backups für die interne Verwendung und zur Weitergabe an eine Backup-Anwendung zu Informationszwecken. Die NDMP-Version einer NDMP-Sitzung wird mit dieser Variable nicht festgelegt.
PATHNAME_SEPARATOR	`return_value`	`none`	Gibt das Trennzeichen für den Pfadnamen an. Dieses Zeichen hängt vom zu sichernden Dateisystem ab. Für ONTAP wird dieser Variablen das Zeichen “/” zugewiesen. Der NDMP-Server setzt diese Variable vor dem Start einer Tape-Backup-Operation.
TYP	`dump` oder `smtape`	`dump`	Gibt den Typ der unterstützten Sicherung an, der für Tape-Backup- und Wiederherstellungsvorgänge verwendet wird.
VERBOSE	`Y` oder `N`	`N`	Erhöht die Anzahl der Protokollmeldungen während der Durchführung eines Tape-Backup oder einer Tape-Wiederherstellung.

Unterstützte Umgebungsvariablen für Dump

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
ACL_START	`return_only`	`none`	Die von der Backup-Operation erzeugte Variable ACL_START ist ein Offset-Wert, der von einer Direct Access Restore- oder einer wiederaufnehmbaren NDMP Backup-Operation verwendet wird. Der Offset-Wert ist der Byte-Offset in der Dump-Datei, an dem die ACL-Daten (Pass V) beginnen und am Ende einer Sicherung zurückgegeben werden. Damit eine Wiederherstellung per Direktzugriff die gesicherten Daten korrekt wiederherstellt, muss der Wert ACL_START beim Start der Wiederherstellung an die Wiederherstellungsoperation übergeben werden. Eine NDMP wiederaufnehmbare Sicherungsoperation verwendet den Wert ACL_START, um der Backup-Anwendung mitzuteilen, wo der nicht wiederaufnehmbare Teil des Sicherungsdatenstroms beginnt.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
BASISDATUM	`0`, `-1` oder `DUMP_DATE` Wert	`-1`	Legt das Startdatum für inkrementelle Backups fest. Wenn auf `-1` gesetzt, ist der inkrementelle BASE_DATE-Spezifizierer deaktiviert. Wenn auf `0` bei einer Stufe-0-Sicherung gesetzt, sind inkrementelle Sicherungen aktiviert. Nach der ersten Sicherung wird der Wert der DUMP_DATE-Variable aus der vorherigen inkrementellen Sicherung der BASE_DATE-Variable zugewiesen. Diese Variablen stellen eine Alternative zu den auf LEVEL/UPDATE basierenden inkrementellen Backups dar.
DIREKT	`Y` oder `N`	`N`	Legt fest, dass bei einer Wiederherstellung direkt zu der Stelle auf dem Band vorgespult wird, an der sich die Dateidaten befinden, anstatt das gesamte Band zu durchsuchen. Für die Wiederherstellung per Direktzugriff muss die Backup-Anwendung Positionsinformationen bereitstellen. Wenn diese Variable auf `Y` gesetzt ist, gibt die Backup-Anwendung die Datei- oder Verzeichnisnamen und die Positionsinformationen an.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
DMP_NAME	`string`	`none`	Gibt den Namen für ein Backup mit mehreren Unterverzeichnissen an. Diese Variable ist für mehrere Teilbaum-Sicherungen obligatorisch.
DUMP_DATE	`return_value`	`none`	Diese Variable wird nicht direkt geändert. Sie wird vom Backup erstellt, wenn die Variable BASE_DATE auf einen anderen Wert als `-1` gesetzt ist. Die Variable DUMP_DATE wird berechnet, indem dem vom Backup-Programm ermittelten 32-Bit-Zeitwert der 32-Bit-Levelwert vorangestellt wird. Der Levelwert wird gegenüber dem zuletzt an die Variable BASE_DATE übergebenen Wert inkrementiert. Der resultierende Wert wird als BASE_DATE Wert bei einem nachfolgenden inkrementellen Backup verwendet.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
ENHANCED_DAR_ENABLED	`Y` oder `N`	`N`	Gibt an, ob die erweiterte DAR-Funktionalität aktiviert ist. Die erweiterte DAR-Funktionalität unterstützt Verzeichnis-DAR und DAR von Dateien mit NT Streams. Sie bietet Leistungsverbesserungen . Erweiterte DAR während der Wiederherstellung ist nur möglich, wenn die folgenden Bedingungen erfüllt sind: • ONTAP unterstützt erweitertes DAR. • Die Dateiversionshistorie ist während des Backups aktiviert (HIST=Y). • Die `ndmpd.offset_map.enable`Option ist auf `on` eingestellt. • Die Variable ENHANCED_DAR_ENABLED ist während der Wiederherstellung auf `Y` gesetzt.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
AUSSCHLIESSEN	`pattern_string`	`none`	Gibt Dateien oder Verzeichnisse an, die beim Sichern von Daten ausgeschlossen werden. Die Ausschlussliste ist eine durch Kommas getrennte Liste von Datei- oder Verzeichnisnamen. Wenn der Name einer Datei oder eines Verzeichnisses mit einem der Namen in der Liste übereinstimmt, wird es vom Backup ausgeschlossen. Für die Angabe von Namen in der Ausschlussliste gelten folgende Regeln: • Es muss der genaue Name der Datei oder des Verzeichnisses verwendet werden. • Das Sternchen (*), ein Platzhalterzeichen, muss entweder das erste oder das letzte Zeichen der Zeichenkette sein. Jede Zeichenkette darf bis zu zwei Sternchen enthalten. • Einem Komma in einem Datei- oder Verzeichnisnamen muss ein Backslash vorangestellt werden. • Die Ausschlussliste kann bis zu 32 Namen enthalten. Dateien oder Verzeichnisse, die für den Ausschluss vom

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
EXTRAKT	`Y`, `N`, oder `E`	`N`	Gibt an, dass Teilstrukturen eines gesicherten Datensatzes wiederhergestellt werden. Die Backup-Anwendung gibt die Namen der zu extrahierenden Unterverzeichnisse an. Wenn eine angegebene Datei mit einem Verzeichnis übereinstimmt, dessen Inhalt gesichert wurde, wird das Verzeichnis rekursiv extrahiert. Um eine Datei, ein Verzeichnis oder einen Qtree während der Wiederherstellung ohne Verwendung von DAR umzubenennen, muss die Umgebungsvariable EXTRACT auf `E` gesetzt werden.
EXTRACT_ACL	`Y` oder `N`	`Y`	Gibt an, dass die ACLs aus der gesicherten Datei bei einem Wiederherstellungsvorgang wiederhergestellt werden. Standardmäßig werden beim Wiederherstellen von Daten auch die ACLs wiederhergestellt, mit Ausnahme von DARs (DIRECT=Y).

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
ERZWINGEN	`Y` oder `N`	`N`	Legt fest, ob bei der Wiederherstellungsoperation der Speicherplatz und die Inode-Verfügbarkeit auf dem Zielvolume überprüft werden müssen. Das Setzen dieser Variablen auf `Y` bewirkt, dass beim Wiederherstellungsvorgang die Prüfungen auf Speicherplatz und Inode-Verfügbarkeit im Zielpfad übersprungen werden. Wenn auf dem Zielvolume nicht genügend Speicherplatz oder Inodes verfügbar sind, stellt der Wiederherstellungsvorgang so viele Daten wieder her, wie es der verfügbare Speicherplatz und die Inode-Verfügbarkeit des Zielvolumes zulassen. Der Wiederherstellungsvorgang stoppt, wenn kein Speicherplatz oder keine Inodes mehr verfügbar sind.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
GESCHICHTE	`Y` oder `N`	`N`	Legt fest, dass Dateiverlaufsinformationen an die Backup-Anwendung gesendet werden. Die meisten kommerziellen Backup-Anwendungen setzen die HIST-Variable auf `Y`. Um die Geschwindigkeit eines Backup-Vorgangs zu erhöhen oder ein Problem mit der Dateiverlaufserfassung zu beheben, kann diese Variable auf `N`gesetzt werden. Die Variable HIST sollte nicht auf `Y` gesetzt werden, wenn die Sicherungsanwendung keine Dateiverlaufsfunktion unterstützt.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
IGNORE_CTIME	`Y` oder `N`	`N`	Gibt an, dass eine Datei nicht inkrementell gesichert wird, wenn sich seit der letzten inkrementellen Sicherung nur ihr ctime-Wert geändert hat. Manche Anwendungen, wie beispielsweise Virenscanner, ändern den ctime-Wert einer Datei innerhalb des Inodes, selbst wenn die Datei oder ihre Attribute unverändert sind. Dadurch kann es vorkommen, dass bei einer inkrementellen Sicherung auch unveränderte Dateien gesichert werden. Die `IGNORE_CTIME` Variable sollte nur dann angegeben werden, wenn inkrementelle Sicherungen aufgrund der Änderung des ctime-Werts unzumutbar viel Zeit oder Speicherplatz beanspruchen.  Der `NDMP dump`Befehl setzt `IGNORE_CTIME`standardmäßig auf `false`. Die Einstellung auf `true`kann zu folgendem Datenverlust führen: 1. Wenn `IGNORE_CTI`

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
IGNORE_QTREES	`Y` oder `N`	`N`	Gibt an, dass beim Wiederherstellungsvorgang keine Qtree-Informationen aus gesicherten Qtrees wiederhergestellt werden.
EBENE	`0-31`	`0`	Legt die Sicherungsebene fest. Stufe 0 kopiert den gesamten Datensatz. Inkrementelle Sicherungsstufen, die durch Werte über 0 angegeben werden, kopieren alle Dateien (neue oder geänderte) seit der letzten inkrementellen Sicherung. Beispielsweise sichert Stufe 1 neue oder geänderte Dateien seit der Sicherung der Stufe 0, Stufe 2 neue oder geänderte Dateien seit der Sicherung der Stufe 1 und so weiter.
LISTE	`Y` oder `N`	`N`	Listet die Namen der gesicherten Dateien und die Inode-Nummern auf, ohne die Daten tatsächlich wiederherzustellen.
LIST_QTREES	`Y` oder `N`	`N`	Listet die gesicherten Qtrees auf, ohne die Daten tatsächlich wiederherzustellen.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
MULTI_SUBTREE_NAMES	`string`	`none`	Gibt an, dass es sich bei der Sicherung um eine Sicherung mehrerer Unterbäume handelt. Mehrere Teilbäume werden in der Zeichenkette angegeben, die eine durch Zeilenumbrüche getrennte, mit einem Nullbyte abgeschlossene Liste von Teilbaumnamen darstellt. Teilbäume werden durch Pfadnamen relativ zu ihrem gemeinsamen Stammverzeichnis angegeben, das als letztes Element der Liste angegeben werden muss. Wenn Sie diese Variable verwenden, müssen Sie auch die Variable DMP_NAME verwenden.
NDMP_UNICODE_ FH	`Y` oder `N`	`N`	Gibt an, dass zusätzlich zum NFS-Namen der Datei auch ein Unicode-Name in die Dateiverlaufsinformationen aufgenommen ist. Diese Option wird von den meisten Backup-Anwendungen nicht verwendet und sollte nur gesetzt werden, wenn die Backup-Anwendung für den Empfang dieser zusätzlichen Dateinamen ausgelegt ist. Die Variable HIST muss ebenfalls gesetzt werden.
NO_ACLS	`Y` oder `N`	`N`	Legt fest, dass ACLs beim Sichern von Daten nicht kopiert werden.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
NON_QUOTA_TREE	`Y` oder `N`	`N`	Legt fest, dass Dateien und Verzeichnisse in Qtrees beim Sichern von Daten ignoriert werden. Wenn auf `Y` gesetzt, werden Elemente in Qtrees des durch die Variable FILESYSTEM angegebenen Datensatzes nicht gesichert. Diese Variable hat nur eine Auswirkung, wenn die Variable FILESYSTEM ein gesamtes Volume angibt. Die Variable NON_QUOTA_TREE funktioniert nur bei einem Backup auf Level 0 und ist wirkungslos, wenn die Variable MULTI_SUBTREE_NAMES angegeben ist. Dateien oder Verzeichnisse, die für den Ausschluss vom Backup angegeben wurden, werden nicht ausgeschlossen, wenn NON_QUOTA_TREE `Y` gleichzeitig gesetzt wird.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
NOWRITE	`Y` oder `N`	`N`	Gibt an, dass beim Wiederherstellungsvorgang keine Daten auf die Festplatte geschrieben werden. Diese Variable wird zum Debugging verwendet.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
REKURSIV	`Y` oder `N`	`Y`	Legt fest, dass Verzeichniseinträge während einer DAR Wiederherstellung erweitert werden. Die Umgebungsvariablen DIRECT und ENHANCED_DAR_ENABLED müssen ebenfalls aktiviert sein (auf `Y` gesetzt). Wenn die Variable RECURSIVE deaktiviert ist (auf `N` gesetzt), werden nur die Berechtigungen und ACLs für alle Verzeichnisse im ursprünglichen Quellpfad vom Tape wiederhergestellt, nicht aber deren Inhalt. Wenn die Variable RECURSIVE auf `N` gesetzt ist oder die Variable RECOVER_FULL_PATHS auf `Y` gesetzt ist, muss der Wiederherstellungspfad mit dem ursprünglichen Pfad enden.  Wenn die Variable RECURSIVE deaktiviert ist und mehr als ein Wiederherstellungspfad vorhanden ist, müssen alle Wiederherstellungspfade im längsten der Wiederherstellungspfade enthalten

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
RECOVER_FULL_PATHS	`Y` oder `N`	`N`	Gibt an, dass nach der DAR die Berechtigungen und ACLs des vollständigen Wiederherstellungspfads wiederhergestellt werden. DIRECT und ENHANCED_DAR_ENABLED müssen ebenfalls aktiviert sein (auf `Y` gesetzt). Wenn RECOVER_FULL_PATHS auf `Y` gesetzt ist, muss der Wiederherstellungspfad mit dem ursprünglichen Pfad enden. Falls Verzeichnisse bereits auf dem Zielvolume vorhanden sind, werden deren Berechtigungen und ACLs nicht vom Tape wiederhergestellt.
AKTUALISIEREN	`Y` oder `N`	`Y`	Aktualisiert die Metadateninformationen, um LEVEL basierte inkrementelle Backups zu ermöglichen.

Für SMTape unterstützte Umgebungsvariablen

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
BASISDATUM	`DUMP_DATE`	`-1`	Legt das Startdatum für inkrementelle Backups fest. `BASE_DATE` ist eine Zeichenkettendarstellung der Referenz-Snapshot-Kennungen. Mit der `BASE_DATE`Zeichenkette wird der Referenz-Snapshot von SMTape gefunden. `BASE_DATE` ist für Basissicherungen nicht erforderlich. Für eine inkrementelle Sicherung wird der Wert der `DUMP_DATE`Variablen aus der vorherigen Basissicherung oder inkrementellen Sicherung der `BASE_DATE`Variablen zugewiesen. Die Backup-Anwendung weist den `DUMP_DATE` Wert aus einem vorherigen SMTape Baseline- oder inkrementellen Backup

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
DUMP_DATE	`return_value`	`none`	Am Ende eines SMTape-Backups enthält DUMP_DATE eine Zeichenfolgenkennung, die den für dieses Backup verwendeten Snapshot identifiziert. Dieser Snapshot kann als Referenz-Snapshot für ein nachfolgendes inkrementelles Backup verwendet werden. Der resultierende Wert von DUMP_DATE wird als BASE_DATE Wert für nachfolgende inkrementelle Backups verwendet.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifiziert die Abfolge der inkrementellen Backups, die mit dem Baseline-Backup verknüpft sind. Die Backup-Set-ID ist eine 128-Bit- eindeutige ID, die während eines Basis-Backups generiert wird. Die Backup-Anwendung weist diese ID während eines inkrementellen Backups der `SMTAPE_BACKUP_SET_ID` Variable als Eingabe zu.
SMTAPE_SNAPSHOT_NAME	Jeder gültige Snapshot, der im Volume verfügbar ist	`Invalid`	Wenn die Variable SMTAPE_SNAPSHOT_NAME auf einen Snapshot gesetzt ist, werden dieser Snapshot und seine älteren Snapshots auf Tape-Backup gesichert. Für das inkrementelle Tape-Backup gibt diese Variable den inkrementellen Snapshot an. Die Variable BASE_DATE stellt den Baseline-Snapshot bereit.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
SMTAPE_DELETE_SNAPSHOT	`Y` oder `N`	`N`	Für einen von SMTape automatisch erstellten Snapshot, wenn die Variable SMTAPE_DELETE_SNAPSHOT auf `Y` gesetzt ist, löscht SMTape diesen Snapshot nach Abschluss des Backup-Vorgangs. Ein von der Backup-Anwendung erstellter Snapshot wird jedoch nicht gelöscht.
SMTAPE_BREAK_MIRROR	`Y` oder `N`	`N`	Wenn die Variable SMTAPE_BREAK_MIRROR auf `Y` gesetzt ist, wird das Volume vom Typ `DP` nach einer erfolgreichen Wiederherstellung in ein `RW` Volume geändert.

Informationen zu gängigen ONTAP NDMP Tape-Backup-Topologien

NDMP unterstützt eine Reihe von Topologien und Konfigurationen zwischen Backup-Anwendungen und Speichersystemen oder anderen NDMP-Servern, die Daten (Dateisysteme) und Tape-Dienste bereitstellen.

Speichersystem zu lokalem Tape

In der einfachsten Konfiguration sichert eine Backup-Anwendung Daten von einem Speichersystem auf ein an das Speichersystem angeschlossenes Tape-Subsystem. Die NDMP-Steuerverbindung besteht über die Netzwerkgrenze. Die NDMP-Datenverbindung, die innerhalb des Speichersystems zwischen den Daten- und Tape-Diensten besteht, wird als NDMP-Lokalkonfiguration bezeichnet.

Speichersystem zu Tape-Anbindung an ein anderes Speichersystem

Eine Backup-Anwendung kann Daten von einem Speichersystem auch auf eine Tape-Bibliothek (einen Medienwechsler mit einem oder mehreren Tape-Laufwerken) sichern, die an ein anderes Speichersystem angeschlossen ist. In diesem Fall wird die NDMP-Datenverbindung zwischen den Daten- und Tape-Diensten durch eine TCP- oder TCP/IPv6-Netzwerkverbindung bereitgestellt. Dies wird als NDMP Three-Way Storage System-to-Storage System Konfiguration bezeichnet.

Speichersystem zu netzwerkgebundener Tape-Bibliothek

NDMP-fähige Tape-Bibliotheken bieten eine Variante der Drei-Wege-Konfiguration. In diesem Fall ist die Tape-Bibliothek direkt an das TCP/IP-Netzwerk angeschlossen und kommuniziert über einen internen NDMP-Server mit der Backup-Anwendung und dem Speichersystem.

Speichersystem zu Datenserver zu Tape oder Datenserver zu Speichersystem zu Tape

NDMP unterstützt auch Speichersystem-zu-Datenserver- und Datenserver-zu-Speichersystem-

Dreierkonfigurationen, wobei diese Varianten weniger verbreitet sind. Speichersystem-zu-Server ermöglicht, dass Speichersystemdaten auf eine an den Backup-Anwendungs-Host angeschlossene Tape-Bibliothek oder auf ein anderes Datenserversystem gesichert werden. Die Server-zu-Speichersystem-Konfiguration ermöglicht die Sicherung von Serverdaten auf eine an das Speichersystem angeschlossene Tape-Bibliothek.

ONTAP unterstützte NDMP-Authentifizierungsverfahren

Sie können ein Authentifizierungsverfahren für NDMP-Verbindungsanfragen festlegen. ONTAP unterstützt zwei Methoden zur Authentifizierung des NDMP-Zugriffs auf ein Speichersystem: Klartext und Challenge.

Im knotenbezogenen NDMP-Modus sind sowohl Challenge als auch Klartext standardmäßig aktiviert. Challenge kann jedoch nicht deaktiviert werden. Klartext kann aktiviert und deaktiviert werden. Im Klartext-Authentifizierungsverfahren wird das Anmeldekennwort als Klartext übertragen.

Im Storage Virtual Machine (SVM)-bezogenen NDMP-Modus ist das Authentifizierungsverfahren standardmäßig Challenge. Im Gegensatz zum node-bezogenen NDMP-Modus können in diesem Modus sowohl Klartext- als auch Challenge-Authentifizierungsverfahren aktiviert und deaktiviert werden.

Verwandte Informationen

Benutzerauthentifizierung im knotenbezogenen NDMP-Modus

Benutzerauthentifizierung im SVM-bezogenen NDMP-Modus

Von ONTAP unterstützte NDMP-Erweiterungen

NDMP v4 bietet einen Mechanismus zur Erstellung von NDMP v4-Protokollerweiterungen, ohne das Kernprotokoll von NDMP v4 zu verändern. Es ist wichtig, die von ONTAP unterstützten NDMP v4-Erweiterungen zu kennen.

Die folgenden NDMP v4-Erweiterungen werden von ONTAP unterstützt:

- Cluster Aware Backup (CAB)

  Diese Erweiterung wird nur im SVM-basierten NDMP-Modus unterstützt.

- Connection Address Extension (CAE) für IPv6-Unterstützung
- Erweiterungsklasse 0x2050

  Diese Erweiterung unterstützt wiederaufnehmbare Sicherungsvorgänge und Snapshot-Verwaltungserweiterungen.

  Die `NDMP_SNAP_RECOVER` Nachricht, die Teil der Snapshot Management Extensions ist, wird verwendet, um einen Wiederherstellungsvorgang einzuleiten und die wiederhergestellten Daten von einem lokalen Snapshot an einen Speicherort im lokalen Dateisystem zu übertragen. In ONTAP ermöglicht diese Nachricht die Wiederherstellung von Volumes und regulären Dateien.

  Die `NDMP_SNAP_DIR_LIST`Meldung ermöglicht das Durchsuchen der Snapshots eines Volumes. Falls während eines laufenden Durchsuchungsvorgangs eine unterbrechungsfreie Operation erfolgt, muss die Backup-Anwendung den Durchsuchungsvorgang erneut initiieren.

- NDMP-Erweiterung für wiederanlaufbare Backups

  Die NDMP-Funktion „Restartable Backup Extension“ (RBE) ermöglicht es, ein Tape-Backup von einem bekannten Prüfpunkt im Datentransfer vor dem Ausfall neu zu starten.

Informationen zu den erweiterten DAR-Funktionen für ONTAP NDMP

Sie können die erweiterte Funktion zur direkten Zugriffswiederherstellung (DAR) für Verzeichnis DAR sowie für DAR von Dateien und NT-Streams verwenden. Die erweiterte DAR-Funktionalität ist standardmäßig aktiviert.

Die Aktivierung der erweiterten DAR-Funktionalität kann die Backup-Performance beeinträchtigen, da eine Offset-Zuordnung erstellt und auf Tape geschrieben werden muss. Die erweiterte DAR-Funktionalität kann sowohl im Node-basierten als auch im Storage Virtual Machine (SVM)-basierten NDMP-Modus aktiviert oder deaktiviert werden.

ONTAP Skalierbarkeitsgrenzen für NDMP-Sitzungen

Sie müssen sich der maximalen Anzahl von NDMP-Sitzungen bewusst sein, die gleichzeitig auf Speichersystemen mit unterschiedlicher System-Speicherkapazität eingerichtet werden können. Diese maximale Anzahl hängt vom Systemspeicher eines Speichersystems ab.

Die in der folgenden Tabelle genannten Grenzwerte gelten für den NDMP-Server. Die im Abschnitt „Skalierbarkeitsgrenzen für Dump-Backup- und Wiederherstellungssitzungen“ genannten Grenzwerte gelten für die Dump- und Wiederherstellungssitzung.

Skalierbarkeitsgrenzen für Dump-Backup und Wiederherstellungssitzungen

Systemspeicher eines Speichersystems	Maximale Anzahl von NDMP-Sitzungen
Weniger als 16 GB	8
Größer oder gleich 16 GB, aber kleiner als 24 GB	20
Größer oder gleich 24 GB	36

Sie können den Systemspeicher Ihres Speichersystems mithilfe des `sysconfig -a` Befehls (verfügbar über die nodeshell) abrufen. Weitere Informationen zu `sysconfig -a` finden sich in der "ONTAP-Befehlsreferenz".

Informationen zur NDMP-Unterstützung mit ONTAP FlexGroup Volumes

Ab ONTAP 9.7 wird NDMP auf FlexGroup Volumes unterstützt.

Ab ONTAP 9.7 wird der Befehl ndmpcopy für den Datentransfer zwischen FlexVol und FlexGroup Volumes unterstützt.

Wenn von ONTAP 9.7 auf eine frühere Version zurückgekehrt wird, bleiben die inkrementellen Übertragungsinformationen der vorherigen Übertragungen nicht erhalten, sodass nach der Rückkehr eine Basiskopie durchgeführt werden muss.

Ab ONTAP 9.8 werden die folgenden NDMP-Funktionen auf FlexGroup Volumes unterstützt:

- Die NDMP_SNAP_RECOVER-Nachricht in der Erweiterungsklasse 0x2050 kann zur Wiederherstellung einzelner Dateien in einem FlexGroup Volume verwendet werden.
- Die NDMP-Erweiterung für wiederaufnehmbare Backups (RBE) wird für FlexGroup Volumes unterstützt.
- Die Umgebungsvariablen EXCLUDE und MULTI_SUBTREE_NAMES werden für FlexGroup Volumes unterstützt.

Informationen zu NDMP mit ONTAP SnapLock Volumes

Durch das Erstellen mehrerer Kopien regulierter Daten ergeben sich redundante Wiederherstellungsszenarien, und mithilfe von NDMP-Dump und -Restore ist es möglich, die Write Once, Read Many (WORM)-Eigenschaften der Quelldateien auf einem SnapLock Volume zu erhalten.

Die WORM-Attribute der Dateien auf einem SnapLock Volume bleiben beim Sichern, Wiederherstellen und Kopieren von Daten erhalten, jedoch werden WORM-Attribute nur bei der Wiederherstellung auf ein SnapLock Volume durchgesetzt. Wenn eine Sicherung von einem SnapLock Volume auf ein anderes Volume als ein SnapLock Volume wiederhergestellt wird, bleiben die WORM-Attribute zwar erhalten, werden jedoch ignoriert und von ONTAP nicht durchgesetzt.

Knotenbezogenen NDMP-Modus für FlexVol Volumes verwalten

Informationen zur Verwaltung des ONTAP node-scoped NDMP-Modus für FlexVol Volumes

NDMP kann auf Knotenebene mithilfe von NDMP-Optionen und NDMP-Befehlen verwaltet werden. Die NDMP-Optionen können mit dem `options` Befehl geändert werden. Für den Zugriff auf ein Speichersystem zur Durchführung von Tape-Backup- und Wiederherstellungsvorgängen sind NDMP-spezifische Anmeldeinformationen erforderlich.

Weitere Informationen zu `options` finden sich in der "ONTAP-Befehlsreferenz".

Befehle zur Verwaltung des ONTAP node-scoped NDMP-Modus

Die `system services ndmp`Befehle können zur Verwaltung von NDMP auf Knotenebene verwendet werden. Einige dieser Befehle sind veraltet und werden in einer zukünftigen Hauptversion entfernt.

Die folgenden NDMP-Befehle können nur auf der erweiterten Berechtigungsstufe verwendet werden:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NDMP-Service aktivieren	`system services ndmp on*`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NDMP-Service deaktivieren	`system services ndmp off*`
NDMP-Konfiguration anzeigen	`system services ndmp show*`
NDMP-Konfiguration ändern	`system services ndmp modify*`
Die Standard-NDMP-Version wird angezeigt	`system services ndmp version*`
NDMP-Service-Konfiguration anzeigen	`system services ndmp service show`
NDMP-Service-Konfiguration ändern	`system services ndmp service modify`
Alle NDMP-Sitzungen werden angezeigt	`system services ndmp status`
Detaillierte Informationen zu allen NDMP-Sitzungen	`system services ndmp probe`
Die angegebene NDMP-Sitzung wird beendet	`system services ndmp kill`
Alle NDMP-Sitzungen beenden	`system services ndmp kill-all`
Das NDMP-Passwort ändern	`system services ndmp password*`
Knotenbezogener NDMP-Modus	`system services ndmp node-scope-mode on*`
Node-spezifischen NDMP-Modus deaktivieren	`system services ndmp node-scope-mode off*`
Status des node-scoped NDMP-Modus anzeigen	`system services ndmp node-scope-mode status*`
Alle NDMP-Sitzungen zwangsweise beenden	`system services ndmp service terminate`
NDMP-Service-Daemon starten	`system services ndmp service start`
Den NDMP-Service-Daemon anhalten	`system services ndmp service stop`
Protokollierung für die angegebene NDMP-Sitzung starten	`system services ndmp log start*`
Protokollierung für die angegebene NDMP-Sitzung beenden	`system services ndmp log stop*`

- Diese Befehle sind veraltet und werden in einer zukünftigen Hauptversion entfernt.

Weitere Informationen zu `system services ndmp` finden sich in der "ONTAP-Befehlsreferenz".

Benutzerauthentifizierung im knotenbezogenen NDMP-Modus

Im knotenbezogenen NDMP-Modus müssen NDMP-spezifische Anmeldeinformationen verwendet werden, um auf ein Speichersystem zuzugreifen und Tape-Backup- sowie Wiederherstellungsvorgänge durchzuführen.

Die Standardbenutzer-ID ist „root“. Vor der Verwendung von NDMP auf einem Node muss sichergestellt werden, dass das Standard-NDMP-Passwort, das dem NDMP-Benutzer zugeordnet ist, geändert wird. Auch die Standard-NDMP-Benutzer-ID kann geändert werden.

Verwandte Informationen

Befehle zur Verwaltung des node-scoped NDMP-Modus

Was der knotenbezogene NDMP-Modus ist

NDMP-Modus mit SVM-Umfang für FlexVol Volumes verwalten

Informationen zur Verwaltung des ONTAP SVM-basierten NDMP-Modus für FlexVol volumes

NDMP kann für jede SVM mithilfe der NDMP-Optionen und -Befehle verwaltet werden. Die NDMP-Optionen können mit dem `vserver services ndmp modify` Befehl geändert werden. Im SVM-bezogenen NDMP-Modus ist die Benutzerauthentifizierung in die rollenbasierte Zugriffssteuerung integriert.

NDMP kann mit dem `vserver modify` Befehl zur Liste der zulässigen oder unzulässigen Protokolle hinzugefügt werden. Standardmäßig befindet sich NDMP in der Liste der zulässigen Protokolle. Wenn NDMP zur Liste der unzulässigen Protokolle hinzugefügt wird, können NDMP-Sitzungen nicht hergestellt werden.

Sie können den LIF-Typ, auf dem eine NDMP-Datenverbindung hergestellt wird, mithilfe der `-preferred -interface-role` Option steuern. Während des Aufbaus einer NDMP-Datenverbindung wählt NDMP eine IP-Adresse, die dem durch diese Option angegebenen LIF-Typ zugeordnet ist. Wenn die IP-Adressen zu keinem dieser LIF-Typen gehören, kann die NDMP-Datenverbindung nicht hergestellt werden. Weitere Informationen zu `vserver services ndmp modify` finden sich in der "ONTAP-Befehlsreferenz".

Befehle zur Verwaltung des ONTAP SVM-basierten NDMP-Modus

Mit den `vserver services ndmp`Befehlen lässt sich NDMP auf jeder Storage Virtual Machine (SVM, früher bekannt als Vserver) verwalten.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NDMP-Service aktivieren	`vserver services ndmp on` NDMP-Service muss auf allen Knoten in einem Cluster immer aktiviert sein. NDMP-Service kann auf einem Knoten mit dem `system services ndmp on` Befehl aktiviert werden. Standardmäßig ist der NDMP-Service auf einem Knoten immer aktiviert.
NDMP-Service deaktivieren	`vserver services ndmp off`
NDMP-Konfiguration anzeigen	`vserver services ndmp show`
NDMP-Konfiguration ändern	`vserver services ndmp modify`
Standardmäßige NDMP-Version	`vserver services ndmp version`
Alle NDMP-Sitzungen werden angezeigt	`vserver services ndmp status`
Detaillierte Informationen zu allen NDMP-Sitzungen	`vserver services ndmp probe`
Eine bestimmte NDMP-Sitzung beenden	`vserver services ndmp kill`
Alle NDMP-Sitzungen beenden	`vserver services ndmp kill-all`
Das NDMP-Passwort generieren	`vserver services ndmp generate-password`

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
NDMP-Erweiterungsstatus anzeigen	`vserver services ndmp extensions show` Dieser Befehl ist auf der Stufe „Erweiterte Berechtigungen“ verfügbar.
NDMP-Erweiterungsstatus (aktivieren oder deaktivieren) ändern	`vserver services ndmp extensions modify` Dieser Befehl ist auf der Stufe „Erweiterte Berechtigungen“ verfügbar.
Protokollierung für die angegebene NDMP-Sitzung starten	`vserver services ndmp log start` Dieser Befehl ist auf der Stufe „Erweiterte Berechtigungen“ verfügbar.
Protokollierung für die angegebene NDMP-Sitzung beenden	`vserver services ndmp log stop` Dieser Befehl ist auf der Stufe „Erweiterte Berechtigungen“ verfügbar.

Weitere Informationen zu `vserver services ndmp` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Befehle zur Verwaltung des SVM-scoped NDMP-Modus

Was die Cluster Aware Backup Erweiterung leistet

Was SVM-basierter NDMP-Modus ist

"Systemadministration"

Informationen zur Cluster Aware Backup Erweiterung für ONTAP NDMP

CAB (Cluster Aware Backup) ist eine Erweiterung des NDMP v4-Protokolls. Diese Erweiterung ermöglicht dem NDMP-Server, eine Datenverbindung auf einem Knoten herzustellen, der ein Volume besitzt. Dies ermöglicht der Backup-Anwendung außerdem festzustellen, ob sich Volumes und Tape-Geräte auf demselben Knoten in einem Cluster befinden.

Damit der NDMP-Server den Knoten, dem ein Volume gehört, identifizieren und eine Datenverbindung zu diesem Knoten herstellen kann, muss die Backup-Anwendung die CAB-Erweiterung unterstützen. Die CAB-Erweiterung erfordert, dass die Backup-Anwendung den NDMP-Server vor dem Aufbau der Datenverbindung über das zu sichernde oder wiederherzustellende Volume informiert. Dadurch kann der NDMP-Server den Knoten, auf dem sich das Volume befindet, ermitteln und die Datenverbindung entsprechend herstellen.

Dank der von der Backup-Anwendung unterstützten CAB-Erweiterung stellt der NDMP-Server Affinitätsinformationen über Volumes und Tape-Geräte bereit. Mithilfe dieser Affinitätsinformationen kann die Backup-Anwendung ein lokales Backup anstelle eines Dreiwege-Backups durchführen, wenn sich ein Volume und ein Tape-Gerät auf demselben Node in einem Cluster befinden.

Verfügbarkeit von ONTAP Volumes und Tape-Geräten für Backup und Wiederherstellung auf verschiedenen LIF-Typen

Sie können eine Backup-Anwendung so konfigurieren, dass sie eine NDMP-Steuerungsverbindung auf jedem LIF-Typ in einem Cluster herstellt. Im NDMP-Modus mit Storage Virtual Machine (SVM)-Bezug lässt sich die Verfügbarkeit von Volumes und Tape-Geräten für Backup- und Restore-Vorgänge abhängig von diesen LIF-Typen und dem Status der CAB-Erweiterung bestimmen.

Die folgenden Tabellen zeigen die Verfügbarkeit von Volumes und Tape-Geräten für NDMP-Steuerungsverbindungs-LIF-Typen und den Status der CAB-Erweiterung:

Verfügbarkeit von Volumes und Tape-Geräten, wenn die CAB-Erweiterung von der Backup-Anwendung nicht unterstützt wird

NDMP-Steuerverbindung LIF-Typ	Verfügbare Volumes für Backup oder Restore	Tape-Geräte für Backup oder Wiederherstellung verfügbar
Node-Management-LIF	Alle von einem Knoten gehosteten Volumes	Tape-Geräte, die mit dem Knoten verbunden sind, auf dem die Node-Management-LIF gehostet wird
Data LIF	Nur Volumes, die zu der SVM gehören, die von einem Knoten gehostet wird, der die Daten-LIF hostet	Keine
Cluster-Management LIF	Alle Volumes, die von einem Knoten gehostet werden, der das Cluster-Management-LIF hostet	Keine
Intercluster-LIF	Alle Volumes, die von einem Knoten gehostet werden, der das Intercluster-LIF hostet	Tape-Geräte, die mit dem Knoten verbunden sind, der das Intercluster-LIF hostet

Verfügbarkeit von Volumes und Tape-Geräten, wenn die CAB-Erweiterung von der Backup-Anwendung unterstützt wird

NDMP-Steuerverbindung LIF-Typ	Verfügbare Volumes für Backup oder Restore	Tape-Geräte für Backup oder Wiederherstellung verfügbar
Node-Management-LIF	Alle von einem Knoten gehosteten Volumes	Tape-Geräte, die mit dem Knoten verbunden sind, auf dem die Node-Management-LIF gehostet wird
Data LIF	Alle Volumes, die zu der SVM gehören, die die Daten-LIF hostet	Keine
Cluster-Management LIF	Alle Volumes im Cluster	Alle Tape-Geräte im Cluster
Intercluster-LIF	Alle Volumes im Cluster	Alle Tape-Geräte im Cluster

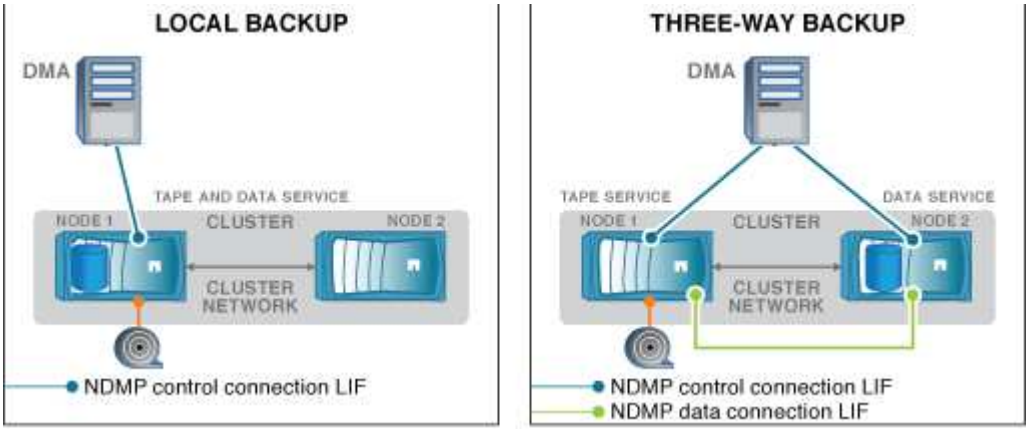
Informationen zu Affinität für ONTAP NDMP

Da die Backup-Anwendung CAB-fähig ist, liefert der NDMP-Server eindeutige Standortinformationen zu Volumes und Tape-Geräten. Mithilfe dieser Affinitätsinformationen kann die Backup-Anwendung ein lokales Backup anstelle eines

Three-Way-Backups durchführen, wenn ein Volume und ein Tape-Gerät die gleiche Affinität aufweisen.

Wenn die NDMP-Steuerungsverbindung auf einem Knotenverwaltungs-LIF, Clusterverwaltungs-LIF oder einem Intercluster-LIF hergestellt ist, kann die Sicherungsanwendung anhand der Affinitätsinformationen feststellen, ob sich ein Volume und ein Tape-Gerät auf demselben Knoten befinden und anschließend entweder eine lokale oder eine Drei-Wege-Sicherung oder -Wiederherstellung durchführen. Wenn die NDMP-Steuerungsverbindung auf einem Daten-LIF hergestellt ist, führt die Sicherungsanwendung immer eine Drei-Wege-Sicherung durch.

Lokale NDMP Backup und Three-way NDMP Backup



Anhand der Affinitätsinformationen zu Volumes und Tape-Geräten führt die DMA (Backup-Anwendung) ein lokales NDMP-Backup auf dem Volume und Tape-Gerät auf Node 1 im Cluster durch. Wenn das Volume von Node 1 auf Node 2 verschoben wird, ändern sich die Affinitätsinformationen zu Volume und Tape-Gerät. Daher wird für ein nachfolgendes Backup von der DMA eine Three-Way-NDMP-Backup-Operation durchgeführt. Dadurch bleibt die Backup-Richtlinie für das Volume unabhängig davon erhalten, auf welchen Node das Volume verschoben wird.

Verwandte Informationen

Was die Cluster Aware Backup Erweiterung leistet

Der NDMP-Server unterstützt sichere ONTAP Steuerungsverbindungen im SVM-Bereichsmodus

Zwischen der Datenverwaltungsanwendung (DMA) und dem NDMP-Server kann eine sichere Steuerverbindung mittels Secure Sockets (SSL/TLS) als Kommunikationsmechanismus hergestellt werden. Diese SSL-Kommunikation basiert auf den Serverzertifikaten. Der NDMP-Server lauscht auf Port 30000 (von der IANA für den „ndmps“-Dienst zugewiesen).

Nachdem die Verbindung vom Client über diesen Port hergestellt wurde, folgt der standardmäßige SSL-Handschlag, bei dem der Server dem Client das Zertifikat präsentiert. Wenn der Client das Zertifikat akzeptiert, ist der SSL-Handschlag abgeschlossen. Nach Abschluss dieses Prozesses ist die gesamte Kommunikation zwischen Client und Server verschlüsselt. Der NDMP-Protokoll-Workflow bleibt unverändert. Die sichere NDMP-Verbindung erfordert lediglich eine serverseitige Zertifikatsauthentifizierung. Ein DMA kann wählen, ob die Verbindung zum sicheren NDMP-Service oder zum standardmäßigen NDMP-Service hergestellt wird.

Der sichere NDMP-Service ist für eine Storage Virtual Machine (SVM) standardmäßig deaktiviert. Der sichere NDMP-Service kann für eine bestimmte SVM mithilfe des `vserver services ndmp modify -vserver`

`vserver -is-secure-control-connection-enabled [true|false]` Befehls aktiviert oder deaktiviert werden.

NDMP ONTAP Datenverbindungstypen

Im NDMP-Modus mit SVM-Bezug hängen die unterstützten NDMP-Datenverbindungstypen vom LIF-Typ der NDMP-Steuerungsverbindung und dem Status der CAB-Erweiterung ab. Dieser NDMP-Datenverbindungstyp gibt an, ob eine lokale oder eine Drei-Wege-NDMP-Sicherung oder -Wiederherstellung möglich ist.

Sie können eine dreiseitige NDMP-Sicherung oder Wiederherstellung über ein TCP- oder TCP/IPv6-Netzwerk durchführen. Die folgenden Tabellen zeigen die NDMP-Datenverbindungstypen basierend auf dem LIF-Typ der NDMP-Steuerverbindung und dem Status der CAB-Erweiterung.

NDMP-Datenverbindungstyp, wenn die CAB-Erweiterung von der Sicherungsanwendung unterstützt wird

NDMP-Steuerverbindung LIF-Typ	NDMP-Datenverbindungstyp
Node-Management-LIF	LOKAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-Management LIF	LOKAL, TCP, TCP/IPv6
Intercluster-LIF	LOKAL, TCP, TCP/IPv6

NDMP-Datenverbindungstyp, wenn die CAB-Erweiterung von der Backup-Anwendung nicht unterstützt wird

NDMP-Steuerverbindung LIF-Typ	NDMP-Datenverbindungstyp
Node-Management-LIF	LOKAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-Management LIF	TCP, TCP/IPv6
Intercluster-LIF	LOKAL, TCP, TCP/IPv6

Verwandte Informationen

Was die Cluster Aware Backup Erweiterung leistet

"Netzwerkmanagement"

ONTAP Benutzerauthentifizierung im SVM-basierten NDMP-Modus

Im Storage Virtual Machine (SVM)-bezogenen NDMP-Modus ist die NDMP-Benutzerauthentifizierung in die rollenbasierte Zugriffssteuerung integriert. Im SVM-Kontext muss der NDMP-Benutzer entweder die Rolle „vsadmin“ oder „vsadmin-backup“ haben. Im Cluster-Kontext muss der NDMP-Benutzer entweder die Rolle „admin“ oder „backup“ haben.

Abgesehen von diesen vordefinierten Rollen kann ein Benutzerkonto, das einer benutzerdefinierten Rolle zugeordnet ist, auch für die NDMP-Authentifizierung verwendet werden, vorausgesetzt, die benutzerdefinierte Rolle verfügt über den Ordner „`vserver services ndmp`“ in ihrem Befehlsverzeichnis und die Zugangsstufe des Ordners ist nicht „`none`“. In diesem Modus müssen Sie ein NDMP-Passwort für ein bestimmtes

Benutzerkonto generieren, das über die rollenbasierte Zugriffssteuerung erstellt wurde. Cluster-Benutzer in einer Admin- oder Backup-Rolle können auf eine Node-Management-LIF, eine Cluster-Management-LIF oder eine Intercluster-LIF zugreifen. Benutzer in einer vsadmin-backup- oder vsadmin-Rolle können nur auf die Daten-LIF für diese SVM zugreifen. Daher variiert je nach Rolle eines Benutzers die Verfügbarkeit von Volumes und Tape-Geräten für Backup- und Restore-Vorgänge.

Dieser Modus unterstützt auch die Benutzerauthentifizierung für NIS- und LDAP-Benutzer. Daher können NIS- und LDAP-Benutzer mit einer gemeinsamen Benutzerkennung und einem gemeinsamen Passwort auf mehrere SVMs zugreifen. Die NDMP-Authentifizierung unterstützt jedoch keine Active Directory-Benutzer.

In diesem Modus muss ein Benutzerkonto mit der SSH-Anwendung und dem Authentifizierungsverfahren „Benutzerpasswort“ verknüpft sein.

Verwandte Informationen

Befehle zur Verwaltung des SVM-scoped NDMP-Modus

"Systemadministration"

Ein NDMP-spezifisches Passwort für ONTAP NDMP Benutzer generieren

Im Storage Virtual Machine (SVM)-bezogenen NDMP-Modus muss ein Passwort für eine bestimmte Benutzer-ID generiert werden. Das generierte Passwort basiert auf dem tatsächlichen Anmeldepasswort des NDMP-Benutzers. Wenn sich das tatsächliche Anmeldepasswort ändert, muss das NDMP-spezifische Passwort erneut generiert werden.

Schritte

1. Mit dem `vserver services ndmp generate-password` Befehl lässt sich ein NDMP-spezifisches Passwort generieren.

   Dieses Passwort kann in allen aktuellen oder zukünftigen NDMP-Operationen verwendet werden, die eine Passworteingabe erfordern.

   > Im Kontext der Storage Virtual Machine (SVM, früher bekannt als Vserver) können NDMP-Passwörter nur für Benutzer generiert werden, die zu dieser SVM gehören.

   Das folgende Beispiel zeigt, wie ein NDMP-spezifisches Passwort für die Benutzer-ID user1 generiert wird:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. Wenn Sie das Passwort für Ihr reguläres Speichersystemkonto ändern, wiederholen Sie dieses Verfahren, um Ihr neues NDMP-spezifisches Passwort zu erhalten.

Wie Tape-Backup und Wiederherstellungsvorgänge während der Notfallwiederherstellung in ONTAP MetroCluster Konfigurationen beeinflusst werden

Tape-Backup- und Wiederherstellungsvorgänge können während der Notfallwiederherstellung in einer MetroCluster Konfiguration gleichzeitig durchgeführt werden. Es ist wichtig zu verstehen, wie diese Vorgänge während der Notfallwiederherstellung beeinflusst werden.

Wenn Tape-Backup- und Wiederherstellungsvorgänge auf einem Volume einer SVM in einer Disaster-Recovery-Beziehung durchgeführt werden, können nach einem Switchover und Switchback weiterhin inkrementelle Tape-Backup- und Wiederherstellungsvorgänge durchgeführt werden.

Über die Dump-Engine für FlexVol Volumes

Informationen zur ONTAP Dump Engine für FlexVol Volumes

Dump ist eine Snapshot-basierte Backup und Recovery Lösung von ONTAP, die das Sichern von Dateien und Verzeichnissen aus einem Snapshot auf ein Tape-Gerät sowie das Wiederherstellen der gesicherten Daten auf ein Speichersystem ermöglicht.

Sie können Ihre Dateisystemdaten, wie Verzeichnisse, Dateien und deren zugehörige Sicherheitseinstellungen, mithilfe der Dump-Sicherung auf ein Tape-Gerät sichern. Es ist möglich, ein gesamtes Volume, einen gesamten Qtree oder einen Teilbaum zu sichern, der weder ein gesamtes Volume noch ein gesamter Qtree ist.

Ein Dump-Backup oder eine Wiederherstellung kann mit NDMP-kompatiblen Backup-Anwendungen durchgeführt werden.

Wenn Sie ein Dump-Backup durchführen, können Sie den für das Backup zu verwendenden Snapshot angeben. Wenn Sie keinen Snapshot für das Backup angeben, erstellt die Dump-Engine einen Snapshot für das Backup. Nach Abschluss der Sicherungsoperation löscht die Speicherabbildsicherung diesen Snapshot.

Mit der Dump-Engine sind Level-0-, inkrementelle oder differentielle Backups auf Tape möglich.

Verwandte Informationen

"Upgrade, Zurücksetzen oder Downgrade"

Wie eine Dump-Sicherung mit ONTAP NDMP funktioniert

Eine Dump-Sicherung schreibt Dateisystemdaten mithilfe eines vordefinierten Prozesses von der Festplatte auf Band. Es ist möglich, ein Volume, einen Qtree oder einen Teilbaum zu sichern, der weder ein vollständiges Volume noch ein vollständiger Qtree ist.

Die folgende Tabelle beschreibt den Prozess, den ONTAP verwendet, um das durch den Dump-Pfad angegebene Objekt zu sichern:

Stufe	Aktion
1	Bei weniger als vollständigen Volume- oder vollständigen Qtree-Backups durchsucht ONTAP die Verzeichnisse, um die zu sichernden Dateien zu identifizieren. Beim Backup eines gesamten Volumes oder Qtrees kombiniert ONTAP diese Phase mit Phase 2.

Stufe	Aktion
2	Bei einer vollständigen Volume- oder vollständigen Qtree-Sicherung identifiziert ONTAP die zu sichernden Verzeichnisse in den Volumes oder Qtrees.
3	ONTAP schreibt die Verzeichnisse auf Band.
4	ONTAP schreibt die Dateien auf Band.
5	ONTAP schreibt die ACL-Informationen (falls zutreffend) auf Tape.

Die Dump-Sicherung verwendet eine Snapshot-Kopie Ihrer Daten für das Backup. Daher ist es nicht erforderlich, das Volume vor dem Start des Backups offline zu nehmen.

Die Speicherabbildsicherung benennt jeden Snapshot, den sie erstellt, als `snapshot_for_backup.n`, wobei `n` eine ganze Zahl ist, die bei 0 beginnt. Jedes Mal, wenn die Speicherabbildsicherung einen Snapshot erstellt, wird die Zahl um 1 erhöht. Die Zahl wird nach einem Neustart des Speichersystems auf 0 zurückgesetzt. Nach Abschluss der Sicherungsoperation löscht die Speicherabbildsicherung diesen Snapshot.

Wenn ONTAP mehrere Dump-Backups gleichzeitig durchführt, erstellt die Dump-Engine mehrere Snapshots. Wenn ONTAP zwei Dump-Backups gleichzeitig ausführt, finden sich die folgenden Snapshots in den Volumes, von denen Daten gesichert werden: `snapshot_for_backup.0` und `snapshot_for_backup.1`.

Beim Backup von einem Snapshot erstellt die Dump-Engine keinen zusätzlichen Snapshot.

Datentypen, die die Dump-Engine sichert

Die Dump-Engine ermöglicht es, Daten auf Band zu sichern, um sich gegen Katastrophen oder Controller-Ausfälle abzusichern. Zusätzlich zur Sicherung von Datenobjekten wie Dateien, Verzeichnissen, Qtrees oder ganzen Volumes kann die Dump-Engine viele Arten von Informationen zu jeder Datei sichern. Kenntnisse über die Datentypen, die die Dump-Engine sichern kann, sowie die zu berücksichtigenden Einschränkungen können bei der Planung des Ansatzes zur Notfallwiederherstellung helfen.

Zusätzlich zur Datensicherung in Dateien kann die Dump-Engine gegebenenfalls folgende Informationen zu jeder Datei sichern:

- UNIX-GID, Besitzer-UID und Dateiberechtigungen
- UNIX-Zugriffs-, Erstellungs- und Änderungszeit
- Dateityp
- Dateigröße
- DOS-Name, DOS-Attribute und Erstellungszeit
- Zugriffskontrolllisten (ACLs) mit 1.024 Zugriffskontrolleinträgen (ACEs)
- Qtree-Informationen
- Junction-Pfade

  Junction-Pfade werden als symbolische Links gesichert.

- LUN und LUN-Klone

  Sie können ein gesamtes LUN-Objekt sichern; jedoch kann keine einzelne Datei innerhalb des LUN-Objekts gesichert werden. Ebenso kann ein gesamtes LUN-Objekt wiederhergestellt werden, jedoch keine einzelne Datei innerhalb des LUN-Objekts.

Die Dump-Engine sichert LUN-Klone als unabhängige LUNs.

- VM-ausgerichtete Dateien

Wenn ein durch Snapshot gesicherter LUN-Klon von Data ONTAP im 7-Mode auf ONTAP migriert wird, wird er zu einer inkonsistenten LUN. Der Dump-Engine sichert inkonsistente LUNs nicht.

Bei der Wiederherstellung von Daten auf einem Volume ist die Client-E/A für die wiederherzustellenden LUNs eingeschränkt. Die LUN-Einschränkung wird erst aufgehoben, wenn der Dump-Wiederherstellungsvorgang abgeschlossen ist. Ebenso ist während eines SnapMirror Single File- oder LUN-Wiederherstellungsvorgangs die Client-E/A sowohl für die wiederherzustellenden Dateien als auch für die wiederherzustellenden LUNs eingeschränkt. Diese Einschränkung wird erst aufgehoben, wenn der Single File- oder LUN-Wiederherstellungsvorgang abgeschlossen ist. Wenn eine Dump-Sicherung auf einem Volume durchgeführt wird, auf dem gerade ein Dump-Wiederherstellungs- oder SnapMirror Single File- oder LUN-Wiederherstellungsvorgang läuft, werden die Dateien oder LUNs mit Client-E/A-Einschränkung nicht in die Sicherung aufgenommen. Diese Dateien oder LUNs werden in einer nachfolgenden Sicherung berücksichtigt, wenn die Client-E/A-Einschränkung aufgehoben ist.

Wenn ein SnapVault sekundäres Volume oder ein Volume SnapMirror Ziel auf Band gesichert wird, werden nur die Daten auf dem Volume gesichert. Die zugehörigen Metadaten werden nicht gesichert. Daher werden beim Wiederherstellen des Volumes nur die Daten auf diesem Volume wiederhergestellt. Informationen über die Volume SnapMirror Beziehungen sind in der Sicherung nicht enthalten und werden daher nicht wiederhergestellt.

Wenn eine Datei gesichert wird, die nur Windows NT-Berechtigungen besitzt, und sie in einem UNIX-artigen Qtree oder Volume wiederhergestellt wird, erhält die Datei die standardmäßigen UNIX-Berechtigungen für diesen Qtree oder dieses Volume.

Wenn eine Datei, die nur UNIX-Berechtigungen hat, in einem NTFS-artigen Qtree oder Volume wiederhergestellt wird, erhält die Datei die standardmäßigen Windows-Berechtigungen für diesen Qtree oder dieses Volume.

Andere Dumps und Wiederherstellungen erhalten die Berechtigungen.

Sie können VM-ausgerichtete Dateien und die `vm-align-sector` Option sichern. Weitere Informationen zu VM-ausgerichteten Dateien finden sich unter "Logische Speicherverwaltung".

Informationen zu Inkrementketten und ONTAP NDMP

Eine Inkrementkette ist eine Reihe inkrementeller Backups desselben Pfades. Da Sie jederzeit eine beliebige Backup-Ebene festlegen können, ist das Verständnis von Inkrementketten erforderlich, um Backups und Wiederherstellungen effektiv durchführen zu können. Es können 31 Ebenen inkrementeller Backup-Operationen durchgeführt werden.

Es gibt zwei Arten von Inkrementketten:

- Eine Kette aufeinanderfolgender inkrementeller Sicherungen, also eine Folge inkrementeller Sicherungen, die mit Level 0 beginnt und bei jeder nachfolgenden Sicherung um 1 erhöht wird.
- Eine nicht aufeinanderfolgende Inkrementkette, bei der inkrementelle Backups Ebenen überspringen oder Ebenen aufweisen, die nicht in der richtigen Reihenfolge vorliegen, wie 0, 2, 3, 1, 4 oder häufiger 0, 1, 1, 1

oder 0, 1, 2, 1, 2.

Inkrementelle Backups basieren auf dem letzten Backup der niedrigeren Ebene. Beispielsweise ergibt die Reihenfolge der Backup-Ebenen 0, 2, 3, 1, 4 zwei Inkrementketten: 0, 2, 3 und 0, 1, 4. Die folgende Tabelle erläutert die Grundlagen der inkrementellen Backups:

Backup-Reihenfolge	Inkrementstufe	Inkrementkette	Basis	Dateien gesichert
1	0	Beide	Dateien auf dem Speichersystem	Alle Dateien im Sicherungspfad
2	2	0, 2, 3	Level-0 Backup	Dateien im Sicherungspfad, die seit dem Level-0-Backup erstellt wurden
3	3	0, 2, 3	Level-2 Backup	Dateien im Sicherungspfad, die seit dem Level-2-Backup erstellt wurden
4	1	0, 1, 4	Level-0-Backup, da dies die aktuellste Stufe ist, die niedriger als das Level-1-Backup ist	Dateien im Sicherungspfad, die seit dem Level-0-Backup erstellt wurden, einschließlich Dateien, die sich in den Level-2- und Level-3-Backups befinden
5	4	0, 1, 4	Das Level-1-Backup, da es eine niedrigere Ebene hat und aktueller ist als die Level-0-, Level-2- oder Level-3-Backups	Dateien, die seit dem Level-1-Backup erstellt wurden

Informationen zum Blockierungsfaktor und ONTAP NDMP

Ein Tape-Block umfasst 1.024 Byte Daten. Während eines Tape-Backups oder einer Wiederherstellung kann die Anzahl der Tape-Blöcke angegeben werden, die bei jedem lesen/schreiben übertragen werden. Diese Zahl wird als *Blocking Factor* bezeichnet.

Sie können einen Blockierungsfaktor von 4 bis 256 verwenden. Wenn geplant ist, ein Backup auf einem anderen System als dem System, das das Backup erstellt hat, wiederherzustellen, muss das Wiederherstellungssystem den für das Backup verwendeten Blockierungsfaktor unterstützen. Wenn beispielsweise ein Blockierungsfaktor von 128 verwendet wird, muss das System, auf dem dieses Backup wiederhergestellt wird, einen Blockierungsfaktor von 128 unterstützen.

Bei einer NDMP-Sicherung bestimmt die MOVER_RECORD_SIZE den Blockierungsfaktor. ONTAP erlaubt

einen Maximalwert von 256 KB für MOVER_RECORD_SIZE.

Zeitpunkt für den Neustart eines ONTAP Dump-Backups

Ein Dump-Backup wird manchmal aufgrund interner oder externer Fehler, wie Tape-Schreibfehlern, Stromausfällen, versehentlichen Benutzerunterbrechungen oder interner Inkonsistenz im Speichersystem, nicht abgeschlossen. Schlägt das Backup aus einem dieser Gründe fehl, besteht die Möglichkeit, es neu zu starten.

Sie können eine Datensicherung unterbrechen und neu starten, um Phasen hoher Auslastung des Speichersystems oder die Belegung anderer begrenzter Ressourcen auf dem Speichersystem, wie zum Beispiel eines Tape-Laufwerks, zu vermeiden. Eine längere Datensicherung kann unterbrochen und später neu gestartet werden, wenn eine dringendere Wiederherstellung (oder Datensicherung) dasselbe Tape-Laufwerk benötigt. Wiederaufnehmbare Datensicherungen bleiben auch nach einem Neustart erhalten. Eine abgebrochene Datensicherung auf Band kann nur dann neu gestartet werden, wenn die folgenden Bedingungen erfüllt sind:

- Das abgebrochene Backup befindet sich in Phase IV.
- Alle zugehörigen Snapshots, die durch den Löschbefehl gesperrt wurden, sind verfügbar.
- Der Dateiversionsverlauf muss aktiviert sein.

Wird ein solcher Löschbefehl abgebrochen und in einem wiederaufnehmbaren Zustand belassen, werden die zugehörigen Snapshots gesperrt. Diese Snapshots werden freigegeben, nachdem der Sicherungskontext gelöscht wurde. Die Liste der Sicherungskontexte kann mit dem `vserver services ndmp restartable backup show` Befehl angezeigt werden.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                  Is Cleanup Pending?
----------- ----------------------------------- -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
           Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                  Volume Name: /vserver1/vol1
          Is Cleanup Pending?: false
           Backup Engine Type: dump
Is Snapshot Auto-created?: true
                    Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                    Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
              Has Offset Map?: true
```

```
                  Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Wie die Wiederherstellung eines Speicherabbilds mit ONTAP NDMP funktioniert

Bei einer Dump-Wiederherstellung werden Dateisystemdaten mithilfe eines vordefinierten Prozesses von Band auf Festplatte geschrieben.

Der Prozess in der folgenden Tabelle zeigt, wie die Wiederherstellung des Dumps funktioniert:

Stufe	Aktion
1	ONTAP katalogisiert die Dateien, die vom Band extrahiert werden müssen.
2	ONTAP erstellt Verzeichnisse und leere Dateien.
3	ONTAP liest eine Datei vom Band, schreibt sie auf die Festplatte und legt die Berechtigungen (einschließlich ACLs) darauf fest.
4	ONTAP wiederholt die Schritte 2 und 3, bis alle angegebenen Dateien vom Band kopiert wurden.

Datentypen, die die Dump-Engine wiederherstellt

Im Falle eines Datenverlusts oder einer Systemstörung bietet die Dump-Engine verschiedene Methoden zur Wiederherstellung aller gesicherten Daten, von einzelnen Dateien über Dateiattribute bis hin zu ganzen Verzeichnissen. Kenntnisse über die Datentypen, die die Dump-Engine wiederherstellen kann, und wann welche Wiederherstellungsmethode anzuwenden ist, können dazu beitragen, Ausfallzeiten zu minimieren.

Daten können auf einer online zugeordneten LUN wiederhergestellt werden. Hostanwendungen können jedoch erst nach Abschluss der Wiederherstellung auf diese LUN zugreifen. Nach Abschluss der Wiederherstellung sollte der Host-Cache der LUN-Daten geleert werden, um die Konsistenz mit den wiederhergestellten Daten sicherzustellen.

Die Dump-Engine kann folgende Daten wiederherstellen:

- Inhalte von Dateien und Verzeichnissen
- UNIX-Dateiberechtigungen
- ACLs

  Wenn eine Datei, die ausschließlich UNIX-Dateiberechtigungen besitzt, in einem NTFS-Qtree oder Volume wiederhergestellt wird, verfügt die Datei über keine Windows NT ACLs. Das Speichersystem verwendet für diese Datei nur die UNIX-Dateiberechtigungen, bis eine Windows NT ACL darauf erstellt wird.

- Qtree-Informationen

Qtree-Informationen werden nur verwendet, wenn ein Qtree im Stammverzeichnis eines Volumes wiederhergestellt wird. Qtree-Informationen werden nicht verwendet, wenn ein Qtree in ein Unterverzeichnis wie `/vs1/vol1/subdir/lowerdir` wiederhergestellt wird und dadurch seine Qtree-Eigenschaften verliert.

- Alle anderen Datei- und Verzeichnisattribute
- Windows NT Streams
- LUNs
  - Eine LUN muss auf Volume-Ebene oder Qtree-Ebene wiederhergestellt werden, damit sie als LUN erhalten bleibt.

    Wird sie in ein Verzeichnis wiederhergestellt, erfolgt die Wiederherstellung als Datei, da keine gültigen Metadaten enthalten sind.
  - Eine 7-Mode LUN wird als LUN auf einem ONTAP Volume wiederhergestellt.
- Ein 7-Mode Volume kann auf ein ONTAP Volume wiederhergestellt werden.
- VM-ausgerichtete Dateien, die auf ein Zielvolume wiederhergestellt werden, übernehmen die VM-Ausrichtungseigenschaften des Zielvolumes.
- Das Zielvolume für einen Wiederherstellungsvorgang kann Dateien mit obligatorischen oder beratenden Sperren enthalten.

  Während der Wiederherstellung auf ein solches Zielvolume ignoriert die Dump-Engine diese Sperren.

Überlegungen vor der Wiederherstellung von Daten mit ONTAP NDMP

Sie können gesicherte Daten entweder am ursprünglichen Speicherort oder an einem anderen Zielort wiederherstellen. Wenn gesicherte Daten an einem anderen Zielort wiederhergestellt werden, muss das Ziel für den Wiederherstellungsvorgang vorbereitet werden.

Bevor Daten entweder an ihrem ursprünglichen Pfad oder an einem anderen Zielort wiederhergestellt werden, sind die folgenden Informationen erforderlich und die folgenden Anforderungen müssen erfüllt sein:

- Die Ebene der Wiederherstellung
- Der Pfad, zu dem die Daten wiederhergestellt werden
- Der während des Backups verwendete Blocking-Faktor
- Bei einer inkrementellen Wiederherstellung müssen alle Bänder in der Sicherungskette enthalten sein.
- Ein Tape-Laufwerk, das verfügbar und mit dem Band, von dem wiederhergestellt werden soll, kompatibel ist

Bevor Daten an einem anderen Zielort wiederhergestellt werden, sind die folgenden Schritte erforderlich:

- Wenn Sie ein Volume wiederherstellen, ist die Erstellung eines neuen Volumes erforderlich.
- Wenn Sie einen Qtree oder ein Verzeichnis wiederherstellen, müssen Dateien umbenannt oder verschoben werden, die wahrscheinlich denselben Namen wie die wiederherzustellenden Dateien haben.

> In ONTAP 9 werden Qtree-Namen im Unicode-Format unterstützt. Frühere Versionen von ONTAP unterstützen dieses Format nicht. Wenn ein Qtree mit Unicode-Namen in ONTAP 9

mithilfe des `ndmpcopy` Befehls oder durch Wiederherstellung eines Backup-Images auf Band in eine frühere Version von ONTAP kopiert wird, wird der Qtree als normales Verzeichnis und nicht als Qtree im Unicode-Format wiederhergestellt.

Wenn eine wiederhergestellte Datei denselben Namen wie eine vorhandene Datei hat, wird die vorhandene Datei durch die wiederhergestellte Datei überschrieben. Die Verzeichnisse werden jedoch nicht überschrieben.

Um eine Datei, ein Verzeichnis oder einen Qtree während der Wiederherstellung ohne Verwendung von DAR umzubenennen, muss die Umgebungsvariable EXTRACT auf `E` gesetzt werden.

Benötigter Speicherplatz auf dem Zielspeichersystem

Sie benötigen auf dem Zielspeichersystem etwa 100 MB mehr Speicherplatz als die Menge der wiederherzustellenden Daten.

Der Wiederherstellungsvorgang prüft beim Start, ob auf dem Zielvolume Speicherplatz und Inodes verfügbar sind. Das Setzen der Umgebungsvariablen FORCE auf `Y` bewirkt, dass der Wiederherstellungsvorgang die Prüfungen auf Speicherplatz und Inode-Verfügbarkeit auf dem Zielpfad überspringt. Wenn auf dem Zielvolume nicht genügend Speicherplatz oder Inodes verfügbar sind, stellt der Wiederherstellungsvorgang so viele Daten wieder her, wie es der verfügbare Speicherplatz und die Inode-Verfügbarkeit auf dem Zielvolume zulassen. Der Wiederherstellungsvorgang endet, wenn kein Speicherplatz oder keine Inodes mehr vorhanden sind.

Skalierbarkeitsgrenzen für ONTAP Dump-Backup und Wiederherstellungssitzungen

Sie müssen sich der maximalen Anzahl von Dump-Backup- und Wiederherstellungssitzungen bewusst sein, die gleichzeitig auf Speichersystemen mit unterschiedlicher System-Speicherkapazität durchgeführt werden können. Diese maximale Anzahl hängt vom Systemspeicher eines Speichersystems ab.

Die in der folgenden Tabelle genannten Grenzwerte gelten für die Dump- oder Wiederherstellungs-Engine. Die in den Skalierbarkeitsgrenzwerten für NDMP-Sitzungen genannten Grenzwerte gelten für den NDMP-Server, welche höher sind als die Grenzwerte der Engine.

Systemspeicher eines Speichersystems	Gesamtzahl der Dump-Backup- und Wiederherstellungssitzungen
Weniger als 16 GB	4
Größer oder gleich 16 GB, aber kleiner als 24 GB	16
Größer oder gleich 24 GB	32

Wenn der `ndmpcopy` Befehl zum Kopieren von Daten innerhalb von Speichersystemen verwendet wird, werden zwei NDMP-Sitzungen eingerichtet, eine für das Dump-Backup und die andere für das Dump-Restore.

Sie können den Systemspeicher Ihres Speichersystems mithilfe des `sysconfig -a` Befehls (verfügbar über die nodeshell) abrufen. Weitere Informationen zu `sysconfig -a` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Skalierbarkeitsgrenzen für NDMP Sitzungen

Wiederstartbare Kontexte können gelöscht werden, indem der ONTAP SVM-Name und die Kontext-ID angegeben werden.

Wenn Sie ein Backup starten möchten, anstatt einen Kontext neu zu starten, kann der Kontext gelöscht werden.

Über diese Aufgabe

Sie können einen wiederaufnehmbaren Kontext mit dem `vserver services ndmp restartable-backup delete` Befehl löschen, indem Sie den SVM-Namen und die Kontext-ID angeben.

Schritte

1. Löschen eines neu startfähigen Kontexts:

   `vserver services ndmp restartable-backup delete -vserver` *`vserver-name`* `-context -id` *`context_identifier`*.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                  Is Cleanup Pending?
----------- ----------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                  Is Cleanup Pending?
----------- ----------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

Funktionsweise von Dump auf einem ONTAP SnapVault sekundäres Volume

Tape-Backup-Operationen können für Daten durchgeführt werden, die auf dem SnapVault sekundären Volume gespiegelt sind. Es kann nur die auf dem SnapVault sekundären Volume gespiegelte Datenmenge auf Band gesichert werden, nicht jedoch die Metadaten der SnapVault Beziehung.

Wenn die Spiegelungsbeziehung zum Datenschutz unterbrochen wird (`snapmirror break` oder wenn eine SnapMirror-Resynchronisierung erfolgt, ist stets ein Baseline-Backup erforderlich.

Verwandte Informationen

- "snapmirror break"

Funktionsweise von Dump bei ONTAP Storage Failover und ARL-Operationen

Bevor Sie Sicherungs- oder Wiederherstellungsvorgänge durchführen, sollte nachvollzogen werden, wie diese Vorgänge mit Storage-Failover (Übernahme und Rückgabe) oder Aggregate Relocation (ARL) ablaufen. Die `-override-vetoes` Option bestimmt das Verhalten der Dump-Engine während eines Storage-Failover- oder ARL-Vorgangs.

Wenn eine Dump-Sicherung oder -Wiederherstellung ausgeführt wird und die `-override-vetoes` Option auf `false` gesetzt ist, wird ein vom Benutzer initiierter Storage-Failover- oder ARL-Vorgang gestoppt. Ist die `-override-vetoes` Option jedoch auf `true` gesetzt, wird der Storage-Failover- oder ARL-Vorgang fortgesetzt und die Dump-Sicherungs- oder -Wiederherstellungsoperation abgebrochen. Wird ein Storage-Failover- oder ARL-Vorgang automatisch vom Storage-System initiiert, wird eine aktive Dump-Sicherungs- oder -Wiederherstellungsoperation immer abgebrochen. Dump-Sicherungs- und -Wiederherstellungsoperationen können auch nach Abschluss eines Storage-Failover- oder ARL-Vorgangs nicht neu gestartet werden.

Dump-Operationen, wenn die CAB-Erweiterung unterstützt wird

Wenn die Backup-Anwendung die CAB-Erweiterung unterstützt, ist es möglich, inkrementelle Dump-Backup- und Wiederherstellungsvorgänge ohne Neukonfiguration der Backup-Richtlinien nach einem Storage-Failover oder einer ARL-Operation fortzusetzen.

Dump-Operationen, wenn die CAB-Erweiterung nicht unterstützt wird

Unterstützt die Sicherungsanwendung die CAB-Erweiterung nicht, können inkrementelle Dump-Backup- und Wiederherstellungsvorgänge weiterhin durchgeführt werden, wenn die in der Sicherungsrichtlinie konfigurierte LIF auf den Knoten migriert wird, der das Zielaggregat hostet. Andernfalls ist nach dem Storage-Failover und dem ARL-Vorgang vor der Durchführung der inkrementellen Sicherung eine Basissicherung erforderlich.

> Für Storage-Failover-Operationen muss die in der Sicherungsrichtlinie konfigurierte LIF auf den Partnerknoten migriert werden.

Verwandte Informationen

"Hochverfügbarkeit"

Funktionsweise von Dump mit ONTAP Volume Move

Tape-Backup- und Wiederherstellungsvorgänge sowie die Volume-Verschiebung können parallel ausgeführt werden, bis das Speichersystem die endgültige Umstellungsphase einleitet. Während der endgültigen Umstellungsphase sind keine neuen Tape-Backup- und Wiederherstellungsvorgänge auf dem Volume zulässig, das verschoben wird. Die laufenden Vorgänge werden jedoch bis zum Abschluss fortgesetzt.

Die folgende Tabelle beschreibt das Verhalten von Tape-Backup- und Wiederherstellungsvorgängen nach dem

Volume-Verschiebevorgang:

Wenn Tape-Backup- und Wiederherstellungsvorgänge in der … durchgeführt werden	Dann…
storage virtual machine (SVM) scoped NDMP-Modus, wenn die CAB-Erweiterung von der Backup-Anwendung unterstützt wird	Inkrementelle Tape-Backup- und Wiederherstellungsvorgänge können auf lesen/schreiben- und Nur-Lese-Volumes weiterhin durchgeführt werden, ohne dass die Sicherungsrichtlinien neu konfiguriert werden müssen.
SVM-bezogener NDMP-Modus, wenn die CAB-Erweiterung von der Backup-Anwendung nicht unterstützt wird	Inkrementelle Tape-Backup- und Wiederherstellungsvorgänge auf lesen/schreiben- und Nur-Lese-Volumes sind weiterhin möglich, wenn die in der Backup-Richtlinie konfigurierte LIF auf den Knoten migriert wird, der das Zielaggregat hostet. Andernfalls ist nach der Volume-Verschiebung eine Basissicherung erforderlich, bevor die inkrementelle Sicherung durchgeführt werden kann.

Wenn eine Volume-Verschiebung stattfindet und das Volume, das zu einer anderen SVM auf dem Zielknoten gehört, denselben Namen wie das verschobene Volume hat, können keine inkrementellen Sicherungsvorgänge des verschobenen Volumes durchgeführt werden.

Funktionsweise eines Dumps, wenn ein ONTAP FlexVol volume voll ist

Vor der Durchführung einer inkrementellen Dump-Sicherung muss sichergestellt werden, dass ausreichend freier Speicherplatz im FlexVol volume vorhanden ist.

Schlägt der Vorgang fehl, muss der freie Speicherplatz im FlexVol volume entweder durch Vergrößern der Größe oder durch Löschen der Snapshots erhöht werden. Anschließend ist der inkrementelle Sicherungsvorgang erneut auszuführen.

Funktionsweise von Dump, wenn sich der Zugriffstyp eines ONTAP-Volumes ändert

Wenn sich der Status eines SnapMirror Zielvolumes oder eines SnapVault sekundären Volumes von lesen/schreiben auf nur lesen oder von nur lesen auf lesen/schreiben ändert, ist eine Baseline-Tape-Backup- oder Wiederherstellungsoperation erforderlich.

SnapMirror Ziel- und SnapVault sekundäre Volumes sind schreibgeschützte Volumes. Bei Tape-Backup- und Restore-Vorgängen auf solchen Volumes ist eine Basissicherung oder ein Restore erforderlich, sobald sich der Status des Volumes von schreibgeschützt zu lesen/schreiben oder von lesen/schreiben zu schreibgeschützt ändert.

Funktionsweise von Dump bei einer ONTAP SnapMirror Wiederherstellung einer einzelnen Datei oder LUN

Bevor mit Hilfe der SnapMirror Technologie Dump-Backup- oder Wiederherstellungsvorgänge auf einem Volume durchgeführt werden, auf dem eine einzelne Datei oder LUN wiederhergestellt wird, ist es wichtig zu verstehen, wie Dump-

Vorgänge mit einer einzelnen Datei- oder LUN-Wiederherstellung zusammenwirken.

Während einer SnapMirror Wiederherstellung einer einzelnen Datei oder LUN wird die Client-E/A für die wiederherzustellende Datei oder LUN eingeschränkt. Wenn die Wiederherstellung einer einzelnen Datei oder LUN abgeschlossen ist, wird die E/A-Einschränkung für die Datei oder LUN aufgehoben. Wenn ein Dump-Backup auf einem Volume durchgeführt wird, auf das eine einzelne Datei oder LUN wiederhergestellt wurde, ist die Datei oder LUN mit Client-E/A-Einschränkung nicht im Dump-Backup enthalten. Bei einem nachfolgenden Backup wird diese Datei oder LUN nach Aufhebung der E/A-Einschränkung auf Band gesichert.

Es ist nicht möglich, auf demselben Volume gleichzeitig eine Dump-Wiederherstellung und eine SnapMirror Einzeldatei- oder LUN-Wiederherstellung durchzuführen.

Wie sich Dump-Backup- und Restore-Vorgänge in ONTAP MetroCluster Konfigurationen auswirken

Bevor Sie Dump-Backup und Restore-Vorgänge in einer MetroCluster Konfiguration durchführen, ist es wichtig zu verstehen, wie sich Dump-Vorgänge auswirken, wenn ein Switchover oder Switchback erfolgt.

Dump-Backup oder Wiederherstellungsvorgang, gefolgt von Switchover

Betrachten Sie zwei Cluster: Cluster 1 und Cluster 2. Während einer Dump-Backup- oder Wiederherstellungsoperation auf Cluster 1, wenn ein Switchover von Cluster 1 zu Cluster 2 eingeleitet wird, tritt Folgendes ein:

- Ist der Wert der `override-vetoes` Option `false`, wird der Switchover abgebrochen und der Backup- oder Recovery-Vorgang fortgesetzt.
- Wenn der Wert der Option `true` ist, wird der Dump-Backup- oder Wiederherstellungsvorgang abgebrochen und die Umschaltung fortgesetzt.

Dump-Backup oder Wiederherstellungsvorgang, gefolgt von Switchback

Es wird ein Switchover von Cluster 1 zu Cluster 2 durchgeführt und ein Dump-Backup- oder Wiederherstellungsvorgang auf Cluster 2 initiiert. Der Dump-Vorgang sichert oder stellt ein Volume wieder her, das sich auf Cluster 2 befindet. Zu diesem Zeitpunkt, wenn ein Switchback von Cluster 2 zu Cluster 1 eingeleitet wird, tritt Folgendes ein:

- Wenn der Wert der `override-vetoes` Option `false` ist, wird der Switchback abgebrochen und der Backup- oder Restore-Vorgang fortgesetzt.
- Wenn der Wert der Option `true` ist, wird der Sicherungs- oder Wiederherstellungsvorgang abgebrochen und der Switchback fortgesetzt.

Sicherungs- oder Wiederherstellungsoperation per Dump, die während eines Switchover oder Switchback initiiert wurde

Während eines Switchover von Cluster 1 zu Cluster 2 schlägt ein Dump-Backup- oder Wiederherstellungsvorgang auf Cluster 1 fehl, und der Switchover wird fortgesetzt.

Wenn während eines Switchback von Cluster 2 zu Cluster 1 ein Dump-Backup oder Wiederherstellungsvorgang von Cluster 2 aus initiiert wird, schlägt der Backup- oder Wiederherstellungsvorgang fehl und der Switchback wird fortgesetzt.

Informationen zur SMTape Engine für FlexVol Volumes

Informationen zur ONTAP SMTape Engine für FlexVol Volumes

SMTape ist eine Disaster Recovery-Lösung von ONTAP, die Datenblöcke auf Tape sichert. Mit SMTape lassen sich Volume-Backups auf Tape durchführen. Ein Backup auf Qtree- oder Subtree-Ebene ist jedoch nicht möglich. SMTape unterstützt Baseline-, Differenzial- und inkrementelle Backups. Für SMTape ist keine Lizenz erforderlich.

Sie können eine SMTape-Sicherung und -Wiederherstellung mithilfe einer NDMP-kompatiblen Backup-Anwendung durchführen. SMTape kann für Backup- und Wiederherstellungsvorgänge nur im NDMP-Modus mit Storage Virtual Machine (SVM)-Bereich verwendet werden.

> Der Reversionsprozess wird nicht unterstützt, wenn eine SMTape Tape-Backup- oder Wiederherstellungssitzung läuft. Es ist erforderlich, zu warten, bis die Sitzung abgeschlossen ist, oder die NDMP-Sitzung abzubrechen.

Mit SMTape können Sie 255 Snapshots sichern. Für nachfolgende Baseline-, inkrementelle oder differentielle Backups müssen ältere, gesicherte Snapshots gelöscht werden.

Vor der Durchführung einer Basiswiederherstellung muss das Volume, auf das die Daten wiederhergestellt werden, vom Typ `DP` sein und sich im eingeschränkten Zustand befinden. Nach einer erfolgreichen Wiederherstellung ist dieses Volume automatisch online. Nachfolgende inkrementelle oder differentielle Wiederherstellungen können auf diesem Volume in der Reihenfolge durchgeführt werden, in der die Backups erstellt wurden.

Informationen zur Verwendung von ONTAP Snapshots während des SMTape-Backups

Es ist wichtig zu verstehen, wie Snapshots bei einer SMTape Basissicherung und einer inkrementellen Sicherung verwendet werden. Es sind außerdem einige Aspekte zu berücksichtigen, wenn eine Sicherung mit SMTape durchgeführt wird.

Basissicherung

Beim Erstellen einer Basissicherung kann der Name des auf Tape zu sichernden Snapshots angegeben werden. Wird kein Snapshot angegeben, wird abhängig vom Zugriffstyp des Volumes (lesen/schreiben oder Nur-Lesezugriff) entweder automatisch ein Snapshot erstellt oder vorhandene Snapshots werden verwendet. Wird ein Snapshot für das Backup angegeben, werden alle Snapshots, die älter als der angegebene Snapshot sind, ebenfalls auf Tape gesichert.

Wenn Sie keinen Snapshot für das Backup angeben, tritt Folgendes ein:

- Für ein lesen/schreiben Volume wird automatisch ein Snapshot erstellt.

  Der neu erstellte Snapshot und alle älteren Snapshots werden auf Tape gesichert.

- Bei einem schreibgeschützten Volume werden alle Snapshots, einschließlich des neuesten Snapshots, auf Tape-Backup gesichert.

  Alle nach dem Start der Datensicherung erstellten Snapshots werden nicht gesichert.

Inkrementelle Datensicherung

Für SMTape inkrementelle oder differenzielle Backup-Operationen erstellen und verwalten die NDMP-konformen Backup-Anwendungen die Snapshots.

Sie müssen bei der Durchführung eines inkrementellen Backup-Vorgangs immer einen Snapshot angeben. Für einen erfolgreichen inkrementellen Backup-Vorgang muss sich der während des vorherigen Backup-Vorgangs (Baseline oder inkrementell) gesicherte Snapshot auf dem Volume befinden, von dem das Backup durchgeführt wird. Um sicherzustellen, dass Sie diesen gesicherten Snapshot verwenden, muss die auf diesem Volume zugewiesene Snapshot-Richtlinie bei der Konfiguration der Backup-Richtlinie berücksichtigt werden.

Überlegungen zu SMTape Backups auf SnapMirror Zielen

- Eine Spiegelbeziehung zum Datenschutz erstellt temporäre Snapshots auf dem Zielvolume für die Replikation.

  Diese Snapshots sollten nicht für SMTape Backup verwendet werden.

- Wenn während eines SMTape-Backup-Vorgangs auf demselben Volume eine SnapMirror-Aktualisierung auf einem Zielvolume in einer Data-Protection-Spiegelbeziehung erfolgt, darf der von SMTape gesicherte Snapshot auf dem Quellvolume nicht gelöscht werden.

  Während des Sicherungsvorgangs sperrt SMTape den Snapshot auf dem Zielvolume, und wenn der entsprechende Snapshot auf dem Quellvolume gelöscht wird, schlägt der nachfolgende SnapMirror-Updatevorgang fehl.

- Diese Snapshots sollten nicht bei inkrementellen Backups verwendet werden.

SMTape Funktionen zur Optimierung von ONTAP Tape-Backup und Wiederherstellungsvorgängen

SMTape-Funktionen wie die Sicherung von Snapshots, inkrementelle und differentielle Backups, die Beibehaltung der Deduplizierungs- und Komprimierungsfunktionen auf wiederhergestellten Volumes sowie Tape-Seeding tragen dazu bei, Tape-Backup und Wiederherstellungsvorgänge zu optimieren.

SMTape bietet folgende Funktionen:

- Bietet eine Lösung zur Notfallwiederherstellung
- Ermöglicht inkrementelle und differentielle Backups
- Sichert Snapshots
- Ermöglicht die Sicherung und Wiederherstellung deduplizierter Volumes und bewahrt die Deduplizierung auf den wiederhergestellten Volumes.
- Sichert komprimierte Volumes und erhält die Komprimierung auf den wiederhergestellten Volumes
- Ermöglicht Tape-Seeding

SMTape unterstützt den Blockierungsfaktor in Vielfachen von 4 KB, im Bereich von 4 KB bis 256 KB.



Daten können nur auf Volumes wiederhergestellt werden, die über maximal zwei aufeinanderfolgende Hauptversionen von ONTAP erstellt wurden.

ONTAP Skalierbarkeitsgrenzen für SMTape-Backup- und Wiederherstellungssitzungen

Bei der Durchführung von SMTape Backup- und Wiederherstellungsvorgängen über NDMP oder CLI (Tape-Seeding) ist die maximale Anzahl von SMTape Backup- und Wiederherstellungssitzungen zu berücksichtigen, die gleichzeitig auf Speichersystemen mit unterschiedlichen System-Speicherkapazitäten durchgeführt werden können. Diese maximale Anzahl hängt vom Systemspeicher eines Speichersystems ab.

Die Skalierbarkeitsgrenzen für SMTape-Backup- und Restore-Sitzungen unterscheiden sich von den NDMP-Sitzungsgrenzen und den Löschbefehl-Sitzungsgrenzen.

Systemspeicher des Speichersystems	Gesamtzahl der SMTape Sicherungs- und Wiederherstellungssitzungen
Weniger als 16 GB	6
Größer oder gleich 16 GB, aber kleiner als 24 GB	16
Größer oder gleich 24 GB	32

Sie können den Systemspeicher Ihres Speichersystems mithilfe des `sysconfig -a` Befehls (verfügbar über die nodeshell) abrufen. Weitere Informationen zu `sysconfig -a` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- Skalierbarkeitsgrenzen für NDMP Sitzungen
- Skalierbarkeitsgrenzen für Dump-Backup und Wiederherstellungssitzungen

Informationen zu ONTAP Tape Seeding

Tape Seeding ist eine SMTape-Funktionalität, die bei der Initialisierung eines Ziel-FlexVol volume in einer Datensicherungs-Spiegelbeziehung unterstützt.

Tape Seeding ermöglicht die Einrichtung einer Datensicherungs-Spiegelbeziehung zwischen einem Quellsystem und einem Zielsystem über eine Verbindung mit geringer Bandbreite.

Die inkrementelle Spiegelung von Snapshots vom Quellsystem zum Zielsystem ist über eine Verbindung mit geringer Bandbreite möglich. Eine initiale Spiegelung des Basis-Snapshots dauert jedoch über eine Verbindung mit geringer Bandbreite lange. In solchen Fällen kann ein SMTape-Backup des Quell-Volumes auf ein Band durchgeführt werden, und das Band kann verwendet werden, um den initialen Basis-Snapshot auf das Zielsystem zu übertragen. Danach lassen sich inkrementelle SnapMirror-Updates zum Zielsystem über die Verbindung mit geringer Bandbreite einrichten.

Wie SMTape mit ONTAP Storage-Failover und ARL-Operationen funktioniert

Bevor Sie SMTape-Backup- oder Wiederherstellungsvorgänge durchführen, sollte nachvollzogen werden, wie diese Vorgänge mit Storage-Failover (Takeover und Giveback) oder einer Aggregate Relocation (ARL) Operation zusammenwirken. Die `-override-vetoes` Option bestimmt das Verhalten der SMTape Engine während eines Storage-Failovers oder einer ARL-Operation.

Wenn ein SMTape-Backup- oder Restore-Vorgang ausgeführt wird und die `-override-vetoes` Option auf

`false` gesetzt ist, wird ein vom Benutzer initiierter Storage-Failover- oder ARL-Vorgang gestoppt und der Backup- oder Restore-Vorgang abgeschlossen. Wenn die Backup-Anwendung die CAB-Erweiterung unterstützt, können inkrementelle SMTape-Backup- und Restore-Vorgänge weiterhin durchgeführt werden, ohne die Backup-Richtlinien neu konfigurieren zu müssen. Wenn jedoch die `-override-vetoes` Option auf `true` gesetzt ist, wird der Storage-Failover- oder ARL-Vorgang fortgesetzt und der SMTape-Backup- oder Restore-Vorgang abgebrochen.

Verwandte Informationen

"Netzwerkmanagement"

"Hochverfügbarkeit"

Wie SMTape mit ONTAP Volume Move funktioniert

SMTape-Backup-Vorgänge und Volume-Verschiebungen können parallel ausgeführt werden, bis das Speichersystem die endgültige Umstellungsphase einleitet. Während der endgültigen Umstellungsphase können keine neuen SMTape-Backup-Vorgänge auf dem Volume, das verschoben wird, ausgeführt werden. Die aktuellen Vorgänge laufen jedoch bis zum Abschluss weiter.

Vor Beginn der Umstellungsphase für ein Volume prüft der Volume-Verschiebungsvorgang, ob auf demselben Volume aktive SMTape-Backup-Vorgänge vorhanden sind. Sind aktive SMTape-Backup-Vorgänge vorhanden, wechselt der Volume-Verschiebungsvorgang in den Status „Umstellung verzögert“ und ermöglicht den Abschluss der SMTape-Backup-Vorgänge. Nach Abschluss dieser Backup-Vorgänge ist der Volume-Verschiebungsvorgang manuell neu zu starten.

Wenn die Backup-Anwendung die CAB-Erweiterung unterstützt, ist es möglich, inkrementelle Tape-Backup- und Wiederherstellungsvorgänge auf lesen/schreiben- und Nur-Lese-Volumes weiterhin durchzuführen, ohne die Backup-Richtlinien neu konfigurieren zu müssen.

Die Wiederherstellung der Basisdaten und die Verschiebung von Volumes können nicht gleichzeitig durchgeführt werden; die inkrementelle Wiederherstellung kann jedoch parallel zu Volume-Verschiebungen ausgeführt werden, wobei das Verhalten dem von SMTape-Backup-Vorgängen während Volume-Verschiebungen ähnelt.

Funktionsweise von SMTape bei ONTAP Volume-Rehost-Operationen

SMTape-Operationen können nicht gestartet werden, wenn ein Volume Rehost-Vorgang auf einem Volume ausgeführt wird. Wenn ein Volume an einem Volume Rehost-Vorgang beteiligt ist, sollten keine SMTape-Sitzungen auf diesem Volume gestartet werden.

Wenn eine Volume Rehost Operation ausgeführt wird, schlägt das SMTape Backup oder die SMTape Wiederherstellung fehl. Wenn ein SMTape Backup oder eine SMTape Wiederherstellung ausgeführt wird, schlagen Volume Rehost Operationen mit einer entsprechenden Fehlermeldung fehl. Diese Bedingung gilt sowohl für NDMP-basierte als auch für CLI-basierte Backup- oder Wiederherstellungsoperationen.

Wie sich eine ONTAP NDMP-Backup-Richtlinie während ADB auswirkt

Wenn der automatische Datenausgleich (ADB) aktiviert ist, analysiert der Ausgleicher die Nutzungsstatistiken der Aggregate, um das Aggregat zu identifizieren, das den konfigurierten oberen Schwellenwert für die Nutzung überschritten hat.

Nachdem der Balancer das Aggregat identifiziert hat, das den Schwellenwert überschritten hat, ermittelt er ein Volume, das auf Aggregate in einem anderen Knoten des Clusters verschoben werden kann, und versucht, dieses Volume zu verschieben. Diese Situation wirkt sich auf die für dieses Volume konfigurierte Backup-Richtlinie aus, da der Benutzer die Backup-Richtlinie neu konfigurieren und die Baseline-Backup-Operation ausführen muss, wenn die Datenmanagementanwendung (DMA) nicht CAB-fähig ist.

Wenn der DMA CAB-fähig ist und die Backup-Richtlinie über eine spezifische Schnittstelle konfiguriert wurde, ist der ADB nicht betroffen.

Wie sich SMTape-Sicherungs- und Wiederherstellungsvorgänge in ONTAP MetroCluster Konfigurationen auswirken

Bevor Sie SMTape-Sicherungs- und Wiederherstellungsvorgänge in einer MetroCluster Konfiguration durchführen, muss nachvollzogen werden, wie sich ein Switchover- oder Switchback-Vorgang auf SMTape-Vorgänge auswirkt.

SMTape Backup oder Wiederherstellungsvorgang, gefolgt von einer Umschaltung

Betrachten Sie zwei Cluster: Cluster 1 und Cluster 2. Während einer SMTape-Sicherung oder -Wiederherstellung auf Cluster 1, wenn ein Switchover von Cluster 1 zu Cluster 2 eingeleitet wird, tritt Folgendes ein:

- Ist der Wert der `-override-vetoes` Option `false`, wird der Umschaltvorgang abgebrochen und die Sicherungs- oder Wiederherstellungsoperation fortgesetzt.
- Ist der Wert der Option `true`, wird der SMTape-Backup- oder Wiederherstellungsvorgang abgebrochen und der Umschaltvorgang fortgesetzt.

SMTape Backup oder Wiederherstellungsvorgang gefolgt von Switchback

Es wird ein Switchover von Cluster 1 zu Cluster 2 durchgeführt und eine SMTape Backup- oder Restore-Operation auf Cluster 2 initiiert. Die SMTape-Operation sichert oder stellt ein Volume wieder her, das sich auf Cluster 2 befindet. Zu diesem Zeitpunkt, wenn ein Switchback von Cluster 2 zu Cluster 1 eingeleitet wird, tritt Folgendes ein:

- Wenn der Wert der `-override-vetoes` Option `false` ist, wird der Rückschaltvorgang abgebrochen und die Sicherungs- oder Wiederherstellungsoperation fortgesetzt.
- Ist der Wert der Option `true`, wird der Sicherungs- oder Wiederherstellungsvorgang abgebrochen und der Rückschaltvorgang fortgesetzt.

SMTape-Backup- oder Wiederherstellungsvorgang während eines Switchover oder Switchback initiiert

Während eines Switchover-Prozesses von Cluster 1 zu Cluster 2 schlägt ein SMTape Backup- oder Wiederherstellungsvorgang auf Cluster 1 fehl, und der Switchover wird fortgesetzt.

Während eines Switchback-Prozesses von Cluster 2 zu Cluster 1 schlägt ein SMTape Backup- oder Wiederherstellungsvorgang, der von Cluster 2 aus initiiert wird, fehl und der Switchback wird fortgesetzt.

Tape-Backup- und Wiederherstellungsvorgänge für FlexVol Volumes überwachen

Überwachung von ONTAP Tape-Backup und Wiederherstellungsvorgängen für FlexVol Volumes

Sie können die Ereignisprotokolldateien einsehen, um die Tape-Backup und

Wiederherstellungsvorgänge zu überwachen. ONTAP protokolliert automatisch wichtige Backup- und Wiederherstellungsereignisse sowie deren Zeitpunkt in einer Protokolldatei namens `backup` im `/etc/log/`Verzeichnis des Controllers. Standardmäßig ist die Protokollierung auf `on` eingestellt.

Eventprotokolldateien können aus folgenden Gründen angezeigt werden:

- Überprüfung, ob das nächtliche Backup erfolgreich war
- Erfassung von Statistiken zu Sicherungsvorgängen
- Zur Verwendung der Informationen in früheren Ereignisprotokolldateien zur Diagnose von Problemen bei Sicherungs- und Wiederherstellungsvorgängen

Die Ereignisprotokolldateien werden wöchentlich rotiert. Die `/etc/log/backup` Datei wird in `/etc/log/backup.0` umbenannt, die `/etc/log/backup.0` Datei wird in `/etc/log/backup.1` umbenannt und so weiter. Das System speichert die Protokolldateien bis zu sechs Wochen; daher können bis zu sieben Meldungsdateien (`/etc/log/backup.[0-5]` und die aktuelle `/etc/log/backup` Datei vorhanden sein.

Zugriff auf die ONTAP Ereignisprotokolldateien für Tape-Backup und Restore-Vorgänge

Sie können auf die Ereignisprotokolldateien für Tape-Backup- und Wiederherstellungsvorgänge im `/etc/log/` Verzeichnis zugreifen, indem Sie den `rdfile` Befehl an der Nodeshell verwenden. Diese Ereignisprotokolldateien können zur Überwachung von Tape-Backup- und Wiederherstellungsvorgängen eingesehen werden.

Über diese Aufgabe

Mit zusätzlichen Konfigurationen, wie beispielsweise einer Zugriffskontrollrolle mit Zugriff auf den `spi` Webdienst oder einem Benutzerkonto, das mit der `http` Zugriffsmethode eingerichtet wurde, ist auch der Zugriff auf diese Protokolldateien über einen Webbrowser möglich.

Schritte

1. Um auf die Nodeshell zuzugreifen, ist folgender Befehl einzugeben:

   `node run -node` *`node_name`*

   `node_name` ist der Name des Knotens.

2. Um auf die Ereignisprotokolldateien für Tape-Backup und Wiederherstellungsvorgänge zuzugreifen, ist folgender Befehl einzugeben:

   `rdfile /etc/log/backup`

Verwandte Informationen

"Systemadministration"

Welches Format haben die Ereignisprotokollmeldungen für Dump und Restore?

ONTAP Dump und Restore Ereignisprotokoll-Nachrichtenformat

Für jeden Sicherungs- und Wiederherstellungsvorgang wird eine Meldung in die

Sicherungsprotokolldatei geschrieben.

Das Format der Ereignisprotokollmeldung für Dump und Restore ist wie folgt:

```
type timestamp identifier event (event_info)
```

Die folgende Liste beschreibt die Felder im Ereignisprotokollnachrichtenformat:

- Jede Logmeldung beginnt mit einem der in der folgenden Tabelle beschriebenen Typindikatoren:

Typ	Beschreibung
Protokoll	Protokollierungsereignis
dmp	Dump-Ereignis
rst	Wiederherstellungsereignis

- `timestamp` zeigt Datum und Uhrzeit des Ereignisses an.
- Das `identifier` Feld für ein Speicherabbildereignis enthält den Speicherabbildpfad und die eindeutige ID des Speicherabbilds. Das `identifier` Feld für ein Wiederherstellungsereignis verwendet nur den Namen des Wiederherstellungszielpfads als eindeutigen Bezeichner. Protokollierungsbezogene Ereignismeldungen enthalten kein `identifier` Feld.

Informationen zu ONTAP Protokollierungsereignissen

Das Ereignisfeld einer Nachricht, die mit einem Logeintrag beginnt, gibt den Beginn einer Protokollierung oder das Ende einer Protokollierung an.

Es enthält eines der in der folgenden Tabelle aufgeführten Ereignisse:

Ereignis	Beschreibung
Start_Protokollierung	Zeigt den Beginn der Protokollierung oder dass die Protokollierung nach ihrer Deaktivierung wieder aktiviert wurde.
Stop_Logging	Gibt an, dass die Protokollierung deaktiviert wurde.

Informationen zu ONTAP Dump-Ereignissen

Das Ereignisfeld für ein Dump-Ereignis enthält einen Ereignistyp, gefolgt von ereignisspezifischen Informationen in Klammern.

Die folgende Tabelle beschreibt die Ereignisse, ihre Beschreibungen und die zugehörigen Ereignisinformationen, die bei einem Dump-Vorgang protokolliert werden können:

Ereignis	Beschreibung	Veranstaltungsinformationen
Start	NDMP dump wird gestartet	Dump-Level und Dump-Typ
Ende	Dumps erfolgreich abgeschlossen	Menge der verarbeiteten Daten
Abbrechen	Der Vorgang wurde abgebrochen.	Menge der verarbeiteten Daten

Ereignis	Beschreibung	Veranstaltungsinformationen
Optionen	Angegebene Optionen sind aufgelistet	Alle Optionen und ihre zugehörigen Werte, einschließlich NDMP-Optionen
Tape_open	Das Band ist zum lesen/schreiben geöffnet	Der neue Tape-Gerät Name
Tape_close	Das Band ist für lesen/schreiben geschlossen	Der Tape-Gerät-Name
Phasenänderung	Ein Dump befindet sich in einer neuen Verarbeitungsphase.	Der neue Phasenname
Fehler	Ein Dump ist auf ein unerwartetes Ereignis gestoßen.	Fehlermeldung
Schnappschuss	Ein Snapshot wird erstellt oder gefunden	Name und Zeitpunkt der Momentaufnahme
Base_dump	Ein Basis-Dump-Eintrag in der internen Metadatei wurde gefunden.	Niveau und Zeitpunkt des Basis-Dumps (nur für inkrementelle Dumps)

Informationen zu ONTAP Wiederherstellungsereignissen

Das Ereignisfeld für ein Wiederherstellungsereignis enthält einen Ereignistyp, gefolgt von ereignisspezifischen Informationen in Klammern.

Die folgende Tabelle enthält Informationen über die Ereignisse, deren Beschreibungen und die zugehörigen Ereignisinformationen, die für einen Wiederherstellungsvorgang aufgezeichnet werden können:

Ereignis	Beschreibung	Veranstaltungsinformationen
Start	Die NDMP-Wiederherstellung ist gestartet	Wiederherstellungsebene und Wiederherstellungstyp
Ende	Wiederherstellung erfolgreich abgeschlossen	Anzahl der Dateien und verarbeitete Datenmenge
Abbrechen	Der Vorgang wurde abgebrochen.	Anzahl der Dateien und verarbeitete Datenmenge
Optionen	Angegebene Optionen sind aufgelistet	Alle Optionen und ihre zugehörigen Werte, einschließlich NDMP-Optionen
Tape_open	Das Band ist zum lesen/schreiben geöffnet	Der neue Tape-Gerät Name
Tape_close	Das Band ist für lesen/schreiben geschlossen	Der Tape-Gerät-Name
Phasenänderung	Die Wiederherstellung tritt in eine neue Verarbeitungsphase ein.	Der neue Phasenname
Fehler	Restore stößt auf ein unerwartetes Ereignis	Fehlermeldung

Aktivieren oder Deaktivieren der Protokollierung für ONTAP Tape-Backup und Restore-Vorgänge

Sie können die Ereignisprotokollierung ein- oder ausschalten.

Schritte

1. Zum Aktivieren oder Deaktivieren der Ereignisprotokollierung den folgenden Befehl in der Clustershell eingeben:

   options *-option_name* backup.log.enable *-option-value* {on | off}

   `on`Schaltet die Ereignisprotokollierung ein.

   `off`schaltet die Ereignisprotokollierung aus.

   Die Ereignisprotokollierung ist standardmäßig aktiviert.

Fehlermeldungen für Tape-Backup und Wiederherstellung von FlexVol Volumes

Fehlermeldungen beim Sichern und Wiederherstellen

Ressourcenbeschränkung: Kein Thread verfügbar

- **Nachricht**

  ```
  Resource limitation: no available thread
  ```

- **Ursache**

  Die maximale Anzahl aktiver lokaler Tape-E/A-Threads ist derzeit belegt. Es sind maximal 16 aktive lokale Tape-Laufwerke möglich.

- **Korrekturmaßnahme**

  Es sollte abgewartet werden, bis einige Bandaufträge abgeschlossen sind, bevor ein neuer Sicherungs- oder Wiederherstellungsauftrag gestartet wird.

Bandreservierung vorweggenommen

- **Nachricht**

  ```
  Tape reservation preempted
  ```

- **Ursache**

  Das Tape-Laufwerk wird von einem anderen Vorgang verwendet oder das Band wurde vorzeitig geschlossen.

- **Korrekturmaßnahme**

  Es sollte sichergestellt sein, dass das Tape-Laufwerk nicht von einem anderen Vorgang verwendet wird und dass die DMA-Anwendung den Auftrag nicht abgebrochen hat; anschließend kann ein erneuter Versuch erfolgen.

Medien konnten nicht initialisiert werden

- **Nachricht**

  `Could not initialize media`

- **Ursache**

  Dieser Fehler kann aus einem der folgenden Gründe auftreten:

  - Das für das Backup verwendete Tape-Laufwerk ist beschädigt oder defekt.
  - Das Band enthält nicht die vollständige Sicherung oder ist beschädigt.
  - Die maximale Anzahl aktiver lokaler Tape-E/A-Threads ist derzeit belegt.

    Es sind maximal 16 aktive lokale Tape-Laufwerke möglich.

- **Korrekturmaßnahme**
  - Wenn das Tape-Laufwerk defekt oder beschädigt ist, sollte der Vorgang mit einem gültigen Tape-Laufwerk wiederholt werden.
  - Wenn das Band nicht die vollständige Sicherung enthält oder beschädigt ist, kann die Wiederherstellung nicht durchgeführt werden.
  - Falls keine Bandressourcen verfügbar sind, sollte abgewartet werden, bis einige Sicherungs- oder Wiederherstellungsaufträge abgeschlossen sind, und anschließend kann der Vorgang erneut versucht werden.

Maximale Anzahl zulässiger Dumps oder Wiederherstellungen (maximales Sitzungslimit) in Bearbeitung

- **Nachricht**

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- **Ursache**

  Die maximale Anzahl an Sicherungs- oder Wiederherstellungsaufträgen wird bereits ausgeführt.

- **Korrekturmaßnahme**

  Der Vorgang kann erneut versucht werden, nachdem einige der aktuell laufenden Aufträge abgeschlossen wurden.

Medienfehler beim Schreiben auf Band

- **Nachricht**

  `Media error on tape write`

- **Ursache**

  Das für das Backup verwendete Band ist beschädigt.

- **Korrekturmaßnahme**

Das Band sollte ausgetauscht und der Backup-Job erneut versucht werden.

Schreibvorgang auf das Band fehlgeschlagen

- **Nachricht**

  ```
  Tape write failed
  ```

- **Ursache**

  Das für das Backup verwendete Band ist beschädigt.

- **Korrekturmaßnahme**

  Das Band sollte ausgetauscht und der Backup-Job erneut versucht werden.

Fehler beim Schreiben auf das Band, neues Band hat einen Medienfehler

- **Nachricht**

  ```
  Tape write failed - new tape encountered media error
  ```

- **Ursache**

  Das für das Backup verwendete Band ist beschädigt.

- **Korrekturmaßnahme**

  Das Band sollte ausgetauscht und das Backup erneut versucht werden.

Schreibvorgang fehlgeschlagen, das neue Band ist beschädigt oder schreibgeschützt.

- **Nachricht**

  ```
  Tape write failed - new tape is broken or write protected
  ```

- **Ursache**

  Das für die Datensicherung verwendete Band ist beschädigt oder schreibgeschützt.

- **Korrekturmaßnahme**

  Das Band sollte ausgetauscht und das Backup erneut versucht werden.

Fehler beim Schreiben auf das Band, das neue Band befindet sich bereits am Ende des Mediums.

- **Nachricht**

  ```
  Tape write failed - new tape is already at the end of media
  ```

- **Ursache**

  Auf dem Band ist nicht genügend Speicherplatz vorhanden, um das Backup abzuschließen.

- **Korrekturmaßnahme**

Das Band sollte ausgetauscht und das Backup erneut versucht werden.

Bandschreibfehler

- **Nachricht**

  ```
  Tape write error - The previous tape had less than the required minimum
  capacity, size MB, for this tape operation, The operation should be restarted
  from the beginning
  ```

- **Ursache**

  Die Bandkapazität ist unzureichend, um die Sicherungsdaten aufzunehmen.

- **Korrekturmaßnahme**

  Bänder mit größerer Kapazität verwenden und den Sicherungsvorgang erneut ausführen.

Medienfehler beim Lesen des Bandes

- **Nachricht**

  ```
  Media error on tape read
  ```

- **Ursache**

  Das Band, von dem die Daten wiederhergestellt werden, ist beschädigt und enthält möglicherweise nicht die vollständigen Backup-Daten.

- **Korrekturmaßnahme**

  Wenn Sie sicher sind, dass sich das vollständige Backup auf dem Band befindet, kann der Wiederherstellungsvorgang erneut versucht werden. Befindet sich das vollständige Backup nicht auf dem Band, ist der Wiederherstellungsvorgang nicht möglich.

Bandlesefehler

- **Nachricht**

  ```
  Tape read error
  ```

- **Ursache**

  Das Tape-Laufwerk ist beschädigt oder das Band enthält nicht das vollständige Backup.

- **Korrekturmaßnahme**

  Ist das Tape-Laufwerk beschädigt, kann ein anderes Tape-Laufwerk verwendet werden. Enthält das Band nicht die vollständige Sicherung, ist eine Wiederherstellung der Daten nicht möglich.

Bereits am Ende des Bands

- **Nachricht**

  ```
  Already at the end of tape
  ```

- **Ursache**

  Das Band enthält keine Daten oder muss zurückgespult werden.

- **Korrekturmaßnahme**

  Wenn das Band keine Daten enthält, das Band mit der Sicherung verwenden und den Wiederherstellungsvorgang erneut versuchen. Andernfalls das Band zurückspulen und den Wiederherstellungsvorgang erneut versuchen.

Die Tape-Aufzeichnungsgröße ist zu klein. Eine größere Größe sollte verwendet werden.

- **Nachricht**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Ursache**

  Der für den Wiederherstellungsvorgang festgelegte Blockierungsfaktor ist kleiner als der Blockierungsfaktor, der während des Backups verwendet wurde.

- **Korrekturmaßnahme**

  Es wird derselbe Blockierungsfaktor verwendet, der während des Backups angegeben wurde.

Die Größe des Banddatensatzes sollte block_size1 und nicht block_size2 betragen.

- **Nachricht**

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- **Ursache**

  Der für die lokale Wiederherstellung angegebene Blockierungsfaktor ist falsch.

- **Korrekturmaßnahme**

  Den Wiederherstellungsauftrag mit `block_size1` als blockierendem Faktor erneut versuchen.

Die Größe der Tape-Aufzeichnung muss im Bereich zwischen 4 KB und 256 KB liegen

- **Nachricht**

  ```
  Tape record size must be in the range between 4KB and 256KB
  ```

- **Ursache**

  Der für den Sicherungs- oder Wiederherstellungsvorgang festgelegte Blockierungsfaktor liegt nicht im zulässigen Bereich.

- **Korrekturmaßnahme**

  Ein Blockierungsfaktor im Bereich von 4 KB bis 256 KB kann angegeben werden.

NDMP-Fehlermeldungen

Netzwerkkommunikationsfehler

- **Nachricht**

  ```
  Network communication error
  ```

- **Ursache**

  Die Kommunikation zu einem entfernten Tape-Gerät in einer NDMP-Dreiwegeverbindung ist fehlgeschlagen.

- **Korrekturmaßnahme**

  Die Netzwerkverbindung zum Remote-Mover sollte überprüft werden.

Meldung vom Lesesocket: Fehlerzeichenfolge

- **Nachricht**

  ```
  Message from Read Socket: error_string
  ```

- **Ursache**

  Die Wiederherstellung der Kommunikation vom entfernten Band in der NDMP 3-Wege-Verbindung weist Fehler auf.

- **Korrekturmaßnahme**

  Die Netzwerkverbindung zum Remote-Mover sollte überprüft werden.

Meldung von Write Dirnet: Fehlerzeichenfolge

- **Nachricht**

  ```
  Message from Write Dirnet: error_string
  ```

- **Ursache**

  Bei der Backup-Kommunikation zu einem entfernten Bandlaufwerk in einer NDMP-Dreiwegeverbindung ist ein Fehler aufgetreten.

- **Korrekturmaßnahme**

  Die Netzwerkverbindung zum Remote-Mover sollte überprüft werden.

Socket-Lesevorgang: EOF empfangen

- **Nachricht**

  ```
  Read Socket received EOF
  ```

- **Ursache**

  Der Versuch, über eine NDMP-Dreiwegeverbindung mit einem entfernten Tape zu kommunizieren, hat das

Dateiende erreicht. Möglicherweise wird eine Dreiwege-Wiederherstellung aus einem Backup-Image mit größerer Blockgröße versucht.

- **Korrekturmaßnahme**

  Die korrekte Blockgröße angeben und den Wiederherstellungsvorgang erneut versuchen.

ndmpd ungültige Versionsnummer: version_number ``

- **Nachricht**

  ```
  ndmpd invalid version number: version_number
  ```

- **Ursache**

  Die angegebene NDMP-Version wird vom Storage-System nicht unterstützt.

- **Korrekturmaßnahme**

  NDMP-Version 4 angeben.

ndmpd Sitzung session_ID nicht aktiv

- **Nachricht**

  ```
  ndmpd session session_ID not active
  ```

- **Ursache**

  Die NDMP-Sitzung existiert möglicherweise nicht.

- **Korrekturmaßnahme**

  Mit dem `ndmpd status`Befehl lassen sich die aktiven NDMP-Sitzungen anzeigen.

Die Volumenreferenz für das Volume „volume_name“ konnte nicht ermittelt werden.

- **Nachricht**

  ```
  Could not obtain vol ref for Volume vol_name
  ```

- **Ursache**

  Die Volumenreferenz konnte nicht ermittelt werden, da das Volumen möglicherweise von anderen Operationen verwendet wird.

- **Korrekturmaßnahme**

  Wiederholen Sie den Vorgang zu einem späteren Zeitpunkt.

Der Datenverbindungstyp ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] wird für ["IPv6"|"IPv4"] Steuerverbindungen nicht unterstützt.

- **Nachricht**

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  ```

```
for ["IPv6"|"IPv4"] control connections
```

- **Ursache**

  Im knotenbezogenen NDMP-Modus muss die hergestellte NDMP-Datenverbindung denselben Netzwerkadresstyp (IPv4 oder IPv6) wie die NDMP-Steuerverbindung aufweisen.

- **Korrekturmaßnahme**

  Wenden Sie sich an Ihren Backup-Anwendungsanbieter.

DATA LISTEN: Fehler bei der Vorbereitung der CAB Datenverbindungsvoraussetzung

- **Nachricht**

```
DATA LISTEN: CAB data connection prepare precondition error
```

- **Ursache**

  Der NDMP-Datenempfang schlägt fehl, wenn die Backup-Anwendung die CAB-Erweiterung mit dem NDMP-Server ausgehandelt hat und ein Unterschied im angegebenen NDMP-Datenverbindungsadressentyp zwischen den NDMP_CAB_DATA_CONN_PREPARE- und den NDMP_DATA_LISTEN-Nachrichten besteht.

- **Korrekturmaßnahme**

  Wenden Sie sich an Ihren Backup-Anwendungsanbieter.

DATENVERBINDUNG: Fehler bei der Vorbereitung der CAB-Datenverbindungsvoraussetzung

- **Nachricht**

```
DATA CONNECT: CAB data connection prepare precondition error
```

- **Ursache**

  Die NDMP-Datenverbindung schlägt fehl, wenn die Backup-Anwendung die CAB-Erweiterung mit dem NDMP-Server ausgehandelt hat und es eine Diskrepanz im angegebenen NDMP-Datenverbindungsadresstyp zwischen den NDMP_CAB_DATA_CONN_PREPARE- und den NDMP_DATA_CONNECT-Nachrichten gibt.

- **Korrekturmaßnahme**

  Wenden Sie sich an Ihren Backup-Anwendungsanbieter.

Fehler: Anzeige fehlgeschlagen: Passwort für Benutzer '<username>' konnte nicht abgerufen werden

- **Nachricht**

```
Error: show failed: Cannot get password for user '<username>'
```

- **Ursache**

  Unvollständige Benutzerkontokonfiguration für NDMP

- **Korrekturmaßnahme**

  Es ist sicherzustellen, dass das Benutzerkonto mit der SSH-Zugriffsmethode verknüpft ist und das Authentifizierungsverfahren das Benutzerpasswort ist.

Fehlermeldungen ausgeben

Das Zielvolume ist schreibgeschützt

- **Nachricht**

  ```
  Destination volume is read-only
  ```

- **Ursache**

  Der Pfad, zu dem die Wiederherstellungsoperation versucht wird, ist schreibgeschützt.

- **Korrekturmaßnahme**

  Es kann versucht werden, die Daten an einem anderen Speicherort wiederherzustellen.

Der Ziel-qtree ist schreibgeschützt

- **Nachricht**

  ```
  Destination qtree is read-only
  ```

- **Ursache**

  Der Qtree, in den die Wiederherstellung erfolgen soll, ist schreibgeschützt.

- **Korrekturmaßnahme**

  Es kann versucht werden, die Daten an einem anderen Speicherort wiederherzustellen.

Dumps auf dem Volume vorübergehend deaktiviert, erneut versuchen

- **Nachricht**

  ```
  Dumps temporarily disabled on volume, try again
  ```

- **Ursache**

  Ein NDMP-Dump-Backup wird auf einem SnapMirror Zielvolume versucht, das Teil einer `snapmirror break` oder einer `snapmirror resync` Operation ist.

- **Korrekturmaßnahme**

  Warten Sie, bis die `snapmirror break` oder `snapmirror resync` Operation abgeschlossen ist und anschließend die Dump-Operation durchgeführt werden kann.

  > Immer wenn sich der Status eines SnapMirror Zielvolumes von lesen/schreiben auf lesen/allein oder von lesen/allein auf lesen/schreiben ändert, ist eine Basissicherung erforderlich.

Verwandte Informationen

- "snapmirror break"
- "SnapMirror Resynchronisierung"

NFS-Labels werden nicht erkannt

- **Nachricht**

  ```
  Error: Aborting: dump encountered NFS security labels in the file system
  ```

- **Ursache**

  NFS-Sicherheitsbezeichnungen werden ab ONTAP 9.9.1 unterstützt, wenn NFSv4.2 aktiviert ist. Allerdings werden NFS-Sicherheitsbezeichnungen derzeit von der Dump-Engine nicht erkannt. Wenn NFS-Sicherheitsbezeichnungen in Dateien, Verzeichnissen oder speziellen Dateien in einem beliebigen Dump-Format vorhanden sind, schlägt der Dump fehl.

- **Korrekturmaßnahme**

  Es ist zu überprüfen, dass keine Dateien oder Verzeichnisse NFS-Sicherheitsbezeichnungen aufweisen.

Es wurden keine Dateien erstellt

- **Nachricht**

  ```
  No files were created
  ```

- **Ursache**

  Es wurde versucht, ein Verzeichnis-DAR durchzuführen, ohne die erweiterte DAR-Funktionalität zu aktivieren.

- **Korrekturmaßnahme**

  Die erweiterte DAR-Funktionalität aktivieren und den DAR erneut versuchen.

Die Wiederherstellung der Datei <file name> ist fehlgeschlagen

- **Nachricht**

  ```
  Restore of the file file name failed
  ```

- **Ursache**

  Wenn eine DAR (Direct Access Recovery) einer Datei durchgeführt wird, deren Dateiname mit dem einer LUN auf dem Zielvolume identisch ist, schlägt die DAR fehl.

- **Korrekturmaßnahme**

  Erneuter DAR-Versuch der Datei.

Fehler beim Kürzen des Quell-Inodes <inode number>…

- **Nachricht**

`Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.`

- **Ursache**

  Der Inode einer Datei wird gelöscht, wenn die Datei wiederhergestellt wird.

- **Korrekturmaßnahme**

  Es sollte abgewartet werden, bis der Wiederherstellungsvorgang auf einem Volume abgeschlossen ist, bevor dieses Volume verwendet wird.

Der für den Dump benötigte Snapshot konnte nicht gesperrt werden.

- **Nachricht**

  `Unable to lock a snapshot needed by dump`

- **Ursache**

  Der für die Sicherung angegebene Snapshot ist nicht verfügbar.

- **Korrekturmaßnahme**

  Die Sicherung kann mit einem anderen Snapshot erneut versucht werden.

  Mit dem `snap list` Befehl lässt sich die Liste der verfügbaren Snapshots anzeigen.

  Weitere Informationen zu `snap list` finden sich in der "ONTAP-Befehlsreferenz".

Bitmap-Dateien konnten nicht gefunden werden

- **Nachricht**

  `Unable to locate bitmap files`

- **Ursache**

  Die für die Datensicherung benötigten Bitmap-Dateien wurden möglicherweise gelöscht. In diesem Fall kann die Datensicherung nicht neu gestartet werden.

- **Korrekturmaßnahme**

  Die Datensicherung wird erneut durchgeführt.

Das Volumen befindet sich vorübergehend in einem Übergangszustand

- **Nachricht**

  `Volume is temporarily in a transitional state`

- **Ursache**

  Das zu sichernde Volume befindet sich vorübergehend im nicht eingebundenen Zustand.

- **Korrekturmaßnahme**

  Nach einer kurzen Wartezeit kann die Datensicherung erneut durchgeführt werden.

SMTape-Fehlermeldungen

Stücke in falscher Reihenfolge

- **Nachricht**

  ```
  Chunks out of order
  ```

- **Ursache**

  Die Sicherungsbänder werden nicht in der richtigen Reihenfolge wiederhergestellt.

- **Korrekturmaßnahme**

  Der Wiederherstellungsvorgang sollte erneut versucht und die Bänder in der richtigen Reihenfolge geladen werden.

Chunk-Format nicht unterstützt

- **Nachricht**

  ```
  Chunk format not supported
  ```

- **Ursache**

  Das Sicherungsabbild ist nicht vom Typ SMTape.

- **Korrekturmaßnahme**

  Wenn das Sicherungsabbild nicht von SMTape stammt, sollte der Vorgang mit einem Band wiederholt werden, das das SMTape-Backup enthält.

Speicherzuweisung fehlgeschlagen

- **Nachricht**

  ```
  Failed to allocate memory
  ```

- **Ursache**

  Dem System ist der Arbeitsspeicher ausgegangen.

- **Korrekturmaßnahme**

  Der Auftrag kann zu einem späteren Zeitpunkt ausgeführt werden, wenn das System weniger ausgelastet ist.

Fehler beim Abrufen des Datenpuffers

- **Nachricht**

```
Failed to get data buffer
```

- **Ursache**

  Das Speichersystem hatte keine Puffer mehr.

- **Korrekturmaßnahme**

  Warten Sie, bis einige Speichersystemoperationen abgeschlossen sind, und versuchen Sie dann den Auftrag erneut.

Snapshot konnte nicht gefunden werden

- **Nachricht**

```
Failed to find snapshot
```

- **Ursache**

  Der für die Sicherung angegebene Snapshot ist nicht verfügbar.

- **Korrekturmaßnahme**

  Es wird geprüft, ob der angegebene Snapshot verfügbar ist. Ist dies nicht der Fall, erfolgt ein erneuter Versuch mit dem korrekten Snapshot.

Snapshot konnte nicht erstellt werden

- **Nachricht**

```
Failed to create snapshot
```

- **Ursache**

  Das Volume enthält bereits die maximale Anzahl an Snapshots.

- **Korrekturmaßnahme**

  Einige Snapshots löschen und anschließend den Sicherungsvorgang erneut versuchen.

Snapshot konnte nicht gesperrt werden

- **Nachricht**

```
Failed to lock snapshot
```

- **Ursache**

  Der Snapshot ist entweder in Verwendung oder wurde gelöscht.

- **Korrekturmaßnahme**

  Wenn der Snapshot von einem anderen Vorgang verwendet wird, sollte abgewartet werden, bis dieser abgeschlossen ist, und anschließend kann die Sicherung erneut versucht werden. Wenn der Snapshot gelöscht wurde, ist eine Sicherung nicht möglich.

Fehler beim Löschen des Snapshots

- **Nachricht**

  `Failed to delete snapshot`

- **Ursache**

  Der automatische Snapshot konnte nicht gelöscht werden, da er von anderen Vorgängen verwendet wird.

- **Korrekturmaßnahme**

  Mit dem `snap` Befehl lässt sich der Status des Snapshots bestimmen. Wenn der Snapshot nicht benötigt wird, kann er manuell gelöscht werden.

Fehler beim Abrufen des neuesten Snapshots

- **Nachricht**

  `Failed to get latest snapshot`

- **Ursache**

  Der neueste Snapshot existiert möglicherweise nicht, da das Volume gerade von SnapMirror initialisiert wird.

- **Korrekturmaßnahme**

  Nach Abschluss der Initialisierung erneut versuchen.

Neues Band konnte nicht geladen werden

- **Nachricht**

  `Failed to load new tape`

- **Ursache**

  Fehler im Tape-Laufwerk oder Medium.

- **Korrekturmaßnahme**

  Das Tape austauschen und den Vorgang erneut versuchen.

Bandinitialisierung fehlgeschlagen

- **Nachricht**

  `Failed to initialize tape`

- **Ursache**

  Diese Fehlermeldung kann aus einem der folgenden Gründe angezeigt werden:

  - Das Sicherungsabbild ist nicht vom Typ SMTape.

- Der angegebene Bandblockierungsfaktor ist falsch.
- Das Band ist beschädigt oder defekt.
- Für die Wiederherstellung wurde das falsche Band eingelegt.

- **Korrekturmaßnahme**
  - Wenn das Sicherungsabbild nicht von SMTape stammt, sollte der Vorgang mit einem Band mit SMTape-Sicherung wiederholt werden.
  - Falls der Blockierungsfaktor falsch ist, sollte der korrekte Blockierungsfaktor angegeben und der Vorgang erneut versucht werden.
  - Wenn das Band beschädigt ist, ist die Wiederherstellung nicht möglich.
  - Wenn das falsche Band eingelegt ist, sollte der Vorgang mit dem richtigen Band wiederholt werden.

Fehler beim Initialisieren des Wiederherstellungsstreams

- **Nachricht**

  ```
  Failed to initialize restore stream
  ```

- **Ursache**

  Diese Fehlermeldung kann aus einem der folgenden Gründe angezeigt werden:

  - Das Sicherungsabbild ist nicht vom Typ SMTape.
  - Der angegebene Bandblockierungsfaktor ist falsch.
  - Das Band ist beschädigt oder defekt.
  - Für die Wiederherstellung wurde das falsche Band eingelegt.

- **Korrekturmaßnahme**
  - Wenn das Sicherungsabbild nicht von SMTape stammt, sollte der Vorgang mit einem Band wiederholt werden, das das SMTape-Backup enthält.
  - Falls der Blockierungsfaktor falsch ist, sollte der korrekte Blockierungsfaktor angegeben und der Vorgang erneut versucht werden.
  - Wenn das Band beschädigt ist, ist die Wiederherstellung nicht möglich.
  - Wenn das falsche Band eingelegt ist, sollte der Vorgang mit dem richtigen Band wiederholt werden.

Fehler beim Lesen des Sicherungsabbilds

- **Nachricht**

  ```
  Failed to read backup image
  ```

- **Ursache**

  Das Band ist beschädigt.

- **Korrekturmaßnahme**

  Wenn das Band beschädigt ist, ist die Wiederherstellung nicht möglich.

Bildheader fehlt oder ist beschädigt

- **Nachricht**

  `Image header missing or corrupted`

- **Ursache**

  Das Band enthält keine gültige SMTape-Backup.

- **Korrekturmaßnahme**

  Erneuter Versuch mit einem Band, das ein gültiges Backup enthält.

Interne Assertion

- **Nachricht**

  `Internal assertion`

- **Ursache**

  Es ist ein interner SMTape Fehler aufgetreten.

- **Korrekturmaßnahme**

  Melden Sie den Fehler und senden Sie die `etc/log/backup` Datei an den technischen Support.

Ungültige Sicherungsimage-Magic-Nummer

- **Nachricht**

  `Invalid backup image magic number`

- **Ursache**

  Das Sicherungsabbild ist nicht vom Typ SMTape.

- **Korrekturmaßnahme**

  Wenn das Sicherungsabbild nicht von SMTape stammt, sollte der Vorgang mit einem Band wiederholt werden, das das SMTape-Backup enthält.

Ungültige Prüfsumme des Backup-Images

- **Nachricht**

  `Invalid backup image checksum`

- **Ursache**

  Das Band ist beschädigt.

- **Korrekturmaßnahme**

  Wenn das Band beschädigt ist, ist die Wiederherstellung nicht möglich.

Ungültiges Eingabeband

- **Nachricht**

  ```
  Invalid input tape
  ```

- **Ursache**

  Die Signatur des Sicherungsabbilds im Bandkopf ist ungültig. Das Band enthält beschädigte Daten oder kein gültiges Sicherungsabbild.

- **Korrekturmaßnahme**

  Der Wiederherstellungsvorgang kann mit einem gültigen Sicherungsabbild erneut ausgeführt werden.

Ungültiger Volume-Pfad

- **Nachricht**

  ```
  Invalid volume path
  ```

- **Ursache**

  Das für die Sicherungs- oder Wiederherstellungsoperation angegebene Volume wurde nicht gefunden.

- **Korrekturmaßnahme**

  Den Auftrag mit einem gültigen Volume-Pfad und Volume-Namen erneut ausführen.

Fehler in Backup-Satz-ID

- **Nachricht**

  ```
  Mismatch in backup set ID
  ```

- **Ursache**

  Das beim Bandwechsel eingelegte Band ist nicht Teil des Backup-Satzes.

- **Korrekturmaßnahme**

  Das richtige Band muss eingelegt werden, anschließend kann der Auftrag erneut versucht werden.

Abweichung im Backup-Zeitstempel

- **Nachricht**

  ```
  Mismatch in backup time stamp
  ```

- **Ursache**

  Das beim Bandwechsel eingelegte Band ist nicht Teil des Backup-Satzes.

- **Korrekturmaßnahme**

  Mit dem `smtape restore -h`Befehl lassen sich die Header-Informationen eines Bandes überprüfen.

Auftrag aufgrund von Systemabschaltung abgebrochen

- **Nachricht**

  ```
  Job aborted due to shutdown
  ```

- **Ursache**

  Das Speichersystem wird neu gestartet.

- **Korrekturmaßnahme**

  Der Auftrag kann nach einem Neustart des Speichersystems erneut ausgeführt werden.

Auftrag aufgrund automatischer Snapshot-Autolöschung abgebrochen

- **Nachricht**

  ```
  Job aborted due to snapshot autodelete
  ```

- **Ursache**

  Das Volume verfügt nicht über genügend Speicherplatz und hat die automatische Löschung von Snapshots ausgelöst.

- **Korrekturmaßnahme**

  Speicherplatz im Volume freigeben und den Auftrag erneut ausführen.

Das Band wird derzeit von anderen Vorgängen verwendet.

- **Nachricht**

  ```
  Tape is currently in use by other operations
  ```

- **Ursache**

  Das Tape-Laufwerk wird von einem anderen Auftrag verwendet.

- **Korrekturmaßnahme**

  Die Datensicherung kann erneut versucht werden, nachdem der aktuell aktive Auftrag abgeschlossen ist.

Bänder außerhalb der Reihenfolge

- **Nachricht**

  ```
  Tapes out of order
  ```

- **Ursache**

  Das erste Band der Bandsequenz für den Wiederherstellungsvorgang besitzt keinen Image-Header.

- **Korrekturmaßnahme**

  Das Band mit dem Image-Header einlegen und den Auftrag erneut versuchen.

Übertragung fehlgeschlagen (Abbruch aufgrund eines MetroCluster Vorgangs)

- **Nachricht**

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- **Ursache**

  Der SMTape Vorgang wird aufgrund eines Switchover oder Switchback Vorgangs abgebrochen.

- **Korrekturmaßnahme**

  Der SMTape-Vorgang erfolgt nach Abschluss des Switchover- oder Switchback-Vorgangs.

Transfer fehlgeschlagen (ARL-initiierter Abbruch)

- **Nachricht**

  ```
  Transfer failed (ARL initiated abort)
  ```

- **Ursache**

  Während ein SMTape-Vorgang läuft, wird der SMTape-Vorgang abgebrochen, wenn eine Aggregat-Relokation eingeleitet wird.

- **Korrekturmaßnahme**

  Der SMTape-Vorgang erfolgt, nachdem der Vorgang zur Umlagerung der Aggregate abgeschlossen ist.

Transfer fehlgeschlagen (CFO-initiierter Abbruch)

- **Nachricht**

  ```
  Transfer failed (CFO initiated abort)
  ```

- **Ursache**

  Der SMTape Vorgang wird aufgrund eines Storage-Failover (Übernahme und Rückgabe) Vorgangs eines CFO-Aggregats abgebrochen.

- **Korrekturmaßnahme**

  Die SMTape-Operation erfolgt, nachdem das Storage-Failover des CFO Aggregats abgeschlossen ist.

Transfer fehlgeschlagen (SFO-initiierter Abbruch)

- **Nachricht**

  ```
  Transfer failed (SFO initiated abort)
  ```

- **Ursache**

  Der SMTape Vorgang wird aufgrund eines Storage-Failover (Übernahme und Rückgabe) abgebrochen.

- **Korrekturmaßnahme**

Der SMTape-Vorgang wird nach Abschluss des Storage-Failover (Takeover und Giveback) durchgeführt.

Zugrundeliegendes Aggregat unter Migration

- **Nachricht**

  `Underlying aggregate under migration`

- **Ursache**

  Wenn ein SMTape-Vorgang auf einem Aggregat gestartet wird, das sich in Migration befindet (Storage-Failover oder Aggregat-Relocation), schlägt der SMTape-Vorgang fehl.

- **Korrekturmaßnahme**

  Der SMTape-Vorgang wird nach Abschluss der Aggregatmigration durchgeführt.

Das Volume befindet sich derzeit in der Migration

- **Nachricht**

  `Volume is currently under migration`

- **Ursache**

  Volumemigration und SMTape Backup können nicht gleichzeitig ausgeführt werden.

- **Korrekturmaßnahme**

  Der Sicherungsauftrag kann nach Abschluss der Volume-Migration erneut ausgeführt werden.

Volume offline

- **Nachricht**

  `Volume offline`

- **Ursache**

  Das zu sichernde Volume ist offline.

- **Korrekturmaßnahme**

  Das Volume online schalten und die Datensicherung erneut versuchen.

Volume nicht eingeschränkt

- **Nachricht**

  `Volume not restricted`

- **Ursache**

  Das Zielvolume, auf das die Daten wiederhergestellt werden, ist nicht eingeschränkt.

- **Korrekturmaßnahme**

  Das Volume einschränken und den Wiederherstellungsvorgang erneut versuchen.

NDMP-Konfiguration

Erfahren Sie mehr über die ONTAP NDMP-Konfiguration

Sie können ein ONTAP 9 Cluster schnell so konfigurieren, dass das Network Data Management Protocol (NDMP) verwendet wird, um Daten direkt mithilfe einer Backup-Applikation eines Drittanbieters auf Tape zu sichern.

Wenn die Backup-Anwendung Cluster Aware Backup (CAB) unterstützt, ist eine Konfiguration von NDMP als *SVM-scoped* oder *node-scoped* möglich:

- Die SVM-basierte Sicherung auf Cluster- (Admin-SVM-) Ebene ermöglicht das Backup aller Volumes, die auf verschiedenen Knoten des Clusters gehostet werden. SVM-basierter NDMP-Service wird, wo möglich, empfohlen.
- Node-scoped NDMP ermöglicht das Sichern aller auf diesem Knoten gehosteten Volumes.

Wenn die Backup-Anwendung CAB nicht unterstützt, ist node-scope NDMP zu verwenden.

SVM-bezogene und knotenbezogene NDMP schließen sich gegenseitig aus, sie können nicht auf demselben Cluster konfiguriert werden.

Node-scoped NDMP ist in ONTAP 9 veraltet.

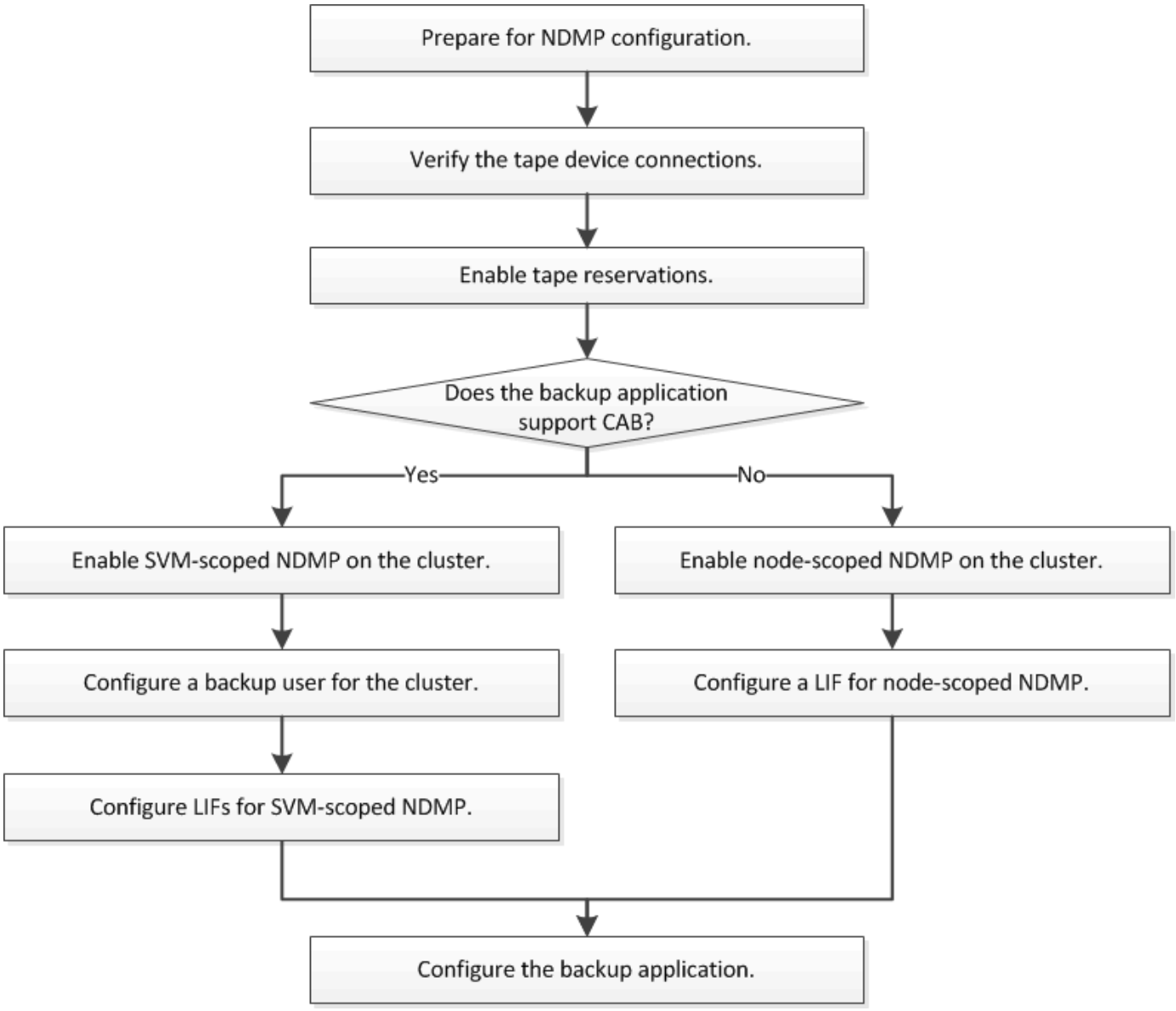
Weitere Informationen zu "Cluster Aware Backup (CAB)".

Vor der Konfiguration von NDMP ist Folgendes zu überprüfen:

- Sie verwenden eine Backup-Anwendung eines Drittanbieters (auch Data Management Application oder DMA genannt).
- Sie sind ein Cluster-Administrator.
- Tape-Geräte und ein optionaler Medienserver sind installiert.
- Tape-Geräte sind über einen Fibre Channel (FC) Switch oder lokal mit dem Cluster verbunden.
- Mindestens ein Tape-Gerät hat eine logische Einheitennummer (LUN) von 0.

Informationen zum ONTAP NDMP Konfigurationsworkflow

Die Einrichtung von Tape-Backup über NDMP umfasst die Vorbereitung der NDMP-Konfiguration, die Überprüfung der Tape-Gerät-Verbindungen, die Aktivierung von Tape-Reservierungen, die Konfiguration von NDMP auf SVM- oder Knotenebene, die Aktivierung von NDMP im Cluster, die Konfiguration eines Backup-Benutzers, die Konfiguration von LIFs und die Konfiguration der Backup-Anwendung.



ONTAP NDMP-Konfigurationen vorbereiten

Bevor Tape-Backup-Zugriff über das Network Data Management Protocol (NDMP) konfiguriert wird, muss überprüft werden, ob die geplante Konfiguration unterstützt wird, ob die Tape-Laufwerke auf jedem Knoten als qualifizierte Laufwerke aufgeführt sind, ob alle Knoten über Intercluster-LIFs verfügen und ob die Backup-Applikation die Cluster Aware Backup (CAB) Erweiterung unterstützt.

Schritte

1. In der Kompatibilitätsmatrix Ihres Anbieters von Applikationen finden sich Informationen zur ONTAP-Unterstützung (NetApp qualifiziert keine Backup-Anwendungen von Drittanbietern mit ONTAP oder NDMP).

   Es sollte überprüft werden, ob die folgenden NetApp-Komponenten kompatibel sind:

   - Die auf dem Cluster ausgeführte Version von ONTAP 9.
   - Anbieter und Version der Backup-Anwendung: zum Beispiel Veritas NetBackup 8.2 oder CommVault.

- Die Bandgerätedetails, wie z. B. Hersteller, Modell und Schnittstelle der Bandlaufwerke: zum Beispiel IBM Ultrium 8 oder HPe StoreEver Ultrium 30750 LTO-8.
- Die Plattformen der Knoten im Cluster: zum Beispiel FAS8700 oder A400.

> Kompatibilitätsmatrizen für ältere ONTAP-Versionen für Backup-Anwendungen sind in der "NetApp Interoperabilitätsmatrix-Tool" zu finden.

2. Es sollte sichergestellt sein, dass Ihre Tape-Laufwerke als qualifizierte Laufwerke in der integrierten Tape-Konfigurationsdatei jedes Node aufgeführt sind:

   a. In der Befehlszeilenschnittstelle lässt sich die integrierte Tape-Konfigurationsdatei mit dem `storage tape show-supported-status` Befehl anzeigen.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                 Is
Tape Drives                      Supported  Support Status
-------------------------------  ---------
-------------------------------
Certance Ultrium 2               true       Dynamically Qualified
Certance Ultrium 3               true       Dynamically Qualified
Digital DLT2000                  true       Qualified
```

   b. Vergleichen Sie Ihre Tape-Laufwerke mit der Liste der qualifizierten Laufwerke in der Ausgabe.

> Die Bezeichnungen der Tape-Geräte in der Ausgabe können geringfügig von den Bezeichnungen auf dem Geräteetikett oder in der Interoperabilitätsmatrix abweichen. Beispielsweise kann Digital DLT2000 auch als DLT2k bezeichnet werden. Diese geringfügigen Namensunterschiede können ignoriert werden.

   c. Wird ein Gerät in der Ausgabe nicht als qualifiziert aufgeführt, obwohl es gemäß der Interoperabilitätsmatrix qualifiziert ist, kann eine aktualisierte Konfigurationsdatei für das Gerät entsprechend den Anweisungen auf der NetApp Support Site heruntergeladen und installiert werden.

      "NetApp Downloads: Konfigurationsdateien für Tape-Geräte"

   Ein qualifiziertes Gerät ist möglicherweise nicht in der integrierten Tape-Konfigurationsdatei aufgeführt, wenn das Tape-Gerät erst nach der Auslieferung des Knotens qualifiziert wurde.

3. Es sollte sichergestellt werden, dass jeder Knoten im Cluster über eine Intercluster-LIF verfügt:

   a. Zeigen Sie die Intercluster-LIFs auf den Knoten mit dem `network interface show -service -policy default-intercluster`-Befehl an.

```
cluster1::> network interface show -service-policy default-
intercluster
```

```
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

b. Falls auf keinem Knoten ein Intercluster-LIF existiert, kann ein Intercluster-LIF mit dem `network interface create` Befehl erstellt werden.

```
cluster1::> network interface create -vserver cluster1 -lif IC2
-service-policy default-intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -service-policy default-
intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

"Netzwerkmanagement"

4. Anhand der mit der Backup-Anwendung gelieferten Dokumentation lässt sich feststellen, ob die Backup-Anwendung Cluster Aware Backup (CAB) unterstützt.

   Die Unterstützung von CAB ist ein Schlüsselfaktor bei der Bestimmung der Art der Datensicherung, die durchgeführt werden kann.

Verwandte Informationen

- "storage tape show"
- "storage tape show-supported-status"

Verbindungen von ONTAP NDMP Tape-Geräten überprüfen

Es ist sicherzustellen, dass alle Laufwerke und Medienwechsler in ONTAP als Geräte sichtbar sind.

Schritte

1. Informationen zu allen Laufwerken und Medienwechslern lassen sich mit dem `storage tape show` Befehl anzeigen.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID               Device Type     Description
Status
----------------------  --------------  ------------------------------
--------
sw4:10.11               tape drive      HP LTO-3
normal
0b.125L1                media changer   HP MSL G3 Series
normal
0d.4                    tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                  media changer   IBM 3573-TL
normal
...
```

2. Wenn ein Tape-Laufwerk nicht angezeigt wird, sollte das Problem überprüft werden.
3. Falls kein Medienwechsler angezeigt wird, können Informationen über Medienwechsler mit dem `storage tape show-media-changer` Befehl angezeigt und das Problem anschließend analysiert werden.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
```

```
Status
-----------------------  ---------  -------  -----------------------
--------
cluster1-01              2b         mc0      in-use
normal
...
```

Verwandte Informationen

- "storage tape show-media-changer"

Bandreservierungen für ONTAP NDMP-Backup-Vorgänge aktivieren

Es ist sicherzustellen, dass Tape-Laufwerke für die Nutzung durch Backup-Applikationen bei NDMP-Backup-Vorgängen reserviert sind.

Über diese Aufgabe

Die Reservierungseinstellungen variieren je nach Backup-Applikation und müssen mit der Backup-Applikation sowie den Knoten oder Servern, die dieselben Laufwerke verwenden, übereinstimmen. Die korrekten Reservierungseinstellungen sind in der Herstellerdokumentation der Backup-Applikation zu finden.

Schritte

1. Reservierungen werden mit dem `options -option-name tape.reservations -option-value persistent` Befehl aktiviert.

   Der folgende Befehl aktiviert Reservierungen mit dem `persistent` Wert:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Es sollte überprüft werden, ob Reservierungen auf allen Knoten mithilfe des `options tape.reservations`-Befehls aktiviert sind, und anschließend die Ausgabe betrachtet werden.

   ```
   cluster1::> options tape.reservations

   cluster1-1
       tape.reservations                persistent

   cluster1-2
       tape.reservations                persistent
   2 entries were displayed.
   ```

SVM-bezogenes NDMP konfigurieren

SVM-bezogenes NDMP auf dem ONTAP Cluster aktivieren

Wenn der DMA die Cluster Aware Backup (CAB) Erweiterung unterstützt, ist das Sichern aller Volumes, die auf verschiedenen Knoten in einem Cluster gehostet werden, möglich, indem SVM-scoped NDMP aktiviert wird, der NDMP-Service auf dem Cluster (admin SVM) aktiviert wird und LIFs für die Daten- und Steuerverbindung konfiguriert werden.

Bevor Sie beginnen

Die CAB-Erweiterung muss vom DMA unterstützt werden.

Über diese Aufgabe

Durch das Deaktivieren des knotenbezogenen NDMP-Modus wird der SVM-bezogene NDMP-Modus auf dem Cluster aktiviert.

Schritte

1. SVM-bezogener NDMP-Modus:

```
cluster1::> system services ndmp node-scope-mode off
```

   Der SVM-basierte NDMP-Modus ist aktiviert.

2. NDMP-Service auf der Administrator-SVM aktivieren:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

   Der Authentifizierungstyp ist standardmäßig auf `challenge` gesetzt und die Authentifizierung im Klartext ist deaktiviert.

   Für eine sichere Kommunikation sollte die Authentifizierung im Klartext deaktiviert bleiben.

3. Es sollte überprüft werden, ob der NDMP-Service aktiviert ist:

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Backup-Benutzer für ONTAP NDMP Authentifizierung aktivieren

Zur Authentifizierung von SVM-scoped NDMP aus der Backup-Anwendung muss ein Administratorbenutzer mit ausreichenden Berechtigungen und ein NDMP-Passwort vorhanden sein.

Über diese Aufgabe

Sie müssen ein NDMP-Passwort für Backup-Admin-Benutzer generieren. Backup-Admin-Benutzer können auf Cluster- oder SVM-Ebene aktiviert werden, und falls erforderlich, kann ein neuer Benutzer erstellt werden. Standardmäßig können sich Benutzer mit den folgenden Rollen für NDMP-Backup authentifizieren:

- Cluster-weit: `admin` oder `backup`
- Einzelne SVMs: `vsadmin` oder `vsadmin-backup`

Wenn Sie einen NIS- oder LDAP-Benutzer verwenden, muss dieser Benutzer auf dem jeweiligen Server existieren. Ein Active Directory-Benutzer kann nicht verwendet werden.

Schritte

1. Die aktuellen Administratorbenutzer und Berechtigungen werden angezeigt:

   `security login show`

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

2. Falls erforderlich kann ein neuer NDMP-Backup-Benutzer mit dem `security login create` Befehl und der passenden Rolle für clusterweite oder individuelle SVM-Berechtigungen erstellt werden.

   Sie können einen lokalen Backup-Benutzernamen oder einen NIS- oder LDAP-Benutzernamen für den `-user-or-group-name` Parameter angeben.

   Der folgende Befehl erstellt den Backup-Benutzer `backup_admin1` mit der `backup` Rolle für den gesamten Cluster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   Der folgende Befehl erstellt den Backup-Benutzer `vsbackup_admin1` mit der `vsadmin-backup` Rolle für eine einzelne SVM:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Geben Sie ein Passwort für den neuen Benutzer ein und bestätigen Sie es.

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

3. Ein Passwort für die Admin-SVM wird mithilfe des `vserver services ndmp generate password` Befehls generiert.

   Das generierte Passwort muss zur Authentifizierung der NDMP-Verbindung durch die Backup-Anwendung verwendet werden.

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1
   -user backup_admin1

    Vserver: cluster1
       User: backup_admin1
   ```

```
Password: qG5CqQHYxw7tE57g
```

ONTAP LIFs für SVM-bezogenes NDMP konfigurieren

Sie müssen die LIFs identifizieren, die für die Herstellung einer Datenverbindung zwischen den Daten- und Tape-Ressourcen sowie für die Steuerungsverbindung zwischen der Admin-SVM und der Backup-Anwendung verwendet werden. Nach der Identifizierung der LIFs ist zu überprüfen, ob die Service- und Failover-Richtlinien festgelegt sind.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Unterstützten Datenverkehr verwalten".

ONTAP 9.10.1 oder höher

Schritte

1. Die auf den Knoten gehostete Intercluster-LIF wird mit dem `network interface show` Befehl und dem `-service-policy` Parameter identifiziert.

   ```
   network interface show -service-policy default-intercluster
   ```

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

2. Die auf den Knoten gehostete Management-LIF wird mit dem `network interface show` Befehl und dem `-service-policy` Parameter identifiziert.

   ```
   network interface show -service-policy default-management
   ```

3. Stellen Sie sicher, dass der Intercluster-LIF den `backup-ndmp-control` Dienst enthält:

   ```
   network interface service-policy show
   ```

   Weitere Informationen zu `network interface service-policy show` finden sich in der "ONTAP-Befehlsreferenz".

4. Stellen Sie sicher, dass die Failover-Richtlinie für alle LIFs entsprechend festgelegt ist:

   a. Es sollte überprüft werden, ob die Failover-Richtlinie für die Cluster-Management-LIF auf `broadcast-domain-wide` gesetzt ist und die Richtlinie für die Intercluster- sowie Node-Management-LIFs auf `local-only` gesetzt ist, indem der `network interface show -failover` Befehl verwendet wird.

      Der folgende Befehl zeigt die Failover-Richtlinie für die Cluster-Management-, Intercluster- und Node-Management-LIFs an:

      ```
      cluster1::> network interface show -failover

                Logical          Home             Failover    Failover
      Vserver   Interface        Node:Port        Policy      Group
      ```

```
-------    --------------   --------------  ----------  --------
cluster    cluster1_clus1   cluster1-1:e0a  local-only  cluster
                                                        Failover
Targets:
                                                        .......
cluster1   cluster_mgmt     cluster1-1:e0m  broadcast-  Default
                                                domain-wide
                                                        Failover
Targets:
                                                        .......
           IC1              cluster1-1:e0a  local-only  Default
                                                        Failover
Targets:
           IC2              cluster1-1:e0b  local-only  Default
                                                        Failover
Targets:
                                                        .......
cluster1-1 c1-1_mgmt1       cluster1-1:e0m  local-only  Default
                                                        Failover
Targets:
                                                        ......
cluster1-2 c1-2_mgmt1       cluster1-2:e0m  local-only  Default
                                                        Failover
Targets:
                                                        ......
```

a. Falls die Failover-Richtlinien nicht ordnungsgemäß eingestellt sind, kann die Failover-Richtlinie mit dem `network interface modify` Befehl und dem `-failover-policy` Parameter geändert werden.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

5. Die für die Datenverbindung erforderlichen LIFs werden mit dem `vserver services ndmp modify` Befehl und dem `preferred-interface-role` Parameter angegeben.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Es sollte überprüft werden, ob die bevorzugte Schnittstellenrolle für den Cluster mit dem `vserver services ndmp show` Befehl festgelegt ist.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9 oder früher

Schritte

1. Die Intercluster-, Cluster-Management- und Node-Management-LIFs lassen sich mit dem `network interface show` Befehl und dem `-role` Parameter identifizieren.

   Der folgende Befehl zeigt die Intercluster-LIFs an:

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   Der folgende Befehl zeigt die Cluster-Management-LIF an:

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

   Der folgende Befehl zeigt die Node-Management-LIFs an:

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

2. Es muss sichergestellt sein, dass die Firewall-Richtlinie für NDMP auf den Intercluster-, Cluster-Management (`cluster-mgmt` und Node-Management (`node-mgmt` LIFs aktiviert ist:

   a. Es sollte überprüft werden, ob die Firewall-Richtlinie für NDMP mit dem `system services firewall policy show` Befehl aktiviert ist.

      Der folgende Befehl zeigt die Firewall-Richtlinie für die Cluster Management LIF an:

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                         ndmp       0.0.0.0/0
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

      Der folgende Befehl zeigt die Firewall-Richtlinie für die Intercluster LIF an:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
```

```
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

Der folgende Befehl zeigt die Firewall-Richtlinie für die Node Management-LIF an:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Falls die Firewall-Richtlinie nicht aktiviert ist, kann die Firewall-Richtlinie mit dem `system services firewall policy modify` Befehl mit dem `-service` Parameter aktiviert werden.

   Der folgende Befehl aktiviert die Firewall-Richtlinie für die Intercluster-LIF:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Stellen Sie sicher, dass die Failover-Richtlinie für alle LIFs entsprechend festgelegt ist:

   a. Es sollte überprüft werden, ob die Failover-Richtlinie für die Cluster-Management-LIF auf `broadcast-domain-wide` gesetzt ist und die Richtlinie für die Intercluster- sowie Node-Management-LIFs auf `local-only` gesetzt ist, indem der `network interface show -failover` Befehl verwendet wird.

Der folgende Befehl zeigt die Failover-Richtlinie für die Cluster-Management-, Intercluster- und Node-Management-LIFs an:

```
cluster1::> network interface show -failover

          Logical            Home               Failover
Failover
Vserver   Interface          Node:Port          Policy
Group
--------- -----------------  ------------------ --------------------
--------
cluster   cluster1_clus1     cluster1-1:e0a     local-only
cluster
                                                    Failover
Targets:
                                                    .......

cluster1  cluster_mgmt       cluster1-1:e0m     broadcast-domain-
wide Default
                                                    Failover
Targets:
                                                    .......
          IC1                 cluster1-1:e0a     local-only
Default
                                                    Failover
Targets:
          IC2                 cluster1-1:e0b     local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m     local-only
Default
                                                    Failover
Targets:
                                                    ......
cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m     local-only
Default
                                                    Failover
Targets:
                                                    ......
```

a. Falls die Failover-Richtlinien nicht ordnungsgemäß eingestellt sind, kann die Failover-Richtlinie mit dem `network interface modify` Befehl und dem `-failover-policy` Parameter geändert werden.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Die für die Datenverbindung erforderlichen LIFs werden mit dem `vserver services ndmp modify` Befehl und dem `preferred-interface-role` Parameter angegeben.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Es sollte überprüft werden, ob die bevorzugte Schnittstellenrolle für den Cluster mit dem `vserver services ndmp show` Befehl festgelegt ist.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                        NDMP Version: 4
                        .......
                        .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

Node-spezifisches NDMP konfigurieren

Knotenbezogenes NDMP auf dem ONTAP Cluster aktivieren

Sie können Volumes sichern, die auf einem einzelnen Knoten gehostet werden, indem Sie knotenbezogenes NDMP aktivieren, den NDMP-Service aktivieren und eine LIF für die Daten- und Steuerverbindung konfigurieren. Dies ist für alle Knoten des Clusters möglich.

Node-scoped NDMP ist in ONTAP 9 veraltet.

Über diese Aufgabe

Bei Verwendung von NDMP im Node-Scope-Modus muss die Authentifizierung pro Node konfiguriert werden. Weitere Informationen finden sich unter "Der Knowledge Base Artikel „How to configure NDMP authentication in the ‘node-scope’ mode“".

Schritte

1. Node-spezifischen NDMP-Modus aktivieren:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP Node-Scope-Mode ist aktiviert.

2. NDMP-Service auf allen Knoten im Cluster aktivieren:

   Die Verwendung des Platzhalters "*" aktiviert den NDMP-Service auf allen Knoten gleichzeitig.

   Sie müssen ein Passwort für die Authentifizierung der NDMP-Verbindung durch die Backup-Anwendung angeben.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Die `-clear-text` Option für die sichere Kommunikation des NDMP-Passworts deaktivieren:

   Die Wildcard-*" `disables the -clear-text` Option wird auf allen Knoten gleichzeitig verwendet.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Es sollte überprüft werden, dass der NDMP-Service aktiviert und die `-clear-text` Option deaktiviert ist:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

ONTAP LIFs für knotenbezogenes NDMP konfigurieren

Es ist erforderlich, eine LIF zu identifizieren, die für die Herstellung einer Datenverbindung und einer Steuerverbindung zwischen dem Node und der Backup-Anwendung verwendet wird. Nach der Identifizierung der LIF sollte überprüft werden, ob die Firewall- und Failover-Richtlinien für die LIF festgelegt sind.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien

ersetzt. Weitere Informationen finden sich unter "Unterstützten Datenverkehr verwalten".

ONTAP 9.10.1 oder höher

Schritte

1. Die auf den Knoten gehostete Intercluster-LIF wird mit dem `network interface show` Befehl und dem `-service-policy` Parameter identifiziert.

   ```
   network interface show -service-policy default-intercluster
   ```

2. Stellen Sie sicher, dass der Intercluster-LIF den `backup-ndmp-control` Dienst enthält:

   ```
   network interface service-policy show
   ```

3. Stellen Sie sicher, dass die Failover-Richtlinie für die Intercluster-LIFs entsprechend konfiguriert ist:

   a. Es sollte überprüft werden, ob die Failover-Richtlinie für die Intercluster-LIFs auf `local-only` gesetzt ist, indem der `network interface show -failover` Befehl verwendet wird.

   ```
   cluster1::> network interface show -failover
               Logical          Home               Failover
   Failover
   Vserver     Interface        Node:Port          Policy       Group
   --------    ---------------  -----------------  ------------
   --------
   cluster1    IC1               cluster1-1:e0a    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
               IC2               cluster1-2:e0b    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   ```

   b. Wenn die Failover-Richtlinie nicht ordnungsgemäß eingestellt ist, kann die Failover-Richtlinie mit dem `network interface modify` Befehl und dem `-failover-policy` Parameter geändert werden.

   ```
   cluster1::> network interface modify -vserver cluster1 -lif IC1
   ```

```
-failover-policy local-only
```

Weitere Informationen zu `network interface show`, `network interface service-policy show` und `network interface modify` in der "ONTAP-Befehlsreferenz".

ONTAP 9.9 oder früher

Schritte

1. Die auf den Knoten gehostete Intercluster-LIF wird mit dem `network interface show` Befehl und dem `-role` Parameter identifiziert.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. Stellen Sie sicher, dass die Firewall-Richtlinie für NDMP auf den Intercluster-LIFs aktiviert ist:

   a. Es sollte überprüft werden, ob die Firewall-Richtlinie für NDMP mit dem `system services firewall policy show` Befehl aktiviert ist.

   Der folgende Befehl zeigt die Firewall-Richtlinie für die Intercluster LIF an:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

b. Falls die Firewall-Richtlinie nicht aktiviert ist, kann die Firewall-Richtlinie mit dem `system services firewall policy modify` Befehl mit dem `-service` Parameter aktiviert werden.

   Der folgende Befehl aktiviert die Firewall-Richtlinie für die Intercluster-LIF:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Stellen Sie sicher, dass die Failover-Richtlinie für die Intercluster-LIFs entsprechend konfiguriert ist:

   a. Es sollte überprüft werden, ob die Failover-Richtlinie für die Intercluster-LIFs auf `local-only` gesetzt ist, indem der `network interface show -failover` Befehl verwendet wird.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. Wenn die Failover-Richtlinie nicht ordnungsgemäß eingestellt ist, kann die Failover-Richtlinie mit dem `network interface modify` Befehl und dem `-failover-policy` Parameter geändert werden.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Weitere Informationen zu `network interface show` und `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

Backup-Anwendungen für ONTAP NDMP Konfiguration konfigurieren

Nachdem der Cluster für den NDMP-Zugriff konfiguriert ist, sind Informationen aus der Clusterkonfiguration zu erfassen und anschließend der restliche Sicherungsprozess in der Sicherungsanwendung zu konfigurieren.

Schritte

1. Die folgenden Informationen, die zuvor in ONTAP konfiguriert wurden, sind bereitzuhalten:
   - Benutzername und Kennwort, die die Sicherungsanwendung zum Herstellen der NDMP-Verbindung benötigt
   - Die IP-Adressen der Intercluster-LIFs, die die Backup-Anwendung benötigt, um eine Verbindung zum Cluster herzustellen
2. In ONTAP werden die Aliase, die ONTAP jedem Gerät zugewiesen hat, mit dem `storage tape alias show` Befehl angezeigt.

   Die Aliase sind oft nützlich bei der Konfiguration der Backup-Anwendung.

   ```
   cluster1::> storage tape show -alias

     Device ID: 2a.0
   Device Type: tape drive
   Description: Hewlett-Packard LTO-5

   Node                         Alias     Mapping
   ---------------------------- --------- ------------------------------
   stsw-3220-4a-4b-02           st2       SN[HU19497WVR]
   ...
   ```

3. Der restliche Sicherungsvorgang wird in der Backup-Anwendung mithilfe der Dokumentation der Backup-Anwendung konfiguriert.

Nachdem Sie fertig sind

Wenn ein Datenmobilitätsereignis wie eine Volume-Verschiebung oder LIF-Migration auftritt, sollte darauf geachtet werden, dass alle unterbrochenen Backup-Vorgänge erneut initialisiert werden können.

Verwandte Informationen

- "storage tape Alias anzeigen"

Informationen zur Replikation zwischen NetApp Element software und ONTAP

Die Geschäftskontinuität auf einem Element System kann sichergestellt werden, indem SnapMirror verwendet wird, um Snapshots eines Element Volumes auf ein ONTAP Ziel zu replizieren. Bei einem Ausfall am Element Standort können Daten vom ONTAP System an Clients bereitgestellt und das Element System nach Wiederherstellung des Dienstes wieder aktiviert werden.

Ab ONTAP 9.4 können Snapshots einer auf einem ONTAP Knoten erstellten LUN auf ein Element System repliziert werden. Eine LUN könnte während eines Ausfalls am Element Standort erstellt worden sein, oder eine LUN wird zur Migration von Daten von ONTAP zu Element Software verwendet.

"Konfiguration der Replikation von NetApp Element Software und ONTAP".

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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