Datensicherung und Disaster Recovery

ONTAP 9

NetApp
February 03, 2026

Inhalt

Datensicherung und Disaster Recovery

Cluster- und SVM-Peering

Weitere Informationen zu ONTAP Cluster und SVM Peering

Sie können Peer-Beziehungen zwischen Quell- und Ziel-Clustern und zwischen Quell- und Ziel-Storage Virtual Machines (SVMs) erstellen. Sie müssen Peer-Beziehungen zwischen diesen Einheiten erstellen, bevor Sie Snapshots mit SnapMirror replizieren können.

ONTAP 9.3 bietet Verbesserungen, die die Konfiguration von Peer-Beziehungen zwischen Clustern und SVMs vereinfachen. Die Peering-Verfahren für Cluster und SVMs sind für alle ONTAP 9-Versionen verfügbar. Sie sollten das entsprechende Verfahren für Ihre ONTAP-Version verwenden.

Die entsprechenden Verfahren werden über die Befehlszeilenschnittstelle (CLI) und nicht mit System Manager oder einem automatisierten Scripting-Tool ausgeführt.

Cluster- und SVM-Peering werden vorbereitet

Grundlagen zu ONTAP Peering

Bevor Sie Snapshots mithilfe von SnapMirror replizieren können, müssen Sie „Peer-Beziehungen“_ zwischen Quell- und Ziel-Clustern sowie zwischen Quell- und Ziel-SVMs erstellen. Eine Peer-Beziehung definiert Netzwerkverbindungen, mit denen Cluster und SVMs einen sicheren Datenaustausch ermöglichen.

Cluster und SVMs in Peer-Beziehungen kommunizieren über das Cluster-Netzwerk mithilfe von logischen Schnittstellen (LIFs) zwischen Clustern._ eine Intercluster LIF ist eine LIF, die den „Intercluster-Core“-Netzwerkschnittstellungsservice unterstützt und normalerweise mithilfe der Service-Richtlinie zur Netzwerkschnittstelle „default-intercluster“ erstellt wird. Sie müssen für jeden Node in den Clustern, die Peering durchführen, Intercluster-LIFs erstellen.

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

Fan-out- und Kaskadentopologien werden unterstützt. In einer Kaskadentopologie müssen lediglich Cluster-Netzwerke zwischen den primären und sekundären Clustern sowie zwischen den sekundären und tertiären Clustern erstellt werden. Sie müssen kein Cluster-Netzwerk zwischen dem primären und dem tertiären Cluster erstellen.

Ein Administrator kann den Intercluster-Core-Service aus der Standard-Intercluster-Service-Richtlinie entfernen (aber nicht ratsam). Wenn dies der Fall ist, sind LIFs, die mit „default-intercluster“ erstellt wurden, tatsächlich keine Intercluster-LIFs. Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die Cluster-Standard-Service-Richtlinie den Intercluster-Core-Service enthält:

```
network interface service-policy show -policy default-intercluster
```

Erfahren Sie mehr über `network interface service-policy show` in der "ONTAP-Befehlsreferenz".

Voraussetzungen für ONTAP Peering

Bevor Sie Cluster-Peering einrichten, sollten Sie bestätigen, dass Konnektivität, Port, IP-Adresse, Subnetz, Firewall, Und die Anforderungen für die Cluster-Benennung erfüllen.

Ab ONTAP 9.6 bietet Cluster Peering standardmäßig Unterstützung für die TLS 1.2 AES-256 GCM-Verschlüsselung für die Datenreplizierung. Die Standard-Sicherheitskiffren („PSK-AES256-GCM-SHA364“) sind erforderlich, damit Cluster Peering auch dann funktioniert, wenn die Verschlüsselung deaktiviert ist.

Ab ONTAP 9.11.1 sind die DHE-PSK-Sicherheitsschlüssel standardmäßig verfügbar.

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

Konnektivitätsanforderungen erfüllen

Jede Intercluster LIF auf dem lokalen Cluster muss in der Lage sein, mit jeder Intercluster LIF auf dem Remote-Cluster zu kommunizieren.

Es ist zwar nicht erforderlich, aber in der Regel ist es einfacher, die IP-Adressen zu konfigurieren, die für Intercluster LIFs im selben Subnetz verwendet werden. Die IP-Adressen können sich im gleichen Subnetz wie 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 Kommunikation zwischen Clustern verwendet werden.
- Das Subnetz muss über genügend IP-Adressen verfügen, um einer Intercluster LIF pro Node zuzuweisen.

  Beispielsweise muss in einem Cluster mit vier Nodes das für die Kommunikation zwischen Clustern verwendete Subnetz vier verfügbare IP-Adressen haben.

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

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

Mit ONTAP können Sie Ihre Peering-Netzwerke von IPv4 zu IPv6 migrieren, da Sie optional beide Protokolle gleichzeitig auf den Intercluster LIFs anwesend sein können. In früheren Versionen waren alle Cluster-Beziehungen für einen gesamten Cluster entweder IPv4 oder IPv6. Somit war eine Änderung der Protokolle ein potenziell störendes Ereignis.

Port-Anforderungen

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Ports müssen folgende Anforderungen erfüllen:

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

  Sie können mehrere IPspaces verwenden, um mit mehreren Clustern zu Punkten. Paarweise ist Vollmaschenverbindung nur innerhalb eines IPspaces erforderlich.

- Die Broadcast-Domäne, die für die Intercluster-Kommunikation verwendet wird, muss mindestens zwei Ports pro Node enthalten, damit die Intercluster-Kommunikation von einem Port zu einem anderen Port ausfallen kann.

  Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Interface Groups (iffrps) sein.

- Alle Ports müssen verkabelt sein.
- Alle Ports müssen sich in einem ordnungsgemäßen Zustand befinden.
- Die MTU-Einstellungen der Ports müssen konsistent sein.

Anforderungen an die Firewall

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

Firewalls und die Cluster-übergreifende Firewall-Richtlinie müssen folgende Protokolle zulassen:

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

  Obwohl HTTPS nicht erforderlich ist, wenn Sie Cluster-Peering über die CLI einrichten, wird später HTTPS erforderlich, wenn Sie den Datenschutz mit System Manager konfigurieren.

Die Standard- `intercluster`Firewallrichtlinie ermöglicht den Zugriff über das HTTPS-Protokoll und von allen IP-Adressen (0.0.0.0/0). Sie können die Richtlinie bei Bedarf ändern oder ersetzen.

Cluster-Anforderungen erfüllen

Cluster müssen die folgenden Anforderungen erfüllen:

- Ein Cluster kann nicht in einer Peer-Beziehung mit mehr als 255 Clustern sein.

Verwenden Sie gemeinsam genutzte oder dedizierte ONTAP-Ports

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Bei der Entscheidung, ob Ports gemeinsam genutzt werden sollen, müssen Sie die Netzwerkbandbreite, das

Replikationsintervall und die Portverfügbarkeit berücksichtigen.

Sie können Ports für einen Peering Cluster gemeinsam nutzen, während Sie auf dem anderen dedizierte Ports verwenden.

Netzwerkbandbreite

Wenn Sie ein High-Speed-Netzwerk wie 10 GbE haben, verfügen Sie möglicherweise über ausreichend lokale LAN-Bandbreite, um eine Replikation mit denselben 10 GbE-Ports durchzuführen, die für den Datenzugriff verwendet werden.

Selbst dann sollten Sie Ihre verfügbare WAN-Bandbreite mit Ihrer LAN-Bandbreite vergleichen. Wenn die verfügbare WAN-Bandbreite deutlich weniger als 10 GbE beträgt, müssen Sie möglicherweise dedizierte Ports verwenden.

Eine Ausnahme von dieser Regel besteht unter Umständen darin, dass alle oder viele Nodes im Cluster Daten replizieren. In diesem Fall wird die Bandbreitenauslastung normalerweise über verschiedene Nodes verteilt.

Wenn Sie keine dedizierten Ports verwenden, sollte die MTU-Größe (Maximum Transmission Unit) des Replikationsnetzwerks in der Regel mit der MTU-Größe des Datennetzwerks übereinstimmen.

Replikationsintervall

Wenn die Replizierung in Zeiten geringerer Auslastung stattfindet, sollten Sie in der Lage sein, Daten-Ports für die Replizierung zu nutzen, auch ohne eine 10-GbE-LAN-Verbindung.

Wenn die Replizierung während der normalen Geschäftszeiten stattfindet, müssen Sie die Menge der zu replizierenden Daten berücksichtigen und entscheiden, ob es so viel Bandbreite erfordert, dass es Konflikte mit den Datenprotokolle verursachen kann. Wenn die Netzwerkauslastung durch Datenprotokolle (SMB, NFS, iSCSI) über 50 % liegt, sollten dedizierte Ports für die Kommunikation zwischen Clustern verwendet werden. Damit wird bei einem Node-Failover die Performance nicht beeinträchtigt.

Port-Verfügbarkeit

Wenn Sie feststellen, dass der Replizierungsverkehr den Datenverkehr beeinträchtigt, können Sie LIFs zwischen Clustern auf jeden anderen Cluster-fähigen, gemeinsam genutzten Port desselben Nodes migrieren.

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

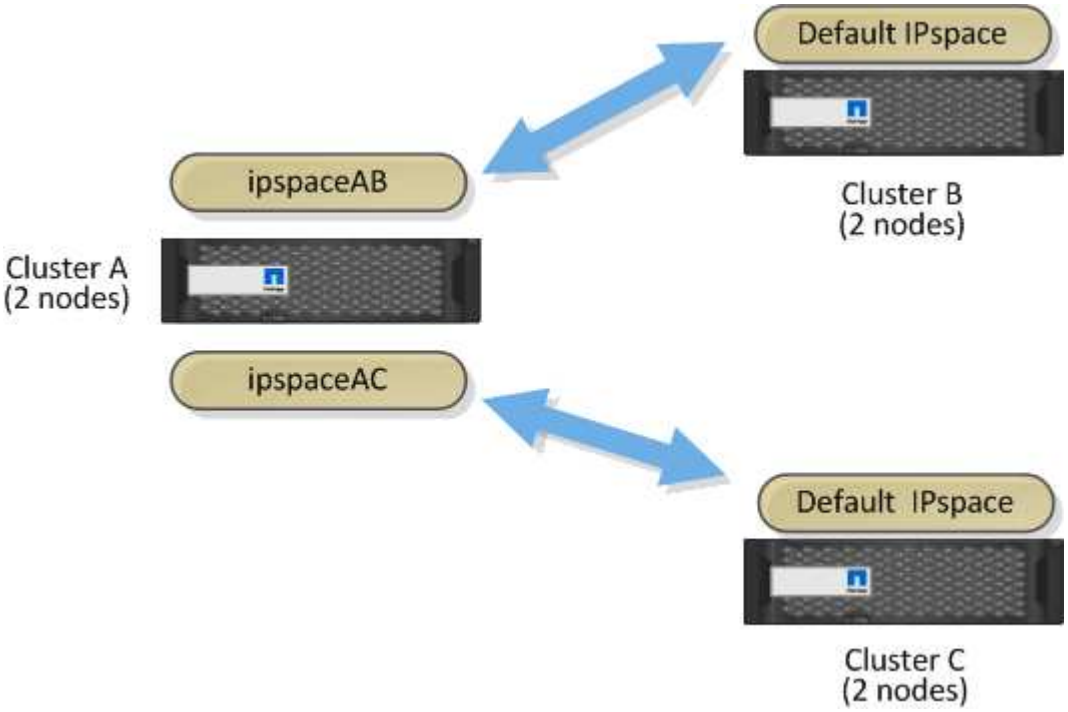
Verwenden Sie benutzerdefinierte ONTAP IPspaces, um den Replikationsdatenverkehr zu isolieren

Sie können benutzerdefinierte IPspaces verwenden, um die Interaktionen eines Clusters mit seinen Peers voneinander zu trennen. Diese Konfiguration, die als *designierte Intercluster-Konnektivität* bezeichnet wird, ermöglicht Service-Providern die Isolierung des Replizierungsdatenverkehrs in mandantenfähigen Umgebungen.

Angenommen, Sie möchten beispielsweise, dass der Replikationsverkehr zwischen Cluster A und Cluster B vom Replikationsverkehr zwischen Cluster A und Cluster C getrennt wird. Um dies zu erreichen, können Sie zwei IPspaces auf Cluster A erstellen

Ein IPspace enthält die Intercluster LIFs, die Sie für die Verbindung mit Cluster B verwenden. Der andere

enthält die Intercluster LIFs, die Sie für die Kommunikation mit Cluster C verwenden, wie in der folgenden Abbildung dargestellt.



Verwandte Informationen

- "Erfahren Sie mehr über die Konfiguration des ONTAP IP-Speicherplatzes"

Konfigurieren Sie Intercluster LIFs

Konfigurieren Sie ONTAP Intercluster LIFs an gemeinsam genutzten Daten-Ports

Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Netzwerkports 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 Sie entweder auf einer Administrator-SVM (Standard-IPspace) oder einer System-SVM (Custom IPspace) erstellen:

Option	Beschreibung
Im 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`*

Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel werden Intercluster LIFs `cluster01_icl01` und erstellt `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. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

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

Erfahren Sie mehr über `network interface show` 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. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
Im 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`

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel wird gezeigt, dass Intercluster LIFs `cluster01_icl01` und `cluster01_icl02` auf dem `e0c` Port `e0d` ein Failover zum Port ausführen.

```
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
```

Konfigurieren Sie ONTAP Intercluster LIFs an dedizierten Ports

Sie können Intercluster-LIFs auf dedizierten Ports konfigurieren. Dadurch wird typischerweise die verfügbare Bandbreite für den Replizierungsverkehr erhöht.

Schritte

1. Liste der Ports im Cluster:

   `network port show`

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Netzwerkports 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. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

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

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

   Im folgenden Beispiel werden Ports `e0e` und `e0f` keine LIFs zugewiesen:

```
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. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

`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 zu `cluster01`:

```
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. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

   `network interface failover-groups show`

   Erfahren Sie mehr über `network interface failover-groups show` 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. Erstellen Sie Intercluster-LIFs auf der System-SVM und weisen Sie sie der Failover-Gruppe zu.

Option	Beschreibung
Im 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`

Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel werden Intercluster LIFs `cluster01_icl01` und `cluster01_icl02` in der Failover-Gruppe erstellt `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. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

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

Erfahren Sie mehr über `network interface show` 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. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
Im 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`

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel zeigt, dass Intercluster LIFs `cluster01_icl01` und `cluster01_icl02` auf dem SVM-`e0e`Port `e0f` ein Failover zum Port durchgeführt werden.

```
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
```

Konfigurieren Sie ONTAP Intercluster LIFs in benutzerdefinierten IPspaces

Sie können Intercluster-LIFs in benutzerdefinierten IPspaces konfigurieren. Auf diese Weise lässt sich der Replizierungs-Datenverkehr in mandantenfähigen Umgebungen isolieren.

Wenn Sie einen benutzerdefinierten IPspace erstellen, erstellt das System eine Storage Virtual Machine (SVM) des Systems, die als Container für die Systemobjekte in diesem IPspace dient. Sie können die neue SVM als Container für alle Intercluster LIFs im neuen IPspace verwenden. Die neue SVM hat den gleichen Namen wie der benutzerdefinierte IPspace.

Schritte

1. Liste der Ports im Cluster:

   `network port show`

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Netzwerkports 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. Erstellen Sie benutzerdefinierte IPspaces auf dem Cluster:

   `network ipspace create -ipspace` *`ipspace`*

   Im folgenden Beispiel wird der benutzerdefinierte IPspace erstellt `ipspace-IC1`:

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

Erfahren Sie mehr über `network ipspace create` in der "ONTAP-Befehlsreferenz".

3. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

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

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

   Im folgenden Beispiel werden Ports `e0e` und `e0f` keine LIFs zugewiesen:

```
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. Entfernen Sie die verfügbaren Ports aus der Standard-Broadcast-Domäne:

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

   Ein Port darf nicht mehrere Broadcast-Domänen gleichzeitig haben. Erfahren Sie mehr über `network port broadcast-domain remove-ports` in der "ONTAP-Befehlsreferenz".

   Im folgenden Beispiel werden Ports `e0e` und `e0f` aus der standardmäßigen Broadcast-Domäne entfernt:

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

5. Vergewissern Sie sich, dass die Ports aus der Standard-Broadcast-Domäne entfernt wurden:

   `network port show`

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel wird gezeigt, dass Ports `e0e` und `e0f` aus der standardmäßigen 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. Erstellen Sie eine Broadcast-Domäne im benutzerdefinierten IPspace:

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

   Im folgenden Beispiel wird die Broadcast-Domain `ipspace-IC1-bd` im IPspace erstellt `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. Vergewissern Sie sich, dass die Broadcast-Domäne erstellt wurde:

   `network port broadcast-domain show`

   Erfahren Sie mehr über `network port broadcast-domain show` 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. Erstellen von Intercluster-LIFs auf der System-SVM, und weisen Sie sie der Broadcast-Domäne zu:

Option	Beschreibung
Im 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 besitzt eine Standard-Failover-Gruppe mit demselben Namen wie die Broadcast-Domäne. Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel werden Intercluster LIFs `cluster01_icl01` und `cluster01_icl02` in der Broadcast-Domäne erstellt `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. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

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

Erfahren Sie mehr über `network interface show` 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. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Option	Beschreibung
Im 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`

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel wird gezeigt, dass Intercluster LIFs `cluster01_icl01` und `cluster01_icl02` auf dem SVM- `e0e`Port ein Failover zum Port`e0f`ausführen:

```
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
```

Konfiguration von Peer-Beziehungen

Erstellung von ONTAP Cluster Peer-Beziehungen

Bevor Sie Ihre Daten schützen können, indem Sie sie zu Zwecken der Datensicherung und Disaster Recovery auf ein Remote-Cluster replizieren, sollten Sie eine Cluster-Peer-Beziehung zwischen dem lokalen und dem Remote-Cluster erstellen.

Über diese Aufgabe

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um eine Snapshot-Replikation einzurichten. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Es stehen verschiedene Standardschutzrichtlinien zur Verfügung. Sie müssen Ihre Schutzrichtlinien erstellt haben, wenn Sie benutzerdefinierte Richtlinien verwenden möchten.

Bevor Sie beginnen

Wenn Sie die ONTAP-CLI verwenden, müssen Sie auf jedem Node in den Clustern, auf denen die Daten

gespeichert werden, mithilfe einer der folgenden Methoden Intercluster LIFs erstellt haben:

- "Konfigurieren Sie Intercluster-LIFs an gemeinsam genutzten Datenports"
- "Konfigurieren Sie Intercluster LIFs an dedizierten Daten-Ports"
- "Konfigurieren Sie Intercluster LIFs in benutzerdefinierten IPspaces"

Schritte

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

System Manager

1. Klicken Sie im lokalen Cluster auf **Cluster > Einstellungen**.
2. Klicken Sie im Abschnitt **Intercluster-Einstellungen** auf **Netzwerkschnittstellen hinzufügen** und geben Sie die IP-Adresse und Subnetzmaske ein, um dem Cluster Intercluster-Netzwerkschnittstellen hinzuzufügen.

   Wiederholen Sie diesen Schritt auf dem Remote-Cluster.
3. Klicken Sie im Remote-Cluster auf **Cluster > Einstellungen**.
4. Klicken Sie ⋮ in den Abschnitt **Cluster Peers** und wählen Sie **Passphrase generieren** aus.
5. Wählen Sie die Remote-ONTAP-Cluster-Version aus.
6. Generierte Passphrase kopieren.
7. Klicken Sie im lokalen Cluster unter **Cluster Peers** auf ⋮ und wählen Sie **Peer Cluster** aus.
8. Fügen Sie im Fenster **Peer Cluster** die Passphrase ein und klicken Sie auf **Cluster-Peering initiieren**.

CLI

1. Erstellen Sie auf dem Ziel-Cluster eine Peer-Beziehung mit dem Quell-Cluster:

   ```
   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` und angeben `-peer-addrs`, `-peer-addrs` kann nur der Cluster, dessen Intercluster-LIFs in angegeben sind, das generierte Passwort verwenden.

   Sie können die `-ipspace` Option ignorieren, wenn Sie keinen benutzerdefinierten IPspace verwenden. Erfahren Sie mehr über `cluster peer create` in der "ONTAP-Befehlsreferenz".

   Wenn Sie die Peering-Beziehung in ONTAP 9.6 oder höher erstellen und keine Cluster-übergreifende Peering-Kommunikation verschlüsseln möchten, müssen Sie die `-encryption-protocol -proposed none` Option verwenden, um die Verschlüsselung zu deaktivieren.

   Im folgenden Beispiel wird eine Cluster-Peer-Beziehung zu einem nicht angegebenen Remote-Cluster erstellt und Peer-Beziehungen zu SVMs `vs1` und `vs2` dem lokalen Cluster vorab autorisiert:

```
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.
```

Im folgenden Beispiel wird eine Cluster-Peer-Beziehung zum Remote-Cluster unter LIF IP-Adressen 192.140.112.103 und 192.140.112.104 erstellt und eine Peer-Beziehung mit jeder SVM auf dem lokalen Cluster vorab autorisiert:

```
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.
```

Im folgenden Beispiel wird eine Cluster-Peer-Beziehung zu einem nicht angegebenen Remote-Cluster erstellt und Peer-Beziehungen zu SVMs`vs1` und `vs2` dem lokalen Cluster vorab autorisiert:

```
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. Authentifizierung des Quellclusters auf dem Quellcluster beim Ziel-Cluster:

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

Erfahren Sie mehr über `cluster peer create` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel wird der lokale Cluster an den Remote-Cluster unter LIF-IP-Adressen 192.140.112.101 und 192.140.112.102 authentifiziert:

```
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. Vergewissern Sie sich, dass 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. Prüfen Sie die Konnektivität und den Status der Knoten in der Peer-Beziehung:

```
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

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Überblick über die Vorbereitung der Volume Disaster Recovery"

ONTAP Intercluster SVM-Peer-Beziehungen erstellen

Mit dem `vserver peer create` Befehl können Sie eine Peer-Beziehung zwischen SVMs auf lokalen und Remote-Clustern erstellen.

Bevor Sie beginnen

- Die Quell- und Ziel-Cluster müssen Peering durchgeführt werden.
- Es müssen „vorab autorisierte“ Peer-Beziehungen für die SVMs auf dem Remote-Cluster vorhanden sein.

Weitere Informationen finden Sie unter "Erstellen 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, wenn Sie eine Cluster-Peer-Beziehung erstellen. Weitere Informationen finden Sie unter "Erstellen einer Cluster-Peer-Beziehung".

Schritte

1. Zeigen Sie im Zielcluster zur Datensicherung die SVMs an, die für Peering vorab autorisiert sind:

   `vserver peer permission show`

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

2. Erstellen Sie im Quell-Cluster für die Datensicherung eine Peer-Beziehung zu einer vorab autorisierten SVM auf dem Ziel-Cluster für die Datensicherung:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Erfahren Sie mehr über `vserver peer create` 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-vserver vs1
   ```

3. Überprüfung der SVM-Peer-Beziehung:

   `vserver peer show`

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

Fügen Sie ONTAP Intercluster SVM-Peer-Beziehungen hinzu

Wenn Sie nach der Konfiguration einer Cluster-Peer-Beziehung eine SVM erstellen, müssen Sie manuell eine Peer-Beziehung für die SVM hinzufügen. Sie können mit dem `vserver peer create` Befehl eine Peer-Beziehung zwischen SVMs erstellen. Nachdem die Peer-Beziehung erstellt wurde, können Sie `vserver peer accept` auf dem Remote-Cluster ausführen, um die Peer-Beziehung zu autorisieren.

Bevor Sie beginnen

Die Quell- und Ziel-Cluster müssen Peering durchgeführt werden.

Über diese Aufgabe

Sie können eine Peer-Beziehungen zwischen SVMs im selben Cluster für das lokale Daten-Backup erstellen. Erfahren Sie mehr über `vserver peer create` in der "ONTAP-Befehlsreferenz".

Administratoren verwenden gelegentlich den `vserver peer reject` Befehl, um eine vorgeschlagene SVM-Peer-Beziehung abzulehnen. Wenn die Beziehung zwischen SVMs im `rejected` Status ist, müssen Sie die Beziehung löschen, bevor Sie eine neue erstellen können. Erfahren Sie mehr über `vserver peer reject` in der "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen Sie für das Quell-Cluster für die Datensicherung eine Peer-Beziehung mit 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`

   Im folgenden Beispiel wird eine Peer-Beziehung zwischen der lokalen`pvs1` SVM und der Remote-SVM erstellt`vs1`

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

   Wenn die lokalen und Remote-SVMs dieselben Namen haben, müssen Sie zum Erstellen der SVM-Peer-Beziehung einen „*local Name*“ verwenden:

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

2. Vergewissern Sie sich beim Quell-Cluster für die Datensicherung, dass die Peer-Beziehung initiiert wurde:

   `vserver peer show-all`

   Erfahren Sie mehr über `vserver peer show-all` in der "ONTAP-Befehlsreferenz".

   Im folgenden Beispiel wird gezeigt, dass die Peer-Beziehung zwischen`pvs1` SVM 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. Zeigen Sie auf dem Ziel-Cluster für die Datensicherung die ausstehende SVM-Peer-Beziehung an:

   `vserver peer show`

   Erfahren Sie mehr über `vserver peer show` in der "ONTAP-Befehlsreferenz".

   Im folgenden Beispiel sind die ausstehenden Peer-Beziehungen für aufgeführt `cluster02`:

```
cluster02::> vserver peer show

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

4. Autorisieren Sie auf dem Ziel-Cluster zur Datensicherung die ausstehende Peer-Beziehung:

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

   Erfahren Sie mehr über `vserver peer accept` 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. Überprüfung der SVM-Peer-Beziehung:

   `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-Peering-Verschlüsselung auf Peer-Beziehungen aktivieren

Ab ONTAP 9.6 ist die Cluster-Peering-Verschlüsselung bei allen neu erstellten Cluster-Peering-Beziehungen standardmäßig aktiviert. Die Cluster-Peering-Verschlüsselung verwendet einen vorab gemeinsam genutzten Schlüssel (PSK) und die Transport Security Layer (TLS) zum sicheren clusterübergreifenden Peering von Kommunikation. Dadurch wird eine zusätzliche Sicherheitsschicht zwischen den Peering Clustern hinzugefügt.

Über diese Aufgabe

Wenn Sie Peering-Cluster auf ONTAP 9.6 oder höher aktualisieren und die Peering-Beziehung in ONTAP 9.5 oder früher erstellt wurde, muss die Cluster-Peering-Verschlüsselung nach dem Upgrade manuell aktiviert werden. Beide Cluster in der Peering-Beziehung müssen ONTAP 9.6 oder höher ausführen, um die Verschlüsselung von Cluster-Peering zu aktivieren.

Schritte

1. Aktivieren Sie auf dem Ziel-Cluster die Verschlüsselung für die Kommunikation mit dem Quell-Cluster:

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

2. Geben Sie bei Aufforderung eine Passphrase ein.
3. Aktivieren Sie auf dem Quell-Cluster für Datensicherung die Verschlüsselung zur Kommunikation mit dem Ziel-Cluster:

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

4. Geben Sie bei der entsprechenden Aufforderung dieselbe Passphrase ein, die im Ziel-Cluster eingegeben wurde.

Erfahren Sie mehr über `cluster peer modify` in der "ONTAP-Befehlsreferenz".

Entfernen Sie die ONTAP Cluster-Peering-Verschlüsselung aus Peer-Beziehungen

Die Cluster-Peering-Verschlüsselung wird standardmäßig für alle in ONTAP 9.6 oder höher erstellten Peer-Beziehungen aktiviert. Wenn Sie keine Verschlüsselung für Cluster-

übergreifende Peering-Kommunikation verwenden möchten, können Sie diese deaktivieren.

Schritte

1. Ändern Sie auf dem Zielcluster die Kommunikation mit dem Quellcluster, um die Verwendung der Cluster-Peering-Verschlüsselung einzustellen:
   - Geben Sie Folgendes ein, um die Verschlüsselung zu entfernen, aber die Authentifizierung beizubehalten:

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

   - So entfernen Sie Verschlüsselung und Authentifizierung:
     i. Ändern Sie die Cluster-Peering-Richtlinie, um nicht authentifizierten Zugriff zu ermöglichen:

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

     ii. Verschlüsselung und Authentifizierungszugriff ändern:

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

2. Wenn Sie dazu aufgefordert werden, geben Sie die Passphrase ein.
3. Bestätigen Sie die Passphrase, indem Sie sie erneut eingeben.
4. Deaktivieren Sie auf dem Quellcluster die Verschlüsselung für die Kommunikation mit dem Ziel-Cluster:
   - Geben Sie Folgendes ein, um die Verschlüsselung zu entfernen, aber die Authentifizierung beizubehalten:

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

   - So entfernen Sie Verschlüsselung und Authentifizierung:
     i. Ändern Sie die Cluster-Peering-Richtlinie, um nicht authentifizierten Zugriff zu ermöglichen:

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

     ii. Verschlüsselung und Authentifizierungszugriff ändern:

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

5. Wenn Sie dazu aufgefordert werden, geben Sie dieselbe Passphrase ein, die Sie auf dem Ziel-Cluster verwendet haben, und geben Sie sie erneut ein.

Verwalten von lokalen Snapshots

Erfahren Sie mehr über das Verwalten lokaler ONTAP-Snapshots

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

Mit einem Snapshot können Sie den gesamten Inhalt eines Volumes wiederherstellen oder einzelne Dateien oder LUNs wiederherstellen. Snapshots werden im Verzeichnis auf dem Volume gespeichert. `.snapshot`

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

Ab ONTAP 9.8 können FlexGroup Volumes 1023 Snapshots enthalten. Weitere Informationen finden Sie unter "Sichern Sie FlexGroup Volumes mit Snapshots".

Erfahren Sie mehr über ONTAP Snapshots zur Langzeitaufbewahrung

SnapMirror Beziehungen mit dem Richtlinientyp „Vault“ oder „Mirror-Vault“ ermöglichen die Erstellung von Snapshots direkt auf dem sekundären Volume der SnapMirror Beziehung. Diese Snapshots werden am Zielort als Backups aufbewahrt. Diese Momentaufnahmen werden häufig für die Langzeitarchivierung erstellt und werden als Langzeitarchivierungs-Momentaufnahmen bezeichnet.

Sie erstellen einen Snapshot zur langfristigen Aufbewahrung, indem Sie in der SnapMirror Richtlinienregel einen Zeitplan für die Snapshot-Erstellung, das SnapMirror-Namenspräfix, die SnapMirror -Bezeichnung und die Aufbewahrungsanzahl angeben. Dieser Snapshot wird auf dem SnapMirror Zielvolume unabhängig von den Aufbewahrungsregeln der Quelle aufbewahrt.

Langzeit-Snapshots sind nur für FlexVol SnapMirror Konfigurationen verfügbar. Für FlexGroup SnapMirror Konfigurationen können keine Langzeit-Snapshots erstellt werden.

In einer SnapMirror Kaskadenbeziehung können Snapshots zur langfristigen Aufbewahrung nur auf dem letzten Volume der Kaskade erstellt werden.

Verwandte Informationen

- "Erfahren Sie, wie kaskadierte Bereitstellungen funktionieren"
- "Definieren Sie einen ONTAP SnapMirror Zeitplan, um eine lokale Kopie auf dem Ziel zu erstellen"

Konfigurieren Sie benutzerdefinierte Snapshot-Richtlinien

Erfahren Sie mehr über das Konfigurieren von benutzerdefinierten ONTAP-Snapshot-Richtlinien

Eine *Snapshot-Richtlinie* definiert, wie das System Snapshots erstellt. Die Richtlinie gibt an, wann Snapshots erstellt werden sollen, wie viele Kopien aufbewahrt werden sollen und wie sie benannt werden sollen. Ein System kann beispielsweise jeden Tag um 12:10 Uhr einen Snapshot erstellen, die beiden neuesten Kopien beibehalten und die Kopien mit „`daily.`“ benennen.. *`timestamp`*

Die Standardrichtlinie für ein Volume erstellt automatisch Snapshots nach dem folgenden Zeitplan. Die ältesten Snapshots werden gelöscht, um Platz für neuere Kopien zu schaffen:

- Maximal sechs stündliche Snapshots wurden fünf Minuten nach der Stunde erstellt.
- Maximal zwei Snapshots täglich von Montag bis Samstag um 10 Minuten nach Mitternacht.
- Maximal zwei wöchentliche Schnappschüsse, die jeden Sonntag um 15 Minuten nach Mitternacht erstellt wurden.

Wenn Sie beim Erstellen eines Volumes keine Snapshot-Richtlinie angeben, übernimmt das Volume die Snapshot-Richtlinie, die mit der zugehörigen Storage Virtual Machine (SVM) verknüpft ist.

Wann eine benutzerdefinierte ONTAP-Snapshot-Richtlinie konfiguriert werden soll

Wenn die standardmäßige Snapshot-Richtlinie für ein Volume nicht geeignet ist, können Sie eine benutzerdefinierte Richtlinie konfigurieren, die die Häufigkeit, Aufbewahrung und den Namen von Snapshots ändert. Der Zeitplan hängt hauptsächlich von der Änderungsrate des aktiven Filesystems ab.

Sie können ein stark beanspruchten Dateisystem wie eine Datenbank stündlich sichern, während Sie selten verwendete Dateien einmal am Tag sichern. Selbst bei einer Datenbank führen Sie in der Regel ein oder zwei Mal am Tag ein vollständiges Backup aus. Gleichzeitig werden die Transaktions-Logs stündlich gesichert.

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

Erstellen Sie einen ONTAP Snapshot-Jobzeitplan

Eine Snapshot-Richtlinie erfordert mindestens einen Snapshot-Jobzeitplan. Sie können System Manager oder den `job schedule cron create` Befehl zum Erstellen eines Jobzeitplans verwenden. Erfahren Sie mehr über `job schedule cron create` in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um einen Snapshot-Jobplan zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Standardmäßig formt ONTAP die Namen von Snapshots, indem es einen Zeitstempel an den Namen des

Jobzeitplans anhängt.

Wenn Sie Werte sowohl für Tag des Monats als auch für Tag der Woche angeben, werden die Werte unabhängig betrachtet. Beispielsweise `Friday 13` wird ein Cron-Zeitplan mit der Spezifikation Tag und Tag des Monats jeden Freitag und am 13. Tag eines jeden Monats ausgeführt, nicht nur an jedem Freitag, dem 13..

Beispiel 1. Schritte

System Manager

1. Navigieren Sie zu **Schutz > Übersicht**, und erweitern Sie die Optionen **Lokale Richtlinieneinstellungen**.
2. Klicken Sie im Bereich **Zeitpläne** auf →.
3. Klicken Sie im Fenster **Zeitpläne** auf + Add .
4. Geben Sie im Fenster **Zeitplan hinzufügen** den Namen des Zeitplans ein und wählen Sie den Kontext und den Zeitplantyp aus.
5. Klicken Sie Auf **Speichern**.

CLI

1. Job-Zeitplan 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` können Sie festlegen `all`, dass der Job jeden Monat, Wochentag und jede Stunde ausgeführt werden soll.

Ab ONTAP 9.10.1 können Sie den Vserver für Ihren Job-Zeitplan angeben:

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

Im folgenden Beispiel wird ein Jobzeitplan mit dem Namen erstellt `myweekly`, der samstags um 3:00 Uhr ausgeführt wird:

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

Im folgenden Beispiel wird ein Zeitplan mit `myweeklymulti` dem Namen erstellt, 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 Sie eine ONTAP Snapshot-Richtlinie

Eine Snapshot-Richtlinie gibt an, wann Snapshots erstellt werden sollen, wie viele Kopien aufbewahrt werden sollen und wie sie benannt werden sollen. Beispielsweise kann ein System jeden Tag um 12:10 Uhr einen Snapshot erstellen, die beiden neuesten Kopien beibehalten und sie mit „`daily.`“ benennen.*`timestamp`*. Eine Snapshot-Richtlinie kann bis zu fünf Jobzeitpläne enthalten.

Über diese Aufgabe

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um eine Snapshot-Richtlinie zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Standardmäßig formt ONTAP die Namen der Snapshots, indem es einen Zeitstempel an den Namen des Jobzeitplans anhängt:

```
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/
```

Sie können ein Präfix für den Namen des Jobplans ersetzen, wenn Sie es bevorzugen.

Die `snapmirror-label` Option besteht für die SnapMirror-Replizierung. Weitere Informationen finden Sie unter "Definieren einer Regel für eine Richtlinie".

Schritte

Sie können eine Snapshot-Richtlinie mit 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 die Optionen **Lokale Richtlinieneinstellungen**.
2. Klicken Sie im Bereich **Snapshot Policies** auf →.
3. Klicken Sie auf der Registerkarte **Snapshot Policies** auf + Add .
4. Geben Sie im Fenster **Add Snapshot Policy** den Richtliniennamen ein und wählen Sie den Umfang aus.
5. Klicken Sie Auf + Add .
6. Um einen Zeitplan auszuwählen, klicken Sie auf den aktuell angezeigten Schichtplannamen, klicken Sie auf ⌄, und wählen Sie einen anderen Zeitplan aus.
7. Geben Sie die maximale Anzahl an zu haltenden Snapshots ein, und geben Sie bei Bedarf das SnapMirror-Label und den SnapLock-Aufbewahrungszeitraum ein.
8. Klicken Sie Auf **Speichern**.

CLI

1. Erstellen Sie eine 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>
```

Im folgenden Beispiel wird eine Snapshot-Richtlinie mit dem Namen erstellt `snap_policy_daily`, die auf einem Zeitplan ausgeführt `daily` wird. Die Policy hat maximal fünf Snapshots, jeder 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
```

Managen Sie Snapshots manuell

Erstellen und löschen Sie Snapshots manuell

Sie können Snapshots manuell erstellen, wenn Sie nicht darauf warten können, dass ein geplanter Snapshot erstellt wird, und Sie können Snapshots löschen, wenn sie nicht mehr benötigt werden.

Über diese Aufgabe

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90,

ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um einen On-Demand-Snapshot zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Erstellen Sie manuell einen Snapshot

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

System Manager

Schritte

1. Navigieren Sie zu **Speicher > Volumes** und wählen Sie die Registerkarte **Snapshots**.
2. Klicken Sie Auf + Add .
3. Akzeptieren Sie im Fenster **Add a Snapshot** den Standard-Snapshot-Namen oder bearbeiten Sie ihn, falls gewünscht.
4. **Optional**: Fügen Sie ein SnapMirror-Label hinzu.
5. Klicken Sie Auf **Hinzufügen**.

CLI

1. Erstellen eines Snapshots:

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

Löschen Sie Snapshots manuell

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

System Manager

Schritte

1. Navigieren Sie zu **Storage > Volumes** und wählen Sie die Registerkarte **Snapshot Copies** aus.
2. Suchen Sie den Snapshot, den Sie löschen möchten, klicken Sie auf ⋮, und wählen Sie **Löschen**.
3. Wählen Sie im Fenster **Snapshot löschen** die Option **Snapshot löschen**.
4. Klicken Sie Auf **Löschen**.

CLI

1. Überprüfen Sie mit dem `volume snapshot show` Befehl, welche Snapshots Sie löschen möchten.

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

In diesem Beispiel werden mit dem Befehl die Snapshots auf Volume vol3 in SVM vs3 angezeigt.

```
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. Snapshot löschen:

Ihr Ziel ist	Diesen Befehl eingeben…
Löschen Sie einen einzelnen Snapshot	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`

Ihr Ziel ist	Diesen Befehl eingeben…
Löschen Sie mehrere Snapshots	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
Löschen Sie alle Snapshots	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

Berechnen Sie vor dem Löschen von Snapshots den wieder zurückforderbaren Speicherplatz

Ab ONTAP 9.10.1 können Sie mit System Manager Snapshots auswählen, die Sie löschen möchten, und den zurückforderbaren Speicherplatz berechnen, bevor Sie sie löschen.

Schritte

1. Klicken Sie Auf **Storage > Volumes**.
2. Wählen Sie das Volume aus, aus dem Sie Snapshots löschen möchten.
3. Klicken Sie auf **Snapshots**.
4. Wählen Sie einen oder mehrere Snapshots aus.
5. Klicken Sie Auf **Speicherplatz Berechnen**.

Verwalten Sie die Snapshot-Reserve

Erfahren Sie mehr über das Management der ONTAP Snapshot Reserve

Die *Snapshot Reserve* legt einen Prozentsatz des Speicherplatzes für Snapshots beiseite, standardmäßig fünf Prozent. Da Snapshots Speicherplatz im aktiven Dateisystem verwenden, wenn die Snapshot-Reserve erschöpft ist, möchten Sie die Snapshot-Reserve gegebenenfalls erhöhen. Alternativ können Sie Snapshots auch automatisch löschen, wenn die Reserve voll ist.

Wann die Snapshot-Reserve erhöht werden soll

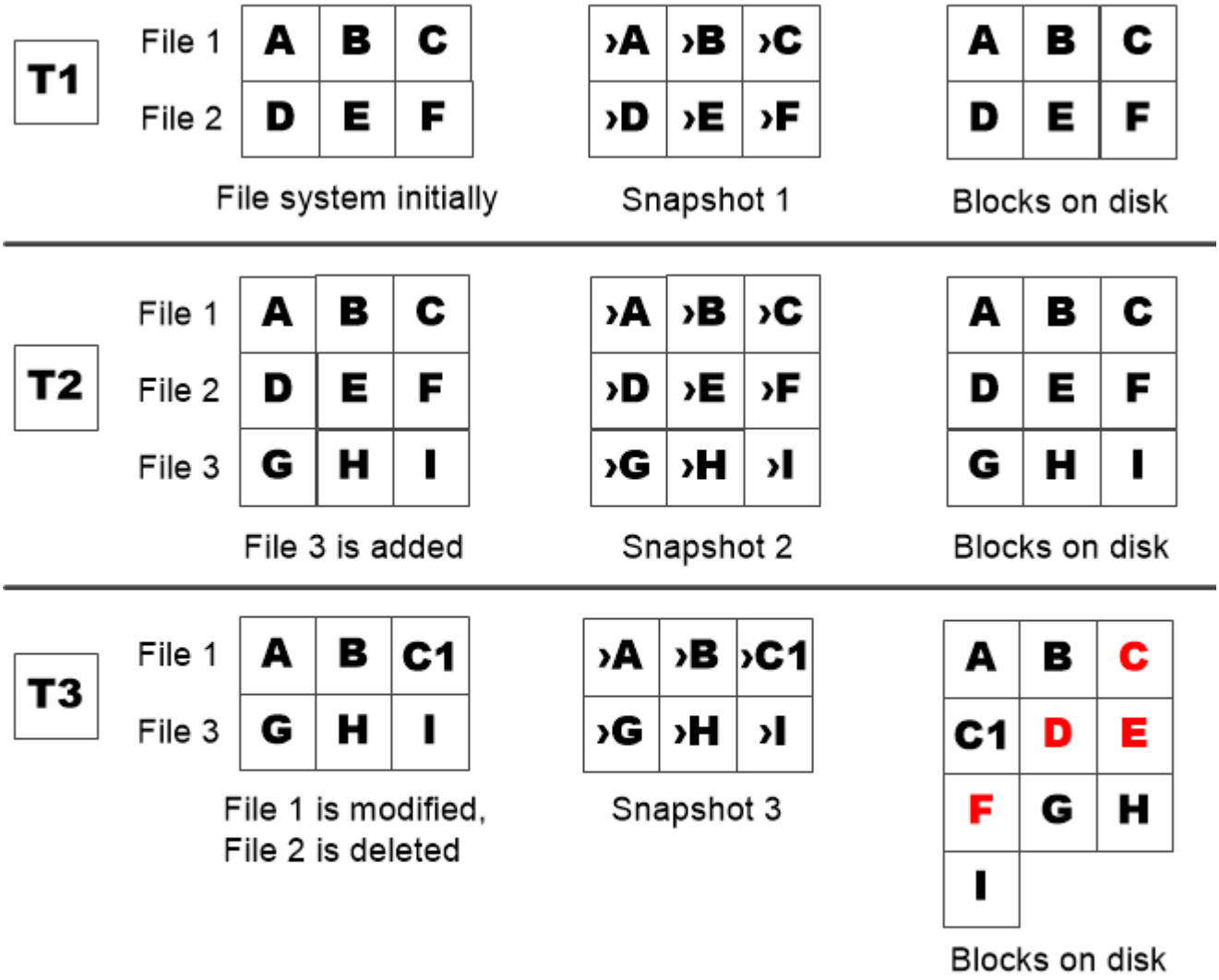
Bei der Entscheidung, ob die Snapshot-Reserve erhöht werden soll, ist zu beachten, dass ein Snapshot nur Änderungen an Dateien seit dem letzten Snapshot aufzeichnet. Sie verbraucht nur dann Speicherplatz, wenn Blöcke im aktiven File-System geändert oder gelöscht werden.

Das bedeutet, dass die Änderungsrate des Dateisystems der entscheidende Faktor bei der Bestimmung des Speicherplatzes ist, der von Snapshots verwendet wird. Unabhängig davon, wie viele Snapshots erstellt

werden, benötigen sie keinen Speicherplatz, wenn sich das aktive Dateisystem nicht geändert hat.

Bei einem FlexVol volume mit Datenbanktransaktionsprotokollen kann z. B. eine Snapshot-Reserve von bis zu 20 % zur Berücksichtigung der höheren Änderungsrate vorhanden sein. Sie möchten nicht nur mehr Snapshots erstellen, um die häufigeren Updates der Datenbank zu erfassen, sondern auch eine größere Snapshot-Reserve einsetzen, um den zusätzlichen Festplattenspeicher, den die Snapshots verbrauchen, zu bewältigen.

Ein Snapshot besteht aus Zeigern auf Blöcke statt aus Kopien von Blöcken. Man kann sich einen Zeiger als „Anspruch“ auf einen Block vorstellen: 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.

Das Löschen von geschützten Dateien kann zu weniger Dateispeicherplatz führen als erwartet

Ein Snapshot verweist auch nach dem Löschen der Datei, die den Block verwendet hat, auf einen Block. Dies erklärt, warum eine erschöpfte Snapshot-Reserve zu dem kontraintuitiven Ergebnis führen könnte, bei dem das Löschen eines gesamten Dateisystems zu weniger Speicherplatz führt als das Dateisystem belegt.

Betrachten wir das folgende Beispiel. Vor dem Löschen von Dateien `df` sieht die Befehlsausgabe wie folgt aus:

```
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 generiert 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 nun die gesamten 3 GB, die früher vom aktiven Dateisystem verwendet wurden, von Snapshots zusätzlich zu den 0.5 GB, die vor dem Löschen verwendet wurden, verwendet.

Da der von den Snapshots verwendete Speicherplatz nun die Snapshot-Reserve überschreitet, überläuft der 2.5 GB “spills” Speicherplatz in den für aktive Dateien reservierten Speicherplatz, so dass Sie mit 0.5 GB freiem Speicherplatz für Dateien, wo Sie vernünftigerweise 3 GB erwartet haben.

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Überwachen Sie den Festplattenverbrauch von ONTAP Snapshots

Sie können den Verbrauch von Snapshot-Festplatten mit dem Befehl überwachen `df`. Der Befehl zeigt den freien Speicherplatz im aktiven Dateisystem und die Snapshot-Reserve an.

Schritt

1. Snapshot-Festplattenverbrauch anzeigen: `df`

   Das folgende Beispiel zeigt den Verbrauch von Snapshot-Festplatten:

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

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Überprüfen Sie die verfügbare ONTAP Snapshot-Reserve auf einem Volume

Vielleicht möchten Sie überprüfen, wie viel Snapshot Reserve auf einem Volume verfügbar ist, indem Sie den Parameter mit dem `volume show` Befehl verwenden

`snapshot-reserve-available`. Erfahren Sie mehr über `volume show` in der "ONTAP-Befehlsreferenz".

Schritt

1. Prüfen Sie die auf einem Volume verfügbare Snapshot-Reserve:

   `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
```

Ändern Sie die ONTAP Snapshot Reserve

Möglicherweise möchten Sie eine größere Snapshot-Reserve konfigurieren, um zu verhindern, dass Snapshots den für das aktive Dateisystem reservierten Speicherplatz verwenden. Sie können die Snapshot-Reserve verringern, wenn Sie nicht mehr so viel Platz für Snapshots benötigen.

Schritt

1. Ändern Sie die Snapshot-Reserve:

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

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

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

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

Automatisches Löschen von ONTAP Snapshots

Sie können mit dem `volume snapshot autodelete modify` Befehl das automatische Löschen von Snapshots auslösen, wenn die Snapshot Reserve überschritten wird. Standardmäßig werden die ältesten Snapshots zuerst gelöscht. Erfahren Sie mehr über `volume snapshot autodelete modify` in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

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

Schritt

1. Snapshots automatisch löschen:

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

   Im folgenden Beispiel werden Snapshots automatisch gelöscht `vol1`, wenn die Snapshot-Reserve erschöpft ist:

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

Wiederherstellen von Dateien aus Snapshots

Stellen Sie eine Datei aus einem ONTAP-Snapshot auf einem NFS- oder SMB-Client wieder her

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

Jedes Verzeichnis im Dateisystem enthält ein Unterverzeichnis mit dem Namen `.snapshot`, auf das NFS- und SMB-Benutzer zugreifen können. 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/
```

Jedes Unterverzeichnis enthält die Dateien, auf die der Snapshot verweist. Wenn Benutzer versehentlich eine Datei löschen oder überschreiben, können sie die Datei in das übergeordnete Lese-/Schreibverzeichnis wiederherstellen, indem sie die Datei aus dem Snapshot-Unterverzeichnis in das Lese-/Schreibverzeichnis kopieren:

```
$ 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 Sie den NFS- und SMB-Client-Zugriff auf das ONTAP Snapshot-Verzeichnis

Sie können den Zugriff auf das Snapshot-Verzeichnis mithilfe der ONTAP-CLI-Option des `volume modify` Befehls aktivieren und deaktivieren `-snapdir-access`. Ab ONTAP 9.10.1 können Sie mit System Manager Client-Systeme für den Zugriff auf ein Snapshot-Verzeichnis auf einem Volume aktivieren oder deaktivieren. Durch die Aktivierung des Zugriffs wird das Snapshot-Verzeichnis für Clients sichtbar, und Windows-Clients können dem Snapshot-Verzeichnis ein Laufwerk zuordnen, 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 Sie die Volume-Einstellungen bearbeiten oder die Share-Einstellungen des Volumes bearbeiten.

Aktivieren oder deaktivieren Sie den Clientzugriff auf das Snapshot-Verzeichnis, indem Sie ein Volume bearbeiten

Schritte

Sie können den Zugriff auf das Snapshot-Verzeichnis des Clients 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. Klicken Sie Auf **Storage > Volumes**.
2. Wählen Sie das Volume aus, das das Snapshot-Verzeichnis enthält, das Sie ein- oder ausblenden möchten.
3. Klicken Sie auf ⋮ und wählen Sie **Bearbeiten**.
4. Aktivieren oder deaktivieren Sie im Abschnitt **Snapshot-Einstellungen (Lokal)** die Option **Clients das Snapshot-Verzeichnis anzeigen**.
5. Klicken Sie Auf **Speichern**.

CLI

1. Überprüfen Sie den Zugriffsstatus des Snapshot-Verzeichnisses:

   ```
   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
   ```

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

2. Aktivieren oder deaktivieren Sie den Zugriff auf das Snapshot-Verzeichnis:

   ```
   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.
   ```

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

Aktivieren oder deaktivieren Sie den Clientzugriff auf das Snapshot-Verzeichnis, indem Sie eine Freigabe bearbeiten

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

Schritte

1. Klicken Sie Auf **Storage > Shares**.
2. Wählen Sie das Volume aus, das das Snapshot-Verzeichnis enthält, das Sie ein- oder ausblenden möchten.
3. Klicken Sie auf ⋮ und wählen Sie **Bearbeiten**.
4. Wählen oder deaktivieren Sie im Abschnitt **Eigenschaften freigeben Clients erlauben, auf das Snapshot-Verzeichnis** zuzugreifen.
5. Klicken Sie Auf **Speichern**.

Stellen Sie eine einzelne Datei aus einem ONTAP-Snapshot wieder her

Mit dem Befehl können Sie `volume snapshot restore-file` eine einzelne Datei oder LUN aus einem Snapshot wiederherstellen. Sie können die Datei an einem anderen Speicherort im übergeordneten Datenträger mit Lese- und Schreibvorgängen wiederherstellen, wenn Sie eine vorhandene Datei nicht ersetzen möchten.

Über diese Aufgabe

Wenn Sie eine vorhandene LUN wiederherstellen, wird ein LUN-Klon erstellt und in Form eines Snapshots gesichert. Während des Wiederherstellungsvorgangs können Sie von lesen und auf die LUN schreiben.

Dateien mit Streams werden standardmäßig wiederhergestellt.

Schritte

1. Listen Sie die Snapshots in einem Volume auf:

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

   Erfahren Sie mehr über `volume snapshot show` in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Snapshots 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. Wiederherstellen einer Datei aus einem Snapshot:

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

Erfahren Sie mehr über `volume snapshot restore-file` in der "ONTAP-Befehlsreferenz".

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

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

Stellen Sie einen Teil einer Datei aus einem ONTAP-Snapshot wieder her

Mit dem Befehl können `volume snapshot partial-restore-file` Sie einen Datenbereich von einem Snapshot, einer LUN oder einer NFS- oder SMB-Containerdatei wiederherstellen, vorausgesetzt, Sie kennen den Startbyteoffset der Daten und die Byte-Anzahl. Mit diesem Befehl können Sie eine der Datenbanken auf einem Host wiederherstellen, der mehrere Datenbanken auf derselben LUN speichert.

Ab ONTAP 9.12.1 ist die partielle Wiederherstellung für Volumes mit verfügbarSnapMirror Active Sync.

Schritte

1. Listen Sie die Snapshots in einem Volume auf:

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

   Erfahren Sie mehr über `volume snapshot show` in der "ONTAP-Befehlsreferenz".

   Das folgende Beispiel zeigt die Snapshots 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. 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 Start-Byte-Offset und die Byte-Anzahl müssen ein Vielfaches von 4,096 sein.

Das folgende Beispiel stellt die ersten 4,096 Bytes der Datei wieder her `myfile.txt`:

```
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
```

Stellen Sie den Inhalt eines Volumes aus einem ONTAP-Snapshot wieder her

Sie können ein Volume zu einem früheren Zeitpunkt wiederherstellen, indem Sie es von einem Snapshot wiederherstellen. Sie können System Manager oder den Befehl verwenden `volume snapshot restore`, um den Inhalt eines Volumes aus einem Snapshot wiederherzustellen. Erfahren Sie mehr über `volume snapshot restore` in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Wenn das Volume über SnapMirror-Beziehungen verfügt, replizieren Sie alle gespiegelten Kopien des Volumes sofort nach der Wiederherstellung von einem Snapshot manuell. Dadurch können nicht nutzbare Spiegelkopien erstellt werden, die gelöscht und neu erstellt werden müssen.

Schritte

Sie können System Manager oder die ONTAP CLI zur Wiederherstellung aus einem früheren Snapshot verwenden.

System Manager

1. Klicken Sie auf **Storage** und wählen Sie ein Volume aus.
2. Klicken Sie unter **Snapshot-Kopien** neben dem Snapshot, den Sie wiederherstellen möchten, und wählen Sie **Wiederherstellen** aus.

CLI

1. Listen Sie die Snapshots in einem Volume auf:

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

Das folgende Beispiel zeigt den Snapshot 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. Wiederherstellen des Inhalts eines Volumes aus einem Snapshot:

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

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

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

SnapMirror Volume-Replizierung

Erfahren Sie mehr über die SnapMirror Volume-Replizierung

Erfahren Sie mehr über asynchrone Disaster Recovery von ONTAP SnapMirror

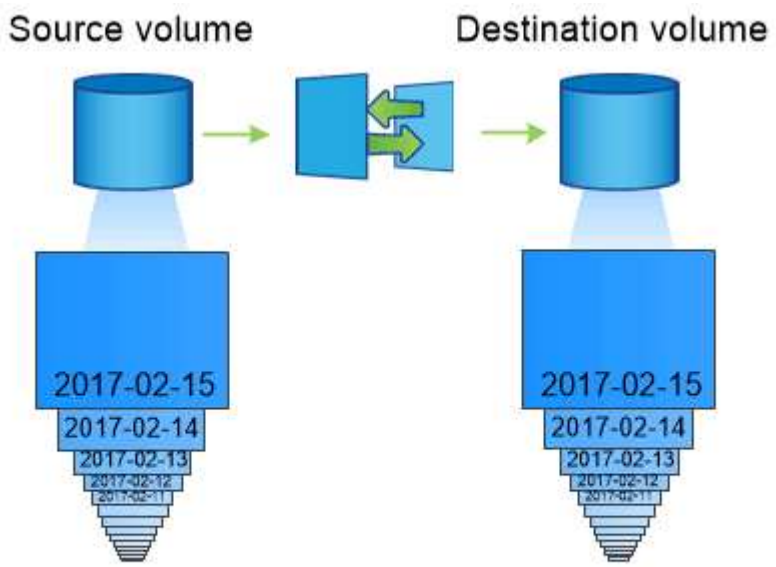
SnapMirror ist eine Disaster Recovery-Technologie für den Failover von primärem Storage zu sekundärem Storage an einem geografisch verteilten Standort. Wie der Name schon andeutet, erstellt SnapMirror ein Replikat, oder *Mirror* Ihrer Arbeitsdaten im Sekundärspeicher, von dem Sie im K-Fall am primären Standort weiter Daten bereitstellen können.

Wenn der primäre Standort weiterhin Daten versorgen kann, können Sie einfach alle benötigten Daten zurück darauf übertragen und nicht Clients vom Spiegel bedienen. Wie der Anwendungsfall für Failover impliziert, sollten die Controller auf dem sekundären System äquivalent oder fast vergleichbar mit den Controllern auf dem Primärsystem sein, um Daten effizient aus dem gespiegelten Storage bereitzustellen.

Datensicherungsbeziehungen

Daten werden auf Volume-Ebene gespiegelt. Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als „ Data Protection Relationship“ bezeichnet._ die Cluster, in denen sich die Volumes befinden, und die SVMs, die Daten aus den Volumes bereitstellen, müssen wie "Peered"„ heißen“. Eine Peer-Beziehung ermöglicht Cluster und SVMs den sicheren Datenaustausch.

Diese Abbildung zeigt die SnapMirror Datensicherungsbeziehungen:



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

Umfang Datensicherungsbeziehungen

Sie können eine Datensicherungsbeziehung direkt zwischen Volumes oder zwischen den SVMs, die Eigentümer der Volumes sind, erstellen. In einer Datensicherungsbeziehung mit SVM, die vollständig oder teilweise von der SVM-Konfiguration, von NFS-Exporten und SMB-Freigaben bis hin zur rollenbasierten Zugriffssteuerung, repliziert wird, sowie die Daten in den Volumes, die die SVM besitzt.

SnapMirror kann auch für besondere Datensicherungsapplikationen eingesetzt werden:

- Eine *Load-Sharing-Mirror* Kopie des SVM Root-Volume stellt sicher, dass im Falle eines Node-Ausfalls oder eines Failover auf die Daten zugegriffen werden kann.
- Eine Datensicherungsbeziehung zwischen *SnapLock Volumes* ermöglicht es Ihnen, WORM-Dateien in den Sekundärspeicher zu replizieren.

  "Archivierung und Compliance mit SnapLock Technologie"

- Ab ONTAP 9.13.1 können Sie SnapMirror asynchron zum Schutz verwendenKonsistenzgruppen. Ab ONTAP 9.14.1 können Sie SnapMirror asynchron verwenden, um mithilfe der Konsistenzgruppenbeziehung Volume-granulare Snapshots auf den Ziel-Cluster zu replizieren. Weitere Informationen finden Sie unter Konfigurieren Sie die asynchrone Sicherung von SnapMirror.

So werden die SnapMirror Datensicherungsbeziehungen initialisiert

Beim ersten Aufruf von SnapMirror führt es einen *Baseline-Transfer* vom Quell-Volume zum Ziel-Volume durch. Die Richtlinie *SnapMirror* für die Beziehung definiert den Inhalt der Baseline und alle Updates.

Ein Basistransfer gemäß der standardmäßigen SnapMirror-Richtlinie `MirrorAllSnapshots` umfasst die folgenden Schritte:

- Erstellen Sie einen Snapshot des Quell-Volumes.
- Übertragen Sie den Snapshot und alle Datenblöcke, die er auf das Ziel-Volume verweist.
- Übertragen Sie die verbleibenden, weniger aktuellen Snapshots auf dem Quellvolume auf das Zielvolume für den Fall, dass der „`Active`“-Spiegel beschädigt ist.

Aktualisierung von SnapMirror Datensicherungsbeziehungen

Updates werden asynchron und folgen dem von Ihnen konfigurierten Zeitplan. Die Aufbewahrung spiegelt die Snapshot-Richtlinie auf der Quelle.

Bei jeder Aktualisierung im Rahmen der `MirrorAllSnapshots` Richtlinie erstellt SnapMirror einen Snapshot des Quell-Volumes und überträgt diesen Snapshot sowie alle Snapshots, die seit der letzten Aktualisierung erstellt wurden. `snapmirror policy show` `MirrorAllSnapshots`Beachten Sie in der folgenden Ausgabe des Befehls für die Richtlinie Folgendes:

- `Create Snapshot` Ist „`true`“ und zeigt an, dass `MirrorAllSnapshots` ein Snapshot erstellt wird, 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 Snapshots, die seit der letzten Aktualisierung erstellt wurden, 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 so wie `MirrorAllSnapshots`, außer dass nur der von SnapMirror erstellte Snapshot bei der Initialisierung und Aktualisierung übertragen wird.

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

Verwandte Informationen

- "Snapmirror-Richtlinien-Show"

Erfahren Sie mehr über ONTAP SnapMirror Disaster Recovery für synchrone Disaster Recovery

Ab ONTAP 9.5 wird die SnapMirror Synchronous (SM-S)-Technologie auf allen FAS und AFF Plattformen unterstützt, die mindestens 16 GB Speicher haben und auf allen ONTAP

Select Plattformen. Die synchrone SnapMirror Technologie ist eine Funktion mit Lizenzierung pro Node, die eine synchrone Datenreplizierung auf Volume-Ebene bietet.

Diese Funktionalität ist sowohl den gesetzlichen als auch den nationalen Vorgaben für synchrone Replizierung in Finanz-, Gesundheitswesen und anderen Branchen gerecht, in denen Datenverluste nicht erforderlich sind.

Synchrone SnapMirror-Vorgänge zulässig

Die Obergrenze der Anzahl der synchronen SnapMirror-Replizierungsvorgänge pro HA-Paar hängt vom Controller-Modell ab.

In der folgenden Tabelle ist die Anzahl der synchronen SnapMirror-Vorgänge aufgeführt, die je nach Plattformtyp und ONTAP Version pro HA-Paar zulässig sind.

Plattform	ONTAP 9.14.1 bis ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	Versionen vor ONTAP 9.9.1
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

Unterstützte Funktionen

Die folgende Tabelle zeigt die Funktionen, die von SnapMirror Synchronous und den ONTAP Versionen unterstützt werden, in denen Unterstützung verfügbar ist.

Funktion	Release wird zuerst unterstützt	Weitere Informationen
Virenschutz auf dem primären Volume der synchronen SnapMirror-Beziehung	ONTAP 9,6	
Von der Anwendung erstellte Snapshot-Replikation	ONTAP 9,7	Wenn ein Schnappschuss zum Zeitpunkt der `snapshot create` Im Betrieb repliziert SnapMirror mithilfe der CLI oder der ONTAP API die Snapshots synchron, sowohl die vom Benutzer erstellten als auch die mit externen Skripten erstellten, nachdem die Anwendungen stillgelegt wurden. Geplante Snapshots, die mithilfe einer Snapshot-Richtlinie erstellt wurden, werden nicht repliziert. Weitere Informationen zum Replizieren von anwendungserstellten Snapshots finden Sie im"NetApp Knowledge Base: So replizieren Sie von Anwendungen erstellte Snapshots mit SnapMirror synchron" .
Automatisches Löschen von Klonen	ONTAP 9,6	

FabricPool Aggregate mit der Tiering-Richtlinie „Keine“, „Snapshot“ oder „automatisch“ werden von der synchronen Quelle und dem synchronen Ziel von SnapMirror unterstützt.	ONTAP 9,5	Das Ziel-Volume in einem FabricPool-Aggregat kann nicht auf „Alle Tiering-Richtlinien“ gesetzt werden.
FC	ONTAP 9,5	Über alle Netzwerke, bei denen die Latenz nicht mehr als 10 ms beträgt
FC-NVMe	ONTAP 9,7	
Dateiklone	ONTAP 9,7	
FPolicy auf das primäre Volume der synchronen SnapMirror-Beziehung	ONTAP 9,6	
Hard- und Soft-Quotas auf dem primären Volume der synchronen SnapMirror-Beziehung	ONTAP 9,6	Die Quota-Regeln werden nicht auf das Ziel repliziert, daher wird die Quota-Datenbank nicht auf das Ziel repliziert.
Synchrone Beziehungen zwischen Clustern	ONTAP 9.14.1	Hochverfügbarkeit wird geboten, wenn Quell- und Ziel-Volumes auf verschiedenen HA-Paaren platziert werden. Wenn das gesamte Cluster ausfällt, ist der Zugriff auf die Volumes erst nach der Wiederherstellung des Clusters möglich. Synchrone SnapMirror-Beziehungen innerhalb eines Clusters tragen zur Gesamtgrenze von simultan beiBeziehungen pro HA-Paar.
ISCSI	ONTAP 9,5	
LUN-Klone und NVMe Namespace-Klone	ONTAP 9,7	
LUN-Klone, die durch von Applikationen erstellte Snapshots gesichert werden	ONTAP 9,7	
Zugriff auf gemischte Protokolle (NFS v3 und SMB)	ONTAP 9,6	
NDMP/NDMP-Wiederherstellung	ONTAP 9.13.1	Sowohl auf dem Quell- als auch auf dem Zielcluster muss ONTAP 9.13.1 oder höher ausgeführt werden, um NDMP mit SnapMirror Synchronous zu verwenden. Weitere Informationen finden Sie unter Datenübertragung mithilfe einer ndmp-Kopie.
Unterbrechungsfreier, synchroner SnapMirror-Betrieb (NDO) nur auf AFF/ASA Plattformen	ONTAP 9.12.1	Dank der Support-Funktion für unterbrechungsfreien Betrieb können Sie viele gängige Wartungsaufgaben ohne Ausfallzeiten durchführen. Zu den unterstützten Vorgängen gehören Takeover und Giveback. Außerdem werden Volumes verschoben, sofern zwischen jedem der beiden Cluster ein einziger Node übrigbleibt.
NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9,6	

NFS v4.1	ONTAP 9,6	
NVMe/TCP	9.10.1	
Entfernung hoher Metadaten Frequenzbegrenzung	ONTAP 9,6	
Sicherheit für sensible Daten während der Übertragung mithilfe von TLS 1.2-Verschlüsselung	ONTAP 9,6	
Wiederherstellung einzelner Dateien und teilweise Dateien	ONTAP 9.13.1	
SMB 2.0 oder höher	ONTAP 9,6	
Synchrone gespiegelte SnapMirror-Kaskade	ONTAP 9,6	Die Beziehung zum Ziel-Volume der synchronen SnapMirror-Beziehung muss eine asynchrone SnapMirror-Beziehung sein.
Disaster Recovery für SVM	ONTAP 9,6	* Eine synchrone SnapMirror Quelle kann auch eine Disaster-Recovery-Quelle der SVM sein, zum Beispiel eine Fan-out-Konfiguration mit SnapMirror Synchronous als ein Bein und SVM Disaster Recovery als der andere. * Eine synchrone SnapMirror-Quelle kann kein Disaster-Recovery-Ziel für SVM sein, da SnapMirror Synchronous die Kaskadierung einer Datensicherungsquelle nicht unterstützt. Sie müssen die synchrone Beziehung freigeben, bevor Sie eine SVM-Disaster-Recovery-Flip-Resynchronisierung im Ziel-Cluster durchführen. * Ein synchroner SnapMirror-Zielort kann keine SVM-Disaster-Recovery-Quelle sein, da die SVM-Disaster-Recovery keine Replikation von DP-Volumes unterstützt. Eine Flip-Resynchronisierung der synchronen Quelle würde eine Disaster Recovery der SVM mit Ausnahme des DP-Volumes im Ziel-Cluster zur Folge haben.
Bandbasierte Wiederherstellung des Quell-Volumes	ONTAP 9.13.1	
Zeitstempel der Parität zwischen Quell- und Ziel-Volumes für NAS	ONTAP 9,6	Wenn Sie ein Upgrade von ONTAP 9.5 auf ONTAP 9.6 durchgeführt haben, wird der Zeitstempel nur für neue und geänderte Dateien im Quell-Volume repliziert. Der Zeitstempel vorhandener Dateien im Quell-Volume wird nicht synchronisiert.

Nicht unterstützte Funktionen

Die folgenden Funktionen werden bei synchronen SnapMirror-Beziehungen nicht unterstützt:

- Autonomer Schutz Durch Ransomware
- Konsistenzgruppen
- DP_Optimized (DPO)-Systeme
- FlexGroup Volumes

- FlexCache Volumes
- Globale Drosselung
- In einer Fan-out-Konfiguration kann nur eine Beziehung eine synchrone SnapMirror-Beziehung sein. Alle anderen Beziehungen aus dem Quell-Volume müssen asynchrone SnapMirror-Beziehungen sein.
- LUN-Verschiebung
- MetroCluster Konfigurationen
- LUNs mit gemischten SAN- und NVMe-Zugriffs sowie NVMe Namespaces werden nicht auf demselben Volume oder derselben SVM unterstützt.
- SnapCenter
- SnapLock Volumes
- Manipulationssichere Snapshots
- Tape Backup oder Wiederherstellung mithilfe von Dump und SMTape auf dem Ziel-Volume
- Durchsatzboden (QoS Min.) für Quell-Volumes
- Volume SnapRestore
- VVol

Betriebsmodi

SnapMirror Synchronous bietet je nach Typ der verwendeten SnapMirror-Richtlinie zwei Betriebsmodi:

- **Sync-Modus** im Sync-Modus werden Applikations-I/O-Vorgänge parallel zu den primären und sekundären Speichersystemen gesendet. Wenn der Schreibvorgang auf dem sekundären Storage aus irgendeinem Grund nicht abgeschlossen wird, kann die Applikation das Schreiben auf den primären Storage fortsetzen. Wenn der Fehlerzustand behoben ist, synchronisiert sich die synchrone SnapMirror Technologie automatisch mit dem sekundären Storage und setzt im synchronen Modus die Replizierung vom primären zum sekundären Storage fort. Im synchronen Modus ist RPO=0 und RTO sehr niedrig, bis ein sekundärer Replizierungsausfall auftritt. RPO und RTO sind nicht bestimmt, entsprechen aber der Zeit zur Behebung des Problems, das zum Scheitern der sekundären Replizierung und zum Abschluss der Resync-Synchronisierung geführt hat.
- **StructSync-Modus** SnapMirror Synchronous kann optional im StructSync-Modus betrieben werden. Wenn der Schreibvorgang auf den sekundären Storage aus irgendeinem Grund nicht abgeschlossen wird, fällt der Applikations-I/O aus. Dadurch wird sichergestellt, dass der Primär- und der Sekundärspeicher identisch sind. Die I/O-Vorgänge der Applikation zum primären `InSync` Status werden erst fortgesetzt, nachdem die SnapMirror-Beziehung wieder in den Status zurückkehrt. Falls der primäre Storage ausfällt, kann der Applikations-I/O nach dem Failover auf dem sekundären Storage fortgesetzt werden, ohne dass die Daten verloren gehen. Im Modus StrictSync ist die RPO immer null und die RTO ist sehr niedrig.

Beziehungsstatus

Der Status einer synchronen SnapMirror-Beziehung befindet sich `InSync` während des normalen Betriebs immer im Status. Wenn die SnapMirror-Übertragung aus irgendeinem Grund fehlschlägt, ist das Ziel nicht mit der Quelle synchronisiert und kann den `OutofSync` Status wechseln.

Bei SnapMirror-synchronen Beziehungen überprüft das System automatisch den Beziehungsstatus `InSync` oder `OutofSync`) in einem festen Intervall. Wenn der Beziehungsstatus lautet `OutofSync`, löst ONTAP automatisch den automatischen Resync-Prozess aus, um die Beziehung wieder in den `InSync` Status zu bringen. Die automatische Neusynchronisierung wird nur dann ausgelöst, wenn der Transfer aufgrund eines Vorgangs, z. B. ungeplanten Storage-Failover am Quell- oder Ziel-System oder aufgrund eines

Netzwerkausfalls, ausfällt. Vom Benutzer initiierte Vorgänge wie `snapmirror quiesce` und `snapmirror break` lösen keine automatische Neusynchronisierung aus.

Wenn `OutofSync` im StructSync-Modus für eine synchrone SnapMirror-Beziehung der Beziehungsstatus lautet, werden alle I/O-Vorgänge zum primären Volume angehalten. Der `OutofSync` Status der synchronen SnapMirror-Beziehung im synchronen Modus stellt keine Unterbrechung für das primäre Volume dar, und I/O-Vorgänge sind auf dem primären Volume zulässig.

Verwandte Informationen

- "Technischer Bericht 4733 zu NetApp: Synchrone Konfiguration mit SnapMirror und Best Practices"
- "Snapmirror-Pause"
- "Snapmirror-Ruhezustand"

Standardmäßige ONTAP Datensicherungsrichtlinien

ONTAP enthält mehrere standardmäßige Sicherungsrichtlinien, die Sie für Ihre Datensicherungsbeziehungen verwenden können. Die von Ihnen verwendete Richtlinie hängt vom Typ der Schutzbeziehung ab.

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

Liste der Standardschutzrichtlinien und -Beschreibungen

Im Folgenden werden die Standardschutzrichtlinien und die zugehörigen Richtlinientypen beschrieben.

Name	Beschreibung	Richtliniente yp
Asynchron	Eine einheitliche asynchrone und Vault-Richtlinie von SnapMirror zur Spiegelung des letzten aktiven Dateisystems und täglicher oder wöchentlicher Snapshots mit einem stündlichen Transferplan	Asynchron
Automatisches FailOver	Richtlinie für SnapMirror-synchron mit einer RTO-Garantie von null, bei der der Client-I/O bei Replizierungsfehlern nicht unterbrochen wird.	Synchron
Automatischer FailoverDuplex	Richtlinie für SnapMirror Synchronous mit Zero-RTO-Garantie und bidirektionaler synchroner Replikation.	Synchron
CloudBackupDefault	Vault-Richtlinie mit täglichen Regeln.	Asynchron
Kontinuierlich	Richtlinie für die S3-Bucket-Spiegelung	Kontinuierlic h
DailyBackup	Vault-Richtlinie mit einer täglichen Regel und einem täglichen Übertragungsplan	Asynchron
DPDefault	Asynchrone SnapMirror-Richtlinie für das Spiegeln aller Snapshots und des aktuellen aktiven Filesystems.	Asynchron

Name	Beschreibung	Richtlinientyp
MirrorAllSnapshots	Asynchrone SnapMirror-Richtlinie für das Spiegeln aller Snapshots und des aktuellen aktiven Filesystems.	Asynchron
MirrorAllSnapshotsDiscardNetwork	Asynchrone SnapMirror-Richtlinie für das Spiegeln aller Snapshots und des aktuellen aktiven Filesystems ohne Netzwerkkonfigurationen.	Asynchron
MirrorAndVault	Eine einheitliche asynchrone und Vault-Richtlinie von SnapMirror zur Spiegelung des letzten aktiven Filesystems und täglicher oder wöchentlicher Snapshots.	Asynchron
MirrorAndVaultDiscardNetwork	Eine asynchrone und Vault-Richtlinie von SnapMirror zur Spiegelung des letzten aktiven Filesystems und täglicher und wöchentlicher Snapshots, bei denen die Netzwerkkonfigurationen nicht berücksichtigt werden.	Asynchron
MirrorLatest	Asynchrone SnapMirror-Richtlinie zum Spiegeln des aktuellen aktiven Filesystems.	Asynchron
SnapCenterSync	Richtlinie für SnapMirror Synchronous for SnapCenter mit von der Applikation erstellter Snapshot-Konfiguration.	Synchron
StrictSync	Richtlinie für SnapMirror Synchronous, bei dem der Client-Zugriff bei einem Replizierungsfehler unterbrochen wird.	Synchron
Synchron	Richtlinie für SnapMirror Synchronous, bei dem der Client-Zugriff bei Replizierungsfehlern nicht unterbrochen wird.	Synchron
Unified7 Jahr	Unified SnapMirror Policy mit 7 Jahren Aufbewahrung.	Asynchron
XDPStandard	Vault-Richtlinie mit täglichen und wöchentlichen Regeln.	Asynchron

Erfahren Sie mehr über von ONTAP StructSync und Synchronisierungsrichtlinien unterstützte Workloads

Die Richtlinien von StrictSync und Sync unterstützen alle LUN-basierten Applikationen mit FC-, iSCSI- und FC-NVMe-Protokollen sowie NFSv3- und NFSv4-Protokollen für Enterprise-Applikationen wie Datenbanken, VMware, Quotas, SMB usw. Ab ONTAP 9.6 kann SnapMirror Synchronous für Enterprise-Fileservices wie Electronic Design Automation (EDA), Home Directories und Workloads bei der Software-Build eingesetzt werden.

In ONTAP 9.5 müssen Sie für eine Sync-Richtlinie bei der Auswahl der NFSv3- oder NFSv4-Workloads ein paar wichtige Aspekte berücksichtigen. Das Ausmaß der Daten-Lese- oder -Schreibvorgänge nach Workloads ist keine Lösung, da die Sync-Richtlinie hohe Lese- und Schreib-I/O-Workloads verarbeiten kann. In ONTAP 9.5 sind Workloads mit einer übermäßigen Erstellung von Dateien, Verzeichniserstellung, Änderung der Dateiberechtigungen oder Änderung der Verzeichnisberechtigungen möglicherweise nicht geeignet (diese werden als Workloads mit hohen Metadaten bezeichnet). Ein typisches Beispiel für einen Workload mit hohen

Metadaten ist ein DevOps-Workload, in dem Sie mehrere Testdateien erstellen, die Automatisierung ausführen und die Dateien löschen. Ein weiteres Beispiel ist ein paralleler Build-Workload, der während der Kompilierung mehrere temporäre Dateien generiert. Der Einfluss einer hohen Geschwindigkeit von Metadatenaktivitäten besteht darin, dass die Synchronisierung zwischen Spiegeln vorübergehend unterbrochen wird, wodurch die Lese- und Schreib-I/O-Vorgänge des Clients beeinträchtigt werden.

Ab ONTAP 9.6 wurden diese Einschränkungen aufgehoben und SnapMirror Synchronous kann für Enterprise-File-Services-Workloads eingesetzt werden, die Umgebungen mit mehreren Benutzern umfassen, wie Home Directorys und Workloads zur Softwareversion.

Verwandte Informationen

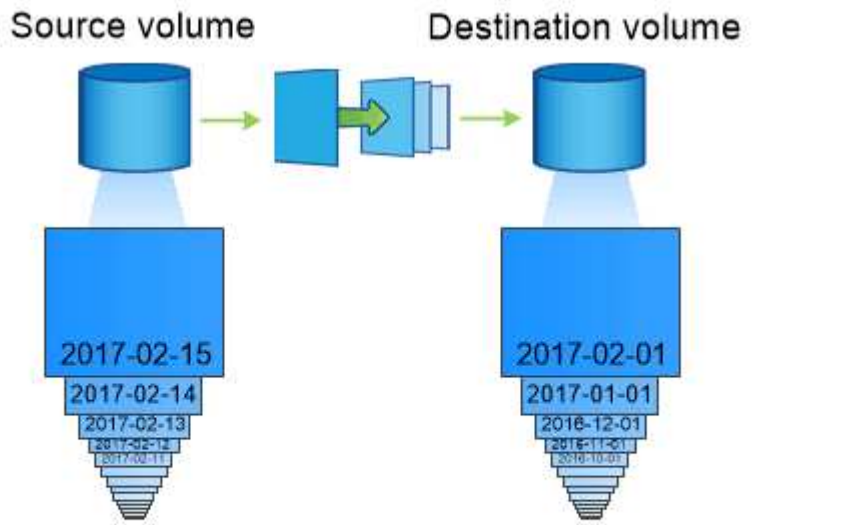
"Synchrone Konfiguration von SnapMirror und Best Practices"

Erfahren Sie mehr über die Vault-Archivierung mit ONTAP SnapMirror Technologie

Die Richtlinien von SnapMirror Vault ersetzen die SnapVault Technologie in ONTAP 9.3 und höher. Sie verwenden eine SnapMirror Vault-Richtlinie für die Disk-to-Disk Snapshot-Replizierung zur Einhaltung von Standards und anderen Governance-Zwecken. Im Gegensatz zu einer SnapMirror-Beziehung, bei der das Ziel normalerweise nur die Snapshots enthält, die derzeit im Quell-Volume vorhanden sind, behält ein Vault-Ziel normalerweise zeitpunktgenaue Snapshots, die über einen viel längeren Zeitraum erstellt wurden.

Möglicherweise möchten Sie monatliche Snapshots Ihrer Daten über einen Zeitraum von 20 Jahren speichern, um beispielsweise gesetzliche Buchhaltungsvorschriften in Ihrem Unternehmen zu erfüllen. Da keine Daten aus dem Vault-Speicher bereitgestellt werden müssen, können Sie langsamere und kostengünstigere Festplatten auf dem Zielsystem verwenden.

Die Abbildung unten zeigt SnapMirror Vault-Datensicherungsbeziehungen.



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-Datensicherungsbeziehungen initialisiert werden

Die SnapMirror-Richtlinie für die Beziehung definiert den Inhalt des Basisplans und etwaige Updates.

Bei einem Basistransfer unter der Standard-Vault-Richtlinie `XDPDefault` wird ein Snapshot des Quell-Volume erstellt und auch die darauf referenzierten Datenblöcke auf das Ziel-Volume übertragen. Im Gegensatz zu SnapMirror Beziehungen enthält ein Vault-Backup keine älteren Snapshots in der Baseline.

Aktualisierung von Vault-Datensicherungsbeziehungen

Updates werden asynchron und folgen dem von Ihnen konfigurierten Zeitplan. Die Regeln, die Sie in der Richtlinie für die Beziehung definieren, identifizieren, welche neuen Snapshots in Updates aufgenommen werden sollen und wie viele Kopien aufbewahrt werden sollen. Die in der Richtlinie definierten Bezeichnungen („`mmonatlich,`“ zum Beispiel) müssen mit einer oder mehreren in der Snapshot-Richtlinie auf der Quelle definierten Bezeichnungen übereinstimmen. Andernfalls schlägt die Replizierung fehl.

Bei jeder Aktualisierung gemäß der `XDPDefault` Richtlinie überträgt SnapMirror Snapshots, die seit der letzten Aktualisierung erstellt wurden, vorausgesetzt, sie haben Labels, die mit den in den Richtlinienregeln definierten Labels übereinstimmen. `snapmirror policy show` `XDPDefault`Beachten Sie in der folgenden Ausgabe des Befehls für die Richtlinie Folgendes:

- `Create Snapshot` Ist „`false`“, was darauf hinweist, dass `XDPDefault` kein Snapshot erstellt wird, wenn SnapMirror die Beziehung aktualisiert.
- `XDPDefault` Verfügt über die Regeln “daily” und “Weekly”, die darauf hinweisen, dass alle Snapshots mit übereinstimmenden Etiketten 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-Richtlinien-Show"

Erfahren Sie mehr über die einheitliche Replizierung mit ONTAP SnapMirror

Mit SnapMirror *Unified Replication* können Sie Disaster Recovery und Archivierung auf demselben Ziel-Volume konfigurieren. Wenn eine einheitliche Replizierung geeignet ist, kann sie die benötigte Menge an sekundärem Storage verringern, die Anzahl der Basistransfers begrenzen und den Netzwerkverkehr senken.

Initialisierung von Unified Datensicherungsbeziehungen

Wie bei SnapMirror führt die einheitliche Datensicherung beim ersten Aufruf einen Basistransfer durch. Die SnapMirror-Richtlinie für die Beziehung definiert den Inhalt des Basisplans und etwaige Updates.

Bei einem Basistransfer unter der standardmäßigen einheitlichen Datenschutzrichtlinie `MirrorAndVault` wird ein Snapshot des Quell-Volume erstellt und auch die Kopie der Datenblöcke auf das Ziel-Volume übertragen. Wie bei der Vault-Archivierung umfasst die einheitliche Datensicherheit keine älteren Snapshots in der Baseline.

Aktualisierung von Unified Datensicherungsbeziehungen

Bei jeder Aktualisierung gemäß der `MirrorAndVault` Richtlinie erstellt SnapMirror einen Snapshot des Quell-Volume und überträgt diesen Snapshot sowie alle Snapshots, die seit der letzten Aktualisierung erstellt wurden, vorausgesetzt, sie haben Labels, die mit den in den Snapshot-Richtlinienregeln definierten Labels übereinstimmen. `snapmirror policy show` `MirrorAndVault`Beachten Sie in der folgenden Ausgabe des Befehls für die Richtlinie Folgendes:

- `Create Snapshot` Ist „`true`“ und zeigt an, dass `MirrorAndVault` ein Snapshot erstellt wird, wenn SnapMirror die Beziehung aktualisiert.
- `MirrorAndVault` Hat die Regeln “sm_created”, “daily” und “Weekly”, die darauf hinweisen, dass sowohl der von SnapMirror erstellte Snapshot als auch die Snapshots mit übereinstimmenden Labels 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 -
-
```

Unified7-Jahres-Politik

Die vorkonfigurierte `Unified7year` Richtlinie funktioniert genau so wie `MirrorAndVault`, außer dass eine vierte Regel monatliche Snapshots überträgt und sie 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

Durch einheitliche Replizierung wird der Inhalt des Basistransfer zum Snapshot beschränkt, der bei der Initialisierung durch SnapMirror erstellt wurde. Bei jeder Aktualisierung erstellt SnapMirror einen weiteren Snapshot der Quelle und überträgt diesen Snapshot sowie alle neuen Snapshots, deren Etiketten mit den in den Snapshot-Richtlinienregeln definierten Labels 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`“ wird unabhängig von den Aufbewahrungsregeln auf der Quelle aufbewahrt, sodass auch wenn der ursprünglich von SnapMirror übertragene Snapshot nicht mehr auf der Quelle verfügbar ist, eine Kopie davon auf dem Ziel verfügbar ist.

Wann sollten Sie die einheitliche Datenreplizierung verwenden

Sie müssen abwägen, welchen Vorteil Sie durch die Aufrechterhaltung einer vollständigen Spiegelung auf die Vorteile einer einheitlichen Replizierung haben: Verringerung des Sekundär-Storage, Begrenzung der Anzahl an Basistransfers und Verringerung des Netzwerk-Traffic.

Der wichtigste Faktor bei der Bestimmung der Angemessenheit der einheitlichen Replikation ist die Änderungsrate des aktiven Dateisystems. Ein herkömmlicher Spiegel könnte besser für ein Volume geeignet sein, das beispielsweise stündliche Snapshots von Datenbanktransaktionsprotokollen hält.

Verwandte Informationen

- "Snapmirror-Richtlinien-Show"

Ein ONTAP Ziel-Volume für die Datensicherung wächst automatisch

Während einer Datensicherung Spiegelungsübertragung wird das Ziel-Volume automatisch vergrößert, wenn das Quell-Volume gewachsen ist, sofern im Aggregat, das das Volume enthält, genügend Platz vorhanden ist.

Dieses Verhalten erfolgt unabhängig von einer automatischen Wachstumseinstellung am Zielort. Sie können das Volume-Wachstum nicht einschränken oder ein Wachstum von ONTAP nicht verhindern.

Datensicherungs-Volumes werden standardmäßig auf den `grow_shrink` Modus für automatische Größenanpassung festgelegt, wodurch das Volume entsprechend der Menge des genutzten Speicherplatzes

vergrößert oder verkleinert werden kann. Die maximale automatische Größe für Datensicherungs-Volumes entspricht der maximalen FlexVol-Größe und ist plattformabhängig. Beispiel:

- FAS8200, Standard-max. Automatische Größe für DP Volume = 100 TB

Weitere Informationen finden Sie unter "NetApp Hardware Universe".

Weitere Informationen zu Fan-out- und Kaskadenimplementierungen der ONTAP Datensicherung

Mithilfe einer Implementierung „ *Fan-out*“ lässt sich die Datensicherung auf mehrere sekundäre Systeme erweitern. Mithilfe einer Implementierung „*Kaskadierung*“ lässt sich die Datensicherung auf tertiäre Systeme erweitern.

Fan-out- und Kaskadenimplementierungen unterstützen jede beliebige Kombination aus SnapMirror DR, SnapVault oder einheitlicher Replizierung. Ab ONTAP 9.5 unterstützen synchrone SnapMirror Beziehungen Fan-out-Implementierungen mit einer oder mehreren asynchronen SnapMirror Beziehungen. In der Fan-out-Konfiguration kann nur eine synchrone SnapMirror-Beziehung vorhanden sein. Alle anderen Beziehungen aus dem Quell-Volume müssen asynchrone SnapMirror-Beziehungen sein. Synchrone SnapMirror Beziehungen unterstützen auch Kaskadenimplementierungen (ab ONTAP 9.6). Die Beziehung vom Ziel-Volume der synchronen SnapMirror Beziehung muss jedoch eine asynchrone SnapMirror-Beziehung darstellen. SnapMirror Active Sync (Unterstützt ab ONTAP 9.13.1) unterstützt auch Fan-out-Konfigurationen.

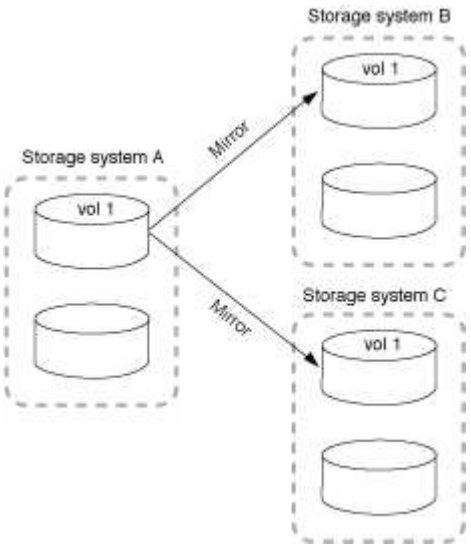
Mithilfe einer *Fan-in*-Implementierung lassen sich Datensicherungsbeziehungen zwischen mehreren Primärsystemen und einem einzigen sekundären System erstellen. Für jede Beziehung muss auf dem sekundären System ein anderes Volume verwendet werden.

Beachten Sie, dass Volumes, die zu einer Fan-out- oder Kaskadenkonfiguration gehören, länger dauern können, um die Synchronisierung erneut zu synchronisieren. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „Vorbereitung“ für einen längeren Zeitraum meldet.

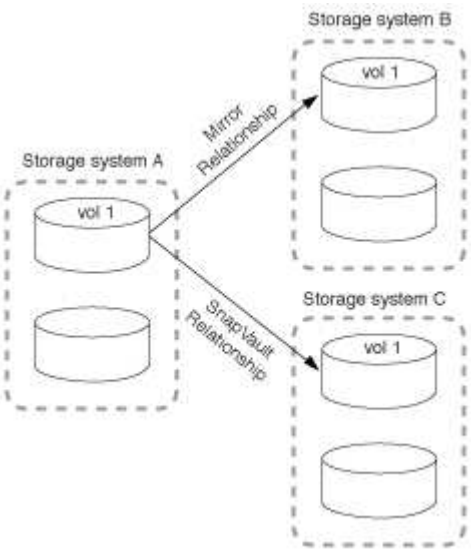
Funktionsweise von Fan-out-Implementierungen

SnapMirror unterstützt mehrere Spiegelungen_ und *Mirror-Vault* Fan-out-Implementierungen.

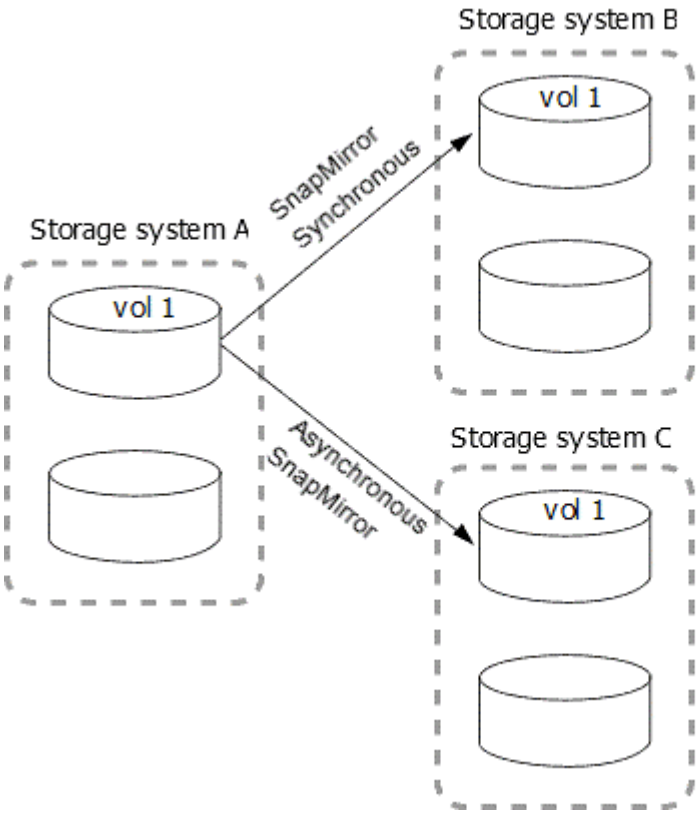
Eine Implementierung von Fan-out-Objekten aus mehreren Spiegelungen besteht aus einem Quell-Volume, das über eine Spiegelbeziehung zu mehreren sekundären Volumes verfügt.



Eine Implementierung von Fan-Vault-Fan-out besteht aus einem Quell-Volume, das über eine Spiegelbeziehung zu einem sekundären Volume und einer SnapVault Beziehung zu einem anderen sekundären Volume verfügt.



Ab ONTAP 9.5 können Fan-out-Implementierungen mit synchronen SnapMirror-Beziehungen erstellt werden. In der Fan-out-Konfiguration kann es sich jedoch nur um eine synchrone SnapMirror-Beziehung handeln, während es sich bei allen anderen Beziehungen des Quell-Volumes um asynchrone SnapMirror-Beziehungen handelt.



Funktionsweise der Kaskadierung

SnapMirror unterstützt *Mirror-Mirror*, *Mirror-Vault*, *Vault-Mirror* und *Vault-Vault* Kaskaden.

Eine Kaskadierung mit Spiegelspiegelung besteht aus einer Kette von Beziehungen, bei denen ein Quell-Volume auf ein sekundäres Volume gespiegelt und das sekundäre Volume auf einem tertiären Volume gespiegelt wird. Falls das sekundäre Volume nicht mehr verfügbar ist, können Sie die Beziehung zwischen dem primären und dem tertiären Volume synchronisieren, ohne einen neuen Basistransfer durchführen zu müssen.

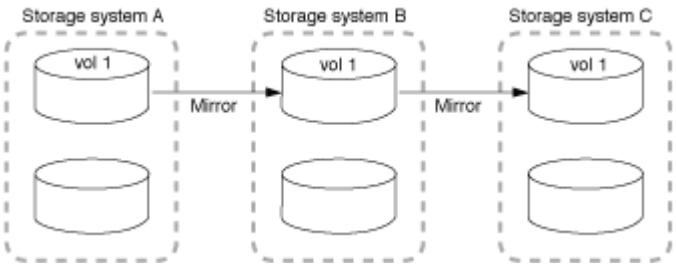
Bei einer Kaskadenstruktur von Volumes werden Langzeit-Snapshots in allen Versionen von ONTAP 9 nur auf dem letzten SnapMirror -Zielvolume der Kaskade unterstützt. Die Aktivierung von Langzeit-Snapshots auf einem beliebigen mittleren Volume in der Kaskade führt dazu, dass Backups und Snapshots verpasst werden. Wenn Sie eine nicht unterstützte Konfiguration verwenden, bei der Langzeit-Snapshots auf einem beliebigen mittleren Volume einer Kaskade aktiviert wurden, wenden Sie sich bitte an den technischen Support und geben Sie die entsprechende Referenz an. "NetApp Knowledge Base: Das Kaskadieren eines Volumes mit aktivierten LTR-Snapshots (Long-Term Retention) wird nicht unterstützt" um Unterstützung zu erhalten.

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

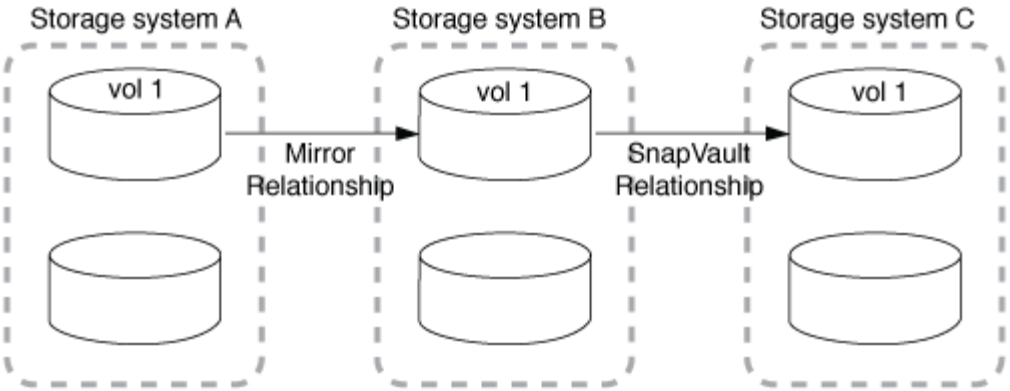
- 9.15.1 und höher
- 9.14.1P2 und P4 bis P14
- 9.13.1P9 bis P17
- 9.12.1 P12 bis P19
- 9.11.1P15 bis P20
- 9.10.1P18 bis P20
- 9.9.1P20

Erfahren Sie mehr über"Snapshots zur langfristigen Aufbewahrung" .

Ab ONTAP 9.6 werden synchrone SnapMirror Beziehungen in einer Kaskadenimplementierung mit Spiegelspiegeln unterstützt. Nur die primären und sekundären Volumes können sich in einer synchronen SnapMirror-Beziehung befinden. Das Verhältnis zwischen sekundären Volumes und tertiären Volumes muss asynchron sein.



Eine Kaskadenbereitstellung mit Spiegelgewölbe setzt sich aus einer Kette von Beziehungen zusammen, bei denen ein Quell-Volume auf ein sekundäres Volume gespiegelt und das sekundäre Volume in ein tertiäres Volume verlagert wird.



Vault-Mirror- und Vault-Vault-Cascade-Bereitstellungen werden ebenfalls unterstützt:

- Eine Kaskadenbereitstellung mit Vault-Spiegelung besteht aus einer Kette von Beziehungen, bei denen ein Quell-Volume auf ein sekundäres Volume archiviert wird und das sekundäre Volume auf ein tertiäres Volume gespiegelt wird.
- Eine Vault-Vault-Kaskadenbereitstellung besteht aus einer Kette von Beziehungen, in denen ein Quellvolume in ein sekundäres Volume und das sekundäre Volume in ein tertiäres Volume verschoben wird.

Verwandte Informationen

- Wiederaufnahme des Schutzes in einer Fan-out-Konfiguration mit SnapMirror Active Sync

Weitere Informationen zur ONTAP SnapMirror Lizenzierung

Ab ONTAP 9.3 wurde die Lizenzierung für die Replizierung zwischen ONTAP Instanzen vereinfacht. In ONTAP 9 Versionen unterstützt die SnapMirror Lizenz sowohl Vault- als auch Mirror-Beziehungen. Sie können eine SnapMirror Lizenz verwenden, um ONTAP Replizierung für Backup- und Disaster-Recovery-Anwendungsfälle zu unterstützen.

Vor der Version ONTAP 9.3 wurde eine separate SnapVault Lizenz benötigt, um Beziehungen zwischen ONTAP Instanzen zu *Vault* zu konfigurieren, bei denen die DP-Instanz eine höhere Anzahl an Snapshots beibehalten konnte, um Backup-Anwendungsfälle mit längeren Aufbewahrungszeiten zu unterstützen. Außerdem war eine SnapMirror Lizenz erforderlich, um Beziehungen zwischen ONTAP Instanzen zu *mirror* zu konfigurieren, wobei jede ONTAP Instanz dieselbe Anzahl von Snapshots (d. h. ein *mirror* image) beibehalten würde, um Anwendungsfälle für Disaster Recovery zu unterstützen, um Cluster Failovers zu ermöglichen. Sowohl SnapMirror als auch SnapVault Lizenzen werden weiterhin verwendet und werden von den Versionen ONTAP 8.x und 9.x unterstützt.

SnapVault Lizenzen funktionieren weiterhin und werden sowohl für ONTAP 8.x- als auch für 9.x-Versionen unterstützt. Die SnapMirror Lizenz kann anstelle einer SnapVault Lizenz verwendet werden und kann sowohl für Spiegelungs- als auch für Vault-Konfigurationen verwendet werden.

Für die asynchrone Replizierung von ONTAP wird ab ONTAP 9.3 eine einzelne Unified Replication Engine zur Konfiguration von Richtlinien für den erweiterten Datensicherungsmodus (XDP) verwendet. Dabei kann die SnapMirror Lizenz für eine Spiegelrichtlinie, eine Vault-Richtlinie oder eine Mirror-Vault-Richtlinie konfiguriert werden. Es ist eine SnapMirror Lizenz auf den Quell- und Ziel-Clustern erforderlich. Wenn bereits eine SnapMirror Lizenz installiert ist, ist keine SnapVault Lizenz erforderlich. Die zeitlich unbegrenzte SnapMirror Lizenz ist in der ONTAP One Softwaresuite enthalten, die auf den neuen AFF und FAS Systemen installiert ist.

Einschränkungen für die Datensicherungskonfiguration werden unter Verwendung verschiedener Faktoren

bestimmt, einschließlich Ihrer ONTAP Version, Hardware-Plattform und der installierten Lizenzen. Weitere Informationen finden Sie unter "Hardware Universe".

SnapMirror synchrone Lizenz

Ab ONTAP 9.5 werden synchrone SnapMirror Beziehungen unterstützt. Für die Erstellung einer SnapMirror Synchronous-Beziehung benötigen Sie die folgenden Lizenzen:

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

  Die SnapMirror Synchronous Lizenz ist Teil der "ONTAP One Lizenzsuite".

  Wenn Ihr System vor Juni 2019 mit einem Premium- oder Flash-Paket erworben wurde, können Sie einen NetApp Master Key herunterladen und die erforderliche synchrone SnapMirror Lizenz von der NetApp Support-Website erhalten: "Master-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 auf Objekt-Storage-Endpunkte. Replizierungsziele können unter Verwendung von On-Premises-Objektspeichern sowie S3- und S3-kompatiblen Public-Cloud-Objekt-Storage-Services konfiguriert werden. SnapMirror-Cloud-Beziehungen werden von ONTAP Systemen bis zu vorkonfigurierten Objekt-Storage-Zielen unterstützt.

SnapMirror Cloud ist nicht als Standalone-Lizenz verfügbar. Pro ONTAP Cluster ist nur eine Lizenz erforderlich. Zusätzlich zu einer SnapMirror-Cloud-Lizenz ist auch die asynchrone SnapMirror-Lizenz erforderlich.

Sie benötigen die folgenden Lizenzen für die Erstellung einer SnapMirror Cloud-Beziehung:

- Sowohl eine SnapMirror Lizenz als auch eine SnapMirror Cloud-Lizenz für die direkte Replizierung auf den Objektspeicher-Endpunkt.
- Bei der Konfiguration eines Workflows für die Replizierung mit mehreren Richtlinien (z. B. Disk-to-Disk-to-Cloud) ist für alle ONTAP Instanzen eine SnapMirror Lizenz erforderlich. Die SnapMirror Cloud Lizenz ist nur für das Quell-Cluster erforderlich, das direkt am Objekt-Storage-Endpunkt repliziert wird.

Ab ONTAP 9.9.1 können Sie "Verwenden Sie System Manager für die SnapMirror Cloud-Replizierung" .

Eine Liste autorisierter Applikationen für Drittanbieter der SnapMirror Cloud ist auf der NetApp Website veröffentlicht.

Für Datensicherheit optimierte Lizenz

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

DPO ist nicht im ONTAP One-Lizenzpaket enthalten, und Sie können kein Upgrade auf das ONTAP One-Lizenzpaket durchführen, wenn die DPO-Lizenz auf einem System installiert ist.

Informationen zu unterstützten Plattformen finden Sie unter "Hardware Universe".

ONTAP DPO-Systeme – Funktionserweiterungen

Ab ONTAP 9.6 erhöht sich bei Installation der DP_optimized (DPO) Lizenz die maximal unterstützte Anzahl von FlexVol Volumes. Ab ONTAP 9.4 unterstützen Systeme mit einer DPO-Lizenz das SnapMirror-Zurückschalten, die Volume-übergreifende Hintergrund-Deduplizierung, die Nutzung von Snapshot-Blöcken als Spender und Data-Compaction.

Ab ONTAP 9.6 ist die maximal unterstützte Anzahl an FlexVol-Volumes auf sekundären oder Datensicherungssystemen gestiegen, wodurch Sie auf bis zu 2,500 FlexVol-Volumes pro Node oder im Failover-Modus auf bis zu 5,000 skalieren können. Die Erhöhung der FlexVol-Volumes wird mit aktiviert"DP_Optimized (DPO)-Lizenz". A "SnapMirror Lizenz" ist weiterhin sowohl auf den Quell- als auch auf den Ziel-Nodes erforderlich.

Ab ONTAP 9.4 werden die folgenden Funktionsverbesserungen für DPO-Systeme vorgenommen:

- „SnapMirror Backoff“: In DPO-Systemen wird der Replizierungsdatenverkehr dieselbe Priorität zugewiesen, die Client-Workloads zugewiesen werden.

  Bei DPO-Systemen ist das Backoff SnapMirror standardmäßig deaktiviert.

- Hintergrund-Deduplizierung von Volumes und Volume-übergreifende Hintergrund-Deduplizierung: Hintergrunddeduplizierung für Volumes und Volume-übergreifende Hintergrund-Deduplizierung 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. Als Best Practice empfiehlt es sich, den Befehl in Zeiten geringerer Auslastung auszuführen, um die Auswirkungen auf die Performance zu verringern.

  Erfahren Sie mehr über `storage aggregate efficiency cross-volume-dedupe start` in der "ONTAP-Befehlsreferenz".

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

  Die neuen Daten können mit den Daten, die in Snapshots eingeschlossen waren, dedupliziert werden. Auf diese Weise werden auch die Snapshot-Blöcke gemeinsam genutzt. Der erhöhte Spenderplatz liefert mehr Einsparungen, besonders wenn das Volume über eine große Anzahl von Snapshots verfügt.

- Data-Compaction: Data-Compaction ist auf DPO Volumes standardmäßig aktiviert.

Erfahren Sie mehr über das Matching von Pfadnamen in ONTAP SnapMirror-Befehlen

Mithilfe der Musteranpassung können Sie die Quell- und Zielpfade in `snapmirror` Befehlen angeben.

```
`snapmirror` Befehle verwenden vollständig qualifizierte Pfadnamen im
folgenden Format: `vserver:volume`. Sie können den Pfadnamen kürzen, indem
Sie nicht den SVM-Namen eingeben. Wenn Sie dies tun, `snapmirror` wird der
lokale SVM-Kontext des Benutzers von dem Befehl vorausgesetzt.
```

Wenn die SVM „vserver1“ heißt und das Volume „vol1“ heißt, lautet der vollständig qualifizierte Pfadname `vserver1:vol1` .

Sie können das Sternchen (*) in Pfaden als Platzhalter verwenden, um übereinstimmende, vollständig qualifizierte Pfadnamen auszuwählen. In der folgenden Tabelle finden Sie Beispiele zur Verwendung des Wildcard zum Auswählen eines Bereichs von Volumes.

`*`	Entspricht allen Pfaden.
`vs*`	Ordnet alle SVMs und Volumes mit SVM-Namen ab `vs`.
`:*src`	Entspricht allen SVMs mit Volume-Namen, die den `src` Text enthalten.
`:vol`	Entspricht allen SVMs mit Volume-Namen beginnend mit `vol`.

```
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    -
```

Erfahren Sie mehr über `snapmirror show` in der "ONTAP-Befehlsreferenz".

Erfahren Sie mehr über erweiterte Abfragen für ONTAP SnapMirror-Beziehungsvorgänge

Sie können *erweiterte Abfragen* verwenden, um SnapMirror Operationen gleichzeitig an vielen SnapMirror Beziehungen durchzuführen. Beispielsweise könnten Sie mehrere nicht initialisierte SnapMirror Beziehungen haben, die Sie mit einem Befehl initialisieren möchten.

Über diese Aufgabe

Sie können erweiterte Anfragen auf folgende SnapMirror Vorgänge anwenden:

- Nicht initialisierte Beziehungen

- Fortsetzen von stillgelegten Beziehungen
- Unterbrochene Beziehungen werden neu synchronisiert
- Aktualisierung von nicht aktiven Beziehungen
- Übertragung von Beziehungsdaten wird abgebrochen

Schritt

1. Ausführung eines SnapMirror Vorgangs über viele Beziehungen:

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

   Mit dem folgenden Befehl werden SnapMirror-Beziehungen initialisiert, die sich in einem `Uninitialized` Status befinden:

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

   Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Kompatible ONTAP Versionen für SnapMirror Beziehungen

Auf den Quell- und Ziel-Volumes müssen kompatible ONTAP Versionen ausgeführt werden, bevor die SnapMirror Datensicherungsbeziehung erstellt wird. Bevor Sie ein Upgrade von ONTAP durchführen, sollten Sie überprüfen, ob Ihre aktuelle ONTAP-Version mit Ihrer Ziel-ONTAP-Version für SnapMirror Beziehungen kompatibel ist.

Einheitliche Replizierungsbeziehungen

Für SnapMirror Beziehungen vom Typ „`XDP`“ unter Verwendung von On-Premises- oder Cloud Volumes ONTAP-Versionen:

Ab ONTAP 9.9.0:

- ONTAP 9.x.0 Versionen sind reine Cloud-Versionen und unterstützen Cloud Volumes ONTAP Systeme. Das Sternchen (*) nach der Release-Version weist auf eine reine Cloud-Version hin.

  ⓘ ONTAP 9.16.0 bildet eine Ausnahme von der Regel, dass nur Cloud-Lösungen verfügbar sind, da es Unterstützung für Folgendes bietet:"ASA r2-Systeme" Die Das Pluszeichen (+) nach der Versionsnummer kennzeichnet eine Version, die sowohl von ASA r2 als auch von der Cloud unterstützt wird. ASA r2-Systeme unterstützen SnapMirror Beziehungen nur zu anderen ASA r2-Systemen.

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

  ⓘ Wenn "Erweiterter Kapazitätsausgleich"auf Volumes in Clustern mit ONTAP 9.16.1 oder höher aktiviert ist, werden SnapMirror-Transfers nicht auf Cluster unterstützt, auf denen ONTAP-Versionen vor ONTAP 9.16.1 ausgeführt werden.

  ⓘ Interoperabilität ist bidirektional.

Interoperabilität für ONTAP Version 9.4 und höher

ONTAP-Version…	Interagiert mit diesen früheren ONTAP-Versionen…																				
	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*	9,8	9,7	9,6	9,5
9.18.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**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**	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**	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.16.0+	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**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**	Nein	Nein	Nein	Nein	Nein
9.15.0*	Nein	**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**	Nein	Nein	Nein	Nein
9.14.0*	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	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.13.0*	Nein	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein
9.12.1	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	**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	**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	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein

9.10.1	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	**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	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9.9*	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	**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	**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**
9,5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**

Synchrone SnapMirror Beziehungen

SnapMirror Synchronous wird für ONTAP Cloud-Instanzen nicht unterstützt.

ONTAP-Version…	Interagiert mit diesen früheren ONTAP-Versionen…													
	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
9.18.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.17.1	**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**	Nein	Nein	Nein	Nein	Nein	Nein
9.15.1	**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**	Nein	Nein	Nein
9.13.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.12.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.11.1	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein
9.10.1	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.9.1	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9,8	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein
9,7	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	**Ja**	**Ja**	**Ja**	**Ja**

9,5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**

SnapMirror SVM Disaster-Recovery-Beziehungen

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

Für SVM-Disaster-Recovery-Daten und SVM-Sicherung:

Die SVM-Disaster Recovery wird nur zwischen Clustern unterstützt, auf denen dieselbe Version von ONTAP ausgeführt wird. **Die Versionsunabhängigkeit wird für die SVM-Replikation nicht unterstützt**.

SVM-Disaster Recovery für SVM-Migration:

- Die Replikation wird in einer einzigen Richtung von einer früheren Version von ONTAP auf der Quelle bis zur gleichen oder neueren Version von ONTAP auf dem Ziel unterstützt.
- Die ONTAP-Version auf dem Ziel-Cluster darf nicht mehr als zwei der wichtigsten On-Premises-Versionen oder zwei der wichtigsten Cloud-Versionen neuer (beginnend mit ONTAP 9.9.0) sein, wie in der Tabelle unten gezeigt.
  - Die Replizierung wird in Anwendungsfällen mit langfristiger Datensicherung nicht unterstützt.

Das Sternchen (*) nach der Release-Version weist auf eine reine Cloud-Version hin.

Um die Unterstützung zu ermitteln, suchen Sie die Quellversion in der linken Tabellenspalte, und suchen Sie dann die Zielversion in der oberen Zeile (DR/Migration für ähnliche Versionen und Migration nur für neuere Versionen).

Wenn Sie ONTAP 9.10.1 oder höher verwenden, können Sie die "SVM-Datenmobilität" Funktion anstelle von SVM DR, um SVMs von einem Cluster in einen anderen zu migrieren.

Quelle	Ziel																				
	9,5	9,6	9,7	9,8	9.9*	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
9,5	DR/Migration	Migration	Migration																			
9,6		DR/Migration	Migration	Migration																		

9,7			DR/Migration	Migration	Migration																
9,8				DR/Migration	Migration	Migration		Migration													
9.9*					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			

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

SnapMirror Disaster Recovery-Beziehungen

Für SnapMirror Beziehungen vom Typ „`DP`“ und vom Richtlinientyp „`async-Mirror`“:

Die Spiegelungen vom DP-Typ können nicht ab ONTAP 9.11.1 initialisiert werden und sind in ONTAP 9.12.1 vollständig veraltet. Weitere Informationen finden Sie unter "Abschreibungsvorgänge für Datensicherungs-SnapMirror Beziehungen".

In der folgenden Tabelle zeigt die Spalte auf der linken Seite die ONTAP-Version auf dem Quell-Volume und in der oberen Zeile die ONTAP-Versionen an, die Sie auf Ihrem Ziel-Volume haben 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.

Informieren Sie sich über ONTAP SnapMirror-Einschränkungen

Sie sollten auf die grundlegenden SnapMirror Einschränkungen achten, bevor Sie eine Datensicherungsbeziehung erstellen.

- Ein Ziel-Volume kann nur ein Quell-Volume haben.

  Ein Quell-Volume kann mehrere Zieldatenträger haben. Das Ziel-Volume kann das Quell-Volume für eine beliebige Art der SnapMirror Replizierungsbeziehung sein.

- Je nach Array-Modell können Sie maximal acht oder sechzehn Ziel-Volumes von einem einzigen Quell-Volume aus ausfächern. Unter finden Sie "Hardware Universe"weitere Informationen zu Ihrer spezifischen Konfiguration.
- Sie können keine Dateien zum Ziel einer SnapMirror DR-Beziehung wiederherstellen.
- Die Quell- oder Ziel-SnapVault-Volumen können nicht 32-bit sein.
- Das Quell-Volume für eine SnapVault-Beziehung sollte kein FlexClone Volume sein.

  Die Beziehung funktioniert, aber die Effizienz von FlexClone Volumes wird nicht erhalten bleiben.

Konfiguration der SnapMirror Volume-Replizierung

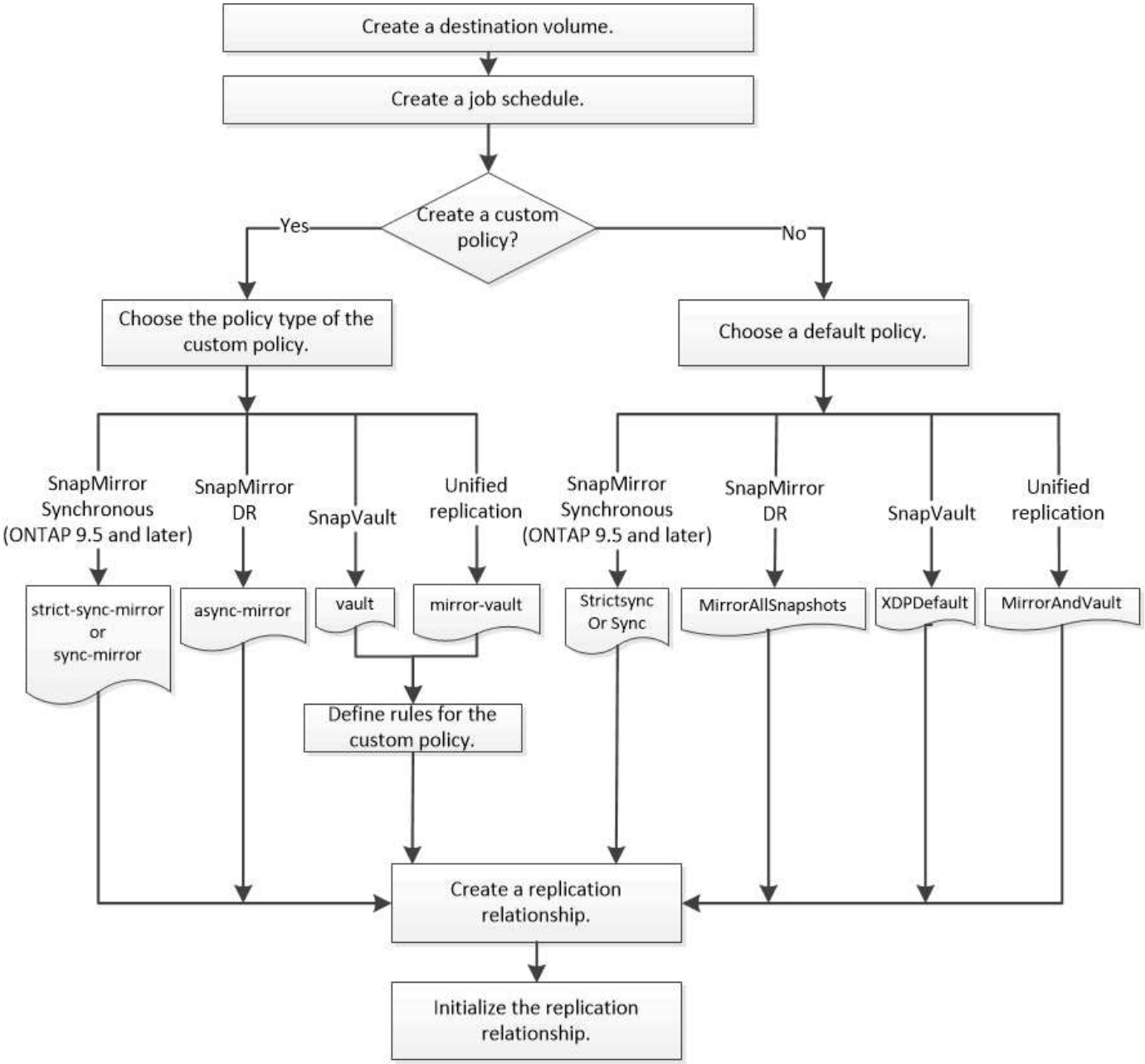
Workflow für die ONTAP SnapMirror Replizierung

SnapMirror bietet drei Arten von Datensicherungsbeziehungen: SnapMirror DR, Archiv (ehemals SnapVault) und einheitliche Replizierung. Sie können denselben grundlegenden Workflow verwenden, um die einzelnen Beziehungstypen zu konfigurieren.

Beginnend mit der allgemeinen Verfügbarkeit in ONTAP 9.9.1, "SnapMirror Active Sync" bietet das Zero Recovery Time Objective (Zero RTO) bzw. Transparent Application Failover (TAF) zur Aktivierung des automatischen Failovers geschäftskritischer Applikationen in SAN-Umgebungen.

Für jede Art der SnapMirror Datensicherungsbeziehung ist der Workflow derselbe: Erstellen Sie ein Ziel-Volume, erstellen Sie einen Job-Zeitplan, legen Sie eine Richtlinie fest, erstellen und initialisieren Sie die Beziehung.

Ab ONTAP 9.3 können Sie mit dem `snapmirror protect` Befehl in einem einzigen Schritt eine Datensicherungsbeziehung konfigurieren. Auch wenn Sie verwenden `snapmirror protect`, müssen Sie jeden Schritt im Workflow verstehen.



Verwandte Informationen

- "Snapmirror-Schutz"

Konfiguration einer ONTAP SnapMirror-Replikationsbeziehung in einem Schritt

Ab ONTAP 9.3 können Sie die `snapmirror protect` Befehl zum Konfigurieren einer Datenschutzbeziehung in einem einzigen Schritt. Sie geben eine Liste der zu replizierenden Volumes, eine SVM auf dem Zielcluster, einen Jobplan und eine SnapMirror Richtlinie an. `snapmirror protect` erledigt den Rest.

Bevor Sie beginnen

- Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.

  "Cluster- und SVM-Peering"

- Die Sprache auf dem Zielvolume muss mit der Sprache auf dem Quellvolume übereinstimmen.

Über diese Aufgabe

Der `snapmirror protect` Befehl wählt ein Aggregat aus, das der angegebenen SVM zugeordnet ist. Wenn der SVM kein Aggregat zugewiesen wird, wählt es alle Aggregate im Cluster aus. Die Auswahl eines Aggregats basiert auf dem freien Speicherplatz und der Anzahl der Volumes im Aggregat.

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

- Erstellt ein Ziel-Volume mit einem entsprechenden Typ und einer entsprechenden Menge an reserviertem Speicherplatz für jedes Volume in der Liste der zu replizierenden Volumes.
- Konfiguriert eine für die angegebene Richtlinie geeignete Replikationsbeziehung.
- Initialisiert die Beziehung.

Der Name des Zieldatenträger ist vom Formular *`source_volume_name_dst`*. Bei einem Konflikt mit einem vorhandenen Namen hängt der Befehl eine Nummer an den Volume-Namen an. Sie können in den Befehlsoptionen ein Präfix und/oder Suffix angeben. Das Suffix ersetzt das vom System bereitgestellte `dst` Suffix.

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

> Initialisierung kann sehr zeitaufwendig sein. `snapmirror protect` Wartet nicht, bis die Initialisierung abgeschlossen ist, bevor der Job abgeschlossen ist. Aus diesem Grund sollten Sie `snapmirror show` anstelle des Befehls den Befehl verwenden `job show`, um zu bestimmen, wann die Initialisierung abgeschlossen ist.

Ab ONTAP 9.5 können synchrone SnapMirror Beziehungen mit dem `snapmirror protect` Befehl erstellt werden.

Erfahren Sie mehr über `snapmirror protect` im "ONTAP-Befehlsreferenz" .

Schritt

1. Erstellen und Initialisieren einer Replikationsbeziehung in einem Schritt:

   Sie müssen die Variablen in Winkelklammern durch die erforderlichen Werte ersetzen, bevor Sie diesen Befehl ausführen.

```
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>
```

Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen. Die `-auto -initialize` Option ist standardmäßig „`true`“.

Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mithilfe der Standardrichtlinie erstellt und initialisiert `MirrorAllSnapshots`:

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

Sie können eine benutzerdefinierte Richtlinie verwenden, wenn Sie es bevorzugen. Weitere Informationen finden Sie unter "Erstellen einer benutzerdefinierten Replikationsrichtlinie".

Im folgenden Beispiel wird eine SnapVault-Beziehung mithilfe der Standardrichtlinie erstellt und initialisiert `XDPDefault`:

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

Im folgenden Beispiel wird eine einheitliche Replikationsbeziehung mithilfe der Standardrichtlinie erstellt und initialisiert `MirrorAndVault`:

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

Im folgenden Beispiel wird eine synchrone SnapMirror-Beziehung mithilfe der Standardrichtlinie erstellt und initialisiert `Sync`:

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

Für Richtlinien für SnapVault und einheitliche Replizierung ist es unter Umständen sinnvoll, einen Zeitplan für die Erstellung einer Kopie des zuletzt übertragenen Snapshots am Zielsystem zu definieren. Weitere Informationen finden Sie unter "Definieren eines Zeitplans zum Erstellen einer lokalen Kopie auf dem Ziel".

Nachdem Sie fertig sind

`snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror Beziehung erstellt wurde.

Erfahren Sie mehr über `snapmirror show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Jobanzeigen"

Konfigurieren Sie eine Replikationsbeziehung in einem Schritt nach dem anderen

Erstellen eines ONTAP SnapMirror Ziel-Volumes

Sie können das `volume create` Ziel-Volume mit dem Befehl auf dem Ziel erstellen. Das Zielvolumen sollte gleich oder größer sein als das Quellvolumen. Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz".

Schritt

1. Ziel-Volume erstellen:

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

   Im folgenden Beispiel wird ein 2-GB-Zielvolume mit dem Namen erstellt `volA_dst`:

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

Erstellen Sie einen Zeitplan für ONTAP SnapMirror-Replikationsjobs

Der Job-Zeitplan legt fest, wann SnapMirror die Datensicherungsbeziehung automatisch aktualisiert, denen der Zeitplan zugewiesen ist. Sie können System Manager oder den `job schedule cron create` Befehl verwenden, um einen Zeitplan für einen Replikationsjob zu erstellen. Erfahren Sie mehr über `job schedule cron create` in der "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Sie weisen beim Erstellen einer Datensicherungsbeziehung einen Job-Zeitplan zu. Wenn Sie keinen Job-Zeitplan zuweisen, müssen Sie die Beziehung manuell aktualisieren.

Schritte

Sie können einen Replikationsjob-Zeitplan mit System Manager oder der ONTAP-CLI erstellen.

System Manager

1. Navigieren Sie zu **Schutz > Übersicht**, und erweitern Sie die Optionen **Lokale Richtlinieneinstellungen**.
2. Klicken Sie im Bereich **Zeitpläne** auf →.
3. Klicken Sie im Fenster **Zeitpläne** auf + Add .
4. Geben Sie im Fenster **Zeitplan hinzufügen** den Namen des Zeitplans ein und wählen Sie den Kontext und den Zeitplantyp aus.
5. Klicken Sie Auf **Speichern**.

CLI

1. Job-Zeitplan 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` können Sie festlegen `all`, dass der Job jeden Monat, Wochentag und jede Stunde ausgeführt werden soll.

Ab ONTAP 9.10.1 können Sie den Vserver für Ihren Job-Zeitplan angeben:

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

Im folgenden Beispiel wird ein Jobzeitplan mit dem Namen erstellt `my_weekly`, der samstags um 3:00 Uhr ausgeführt wird:

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

Passen Sie eine SnapMirror Replizierungsrichtlinie an

Erstellen Sie eine benutzerdefinierte ONTAP SnapMirror-Replizierungsrichtlinie

Sie können eine benutzerdefinierte Replikationsrichtlinie erstellen, wenn die Standardrichtlinie für eine Beziehung nicht geeignet ist. Sie können beispielsweise Daten in einer Netzwerkübertragung komprimieren oder die Anzahl der von SnapMirror

unternommenen Versuche ändern, Snapshots zu übertragen.

Sie können eine Standard- oder benutzerdefinierte Richtlinie verwenden, wenn Sie eine Replikationsbeziehung erstellen. Für ein benutzerdefiniertes Archiv (früher SnapVault) oder eine einheitliche Replikationsrichtlinie müssen Sie eine oder mehrere *Rules* definieren, die festlegen, welche Snapshots während der Initialisierung und Aktualisierung übertragen werden. Sie können auch einen Zeitplan für die Erstellung lokaler Snapshots auf dem Ziel definieren.

Der Typ_Policy_ der Replikationsrichtlinie bestimmt die Art der von ihr unterstützten Beziehung. In der folgenden Tabelle sind die verfügbaren Richtlinientypen aufgeführt.

Richtlinientyp	Beziehungstyp
Asynchrone Spiegelung	SnapMirror DR
Vault	SnapVault
Mirror-Vault	Einheitliche Replizierung
Strenger Sync-Mirror	SnapMirror synchron im StructSync-Modus (unterstützt ab ONTAP 9.5)
Synchrone Spiegelung	SnapMirror synchron im Sync-Modus (unterstützt ab ONTAP 9.5)

Wenn Sie eine benutzerdefinierte Replikationsrichtlinie erstellen, empfiehlt es sich, die Richtlinie nach einer Standardrichtlinie zu modellieren.

Schritte

Sie können mit System Manager oder der ONTAP CLI benutzerdefinierte Datensicherungsrichtlinien erstellen. Ab ONTAP 9.11.1 können Sie mit System Manager benutzerdefinierte Mirror- und Vault-Richtlinien erstellen und ältere Richtlinien anzeigen und auswählen. Diese Funktion ist auch in ONTAP 9.8P12 und späteren Patches für ONTAP 9.8 verfügbar.

Erstellen Sie benutzerdefinierte Sicherungsrichtlinien für das Quell- und Ziel-Cluster.

System Manager

1. Klicken Sie Auf **Schutz > Übersicht > Lokale Richtlinieneinstellungen**.
2. Klicken Sie unter **Schutzrichtlinien** auf →.
3. Klicken Sie im Bereich **Schutzrichtlinien** auf + Add .
4. Geben Sie den neuen Richtliniennamen ein, und wählen Sie den Richtlinienumfang aus.
5. Wählen Sie einen Richtlinientyp aus. Um eine nur-Vault- oder nur-Mirror-Policy hinzuzufügen, wählen Sie **Asynchronous** und klicken Sie auf **alten Policy-Typ verwenden**.
6. Füllen Sie die erforderlichen Felder aus.
7. Klicken Sie Auf **Speichern**.
8. Wiederholen Sie diese Schritte auf dem anderen Cluster.

CLI

1. Erstellen einer benutzerdefinierten Replizierungsrichtlinie:

```
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 können Sie mithilfe des Parameters den Zeitplan zum Erstellen eines gemeinsamen Snapshot-Zeitplans für synchrone SnapMirror-Beziehungen festlegen `-common-snapshot -schedule`. Standardmäßig beträgt der allgemeine Snapshot-Zeitplan für synchrone SnapMirror-Beziehungen eine Stunde. Sie können einen Wert zwischen 30 Minuten und zwei Stunden für den Snapshot-Zeitplan für synchrone SnapMirror-Beziehungen angeben.

Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für SnapMirror DR erstellt, die Netzwerkkomprimierung für Datentransfers ermöglicht:

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

Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für SnapVault erstellt:

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

Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für einheitliche Replizierung erstellt:

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

Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für die synchrone SnapMirror-Beziehung im StructSync-Modus erstellt:

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

Erfahren Sie mehr über `snapmirror policy create` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Für die Richtlinienarten „`Vault`“ und „`mmirror-Vault`“ müssen Sie Regeln definieren, die festlegen, welche Snapshots während der Initialisierung und Aktualisierung übertragen werden.

Verwenden Sie die `snapmirror policy show` Befehl, um zu überprüfen, ob die SnapMirror -Richtlinie erstellt wurde.

Erfahren Sie mehr über `snapmirror policy show` im "ONTAP-Befehlsreferenz" .

Definieren einer Regel für eine ONTAP SnapMirror-Richtlinie

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

Über diese Aufgabe

Jede Richtlinie mit dem `vault` Richtlinientyp oder `mirror-vault` muss über eine Regel verfügen, die angibt, welche Snapshots repliziert werden sollen. Die Regel `bi-monthly` gibt beispielsweise an, dass nur Snapshots repliziert werden sollen, denen das SnapMirror-Label zugewiesen `bi-monthly` ist. Sie geben das SnapMirror-Label an, wenn Sie die Snapshot-Richtlinie auf der Quelle konfigurieren.

Jeder Richtlinientyp ist einer oder mehreren systemdefinierten Regeln zugeordnet. Diese Regeln werden einer Richtlinie automatisch zugewiesen, wenn Sie ihren Richtlinientyp angeben. Die folgende Tabelle zeigt die systemdefinierten Regeln.

Systemdefinierte Regel	Wird in Richtlinientypen verwendet	Ergebnis
sm_erstellt	Asynchrone Spiegelung, Spiegelung/Vault, Sync, StrictSync	Ein von SnapMirror erstellter Snapshot wird bei der Initialisierung und Aktualisierung übertragen.

All_Source_Snapshots	Asynchrone Spiegelung	Neue Snapshots auf der Quelle werden bei der Initialisierung und Aktualisierung übertragen.
Täglich	Vault, Mirror-Vault	Neue Snapshots auf der Quelle mit dem SnapMirror-Label `daily` werden bei Initialisierung und Aktualisierung übertragen.
Wöchentlich	Vault, Mirror-Vault	Neue Snapshots auf der Quelle mit dem SnapMirror-Label `weekly` werden bei Initialisierung und Aktualisierung übertragen.
Monatlich	Mirror-Vault	Neue Snapshots auf der Quelle mit dem SnapMirror-Label `monthly` werden bei Initialisierung und Aktualisierung übertragen.
Applikationskonsistent	Sync, StrictSync	Snapshots mit dem SnapMirror-Label `app_consistent` auf der Quelle werden synchron auf das Ziel repliziert. Unterstützt ab ONTAP 9.7.

Mit Ausnahme des Richtlinientyps „`async-Mirror`“ können Sie bei Bedarf zusätzliche Regeln für Standard- oder benutzerdefinierte Richtlinien festlegen. Beispiel:

- Für die Standardrichtlinie `MirrorAndVault` können Sie eine Regel erstellen, die aufgerufen wird `bi-monthly`, um Snapshots auf der Quelle mit dem SnapMirror-Label abzugleichen. `bi-monthly`
- Für eine benutzerdefinierte Richtlinie mit dem `mirror-vault` Richtlinientyp können Sie eine Regel erstellen, die aufgerufen wird, um Snapshots auf der Quelle mit dem `bi-weekly` SnapMirror-Label abzugleichen `bi-weekly`.

Schritt

1. Definieren Sie eine Regel für eine Richtlinie:

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

   Im folgenden Beispiel wird `bi-monthly` der Standardrichtlinie eine Regel mit dem Label SnapMirror hinzugefügt `MirrorAndVault`:

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

   Im folgenden Beispiel wird `bi-weekly` der benutzerdefinierten `my_snapvault` Richtlinie eine Regel mit der Beschriftung „SnapMirror“ hinzugefügt:

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

Im folgenden Beispiel wird `app_consistent` der benutzerdefinierten `Sync` Richtlinie eine Regel mit der Beschriftung „SnapMirror“ hinzugefügt:

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

Erfahren Sie mehr über `snapmirror policy add-rule` in der "ONTAP-Befehlsreferenz".

Anschließend können Sie Snapshots vom Quellcluster replizieren, die mit dem SnapMirror-Label übereinstimmen:

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

Definieren Sie einen ONTAP SnapMirror Zeitplan, um eine lokale Kopie auf dem Ziel zu erstellen

Bei SnapVault- und vereinheitlichten Replizierungsbeziehungen können Sie sich durch Erstellen einer Kopie des zuletzt übertragenen Snapshots vor der Beschädigung eines aktualisierten Snapshots am Ziel schützen. Diese „lokale Kopie“ wird unabhängig von den Aufbewahrungsregeln auf der Quelle aufbewahrt, so dass auch wenn der ursprünglich von SnapMirror übertragene Snapshot nicht mehr auf der Quelle verfügbar ist, eine Kopie davon auf dem Zielort verfügbar ist.

Über diese Aufgabe

Den Zeitplan für die Erstellung einer lokalen Kopie legen Sie im `-schedule` Option der `snapmirror policy add-rule` Befehl.

Schritt

1. Legen Sie einen Zeitplan für das Erstellen einer lokalen Kopie auf dem Ziel fest:

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

   Ein Beispiel zum Erstellen eines Jobplans finden Sie unter "Erstellen eines Replikationsauftragplans".

   Im folgenden Beispiel wird ein Zeitplan zum Erstellen einer lokalen Kopie zur Standardrichtlinie hinzugefügt `MirrorAndVault`:

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

Im folgenden Beispiel wird ein Zeitplan zum Erstellen einer lokalen Kopie zur benutzerdefinierten `my_unified` Richtlinie hinzugefügt:

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

Erfahren Sie mehr über `snapmirror policy add-rule` in der "ONTAP-Befehlsreferenz".

Eine ONTAP SnapMirror Replizierungsbeziehung anlegen

Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als *„Data Protection Relationship“ bezeichnet.* Sie können mit dem `snapmirror create` Befehl Datensicherungsbeziehungen für SnapMirror DR, SnapVault oder einheitliche Replizierung erstellen.

> Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um eine Replikationsbeziehung zu erstellen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Ab ONTAP 9.11.1 können Sie mit System Manager vorkonfigurierte und individuelle Mirror- und Vault-Richtlinien auswählen, ältere Richtlinien anzeigen und auswählen und die in einer Sicherungsrichtlinie definierten Übertragungszeitpläne überschreiben, wenn Volumes und Storage VMs geschützt sind. Diese Funktion ist auch in ONTAP 9.8P12 und späteren Patches für ONTAP 9.8 verfügbar.

> Wenn Sie ONTAP 9.8P12 oder höher ONTAP 9.8 Patch Release verwenden und SnapMirror mit System Manager konfiguriert haben, sollten Sie die Patch-Releases von ONTAP 9.9.1P13 oder höher und ONTAP 9.10.1P10 oder höher verwenden, wenn Sie ein Upgrade auf ONTAP 9.9.1 oder ONTAP 9.10.1 Versionen planen.

Bevor Sie beginnen

- Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.

  "Cluster- und SVM-Peering"

- Die Sprache auf dem Zielvolume muss mit der Sprache auf dem Quellvolume übereinstimmen.

Über diese Aufgabe

Bis ONTAP 9.3 verwendete SnapMirror im DP-Modus aufgerufen und im XDP-Modus aufgerufen, verschiedene Replizierungs-Engines mit verschiedenen Ansätzen für die Versionsabhängigkeit:

- SnapMirror rief im DP-Modus eine *versionsabhängige* Replizierungsmodul ins Einsatz, bei der die ONTAP Version auf dem primären und sekundären Storage identisch sein musste:

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

- Im XDP-Modus rief SnapMirror eine *versionsflexible* Replizierungs-Engine zur Unterstützung

verschiedener ONTAP Versionen auf primärem und sekundärem Storage auf:

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

Dank der Performance-Verbesserungen überwiegen die bedeutenden Vorteile von versionsflexiblem SnapMirror den leichten Vorteil des Replizierungsdurchsatzes durch den versionsabhängigen Modus. Aus diesem Grund wurde ab ONTAP 9.3 der XDP-Modus als neue Standardeinstellung verwendet, und alle Aufrufe des DP-Modus auf der Kommandozeile oder in neuen oder bestehenden Skripten werden automatisch in den XDP-Modus konvertiert.

Bestehende Beziehungen sind nicht betroffen. Wenn bereits eine Beziehung vom Typ DP verwendet wird, ist diese weiterhin vom Typ DP. Die folgende Tabelle zeigt das Verhalten, das Sie erwarten können.

Wenn Sie angeben…	Der Typ ist…	Die Standardrichtlinie (wenn Sie keine Richtlinie angeben) lautet…
DATENSICHERUNG	XDP	MirrorAllSnapshots (SnapMirror DR)
Nichts	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	XDPStandard (SnapVault)

Siehe auch die Beispiele im nachfolgenden Verfahren.

Die einzigen Ausnahmen von der Konvertierung sind wie folgt:

- Beziehungen für SVM-Datensicherung setzen weiterhin den DP-Modus ein.

  Geben Sie XDP explizit an, um den XDP-Modus mit der Standardrichtlinie `MirrorAllSnapshots` zu erhalten.

- Beziehungen zur Lastfreigabe für den Datenschutz setzen die Standards weiterhin im DP-Modus um.
- Beziehungen zu SnapLock für Datensicherheit werden weiterhin im DP-Modus standardmäßig aktiviert.
- Explizite Aufrufe von DP setzen weiterhin den DP-Modus ein, wenn Sie die folgende clusterweite Option festlegen:

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

  Diese Option wird ignoriert, wenn Sie DP nicht explizit aufrufen.

Ab ONTAP 9.14.1 wird die `-backoff-level` Option zu den Befehlen , und hinzugefügt `snapmirror create` `snapmirror modify` `snapmirror restore` , um die Rückgabelevel pro Beziehung festzulegen. Die Option wird nur mit FlexVol SnapMirror Beziehungen unterstützt. Der optionale Befehl gibt die Ausschaltebene für SnapMirror aufgrund von Client-OPS an. Rückgabewerte können hoch, mittel oder keine sein. Der Standardwert ist High.

Ab ONTAP 9.5 werden synchrone SnapMirror Beziehungen unterstützt.

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

Schritte

Sie können System Manager oder die ONTAP CLI zum Erstellen einer Replizierungsbeziehung verwenden.

System Manager

1. Wählen Sie das zu schützenden Volume oder LUN aus: Klicken Sie auf **Storage > Volumes** oder **Storage > LUNs**, und klicken Sie dann auf den gewünschten Volume oder LUN-Namen.
2. Klicken Sie Auf Protect.
3. Wählen Sie das Ziel-Cluster und die Storage-VM aus.
4. Die asynchrone Richtlinie ist standardmäßig ausgewählt. Um eine synchrone Richtlinie auszuwählen, klicken Sie auf **Weitere Optionen**.
5. Klicken Sie Auf **Schutz**.
6. Klicken Sie auf die Registerkarte **SnapMirror (lokal oder Remote)** für das ausgewählte Volume oder LUN, um zu überprüfen, ob der Schutz korrekt eingerichtet ist.

CLI

1. Erstellen Sie im Zielcluster eine Replikationsbeziehung:

   Sie müssen die Variablen in Winkelklammern durch die erforderlichen Werte ersetzen, bevor Sie diesen Befehl ausführen.

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

   Der `schedule` Parameter ist beim Erstellen synchroner SnapMirror-Beziehungen nicht anwendbar.

   Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mithilfe der Standardrichtlinie erstellt `MirrorLatest`:

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

   Im folgenden Beispiel wird eine SnapVault-Beziehung mithilfe der Standardrichtlinie erstellt `XDPDefault`:

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

   Im folgenden Beispiel wird mithilfe der Standardrichtlinie eine einheitliche Replizierungsbeziehung erstellt `MirrorAndVault`:

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

Im folgenden Beispiel wird mithilfe der benutzerdefinierten `my_unified` Richtlinie eine einheitliche Replizierungsbeziehung erstellt:

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

Im folgenden Beispiel wird eine synchrone SnapMirror-Beziehung mithilfe der Standardrichtlinie erstellt `Sync`:

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

Im folgenden Beispiel wird eine synchrone SnapMirror-Beziehung mithilfe der Standardrichtlinie erstellt `StrictSync`:

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

Im folgenden Beispiel wird eine SnapMirror DR-Beziehung erstellt. Wenn der DP-Typ automatisch in XDP konvertiert wird und keine Richtlinie angegeben ist, wird standardmäßig die Richtlinie verwendet `MirrorAllSnapshots`:

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

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

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

Im folgenden Beispiel wird eine SnapMirror DR-Beziehung erstellt. Wenn keine Richtlinie angegeben ist, wird standardmäßig die `XDPDefault` Richtlinie wie folgt verwendet:

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

Im folgenden Beispiel wird eine synchrone SnapMirror-Beziehung zur vordefinierten Policy erstellt `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 von „App_consistent“ erstellt wird `snapmirror-label`.

Nachdem Sie fertig sind

`snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror Beziehung erstellt wurde.

Erfahren Sie mehr über `snapmirror show` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Erstellen und Löschen von SnapMirror Failover-Test-Volumes".

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Volume Backup mit SnapVault – Übersicht"

Verwandte Informationen

- "snapmirror erstellen"

Initialisieren Sie eine ONTAP SnapMirror Replizierungsbeziehung

Bei allen Beziehungstypen führt die Initialisierung einen *Baseline Transfer* durch: Es erstellt einen Snapshot des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die es auf das Ziel-Volume verweist. Andernfalls hängt der Inhalt der Übertragung von der Richtlinie ab.

Bevor Sie beginnen

Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.

"Cluster- und SVM-Peering"

Über diese Aufgabe

Initialisierung kann sehr zeitaufwendig sein. Möglicherweise möchten Sie den Basistransfer in Zeiten geringerer Auslastung durchführen.

Ab ONTAP 9.5 werden synchrone SnapMirror Beziehungen unterstützt.

Sie sollten sich darüber im Klaren sein, dass die Initialisierung nicht automatisch fortgesetzt wird, wenn ein Dateisystem aus irgendeinem Grund neu gestartet wird, z. B. bei einem Neustart des Knotens, einer Übernahme/Rückgabe oder einer Panik, sondern manuell neu gestartet werden muss.

Schritt

1. Initialisieren einer Replikationsbeziehung:

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

   Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf initialisiert `svm_backup`:

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

   Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Stellen Sie sicher, dass ein gemeinsamer Snapshot in einer ONTAP Mirror-Vault-Implementierung vorhanden ist

Sie können die `snapmirror snapshot-owner create` Befehl zum Speichern eines beschrifteten Snapshots auf dem sekundären Server in einer Mirror-Vault-Bereitstellung. Dadurch wird sichergestellt, dass für die Aktualisierung der Vault-Beziehung ein gemeinsamer Snapshot vorhanden ist.

Über diese Aufgabe

Wenn Sie eine kombinierte Mirror-Vault Fan-out- oder Kaskadenbereitstellung verwenden, sollten Sie beachten, dass Updates fehlschlagen, wenn kein gemeinsamer Snapshot auf den Quell- und Ziel-Volumes vorhanden ist.

Das ist nie ein Problem für die Spiegelbeziehung in einer Fan-out- oder Kaskadenimplementierung, da SnapMirror vor der Aktualisierung immer einen Snapshot des Quell-Volumes erstellt.

Es kann jedoch ein Problem für die Vault-Beziehung sein, da SnapMirror bei Aktualisierung einer Vault-Beziehung keinen Snapshot des Quell-Volumes erstellt. Sie müssen den verwenden `snapmirror snapshot-owner create`, um sicherzustellen, dass es mindestens einen gemeinsamen Snapshot sowohl auf der Quelle als auch auf dem Ziel der Vault-Beziehung gibt. "Weitere Informationen zu Fan-out- und Kaskadenimplementierungen für die Datensicherung".

Schritte

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

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

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

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

Erfahren Sie mehr über `snapmirror snapshot-owner create` im "ONTAP-Befehlsreferenz" .

2. Aktualisieren Sie die Spiegelbeziehung, wie in beschrieben"Manuelles Aktualisieren einer Replikationsbeziehung".

   Alternativ können Sie auf die geplante Aktualisierung der Spiegelbeziehung warten.

3. Den beschrifteten Snapshot an das Vault-Ziel übertragen:

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

   Im folgenden Beispiel wird der Snapshot übertragen `snap1`

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   -source-snapshot snap1
   ```

   Der beschriftete Snapshot wird beibehalten, wenn die Vault-Beziehung aktualisiert wird.

   Erfahren Sie mehr über `snapmirror update` in der "ONTAP-Befehlsreferenz".

4. Entfernen Sie auf dem Quell-Volume den Eigentümer aus dem beschrifteten Snapshot:

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

   In den folgenden Beispielen wird als Eigentümer des `snap1` Snapshots entfernt `ApplicationA`:

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

   Erfahren Sie mehr über `snapmirror snapshot-owner delete` in der "ONTAP-Befehlsreferenz".

Beispiel: Konfiguration einer ONTAP SnapMirror Vault-Vault-Kaskade

Ein Beispiel zeigt in konkreten Worten, wie Sie Replikationsbeziehungen nacheinander konfigurieren können. Sie können die im Beispiel konfigurierte Vault-Vault-Kaskadenbereitstellung verwenden, um mehr als 251 Snapshots mit der Bezeichnungzu

erhalten `my-weekly`.

Bevor Sie beginnen

Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.

Über diese Aufgabe

Im Beispiel wird Folgendes vorausgesetzt:

- Sie haben Snapshots auf dem Quellcluster mit den SnapMirror-Labels, , `my-weekly` und `my-monthly` konfiguriert `my-daily`.
- Sie haben Zielvolumes mit dem Namen auf den sekundären und tertiären Zielclustern konfiguriert `volA`.
- Sie haben Zeitpläne für Replikationsjobs konfiguriert, die auf den sekundären und tertiären Zielclustern benannt `my_snapvault` sind.

Das Beispiel zeigt, wie Replikationsbeziehungen auf Grundlage von zwei benutzerdefinierten 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. Überprüfen Sie auf dem sekundären Ziel-Cluster die Richtlinie:

   ```
   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. Erstellen Sie auf dem sekundären Ziel-Cluster die Beziehung zum Quell-Cluster:

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

7. Initialisieren Sie auf dem sekundären Ziel-Cluster die Beziehung mit dem Quell-Cluster:

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

8. Erstellen Sie auf dem tertiären Zielcluster die `snapvault_tertiary` folgende Richtlinie:

   ```
   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 Zielcluster 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. Überprüfen Sie auf dem tertiären Ziel-Cluster die Richtlinie:

```
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. Initialisieren Sie auf dem tertiären Ziel-Cluster die Beziehung mit dem sekundären Cluster:

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

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror Initialisierung"
- "Snapmirror-Richtlinie Add-Rule"
- "Snapmirror-Richtlinie erstellen"
- "Snapmirror-Richtlinien-Show"

Managen Sie die SnapMirror Volume-Replizierung

Konvertieren einer vorhandenen ONTAP SnapMirror-DP-Beziehung in XDP

Wenn Sie ein Upgrade auf ONTAP 9.12.1 oder höher durchführen, müssen Sie DP-

Beziehungen in XDP konvertieren, bevor Sie ein Upgrade durchführen. ONTAP 9.12.1 und höher unterstützt keine DP-Beziehungen. Kunden können bestehende DP-Beziehungen einfach in XDP konvertieren und so von versionsflexiblem SnapMirror profitieren.

Vor dem Upgrade auf ONTAP 9.12.1 müssen Sie bestehende DP-Beziehungen in XDP konvertieren, bevor Sie ein Upgrade auf ONTAP 9.12.1 und neuere Versionen durchführen können.

Über diese Aufgabe

- SnapMirror konvertiert vorhandene DP-Beziehungen nicht automatisch in XDP. Um die Beziehung umzuwandeln, müssen Sie die bestehende Beziehung unterbrechen und löschen, eine neue XDP-Beziehung erstellen und die Beziehung neu synchronisieren.
- Bei der Planung der Konvertierung sollten Sie beachten, dass die Vorarbeit und die Data Warehousing-Phase einer XDP-SnapMirror-Beziehung viel Zeit in Anspruch nehmen können. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „Vorbereitung“ für einen längeren Zeitraum meldet.

> Nachdem Sie einen SnapMirror Beziehungstyp von DP in XDP konvertiert haben, werden die speicherplatzsparenden Einstellungen, wie Autosize und Platzgarantie, nicht mehr zum Ziel repliziert.

Schritte

1. Aus dem Ziel-Cluster, sicherstellen, dass die SnapMirror-Beziehung vom Typ DP ist, dass der Mirror-Zustand SnapMirrored ist, der Beziehungsstatus ist Idle, und die Beziehung ist gesund:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   Im folgenden Beispiel wird die Ausgabe des `snapmirror show` Befehls angezeigt:

```
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
```

Vielleicht finden Sie es hilfreich, eine Kopie der `snapmirror show` Befehlsausgabe aufzubewahren, um den vorhandenen Überblick über die Beziehungseinstellungen zu behalten. Erfahren Sie mehr über `snapmirror show` in der "ONTAP-Befehlsreferenz".

2. Stellen Sie von den Quell- und Zielvolumes sicher, dass beide Volumes einen gemeinsamen Snapshot haben:

```
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 Updates während der Konvertierung nicht ausgeführt werden, müssen die bestehende DP-Typ-Beziehung stillgelegt werden:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf stillgelegt `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Erfahren Sie mehr über `snapmirror quiesce` in der "ONTAP-Befehlsreferenz".

4. Bestehende DP-TYPE Beziehung aufbrechen:

```
snapmirror break -destination-path <SVM:volume>
```

Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf unterbrochen `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

5. Wenn das automatische Löschen von Snapshots auf dem Zielvolume aktiviert ist, deaktivieren Sie es:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

Im folgenden Beispiel wird das automatische Löschen von Snapshots auf dem Zielvolume deaktiviert `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Vorhandene DP-Typ-Beziehung löschen:

```
snapmirror delete -destination-path <SVM:volume>
```

Erfahren Sie mehr über `snapmirror-delete` in der "ONTAP-Befehlsreferenz".

Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf gelöscht `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Freigabe der Disaster-Recovery-Beziehung der SVM an der Quelle:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

Im folgenden Beispiel werden die Disaster-Recovery-Beziehung für SVM veröffentlicht:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

Erfahren Sie mehr über `snapmirror release` in der "ONTAP-Befehlsreferenz".

8. Sie können die Ausgabe, die Sie aus dem `snapmirror show` Befehl erhalten 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. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

Im folgenden Beispiel wird unter SnapMirror `volA svm1 volA_dst svm_backup` Verwendung der Standardrichtlinie eine Disaster Recovery-Beziehung zwischen dem Quell-Volume auf und dem Ziel-Volume erstellt `MirrorAllSnapshots`:

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

9. Neusynchronisierung der Quell- und Ziel-Volumes:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Um die Resynchronisierungszeit zu verbessern, können Sie die `-quick-resync` Option, Sie sollten sich jedoch darüber im Klaren sein, dass Einsparungen bei der Speichereffizienz verloren gehen können.

> Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen. Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf neu synchronisiert `svm_backup`:

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

Erfahren Sie mehr über `snapmirror resync` im "ONTAP-Befehlsreferenz" .

10. Wenn Sie das automatische Löschen von Snapshots deaktiviert haben, aktivieren Sie es erneut:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Nachdem Sie fertig sind

1. `snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror Beziehung erstellt wurde.

   Erfahren Sie mehr über `snapmirror show` in der "ONTAP-Befehlsreferenz".

2. Sobald das SnapMirror XDP-Ziellaufwerk mit der Aktualisierung der Snapshots gemäß der SnapMirror-Richtlinie beginnt, verwenden Sie die Befehlsausgabe `snapmirror list-destinations` des Befehls aus dem Quellcluster, um die neue SnapMirror XDP-Beziehung anzuzeigen.

Weitere Informationen zu DP-Beziehungen

Ab ONTAP 9.3 ist der XDP-Modus der Standard, und alle Aufrufe des DP-Modus auf der Befehlszeile oder in neuen oder vorhandenen Skripten werden automatisch in den XDP-Modus konvertiert.

Bestehende Beziehungen sind nicht betroffen. Wenn bereits eine Beziehung vom Typ DP verwendet wird, ist diese weiterhin vom Typ DP. Ab ONTAP 9.5 ist MirrorAndVault die Standardrichtlinie, wenn kein Datenschutzmodus angegeben ist oder wenn der XDP-Modus als Beziehungstyp angegeben ist. Die folgende Tabelle zeigt das erwartete Verhalten.

Wenn Sie angeben…	Der Typ ist…	Die Standardrichtlinie (wenn Sie keine Richtlinie angeben) lautet…

DATENSICHERUNG	XDP	MirrorAllSnapshots (SnapMirror DR)
Nichts	XDP	MirrorAndVault (einheitliche Replizierung)
XDP	XDP	MirrorAndVault (einheitliche Replizierung)

Wie die Tabelle zeigt, stellen die Standardrichtlinien, die XDP unter verschiedenen Umständen zugewiesen sind, sicher, dass die Konvertierung die funktionale Äquivalenz der vorherigen Typen beibehält. Natürlich können Sie je nach Bedarf unterschiedliche Richtlinien verwenden, einschließlich Richtlinien für eine einheitliche Replizierung:

Wenn Sie angeben…	Und die Richtlinie lautet…	Ihr Ergebnis ist…
DATENSICHERUNG	MirrorAllSnapshots	SnapMirror DR
XDPStandard	SnapVault	MirrorAndVault
Einheitliche Replizierung	XDP	MirrorAllSnapshots
SnapMirror DR	XDPStandard	SnapVault

Die einzigen Ausnahmen von der Konvertierung sind wie folgt:

- Beziehungen für die SVM-Datensicherung setzen weiterhin in ONTAP 9.3 und früher den DP-Modus ein.

  Seit ONTAP 9.4 ist bei den SVM-Datensicherungsbeziehungen standardmäßig der XDP-Modus aktiviert.

- Beziehungen zwischen Root-Volumes zum Load-Sharing von Daten werden weiterhin standardmäßig im DP-Modus eingesetzt.
- Beziehungen zu SnapLock zur Datensicherung setzen weiterhin im DP-Modus in ONTAP 9.4 und früher ein.

  Ab ONTAP 9.5 ist bei SnapLock-Datensicherungsbeziehungen der XDP-Modus standardmäßig aktiviert.

- Explizite Aufrufe von DP setzen weiterhin den DP-Modus ein, wenn Sie die folgende clusterweite Option festlegen:

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

  Diese Option wird ignoriert, wenn Sie DP nicht explizit aufrufen.

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror löschen"

- "Snapmirror-Ruhezustand"
- "snapmirror Release"
- "SnapMirror-Neusynchronisierung"

Konvertieren Sie den Typ einer ONTAP SnapMirror-Beziehung

Ab ONTAP 9.5 wird SnapMirror Synchronous unterstützt. Sie können eine asynchrone SnapMirror-Beziehung in eine synchrone SnapMirror-Beziehung oder umgekehrt konvertieren, ohne einen Basistransfer durchzuführen.

Über diese Aufgabe

Sie können eine asynchrone SnapMirror-Beziehung nicht in eine synchrone SnapMirror-Beziehung umwandeln oder umgekehrt, indem Sie die SnapMirror-Richtlinie ändern.

Schritte

- **Umwandlung einer asynchronen SnapMirror-Beziehung in eine synchrone SnapMirror-Beziehung**

  a. Löschen Sie im Ziel-Cluster die asynchrone SnapMirror-Beziehung:

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. Geben Sie aus dem Quell-Cluster die SnapMirror-Beziehung frei, 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. Erstellen Sie aus dem Ziel-Cluster eine synchrone SnapMirror-Beziehung:

  ```
  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. Synchrone SnapMirror-Beziehung erneut synchronisieren:

  ```
  snapmirror resync -destination-path <destination_SVM:destination_volume>
  ```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- **Konvertierung einer synchronen SnapMirror-Beziehung in eine asynchrone SnapMirror-Beziehung**

  a. Beenden Sie aus dem Ziel-Cluster die vorhandene synchrone SnapMirror-Beziehung:

  `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

  ```
  cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
  ```

  b. Löschen Sie im Ziel-Cluster die asynchrone SnapMirror-Beziehung:

  `snapmirror delete -destination-path <SVM:volume>`

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  c. Geben Sie aus dem Quell-Cluster die SnapMirror-Beziehung frei, 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. Erstellen Sie aus dem Ziel-Cluster eine asynchrone SnapMirror-Beziehung:

  `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. Synchrone SnapMirror-Beziehung erneut synchronisieren:

  `snapmirror resync -destination-path <destination_SVM:destination_volume>`

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror löschen"
- "Snapmirror-Ruhezustand"
- "snapmirror Release"

- "SnapMirror-Neusynchronisierung"

Konvertieren Sie den Modus einer synchronen ONTAP SnapMirror-Beziehung

Ab ONTAP 9.5 werden synchrone SnapMirror Beziehungen unterstützt. Sie können den Modus einer synchronen SnapMirror-Beziehung von StructSync in Sync umwandeln oder umgekehrt.

Über diese Aufgabe

Sie können die Richtlinie einer synchronen SnapMirror-Beziehung nicht ändern, um ihren Modus zu konvertieren.

Schritte

1. Beenden Sie aus dem Ziel-Cluster die vorhandene synchrone SnapMirror-Beziehung:

   `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
   ```

2. Löschen Sie auf dem Ziel-Cluster die vorhandene synchrone SnapMirror-Beziehung:

   `snapmirror delete -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror delete -destination-path vs1_dr:vol1
   ```

3. Geben Sie aus dem Quell-Cluster die SnapMirror-Beziehung frei, 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. Erstellen Sie aus dem Ziel-Cluster eine synchrone SnapMirror-Beziehung, indem Sie den Modus angeben, in den Sie die synchrone SnapMirror-Beziehung konvertieren möchten:

   `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. Synchronisieren Sie die SnapMirror Beziehung vom Ziel-Cluster neu:

```
snapmirror resync -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror löschen"
- "Snapmirror-Ruhezustand"
- "snapmirror Release"
- "SnapMirror-Neusynchronisierung"

Erstellen und Löschen von ONTAP SnapMirror-Failover-Test-Volumes

Ab ONTAP 9.14.1 können Sie mit System Manager einen Volume-Klon erstellen und SnapMirror Failover und Disaster Recovery testen, ohne die aktive SnapMirror Beziehung zu unterbrechen. Nach Abschluss des Tests können Sie die zugehörigen Daten bereinigen und das Testvolumen löschen.

Erstellung eines SnapMirror Failover-Test-Volumes

Über diese Aufgabe

- Sie können Failover-Tests für synchrone und asynchrone SnapMirror Beziehungen durchführen.
- Zur Durchführung des Disaster-Recovery-Tests wird ein Volume-Klon erstellt.
- Das Klon-Volume wird auf derselben Storage-VM wie das SnapMirror Ziel erstellt.
- FlexVol und FlexGroup SnapMirror Beziehungen können genutzt werden.
- Wenn für die ausgewählte Beziehung bereits ein Testklon vorhanden ist, können Sie keinen weiteren Klon für diese Beziehung erstellen.
- SnapLock Vault-Beziehungen werden nicht unterstützt.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein.
- Die SnapMirror Lizenz muss auf dem Quell- und Ziel-Cluster installiert sein.

Schritte

1. Wählen Sie auf dem Zielcluster **Schutz > Beziehungen** aus.
2. Wählen Sie ⋮ neben der Beziehungsquelle und wählen Sie **Failover testen**.
3. Wählen Sie im Fenster **Test Failover Test Failover** aus.
4. Wählen Sie **Storage > Volumes** aus, und überprüfen Sie, ob das Test-Failover-Volume aufgeführt ist.
5. Wählen Sie **Storage > Shares**.
6. Wählen Sie + Add **Share**.
7. Geben Sie im Fenster **Share hinzufügen** einen Namen für die Freigabe in das Feld **Share Name** ein.
8. Wählen Sie im Feld **Ordner Durchsuchen**, wählen Sie das Testklonvolume und **Speichern** aus.

9. Wählen Sie unten im Fenster **Share hinzufügen Save**.
10. Suchen Sie im Fensterbereich **Speicher > Freigaben** die erstellte Freigabe und wählen Sie aus, ⌄ um die Freigabeinformationen anzuzeigen.
11. Kopieren oder notieren Sie unter **SMB/CIFS Access** den Zugriffspfad für die Freigabe, z. B. `\\123.456.7.890\failover_test`.
12. Verwenden Sie den SMB-Zugriffspfad, um die Freigabe auf dem Client zu öffnen und sicherzustellen, dass das Test-Volume Lese- und Schreibfunktionen besitzt.

Bereinigen Sie die Failover-Daten, und löschen Sie das Test-Volume

Nachdem Sie die Failover-Tests abgeschlossen haben, können Sie alle dem Test-Volume zugeordneten Daten bereinigen und löschen.

Schritte

1. Wählen Sie auf dem Zielcluster **Schutz > Beziehungen** aus.
2. Wählen Sie ⋮ neben der Beziehungsquelle die Option **Clean Up Test Failover**.
3. Wählen Sie im Fenster **Clean Up Test Failover Clean Up** aus.
4. Wählen Sie **Storage > Volumes** aus, und überprüfen Sie, ob das Testvolume gelöscht wurde.

Stellen Sie Daten von einem SnapMirror DR-Ziel-Volume bereit

Das ONTAP SnapMirror-Ziel-Volume kann beschrieben werden

Sie müssen das Ziel-Volume schreibbar machen, bevor Sie Daten vom Volume an die Clients bereitstellen können. Um Daten von einem gespiegelten Ziel aus bereitzustellen, wenn eine Quelle nicht mehr verfügbar ist, beenden Sie geplante Transfers zum Ziel, und unterbrechen Sie anschließend die SnapMirror Beziehung, um das Ziel beschreibbar zu machen.

Über diese Aufgabe

Sie müssen diese Aufgabe über die Ziel-SVM oder das Ziel-Cluster ausführen.

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um ein Ziel-Volume beschreibbar zu machen.

System Manager

1. Wählen Sie die Schutzbeziehung aus: Klicken Sie auf **Schutz > Beziehungen**, und klicken Sie dann auf den gewünschten Volume-Namen.
2. Klicken Sie Auf ⋮.
3. Geplante Transfers stoppen : Klicken Sie **Pause**.
4. Machen Sie das Ziel beschreibbar: Klicken Sie auf **break**.
5. Gehen Sie zur Hauptseite **Relationships**, um zu überprüfen, ob der Beziehungsstatus als „unterbrochen“ angezeigt wird.

Nächste Schritte

Sie müssen "Die Replikationsbeziehung erneut synchronisieren" ein Ziel-Volume schreiben lassen.

Wenn das deaktivierte Quell-Volume wieder verfügbar ist, sollten Sie die Beziehung erneut synchronisieren, um die aktuellen Daten auf das ursprüngliche Quell-Volume zu kopieren.

CLI

1. Geplante Transfers zum Ziel anhalten:

   ```
   snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   Im folgenden Beispiel werden geplante Transfers zwischen dem Quell-Volume `volA` `svm1` `volA_dst` am und dem Ziel-Volume am angehalten `svm_backup`:

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

   Erfahren Sie mehr über `snapmirror quiesce` in der "ONTAP-Befehlsreferenz".

2. Laufende Transfers zum Ziel anhalten:

   ```
   snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   ⓘ Dieser Schritt ist für synchrone SnapMirror-Beziehungen (ab ONTAP 9.5 unterstützt) nicht erforderlich.

   Das folgende Beispiel stoppt laufende Transfers zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf `svm_backup`:

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

Erfahren Sie mehr über `snapmirror abort` in der "ONTAP-Befehlsreferenz".

3. SnapMirror DR-Beziehung unterbrechen:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf unterbrochen `svm_backup`:

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

Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

Nächste Schritte

Sie müssen "Synchronisieren Sie die Replikationsbeziehung erneut" ein Ziel-Volume schreiben lassen.

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Übersicht über die Disaster Recovery von Volumes"

Konfigurieren Sie das ONTAP SnapMirror Ziel-Volume für den Datenzugriff

Nachdem das Ziel-Volume schreibbar gemacht wurde, muss das Volume für den Datenzugriff konfiguriert werden. NAS-Clients, NVMe-Subsystem und SAN-Hosts können auf die Daten vom Ziel-Volume zugreifen, bis das Quell-Volume wieder aktiviert ist.

NAS-Umgebung:

1. Mounten Sie das NAS-Volume mithilfe desselben Verbindungspfads, an den das Quell-Volume in der Quell-SVM angehängt war, in den Namespace.
2. Wenden Sie die entsprechenden ACLs auf die SMB-Freigaben am Ziel-Volume an.
3. Weisen Sie die NFS-Exportrichtlinien dem Ziel-Volume zu.
4. Wenden Sie die Kontingentregeln auf das Ziel-Volume an.
5. Leiten Sie die Clients an das Ziel-Volume weiter.
6. NFS- und SMB-Freigaben erneut auf den Clients einbinden.

SAN-Umgebung:

1. Ordnen Sie die LUNs im Volume der entsprechenden Initiatorgruppe zu.
2. Erstellen Sie für iSCSI-Sitzungen von den SAN-Host-Initiatoren zu den SAN-LIFs.

3. Führen Sie auf dem SAN-Client einen erneuten Speicherscan durch, um die verbundenen LUNs zu erkennen.

Weitere Informationen zur NVMe Umgebung finden Sie unter "SAN Administration".

Aktivieren Sie das ursprüngliche ONTAP SnapMirror-Quell-Volume erneut

Sie können die ursprüngliche Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes wiederherstellen, wenn Sie nicht mehr Daten vom Bestimmungsort bereitstellen müssen.

Über diese Aufgabe

- Für das folgende Verfahren wird vorausgesetzt, dass die Basis im ursprünglichen Quell-Volume intakt ist. Wenn die Baseline nicht intakt ist, müssen Sie die Beziehung zwischen dem Volume, das Sie Daten vom und dem ursprünglichen Quell-Volume bereitstellen, erstellen und initialisieren, bevor Sie den Vorgang durchführen.
- Die Hintergrundvorbereitung und die Data Warehousing-Phase einer XDP-SnapMirror-Beziehung nehmen viel Zeit in Anspruch. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „Vorbereitung“ für einen längeren Zeitraum meldet.

Schritte

1. Umkehren der ursprünglichen Datensicherungsbeziehung:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Erfahren Sie mehr über `snapmirror resync` in der "ONTAP-Befehlsreferenz".

   > Sie müssen diesen Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausführen. Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen. Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein allgemeiner Snapshot vorhanden ist. Verwenden Sie `snapmirror initialize` , um die Beziehung neu zu initialisieren. Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

   Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Quellvolume, `volA` auf `svm1`, und dem Volumen, von dem Sie Daten bereitstellen, `volA_dst` auf umgekehrt `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. Wenn Sie bereit sind, den Datenzugriff zur Originalquelle wiederherzustellen, stoppen Sie den Zugriff auf das ursprüngliche Ziel-Volume. Eine Möglichkeit besteht darin, die ursprüngliche Ziel-SVM zu stoppen:

   `vserver stop -vserver` *`SVM`*

Sie müssen diesen Befehl von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster ausführen. Dieser Befehl verhindert den Benutzerzugriff auf die gesamte ursprüngliche Ziel-SVM. Sie können den Zugriff auf das ursprüngliche Ziellaufwerk mithilfe anderer Methoden beenden.

Im folgenden Beispiel wird die ursprüngliche Ziel-SVM angehalten:

```
cluster_dst::> vserver stop svm_backup
```

Erfahren Sie mehr über `vserver stop` in der "ONTAP-Befehlsreferenz".

3. Aktualisierung der umgekehrten Beziehung:

`snapmirror update -source-path SVM:volume -destination-path SVM:volume`

Sie müssen diesen Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausführen.

Das folgende Beispiel aktualisiert die Beziehung zwischen dem Volumen, das Sie Daten von, `volA_dst` auf `svm_backup`, und dem ursprünglichen Quell-Volume `volA` auf bereitstellen `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Erfahren Sie mehr über `snapmirror update` in der "ONTAP-Befehlsreferenz".

4. Halten Sie geplante Transfers von der ursprünglichen SVM oder dem ursprünglichen Quell-Cluster für die umgekehrte Beziehung ab:

`snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

Sie müssen diesen Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausführen.

Im folgenden Beispiel werden geplante Übertragungen zwischen dem ursprünglichen Zielvolume, `volA_dst` ein `svm_backup` und dem ursprünglichen Quellvolume `volA` am gestoppt `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Erfahren Sie mehr über `snapmirror quiesce` in der "ONTAP-Befehlsreferenz".

5. Wenn das endgültige Update abgeschlossen ist und die Beziehung für den Beziehungsstatus „stillgelegt“ anzeigt, führen Sie den folgenden Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster aus, um die umgekehrte Beziehung zu unterbrechen:

`snapmirror break -source-path SVM:volume -destination-path SVM:volume`

> Sie müssen diesen Befehl von der ursprünglichen Quell-SVM oder dem Quell-Cluster ausführen.

Das folgende Beispiel bricht 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
```

Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

6. Löschen Sie in der ursprünglichen SVM oder dem ursprünglichen Quell-Cluster die verkehrte Datensicherungsbeziehung:

`snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

> Sie müssen diesen Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausführen.

Im folgenden Beispiel wird die umgekehrte Beziehung zwischen dem ursprünglichen Quellvolume, `volA` ON `svm1`, und dem Volumen, von dem Sie Daten bereitstellen, `volA_dst` auf gelöscht `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Erfahren Sie mehr über `snapmirror delete` in der "ONTAP-Befehlsreferenz".

7. Lassen Sie die umgekehrte Beziehung von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster los.

`snapmirror release -source-path SVM:volume -destination-path SVM:volume`

> Sie müssen diesen Befehl von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster ausführen.

Im folgenden Beispiel wird die umgekehrte Beziehung zwischen dem ursprünglichen Zielvolume, `volA_dst svm_backup volA` auf , und dem ursprünglichen Quellvolume auf freigegeben `svm1`:

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

Erfahren Sie mehr über `snapmirror release` in der "ONTAP-Befehlsreferenz".

8. Wiederherstellung der ursprünglichen Datensicherungsbeziehung vom ursprünglichen Zielort:

`snapmirror resync -source-path SVM:volume -destination-path SVM:volume`

Das folgende Beispiel stellt die Beziehung zwischen dem ursprünglichen Quell-Volume, `volA svm1 volA_dst` auf , und dem ursprünglichen Ziel-Volume wieder her, auf `svm_backup`:

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

Erfahren Sie mehr über `snapmirror resync` in der "ONTAP-Befehlsreferenz".

9. Starten Sie bei Bedarf die ursprüngliche Ziel-SVM:

`vserver start -vserver SVM`

Im folgenden Beispiel wird die ursprüngliche Ziel-SVM gestartet:

```
cluster_dst::> vserver start svm_backup
```

Erfahren Sie mehr über `vserver start` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

```
`snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror
Beziehung erstellt wurde.
```

Erfahren Sie mehr über `snapmirror show` in der "ONTAP-Befehlsreferenz".

Wiederherstellung von Dateien aus einem SnapMirror Ziel-Volume

Wiederherstellung einer Datei, einer LUN oder eines NVMe Namespace aus einem ONTAP SnapMirror-Ziel

Sie können eine einzelne Datei, eine LUN, einen Satz von Dateien oder LUNs aus einem Snapshot oder einen NVMe-Namespace von einem SnapMirror-Ziel-Volume wiederherstellen. Ab ONTAP 9.7 können auch NVMe-Namespaces von einem synchronen SnapMirror-Ziel wiederhergestellt werden. Sie können Dateien auf dem ursprünglichen Quell-Volume oder auf einem anderen Volume wiederherstellen.

Bevor Sie beginnen

Um eine Datei oder LUN von einem synchronen SnapMirror-Ziel wiederherzustellen (unterstützt ab ONTAP 9.5), müssen Sie zuerst die Beziehung löschen und freigeben.

Über diese Aufgabe

Das Volume, auf dem Sie Dateien oder LUNs wiederherstellen (das Zielvolume), muss ein Lese-/Schreib-Volume sein:

- SnapMirror führt eine *inkrementelle Wiederherstellung* durch, wenn die Quell- und Ziel-Volumes einen gemeinsamen Snapshot haben (wie es normalerweise der Fall ist, wenn Sie auf das ursprüngliche Quell-

Volume wiederherstellen).

- Andernfalls führt SnapMirror eine *Baseline restore* durch, in der der angegebene Snapshot und alle Datenblöcke, auf die er sich bezieht, an das Ziel-Volume übertragen werden.

Schritte

1. Führen Sie die Snapshots im Zielvolume auf:

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

   Erfahren Sie mehr über `volume snapshot show` in der "ONTAP-Befehlsreferenz".

   Im folgenden Beispiel werden die Snapshots auf dem Ziel angezeigt `vserverB:secondary1`:

```
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. Stellen Sie eine einzelne Datei oder eine LUN oder einen Satz von Dateien oder LUNs aus einem Snapshot in einem SnapMirror-Zielvolume wieder her:

   `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>`

   Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

   Mit dem folgenden Befehl werden die Dateien und `file2` vom Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` an der gleichen Stelle im aktiven Dateisystem des ursprünglichen

Quellvolume `primary1` wiederhergestellt `file1`:

```
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
```

Mit dem folgenden Befehl werden die Dateien und `file2` vom Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` an einen anderen Speicherort im aktiven Dateisystem des ursprünglichen Quellvolume `primary1` wiederhergestellt `file1`.

Der Zieldateipfad beginnt mit dem Symbol @, gefolgt vom Pfad der Datei aus dem Stammverzeichnis des ursprünglichen Quell-Volumes. In diesem Beispiel `file1` wird in wiederhergestellt `/dir1/file1.new`, und file2 wird wiederhergestellt auf `/dir2.new/file2` `primary1`:

```
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
```

Mit dem folgenden Befehl werden die Dateien `file1` und `file3` vom Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` an verschiedenen Orten im aktiven Dateisystem des ursprünglichen Quellvolume `primary1` wiederhergestellt und von `snap1` an demselben Ort im aktiven Dateisystem von `primary1` wiederhergestellt `file2`.

In diesem Beispiel `file1` wird die Datei wiederhergestellt `/dir1/file1.new` und `file3` wiederhergestellt in `/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 Wiederherstellung"

Sie können den Inhalt eines gesamten Volumes aus einem Snapshot auf einem SnapMirror-Ziel-Volume wiederherstellen. Sie können den Inhalt des Volumes auf dem ursprünglichen Quell-Volume oder auf einem anderen Volume wiederherstellen.

Über diese Aufgabe

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um Daten wiederherzustellen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Das Ziel-Volume für den Wiederherstellungsvorgang muss einer der folgenden Werte aufweisen:

- Ein Lese-/Schreibvolume. In diesem Fall führt SnapMirror eine *inkrementelle Wiederherstellung* durch, vorausgesetzt, dass die Quell- und Zielvolumes einen gemeinsamen Snapshot haben (wie es normalerweise der Fall ist, wenn Sie das ursprüngliche Quellvolume wiederherstellen).

  Der Befehl schlägt fehl, wenn kein gemeinsamer Snapshot vorhanden ist. Sie können den Inhalt eines Volumes nicht auf einem leeren Lese-/Schreib-Volume wiederherstellen.

- Ein leeres Datensicherungs-Volume. In diesem Fall führt SnapMirror eine *Baseline restore* durch, in der der angegebene Snapshot und alle von ihm referenzierten Datenblöcke an das Quell-Volume übertragen werden.

Die Wiederherstellung des Inhalts eines Volumes ist eine Unterbrechung des Vorgangs. SMB Traffic darf nicht auf dem primären SnapVault Volume ausgeführt werden, wenn ein Wiederherstellungsvorgang ausgeführt wird.

Wenn auf dem Ziel-Volume für den Wiederherstellungsvorgang die Komprimierung aktiviert ist und auf dem Quell-Volume keine Komprimierung aktiviert ist, deaktivieren Sie die Komprimierung auf dem Ziel-Volume. Sie müssen die Komprimierung erneut aktivieren, nachdem der Wiederherstellungsvorgang abgeschlossen ist.

Alle für das Ziel-Volume definierten Kontingentregeln werden vor der Wiederherstellung deaktiviert. Sie können den `volume quota modify` Befehl verwenden, um Kontingentregeln neu zu aktivieren, nachdem die Wiederherstellung abgeschlossen ist.

Wenn Daten in einem Volume verloren gehen oder beschädigt werden, können Sie ein Rollback Ihrer Daten durchführen, indem Sie sie von einem früheren Snapshot wiederherstellen.

Dieses Verfahren ersetzt die aktuellen Daten auf dem Quell-Volume durch Daten aus einer früheren Snapshot-Version. Sie sollten diese Aufgabe für das Ziel-Cluster ausführen.

Schritte

Sie können die Inhalte eines Volumes mithilfe von System Manager oder der ONTAP CLI wiederherstellen.

System Manager

1. Klicken Sie auf **Schutz > Beziehungen** und dann auf den Namen des Quellvolumens.
2. Klicken Sie auf ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle** wird das Quell-Volume standardmäßig ausgewählt. Klicken Sie auf **anderes Volume**, wenn Sie ein anderes Volume als die Quelle auswählen möchten.
4. Wählen Sie unter **Destination** den Snapshot aus, den Sie wiederherstellen möchten.
5. Wenn sich Ihre Quelle und Ihr Ziel auf verschiedenen Clustern befinden, klicken Sie auf dem Remote-Cluster auf **Schutz > Beziehungen**, um den Wiederherstellungsfortschritt zu überwachen.

CLI

1. Führen Sie die Snapshots im Zielvolume auf:

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

Im folgenden Beispiel werden die Snapshots auf dem Ziel angezeigt `vserverB:secondary1`:

```
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. Wiederherstellen des Inhalts eines Volumes aus einem Snapshot in einem SnapMirror-Zielvolume:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
```

`<snapshot>`

> Sie müssen diesen Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster ausführen.

Mit dem folgenden Befehl wird der Inhalt des ursprünglichen Quelldatenträgers aus dem Snapshot `daily.2013-01-25_0010` im ursprünglichen Zielvolume `secondary1` wiederhergestellt `primary1`:

```
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. Mounten Sie das wiederhergestellte Volume erneut, und starten Sie alle Applikationen, die das Volume verwenden.

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Volume-Wiederherstellung mithilfe von SnapVault – Übersicht"

Verwandte Informationen

- "snapmirror Wiederherstellung"
- "Volume-Snapshot werden angezeigt"

Manuelles Aktualisieren einer ONTAP SnapMirror Replikationsbeziehung

Möglicherweise müssen Sie eine Replikationsbeziehung manuell aktualisieren, wenn ein Update fehlschlägt, da das Quell-Volume verschoben wurde.

Über diese Aufgabe

SnapMirror bricht alle Transfers von einem verschobenen Quell-Volume ab, bis Sie die Replizierungsbeziehung manuell aktualisieren.

Ab ONTAP 9.5 werden synchrone SnapMirror Beziehungen unterstützt. Obwohl die Quell- und Ziel-Volumes in diesen Beziehungen zu jeder Zeit synchron sind, wird die Ansicht vom sekundären Cluster nur stündlich zum primären Volume synchronisiert. Wenn Sie die Point-in-Time-Daten am Ziel anzeigen möchten, sollten Sie eine manuelle Aktualisierung durchführen, indem Sie den `snapmirror update` Befehl ausführen.

Schritt

1. Manuelles Aktualisieren einer Replikationsbeziehung:

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

> Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen. Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein allgemeiner Snapshot vorhanden ist. Verwenden Sie `snapmirror initialize` , um die Beziehung neu zu initialisieren. Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf aktualisiert `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Erfahren Sie mehr über `snapmirror update` in der "ONTAP-Befehlsreferenz".

Neusynchronisierung einer ONTAP SnapMirror Replizierungsbeziehung

Sie müssen eine Replikationsbeziehung neu synchronisieren, nachdem Sie ein Zielvolume schreibbar gemacht haben, nachdem ein Update fehlschlägt, weil auf den Quell- und Zielvolumes kein gemeinsamer Snapshot vorhanden ist, oder wenn Sie die Replikationsrichtlinie für die Beziehung ändern möchten.

Ab ONTAP 9.8 können Sie mit System Manager eine erneute Synchronisierung durchführen, um eine vorhandene Sicherungsbeziehung zu löschen und die Funktionen der Quell- und Ziel-Volumes rückgängig zu machen. Anschließend verwenden Sie das Ziel-Volume, um Daten bereitzustellen, während Sie die Quelle reparieren oder ersetzen, die Quelle aktualisieren und die ursprüngliche Konfiguration der Systeme wiederherstellen.

> System Manager unterstützt keine umgekehrte Resynchronisierung mit Intracluster-Beziehungen. Sie können die ONTAP CLI verwenden, um Vorgänge für die umgekehrte Neusynchronisierung mit Intracluster-Beziehungen durchzuführen.

Über diese Aufgabe

- Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.
- Volumes, die Teil einer Fan-out- oder Kaskadenkonfiguration sind, können zur erneuten Synchronisierung länger dauern. Es ist nicht ungewöhnlich, dass die SnapMirror Beziehung den Status „Vorbereitung“ für einen längeren Zeitraum meldet.
- Ab ONTAP 9.13.1 versucht ONTAP standardmäßig, die Schnellsynchronisierung zu nutzen, um die Resynchronisierungszeit zu verkürzen. Folgende Bedingungen müssen erfüllt sein, damit die Schnellsynchronisierung standardmäßig verwendet wird:
  - FlexVol -Volumes haben keine Klone auf dem Volume

- Bei Verwendung der MirrorAllSnapshots-Richtlinie

> Verwendung `-quick-resync` kann aufgrund der Reduzierung der Speichereffizienz bei übertragenen Datenblöcken zusätzlichen Speicherplatz auf dem Resynchronisierungszielvolume beanspruchen. Dieser zusätzliche Speicherplatzverbrauch wird im Rahmen der Inline- oder Post-Replikations-Speichereffizienzanwendung auf dem Resynchronisierungsziel kompensiert.

Der `-quick-resync` Der Parameter ist optional. Sie können die Schnellsynchronisierung aktivieren oder deaktivieren, indem Sie die folgende Option verwenden: `-quick-resync true|false` Parameter mit dem `snapmirror resync` Befehl.

Für weitere Informationen über `-quick-resync`siehe die "ONTAP-Befehlsreferenz"Die

Schritte

Diese Aufgabe können Sie mit System Manager oder der ONTAP-CLI ausführen. Wenn Sie die ONTAP-CLI verwenden, ist das Verfahren unabhängig davon, ob Sie ein Zielvolume beschreibbar machen oder die Replikationsbeziehung aktualisieren.

System Manager reversynchronisieren

Nachdem Sie "Eine Beziehung durchbrechen"ein Ziel beschreibbar gemacht haben, kehren Sie zurück, wie die Beziehung synchronisiert wird:

1. Klicken Sie auf dem Ziel-Cluster auf **Schutz > Beziehungen**.
2. Bewegen Sie den Mauszeiger über die unterbrochene Beziehung, die Sie umkehren möchten, klicken Sie auf ⋮, und wählen Sie **Resync umkehren**.
3. Klicken Sie im Fenster **Reverse Resync Relationship** auf **Reverse Resync**.
4. Überwachen Sie unter **Relationships** den Fortschritt der umgekehrten Neusynchronisierung, indem Sie **Transferstatus** für die Beziehung anzeigen.

Nächste Schritte

Wenn die ursprüngliche Quelle wieder verfügbar ist, können Sie die ursprüngliche Beziehung wiederherstellen, indem Sie die umgekehrte Beziehung unterbrechen und einen weiteren umgekehrten Resync-Vorgang durchführen. Bei der umgekehrten Resynchronisierung werden alle Änderungen vom Standort kopiert, der Daten an die ursprüngliche Quelle bereitstellt, und die ursprüngliche Quelle wird wieder schreibgeschützt.

System Manager neu synchronisieren

1. Klicken Sie Auf **Schutz > Beziehungen**.
2. Bewegen Sie den Mauszeiger über die Beziehung, die Sie neu synchronisieren möchten, und klicken Sie auf ⋮ , und wählen Sie dann **Pause**.
3. Wenn der Beziehungsstatus „abgebrochen“ anzeigt, klicken Sie auf ⋮ und wählen Sie dann **Resync**.
4. Überwachen Sie unter **Relationships** den Fortschritt der Neusynchronisierung, indem Sie den Beziehungsstatus überprüfen. Nach Abschluss der Resynchronisierung ändert sich der Status in „gespiegelt“.

CLI

1. Neusynchronisierung der Quell- und Ziel-Volumes:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

ⓘ Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume auf und dem Ziel-Volume auf neu synchronisiert `volA` `svm1` `volA_dst` `svm_backup`:

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

Erfahren Sie mehr über `snapmirror resync` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Synchronisieren Sie die Daten auf einer ONTAP SnapMirror Ziel-SVM erneut"

Löschen einer ONTAP SnapMirror Volume-Replikationsbeziehung

Sie können die `snapmirror delete` `snapmirror release` Befehle und verwenden, um eine Volume-Replikationsbeziehung zu löschen. Sie können dann nicht benötigte Ziel-Volumes manuell löschen.

Über diese Aufgabe

Mit dem `snapmirror release` Befehl werden alle von SnapMirror erstellten Snapshots aus der Quelle gelöscht. Sie können die Option verwenden `-relationship-info-only`, um die Snapshots beizubehalten.

Schritte

1. Replikationsbeziehung stilllegen:

   ```
   snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>
   ```

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   Erfahren Sie mehr über `snapmirror quiesce` in der "ONTAP-Befehlsreferenz".

2. (Optional) Ballen Sie die Replikationsbeziehung auf, wenn das Zielvolume ein Lese-/Schreibvolume sein muss. Sie können diesen Schritt überspringen, wenn Sie das Zielvolume löschen möchten oder wenn Sie das Volume nicht lesen/schreiben müssen:

   ```
   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
   ```

   Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

3. Löschen Sie die Replikationsbeziehung:

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

   Sie müssen diesen Befehl vom Ziel-Cluster oder der Ziel-SVM ausführen.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf gelöscht `svm_backup`:

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

Erfahren Sie mehr über `snapmirror delete` in der "ONTAP-Befehlsreferenz".

4. Informationen zu Replikationsbeziehungen von der Quell-SVM freigeben:

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

Sie müssen diesen Befehl vom Quellcluster oder der Quell-SVM ausführen.

Im folgenden Beispiel werden Informationen für die angegebene Replikationsbeziehung von der Quell-SVM freigegeben `svm1`:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Erfahren Sie mehr über `snapmirror release` in der "ONTAP-Befehlsreferenz".

Management der Storage-Effizienz auf ONTAP SnapMirror Volumes

SnapMirror bewahrt die Storage-Effizienz auf den Quell- und Ziel-Volumes auf, außer wenn die nachgelagerte Datenkomprimierung auf dem Ziel-Volume aktiviert ist. In diesem Fall geht die gesamte Storage-Effizienz auf dem Ziel-Volume verloren. Um dieses Problem zu beheben, müssen Sie die nachgelagerte Komprimierung auf dem Ziel-Volume deaktivieren, die Beziehung manuell aktualisieren und die Storage-Effizienz erneut aktivieren.

Über diese Aufgabe

Sie können mit dem `volume efficiency show` Befehl bestimmen, ob die Effizienz auf einem Volume aktiviert ist. Erfahren Sie mehr über `volume efficiency show` in der "ONTAP-Befehlsreferenz".

Überprüfen Sie, ob SnapMirror die Storage-Effizienz aufrechtzuerhalten, indem Sie sich die SnapMirror Prüfprotokolle ansehen und die Übertragungsbeschreibung ermitteln. Wenn die Transferbeschreibung angezeigt wird `transfer_desc=Logical Transfer with Storage Efficiency`, hält SnapMirror die Speichereffizienz aufrecht. Wenn die Transferbeschreibung angezeigt wird `transfer_desc=Logical Transfer`, hält SnapMirror die Speichereffizienz nicht aufrecht. 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

- Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.

"Cluster- und SVM-Peering"

- Sie müssen die nachgelagerte Komprimierung auf dem Ziel-Volume deaktivieren.
- Logischer Transfer mit Storage: Ab ONTAP 9.3 ist kein manuelles Update mehr erforderlich, um die Storage-Effizienz erneut zu aktivieren. Wenn SnapMirror feststellt, dass die nachgelagerte Komprimierung deaktiviert wurde, wird die Storage-Effizienz automatisch bei dem nächsten geplanten Update aktiviert. Die Quelle und das Ziel müssen ONTAP 9.3 ausführen.
- Seit ONTAP 9.3 managen AFF Systeme Storage-Effizienzeinstellungen anders als FAS Systeme, nachdem ein Ziel-Volume beschrieben werden kann:
  - Nachdem Sie ein Zielvolume mit dem Befehl `snapmirror break` Befehl wird die Caching-Richtlinie auf dem Volume automatisch auf `auto` (Standard).

    Dieses Verhalten gilt nur für FlexVol Volumes und nicht für FlexGroup Volumes.

    Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

  - Bei der Neusynchronisierung wird die Caching-Richtlinie automatisch auf `none` , und Deduplizierung und Inline-Komprimierung werden unabhängig von Ihren ursprünglichen Einstellungen automatisch deaktiviert. Sie müssen die Einstellungen nach Bedarf manuell ändern.

Manuelle Updates mit aktivierter Storage-Effizienz können sehr zeitaufwendig sein. Möglicherweise möchten Sie den Betrieb in Zeiten geringerer Auslastung ausführen.

Schritte

1. Aktualisierung einer Replizierungsbeziehung und erneute Aktivierung der Storage-Effizienz:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen. Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein allgemeiner Snapshot vorhanden ist. Verwenden Sie `snapmirror initialize` , um die Beziehung neu zu initialisieren. Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA_dst` auf aktualisiert `svm_backup` und die Storage-Effizienz wieder aktiviert:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

Erfahren Sie mehr über `snapmirror update` in der "ONTAP-Befehlsreferenz".

Verwenden Sie die globale ONTAP SnapMirror-Drosselung

Globale Netzwerkdrosselung ist für alle SnapMirror- und SnapVault-Transfers auf Node-

Ebene verfügbar.

Über diese Aufgabe

Die globale Drosselung von SnapMirror schränkt die durch ein- und/oder ausgehende SnapMirror- und SnapVault-Transfers verwendete Bandbreite ein. Die Einschränkung wird auf allen Nodes im Cluster clusterweit durchgesetzt.

Wenn die ausgehende Drosselklappe beispielsweise auf 100 Mbit/s eingestellt ist, hat jeder Knoten im Cluster die ausgehende Bandbreite auf 100 Mbit/s eingestellt. Wenn die globale Drosselung deaktiviert ist, ist sie auf allen Knoten deaktiviert.

Obwohl Datenübertragungsraten häufig in Bits pro Sekunde (bps) angegeben werden, müssen die Drosselwerte in Kilobyte pro Sekunde (kbps) eingegeben werden.

> In ONTAP 9.9.1 und früheren Versionen hat die Drosselung keine Auswirkungen auf `volume move` Transfers oder Spiegelübertragungen mit Lastverteilung. Ab ONTAP 9.10.0 können Sie eine Option zum Drosseln eines Volume-Verschiebungsvorgangs angeben. Weitere Informationen finden Sie unter "Wie Sie die Volumenbewegung in ONTAP 9.10 und höher drosseln".

Globale Drosselung arbeitet mit der Gaspedalfunktion für SnapMirror und SnapVault Transfers. Die Drosselung pro Beziehung wird so lange durchgesetzt, bis die kombinierte Bandbreite der Transfers den Wert der globalen Drosselung überschreitet, nach der die globale Drosselung durchgesetzt wird. Ein Drosselungswert `0` bedeutet, dass die globale Drosselung deaktiviert ist.

> Die globale SnapMirror-Drosselung hat keine Auswirkungen auf synchrone SnapMirror-Beziehungen, wenn sie in-Sync sind. Die Drosselung wirkt sich jedoch auf die synchronen SnapMirror-Beziehungen aus, wenn sie eine asynchrone Übertragungsphase, z. B. einen Initialisierungsvorgang, oder nach einem Ereignis aus dem Synchronisierungsvorgang durchführen. Aus diesem Grund wird die Aktivierung der globalen Drosselung mit synchronen SnapMirror-Beziehungen nicht empfohlen.

Schritte

1. Globale Drosselung aktivieren:

   `options -option-name replication.throttle.enable on|off`

   Das folgende Beispiel zeigt, wie Sie die globale SnapMirror-Drosselung auf aktivieren `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Geben Sie die maximale Bandbreite an, die von eingehenden Transfers auf dem Ziel-Cluster verwendet wird:

   `options -option-name replication.throttle.incoming.max_kbs <KBps>`

   Die empfohlene minimale Drosselungsbandbreite beträgt 4 Kilobyte pro Sekunde (Kbit/s) und die maximale Bandbreite bis zu 2 Terabyte pro Sekunde (Tbit/s). Der Standardwert für diese Option ist `unlimited`, was bedeutet, dass es keine Begrenzung der gesamten Bandbreite verwendet.

   Das folgende Beispiel zeigt, wie die maximale Gesamtbandbreite, die bei eingehenden Übertragungen

verwendet wird, auf 100 Megabit pro Sekunde (Mbit/s) eingestellt wird:

```
cluster_dst::> options -option-name
replication.throttle.incoming.max_kbs 12500
```

100 Megabit pro Sekunde (Mbit/s) = 12500 Kilobyte pro Sekunde (Kbit/s)

3. Geben Sie die maximale Bandbreite an, die bei ausgehenden Transfers auf dem Quellcluster verwendet wird:

   `options -option-name replication.throttle.outgoing.max_kbs <KBps>`

   Die empfohlene minimale Drosselbandbreite beträgt 4 kbps und die maximale Bandbreite beträgt bis zu 2 Tbps. Der Standardwert für diese Option ist `unlimited`, was bedeutet, dass es keine Begrenzung der gesamten Bandbreite verwendet. Parameterwerte werden in Kilobyte pro Sekunde (kbps) angegeben.

   Das folgende Beispiel zeigt, wie die maximale Bandbreite für ausgehende Übertragungen auf 100 Mbit/s eingestellt wird:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

Management der SnapMirror SVM-Replizierung

Erfahren Sie mehr über die ONTAP SnapMirror SVM-Replizierung

Mit SnapMirror können Sie eine Datensicherungsbeziehung zwischen SVMs erstellen. In dieser Art der Datensicherungsbeziehung wird die gesamte Konfiguration oder Teile der SVM, von NFS-Exporten und SMB-Freigaben bis hin zur rollenbasierten Zugriffssteuerung, repliziert sowie die Daten in den Volumes, die die SVM besitzt.

Unterstützte Beziehungstypen

Es können nur SVMs mit Datenbereitungsdaten repliziert werden. Die folgenden Typen von Datensicherungsbeziehungen werden unterstützt:

- *SnapMirror DR,* in dem das Ziel normalerweise nur die Snapshots enthält, die derzeit auf der Quelle vorhanden sind.

  Ab ONTAP 9.9 ändert sich dieses Verhalten, wenn Sie die Mirror-Vault-Richtlinie verwenden. Ab ONTAP 9.9 können Sie verschiedene Snapshot-Richtlinien auf der Quelle und dem Ziel erstellen. Die Snapshots auf dem Ziel werden dabei nicht durch Snapshots auf der Quelle überschrieben:

  - Sie werden während normaler geplanter Vorgänge, Updates und Neusynchronisierung nicht vom Quell- zum Ziel überschrieben
  - Sie werden während der Pausen nicht gelöscht.
  - Sie werden während der Flip-Resynchronisierung nicht gelöscht. Wenn Sie eine SVM-Disaster-

Beziehung mithilfe der Mirror-Vault-Richtlinie über ONTAP 9.9.1 und höher konfigurieren, verhält sich die Richtlinie wie folgt:

  - Benutzerdefinierte Snapshot-Richtlinien an der Quelle werden nicht auf das Ziel kopiert.
  - Systemdefinierte Snapshot-Richtlinien werden nicht auf das Ziel kopiert.
  - Die Volume-Zuordnung zu Benutzer- und systemdefinierten Snapshot-Richtlinien wird nicht auf das Ziel kopiert. + SVM.

- *SnapMirror Unified Replication*, bei der das Ziel sowohl für DR als auch für die langfristige Aufbewahrung konfiguriert ist.

Weitere Informationen zur einheitlichen Replikation von SnapMirror finden Sie unter "Grundlagen der SnapMirror Unified Replication".

Der Typ_Policy_ der Replikationsrichtlinie bestimmt die Art der von ihr unterstützten Beziehung. In der folgenden Tabelle sind die verfügbaren Richtlinientypen aufgeführt.

Richtlinientyp	Beziehungstyp
Asynchrone Spiegelung	SnapMirror DR
Mirror-Vault	Einheitliche Replizierung

XDP ersetzt DP als Standardvorgabe für die SVM-Replizierung in ONTAP 9.4

Seit ONTAP 9.4 ist bei den SVM-Datensicherungsbeziehungen standardmäßig der XDP-Modus aktiviert. Beziehungen für die SVM-Datensicherung setzen weiterhin in ONTAP 9.3 und früher den DP-Modus ein.

Vorhandene Beziehungen werden vom XDP-Standard nicht beeinflusst. Wenn bereits eine Beziehung vom Typ DP verwendet wird, ist diese weiterhin vom Typ DP. Die folgende Tabelle zeigt das Verhalten, das Sie erwarten können.

Wenn Sie angeben…	Der Typ ist…	Die Standardrichtlinie (wenn Sie keine Richtlinie angeben) lautet…
DATENSICHERUNG	XDP	MirrorAllSnapshots (SnapMirror DR)
Nichts	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	MirrorAndVault (einheitliche Replizierung)

Informationen zum Konvertieren von DP-Beziehungen in XDP-Beziehungen und andere Details finden Sie hier: "Konvertieren einer vorhandenen ONTAP-DP-Beziehung in XDP".

Die Versionsunabhängigkeit wird bei der SVM-Replizierung nicht unterstützt. Bei einer SVM-Konfiguration für Disaster Recovery muss sich die Ziel-SVM auf einem Cluster befinden, auf dem dieselbe ONTAP-Version wie das SVM-Quell-Cluster ausgeführt wird, um Failover- und Failback-Vorgänge zu unterstützen.

"Kompatible ONTAP Versionen für SnapMirror Beziehungen"

Replizierung von SVM-Konfigurationen

Der Inhalt einer SVM-Replizierungsbeziehung wird durch die Interaktion der folgenden Felder bestimmt:

- Mit der `-identity-preserve true` Option des `snapmirror create` Befehls wird die gesamte SVM-Konfiguration repliziert.

  Die `-identity-preserve false` Option repliziert nur die Volumes und Authentifizierungs- und Autorisierungskonfigurationen der SVM sowie die in aufgeführten Protokoll- und Namensservice-Einstellungen"Konfigurationen, die in SVM-Disaster-Recovery-Beziehungen repliziert werden".

- `-discard-configs network`Bei der Option des `snapmirror policy create` Befehls sind LIFs und zugehörige Netzwerkeinstellungen von der SVM-Replizierung ausgeschlossen, und zwar für Anwendungsfälle, 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.

Andernfalls ist die SVM-Replizierung nahezu identisch mit der Volume-Replizierung. Sie können nahezu denselben Workflow für die SVM-Replizierung einsetzen wie bei der Volume-Replizierung.

Support-Details

Die folgende Tabelle enthält Support-Details zur SnapMirror SVM-Replizierung.

Ressource oder Funktion	Support-Details
Bereitstellungstypen	• Von einer einzelnen Quelle zu einem einzigen Ziel • Ab ONTAP 9.4 Fan-out: Sie können nur an zwei Zielorten Fan-out. Standardmäßig ist pro Quell-SVM nur eine -Identity-Preserve True Relationship zulässig.
Beziehungstypen	• SnapMirror Disaster Recovery • Einheitliche SnapMirror -Replikation
Replizierungsumfang	Nur Intercluster. Sie können SVMs nicht in demselben Cluster replizieren.
Autonomer Schutz Durch Ransomware	• Unterstützt ab ONTAP 9.12.1. Weitere Informationen finden Sie unter "Autonomer Schutz Durch Ransomware".

Asynchrone Unterstützung von Konsistenzgruppen	Ab ONTAP 9.14.1 werden maximal 32 Disaster-Recovery-Beziehungen für SVMs unterstützt, wenn Konsistenzgruppen vorhanden sind. Weitere Informationen finden Sie unter "Sichern einer Konsistenzgruppe" und "Einschränkungen für Konsistenzgruppen" .
FabricPool	Ab ONTAP 9.6 wird die SnapMirror SVM-Replizierung mit FabricPool unterstützt. In einer SVM-DR-Beziehung müssen Quell- und Ziel-Volumes keine FabricPool-Aggregate verwenden, sondern sie müssen dieselbe Tiering-Richtlinie verwenden. Ab ONTAP 9.12.1 wird die SnapMirror SVM Replizierung mit gemeinsamen FabricPool und FlexGroup Volumes unterstützt. Vor 9.12.1 konnten zwei dieser Funktionen miteinander kombiniert werden, aber nicht alle drei.

MetroCluster	Ab ONTAP 9.11.1 können beide Seiten der Disaster-Recovery-Beziehung einer SVM innerhalb einer MetroCluster Konfiguration als Quelle für zusätzliche SVM-Disaster-Recovery-Konfigurationen fungieren. Ab ONTAP 9.5 wird die SnapMirror SVM-Replizierung auf MetroCluster Konfigurationen unterstützt. • Bei älteren Versionen als ONTAP 9.10.X kann eine MetroCluster-Konfiguration nicht Ziel einer SVM-Disaster-Recovery-Beziehung sein. • In Versionen ab ONTAP 9.10.1 kann eine MetroCluster-Konfiguration lediglich zu Migrationszwecken als Ziel einer SVM-Disaster-Recovery-Beziehung dienen. Zudem muss sie alle in beschriebenen Anforderungen erfüllen "TR-4966: Migration einer SVM in eine MetroCluster Lösung". • Nur eine aktive SVM innerhalb einer MetroCluster-Konfiguration kann als Quelle einer SVM Disaster-Recovery-Beziehung verwendet werden. Eine Quelle kann eine synchrone Quell-SVM vor der Umschaltung oder eine synchrone Ziel-SVM nach der Umschaltung sein. • Wenn eine MetroCluster-Konfiguration sich in einem stabilen Zustand befindet, kann die MetroCluster SVM, die synchrone Ziel-SVM, nicht als Quelle für eine SVM Disaster-Recovery-Beziehung dienen, da die Volumes nicht online sind. • Wenn die SVM für die synchrone Quelle die Quelle der SVM für die Disaster-Recovery-Beziehung ist, werden die SVM für die Quell-Disaster-Recovery-Beziehung zum MetroCluster-Partner repliziert. • Während der Umschaltungs- und Switchback-Prozesse schlägt die Replizierung auf das Disaster-Recovery-Ziel der SVM möglicherweise fehl. Nach Abschluss des Switchover- oder Switchback-Prozesses werden jedoch die nächsten geplanten Aktualisierungen für die SVM-Disaster Recovery erfolgreich durchgeführt.
Konsistenzgruppe	Unterstützt ab ONTAP 9.14.1. Weitere Informationen finden Sie unter Sichern einer Konsistenzgruppe.

ONTAP S3	Nicht unterstützt durch SVM Disaster Recovery.
SnapMirror Synchronous	Nicht unterstützt durch SVM Disaster Recovery.
Versionsunabhängigkeit	Nicht unterstützt.
Volume-Verschlüsselung	• Verschlüsselte Volumes auf der Quelle werden auf dem Ziel verschlüsselt. • Onboard Key Manager oder KMIP-Server müssen auf dem Ziel konfiguriert sein. • Neue Verschlüsselungsschlüssel werden am Zielspeicherort generiert. • Wenn das Ziel keinen Knoten enthält, der Volume .Encryption unterstützt, ist die Replikation erfolgreich, aber die Ziel-Volumes sind nicht verschlüsselt.

Konfigurationen, die in SVM-Disaster-Recovery-Beziehungen repliziert werden

Die folgende Tabelle zeigt das Zusammenspiel zwischen 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` Satz	**Richtlinie mit `-discard-configs network` Set**	
Netzwerk	NAS-LIFs	Ja.	Nein	Nein
LIF-Kerberos-Konfiguration	Ja.	Nein	Nein	SAN LIFs
Nein	Nein	Nein	Firewallrichtlinien	Ja.
Ja.	Nein	Service-Richtlinien	Ja.	Ja.
Nein	Routen	Ja.	Nein	Nein
Broadcast-Domäne	Nein	Nein	Nein	Subnetz
Nein	Nein	Nein	IP-Bereich	Nein
Nein	Nein	SMB	SMB-Server	Ja.

Ja.	Nein	Lokale Gruppen und lokaler Benutzer	Ja.	Ja.
Ja.	Berechtigung	Ja.	Ja.	Ja.
Schattenkopie	Ja.	Ja.	Ja.	BranchCache
Ja.	Ja.	Ja.	Serveroptionen	Ja.
Ja.	Ja.	Serversicherheit	Ja.	Ja.
Nein	Home Directory damit füllt	Ja.	Ja.	Ja.
Symbolischer Link	Ja.	Ja.	Ja.	FPolicy, Fsicherheitsrichtlinie und Fsicherheitsrichtlinie n NTFS
Ja.	Ja.	Ja.	Namenszuweisung und Gruppenzuordnung	Ja.
Ja.	Ja.	Audit-Informationen	Ja.	Ja.
Ja.	NFS	Exportrichtlinien	Ja.	Ja.
Nein	Exportrichtlinien	Ja.	Ja.	Nein
NFS-Server	Ja.	Ja.	Nein	RBAC
Sicherheitszertifikate	Ja.	Ja.	Nein	Benutzer anmelden, öffentlichen Schlüssel, Rolle und Rollenkonfiguration
Ja.	Ja.	Ja.	SSL	Ja.
Ja.	Nein	Name Services	DNS- und DNS-Hosts	Ja.
Ja.	Nein	UNIX-Benutzer und UNIX-Gruppe	Ja.	Ja.

Ja.	Kerberos-Bereich und Kerberos-Keyblockes	Ja.	Ja.	Nein
LDAP- und LDAP-Client	Ja.	Ja.	Nein	Netzgruppe
Ja.	Ja.	Nein	NIS	Ja.
Ja.	Nein	Web- und Webzugriff	Ja.	Ja.
Nein	Datenmenge	Objekt	Ja.	Ja.
Ja.	Snapshots und Snapshot-Richtlinie	Ja.	Ja.	Ja.
Richtlinie für automatisches Löschen	Nein	Nein	Nein	Effizienzrichtlinie
Ja.	Ja.	Ja.	Kontingentrichtlinie und Kontingentrichtlinie	Ja.
Ja.	Ja.	Wiederherstellungs warteschlange	Ja.	Ja.
Ja.	Root-Volume	Namespace	Ja.	Ja.
Ja.	Benutzerdaten	Nein	Nein	Nein
Qtrees	Nein	Nein	Nein	Kontingente
Nein	Nein	Nein	QoS auf Dateiebene	Nein
Nein	Nein	Attribute: Zustand des Root-Volumes, der Platzgarantie, der Größe, der Autosize und der Gesamtzahl 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	Portsätze	Nein
Nein	Nein	Seriennummern	Nein	Nein
Nein	SNMP	v3-Benutzer	Ja.	Ja.

Grenzen des SVM Disaster Recovery Storage

Die folgende Tabelle zeigt die empfohlene maximale Anzahl an Volumes und SVM-Disaster-Recovery-Beziehungen, die pro Storage-Objekt unterstützt werden. Grenzen sollten häufig plattformabhängig sein. Weitere "Hardware Universe"Informationen zu den Einschränkungen für Ihre spezifische Konfiguration finden Sie im.

Storage Objekt	Grenze
SVM	300 flexible Volumes
HA-Paar	1,000 Flexible Volumes
Cluster	128 SVM-Disaster-Beziehungen

Verwandte Informationen

- "snapmirror erstellen"
- "Snapmirror-Richtlinie erstellen"

Replizieren der SVM -Konfigurationen

Workflow für die ONTAP SnapMirror SVM-Replizierung

Bei der SnapMirror SVM-Replizierung wird die Ziel-SVM erstellt, ein Zeitplan für Replizierungsjobs erstellt und eine SnapMirror Beziehung erstellt bzw. initialisiert.

Sie sollten bestimmen, welcher Replikations-Workflow Ihren Anforderungen am besten entspricht:

- "Replizierung einer gesamten SVM-Konfiguration"
- "Schließt LIFs und zugehörige Netzwerkeinstellungen von der SVM-Replizierung aus"
- "Ausluden von Netzwerk-, Name-Service- und anderen Einstellungen aus der SVM-Konfiguration"

Kriterien zum Platzieren von Volumes auf ONTAP SnapMirror Ziel-SVMs

Bei der Replizierung von Volumes von der Quell-SVM zu der Ziel-SVM ist es wichtig, die

Kriterien bei der Auswahl der Aggregate zu kennen.

Aggregate werden basierend auf den folgenden Kriterien ausgewählt:

- Volumes werden immer in nicht-Root-Aggregaten platziert.
- Nicht-Root-Aggregate werden basierend auf dem verfügbaren freien Speicherplatz und der Anzahl der Volumes ausgewählt, die bereits auf dem Aggregat gehostet sind.

  Aggregate mit mehr freiem Speicherplatz und weniger Volumes werden vorrangig behandelt. Es wird das Aggregat mit der höchsten Priorität ausgewählt.

- Quell-Volumes auf FabricPool-Aggregaten werden mit derselben Tiering-Richtlinie auf FabricPool-Aggregaten am Ziel-Volume platziert.
- Wenn sich ein Volume auf der Quell-SVM auf einem Flash Pool Aggregat befindet, wird das Volume auf einem Flash Pool Aggregat auf der Ziel-SVM platziert, sofern ein solches Aggregat existiert und über genügend freien Speicherplatz verfügt.
- `-space-guarantee`Ist die Option des replizierten Volumes auf festgelegt `volume`, werden nur Aggregate mit freiem Speicherplatz betrachtet, die größer als die Volume-Größe sind.
- Die Volume-Größe wird während der Replizierung automatisch auf der Ziel-SVM vergrößert, basierend auf der Größe des Quell-Volumes.

  Falls Sie die Größe der Ziel-SVM vorab reservieren möchten, müssen Sie die Größe des Volume ändern. Die Volume-Größe verkleinert sich nicht automatisch auf der Ziel-SVM basierend auf der Quell-SVM.

Um ein Volume von einem Aggregat zu einem anderen zu verschieben, können Sie den `volume move` Befehl auf der Ziel-SVM verwenden.

Replizierung einer gesamten ONTAP SVM-Konfiguration

Sie können eine SVM-Disaster-Recovery-Beziehung (SVM DR) erstellen, um eine SVM-Konfiguration auf eine andere zu replizieren. Falls es am primären Standort zu einem Ausfall kommt, können Sie die Ziel-SVM schnell aktivieren.

Bevor Sie beginnen

Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden. Weitere Informationen finden Sie unter "Erstellen einer Cluster-Peer-Beziehung" und "Erstellen einer SVM-Peer-Beziehung".

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Bei diesem Workflow wird vorausgesetzt, dass Sie bereits eine Standardrichtlinie oder eine benutzerdefinierte Replizierungsrichtlinie verwenden.

Ab ONTAP 9.9 können Sie mit der Richtlinie für Mirror-Vault verschiedene Snapshot-Richtlinien auf der Quell- und Ziel-SVM erstellen. Die Snapshots auf dem Ziel werden nicht durch Snapshots auf der Quelle überschrieben. Weitere Informationen finden Sie unter "Allgemeines zur Replizierung von SnapMirror SVMs".

Führen Sie dieses Verfahren vom Ziel aus. Wenn Sie eine neue Schutzrichtlinie erstellen müssen, zum Beispiel wenn Ihre Quell-Storage-VM SMB konfiguriert ist, sollten Sie die Richtlinie erstellen und die Option **Identity preserve** verwenden. Weitere Informationen finden Sie unter "Erstellen benutzerdefinierter

Datensicherungsrichtlinien".

Schritte

Sie können diese Aufgabe über System Manager oder die ONTAP CLI ausführen.

System Manager

1. Klicken Sie auf dem Ziel-Cluster auf **Schutz > Beziehungen**.
2. Klicken Sie unter **Beziehungen** auf **Schutz** und wählen Sie **Storage VMs (DR)**.
3. Wählen Sie eine Schutzrichtlinie aus. Wenn Sie eine benutzerdefinierte Schutzrichtlinie erstellt haben, wählen Sie diese aus, und wählen Sie dann das Quellcluster und die Storage VM aus, die repliziert werden sollen. Sie können auch eine neue Ziel-Storage-VM erstellen, indem Sie einen neuen Namen für die Storage VM eingeben.
4. Ändern Sie bei Bedarf die Zieleinstellungen, um die Identitätserhaltung außer Kraft zu setzen und Netzwerkschnittstellen und -Protokolle ein- oder auszuschließen.
5. Klicken Sie Auf **Speichern**.

CLI

1. Ziel-SVM erstellen:

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   Der SVM-Name muss über die Quell- und Ziel-Cluster hinweg eindeutig sein.

   Im folgenden Beispiel wird eine Ziel-SVM mit dem Namen erstellt `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

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

2. Erstellen Sie über den `vserver peer create` Befehl aus dem Ziel-Cluster eine SVM-Peer-Beziehung.

   Weitere Informationen finden Sie unter "Erstellen einer SVM-Peer-Beziehung".

   Erfahren Sie mehr über `vserver peer create` in der "ONTAP-Befehlsreferenz".

3. Erstellen eines Replikationsauftragplans:

   ```
   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` können Sie festlegen `all`, dass der Job jeden Monat, Wochentag und jede Stunde ausgeführt werden soll.

   > Der unterstützte Zeitplan (RPO) für FlexVol Volumes in einer SVM SnapMirror Beziehung beträgt mindestens 15 Minuten. Der unterstützte Zeitplan (RPO) für FlexGroup Volumes in einer SVM SnapMirror Beziehung beträgt mindestens 30 Minuten.

Im folgenden Beispiel wird ein Jobzeitplan mit dem Namen erstellt `my_weekly`, der samstags um 3:00 Uhr ausgeführt wird:

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

Erfahren Sie mehr über `job schedule cron create` in der "ONTAP-Befehlsreferenz".

4. Erstellen Sie auf der Ziel-SVM oder dem Ziel-Cluster eine Replizierungsbeziehung:

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

> In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben.

Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mithilfe der Standardrichtlinie erstellt `MirrorAllSnapshots`:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

Im folgenden Beispiel wird mithilfe der Standardrichtlinie eine einheitliche Replizierungsbeziehung erstellt `MirrorAndVault`:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Wenn Sie eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt haben `async-mirror`, wird im folgenden Beispiel eine SnapMirror-DR-Beziehung erstellt:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

Wenn Sie eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt haben `mirror-vault`, wird im folgenden Beispiel eine einheitliche Replikationsbeziehung erstellt:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

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

5. Ziel-SVM stoppen:

```
vserver stop -vserver <SVM_name>
```

Im folgenden Beispiel wird eine Ziel-SVM mit dem Namen „svm_Backup“ angehalten:

```
cluster_dst::> vserver stop -vserver svm_backup
```

Erfahren Sie mehr über `vserver stop` in der "ONTAP-Befehlsreferenz".

6. Initialisieren Sie die SVM-Replizierungsbeziehung von der Ziel-SVM oder dem Ziel-Cluster:

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

> In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben.

Im folgenden Beispiel wird die Beziehung zwischen der Quell-SVM, `svm1`, und der Ziel-SVM initialisiert `svm_backup`:

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

Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Ausschließen von LIFs und zugehörigen Netzwerkeinstellungen von der ONTAP SnapMirror SVM-Replizierung

Wenn sich die Quell- und Ziel-SVMs in unterschiedlichen Subnetzen befinden, können Sie mit `-discard-configs network` `snapmirror policy create` der Option des Befehls LIFs und zugehörige Netzwerkeinstellungen von der SVM-Replizierung ausschließen.

Bevor Sie beginnen

Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.

Weitere Informationen finden Sie unter "Erstellen einer Cluster-Peer-Beziehung" und "Erstellen einer SVM-Peer-Beziehung".

Über diese Aufgabe

Die `-identity-preserve` Option des `snapmirror create` Befehls muss `true` beim Erstellen der SVM-Replizierungsbeziehung auf festgelegt werden.

Schritte

1. Ziel-SVM erstellen:

   `vserver create -vserver SVM -subtype dp-destination`

   Der SVM-Name muss über die Quell- und Ziel-Cluster hinweg eindeutig sein.

   Im folgenden Beispiel wird eine Ziel-SVM mit dem Namen erstellt `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Erstellen Sie über den `vserver peer create` Befehl aus dem Ziel-Cluster eine SVM-Peer-Beziehung.

   Weitere Informationen finden Sie unter "Erstellen einer SVM-Peer-Beziehung".

   Erfahren Sie mehr über `vserver peer create` in der "ONTAP-Befehlsreferenz".

3. Job-Zeitplan 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` können Sie festlegen `all`, dass der Job jeden Monat, Wochentag und jede Stunde ausgeführt werden soll.

   > Der unterstützte Zeitplan (RPO) für FlexVol Volumes in einer SVM SnapMirror Beziehung beträgt mindestens 15 Minuten. Der unterstützte Zeitplan (RPO) für FlexGroup Volumes in einer SVM SnapMirror Beziehung beträgt mindestens 30 Minuten.

   Im folgenden Beispiel wird ein Jobzeitplan mit dem Namen erstellt `my_weekly`, der samstags um 3:00 Uhr ausgeführt wird:

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

4. Erstellen einer benutzerdefinierten Replizierungsrichtlinie:

   `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`

Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für SnapMirror DR erstellt, die LIFs ausschließt:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

Im folgenden Beispiel wird eine benutzerdefinierte Replizierungsrichtlinie für die einheitliche Replizierung erstellt, bei der LIFs ausgeschlossen sind:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

> Ziehen Sie in Betracht, für zukünftige Failover- und Failback-Szenarien dieselbe benutzerdefinierte SnapMirror-Richtlinie auf dem Quell-Cluster zu erstellen.

Erfahren Sie mehr über `snapmirror policy create` in der "ONTAP-Befehlsreferenz".

5. Führen Sie auf der Ziel-SVM oder dem Ziel-Cluster den folgenden Befehl aus, um eine Replizierungsbeziehung 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`

> In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Sehen Sie sich die Beispiele unten an.

Im folgenden Beispiel wird eine SnapMirror DR-Beziehung erstellt, bei der LIFs ausgeschlossen sind:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
-identity-preserve true
```

Im folgenden Beispiel wird eine SnapMirror Replizierungsbeziehung erstellt, die LIFs nicht 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
```

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

6. Ziel-SVM stoppen:

`vserver stop`

SVM name

Im folgenden Beispiel wird die Ziel-SVM mit dem Namen svm_Backup angehalten:

```
cluster_dst::> vserver stop -vserver svm_backup
```

7. Initialisieren Sie von der Ziel-SVM oder dem Ziel-Cluster eine Replizierungsbeziehung:

`snapmirror initialize -source-path SVM: -destination-path SVM:`

Im folgenden Beispiel wird die Beziehung zwischen der Quelle `svm1` und dem Ziel initialisiert `svm_backup`:

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

Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Sie müssen das Netzwerk und die Protokolle auf der Ziel-SVM für den Datenzugriff bei einem Ausfall konfigurieren.

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror Initialisierung"
- "Snapmirror-Richtlinie erstellen"

Ausschließen von Netzwerk-, Name-Service- und anderen Einstellungen von der SVM-Replizierung mit ONTAP

Möglicherweise möchten Sie Netzwerk-, Name-Service- und andere Einstellungen von einer SVM-Replizierungsbeziehung ausschließen, um Konflikte oder Konfigurationsunterschiede mit der Ziel-SVM zu vermeiden.

Sie können mit der `-identity-preserve false` Option des `snapmirror create` Befehls nur die Volumes und Sicherheitskonfigurationen einer SVM replizieren. Einige Protokoll- und Namensdiensteinstellungen bleiben ebenfalls erhalten.

Über diese Aufgabe

Eine Liste der erhaltenen Protokoll- und Namensdiensteinstellungen finden Sie unter "Konfigurationen in SVM-DR-Beziehungen repliziert".

Bevor Sie beginnen

Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.

Weitere Informationen finden Sie unter "Erstellen einer Cluster-Peer-Beziehung" und "Erstellen einer SVM-

Peer-Beziehung".

Schritte

1. Ziel-SVM erstellen:

   `vserver create -vserver SVM -subtype dp-destination`

   Der SVM-Name muss über die Quell- und Ziel-Cluster hinweg eindeutig sein.

   Im folgenden Beispiel wird eine Ziel-SVM mit dem Namen erstellt `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Erstellen Sie über den `vserver peer create` Befehl aus dem Ziel-Cluster eine SVM-Peer-Beziehung.

   Weitere Informationen finden Sie unter "Erstellen einer SVM-Peer-Beziehung".

   Erfahren Sie mehr über `vserver peer create` in der "ONTAP-Befehlsreferenz".

3. Erstellen eines Replikationsauftragplans:

   `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` können Sie festlegen `all`, dass der Job jeden Monat, Wochentag und jede Stunde ausgeführt werden soll.

   > Der unterstützte Zeitplan (RPO) für FlexVol Volumes in einer SVM SnapMirror Beziehung beträgt mindestens 15 Minuten. Der unterstützte Zeitplan (RPO) für FlexGroup Volumes in einer SVM SnapMirror Beziehung beträgt mindestens 30 Minuten.

   Im folgenden Beispiel wird ein Jobzeitplan mit dem Namen erstellt `my_weekly`, der samstags um 3:00 Uhr ausgeführt wird:

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

4. Erstellen einer Replikationsbeziehung, die Netzwerk, Name Service und andere Konfigurationseinstellungen ausschließt:

   `snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Sehen Sie sich die Beispiele unten an. Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen.

   Im folgenden Beispiel wird eine SnapMirror-DR-Beziehung mithilfe der Standardrichtlinie erstellt `MirrorAllSnapshots`. Bei der Beziehung werden Netzwerk, Name Service und andere

Konfigurationseinstellungen von der SVM-Replizierung ausgeschlossen:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

Im folgenden Beispiel wird mithilfe der Standardrichtlinie eine einheitliche Replikationsbeziehung erstellt `MirrorAndVault`. 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
```

Wenn Sie eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt haben `async-mirror`, wird im folgenden Beispiel eine SnapMirror-DR-Beziehung erstellt. Bei der Beziehung werden Netzwerk, Name Service und andere Konfigurationseinstellungen von der SVM-Replizierung ausgeschlossen:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Wenn Sie eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt haben `mirror-vault`, wird im folgenden Beispiel eine einheitliche Replikationsbeziehung erstellt. Bei der Beziehung werden Netzwerk, Name Service und andere Konfigurationseinstellungen von der SVM-Replizierung ausgeschlossen:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

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

5. Ziel-SVM stoppen:

   `vserver stop`

   `SVM name`

   Im folgenden Beispiel wird eine Ziel-SVM namens dvs1 angehalten:

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. Wenn Sie SMB verwenden, müssen Sie auch einen SMB-Server konfigurieren.

Siehe "Nur SMB: Erstellen eines SMB-Servers".

7. Initialisieren Sie die SVM-Replizierungsbeziehung von der Ziel-SVM oder dem Ziel-Cluster:

   `snapmirror initialize -source-path SVM_name: -destination-path SVM_name:`

   Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Sie müssen das Netzwerk und die Protokolle auf der Ziel-SVM für den Datenzugriff bei einem Ausfall konfigurieren.

Geben Sie lokale Tiers an, die für ONTAP SnapMirror SVM DR-Beziehungen verwendet werden sollen

Nach dem Erstellen einer SVM für Disaster Recovery können Sie die Option mit `vserver modify` dem Befehl verwenden `aggr-list`, um zu begrenzen, welche lokalen Tiers zum Hosten der SVM-DR-Ziel-Volumes verwendet werden.

Schritte

1. Ziel-SVM erstellen:

   `vserver create -vserver SVM -subtype dp-destination`

2. Ändern Sie die Aggr-Liste der Disaster-Recovery-SVM, um die lokalen Tiers zu begrenzen, die zum Hosten des Volumes der Disaster-Recovery-SVM verwendet werden:

   `cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>`

Erstellen eines SMB-Servers für eine ONTAP SnapMirror-Ziel-SVM in einer DR-Beziehung

Wenn die Quell-SVM über eine SMB-Konfiguration verfügt und Sie auf `false` festgelegt `identity-preserve` haben, müssen Sie einen SMB-Server für die Ziel-SVM erstellen. Für einige SMB-Konfigurationen ist ein SMB-Server erforderlich, z. B. Freigaben während der Initialisierung der SnapMirror-Beziehung.

Schritte

1. Starten Sie die Ziel-SVM mit dem `vserver start` Befehl.

   ```
   destination_cluster::> vserver start -vserver dvs1
   [Job 30] Job succeeded: DONE
   ```

   Erfahren Sie mehr über `vserver start` in der "ONTAP-Befehlsreferenz".

2. Überprüfen Sie `running` `dp-destination` mit dem `vserver show` Befehl, ob die Ziel-SVM den Status und den Subtyp aufweist.

```
destination_cluster::> vserver show
                                    Admin      Operational Root
Vserver  Type    Subtype            State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

Erfahren Sie mehr über `vserver show` in der "ONTAP-Befehlsreferenz".

3. Erstellen Sie mithilfe des `network interface create` Befehls ein LIF.

```
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
```

Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

4. Erstellen Sie mit dem `network route create` Befehl eine Route.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Netzwerkmanagement"

Erfahren Sie mehr über `network route create` in der "ONTAP-Befehlsreferenz".

5. Konfigurieren Sie DNS mit dem `vserver services dns create` Befehl.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

Erfahren Sie mehr über `vserver services dns create` in der "ONTAP-Befehlsreferenz".

6. Fügen Sie den bevorzugten Domänencontroller mit dem `vserver cifs domain preferred-dc add` Befehl hinzu.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

Erfahren Sie mehr über `vserver cifs domain preferred-dc add` in der "ONTAP-Befehlsreferenz".

7. Erstellen Sie den SMB-Server mit dem `vserver cifs create` Befehl.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

Erfahren Sie mehr über `vserver cifs create` in der "ONTAP-Befehlsreferenz".

8. Ziel-SVM mit dem `vserver stop` Befehl stoppen.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Erfahren Sie mehr über `vserver stop` in der "ONTAP-Befehlsreferenz".

Ausschluss von Volumes aus einer ONTAP SnapMirror SVM DR-Beziehung

Standardmäßig werden alle RW-Daten-Volumes der Quell-SVM repliziert. Wenn Sie nicht alle Volumes auf der Quell-SVM sichern möchten, können Sie mit der `-vserver-dr -protection unprotected` Option des `volume modify` Befehls Volumes von der SVM-Replizierung ausschließen.

Schritte

1. Volume von SVM-Replizierung ausschließen:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

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

   Im folgenden Beispiel ist 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-Replizierung aufnehmen möchten, die Sie ursprünglich ausgeschlossen haben, führen Sie den folgenden Befehl aus:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection protected`

   Im folgenden Beispiel wird das Volume `volA_src` in der SVM-Replizierung erfasst:

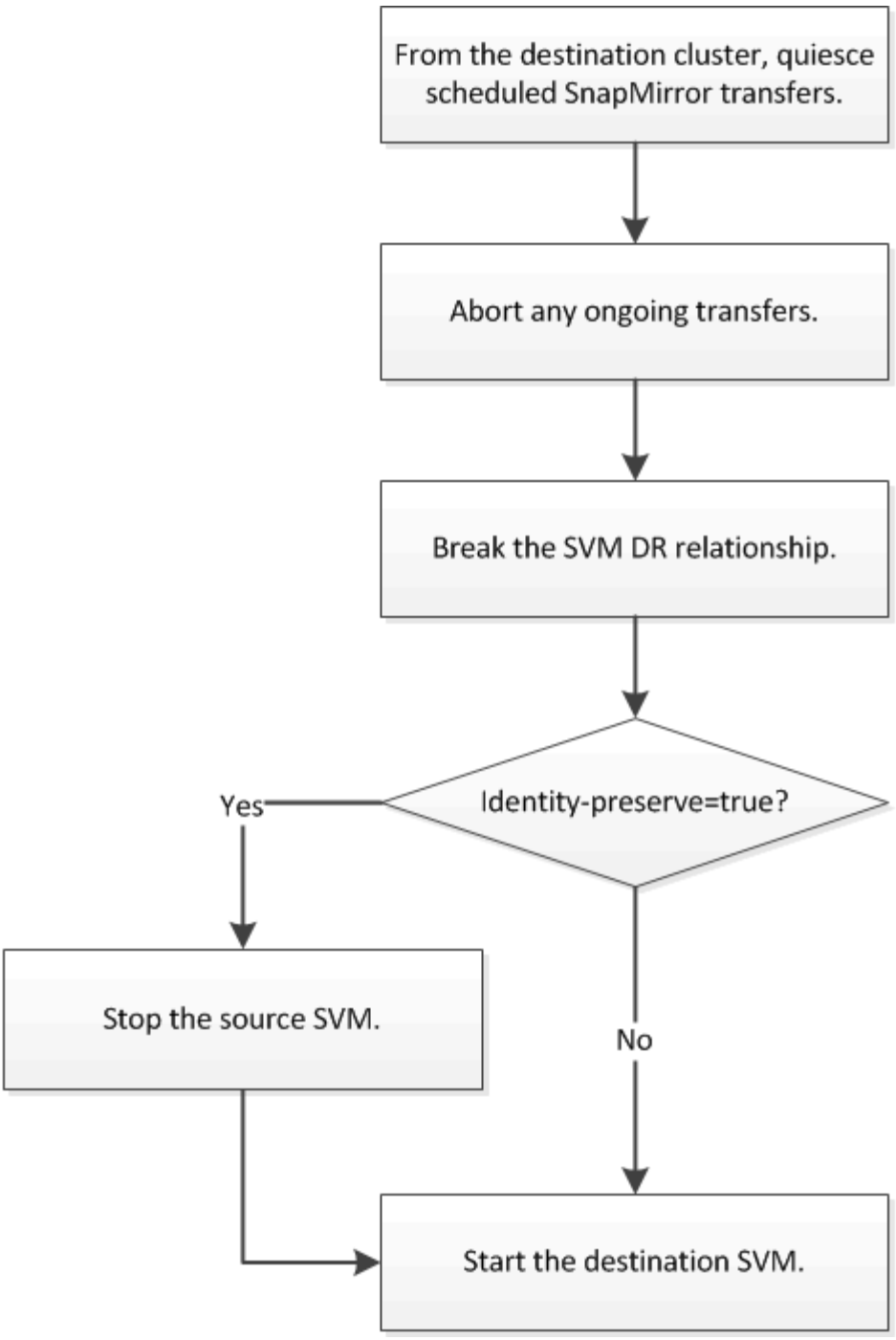
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Erstellen und initialisieren Sie die SVM-Replizierungsbeziehung, wie in beschrieben."Replizierung einer gesamten SVM-Konfiguration"

Bereitstellen von Daten von einem SnapMirror SVM DR-Ziel

Disaster-Recovery-Workflow von ONTAP SnapMirror SVM

Um nach einem Notfall die Daten der Ziel-SVM wiederherstellen zu können, müssen Sie die Ziel-SVM aktivieren. Die Aktivierung der Ziel-SVM beinhaltet das Anhalten geplanter SnapMirror Transfers, das Abbrechen fortlaufender SnapMirror Transfers, das Aufbrechen der Replizierungsbeziehung, das Anhalten der Quell-SVM und das Starten der Ziel-SVM.



Konfigurieren Sie das ONTAP SnapMirror SVM-Ziel-Volume als beschreibbar

Sie müssen SVM Ziel-Volumes schreibbar machen, bevor Sie Daten an Clients bereitstellen können.

Das Verfahren ist weitgehend identisch mit dem Verfahren zur Volume-Replikation, mit einer Ausnahme. Wenn Sie beim Erstellen der SVM-Replikationsbeziehung festlegen `-identity-preserve true` , müssen Sie die Quell-SVM vor der Aktivierung der Ziel-SVM anhalten.

Über diese Aufgabe

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

In einem Disaster-Recovery-Szenario können Sie kein SnapMirror Update von der Quell-SVM auf die SVM für das Disaster-Recovery-Ziel-SVM durchführen, da Ihre Quell-SVM und deren Daten nicht zugänglich sind, und da Updates aufgrund der letzten Neusynchronisierung möglicherweise schlecht oder beschädigt sind.

Ab ONTAP 9.8 können Sie mit System Manager im Notfall eine Ziel-Storage-VM aktivieren. Durch die Aktivierung der Ziel-Storage-VM werden die SVM Ziel-Volumes beschreibbar und können Sie Daten für die Clients bereitstellen.

Schritte

Sie können diese Aufgabe über System Manager oder die ONTAP CLI ausführen.

System Manager

1. Wenn auf das Quellcluster zugegriffen werden kann, überprüfen Sie, ob die SVM angehalten wurde: Navigieren Sie zu **Storage > Storage VMs** und prüfen Sie die Spalte **State** für die SVM.
2. Wenn der Quell-SVM-Status "läuft" ist, stoppen Sie ihn: Wählen Sie ⋮ und wählen Sie **Stop**.
3. Suchen Sie auf dem Ziel-Cluster die gewünschte Schutzbeziehung: Navigieren Sie zu **Schutz > Beziehungen**.
4. Bewegen Sie den Mauszeiger über den Namen der gewünschten Quell-Speicher-VM, klicken Sie auf ⋮, und wählen Sie **Ziel-Speicher-VM aktivieren**.
5. Wählen Sie im Fenster **Zielspeicher VM aktivieren Zielspeicher VM aktivieren und die Beziehung unterbrechen**.
6. Klicken Sie Auf **Aktivieren**.

CLI

1. Versetzen Sie die SVM vom Ziel-SVM oder Zielcluster in den Ruhezustand, um geplante Übertragungen zum Ziel zu stoppen:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

ⓘ In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel werden geplante Transfers zwischen der Quell-SVM `svm1` und der Ziel-SVM angehalten `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

Erfahren Sie mehr über `snapmirror quiesce` in der "ONTAP-Befehlsreferenz".

2. Stoppen Sie den laufenden Transfer von der Ziel-SVM oder dem Ziel-Cluster zum Ziel:

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

ⓘ In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Das folgende Beispiel stoppt laufende Transfers zwischen der Quell-SVM `svm1` und der Ziel-SVM `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

Erfahren Sie mehr über `snapmirror abort` in der "ONTAP-Befehlsreferenz".

3. Unterbrechen Sie die Replizierungsbeziehung von der Ziel-SVM oder dem Ziel-Cluster:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel wird die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM unterbrochen `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

4. Wenn Sie `-identity-preserve true` beim Erstellen der SVM-Replizierungsbeziehung festlegen, beenden Sie die Quell-SVM:

```
vserver stop -vserver <SVM>
```

Das folgende Beispiel stoppt die Quell-SVM `svm1`:

```
cluster_src::> vserver stop svm1
```

5. Starten der Ziel-SVM:

```
vserver start -vserver <SVM>
```

Das folgende Beispiel startet die Ziel-SVM `svm_backup`:

```
cluster_dst::> vserver start svm_backup
```

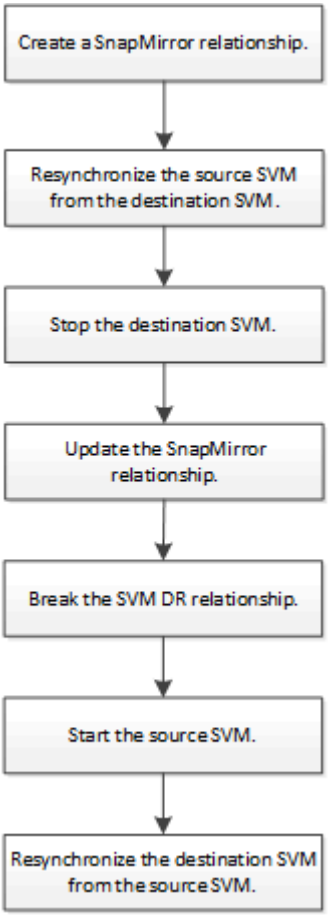
Nachdem Sie fertig sind

SVM-Ziel-Volumes für den Datenzugriff konfigurieren, wie in beschrieben."Konfiguration des Ziel-Volume für den Datenzugriff"

Reaktivieren Sie die SnapMirror Quell-SVM

Workflow zur erneuten Aktivierung der ONTAP SnapMirror Quell-SVM

Falls die Quell-SVM nach einem Ausfall vorhanden ist, können Sie sie erneut aktivieren und schützen, indem Sie die Disaster-Recovery-Beziehung zu SVM neu erstellen.



Aktivieren Sie die ursprüngliche ONTAP SnapMirror Quell-SVM erneut

Sie können die ursprüngliche Datensicherungsbeziehung zwischen Quell- und Ziel-SVM wiederherstellen, wenn Sie keine Daten mehr vom Ziel-Storage bereitstellen müssen. Das Verfahren ist weitgehend identisch mit dem Verfahren zur Volume-Replikation, mit einer Ausnahme. Vor der erneuten Aktivierung der Quell-SVM müssen Sie die Ziel-SVM beenden.

Bevor Sie beginnen

- Falls Sie die Größe des Ziel-Volumes erhöht und gleichzeitig die Daten bereit gestellt haben, sollten Sie vor der Reaktivierung des Quell-Volume die maximale Autogröße auf dem ursprünglichen Quell-Volume manuell erhöhen, um sicherzustellen, dass dieses ausreichend wachsen kann.

"Wenn ein Ziellaufwerk automatisch wächst"

Um Datenverlust zu vermeiden, sollte der Cluster-Administrator die Schreibvorgänge vom Client anhalten, bevor er die ursprüngliche Quell-SVM reaktiviert.

Über diese Aufgabe

Ab ONTAP 9.11.1 können Sie die Resynchronisierung während einer Disaster-Recovery-Probe verkürzen, indem Sie die CLI `-quick-resync true`-Option des `snapmirror resync` Befehls verwenden, während Sie eine SVM DR-Beziehung umkehren. Durch eine schnelle Neusynchronisierung kann sich die Zeit bis zur Produktionsrückführung verkürzen, da das Data Warehouse neu aufgebaut und Vorgänge wiederhergestellt werden müssen. Erfahren Sie mehr über `snapmirror resync` in der "ONTAP-Befehlsreferenz".

> Schnelle Neusynchronisierung sorgt nicht für eine Aufrechterhaltung der Storage-Effizienz der Ziel-Volumes. Durch die Aktivierung der schnellen Neusynchronisierung kann der Volume-Platz erhöht werden, der von den Ziel-Volumes belegt wird.

Bei diesem Verfahren wird vorausgesetzt, dass die Basis im ursprünglichen Quell-Volume intakt ist. Wenn die Baseline nicht intakt ist, müssen Sie die Beziehung zwischen dem Volume, das Sie Daten vom und dem ursprünglichen Quell-Volume bereitstellen, erstellen und initialisieren, bevor Sie den Vorgang durchführen.

Ab ONTAP 9.8 können Sie mit dem System Manager eine Quellspeicher-VM nach einem Ausfall reaktivieren.

Schritte

Diese Aufgabe können Sie mit dem System Manager oder der ONTAP Befehlszeilenschnittstelle (CLI) ausführen.

System Manager ONTAP 9.17.1 und höher

1. Wählen Sie im Zielcluster die gewünschte Schutzbeziehung aus: Klicken Sie auf **Schutz > Replikation**.
2. Bewegen Sie den Mauszeiger über den Quellnamen, klicken Sie ⋮ und klicken Sie auf **Umgekehrte Resynchronisierung**.
3. Klicken Sie im Fenster **Reverse Resync Relationship** auf **Reverse Resync**.

   Die Beziehung verschwindet aus der **Replikationstabelle** und wird nun vom ursprünglichen Quellcluster verwaltet.
4. Klicken Sie im ursprünglichen Quellcluster auf **Schutz > Replikation** und überprüfen Sie, ob die umgekehrte Resynchronisierung abgeschlossen ist, indem Sie prüfen, ob der Status **Gespiegelt** anzeigt.
5. Navigieren Sie im ursprünglichen Zielcluster zu **Cluster > Storage VMs**.
6. Suchen Sie die Speicher-VM, bewegen Sie den Mauszeiger über den Namen der Speicher-VM und klicken Sie. ⋮ und klicken Sie auf **Stopp**.
7. Klicken Sie im Fenster **Speicher-VM stoppen** auf **Stoppen**.
8. Navigieren Sie im Quellcluster zu **Schutz > Replikation** und suchen Sie die Speicher-VM, die Sie reaktivieren möchten. Bewegen Sie den Mauszeiger über den Namen der Speicher-VM und klicken Sie auf ⋮ und klicken Sie auf **Zielspeicher-VM aktivieren**.
9. Im Fenster **Ziel-Speicher-VM aktivieren** wählen Sie **Ziel-Speicher-VM aktivieren und Beziehung aufheben** und klicken Sie auf **Aktivieren**.
10. Wenn Sie zur Seite **Replikation** zurückkehren, bewegen Sie den Mauszeiger erneut über den Namen der Speicher-VM und klicken Sie auf ⋮ und klicken Sie auf **Umgekehrte Resynchronisierung**.

System Manager ONTAP 9.16.1 und früher

1. Wählen Sie auf dem Zielcluster die gewünschte Schutzbeziehung aus: Klicken Sie auf **Schutz > Beziehungen**.
2. Bewegen Sie den Mauszeiger über den Quellnamen, klicken Sie ⋮ und klicken Sie auf **Umgekehrte Resynchronisierung**.
3. Klicken Sie im Fenster **Reverse Resync Relationship** auf **Reverse Resync**.

   Die Beziehung verschwindet aus der Tabelle **Relationships**, da sie nun vom ursprünglichen Quellcluster verwaltet wird.
4. Klicken Sie im ursprünglichen Quellcluster auf **Schutz > Beziehungen** und überprüfen Sie, ob die umgekehrte Resynchronisierung abgeschlossen ist, indem Sie prüfen, ob der Status als **Gespiegelt** angezeigt wird.
5. Navigieren Sie im ursprünglichen Zielcluster zu **Speicher > Speicher-VMs**.
6. Suchen Sie die Speicher-VM, bewegen Sie den Mauszeiger über den Namen der Speicher-VM und klicken Sie. ⋮ und klicken Sie auf **Stopp**.
7. Klicken Sie im Fenster **Speicher-VM stoppen** auf **Stoppen**.
8. Suchen Sie im Quellcluster die Speicher-VM (die nun die Quell-SVM der umgekehrten Beziehung ist), bewegen Sie den Mauszeiger über den SVM-Namen und klicken Sie auf ⋮ und klicken Sie auf **Zielspeicher-VM aktivieren**.
9. Im Fenster **Ziel-Speicher-VM aktivieren** wählen Sie **Ziel-Speicher-VM aktivieren und Beziehung**

aufheben und klicken Sie auf **Aktivieren**.

10. Wenn Sie zur Seite **Beziehungen** zurückkehren, bewegen Sie den Mauszeiger erneut über den Namen der Speicher-VM und klicken Sie auf ⋮ und klicken Sie auf **Umgekehrte Resynchronisierung**.

CLI

1. Erstellen Sie aus der ursprünglichen SVM oder dem ursprünglichen Quell-Cluster eine Reverse-SVM-DR-Beziehung. Dabei verwenden Sie dieselbe Konfiguration, Richtlinie und dieselben Einstellungen wie für die ursprüngliche SVM-DR-Beziehung:

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

ⓘ In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel wird eine Beziehung zwischen der SVM, von der aus Sie Daten bereitstellen, `svm_backup` und der ursprünglichen Quell-SVM erstellt `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

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

2. Führen Sie in der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster den folgenden Befehl aus, um die Datensicherungsbeziehung umzukehren:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

ⓘ In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.

ⓘ Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein allgemeiner Snapshot vorhanden ist. Verwenden Sie `snapmirror initialize`, um die Beziehung neu zu initialisieren.

Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen SVM `svm1` und der SVM, von der aus Sie Daten bereitstellen, rückgängig gemacht `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

Beispiel mit -Quick-Resync-Option:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. Wenn Sie den Datenzugriff auf die ursprüngliche Quell-SVM wiederherstellen möchten, beenden Sie die ursprüngliche Ziel-SVM, um alle Clients, die derzeit mit der ursprünglichen Ziel-SVM verbunden sind, zu trennen.

```
vserver stop -vserver <SVM>
```

Im folgenden Beispiel wird die ursprüngliche Ziel-SVM angehalten, die derzeit Daten bereitstellt:

```
cluster_dst::> vserver stop svm_backup
```

4. Mit dem `vserver show` Befehl überprüfen Sie, ob die ursprüngliche Ziel-SVM den Status „angehalten“ aufweist.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. Führen Sie für die ursprüngliche Quell-SVM oder das ursprüngliche Quell-Cluster den folgenden Befehl aus, um die endgültige Aktualisierung der umgekehrten Beziehung durchzuführen, um alle Änderungen von der ursprünglichen Ziel-SVM auf die ursprüngliche Quell-SVM zu übertragen:

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

> In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, von der aus Sie Daten bereitstellen,`svm_backup`, und der ursprünglichen Quell-SVM aktualisiert `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

Erfahren Sie mehr über `snapmirror update` in der "ONTAP-Befehlsreferenz".

6. Führen Sie in der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster den folgenden Befehl aus, um geplante Transfers für die umgekehrte Beziehung zu beenden:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

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 endgültige Update abgeschlossen ist und die Beziehung für den Beziehungsstatus „stillgelegt“ anzeigt, führen Sie den folgenden Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster aus, um die umgekehrte Beziehung zu unterbrechen:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, von der aus Sie Daten bereitstellten, `svm_backup` und der ursprünglichen Quell-SVM, unterbrochen `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

8. Wenn die ursprüngliche Quell-SVM zuvor angehalten wurde, starten Sie aus dem ursprünglichen Quell-Cluster die ursprüngliche Quell-SVM:

```
vserver start -vserver <SVM>
```

Im folgenden Beispiel wird die ursprüngliche Quell-SVM gestartet:

```
cluster_src::> vserver start svm1
```

9. Wiederherstellung der ursprünglichen Datensicherungsbeziehung von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Das folgende Beispiel stellt die Beziehung zwischen der ursprünglichen Quell-SVM, `svm1` und der ursprünglichen Ziel-SVM wieder her `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. Führen Sie für die ursprüngliche Quell-SVM oder das ursprüngliche Quell-Cluster den folgenden Befehl aus, um die umgekehrte Datensicherungsbeziehung zu löschen:

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

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. Geben Sie für die ursprüngliche Ziel-SVM oder das ursprüngliche Ziel-Cluster die umgekehrte Datensicherungsbeziehung frei:

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel werden die umgekehrte Beziehung zwischen der ursprünglichen Ziel-SVM, SVM_Backup und der ursprünglichen Quell-SVM veröffentlicht. `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

Wie es weiter geht

- `snapmirror show`Überprüfen Sie mit dem Befehl, ob die SnapMirror Beziehung erstellt wurde.

  Erfahren Sie mehr über `snapmirror show` in der "ONTAP-Befehlsreferenz".

- Setzen Sie die Schreibvorgänge von Ihrem Client zur ursprünglichen Quell-SVM fort.

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror löschen"
- "snapmirror Initialisierung"
- "Snapmirror-Ruhezustand"
- "snapmirror Release"
- "SnapMirror-Neusynchronisierung"

Reaktivieren Sie die ursprüngliche ONTAP SnapMirror Quell-SVM für FlexGroup Volumes

Sie können die ursprüngliche Datensicherungsbeziehung zwischen Quell- und Ziel-SVM wiederherstellen, wenn Sie keine Daten mehr vom Ziel-Storage bereitstellen müssen. Um die ursprüngliche Quell-SVM erneut zu aktivieren, wenn Sie FlexGroup Volumes verwenden, müssen Sie einige weitere Schritte durchführen. Dazu gehören das Löschen der ursprünglichen SVM-DR-Beziehung und das Freigeben der ursprünglichen Beziehung, bevor Sie die Beziehung rückgängig machen. Außerdem müssen Sie die umgekehrte Beziehung freigeben und die ursprüngliche Beziehung neu erstellen, bevor Sie geplante Transfers anhalten.

Schritte

1. Löschen Sie auf der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster die ursprüngliche SVM-DR-Beziehung:

   ```
   snapmirror delete -source-path SVM: -destination-path SVM:
   ```

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

   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. Geben Sie von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster die ursprüngliche Beziehung frei, während die Snapshots intakt bleiben:

   ```
   snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
   -only true
   ```

In den `-source-path -destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel wird die ursprüngliche Beziehung zwischen der ursprünglichen Quell-SVM, svm1, und der ursprünglichen Ziel-SVM, freigegeben `svm_backup`.

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. Erstellen Sie aus der ursprünglichen SVM oder dem ursprünglichen Quell-Cluster eine Reverse-SVM-DR-Beziehung. Dabei verwenden Sie dieselbe Konfiguration, Richtlinie und dieselben Einstellungen wie für die ursprüngliche SVM-DR-Beziehung:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   In den `-source-path -destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

   Im folgenden Beispiel wird eine Beziehung zwischen der SVM, von der aus Sie Daten bereitstellen, `svm_backup` und der ursprünglichen Quell-SVM erstellt `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

4. Führen Sie in der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster den folgenden Befehl aus, um die Datensicherungsbeziehung umzukehren:

   `snapmirror resync -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   In den `-source-path -destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

   Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.

   Der Befehl schlägt fehl, wenn auf der Quelle und dem Ziel kein allgemeiner Snapshot vorhanden ist. Verwenden Sie `snapmirror initialize`, um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen SVM `svm1` und der SVM, von der aus Sie Daten bereitstellen, rückgängig gemacht `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

5. Wenn Sie den Datenzugriff auf die ursprüngliche Quell-SVM wiederherstellen möchten, beenden Sie die ursprüngliche Ziel-SVM, um alle Clients, die derzeit mit der ursprünglichen Ziel-SVM verbunden sind, zu trennen.

   `vserver stop -vserver SVM`

   Im folgenden Beispiel wird die ursprüngliche Ziel-SVM angehalten, die derzeit Daten bereitstellt:

   ```
   cluster_dst::> vserver stop svm_backup
   ```

6. Mit dem `vserver show` Befehl überprüfen Sie, ob die ursprüngliche Ziel-SVM den Status „angehalten“ aufweist.

   ```
   cluster_dst::> vserver show
                                     Admin      Operational Root
   Vserver        Type    Subtype    State      State       Volume
   Aggregate
   --------       ------- ---------- ---------- ----------- ----------
   ----------
   svm_backup     data    default    stopped    stopped     rv
   aggr1
   ```

7. Führen Sie für die ursprüngliche Quell-SVM oder das ursprüngliche Quell-Cluster den folgenden Befehl aus, um die endgültige Aktualisierung der umgekehrten Beziehung durchzuführen, um alle Änderungen von der ursprünglichen Ziel-SVM auf die ursprüngliche Quell-SVM zu übertragen:

   `snapmirror update -source-path SVM: -destination-path SVM:`

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, von der aus Sie Daten bereitstellen,`svm_backup`, und der ursprünglichen Quell-SVM aktualisiert `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup: -destination
   -path svm1:
   ```

   Erfahren Sie mehr über `snapmirror update` in der "ONTAP-Befehlsreferenz".

8. Führen Sie in der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster den folgenden Befehl aus, um geplante Transfers für die umgekehrte Beziehung zu beenden:

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

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:
```

Erfahren Sie mehr über `snapmirror quiesce` in der "ONTAP-Befehlsreferenz".

9. Wenn das endgültige Update abgeschlossen ist und die Beziehung für den Beziehungsstatus „stillgelegt“ anzeigt, führen Sie den folgenden Befehl von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster aus, um die umgekehrte Beziehung zu unterbrechen:

   `snapmirror break -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > In den `-source-path -destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, von der aus Sie Daten bereitstellten, `svm_backup` und der ursprünglichen Quell-SVM, unterbrochen `svm1`:

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

   Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

10. Wenn die ursprüngliche Quell-SVM zuvor angehalten wurde, starten Sie aus dem ursprünglichen Quell-Cluster die ursprüngliche Quell-SVM:

    `vserver start -vserver` *`SVM`*

    Im folgenden Beispiel wird die ursprüngliche Quell-SVM gestartet:

    ```
    cluster_src::> vserver start svm1
    ```

11. Löschen Sie ausgehend von der ursprünglichen SVM oder dem ursprünglichen Quell-Cluster die umgekehrte SVM-DR-Beziehung:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    > In den `-source-path -destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

    Im folgenden Beispiel wird die umgekehrte Beziehung zwischen der ursprünglichen Ziel-SVM, SVM_Backup, und der ursprünglichen Quell-SVM, gelöscht `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. Geben Sie von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster die umgekehrte Beziehung frei, während die Snapshots intakt bleiben:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

    Im folgenden Beispiel werden die vertauschte Beziehung zwischen der ursprünglichen Ziel-SVM, svm_Backup und der ursprünglichen Quell-SVM, svm1, freigegeben:

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1: -relationship-info-only true
    ```

13. Stellen Sie die ursprüngliche Beziehung aus der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster wieder her. Verwenden Sie dieselbe Einstellung für Konfiguration, Richtlinie und Identitätsbewahrung wie für die ursprüngliche SVM-DR-Beziehung:

    `snapmirror create -source-path SVM: -destination-path SVM:`

    > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

    Das folgende Beispiel erstellt eine Beziehung zwischen der ursprünglichen Quell-SVM, `svm1`, und dem ursprünglichen Ziel-SVM, `svm_backup`:

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

14. Wiederherstellung der ursprünglichen Datensicherungsbeziehung von der ursprünglichen Ziel-SVM oder dem ursprünglichen Ziel-Cluster

    `snapmirror resync -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

    > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

    Das folgende Beispiel stellt die Beziehung zwischen der ursprünglichen Quell-SVM, `svm1` und der ursprünglichen Ziel-SVM wieder her `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror löschen"
- "snapmirror Initialisierung"
- "Snapmirror-Ruhezustand"
- "snapmirror Release"
- "SnapMirror-Neusynchronisierung"

Synchronisieren Sie die Daten auf einer ONTAP SnapMirror Ziel-SVM erneut

ONTAP 9.11.1 bietet die Option, die Wiederherstellung eines gesamten Data Warehouses zu umgehen, wenn Sie eine Disaster-Recovery-Probe durchführen. So können Sie die Produktion schneller wiederkehren.

Ab ONTAP 9.8 können Sie mit System Manager die Daten- und Konfigurationsdetails von der Quell-Storage-VM zur Ziel-Storage-VM in einer unterbrochenen Sicherungsbeziehung neu synchronisieren und die Beziehung wiederherstellen.

Sie führen die Neusynchronisierung nur vom Ziel der ursprünglichen Beziehung durch. Der Resync löscht alle Daten in der Ziel-Storage-VM, die neuer sind als die Daten in der Quell-Storage-VM.

Schritte

Diese Aufgabe können Sie mit System Manager oder der ONTAP-CLI ausführen.

System Manager

1. Wählen Sie im Ziel die gewünschte Schutzbeziehung aus: Klicken Sie auf **Schutz > Beziehungen**.
2. Wählen Sie optional **Schnelle Resynchronisierung durchführen** aus, um einen kompletten Data Warehouse-Wiederaufbau während einer Disaster-Recovery-Probe zu umgehen.
3. Klicken Sie auf ⋮ **Resync**.
4. Überwachen Sie unter **Relationships** den Fortschritt der Neusynchronisierung, indem Sie **Transferstatus** für die Beziehung anzeigen.

CLI

1. Synchronisieren Sie die Beziehung vom Ziel-Cluster aus neu:

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

Verwandte Informationen

- "SnapMirror-Neusynchronisierung"

Umwandeln einer ONTAP SnapMirror Volume-DR-Beziehung in eine SVM-DR-Beziehung

Sie können Replizierungsbeziehungen zwischen Volumes in eine Replizierungsbeziehung zwischen den Storage Virtual Machines (SVMs) umwandeln, die die Volumes besitzen, vorausgesetzt, dass jedes Volume des Quellvolumes (mit Ausnahme des Root-Volumes) repliziert wird. Und jedes Volumen auf dem Quelldatenträger (einschließlich des Wurzelvolumens) hat den gleichen Namen wie das Volumen auf dem Zielspeicherort.

Über diese Aufgabe

Verwenden Sie den `volume rename` Befehl, wenn die SnapMirror-Beziehung inaktiv ist, um Ziel-Volumes umzubenennen, falls erforderlich. Erfahren Sie mehr über `volume rename` in der "ONTAP-Befehlsreferenz".

Schritte

1. Führen Sie auf der Ziel-SVM oder dem Ziel-Cluster den folgenden Befehl aus, um die Quell- und Ziel-Volumes neu zu synchronisieren:

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

   Erfahren Sie mehr über `snapmirror resync` in der "ONTAP-Befehlsreferenz".

   > Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume `volA` auf `svm1` und dem Ziel-Volume `volA` auf neu synchronisiert `svm_backup`:

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

2. Erstellen Sie eine SVM-Replizierungsbeziehung zwischen den Quell- und Ziel-SVMs, wie in beschrieben"Replizierung von SVM-Konfigurationen".

   Sie müssen die `-identity-preserve true` Option des `snapmirror create` Befehls beim Erstellen Ihrer Replikationsbeziehung verwenden.

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

3. Ziel-SVM stoppen:

   ```
   vserver stop -vserver SVM
   ```

   Erfahren Sie mehr über `vserver stop` in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel stoppt die Ziel-SVM `svm_backup`:

```
cluster_dst::> vserver stop svm_backup
```

4. Führen Sie auf der Ziel-SVM oder dem Ziel-Cluster den folgenden Befehl aus, um die Quell- und Ziel-SVMs neu zu synchronisieren:

   `snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP -policy <policy>`

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.
   >
   > Auch wenn die Resynchronisierung keinen Basistransfer erfordert, kann sie zeitaufwendig sein. Möglicherweise möchten Sie die Neusynchronisierung in Zeiten nach außerhalb der Stoßzeiten durchführen.

   Im folgenden Beispiel wird die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM neu synchronisiert `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Verwandte Informationen

- "snapmirror erstellen"
- "SnapMirror-Neusynchronisierung"

Löschen einer ONTAP SnapMirror SVM-Replikationsbeziehung

Sie können die `snapmirror delete` `snapmirror release` Befehle und verwenden, um eine SVM-Replizierungsbeziehung zu löschen. Sie können dann nicht benötigte Ziel-Volumes manuell löschen. Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Über diese Aufgabe

Mit dem `snapmirror release` Befehl werden alle von SnapMirror erstellten Snapshots aus der Quelle gelöscht. Sie können die Option verwenden `-relationship-info-only`, um die Snapshots beizubehalten.

Schritte

1. Führen Sie den folgenden Befehl von der Ziel-SVM oder dem Ziel-Cluster aus, um die Replizierungsbeziehung zu unterbrechen:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

Im folgenden Beispiel wird die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM unterbrochen `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

Erfahren Sie mehr über `snapmirror break` in der "ONTAP-Befehlsreferenz".

2. Führen Sie den folgenden Befehl von der Ziel-SVM oder dem Ziel-Cluster aus, um die Replikationsbeziehung zu löschen:

   `snapmirror delete -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der Quell-SVM `svm1` und der Ziel-SVM gelöscht `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

   Erfahren Sie mehr über `snapmirror delete` in der "ONTAP-Befehlsreferenz".

3. Führen Sie den folgenden Befehl für das Quell-Cluster bzw. die Quell-SVM aus, um die Informationen für die Replizierungsbeziehung von der Quell-SVM freizugeben:

   `snapmirror release -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > In den `-source-path` `-destination-path` Optionen und müssen Sie nach dem SVM-Namen einen Doppelpunkt (:) eingeben. Siehe das folgende Beispiel.

   Im folgenden Beispiel werden Informationen für die angegebene Replikationsbeziehung von der Quell-SVM freigegeben `svm1`:

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

   Erfahren Sie mehr über `snapmirror release` in der "ONTAP-Befehlsreferenz".

Management der SnapMirror Root-Volume-Replizierung

Erfahren Sie mehr über die ONTAP SnapMirror-Root-Volume-Replikation

Jede SVM in einer NAS-Umgebung verfügt über einen eindeutigen Namespace. Der

Einstiegspunkt zur Namespace-Hierarchie ist das SVM_Root-Volume_ mit Betriebssystem und zugehörigen Informationen. Damit Clients im Falle eines Node-Ausfalls oder eines Failover weiterhin auf die Daten zugreifen können, sollte eine gespiegelte Kopie des SVM-Root-Volumes erstellt werden.

Die Load-Sharing-Spiegelungen für SVM Root-Volumes dienen hauptsächlich nicht mehr zur Lastverteilung, sondern dienen der Disaster Recovery.

- Wenn das Root-Volume vorübergehend nicht verfügbar ist, bietet die Load-Sharing-Spiegelung automatisch schreibgeschützten Zugriff auf Root-Volume-Daten.
- Wenn das Root-Volume dauerhaft nicht verfügbar ist, können Sie eines der Load-Sharing-Volumes heraufstufen, um Schreibzugriff auf das Root-Volume-Daten zu ermöglichen.

Erstellen und Initialisieren von ONTAP-Spiegelbeziehungen zur Lastverteilung

Sie sollten für jedes SVM-Root-Volume, das NAS-Daten im Cluster bereitstellt, einen Load-Sharing-Spiegel (LSM) erstellen. Für Cluster mit zwei oder mehr HA-Paaren sollten Sie Load-Sharing-Spiegel der SVM-Root-Volumes in Betracht ziehen, um sicherzustellen, dass der Namespace für Clients zugänglich bleibt, falls beide Knoten eines HA-Paares ausfallen. Load-Sharing-Spiegel sind nicht für Cluster mit einem einzigen HA-Paar geeignet.

Bevor Sie beginnen

Ab ONTAP 9.16.1 kann beim Erstellen einer Lastverteilungsspiegelbeziehung für die Ziel-SVM kein Speicherlimit aktiviert werden.

Über diese Aufgabe

Wenn Sie auf demselben Node ein LSM erstellen und der Node nicht verfügbar ist, liegt ein Single Point of Failure bei und Sie verfügen nicht über eine zweite Kopie, um sicherzustellen, dass die Daten für Clients verfügbar bleiben. Wenn Sie aber das LSM auf einem anderen Node als dem mit dem Root-Volume oder auf einem anderen HA-Paar erstellen, sind die Daten im Falle eines Ausfalls weiterhin verfügbar.

Beispiel: In einem Cluster mit vier Nodes mit einem Root-Volume auf drei Nodes:

- Erstellen Sie für das Root-Volume in HA 1 Node 1 das LSM auf HA 2 Node 1 oder HA 2 Node 2.
- Erstellen Sie für das Root-Volume in HA 1 Node 2 das LSM auf HA 2 Node 1 oder HA 2 Node 2.
- Erstellen Sie für das Root-Volume in HA 2 Node 1 das LSM auf HA 1 Node 1 oder HA 1 Node 2.

Schritte

1. Zielvolume für das LSM erstellen:

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

   Das Zielvolumen sollte gleich oder größer sein als das Root-Volume.

   Es empfiehlt sich, das Root- und Ziel-Volume mit Suffixen wie `_root` und `_m1`zu benennen.

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

Das folgende Beispiel erstellt ein Load-Sharing-Spiegelvolume 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. "Erstellen Sie einen Zeitplan für Replikations-Jobs".
3. Erzeugung einer Load-Sharing-Mirror-Beziehung zwischen dem SVM Root-Volume und dem Ziel-Volume für das LSM:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

Das folgende Beispiel erstellt eine Load-Sharing-Spiegelbeziehung zwischen dem Root-Volume `svm1_root` und dem Load-Sharing-Spiegelvolume `svm1_m1`:

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

Das Typattribut der Load-Sharing-Spiegelung ändert sich von `DP` zu `LS`.

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

4. Initialisieren Sie die Load-Sharing-Spiegelung:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

Im folgenden Beispiel wird die Load-Sharing-Spiegelung für das Root-Volume initialisiert `svm1_root`:

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

Erfahren Sie mehr über `snapmirror initialize` in der "ONTAP-Befehlsreferenz".

Aktualisieren einer ONTAP-Beziehung zur Lastverteilung einer Spiegelung

LSM-Beziehungen (Load-Sharing Mirror) werden automatisch für SVM-Root-Volumes aktualisiert, nachdem ein Volume in der SVM gemountet oder abgehängt wurde, sowie während `volume create` Operationen, die die Option umfassen `junction-path`. Sie können eine LSM-Beziehung manuell aktualisieren, wenn sie vor dem nächsten geplanten Update aktualisiert werden soll.

Mirror Relationships werden unter folgenden Umständen automatisch aktualisiert:

- Es ist Zeit für ein geplantes Update
- Auf einem Volume im SVM-Root-Volume wird ein Mount- oder Unmount-Vorgang durchgeführt
- A `volume create` Befehl ausgegeben wird, der die `junction-path` Option

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

Schritt

1. Manuelles Aktualisieren einer Mirror-Beziehung zur Lastverteilung:

   Sie müssen die Variablen in Winkelklammern durch die erforderlichen Werte ersetzen, bevor Sie diesen Befehl ausführen.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   Das folgende Beispiel aktualisiert die Load-Sharing-Spiegelbeziehung für das Root-Volume `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

   Erfahren Sie mehr über `snapmirror update` in der "ONTAP-Befehlsreferenz".

Hochstufen einer ONTAP-Spiegelung zur Lastverteilung

Wenn ein Root-Volume dauerhaft nicht verfügbar ist, können Sie das LSM-Volumen (Load Sharing Mirror) heraufstufen, um Schreibzugriff auf das Root-Volume-Daten zu ermöglichen.

Bevor Sie beginnen

Sie müssen Befehle der erweiterten Berechtigungsebene für diese Aufgabe verwenden.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Hochstufen eines LSM-Volumes:

   Sie müssen die Variablen in Winkelklammern durch die erforderlichen Werte ersetzen, bevor Sie diesen Befehl ausführen.

   ```
   snapmirror promote -destination-path <SVM:volume>
   ```

   Im folgenden Beispiel wird das Volume `svm1_m2` als neues SVM-Root-Volume befördert:

```
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
```

Geben Sie Ein. `y` ONTAP macht das LSM Volumen zu einem Lese-/Schreib-Volumen und löscht das ursprüngliche Root-Volumen, wenn er zugänglich ist.

> Das hochgestuften Root-Volume verfügt möglicherweise nicht über alle Daten, die sich im ursprünglichen Root-Volume befand, wenn die letzte Aktualisierung in letzter Zeit nicht erfolgt war.

Erfahren Sie mehr über `snapmirror promote` in der "ONTAP-Befehlsreferenz".

3. Zurück zur Administrator-Berechtigungsebene:

```
set -privilege admin
```

4. Benennen Sie das beworbene Volume nach der Namenskonvention um, die Sie für das Root-Volume verwendet haben:

   Sie müssen die Variablen in Winkelklammern durch die erforderlichen Werte ersetzen, bevor Sie diesen Befehl ausführen.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

   Im folgenden Beispiel wird das hochgestufte Volume `svm1_m2` mit dem Namen umbenannt `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Schützen Sie das umbenannte Root-Volume, wie in Schritt 3 bis Schritt 4 in beschrieben"Erstellen und Initialisieren von Mirror-Beziehungen zur Lastverteilung".

Backup in die Cloud

Installieren Sie eine ONTAP SnapMirror Cloud-Lizenz

SnapMirror-Cloud-Beziehungen können über vorqualifizierte Backup-Applikationen von Drittanbietern orchestriert werden. Ab ONTAP 9.9.1 können Sie System Manager auch

zur Orchestrierung der SnapMirror Cloud-Replizierung verwenden. Wenn Sie mit System Manager On-Premises-ONTAP zu Objekt-Storage-Backups orchestrieren, sind sowohl SnapMirror- als auch SnapMirror Cloud-Kapazitätslizenzen erforderlich. Außerdem müssen Sie die SnapMirror Cloud API-Lizenz anfordern und installieren.

Über diese Aufgabe

Bei den Lizenzen für SnapMirror Cloud und SnapMirror S3 handelt es sich um Cluster-Lizenzen und nicht um Node-Lizenzen. Sie werden also nicht mit dem Lizenzpaket ONTAP One ausgeliefert. Diese Lizenzen sind in dem separaten ONTAP One Kompatibilitätspaket enthalten. Wenn Sie SnapMirror Cloud aktivieren möchten, müssen Sie dieses Bundle anfordern.

Zusätzlich ist für die Orchestrierung von SnapMirror Cloud Backups in Objekt-Storage bei System Manager ein SnapMirror Cloud API-Schlüssel erforderlich. Bei dieser API-Lizenz handelt es sich um eine Cluster-weite Einzelinstanz-Lizenz, d. h., sie muss nicht auf jedem Node im Cluster installiert werden.

Schritte

Sie müssen das ONTAP One Compatibility Bundle und die SnapMirror Cloud API Lizenz anfordern, herunterladen und dann mit System Manager installieren.

1. Suchen Sie die Cluster-UUID für den Cluster, den Sie lizenzieren möchten, und notieren Sie ihn.

   Die Cluster-UUID ist erforderlich, wenn Sie Ihre Anforderung senden, das ONTAP One Compatibility Bundle für Ihr Cluster zu bestellen.

2. Wenden Sie sich an Ihr NetApp Vertriebsteam und fordern Sie das ONTAP One Compatibility Bundle an.
3. Befolgen Sie die Anweisungen auf der NetApp Support-Website, um die SnapMirror Cloud-API-Lizenz anzufordern.

   "Lizenzschlüssel für SnapMirror Cloud-API anfordern"

4. Wenn Sie die Lizenzdateien erhalten und heruntergeladen haben, laden Sie die ONTAP-Cloud-Kompatibilitäts-NLF und die SnapMirror-Cloud-API-NLF mit System Manager auf das Cluster hoch:
   a. Klicken Sie Auf **Cluster > Einstellungen**.
   b. Klicken Sie im Fenster **Einstellungen** auf **Lizenzen**.
   c. Klicken Sie im Fenster **Lizenzen** auf + Add .
   d. Klicken Sie im Dialogfeld **Lizenz hinzufügen** auf **Durchsuchen**, um die heruntergeladene Lizenzdatei auszuwählen, und klicken Sie dann auf **Hinzufügen**, um die Datei auf den Cluster hochzuladen.

Verwandte Informationen

"Daten mit SnapMirror in der Cloud sichern"

"Suche nach NetApp Softwarelizenzen"

Daten-Backups in der Cloud mit ONTAP SnapMirror –

Ab ONTAP 9.9 können Sie Ihre Daten-Backups in der Cloud erstellen und Ihre Daten aus dem Cloud-Storage auf einem anderen Volume mit System Manager wiederherstellen. Sie können StorageGRID oder ONTAP S3 als Cloud-Objektspeicher verwenden.

Beginnend mit ONTAP 9.18.1:

- SnapMirror cloud unterstützt Sicherungs- und Wiederherstellungsvorgänge für FlexGroup Volumes auf MetroCluster Konfigurationen mithilfe des bestehenden "ONTAP REST-APIs". Diese Funktionalität ermöglicht es Ihnen, SnapMirror cloud-Beziehungen für FlexGroup Volumes auf MetroCluster Konfigurationen zu erstellen, die nach einem Switchover und Switchback vom Partnerstandort aus verwaltet werden.

Ab ONTAP 9.16.1:

- SnapMirror Cloud Backup unterstützt Fan-out-Beziehungen. Das bedeutet, dass SnapMirror Backups gleichzeitig auf zwei verschiedenen Objektspeichern erstellt werden können. Mit ONTAP 9.16.1 unterstützt SnapMirror Cloud zwei Fan-out-Beziehungen. Fan-Outs können auf zwei Objektspeicher und auf einen oder zwei Buckets in zwei verschiedenen Objektspeichern ausgeführt werden. Versuche, mehr als zwei Fan-out-Beziehungen zu erstellen, schlagen fehl.
- Die SnapMirror Cloud unterstützt Backups von Volumes, die in die Cloud migriert wurden, mithilfe eines effizienteren Synchronisierungsprozesses"ONTAP REST-APIs", der auf bestehenden Daten läuft. Die Funktion unterstützt SnapMirror Cloud-Backups von einem migrierten Volume in der Cloud zum selben Ziel-Objektspeicher-Endpunkt, ohne dass ein neuer Basisplanvorgang erforderlich ist. Es werden sowohl FlexVol- als auch FlexGroup-Volumes unterstützt.

Bevor Sie die SnapMirror-Cloud-Funktion verwenden, sollten Sie einen Lizenzschlüssel für die SnapMirror-API auf der NetApp Support-Website anfordern: "Lizenzschlüssel für SnapMirror Cloud-API anfordern". Wenn Sie die Anweisungen befolgen, sollten Sie eine einfache Beschreibung Ihrer Geschäftsmöglichkeit angeben und den API-Schlüssel anfordern, indem Sie eine E-Mail an die angegebene E-Mail-Adresse senden. Sie sollten innerhalb von 24 Stunden eine E-Mail-Antwort erhalten, die weitere Anweisungen zum Erwerb des API-Schlüssels enthält.

Fügen Sie einen Cloud-Objektspeicher hinzu

Bevor Sie SnapMirror Cloud-Backups konfigurieren, müssen Sie einen StorageGRID oder ONTAP S3 Cloud-Objektspeicher hinzufügen.

Schritte

1. Klicken Sie Auf **Schutz > Übersicht > Cloud Object Stores**.
2. Klicken Sie Auf + Add .

Sichern Sie das Backup mit der Standardrichtlinie

Mit der standardmäßigen Cloud-Sicherungsrichtlinie DailyBackup können Sie schnell ein SnapMirror Cloud-Backup für ein vorhandenes Volume konfigurieren.

Schritte

1. Klicken Sie auf **Schutz > Übersicht** und wählen Sie **Sichern von Volumes in der Cloud**.
2. Wenn Sie zum ersten Mal Backups in der Cloud durchführen, geben Sie Ihren Lizenzschlüssel für die SnapMirror Cloud-API wie angegeben in das Lizenzfeld ein.
3. Klicken Sie auf **Authentifizieren und fortfahren**.
4. Wählen Sie ein Quell-Volume aus.
5. Wählen Sie einen Cloud-Objektspeicher aus.
6. Klicken Sie Auf **Speichern**.

Erstellen einer benutzerdefinierten Cloud-Backup-Richtlinie

Wenn Sie nicht die Standard-Cloud-Richtlinie von DailyBackup für Ihre SnapMirror-Cloud-Backups verwenden möchten, können Sie Ihre eigene Richtlinie erstellen.

Schritte

1. Klicken Sie auf **Schutz > Übersicht > Lokale Richtlinieneinstellungen** und wählen Sie **Schutzrichtlinien**.
2. Klicken Sie auf **Hinzufügen** und geben Sie die neuen Richtlinien-Details ein.
3. Wählen Sie im Abschnitt **Richtlinientyp** die Option **in der Cloud sichern** aus, um anzugeben, dass Sie eine Cloud-Richtlinie erstellen.
4. Klicken Sie Auf **Speichern**.

Erstellen Sie ein Backup auf der Seite Volumes

Sie können die Seite System Manager **Volumes** verwenden, wenn Sie Cloud-Backups für mehrere Volumes gleichzeitig auswählen und erstellen möchten oder wenn Sie eine benutzerdefinierte Schutzrichtlinie verwenden möchten.

Schritte

1. Klicken Sie Auf **Storage > Volumes**.
2. Wählen Sie die Volumes aus, die Sie in der Cloud sichern möchten, und klicken Sie auf **Protect**.
3. Klicken Sie im Fenster **Protect Volume** auf **More Options**.
4. Wählen Sie eine Richtlinie aus.

   Sie können die Standardrichtlinie, DailyBackup oder eine von Ihnen erstellte benutzerdefinierte Cloud-Richtlinie auswählen.

5. Wählen Sie einen Cloud-Objektspeicher aus.
6. Klicken Sie Auf **Speichern**.

Wiederherstellung aus der Cloud

Mit System Manager können gesicherte Daten aus dem Cloud-Storage auf einem anderen Volume im Quell-Cluster wiederhergestellt werden.

> Wenn Sie ONTAP 9.16.1 oder höher verwenden und einzelne Dateien in der SnapMirror Cloud auf einem FlexGroup Volume wiederherstellen, sollten Sie Dateien nur in einem neuen Verzeichnis im FlexGroup Volume wiederherstellen, und auf dem FlexGroup Ziel-Volume müssen granulare Daten festgelegt werden. `advanced` Weitere Informationen zum Einstellen der `-granular-data advanced` Option finden Sie unter "Gleichen Sie ONTAP FlexGroup-Volumes aus, indem Sie Dateidaten neu verteilen".

Schritte

1. Klicken Sie im Quellcluster einer SnapMirror-zu-Cloud-Beziehung auf **Speicher > Volumes**.
2. Wählen Sie das wiederherzustellende Volume aus.
3. Wählen Sie die Registerkarte * Backup to Cloud* aus.
4. Klicken Sie ⋮ neben dem Quellvolume, das Sie wiederherstellen möchten, um das Menü anzuzeigen, und wählen Sie **Wiederherstellen**.

5. Wählen Sie unter **Source** eine Speicher-VM aus und geben Sie dann den Namen des Volumes ein, auf dem die Daten wiederhergestellt werden sollen.
6. Wählen Sie unter **Destination** den Snapshot aus, den Sie wiederherstellen möchten.
7. Klicken Sie Auf **Speichern**.

Löschen einer SnapMirror Cloud-Beziehung

Mit System Manager können Sie eine Cloud-Beziehung löschen.

Schritte

1. Klicken Sie auf **Storage > Volumes** und wählen Sie das Volume aus, das Sie löschen möchten.
2. Klicken Sie neben dem Quellvolume auf ⋮ und wählen Sie **Löschen**.
3. Wählen Sie **Löschen Sie den Endpunkt des Cloud-Objektspeichers (optional)** aus, wenn Sie den Endpunkt des Cloud-Objektspeichers löschen möchten.
4. Klicken Sie Auf **Löschen**.

Cloud-Objektspeicher entfernen

Mit System Manager kann ein Cloud-Objektspeicher entfernt werden, wenn er nicht Teil einer Cloud-Backup-Beziehung ist. Ein Cloud-Objektspeicher, der Teil einer Cloud-Backup-Beziehung ist, kann auch nicht gelöscht werden.

Schritte

1. Klicken Sie Auf **Schutz > Übersicht > Cloud Object Stores**.
2. Wählen Sie den zu löschenden Objektspeicher aus, klicken Sie auf ⋮ und wählen Sie **Löschen**.

Daten sichern mit NetApp Backup and Recovery

Ab ONTAP 9.9.1 können Sie mit System Manager Daten in der Cloud mithilfe des NetApp Backup and Recovery-Dienstes sichern.

Backup and Recovery unterstützt FlexVol Lese-/Schreib-Volumes und Data-Protection-Volumes (DP). Ab ONTAP 9.12.1 unterstützt Backup and Recovery FlexGroup -Volumes und SnapLock -Volumes.

Erfahren Sie mehr über "NetApp Backup und Recovery" .

Bevor Sie beginnen

Sie sollten die folgenden Schritte ausführen, um ein Konto in der NetApp Konsole einzurichten. Für das Dienstkonto müssen Sie die Rolle „Kontoadministrator“ erstellen. (Andere Dienstkontorollen verfügen nicht über die erforderlichen Berechtigungen, um eine Verbindung vom System Manager herzustellen.)

1. "Erstellen Sie ein Konto in der NetApp Konsole" .
2. "Erstellen Sie einen Konsolenagenten in der NetApp Konsole"bei 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 können Sie StorageGRID als Cloud-Backup-Anbieter auswählen, jedoch nur, wenn die NetApp Konsole vor Ort bereitgestellt wird. Der Konsolenagent muss vor Ort installiert und über die Software-as-a-Service-Anwendung (SaaS) der NetApp -Konsole verfügbar sein.

3. "Abonnieren Sie NetApp Backup and Recovery in der NetApp -Konsole"(erfordert die entsprechende Lizenz).
4. "Generieren Sie einen Zugriffsschlüssel und einen geheimen Schlüssel mit der NetApp Konsole" .

Registrieren Sie den Cluster bei der NetApp Konsole

Sie können den Cluster bei der NetApp Konsole registrieren, indem Sie entweder die Konsole oder den System Manager verwenden.

Schritte

1. Gehen Sie in System Manager zu **Protection Overview**.
2. Geben Sie unter * NetApp Backup and Recovery* die folgenden Details an:
   - Client-ID
   - Geheimschlüssel des Kunden
3. Wählen Sie **Registrieren und fortfahren**.

NetApp Backup und Recovery aktivieren

Nachdem der Cluster bei der NetApp Konsole registriert wurde, müssen Sie NetApp Backup and Recovery aktivieren und die erste Sicherung in die Cloud starten.

Schritte

1. Wählen Sie im System Manager **Schutz > Übersicht**, und blättern Sie dann zum Abschnitt **Cloud Backup Service**.
2. Geben Sie die **Client-ID** und **Client Secret** ein.

   Ab ONTAP 9.10.1 erfahren Sie mehr über die Kosten für die Nutzung der Cloud, indem Sie **Weitere Informationen zu den Kosten für die Nutzung der Cloud** auswählen.

3. Wählen Sie **Verbinden und Cloud Backup Service aktivieren**.
4. Geben Sie auf der Seite * NetApp Backup and Recovery aktivieren* je nach ausgewähltem Anbieter die folgenden Details ein.

Für diesen Cloud-Provider…	Geben Sie die folgenden Daten ein…
Azure	• Azure-Abonnement-ID • Region • Name der Ressourcengruppe (vorhanden oder neu)

AWS	• Konto-ID für AWS • Zugriffsschlüssel • Geheimer Schlüssel • Region
Google Cloud-Projekt (GCP)	• Name des Google Cloud-Projekts • Google Cloud Access-Schlüssel • Google Cloud Secret-Schlüssel • Region
StorageGRID (ONTAP 9.10.1 und höher und nur für die lokale Bereitstellung der NetApp Konsole)	• Server • SG-Zugriffsschlüssel • SG Geheimschlüssel

5. Wählen Sie eine **Schutzrichtlinie**:
   - **Bestehende Richtlinie**: Wählen Sie eine bestehende Richtlinie.
   - **Neue Richtlinie**: Geben Sie einen Namen an und richten Sie einen Übertragungsplan ein.

     Ab ONTAP 9.10.1 können Sie angeben, ob die Archivierung mit Azure oder AWS aktiviert werden soll.

     Wenn Sie die Archivierung für ein Volume mit Azure oder AWS aktivieren, können Sie die Archivierung nicht deaktivieren.

     Wenn Sie die Archivierung für Azure oder AWS aktivieren, geben Sie Folgendes an:

     - Die Anzahl der Tage, nach denen das Volume archiviert wird.
     - Die Anzahl der im Archiv zu behaltenden Backups. Geben Sie „0“ (Null) an, um das letzte Backup zu archivieren.
     - Wählen Sie für AWS die Archiv-Storage-Klasse aus.
6. Wählen Sie die Volumes aus, die Sie sichern möchten.
7. Wählen Sie **Speichern**.

Bearbeiten Sie die für NetApp Backup and Recovery verwendete Schutzrichtlinie

Sie können ändern, welche Schutzrichtlinie mit NetApp Backup and Recovery verwendet wird.

Schritte

1. Wählen Sie im System Manager **Schutz > Übersicht**, und blättern Sie dann zum Abschnitt **Cloud Backup Service**.
2. Wählen Sie ⋮, dann **Bearbeiten**.
3. Wählen Sie eine **Schutzrichtlinie**:
   - **Bestehende Richtlinie**: Wählen Sie eine bestehende Richtlinie.

- **Neue Richtlinie**: Geben Sie einen Namen an und richten Sie einen Übertragungsplan ein.

  Ab ONTAP 9.10.1 können Sie angeben, ob die Archivierung mit Azure oder AWS aktiviert werden soll.

  Wenn Sie die Archivierung für ein Volume mit Azure oder AWS aktivieren, können Sie die Archivierung nicht deaktivieren.

  Wenn Sie die Archivierung für Azure oder AWS aktivieren, geben Sie Folgendes an:

  - Die Anzahl der Tage, nach denen das Volume archiviert wird.
  - Die Anzahl der im Archiv zu behaltenden Backups. Geben Sie „0“ (Null) an, um das letzte Backup zu archivieren.
  - Wählen Sie für AWS die Archiv-Storage-Klasse aus.

4. Wählen Sie **Speichern**.

Sicherung neuer Volumes oder LUNs in der Cloud

Wenn Sie ein neues Volume oder eine neue LUN erstellen, kann eine SnapMirror-Sicherungsbeziehung eingerichtet werden, die ein Backup in der Cloud für das Volume oder die LUN ermöglicht.

Bevor Sie beginnen

- Sie sollten eine SnapMirror Lizenz haben.
- Intercluster LIFs sollten konfiguriert werden.
- NTP sollte konfiguriert sein.
- Cluster muss ONTAP 9.9.1 oder höher ausführen.

Über diese Aufgabe

Die folgenden Cluster-Konfigurationen bieten keinen Schutz für neue Volumes oder LUNs in der Cloud:

- Der Cluster darf sich nicht in einer MetroCluster-Umgebung befinden.
- SVM-DR wird nicht unterstützt.
- FlexGroup -Volumes können nicht mit NetApp Backup and Recovery gesichert werden.

Schritte

1. Wenn Sie ein Volume oder eine LUN bereitstellen, aktivieren Sie auf der Seite **Protection** in System Manager das Kontrollkästchen **Enable SnapMirror (Local oder Remote)**.
2. Wählen Sie den Richtlinientyp „Sicherungs- und Wiederherstellungsrichtlinie“ aus.
3. Wenn „Backup und Wiederherstellung“ nicht aktiviert ist, wählen Sie „Sicherung mit NetApp Backup und Wiederherstellung aktivieren“ aus.

Schutz vorhandener Volumes oder LUNs in der Cloud

Sie können eine SnapMirror Sicherungsbeziehung für vorhandene Volumes und LUNs erstellen.

Schritte

1. Wählen Sie ein vorhandenes Volume oder eine vorhandene LUN aus, und wählen Sie **protect** aus.

2. Geben Sie auf der Seite **Volumes schützen** als Schutzrichtlinie **Sicherung mit NetApp Backup and Recovery** an.
3. Wählen Sie **Schutz**.
4. Aktivieren Sie auf der Seite **Schutz** das Kontrollkästchen **SnapMirror aktivieren (lokal oder Remote)**.
5. Wählen Sie **Verbinden und NetApp Backup and Recovery aktivieren**.

Wiederherstellung von Daten aus Backup-Dateien

Sie können Sicherungsverwaltungsvorgänge wie das Wiederherstellen von Daten, Aktualisieren von Beziehungen und Löschen von Beziehungen nur durchführen, wenn Sie die NetApp Konsole verwenden. Weitere Informationen finden Sie unter "Wiederherstellen von Daten aus Backup-Dateien" für weitere Informationen.

Archivierung und Compliance mit SnapLock Technologie

Erfahren Sie mehr über ONTAP SnapLock

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

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

Mit SnapLock können Sie Dateien und Snapshots in WORM-Storage übertragen und Aufbewahrungszeiträume für WORM-geschützte Daten festlegen. SnapLock WORM Storage nutzt die NetApp Snapshot Technologie und kann die SnapMirror Replikation nutzen, und SnapVault Backups als Basistechnologie für den Schutz der Backup Recovery für Daten. Erfahren Sie mehr über WORM-Speicherung: "Worm-Speicherung gemäß NetApp SnapLock - TR-4526".

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

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

- Sie können SnapLock für SnapVault verwenden, um WORM-gesicherte Snapshots auf dem Sekundärspeicher zu erstellen. Siehe "Setzen Sie Snapshots auf WORM".
- WORM-Dateien können zur Disaster Recovery an einen anderen geografischen Standort repliziert werden. Siehe "Spiegelung VON WORM-Dateien".

SnapLock ist eine lizenzbasierte Funktion von ONTAP. Mit einer einzigen Lizenz sind Sie berechtigt, SnapLock im strikten Compliance-Modus zu nutzen, um externe Vorgaben wie SEC Rule 17a-4(f) zu erfüllen, und im weniger strengen Enterprise-Modus, um intern vorgeschriebene Vorschriften zum Schutz digitaler Vermögenswerte zu erfüllen. SnapLock -Lizenzen sind Teil der "ONTAP One" Software-Suite.

SnapLock wird auf allen AFF und FAS Systemen sowie auf ONTAP Select unterstützt. SnapLock ist keine rein softwarebasierte Lösung, sondern eine integrierte Hardware- und Softwarelösung. Diese Unterscheidung ist wichtig für strenge WORM-Regelungen wie SEC 17a-4(f), die eine integrierte Hardware- und Softwarelösung erfordert. Weitere Informationen finden Sie unter "SEC Guidance to Broker-Dealers on the use of Electronic Storage Media".

Ihre Möglichkeiten mit SnapLock

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

- "Übertragung von Dateien an DIE WORM-Funktion"
- "Setzen Sie Snapshots für sekundären Storage auf WORM"
- "SPIEGELN VON WORM-Dateien für das Disaster Recovery"
- "BEWAHREN SIE WORM-Dateien bei Rechtsstreitigkeiten mithilfe der gesetzlichen Aufbewahrung auf"
- "LÖSCHEN SIE WORM-Dateien mit der Funktion „privilegiertes Löschen“"
- "Legen Sie den Aufbewahrungszeitraum für Dateien fest"
- "SnapLock Volumes werden verschoben"
- "Sperren Sie einen Snapshot, um sich vor Ransomware-Angriffen zu schützen"
- "Überprüfen Sie die Verwendung von SnapLock mit dem Überwachungsprotokoll"
- "Verwenden Sie SnapLock-APIs"

SnapLock Compliance und Enterprise Modi

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

SnapLock-Modus	Sicherungsstufe	WORM-Datei wird während der Aufbewahrung gelöscht
Compliance-Modus	Auf Festplattenebene	Kann nicht gelöscht werden
Enterprise-Modus	Auf Dateiebene	Kann vom Compliance-Administrator mithilfe eines geprüften „privilegierten Löschverfahrens“ gelöscht werden

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

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

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

Dar	SnapLock-Compliance	SnapLock Enterprise

Aktivieren und löschen Sie Dateien mit privilegierter Löschung	Nein	Ja.
Festplatten neu initialisieren	Nein	Ja.
Zerstören Sie SnapLock Aggregate und Volumes während der Aufbewahrungsdauer	Nein	Ja, mit Ausnahme des SnapLock Revisionsprotokoll-Volumes
Benennen Sie Aggregate oder Volumes um	Nein	Ja.
Verwenden Sie nicht NetApp Festplatten	Nein	Nein
Verwenden Sie das SnapLock Volume zur Audit-Protokollierung	Ja.	Ja, ab ONTAP 9.5

Unterstützte und nicht unterstützte Funktionen in SnapLock

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

Funktion	Unterstützt durch SnapLock Compliance	Unterstützt durch SnapLock Enterprise
Konsistenzgruppen	Nein	Nein
Verschlüsselte Volumes	Ja, erfahren Sie mehr über Verschlüsselung und SnapLock .	Ja, erfahren Sie mehr über Verschlüsselung und SnapLock .
FabricPool auf SnapLock Aggregaten	Nein	Ja, ab ONTAP 9.8. Erfahren Sie mehr über 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, ab ONTAP 9.11.1. Erfahren Sie mehr über [flexgroup].	Ja, ab ONTAP 9.11.1. Erfahren Sie mehr über [flexgroup].
LUNs	Nein. Erfahren Sie mehr über LUN SupportSnapLock.	Nein. Erfahren Sie mehr über LUN SupportSnapLock.

MetroCluster Konfigurationen	Ja, ab ONTAP 9.3. Erfahren Sie mehr über MetroCluster Support.	Ja, ab ONTAP 9.3. Erfahren Sie mehr über MetroCluster Support.
Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV)	Ja, ab ONTAP 9.13.1. Erfahren Sie mehr über MAV Support.	Ja, ab ONTAP 9.13.1. Erfahren Sie mehr über MAV Support.
San	Nein	Nein
SnapRestore mit einer Datei	Nein	Ja.
SnapMirror Active Sync	Nein	Nein
SnapRestore	Nein	Ja.
SMTape	Nein	Nein
SnapMirror Synchronous	Nein	Nein
SSDs	Ja.	Ja.
Funktionen für effizienteren Storage	Ja, ab ONTAP 9.9.1. Erfahren Sie mehr über Support für Storage-Effizienz.	Ja, ab ONTAP 9.9.1. Erfahren Sie mehr über Support für Storage-Effizienz.

FabricPool auf SnapLock Enterprise-Aggregaten

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

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

FlexGroup Volumes

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

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

Sie sollten auch die folgenden Verhaltensweisen beachten:

- Die Volume Compliance-Uhr (VCC) eines FlexGroup-Volumes wird durch den VCC der Root-Komponente bestimmt. Alle nicht-Root-Bestandteile werden ihren VCC eng mit dem Root-VCC synchronisiert.

- Die SnapLock-Konfigurationseigenschaften werden nur auf der gesamten FlexGroup festgelegt. Einzelne Komponenten können nicht über unterschiedliche Konfigurationseigenschaften verfügen, z. B. Standardaufbewahrungszeit und automatische Verschiebungszeit.

LUN Support

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

MetroCluster Support

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

SnapLock-Compliance

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

SnapLock Enterprise

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

MetroCluster-Konfigurationen und Compliance-Uhren

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

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

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

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

Ab ONTAP 9.13.1 kann ein Cluster-Administrator die Verifizierung mehrerer Administratoren auf einem Cluster explizit aktivieren, sodass vor der Ausführung einiger SnapLock-Vorgänge eine Quorumgenehmigung erforderlich ist. Wenn die MAV aktiviert ist, müssen SnapLock Volume-Eigenschaften wie Default-Retention-Time, Minimum-Retention-Time, Maximum-Retention-Time, Volume-Append-Mode, Autocommit-Period und

Privileged-delete genehmigt werden. Erfahren Sie mehr über "MAV".

Storage-Effizienz

Ab ONTAP 9.9 unterstützt SnapLock Storage-Effizienzfunktionen wie Data-Compaction, Volume-übergreifende Deduplizierung und die anpassungsfähige Komprimierung für SnapLock Volumes und Aggregate. Weitere Informationen zur Storage-Effizienz finden Sie unter "Überblick über die ONTAP Storage-Effizienz".

Verschlüsselung

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

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

Verschlüsselte Volumes werden auf SnapLock -Aggregaten unterstützt.

Umstieg Von 7-Mode

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

Konfigurieren Sie SnapLock

Erfahren Sie mehr über die Konfiguration von ONTAP SnapLock

Bevor Sie SnapLock verwenden, müssen Sie SnapLock konfigurieren, indem Sie verschiedene Aufgaben durchführen, z. B. "Installieren Sie die SnapLock-Lizenz" für jeden Node, der ein Aggregat mit einem SnapLock-Volume hostet, initialisieren Sie den "Compliance-Uhr", erstellen Sie ein SnapLock-Aggregat für Cluster, auf denen ONTAP Versionen vor ONTAP 9.10.1 ausgeführt "Erstellen und Mounten eines SnapLock Volumes"werden, und mehr.

Initialisieren der ONTAP Compliance Clock

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

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

Bevor Sie beginnen

So initialisieren Sie die Compliance-Uhr neu:

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

Allgemeine Anforderungen für die Initialisierung der Compliance Clock:

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

Über diese Aufgabe

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

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

Schritte

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

System Manager

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

CLI

1. Initialisieren Sie die System-Compliance-Uhr:

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

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

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

   Erfahren Sie mehr über `snaplock compliance-clock initialize` 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 diese Vorgehensweise für jeden Node, der ein SnapLock Aggregat hostet.

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

Sie können die SnapLock Compliance Clock-Synchronisierungsfunktion aktivieren, wenn ein NTP-Server konfiguriert ist.

Bevor Sie beginnen

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

Über diese Aufgabe

Wenn der SnapLock Secure Clock Daemon eine Schräglage entdeckt, die über den Schwellenwert hinausgeht, verwendet ONTAP die Systemzeit, um die System- und Volume Compliance-Uhren zurückzusetzen. Als Schwellwert wird ein Zeitraum von 24 Stunden festgelegt. Das bedeutet, dass die System-Compliance-Uhr nur dann mit der Systemuhr synchronisiert wird, wenn die Schräglage älter als einen Tag ist.

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

Schritte

1. Aktivieren Sie die SnapLock Compliance Clock-Synchronisierungsfunktion, wenn ein NTP-Server konfiguriert ist:

   `snaplock compliance-clock ntp`

   Der folgende Befehl aktiviert die Synchronisierungsfunktion der Compliance Clock des Systems:

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

   Erfahren Sie mehr über `snaplock compliance-clock ntp modify` in der "ONTAP-Befehlsreferenz".

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

   `snaplock compliance-clock ntp show`

   Der folgende Befehl überprüft, ob die Synchronisierungsfunktion der System-Compliance-Uhr aktiviert ist:

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

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

   Erfahren Sie mehr über `snaplock compliance-clock ntp show` in der "ONTAP-Befehlsreferenz".

Erstellen Sie ein ONTAP SnapLock -Aggregat

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

Bevor Sie beginnen

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

Upgrade-Überlegungen

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

Überlegungen zurücksetzen

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

Über diese Aufgabe

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

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

Schritte

1. Erstellung eines SnapLock Aggregats:

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

Mit dem folgenden Befehl wird ein SnapLock- `Compliance`Aggregat erstellt, `aggr1` das mit drei Festplatten benannt `node1` ist:

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

Erfahren Sie mehr über `storage aggregate create` in der "ONTAP-Befehlsreferenz".

Erstellen und Mounten von ONTAP SnapLock -Volumes

Sie müssen für die Dateien oder Snapshots, die in den WORM-Status übergeben werden

sollen, ein SnapLock Volume erstellen. Ab ONTAP 9.10.1 wird jedes der erstellten Volumes unabhängig vom Aggregattyp standardmäßig als nicht-SnapLock Volume erstellt. Sie müssen die `-snaplock-type` Option verwenden, um ein SnapLock-Volume explizit zu erstellen, indem Sie als SnapLock-Typ entweder Compliance oder Enterprise angeben. Standardmäßig ist der SnapLock-Typ auf eingestellt `non-snaplock`.

Bevor Sie beginnen

- Das SnapLock Aggregat muss online sein.
- Sie sollten "Vergewissern Sie sich, dass eine SnapLock-Lizenz installiert ist". Wenn auf dem Node keine SnapLock-Lizenz installiert ist, müssen Sie "Installieren"sie ausführen. Diese Lizenz ist in enthalten"ONTAP One". Vor ONTAP One war die SnapLock-Lizenz im Paket für Sicherheit und Compliance enthalten. Das Paket „Sicherheit und Compliance“ wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl derzeit nicht erforderlich, können Bestandskunden wählen"Upgrade auf ONTAP One".
- "Die Compliance Clock auf dem Knoten muss initialisiert werden".

Über diese Aufgabe

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

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

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

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

System Manager

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

Schritte

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

CLI

1. SnapLock Volume erstellen:

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

Erfahren Sie mehr über `volume create` in der "ONTAP-Befehlsreferenz". Für SnapLock-Volumes stehen folgende Optionen nicht zur Verfügung: `-nvfail`, `-atime-update`, , `-is-autobalance -eligible` `-space-mgmt-try-first` Und `vmalign`.

Mit dem folgenden Befehl wird ein SnapLock- `Compliance`Volume mit dem Namen `vol1` auf erstellt `aggr1` `vs1`:

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

Mounten Sie ein SnapLock Volume

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

Bevor Sie beginnen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

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

Schritte

1. Mounten eines SnapLock Volume:

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

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

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

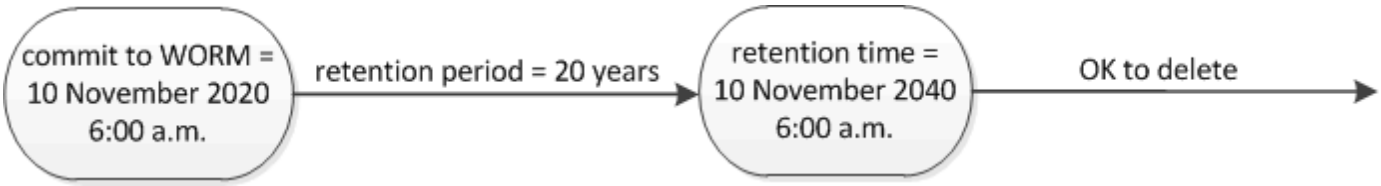
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Legen Sie die ONTAP SnapLock Aufbewahrungszeit fest

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

Allgemeines zu Aufbewahrungszeitraum und Aufbewahrungszeit

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



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

Wichtige Überlegungen zur Replizierung

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

Wichtige Überlegungen zum Wechsel

ONTAP verhindert, dass Sie einen Cluster von ONTAP 9.10.1 auf eine frühere ONTAP -Version zurücksetzen, wenn Dateien mit einer Aufbewahrungsdauer nach „19. Januar 2071, 8:44:07 Uhr“ vorhanden sind.

Die Aufbewahrungsfristen verstehen

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

- Mindestaufbewahrungsdauer (`min`), mit einem Standardwert von 0
- Maximale Aufbewahrungsfrist (`max`), mit einem Verzug von 30 Jahren
- Standardaufbewahrungszeitraum, wobei der Standard `min` sowohl für den Compliance-Modus als auch für den Enterprise-Modus mit ONTAP 9.10.1 gleich ist. In älteren Versionen als ONTAP 9.10.1 von ONTAP hängt die standardmäßige Aufbewahrungsdauer von dem Modus ab:
  - Für den Compliance-Modus ist der Standardwert gleich `max` .
  - Für den Enterprise-Modus ist der Standardwert gleich `min` .
- Nicht festgelegte Aufbewahrungsdauer.

> In Versionen vor ONTAP 9.10.1 wird eine Datei im Compliance-Modus standardmäßig 30 Jahre lang aufbewahrt, wenn die Aufbewahrungszeit nicht explizit festgelegt wird, bevor sie in den WORM-Zustand versetzt wird, und wenn die Standardeinstellungen nicht geändert werden. Diese Änderung kann nicht rückgängig gemacht werden. In ähnlicher Weise wird in ONTAP 9.10.1 und späteren Versionen die Datei, wenn Sie die Aufbewahrungszeit nicht explizit festlegen, bevor Sie sie in den WORM-Zustand versetzen, und wenn Sie die Standardeinstellungen nicht ändern, 0 Jahre lang aufbewahrt, also effektiv gar nicht.

Ab ONTAP 9.8 können Sie die Aufbewahrungsfrist für Dateien in einem Volume auf `unspecified`, einstellen, damit die Datei beibehalten werden kann, bis Sie eine absolute Aufbewahrungszeit festlegen. Sie können eine Datei mit absoluter Aufbewahrungszeit auf unbestimmte Aufbewahrung und zurück zur absoluten Aufbewahrung setzen, solange die neue absolute Aufbewahrungszeit später ist als die zuvor festgelegte absolute Zeit.

Ab ONTAP 9.12.1 verfügen WORM-Dateien mit festgesetzten Aufbewahrungsfristen `unspecified` garantiert über einen Aufbewahrungszeitraum auf den für das SnapLock Volume konfigurierten Mindestaufbewahrungszeitraum. Wenn Sie die Aufbewahrungsdauer der Datei von `unspecified` in eine absolute Aufbewahrungszeit ändern, muss die neue angegebene Aufbewahrungszeit größer sein als die für die Datei bereits festgelegte Mindestaufbewahrungszeit.

Legen Sie den Standardaufbewahrungszeitraum fest

Sie können den `volume snaplock modify` Befehl verwenden, um den Standardaufbewahrungszeitraum für Dateien auf einem SnapLock Volume festzulegen.

Bevor Sie beginnen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

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

> Der Standardaufbewahrungszeitraum muss größer oder gleich (>=) dem Mindestaufbewahrungszeitraum und kleiner als oder gleich (<=) dem maximalen Aufbewahrungszeitraum sein.

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

Die Werte und Bereiche für die maximalen und minimalen Aufbewahrungsfristen sind identisch, mit Ausnahme von `max` und `min`, die nicht anwendbar sind. Weitere Informationen zu dieser Aufgabe finden Sie unter "Stellen Sie die Übersicht über die Aufbewahrungszeit ein".

Sie können mit dem `volume snaplock show` Befehl die Einstellungen für den Aufbewahrungszeitraum für das Volume anzeigen. Erfahren Sie mehr über `volume snaplock show` in der "ONTAP-Befehlsreferenz".

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

Schritte

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

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

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

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

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

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

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

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

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

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

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

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

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

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Legen Sie die Aufbewahrungszeit für eine Datei explizit fest

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

Über diese Aufgabe

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

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

Schritte

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

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

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

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

Legen Sie den Aufbewahrungszeitraum für die Datei nach einem Ereignis fest

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

Bevor Sie beginnen

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

  "Erstellen Sie ein SnapLock-Administratorkonto"

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

Über diese Aufgabe

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

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

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

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

Für erweiterte Verwendung siehe "Worm-Speicherung gemäß NetApp SnapLock".

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

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

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

Schritte

1. EBR-Richtlinie erstellen:

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

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

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

2. Anwenden einer EBR-Richtlinie:

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

   Der folgende Befehl wendet die EBR-Richtlinie `employee_exit` auf `vs1` alle Dateien im Verzeichnis an `d1`:

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

Verwandte Informationen

- "Snaplock-Ereignisaufbewahrungsrichtlinie erstellen"
- "Snaplock-Ereignisaufbewahrung anwenden"

Erstellen Sie ein ONTAP SnapLock-geschütztes Audit-Protokoll

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

Aktivierung und das Löschen privilegierter Vorgänge sowie die Verschiebung von SnapLock Volumes.

Ab ONTAP 9.10.1 erstellen Sie kein SnapLock Aggregat mehr. Sie müssen die Option -SnapLock-type für verwenden"Explizit ein SnapLock Volume erstellen", indem Sie entweder Compliance oder Enterprise als SnapLock-Typ angeben.

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

- Sie können den `snaplock log file show` Befehl verwenden, um die Protokolldateien auf dem Überwachungsprotokoll-Volume anzuzeigen.
- Sie können den `snaplock log file archive` Befehl verwenden, um die aktuelle Protokolldatei zu archivieren und eine neue zu erstellen, was in Fällen nützlich ist, in denen Sie Überwachungsprotokollinformationen in einer separaten Datei aufzeichnen müssen.

Erfahren Sie mehr über `snaplock log file show` und `snaplock log file archive` in der "ONTAP-Befehlsreferenz".

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

Schritte

1. Erstellen Sie ein SnapLock Aggregat.

   Erstellen Sie ein SnapLock Aggregat

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

   SnapLock Volume erstellen

3. SVM für Audit-Protokollierung konfigurieren:

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

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

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

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

Erfahren Sie mehr über `snaplock log create` in der "ONTAP-Befehlsreferenz".

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

   Mounten Sie ein SnapLock Volume

Überprüfen der ONTAP SnapLock -Einstellungen

Mit den `volume file fingerprint start` `volume file fingerprint dump` Befehlen und lassen sich wichtige Informationen über Dateien und Volumes einschließlich des Dateityps (normal, WORM oder WORM ANZEIGEFÄHIG), des Ablaufdatums des Volumes und so weiter anzeigen.

Schritte

1. Generieren eines Dateiprints:

   ```
   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 Session ID, die Sie als Eingabe für den `volume file fingerprint dump` Befehl verwenden können.

Sie können den `volume file fingerprint show` Befehl mit dem Session ID verwenden, um den Fortschritt des Fingerabdruckvorgangs zu überwachen. Vergewissern Sie sich, dass der Vorgang abgeschlossen ist, bevor Sie versuchen, den Fingerabdruck anzuzeigen.

2. Zeigen Sie den Fingerabdruck für die Datei an:

`volume file fingerprint dump -session-id <session_ID>`

```
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
```

MANAGEN von WORM-Dateien

Verwalten Sie WORM-Dateien mit ONTAP SnapLock

ES gibt folgende Möglichkeiten, WORM-Dateien zu verwalten:

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

Übertragen Sie Dateien mit ONTAP SnapLock in WORM

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

Manuelles Versetzen von Dateien in DIE WORM-FUNKTION

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritte

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

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

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

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

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

Automatisches Versetzen von Dateien in DIE WORM-FUNKTION

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

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

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

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

Schritte

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

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

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

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

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

ERSTELLEN einer ANGEHÄNGBAREN WORM-Datei

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

Schritte

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

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Aufbewahrungszeit von 21. November 2020 6:00 Uhr auf einer Datei mit der Nulllänge festzulegen `document.txt`:

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

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

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

   ```
   chmod 444 document.txt
   ```

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

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

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

   ```
   chmod 777 document.txt
   ```

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

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

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

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

Schritte

1. VAM aktivieren:

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

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

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

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

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

   Die Dateien sind standardmäßig WORM-appensible.

Übertragen Sie Snapshots an WORM auf einem ONTAP Vault-Ziel

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

sodass die Snapshots nicht explizit auf WORM übergeben werden müssen.

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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

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

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

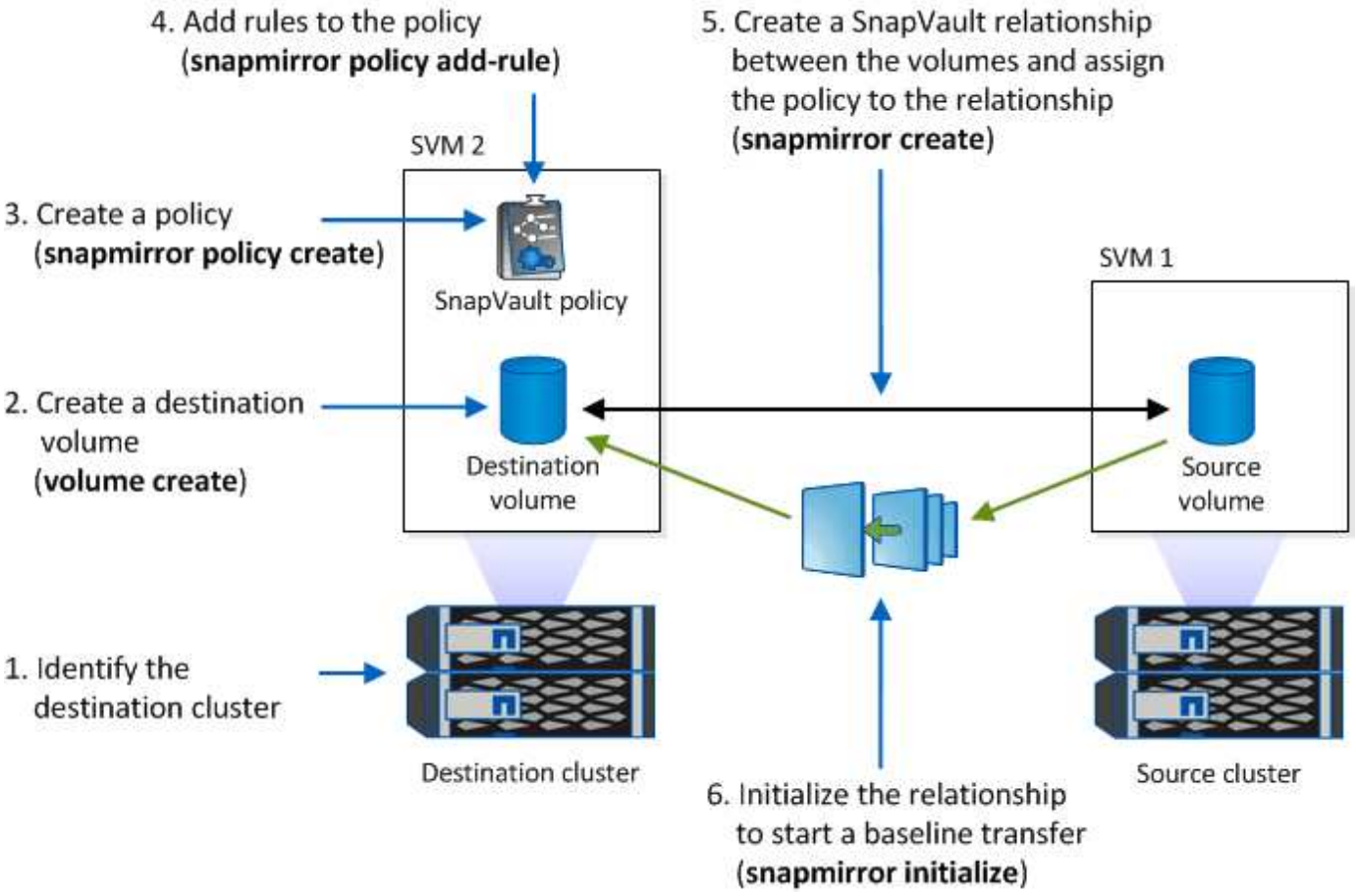
Ab ONTAP 9.14.1 können Sie in der SnapMirror-Richtlinie der SnapMirror-Beziehung Aufbewahrungszeiträume für bestimmte SnapMirror-Labels festlegen, sodass die replizierten Snapshots vom Quell- zum Ziel-Volume für den in der Regel festgelegten Aufbewahrungszeitraum beibehalten werden. Wenn kein Aufbewahrungszeitraum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

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

Bei MetroCluster Konfigurationen sollten Sie die folgenden Aspekte beachten:

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

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



Schritte

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

System Manager

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

CLI

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Verwandte Informationen

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

Spiegeln Sie WORM-Dateien mit ONTAP SnapMirror für die Notfallwiederherstellung

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

Voraussetzungen

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

Über diese Aufgabe

- Ab ONTAP 9.5 können Sie WORM-Dateien mit dem XDP-Typ (erweiterte Datensicherung) SnapMirror Beziehung replizieren, anstatt die DP-Beziehung (Datenschutz) zu verwenden. XDP-Modus ist unabhängig von der ONTAP-Version und ist in der Lage, Dateien im selben Block zu differenzieren, was die Resynchronisierung replizierter Compliance-Modus-Volumes erheblich erleichtert. Informationen zum Konvertieren einer vorhandenen DP-Beziehung in eine XDP-Beziehung finden Sie unter "Datensicherung".
- Resync-Vorgang auf einer DP-Typ SnapMirror-Beziehung schlägt für ein Compliance-Modus-Volume fehl, wenn SnapLock feststellt, dass es zu einem Datenverlust führt. Wenn eine Neusynchronisierung fehlschlägt, können Sie den `volume clone create` Befehl verwenden, um einen Klon des Ziel-Volume zu erstellen. Sie können dann das Quell-Volume mit dem Klon neu synchronisieren.
- Eine SnapMirror -Beziehung eines SnapLock -Volumes unterstützt nur die `MirrorAllSnapshots` Richtlinie vom Typ „Async-Mirror“. Die Aufbewahrungsdauer eines SnapLock -Volumes wird durch die maximale Aufbewahrungsdauer aller darin enthaltenen WORM-Dateien bestimmt. Da es sich beim Ziel um eine DR-Kopie der Quelle handelt, ist die Aufbewahrungsdauer des Ziel- SnapLock -Volumes dieselbe wie die der Quelle.
- Eine SnapMirror-Beziehung des Typs XDP zwischen SnapLock-konformen Volumes unterstützt eine Resynchronisierung nach einer Pause, auch wenn Daten auf dem Ziel von der Quelle nach der Pause umgeleitet wurden.

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

  - Die Verfallszeit des Zieldatums
  - Wenn die Ablaufzeit des Datenträgers in der Vergangenheit liegt oder noch nicht eingestellt wurde, wird der Snapshot für einen Zeitraum von 30 Tagen gesperrt
  - Wenn das Ziel legal-holds hat, wird die tatsächliche Gültigkeitsdauer des Volumes maskiert und als ‘unbestimmt’ angezeigt. Der Snapshot wird jedoch für die Dauer der tatsächlichen Gültigkeitsdauer des Volumes gesperrt.

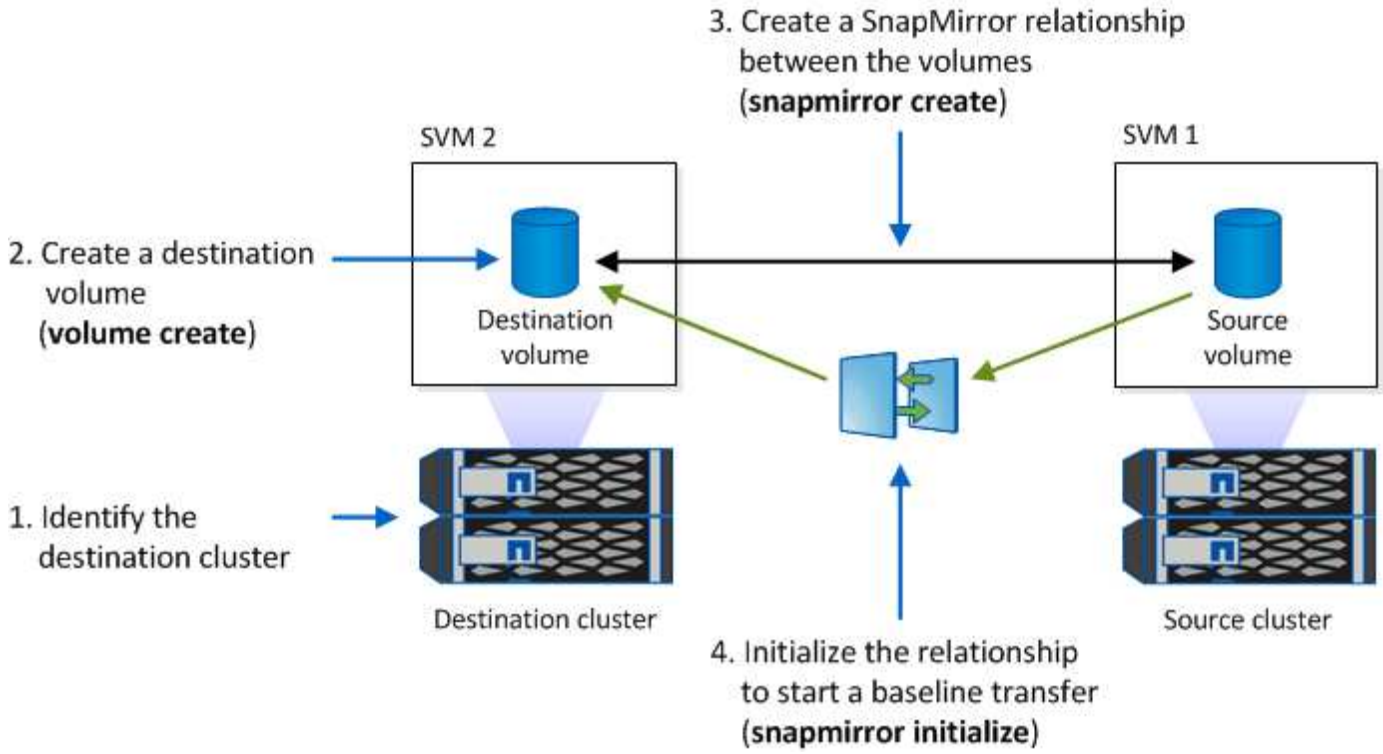
Wenn das Ziellaufwerk eine Ablauffrist hat, die später als das Quellvolumen ist, wird die Gültigkeitsdauer des Zieldatums beibehalten und wird nach der Resynchronisierung nicht durch den Ablaufzeitraum des Quellvolumens überschrieben.

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

Ein gesperrter Snapshot auf dem Ziellaufwerk, der zur Erfassung der divergierenden Daten erstellt wurde, kann mithilfe der CLI durch Ausführen des Befehls auf die Quelle kopiert werden `snapmirror update -s snapshot`. Der nach dem Kopieren kopierte Snapshot wird weiterhin an der Quelle gesperrt.

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

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


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

System Manager

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

Schritte

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

CLI

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

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

   > ⓘ Ab ONTAP 9.10.1 können SnapLock und Nicht- SnapLock -Volumes auf demselben Aggregat vorhanden sein. Daher müssen Sie bei Verwendung von ONTAP 9.10.1 kein separates SnapLock -Aggregat mehr erstellen. Mit der Option „Volume -Snaplock -Type“ geben Sie einen Compliance- oder Enterprise- SnapLock -Volumetyp an. In ONTAP -Versionen vor ONTAP 9.10.1 wird der SnapLock -Modus – Compliance oder Enterprise – vom Aggregat übernommen. Die Spracheinstellung des Zielvolumes muss mit der Spracheinstellung des Quellvolumes übereinstimmen.

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

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

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

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

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

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

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

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

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

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

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

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

   Mit dem folgenden Befehl wird eine SnapMirror-Beziehung zwischen dem Quell-Volume `srcvolA` `SVM1` `dstvolB` auf und dem Ziel-Volume auf erstellt `SVM2` und die Policy `SVM1-mirror` und den Zeitplan zugewiesen `weekendcron`:

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

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

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

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

   Der Initialisierungsvorgang führt einen *Baseline Transfer* zum Ziel-Volume durch. SnapMirror erstellt einen Snapshot des Quell-Volume, überträgt dann die Kopie und alle Datenblöcke, die es auf das Ziel-Volume verweist. Außerdem werden alle anderen Snapshots auf dem Quell-Volume an das Ziel-Volume übertragen.

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

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

Verwandte Informationen

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

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

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

Bevor Sie beginnen

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

  "Erstellen Sie ein SnapLock-Administratorkonto"

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

Über diese Aufgabe

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

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

Schritte

1. Gesetzliche Aufbewahrungspflichten starten:

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

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

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

2. Beenden einer gesetzlichen Aufbewahrungspflichten:

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

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

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

Verwandte Informationen

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

Löschen Sie WORM-Dateien mit ONTAP SnapLock

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

Erstellen Sie ein SnapLock-Administratorkonto

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

Bevor Sie beginnen

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

Schritte

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

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

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

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

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

Aktivieren Sie die Funktion „privilegiertes Löschen“

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

Über diese Aufgabe

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

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

Schritte

1. Privilegiertes Löschen für ein SnapLock Enterprise Volume aktivieren:

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

   Mit dem folgenden Befehl wird die privilegierte Löschfunktion für das Enterprise-Volume aktiviert `dataVol` `SVM1`:

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

LÖSCHEN SIE WORM-Dateien im Enterprise-Modus

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

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können eine abgelaufene WORM-Datei nicht mit einem privilegierten Löschvorgang löschen. Sie können mit dem `volume file retention show` Befehl die Aufbewahrungszeit der WORM-Datei anzeigen, die Sie löschen möchten. Erfahren Sie mehr über `volume file retention show` in der "ONTAP-Befehlsreferenz".

Schritt

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

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

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

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

Verschieben eines ONTAP SnapLock -Volumes

Ab ONTAP 9.8 können Sie ein SnapLock Volume zu einem Zielaggregat desselben Typs verschieben: Von Enterprise zu Enterprise oder Compliance zu Compliance. Zum Verschieben eines SnapLock Volumes muss Ihnen die SnapLock-Sicherheitsrolle zugewiesen werden.

Erstellen Sie ein SnapLock-Sicherheitsadministratorkonto

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

Schritt

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

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

   Mit dem folgenden Befehl kann das SVM-Administratorkonto `SnapLockAdmin` mit der vordefinierten `snaplock` Rolle `cluster1` über ein Passwort auf die Admin-SVM zugreifen:

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

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

SnapLock Volumes werden verschoben

Sie können mit dem `volume move` Befehl ein SnapLock Volume zu einem Ziel-Aggregat verschieben.

Bevor Sie beginnen

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

"Erstellen eines Prüfprotokolls".

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

Schritte

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

   ```
   ssh snaplock_user@cluster_mgmt_ip
   ```

2. Verschieben eines SnapLock Volumes:

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

3. Prüfen Sie den Status der Volume-Verschiebung:

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

Sperren Sie einen ONTAP Snapshot zum Schutz vor Ransomware-Angriffen

Ab ONTAP 9.12.1 können Sie einen Snapshot auf einem nicht-SnapLock-Volume sperren, um Schutz vor Ransomware-Angriffen zu bieten. Das Sperren von Snapshots stellt sicher, dass sie nicht versehentlich oder böswillig gelöscht werden können.

Sie verwenden die SnapLock Compliance-Uhrfunktion, um Snapshots für einen bestimmten Zeitraum zu sperren, sodass sie erst gelöscht werden können, wenn die Ablaufdatum erreicht ist. Durch das Sperren von Snapshots werden sie manipulationssicher und vor Ransomware-Bedrohungen geschützt. Sie können gesperrte Snapshots verwenden, um Daten wiederherzustellen, falls ein Volume durch einen Ransomware-Angriff kompromittiert wird.

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

Anforderungen und Überlegungen zu manipulationssicheren Snapshots

- Wenn Sie die ONTAP-CLI verwenden, muss auf allen Nodes im Cluster ONTAP 9.12.1 oder höher ausgeführt werden. Wenn Sie System Manager verwenden, muss auf allen Nodes ONTAP 9.13.1 oder höher ausgeführt werden.
- "Die SnapLock-Lizenz muss auf dem Cluster installiert sein". Diese Lizenz ist in enthalten"ONTAP One".
- "Die Compliance-Uhr auf dem Cluster muss initialisiert werden".
- Wenn die Snapshot-Sperrung auf einem Volume aktiviert ist, können Sie die Cluster auf eine Version von ONTAP höher als ONTAP 9.12.1 aktualisieren. Sie können jedoch nicht auf eine frühere Version von

ONTAP zurücksetzen, bis alle gesperrten Snapshots ihr Ablaufdatum erreicht haben und gelöscht und die Snapshot Sperrung deaktiviert ist.

- Wenn ein Snapshot gesperrt ist, wird die Gültigkeitsdauer des Volumes auf die Ablaufzeit des Snapshots eingestellt. Wenn mehr als ein Snapshot gesperrt ist, spiegelt die Gültigkeitsdauer des Volumes die größte Verfallszeit unter allen Snapshots wider.
- Die Aufbewahrungsfrist für gesperrte Snapshots hat Vorrang vor der Anzahl der Snapshot-Aufbewahrung, was bedeutet, dass die Begrenzung der Anzahl beibehalten nicht eingehalten wird, wenn die Snapshot-Aufbewahrungsfrist für gesperrte Snapshots nicht abgelaufen ist.
- In einer SnapMirror Beziehung können Sie in einer Regel für die Richtlinie „Mirror-Vault“ eine Aufbewahrungsfrist festlegen, und der Aufbewahrungszeitraum wird für auf das Ziel-Volume replizierte Snapshots angewendet, wenn für das Ziel-Volume die Snapshot-Sperrung aktiviert ist. Die Aufbewahrungsfrist hat Vorrang vor der Anzahl behalten. Snapshots, die ihr Ablaufdatum nicht überschritten haben, werden z. B. auch dann beibehalten, wenn die Anzahl der Bewahren Daten überschritten wird.
- Sie können einen Snapshot auf einem Volume ohne SnapLock umbenennen. Umbenennungsvorgänge für Snapshots auf dem primären Volume einer SnapMirror-Beziehung werden nur auf dem sekundären Volume wiedergegeben, wenn die Richtlinie MirrorAllSnapshots ist. Bei anderen Richtlinientypen wird der umbenannte Snapshot während der Aktualisierungen nicht propagiert.
- Wenn Sie die ONTAP CLI verwenden, können Sie einen gesperrten Snapshot mit dem Befehl nur wiederherstellen `volume snapshot restore`, wenn es sich bei dem gesperrten Snapshot um den aktuellsten handelt. Wenn nach der Wiederherstellung noch nicht abgelaufene Snapshots vorhanden sind, schlägt die Snapshot-Wiederherstellung fehl.

Durch manipulationssichere Snapshots unterstützte Funktionen

- "Cloud Volumes ONTAP"
- FlexGroup Volumes

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

- Konvertierung von FlexVol zu FlexGroup

  Sie können eine FlexVol volume mit gesperrten Snapshots in ein FlexGroup Volume konvertieren. Snapshots bleiben nach der Konvertierung gesperrt.

- SnapMirror asynchron

  Die Compliance-Uhr muss sowohl auf der Quelle als auch auf dem Ziel initialisiert werden.

- SVM-Datenmobilität (verwendet für die Migration oder Verschiebung einer SVM von einem Quell-Cluster zu einem Ziel-Cluster)

  Unterstützt ab ONTAP 9.14.1.

- SnapMirror-Richtlinie, die den `-schedule` Parameter verwendet
- SVM-DR

  Die Compliance-Uhr muss sowohl auf der Quelle als auch auf dem Ziel initialisiert werden.

- Volume-Klon und Dateiklon

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

- FlexCache Volumes

  Unterstützt ab ONTAP 9.16.1.

Nicht unterstützte Funktionen

Die folgenden Funktionen werden derzeit bei manipulationssicheren Snapshots nicht unterstützt:

- Konsistenzgruppen
- "FabricPool"

  Manipulationssichere Snapshots bieten unveränderliche Schutzmechanismen, die nicht gelöscht werden können. Da FabricPool Daten löschen muss, können FabricPool- und Snapshot-Sperren nicht auf demselben Volume aktiviert werden.

- SMTape
- SnapMirror Active Sync
- SnapMirror Synchronous

Aktivieren Sie die Snapshot-Sperrung bei der Erstellung eines Volumes

Ab ONTAP 9.12.1 können Sie die Snapshot-Sperrung aktivieren, wenn Sie ein neues Volume erstellen oder ein vorhandenes Volume ändern. Dazu verwenden Sie die `-snapshot-locking-enabled` Option mit den `volume create` Befehlen und `volume modify` in der CLI. Ab ONTAP 9.13.1 können Sie System Manager verwenden, um die Snapshot-Sperrung zu aktivieren.

System Manager

1. Navigieren Sie zu **Storage > Volumes** und wählen Sie **Add**.
2. Wählen Sie im Fenster **Volume hinzufügen Weitere Optionen**.
3. Geben Sie den Namen, die Größe, die Exportrichtlinie und den Freigabenamen des Volumes ein.
4. Wählen Sie **Snapshot sperren aktivieren**. Diese Auswahl wird nicht angezeigt, wenn die SnapLock-Lizenz nicht installiert ist.
5. Wenn sie noch nicht aktiviert ist, wählen Sie **SnapLock-Compliance-Uhr initialisieren** aus.
6. Speichern Sie die Änderungen.
7. Wählen Sie im Fenster **Volumes** das Volume aus, das Sie aktualisiert haben, und wählen Sie **Übersicht**.
8. Überprüfen Sie, ob **SnapLock Snapshot Locking** als **aktiviert** angezeigt wird.

CLI

1. Geben Sie den folgenden Befehl ein, um ein neues Volume zu erstellen und die Snapshot-Sperrung zu aktivieren:

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   Mit dem folgenden Befehl wird die Snapshot-Sperrung auf einem neuen Volume mit dem Namen vol1 aktiviert:

   ```
   > 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 Sie die Snapshot-Sperrung auf einem vorhandenen Volume

Ab ONTAP 9.12.1 können Sie die Snapshot-Sperrung auf einem vorhandenen Volume mithilfe der ONTAP CLI aktivieren. Ab ONTAP 9.13.1 können Sie System Manager verwenden, um die Snapshot-Sperrung auf einem vorhandenen Volume zu aktivieren.

System Manager

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie ⋮ und dann **Bearbeiten > Lautstärke**.
3. Suchen Sie im Fenster **Volume bearbeiten** den Abschnitt Snapshots (Local) Settings und wählen Sie **Snapshot locking aktivieren** aus.

   Diese Auswahl wird nicht angezeigt, wenn die SnapLock-Lizenz nicht installiert ist.
4. Wenn sie noch nicht aktiviert ist, wählen Sie **SnapLock-Compliance-Uhr initialisieren** aus.
5. Speichern Sie die Änderungen.
6. Wählen Sie im Fenster **Volumes** das Volume aus, das Sie aktualisiert haben, und wählen Sie **Übersicht**.
7. Stellen Sie sicher, dass * SnapLock Snapshot-Sperre* als **Aktiviert** angezeigt wird.

CLI

1. Geben Sie den folgenden Befehl ein, um ein vorhandenes Volume zu ändern und die Snapshot-Sperrung zu aktivieren:

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

Erstellen Sie eine gesperrte Snapshot-Richtlinie und wenden Sie die Aufbewahrung an

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

Erstellen Sie eine Snapshot-Sperrrichtlinie

System Manager

1. Navigieren Sie zu **Storage > Storage VMs** und wählen Sie eine Storage VM aus.
2. Wählen Sie **Einstellungen**.
3. Suchen Sie **Snapshot Policies** und wählen Sie →.
4. Geben Sie im Fenster **Add Snapshot Policy** den Richtliniennamen ein.
5. Wählen Sie + Add .
6. Geben Sie die Details des Snapshot-Zeitplans an, einschließlich des Plannamens, der maximalen Anzahl der zu haltenden Snapshots und des SnapLock-Aufbewahrungszeitraums.
7. Geben Sie in der Spalte **SnapLock Retention Period** die Anzahl der Stunden, Tage, Monate oder Jahre ein, um die Snapshots zu behalten. Eine Snapshot-Richtlinie mit einer Aufbewahrungsfrist von 5 Tagen sperrt einen Snapshot beispielsweise 5 Tage ab dem Zeitpunkt, zu dem er erstellt wird. Er kann in dieser Zeit nicht gelöscht werden. Folgende Aufbewahrungszeiträume werden unterstützt:
   - Jahre: 0 - 100
   - Monate: 0 - 1200
   - Tage: 0 - 36500
   - Öffnungszeiten: 0 - 24
8. Speichern Sie die Änderungen.

CLI

1. Geben Sie zum Erstellen einer Snapshot-Richtlinie den folgenden Befehl ein:

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   Mit dem folgenden Befehl wird eine Snapshot-Sperrrichtlinie erstellt:

   ```
   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 unter aktiver Aufbewahrung liegt. Das heißt, die Aufbewahrungszahl wird nicht berücksichtigt, wenn es gesperrte Snapshots gibt, die noch nicht abgelaufen sind.

Wenden Sie eine Sperrrichtlinie auf ein Volume an

System Manager

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie ⋮ und dann **Bearbeiten > Lautstärke**.
3. Wählen Sie im Fenster **Volume bearbeiten** die Option **Snapshots planen**.
4. Wählen Sie die Snapshot-Sperrrichtlinie aus der Liste aus.
5. Wenn die Snapshot-Sperrung noch nicht aktiviert ist, wählen Sie **Snapshot-Sperrung aktivieren**.
6. Speichern Sie die Änderungen.

CLI

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

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

Wenden Sie den Aufbewahrungszeitraum während der manuellen Snapshot-Erstellung an

Sie können eine Aufbewahrungsfrist für Snapshots anwenden, wenn Sie einen Snapshot manuell erstellen. Die Snapshot-Sperrung muss auf dem Volume aktiviert sein. Andernfalls wird die Einstellung für den Aufbewahrungszeitraum ignoriert.

System Manager

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

CLI

1. Geben Sie den folgenden Befehl ein, um einen Snapshot manuell zu erstellen und eine Aufbewahrungsfrist für die Sperrung anzuwenden:

   ```
   volume snapshot create -volume <volume_name> -snapshot <snapshot name>
   -snaplock-expiry-time <expiration_date_time>
   ```

   Mit dem folgenden Befehl wird ein neuer Snapshot erstellt und der Aufbewahrungszeitraum festgelegt:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Anwenden des Aufbewahrungszeitraums auf einen vorhandenen Snapshot

System Manager

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

CLI

1. Um einen vorhandenen Snapshot manuell auf eine Aufbewahrungsfrist anzuwenden, geben Sie den folgenden Befehl ein:

   ```
   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 vorhandenen Snapshot angewendet:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Ändern Sie eine vorhandene Richtlinie, um die langfristige Aufbewahrung anzuwenden

In einer SnapMirror Beziehung können Sie in einer Regel für die Richtlinie „Mirror-Vault“ eine Aufbewahrungsfrist festlegen, und der Aufbewahrungszeitraum wird für auf das Ziel-Volume replizierte Snapshots angewendet, wenn für das Ziel-Volume die Snapshot-Sperrung aktiviert ist. Die Aufbewahrungsfrist hat Vorrang vor der Anzahl behalten. Snapshots, die ihr Ablaufdatum nicht überschritten haben, werden z. B. auch dann beibehalten, wenn die Anzahl der Bewahren Daten überschritten wird.

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

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

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

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

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

Erfahren Sie mehr über `snapmirror policy add-rule` in der "ONTAP-Befehlsreferenz".

Konsistenzgruppen

Erfahren Sie mehr über ONTAP Consistency Groups

Eine Konsistenzgruppe ist eine Sammlung von Volumes, die als eine Einheit gemanagt werden. In ONTAP sorgen Konsistenzgruppen für ein einfaches Management und eine Garantie für die Sicherung eines Applikations-Workloads, der sich über mehrere Volumes erstreckt.

Sie können Konsistenzgruppen verwenden, um das Storage-Management zu vereinfachen. Stellen Sie sich vor, Sie verfügen über eine wichtige Datenbank mit zwanzig LUNs. Sie können die LUNs auf individueller Basis managen oder die LUNs als einzelnen Datensatz behandeln und sie in einer einzigen Konsistenzgruppe organisieren.

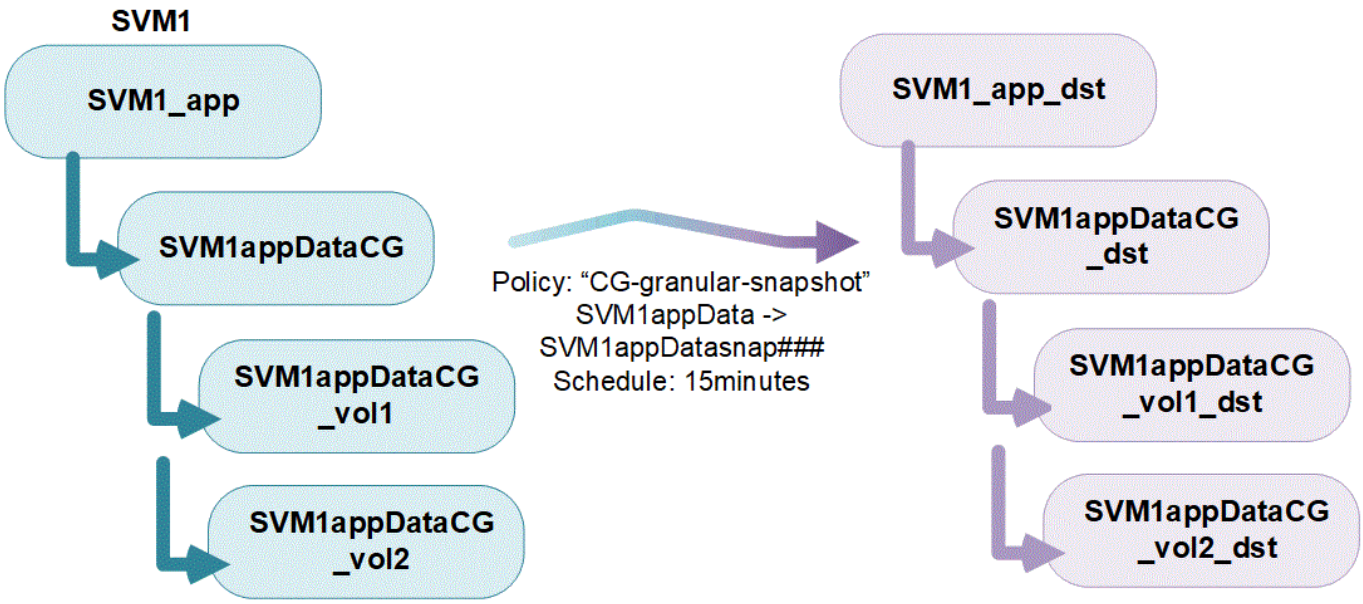
Consistency Groups erleichtern das Management von Applikations-Workloads. Sie ermöglichen einfach konfigurierte lokale und Remote-Schutzrichtlinien sowie simultane absturzkonsistente oder applikationskonsistente Snapshots einer Volume-Sammlung zu einem bestimmten Zeitpunkt. Snapshots einer Consistency Groups ermöglichen die Wiederherstellung eines gesamten Applikations-Workloads.

Erfahren Sie mehr über Konsistenzgruppen

Konsistenzgruppen unterstützen unabhängig vom Protokoll (NAS, SAN oder NVMe) jedes FlexVol Volume und können über die Rest-API von ONTAP oder im System Manager unter dem Menüpunkt **Storage > Konsistenzgruppen** gemanagt werden. Ab ONTAP 9.14.1 können Konsistenzgruppen über die ONTAP CLI verwaltet werden.

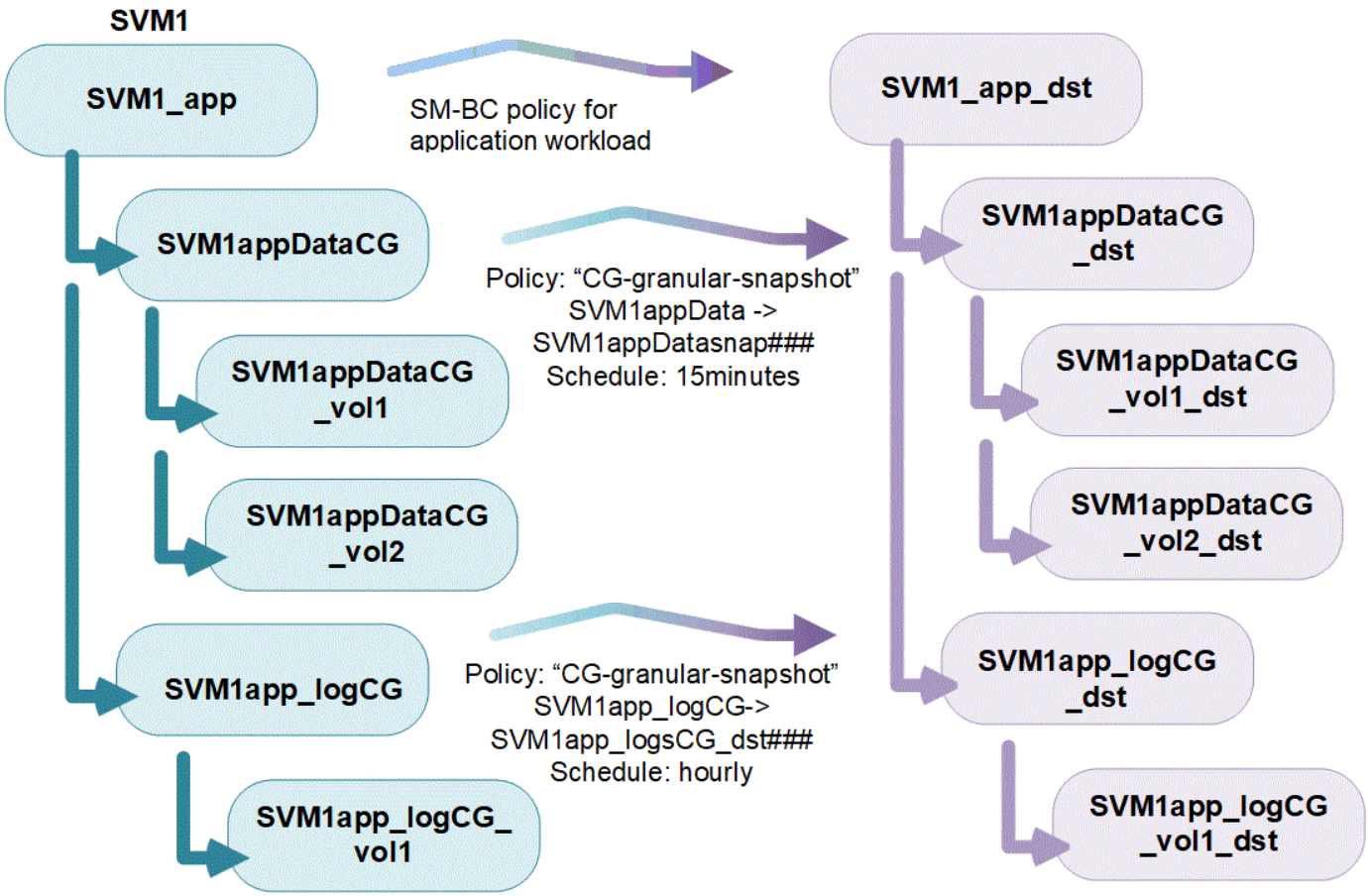
Consistency Groups können als einzelne Entitäten – als Sammlung von Volumes – oder in einer hierarchischen Beziehung existieren, die aus anderen Consistency Groups besteht. Einzelne Volumes können über eine eigene Snapshot-Richtlinie auf Volume-Granularität verfügen. Darüber hinaus kann es eine Snapshot-Richtlinie für die gesamte Konsistenzgruppe geben. Für die Konsistenzgruppe können nur eine aktive SnapMirror Synchronisierungsbeziehung und eine gemeinsame SnapMirror-Richtlinie verwendet werden, die zur Wiederherstellung der gesamten Konsistenzgruppe verwendet werden kann.

Im folgenden Diagramm wird veranschaulicht, wie Sie eine einzelne Konsistenzgruppe verwenden könnten. Die Daten für eine Applikation, die auf `SVM1` zwei Volumes gehostet wird: `vol1` Und `vol2`. Eine Snapshot-Richtlinie auf der Konsistenzgruppe erfasst alle 15 Minuten Snapshots der Daten.



Bei größeren Applikations-Workloads sind möglicherweise mehrere Konsistenzgruppen erforderlich. In diesen Situationen können Sie hierarchische Konsistenzgruppen erstellen, wobei eine einzelne Konsistenzgruppe zu den untergeordneten Komponenten einer übergeordneten Konsistenzgruppe wird. Die übergeordnete Konsistenzgruppe kann bis zu fünf untergeordnete Konsistenzgruppen enthalten. Wie bei einzelnen Konsistenzgruppen kann zur Wiederherstellung des Applikations-Workloads eine Richtlinie zur aktiven Synchronisierung von SnapMirror Remote auf die gesamte Konfiguration von Konsistenzgruppen (übergeordnet und untergeordnet) angewendet werden.

Im folgenden Beispiel wird eine Anwendung auf gehostet `SVM1`. Der Administrator hat eine übergeordnete Konsistenzgruppe erstellt, `SVM1_app` die zwei untergeordnete Konsistenzgruppen enthält: `SVM1appDataCG` Für die Daten und `SVM1app_logCG` für die Protokolle. Jede Child-Konsistenzgruppe verfügt über eine eigene Snapshot-Richtlinie. 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 Richtlinie zur aktiven Synchronisierung von SnapMirror, die die Daten repliziert, um einen unterbrechungsfreien Service bei einem Ausfall zu gewährleisten.



Ab ONTAP 9.12.1 unterstützen Klonen und ändern Konsistenzgruppen die Mitglieder der Konsistenz Hinzufügen oder Entfernen von Volumessowohl in System Manager als auch in der ONTAP-REST-API. Ab ONTAP 9.12.1 unterstützt die ONTAP-REST-API zudem:

- Erstellen von Konsistenzgruppen mit neuen NFS- oder SMB-Volumes oder NVMe-Namespaces
- Vorhandene Konsistenzgruppen werden neu oder vorhandene NFS- oder SMB-Volumes oder NVMe-Namespaces hinzugefügt.

Weitere Informationen zur ONTAP REST API finden Sie unter "Referenzdokumentation zur ONTAP REST-API".

Überwachen von Konsistenzgruppen

Ab ONTAP 9.13.1 bieten Konsistenzgruppen das Kapazitäts- und Performance-Monitoring in Echtzeit sowie darüber hinaus Erkenntnisse zur Performance von Applikationen und einzelnen Konsistenzgruppen.

Die Überwachungsdaten werden alle fünf Minuten aktualisiert und bis zu einem Jahr aufbewahrt. Sie können Metriken verfolgen für:

- Performance: IOPS, Latenz und Durchsatz
- Kapazität: Größe, genutzte logische Kapazität, verfügbar

Sie können Überwachungsdaten auf der Registerkarte **Übersicht** des Consistency Group Menüs in System Manager anzeigen oder in der REST API anfordern. Ab ONTAP 9.14.1 können Sie mithilfe des `consistency-group metrics show` Befehls Konsistenzgruppenmetriken mit der CLI anzeigen. Erfahren Sie mehr über `consistency-group metrics show` in der "ONTAP-Befehlsreferenz".

In ONTAP 9.13.1 können Sie Verlaufsmetriken nur mit der REST-API abrufen. Ab ONTAP 9.14.1 sind auch Verlaufsmetriken in System Manager verfügbar.

Schützen Sie Konsistenzgruppen

Konsistenzgruppen ermöglichen applikationskonsistente Sicherung, wodurch die Konsistenz Ihrer Daten über mehrere Volumes oder LIFs hinweg gewährleistet wird. Beim Erstellen eines Snapshots einer Konsistenzgruppe wird in der Konsistenzgruppe ein „Zaun“ eingerichtet. Der Zaun initiiert eine Warteschlange für I/O, bis der Snapshot-Vorgang abgeschlossen ist. Dies gewährleistet die Point-in-Time-Konsistenz der Daten über alle Entitäten in der Konsistenzgruppe hinweg. Der Zaun kann zu transienten Spitzen in der Latenz bei der Snapshot-Erstellung führen, wie z. B. eine geplante Snapshot-Richtlinie oder die Erstellung eines Snapshots mit System Manager. Weitere Informationen zum Kontext von REST-API und CLI finden Sie in "ONTAP REST API-Dokumentation"und "ONTAP-Befehlsreferenz".

Konsistenzgruppen bieten Schutz über:

- Snapshot-Richtlinien
- SnapMirror Active Sync
- [mcc] (Ab ONTAP 9.11.1)
- SnapMirror asynchron (Ab ONTAP 9.13.1)
- "Disaster Recovery für SVM" (Ab ONTAP 9.14.1)

Das Erstellen einer Konsistenzgruppe aktiviert den Schutz nicht automatisch. Richtlinien für den lokalen und Remote-Schutz können beim Erstellen einer Konsistenzgruppe oder nach dem Erstellen festgelegt werden.

Informationen zum Konfigurieren des Schutzes für eine Konsistenzgruppe finden Sie unter "Sichern einer Konsistenzgruppe".

Um den Fernschutz zu verwenden, müssen Sie die Anforderungen für erfüllenSnapMirror Active Sync.

SnapMirror Beziehungen mit aktiver Synchronisierung können nicht auf Volumes eingerichtet werden, die für den NAS-Zugriff gemountet wurden.

Unterstützung von Konsistenzgruppen durch mehrere Administratoren

Ab ONTAP 9.16.1 können Sie die Multi-Admin-Verifizierung (MAV) mit Konsistenzgruppen verwenden, um sicherzustellen, dass bestimmte Vorgänge, wie das Erstellen, Ändern oder Löschen von Konsistenzgruppen, nur nach Genehmigungen von designierten Administratoren ausgeführt werden können. So wird verhindert, dass kompromittierte, böswillige oder unerfahrene Administratoren unerwünschte Änderungen an bestehenden Konfigurationen vornehmen.

"Weitere Informationen ."

Konsistenzgruppen in MetroCluster Konfigurationen

Ab ONTAP 9.11.1 können Sie Konsistenzgruppen mit neuen Volumes auf einem Cluster innerhalb einer MetroCluster Konfiguration bereitstellen. Diese Volumes werden auf gespiegelten Aggregaten bereitgestellt.

Nachdem sie bereitgestellt wurden, können Sie Volumes, die mit Konsistenzgruppen verbunden sind, zwischen gespiegelten und nicht gespiegelten Aggregaten verschieben. Daher können sich Volumes, die mit Konsistenzgruppen verbunden sind, auf gespiegelten Aggregaten, nicht gespiegelten Aggregaten oder beidem befinden. Sie können gespiegelte Aggregate mit Volumes von Konsistenzgruppen ändern, um nicht gespiegelt

zu werden. Auf ähnliche Weise können Sie nicht gespiegelte Aggregate ändern, die mit Konsistenzgruppen verknüpfte Volumes enthalten, um die Spiegelung zu ermöglichen.

Volumes und Snapshots zu Konsistenzgruppen, die auf gespiegelten Aggregaten platziert werden, werden am Remote-Standort (Standort B) repliziert. Der Inhalt der Volumes auf Standort B garantiert der Konsistenzgruppe eine Schreibreihenfolge, bei einem Ausfall können Sie eine Wiederherstellung von Standort B durchführen. Sie können mithilfe der Konsistenzgruppe auf Snapshots von Konsistenzgruppen mit der REST-API und System Manager auf Clustern zugreifen, die ONTAP 9.11.1 oder höher ausführen. Ab ONTAP 9.14.1 können Sie auch über die ONTAP CLI auf Snapshots zugreifen.

Wenn sich einige oder alle Volumes einer Konsistenzgruppe auf nicht gespiegelten Aggregaten befinden, die derzeit nicht zugänglich sind, WERDEN VORGÄNGE in der Konsistenzgruppe ANGEZEIGT, so als ob die lokalen Volumes oder Hosting-Aggregate offline sind.

Konfigurationen von Konsistenzgruppen für die Replikation

Wenn an Standort B ONTAP 9.10.1 oder eine frühere Version ausgeführt wird, werden nur die Volumes repliziert, die den Konsistenzgruppen auf gespiegelten Aggregaten zugeordnet sind. Die Konfigurationen der Konsistenzgruppen werden nur an Standort B repliziert, wenn beide Standorte ONTAP 9.11.1 oder höher ausführen. Nachdem Standort B auf ONTAP 9.11.1 aktualisiert wurde, werden die Daten für Konsistenzgruppen auf Standort A repliziert, bei denen alle zugehörigen Volumes in gespiegelten Aggregaten platziert sind

> Es wird empfohlen, mindestens 20 % freien Speicherplatz für gespiegelte Aggregate vorzuhalten, um eine optimale Speicherleistung und Verfügbarkeit zu gewährleisten. Obwohl für nicht gespiegelte Aggregate 10 % empfohlen werden, können die zusätzlichen 10 % Speicherplatz vom Dateisystem genutzt werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Redirect-on-Write-Architektur von ONTAP. Die Nichteinhaltung dieser bewährten Vorgehensweisen kann sich negativ auf die Leistung auswirken.

Upgrade-Überlegungen

Beim Upgrade auf ONTAP 9.10.1 oder höher werden Consistency Groups, die mit SnapMirror Active Sync (früher bekannt als SnapMirror Business Continuity) in ONTAP 9.8 und 9.9.1 erstellt wurden, automatisch aktualisiert und unter **Speicher > Consistency Groups** im Systemmanager oder der ONTAP REST API verwaltet. Weitere Informationen zum Upgrade von ONTAP 9.8 oder 9.9.1 finden Sie unter "Upgrade und Überlegungen zu SnapMirror Active Sync Wechsel".

In der REST-API erstellte Snapshots von Konsistenzgruppen können über die Konsistenzgruppenschnittstelle von System Manager und über REST-API-Endpunkte von Konsistenzgruppen gemanagt werden. Ab ONTAP 9.14.1 können Konsistenzgruppen-Snapshots auch über die ONTAP CLI verwaltet werden.

> Snapshots, die mit den ONTAPI Befehlen erstellt `cg-start` wurden und `cg-commit` nicht als Snapshots von Konsistenzgruppen erkannt werden, können daher nicht über die Konsistenzgruppenschnittstelle von System Manager oder die Endpunkte der Konsistenzgruppe in der ONTAP REST API gemanagt werden. Ab ONTAP 9.14.1 können diese Snapshots mithilfe einer asynchronen SnapMirror-Richtlinie auf dem Ziel-Volume gespiegelt werden. Weitere Informationen finden Sie unter SnapMirror asynchron konfigurieren.

Unterstützte Funktionen von Version

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Hierarchische Konsistenzgruppen	✓	✓	✓	✓	✓	✓	✓
Lokaler Schutz durch Snapshots	✓	✓	✓	✓	✓	✓	✓
SnapMirror Active Sync	✓	✓	✓	✓	✓	✓	✓
MetroCluster Support	✓	✓	✓	✓	✓	✓	
Zwei-Phasen-Commits (nur REST API)	✓	✓	✓	✓	✓	✓	
Applikations- und Komponenten-Tags	✓	✓	✓	✓	✓		
Klonen von Konsistenzgruppen	✓	✓	✓	✓	✓		
Hinzufügen und Entfernen von Volumes	✓	✓	✓	✓	✓		
Erstellen Sie CGS mit neuen NAS-Volumes	✓	✓	✓	✓	Nur REST API		
CGS mit neuen NVMe-Namespaces erstellen	✓	✓	✓	✓	Nur REST API		
Verschieben Sie Volumes zwischen untergeordneten Konsistenzgruppen	✓	✓	✓	✓			
Ändern der Geometrie der Konsistenzgruppe	✓	✓	✓	✓			
Monitoring	✓	✓	✓	✓			
Überprüfung durch mehrere Administratoren	✓						
SnapMirror asynchron (nur einzelne Konsistenzgruppen)	✓	✓	✓	✓			
SVM-Disaster Recovery (nur einzelne Konsistenzgruppen)	✓	✓	✓				
CLI Support	✓	✓	✓				

Weitere Informationen zu Konsistenzgruppen

Verwandte Informationen

- "Dokumentation zur ONTAP Automatisierung"
- SnapMirror Active Sync
- Grundlagen der asynchronen Disaster Recovery von SnapMirror
- "MetroCluster-Dokumentation"
- "Überprüfung durch mehrere Administratoren"
- "ONTAP-Befehlsreferenz"

Erfahren Sie mehr über die Beschränkungen der ONTAP Konsistenzgruppe

Berücksichtigen Sie beim Planen und Verwalten von Konsistenzgruppen Objektbeschränkungen im Umfang des Clusters und der übergeordneten oder untergeordneten Konsistenzgruppe.

Erzwungene Grenzwerte

In der folgenden Tabelle werden die Grenzwerte für Konsistenzgruppen aufgeführt. Für Konsistenzgruppen, die SnapMirror Active Sync verwenden, gelten gesonderte Einschränkungen. Weitere Informationen finden Sie unter "Einschränkungen bei der aktiven SnapMirror Synchronisierung".

Grenze	Umfang	Minimum	Maximal
Anzahl der Konsistenzgruppen	Cluster	0	Entspricht der maximalen Volume-Anzahl im Cluster*

Anzahl der übergeordneten Konsistenzgruppen	Cluster	0	Die maximale Anzahl der Volumes im Cluster entspricht
Anzahl der einzelnen und übergeordneten Konsistenzgruppen	Cluster	0	Die maximale Anzahl der Volumes im Cluster entspricht
Anzahl der Volumes in einer Konsistenzgruppe	Eine Konsistenzgruppe	1 Lautstärke	80 Bände
Anzahl von Volumes in einer Konsistenzgruppe mit SnapMirror asynchron	Eine Konsistenzgruppe	1 Lautstärke	• Ab ONTAP 9.15.1: 80 Bände • In ONTAP 9.13.1 und 9.14.1: 16 Bände
Anzahl der Volumes im untergeordneten Element einer übergeordneten Konsistenzgruppe	Übergeordnete Konsistenzgruppe	1 Lautstärke	80 Bände
Anzahl der Volumes in einer untergeordneten Konsistenzgruppe	Untergeordnete Konsistenzgruppe	1 Lautstärke	80 Bände
Anzahl der untergeordneten Konsistenzgruppen in einer übergeordneten Konsistenzgruppe	Übergeordnete Konsistenzgruppe	1 Konsistenzgruppe	5 Konsistenzgruppen
Anzahl der SVM-Disaster-Recovery-Beziehungen mit einer Konsistenzgruppe (verfügbar ab ONTAP 9.14.1)	Cluster	0	32

* Es können maximal 50 Konsistenzgruppen, die mit asynchronem SnapMirror aktiviert sind, auf einem Cluster gehostet werden.

Nicht erzwungene Grenzwerte

Der unterstützte Mindestzeitplan für Konsistenzgruppen beträgt 30 Minuten. Dies basiert auf "Testen für FlexGroup Volumes", die dieselbe Snapshot Infrastruktur wie Konsistenzgruppen verwenden.

Konfigurieren einer einzelnen ONTAP Konsistenzgruppe

Konsistenzgruppen können mit vorhandenen Volumes oder neuen LUNs oder Volumes erstellt werden (je nach Version der ONTAP). Ein Volume oder eine LUN kann jeweils nur einer Konsistenzgruppe zugeordnet werden.

Über diese Aufgabe

- In ONTAP 9.10.1 bis 9.11.1 wird das Ändern der Mitglieds-Volumes einer Konsistenzgruppe nach dem

Erstellen nicht unterstützt.

Ab ONTAP 9.12.1 können Sie die Mitglieds-Volumes einer Konsistenzgruppe ändern. Weitere Informationen zu diesem Vorgang finden Sie unter Ändern einer Konsistenzgruppe.

- Ab ONTAP 9.17.1 können Sie das NVMe-Protokoll auswählen, um einen Host einem NVMe-Subsystem für VMware-Workloads in einer SnapMirror Active Sync-Konfiguration zuzuordnen.

Erstellen einer Konsistenzgruppe mit neuen LUNs oder Volumes

In ONTAP 9.10.1 bis 9.12.1 können Sie eine Konsistenzgruppe erstellen, die neue LUNs verwendet. Ab ONTAP 9.13.1 unterstützt System Manager auch das Erstellen einer Konsistenzgruppe mit neuen NVMe-Namespaces oder neuen NAS-Volumes. (Ab ONTAP 9.12.1 wird dies auch in der ONTAP-REST-API unterstützt.)

System Manager (ONTAP 9.16.1 und früher)

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie **+Add** und wählen Sie dann das Protokoll für Ihr Speicherobjekt aus.

   In ONTAP 9.10.1 bis 9.12.1 ist die einzige Option für ein neues Speicherobjekt **mit neuen LUNs**. Ab ONTAP 9.13.1 unterstützt System Manager das Erstellen von Konsistenzgruppen mit neuen NVMe-Namespaces und neuen NAS-Volumes.

3. Benennen Sie die Konsistenzgruppe. Geben Sie die Anzahl der Volumes oder LUNs und die Kapazität pro Volume oder LUN an.
   a. **Anwendungstyp**: Wenn Sie ONTAP 9.12.1 oder höher verwenden, wählen Sie einen Anwendungstyp aus. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ von **Other** zugewiesen. Erfahren Sie mehr über das Markieren von Konsistenz in Applikations- und Komponenten-Tags. Wenn Sie eine Consistency Group mit einer Remote-Schutz-Policy erstellen möchten, müssen Sie **andere** verwenden.
   b. Für **Neue LUNs**: Wählen Sie das Host-Betriebssystem und das LUN-Format aus. Geben Sie die Informationen zum Host-Initiator ein.
   c. Für **Neue NAS-Volumes**: Wählen Sie die entsprechende Exportoption (NFS oder SMB/CIFS) basierend auf der NAS-Konfiguration Ihrer SVM.
   d. Für **Neue NVMe-Namespaces**: Wählen Sie das Host-Betriebssystem und das NVMe-Subsystem aus.
4. Um Schutzrichtlinien zu konfigurieren, fügen Sie eine untergeordnete Consistency Group hinzu, oder wählen Sie **Weitere Optionen** aus.
5. Wählen Sie **Speichern**.
6. Bestätigen Sie, dass Ihre Konsistenzgruppe erstellt wurde, indem Sie zum Hauptmenü der Konsistenzgruppe zurückkehren. Dort wird sie nach Abschluss des Jobs angezeigt. Wenn Sie eine Schutzrichtlinie festlegen, wissen Sie, dass sie angewendet wurde, wenn Sie unter der entsprechenden Richtlinie, Remote oder lokal, einen grünen Schild sehen.

System Manager (ONTAP 9.17.1 und höher)

Schritte

1. Wählen Sie **Schutz > Konsistenzgruppen**.
2. Wählen Sie **+Add** und wählen Sie dann das Protokoll für Ihr Speicherobjekt aus.
3. Benennen Sie die Konsistenzgruppe. Geben Sie die Anzahl der Volumes oder LUNs und die Kapazität pro Volume oder LUN an. **Anwendungstyp**: Wählen Sie einen Anwendungstyp. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ **Sonstige** zugewiesen. Weitere Informationen zum Taggen von Konsistenz finden Sie unter Applikations- und Komponenten-Tags Wenn Sie eine Konsistenzgruppe mit einer Remote-Schutzrichtlinie erstellen möchten, müssen Sie **Andere** verwenden.
   a. Für **Neue LUNs**: Wählen Sie das Host-Betriebssystem und das LUN-Format aus. Geben Sie die Informationen zum Host-Initiator ein.
   b. Für **Neue NAS-Volumes**: Wählen Sie die entsprechende Exportoption (NFS oder SMB/CIFS) basierend auf der NAS-Konfiguration Ihrer SVM.
   c. Für **Neue NVMe-Namespaces**: Wählen Sie das Host-Betriebssystem und das NVMe-Subsystem aus.

4. Um Schutzrichtlinien zu konfigurieren, fügen Sie eine untergeordnete Consistency Group hinzu, oder wählen Sie **Weitere Optionen** aus.
5. Wählen Sie **Speichern**.
6. Bestätigen Sie, dass Ihre Konsistenzgruppe erstellt wurde, indem Sie zum Hauptmenü der Konsistenzgruppe zurückkehren. Dort wird sie nach Abschluss des Jobs angezeigt. Wenn Sie eine Schutzrichtlinie festlegen, wissen Sie, dass sie angewendet wurde, wenn Sie unter der entsprechenden Richtlinie, Remote oder lokal, einen grünen Schild sehen.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der ONTAP CLI eine neue Konsistenzgruppe mit neuen Volumes erstellen. Die spezifischen Parameter hängen davon ab, ob die Volumes SAN, NVMe oder NFS sind.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Erstellen einer Konsistenzgruppe mit NFS-Volumes

1. Erstellen Sie die Konsistenzgruppe:

```
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>
```

Erstellen einer Konsistenzgruppe mit SAN-Volumes

1. Erstellen Sie die Konsistenzgruppe:

```
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>
```

Erstellen einer Konsistenzgruppe mit NVMe-Namespaces

1. Erstellen Sie die Konsistenzgruppe:

```
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>
```

   Erfahren Sie mehr über `consistency-group create` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

1. Überprüfen Sie, ob Ihre Konsistenzgruppe mit dem `consistency-group show` Befehl erstellt wurde.

   Erfahren Sie mehr über `consistency-group show` in der "ONTAP-Befehlsreferenz".

Erstellen einer Konsistenzgruppe mit vorhandenen Volumes

Sie können vorhandene Volumes zum Erstellen einer Konsistenzgruppe verwenden.

System Manager (ONTAP 9.16.1 und früher)

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie **+Add** und dann **mit vorhandenen Volumes** aus.
3. Benennen Sie die Konsistenzgruppe, und wählen Sie die Storage-VM aus.
   a. **Anwendungstyp**: Wenn Sie ONTAP 9.12.1 oder höher verwenden, wählen Sie einen Anwendungstyp aus. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ von **Other** zugewiesen. Erfahren Sie mehr über das Markieren von Konsistenz in Applikations- und Komponenten-Tags. Wenn die Konsistenzgruppe eine SnapMirror-Beziehung hat, müssen Sie **andere** 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 nicht bereits zu einer Konsistenzgruppe gehören, können ausgewählt werden.

   > Beim Erstellen einer Konsistenzgruppe mit vorhandenen Volumes unterstützt die Konsistenzgruppe FlexVol Volumes. Volumes mit synchronen oder asynchronen SnapMirror Beziehungen können Konsistenzgruppen hinzugefügt werden, sie sind jedoch nicht an Konsistenzgruppen orientiert. Konsistenzgruppen unterstützen keine S3-Buckets oder Storage-VMs mit SVMDR-Beziehungen.

5. Wählen Sie **Speichern**.
6. Vergewissern Sie sich, dass Ihre Konsistenzgruppe erstellt wurde, indem Sie zum Haupt-Konsistenzgruppenmenü zurückkehren, wo sie nach Abschluss des ONTAP Jobs angezeigt wird. Wenn Sie eine Schutzrichtlinie ausgewählt haben, bestätigen Sie, dass sie richtig eingestellt wurde, indem Sie Ihre Konsistenzgruppe im Menü auswählen. Wenn Sie eine Schutzrichtlinie festlegen, wissen Sie, dass sie angewendet wurde, wenn Sie unter der entsprechenden Richtlinie einen grünen Schild sehen, entweder Remote oder lokal.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der ONTAP CLI eine Konsistenzgruppe mit vorhandenen Volumes erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Geben Sie den `consistency-group create` Befehl ein. 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>
   ```

   Erfahren Sie mehr über `consistency-group create` in der "ONTAP-Befehlsreferenz".

2. Zeigen Sie mit dem `consistency-group show` Befehl Ihre Konsistenzgruppe an.

   Erfahren Sie mehr über `consistency-group show` in der "ONTAP-Befehlsreferenz".

Nächste Schritte

- Sichern einer Konsistenzgruppe
- Ändern einer Konsistenzgruppe
- Klonen einer Konsistenzgruppe

Konfigurieren einer hierarchischen ONTAP Konsistenzgruppe

Mithilfe von hierarchischen Konsistenzgruppen können Sie große Workloads über mehrere Volumes hinweg managen, indem Sie eine übergeordnete Konsistenzgruppe erstellen, die als übergeordnete Konsistenzgruppe für untergeordnete Konsistenzgruppen dient.

Hierarchische Konsistenzgruppen verfügen über ein übergeordnetes Objekt, das bis zu fünf individuelle Konsistenzgruppen umfassen kann. Hierarchische Konsistenzgruppen können unterschiedliche lokale Snapshot-Richtlinien über Konsistenzgruppen oder einzelne Volumes hinweg unterstützen. Wenn Sie eine Remote-Schutzrichtlinie verwenden, gilt diese für die gesamte hierarchische Konsistenzgruppe (übergeordnete und untergeordnete Elemente).

Beginnend mit ONTAP 9.13.1, können Sie Ändern Sie die Geometrie der Konsistenzgruppenund Verschieben Sie Volumes zwischen untergeordneten Konsistenzgruppen.

Objektgrenzen für Konsistenzgruppen finden Sie unter Objektbeschränkungen für Konsistenzgruppen.

Hierarchische Konsistenzgruppe mit neuen LUNs oder Volumes erstellen

Beim Erstellen einer hierarchischen Konsistenzgruppe können Sie sie mit neuen LUNs füllen. Ab ONTAP 9.13.1 können auch neue NVMe-Namespaces und NAS-Volumes verwendet werden.

System Manager

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie **+Add** und wählen Sie dann das Protokoll für Ihr Speicherobjekt aus.

   In ONTAP 9.10.1 bis 9.12.1 ist die einzige Option für ein neues Speicherobjekt **mit neuen LUNs**. Ab ONTAP 9.13.1 unterstützt System Manager das Erstellen von Konsistenzgruppen mit neuen NVMe-Namespaces und neuen NAS-Volumes.

3. Benennen Sie die Konsistenzgruppe. Geben Sie die Anzahl der Volumes oder LUNs und die Kapazität pro Volume oder LUN an.
   a. **Anwendungstyp**: Wenn Sie ONTAP 9.12.1 oder höher verwenden, wählen Sie einen Anwendungstyp aus. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ von **Other** zugewiesen. Erfahren Sie mehr über das Markieren von Konsistenz in Applikations- und Komponenten-Tags. Wenn Sie eine Richtlinie für den Remote-Schutz verwenden möchten, müssen Sie **andere** wählen.
4. Wählen Sie das Host-Betriebssystem und das LUN-Format aus. Geben Sie die Informationen zum Host-Initiator ein.
   a. Für **Neue LUNs**: Wählen Sie das Host-Betriebssystem und das LUN-Format aus. Geben Sie die Informationen zum Host-Initiator ein.
   b. Für **Neue NAS-Volumes**: Wählen Sie die entsprechende Exportoption (NFS oder SMB/CIFS) basierend auf der NAS-Konfiguration Ihrer SVM.
   c. Für **Neue NVMe-Namespaces**: Wählen Sie das Host-Betriebssystem und das NVMe-Subsystem aus.
5. Um eine untergeordnete Consistency Group hinzuzufügen, wählen Sie **More options** und dann **+Add child Consistency Group** aus.
6. Wählen Sie das Performance-Level, die Anzahl der LUNs oder Volumes und die Kapazität pro LUN oder Volume aus. Legen Sie die entsprechenden Exportkonfigurationen oder Betriebssysteminformationen auf der Grundlage des verwendeten Protokolls fest.
7. Wählen Sie optional eine lokale Snapshot-Richtlinie aus und legen Sie die Zugriffsberechtigungen fest.
8. Wiederholen Sie dies für bis zu fünf Child-Konsistenzgruppen.
9. Wählen Sie **Speichern**.
10. Überprüfen Sie, ob die Konsistenzgruppe erstellt wurde, indem Sie zum Hauptmenü der Konsistenzgruppe zurückkehren, wo sie nach Abschluss des ONTAP-Jobs angezeigt wird. Wenn Sie eine Schutzrichtlinie festlegen, achten Sie auf die entsprechende Richtlinie, Remote oder lokal, die einen grünen Schild mit einem Häkchen anzeigen soll.

CLI

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Wenn Sie in der CLI mit neuen Volumes eine hierarchische Konsistenzgruppe erstellen, müssen Sie jede untergeordnete Konsistenzgruppe einzeln erstellen.

Schritt

1. Erstellen Sie die neue Konsistenzgruppe mit dem `consistency-group create` Befehl.

   ```
   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 aufgefordert werden, bestätigen Sie, dass Sie die neue übergeordnete Konsistenzgruppe erstellen möchten. Geben Sie Ein. `y`
3. Wiederholen Sie optional Schritt 1, um weitere untergeordnete Konsistenzgruppen zu erstellen.

   Erfahren Sie mehr über `consistency-group create` in der "ONTAP-Befehlsreferenz".

Erstellen einer hierarchischen Konsistenzgruppe mit vorhandenen Volumes

Vorhandene Volumes können in einer hierarchischen Konsistenzgruppe organisiert werden.

System Manager

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie **+Add** und dann **mit vorhandenen Volumes** aus.
3. Wählen Sie die Storage-VM aus.
4. Wählen Sie die vorhandenen Volumes aus, die einbezogen werden sollen. Nur Volumes, die nicht bereits zu einer Konsistenzgruppe gehören, können ausgewählt werden.
5. Um eine untergeordnete Consistency Group hinzuzufügen, wählen Sie **+Child Consistency Group** hinzufügen. Erstellen Sie die erforderlichen Konsistenzgruppen, die automatisch benannt werden.
   a. **Komponententyp**: Wenn Sie ONTAP 9.12.1 oder höher verwenden, wählen Sie einen Komponententyp von „Daten“, „Logs“ oder „Sonstige“ aus. Wenn kein Wert ausgewählt ist, wird der Konsistenzgruppe standardmäßig der Typ von **Other** zugewiesen. Erfahren Sie mehr über das Markieren von Konsistenz in Applikations- und Komponenten-Tags. Wenn Sie eine Richtlinie für den Remote-Schutz verwenden möchten, müssen Sie **andere** verwenden.
6. Weisen Sie jeder Konsistenzgruppe vorhandene Volumes zu.
7. Wählen Sie optional eine lokale Snapshot-Richtlinie aus.
8. Wiederholen Sie dies für bis zu fünf Child-Konsistenzgruppen.
9. Wählen Sie **Speichern**.
10. Überprüfen Sie, ob die Konsistenzgruppe erstellt wurde, indem Sie zum Hauptmenü der Konsistenzgruppe zurückkehren, wo sie nach Abschluss des ONTAP-Jobs angezeigt wird. Wenn Sie eine Schutzrichtlinie ausgewählt haben, bestätigen Sie, dass die Richtlinie richtig eingestellt wurde, indem Sie Ihre Konsistenzgruppe aus dem Menü auswählen. Unter dem entsprechenden Richtlinientyp wird ein grüner Schild mit einem Häkchen angezeigt.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der CLI eine hierarchische Konsistenzgruppe erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Stellen Sie eine neue übergeordnete Konsistenzgruppe bereit, und weisen Sie Volumes einer neuen untergeordneten Konsistenzgruppe zu:

   ```
   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 ein `y`, um zu bestätigen, dass Sie eine neue übergeordnete und untergeordnete Konsistenzgruppe erstellen möchten.

   Erfahren Sie mehr über `consistency-group create` in der "ONTAP-Befehlsreferenz".

Nächste Schritte

- Ändern Sie die Geometrie einer Konsistenzgruppen
- Ändern einer Konsistenzgruppe
- Sichern einer Konsistenzgruppe

Schützen Sie ONTAP Consistency Groups

Konsistenzgruppen bieten einfach lokalen und Remote-Schutz für SAN-, NAS- und NVMe-Applikationen, die mehrere Volumes umfassen.

Das Erstellen einer Konsistenzgruppe aktiviert den Schutz nicht automatisch. Sicherungsrichtlinien können zum Zeitpunkt der Erstellung oder nach der Erstellung der Konsistenzgruppe festgelegt werden. Sie können Konsistenzgruppen schützen, indem Sie:

- Lokale Snapshots
- SnapMirror Active Sync (SnapMirror Business Continuity in Versionen von ONTAP vor 9.15.1)
- MetroCluster (Beginn 9.11.1)
- SnapMirror asynchron (ab 9.13.1)
- Asynchrone SVM-Disaster Recovery (Anfang 9.14.1)

Wenn Sie geschachtelte Konsistenzgruppen verwenden, können Sie verschiedene Schutzrichtlinien für die übergeordneten und untergeordneten Konsistenzgruppen festlegen.

Ab ONTAP 9.11.1 bieten Konsistenzgruppen Erstellen von Snapshots von Konsistenzgruppen in zwei Phasenan. Der zweiphasige Snapshot führt eine Vorabprüfung durch, um sicherzustellen, dass der Snapshot erfolgreich erfasst wird.

Die Wiederherstellung kann für eine gesamte Konsistenzgruppe, eine einzelne Konsistenzgruppe in einer hierarchischen Konfiguration oder für einzelne Volumes innerhalb der Konsistenzgruppe erfolgen. Eine Recovery kann durchgeführt werden, indem die Konsistenzgruppe ausgewählt, die wiederhergestellt werden soll, der Snapshot-Typ ausgewählt und dann der Snapshot identifiziert wird, auf dem die Wiederherstellung basieren soll. Weitere Informationen zu diesem Prozess finden Sie unter "Stellen Sie ein Volume aus einem früheren Snapshot wieder her".

Konfigurieren Sie eine lokale Snapshot-Richtlinie

Durch das Festlegen einer lokalen Snapshot-Schutzrichtlinie können Sie eine Richtlinie erstellen, die alle Volumes in einer Konsistenzgruppe abdeckt.

Über diese Aufgabe

Der unterstützte Mindestzeitplan für Konsistenzgruppen beträgt 30 Minuten. Dies basiert auf "Testen für FlexGroup Volumes", die dieselbe Snapshot Infrastruktur wie Konsistenzgruppen verwenden.

System Manager

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die Konsistenzgruppe aus, die Sie im Menü Konsistenzgruppe erstellt haben.
3. Wählen Sie oben rechts auf der Übersichtsseite für die Konsistenzgruppe **Bearbeiten** aus.
4. Aktivieren Sie das Kontrollkästchen neben **Snapshots planen (lokal)**.
5. Wählen Sie eine Snapshot-Richtlinie aus. Informationen zum Konfigurieren einer neuen benutzerdefinierten Richtlinie finden Sie unter "Erstellen einer benutzerdefinierten Datensicherungsrichtlinie".
6. Wählen Sie **Speichern**.
7. Kehren Sie zum Menü „Übersicht der Konsistenzgruppen“ zurück. In der linken Spalte unter **Snapshots (Local)** wird der Status neben geschützt angezeigt.

CLI

Ab ONTAP 9.14.1 können Sie die Schutzrichtlinie einer Konsistenzgruppe über die CLI ändern.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Geben Sie den folgenden Befehl ein, um die Schutzrichtlinie festzulegen oder zu ändern:

   Wenn Sie die Schutzrichtlinie 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

Wenn Sie einen Snapshot Ihrer Konsistenzgruppe außerhalb einer normalerweise geplanten Richtlinie erstellen müssen, können Sie einen On-Demand-Snapshot erstellen.

System Manager

Schritte

1. Navigieren Sie zu **Storage** > **Consistency Groups**.
2. Wählen Sie die Konsistenzgruppe aus, für die Sie einen On-Demand-Snapshot erstellen möchten.
3. Wechseln Sie zur Registerkarte **Snapshot copies** und wählen Sie **+Add**.
4. Geben Sie einen **Name** und ein **SnapMirror Label** an. Wählen Sie im Dropdown-Menü für **Konsistenz** die Option **Application consistent** oder **Crash consistent** aus.
5. Wählen Sie **Speichern**.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der CLI einen On-Demand Snapshot einer Konsistenzgruppe erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Erstellen Sie den Snapshot:

   Standardmäßig ist der Snapshot-Typ absturzkonsistent. Sie können den Snapshot-Typ mit dem optionalen Parameter ändern `-type`.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Erstellen von Snapshots mit zwei Phasen einer Konsistenzgruppe

Ab ONTAP 9.11.1 unterstützen Konsistenzgruppen zwei-Phasen-Commits für die Erstellung von Konsistenzgruppen (CG)-Snapshots, die vor dem Übergeben des Snapshots eine Vorabprüfung ausführen. Diese Funktion ist nur für die ONTAP REST API verfügbar.

Die Erstellung von CG-Snapshots in zwei Phasen ist nur für die Snapshot-Erstellung verfügbar, nicht für das Bereitstellen von Konsistenzgruppen und das Wiederherstellen von Konsistenzgruppen.

Ein zweiphasiger CG-Snapshot unterteilt die Erstellung des Snapshots in zwei Phasen:

1. In der ersten Phase führt die API Vorabprüfungen aus und löst die Snapshot-Erstellung aus. Die erste Phase enthält einen Timeout-Parameter, der die Zeit angibt, die der Snapshot erfolgreich festschreiben muss.
2. Wenn die Anforderung in Phase 1 erfolgreich abgeschlossen wurde, können Sie die zweite Phase innerhalb des festgelegten Intervalls ab der ersten Phase aufrufen und den Snapshot an den entsprechenden Endpunkt übertragen.

Bevor Sie beginnen

- Um die Erstellung von CG-Snapshots in zwei Phasen zu verwenden, müssen auf allen Nodes im Cluster

ONTAP 9.11.1 oder höher ausgeführt werden.

- Es wird jeweils nur ein aktiver Aufruf eines Snapshot einer Konsistenzgruppe unterstützt, unabhängig davon, ob es sich um eine ein- oder zwei-Phasen-Instanz einer Konsistenzgruppe handelt. Der Versuch, einen Snapshot-Vorgang aufzurufen, während ein anderer ausgeführt wird, führt zu einem Fehler.
- Wenn Sie die Snapshot-Erstellung aufrufen, können Sie einen optionalen Timeout-Wert zwischen 5 und 120 Sekunden festlegen. Wenn kein Timeout-Wert angegeben wird, wird die Zeit für den Vorgang standardmäßig auf 7 Sekunden überschritten. Legen Sie in der API den Timeout-Wert mit dem `action_timeout` Parameter fest. Verwenden Sie in der CLI das `-timeout` Flag.

Schritte

Sie können einen zweiphasigen Snapshot mit der REST-API oder ab ONTAP 9.14.1 auch mit der ONTAP-CLI erstellen. Dieser Vorgang wird von System Manager nicht unterstützt.

> Wenn Sie die Snapshot-Erstellung mit der API aufrufen, müssen Sie den Snapshot mit der API übergeben. Wenn Sie die Snapshot-Erstellung mit der CLI aufrufen, müssen Sie den Snapshot mit der CLI übergeben. Mischmethoden werden nicht unterstützt.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der CLI einen zweiphasigen Snapshot erstellen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Initiieren des Snapshots:

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Überprüfen Sie, ob der Snapshot erstellt wurde:

   ```
   consistency-group snapshot show
   ```

3. Snapshot festschreiben:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. Rufen Sie die Snapshot-Erstellung auf. Senden Sie eine POST-Anforderung mit dem `action=start` Parameter an den Endpunkt der Konsistenzgruppe.

   ```
   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-Anforderung erfolgreich war, enthält die Ausgabe eine Snapshot-UUID. Übermitteln Sie mithilfe dieser UUID eine PATCH-Anforderung, um den Snapshot zu übergeben.

```
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.
```

Legen Sie den Remote-Schutz für eine Konsistenzgruppe fest

Konsistenzgruppen bieten Remote-Schutz über SnapMirror Active Sync und ab ONTAP 9.13.1 SnapMirror Asynchronous.

Konfiguration des Schutzes mit SnapMirror Active Sync

Sie können SnapMirror Active Sync verwenden, um sicherzustellen, dass Snapshots von Konsistenzgruppen, die in der Konsistenzgruppe erstellt werden, auf das Ziel kopiert werden. Weitere Informationen über SnapMirror Active Sync oder die Konfiguration von SnapMirror Active Sync über die CLI finden Sie unter Schutz für Business Continuity konfigurieren.

Bevor Sie beginnen

- SnapMirror Beziehungen mit aktiver Synchronisierung können nicht auf Volumes eingerichtet werden, die für den NAS-Zugriff gemountet wurden.
- Die Richtlinienbeschriftungen im Quell- und Ziel-Cluster müssen übereinstimmen.
- SnapMirror Active Sync repliziert Snapshots standardmäßig nicht, es sei denn, eine Regel mit einem SnapMirror-Label wird der vordefinierten Richtlinie hinzugefügt `AutomatedFailOver` und die Snapshots werden mit diesem Label erstellt.

  Weitere Informationen zu diesem Prozess finden Sie unter "Sicherung mit aktiver SnapMirror Synchronisierung".

- Kaskadenimplementierungen Werden bei aktiver SnapMirror-Synchronisierung nicht unterstützt.
- Ab ONTAP 9.13.1 ist Fügen Sie einer Konsistenzgruppe Volumes hinzueine aktive SnapMirror Active Sync Beziehung unterbrechungsfrei möglich. Bei allen anderen Änderungen an einer Konsistenzgruppe müssen Sie die SnapMirror Beziehung „Active Sync“ unterbrechen, die Konsistenzgruppe ändern, dann die Beziehung wiederherstellen und neu synchronisieren.

Informationen zum Konfigurieren der aktiven SnapMirror-Synchronisierung mit der CLI finden Sie unter Sicherung mit aktiver SnapMirror Synchronisierung.

Schritte für System Manager

1. Stellen Sie sicher, dass Sie die erfüllt haben"Voraussetzungen für die Nutzung von SnapMirror Active Sync".
2. Wählen Sie **Storage > Consistency Groups** aus.

3. Wählen Sie die Konsistenzgruppe aus, die Sie im Menü Konsistenzgruppe erstellt haben.
4. Rechts oben auf der Übersichtsseite wählen Sie **Mehr** und dann **schützen**.
5. System Manager füllt die Informationen auf der Quellseite automatisch aus. Wählen Sie die entsprechende Cluster- und Storage-VM für das Ziel aus. Wählen Sie eine Schutzrichtlinie aus. Vergewissern Sie sich, dass **Beziehung initialisieren** überprüft wird.
6. Wählen Sie **Speichern**.
7. Die Konsistenzgruppe muss initialisiert und synchronisiert werden. Bestätigen Sie, dass die Synchronisierung erfolgreich abgeschlossen wurde, indem Sie zum Menü **Consistency Group** zurückkehren. Der Status **SnapMirror (Remote)** wird neben angezeigt `Protected` .

SnapMirror asynchron konfigurieren

Ab ONTAP 9.13.1 können Sie den asynchronen Schutz von SnapMirror für eine einzelne Konsistenzgruppe konfigurieren. Ab ONTAP 9.14.1 können Sie SnapMirror asynchron verwenden, um mithilfe der Konsistenzgruppenbeziehung Volume-granulare Snapshots auf den Ziel-Cluster zu replizieren.

Über diese Aufgabe

Um Snapshots auf Volume-Ebene zu replizieren, müssen Sie ONTAP 9.14.1 oder höher ausführen. Für MirrorAndVault- und Vault-Richtlinien muss das SnapMirror-Label der Volume-granular-Snapshot-Richtlinie mit der SnapMirror-Richtlinienregel der Consistency Group übereinstimmen. Volume-granulare Snapshots halten den behalten-Wert der SnapMirror-Richtlinie der Konsistenzgruppe ein. Diese wird unabhängig von den Snapshots der Konsistenzgruppe berechnet. Wenn Sie zum Beispiel eine Richtlinie haben, um zwei Snapshots auf dem Ziel zu behalten, können Sie zwei Volume-granulare Snapshots und zwei Snapshots von Konsistenzgruppen haben.

Beim erneuten Synchronisieren der SnapMirror-Beziehung mit Volume-granularen Snapshots können Sie Volume-granulare Snapshots mit dem Flag beibehalten `-preserve`. Snapshots mit Volume-Granularität, die neuer sind als Snapshots von Konsistenzgruppen, werden beibehalten. Wenn kein Snapshot einer Konsistenzgruppe vorhanden ist, können im Resynchronisierungsvorgang keine Volume-granularen Snapshots übertragen werden.

Bevor Sie beginnen

- Der asynchrone Schutz von SnapMirror ist nur für eine einzelne Konsistenzgruppe verfügbar. Sie wird für hierarchische Konsistenzgruppen nicht unterstützt. Informationen zum Konvertieren einer hierarchischen Konsistenzgruppe in eine einzige Konsistenzgruppe finden Sie unter Ändern der Architektur von Konsistenzgruppen.
- Die Richtlinienbeschriftungen im Quell- und Ziel-Cluster müssen übereinstimmen.
- Fügen Sie einer Konsistenzgruppe Volumes hinzuEine aktive asynchrone SnapMirror-Beziehung unterbrechungsfrei ausgeführt werden kann. Bei allen anderen Änderungen an einer Konsistenzgruppe müssen Sie die SnapMirror Beziehung unterbrechen, die Konsistenzgruppe ändern, dann die Beziehung wiederherstellen und neu synchronisieren.
- Konsistenzgruppen, die für den Schutz mit SnapMirror asynchron aktiviert sind, weisen unterschiedliche Limits auf. Weitere Informationen finden Sie unter Einschränkungen für Konsistenzgruppen.
- Wenn Sie eine asynchrone Sicherungsbeziehung von SnapMirror für mehrere einzelne Volumes konfiguriert haben, können Sie diese Volumes in eine Konsistenzgruppe konvertieren, während die vorhandenen Snapshots beibehalten werden. So konvertieren Sie Volumes erfolgreich:
  - Es muss ein gemeinsamer Snapshot der Volumen sein.
  - Sie müssen die bestehende SnapMirror-Beziehung unterbrechen und Fügen Sie die Volumes einer einzelnen Konsistenzgruppe hinzudie Beziehung mit dem folgenden Workflow erneut synchronisieren.

Schritte

1. Wählen Sie im Zielcluster **Storage > Consistency Groups** aus.
2. Wählen Sie die Konsistenzgruppe aus, die Sie im Menü Konsistenzgruppe erstellt haben.
3. Rechts oben auf der Übersichtsseite wählen Sie **Mehr** und dann **schützen**.
4. System Manager füllt die Informationen auf der Quellseite automatisch aus. Wählen Sie die entsprechende Cluster- und Storage-VM für das Ziel aus. Wählen Sie eine Schutzrichtlinie aus. Vergewissern Sie sich, dass **Beziehung initialisieren** überprüft wird.

   Wenn Sie eine asynchrone Richtlinie auswählen, haben Sie die Option **Übertragungszeitplan überschreiben**.

   > Der unterstützte Mindestzeitplan (Recovery Point Objective oder RPO) für Konsistenzgruppen mit asynchronem SnapMirror beträgt 30 Minuten.

5. Wählen Sie **Speichern**.
6. Die Konsistenzgruppe muss initialisiert und synchronisiert werden. Bestätigen Sie, dass die Synchronisierung erfolgreich abgeschlossen wurde, indem Sie zum Menü **Consistency Group** zurückkehren. Der Status **SnapMirror (Remote)** wird neben angezeigt `Protected` .

SVM-Disaster Recovery konfigurieren

Ab ONTAP 9.14.1 Disaster Recovery für SVMunterstützt Konsistenzgruppen und ermöglicht es Ihnen, Konsistenzgruppeninformationen von der Quelle auf das Ziel-Cluster zu spiegeln.

Wenn Sie das SVM-Disaster Recovery auf einer SVM aktivieren, die bereits eine Konsistenzgruppe enthält, folgen Sie den SVM-Konfigurations-Workflows für System Manager oder der CLI VON ONTAP.

Wenn Sie einer SVM eine Konsistenzgruppe hinzufügen, die sich in einer aktiven und funktionierenden SVM-Disaster-Recovery-Beziehung befindet, müssen Sie die SVM-Disaster-Recovery-Beziehung vom Ziel-Cluster aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Sie eine Replikationsbeziehung manuell. Sie müssen die Beziehung jedes Mal aktualisieren, wenn Sie die Konsistenzgruppe erweitern.

Einschränkungen

- SVM-Disaster Recovery unterstützt keine hierarchischen Konsistenzgruppen.
- SVM-Disaster Recovery unterstützt keine Konsistenzgruppen, die mit asynchronem SnapMirror geschützt sind. Sie müssen die SnapMirror Beziehung unterbrechen, bevor Sie die Disaster Recovery für SVMs konfigurieren.
- Auf beiden Clustern muss ONTAP 9.14.1 oder höher ausgeführt werden.
- Fan-out-Beziehungen werden für SVM-Disaster-Recovery-Konfigurationen, die Konsistenzgruppen enthalten, nicht unterstützt.
- Weitere Grenzwerte finden Sie unter Einschränkungen für Konsistenzgruppen.

Beziehungen visualisieren

System Manager visualisiert LUN-Zuordnungen im Menü **Schutz > Beziehungen**. Wenn Sie eine Quellbeziehung auswählen, zeigt System Manager eine Visualisierung der Quellbeziehungen an. Durch Auswahl eines Volumes können Sie sich näher mit diesen Beziehungen befassen, um eine Liste der enthaltenen LUNs und der Beziehungen zu Initiatorgruppen anzuzeigen. Diese Informationen können als Excel-Arbeitsmappe aus der Ansicht der einzelnen Volumes heruntergeladen werden. Der Download-Vorgang

läuft im Hintergrund.

Verwandte Informationen

- "Klonen einer Konsistenzgruppe"
- "Konfigurieren von Snapshots"
- "Erstellen benutzerdefinierter Datensicherungsrichtlinien"
- "Wiederherstellung aus Snapshots"
- "Stellen Sie ein Volume aus einem früheren Snapshot wieder her"
- "Übersicht über SnapMirror Active Sync"
- "Dokumentation zur ONTAP Automatisierung"
- Grundlagen der asynchronen Disaster Recovery von SnapMirror

Ändern Sie Mitgliedsvolumes in einer ONTAP Konsistenzgruppe

Ab ONTAP 9.12.1 können Sie eine Konsistenzgruppe ändern, indem Sie Volumes entfernen oder hinzufügen (erweitern der Konsistenzgruppe). Ab ONTAP 9.13.1 können Sie Volumes zwischen untergeordneten Konsistenzgruppen verschieben, wenn sie ein gemeinsames übergeordnetes Objekt verwenden.

Hinzufügen von Volumes zu einer Konsistenzgruppe

Ab ONTAP 9.12.1 können Sie unterbrechungsfrei Volumes zu einer Konsistenzgruppe hinzufügen.

Über diese Aufgabe

- Sie können keinen Volumes hinzufügen, die einer anderen Konsistenzgruppe zugeordnet sind.
- Konsistenzgruppen unterstützen NAS-, SAN- und NVMe-Protokolle.
- Sie können einer Konsistenzgruppe bis zu 16 Volumes gleichzeitig hinzufügen, wenn die Anpassungen sich innerhalb der gesamten befindenEinschränkungen für Konsistenzgruppen.
- Ab ONTAP 9.13.1 können Sie Volumes unterbrechungsfrei zu einer Konsistenzgruppe mit einer aktiven SnapMirror-Synchronisierung oder einer asynchronen SnapMirror-Sicherungsrichtlinie hinzufügen.
- Wenn Sie Volumes zu einer durch SnapMirror Active Sync geschützten Konsistenzgruppe hinzufügen, ändert sich der Status der SnapMirror Beziehung für die aktive Synchronisierung in „erweitern“, bis Spiegelung und Schutz für das neue Volume konfiguriert sind. Wenn auf dem primären Cluster ein Ausfall auftritt, bevor dieser Prozess abgeschlossen ist, wird die Konsistenzgruppe im Rahmen des Failover-Vorgangs zurück auf ihre ursprüngliche Zusammensetzung zurückgesetzt.
- In ONTAP 9.12.1 und älteren Versionen können Sie Volumes nicht zu einer Konsistenzgruppe in einer aktiven SnapMirror Synchronisierungsbeziehung hinzufügen. Sie müssen zuerst die SnapMirror Active Sync Beziehung löschen, die Konsistenzgruppe ändern und dann den Schutz mit SnapMirror Active Sync wiederherstellen.
- Ab ONTAP 9.12.1 unterstützt die ONTAP-REST-API das Hinzufügen von *New* oder vorhandenen Volumes zu einer Konsistenzgruppe. Weitere Informationen zur ONTAP REST API finden Sie unter "Referenzdokumentation zur ONTAP REST-API".

  Ab ONTAP 9.13.1 wird diese Funktionalität in System Manager unterstützt.

- Beim erweitern einer Konsistenzgruppe gelten die vor der Änderung erfassten Snapshots der Konsistenzgruppe als teilweise. Bei jedem Wiederherstellungsvorgang, der auf diesem Snapshot basiert,

wird die Konsistenzgruppe zum Zeitpunkt des Snapshots wiedergegeben.

- Wenn Sie ONTAP 9.10.1 bis 9.11.1 verwenden, können Sie eine Konsistenzgruppe nicht ändern. Zum Ändern der Konfiguration einer Konsistenzgruppe in ONTAP 9.10.1 oder 9.11.1 müssen Sie die Konsistenzgruppe löschen und dann eine neue Konsistenzgruppe mit den Volumes erstellen, die Sie aufnehmen möchten.
- Ab ONTAP 9.14.1 können Sie Snapshots mit granularem Volume unter Verwendung von SnapMirror asynchron in das Ziel-Cluster replizieren. Bei der Erweiterung einer Consistency Group unter Verwendung von SnapMirror Asynchronous werden Volume-granulare Snapshots erst nach dem erweitern der Consistency Group repliziert, wenn die SnapMirror-Richtlinie MirrorAll oder MirrorAndVault lautet. Es werden nur Snapshots mit Volume-Granularität repliziert, die neuer sind als der Snapshot der BasisKonsistenzgruppe.
- Wenn Sie Volumes zu einer Konsistenzgruppe in einer SVM-Disaster-Recovery-Beziehung hinzufügen (unterstützt ab ONTAP 9.14.1), müssen Sie die SVM-Disaster-Recovery-Beziehung nach der Erweiterung der Konsistenzgruppe vom Zielcluster aus aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Sie eine Replikationsbeziehung manuell .
- Wenn Sie NVMe mit ONTAP 9.17.1 verwenden, können Sie eine Konsistenzgruppe nicht ändern.

Beispiel 2. Schritte

System Manager

Ab ONTAP 9.12.1 können Sie diesen Vorgang mit System Manager ausführen.

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die Konsistenzgruppe aus, die Sie ändern möchten.
3. Wenn Sie eine einzelne Consistency Group ändern, wählen Sie oben im Menü **Volumes** die Option **Mehr** und dann **Expand**, um ein Volume hinzuzufügen.

   Wenn Sie eine untergeordnete Konsistenzgruppe ändern, geben Sie die übergeordnete Konsistenzgruppe an, die Sie ändern möchten. Klicken Sie auf die Schaltfläche **>**, um die untergeordneten Konsistenzgruppen anzuzeigen, und wählen Sie dann neben dem Namen der untergeordneten Konsistenzgruppe aus ⋮, die Sie ändern möchten. Wählen Sie in diesem Menü die Option **erweitern**.
4. Wählen Sie bis zu 16 Volumes aus, die der Konsistenzgruppe hinzugefügt werden sollen.
5. Wählen Sie **Speichern**. Wenn der Vorgang abgeschlossen ist, zeigen Sie die neu hinzugefügten Volumes im Menü **Volumes** der Konsistenzgruppe an.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der ONTAP-CLI Volumes zu einer Konsistenzgruppe hinzufügen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Fügen Sie vorhandene Volumes hinzu

1. Geben Sie den folgenden Befehl ein. Der `-volumes` Parameter akzeptiert eine durch Kommas getrennte Liste von Volumes.

   ⓘ Schließen Sie den `-parent-consistency-group` Parameter nur ein, wenn die Konsistenzgruppe sich in einer hierarchischen Beziehung befindet.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Hinzufügen neuer Volumes

Das Verfahren zum Hinzufügen neuer Volumes hängt von dem verwendeten Protokoll ab.

ⓘ Beziehen Sie nur die `-parent-consistency-group` Parameter, wenn die Konsistenzgruppe in einer hierarchischen Beziehung steht.

- So fügen Sie neue Volumes hinzu, 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
```

- So fügen Sie neue NFS-Volumes hinzu:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- So fügen Sie neue SAN-Volumes hinzu:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- So fügen Sie neue NVMe-Namespaces hinzu:

```
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
```

Entfernen von Volumes aus einer Konsistenzgruppe

Volumes, die aus einer Konsistenzgruppe entfernt wurden, werden nicht gelöscht. Sie bleiben im Cluster aktiv.

Über diese Aufgabe

- Sie können Volumes nicht aus einer Konsistenzgruppe in einer SnapMirror Active Sync- oder SVM-Disaster-Recovery-Beziehung entfernen. Sie müssen zuerst die SnapMirror Active Sync Beziehung löschen, um die Konsistenzgruppe zu ändern, und dann die Beziehung wieder herstellen.
- Wenn eine Konsistenzgruppe nach dem Entfernen keine Volumes enthält, wird die Konsistenzgruppe gelöscht.
- Wenn ein Volume aus einer Konsistenzgruppe entfernt wird, bleiben die vorhandenen Snapshots der Konsistenzgruppe erhalten, gelten jedoch als ungültig. Die vorhandenen Snapshots können nicht verwendet werden, um den Inhalt der Konsistenzgruppe wiederherzustellen. Volume-granulare Snapshots sind weiterhin gültig.
- Wenn Sie ein Volume aus dem Cluster löschen, wird es automatisch aus der Konsistenzgruppe entfernt.
- Zum Ändern der Konfiguration einer Konsistenzgruppe in ONTAP 9.10.1 oder 9.11.1 müssen Sie die Konsistenzgruppe löschen und dann eine neue Konsistenzgruppe mit den gewünschten Mitglied-Volumes erstellen.
- Wenn Sie ein Volume aus dem Cluster löschen, wird es automatisch aus der Konsistenzgruppe entfernt.

System Manager

Ab ONTAP 9.12.1 können Sie diesen Vorgang mit System Manager ausführen.

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die einzelne oder untergeordnete Konsistenzgruppe aus, die Sie ändern möchten.
3. Aktivieren Sie im Menü **Volumes** die Kontrollkästchen neben den einzelnen Volumes, die Sie aus der Konsistenzgruppe entfernen möchten.
4. Wählen Sie **Volumes aus der Consistency Group entfernen** aus.
5. Bestätigen Sie, dass Sie verstehen, dass das Entfernen der Volumes dazu führt, dass alle Snapshots der Konsistenzgruppe ungültig werden, und wählen Sie **Remove**.

CLI

Ab ONTAP 9.14.1 können Sie Volumes mithilfe der CLI aus einer Konsistenzgruppe entfernen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Entfernen Sie die Volumes. Der `-volumes` Parameter akzeptiert eine durch Kommas getrennte Liste von Volumes.

   Schließen Sie den `-parent-consistency-group` Parameter nur ein, wenn die Konsistenzgruppe sich in einer hierarchischen Beziehung befindet.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Verschieben von Volumes zwischen Konsistenzgruppen

Ab ONTAP 9.13.1 können Sie Volumes zwischen untergeordneten Konsistenzgruppen verschieben, die ein übergeordnetes Objekt verwenden.

Über diese Aufgabe

- Sie können Volumes nur zwischen Konsistenzgruppen verschieben, die unter derselben übergeordneten Konsistenzgruppe geschachtelt sind.
- Vorhandene Snapshots von Konsistenzgruppen sind ungültig und können als Snapshots von Konsistenzgruppen nicht mehr aufgerufen werden. Einzelne Volume Snapshots bleiben gültig.
- Snapshots der übergeordneten Konsistenzgruppe bleiben gültig.
- Wenn Sie alle Volumes aus einer untergeordneten Konsistenzgruppe verschieben, wird diese Konsistenzgruppe gelöscht.
- Änderungen an einer Konsistenzgruppe müssen eingehalten werdenEinschränkungen für

Konsistenzgruppen.

System Manager

Ab ONTAP 9.12.1 können Sie diesen Vorgang mit System Manager ausführen.

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die übergeordnete Konsistenzgruppe aus, die die Volumes enthält, die Sie verschieben möchten. Suchen Sie die untergeordnete Consistency Group und erweitern Sie dann das Menü **Volumes**. Wählen Sie die Volumes aus, die Sie verschieben möchten.
3. Wählen Sie **Verschieben**.
4. Legen Sie fest, ob die Volumes in eine neue Konsistenzgruppe oder eine vorhandene Gruppe verschoben werden sollen.
   a. Um zu einer vorhandenen Consistency Group zu wechseln, wählen Sie **vorhandene untergeordnete Consistency Group** und wählen Sie dann den Namen der Consistency Group aus dem Dropdown-Menü aus.
   b. Um zu einer neuen Consistency Group zu wechseln, wählen Sie **Neue untergeordnete Consistency Group** aus. Geben Sie einen Namen für die neue untergeordnete Konsistenzgruppe ein, und wählen Sie einen Komponententyp aus.
5. Wählen Sie **Verschieben**.

CLI

Ab ONTAP 9.14.1 können Sie Volumes mithilfe der ONTAP CLI zwischen Konsistenzgruppen verschieben.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Verschieben Sie Volumes in eine neue untergeordnete Konsistenzgruppe

1. Mit dem folgenden Befehl wird eine neue untergeordnete Konsistenzgruppe erstellt, die die zugewiesenen Volumes enthält.

   Wenn Sie die neue Konsistenzgruppe erstellen, können Sie neue Snapshot-, QoS- und Tiering-Richtlinien zuweisen.

   ```
   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]
   ```

Verschieben Sie Volumes in eine vorhandene untergeordnete Konsistenzgruppe

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

- Einschränkungen für Konsistenzgruppen
- Klonen einer Konsistenzgruppe

Ändern der ONTAP Konsistenzgruppengeometrie

Ab ONTAP 9.13.1 können Sie die Geometrie einer Konsistenzgruppe ändern. Wenn Sie die Geometrie einer Konsistenzgruppe ändern, können Sie die Konfiguration von untergeordneten oder übergeordneten Konsistenzgruppen ändern, ohne dass laufende I/O-Vorgänge unterbrochen werden.

Das Ändern der Konsistenzgruppengeometrie hat Auswirkungen auf vorhandene Snapshots der Konsistenzgruppe. Weitere Informationen finden Sie unter die spezifische Änderung der Geometrie, die Sie durchführen möchten.

> Sie können die Geometrie einer Konsistenzgruppe nicht ändern, die mit einer Remote-Schutzrichtlinie konfiguriert ist. Sie müssen zuerst die Schutzbeziehung unterbrechen, die Geometrie ändern und dann den Remoteschutz wiederherstellen.

Fügen Sie eine neue untergeordnete Konsistenzgruppe hinzu

Ab ONTAP 9.13.1 können Sie einer vorhandenen übergeordneten Konsistenzgruppe eine neue untergeordnete Konsistenzgruppe hinzufügen.

Über diese Aufgabe

- Eine übergeordnete Konsistenzgruppe kann maximal fünf untergeordnete Konsistenzgruppen enthalten. Einschränkungen für KonsistenzgruppenWeitere Grenzwerte finden Sie unter.
- Sie können einer einzelnen Konsistenzgruppe keine untergeordnete Konsistenzgruppe hinzufügen. Sie müssen zuerst [Werben] die Konsistenzgruppe erstellen, dann können Sie eine untergeordnete Konsistenzgruppe hinzufügen.
- Vorhandene Snapshots der vor dem Expand-Vorgang erfassten Konsistenzgruppe gelten als teilweise Snapshots. Bei jedem Wiederherstellungsvorgang, der auf diesem Snapshot basiert, wird die Konsistenzgruppe zum Zeitpunkt des Snapshots wiedergegeben.

Beispiel 3. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

Fügen Sie eine neue untergeordnete Konsistenzgruppe hinzu

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die übergeordnete Konsistenzgruppe aus, der Sie eine untergeordnete Konsistenzgruppe hinzufügen möchten.
3. Wählen Sie neben dem Namen der übergeordneten Consistency Group die Option **Mehr** und dann **Neue untergeordnete Consistency Group hinzufügen**.
4. Geben Sie einen Namen für Ihre Konsistenzgruppe ein.
5. Legen Sie fest, ob Sie neue oder vorhandene Volumes hinzufügen möchten.
   a. Wenn Sie vorhandene Volumes hinzufügen, wählen Sie **existierende Volumes** und wählen Sie dann die Volumes aus dem Dropdown-Menü aus.
   b. Wenn Sie neue Volumes hinzufügen, wählen Sie **Neue Volumes** und geben Sie dann die Anzahl der Volumes und deren Größe an.
6. Wählen Sie **Hinzufügen**.

CLI

Ab ONTAP 9.14.1 können Sie eine untergeordnete Konsistenzgruppe über die ONTAP CLI hinzufügen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Fügen Sie eine untergeordnete Konsistenzgruppe mit neuen Volumes hinzu

1. Erstellen Sie die neue Konsistenzgruppe. Geben Sie Werte für den Konsistenzgruppennamen, das Volume-Präfix, die Anzahl der Volumes, die Volume-Größe, den Storage-Service, und den Namen der Exportrichtlinie:

   ```
   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
   ```

Fügen Sie eine untergeordnete Konsistenzgruppe mit vorhandenen Volumes hinzu

1. Erstellen Sie die neue Konsistenzgruppe. 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
   ```

Trennen Sie eine untergeordnete Konsistenzgruppe

Ab ONTAP 9.13.1 können Sie eine untergeordnete Konsistenzgruppe aus ihrem übergeordneten Element entfernen und in eine individuelle Konsistenzgruppe konvertieren.

Über diese Aufgabe

- Das Trennen einer untergeordneten Konsistenzgruppe führt dazu, dass die Snapshots der übergeordneten Konsistenzgruppe ungültig werden und nicht mehr zugänglich sind. Granulare Volume-Snapshots sind weiterhin gültig.
- Vorhandene Snapshots der einzelnen Konsistenzgruppe bleiben gültig.
- Dieser Vorgang schlägt fehl, wenn eine vorhandene einzelne Konsistenzgruppe den gleichen Namen wie die untergeordnete Konsistenzgruppe hat, die Sie trennen möchten. Wenn in diesem Szenario Sie auftreten, müssen Sie die Konsistenzgruppe umbenennen, wenn Sie sie trennen.

Beispiel 4. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

Trennen Sie eine untergeordnete Konsistenzgruppe

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die übergeordnete Konsistenzgruppe aus, die das untergeordnete Element enthält, das Sie entfernen möchten.
3. Wählen Sie neben der untergeordneten Consistency Group, die Sie entfernen möchten, die Option **Mehr** und dann **vom übergeordneten Element trennen**.
4. Optional können Sie die Konsistenzgruppe umbenennen und einen Applikationstyp auswählen.
5. Wählen Sie **Trennen**.

CLI

Ab ONTAP 9.14.1 können Sie eine untergeordnete Konsistenzgruppe über die ONTAP CLI trennen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Trennen Sie eine untergeordnete Konsistenzgruppe

1. Entfernen Sie die Konsistenzgruppe. Benennen Sie optional die getrennte Konsistenzgruppe mit dem `-new-name` Parameter um.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Verschieben Sie eine vorhandene einzelne Konsistenzgruppe unter eine übergeordnete Konsistenzgruppe

Ab ONTAP 9.13.1 können Sie eine vorhandene einzelne Konsistenzgruppe in eine untergeordnete Konsistenzgruppe konvertieren. Sie können die Konsistenzgruppe entweder unter eine vorhandene übergeordnete Konsistenzgruppe verschieben oder während des Verschiebens eine neue übergeordnete Konsistenzgruppe erstellen.

Über diese Aufgabe

- Die übergeordnete Konsistenzgruppe muss vier oder weniger untergeordnete Elemente aufweisen. Eine übergeordnete Konsistenzgruppe kann maximal fünf untergeordnete Konsistenzgruppen enthalten. Einschränkungen für KonsistenzgruppenWeitere Grenzwerte finden Sie unter.
- Vorhandene Snapshots der vor diesem Vorgang erfassten *parent* Konsistenzgruppe gelten als teilweise Snapshots. Bei jedem Wiederherstellungsvorgang, der auf einem dieser Snapshots basiert, wird die Konsistenzgruppe zum Zeitpunkt des Snapshots wiedergegeben.
- Vorhandene Snapshots der Konsistenzgruppe bleiben gültig.

Beispiel 5. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

Verschieben Sie eine vorhandene einzelne Konsistenzgruppe unter eine übergeordnete Konsistenzgruppe

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die Konsistenzgruppe aus, die Sie konvertieren möchten.
3. Wählen Sie **Mehr** und dann **unter verschiedene Consistency Group verschieben**.
4. Geben Sie optional einen neuen Namen für die Konsistenzgruppe ein, und wählen Sie einen Komponententyp aus. Standardmäßig ist der Komponententyp „Sonstige“.
5. Wählen Sie diese Option, wenn Sie zu einer vorhandenen übergeordneten Konsistenzgruppe migrieren oder eine neue übergeordnete Konsistenzgruppe erstellen möchten:
   a. Um in eine vorhandene übergeordnete Konsistenzgruppe zu migrieren, wählen Sie **vorhandene Konsistenzgruppe** aus, und wählen Sie dann die Konsistenzgruppe aus dem Dropdown-Menü aus.
   b. Um eine neue übergeordnete Konsistenzgruppe zu erstellen, wählen Sie **Neue Konsistenzgruppe** und geben Sie dann einen Namen für die neue Konsistenzgruppe ein.
6. Wählen Sie **Verschieben**.

CLI

Ab ONTAP 9.14.1 können Sie eine einzelne Konsistenzgruppe mithilfe der ONTAP CLI unter eine übergeordnete Konsistenzgruppe verschieben.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Verschieben Sie eine Konsistenzgruppe unter eine neue übergeordnete Konsistenzgruppe

1. Erstellen Sie die neue übergeordnete Konsistenzgruppe. Mit dem `-consistency-groups` Parameter werden alle vorhandenen Konsistenzgruppen auf das neue übergeordnete Objekt migriert.

   ```
   consistency-group attach -vserver svm_name -consistency-group
   parent_consistency_group -consistency-groups child_consistency_group
   ```

Verschieben Sie eine Konsistenzgruppe unter einer vorhandenen Konsistenzgruppe

1. Verschieben der Konsistenzgruppe:

   ```
   consistency-group add -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   ```

Hochstufen einer untergeordneten Konsistenzgruppe

Ab ONTAP 9.13.1 können Sie eine einzelne Konsistenzgruppe in eine übergeordnete Konsistenzgruppe

heraufstufen. Wenn Sie die einzelne Konsistenzgruppe zu einem übergeordneten Element heraufstufen, erstellen Sie außerdem eine neue untergeordnete Konsistenzgruppe, die alle Volumes der ursprünglichen, einzelnen Konsistenzgruppe übernimmt.

Über diese Aufgabe

- Wenn Sie eine untergeordnete Konsistenzgruppe in eine übergeordnete Konsistenzgruppe konvertieren möchten, müssen Sie zuerst [detach] die untergeordnete Konsistenzgruppe ausführen und dann das folgende Verfahren ausführen.
- Vorhandene Snapshots der Konsistenzgruppe bleiben nach dem Hochstufen der Konsistenzgruppe gültig.

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

Hochstufen einer untergeordneten Konsistenzgruppe

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die Konsistenzgruppe aus, die Sie hochstufen möchten.
3. Wählen Sie **Mehr** und dann **auf übergeordnete Consistency Group hochstufen**.
4. Geben Sie einen **Namen** ein und wählen Sie einen **Komponententyp** für die untergeordnete Consistency Group aus.
5. Wählen Sie **Heraufstufen**.

CLI

Ab ONTAP 9.14.1 können Sie eine einzelne Konsistenzgruppe mithilfe der ONTAP CLI unter eine übergeordnete Konsistenzgruppe verschieben.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Hochstufen einer untergeordneten Konsistenzgruppe

1. Hochstufen der Konsistenzgruppe. Mit diesem Befehl wird eine übergeordnete und eine untergeordnete Konsistenzgruppe erstellt.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

Stufen Sie ein übergeordnetes Objekt auf eine einzelne Konsistenzgruppe zurück

Ab ONTAP 9.13.1 können Sie eine übergeordnete Konsistenzgruppe auf eine einzige Konsistenzgruppe herunterstufen. Durch Zurückstufen des übergeordneten Elements wird die Hierarchie der Konsistenzgruppe reduziert, wobei alle zugeordneten untergeordneten Konsistenzgruppen entfernt werden. Alle Volumes in der Konsistenzgruppe verbleiben in der neuen, einzelnen Konsistenzgruppe.

Über diese Aufgabe

- Vorhandene Snapshots der *parent* Konsistenzgruppe bleiben nach dem Herabstufen auf eine einzelne Konsistenz weiterhin gültig. Vorhandene Snapshots einer der zugeordneten *child* Consistency Groups

dieses übergeordneten Objekts werden bei der Herabstufung ungültig. Der Zugriff auf die einzelnen Volume Snapshots innerhalb der Child-Konsistenzgruppe ist weiterhin als Snapshots mit Volume-Granularität möglich.

Beispiel 6. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

Stufen Sie eine Konsistenzgruppe zurück

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die übergeordnete Konsistenzgruppe aus, die Sie herunterstufen möchten.
3. Wählen Sie **Mehr** und dann **auf einzelne Consistency Group zurückstufen**.
4. Eine Warnung weist Sie darauf hin, dass alle zugeordneten untergeordneten Konsistenzgruppen gelöscht werden und ihre Volumes unter die neue einzelne Konsistenzgruppe verschoben werden. Wählen Sie **Zurückstufen**, um zu bestätigen, dass Sie die Auswirkungen verstehen.

CLI

Ab ONTAP 9.14.1 können Sie eine Konsistenzgruppe mithilfe der ONTAP CLI zurückstufen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Stufen Sie eine Konsistenzgruppe zurück

1. Stufen Sie die Konsistenzgruppe zurück. Verwenden Sie den optionalen `-new-name` Parameter, um die Konsistenzgruppe umzubenennen.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Ändern Sie die Anwendungs- und Komponenten-Tags der ONTAP Konsistenzgruppe

Ab ONTAP 9.12.1 unterstützen Konsistenzgruppen das Komponenten- und Applikations-Tagging. Applikations- und Komponenten-Tags sind ein Managementtool, mit dem Sie verschiedene Workloads in Ihren Konsistenzgruppen filtern und identifizieren können.

Über diese Aufgabe

Konsistenzgruppen bieten zwei Arten von Tags:

- **Anwendungs-Tags**: Diese gelten für einzelne und übergeordnete Konsistenzgruppen. Applikations-Tags bieten Kennzeichnung für Workloads wie MongoDB, Oracle oder SQL Server. Das Standard-Anwendungs-Tag für Konsistenzgruppen ist „Sonstige“.
- **Komponenten-Tags**: Kinder in hierarchischen Konsistenzgruppen haben Komponenten-Tags anstelle von Anwendungs-Tags. Die Optionen für Komponenten-Tags sind „Daten“, „Protokolle“ oder „andere“. Der

Standardwert ist „Other“.

Sie können Tags beim Erstellen von Konsistenzgruppen oder nach dem Erstellen der Konsistenzgruppen anwenden.

Wenn die Konsistenzgruppe über eine aktive SnapMirror-Synchronisierungsbeziehung verfügt, müssen Sie **andere** als Anwendungs- oder Komponenten-Tag verwenden.

Schritte

Ab ONTAP 9.12.1 können Sie Applikations- und Komponenten-Tags mit System Manager ändern. Ab ONTAP 9.14.1 können Sie die Anwendungs- und Komponenten-Tags über die ONTAP-CLI ändern.

System Manager

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie die Konsistenzgruppe aus, deren Tag Sie ändern möchten. Wählen Sie neben dem Namen der Konsistenzgruppe und dann **Edit** aus .
3. Wählen Sie im Dropdown-Menü die entsprechende Anwendungs- oder Komponentenkennung aus.
4. Wählen Sie **Speichern**.

CLI

Ab ONTAP 9.14.1 können Sie die Applikations- oder Komponenten-Tag einer vorhandenen Konsistenzgruppe mithilfe der ONTAP CLI ändern.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Ändern Sie das Anwendungs-Tag

1. Anwendungs-Tags akzeptieren eine begrenzte Anzahl voreingestellter Zeichenfolgen. Führen Sie den folgenden Befehl aus, um die Liste der akzeptierten Zeichenfolgen anzuzeigen:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Wählen Sie den entsprechenden String in der Ausgabe aus und ändern Sie die Konsistenzgruppe:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Ändern Sie das Komponenten-Tag

1. Ändern Sie den Komponententyp. Der Komponententyp kann Daten, Protokolle oder andere sein. Wenn Sie SnapMirror Active Sync verwenden, muss es „andere“ 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 können Sie eine Konsistenzgruppe klonen, um eine Kopie einer Konsistenzgruppe und ihres Inhalts zu erstellen. Durch das Klonen einer Konsistenzgruppe wird eine Kopie der Konfiguration der Konsistenzgruppe, ihrer Metadaten wie Applikationstyp und aller Volumes und ihrer Inhalte wie Dateien, Verzeichnisse, LUNs oder NVMe Namespaces erstellt.

Über diese Aufgabe

Beim Klonen einer Konsistenzgruppe können Sie sie mit der aktuellen Konfiguration klonen, jedoch mit dem vorhandenen Volume-Inhalt oder auf Grundlage eines vorhandenen KonsistenzgruppenSnapshot.

Das Klonen einer Konsistenzgruppe wird nur für die gesamte Konsistenzgruppe unterstützt. Sie können eine einzelne Child-Konsistenzgruppe nicht in einer hierarchischen Beziehung klonen: Nur die vollständige Konfiguration der Konsistenzgruppe kann geklont werden.

Wenn Sie eine Konsistenzgruppe klonen, sind die folgenden Komponenten nicht geklont:

- IGroups
- LUN-Zuordnungen
- NVMe-Subsysteme
- NVMe Namespace-Subsystemzuordnungen

Bevor Sie beginnen

- Wenn Sie eine Konsistenzgruppe klonen, erstellt ONTAP keine SMB-Freigaben für die geklonten Volumes, falls kein Freigabename angegeben wird. * Geklonte Consistency Groups werden nicht gemountet, wenn kein Verbindungspfad angegeben ist.
- Wenn Sie versuchen, eine Konsistenzgruppe auf der Grundlage eines Snapshots zu klonen, der die aktuellen konstituierenden Volumes der Konsistenzgruppe nicht widerspiegelt, schlägt der Vorgang fehl.
- Nachdem Sie eine Konsistenzgruppe geklont haben, müssen Sie die entsprechende Zuordnung durchführen.

  Zuordnen von Initiatorgruppen zu mehreren LUNsZuordnen eines NVMe Namespace zu einem SubsystemWeitere Informationen finden Sie unter oder.

- Das Klonen einer Konsistenzgruppe wird für eine Konsistenzgruppe in einer aktiven synchronen SnapMirror Beziehung oder zu zugehörigen DP Volumes nicht unterstützt.

System Manager

Schritte

1. Wählen Sie **Storage > Consistency Groups** aus.
2. Wählen Sie im Menü **Consistency Group** die Konsistenzgruppe aus, die Sie klonen möchten.
3. Wählen Sie oben rechts auf der Übersichtsseite für die Konsistenzgruppe **Klonen** aus.
4. Geben Sie einen Namen für die neue, geklonte Konsistenzgruppe ein, oder übernehmen Sie den Standardnamen.
   a. Wählen Sie, ob Sie aktivieren möchten**"Thin Provisioning"**.
   b. Wählen Sie **Split Clone**, wenn Sie die Konsistenzgruppe von ihrer Quelle trennen und zusätzlichen Speicherplatz für die geklonte Konsistenzgruppe zuweisen möchten.
5. Um die Konsistenzgruppe in ihrem aktuellen Zustand zu klonen, wählen Sie **Neuen Snapshot hinzufügen**.

   Um die Consistency Group auf der Grundlage eines Snapshots zu klonen, wählen Sie **vorhandenen Snapshot verwenden**. Wenn Sie diese Option auswählen, wird ein neues Untermenü geöffnet. Wählen Sie den Snapshot aus, den Sie als Basis für den Klonvorgang verwenden möchten.
6. Wählen Sie **Clone**.
7. Kehren Sie zum Menü **Consistency Group** zurück, um zu bestätigen, dass Ihre Konsistenzgruppe geklont wurde.

CLI

Ab ONTAP 9.14.1 können Sie eine Konsistenzgruppe mithilfe der CLI mit den Anmeldedaten für den Cluster-Administrator klonen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Klonen einer Konsistenzgruppe

1. Mit dem `consistency-group clone create` Befehl wird die Konsistenzgruppe im aktuellen Point-in-Time-Status klonen. Um den Klonvorgang auf einem Snapshot zu basieren, schließen Sie den `-source-snapshot` Parameter ein.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

   Erfahren Sie mehr über `consistency-group clone create` in der "ONTAP-Befehlsreferenz".

Nächste Schritte

- Zuordnen von Initiatorgruppen zu mehreren LUNs
- Zuordnen eines NVMe Namespace zu einem Subsystem

Löschen einer ONTAP Konsistenzgruppe

Wenn Sie beschließen, dass Sie keine Konsistenzgruppe mehr benötigen, können Sie sie löschen.

Über diese Aufgabe

- Durch das Löschen einer Konsistenzgruppe wird die Instanz der Konsistenzgruppe gelöscht und hat Auswirkungen auf die konstituierenden Volumes oder LUNs. Das Löschen einer Konsistenzgruppe führt nicht zum Löschen der auf jedem Volume vorhandenen Snapshots, aber sie sind als Snapshots der Konsistenzgruppe nicht mehr zugänglich. Die Snapshots können jedoch weiterhin als normale granulare Volume-Snapshots gemanagt werden.
- ONTAP löscht automatisch eine Konsistenzgruppe, wenn alle Volumes in der Konsistenzgruppe gelöscht werden.
- Durch das Löschen einer übergeordneten Konsistenzgruppe werden alle zugeordneten untergeordneten Konsistenzgruppen gelöscht.
- Wenn Sie eine ONTAP-Version zwischen 9.10.1 und 9.12.0 verwenden, können Volumes nur 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 können Sie Volumes aus einer Konsistenzgruppe entfernen, ohne die Konsistenzgruppe zu löschen. Weitere Informationen zu diesem Vorgang finden Sie unter Ändern einer Konsistenzgruppe.

Beispiel 7. Schritte

System Manager

1. Wählen Sie **Storage > Consistency Groups** aus.
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 können Sie eine Konsistenzgruppe über die CLI löschen.

Bevor Sie beginnen

- Sie müssen sich auf der Administratorberechtigungsebene befinden, um diese Aufgabe ausführen zu können.
- Ab ONTAP 9.15.1 kann jeder Benutzer mit Administratorrechten diese Aufgabe ausführen. In ONTAP 9.14.1 müssen Sie Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Löschen einer Konsistenzgruppe

1. Löschen Sie die Konsistenzgruppe:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror Active Sync

Einführung

Erfahren Sie mehr über ONTAP SnapMirror Active Sync

SnapMirror Active Sync, auch bekannt als SnapMirror Business Continuity (SM-BC), ermöglicht die Weiterfunktion von Geschäftsdiensten im Falle eines vollständigen Site-Ausfalls. Diese Technologie ermöglicht ein nahtloses Failover von Anwendungen auf eine sekundäre Kopie ohne manuelle Eingriffe oder benutzerdefinierte Skripts.

NetApp SnapMirror Active Sync (SM-as) ist als granularerer, kostengünstigerer und benutzerfreundlicherer Schutz auf Anwendungsebene mit automatischem Failover konzipiert. SnapMirror Active Sync ermöglicht die Aufrechterhaltung des Betriebs unternehmenskritischer Dienste, selbst bei einem vollständigen Site-Ausfall. Mit SnapMirror Active Sync können Sie jetzt mehrere Volumes einer Anwendung synchron zwischen Sites an geografisch verteilten Standorten replizieren (indem Sie sie einer Konsistenzgruppe hinzufügen). Sie können im Falle einer Störung der primären Kopie automatisch ein Failover auf die sekundäre Kopie durchführen und so die Geschäftskontinuität für Tier-1-Anwendungen gewährleisten.

In einigen Ländern schreiben die Vorschriften für Finanzinstitute vor, dass Unternehmen regelmäßig von ihren sekundären Rechenzentren aus bedient werden können. SnapMirror Active Sync ermöglicht mit seinen Hochverfügbarkeitsclustern diese Rechenzentrumsumschaltungen zur Gewährleistung der Geschäftskontinuität.

SnapMirror Active Sync ist ab ONTAP 9.9.1 verfügbar und wird auf AFF und All-Flash SAN Array (ASA)-Clustern unterstützt. Der primäre und der sekundäre Cluster müssen vom gleichen Typ sein: entweder ASA, ASA r2 oder AFF. SnapMirror Active Sync schützt Anwendungen mit iSCSI- oder FCP-LUNs oder NVMe-Namespaces.

SnapMirror Active Sync unterstützt sowohl symmetrische als auch asymmetrische Konfigurationen. Die Unterstützung für symmetrisches Aktiv/Aktiv wurde in ONTAP 9.15.1 eingeführt. Durch die symmetrische Aktiv/Aktiv-Konfiguration können beide Kopien einer geschützten LUN Lese- und Schreib-E/A-Vorgänge mit bidirektionaler synchroner Replikation durchführen, sodass jede LUN-Kopie lokale E/A-Anforderungen erfüllen kann.

Ab Juli 2024 wurden die Inhalte aus zuvor als PDFs veröffentlichten technischen Berichten in die ONTAP Produktdokumentation integriert. Die Dokumentation zur aktiven Synchronisierung von ONTAP SnapMirror enthält nun Inhalte aus *TR-4878: SnapMirror Active Sync*.

Vorteile

SnapMirror Active Sync bietet folgende Vorteile:

- Kontinuierliche Verfügbarkeit für geschäftskritische Applikationen:
- Fähigkeit, kritische Applikationen abwechselnd von primären und sekundären Standorten zu hosten
- Vereinfachtes Applikationsmanagement durch Consistency Groups für eine abhängige Konsistenz der Schreibreihenfolge
- Die Fähigkeit, ein Failover für jede Anwendung zu testen.
- Sofortige Erstellung von gespiegelten Klonen ohne Beeinträchtigung der Applikationsverfügbarkeit
- Bereitstellung geschützter und nicht geschützter Workloads im selben ONTAP-Cluster.
- LUN, NVMe-Namespace, NVMe-Subsystem oder Speichereinheitenidentität bleiben gleich, sodass die Anwendung sie als gemeinsam genutztes virtuelles Gerät betrachtet.

- Sekundäre Cluster können mit der Flexibilität wiederverwendet werden, um sofort Klone für die Anwendungsnutzung für Entwicklungs- und Testzwecke sowie für UAT- oder Reporting-Zwecke zu erstellen, ohne die Applikations-Performance oder -Verfügbarkeit zu beeinträchtigen.

SnapMirror Active Sync ermöglicht Ihnen den Schutz Ihrer Daten-LUNs oder NVMe-Namespaces. Dadurch wird ein transparentes Failover von Anwendungen zur Gewährleistung der Geschäftskontinuität im Notfall ermöglicht. Weitere Informationen finden Sie unter "Anwendungsfälle" .

Schlüsselkonzepte

SnapMirror Active Sync verwendet Konsistenzgruppen, um sicherzustellen, dass Ihre Daten repliziert werden. SnapMirror Active Sync verwendet den ONTAP Mediator oder, ab ONTAP 9.17.1, den Cloud Mediator für automatisiertes Failover und stellt so sicher, dass die Daten im Katastrophenfall bereitgestellt werden. Bei der Planung Ihrer SnapMirror Active Sync-Bereitstellung ist es wichtig, die wesentlichen Konzepte und die Architektur von SnapMirror Active Sync zu verstehen.

Asymmetrie und Symmetrie

In symmetrischen Aktiv/Aktiv-Konfigurationen können beide Standorte für aktive E/A auf den lokalen Speicher zugreifen. Symmetrisches Aktiv/Aktiv ist für Clusteranwendungen wie VMware vMSC, Windows Failover Cluster mit SQL und Oracle RAC optimiert.

In asymmetrischen Aktiv/Aktiv-Konfigurationen werden Daten auf der sekundären Site an eine LUN, einen Namespace oder eine Speichereinheit weitergeleitet.

Weitere Informationen finden Sie unter Architektur der aktiven Synchronisierung von SnapMirror.

Konsistenzgruppe

Für AFF und ASA -Systeme ist ein "Konsistenzgruppe" ist eine Sammlung von FlexVol -Volumes, die eine Konsistenzgarantie für die Anwendungs-Workload bieten, die zur Gewährleistung der Geschäftskontinuität geschützt werden muss. In ASA R2-Systemen ist eine Konsistenzgruppe eine Sammlung von Speichereinheiten.

Der Zweck einer Konsistenzgruppe besteht darin, gleichzeitig Snapshots von Volumes oder Speichereinheiten zu erstellen und so absturzkonsistente Kopien der Sammlung zu einem bestimmten Zeitpunkt sicherzustellen. Eine Konsistenzgruppe stellt sicher, dass alle Volumes eines Datensatzes stillgelegt und zum exakt gleichen Zeitpunkt erneut gesichert werden. Dies ermöglicht einen datenkonsistenten Wiederherstellungspunkt für alle Volumes oder Speichereinheiten, die den Datensatz unterstützen. Eine Konsistenzgruppe gewährleistet dadurch die abhängige Konsistenz der Schreibreihenfolge. Wenn Sie Anwendungen zur Geschäftskontinuität schützen möchten, muss die Gruppe der dieser Anwendung zugehörigen Volumes oder Speichereinheiten einer Konsistenzgruppe hinzugefügt werden, um eine Datenschutzbeziehung zwischen einer Quell- und einer Zielkonsistenzgruppe herzustellen. Die Quell- und Zielkonsistenzgruppe müssen dieselbe Anzahl und denselben Typ von Volumes enthalten.

Konstitutive

Ein einzelnes Volume, LUN oder NVMe-Namespace (ab ONTAP 9.17.1), das Teil der Konsistenzgruppe ist, die in der SnapMirror Active Sync-Beziehung geschützt ist.

ONTAP Mediator

Der "ONTAP Mediator" empfängt Zustandsinformationen zu verbundenen ONTAP Clustern und -Knoten, koordiniert die Zusammenarbeit und ermittelt, ob jeder Knoten/Cluster fehlerfrei und betriebsbereit ist. ONTAP Mediator liefert Zustandsinformationen zu:

- Peer ONTAP Cluster

- Peer ONTAP Cluster Nodes
- Konsistenzgruppen (zur Definition der Failover-Einheiten in einer SnapMirror Active Sync Beziehung), für jede Konsistenzgruppe sind die folgenden Informationen angegeben:
  - Replikationsstatus: Nicht initialisiert, synchron oder nicht synchronisiert
  - Welcher Cluster hostet die primäre Kopie
  - Operationskontext (wird für geplanten Failover verwendet)

Mit diesen ONTAP Mediator-Integritätsinformationen können Cluster zwischen verschiedenen Arten von Ausfällen unterscheiden und bestimmen, ob ein automatisiertes Failover durchgeführt werden soll. ONTAP Mediator ist eine der drei Parteien des SnapMirror Active Sync Quorums zusammen mit beiden ONTAP Clustern (primär und sekundär). Um einen Konsens zu erreichen, müssen mindestens zwei Parteien im Quorum einer bestimmten Operation zustimmen.

Ab ONTAP 9.15.1 zeigt System Manager den Status der aktiven SnapMirror Synchronisierungsbeziehung von einem der beiden Cluster an. Sie können den Status des ONTAP Mediators auch von einem der Cluster aus im System Manager überwachen. In früheren Versionen von ONTAP zeigt System Manager den Status der aktiven SnapMirror Synchronisierungsbeziehungen vom Quell-Cluster an.

ONTAP Cloud Mediator

ONTAP Cloud Mediator ist ab ONTAP 9.17.1 verfügbar. ONTAP Cloud Mediator bietet dieselben Dienste wie ONTAP Mediator, außer dass es mithilfe der NetApp Konsole in der Cloud gehostet wird.

Geplantes Failover

Ein manueller Vorgang zum Ändern der Rollen von Kopien in einer aktiven SnapMirror Synchronisierungsbeziehung. Die primären Standorte werden zum sekundären Standort und der sekundäre zum primären Standort.

Automatisches ungeplantes Failover (AUFO)

Ein automatischer Vorgang zum Durchführen eines Failovers der Spiegelkopie. Der Vorgang erfordert Unterstützung durch den ONTAP Mediator, um festzustellen, dass die primäre Kopie nicht verfügbar ist.

Primary-First und Primary Bias

Die aktive Synchronisierung von SnapMirror nutzt ein Prinzip der primären Priorität, das der primären Kopie vorgibt, um I/O-Anfragen bei einer Netzwerkpartition zu bedienen.

Primär-Bias ist eine spezielle Quorum-Implementierung, die die Verfügbarkeit eines durch SnapMirror aktiv synchron geschützten Datensatzes verbessert. Wenn die primäre Kopie verfügbar ist, tritt Primary-Bias in Kraft, wenn der ONTAP Mediator nicht von beiden Clustern aus erreichbar ist.

Primary-First- und Primary-Bias werden ab ONTAP 9.15.1 in SnapMirror Active Sync unterstützt. Primäre Kopien werden in System Manager festgelegt und mit der REST-API und CLI ausgegeben.

Out-of-Sync (OOS)

Wenn die Anwendungs-I/O nicht auf das sekundäre Speichersystem repliziert wird, wird es als **nicht synchron** gemeldet. Ein Status „nicht synchron“ bedeutet, dass die sekundären Volumes nicht mit dem primären Volume (Quelle) synchronisiert werden und dass die SnapMirror Replizierung nicht stattfindet.

Wenn der Spiegelzustand `Snapmirrored` , dies zeigt an, dass eine SnapMirror -Beziehung hergestellt wurde und die Datenübertragung abgeschlossen ist, was bedeutet, dass das Zielvolume mit dem Quellvolume auf dem neuesten Stand ist.

Die aktive Synchronisierung von SnapMirror unterstützt die automatische Neusynchronisierung, sodass Kopien in den InSync Status zurückkehren können.

Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync "Automatische Neukonfiguration in Fan-out-Konfigurationen".

Einheitliche und uneinheitliche Konfiguration

- **Uniform Host Access** bedeutet, dass Hosts von beiden Standorten mit allen Pfaden zu Storage Clustern auf beiden Standorten verbunden sind. Standortübergreifende Pfade sind über Entfernungen verteilt.
- **Uneinheitlicher Hostzugriff** bedeutet, dass Hosts an jedem Standort nur mit dem Cluster am selben Standort verbunden sind. Standortübergreifende Pfade und gestreckte Pfade sind nicht miteinander verbunden.

Jeder SnapMirror Active Sync Bereitstellung wird ein einheitlicher Host-Zugriff unterstützt. Ein nicht einheitlicher Host-Zugriff wird nur für symmetrische aktiv/aktiv-Implementierungen unterstützt.

Kein RPO

RPO steht für das Recovery Point Objective. Dies ist die Menge an Datenverlusten, die in einem bestimmten Zeitraum als akzeptabel erachtet werden. Ein RPO von null bedeutet, dass kein Datenverlust akzeptabel ist.

Kein RTO

RTO steht für die Recovery Time Objective. Diese Zeitdauer wird für eine Applikation nach einem Ausfall, Ausfall oder anderen Datenverlusten für die unterbrechungsfreie Wiederherstellung des normalen Betriebs erachtet. Kein RTO bedeutet, dass keine Ausfallzeiten akzeptabel sind.

SnapMirror Active Sync-Konfigurationsunterstützung durch ONTAP -Version

Die Unterstützung für SnapMirror Active Sync variiert je nach Ihrer ONTAP-Version:

ONTAP-Version	Unterstützte Cluster	Unterstützte Protokolle	Unterstützte Konfigurationen

9.17.1 und höher	• AFF • ASA • C-Serie • ASA r2	• ISCSI • FC • NVMe für VMware-Workloads	• Asymmetrisch aktiv/aktiv Asymmetrisches Aktiv/Aktiv unterstützt ASA r2 und NVMe nicht. Weitere Informationen zur NVMe-Unterstützung finden Sie unter "Konfiguration, Support und Einschränkungen von NVMe" . • Symmetrische aktiv/aktiv-Lösung
9.16.1 und höher	• AFF • ASA • C-Serie • ASA r2	• ISCSI • FC	• Asymmetrisch aktiv/aktiv • Symmetrische Aktiv/Aktiv-Konfigurationen unterstützen 4-Knoten-Cluster in ONTAP 9.16.1 und höher. Für ASA r2 werden nur 2-Knoten-Cluster unterstützt.
9.15.1 und höher	• AFF • ASA • C-Serie	• ISCSI • FC	• Asymmetrisch aktiv/aktiv • Symmetrische Aktiv/Aktiv-Konfigurationen unterstützen 2-Knoten-Cluster in ONTAP 9.15.1. 4-Knoten-Cluster werden in ONTAP 9.16.1 und höher unterstützt.

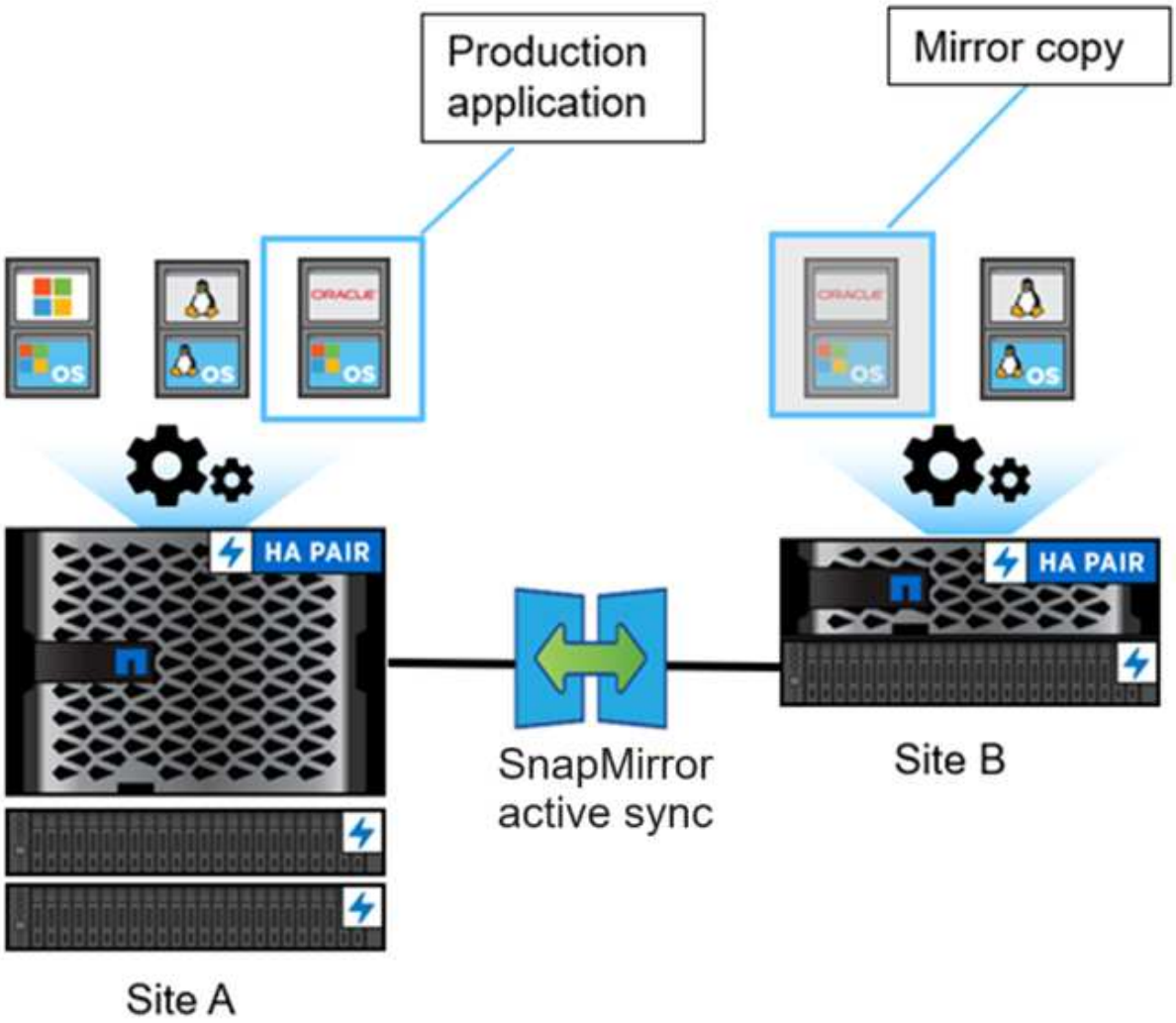
9.9.1 und höher	• AFF • ASA • C-Serie	• ISCSI • FC	Asymmetrisch aktiv/aktiv

Primäre und sekundäre Cluster müssen vom gleichen Typ sein: entweder "ASA" , "ASA r2" oder AFF.

ONTAP SnapMirror Active-Sync-Architektur

Die SnapMirror Active Sync-Architektur ermöglicht aktive Workloads auf beiden Clustern, wobei primäre Workloads gleichzeitig von beiden Clustern aus bedient werden können. In einigen Ländern schreiben die Vorschriften für Finanzinstitute vor, dass Unternehmen auch von ihren sekundären Rechenzentren aus regelmäßig gewartet werden können. Diese sogenannten „Tick-Tock“-Bereitstellungen werden durch die aktive Synchronisierung von SnapMirror ermöglicht.

Die Datensicherungsbeziehung zum Schutz der Geschäftskontinuität wird zwischen dem Quell- und dem Zielspeichersystem 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-Vorgänge synchron in die gespiegelte Konsistenzgruppe repliziert.



Obwohl in der Datensicherungsbeziehung zwei separate Datenkopien vorhanden sind, betrachtet der Anwendungshost diese als gemeinsam genutztes virtuelles Gerät mit mehreren Pfaden, da SnapMirror Active Sync dieselbe LUN- oder NVMe-Namespace-Identität beibehält. Es wird jedoch immer nur auf eine LUN- oder NVMe-Namespace-Kopie geschrieben. Wenn ein Fehler das primäre Speichersystem offline schaltet, erkennt ONTAP dies und nutzt den Mediator zur erneuten Bestätigung. Können weder ONTAP noch der Mediator den primären Standort anpingen, führt ONTAP den automatischen Failover-Vorgang durch. Dieser Prozess führt dazu, dass nur eine bestimmte Anwendung fehlschlägt, ohne dass manuelle Eingriffe oder Skripts erforderlich sind, die zuvor für das Failover erforderlich waren.

Weitere wichtige Punkte:

- Nicht gespiegelte Volumes werden unterstützt, die außerhalb des Sicherungsbereichs für Business Continuity liegen.
- Es wird nur eine andere asynchrone Beziehung von SnapMirror für Volumes unterstützt, die zur Gewährleistung der Business Continuity geschützt sind.
- Kaskadentopologien werden nicht mit Schutz für Business Continuity unterstützt.

Die Rolle der Mediatoren

SnapMirror Active Sync verwendet einen Mediator, der als passiver Zeuge für SnapMirror Active Sync-Kopien

fungiert. Im Falle einer Netzwerkpartitionierung oder Nichtverfügbarkeit einer Kopie ermittelt SnapMirror Active Sync mithilfe des Mediators, welche Kopie weiterhin I/O bereitstellt, während die I/O-Leistung der anderen Kopie eingestellt wird. Zusätzlich zum lokalen ONTAP Mediator können Sie ab ONTAP 9.17.1 ONTAP Cloud Mediator installieren, um die gleiche Funktionalität in einer Cloud-Bereitstellung bereitzustellen. Sie können ONTAP Mediator oder ONTAP Cloud Mediator verwenden, jedoch nicht beide gleichzeitig.

Der Mediator spielt in SnapMirror Active Sync-Konfigurationen als passiver Quorum-Zeuge eine entscheidende Rolle. Er stellt die Quorum-Aufrechterhaltung sicher und erleichtert den Datenzugriff bei Ausfällen. Es fungiert als Ping-Proxy für Controller, um die Aktivität von Peer-Controllern zu bestimmen. Obwohl der Mediator keine Umschaltvorgänge aktiv auslöst, erfüllt er eine wichtige Funktion: Er ermöglicht dem verbleibenden Knoten, den Status seines Partners bei Netzwerkkommunikationsproblemen zu überprüfen. In seiner Rolle als Quorum-Zeuge bietet der ONTAP Mediator einen alternativen Pfad (und fungiert somit als Proxy) zum Peer-Cluster.

Darüber hinaus ermöglicht es Clustern, diese Informationen als Teil des Quorum-Prozesses abzurufen. Es verwendet das Node-Management-LIF und das Cluster-Management-LIF für Kommunikationszwecke. Es stellt redundante Verbindungen über mehrere Pfade her, um zwischen Site-Ausfällen und InterSwitch Link (ISL)-Ausfällen zu unterscheiden. Wenn ein Cluster aufgrund eines Ereignisses die Verbindung zur Mediator-Software und all seinen Knoten verliert, gilt er als nicht erreichbar. Dies löst eine Warnung aus und ermöglicht ein automatisches Failover auf die Spiegelkonsistenzgruppe am sekundären Standort, wodurch unterbrechungsfreie E/A für den Client sichergestellt wird. Der Replikationsdatenpfad basiert auf einem Heartbeat-Mechanismus. Wenn eine Netzwerkstörung oder ein Ereignis länger als einen bestimmten Zeitraum anhält, kann dies zu Heartbeat-Ausfällen führen und die Beziehung asynchron machen. Das Vorhandensein redundanter Pfade, wie z. B. ein LIF-Failover auf einen anderen Port, kann den Heartbeat jedoch aufrechterhalten und solche Störungen verhindern.

ONTAP Mediator

ONTAP Mediator wird in einer dritten Fehlerdomäne installiert, die sich von den beiden von ihm überwachten ONTAP Clustern unterscheidet. Dieses Setup besteht aus drei Schlüsselkomponenten:

- Primärer ONTAP-Cluster, der die primäre Konsistenzgruppe des SnapMirror Active Sync hostet
- Sekundärer ONTAP Cluster, der die gespiegelte Konsistenzgruppe hostet
- ONTAP Mediator

ONTAP Mediator wird für folgende Zwecke verwendet:

- Stellen Sie ein Quorum fest
- Kontinuierliche Verfügbarkeit durch automatisches Failover (AUFO)
- Geplante Failover (PFO)

ONTAP Mediator 1.7 kann zehn Clusterpaare zur Gewährleistung der Geschäftskontinuität verwalten.

Wenn der ONTAP Mediator nicht verfügbar ist, können Sie keine geplanten oder automatisierten Failover durchführen. Die Anwendungsdaten werden weiterhin synchron und ohne Unterbrechung repliziert, sodass kein Datenverlust auftritt.

ONTAP Cloud Mediator

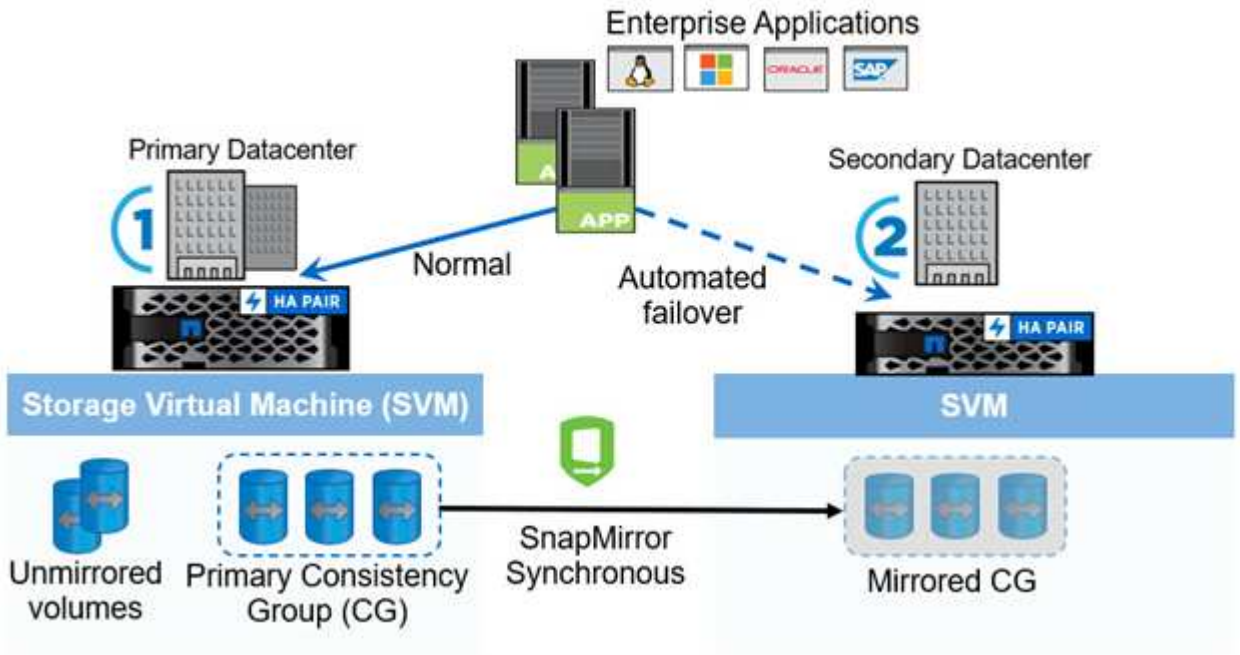
Ab ONTAP 9.17.1 ist ONTAP Cloud Mediator als Cloud-basierter Dienst in der NetApp Konsole zur Verwendung mit SnapMirror Active Sync verfügbar. Ähnlich wie ONTAP Mediator bietet ONTAP Cloud Mediator die folgenden Funktionen in einer SnapMirror Active Sync-Beziehung:

- Bietet einen dauerhaften und abgeschirmten Speicher für HA- oder SnapMirror Active Sync-Metadaten.
- Dient als Ping-Proxy für Controller-Lebendigkeit.
- Bietet synchrone Funktionen für die Integritätsabfrage von Nodes zur Unterstützung der Quorumbestimmung.

Der ONTAP Cloud Mediator vereinfacht die Bereitstellung von SnapMirror Active Sync, indem er den NetApp Console-Cloud-Service als dritten Standort verwendet, den Sie nicht verwalten müssen. Der ONTAP Cloud Mediator bietet die gleiche Funktionalität wie der lokale ONTAP Mediator, reduziert jedoch den operativen Aufwand für die Wartung eines dritten Standorts. Im Gegensatz dazu ist ONTAP Mediator als Paket erhältlich und muss auf einem Linux-Host an einem dritten Standort mit unabhängiger Stromversorgung und Netzwerkinfrastruktur installiert werden.

Workflow für den aktiven Synchronisierungsvorgang von SnapMirror

Die folgende Abbildung zeigt das Design der aktiven SnapMirror Synchronisierung auf hoher Ebene.



Das Diagramm zeigt eine Enterprise-Applikation, die auf einer Storage-VM (SVM) im primären Datacenter gehostet wird. Die SVM enthält fünf Volumes, drei davon sind Teil einer Konsistenzgruppe. Die drei Volumes in der Konsistenzgruppe werden in einem sekundären Datacenter gespiegelt. Unter normalen Bedingungen werden alle Schreibvorgänge im primären Datacenter durchgeführt. Dieses Datacenter dient praktisch als Quelle für I/O-Vorgänge, während das sekundäre Datacenter als Ziel dient.

Im Falle eines Katastrophenszenarios im primären Rechenzentrum weist ONTAP das sekundäre Rechenzentrum an, als primäres Rechenzentrum zu fungieren und alle E/A-Vorgänge durchzuführen. Es werden nur die Volumes bedient, die in der Konsistenzgruppe gespiegelt sind. Alle Vorgänge, die die anderen beiden Volumes auf dem SVM betreffen, sind vom Katastrophenereignis betroffen.

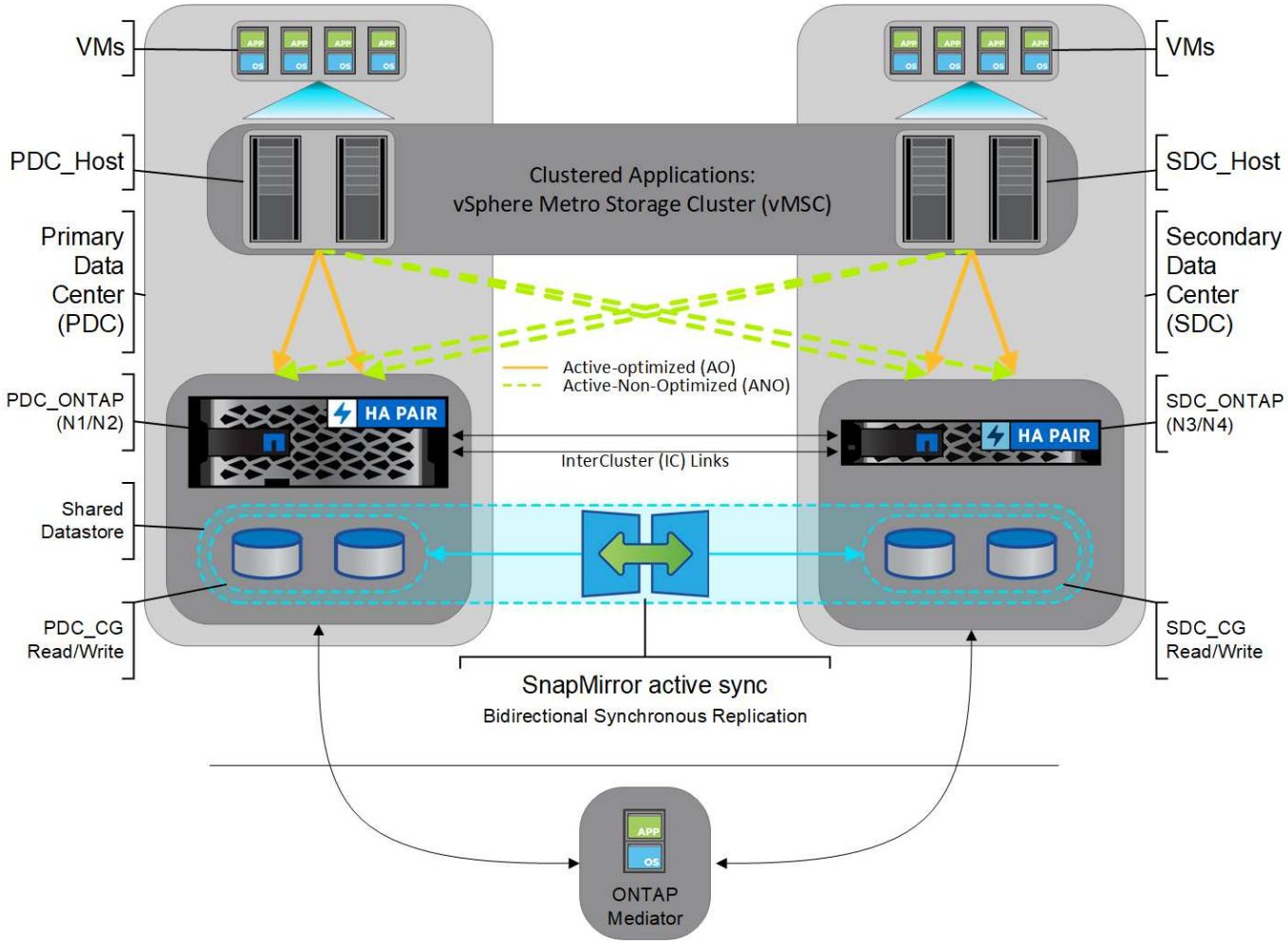
Symmetrische aktiv/aktiv-Lösung

SnapMirror Active Sync bietet asymmetrische und symmetrische Lösungen.

In asymmetrischen Konfigurationen stellt die primäre Speicherkopie einen aktiv optimierten Pfad bereit und bedient aktiv Client-E/A. Der sekundäre Standort verwendet einen Remotepfad für E/A. Die Speicherpfade des

sekundären Standorts gelten als aktiv nicht optimiert. Der Zugriff auf die Schreib-LUN erfolgt über den Proxy des sekundären Standorts. Das 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. Das bedeutet, dass Hosts auf beiden Seiten auf lokalen Speicher für aktive E/A zugreifen können. Ab ONTAP 9.16.1 wird symmetrisches Aktiv/Aktiv auf Clustern mit bis zu vier Knoten unterstützt. Ab ONTAP 9.17.1 unterstützen symmetrische Aktiv/Aktiv-Konfigurationen das NVMe-Protokoll auf Clustern mit zwei Knoten.



Symmetrische aktiv/aktiv-Lösung ist für geclusterte Applikationen wie VMware Metro Storage Cluster, Oracle RAC und Windows Failover Clustering mit SQL bestimmt.

Anwendungsfälle für ONTAP SnapMirror Active Sync

Die Anforderungen einer global vernetzten Geschäftsumgebung erfordern eine schnelle Wiederherstellung geschäftskritischer Anwendungsdaten ohne Datenverlust im Falle einer Störung wie einem Cyberangriff, einem Stromausfall oder einer Naturkatastrophe. Diese Anforderungen sind in Bereichen wie dem Finanzwesen und der Einhaltung gesetzlicher Vorschriften wie der Datenschutz-Grundverordnung (DSGVO) noch höher.

SnapMirror Active Sync bietet folgende Anwendungsfälle:

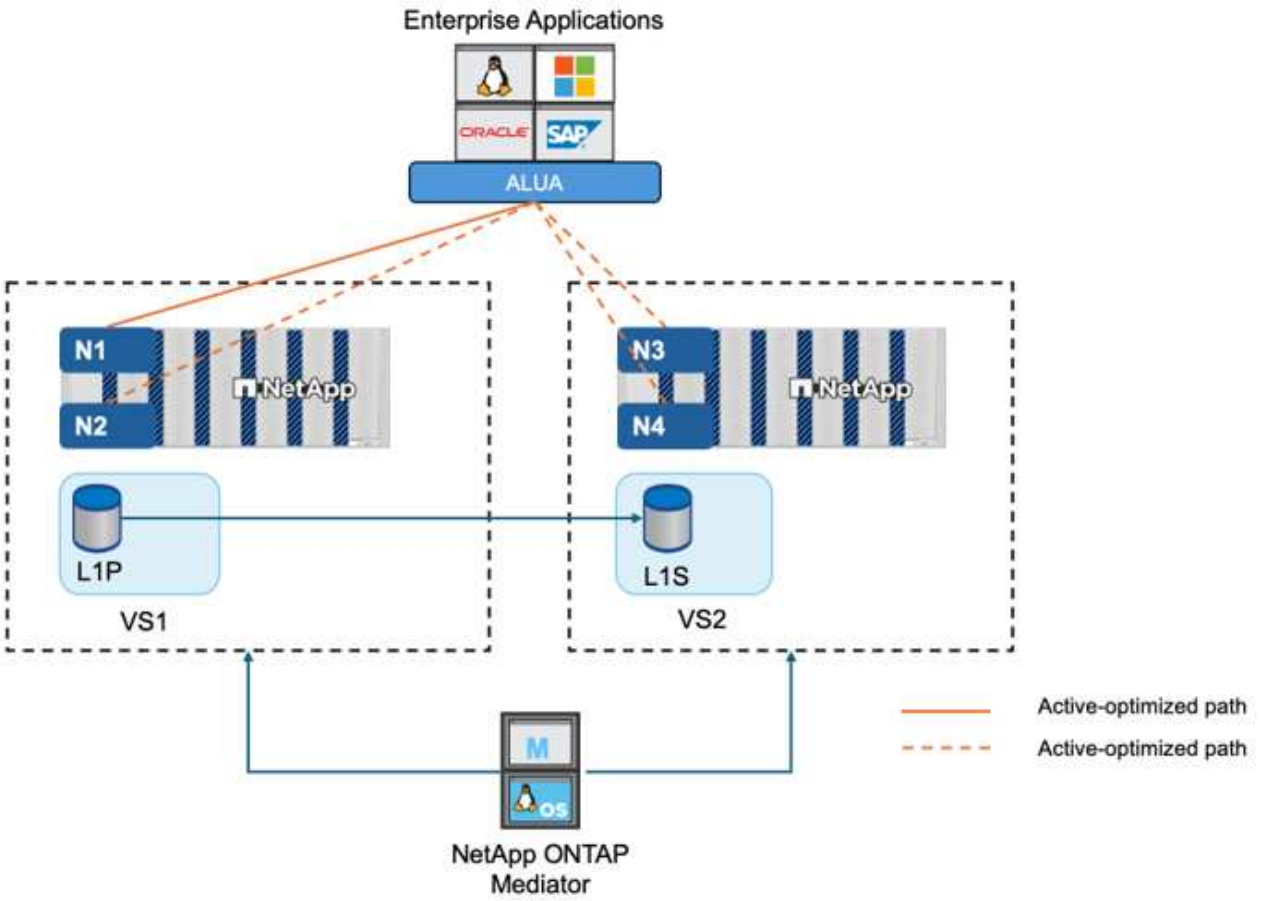
Applikationsimplementierung für Recovery Time Objective (RTO) von null

In einer SnapMirror Active Sync-Bereitstellung verfügen Sie über einen primären und einen sekundären

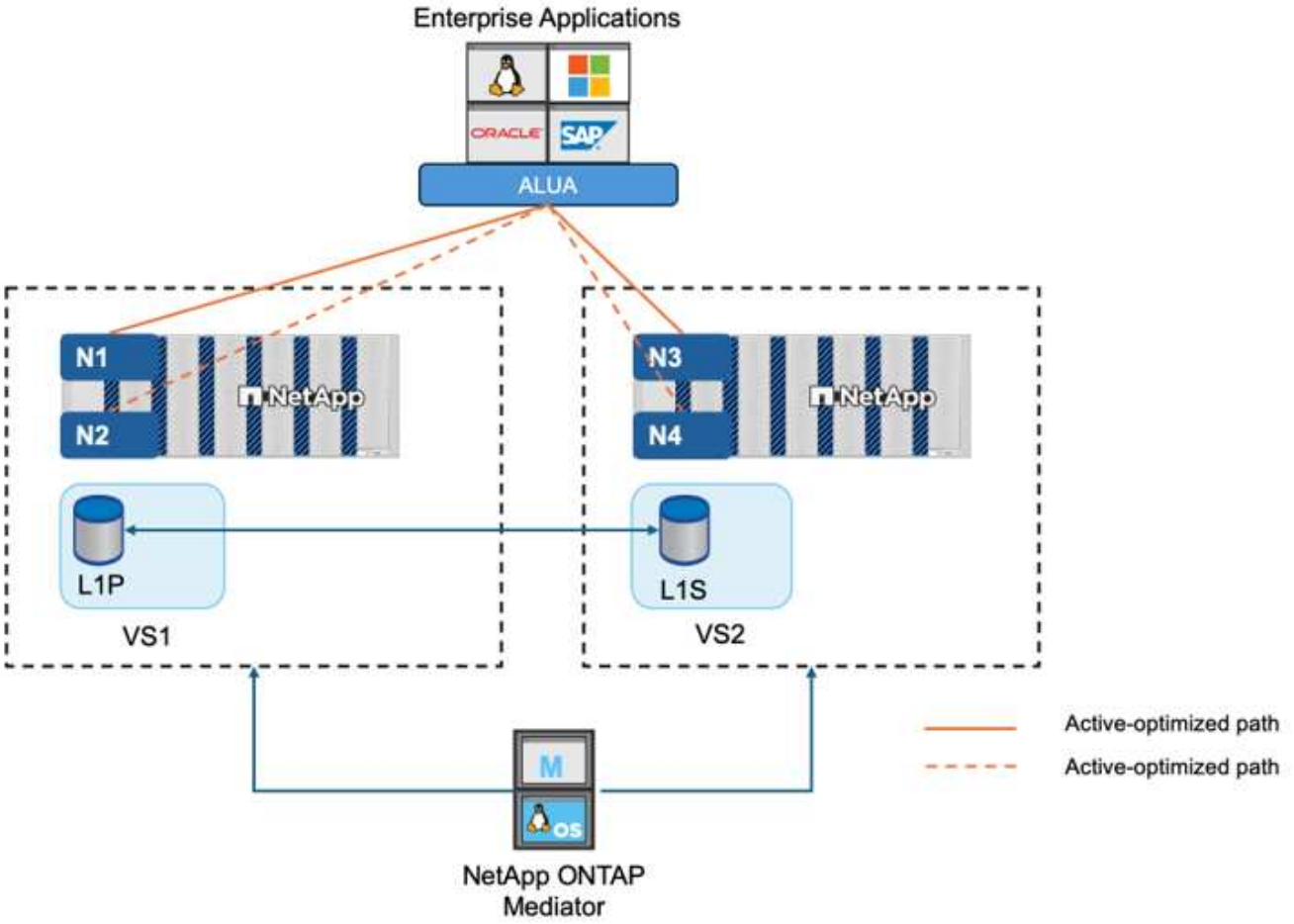
Cluster. Eine LUN im primären Cluster `L1P`) hat einen Spiegel `L1S`) auf der sekundären LUN; beide LUNs haben dieselbe serielle ID und werden dem Host als Lese-/Schreib-LUNs gemeldet. In asymmetrischen Konfigurationen werden Lese- und Schreibvorgänge jedoch nur auf der primären LUN ausgeführt. `L1P` . Alle Schreibvorgänge auf dem Spiegel `L1S` werden durch einen Proxy bedient.

Applikationseinsatz für null RTO oder transparentes Applikations-Failover (TAF)

TAF basiert auf einem softwarebasierten Pfad-Failover des Hosts mit MPIO, um einen unterbrechungsfreien Zugriff auf den Speicher zu gewährleisten. Beide LUN-Kopien – z. B. die primäre (L1P) und die gespiegelte Kopie (L1S) – haben dieselbe Identität (Seriennummer) und werden dem Host als lesbar und schreibbar gemeldet. In asymmetrischen Konfigurationen werden Lese- und Schreibvorgänge jedoch nur vom primären Volume ausgeführt. I/Os an die gespiegelte Kopie werden an die primäre Kopie weitergeleitet. Der bevorzugte Pfad des Hosts zu L1 ist VS1:N1, basierend auf dem ALUA-Zugriffsstatus „A/O“ (Asymmetrischer Logical Unit Access). ONTAP Mediator wird als Teil der Bereitstellung benötigt, hauptsächlich um bei einem Speicherausfall auf dem primären Volume ein Failover (geplant oder ungeplant) durchzuführen.



TAF arbeitet in zwei Modi: Automatisiertes Failover und Automatisiertes Failover-Duplex. Beim Automatisierten Failover werden Lese- und Schreibvorgänge nur vom primären Volume ausgeführt. Daher werden E/A-Vorgänge an die Spiegelkopie (die selbst keine Schreibvorgänge ausführen kann) an die primäre Kopie weitergeleitet. Beim Automatisierten Failover-Duplex können sowohl die primäre als auch die sekundäre Kopie E/A-Vorgänge ausführen, sodass kein Proxy erforderlich ist.



Wenn Sie NVMe für den Hostzugriff mit ONTAP 9.17.1 verwenden, wird nur die Richtlinie AutomatedFailoverDuplex unterstützt.

Die aktive Synchronisierung von SnapMirror verwendet ALUA, einen Mechanismus, der ein Multipathing-Software für Applikationshosts mit Pfaden ermöglicht, die mit Prioritäten beworben werden, und Zugriffsverfügbarkeit für die Kommunikation des Applikations-Hosts mit dem Storage-Array. ALUA markiert aktive optimierte Pfade zu den Controllern, die die LUN besitzen, 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 erkennen können. Das ONTAP NVMe-Ziel veröffentlicht die entsprechenden Pfadzustände, damit Anwendungshosts den optimalen Pfad für einen geschützten NVMe-Namespace verwenden können.

Geclusterte Applikationen

Clusteranwendungen, darunter VMware Metro Storage Cluster, Oracle RAC und Windows Failover Clustering mit SQL, erfordern gleichzeitigen Zugriff, damit ein Failover der VMs auf andere Sites ohne Leistungseinbußen erfolgen kann. SnapMirror Active Sync Symmetric Active/Active bedient IO lokal mit bidirektionaler Replikation, um die Anforderungen von Clusteranwendungen zu erfüllen. Ab ONTAP 9.16.1 wird symmetrisches Aktiv/Aktiv in einer Konfiguration in Clustern mit vier Knoten unterstützt, wobei die Clustergrenze von zwei Knoten in ONTAP 9.15.1 erweitert wird.

Notfallszenario

Synchrone Replizierung mehrerer Volumes für eine Applikation zwischen Standorten an geografisch verteilten Standorten Bei Unterbrechungen des primären Storage kann automatisch ein Failover auf die sekundäre

Kopie durchgeführt werden. Dies ermöglicht Business Continuity für Tier-1-Applikationen. Wenn der Standort, der das primäre Cluster hostet, einen Ausfall durchbricht, kennzeichnet die Host-Multipathing-Software alle Pfade durch das Cluster als inaktiv und verwendet Pfade vom sekundären Cluster. Das Ergebnis ist ein unterbrechungsfreier Failover, der durch ONTAP Mediator auf die gespiegelte Kopie aktiviert wird.

Erweiterte Anwendungsunterstützung

SnapMirror Active Sync bietet Flexibilität mit benutzerfreundlicher Granularität auf Anwendungsebene und automatischem Failover. SnapMirror Active Sync verwendet die bewährte synchrone Replikation von SnapMirror über ein IP-Netzwerk, um Daten mit hoher Geschwindigkeit über LAN oder WAN zu replizieren und so eine hohe Datenverfügbarkeit und schnelle Datenreplikation für Ihre geschäftskritischen Anwendungen wie Oracle, Microsoft SQL Server usw. sowohl in virtuellen als auch in physischen Umgebungen zu erreichen.

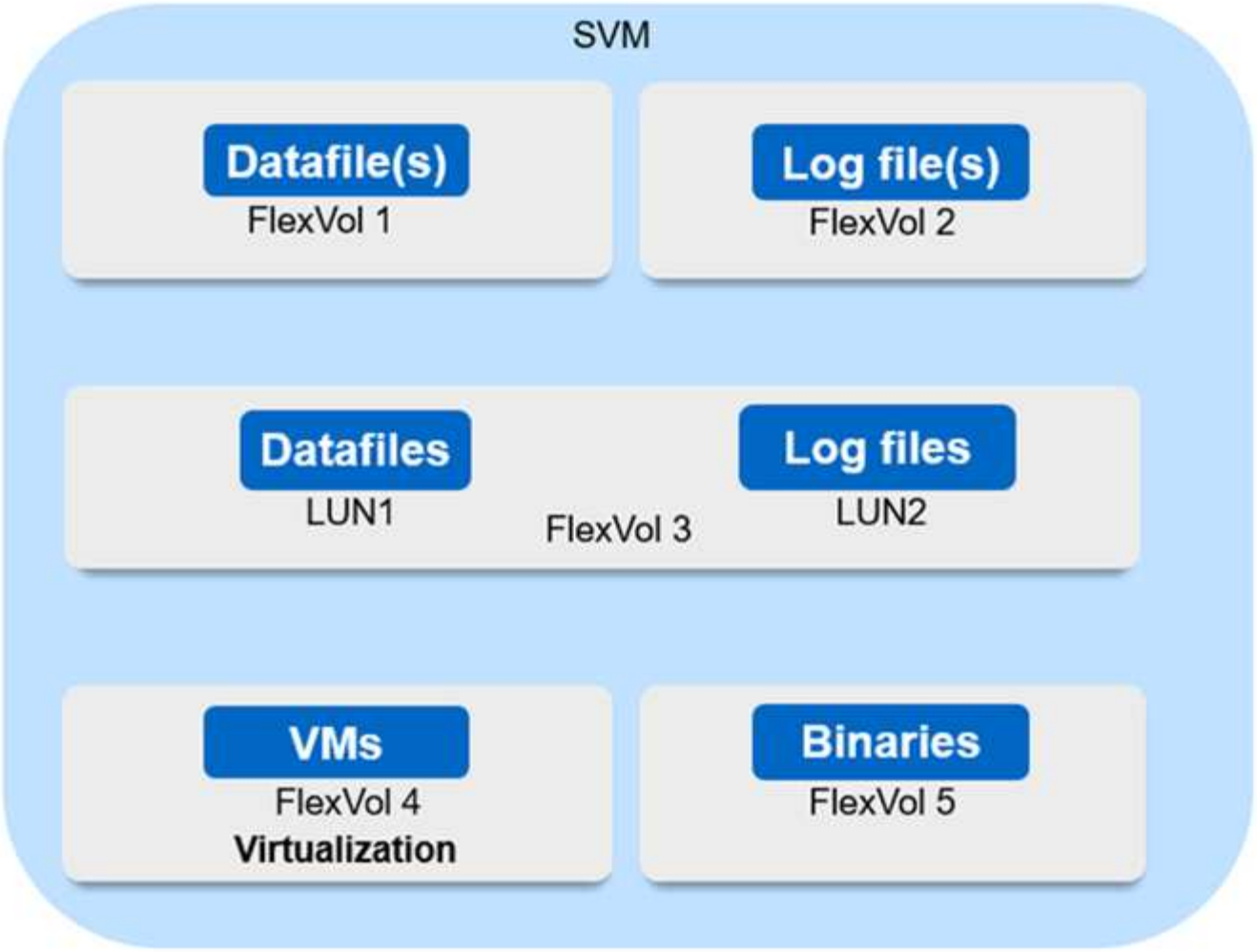
SnapMirror Active Sync ermöglicht die Weiterführung unternehmenskritischer Geschäftsdienste auch bei einem vollständigen Site-Ausfall mit TAF zur sekundären Kopie. Zum Auslösen dieses Failovers sind keine manuellen Eingriffe oder zusätzliche Skripts erforderlich.

Bereitstellungsstrategie und Best Practices für ONTAP SnapMirror Active Sync

Es ist wichtig, dass Ihre Datenschutzstrategie die Workloads klar identifiziert, die zur Gewährleistung der Geschäftskontinuität geschützt werden müssen. Der wichtigste Schritt in Ihrer Datenschutzstrategie besteht darin, Klarheit über das Datenlayout Ihrer Unternehmensanwendungen zu schaffen, damit Sie entscheiden können, wie Sie die Datenmengen verteilen und die Geschäftskontinuität schützen. Da das Failover auf der Ebene der Konsistenzgruppe auf Anwendungsbasis erfolgt, müssen Sie der Konsistenzgruppe unbedingt die erforderlichen Datenvolumes hinzufügen.

SVM-Konfiguration

In dem Diagramm ist eine empfohlene SVM-Konfiguration (Storage VM) für SnapMirror Active Sync dargestellt.



- Für Daten-Volumes:
  - Zufällige Lese-Workloads werden von sequenziellen Schreibzugriffen isoliert. Daher werden die Daten und Log-Dateien je nach Datenbankgröße in der Regel auf separaten Volumes platziert.
    - Bei großen kritischen Datenbanken befindet sich die einzelne Datendatei auf FlexVol 1 und die entsprechende Protokolldatei auf FlexVol 2.
    - Zur besseren Konsolidierung werden kleine und mittelgroße nicht kritische Datenbanken so gruppiert, dass sich alle Datendateien auf FlexVol 1 befinden und die entsprechenden Log-Dateien auf FlexVol 2 sind. Durch diese Gruppierung verlieren Sie jedoch die Granularität auf Applikationsebene.
  - Eine weitere Variante ist, alle Dateien innerhalb derselben FlexVol 3 zu haben, mit Dateien in LUN1 und deren Protokolldateien in LUN 2.
- Wenn Ihre Umgebung virtualisiert ist, müssten alle VMs für verschiedene Enterprise-Applikationen in einem Datastore gemeinsam genutzt werden. In der Regel werden die VMs und Applikationsbinärdateien mit SnapMirror asynchron repliziert.

Planen

Voraussetzungen für ONTAP SnapMirror Active Sync

Stellen Sie bei der Planung Ihrer SnapMirror Active Sync Implementierung sicher, dass

Sie die verschiedenen Anforderungen an Hardware, Software und Systemkonfiguration erfüllt haben.

Trennt

In der folgenden Tabelle sind die unterstützten NetApp Cluster-Konfigurationen aufgeführt.

Cluster-Typ	Unterstützte Modelle	Unterstützte Funktionen	Maximal unterstützte Clusterknoten
AFF	A-Series, C-Series	Automated Failover Duplex (Symmetrisch Aktiv/Aktiv), Automated Failover (Asymmetrisch Aktiv/Aktiv)	• 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/Aktiv)	• 2 (ONTAP 9.9.1 oder höher • 4 (ONTAP 9.16.1 mit symmetrischen Aktiv/Aktiv-Konfigurationen)
ASA r2	Alle	Automatisierte Ausfallsicherung Duplex (symmetrisch aktiv/aktiv)	• 2 (ONTAP 9.17.1 oder früher) • 4 (ONTAP 9.18.1 oder höher)

In der folgenden Tabelle wird die Fähigkeit zur Replikation zwischen Cluster-Typen dargestellt.

Clustertyp 1	Clustertyp 2	Replizierung unterstützt?
AFF A-Serie	AFF C-Serie	Ja.
ASA r2 A-Serie	ASA r2 C-Serie	Ja.
AFF	ASA	Nein
ASA	ASA r2	Nein
ASA r2	ASA r2	Ja.

Software

- ONTAP 9.9.1 oder höher
- ONTAP Mediator 1.2 oder höher
- Ein Linux-Server oder eine virtuelle Maschine für ONTAP Mediator, auf dem eines der folgenden

ausgeführt wird:

Version des ONTAP Mediators	Unterstützte Linux-Versionen
1,11	• Red Hat Enterprise Linux ◦ Kompatibel: 9.5 [1] ◦ Empfohlen: 10.1, 10.0, 9.7, 9.6, 9.4 und 8.10 • Rocky Linux 10,1, 9.7 und 8.10 • Oracle Linux 10.0 und 9.6
1,10	• Red Hat Enterprise Linux ◦ Kompatibel: 9.5 [1] ◦ Empfohlen: 10,0, 9,6, 9,4 und 8,10 • Rocky Linux 10,0, 9.6 und 8.10
1.9.1	• Red Hat Enterprise Linux ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8 • Rocky Linux 9.5 und 8.10
1,9	• Red Hat Enterprise Linux ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8 • Rocky Linux 9.5 und 8.10
1,8	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 und 8.8 • Rocky Linux 9.4 und 8.10
1,7	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.3, 9.2, 9.1, 9.0, 8.9 und 8.8 • Rocky Linux 9.3 und 8.9
1,6	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.2, 9.1, 9.0 und 8.8 • Rocky Linux 9.2 und 8.8

1,5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6

1. Kompatibel bedeutet, dass Red Hat diese RHEL-Versionen nicht mehr unterstützt, ONTAP Mediator jedoch weiterhin darauf installiert werden kann.

Lizenzierung

Die folgenden SnapMirror -Lizenzen sind als Teil der ONTAP One-Lizenzsuite verfügbar und müssen auf beiden Clustern angewendet werden:

- SnapMirror Synchronous
- SnapMirror

> Wenn Ihre ONTAP -Speichersysteme vor Juni 2019 erworben wurden, siehe "ONTAP Masterlizenzschlüssel" um die erforderliche SnapMirror Synchronisierungslizenz zu erhalten.

- Für vSphere Metro Storage Cluster (vMSC) ist eine VMware vSphere-Lizenz erforderlich.

Netzwerkumgebung

- Die Latenzzeit zwischen den Clustern muss weniger als 10 Millisekunden betragen.
- Ab ONTAP 9.14.1 "Persistente SCSI-3-Reservierungen"werden diese ab SnapMirror Active Sync unterstützt.

Unterstützte Protokolle

SnapMirror Active Sync unterstützt SAN-Protokolle.

- Die Protokolle FC und iSCSI werden ab ONTAP 9.9.1 unterstützt.
- Das NVMe-Protokoll wird mit VMware-Workloads ab ONTAP 9.17.1 unterstützt.

  SnapMirror Active Sync unterstützt Folgendes mit dem NVMe-Protokoll nicht:

  - Symmetrische Aktiv/Aktiv-Konfigurationen mit 4 Knoten
  - Asymmetrische Aktiv/Aktiv-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 Namespaces in derselben Konsistenzgruppe.

IP-Bereich

Der Standard-IP-Bereich wird von SnapMirror Active Sync für Cluster-Peer-Beziehungen benötigt. Benutzerdefinierte IP-Bereiche werden nicht unterstützt.

NTFS-Sicherheitsstil

NTFS-Sicherheitstil wird auf aktiven SnapMirror Sync Volumes **nicht** unterstützt.

ONTAP Mediator

- ONTAP Mediator muss extern bereitgestellt und für ein transparentes Anwendungs-Failover an ONTAP angeschlossen werden.
- Um die volle Funktionalität zu gewährleisten 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 Fehlerdomäne installiert werden, getrennt von den beiden ONTAP-Clustern.
- Bei der Installation von ONTAP Mediator sollten Sie das selbstsignierte Zertifikat durch ein gültiges Zertifikat ersetzen, das von einer gängigen, zuverlässigen Zertifizierungsstelle signiert wurde.
- Weitere Informationen zu ONTAP Mediator finden Sie unter "Vorbereiten der Installation von ONTAP Mediator" .

Andere Voraussetzungen

- In Versionen vor ONTAP 9.15.1 werden SnapMirror Active Sync-Beziehungen auf Lese-/Schreibzielvolumes (Volumes, die in einem asymmetrischen Active-Active-Modus von DP in Lese-/Schreibzugriff konvertiert wurden) nicht unterstützt. Bevor Sie ein Lese-/Schreib-Volume verwenden können, müssen Sie es in ein DP-Volume konvertieren, indem Sie eine SnapMirror -Beziehung auf Volume-Ebene erstellen (entweder asynchron oder synchron) und dann die Beziehung löschen. Weitere Informationen finden Sie unter "Konvertieren Sie eine vorhandene SnapMirror Beziehung zu SnapMirror Active Sync" .
- Speicher-VMs, die SnapMirror Active Sync verwenden, können nicht als Clientcomputer mit Active Directory verbunden werden.

Weitere Informationen

- "Hardware Universe"
- "ONTAP Mediator Übersicht"

ONTAP SnapMirror Active Sync-Interoperabilität

SnapMirror Active Sync ist mit zahlreichen Betriebssystemen, Applikations-Hosts und weiteren Funktionen von ONTAP kompatibel.

Weitere Informationen zu Supportmöglichkeiten und Interoperabilität, die hier nicht behandelt werden, finden Sie im Interoperabilitäts-Matrix-Tool ("IMT").

Applikations-Hosts

SnapMirror Active Sync unterstützt Hypervisoren wie Hyper-V, ESXi, Betriebssysteme wie Red Hat Enterprise Linux (RHEL), Windows Server und Clusterlösungen wie vSphere Metro Storage Cluster (vMSC) und, beginnend mit ONTAP 9.14.1, Windows Server Failover Cluster.

Betriebssysteme

SnapMirror Active Sync wird von zahlreichen Betriebssystemen unterstützt, darunter:

- AIX über PVR (ab ONTAP 9.11.1)
- HP-UX (ab ONTAP 9.10.1)
- Solaris 11.4 (ab ONTAP 9.10.1)

AIX

Ab ONTAP 9.11.1 wird AIX mit SnapMirror Active Sync über Standard Engineering Feature Policy Variance Request (FPVR) unterstützt, unter der Voraussetzung, dass die folgenden Bestimmungen verstanden werden:

- SnapMirror Active Sync bietet zwar eine RPO-Datensicherung ohne, aber für den Failover-Prozess mit AIX sind zusätzliche Schritte erforderlich, um die Pfadänderung zu erkennen. Bei LUNs, die nicht Teil einer Root-Volume-Gruppe sind, wird eine I/O-Pause angezeigt, bis ein `cfgmgr` Befehl ausgeführt wird. Dieser Vorgang ist automatisiert und die meisten Applikationen nehmen den Betrieb ohne weitere Unterbrechungen wieder auf.
- LUNs, die Teil einer Root-Volume-Gruppe sind, sollten im Allgemeinen nicht durch SnapMirror Active Sync geschützt werden. `cfgmgr`Nach einem Failover kann der Befehl nicht ausgeführt werden. Das bedeutet, dass ein Neustart erforderlich ist, um die Änderungen in SAN-Pfaden zu erkennen. Sie können für die Root-Volume-Gruppe nach wie vor eine RPO-Datensicherung von null erzielen, jedoch ist der Failover nicht möglich.

Weitere Informationen über SnapMirror Active Sync mit AIX erhalten Sie von Ihrem NetApp Account Team.

HP-UX ERHÄLTLICH

Ab ONTAP 9.10.1 wird SnapMirror Active Sync für HP-UX unterstützt.

Automatischer ungeplanter Failover mit HP-UX

Ein automatisches ungeplantes Failover-Ereignis (AUFO) auf dem isolierten Mastercluster kann durch einen Dual-Event-Fehler 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 im Gegensatz zu anderen AUFO-Ereignissen als seltenes Ereignis.

- In diesem Szenario kann es mehr als 120 Sekunden dauern, bis die I/O-Vorgänge auf dem HP-UX-Host fortgesetzt werden. Je nach laufenden Applikationen kann dies keine I/O-Unterbrechungen oder Fehlermeldungen führen.
- Um Abhilfe zu schaffen, müssen Sie Anwendungen auf dem HP-UX-Host neu starten, die eine Unterbrechungstoleranz von weniger als 120 Sekunden aufweisen.

Solaris

Ab ONTAP 9.10.1 unterstützt SnapMirror Active Sync Solaris 11.4.

Um sicherzustellen, dass die Solaris-Clientanwendungen bei einer ungeplanten Site-Failover-Umschaltung in einer SnapMirror Active Sync-Umgebung unterbrechungsfrei laufen, ändern Sie die Standardeinstellungen des Solaris-Betriebssystems. Informationen zum Konfigurieren von Solaris mit den empfohlenen Einstellungen finden Sie im"NetApp Knowledge Base: Solaris Host unterstützt empfohlene Einstellungen in SnapMirror Active Sync" .

ONTAP Interoperabilität

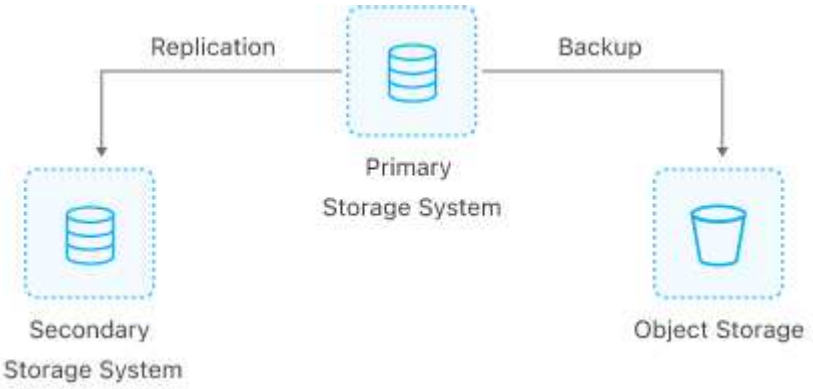
Die aktive Synchronisierung von SnapMirror mit den Komponenten von ONTAP erweitert die Datensicherungsfunktionen von SnapMirror.

FabricPool

SnapMirror Active Sync unterstützt Quell- und Ziel-Volumes auf FabricPool Aggregaten mit Tiering-Richtlinien von „Keine“, „Snapshot“ oder „automatisch“. SnapMirror Active Sync unterstützt keine FabricPool Aggregate mit einer Tiering Policy von Alle.

Fan-out-Konfigurationen

InFan-out-Konfigurationen , Ihr Quellvolume kann auf einen SnapMirror Active Sync-Zielendpunkt und auf eine asynchrone SnapMirror -Beziehung gespiegelt werden.



SnapMirror Active Sync unterstützt Fan-out-Konfigurationen die `MirrorAllSnapshots` Richtlinie und ab ONTAP 9.11.1 auch die Richtlinie. `MirrorAndVault` Fan-out-Konfigurationen werden bei der SnapMirror Active Sync mit der `XDPDefault` Richtlinie nicht unterstützt.

Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync nach einem Failover die automatische Neukonfiguration im Fan-out-Bereich. Wenn das Failover vom primären zum sekundären Standort erfolgreich war, wird der tertiäre Standort automatisch neu konfiguriert, um den sekundären Standort als Quelle zu behandeln. Der asynchrone Fan-out-Teil kann eine Konsistenzgruppenbeziehung oder eine unabhängige Volume-Beziehung sein. Die Neukonfiguration funktioniert für einen der Fälle. Die Neukonfiguration wird entweder durch einen geplanten oder einen ungeplanten Failover ausgelöst. Die Neukonfiguration erfolgt außerdem im Falle eines Failback zum primären Standort.

Informationen zum Verwalten Ihrer Fan-out-Konfiguration in früheren Versionen von ONTAP finden Sie unter Setzen Sie den Schutz in der Fan-out-Konfiguration fort.

NDMP-Wiederherstellung

Ab ONTAP 9.13.1 können Sie SnapMirror Active Sync verwendenNDMP zum Kopieren und Wiederherstellen von Daten. Mithilfe von NDMP können Sie Daten auf die aktive synchrone SnapMirror Quelle verschieben, um eine Wiederherstellung abzuschließen, ohne den Schutz zu unterbrechen. Dies ist insbesondere bei Fan-out-Konfigurationen von Vorteil.

SnapCenter

SnapMirror Active Sync wird ab SnapCenter unterstütztSnapCenter 5.0. SnapCenter ermöglicht das Erstellen von Snapshots zur Sicherung und Wiederherstellung von Applikationen und Virtual Machines. Dies ermöglicht stets verfügbare Storage-Lösungen mit Granularität auf Applikationsebene.

SnapRestore

SnapMirror Active Sync unterstützt SnapRestore mit einer teilweisen oder einzelnen Datei.

Single File SnapRestore

Ab ONTAP 9.11.1 SnapRestore mit einer Dateiwird es für aktive SnapMirror Sync Volumes unterstützt. Sie können eine einzelne Datei aus einem Snapshot wiederherstellen, der von der aktiven synchronen SnapMirror-Quelle auf das Ziel repliziert wird. Da Volumes eine oder mehrere LUNs enthalten können, hilft Ihnen diese Funktion bei der Implementierung einer weniger Betriebsunterbrechung. Sie können eine einzelne LUN granular wiederherstellen, ohne die anderen LUNs zu unterbrechen. Single File SnapRestore bietet zwei Optionen: In-Place und Out-of-Place.

SnapRestore der Teildatei

Ab ONTAP 9.12.1 "Partielle LUN-Wiederherstellung"wird es für aktive SnapMirror Sync Volumes unterstützt. Sie können Daten aus von Applikationen erstellten Snapshots wiederherstellen, die zwischen den SnapMirror Quell- (Volume) und den Ziel-Volumes (Snapshot) repliziert wurden. Eine partielle LUN- oder Dateiwiederherstellung kann erforderlich sein, wenn Sie eine Datenbank auf einem Host wiederherstellen müssen, der mehrere Datenbanken auf derselben LUN speichert. Wenn Sie diese Funktionalität verwenden, müssen Sie den Anfangsbyteoffset der Daten und die Byte-Anzahl kennen.

Große LUNs und große Volumes

Die Unterstützung großer LUNs und großer Volumes (mehr als 100 TB) hängt von der von Ihnen verwendeten Version von ONTAP und Ihrer Plattform ab.

ONTAP 9.12.1P2 und höher

- Bei ONTAP 9.12.1 P2 und höher unterstützt die SnapMirror Active Sync große LUNs und große Volumes von mehr als 100 TB auf ASA und AFF (A-Serie und C-Serie). Primäre und sekundäre Cluster müssen vom gleichen Typ sein: Entweder ASA oder AFF. Die Replizierung von AFF A-Serie auf die AFF C-Serie und umgekehrt wird unterstützt.

> Für ONTAP Versionen 9.12.1P2 und höher müssen Sie sicherstellen, dass sowohl die primären als auch die sekundären Cluster entweder rein Flash-basierte SAN-Arrays (ASA) oder rein Flash-basierte Arrays (AFF) sind und dass auf beiden Systemen ONTAP 9.12.1 P2 oder höher installiert ist. Wenn auf dem sekundären Cluster eine Version vor ONTAP 9.12.1P2 ausgeführt wird oder der Array-Typ nicht mit dem primären Cluster identisch ist, kann die synchrone Beziehung ausfallen, wenn das primäre Volume größer als 100 TB ist.

ONTAP 9.9.1 - 9.12.1P1

- Für ONTAP-Versionen zwischen ONTAP 9.9.1 und 9.12.1 P1 (inklusive) werden große LUNs und große Volumen über 100 TB nur auf rein Flash-basierten SAN-Arrays unterstützt. Die Replizierung von AFF A-Serie auf die AFF C-Serie und umgekehrt wird unterstützt.

> Bei ONTAP-Versionen zwischen ONTAP 9.9.1 und 9.12.1 P2 müssen Sie sicherstellen, dass sowohl die primären als auch die sekundären Cluster All-Flash-SAN-Arrays sind und auf beiden Systemen ONTAP 9.9.1 oder höher installiert ist. Wenn auf dem sekundären Cluster eine ältere Version als ONTAP 9.9.1 ausgeführt wird oder es sich nicht um ein All-Flash-SAN-Array handelt, kann die synchrone Beziehung ausfallen, wenn das primäre Volume größer als 100 TB ist.

Weitere Informationen

- "Konfigurieren eines AIX-Hosts für SnapMirror Active Sync"

Objektlimits für ONTAP SnapMirror Active Sync

Beachten Sie bei der Vorbereitung auf die Verwendung der aktiven SnapMirror Synchronisierung die folgenden Objektgrenzen.

Konsistenzgruppen in einem Cluster

Die Einschränkungen für Konsistenzgruppen für ein Cluster mit aktiver SnapMirror Synchronisierung werden basierend auf Beziehungen berechnet und hängen von der Version der verwendeten ONTAP ab. Einschränkungen 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 Cluster mit vier Nodes in symmetrischen aktiv/aktiv-Konfigurationen. In einem Cluster mit vier Nodes werden 100 Konsistenzgruppen unterstützt.

Volumes pro Konsistenzgruppe

Die maximale Anzahl von Volumes pro Konsistenzgruppe mit SnapMirror Active Sync 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

Volume-Limits bei aktiver SnapMirror Synchronisierung werden basierend auf der Anzahl der Endpunkte und nicht auf der Anzahl der Beziehungen berechnet. Eine Konsistenzgruppe mit 12 Volumes steuert 12 Endpunkte auf dem primären und dem sekundären Cluster bei. Sowohl SnapMirror Active Sync als auch synchrone SnapMirror Beziehungen tragen zur Gesamtzahl der Endpunkte bei.

Diese Grenzwerte gelten für FAS -, AFF - und ASA -Systeme. Wenn Sie ein ASA r2 -System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20) haben, lesen Sie "ASA r2 Dokumentation" .

Die maximale Anzahl der Endpunkte pro Plattform ist in der folgenden Tabelle enthalten.

Plattform	Endpunkte pro HA für SnapMirror Active Sync			Endpunkte für synchrone Synchronisierung und aktive SnapMirror Synchronisierung insgesamt pro HA		
	ONTAP 9.11.1 und höher	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.11.1 und höher	ONTAP 9.10.1	ONTAP 9.9.1
AFF	400*	200	60	400	200	80
ASA	400*	200	60	400	200	80

* ab ONTAP 9.16.1 unterstützt SnapMirror Active Sync Cluster mit vier Nodes in symmetrischen aktiv/aktiv-Konfigurationen. Die Gesamtgrenze für ein Cluster mit vier Nodes liegt bei 800 Endpunkten.

SAN-Objektbeschränkungen

Die EINSCHRÄNKUNGEN FÜR SAN-Objekte sind in der folgenden Tabelle enthalten. Die Grenzen gelten unabhängig von der Plattform.

Objekt in einer SnapMirror Active Sync-Beziehung	Zählen
LUNs pro Volume	• 256 (ONTAP 9.9.1 – ONTAP 9.15.0) • 512 (ONTAP 9.15.1 und höher)
Anzahl eindeutiger LUNs, Namespaces oder Speichereinheiten pro 2 x 2 SnapMirror Active Sync-Lösung	4.096

Objekt in einer SnapMirror Active Sync-Beziehung	Zählen
Anzahl eindeutiger LUNs, Namespaces oder Speichereinheiten pro 4 x 4 SnapMirror Active-Sync-Lösung (verfügbar ab ONTAP 9.16.1)	6.144
LIFs pro SVM (mit mindestens einem Volume in einer SnapMirror Active Sync-Beziehung)	256
Inter-Cluster-LIFs pro Node	4
Inter-Cluster LIFs pro Cluster	8

NVMe-Objektlimits

Ab ONTAP 9.17.1 unterstützt SnapMirror Active Sync das NVMe-Protokoll. Die NVMe-Objektlimits sind in der folgenden Tabelle aufgeführt.

Maximale Objekte in einer SnapMirror Active Sync-Beziehung	Zählen
Anzahl der Namespace-Maps pro Knoten	4K
Clustergröße	2 Knoten
Anzahl der Konsistenzgruppen pro HA-Paar	50
Anzahl der Volumes in einer einzelnen NVMe SnapMirror Active Sync Consistency Group	80
Anzahl der Volumes in einem HA-Paar	400
NVMe-Subsysteme pro Konsistenzgruppe	16
Namespace-Zuordnungen pro Konsistenzgruppe	256

Verwandte Informationen

- "Hardware Universe"
- "Einschränkungen für Konsistenzgruppen"

Konfigurieren

Konfigurieren Sie ONTAP -Cluster für SnapMirror Active Sync

SnapMirror Active Sync verwendet Peering-Cluster, um Ihre Daten im Falle eines Failovers zu schützen. Bevor Sie ONTAP Mediator oder ONTAP Cloud Mediator für SnapMirror Active Sync konfigurieren, müssen Sie zunächst sicherstellen, dass der Cluster korrekt konfiguriert ist.

Bevor Sie beginnen

Bevor Sie ONTAP Mediator oder ONTAP Cloud Mediator konfigurieren, sollten Sie Folgendes bestätigen:

1. Zwischen den Clustern besteht eine Cluster-Peering-Beziehung.

Der standardmäßige IPspace wird von der aktiven SnapMirror Synchronisierung für Cluster-Peer-Beziehungen benötigt. Ein benutzerdefinierter IPspace wird nicht unterstützt.

"Erstellen einer Cluster-Peer-Beziehung"

2. Die SVMs werden auf jedem Cluster erstellt.

   "Erstellen einer SVM"

3. Zwischen den SVMs auf jedem Cluster besteht eine Peer-Beziehung.

   "Erstellen einer SVM-Peering-Beziehung"

4. Die Volumes sind für Ihre LUNs vorhanden.

   "Erstellen eines Volumes"

5. Auf jedem Knoten in beiden Clustern wird mindestens ein SAN LIF (entweder FC oder iSCSI, je nach Bedarf) erstellt.

   "Überlegungen zu LIFs in einer Cluster-SAN-Umgebung"

   "Erstellen einer LIF"

6. Die erforderlichen LUNs werden erstellt und einer Igroup zugeordnet, die zum Zuordnen von LUNs zum Initiator auf dem Anwendungshost verwendet wird.

   "LUNs erstellen und Initiatorgruppen zuordnen"

7. Der Anwendungshost wird erneut gescannt, um neue LUNs zu erkennen.

Konfigurieren Sie den ONTAP Mediator für SnapMirror Active Sync

SnapMirror Active Sync verwendet Peering-Cluster, um Ihre Daten im Fall eines Failover-Szenarios zu schützen. ONTAP Mediator ist eine wichtige Ressource, die durch die Überwachung des Zustands jedes Clusters die Geschäftskontinuität gewährleistet. Um SnapMirror Active Sync zu konfigurieren, müssen Sie zunächst ONTAP Mediator installieren und die ordnungsgemäße Konfiguration Ihrer primären und sekundären Cluster sicherstellen.

Nachdem Sie ONTAP Mediator installiert und Ihre Cluster konfiguriert haben, Initialisieren Sie ONTAP Mediator für SnapMirror Active Sync mit selbstsignierten Zertifikaten . Sie müssen dann Erstellen, Initialisieren und Zuordnen der Konsistenzgruppe für die aktive SnapMirror Synchronisierung.

ONTAP Mediator

ONTAP Mediator bietet einen persistenten und abgeschirmten Speicher für Hochverfügbarkeitsmetadaten (HA), die von den ONTAP-Clustern in einer SnapMirror Active Sync-Beziehung verwendet werden. Darüber hinaus bietet ONTAP Mediator eine synchrone Knoten-Integritätsabfrage-Funktion zur Unterstützung der Quorumbestimmung und dient als Ping-Proxy zur Erkennung der Controller-Lebendigkeit.

Jede Cluster-Peer-Beziehung kann nur einer einzelnen ONTAP-Mediatorinstanz zugeordnet werden. HA Mediator-Instanzen werden nicht unterstützt. Wenn sich ein Cluster in mehreren Peer-Beziehungen zu

anderen Clustern befindet, stehen die folgenden ONTAP-Mediatoroptionen zur Verfügung:

- Wenn SnapMirror Active Sync für jede Beziehung konfiguriert ist, kann jede Cluster-Peer-Beziehung eine eigene eindeutige ONTAP-Mediatorinstanz haben.
- Der Cluster kann dieselbe ONTAP Mediatorinstanz für alle Peer-Beziehungen verwenden.

Wenn beispielsweise Cluster B eine Peer-Beziehung zu Cluster A, Cluster C und Cluster D hat, können alle drei Cluster-Peer-Beziehungen eine eindeutige zugeordnete ONTAP-Mediatorinstanz haben, wenn SnapMirror Active Sync für jede Beziehung konfiguriert ist. Alternativ kann Cluster B für alle drei Peer-Beziehungen dieselbe ONTAP Mediatorinstanz verwenden. In diesem Szenario wird dieselbe Instanz von ONTAP Mediator dreimal für den Cluster aufgelistet.

Ab ONTAP 9.17.1 können Sie konfigurieren "ONTAP Cloud Mediator" Um den Zustand Ihres Clusters in einer SnapMirror Active Sync-Konfiguration zu überwachen, können Sie jedoch nicht beide Mediatoren gleichzeitig verwenden.

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** im"Versionshinweise zu ONTAP" für wichtige Informationen zu diesen Konfigurationen.

Voraussetzungen für ONTAP Mediator

- ONTAP Mediator bringt eigene Voraussetzungen mit sich. Sie müssen diese Voraussetzungen erfüllen, bevor Sie ONTAP Mediator installieren.

  Weitere Informationen finden Sie unter "Vorbereiten der Installation des ONTAP Mediator-Dienstes" .

- Standardmäßig stellt der ONTAP Mediator den Dienst über den TCP-Port 31784 bereit. Sie sollten sicherstellen, dass Port 31784 zwischen den ONTAP Clustern und dem ONTAP Mediator geöffnet und verfügbar ist.

Installieren Sie ONTAP Mediator und bestätigen Sie die Clusterkonfiguration

Führen Sie jeden der folgenden Schritte aus, um ONTAP Mediator zu installieren und die Clusterkonfiguration zu überprüfen. Bei jedem Schritt sollten Sie bestätigen, dass die spezifische Konfiguration durchgeführt wurde. Jeder Schritt enthält einen Link zu dem spezifischen Verfahren, das Sie befolgen müssen.

Schritte

1. Installieren Sie ONTAP Mediator, bevor Sie überprüfen, ob Ihre Quell- und Zielcluster richtig konfiguriert sind.

   Vorbereiten der Installation oder Aktualisierung von ONTAP Mediator

2. Bestätigen Sie, dass zwischen den Clustern eine Cluster-Peering-Beziehung besteht.

   Der standardmäßige IPspace wird von der aktiven SnapMirror Synchronisierung für Cluster-Peer-Beziehungen benötigt. Ein benutzerdefinierter IPspace wird nicht unterstützt.

   "Konfigurieren Sie ONTAP -Cluster für SnapMirror Active Sync"

Initialisieren Sie ONTAP Mediator für SnapMirror Active Sync mit selbstsignierten Zertifikaten

Nachdem Sie ONTAP Mediator installiert und Ihre Clusterkonfiguration bestätigt haben, müssen Sie ONTAP Mediator für die Clusterüberwachung initialisieren. Sie können ONTAP Mediator über den System Manager

oder die ONTAP CLI initialisieren.

System Manager

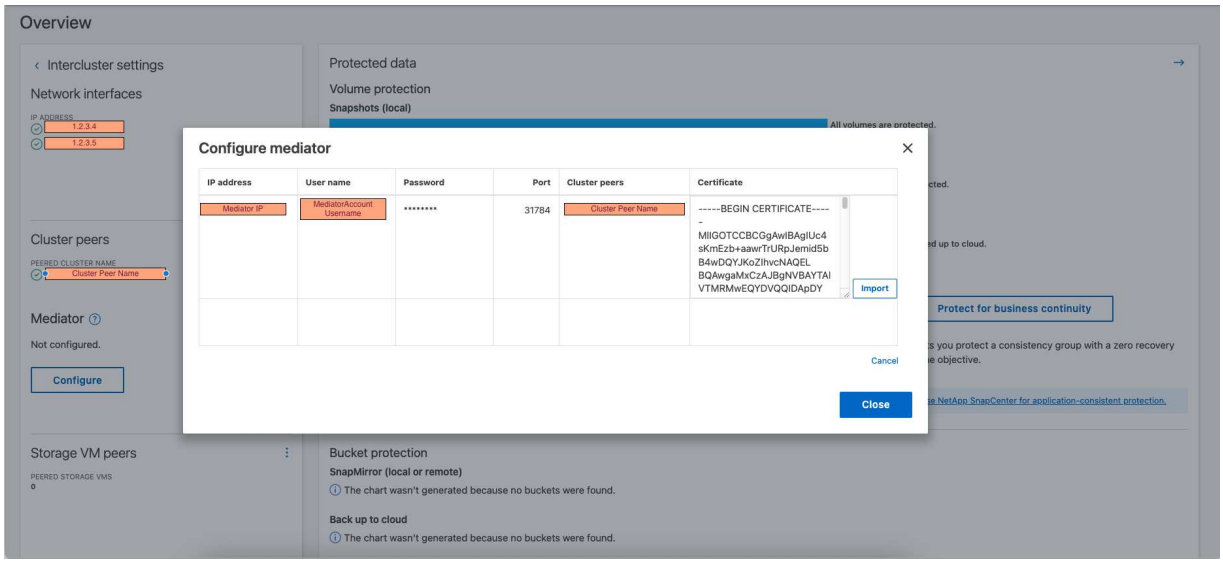
Mit System Manager können Sie ONTAP Mediator für automatisiertes Failover konfigurieren. Sie können auch die selbst signierte SSL und CA durch das Drittanbieter validierte SSL-Zertifikat und CA ersetzen, wenn Sie noch nicht getan haben.

Von ONTAP 9.14.1 bis 9.8 wird SnapMirror Active Sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

ONTAP Mediator 1.9 und höher

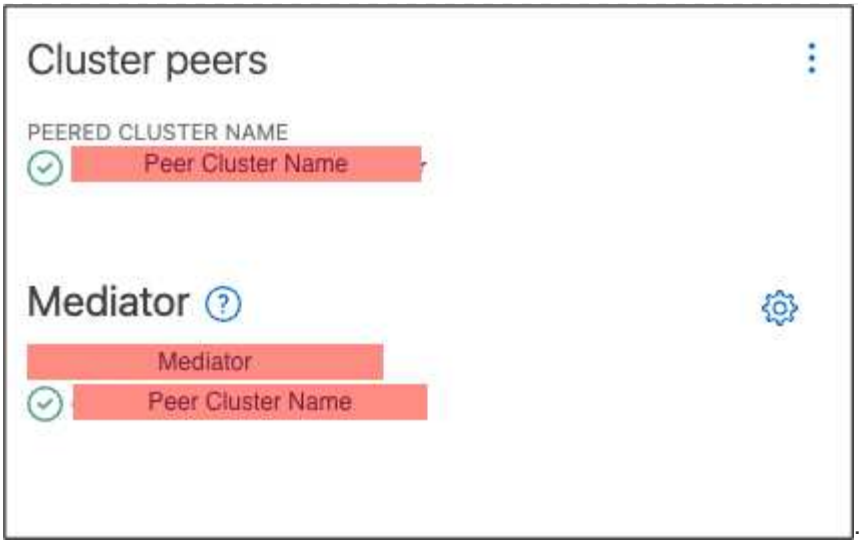
1. Navigieren Sie zu **Schutz > Übersicht > Mediator > Konfigurieren**.
2. Wählen Sie **Hinzufügen** und geben Sie die folgenden ONTAP Mediator-Informationen ein:
   - IPv4-Adresse
   - Benutzername
   - Passwort
   - Zertifikat
3. Sie können die Zertifikateingabe auf zwei Arten bereitstellen:
   - **Option (A)**: Wählen Sie **Import**, um zur `intermediate.crt` Datei zu navigieren und sie zu importieren.
   - **Option (b)**: Kopieren Sie den Inhalt der `intermediate.crt` Datei und fügen Sie ihn in das Feld **Zertifikat** ein.

     Wenn alle Details korrekt eingegeben wurden, wird das bereitgestellte Zertifikat auf allen Peer-Clustern installiert.



Wenn das Hinzufügen des Zertifikats abgeschlossen ist, wird ONTAP Mediator zum ONTAP-Cluster hinzugefügt.

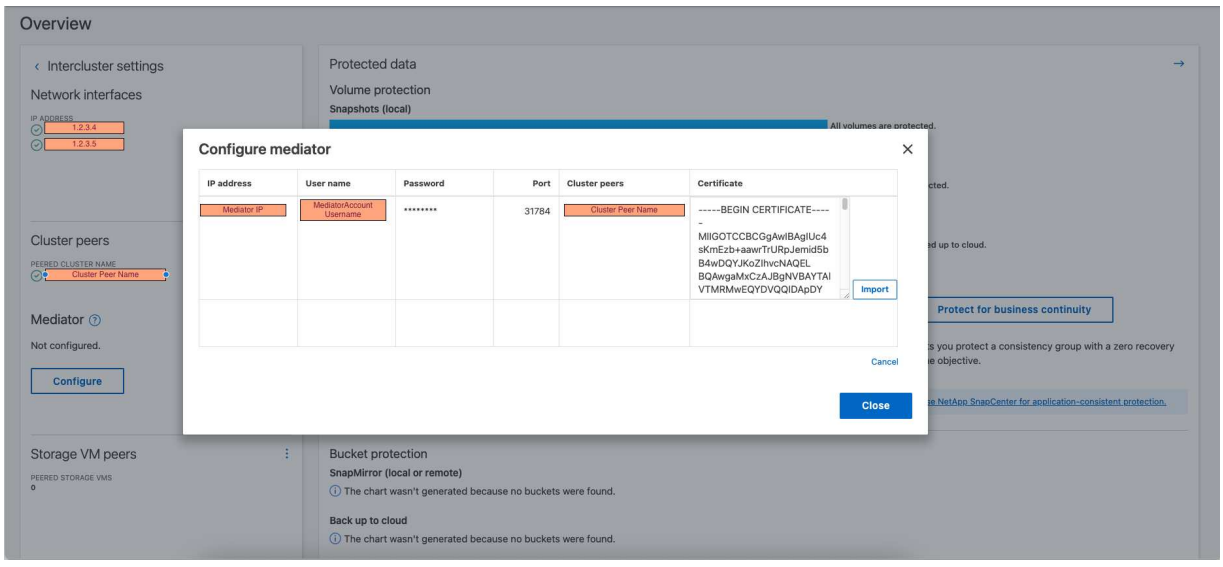
Die folgende Abbildung zeigt eine erfolgreiche ONTAP Mediator-Konfiguration:



ONTAP Mediator 1.8 und früher

1. Navigieren Sie zu **Schutz > Übersicht > Mediator > Konfigurieren**.
2. Wählen Sie **Hinzufügen** und geben Sie die folgenden ONTAP Mediator-Informationen ein:
   - IPv4-Adresse
   - Benutzername
   - Passwort
   - Zertifikat
3. Sie können die Zertifikateingabe auf zwei Arten bereitstellen:
   - **Option (A)**: Wählen Sie **Import**, um zur `ca.crt` Datei zu navigieren und sie zu importieren.
   - **Option (b)**: Kopieren Sie den Inhalt der `ca.crt` Datei und fügen Sie ihn in das Feld **Zertifikat** ein.

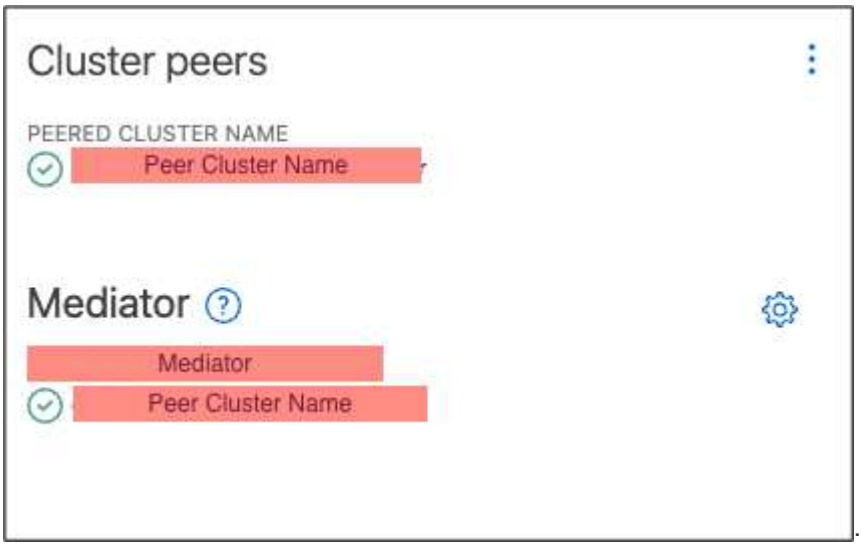
     Wenn alle Details korrekt eingegeben wurden, wird das bereitgestellte Zertifikat auf allen Peer-Clustern installiert.



Wenn das Hinzufügen des Zertifikats abgeschlossen ist, wird ONTAP Mediator zum ONTAP-

Cluster hinzugefügt.

Die folgende Abbildung zeigt eine erfolgreiche ONTAP Mediator-Konfiguration:



CLI

Sie können ONTAP Mediator entweder vom primären oder sekundären Cluster aus über die ONTAP CLI initialisieren. Wenn Sie den `mediator add` Befehl auf einem Cluster, ONTAP Mediator wird automatisch auf dem anderen Cluster hinzugefügt.

Bei Verwendung von ONTAP Mediator zur Überwachung einer SnapMirror Active-Sync-Beziehung kann ONTAP Mediator in ONTAP nicht ohne ein gültiges selbstsigniertes oder CA-Zertifikat initialisiert werden. Sie fügen dem Zertifikatspeicher für Peered-Cluster ein gültiges Zertifikat hinzu. Bei Verwendung von ONTAP Mediator zur Überwachung von MetroCluster-IP-Systemen wird HTTPS nach der Erstkonfiguration nicht mehr verwendet; daher sind keine Zertifikate erforderlich.

ONTAP Mediator 1.9 und höher

1. Finden Sie das ONTAP Mediator CA-Zertifikat im Installationsverzeichnis der ONTAP Mediator Linux VM/Host-Software `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Fügen Sie dem Zertifikatspeicher im Peering-Cluster eine gültige Zertifizierungsstelle hinzu.

   Beispiel:

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. Fügen Sie das ONTAP Mediator CA-Zertifikat zu einem ONTAP-Cluster hinzu. Geben Sie bei der entsprechenden Aufforderung das von ONTAP Mediator erhaltene CA-Zertifikat ein. Wiederholen Sie die Schritte auf allen Peer-Clustern:

   ```
   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 intermediate.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. Zeigen Sie das selbstsignierte Zertifizierungsstellenzertifikat an, das unter Verwendung des generierten Namens des Zertifikats installiert wurde:

   `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. Initialisieren Sie ONTAP Mediator auf einem der Cluster. ONTAP Mediator wird automatisch für den anderen Cluster 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. Prüfen Sie optional den Job-ID-Status `job show -id`, um zu überprüfen, ob der Befehl SnapMirror Mediator add erfolgreich ausgeführt wurde.

   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. Überprüfen Sie den Status der ONTAP Mediatorkonfiguration:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` zeigt 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. Finden Sie das ONTAP Mediator CA-Zertifikat im Installationsverzeichnis der ONTAP Mediator Linux VM/Host-Software `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Fügen Sie dem Zertifikatspeicher im Peering-Cluster eine gültige Zertifizierungsstelle hinzu.

   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, legen Sie das vom ONTAP Mediator erhaltene Zertifizierungsstellenzertifikat ein. Wiederholen Sie die Schritte auf allen Peer-Clustern:

   ```
   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. Zeigen Sie das selbstsignierte Zertifizierungsstellenzertifikat an, das unter Verwendung des generierten Namens des Zertifikats installiert wurde:

   `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. Initialisieren Sie ONTAP Mediator auf einem der Cluster. ONTAP Mediator wird automatisch für den anderen Cluster 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. Prüfen Sie optional den Job-ID-Status `job show -id`, um zu überprüfen, ob der Befehl SnapMirror Mediator add erfolgreich ausgeführt wurde.

   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. Überprüfen Sie den Status der ONTAP Mediatorkonfiguration:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` zeigt 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 müssen Sie ONTAP Mediator neu initialisieren. Es kann Situationen geben, die eine Neuinitialisierung von ONTAP Mediator erfordern, z. B. eine Änderung der ONTAP Mediator-IP-Adresse, ein abgelaufenes Zertifikat usw.

Das folgende Verfahren veranschaulicht die Neuinitialisierung von ONTAP Mediator für einen bestimmten Fall, wenn ein selbst signiertes Zertifikat durch ein Zertifikat eines Drittanbieters ersetzt werden muss.

Über diese Aufgabe

Sie müssen die selbstsignierten Zertifikate des SnapMirror Active Sync-Clusters durch Zertifikate von Drittanbietern ersetzen, die ONTAP Mediator-Konfiguration von ONTAP entfernen und dann ONTAP Mediator hinzufügen.

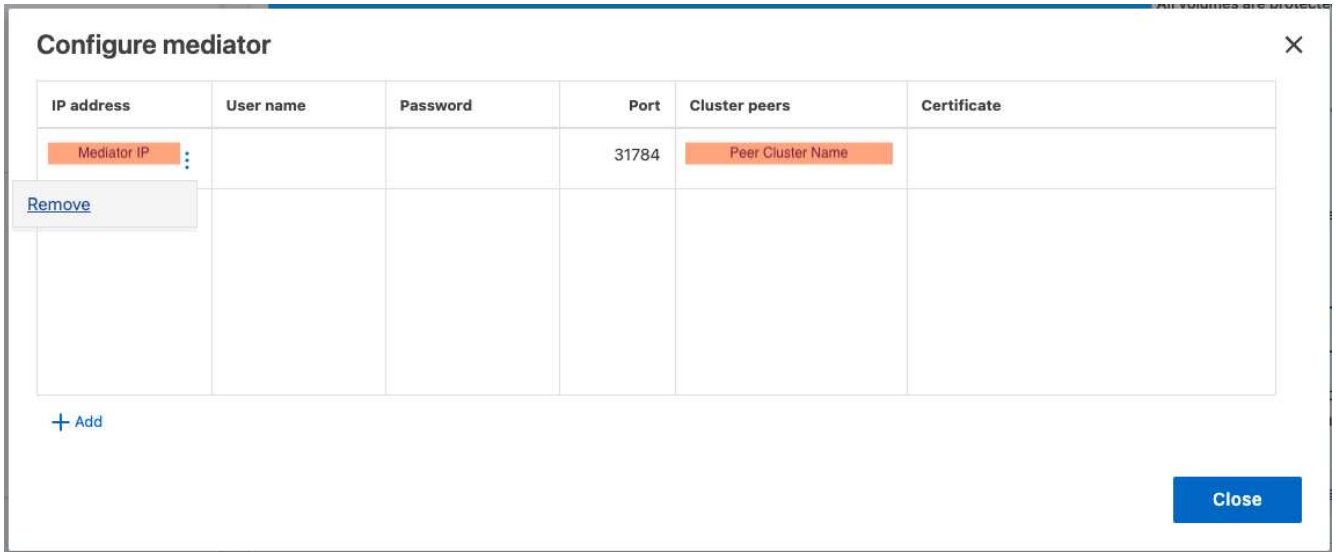
System Manager

Mit System Manager müssen Sie die mit dem alten selbstsignierten Zertifikat konfigurierte ONTAP Mediator-Version aus dem ONTAP-Cluster entfernen und den ONTAP-Cluster mit dem neuen Drittanbieterzertifikat neu konfigurieren.

Schritte

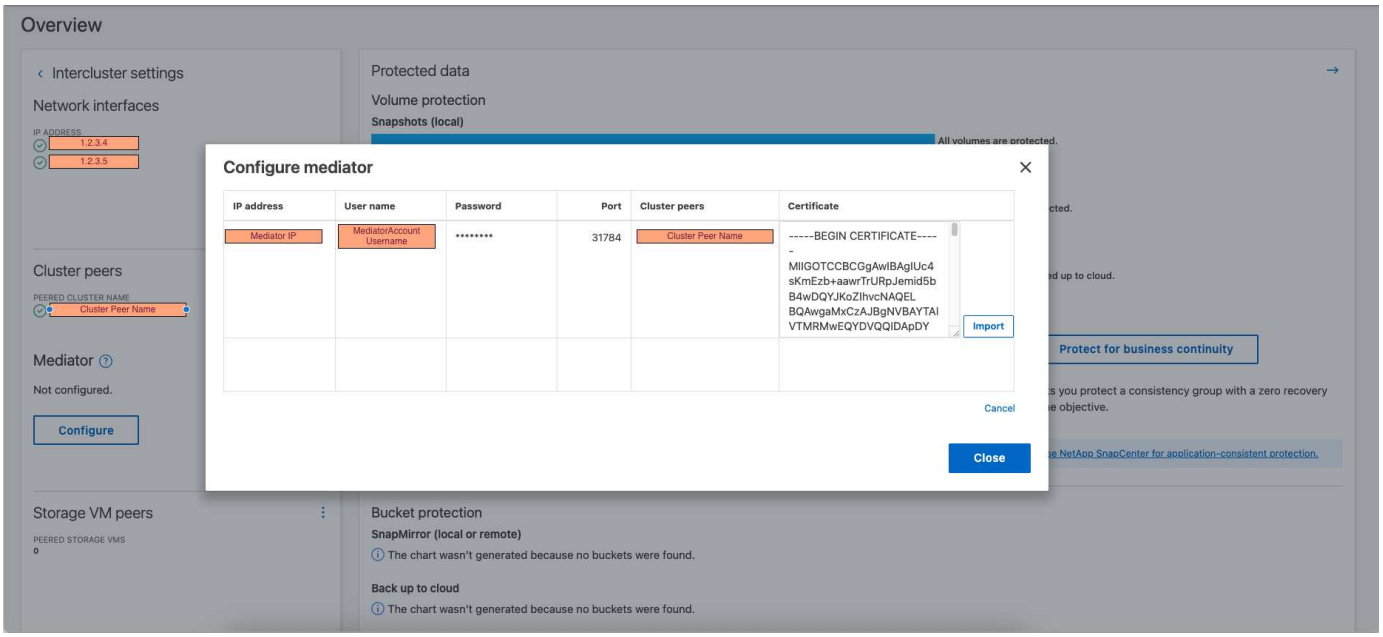
1. Wählen Sie das Menüoptionensymbol und wählen Sie **Entfernen**, um ONTAP Mediator zu entfernen.

> Mit diesem Schritt wird die selbstsignierte Server-Ca nicht aus dem ONTAP-Cluster entfernt. NetApp empfiehlt, die Registerkarte **Zertifikat** zu öffnen und sie manuell zu entfernen, bevor Sie den nächsten Schritt unten ausführen, um ein Zertifikat eines Drittanbieters hinzuzufügen:



2. Fügen Sie ONTAP Mediator erneut mit dem richtigen Zertifikat hinzu.

ONTAP Mediator ist jetzt mit dem neuen selbstsignierten Zertifikat eines Drittanbieters konfiguriert.



CLI

Sie können ONTAP Mediator entweder vom primären oder sekundären Cluster aus neu initialisieren, indem Sie die ONTAP CLI verwenden, um das selbstsignierte Zertifikat durch das Drittanbieterzertifikat zu ersetzen.

ONTAP Mediator 1.9 und höher

1. Entfernen Sie die `intermediate.crt` zuvor selbst signierte Installation, wenn Sie selbstsignierte Zertifikate für alle Cluster verwendet haben. 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. Entfernen Sie den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror Active Sync Cluster mit `-force true`:

   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. Anweisungen zum Abrufen von Zertifikaten von einer untergeordneten Zertifizierungsstelle finden Sie `intermediate.crt` in den unter beschriebenen Schritten"Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern". Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern

Der `intermediate.crt` verfügt über bestimmte Eigenschaften, die er von der Anforderung ableitet, die an die in der Datei definierte PKI-Autorität gesendet werden muss `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Fügen Sie das neue ONTAP Mediator-CA-Zertifikat `intermediate.crt` eines Drittanbieters über den Installationsort für 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. Fügen Sie die `intermediate.crt` Datei dem Peering-Cluster hinzu. Wiederholen Sie diesen Schritt für alle Peer-Cluster:

   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. Entfernen Sie den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror Active Sync Cluster:

   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. Fügen Sie ONTAP Mediator erneut hinzu:

   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 Beziehungen der SnapMirror-Konsistenzgruppe mit dem Mediator synchronisiert sind; ein Status von `true` zeigt eine erfolgreiche Synchronisierung an.

ONTAP Mediator 1.8 und früher

1. Entfernen Sie die `ca.crt` zuvor selbst signierte Installation, wenn Sie selbstsignierte Zertifikate für alle Cluster verwendet haben. 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. Entfernen Sie den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror Active Sync Cluster mit `-force true`:

   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. Anweisungen zum Abrufen von Zertifikaten von einer untergeordneten Zertifizierungsstelle finden Sie `ca.crt` in den unter beschriebenen Schritten"Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern". Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern

   > Der `ca.crt` verfügt über bestimmte Eigenschaften, die er von der Anforderung ableitet, die an die in der Datei definierte PKI-Autorität gesendet werden muss `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Fügen Sie das neue ONTAP Mediator-CA-Zertifikat `ca.crt` eines Drittanbieters über den Installationsort für 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. Fügen Sie die `intermediate.crt` Datei dem Peering-Cluster hinzu. Wiederholen Sie diesen Schritt für alle Peer-Cluster:

   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. Entfernen Sie den zuvor konfigurierten ONTAP Mediator aus dem SnapMirror Active Sync Cluster:

   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. Fügen Sie ONTAP Mediator erneut hinzu:

   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 Beziehungen der SnapMirror-Konsistenzgruppe mit dem Mediator synchronisiert sind; ein Status von `true` zeigt eine erfolgreiche Synchronisierung an.

Verwandte Informationen

- "Jobanzeigen"
- "Sicherheitszertifikat löschen"
- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "SnapMirror Mediator hinzufügen"
- "SnapMirror Mediator entfernen"
- "Snapmirror Mediator-Show"

Vorbereiten der Konfiguration von ONTAP Cloud Mediator

Bevor Sie "ONTAP Cloud Mediator konfigurieren" müssen Sie sicherstellen, dass die Voraussetzungen erfüllt sind.

Anforderungen an die Firewall

Die Firewall-Einstellung auf dem Domänencontroller muss HTTPS-Verkehr zulassen `api.bluexp.netapp.com` aus beiden Clustern.

Proxyserver-Anforderungen

Wenn Sie Proxyserver für SnapMirror Active Sync verwenden, stellen Sie sicher, dass die Proxyserver erstellt wurden und Sie über die folgenden Proxyserverinformationen verfügen:

- HTTPS-Proxy-IP
- Port
- Benutzername
- Passwort

Latenz

Die empfohlene Ping-Latenz zwischen dem NetApp Console-Cloud-Server und den SnapMirror Active Sync-Cluster-Peers beträgt weniger als 200 ms.

Stammzertifizierungsstellenzertifikate

Überprüfen des Clusters auf Zertifikate

ONTAP wird mit vorinstallierten bekannten Root-CA-Zertifikaten geliefert, sodass Sie in den meisten Fällen das Root-CA-Zertifikat des NetApp Console-Servers nicht installieren müssen. Bevor Sie mit der Konfiguration des ONTAP Cloud Mediators beginnen, können Sie den Cluster überprüfen, um sicherzustellen, dass die Zertifikate vorhanden sind:

Beispiel:

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
```

```
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

Proxyserver auf installierte Zertifikate prüfen

Wenn Sie einen Proxy verwenden, um eine Verbindung zum ONTAP Cloud Mediator-Dienst in der NetApp Konsole herzustellen, stellen Sie sicher, dass die Stamm-CA-Zertifikate des Proxyservers in ONTAP installiert sind:

Beispiel:

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

Laden Sie das CA-Zertifikat herunter:

Bei Bedarf können Sie die Root-CA-Zertifikate von der Website der Zertifizierungsstelle herunterladen und auf den Clustern installieren.

Beispiel:

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

Konfigurieren Sie den ONTAP Cloud Mediator für SnapMirror Active Sync

Ab ONTAP 9.17.1 können Sie mit ONTAP Cloud Mediator die Geschäftskontinuität gewährleisten, indem Sie den Zustand jedes Clusters überwachen. ONTAP Cloud Mediator ist ein Cloud-basierter Dienst. Wenn Sie ONTAP Cloud Mediator mit SnapMirror Active Sync verwenden, müssen Sie zunächst bestätigen, dass die NetApp -Konsolendienste und Clientinformationen konfiguriert sind, und ein ordnungsgemäßes Cluster-Peering sicherstellen.

Wie ONTAP Mediator bietet ONTAP Cloud Mediator einen persistenten und abgeschirmten Speicher für Hochverfügbarkeitsmetadaten (HA), die von den ONTAP Clustern in einer SnapMirror Active-Sync-Beziehung verwendet werden. ONTAP Cloud Mediator bietet eine synchrone Knotenzustandsabfragefunktion zur Unterstützung der Quorum-Bestimmung und dient als Ping-Proxy zur Controller-Aktivitätserkennung.

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** im"Versionshinweise zu ONTAP" für wichtige Informationen zu diesen Konfigurationen.

Bevor Sie beginnen

Bevor Sie ONTAP Cloud Mediator konfigurieren, sollten Sie die folgenden Informationen bestätigen:

- Der Cluster ist konfiguriert.

  "Konfigurieren Sie ONTAP -Cluster für SnapMirror Active Sync"

- Sie haben Ihre NetApp Console-Organisations-ID aus der NetApp Console kopiert und ein Console-Mitgliedsdienstkonto erstellt, das Sie bei der Konfiguration von ONTAP Cloud Mediator verwenden können. Beim Erstellen des Dienstkontos muss die Organisation auf das Abonnement eingestellt sein, in dem Sie ONTAP Cloud Mediator konfiguriert haben. Die Kategorie muss auf „Anwendung“ und der Rollentyp auf „ONTAP Mediator Setup-Rolle“ eingestellt sein. Sie müssen die Client-ID und das Client-Geheimnis beim Erstellen der Rolle speichern.

  "NetApp Konsolenmitglieder und Dienstkonten hinzufügen"

Schritte

Sie können ONTAP Cloud Mediator mithilfe von System Manager oder der ONTAP CLI hinzufügen.

System Manager

1. Navigieren Sie zu **Schutz > Übersicht > Mediator** und wählen Sie **Hinzufügen**.
2. Wählen Sie im Fenster **Mediator hinzufügen** als Mediatortyp **Cloud** aus und geben Sie die folgenden Informationen ein:
   - NetApp Console-Organisations-ID
   - NetApp -Konsolen-Client-ID
   - NetApp Console-Client-Geheimnis
3. Wählen Sie den Cluster-Peer aus.
4. Wenn Sie einen HTTP-Proxy verwenden und dieser noch nicht konfiguriert ist, geben Sie die HTTP-Proxy-Informationen für die lokalen und Remote-Hosts ein.

   Es wird empfohlen, für jeden Cluster-Peer einen anderen Proxyserver zu verwenden.
5. Optional: Wenn in ONTAP ein Stamm-CA-Zertifikat installiert werden muss, insbesondere bei Verwendung eines Proxyservers, fügen Sie das Zertifikat in das bereitgestellte Textfeld ein.
6. Wählen Sie **Hinzufügen**.
7. Navigieren Sie zu **Schutz > Übersicht** und überprüfen Sie den Status der Beziehung zwischen den SnapMirror Active Sync-Clustern und ONTAP Cloud Mediator.

CLI

1. Konfigurieren Sie ONTAP Cloud Mediator:
   `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. Überprüfen Sie den Status des ONTAP Cloud Mediators:
   `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
```

Schützen Sie sich mit ONTAP SnapMirror Active Sync

SnapMirror Active Sync bietet asymmetrischen Schutz und ab ONTAP 9.15.1 symmetrischen aktiv/aktiv-Schutz.

Konfigurieren Sie den asymmetrischen Schutz

Bei der Konfiguration von asymmetrischem Schutz mithilfe von SnapMirror Active Sync müssen LUNs auf dem ONTAP Quell-Cluster ausgewählt und einer Konsistenzgruppe hinzugefügt werden.

Bevor Sie beginnen

- Sie müssen über eine synchrone SnapMirror Lizenz verfügen.
- Sie müssen ein Cluster- oder Storage-VM-Administrator sein.
- Alle zusammengehörigen Volumes einer Konsistenzgruppe müssen sich in einer einzelnen Storage VM (SVM) befinden.
  - LUNs können auf verschiedenen Volumes residieren.
- Das Quell- und Ziel-Cluster kann nicht identisch sein.
- Sie können keine Beziehungen zu SnapMirror aktiven synchronen Konsistenzgruppen über ASA-Cluster und nicht-ASA-Cluster hinweg aufbauen.
- Der standardmäßige IPspace wird von der aktiven SnapMirror Synchronisierung für Cluster-Peer-Beziehungen benötigt. Benutzerdefinierter IPspace wird nicht unterstützt.
- Der Name der Konsistenzgruppe muss eindeutig sein.
- Die Volumes auf dem sekundären (Ziel-) Cluster müssen den Typ DP aufweisen.
- Die primären und sekundären SVMs müssen in einer Peering-Beziehung vorliegen.

Schritte

Sie können eine Konsistenzgruppe mithilfe der ONTAP CLI oder von System Manager konfigurieren.

Ab ONTAP 9.10.1 bietet ONTAP einen Consistency Group-Endpunkt und ein Menü im System Manager mit zusätzlichen Verwaltungsdienstprogrammen. Wenn Sie ONTAP 9.10.1 oder höher verwenden, lesen Sie "Konfigurieren einer Konsistenzgruppe" Dann "Schutz konfigurieren" um eine SnapMirror Active-Sync-Beziehung zu erstellen.

> Von ONTAP 9.14.1 bis 9.8 wird SnapMirror Active Sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

System Manager

1. Navigieren Sie im primären Cluster zu **Schutz > Übersicht > Schutz für Business Continuity > LUNs schützen**.
2. Wählen Sie die zu schützenden LUNs aus, und fügen Sie sie einer Schutzgruppe hinzu.
3. Wählen Sie das Ziel-Cluster und die SVM aus.
4. **Initialize Relationship** ist standardmäßig ausgewählt. Klicken Sie auf **Speichern**, um den Schutz zu starten.
5. Gehen Sie zu **Dashboard > Performance**, um die IOPS-Aktivität für die LUNs zu überprüfen.
6. Verwenden Sie auf dem Ziel-Cluster System Manager, um zu überprüfen, ob der Schutz für die Business Continuity-Beziehung synchron ist: **Schutz > Beziehungen**.

CLI

1. Erstellen einer Konsistenzgruppenbeziehung vom Ziel-Cluster
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   Mit dem `cg-item-mappings` Parameter `snapmirror create` im Befehl können Sie bis zu 12 zusammengehörige Volumes zuordnen.

   Im folgenden Beispiel werden zwei Konsistenzgruppen erstellt: `cg_src_ on the source with` `vol1` Und `vol2` eine Konsistenzgruppe mit einem gespiegelten 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. Initialisieren Sie vom Ziel-Cluster die Konsistenzgruppe.

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. Bestätigen Sie, dass der Initialisierungsvorgang erfolgreich abgeschlossen wurde. Der Status sollte sein `InSync`.

   ```
   snapmirror show
   ```

4. Erstellen Sie auf jedem Cluster eine Initiatorgruppe, damit Sie dem Initiator auf dem Applikations-Host LUNs zuordnen können.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*

   Erfahren Sie mehr über `lun igroup create` in der "ONTAP-Befehlsreferenz".

5. Ordnen Sie auf jedem Cluster LUNs der Initiatorgruppe zu:

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. Überprüfen Sie mit dem `lun map` Befehl, ob die LUN-Zuordnung erfolgreich abgeschlossen wurde. Anschließend können Sie die neuen LUNs auf dem Anwendungshost ermitteln.

Symmetrischer aktiv/aktiv-Schutz konfigurieren

Sie können symmetrischen Schutz mit System Manager oder der ONTAP CLI einrichten. In beiden Schnittstellen gibt es verschiedene Schritte für Einheitliche und nicht einheitliche Konfigurationen.

Bevor Sie beginnen

- Auf beiden Clustern muss ONTAP 9.15.1 oder höher ausgeführt werden.
- Symmetrische aktiv/aktiv-Konfigurationen erfordern die `AutomatedFailoverDuplex` Schutzrichtlinie. Alternativ können Sie Individuelle SnapMirror-Richtlinie erstellenden `-type` IS zur Verfügung stellen `automated-failover-duplex`.
- In ONTAP 9.15.1 werden symmetrische aktiv/aktiv-Systeme nur bei Clustern mit 2 Nodes unterstützt.
- Ab ONTAP 9.16.1 GA unterstützt SnapMirror Active Sync symmetrische aktiv/aktiv-Konfigurationen auf Clustern mit vier Nodes.
  - Um SnapMirror Active Sync auf einem Cluster mit vier Nodes zu verwenden, muss ONTAP 9.16.1 GA oder höher ausgeführt werden.
  - Bevor Sie eine Konfiguration mit vier Nodes bereitstellen, müssen Sie Cluster Peer-Beziehung erstellen.
  - Überprüfen Sie die Begrenzungen für Cluster mit vier Nodes.
  - Wenn Sie zu einem Cluster mit zwei Nodes zurückkehren, müssen Sie die aktiven synchronen SnapMirror-Beziehungen aus dem Cluster entfernen, bevor Sie zurückkehren.
  - Sie können die Konfiguration mit vier Nodes zum Upgrade von Storage und Controllern verwenden. Dieser Vorgang läuft unterbrechungsfrei ab und erweitert das Cluster, während Volumes in die neuen Nodes verschoben werden. Weitere Informationen finden Sie unter "Aktualisieren eines Clusters".
- Ab ONTAP 9.17.1 können Sie symmetrischen Aktiv/Aktiv-Schutz auf NVMe-Namespaces nur konfigurieren, wenn auf beiden Clustern ONTAP 9.17.1 oder höher ausgeführt wird.

Konfigurieren Sie symmetrischen Aktiv/Aktiv-Schutz mithilfe einer SCSI SnapMirror Active Sync-Konfiguration

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um symmetrischen Aktiv/Aktiv-Schutz mithilfe von SCSI-Protokoll-Hostzuordnungen zu konfigurieren.

System Manager

Schritte für eine einheitliche Konfiguration

1. Am primären Standort "Erstellen Sie mithilfe der neuen LUNs eine Konsistenzgruppe."
   a. Geben Sie beim Erstellen der Konsistenzgruppe Host-Initiatoren an, um Initiatorgruppen zu erstellen.
   b. Aktivieren Sie das Kontrollkästchen **SnapMirror aktivieren**, und wählen Sie dann die `AutomatedFailoverDuplex` Richtlinie aus.
   c. Aktivieren Sie im daraufhin angezeigten Dialogfeld das Kontrollkästchen **Initiatorgruppen replizieren**, um Initiatorgruppen zu replizieren. Legen Sie in **Annäherungseinstellungen bearbeiten** proximale SVMs für Ihre Hosts fest.
   d. Wählen Sie **Speichern**.

Schritte für eine nicht einheitliche Konfiguration

1. Am primären Standort "Erstellen Sie mithilfe der neuen LUNs eine Konsistenzgruppe."
   a. Geben Sie beim Erstellen der Konsistenzgruppe Host-Initiatoren an, um Initiatorgruppen zu erstellen.
   b. Aktivieren Sie das Kontrollkästchen **SnapMirror aktivieren**, und wählen Sie dann die `AutomatedFailoverDuplex` Richtlinie aus.
   c. Wählen Sie **Speichern**, um die LUNs, Konsistenzgruppe, Initiatorgruppe, SnapMirror Beziehung und igroup-Zuordnung zu erstellen.
2. Erstellen Sie am sekundären Standort eine Initiatorgruppe und ordnen Sie die LUNs zu.
   a. Navigieren Sie zu **Hosts** > **SAN-Initiatorgruppen**.
   b. Wählen Sie **+Add**, um eine neue Initiatorgruppe zu erstellen.
   c. Geben Sie einen **Namen** ein, wählen Sie das **Host-Betriebssystem** und dann **Initiator Group Members**.
   d. Wählen Sie **Speichern**, um die Beziehung zu initialisieren.
3. Ordnen Sie die neue Initiatorgruppe den Ziel-LUNs zu.
   a. Navigieren Sie zu **Storage** > **LUNs**.
   b. Wählen Sie alle LUNs aus, die der Initiatorgruppe zugeordnet werden sollen.
   c. Wählen Sie **Mehr** und dann **Initiatorgruppen zuordnen**.

CLI

Schritte für eine einheitliche Konfiguration

1. Erstellen einer neuen SnapMirror Beziehung, bei der alle Volumes in der Applikation gruppiert werden. Stellen Sie sicher, dass Sie die `AutomatedFailOverDuplex` Richtlinie für die bidirektionale synchrone Replikation festlegen.

   ```
   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 und 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. Initialisieren Sie die SnapMirror-Beziehung:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. Bestätigen Sie, dass der Vorgang erfolgreich `Mirrored State` `SnapMirrored` `Relationship Status` `Insync` war, indem Sie darauf warten, dass die als und die AS angezeigt werden.

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

4. Konfigurieren Sie auf Ihrem Host die Host-Konnektivität mit Zugriff auf die einzelnen Cluster entsprechend Ihren Anforderungen.
5. Richten Sie die igroup-Konfiguration ein. Legen Sie die bevorzugten Pfade für Initiatoren auf dem lokalen Cluster fest. Geben Sie die Option zum Replizieren der Konfiguration auf das Peer-Cluster für die umgekehrte Affinität an.

   ```
   SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
   <igroup_name> -replication-peer <peer_svm_name> -initiator <host>
   ```

   > Ab ONTAP 9.16.1 verwenden Sie den `-proximal-vserver local` Parameter in diesem Befehl.

   ```
   SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
   <os_type> -initiator <host>
   ```

   > Ab ONTAP 9.16.1 verwenden Sie den `-proximal-vserver peer` Parameter in diesem Befehl.

6. Ermitteln Sie vom Host aus die Pfade und überprüfen Sie, ob die Hosts über einen aktiven/optimierten Pfad zur Storage-LUN vom bevorzugten Cluster verfügen.
7. Implementieren Sie die Applikation und verteilen Sie die VM Workloads über Cluster, um den erforderlichen Lastausgleich zu erreichen.

Schritte für eine nicht einheitliche Konfiguration

1. Erstellen einer neuen SnapMirror Beziehung, bei der alle Volumes in der Applikation gruppiert werden. Stellen Sie sicher, dass Sie die `AutomatedFailOverDuplex` Richtlinie für die bidirektionale synchrone Replikation festlegen.

   ```
   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 und 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. Initialisieren Sie die SnapMirror-Beziehung:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. Bestätigen Sie, dass der Vorgang erfolgreich `Mirrored State` `SnapMirrored` `Relationship Status` `Insync` war, indem Sie darauf warten, dass die als und die AS angezeigt werden.

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

4. Konfigurieren Sie auf Ihrem Host die Host-Konnektivität mit Zugriff auf die einzelnen Cluster entsprechend Ihren Anforderungen.
5. Legen Sie die igroup-Konfigurationen auf den Quell- und Ziel-Clustern fest.

   ```
   # 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. Ermitteln Sie vom Host aus die Pfade und überprüfen Sie, ob die Hosts über einen aktiven/optimierten Pfad zur Storage-LUN vom bevorzugten Cluster verfügen.
7. Implementieren Sie die Applikation und verteilen Sie die VM Workloads über Cluster, um den erforderlichen Lastausgleich zu erreichen.

Konfigurieren Sie symmetrischen Aktiv/Aktiv-Schutz mithilfe einer NVMe SnapMirror Active Sync-Konfiguration

Bevor Sie beginnen

Zusätzlich zu den Anforderungen für die Konfiguration des symmetrischen Aktiv/Aktiv-Schutzes sollten Sie sich über die unterstützten und nicht unterstützten Konfigurationen bei der Verwendung des NVMe-Protokolls im Klaren sein.

- Konsistenzgruppen können ein oder mehrere Subsysteme haben.
- Volumes innerhalb der Konsistenzgruppe können Namespace-Zuordnungen von mehreren Subsystemen haben.
- Subsysteme können keine Namespace-Zuordnungen haben, die zu mehr als einer Konsistenzgruppe gehören.
- Subsysteme können nicht über Namespace-Zuordnungen verfügen, die zu einer Konsistenzgruppe gehören, und über Namespace-Zuordnungen, die nicht zu einer Konsistenzgruppe gehören.
- Subsysteme müssen über Namespace-Zuordnungen verfügen, die Teil derselben Konsistenzgruppe sind.

Schritte

Ab ONTAP 9.17.1 können Sie mit System Manager oder der ONTAP CLI eine Konsistenzgruppe erstellen und

symmetrischen Aktiv/Aktiv-Schutz mithilfe von NVMe-Protokoll-Host-Mappings konfigurieren.

System Manager

1. Auf der primären Site "Erstellen Sie eine Konsistenzgruppe mit neuen Volumes oder NVMe-Namespaces."
2. Wählen Sie **+Hinzufügen** und wählen Sie **Neue NVMe-Namespaces verwenden**.
3. Geben Sie den Namen der Konsistenzgruppe ein.
4. Wählen Sie **Mehr**.
5. Wählen Sie im Abschnitt **Schutz** die Option * SnapMirror aktivieren* und anschließend die `AutomatedFailoverDuplex` Politik.
6. Wählen Sie im Abschnitt **Host-Zuordnung** entweder **Vorhandenes NVMe-Subsystem** oder **Neues NVMe-Subsystem**.
7. Wählen Sie **In der Nähe von**, um das proximale SVM zu ändern. Das Quell-SVM ist standardmäßig ausgewählt.
8. Fügen Sie bei Bedarf ein weiteres NVMe-Subsystem hinzu.

CLI

1. Erstellen Sie eine neue SnapMirror Beziehung, die alle Volumes gruppiert, die alle von der Anwendung verwendeten NVMe-Namespaces enthalten. Stellen Sie sicher, dass Sie Folgendes festlegen: `AutomatedFailOverDuplex` Richtlinie zum Einrichten einer bidirektionalen synchronen Replikation.

   ```
   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. Initialisieren Sie die SnapMirror-Beziehung:
   `snapmirror initialize -destination-path <destination-consistency-group>`

   Beispiel:

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. Bestätigen Sie, dass der Vorgang erfolgreich `Mirrored State` `SnapMirrored` `Relationship Status` `Insync` war, indem Sie darauf warten, dass die als und die AS angezeigt werden.

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

   Die mit den NVMe-Namespaces in den primären Volumes verknüpften NVMe-Subsysteme werden automatisch in den sekundären Cluster repliziert.

4. Konfigurieren Sie auf Ihrem Host die Host-Konnektivität mit Zugriff auf die einzelnen Cluster entsprechend Ihren Anforderungen.
5. Geben Sie den SVM an, der sich in der Nähe Ihrer Hosts befindet. Dies ermöglicht dem Host den Zugriff auf den NVMe-Namespace über einen Pfad vom bevorzugten Cluster. Dies kann der SVM im primären Cluster oder im DR-Cluster sein.

   Der folgende Befehl gibt an, dass SVM VS_A proximal zu Host H1 ist und legt VS_A als proximalen SVM fest:

   ```
   SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
   -proximal-vservers <VS_A>
   ```

   Der folgende Befehl gibt an, dass SVM VS_B proximal zu Host H2 ist und legt VS_B als proximalen SVM fest:

   ```
   SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
   -proximal-vservers <VS_B>
   ```

6. Ermitteln Sie vom Host aus die Pfade und überprüfen Sie, ob die Hosts über einen aktiven/optimierten Pfad zum Speicher vom bevorzugten Cluster verfügen.
7. Implementieren Sie die Applikation und verteilen Sie die VM Workloads über Cluster, um den erforderlichen Lastausgleich zu erreichen.

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror Initialisierung"
- "Snapmirror-Show"

Konvertieren Sie eine vorhandene ONTAP SnapMirror -Beziehung in eine SnapMirror Active Sync-Beziehung

Wenn Sie SnapMirror-Schutz konfiguriert haben, können Sie die Beziehung zu SnapMirror Active Sync konvertieren. Ab ONTAP 9.15.1 können Sie die Beziehung in symmetrischen aktiv/aktiv-Schutz konvertieren.

Konvertieren Sie eine vorhandene iSCSI- oder FC- SnapMirror Beziehung in eine asymmetrische SnapMirror Active-Sync-Beziehung

Wenn zwischen Quell- und Zielcluster eine bestehende iSCSI- oder FC- SnapMirror -synchrone Beziehung besteht, können Sie diese in eine asymmetrische SnapMirror Active-Sync-Beziehung umwandeln. Dadurch können Sie die gespiegelten Volumes einer Konsistenzgruppe zuordnen und so einen RPO von null bei einem Multi-Volume-Workload sicherstellen. Darüber hinaus können Sie vorhandene SnapMirror -Snapshots beibehalten, falls Sie zu einem Zeitpunkt vor dem Aufbau der SnapMirror -Active-Sync-Beziehung zurückkehren müssen.

Über diese Aufgabe

- Sie müssen ein Cluster- und SVM-Administrator auf den primären und sekundären Clustern sein.
- Sie können keine RPO von null auf ein RTO von null konvertieren, indem Sie die SnapMirror Richtlinie ändern.
- Sie müssen sicherstellen, dass die LUNs nicht zugeordnet sind, bevor Sie den `snapmirror create`

Befehl ausgeben.

Wenn die vorhandenen LUNs auf dem sekundären Volume zugeordnet sind und die `AutomatedFailover` Richtlinie konfiguriert ist, `snapmirror create` löst der Befehl einen Fehler aus.

Bevor Sie beginnen

- Zwischen dem primären und sekundären Cluster muss eine synchrone SnapMirror -Beziehung mit Null-RPO bestehen.
- Die Zuordnung aller LUNs auf dem Ziel-Volume muss aufgehoben werden, bevor die SnapMirror Beziehung zum RTO von null erstellt werden kann.
- SnapMirror Active Sync unterstützt nur SAN-Protokolle (nicht NFS/CIFS). Stellen Sie sicher, dass für den NAS-Zugriff keine Komponente der Konsistenzgruppe bereitgestellt ist.
- "ONTAP Mediator" muss für die aktive Synchronisierung von SnapMirror konfiguriert sein.

Schritte

1. Führen Sie aus dem sekundären Cluster ein SnapMirror Update der bestehenden Beziehung durch:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Überprüfen Sie, ob das SnapMirror Update erfolgreich abgeschlossen wurde:

   ```
   SiteB::>snapmirror show
   ```

3. Halten Sie jede der synchronen Beziehungen mit einem RPO von null an:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Sie löschen jede der synchronen Beziehungen ohne RPO:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Geben Sie die Quell-SnapMirror-Beziehung frei, behalten Sie aber die gemeinsamen Snapshots bei:

   ```
   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. Synchrone SnapMirror-Beziehung mit einem RTO von null:

   ```
   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. Neusynchronisierung der Konsistenzgruppe:

   ```
   SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. Wiederherstellen aller Pfade zu den LUNs durch erneute Überprüfung der Host-LUN-I/O-Pfade

Konvertieren Sie eine vorhandene iSCSI- oder FC- SnapMirror Beziehung in eine symmetrische Aktiv/Aktiv-Beziehung

Ab ONTAP 9.15.1 können Sie eine vorhandene iSCSI- oder FC- SnapMirror -Beziehung in eine symmetrische Aktiv/Aktiv-Beziehung mit SnapMirror Active Sync konvertieren.

Bevor Sie beginnen

- Sie müssen ONTAP 9.15.1 oder höher ausführen.
- Zwischen dem primären und dem sekundären Cluster muss eine synchrone SnapMirror Beziehung zum RPO von null bestehen.
- Die Zuordnung aller LUNs auf dem Ziel-Volume muss aufgehoben werden, bevor die SnapMirror Beziehung zum RTO von null erstellt werden kann.
- SnapMirror Active Sync unterstützt nur SAN-Protokolle (nicht NFS/CIFS). Stellen Sie sicher, dass für den NAS-Zugriff keine Komponente der Konsistenzgruppe bereitgestellt ist.
- "ONTAP Mediator" muss für die aktive Synchronisierung von SnapMirror konfiguriert sein.

Schritte

1. Führen Sie aus dem sekundären Cluster ein SnapMirror Update der bestehenden Beziehung durch:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Überprüfen Sie, ob das SnapMirror Update erfolgreich abgeschlossen wurde:

   ```
   SiteB::>snapmirror show
   ```

3. Halten Sie jede der synchronen Beziehungen mit einem RPO von null an:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Sie löschen jede der synchronen Beziehungen ohne RPO:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Geben Sie die Quell-SnapMirror-Beziehung frei, behalten Sie aber die gemeinsamen Snapshots bei:

   ```
   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. Erstellen Sie eine synchrone SnapMirror-Beziehung von null RTO mit der Richtlinie für AutoatedFailoverDuplex:

   ```
   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 die vorhandenen Hosts lokal das primäre Cluster sind, fügen Sie den Host zum sekundären Cluster hinzu, und stellen Sie die Verbindung mit dem entsprechenden Zugriff auf jedes Cluster her.
8. Löschen Sie am sekundären Standort die LUN-Zuordnungen der Initiatorgruppen, die Remote-Hosts zugeordnet sind.

   Stellen Sie sicher, dass die Initiatorgruppe keine Zuordnungen für nicht replizierte LUNs enthält.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

9. Ändern Sie am primären Standort die Initiatorkonfiguration für vorhandene Hosts, um den proximalen Pfad für Initiatoren auf dem lokalen Cluster festzulegen.

   ```
   SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
   <host> -proximal-vserver <server>
   ```

10. Fügen Sie eine neue Initiatorgruppe und einen neuen Initiator für die neuen Hosts hinzu und legen Sie die Host-Nähe für die Host-Affinität zu ihrem lokalen Standort fest. Ennable-igroup-Replikation zur Replikation der Konfiguration und Invertierung der Hostlokalität auf dem Remote-Cluster.

    ```
    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/optimierten Pfad zur Storage-LUN vom bevorzugten Cluster verfügen
12. Implementieren Sie die Applikation und verteilen Sie die VM-Workloads über Cluster hinweg.
13. Neusynchronisierung der Konsistenzgruppe:

    ```
    SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
    ```

14. Wiederherstellen aller Pfade zu den LUNs durch erneute Überprüfung der Host-LUN-I/O-Pfade

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror löschen"
- "Snapmirror-Ruhezustand"
- "snapmirror Release"
- "SnapMirror-Neusynchronisierung"
- "Snapmirror-Show"

Konvertieren Sie den aktiven Synchronisierungsbeziehungstyp von ONTAP SnapMirror

Ab ONTAP 9.15.1 können Sie zwischen Typen von SnapMirror Active Sync-Schutz konvertieren: Von asymmetrisch zu symmetrisch aktiv/aktiv und umgekehrt.

Konvertieren in eine symmetrische aktiv/aktiv-Beziehung

Sie können eine aktive Synchronisierungsbeziehung von iSCSI oder FC SnapMirror mit asymmetrischem Schutz in eine symmetrische Aktiv/Aktiv-Verbindung umwandeln.

Bevor Sie beginnen

- Auf beiden Clustern muss ONTAP 9.15.1 oder höher ausgeführt werden.
- Symmetrische aktiv/aktiv-Konfigurationen erfordern die `AutomatedFailoverDuplex` Schutzrichtlinie. Alternativ können Sie Individuelle SnapMirror-Richtlinie erstellenden `-type` IS zur Verfügung stellen `automated-failover-duplex`.

System Manager

Schritte für eine einheitliche Konfiguration

1. Ziel-Initiatorgruppe entfernen:
   a. Navigieren Sie auf dem Zielcluster zu **Hosts** > **SAN-Initiatorgruppen**.
   b. Wählen Sie die Initiatorgruppe mit der SnapMirror Beziehung aus und dann **Löschen**.
   c. Wählen Sie im Dialogfeld das Feld **Zuordnung der zugeordneten LUNs aufheben** und dann **Löschen**.
2. Bearbeiten Sie die SnapMirror Active Sync Beziehung.
   a. Navigieren Sie zu **Schutz** > **Beziehungen**.
   b. Wählen Sie das Kabob-Menü neben der Beziehung, die Sie ändern möchten, und dann **Bearbeiten**.
   c. Ändern Sie die **Schutzrichtlinie** auf AutomaticteFailoverDuplex.
   d. Wenn Sie auswählen `AutoMatedFailoverDuplex`, wird ein Dialogfeld zum Ändern der Host-Näherungseinstellungen angezeigt. Wählen Sie für die Initiatoren die entsprechende Option für **Initiator proximal bis** und dann **Speichern**.
   e. Wählen Sie **Speichern**.
3. Bestätigen Sie im Menü **Schutz** den erfolgreichen Vorgang, wenn die Beziehung als angezeigt wird `InSync`.

Schritte für eine nicht einheitliche Konfiguration

1. Ziel-Initiatorgruppe entfernen:
   a. Navigieren Sie am sekundären Standort zu **Hosts** > **SAN-Initiatorgruppen**.
   b. Wählen Sie die Initiatorgruppe mit der SnapMirror Beziehung aus und dann **Löschen**.
   c. Wählen Sie im Dialogfeld das Feld **Zuordnung der zugeordneten LUNs aufheben** und dann **Löschen**.
2. Neue Initiatorgruppe erstellen:
   a. Wählen Sie im Menü **SAN-Initiatorgruppen** auf dem Zielstandort **Hinzufügen**.
   b. Geben Sie einen **Namen** ein, wählen Sie das **Host-Betriebssystem** und dann **Initiator Group Members**.
   c. Wählen Sie **Speichern**.
3. Ordnen Sie die neue Initiatorgruppe den Ziel-LUNs zu.
   a. Navigieren Sie zu **Storage** > **LUNs**.
   b. Wählen Sie alle LUNs aus, die der Initiatorgruppe zugeordnet werden sollen.
   c. Wählen Sie **Mehr** und dann **Initiatorgruppen zuordnen**.
4. Bearbeiten Sie die SnapMirror Active Sync Beziehung.
   a. Navigieren Sie zu **Schutz** > **Beziehungen**.
   b. Wählen Sie das Kabob-Menü neben der Beziehung, die Sie ändern möchten, und dann **Bearbeiten**.
   c. Ändern Sie die **Schutzrichtlinie** auf AutomaticteFailoverDuplex.
   d. Durch Auswahl von AutoMatedFailoverDuplex wird die Option zum Ändern der Einstellungen für

die Host-Nähe aktiviert. Wählen Sie für die Initiatoren die entsprechende Option für **Initiator proximal bis** und dann **Speichern**.

e. Wählen Sie **Speichern**.

5. Bestätigen Sie im Menü **Schutz** den erfolgreichen Vorgang, wenn die Beziehung als angezeigt wird `InSync`.

CLI

Schritte für eine einheitliche Konfiguration

1. Ändern Sie die SnapMirror-Richtlinie von `AutomatedFailover` zu `AutomatedFailoverDuplex`:

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. Durch das Ändern der Richtlinie wird eine Neusynchronisierung ausgelöst. Warten Sie, bis die Resynchronisierung abgeschlossen ist, und bestätigen Sie die Beziehung `Insync`:

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

3. Wenn die vorhandenen Hosts lokal das primäre Cluster sind, fügen Sie den Host dem zweiten Cluster hinzu und stellen Sie die Verbindung mit dem entsprechenden Zugriff auf jedes Cluster her.
4. Löschen Sie am sekundären Standort die LUN-Zuordnungen der Initiatorgruppen, die Remote-Hosts zugeordnet sind.

> Stellen Sie sicher, dass die Initiatorgruppe keine Zuordnungen für nicht replizierte LUNs enthält.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

5. Legen Sie auf dem primären Standort die Berechtigungsebene auffolgende Einstellung fest `advanced`:

```
SiteA::> set -privilege advanced
```

6. Ändern Sie die Initiatorkonfiguration für vorhandene Hosts, um den proximalen Pfad für Initiatoren auf dem lokalen Cluster festzulegen.

```
SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
-initiator <host> -proximal-vserver <server>
```

> Nachdem Sie diesen Schritt durchgeführt haben, können Sie die Berechtigungsebene wieder auf „admin“ setzen.

7. Fügen Sie eine neue Initiatorgruppe und einen neuen Initiator für die neuen Hosts hinzu und legen Sie die Host-Nähe für die Host-Affinität zu ihrem lokalen Standort fest. Ennable-igroup-Replikation zur Replikation der Konfiguration und Invertierung der Hostlokalität auf dem Remote-Cluster.

```
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/optimierten Pfad zur Storage-LUN vom bevorzugten Cluster verfügen
9. Implementieren Sie die Applikation und verteilen Sie die VM-Workloads über Cluster hinweg.

Schritte für eine nicht einheitliche Konfiguration

1. Ändern Sie die SnapMirror-Richtlinie von `AutomatedFailover` zu `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. Durch das Ändern der Richtlinie wird eine Neusynchronisierung ausgelöst. Warten Sie, bis die Resynchronisierung abgeschlossen ist, und bestätigen Sie die Beziehung `Insync`:

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

3. Wenn sich die vorhandenen Hosts lokal zum primären Cluster befinden, fügen Sie den Host zum zweiten Cluster hinzu, und stellen Sie die Verbindung mit dem entsprechenden Zugriff auf jedes Cluster her.
4. Fügen Sie am sekundären Standort eine neue Initiatorgruppe und einen neuen Initiator für die neuen Hosts hinzu und legen Sie die Host-Nähe für die Host-Affinität zum lokalen Standort fest. Ordnen Sie die LUNs der Initiatorgruppe zu.

   ```
   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/optimierten Pfad zur Storage-LUN vom bevorzugten Cluster verfügen
6. Implementieren Sie die Applikation und verteilen Sie die VM-Workloads über Cluster hinweg.

Konvertieren Sie von einer symmetrischen Aktiv/Aktiv- in eine asymmetrische iSCSI- oder FC-Beziehung

Wenn Sie symmetrischen Aktiv/Aktiv-Schutz mit iSCSI oder FC konfiguriert haben, können Sie die Beziehung mithilfe der ONTAP CLI in asymmetrischen Schutz umwandeln.

Schritte

1. Verschieben Sie alle VM-Workloads auf den lokalen Host in das Quellcluster.
2. Entfernen Sie die igroup-Konfiguration für die Hosts, die die VM-Instanzen nicht verwalten, und ändern Sie dann die igroup-Konfiguration, um die igroup-Replikation zu beenden.

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. Heben Sie am sekundären Standort die Zuordnung der LUNs auf.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. Löschen Sie am sekundären Standort die symmetrische aktiv/aktiv-Beziehung.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. Geben Sie am primären Standort die symmetrische aktiv/aktiv-Beziehung frei.
   `SiteA::> snapmirror release -destination-path <destination_path> -relationship -info-only true`
6. Erstellen Sie vom sekundären Standort aus eine Beziehung zu demselben Volume-Satz mit der Richtlinie, um die Beziehung neu zu `AutomatedFailover` synchronisieren.

```
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 Consistency Group am sekundären Standort muss "Zu löschen" vor dem Neuerstellen der Beziehung erstellt werden. Die Zielvolumes "Muss in Typ DP konvertiert werden". Um die Volumes in DP zu konvertieren, führen Sie den Befehl mit einer nicht-- `AutomatedFailover`Richtlinie aus `snapmirror resync: MirrorAndVault`, `MirrorAllSnapshots`, Oder `Sync`.

7. Bestätigen Sie, dass `Snapmirrored` der Beziehungsstatus „Spiegelstatus `Insync`“ lautet.

   `snapmirror show -destination-path` *`destination_path`*

8. Ermitteln Sie die Pfade vom Host erneut.

Verwandte Informationen

- "snapmirror löschen"
- "Snapmirror ändern"
- "snapmirror Release"
- "SnapMirror-Neusynchronisierung"
- "Snapmirror-Show"

Management der aktiven SnapMirror Synchronisierung und Sicherung von Daten

Erstellen Sie einen gemeinsamen Snapshot zwischen ONTAP Consistency Groups

Zusätzlich zu den regelmäßig geplanten Snapshot-Vorgängen können Sie manuell einen gemeinsamen Speicher zwischen den Volumes in der primären SnapMirror-Konsistenzgruppe und den Volumes in der sekundären SnapMirror-Konsistenzgruppe erstellen"snapshot".

Über diese Aufgabe

Das Zeitintervall für die Erstellung von Snapshots beträgt 12 Stunden.

Bevor Sie beginnen

- Die SnapMirror-Gruppenbeziehung muss synchron sein.

Schritte

1. Erstellen Sie einen gemeinsamen Snapshot:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Überwachen Sie den Fortschritt des Updates:

```
destination::>snapmirror show -fields newest-snapshot
```

Verwandte Informationen

- "Snapmirror-Show"

Führen Sie ein geplantes Failover von ONTAP Clustern in einer SnapMirror Active Sync-Beziehung durch

Bei einem geplanten Failover von ONTAP Clustern in einer aktiven SnapMirror Synchronisierungsbeziehung wechseln Sie die Rollen des primären und sekundären Clusters, sodass das sekundäre Cluster vom primären Cluster übernimmt. Während eines Failovers verarbeitet das sekundäre Cluster normalerweise Input- und Output-Anfragen lokal, ohne den Client-Betrieb zu unterbrechen.

Sie können ein geplantes Failover durchführen, um den Zustand Ihrer Disaster-Recovery-Konfiguration zu testen oder Wartungsarbeiten am primären Cluster durchzuführen.

Über diese Aufgabe

Der Administrator des sekundären Clusters initiiert einen geplanten Failover. Der Vorgang erfordert das Umschalten der primären und sekundären Rollen, damit das sekundäre Cluster vom primären Standort übernommen wird. Das neue primäre Cluster kann dann ohne Unterbrechung der Client-Prozesse mit der lokalen Verarbeitung von ein- und Ausgabeanfragen beginnen.

Bevor Sie beginnen

- Die SnapMirror Active Sync Beziehung muss synchron sein.
- Sie können kein geplantes Failover initiieren, wenn gerade ein unterbrechungsfreier Betrieb läuft. Zu den unterbrechungsfreien Abläufen gehören Verschiebung von Volumes, Verschiebung von Aggregaten und Failover für Storage.
- Der ONTAP-Mediator muss konfiguriert, verbunden und quorumfähig sein.

Schritte

Sie können ein geplantes Failover mithilfe der ONTAP CLI oder System Manager durchführen.

System Manager

Von ONTAP 9.14.1 bis 9.8 wird SnapMirror Active Sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

1. Wählen Sie in System Manager **Schutz > Übersicht > Beziehungen**.
2. Identifizieren Sie die SnapMirror Active Sync Beziehung, die Sie für ein Failover verwenden möchten. Wählen Sie … neben dem Namen der Beziehung das Feld neben dem Namen der Beziehung aus, und wählen Sie dann **Failover**.
3. Verwenden Sie zum Überwachen des Status des Failover `snapmirror failover show` in der ONTAP-CLI.

CLI

1. Initiieren Sie vom Ziel-Cluster den Failover-Vorgang:

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. Überwachen Sie den Status des Failover:

   ```
   destination::>snapmirror failover show
   ```

3. Nach Abschluss des Failover-Vorgangs können Sie vom Ziel aus den Status der SnapMirror Synchronous Protection Relationship überwachen:

   ```
   destination::>snapmirror show
   ```

Verwandte Informationen

- "Snapmirror-Failover-Show"
- "Snapmirror-Failover-Start"
- "Snapmirror-Show"

Wiederherstellung nach automatischen, ungeplanten ONTAP Cluster-Failover-Vorgängen

Ein automatisches ungeplantes Failover (AUFO) erfolgt, wenn der primäre Cluster ausfällt oder isoliert ist. Der ONTAP Mediator erkennt, wenn ein Failover auftritt, und führt automatisch einen ungeplanten Failover zum sekundären Cluster durch. Dieser Vorgang wird nur mit Unterstützung des ONTAP Mediators durchgeführt. Der sekundäre Cluster wird zum primären Cluster konvertiert und beginnt mit der Bereitstellung von Clients. Dieser Vorgang wird nur mit Unterstützung durch den ONTAP Mediator durchgeführt.

Nach dem automatischen, ungeplanten Failover ist es wichtig, die Host-LUN-I/O-Pfade erneut zu prüfen, damit keine I/O-Pfade verloren gehen.

Stellen Sie die Sicherungsbeziehung nach einem ungeplanten Failover wieder her

Sie können die Sicherungsbeziehung mit System Manager oder der ONTAP CLI wiederherstellen.

System Manager

Schritte

Von ONTAP 9.14.1 bis 9.8 wird SnapMirror Active Sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

1. Navigieren Sie zu **Schutz > Beziehungen** und warten Sie, bis der Beziehungsstatus „InSync“ angezeigt wird.
2. Um die Vorgänge auf dem ursprünglichen Quellcluster fortzusetzen, klicken Sie auf ⋮ und wählen Sie **Failover** aus.

CLI

Sie können den Status des automatischen ungeplanten Failovers mit dem `snapmirror failover show` Befehl überwachen.

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: -
```

Weitere "EMS-Referenz"Informationen zu Ereignismeldungen und Korrekturmaßnahmen finden Sie im.

Setzen Sie den Schutz in einer Fan-out-Konfiguration nach dem Failover fort

Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync nach einem Failover die automatische Neukonfiguration im Fan-out-Bereich. Der asynchrone Fan-out-Teil kann eine Konsistenzgruppenbeziehung oder eine unabhängige Volume-Beziehung sein. Weitere Informationen finden Sie unter "Fan-out-Konfigurationen".

Wenn Sie ONTAP 9.14.1 oder eine frühere Version verwenden und ein Failover auf dem sekundären Cluster in der aktiven synchronen SnapMirror Beziehung eintritt, wird das asynchrone Ziel von SnapMirror nicht mehr gesund. Sie müssen den Schutz manuell wiederherstellen, indem Sie die Beziehung zum asynchronen Endpunkt von SnapMirror löschen und neu erstellen.

Schritte

1. Überprüfen Sie, ob der Failover erfolgreich abgeschlossen wurde:
   `snapmirror failover show`
2. Löschen Sie auf dem asynchronen Endpunkt von SnapMirror den Fan-out-Endpunkt:
   `snapmirror delete -destination-path` *`destination_path`*

3. Erstellen Sie am dritten Standort asynchrone SnapMirror Beziehungen zwischen dem neuen primären Volume der aktiven Synchronisierung von SnapMirror und dem asynchronen Fan-out-Ziel-Volume:
`snapmirror create -source-path source_path -destination-path destination_path -policy MirrorAllSnapshots -schedule schedule`
4. Neusynchronisierung der Beziehung:
`snapmirror resync -destination-path destination_path`
5. Überprüfen Sie den Beziehungsstatus und den Systemzustand:
`snapmirror show`

Verwandte Informationen

- "snapmirror erstellen"
- "snapmirror löschen"
- "Snapmirror-Failover-Show"
- "SnapMirror-Neusynchronisierung"
- "Snapmirror-Show"

Überwachen Sie die aktiven Synchronisierungsvorgänge von ONTAP SnapMirror

Sie können die folgenden aktiven SnapMirror Synchronisierungsvorgänge überwachen, um den Zustand Ihrer SnapMirror Active Sync Konfiguration sicherzustellen:

- ONTAP Mediator
- Geplante Failover-Vorgänge
- Automatische ungeplante Failover-Vorgänge
- Verfügbarkeit der aktiven Synchronisierung von SnapMirror

> Ab ONTAP 9.15.1 zeigt System Manager den Status der aktiven SnapMirror Synchronisierungsbeziehung von einem der beiden Cluster an. Sie können den Status des ONTAP Mediators auch von einem der Cluster aus im System Manager überwachen.

ONTAP Mediator

Während des normalen Betriebs sollte der ONTAP-Mediatorstatus verbunden sein. Wenn es sich in einem anderen Zustand befindet, kann dies auf einen Fehlerzustand hinweisen. Sie können den überprüfen"EMS-Meldungen (Event Management System", um den Fehler und geeignete Korrekturmaßnahmen zu ermitteln.

Geplante Failover-Vorgänge

Sie können mit dem `snapmirror failover show` Befehl den Status und den Fortschritt eines geplanten Failover-Vorgangs überwachen. Beispiel:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Sobald der Failover-Vorgang abgeschlossen ist, können Sie den SnapMirror Sicherungsstatus vom neuen Ziel-Cluster aus überwachen. Beispiel:

```
ClusterA::> snapmirror show
```

Weitere "EMS-Referenz"Informationen zu Ereignismeldungen und Korrekturmaßnahmen finden Sie im.

Automatische ungeplante Failover-Vorgänge

Während eines ungeplanten automatischen Failover können Sie mit dem `snapmirror failover show` Befehl den Status des Vorgangs überwachen.

```
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: -
```

Weitere "EMS-Referenz"Informationen zu Ereignismeldungen und Korrekturmaßnahmen finden Sie im.

Verfügbarkeit der aktiven Synchronisierung von SnapMirror

Sie können die Verfügbarkeit der aktiven SnapMirror Synchronisierungsbeziehung mit einer Reihe von Befehlen überprüfen, entweder auf dem primären Cluster, dem sekundären Cluster oder beidem.

Die von Ihnen verwendeten Befehle enthalten den `snapmirror mediator show` Befehl sowohl für das primäre als auch `snapmirror show` `volume show` für das sekundäre Cluster, um den Verbindungs- und den Quorum-Status, den Befehl und den Befehl zu überprüfen. 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 zu einer ONTAP Konsistenzgruppe

Wenn sich die Workload-Anforderungen Ihrer Applikationen ändern, müssen Sie möglicherweise Volumes einer Konsistenzgruppe hinzufügen oder aus ihr entfernen, um Business Continuity zu gewährleisten. Der Prozess zum Hinzufügen und Entfernen von

Volumes in einer aktiven SnapMirror aktiven Sync Beziehung hängt von der verwendeten Version von ONTAP ab.

In den meisten Fällen führt dies zu Unterbrechungen des Betriebs, die dazu führen, dass Sie die SnapMirror Beziehung löschen, die Konsistenzgruppe ändern und den Schutz wieder aufnehmen. Ab ONTAP 9.13.1 ist das Hinzufügen von Volumes zu einer Konsistenzgruppe mit einer aktiven SnapMirror Beziehung ein unterbrechungsfreier Vorgang.

Über diese Aufgabe

- In ONTAP 9.9 können Sie mithilfe der ONTAP-CLI Volumes zu einer Konsistenzgruppe hinzufügen oder entfernen.
- Ab ONTAP 9.10.1 wird empfohlen, die Verwaltung "Konsistenzgruppen" über System Manager oder über die ONTAP REST-API durchzuführen.

  Wenn Sie die Zusammensetzung der Consistency Group durch Hinzufügen oder Entfernen eines Volumes ändern möchten, müssen Sie zuerst die ursprüngliche Beziehung löschen und dann die Consistency Group erneut mit der neuen Zusammensetzung erstellen.

- Ab ONTAP 9.13.1 können Sie Volumes mit einer aktiven SnapMirror -Beziehung unterbrechungsfrei von der Quelle oder dem Ziel zu einer Konsistenzgruppe hinzufügen. Diese Aktion wird vom NVMe-Protokoll nicht unterstützt.

  Das Entfernen von Volumes verursacht Unterbrechungen. Sie müssen die SnapMirror-Beziehung löschen, bevor Sie Volumes entfernen.

ONTAP 9.9.1-9.13.0

Bevor Sie beginnen

- Sie können nicht damit beginnen, die Konsistenzgruppe zu ändern, während sie `InSync` den Status aufweist.
- Das Ziel-Volume sollte vom Typ DP sein.
- Das neue Volume, das Sie zur Erweiterung der Konsistenzgruppe hinzufügen, muss über ein Paar gemeinsamer Snapshots zwischen den Quell- und Zielvolumes verfügen.

Schritte

Die in zwei Volume-Zuordnungen gezeigten Beispiele: `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. Überprüfen Sie mit dem Befehl, ob auf den Quell- und Ziel-Clustern 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. Wenn kein gemeinsamer Snapshot vorhanden ist, erstellen und initialisieren Sie eine FlexVol SnapMirror Beziehung:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Löschen Sie die Konsistenzgruppenbeziehung:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

4. Geben Sie die Quell-SnapMirror-Beziehung frei und behalten Sie die gemeinsamen Snapshots bei:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. LUN-Zuordnung aufheben und die vorhandene Konsistenzgruppe löschen:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > Die Zuordnung der Ziel-LUNs wird aufgehoben, während die LUNs auf der primären Kopie weiterhin für den Host-I/O bereit sind

   ```
   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,** löschen Sie die Konsistenzgruppe auf der Quelle und erstellen Sie sie mit der richtigen Zusammensetzung neu. Folgen Sie den Schritten in "Löschen einer Konsistenzgruppe" und dann "Konfigurieren einer einzelnen Konsistenzgruppe" . In ONTAP 9.10.1 und höher müssen Sie die Lösch- und Erstellungsvorgänge im System Manager oder mit der ONTAP REST API durchführen; es gibt kein CLI-Verfahren.

   Wenn Sie ONTAP 9.9 verwenden, fahren Sie mit dem nächsten Schritt fort.

7. Erstellen Sie die neue Consistency Group auf dem Ziel mit der neuen Zusammensetzung:

   ```
   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. Synchronisieren Sie die RTO-Konsistenzgruppenbeziehung mit Null, um sicherzustellen, dass sie synchronisiert ist:

   ```
   destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

9. Ordnen Sie die LUNs, die Sie in Schritt 5 nicht zugeordnet haben, erneut zu:

   ```
   destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
   ```

10. Wiederherstellen aller Pfade zu den LUNs durch erneute Überprüfung der Host-LUN-I/O-Pfade

ONTAP 9.13.1 und höher

Ab ONTAP 9.13.1 können Sie Volumes unterbrechungsfrei zu einer Konsistenzgruppe mit einer aktiven SnapMirror-Beziehung hinzufügen. SnapMirror Active Sync unterstützt das Hinzufügen von Volumes sowohl aus der Quelle als auch aus dem Ziel.

> ⓘ Von ONTAP 9.14.1 bis 9.8 wird SnapMirror Active Sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

Weitere Informationen zum Hinzufügen von Volumes aus der Quell-Konsistenzgruppe finden Sie unter Ändern einer Konsistenzgruppe.

Fügen Sie ein Volume aus dem Ziel-Cluster hinzu

1. Wählen Sie auf dem Zielcluster **Schutz** > **Beziehungen**.
2. Suchen Sie die SnapMirror Konfiguration, der Sie Volumes hinzufügen möchten. Wählen Sie ⋮ dann **erweitern**.
3. Wählen Sie die Volume-Beziehungen aus, deren Volumes zur Konsistenzgruppe hinzugefügt werden sollen
4. Wählen Sie **Erweitern**.

Verwandte Informationen

- "snapmirror löschen"
- "snapmirror Initialisierung"
- "snapmirror Release"
- "SnapMirror-Neusynchronisierung"

Upgrade und Wiederherstellung mit ONTAP SnapMirror Active Sync

SnapMirror Active Sync wird ab ONTAP 9.9 unterstützt. Das Upgrade und Zurücksetzen des ONTAP Clusters oder Controllers hat Auswirkungen auf die aktiven SnapMirror Synchronisierungsbeziehungen, je nach ONTAP Version, auf die Sie aktualisieren oder zurücksetzen.

Aktualisieren eines Clusters

Ab ONTAP 9.16.1 unterstützt SnapMirror Active Sync Cluster mit vier Nodes in symmetrischen aktiv/aktiv-Konfigurationen. Sie können das Cluster mit vier Nodes zum Upgrade der Controller und des Storage verwenden.

Bevor Sie beginnen

- Lesen Sie die "Anforderungen für Cluster mit vier Nodes".
- Sie können während des Tech Refresh-Prozesses asymmetrische Konfigurationen erstellen. Nach Abschluss der Aktualisierung sollten Sie jedoch zu einer symmetrischen Konfiguration zurückkehren.
- Diese Anweisungen gelten für eine bestehende Konfiguration mit vier Nodes mit 50 oder weniger Konsistenzgruppen und 400 oder weniger Volume-Endpunkten.

Schritte

1. "Verschieben Sie alle aktiven synchronen SnapMirror Volumes auf ein HA-Paar (High Availability, Hochverfügbarkeit)".
2. "Entfernen Sie die nicht verwendeten Nodes aus dem Cluster".
3. "Die neuen Nodes werden dem Cluster hinzugefügt".
4. "Verschieben Sie alle Volumes" In die neuen Knoten ein.
5. "Entfernen Sie die nicht verwendeten Nodes aus dem Cluster" Dann ersetzen Sie sie "Mit den neuen Knoten".

Upgrade von ONTAP mit aktiver SnapMirror Synchronisierung

Um SnapMirror Active Sync zu verwenden, müssen auf allen Nodes auf dem Quell- und Ziel-Cluster ONTAP 9.9.1 oder höher ausgeführt werden.

Wenn Sie ONTAP mit aktiven SnapMirror-Synchronisierungsbeziehungen aktualisieren, sollten Sie verwendenAutomatisierte unterbrechungsfreie Upgrades (ANDU). Durch die Verwendung von ANDU wird sichergestellt, dass Ihre aktiven SnapMirror Synchronisierungsbeziehungen während des Upgrade-Prozesses synchron und ordnungsgemäß sind.

Es gibt keine Konfigurationsschritte, um die Bereitstellung der aktiven Synchronisierung von SnapMirror für ONTAP Upgrades vorzubereiten. Es wird jedoch empfohlen, vor und nach dem Upgrade Folgendes zu überprüfen:

- Aktive SnapMirror Synchronisierungsbeziehungen sind synchron.
- Im Ereignisprotokoll gibt es keine mit SnapMirror verbundenen Fehler.
- Der Mediator ist aus beiden Clustern online und gesund.
- Alle Hosts können alle Pfade ordnungsgemäß sehen, um LUNs zu schützen.

Wenn Sie Cluster von ONTAP 9.9.1 oder 9.9.1 auf ONTAP 9.10.1 und höher aktualisieren, erstellt ONTAP neue KonsistenzgruppenQuell- und Ziel-Cluster für aktive SnapMirror Synchronisierungsbeziehungen, die mit System Manager konfiguriert werden können.

Die `snapmirror quiesce` `snampirror resume` Befehle und werden bei der aktiven SnapMirror-Synchronisierung nicht unterstützt.

Kehren Sie von ONTAP 9.10.1 zu ONTAP 9.9.1 zurück

Um Beziehungen zwischen 9.10.1 und 9.9 zurückzusetzen, müssen aktive SnapMirror Synchronisierungsbeziehungen, gefolgt von der Instanz von 9.10.1 Konsistenzgruppen gelöscht werden. Konsistenzgruppen mit einer aktiven SnapMirror Beziehung zur aktiven Synchronisierung können nicht gelöscht werden. Alle FlexVol-Volumes, die auf 9.10.1 aktualisiert wurden, die zuvor mit einem anderen intelligenten Container oder einer Enterprise-Applikation in 9.9.1 oder früher verbunden waren, werden nicht mehr wieder zugeordnet. Durch das Löschen von Konsistenzgruppen werden die zusammengehörigen Volumes oder granularen Volume-Snapshots nicht gelöscht. "Löschen einer Konsistenzgruppe"Weitere Informationen zu dieser Aufgabe finden Sie unter ONTAP 9.10.1 und höher.

Zurück von ONTAP 9.9.1

Die aktive Synchronisierung von SnapMirror wird bei gemischten ONTAP Clustern nicht unterstützt als bei Versionen vor ONTAP 9.9.1.

Wenn Sie von ONTAP 9.9.1 auf eine frühere Version von ONTAP zurücksetzen, müssen Sie Folgendes beachten:

- Wenn der Cluster ein Ziel für die aktive SnapMirror Synchronisierung hostet, ist das Zurücksetzen auf ONTAP 9.8 oder eine frühere Version erst zulässig, wenn die Beziehung unterbrochen und gelöscht wird.
- Wenn der Cluster eine SnapMirror Quelle für aktive Synchronisierung hostet, ist das Zurücksetzen auf ONTAP 9.8 oder eine frühere Version erst zulässig, wenn die Beziehung freigegeben wird.
- Alle vom Benutzer erstellten Richtlinien zur aktiven SnapMirror Synchronisierung müssen vor dem Zurücksetzen auf ONTAP 9.8 oder eine frühere Version gelöscht werden.

Um diese Anforderungen zu erfüllen, siehe "Entfernen Sie eine SnapMirror Active Sync Konfiguration".

Schritte

1. Bestätigen Sie die Bereitschaft zum Zurücksetzen, und geben Sie den folgenden Befehl von einem der Cluster in der SnapMirror Active Sync Beziehung ein:

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   In der folgenden Beispielausgabe wird ein Cluster angezeigt, das nicht zum Zurücksetzen bereit ist, und enthält Anweisungen zum Bereinigen.

   ```
   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. Wenn Sie die Anforderungen der Rückstellprüfung erfüllt haben, lesen Sie "ONTAP zurücksetzen".

Verwandte Informationen

- "Netzwerkschnittstelle"
- "Snapmirror-Pause"
- "Snapmirror-Richtlinie löschen"
- "Snapmirror-Richtlinien-Show"
- "Snapmirror-Ruhezustand"
- "Snapmirror-Show"

Entfernen einer ONTAP SnapMirror Active Sync-Konfiguration

Wenn Sie keinen synchronen RTO-Schutz mehr für SnapMirror benötigen, können Sie Ihre SnapMirror Active Sync Beziehung löschen.

Entfernen Sie eine asymmetrische Konfiguration

- Bevor Sie die SnapMirror Active Sync Beziehung löschen, muss die Zuordnung aller LUNs im Ziel-Cluster aufgehoben werden.
- Nachdem die LUN nicht zugeordnet und der Host erneut gescannt wird, werden die Hosts vom SCSI-Ziel benachrichtigt, dass sich die LUN-Inventur geändert hat. Die vorhandenen LUNs auf sekundären Volumes von null Sekunden ändern sich, um eine neue Identität anzuzeigen, nachdem die RTO-Beziehung von null gelöscht wurde. Hosts erkennen die sekundären Volume LUNs als neue LUNs, die keine Beziehung zu den Quell-Volume LUNs haben.
- Die sekundären Volumes bleiben DP-Volumen, nachdem die Beziehung gelöscht wurde. Sie können den `snapmirror break` Befehl zum Konvertieren in Lesen/Schreiben ausgeben.
- Das Löschen der Beziehung ist im Failover-Zustand nicht zulässig, wenn die Beziehung nicht rückgängig gemacht wird.

Schritte

1. Entfernen Sie aus dem sekundären Cluster die SnapMirror Active Sync Konsistenzgruppenbeziehung zwischen dem Quell-Endpunkt und dem Zielendpunkt:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. Geben Sie aus dem primären Cluster die Konsistenzgruppenbeziehung und die für die Beziehung erstellten Snapshots frei:

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. Führen Sie einen Hostscan durch, um den LUN-Bestand zu aktualisieren.

4. Ab ONTAP 9.10.1 wird durch Löschen der SnapMirror Beziehung die Konsistenzgruppe nicht gelöscht. Wenn Sie die Konsistenzgruppe löschen möchten, müssen Sie System Manager oder DIE ONTAP REST API verwenden. Weitere Informationen finden Sie unter Löschen einer Konsistenzgruppe .

Entfernen Sie die symmetrische Aktiv/Aktiv-Konfiguration von iSCSI oder FC

Sie können eine symmetrische Konfiguration mit System Manager oder der ONTAP CLI entfernen. In beiden Schnittstellen gibt es verschiedene Schritte für Einheitliche und nicht einheitliche Konfigurationen.

System Manager

Schritte für eine einheitliche Konfiguration

1. Entfernen Sie am primären Standort die Remote-Hosts von der Initiatorgruppe und beenden Sie die Replikation.
   a. Navigieren Sie zu **Hosts** > **SAN-Initiatorgruppen**.
   b. Wählen Sie die zu ändernde Initiatorgruppe und anschließend **Bearbeiten** aus.
   c. Entfernen Sie den Remote-Initiator und beenden Sie die igroup-Replikation. Wählen Sie **Speichern**.
2. Löschen Sie am sekundären Standort die replizierte Beziehung, indem Sie die Zuordnung der LUNs aufheben.
   a. Navigieren Sie zu **Hosts** > **SAN-Initiatorgruppen**.
   b. Wählen Sie die Initiatorgruppe mit der SnapMirror Beziehung aus und dann **Löschen**.
   c. Wählen Sie im Dialogfeld das Feld **Zuordnung der zugeordneten LUNs aufheben** und dann **Löschen**.
   d. Navigieren Sie zu **Schutz** > **Beziehungen**.
   e. Wählen Sie die SnapMirror Active Sync Beziehung und dann **Release**, um die Beziehungen zu löschen.

Schritte für eine nicht einheitliche Konfiguration

1. Entfernen Sie am primären Standort die Remote-Hosts von der Initiatorgruppe und beenden Sie die Replikation.
   a. Navigieren Sie zu **Hosts** > **SAN-Initiatorgruppen**.
   b. Wählen Sie die zu ändernde Initiatorgruppe und anschließend **Bearbeiten** aus.
   c. Entfernen Sie den Remote-Initiator und beenden Sie die igroup-Replikation. Wählen Sie **Speichern**.
2. Entfernen Sie am sekundären Standort die SnapMirror Active Sync Beziehung.
   a. Navigieren Sie zu **Schutz** > **Beziehungen**.
   b. Wählen Sie die SnapMirror Active Sync Beziehung und dann **Release**, um die Beziehungen zu löschen.

CLI

Schritte für eine einheitliche Konfiguration

1. Verschieben Sie alle VM-Workloads auf den lokalen Host in den Quellcluster der aktiven SnapMirror Synchronisierung.
2. Entfernen Sie auf dem Quell-Cluster die Initiatoren aus der Initiatorgruppe und ändern Sie die igroup-Konfiguration, um die igroup-Replizierung 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. Löschen Sie am sekundären Standort die LUN-Zuordnung und entfernen Sie die igroup-Konfiguration:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. Löschen Sie am sekundären Standort die SnapMirror Active Sync Beziehung.

   ```
   SiteB::> snapmirror delete -destination-path destination_path
   ```

5. Geben Sie am primären Standort die SnapMirror Active Sync Beziehung vom primären Standort frei.

   ```
   SiteA::> snapmirror release -destination-path <destination_path>
   ```

6. Ermitteln Sie die Pfade neu, um zu überprüfen, ob nur der lokale Pfad für den Host verfügbar ist.

Schritte für eine nicht einheitliche Konfiguration

1. Verschieben Sie alle VM-Workloads auf den lokalen Host in den Quellcluster der aktiven SnapMirror Synchronisierung.
2. Entfernen Sie auf dem Quell-Cluster die Initiatoren aus der Initiatorgruppe.

   ```
   SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
   <host2>
   ```

3. Löschen Sie am sekundären Standort die LUN-Zuordnung und entfernen Sie die igroup-Konfiguration:

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
   <>
   SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
   ```

4. Löschen Sie am sekundären Standort die SnapMirror Active Sync Beziehung.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. Geben Sie am primären Standort die SnapMirror Active Sync Beziehung vom primären Standort frei.

   ```
   SiteA::> snapmirror release -destination-path <destination_path>
   ```

6. Ermitteln Sie die Pfade neu, um zu überprüfen, ob nur der lokale Pfad für den Host verfügbar ist.

Entfernen einer symmetrischen NVMe-Aktiv/Aktiv-Konfiguration

System Manager

Schritte

1. Navigieren Sie im Quellcluster zu **Schutz > Replikation**.
2. Suchen Sie die Beziehung, die Sie entfernen möchten, wählen Sie ⋮ und wählen Sie **Löschen**.

CLI

1. Löschen Sie aus dem Zielcluster die SnapMirror -Active-Sync-Beziehung.

   ```
   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 Namespaces werden aus dem sekundären Cluster entfernt.

2. Geben Sie vom Quellcluster aus die SnapMirror -Active-Sync-Beziehung vom primären Standort frei.

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

   Beispiel:

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. Ermitteln Sie die Pfade neu, um zu überprüfen, ob nur der lokale Pfad für den Host verfügbar ist.

Verwandte Informationen

- "Snapmirror-Pause"
- "snapmirror löschen"
- "snapmirror Release"

Entfernen Sie ONTAP Mediator oder ONTAP Cloud Mediator

Wenn Sie eine vorhandene ONTAP Mediator- oder ONTAP Cloud Mediator-Konfiguration aus Ihren ONTAP Clustern entfernen möchten, können Sie dies mithilfe des `snapmirror mediator remove` Befehl. Sie können beispielsweise immer nur einen Mediatortyp gleichzeitig verwenden. Sie müssen also eine Instanz entfernen, bevor Sie die andere installieren.

Schritte

Sie können ONTAP Mediator oder ONTAP Cloud Mediator entfernen, indem Sie einen der folgenden Schritte ausführen.

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

Der Löschvorgang von ONTAP SnapMirror schlägt im Übernahmezustand fehl

Verwenden Sie die folgenden Informationen, wenn die `snapmirror delete` Der Befehl schlägt fehl, wenn sich eine SnapMirror Active Sync Consistency Group-Beziehung im Übernahmestatus befindet.

Problem:

Wenn ONTAP 9.9.1 auf einem Cluster installiert ist, führt die Ausführung des `snapmirror delete` Der Befehl schlägt fehl, wenn sich eine SnapMirror Active Sync Consistency Group-Beziehung im Übernahmestatus befindet.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Nutzen

Wenn sich die Knoten in einer SnapMirror-Active-Sync-Beziehung im Übernahmezustand befinden, führen Sie den SnapMirror-Lösch- und Freigabevorgang mit der Option „-force“ auf „true“ aus.

```
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 löschen"

Fehler beim Erstellen einer ONTAP SnapMirror -Beziehung und Initialisieren der Konsistenzgruppe

Verwenden Sie die folgenden Informationen, wenn die Erstellung einer SnapMirror -Beziehung und die Initialisierung der Konsistenzgruppe fehlschlagen.

Problem:

Die Erstellung der SnapMirror Beziehung und die Initialisierung der Konsistenzgruppe ist fehlgeschlagen.

Lösung:

Vergewissern Sie sich, dass Sie das Limit von Konsistenzgruppen pro Cluster nicht überschritten haben. Die Einschränkungen von Konsistenzgruppen in SnapMirror Active Sync sind plattformunabhängig und unterscheiden sich je nach Version der ONTAP. Informationen zu "Objektbeschränkungen"Ihrer ONTAP-Version finden Sie unter.

Fehler:

Wenn die Konsistenzgruppe nicht initialisiert wird, überprüfen Sie den Status Ihrer Konsistenzgruppeninitialisierungen mit der ONTAP REST API, System Manager oder dem Befehl `sn show -expand`.

Von ONTAP 9.14.1 bis 9.8 wird SnapMirror Active Sync als SnapMirror Business Continuity (SM-BC) bezeichnet.

Lösung:

Wenn die Konsistenzgruppen nicht initialisiert werden können, entfernen Sie die SnapMirror Active Sync Beziehung, löschen Sie die Konsistenzgruppe, erstellen Sie die Beziehung neu, und initialisieren Sie sie. Dieser Workflow unterscheidet sich je nach der verwendeten ONTAP Version.

Wenn Sie ONTAP 9.9.1 verwenden	Wenn Sie ONTAP 9.10.1 oder höher verwenden

1. "Entfernen Sie die SnapMirror Active Sync Konfiguration" 2. "Erstellen Sie eine Konsistenzgruppenbeziehung und initialisieren Sie dann die Konsistenzgruppenbeziehung"	1. Suchen Sie unter **Schutz > Beziehungen** die SnapMirror Active Sync Beziehung auf der Konsistenzgruppe. Wählen Sie ⋮, dann **Delete**, um die SnapMirror Active Sync Beziehung zu entfernen. 2. "Löschen Sie die Konsistenzgruppe" 3. "Konfigurieren Sie die Konsistenzgruppe"

Geplantes ONTAP Cluster-Failover fehlgeschlagen

Verwenden Sie die folgenden Informationen, wenn der geplante Failover-Vorgang nicht erfolgreich ist.

Problem:

Nach dem Ausführen des `snapmirror failover start` `snapmirror failover show` Befehls wird in der Ausgabe des Befehls eine Meldung angezeigt, dass gerade ein unterbrechungsfreier Vorgang ausgeführt wird.

```
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:

Geplante Failovers können nicht gestartet werden, wenn gerade ein unterbrechungsfreier Vorgang durchgeführt wird, einschließlich Volume-Verschiebung, Aggregatverschiebung und Storage Failover.

Lösung:

Warten Sie, bis der unterbrechungsfreie Betrieb abgeschlossen ist, und versuchen Sie es erneut.

Verwandte Informationen

- "Snapmirror-Failover-Show"
- "Snapmirror-Failover-Start"

ONTAP Mediator oder ONTAP Cloud Mediator nicht erreichbar oder Mediator-Quorum-Status ist falsch

Verwenden Sie die folgenden Informationen, wenn der ONTAP Mediator oder ONTAP Cloud Mediator nicht erreichbar ist oder der Quorum-Status des Mediators falsch ist.

Problem:

Nach der Ausführung des `snapmirror failover start` Befehl, die Ausgabe für die `snapmirror`

`failover show` Der Befehl zeigt eine Meldung an, die angibt, dass entweder der ONTAP Mediator oder der ONTAP Cloud Mediator nicht konfiguriert ist.

Sehen "Konfigurieren Sie den ONTAP Mediator und die Cluster für SnapMirror Active Sync" oder "Konfigurieren Sie den ONTAP Cloud Mediator für SnapMirror Active Sync" .

```
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 gibt Probleme mit der Netzwerkverbindung.

Lösung:

Wenn der ONTAP-Mediator nicht konfiguriert ist, müssen Sie den ONTAP-Mediator konfigurieren, bevor Sie eine aktive SnapMirror-Synchronisierungsbeziehung herstellen können. Beheben Sie alle Probleme mit der Netzwerkverbindung. Stellen Sie sicher, dass Mediator verbunden ist und der Quorum-Status sowohl am Quell- als auch am Zielstandort TRUE ist. Verwenden Sie dazu den befehl snapmirror Mediator show. Weitere Informationen finden Sie unter "Konfigurieren Sie den ONTAP Mediator".

```
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

Verwenden Sie die folgenden Informationen, wenn der ONTAP Cloud Meditor mit einem Fehler ausfällt, der besagt, dass die Ping-Latenz höher als die empfohlene Latenz ist.

Problem:

Systemmanager: Der Cloud Mediator-Dienst ist erreichbar, reagiert aber langsam.

CLI: Die `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 der Nähe der NetApp Console-Cloud oder es gibt Engpässe im Netzwerkpfad.

Lösung:

- Überprüfen Sie den geografischen Standort und die Nähe zur NetApp Console Cloud (USA-Ost).
- Optimieren Sie den Netzwerkpfad oder beheben Sie Engpässe.
- Messen Sie die Round Trip Time (RTT) mithilfe von Netzwerktools und reduzieren Sie die Latenz auf die empfohlenen Grenzwerte.
- Verwenden Sie einen HTTP-Proxy, um die Leistung zu verbessern.

Sehen "Konfigurieren Sie den ONTAP Cloud Mediator und die Cluster für SnapMirror Active Sync" .

Der automatische ungeplante Failover wird nicht an Standort B ausgelöst

Verwenden Sie die folgenden Informationen, wenn ein Fehler an Standort A kein ungeplantes Failover an Standort B auslöst.

Problem:

Ein Fehler an Standort A löst kein ungeplantes Failover auf Standort B aus

Mögliche Ursache #1:

Der ONTAP Mediator oder der ONTAP Cloud Mediator ist nicht konfiguriert. Um festzustellen, ob dies die Ursache ist, führen Sie den `snapmirror mediator show` Befehl auf dem Cluster von Site B.

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

Dieses Beispiel zeigt, dass der Mediator auf Site B nicht konfiguriert ist.

Lösung:

Stellen Sie sicher, dass Mediator auf beiden Clustern konfiguriert ist, dass der Status „Verbunden“ lautet und „Quorum“ auf „True“ gesetzt ist.

Mögliche Ursache #2:

Die SnapMirror Konsistenzgruppe ist nicht synchron. Um festzustellen, ob dies die Ursache ist, sehen Sie im Ereignisprotokoll nach, um anzuzeigen, ob die Konsistenzgruppe während der Zeit, zu der der Standort A-Fehler aufgetreten ist, synchronisiert wurde.

```
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:

Führen Sie die folgenden Schritte durch, um einen erzwungenen Failover an Standort B durchzuführen

1. Heben Sie die Zuordnung aller LUNs, die der Konsistenzgruppe angehören, von Standort B. auf
2. Löschen Sie die SnapMirror Konsistenzgruppenbeziehung mit der `force` Option.
3. Geben Sie den `snapmirror break` Befehl für die Volumes der Konsistenzgruppe ein, um Volumes von DP in Lese-/Schreibzugriff zu konvertieren, um I/O von Standort B zu aktivieren
4. Starten Sie die Knoten Standort A, um eine RTO-Beziehung von Standort B zu Standort A zu erstellen
5. Geben Sie die Konsistenzgruppe mit auf Standort A frei `relationship-info-only`, um den gemeinsamen Snapshot beizubehalten und die Zuordnung der LUNs, die zur Konsistenzgruppe gehören, aufzuheben.
6. Konvertieren Sie Volumes an Standort A von Lese-/Schreibzugriff nach DP, indem Sie eine Beziehung auf Volume-Ebene mit der Sync-Richtlinie oder der asynchronen Richtlinie einrichten.
7. Geben Sie das `snapmirror resync` ein, um die Beziehungen zu synchronisieren.
8. Löschen Sie die SnapMirror Beziehungen mit der Sync-Richtlinie auf Standort A
9. Geben Sie die SnapMirror-Beziehungen mit der Synchronisierungsrichtlinie unter Verwendung von `relationship-info-only true` vor Ort B frei
10. Erstellen Sie eine Konsistenzgruppenbeziehung von Standort B zu Standort A
11. Führen Sie eine Neusynchronisierung von Konsistenzgruppen von Standort A durch, und überprüfen Sie dann, ob die Konsistenzgruppe synchron ist.
12. Wiederherstellen aller Pfade zu den LUNs durch erneute Überprüfung der Host-LUN-I/O-Pfade

Verwandte Informationen

- "Snapmirror-Pause"
- "Snapmirror Mediator-Show"
- "SnapMirror-Neusynchronisierung"

Verbindung zwischen Site B und ONTAP Mediator ausgefallen und Site A ausgefallen

Um die Verbindung des ONTAP Mediators oder des ONTAP Cloud Mediators zu überprüfen, verwenden Sie die `snapmirror mediator show` Befehl. Wenn der Verbindungsstatus „Nicht erreichbar“ lautet und Site B Site A nicht erreichen kann,

erhalten Sie eine Ausgabe ähnlich der folgenden. Folgen Sie den Schritten in der Lösung, um die Verbindung wiederherzustellen.

Beispiel:

Verwenden Sie den ONTAP Cloud Mediator, um den Befehl „snapmirror mediator show“ auszugeben:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
--------------- ---------------- ----------------- ------------ -------
0.0.0.0         C1_cluster       unreachable       true         cloud
```

Verwenden Sie den ONTAP Mediator, um den Befehl „snapmirror mediator show“ auszugeben:

```
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
```

Nutzen

Erzwingen Sie ein Failover, um I/O von Standort B zu aktivieren, und stellen Sie dann eine RTO-Beziehung von Standort B zu Standort A auf Null ein. Führen Sie die folgenden Schritte aus, um ein erzwungenes Failover an Standort B durchzuführen

1. Alle LUNs, die zur Konsistenzgruppe von Standort B gehören, müssen entfernt werden. Dies wird fehlschlagen, daher müssen Sie zuerst die igroup ändern, um die Replikations-Peer-SVM zu entfernen, und anschließend die LUN-Zuordnung löschen.

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. Löschen Sie die SnapMirror Consistency Group-Beziehung mit der Force-Option.

2. Geben Sie den Befehl SnapMirror Break (`snapmirror break -destination_path svm:_volume_`) auf den Volumes der Consistency Group ein, um Volumes von DP in RW zu konvertieren, um I/O von Standort B zu aktivieren

   Sie müssen für jede Beziehung in der Konsistenzgruppe den SnapMirror Break-Befehl ausgeben. Wenn die Konsistenzgruppe beispielsweise drei Volumes enthält, geben Sie den Befehl für jedes Volume aus.

3. Starten Sie die Knoten Standort A, um eine RTO-Beziehung von Standort B zu Standort A zu erstellen
4. Geben Sie die Konsistenzgruppe mit „Relationship-Info-only“ auf Standort A frei, um den gemeinsamen Snapshot beizubehalten und die Zuordnung der LUNs zur Konsistenzgruppe aufzuheben.
5. Konvertieren Sie Volumes an Standort A von RW nach DP, indem Sie eine Beziehung auf Volume-Ebene mit einer Sync-Richtlinie oder einer asynchronen Richtlinie einrichten.
6. Geben Sie den `snapmirror resync` Befehl ein, um die Beziehungen zu synchronisieren.
7. Löschen Sie die SnapMirror Beziehungen mit der Sync-Richtlinie auf Standort A
8. Lassen Sie die SnapMirror Beziehungen mit Sync-Richtlinie unter Verwendung von Relationship-info-only True auf Site B. frei
9. Erstellen Sie eine Konsistenzgruppenbeziehung zwischen Standort B und Standort A.
10. Synchronisieren Sie die Konsistenzgruppe aus dem Quell-Cluster neu. Überprüfen Sie, ob der Status der Konsistenzgruppe synchron ist.
11. Scannen Sie die Host-LUN-I/O-Pfade erneut, um alle Pfade zu den LUNs wiederherzustellen.

Verwandte Informationen

- "Snapmirror-Pause"
- "Snapmirror Mediator-Show"
- "SnapMirror-Neusynchronisierung"
- "Snapmirror-Show"

Verbindung zwischen Site A und ONTAP Mediator ausgefallen und Site B ausgefallen

Bei der Verwendung von SnapMirror Active Sync verlieren Sie möglicherweise die Verbindung zwischen dem ONTAP Mediator oder Ihren Peering-Clustern. Sie können das Problem diagnostizieren, indem Sie die Verbindung, Verfügbarkeit und den Konsens der verschiedenen Teile der SnapMirror Active Sync Beziehung überprüfen und dann die Verbindung forcieren.

Was zu prüfen ist	CLI-Befehl	Anzeige
Mediator von Standort A	`snapmirror mediator show`	Der Verbindungsstatus wird als angezeigt `unreachable`
Anschluss an Standort B	`cluster peer show`	Verfügbarkeit wird als angezeigt `unavailable`
Konsensstatus des aktiven SnapMirror Sync Volume	`volume show volume_name -fields smbc-consensus`	Das `sm-bc consensus` Feld wird angezeigt `Awaiting-consensus`

Weitere Informationen zur Diagnose und Lösung dieses Problems finden Sie im"NetApp Knowledge Base: Verbindung zwischen Site A und Mediator unterbrochen und Site B unterbrochen, wenn SnapMirror Active Sync verwendet wird" .

Verwandte Informationen

- "Cluster-Peer-Show"
- "Snapmirror Mediator-Show"

Der Löschvorgang von ONTAP SnapMirror schlägt fehl, wenn auf dem Zielvolume ein Zaun festgelegt ist

Verwenden Sie die folgenden Informationen, wenn der Löschvorgang von SnapMirror fehlschlägt, wenn für eines der Zielvolumes ein Umleitungszaun festgelegt ist.

Problem:

Der Löschvorgang von SnapMirror schlägt fehl, wenn für eines der Ziel-Volumes ein Umleitungszaun festgelegt ist.

Nutzen

Führen Sie die folgenden Vorgänge durch, um die Umleitung erneut zu versuchen und den Zaun vom Ziel-Volume zu entfernen.

- SnapMirror Neusynchronisierung
- SnapMirror Update

Der Vorgang zum Verschieben des Volumes bleibt hängen, wenn der primäre ONTAP Server ausgefallen ist

Verwenden Sie die folgenden Informationen, wenn ein Volume-Verschiebungsvorgang auf unbestimmte Zeit im Cutover-Deferred-Status hängen bleibt, wenn der primäre Standort in einer SnapMirror Active Sync-Beziehung ausgefallen ist.

Problem:

Ein Volume-Verschiebungsvorgang bleibt dauerhaft in einem zurückgestellten Zustand der Umstellung hängen, wenn der primäre Standort in einer aktiven SnapMirror Sync-Beziehung ausfällt. Wenn der primäre Standort ausfällt, führt der sekundäre Standort ein automatisches ungeplantes Failover (AUFO) durch. Wenn eine Volume-Verschiebung ausgeführt wird, wenn der AUFO ausgelöst wird, bleibt die Volume-Verschiebung hängen.

Lösung:

Abbrechen der Instanz, die sich in der Volume-Verschiebung befindet, und Starten Sie die Volume-Verschiebung neu.

Die ONTAP SnapMirror Version schlägt fehl, wenn der Snapshot nicht gelöscht werden kann

Verwenden Sie die folgenden Informationen, wenn der SnapMirror Releasevorgang fehlschlägt, weil der Snapshot nicht gelöscht werden kann.

Problem:

Der SnapMirror-Release-Vorgang schlägt fehl, wenn der Snapshot nicht gelöscht werden kann.

Lösung:

Der Snapshot enthält ein transientes Tag. Verwenden Sie den `snapshot delete` Befehl mit der `-ignore -owners` Option, um den transienten Snapshot zu entfernen.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Wiederholen Sie den `snapmirror release` Befehl.

Verwandte Informationen

- "snapmirror Release"

Der Referenz-Snapshot für die Volume-Verschiebung wird als neuster SnapMirror-Snapshot für die ONTAP SnapMirror -Beziehung angezeigt.

Verwenden Sie die folgenden Informationen, wenn der Referenz-Snapshot der Volumeverschiebung nach einer Volumeverschiebungsoperation als der neueste für die SnapMirror -Beziehung angezeigt wird.

Problem:

Nach Durchführung eines Volume-Verschiebungsvorgangs auf einem Konsistenzgruppenvolume wird der Referenz-Snapshot für Volume-Verschiebung möglicherweise fälschlicherweise als der neueste für die SnapMirror-Beziehung angezeigt.

Sie können den neuesten Snapshot mit dem folgenden Befehl anzeigen:

```
snapmirror show -fields newest-snapshot status -expand
```

Lösung:

Führen Sie `snapmirror resync` nach Abschluss des Volume-Verschiebens manuell einen oder warten Sie auf die nächste automatische Neusynchronisierung.

Verwandte Informationen

- "SnapMirror-Neusynchronisierung"
- "Snapmirror-Show"

ONTAP Mediator für MetroCluster und SnapMirror Active Sync

Erfahren Sie mehr über ONTAP Mediator

Diese Dokumentation bezieht sich auf die On-Premise-Version von ONTAP Mediator. Informationen zum ONTAP Cloud Mediator, verfügbar ab ONTAP 9.17.1, finden Sie im "SnapMirror Active Sync-Dokumentation" .

ONTAP Mediator bietet mehrere Funktionen für ONTAP-Features:

- Persistenter Speicher mit Fencing für HA-Metadaten
- Dient als Ping-Proxy für Controller-Lebendigkeit.
- Bietet synchrone Funktionen für die Integritätsabfrage von Nodes zur Unterstützung der Quorumbestimmung.

ONTAP Mediator bietet zwei zusätzliche systemctl-Dienste:

- **`ontap_mediator.service`**

  Wartet den REST-API-Server zur Verwaltung der ONTAP-Beziehungen.

- **`mediator-scst.service`**

  Steuert das Starten und Herunterfahren des iSCSI-Moduls (SCST).

Für den Systemadministrator bereitgestellte Tools

Für den Systemadministrator bereitgestellte Tools:

- **`/usr/local/bin/mediator_change_password`**

  Legt ein neues API-Passwort fest, wenn der aktuelle API-Benutzername und das aktuelle Passwort angegeben werden.

- **`/usr/local/bin/mediator_change_user`**

  Legt einen neuen API-Benutzernamen fest, wenn der aktuelle API-Benutzername und das aktuelle Passwort angegeben werden.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  Generiert eine lokale tgz-Datei mit allen nützlichen Support-Informationen, die für die Kommunikation mit dem NetApp Kunden-Support benötigt werden. Dazu gehören Anwendungskonfiguration, Protokolle und einige Systeminformationen. Die Bundles werden auf der lokalen Festplatte generiert und können bei Bedarf manuell übertragen werden. Speicherort: /Opt/netapp/Data/Support_Bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  Entfernt das Paket ONTAP Mediator und das SCST-Kernelmodul. Dies schließt sämtliche Konfigurations-, Protokoll- und Mailbox-Daten ein.

- **`/usr/local/bin/mediator_unlock_user`**

  Gibt eine Sperre für das API-Benutzerkonto frei, wenn das Limit für Authentifizierungsversuche erreicht wurde. Diese Funktion wird verwendet, um die Herleitung von Brute Force-Passwörtern zu verhindern. Der Benutzer wird aufgefordert, den richtigen Benutzernamen und das richtige Passwort einzugeben.

- **`/usr/local/bin/mediator_add_user`**

  (Nur Support) wird verwendet, um den API-Benutzer bei der Installation hinzuzufügen.

Besondere Hinweise

ONTAP Mediator setzt bei der iSCSI-Bereitstellung auf SCST (siehe http://scst.sourceforge.net/index.html). Dieses Paket ist ein Kernelmodul, das während der Installation speziell für den Kernel kompiliert wird. Für Aktualisierungen des Kernels muss SCST möglicherweise neu installiert werden. Alternativ können Sie ONTAP Mediator deinstallieren und anschließend erneut installieren und anschließend die ONTAP-Beziehung neu konfigurieren.

Alle Aktualisierungen des Server-OS-Kernels sollten mit einem Wartungsfenster in ONTAP koordiniert werden.

Neue Funktionen in ONTAP Mediator

Mit jeder Version werden neue Verbesserungen für ONTAP Mediator bereitgestellt. Was ist neu?

Vorgestellt Werden

Informationen zur SCST-Version finden Sie im SCST Support-Matrix.

Version des ONTAP Mediators	Vorgestellt Werden
1,11	• Unterstützung für RHEL: ◦ Kompatibel: 9.5. ◦ Empfohlen: 10.1, 10.0, 9.7, 9.6, 9.4 und 8.10. • Unterstützung für Rocky Linux 10.1, 9.7 und 8.10. • Unterstützung für Oracle Linux 10.0 und 9.6. • Fügt Unterstützung für IPv6 für MetroCluster IP-Konfigurationen hinzu. • Fügt Unterstützung für fapolicyd hinzu.
1,10	• Unterstützung für RHEL: ◦ Kompatibel: 9.5. ◦ Empfohlen: 10.0, 9.6, 9.4 und 8.10. • Unterstützung für Rocky Linux 10.0, 9.6 und 8.10. • Aktualisiert die Basis-Python-Version von Python 3.9 auf Python 3.12.
1.9.1	• Unterstützung für RHEL: ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8. • Unterstützung für Rocky Linux 9.5 und 8.10. • Fügt neue Zertifikate zur Überprüfung von Codesignaturen hinzu. • Unterstützung für das Überspringen von Code-Signaturprüfungen mithilfe der `-skip-code-signature-check` Flagge. • Das Installationsprogramm zeigt Warnungen an, wenn es abgelaufene Codesignaturzertifikate erkennt.

1,9	• Unterstützung für RHEL: ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8. • Unterstützung für Rocky Linux 9.5 und 8.10. • FIPS-Unterstützung für RHEL und Rocky Linux. • Performance-Verbesserungen für mehr Skalierbarkeit. • Verbesserte Dateinamen, um die Einrichtung von PKI-signierten Zertifikaten zu vereinfachen.
1,8	• Unterstützung für RHEL: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 und 8.8. • Unterstützung für Rocky Linux 9.4 und 8.10.
1,7	• Unterstützung für RHEL: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.3, 9.2, 9.1, 9.0, 8.9 und 8.8. • Unterstützung für Rocky Linux 9.3 und 8.9. • Unterstützung von SAN-Daten (Subject Alternative Name) in selbstsignierten Zertifikaten und von Drittanbietern signierten Zertifikaten.
1,6	• Python 3.9-Updates. • Unterstützung für RHEL: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4. ◦ Empfohlen: 9.2, 9.1, 9.0 und 8.8. • Unterstützung für Rocky Linux 9.2 und 8.8. • Nicht mehr unterstützte RHEL 7.x/CentOS-Versionen.
1,5	• Unterstützung für RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6. • Enthält Abschreibungswarnungen für RHEL 7.x / CentOS 7.x. • Optimiert die Geschwindigkeit für größere SnapMirror Active Sync Systeme. • Dem Installationsprogramm wurde eine kryptografische Codesignatur hinzugefügt.
1,4	• Unterstützung für RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6. • Zusätzliche Unterstützung für Secure Boot (SB) der UFEI-basierten Firmware.

1,3	• Unterstützung für RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6.
1,2	• Unterstützung für RHEL 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6. • Unterstützung für CentOS 7.9, 7.8, 7.7 und 7.6. • Unterstützung für HTTPS-Mailboxen. • Zur Verwendung mit ONTAP 9.8+ MCC-IP AUSO und SnapMirror Active Sync ZRTO.
1,1	• Unterstützung für RHEL 8.0 und 7.6. • Unterstützung für CentOS 7.6. • Eliminiert Perl-Abhängigkeiten.
1,0	• Unterstützung von iSCSI-Mailboxen. • Zur Verwendung mit ONTAP 9.7+ MCC-IP AUSO. • Unterstützung für RHEL/CentOS 7.6.

OS Support-Matrix

Betriebssystem für ONTAP Mediator	1,11	1,10	1.9.1	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
RHEL 10,1	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 10.0	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,7	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9.6	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,5	Kompatibel	Kompatibel	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,4	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein

RHEL 9,3	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,2	Nein	Nein	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,1	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9,0	Nein	Nein	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8.10	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,9	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,8	Nein	Nein	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,7	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,6	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8,5	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
RHEL 8,4	Nein	Nein	Kompatibel	Kompatibel	Ja.	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
RHEL 8,3	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Nein	Nein	Nein
RHEL 8,2	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Nein	Nein	Nein
RHEL 8,1	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Nein	Nein
RHEL 8,0	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Ja.	Nein

RHEL und CentOS 7.9	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Kompatibel	Nein	Nein
RHEL und CentOS 7.8	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Nein	Nein
RHEL und CentOS 7.7	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Nein	Nein
RHEL und CentOS 7.6	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Ja.	Ja (nur RHEL)
CentOS 8 und Stream	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	1. A.	1. A.	1. A.
Rocky Linux 10,0	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Rocky Linux 9	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	1. A.	1. A.	1. A.	1. A.	1. A.	1. A.
Rocky Linux 8	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.	1. A.	1. A.	1. A.	1. A.	1. A.	1. A.
Oracle Linux 10,0	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
Oracle Linux 9	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein

- „Ja“ bedeutet, dass das Betriebssystem für die Installation von ONTAP Mediator empfohlen wird und

vollständig kompatibel und unterstützt ist.

- „Nein“ bedeutet, dass Betriebssystem und ONTAP Mediator nicht kompatibel sind.
- „Kompatibel“ bedeutet, dass Red Hat diese RHEL-Versionen nicht mehr unterstützt, ONTAP Mediator jedoch weiterhin darauf installiert werden kann.
- ONTAP Mediator 1.6 fügt Unterstützung für Rocky Linux 9 und 8 hinzu.
- ONTAP Mediator 1.5 war die letzte unterstützte Version für RHEL 7.x-Filialbetriebssysteme.
- CentOS 8 wurde für alle Versionen entfernt, da es erneut verzweigt wurde. CentOS Stream wurde als nicht geeignetes Produktionsziel-OS angesehen. Es ist keine Unterstützung geplant.

SCST Support-Matrix

Die folgende Tabelle zeigt die unterstützte SCST-Version für jede Version von ONTAP Mediator.

Version des ONTAP Mediators	Unterstützte SCST Version
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	Scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	Scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	Scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	Scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	Scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	Scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	Scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	Scst-3.5.0.tar.bz2
ONTAP Mediator 1.2	Scst-3.4.0.tar.bz2
ONTAP Mediator 1.1	Scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	Scst-3.3.0.tar.bz2

Installation oder Upgrade

Zusammenfassung des Installationsablaufs von ONTAP Mediator

Die Installation von ONTAP Mediator umfasst die Vorbereitung der Installation, die Bereitstellung des Zugriffs auf Repositorys, das Herunterladen des Installationspakets, die Überprüfung der Codesignatur, die Installation des ONTAP Mediator-Pakets und die Durchführung von Konfigurationsaufgaben nach der Installation.

1. **"Vorbereiten der Installation oder Aktualisierung von ONTAP Mediator"**

Um ONTAP Mediator zu installieren oder zu aktualisieren, müssen Sie sicherstellen, dass alle Voraussetzungen erfüllt sind.

2 **"Upgrade von Host-Betriebssystem und Mediator"**

Wenn Sie eine vorhandene Version von ONTAP Mediator aktualisieren, müssen Sie zuerst die vorherige Version deinstallieren und dann die neue Version installieren. Wenn Sie ONTAP Mediator zum ersten Mal installieren, können Sie diesen Schritt überspringen.

3 **"Gewähren von Repository-Zugriff"**

Sie sollten den Zugriff auf Repositorys aktivieren, damit ONTAP Mediator während des Installationsvorgangs auf die erforderlichen Pakete zugreifen kann.

4 **"Laden Sie das Installationspaket für ONTAP Mediator herunter"**

Laden Sie das ONTAP Mediator-Installationspaket von der ONTAP Mediator-Downloadseite herunter.

5 **"Überprüfen Sie die Codesignatur des ONTAP Mediator-Installationspakets"**

NetApp empfiehlt, die Codesignatur des ONTAP Mediators zu überprüfen, bevor Sie das ONTAP Mediator-Installationspaket installieren.

6 **"Installieren Sie ONTAP Mediator"**

Um ONTAP Mediator zu installieren, müssen Sie das Installationspaket herunterladen und das Installationsprogramm auf dem Host ausführen.

7 **"Überprüfen Sie die ONTAP Mediator-Installation"**

Überprüfen Sie nach der Installation von ONTAP Mediator, ob es erfolgreich ausgeführt wird.

8 **"Durchführen von Konfigurationsaufgaben nach der Installation"**

Nachdem ONTAP Mediator installiert und ausgeführt wird, müssen zusätzliche Konfigurationsaufgaben ausgeführt werden, um die Funktionen von ONTAP Mediator zu verwenden.

Installieren oder aktualisieren Sie ONTAP Mediator

Um ONTAP Mediator zu installieren oder zu aktualisieren, müssen Sie alle Voraussetzungen erfüllen, das Installationspaket herunterladen und das Installationsprogramm auf dem Host ausführen.

- Ab ONTAP 9.8 können Sie jede Version von ONTAP Mediator verwenden, um eine aktive SnapMirror Sync Beziehung zu überwachen.
- Sie können jede Version von ONTAP Mediator verwenden, um eine MetroCluster -IP-Konfiguration zu überwachen.

Überlegungen zur Installation und zum Upgrade

Bitte beachten Sie diese Punkte, bevor Sie ONTAP Mediator aktualisieren oder installieren.

> ONTAP Mediator 1.8 und ältere Versionen sind nicht mit dem FIPS-Modus von Red Hat Enterprise Linux (RHEL) kompatibel und verhindern daher eine erfolgreiche Installation. Sie können mit folgendem Befehl überprüfen, ob der FIPS-Modus aktiviert ist: `fips-mode-setup --check` Befehl. Sie können den FIPS-Modus deaktivieren, indem Sie `fips-modesetup --disable` Befehl. Führen Sie nach dem Deaktivieren des FIPS-Modus einen Neustart durch, um ONTAP Mediator 1.8 oder früher erfolgreich zu installieren.

- Sie sollten ONTAP Mediator auf die neueste Version aktualisieren. Ältere Versionen funktionieren weiterhin mit allen ONTAP Releases, neuere Versionen enthalten jedoch Sicherheitspatches für Drittanbieterkomponenten.
- Wenn Sie ein Upgrade auf eine neue ONTAP Mediator-Version durchführen, wird das Installationsprogramm automatisch auf die empfohlene SCST-Version aktualisiert, sofern keine höhere Version verfügbar ist. Anweisungen zur manuellen Installation einer höheren SCST-Version finden Sie unter "ONTAP Mediator verwalten". Informationen zu unterstützten Versionen finden Sie im "SCST Support-Matrix".

> - Falls die Installation fehlschlägt, müssen Sie möglicherweise auf eine neuere Version von ONTAP Mediator aktualisieren.
> - Ab dem 15. Juni 2025 können Sie ONTAP Mediator 1.9 und 1.8 nicht mehr installieren oder aktualisieren, da deren Code Signing-Zertifikate abgelaufen sind. Wenn die Installation oder das Upgrade fehlschlägt, verwenden Sie stattdessen die Patch-Version von ONTAP Mediator 1.9.1.

- Wenn Sie das `yum-utils` Paket installieren, können Sie den `needs-restarting` Befehl verwenden.
- Ab ONTAP Mediator 1.11 wird IPv6 für MetroCluster -IP-Konfigurationen unterstützt.

Host-Anforderungen erfüllt

Befolgen Sie diese Anforderungen, wenn Sie RHEL oder Rocky Linux installieren und die zugehörigen Repositories konfigurieren.

> Wenn Sie den Installations- oder Konfigurationsprozess ändern, müssen Sie möglicherweise weitere Schritte ausführen.

Anforderungen für die Linux-Distribution

- Installieren Sie RHEL oder Rocky Linux gemäß den Best Practices von Red Hat. Da CentOS 8.x das Ende seines Lebenszyklus erreicht hat, werden kompatible Versionen von CentOS 8.x nicht empfohlen.
- Stellen Sie bei der Installation von ONTAP Mediator sicher, dass das System Zugriff auf das erforderliche Repository hat, damit das Installationsprogramm alle erforderlichen Softwareabhängigkeiten abrufen und installieren kann.
- Um dem yum-Installer zu ermöglichen, abhängige Software in den RHEL-Repositorys zu finden, registrieren Sie das System während der Installation oder danach mit einer gültigen Red hat Subskription.

> Weitere Informationen finden Sie in der Dokumentation zu Red hat Subscription Manager.

Netzwerkanforderungen

Stellen Sie sicher, dass die folgenden Ports für ONTAP Mediator verfügbar und nicht verwendet werden:

Port/Services	Quelle	Richtung	Ziel	Zweck
22/tcp	Management-Host	Eingehend	ONTAP Mediator	(Optional) SSH / ONTAP Mediatormanagement
31784/tcp	Cluster-Management-LIFs	Eingehend	Web-Server ONTAP Mediator	(ERFORDERLICH) REST-API (HTTPS)
3260/tcp [1]	Node-Daten-LIFs oder Node-Management-LIFs	Bidirektional	ONTAP Mediator iSCSI-Ziele	(Erforderlich für MetroCluster IP-Konfigurationen) iSCSI-Datenverbindung für Mailboxen

Für SMBC-Kunden muss für ONTAP Port 3260 nicht aktiviert oder verbunden sein.

- Wenn Sie eine Firewall eines Drittanbieters verwenden, siehe"Firewall-Anforderungen für ONTAP Mediator" Die
- Stellen Sie bei Linux-Hosts ohne Internetzugang sicher, dass die erforderlichen Pakete in einem lokalen Repository verfügbar sind.

  Wenn Sie Link Aggregation Control Protocol (LACP) in einer Linux-Umgebung verwenden, konfigurieren Sie den Kernel und setzen Sie den `sysctl net.ipv4.conf.all.arp_ignore` auf `2`.

Anforderungen an das Betriebssystem

Ihr Betriebssystem muss die folgenden Anforderungen erfüllen:

- 64-Bit physische Installation oder virtuelle Maschine
- 8 GB RAM
- 1 GB Festplattenspeicher (wird für die Installation von Anwendungen, Serverprotokollen und die Datenbank verwendet)
- Benutzer: Root-Zugriff

Die folgende Tabelle zeigt die unterstützten Betriebssysteme für jede Version von ONTAP Mediator.

Version des ONTAP Mediators	Unterstützte Linux-Versionen
1,11	• Red Hat Enterprise Linux ◦ Kompatibel: 9.5 [1] ◦ Empfohlen: 10.1, 10.0, 9.7, 9.6, 9.4 und 8.10 • Rocky Linux 10,1, 9.7 und 8.10 • Oracle Linux 10.0 und 9.6

1,10	• Red Hat Enterprise Linux ◦ Kompatibel: 9.5 [1] ◦ Empfohlen: 10,0, 9,6, 9,4 und 8,10 • Rocky Linux 10,0, 9.6 und 8.10
1.9.1	• Red Hat Enterprise Linux ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8 • Rocky Linux 9.5 und 8.10
1,9	• Red Hat Enterprise Linux ◦ Kompatibel: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.5, 9.4, 9.2, 9.0, 8.10 und 8.8 • Rocky Linux 9.5 und 8.10
1,8	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 und 8.8 • Rocky Linux 9.4 und 8.10
1,7	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.3, 9.2, 9.1, 9.0, 8.9 und 8.8 • Rocky Linux 9.3 und 8.9
1,6	• Red Hat Enterprise Linux: ◦ Kompatibel: 8.7, 8.6, 8.5 und 8.4 [1] ◦ Empfohlen: 9.2, 9.1, 9.0 und 8.8 • Rocky Linux 9.2 und 8.8
1,5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6
1,3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6

1,2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 und 7.6 • CentOS: 7.9, 7.8, 7.7 und 7.6

1. Kompatibel bedeutet, dass Red Hat diese RHEL-Versionen nicht mehr unterstützt, ONTAP Mediator jedoch weiterhin darauf installiert werden kann.

BS-erforderliche Pakete

Die folgenden Pakete werden von ONTAP Mediator benötigt:

Die Pakete werden entweder vorinstalliert oder automatisch vom ONTAP Mediator Installer installiert.

Alle RHEL/CentOS Versionen	Zusätzliche Pakete für RHEL 10.x / Rocky Linux 10	Zusätzliche Pakete für RHEL 9.x / Rocky Linux 9	Zusätzliche Pakete für RHEL 8.x / Rocky Linux 8
• openssl • openssl-devel • Kernel-devel-€ (uname -r) • gcc • Make • Libselinux-utils • Patch • bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeuMaker • Efibootmgr • Mokutil	• python3.12 • python3.12-devel	• Elfutils-libelf-devel • Politicoreutils-Python-utils • python3 • python3-devel	• Elfutils-libelf-devel • Politicoreutils-Python-utils • Redhat-lsb-Core • Python39 • Python39-devel

Das Mediator-Installationspaket ist eine selbst extrahierende komprimierte tar-Datei, die Folgendes enthält:

- Eine RPM-Datei, die alle Abhängigkeiten enthält, die nicht aus dem Repository des unterstützten Release abgerufen werden können.
- Ein Installationsskript.

Ein gültiges SSL-Zertifikat wird empfohlen.

Überlegungen zum Betriebssystem-Upgrade und zur Kernel-Kompatibilität

- Sie können alle Bibliothekspakete außer dem Kernel aktualisieren, aber möglicherweise müssen Sie das System neu starten, um die Änderungen im ONTAP Mediator anzuwenden. Planen Sie Ausfallzeiten ein, falls ein Neustart erforderlich ist.
- Sie sollten den Betriebssystemkernel auf dem neuesten Stand halten. Aktualisieren Sie den Kernel auf

eine unterstützte Version, die in der Liste aufgeführt ist."ONTAP Mediator-Versionsmatrix" Die Das System muss neu gestartet werden, planen Sie daher ein Wartungsfenster für den Ausfall ein.

- Deinstallieren Sie das SCST-Kernelmodul vor dem Neustart und installieren Sie es anschließend wieder.
- Halten Sie eine unterstützte Version von SCST bereit, die Sie vor dem Kernel-OS-Upgrade neu installieren können.

- Die Kernel-Version muss mit der Betriebssystemversion übereinstimmen.
- Aktualisieren Sie den Kernel nicht über die für Ihre ONTAP Mediator-Version unterstützte Betriebssystemversion hinaus, da das getestete SCST-Modul wahrscheinlich nicht funktionieren wird.

Installieren Sie ONTAP Mediator, wenn UEFI Secure Boot aktiviert ist

ONTAP Mediator kann auf einem System mit oder ohne aktiviertem UEFI Secure Boot installiert werden.

Über diese Aufgabe

Sie können den UEFI-sicheren Start vor der Installation von ONTAP Mediator deaktivieren, wenn dieser nicht benötigt wird oder wenn Sie Probleme bei der Installation von ONTAP Mediator beheben. Deaktivieren Sie die UEFI Secure Boot-Option in den Computereinstellungen.

Detaillierte Anweisungen zum Deaktivieren des UEFI Secure Boot finden Sie in der Dokumentation zu Ihrem Host-Betriebssystem.

Um ONTAP Mediator mit aktiviertem UEFI Secure Boot zu installieren, müssen Sie einen Sicherheitsschlüssel registrieren, bevor der Dienst gestartet werden kann. Der Schlüssel wird während des Kompilierungsschritts der SCST-Installation generiert und als privates öffentliches Schlüsselpaar auf Ihrer Maschine gespeichert. Verwenden Sie das `mokutil` Dienstprogramm, um den öffentlichen Schlüssel als Machine Owner Key (MOK) zu Ihrer UEFI-Firmware hinzuzufügen, sodass das System dem signierten Modul vertrauen und laden kann. Speichern Sie die `mokutil` Passphrase an einem sicheren Ort, da dies erforderlich ist, wenn Sie Ihr System neu starten, um das MOK zu aktivieren.

Schritte

1. Überprüfen Sie, ob UEFI Secure Boot auf Ihrem System aktiviert ist:

   ```
   mokutil --sb-state
   ```

   Die Ergebnisse zeigen an, ob UEFI Secure Boot auf diesem System aktiviert ist.

Wenn…	Gehe zu…
UEFI Secure Boot ist aktiviert	
UEFI Secure Boot ist deaktiviert	"Aktualisieren Sie das Host-Betriebssystem und dann ONTAP Mediator"

- Sie werden aufgefordert, eine Passphrase zu erstellen, die Sie an einem sicheren Ort speichern müssen. Sie benötigen diese Passphrase, um den Schlüssel im UEFI Boot Manager zu aktivieren.
- ONTAP Mediator 1.2.0 und frühere Versionen unterstützen diesen Modus nicht.

2. Wenn das `mokutil` Dienstprogramm nicht installiert ist, führen Sie den folgenden Befehl aus:

```
yum install mokutil
```

Aktualisieren Sie das Host-Betriebssystem und den ONTAP Mediator

Um das Host-Betriebssystem für ONTAP Mediator auf eine neuere Version zu aktualisieren, müssen Sie ONTAP Mediator zuerst deinstallieren.

Über diese Aufgabe

Vor dem Upgrade des Host-Betriebssystems für ONTAP Mediator mit dem leapp-upgrade-Tool muss ONTAP Mediator deinstalliert werden. Das Tool prüft, ob in registrierten Repositories neue RPM-Versionen verfügbar sind.

Der ONTAP Mediator Installer installiert eine .rpm-Datei, die das Tool leapp-upgrade in die Suche einbezieht. Da das Installationsprogramm die Datei entpackt, anstatt sie aus einem registrierten Repository herunterzuladen, kann das Tool kein Upgrade finden. Sie müssen das Tool leapp-upgrade verwenden, um das Paket zu deinstallieren.

Schritte

1. Sichern Sie die Protokolldateien:

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Führen Sie das Upgrade mit dem leapp-upgrade-Tool durch:

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. ONTAP Mediator neu installieren:

> Führen Sie die restlichen Schritte unmittelbar nach der Neuinstallation von ONTAP Mediator aus, um einen Verlust von Protokolldateien zu verhindern.

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Stoppen Sie ontap_mediator:

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Ersetzen Sie die Protokolldateien:

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Start ontap_mediator:

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Verbinden Sie alle ONTAP Cluster wieder mit dem aktualisierten ONTAP Mediator:

MetroCluster über IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

SnapMirror Active Sync

Für SnapMirror Active Sync ist keine Neuinstallation der außerhalb von /opt/netapp gespeicherten TLS-Zertifikate erforderlich. Sichern und stellen Sie die in /opt/netapp gespeicherten Zertifikate wieder her.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                         ONTAPMediatorCA                        server-
ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

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: 44786524464C5113D5EC966779D3002135EA4254
```

```
The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


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: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

Verwandte Informationen

- "Sicherheitszertifikat löschen"
- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "SnapMirror Mediator hinzufügen"
- "SnapMirror Mediator entfernen"
- "Speicher-ISCSI-Initiator anzeigen"

Bereitstellung von Repository-Zugriff für die Installation von ONTAP Mediator

Sie sollten den Zugriff auf Repositorys aktivieren, damit ONTAP Mediator während des Installationsvorgangs auf die erforderlichen Pakete zugreifen kann.

Schritte

1. Legen Sie fest, auf welche Repositorys zugegriffen werden muss, wie in der folgenden Tabelle dargestellt:

Wenn Ihr Betriebssystem…	Zugriff auf diese Repositorys ist erforderlich…
RHEL 10.x	• rhel-10-für-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-für-x86_64-baseos-eff • rhel-9-für-x86_64-appstream-Effektivwert
RHEL 8.x	• rhel-8-für-x86_64-baseos-eff • rhel-8-für-x86_64-appstream-Effektivwert
RHEL 7.x	• rhel-7-Server-fakultative-Rpms
CentOS 7.x	• C7.6.1810 - Basis-Repository
Rocky Linux 10	• appstream • Baseos
Rocky Linux 9	• appstream • Baseos
Rocky Linux 8	• appstream • Baseos

2. Verwenden Sie eines der folgenden Verfahren, um den Zugriff auf die oben aufgeführten Repositories zu ermöglichen, damit ONTAP Mediator während des Installationsvorgangs auf die erforderlichen Pakete zugreifen kann.

Wenn ONTAP Mediator Abhängigkeiten von Python-Modulen in den Repositories "Extras" und "Optional" hat, muss er möglicherweise auf die `rhel-X-for-x86_64-extras-rpms` Und `rhel-X-for-x86_64-optional-rpms` Dateien.

Vorgehensweise für das Betriebssystem RHEL 10.x

Verwenden Sie dieses Verfahren, wenn Ihr Betriebssystem **RHEL 10.x** ist, um den Zugriff auf Repositorys zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

2. Führen Sie den `yum repolist` Befehl aus.

Die neu abonnierten Repositories sollten in der Liste angezeigt werden.

Verfahren für das RHEL 9.x-Betriebssystem

Gehen Sie folgendermaßen vor, wenn Ihr Betriebssystem **RHEL 9.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Führen Sie den `yum repolist` Befehl aus.

Die neu abonnierten Repositories sollten in der Liste angezeigt werden.

Verfahren für das RHEL 8.x-Betriebssystem

Gehen Sie folgendermaßen vor, wenn Ihr Betriebssystem **RHEL 8.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Führen Sie den `yum repolist` Befehl aus.

Die neu abonnierten Repositories sollten in der Liste angezeigt werden.

Verfahren für das RHEL 7.x-Betriebssystem

Gehen Sie folgendermaßen vor, wenn Ihr Betriebssystem **RHEL 7.x** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie das erforderliche Repository:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

Das folgende Beispiel zeigt die Ausführung dieses Befehls:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. Führen Sie den `yum repolist` Befehl aus.

Das folgende Beispiel zeigt die Ausführung dieses Befehls. In der Liste sollte das Repository „RHEL-7-Server-fakultative-rpms“ erscheinen.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                      repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
Linux 7 Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

Verfahren für das Betriebssystem CentOS 7.x

Gehen Sie folgendermaßen vor, wenn Ihr Betriebssystem **CentOS 7.x** ist, um den Zugriff auf Repositories zu ermöglichen:

> Die folgenden Beispiele zeigen ein Repository für CentOS 7.6 und funktionieren möglicherweise nicht für andere CentOS-Versionen. Verwenden Sie das Basis-Repository für Ihre Version von CentOS.

Schritte

1. Fügen Sie das C7.6.1810 - Basis-Repository hinzu. Das C7.6.1810 - Base Vault Repository enthält das für ONTAP Mediator erforderliche "Kernel-devel" Paket.
2. Fügen Sie die folgenden Zeilen zu /etc/yum.repos.d/CentOS-Vault.repo hinzu.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Führen Sie den `yum repolist` Befehl aus.

   Das folgende Beispiel zeigt die Ausführung dieses Befehls. Das CentOS-7.6.1810 - Base Repository sollte in der Liste angezeigt werden.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                    repo name                status
C7.6.1810-base/x86_64      CentOS-7.6.1810 - Base   10,019
base/7/x86_64              CentOS-7 - Base          10,097
extras/7/x86_64            CentOS-7 - Extras        307
updates/7/x86_64           CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Vorgehensweise für die Betriebssysteme Rocky Linux 10, 9 oder 8

Verwenden Sie dieses Verfahren, wenn Ihr Betriebssystem **Rocky Linux 10**, **Rocky Linux 9** oder **Rocky Linux 8** ist, um den Zugriff auf Repositories zu ermöglichen:

Schritte

1. Abonnieren Sie die erforderlichen Repositorys:

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. Führen Sie einen `clean` Vorgang durch:

```
dnf clean all
```

3. Überprüfen Sie die Liste der Repositorys:

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 10 - AppStream
baseos                          Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 8 - AppStream
baseos                          Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

Laden Sie das Installationspaket für ONTAP Mediator herunter

Laden Sie das ONTAP Mediator-Installationspaket herunter und installieren Sie es.

Schritte

1. Laden Sie das ONTAP Mediator-Installationspaket von der ONTAP Mediator-Downloadseite herunter.

   "Download-Seite für ONTAP Mediator"

2. Stellen Sie sicher, dass Sie das Mediator-Installationspaket im aktuellen Arbeitsverzeichnis abgelegt haben:

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
   ```

   ```
   ontap-mediator-1.11.0.tgz
   ```

   Für ONTAP Mediator Versionen 1.4 und früher wird der Installer benannt `ontap-mediator`.

   Falls Ihr System keinen Internetzugang hat, stellen Sie sicher, dass das Installationsprogramm auf die erforderlichen Pakete zugreifen kann.

3. Verschieben Sie das Mediator-Installationspaket gegebenenfalls in das Installationsverzeichnis.
4. Entpacken Sie das Installationspaket:

   ```
   tar xvfz ontap-mediator-1.11.0.tgz
   ```

```
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

Überprüfen Sie die ONTAP Mediator-Code-Signatur

NetApp empfiehlt, die Codesignatur des ONTAP Mediators vor der Installation zu überprüfen. Dieser Schritt ist optional.

Bevor Sie beginnen

Stellen Sie sicher, dass Ihr System diese Anforderungen erfüllt, bevor Sie die Codesignatur des ONTAP Mediators überprüfen.

- Ab dem 15. Juni 2025 ist eine Installation oder ein Upgrade auf ONTAP Mediator 1.9 und 1.8 nicht mehr möglich, da die Zertifikate zur Codesignatur-Verifizierung abgelaufen sind. Installieren oder aktualisieren Sie stattdessen ONTAP Mediator 1.11 oder 1.10.
- Wenn das System die folgenden Anforderungen nicht erfüllt, ist der Überprüfungsprozess nicht erforderlich und Sie können direkt zu gehen"Installieren Sie das Installationspaket für den ONTAP Mediator".

- openssl-Versionen 1.0.2 bis 3.0 für grundlegende Überprüfung
- openssl Version 1.1.0 oder höher für den Betrieb der TSA (Time Stamping Authority)
- Öffentlicher Internetzugang zur OCSP-Verifizierung

Das Downloadpaket enthält folgende Dateien:

Datei	Beschreibung
`ONTAP-Mediator-production.pub`	Der öffentliche Schlüssel, der zur Überprüfung der Signatur verwendet wird
`csc-prod-chain-ONTAP-Mediator.pem`	Die öffentliche Zertifizierung CA-Kette des Vertrauens
`csc-prod-ONTAP-Mediator.pem`	Das Zertifikat, mit dem der Schlüssel generiert wird
`ontap-mediator-1.11.0`	Die Installationsdatei für Version 1.11

`ontap-mediator-1.11.0.sig`	Der SHA-256 wurde gehasht, dann RSA-signiert mit dem csc-prod-Schlüssel, Signatur für das Installationsprogramm
`ontap-mediator-1.11.0.sig.tsr`	Die Annullierungsanfrage für die Verwendung durch OCSCP für die Unterschrift des Installers
`ontap-mediator-1.11.0.tsr`	Die Anforderungsdatei für die Zeitstempelsignierung
`tsa-prod-ONTAP-Mediator.pem`	Das öffentliche Zertifikat für den TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	Das öffentliche Zertifikat CA-Kette für den TSR

Schritte

1. Führen Sie die Sperrprüfung `csc-prod-ONTAP-Mediator.pem` mit dem Online Certificate Status Protocol (OCSP) durch.
   a. Ermitteln Sie die OCSP-URL für das Zertifikat. Entwicklerzertifikate liefern möglicherweise keine URI:

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. Erstellen Sie eine OCSP-Anfrage für das Zertifikat.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. Verbinden Sie sich mit dem OCSP-Manager, um die OCSP-Anfrage zu senden:

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. Überprüfung der Vertrauenskette des Kundensupportzentrums und der Ablaufdaten am lokalen Host:

   `openssl verify`

   Die `openssl` Version vom PFAD muss eine gültige `cert.pem` (nicht selbstsignierte) Version haben.

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Überprüfen Sie die `ontap-mediator-1.11.0.sig.tsr` Und `ontap-mediator-1.11.0.tsr` Dateien, die die zugehörigen Zertifikate verwenden:

OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-
1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
```

OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-
1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```

`.tsr`Die Dateien enthalten den Zeitstempel der Antwort des Installationsprogramms und die Codesignatur. Die Verarbeitung bestätigt, dass der Zeitstempel eine gültige Signatur der TSA aufweist und dass Ihre Eingabedatei nicht verändert wurde. Die Überprüfung wird lokal von Ihrem Rechner durchgeführt. Sie müssen nicht auf die TSA-Server zugreifen.

4. Überprüfen Sie die Signaturen gegen den Schlüssel:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

Installieren Sie das Installationspaket für den ONTAP Mediator

Um ONTAP Mediator zu installieren, müssen Sie das Installationspaket herunterladen und das Installationsprogramm auf dem Host ausführen.

Schritte

1. Führen Sie das Installationsprogramm aus, und reagieren Sie auf die Eingabeaufforderungen, falls erforderlich:

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

Um die Signaturprüfung während der Installation zu überspringen, verwenden Sie diesen Befehl: `./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code-signature-check`

Das Installationsprogramm erstellt die erforderlichen Konten und installiert die benötigten Pakete. Falls der Mediator bereits installiert ist, werden Sie zum Upgrade aufgefordert.

Beispiel für die Installation des ONTAP Mediators (Konsolenausgang)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[root@mediator_host ~]#./ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? yes/no: yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Would you like to use the default account names: netapp +
mediatoradmin? (Y(es)/n(o)): yes



Enter ONTAP Mediator user account (mediatoradmin) password:
```

```
Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.


+ Checking for default Linux firewall


+ Installing required packages.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
=========================
 Package
Architecture                                        Version
Repository                                              Size
================================================================================
================================================================================
================================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                              0.192-5.el10
```

```
AppStream                                          50 k
 gcc
x86_64                                        14.2.1-7.el10
AppStream                                          37 M
 kernel-devel
x86_64                                        6.12.0-55.9.1.el10_0
AppStream                                          22 M
 make
x86_64                                        1:4.4.1-9.el10
BaseOS                                            591 k
 openssl-devel
x86_64                                        1:3.2.2-16.el10
AppStream                                         3.9 M
 patch
x86_64                                        2.7.6-26.el10
AppStream                                         134 k
 perl-ExtUtils-MakeMaker
noarch                                        2:7.70-513.el10
AppStream                                          297 k
 python3-devel
x86_64                                        3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                        23.3.2-7.el10
AppStream                                         3.2 M
Installing dependencies:
 annobin-docs
noarch                                        12.92-1.el10
AppStream                                          94 k
 annobin-plugin-gcc
x86_64                                        12.92-1.el10
AppStream                                         985 k
 bison
x86_64                                        3.8.2-9.el10
AppStream                                         1.0 M
 cmake-filesystem
x86_64                                        3.30.5-2.el10
AppStream                                          29 k
 cpp
x86_64                                        14.2.1-7.el10
AppStream                                          12 M
 dwz
x86_64                                        0.15-7.el10
AppStream                                         139 k
 efi-srpm-macros
```

```
noarch                                          6-6.el10
AppStream                                          25 k
 flex
x86_64                                          2.6.4-19.el10
AppStream                                         303 k
 fonts-srpm-macros
noarch                                          1:2.0.5-18.el10
AppStream                                          29 k
 forge-srpm-macros
noarch                                          0.4.0-6.el10
AppStream                                          23 k
 gcc-plugin-annobin
x86_64                                          14.2.1-7.el10
AppStream                                          62 k
 glibc-devel
x86_64                                          2.39-37.el10
AppStream                                         641 k
 go-srpm-macros
noarch                                          3.6.0-4.el10
AppStream                                          29 k
 kernel-headers
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                         2.3 M
 kernel-srpm-macros
noarch                                          1.0-25.el10
AppStream                                          11 k
 libxcrypt-devel
x86_64                                          4.4.36-10.el10
AppStream                                          33 k
 libzstd-devel
x86_64                                          1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                          1-15.el10
AppStream                                          10 k
 m4
x86_64                                          1.4.19-11.el10
AppStream                                         309 k
 ocaml-srpm-macros
noarch                                          10-4.el10
AppStream                                          10 k
 openblas-srpm-macros
noarch                                          2-19.el10
AppStream                                         9.0 k
 package-notes-srpm-macros
```

```
noarch                                          0.5-13.el10
AppStream                                          11 k
 perl-AutoSplit
noarch                                          5.74-512.el10
AppStream                                          23 k
 perl-Benchmark
noarch                                          1.25-512.el10
AppStream                                          28 k
 perl-CPAN-Meta-Requirements
noarch                                          2.143-11.el10
AppStream                                          39 k
 perl-CPAN-Meta-YAML
noarch                                          0.018-512.el10
AppStream                                          29 k
 perl-Devel-PPPort
x86_64                                          3.72-512.el10
AppStream                                         223 k
 perl-ExtUtils-Command
noarch                                          2:7.70-513.el10
AppStream                                          16 k
 perl-ExtUtils-Constant
noarch                                          0.25-512.el10
AppStream                                          47 k
 perl-ExtUtils-Install
noarch                                          2.22-511.el10
AppStream                                          47 k
 perl-ExtUtils-Manifest
noarch                                          1:1.75-511.el10
AppStream                                          37 k
 perl-ExtUtils-ParseXS
noarch                                          1:3.51-512.el10
AppStream                                         190 k
 perl-File-Compare
noarch                                          1.100.800-512.el10
AppStream                                          15 k
 perl-File-Copy
noarch                                          2.41-512.el10
AppStream                                          22 k
 perl-I18N-Langinfo
x86_64                                          0.24-512.el10
AppStream                                          28 k
 perl-JSON-PP
noarch                                          1:4.16-512.el10
AppStream                                          69 k
 perl-Test-Harness
noarch                                          1:3.48-512.el10
```

```
AppStream                                          288 k
 perl-lib
x86_64                                          0.65-512.el10
AppStream                                           16 k
 perl-srpm-macros
noarch                                          1-57.el10
AppStream                                          9.7 k
 perl-version
x86_64                                          8:0.99.32-4.el10
AppStream                                           68 k
 pyproject-srpm-macros
noarch                                          1.16.2-1.el10
AppStream                                           16 k
 python-srpm-macros
noarch                                          3.12-9.1.el10
AppStream                                           26 k
 python3-pyparsing
noarch                                          3.1.1-7.el10
BaseOS                                             273 k
 qt6-srpm-macros
noarch                                          6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                          288-1.el10
AppStream                                           83 k
 rust-toolset-srpm-macros
noarch                                          1.84.1-1.el10
AppStream                                           13 k
 systemtap-sdt-devel
x86_64                                          5.2-2.el10
AppStream                                           78 k
 systemtap-sdt-dtrace
x86_64                                          5.2-2.el10
AppStream                                           72 k
 zlib-ng-compat-devel
x86_64                                          2.2.3-1.el10
AppStream                                           41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                          2.150010-511.el10
AppStream                                          202 k
 perl-Encode-Locale
noarch                                          1.05-31.el10
AppStream                                           21 k
 perl-Time-HiRes
```

```
x86_64                                                 4:1.9777-511.el10
AppStream                                                  62 k
 perl-devel
x86_64                                                 4:5.40.1-512.el10
AppStream                                                 772 k
 perl-doc
noarch                                                 5.40.1-512.el10
AppStream                                                 4.9 M

Transaction Summary
================================================================================
================================================================================
================================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
```

```
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```

```
  Installing       : perl-Benchmark-1.25-512.el10.noarch
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                  elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                       fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64               go-
```

```
srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                          make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch       perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch  perl-CPAN-Meta-YAML-0.018-
512.el10.noarch   perl-Devel-PPPort-3.72-512.el10.x86_64          perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch  perl-ExtUtils-Constant-
0.25-512.el10.noarch       perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch  perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch  perl-File-Compare-
1.100.800-512.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64         perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64          perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch             perl-version-8:0.99.32-
4.el10.x86_64              pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch             qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20250715160240.log)
    This step takes several minutes. View progress in the log file.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that a reboot is
needed.
     SCST does not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

Registrieren Sie den Sicherheitsschlüssel für UEFI Secure Boot

Ab ONTAP Mediator 1.4 ist der Secure-Boot-Mechanismus auf UEFI-Systemen aktiviert. Wenn Secure Boot aktiviert ist, müssen Sie nach der Installation zusätzliche Schritte unternehmen, um den Sicherheitsschlüssel zu registrieren.

Schritte

1. Befolgen Sie die Anweisungen in der README-Datei, um das SCST-Kernelmodul zu signieren:

   ```
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
   signing
   ```

2. Suchen Sie die erforderlichen Schlüssel:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

> Nach der Installation werden im System die README-Dateien und der Speicherort der Schlüssel angezeigt.

3. Öffentlichen Schlüssel zur MOK-Liste hinzufügen:

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

> Sie können den privaten Schlüssel an seinem Standardspeicherort belassen oder ihn an einen sicheren Ort verschieben. Sie müssen den öffentlichen Schlüssel an seinem aktuellen Speicherort belassen, damit der Boot Manager ihn verwenden kann. Weitere Informationen finden Sie in der Datei README.module-signing:
>
> ```
> [root@hostname ~]# ls
> /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
> README.module-signing scst_module_key.der scst_module_key.priv
> ```

4. Starten Sie den Host neu und verwenden Sie den UEFI Boot Manager Ihres Geräts, um das neue MOK zu genehmigen. Sie benötigen die mitgelieferte Passphrase für die `mokutil` Nutzen in"Installieren Sie ONTAP Mediator, wenn UEFI Secure Boot aktiviert ist" Die

Signieren von SCST-Kernelmodulen

Nach der Installation von ONTAP Mediator, wenn der systemctl-Status `mediator-scst` Wird als fehlgeschlagen (inaktiv) angezeigt, befolgen Sie diese Schritte, um das SCST-Kernelmodul zu signieren.

Schritte

1. Während des Build-Prozesses wird ein öffentliches/privates Schlüsselpaar generiert. `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` Verzeichnis, indem Sie den folgenden Befehl verwenden:

```
[root@mediator-host ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
[root@mediator-host ~]#
```

2. Starten Sie den Vorgang des Importierens des öffentlichen Schlüssels in das UEFI-Schlüsselrepository, indem Sie die folgenden Befehle ausführen:

```
[root@mediator-host ~]# mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
input password:
input password again:

[root@mediator-host ~]#
```

3. Die Software mokutil verlangt während des Importvorgangs ein temporäres Passwort für diesen Schlüssel.
4. Überprüfen Sie, ob der Importvorgang mit dem `mokutil --list-new` und starten Sie das System anschließend neu. Der Bootloader startet den EFI MOK Manager.
5. Verwenden Sie die Menüs auf dem Bildschirm, um den SCST-Kernelmodulschlüssel zu aktivieren. Nach dem Booten ausführen `systemctl status mediator-scst` Die Sobald der Dienst startet, werden die SCST-Kernelmodule signiert.

Überprüfen Sie den Installationsstatus des ONTAP Mediators

Überprüfen Sie nach der Installation von ONTAP Mediator, ob es erfolgreich ausgeführt wird.

Schritte

1. Zeigen Sie den Status von ONTAP Mediator an:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Bestätigen Sie die von ONTAP Mediator verwendeten Ports:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

         tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

         tcp6   0    0 :::3260          :::*            LISTEN
```

Konfiguration des ONTAP Mediators nach der Installation

Nachdem ONTAP Mediator installiert und ausgeführt wird, müssen zusätzliche Konfigurationsaufgaben im ONTAP-Speichersystem ausgeführt werden, um die Funktionen von ONTAP Mediator nutzen zu können:

- Informationen zur Verwendung von ONTAP Mediator in einer MetroCluster-IP-Konfiguration finden Sie unter "Konfigurieren Sie ONTAP Mediator über eine MetroCluster-IP-Konfiguration" .
- Informationen zur Verwendung von SnapMirror Active Sync finden Sie unter "Installieren Sie ONTAP Mediator und bestätigen Sie die ONTAP-Clusterkonfiguration".

Konfigurieren Sie die Sicherheitsrichtlinien von ONTAP Mediator

ONTAP Mediator unterstützt mehrere konfigurierbare Sicherheitseinstellungen. Die Standardwerte für alle Einstellungen werden in einer schreibgeschützten Datei angegeben `low_space_threshold_mib: 10`:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Alle Werte, die in das gesetzt `ontap_mediator.user_config.yaml` werden, überschreiben die Standardwerte und werden bei allen ONTAP Mediator Upgrades beibehalten.

Nach der Änderung `ontap_mediator.user_config.yaml` , starten Sie ONTAP Mediator neu:

```
systemctl restart ontap_mediator
```

Attribute des ONTAP Mediators ändern

Die in diesem Abschnitt beschriebenen Attribute des ONTAP Mediators können bei Bedarf geändert werden.

> Andere Standardwerte im `ontap_mediator.config.yaml` sollten nicht geändert werden, da geänderte Werte während der ONTAP Mediator-Upgrades nicht beibehalten werden.

Sie ändern die Attribute vonONTAP Mediator, indem Sie die erforderlichen Variablen in die Datei kopieren `ontap_mediator.user_config.yaml`, um die Standardeinstellungen zu überschreiben.

Installieren Sie SSL-Zertifikate von Drittanbietern

Wenn Sie die selbstsignierten Standardzertifikate durch SSL-Zertifikate von Drittanbietern ersetzen müssen, ändern Sie bestimmte Attribute in den folgenden Dateien:

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

Die Variablen in diesen Dateien werden verwendet, um die von ONTAP Mediator verwendeten Zertifikatsdateien zu steuern.

ONTAP Mediator 1.9 und höher

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der Datei enthalten `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`.

Variabel	Pfad
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` Dient zum Festlegen des Ablaufs von Clientzertifikaten. Der Maximalwert beträgt drei Jahre (1095 Tage).
- `x509_passin_pwd` Ist die Passphrase für das signierte Clientzertifikat.

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der Datei enthalten `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Variabel	Pfad
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`

ONTAP Mediator 1.8 und früher

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der Datei enthalten `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`.

Variabel	Pfad
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days` Dient zum Festlegen des Ablaufs von Clientzertifikaten. Der Maximalwert beträgt drei Jahre (1095 Tage).
- `x509_passin_pwd` Ist die Passphrase für das signierte Clientzertifikat.

Die in der folgenden Tabelle aufgeführten Standardvariablen sind in der Datei enthalten `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`.

Variabel	Pfad
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

Wenn Sie diese Attribute ändern, starten Sie ONTAP Mediator neu, um die Änderungen anzuwenden. Ausführliche Anweisungen zum Ersetzen von Standardzertifikaten durch Zertifikate von Drittanbietern finden Sie unter "Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern".

Schutz vor Kennwortangriffen

Die folgenden Einstellungen bieten Schutz vor Brute-Force-Passwortraten.

Um die Funktion zu aktivieren, legen Sie einen Wert für die `window_seconds` und die `retry_limit`fest.

Beispiele:

- Geben Sie ein 5-Minuten-Fenster für Vermutungen ein, und setzen Sie dann die Anzahl auf Null-Fehler zurück:

  ```
  authentication_lock_window_seconds: 300
  ```

- Sperren Sie das Konto, wenn innerhalb des Zeitrahmens fünf Fehler auftreten:

  ```
  authentication_retry_limit: 5
  ```

- Verringern Sie die Auswirkungen von Brute-Force-Passwortraten, indem Sie eine Verzögerung festlegen, die vor der Ablehnung jedes Versuchs auftritt, wodurch die Angriffe verlangsamt werden.

  ```
  authentication_failure_delay_seconds: 5
  ```

  ```
  authentication_failure_delay_seconds: 0   # seconds (float) to delay
  failed auth attempts prior to response, 0 = no delay
  authentication_lock_window_seconds: null  # seconds (int) since the
  oldest failure before resetting the retry counter, null = no window
  authentication_retry_limit: null          # number of retries to allow
  before locking API access, null = unlimited
  ```

Regeln zur Passwortkomplexität

Die folgenden Felder steuern die Regeln für die Passwortkomplexität des ONTAP Mediator API-Benutzerkontos.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

Kontrolle des freien Speicherplatzes

Es gibt Einstellungen, die den erforderlichen freien Speicherplatz auf der Festplatte steuern `/opt/netapp/lib/ontap_mediator`.

Wenn der Platz unter dem festgelegten Schwellenwert liegt, gibt der Dienst ein Warnungsereignis aus.

```
low_space_threshold_mib: 10
```

Kontrolle des reservierten Protokollspeichers

Die RESERVE_LOG_SPACE wird durch bestimmte Einstellungen gesteuert. Standardmäßig erstellt die ONTAP Mediator-Installation einen separaten Speicherplatz für die Protokolle. Das Installationsprogramm erstellt eine neue Datei mit fester Größe und insgesamt 700 MB Speicherplatz, die explizit für die ONTAP Mediator-Protokollierung verwendet wird.

So deaktivieren Sie diese Funktion und verwenden den Standardspeicherplatz:

1. Ändern Sie den Wert von RESERVE_LOG_SPACE in der folgenden Datei von 1 auf 0:

   `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

2. Mediator neu starten:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

   ```
   RESERVE_LOG_SPACE=0
   ```

   b. `systemctl restart ontap_mediator`

Um die Funktion wieder zu aktivieren, ändern Sie den Wert von 0 auf 1, und starten Sie den Mediator neu.

> Durch Umschalten zwischen Festplattenspeicherplätzen werden vorhandene Protokolle nicht gelöscht. Alle vorherigen Protokolle werden gesichert und anschließend auf den aktuellen Speicherplatz verschoben, nachdem Mediator gewechselt und neu gestartet wurde.

ONTAP Mediator verwalten

Verwalten Sie ONTAP Mediator, einschließlich der Änderung der Benutzeranmeldeinformationen, des Stoppens und erneuten Aktivierens des Dienstes, der Überprüfung seines Zustands und der Installation oder Deinstallation von SCST zur Hostwartung. Sie können auch Zertifikate verwalten, z. B. selbstsignierte Zertifikate neu generieren, diese durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen und Probleme mit Zertifikaten beheben.

Ändern Sie den Benutzernamen

Sie können den Benutzernamen wie folgt ändern.

Über diese Aufgabe

Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.

Wenn Sie diesen Befehl nicht erreichen können, müssen Sie möglicherweise den Befehl mit dem vollständigen Pfad ausführen, wie im folgenden Beispiel dargestellt:

```
/usr/local/bin/mediator_username
```

Schritte

Ändern Sie den Benutzernamen durch Auswahl einer der folgenden Optionen:

- **Option (a)**: Führen Sie den Befehl aus `mediator_change_user` und antworten Sie auf die Eingabeaufforderungen wie im folgenden Beispiel gezeigt:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- **Option (b)**: Führen Sie den folgenden Befehl aus:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

Ändern Sie das Passwort

Sie können das Passwort wie folgt ändern.

Über diese Aufgabe

Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.

Wenn Sie diesen Befehl nicht erreichen können, müssen Sie möglicherweise den Befehl mit dem vollständigen Pfad ausführen, wie im folgenden Beispiel dargestellt:

```
/usr/local/bin/mediator_change_password
```

Schritte

Ändern Sie das Passwort, indem Sie eine der folgenden Optionen auswählen:

- **Option (a)**: Führen Sie den `mediator_change_password` Befehl aus und antworten Sie auf die Eingabeaufforderungen wie im folgenden Beispiel gezeigt:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
              Old Password:
              New Password:
         Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- **Option (b)**: Führen Sie den folgenden Befehl aus:

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

Das Beispiel zeigt, dass das Passwort von „mediator1“ in „mediator2“ geändert wird.

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
The password has been updated successfully.
[root@mediator-host ~]#
```

Stoppen Sie ONTAP Mediator

Um ONTAP Mediator zu stoppen, führen Sie die folgenden Schritte aus:

Schritte

1. Stoppen Sie ONTAP Mediator:

```
systemctl stop ontap_mediator
```

2. SCST stoppen:

```
systemctl stop mediator-scst
```

3. Deaktivieren Sie ONTAP Mediator und SCST:

```
systemctl disable ontap_mediator mediator-scst
```

ONTAP Mediator erneut aktivieren

Um ONTAP Mediator wieder zu aktivieren, führen Sie die folgenden Schritte aus:

Schritte

1. Aktivieren Sie ONTAP Mediator und SCST:

```
systemctl enable ontap_mediator mediator-scst
```

2. SCST starten:

```
systemctl start mediator-scst
```

3. ONTAP Mediator starten:

```
systemctl start ontap_mediator
```

Überprüfen Sie, ob ONTAP Mediator fehlerfrei ist

Überprüfen Sie nach der Installation von ONTAP Mediator, ob es erfolgreich ausgeführt wird.

Schritte

1. Zeigen Sie den Status von ONTAP Mediator an:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Bestätigen Sie die von ONTAP Mediator verwendeten Ports:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Deinstallieren Sie ONTAP Mediator

Bei Bedarf können Sie ONTAP Mediator entfernen.

Bevor Sie beginnen

Sie müssen ONTAP Mediator von ONTAP trennen, bevor Sie es entfernen.

Über diese Aufgabe

Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.

Wenn Sie diesen Befehl nicht erreichen können, müssen Sie möglicherweise den Befehl mit dem vollständigen Pfad ausführen, wie im folgenden Beispiel dargestellt:

`/usr/local/bin/uninstall_ontap_mediator`

Schritt

1. Deinstallieren Sie ONTAP Mediator:

   `uninstall_ontap_mediator`

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

Erstellen Sie ein temporäres selbstsigniertes Zertifikat neu

Ab ONTAP Mediator 1.7 können Sie ein temporäres selbstsigniertes Zertifikat mithilfe des folgenden Verfahrens neu erstellen.

> Dieses Verfahren wird nur auf Systemen unterstützt, auf denen ONTAP Mediator 1.7 oder höher ausgeführt wird.

Über diese Aufgabe

- Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.
- Sie können diese Aufgabe nur ausführen, wenn die generierten selbstsignierten Zertifikate aufgrund von Änderungen am Hostnamen oder der IP-Adresse des Hosts nach der Installation von ONTAP Mediator veraltet sind.
- Nachdem das temporäre selbstsignierte Zertifikat durch ein vertrauenswürdiges Zertifikat eines Drittanbieters ersetzt wurde, führen Sie *Not* mit dieser Aufgabe aus, um ein Zertifikat zu regenerieren. Wenn kein selbstsigniertes Zertifikat vorhanden ist, schlägt dieses Verfahren fehl.

Schritt

Führen Sie den folgenden Schritt durch, um ein neues temporäres selbstsigniertes Zertifikat für den aktuellen Host zu erstellen:

1. Starten Sie ONTAP Mediator neu:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

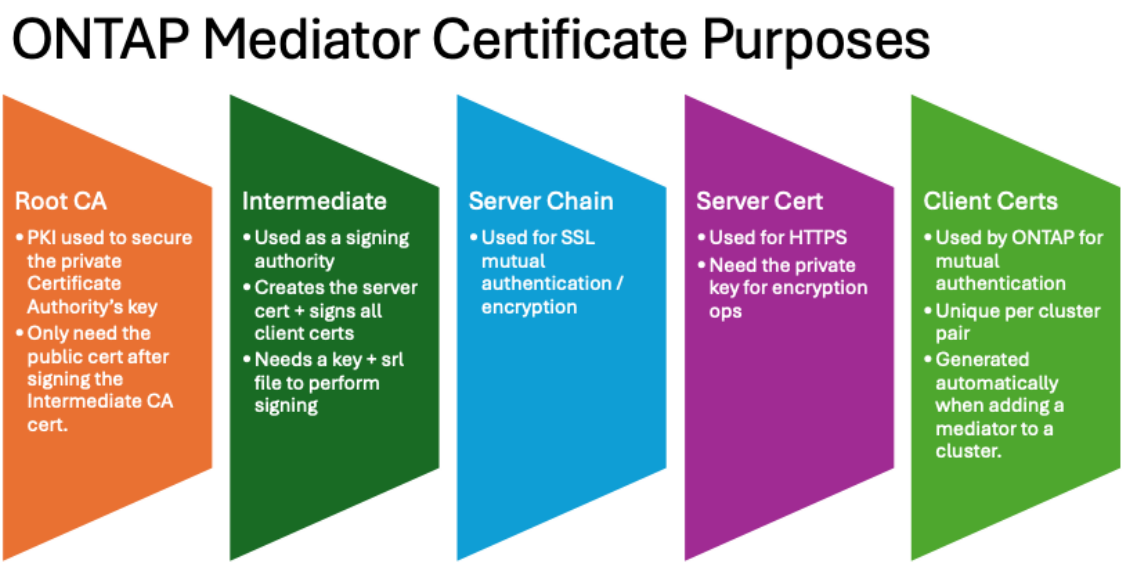
Ersetzen Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern

Wenn unterstützt, können Sie selbstsignierte Zertifikate durch vertrauenswürdige Zertifikate von Drittanbietern ersetzen.

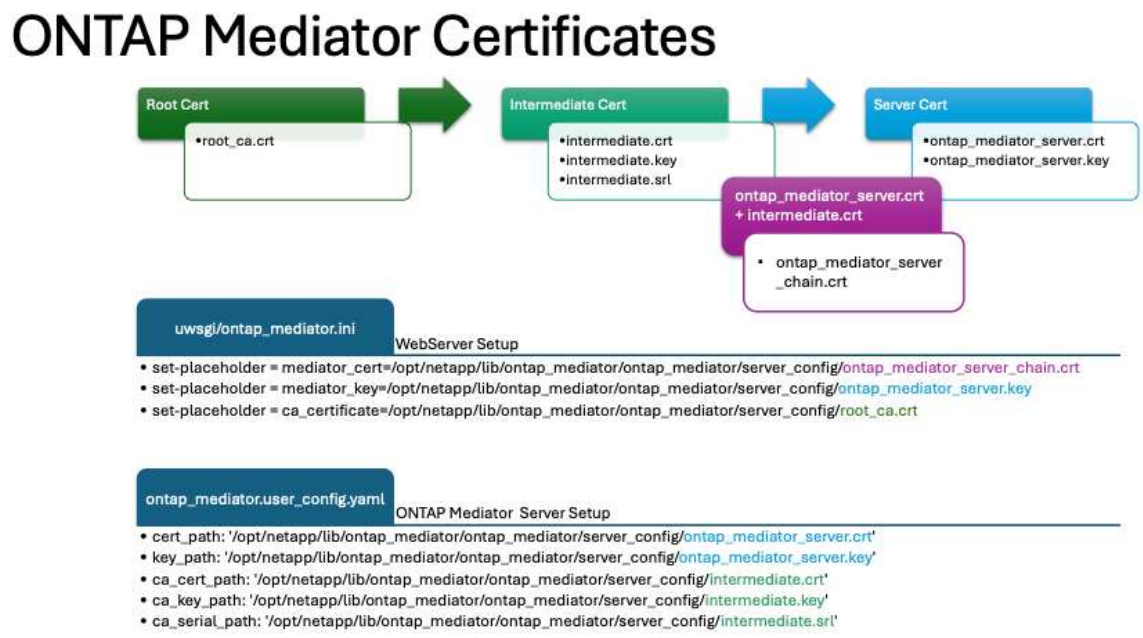
- Zertifikate von Drittanbietern werden erst ab ONTAP 9.16.1 und einigen früheren ONTAP Patch-Versionen unterstützt. Siehe "NetApp Bugs Online Fehler-ID CONTAP-243278".
- Zertifikate von Drittanbietern werden nur auf Systemen unterstützt, auf denen ONTAP Mediator 1.7 oder höher ausgeführt wird.

Über diese Aufgabe

- Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.
- Sie können diese Aufgabe ausführen, wenn die generierten selbstsignierten Zertifikate durch Zertifikate ersetzt werden müssen, die von einer vertrauenswürdigen untergeordneten Zertifizierungsstelle (CA) erhalten wurden. Um dies zu erreichen, sollten Sie Zugriff auf eine vertrauenswürdige Public-Key-Infrastruktur (PKI) haben.
- Die folgende Abbildung zeigt die Zwecke jedes ONTAP Mediatorzertifikats.



- Das folgende Bild zeigt die Konfiguration für die Einrichtung des Webservers und des ONTAP Mediators.



Schritt 1: Erhalten Sie ein Zertifikat von einem Drittanbieter, der ein CA-Zertifikat ausstellt

Sie können ein Zertifikat von einer PKI-Autorität über das folgende Verfahren erhalten.

Das folgende Beispiel zeigt, wie die selbstsignierten Zertifikatakteure durch die Zertifikatakteure von Drittanbietern ersetzt werden, die sich unter befinden

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.

Das Beispiel veranschaulicht die notwendigen Kriterien für die für ONTAP Mediator erforderlichen Zertifikate. Sie können die Zertifikate von einer PKI-Autorität auf eine andere Weise beziehen als bei diesem Verfahren. Passen Sie das Verfahren an Ihre Geschäftsanforderungen an.

ONTAP Mediator 1.9 und höher

1. Erstellen Sie einen privaten Schlüssel `intermediate.key` und eine Konfigurationsdatei `openssl_ca.cnf`, die von der PKI-Autorität zur Generierung eines Zertifikats verwendet wird.

   a. Generieren Sie den privaten Schlüssel `intermediate.key`:

      Beispiel

   ```
   openssl genrsa -aes256 -out intermediate.key 4096
   ```

   a. Die Konfigurationsdatei `openssl_ca.cnf` (unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definiert die Eigenschaften, über die das generierte Zertifikat verfügen muss.

2. Verwenden Sie den privaten Schlüssel und die Konfigurationsdatei, um eine Zertifikatsignierungsanforderung zu erstellen `intermediate.csr`:

   Beispiel:

   ```
   openssl req -key <private_key_name>.key -new -out
   <certificate_csr_name>.csr -config <config_file_name>.cnf
   ```

   ```
   [root@scs000216655 server_config]# openssl req -key intermediate.key
   -new -config openssl_ca.cnf -out intermediate.csr
   Enter pass phrase for intermediate.key:
   [root@scs000216655 server_config]# cat intermediate.csr
   -----BEGIN CERTIFICATE REQUEST-----
   <certificate_value>
   -----END CERTIFICATE REQUEST-----
   ```

3. Senden Sie die Zertifikatsignierungsanforderung `intermediate.csr` an eine PKI-Autorität zur Signatur.

   Die PKI-Behörde prüft die Anfrage und unterzeichnet die `.csr` , Generieren des Zertifikats `intermediate.crt` . Darüber hinaus benötigen Sie die `root_ca.crt` Zertifikat, das die `intermediate.crt` Zertifikat der PKI-Behörde.

   Für SnapMirror Business Continuity (SM-BC)-Cluster müssen Sie die `intermediate.crt` Und `root_ca.crt` Zertifikate an einen ONTAP Cluster. Sehen"Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync" .

ONTAP Mediator 1.8 und früher

1. Erstellen Sie einen privaten Schlüssel `ca.key` und eine Konfigurationsdatei `openssl_ca.cnf`, die von der PKI-Autorität zur Generierung eines Zertifikats verwendet wird.

   a. Generieren Sie den privaten Schlüssel `ca.key`:

      Beispiel

```
openssl genrsa -aes256 -out ca.key 4096
```

a. Die Konfigurationsdatei `openssl_ca.cnf` (unter `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) definiert die Eigenschaften, über die das generierte Zertifikat verfügen muss.

2. Verwenden Sie den privaten Schlüssel und die Konfigurationsdatei, um eine Zertifikatsignierungsanforderung zu erstellen `ca.csr`:

Beispiel:

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. Senden Sie die Zertifikatsignierungsanforderung `ca.csr` an eine PKI-Autorität zur Signatur.

Die PKI-Autorität überprüft die Anforderung und signiert den `.csr`, das Zertifikat zu generieren `ca.crt`. Darüber hinaus müssen Sie das Zertifikat von der PKI-Behörde erhalten `root_ca.crt that signed the `ca.crt`.

Für SnapMirror-Cluster für Business Continuity (SM-BC) müssen Sie einem ONTAP-Cluster die Zertifikate und hinzufügen `ca.crt root_ca.crt` . Siehe "Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync".

Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren

ONTAP Mediator 1.9 und höher

Ein Server-Zertifikat muss durch den privaten Schlüssel `intermediate.key` und das Drittanbieter-Zertifikat signiert werden `intermediate.crt`. Darüber hinaus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` enthält die Konfigurationsdatei bestimmte Attribute, die die Eigenschaften angeben, die für von OpenSSL ausgegebene Serverzertifikate erforderlich sind.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, führen Sie den folgenden Befehl aus dem Ordner aus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. Um ein Serverzertifikat aus der CSR zu generieren, führen Sie den folgenden Befehl aus dem `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner:

   > Diese Dateien wurden von einer PKI-Behörde abgerufen. Wenn Sie einen anderen Zertifikatnamen verwenden, ersetzen Sie `intermediate.crt` und `intermediate.key` durch die entsprechenden Dateinamen.

   ```
   openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
   intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
   -req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
   ```

   - Die `-CAcreateserial` Option wird verwendet, um die Dateien zu generieren `intermediate.srl`.

ONTAP Mediator 1.8 und früher

Ein Server-Zertifikat muss durch den privaten Schlüssel `ca.key` und das Drittanbieter-Zertifikat signiert werden `ca.crt`. Darüber hinaus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` enthält die Konfigurationsdatei bestimmte Attribute, die die Eigenschaften angeben, die für von OpenSSL ausgegebene Serverzertifikate erforderlich sind.

Die folgenden Befehle können ein Serverzertifikat generieren.

Schritte

1. Um eine Serverzertifikatsignierungsanforderung (CSR) zu generieren, führen Sie den folgenden Befehl aus dem Ordner aus `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. Um ein Serverzertifikat aus der CSR zu generieren, führen Sie den folgenden Befehl aus dem

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` Ordner:

> Diese Dateien wurden von einer PKI-Behörde abgerufen. Wenn Sie einen anderen Zertifikatnamen verwenden, ersetzen Sie `ca.crt` und `ca.key` durch die entsprechenden Dateinamen.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- Die `-CAcreateserial` Option wird verwendet, um die Dateien zu generieren `ca.srl`.

Schritt 3: Ersetzen Sie neue Drittanbieter-CA-Zertifikat und Server-Zertifikat in ONTAP Mediator-Konfiguration

ONTAP Mediator 1.10 und höher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei bereitgestellt, die sich unter befindet. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . Die Datei enthält die folgenden Attribute:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` Und `key_path` sind Serverzertifikatvariablen.
- `ca_cert_path`, `ca_key_path` Und `ca_serial_path` sind CA-Zertifikatvariablen.

Schritte

1. Ersetzen Sie alle `intermediate.*` Dateien durch Zertifikate von Drittanbietern.
2. Erstellen Sie eine Zertifikatskette aus den `intermediate.crt` Zertifikaten und `ontap_mediator_server.crt` :

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` Datei.

   Aktualisieren Sie die Werte von `ssl_keyfile` , `ssl_certfile` , Und `ssl_ca_certs` :

   ```
   ssl_keyfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

   ssl_ca_certs:
   ```

/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt

- Der ssl_keyfile Wert ist der Schlüsselpfad in der ontap_mediator_server.crt Datei, die ontap_mediator_server.key .
- Der ssl_certfile Wert ist der Pfad des ontap_mediator_server_chain.crt Datei.
- Der ssl_ca_certs Wert ist der Pfad des root_ca.crt Datei.

4. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:
   - Eigentümer Der Linux-Gruppe: netapp:netapp
   - Linux-Berechtigungen: 600
5. Starten Sie ONTAP Mediator neu:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 und 1.9

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei bereitgestellt, die sich unter befindet. /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml . Die Datei enthält die folgenden Attribute:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- cert_path Und key_path sind Serverzertifikatvariablen.
- ca_cert_path, ca_key_path Und ca_serial_path sind CA-Zertifikatvariablen.

Schritte

1. Ersetzen Sie alle intermediate.* Dateien durch Zertifikate von Drittanbietern.
2. Erstellen Sie eine Zertifikatskette aus den intermediate.crt Zertifikaten und ontap_mediator_server.crt :

```
cat ontap_mediator_server.crt intermediate.crt >
```

```
ontap_mediator_server_chain.crt
```

3. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

   Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key`und `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - Der `mediator_cert` Wert ist der Pfad der `ontap_mediator_server_chain.crt` Datei.
   - Das `mediator_key value` ist der Schlüsselpfad in der `ontap_mediator_server.crt` Datei, das heißt `ontap_mediator_server.key`.
   - Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.

4. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:
   - Eigentümer Der Linux-Gruppe: `netapp:netapp`
   - Linux-Berechtigungen: `600`
5. Starten Sie ONTAP Mediator neu:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediator 1.8 und früher

Die Zertifikatskonfiguration wird ONTAP Mediator in der Konfigurationsdatei bereitgestellt, die sich unter befindet. `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . Die Datei enthält die folgenden Attribute:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path` Und `key_path` sind Serverzertifikatvariablen.
- `ca_cert_path`, `ca_key_path` Und `ca_serial_path` sind CA-Zertifikatvariablen.

Schritte

1. Ersetzen Sie alle `ca.*` Dateien durch Zertifikate von Drittanbietern.
2. Erstellen Sie eine Zertifikatskette aus den `ca.crt` Zertifikaten und `ontap_mediator_server.crt` :

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

   Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key`und `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - Der `mediator_cert` Wert ist der Pfad der `ontap_mediator_server_chain.crt` Datei.
   - Das `mediator_key value` ist der Schlüsselpfad in der `ontap_mediator_server.crt` Datei, das heißt `ontap_mediator_server.key`.
   - Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.
4. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:
   - Eigentümer Der Linux-Gruppe: `netapp:netapp`

- Linux-Berechtigungen: `600`

5. Starten Sie ONTAP Mediator neu:

```
systemctl restart ontap_mediator
```

Schritt 4: Verwenden Sie optional einen anderen Pfad oder Namen für Ihre Drittanbieter-Zertifikate

ONTAP Mediator 1.10 und höher

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als verwenden `intermediate.*` oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Konfigurieren Sie die `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` Datei so, dass die standardmäßigen Variablenwerte in der Datei überschrieben `ontap_mediator.config.yaml` werden.

   Wenn Sie von einer PKI-Autorität erhalten `intermediate.crt` haben und den privaten Schlüssel am Speicherort speichern `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, sollte die `ontap_mediator.user_config.yaml` Datei wie folgt aussehen:

   > Wenn Sie `intermediate.crt` das Zertifikat signiert `ontap_mediator_server.crt` haben, wird die `intermediate.srl` Datei generiert. Weitere Informationen finden Sie unter Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren .

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. Wenn Sie eine Zertifikatsstruktur verwenden, bei der die `root_ca.crt` Zertifikat bietet eine `intermediate.crt` Zertifikat, das die `ontap_mediator_server.crt` Zertifikat, erstellen Sie eine Zertifikatskette aus dem `intermediate.crt` Und `ontap_mediator_server.crt` Zertifikate:

> Sie sollten die Zertifikate und von einer PKI-Behörde erhalten haben, die Sie zuvor im Verfahren erhalten haben `intermediate.crt` `ontap_mediator_server.crt` .

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` Datei.

   Aktualisieren Sie die Werte von `ssl_keyfile` , `ssl_certfile` , Und `ssl_ca_certs` :

   ```
   ssl_keyfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
   or_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
   or_server_chain.crt

   ssl_ca_certs:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - Der `ssl_keyfile` Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt` Datei, die `ontap_mediator_server.key` .
   - Der `ssl_certfile` Wert ist der Pfad des `ontap_mediator_server_chain.crt` Datei.
   - Der `ssl_ca_certs` Wert ist der Pfad des `root_ca.crt` Datei.

   > Für SnapMirror Business Continuity (SM-BC)-Cluster müssen Sie die `intermediate.crt` Und `root_ca.crt` Zertifikate an einen ONTAP Cluster. Sehen"Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync" .

c. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:

   - Eigentümer Der Linux-Gruppe: `netapp:netapp`
   - Linux-Berechtigungen: `600`

2. Starten Sie ONTAP Mediator neu, wenn die Zertifikate in der Konfigurationsdatei aktualisiert wurden:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediator 1.9.1 und 1.9

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als verwenden `intermediate.*` oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Konfigurieren Sie die `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` Datei so, dass die standardmäßigen Variablenwerte in der Datei überschrieben `ontap_mediator.config.yaml` werden.

   Wenn Sie von einer PKI-Autorität erhalten `intermediate.crt` haben und den privaten Schlüssel am Speicherort speichern `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, sollte die `ontap_mediator.user_config.yaml` Datei wie folgt aussehen:

Wenn Sie `intermediate.crt` das Zertifikat signiert `ontap_mediator_server.crt` haben, wird die `intermediate.srl` Datei generiert. Weitere Informationen finden Sie unter Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren .

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. Wenn Sie eine Zertifikatsstruktur verwenden, bei der die `root_ca.crt` Zertifikat bietet eine `intermediate.crt` Zertifikat, das die `ontap_mediator_server.crt` Zertifikat, erstellen Sie eine Zertifikatskette aus dem `intermediate.crt` Und `ontap_mediator_server.crt` Zertifikate:

Sie sollten die Zertifikate und von einer PKI-Behörde erhalten haben, die Sie zuvor im Verfahren erhalten haben `intermediate.crt` `ontap_mediator_server.crt` .

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key`und `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `mediator_cert` Wert ist der Pfad der `ontap_mediator_server_chain.crt` Datei.
- Der `mediator_key` Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt` Datei `ontap_mediator_server.key`.
- Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.

Für SnapMirror Business Continuity (SM-BC)-Cluster müssen Sie die `intermediate.crt` Und `root_ca.crt` Zertifikate an einen ONTAP Cluster. Sehen"Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync" .

c. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:

- Eigentümer Der Linux-Gruppe: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. Starten Sie ONTAP Mediator neu, wenn die Zertifikate in der Konfigurationsdatei aktualisiert wurden:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 und früher

Sie können Zertifikate von Drittanbietern mit einem anderen Namen als verwenden `ca.*` oder die Zertifikate von Drittanbietern an einem anderen Ort speichern.

Schritte

1. Konfigurieren Sie die `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.`

`user_config.yaml` Datei so, dass die standardmäßigen Variablenwerte in der Datei überschrieben `ontap_mediator.config.yaml` werden.

Wenn Sie von einer PKI-Autorität erhalten `ca.crt` haben und den privaten Schlüssel am Speicherort speichern `ca.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, sollte die `ontap_mediator.user_config.yaml` Datei wie folgt aussehen:

> Wenn Sie `ca.crt` das Zertifikat signiert `ontap_mediator_server.crt` haben, wird die `ca.srl` Datei generiert. Weitere Informationen finden Sie unter Schritt 2: Erstellen Sie ein Serverzertifikat, indem Sie mit einer Drittanbieter-CA-Zertifizierung signieren .

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. Wenn Sie eine Zertifikatstruktur verwenden, in der das `root_ca.crt` Zertifikat ein Zertifikat bereitstellt `ca.crt` , das das Zertifikat signiert `ontap_mediator_server.crt` , erstellen Sie eine Zertifikatskette aus den `ca.crt` Zertifikaten und `ontap_mediator_server.crt` :

Sie sollten die Zertifikate und von einer PKI-Behörde erhalten haben, die Sie zuvor im Verfahren erhalten haben `ca.crt` `ontap_mediator_server.crt` .

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. Aktualisieren Sie die `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` Datei.

Aktualisieren Sie die Werte von `mediator_cert`, `mediator_key`und `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- Der `mediator_cert` Wert ist der Pfad der `ontap_mediator_server_chain.crt` Datei.
- Der `mediator_key` Wert ist der Schlüsselpfad in der `ontap_mediator_server.crt` Datei `ontap_mediator_server.key`.
- Der `ca_certificate` Wert ist der Pfad der `root_ca.crt` Datei.

Für SnapMirror-Cluster für Business Continuity (SM-BC) müssen Sie einem ONTAP-Cluster die Zertifikate und hinzufügen `ca.crt` `root_ca.crt` . Siehe "Konfigurieren Sie ONTAP Mediator und Cluster für SnapMirror Active Sync".

c. Stellen Sie sicher, dass die folgenden Attribute der neu generierten Zertifikate korrekt festgelegt sind:

- Eigentümer Der Linux-Gruppe: `netapp:netapp`
- Linux-Berechtigungen: `600`

2. Starten Sie ONTAP Mediator neu, wenn die Zertifikate in der Konfigurationsdatei aktualisiert wurden:

```
systemctl restart ontap_mediator
```

Fehlerbehebung bei zertifikatbezogenen Problemen

Sie können bestimmte Eigenschaften der Zertifikate überprüfen.

Überprüfen Sie den Ablauf des Zertifikats

Verwenden Sie den folgenden Befehl, um den Gültigkeitsbereich des Zertifikats zu identifizieren.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

Überprüfen Sie die X509v3-Erweiterungen in der CA-Zertifizierung

Verwenden Sie den folgenden Befehl, um die X509v3-Erweiterungen in der CA-Zertifizierung zu überprüfen.

ONTAP Mediator 1.9 und höher

Die **v3_ca** in definierten Eigenschaften `openssl_ca.cnf` werden wie in angezeigt `X509v3 extensions` `intermediate.crt`.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediator 1.8 und früher

Die **v3_ca** in definierten Eigenschaften `openssl_ca.cnf` werden wie in angezeigt `X509v3 extensions` `ca.crt`.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

Überprüfen Sie X509v3-Erweiterungen in Serverzertifikaten und Subject Alt-Namen

Die `v3_req` in der `openssl_server.cnf` Konfigurationsdatei definierten Eigenschaften werden als `X509v3 extensions` im Zertifikat angezeigt.

Im folgenden Beispiel erhalten Sie die Variablen in der `alt_names` Abschnitte durch Ausführen der Befehle `hostname -A` Und `hostname -I` auf der Linux-VM, auf der ONTAP Mediator installiert ist.

Erkundigen Sie sich bei Ihrem Netzwerkadministrator nach den korrekten Werten der Variablen.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Vergewissern Sie sich, dass ein privater Schlüssel mit einem Zertifikat übereinstimmt

Sie können überprüfen, ob ein bestimmter privater Schlüssel mit einem Zertifikat übereinstimmt.

Verwenden Sie die folgenden OpenSSL-Befehle auf dem Schlüssel bzw. dem Zertifikat.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

Wenn das `-modulus` Attribut für beide übereinstimmen, zeigt es an, dass der private Schlüssel und das Zertifikatspaar kompatibel sind und miteinander arbeiten können.

Überprüfen Sie, ob ein Serverzertifikat aus einem bestimmten CA-Zertifikat erstellt wurde

Mit dem folgenden Befehl können Sie überprüfen, ob das Serverzertifikat aus einem bestimmten CA-Zertifikat erstellt wird.

ONTAP Mediator 1.9 und höher

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP Mediator 1.8 und früher

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

Wenn die OCSP-Validierung (Online Certificate Status Protocol) verwendet wird, verwenden Sie den Befehl "openssl-Verify".

Warten Sie das Host-Betriebssystem für ONTAP Mediator

Um eine optimale Leistung zu erzielen, stellen Sie sicher, dass das Host-Betriebssystem für ONTAP Mediator regelmäßig gewartet wird.

Starten Sie den Host neu

Starten Sie den Host nur neu, wenn die Cluster fehlerfrei sind. Cluster können nicht auf Fehler reagieren, während ONTAP Mediator offline ist. Legen Sie einen Zeitpunkt für die Wartung fest, bevor Sie das System neu starten.

ONTAP Mediator wird während eines Neustarts automatisch fortgesetzt und stellt zuvor konfigurierte Beziehungen mit ONTAP Clustern wieder her.

Updates des Host-Pakets

Aktualisieren Sie alle Bibliotheken oder Yum-Pakete außer dem Kernel. Starten Sie den Host bei Bedarf neu, damit die Änderungen wirksam werden. Planen Sie vor dem Neustart des Hosts ein Servicefenster ein.

Wenn Sie das `yum-utils` Paket installieren, verwenden Sie den `needs-restarting` Befehl, um zu erkennen, ob Paketänderungen einen Neustart erfordern.

Führen Sie nach der Aktualisierung der ONTAP Mediator-Abhängigkeiten einen Neustart durch, da die Änderungen nicht sofort wirksam werden.

Aktualisieren Sie den Kernel des Host-Betriebssystems.

SCST muss für den von Ihnen verwendeten Kernel kompiliert werden. Um das Betriebssystem zu aktualisieren, müssen Sie einen Wartungstermin einplanen.

Schritte

Führen Sie diese Schritte aus, um den Kernel des Host-Betriebssystems zu aktualisieren.

> Überprüfen Sie vor dem Upgrade des Kernels, ob das Betriebssystem und die ONTAP Mediator-Version kompatibel sind. Informationen zu unterstützten Versionen finden Sie im"OS Support-Matrix" .

1. Stoppen Sie ONTAP Mediator.
2. Deinstallieren Sie das SCST-Paket, sieheDurchführen von Host-Wartungsarbeiten . (SCST bietet keinen Upgrade-Mechanismus.)
3. Aktualisieren Sie das Betriebssystem, und starten Sie es neu.
4. Installieren Sie das SCST-Paket erneut.
5. Aktivieren Sie ONTAP Mediator erneut.

Durchführen von Host-Wartungsarbeiten

Das Upgrade des VM-Kernels kann Kompatibilitätsprobleme mit SCST-Modulen verursachen. Deinstallieren Sie SCST manuell und installieren Sie es erneut.

Schritt 1: Deinstallieren Sie SCST

Um SCST zu deinstallieren, verwenden Sie das Tar-Paket für Ihre ONTAP Mediator-Version.

Schritte

1. Laden Sie das entsprechende SCST-Paket herunter (wie in der folgenden Tabelle gezeigt) und extrahieren Sie es.

Für diese Version …	Verwenden Sie dieses tar-Bündel…
ONTAP Mediator 1.11	scst-3.9.tar.gz
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	Scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	Scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	Scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	Scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	Scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	Scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	Scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	Scst-3.5.0.tar.bz2
ONTAP Mediator 1.1	Scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	Scst-3.3.0.tar.bz2

   a. Greifen Sie auf das Open Source-Paket zu über"SCST Sourceforge-Downloads" .
   b. Wählen Sie **Freigegebene Versionen herunterladen**.
   c. Extrahieren Sie das Paket auf Ihre VM.

2. Führen Sie die folgenden Deinstallationsbefehle im `scst` Verzeichnis:
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Schritt 2: SCST installieren

Um SCST manuell zu installieren, benötigen Sie das SCST-Tar-Bundle, das für die installierte Version von ONTAP Mediator verwendet wird (siehe SCST-Tabelle).

> Führen Sie diesen Schritt aus, bevor Sie den ONTAP Mediator installieren. Wenn die von Ihnen verwendete SCST-Version neuer ist als die mit dem ONTAP Mediator-Installationsprogramm gebündelte Version, überspringt das Installationsprogramm diesen Schritt.

1. Führen Sie die folgenden Installationsbefehle im `scst` Verzeichnis:
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`

      > Wenn Sie eine Erstinstallation durchführen und ONTAP Mediator vorinstallieren möchten, führen Sie den folgenden Befehl aus, bevor Sie mit dem nächsten Schritt fortfahren:
      >
      > `mkdir -p /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys`

   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

      > Wenn Sie SCST bei einer Erstinstallation vor ONTAP Mediator vorinstallieren, überspringen Sie diesen Schritt. Das Installationsprogramm wendet relevante SCST-Patches an.

2. Wenn Secure Boot aktiviert ist, führen Sie vor dem Neustart optional die folgenden Schritte aus:
   a. Bestimmen Sie jeden Dateinamen für die `scst_vdisk` , `scst` , Und `iscsi_scst` Module:

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. Bestimmen Sie die Kernel-Version:

      ```
      [root@localhost ~]# uname -r
      ```

c. Signieren Sie jede Moduldatei mit dem Kernel:

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. Installieren Sie den UEFI-Schlüssel mit der Firmware.

Anweisungen zur Installation des UEFI-Schlüssels finden Sie unter:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

Der generierte UEFI-Schlüssel befindet sich unter:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. Starten Sie das System neu:

```
reboot
```

Host ändert sich zum Hostnamen oder IP

Über diese Aufgabe

- Führen Sie diese Aufgabe auf dem Linux-Host aus, auf dem Sie ONTAP Mediator installiert haben.
- Führen Sie diese Schritte nur durch, wenn die selbstsignierten Zertifikate nicht mehr gültig sind, weil sich der Hostname oder die IP-Adresse nach der Installation von ONTAP Mediator geändert hat.
- Nachdem das temporäre selbstsignierte Zertifikat durch ein vertrauenswürdiges Drittanbieterzertifikat ersetzt wurde, verwenden Sie diese Aufgabe *nicht*, um ein Zertifikat neu zu generieren. Wenn Sie kein selbstsigniertes Zertifikat besitzen, können Sie dieses Verfahren nicht verwenden.

Schritt

Erstellen Sie ein temporäres selbstsigniertes Zertifikat für den aktuellen Host:

1. Starten Sie ONTAP Mediator neu:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Erfahren Sie mehr über die MetroCluster IP-Site-Verwaltung mit ONTAP System Manager

MetroCluster Konfigurationen spiegeln synchron Daten und Konfigurationen zwischen zwei ONTAP-Clustern an separaten Standorten. Ab ONTAP 9.8 bietet sich System Manager als vereinfachte Schnittstelle zum Management einer MetroCluster IP Konfiguration an.

> Sie können MetroCluster-Vorgänge nur mit System Manager in einer MetroCluster IP-Konfiguration ausführen. In einer MetroCluster FC-Konfiguration können Sie weiterhin mit System Manager jeden Node in der MetroCluster-Konfiguration verwalten, jedoch keine MetroCluster-spezifischen Vorgänge ausführen.

In der Regel richten Sie Cluster in einer MetroCluster-Konfiguration an zwei verschiedenen geografischen Standorten ein und konfigurieren sie. Anschließend richten Sie Peering zwischen den Clustern ein, damit sie Daten synchronisieren und teilen. Die beiden Cluster im Peering-Netzwerk bieten bidirektionale Disaster

Recovery (DR), bei der jedes Cluster als Quelle und Backup des anderen Clusters dienen kann. In MetroCluster IP-Konfigurationen mit acht oder vier Nodes besteht jeder Standort aus Storage-Controllern, die als ein oder zwei HA-Paare konfiguriert sind.

Sie können "ONTAP Mediator installieren" an einem dritten Standort den Status der Nodes und ihrer DR-Partner überwachen. ONTAP Mediator kann im Katastrophenfall eine Mediator-unterstützte ungeplante Umschaltung (MAUSO) implementieren.

Sie können auch eine ausgehandelte Umschaltung durchführen, um eines der Cluster für geplante Wartungsarbeiten herunterzufahren. Das Partner-Cluster wickelt alle Daten-I/O-Vorgänge für beide Cluster ab, bis Sie das Cluster aufrufen und einen Switchback-Vorgang durchführen.

Die Verfahren zum Einrichten und Verwalten einer MetroCluster-IP-Konfiguration mit System Manager finden Sie in der "MetroCluster-Dokumentation".

Datensicherung mithilfe von Tape Backup

Erfahren Sie mehr über die Bandsicherung von ONTAP FlexVol -Volumes

ONTAP unterstützt Tape-Backups und -Restores mithilfe des Network Data Management Protocol (NDMP). Mit NDMP können Sie Daten in Storage-Systemen direkt auf Tape sichern, was eine effiziente Nutzung der Netzwerkbandbreite ermöglicht. ONTAP unterstützt sowohl Dump- als auch SMTape-Engines für Tape-Backup.

Mithilfe von NDMP-konformen Backup-Applikationen können Sie eine Dump- oder SMTape-Sicherung bzw. -Wiederherstellung durchführen. Nur NDMP Version 4 wird unterstützt.

Tape Backup mit Dump

Dump ist ein Snapshot-basiertes Backup, in dem Ihre Dateisystemdaten auf Band gesichert werden. Die ONTAP Dump Engine sichert Dateien, Verzeichnisse und die Informationen zur entsprechenden Zugriffssteuerungsliste (ACL) auf Tapes. Sie können ein gesamtes Volume, einen vollständigen qtree oder Subbaum ohne vollständige Volumes oder einen kompletten qtree sichern. Dump unterstützt Basis-, Differenzial- und inkrementelle Backups.

Tape Backup mit SMTape

SMTape ist eine Snapshot-basierte Disaster Recovery-Lösung von ONTAP, die Datenblöcke auf Tapes sichert. Mit SMTape können Volume-Backups auf Tapes durchgeführt werden. Sie können jedoch keine Sicherung auf qtree- oder Subbaum-Ebene durchführen. SMTape unterstützt Basis-, Differenzial- und inkrementelle Backups.

Ab ONTAP 9.13.1 unterstützt Tape Backup mit SMTape mit SnapMirror Active Sync.

ONTAP -Bandsicherungs- und Wiederherstellungsworkflow

Sie können Backup- und Restore-Vorgänge auf Tape mithilfe einer NDMP-fähigen Backup-Applikation durchführen.

Über diese Aufgabe

Der Workflow für Tape-Backup und -Wiederherstellung bietet einen Überblick über die Aufgaben, die mit der Durchführung von Tape-Backup- und Restore-Vorgängen verbunden sind. Ausführliche Informationen zur Durchführung eines Backup- und Wiederherstellungsvorgangs finden Sie in der Dokumentation der Backup-

Anwendung.

Schritte

1. Richten Sie eine Tape Library-Konfiguration ein, indem Sie sich für eine von NDMP unterstützte Tape-Topologie entscheiden.
2. Aktivieren Sie NDMP-Services auf Ihrem Storage-System.

   Sie können die NDMP-Services entweder auf Node-Ebene oder auf Storage Virtual Machine (SVM)-Ebene aktivieren. Das hängt von dem NDMP-Modus ab, in dem Sie die Bandsicherung und den Wiederherstellungsvorgang durchführen möchten.

3. Nutzen Sie NDMP-Optionen zum Managen von NDMP auf Ihrem Storage-System.

   NDMP-Optionen können entweder auf Node-Ebene oder auf SVM-Ebene genutzt werden. Das hängt von dem NDMP-Modus ab, in dem Sie die Bandsicherung und den Wiederherstellungsvorgang durchführen möchten.

   Sie können die NDMP-Optionen auf Node-Ebene mit dem `system services ndmp modify` Befehl und mit dem Befehl auf SVM-Ebene ändern `vserver services ndmp modify`. Erfahren Sie mehr über `system services ndmp modify` und `vserver services ndmp modify` in der "ONTAP-Befehlsreferenz".

4. Führen Sie ein Tape-Backup oder eine Wiederherstellung mithilfe einer NDMP-fähigen Backup-Applikation durch.

   ONTAP unterstützt sowohl Dump- als auch SMTape-Engines für Tape-Backup und -Wiederherstellung.

   Weitere Informationen zur Verwendung der Backup-Anwendung (auch als *Data Management Applications* oder *DMAs* bezeichnet) zur Durchführung von Backup- oder Wiederherstellungsvorgängen finden Sie in der Dokumentation Ihrer Backup-Anwendung.

Verwandte Informationen

Gängige NDMP Tape-Backup-Topologien

Allgemeines zur Dump-Engine für FlexVol-Volumes

Anwendungsfälle für ONTAP SMTape und Dump-Backup-Engines

ONTAP unterstützt zwei Backup Engines: SMTape und Dump. Sie sollten die Anwendungsfälle für SMTape und Dump Backup-Engines kennen, um Sie bei der Auswahl der Backup Engine zu unterstützen, die Tape-Backup- und Restore-Vorgänge durchgeführt werden soll.

Dump kann in den folgenden Fällen verwendet werden:

- Direct Access Recovery (DAR) von Dateien und Verzeichnissen
- Sicherung einer Untergruppe von Unterverzeichnissen oder Dateien in einem bestimmten Pfad
- Ausschließen von bestimmten Dateien und Verzeichnissen während der Backups
- Langfristige Backup-Aufbewahrung

SMTape kann in den folgenden Fällen eingesetzt werden:

- Disaster Recovery-Lösung
- Beibehalten der Deduplizierungseinsparungen und der Deduplizierungseinstellungen auf den gesicherten Daten während einer Wiederherstellung
- Backup großer Volumes

Verwalten Sie Bandlaufwerke

Erfahren Sie mehr über die Verwaltung von ONTAP Bandlaufwerken

Sie können die Bandbibliotheken-Verbindungen überprüfen und Informationen zum Bandlaufwerk anzeigen, bevor Sie ein Bandsicherungs- oder Wiederherstellungsvorgang durchführen. Sie können ein nicht qualifiziertes Bandlaufwerk verwenden, indem Sie dieses auf ein qualifiziertes Bandlaufwerk emulieren. Zusätzlich zur Anzeige vorhandener Aliase können Sie auch Bandaliase zuweisen und entfernen.

Wenn Sie Daten auf Band sichern, werden die Daten in Banddateien gespeichert. Dateimarken trennen die Banddateien, und die Dateien haben keine Namen. Sie geben eine Banddatei nach ihrer Position auf dem Band an. Sie schreiben eine Banddatei mit einem Bandgerät. Wenn Sie die Banddatei lesen, müssen Sie ein Gerät angeben, das denselben Komprimierungstyp hat, den Sie zum Schreiben dieser Banddatei verwendet haben.

ONTAP -Befehle zur Verwaltung von Bandlaufwerken, Medienwechslern und Bandlaufwerksvorgängen

Es gibt Befehle zur Anzeige von Informationen über Bandlaufwerke und Medienwechsler in einem Cluster, um ein Bandlaufwerk online zu schalten und offline zu schalten, die Position der Bandlaufwerkkassette zu ändern, den Aliasnamen des Bandlaufwerks einzustellen und zu löschen und ein Bandlaufwerk zurückzusetzen. Sie können auch Statistiken zu Bandlaufwerken anzeigen und zurücksetzen.

Ihr Ziel ist	Befehl
Bringen Sie ein Bandlaufwerk online	`storage tape online`
Löschen Sie einen Alias-Namen für Bandlaufwerk oder Medienwechsler	`storage tape alias clear`
Aktivieren oder deaktivieren Sie einen Bandlaufvorgang für ein Bandlaufwerk	`storage tape trace`
Ändern Sie die Position der Bandlaufwerk-Patrone	`storage tape position`
Setzen Sie ein Bandlaufwerk zurück	`storage tape reset` Dieser Befehl ist nur auf der erweiterten Berechtigungsebene verfügbar.

Ihr Ziel ist	Befehl
Legen Sie einen Alias-Namen für Bandlaufwerk oder Medienwechsler fest	`storage tape alias set`
Versetzen Sie ein Bandlaufwerk in den Offline-Modus	`storage tape offline`
Hier finden Sie Informationen zu allen Bandlaufwerken und Medienwechslern	`storage tape show`
Zeigen Sie Informationen über Bandlaufwerke an, die mit dem Cluster verbunden sind	• `storage tape show-tape-drive` • `system node hardware tape drive show`
Zeigen Sie Informationen über an den Cluster angeschlossene Medienwechsler an	`storage tape show-media-changer`
Zeigen Sie Fehlerinformationen zu Bandlaufwerken an, die mit dem Cluster verbunden sind	`storage tape show-errors`
Zeigen Sie alle für ONTAP geeigneten und unterstützten Bandlaufwerke an, die mit jedem Node im Cluster verbunden sind	`storage tape show-supported-status`
Zeigen Sie Aliase aller Bandlaufwerke und Medienwechsler an, die mit jedem Knoten im Cluster verbunden sind	`storage tape alias show`
Setzen Sie den Statistikwert eines Bandlaufwerks auf Null zurück	`storage stats tape zero tape_name` Sie müssen diesen Befehl in der nodeshell verwenden.
View Tape-Laufwerke, die von ONTAP unterstützt werden	`storage show tape supported [-v]` Sie müssen diesen Befehl in der nodeshell verwenden. Sie können die `-v` Option verwenden, um weitere Details zu den einzelnen Bandlaufwerken anzuzeigen.
Zeigen Sie Statistiken zu Bandgeräten an, um die Bandleistung zu verstehen und das Nutzungsmuster zu überprüfen	`storage stats tape tape_name` Sie müssen diesen Befehl in der nodeshell verwenden.

Verwandte Informationen

- "Speicherband"
- "Speicherband-Show"

- "Speicherband zeigt den unterstützten Status an"
- "Speicherband Show-Bandlaufwerk"
- "Speicherband-Alias löschen"
- "Speicherband-Aliassatz"
- "Speicherbandalias anzeigen"
- "Speicherbandspur"

Verwenden Sie ein nicht qualifiziertes Bandlaufwerk für die ONTAP Bandsicherung

Sie können ein nicht qualifiziertes Bandlaufwerk auf einem Speichersystem verwenden, wenn es ein qualifiziertes Bandlaufwerk emulieren kann. Sie wird dann wie ein qualifiziertes Bandlaufwerk behandelt. Um ein nicht qualifiziertes Bandlaufwerk zu verwenden, müssen Sie zunächst feststellen, ob es eines der qualifizierten Bandlaufwerke emuliert.

Über diese Aufgabe

Ein nicht-qualifiziertes Bandlaufwerk ist ein Laufwerk, das an das Storage-System angeschlossen ist, jedoch von ONTAP nicht unterstützt oder erkannt wird.

Schritte

1. Zeigen Sie die nicht qualifizierten Bandlaufwerke an `storage tape show-supported-status`, die mit einem Speichersystem verbunden sind, mit dem Befehl an.

   Mit dem folgenden Befehl werden Bandlaufwerke angezeigt, die an das Speichersystem angeschlossen sind, sowie der Support und Qualifikationsstatus der einzelnen Bandlaufwerke. Außerdem werden die nicht qualifizierten Bandlaufwerke aufgeführt. `tape_drive_vendor_name` Ist ein nicht qualifiziertes Bandlaufwerk, das an das Speichersystem angeschlossen ist, aber nicht von ONTAP 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. Emulieren Sie das qualifizierte Bandlaufwerk.

"NetApp Downloads: Konfigurationsdateien für Bandgeräte"

Verwandte Informationen

- Welche qualifizierten Bandlaufwerke sind
- "Speicherband zeigt den unterstützten Status an"

Weisen Sie einem Bandlaufwerk oder Medienwechsler Bandaliase für die ONTAP Bandsicherung zu

Zur einfachen Geräteerkennung können Sie einem Bandlaufwerk oder einem Mittelwechsler Bandaliase zuweisen. Aliase stellen eine Korrespondenz zwischen den logischen Namen von Sicherungsgeräten und einem Namen dar, der permanent dem Bandlaufwerk oder dem Mittelwechsler zugewiesen ist.

Schritte

1. Weisen Sie einem Bandlaufwerk oder einem Medienwechsler mit dem `storage tape alias set` Befehl einen Alias zu.

   Erfahren Sie mehr über `storage tape alias set` in der "ONTAP-Befehlsreferenz".

   Sie können die SN-Informationen über die Bandlaufwerke mit dem `system node hardware tape drive show` Befehl und über Bandbibliotheken mit den `system node hardware tape library show` Befehlen anzeigen.

   Mit dem folgenden Befehl wird ein Alias-Name auf ein Bandlaufwerk mit der Seriennummer SN[123456]L4 festgelegt, das an den Knoten angeschlossen ist, cluster1-01:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name st3
   -mapping SN[123456]L4
   ```

   Mit dem folgenden Befehl wird ein Alias-Name auf einen Medienwechsler mit der Seriennummer SN[65432], die an den Knoten angeschlossen ist, cluster1-01:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name mc1
   -mapping SN[65432]
   ```

Verwandte Informationen

- Verwenden Sie das Tape-Aliasing
- Entfernen von Bandaliasen
- "Speicherband-Aliassatz"

Entfernen Sie Bandaliase zu einem Bandlaufwerk oder Medienwechsler für die ONTAP Bandsicherung

Sie können Aliase mit dem `storage tape alias clear` Befehl entfernen, wenn für ein Bandlaufwerk oder einen Medienwechsler keine persistenten Aliase mehr erforderlich sind.

Schritte

1. Entfernen Sie einen Alias von einem Bandlaufwerk oder einem Medienwechsler mit dem `storage tape alias clear` Befehl.

   Erfahren Sie mehr über `storage tape alias clear` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl werden die Aliase aller Bandlaufwerke entfernt, indem der Umfang der Alias-Clear-Operation auf angegeben wird `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

Nachdem Sie fertig sind

Wenn Sie eine Bandsicherung oder einen Wiederherstellungsvorgang mit NDMP durchführen, müssen Sie dem Bandlaufwerk oder Mittelwechsler einen neuen Alias-Namen zuweisen, um weiterhin auf das Bandgerät zugreifen zu können.

Verwandte Informationen

- Verwenden Sie das Tape-Aliasing
- Bandaliasen werden zugewiesen
- "Speicherband-Alias löschen"

Aktivieren oder Deaktivieren von ONTAP -Bandreservierungen

Mit der `tape.reservations` Option können Sie steuern, wie ONTAP die Reservierungen von Tape-Geräten verwaltet. Standardmäßig ist die Tape-Reservierung deaktiviert.

Über diese Aufgabe

Die Aktivierung der Option zur Bandreservierung kann Probleme verursachen, wenn Bandlaufwerke, Mittelwechsler, Brücken oder Bibliotheken nicht ordnungsgemäß funktionieren. Wenn Bandbefehle melden, dass das Gerät reserviert ist, wenn keine anderen Speichersysteme das Gerät verwenden, sollte diese Option deaktiviert werden.

Schritte

1. Um entweder den SCSI-Reserve-/Release-Mechanismus oder SCSI Persistent Reservationsor zum Deaktivieren von Bandreservierungen zu verwenden, geben Sie folgenden Befehl in der clustershell ein:

   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi` Wählt den SCSI-Reserve-/Freigabemechanismus aus.

   `persistent` Wählt SCSI Persistent Reservations aus.

   `off` Deaktiviert Bandreservierungen.

Verwandte Informationen

Welche Tape-Reservierungen sind

ONTAP -Befehle zum Überprüfen von Bandbibliotheksverbindungen

Sie können Informationen über den Verbindungspfad zwischen einem Speichersystem und einer mit dem Speichersystem verbundenen Bandbibliothek anzeigen. Sie können diese Informationen verwenden, um den Verbindungspfad zur Konfiguration der Bandbibliothek zu überprüfen oder um Probleme mit den Verbindungspfaden zu beheben.

Sie können die folgenden Details der Tape Library anzeigen, um die Tape Library-Verbindungen zu überprüfen, nachdem Sie eine neue Tape Library hinzugefügt oder erstellt haben, oder nach dem Wiederherstellen eines fehlerhaften Pfads in einem Single Path oder Multipath-Zugriff auf eine Tape Library. Sie können diese Informationen auch zur Fehlerbehebung bei pfadbezogenen Fehlern verwenden oder wenn der Zugriff auf eine Bandbibliothek fehlschlägt.

- Node, mit dem die Bandbibliothek verbunden ist
- Geräte-ID
- NDMP-Pfad
- Name der Tape-Bibliothek
- Ziel-Port- und Initiator-Port-IDs
- Single Path- oder Multipath-Zugriff auf eine Tape Library für jedes Ziel oder FC Initiator-Port
- Details zur Datenintegrität im Zusammenhang mit dem Pfad, z. B. „`Pfadfehler`“ und „`Pfad Qual`“
- LUN-Gruppen und LUN-Anzahl

Ihr Ziel ist	Befehl
Zeigen Sie Informationen zu einer Tape Library in einem Cluster an	`system node hardware tape library show`
Zeigen Sie Pfadinformationen für eine Tape-Bibliothek an	`storage tape library path show`
Zeigen Sie für jeden Initiator-Port Pfadinformationen für eine Tape Library an	`storage tape library path show-by-initiator`
Anzeigen der Verbindungsinformationen zwischen einer Speicher-Bandbibliothek und einem Cluster	`storage tape library config show`

Verwandte Informationen

- "Speicherbandbibliothekskonfiguration anzeigen"
- "Systemknoten-Hardware-Bandbibliothek anzeigen"
- "Speicherbandbibliothekspfad anzeigen"
- "Speicherbandbibliothekspfad Show-by-Initiator"

Allgemeines zu Bandlaufwerken

Erfahren Sie mehr über qualifizierte ONTAP Bandlaufwerke

Sie müssen ein qualifiziertes Bandlaufwerk verwenden, das getestet wurde und für die ordnungsgemäße Verwendung auf einem Speichersystem geeignet ist. Sie können Tape-Aliasing befolgen und auch Bandreservierungen aktivieren, um sicherzustellen, dass zu einem bestimmten Zeitpunkt nur ein Speichersystem auf ein Bandlaufwerk zugreift.

Ein qualifiziertes Bandlaufwerk ist ein Bandlaufwerk, das getestet wurde und für den ordnungsgemäßen Einsatz auf Storage-Systemen eingesetzt wurde. Sie können Bandlaufwerke für vorhandene ONTAP Versionen unter Verwendung der Tape-Konfigurationsdatei qualifizieren.

Format der ONTAP -Bandkonfigurationsdatei

Das Dateiformat der Tape-Konfiguration umfasst Felder wie Anbieter-ID, Produkt-ID und Angaben zu den Komprimierungstypen für ein Bandlaufwerk. Diese Datei besteht außerdem aus optionalen Feldern zur Aktivierung der Autoload-Funktion eines Bandlaufwerks und zum Ändern der Befehlszeitlimits eines Bandlaufwerks.

In der folgenden Tabelle wird das Format der Bandkonfigurationsdatei angezeigt:

Element	Größe	Beschreibung
`vendor_id` (Zeichenfolge)	Bis zu 8 Byte	Die vom `SCSI Inquiry` Befehl gemeldete Hersteller-ID.
`product_id`(Zeichenfolge)	Bis zu 16 Byte	Die vom `SCSI Inquiry` Befehl gemeldete Produkt-ID.
`id_match_size`(Nummer)		Die Anzahl der Bytes der Produkt-ID, die zur Suche nach dem zu identifizierenden Bandlaufwerk verwendet werden soll, beginnend mit dem ersten Zeichen der Produkt-ID in den Anfragedaten.
`vendor_pretty` (Zeichenfolge)	Bis zu 16 Byte	Wenn dieser Parameter vorhanden ist, wird er durch den String angegeben, der durch den Befehl angezeigt `storage tape show -device-names` wird; andernfalls wird INQ_VENDOR_ID angezeigt.
`product_pretty`(Zeichenfolge)	Bis zu 16 Byte	Wenn dieser Parameter vorhanden ist, wird er durch den String angegeben, der durch den Befehl angezeigt `storage tape show -device-names` wird; andernfalls wird INQ_PRODUCT_ID angezeigt.

Die `vendor_pretty` `product_pretty` Felder und sind optional, aber wenn eines dieser Felder einen Wert hat, muss das andere auch einen Wert haben.

In der folgenden Tabelle werden die Beschreibung, der Dichtecode und der Komprimierungsalgorithmus für die verschiedenen Kompressionstypen wie `l`, , `m` `h` und erläutert `a`:

Element	Größe	Beschreibung
`{l	m	h
a}_description=(string)`	Bis zu 24 Byte	Der String, `sysconfig -t` der für den Befehl nodeshell gedruckt werden soll, der die Eigenschaften der jeweiligen Dichteeinstellung beschreibt.
`{l	m	h
a}_density=(hex codes)`		Der Dichtecode, der im SCSI-Modus-Seitenblockdeskriptor festgelegt werden soll, entspricht dem gewünschten Dichtecode für l, m, h oder a.
`{l	m	h
a}_algorithm=(hex codes)`		Der Kompressionsalgorithmus, der in der SCSI Compression Mode Page eingestellt werden soll, entspricht dem Dichtecode und der gewünschten Dichtecharakteristik.

In der folgenden Tabelle werden die optionalen Felder beschrieben, die in der Bandkonfigurationsdatei verfügbar sind:

Feld	Beschreibung
`autoload=(Boolean yes/no)`	Dieses Feld ist auf eingestellt `yes`, wenn das Bandlaufwerk über eine automatische Ladefunktion verfügt. Das heißt, nachdem die Bandkassette eingesetzt wurde, wird das Bandlaufwerk bereit, ohne dass ein `SCSI load` Befehl (Start/Stop Unit) ausgeführt werden muss. Die Standardeinstellung für dieses Feld ist `no`.

Feld	Beschreibung
`cmd_timeout_0x`	Einzelner Zeitüberschreitungswert. Sie müssen dieses Feld nur verwenden, wenn Sie einen anderen Timeout-Wert als den Wert angeben möchten, der vom Bandtreiber als Standard verwendet wird. In der Beispieldatei werden die vom Bandlaufwerk verwendeten Standard-SCSI-Befehlszeitlimits aufgeführt. Der Timeout-Wert kann in Minuten (m), Sekunden (s) oder Millisekunden (ms) angegeben werden. Sie sollten dieses Feld nicht ändern.

Sie können die Tape-Konfigurationsdatei von der NetApp Support-Website herunterladen und anzeigen.

Beispiel für ein Dateiformat einer Bandkonfiguration

Das Dateiformat der Bandkonfiguration für das HP LTO5 ULTRIUM-Bandlaufwerk lautet 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 GB“

`l_density`=0x00

`l_algorithm`=0x00

`m_description`= „LTO-3(ro)/4 8/1.600 GB cmp“

`m_density`=0x00

`m_algorithm`=0x01

`h_description`= „LTO-5 1.600 GB“

`h_density`=0x58

`h_algorithm`=0x00

`a_description`= „LTO-5 3200 GB cmp“

`a_density`=0x58

`a_algorithm`=0x01

`autoload`= „Ja“

Verwandte Informationen

- "NetApp Tools: Konfigurationsdateien für Tape-Geräte"
- "Speicherband-Show"

Wie das ONTAP -Speichersystem ein Bandlaufwerk dynamisch qualifiziert

Das Storage-System stimmt ein Bandlaufwerk dynamisch ab, indem es seine Anbieter-ID und Produkt-ID mit den Informationen in der Tape-Qualifizierungstabelle abstimmt.

Beim Anschließen eines Bandlaufwerks an das Speichersystem wird nach einer Anbieter-ID und einer Produkt-ID-Übereinstimmung zwischen den während der Tape-Erkennung erhaltenen Informationen und den Informationen in der internen Bandqualifizierungstabelle sucht. Wenn das Speichersystem eine Übereinstimmung erkennt, wird das Bandlaufwerk als qualifiziert markiert und kann auf das Bandlaufwerk zugreifen. Wenn das Speichersystem keine Übereinstimmung finden kann, bleibt das Bandlaufwerk im ungequalifizierten Zustand und wird nicht aufgerufen.

Übersicht über Bandgeräte

Erfahren Sie mehr über ONTAP Bandgeräte

Ein Bandgerät ist eine Darstellung eines Bandlaufwerks. Es handelt sich um eine spezielle Kombination aus Rückwind- und Komprimierungsfunktionen eines Bandlaufwerks.

Für jede Kombination aus Rewind- und Komprimierungsfunktionen wird ein Bandgerät erstellt. Daher kann es bei einem Bandlaufwerk oder einer Bandbibliothek mehrere Bandgeräte geben. Sie müssen ein Bandgerät angeben, um Bänder zu verschieben, zu schreiben oder zu lesen.

Wenn Sie ein Bandlaufwerk oder eine Bandbibliothek auf einem Speichersystem installieren, erstellt ONTAP Bandgeräte, die dem Bandlaufwerk oder der Bandbibliothek zugeordnet sind.

ONTAP erkennt Bandlaufwerke und Tape Libraries und weist ihnen logische Zahlen und Bandgeräte zu. ONTAP erkennt Fibre Channel-, SAS- und parallele SCSI-Bandlaufwerke und -Bibliotheken, wenn sie mit den Schnittstellen-Ports verbunden sind. ONTAP erkennt diese Laufwerke, wenn ihre Schnittstellen aktiviert sind.

Format eines ONTAP -Bandgerätenamens

Jedes Bandgerät verfügt über einen zugeordneten Namen, der in einem definierten Format angezeigt wird. Das Format enthält Informationen zum Gerätetyp, zum Rückwind, zum Alias und zum Kompressionstyp.

Das Format eines Bandgerätnamens lautet wie folgt:

`rewind_type st alias_number compression_type`

`rewind_type` Ist der Rücklauf-Typ.

In der folgenden Liste werden die verschiedenen Werte für den Rückwind beschrieben:

- **R**

  ONTAP windet das Band erneut, nachdem die Tape-Datei geschrieben wurde.

- **Nr**

  ONTAP fillaesst das Tape nach dem Schreiben der Tape-Datei nicht mehr zurück. Sie müssen diesen Rewind-Typ verwenden, wenn Sie mehrere Banddateien auf demselben Band schreiben möchten.

- **Ur**

  Dies ist die Art des erneuten Entlads/Neueinzuspulen. Wenn Sie diesen Rückwind-Typ verwenden, entlädt die Bandbibliothek das Band, wenn es das Ende einer Banddatei erreicht, und lädt dann das nächste Band, falls vorhanden.

  Sie dürfen diesen Rückwind nur unter folgenden Umständen verwenden:

  - Das mit diesem Gerät verbundene Bandlaufwerk befindet sich in einer Bandbibliothek oder befindet sich im Bibliotheksmodus.
  - Das mit diesem Gerät verbundene Bandlaufwerk ist an ein Speichersystem angeschlossen.
  - In der für dieses Bandlaufwerk definierten Library-Bandsequenz sind ausreichend Bänder für den Vorgang verfügbar, den Sie gerade durchführen.

> Wenn Sie ein Band mit einem Rückspulen-Gerät aufnehmen, müssen Sie das Band vor dem Lesen zurückspulen.

`st` Ist die Standardbezeichnung für ein Bandlaufwerk.

`alias_number` Ist der Alias, den ONTAP dem Bandlaufwerk zuweist. Wenn ONTAP ein neues Bandlaufwerk erkennt, weist ONTAP dem Bandlaufwerk einen Alias zu.

`compression_type` Ist ein laufwerksspezifischer Code für die Dichte der Daten auf dem Band und den Typ der Komprimierung.

Die folgende Liste beschreibt die verschiedenen Werte für `compression_type`:

- **A**

  Höchste Komprimierung

- **H**

  Hohe Komprimierung

- **M**

  Mittlere Komprimierung

- **L**

  Niedrige Komprimierung

Beispiele

`nrst0a` Gibt ein Gerät ohne Rücklauf auf Bandlaufwerk 0 mit der höchsten Komprimierung an.

Beispiel für eine Liste mit Bandgeräten

Das folgende Beispiel zeigt die Bandgeräte, die mit HP Ultrium 2-SCSI verbunden sind:

```
        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)
```

In der folgenden Liste werden die Abkürzungen im vorhergehenden Beispiel beschrieben:

- GB—GB; dies ist die Kapazität des Bandes.
- w/Kompr. Mit Komprimierung; dieser zeigt die Tape-Kapazität mit Komprimierung an.

Unterstützte Anzahl gleichzeitiger ONTAP Bandgeräte

ONTAP unterstützt für jedes Speichersystem (pro Node) in einer beliebigen Kombination aus Fibre-Channel-, SCSI- oder SAS-Anbindungen maximal 64 gleichzeitige Bandlaufanbindungen, 16 mittlere Wechsler und 16 Bridge- oder Router-Geräte.

Bandlaufwerke oder mittlere Wechsler können Geräte in physischen oder virtuellen Bandbibliotheken oder Standalone-Geräten sein.

> Obwohl ein Speichersystem 64 Verbindungen von Bandlaufwerken erkennen kann, hängt die maximale Anzahl von Backup- und Wiederherstellungssitzungen von den Skalierbarkeitsgrenzen der Backup Engine ab, die gleichzeitig durchgeführt werden können.

Verwandte Informationen

Skalierbarkeitsgrenzen für Dump Backup und Restore-Sessions

Tape-Aliasing

Übersicht über Bandglättung

Aliasing vereinfacht den Prozess der Geräteidentifizierung. Aliasing bindet einen physischen Pfadnamen (PPN) oder eine Seriennummer (SN) eines Bandes oder eines Mittelwechsels an einen dauerhaften, aber veränderbaren Aliasnamen.

In der folgenden Tabelle wird beschrieben, wie Sie mit Tape Aliasing sicherstellen können, dass ein Bandlaufwerk (oder Bandbibliothek oder Mediumwechsler) immer mit einem einzigen Aliasnamen verknüpft ist:

Szenario	Neuzuweisen des Alias
Wenn das System neu gebootet wird	Das Bandlaufwerk wird automatisch seinen vorherigen Alias neu zugewiesen.
Wenn ein Bandgerät zu einem anderen Port bewegt wird	Der Alias kann so eingestellt werden, dass er auf die neue Adresse zeigt.
Wenn mehrere Systeme ein bestimmtes Bandgerät verwenden	Der Benutzer kann festlegen, dass der Alias für alle Systeme gleich ist.

Wenn Sie ein Upgrade von Data ONTAP 8.1.x auf Data ONTAP 8.2.x durchführen, ändert die Bandalias-Funktion von Data ONTAP 8.2.x die vorhandenen Bandnamen. In einem solchen Fall müssen Sie möglicherweise die Bandalias-Namen in der Backup-Anwendung aktualisieren.

Das Zuweisen von Bandaliasen stellt eine Korrespondenz zwischen den logischen Namen von Sicherungsgeräten (z. B. st0 oder mc1) und einem Namen dar, der dauerhaft einem Port, einem Bandlaufwerk oder einem Mittelwechsler 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 auf das Gerät gibt es alle Fehlermeldungen unter Verwendung des physischen Pfads zurück.

Für Aliasing stehen zwei Arten von Namen zur Verfügung: Name des physischen Pfads und Seriennummer.

Erfahren Sie mehr über physische Pfadnamen

PPPNs (Physical Path Names) sind die numerischen Adresssequenzen, die ONTAP Bandlaufwerken und Bandbibliotheken basierend auf dem SCSI-2/3-Adapter oder Switch (bestimmte Position) zuweisen, die sie mit dem Speichersystem verbunden sind. PPNS werden auch als elektrische Namen bezeichnet.

PPNS von Direct-Attach-Geräten verwenden das folgende Format: `host_adapter. device_id_lun`

Der LUN-Wert wird nur für Band- und Medienwechsler-Geräte angezeigt, deren LUN-Werte nicht Null sind. Wenn der LUN-Wert Null ist, `lun` wird der Teil des PPN nicht angezeigt.

Der PPN 8.6 zeigt beispielsweise an, dass die Host-Adapternummer 8, die Geräte-ID 6 und die Nummer der logischen Einheit (LUN) 0 ist.

SAS Tape-Geräte sind ebenfalls Direct-Attached-Geräte. Beispiel: Der PPN 5c.4 zeigt an, dass in einem Speichersystem der SAS-HBA in Steckplatz 5 angeschlossen ist, das SAS-Band mit Port C des SAS-HBA verbunden ist und die Geräte-ID 4 lautet.

PPNS von Fibre Channel-Switch-angeschlossenen Geräten verwenden das folgende Format: `switch:port_id. device_id_lun`

Zum Beispiel zeigt der PPN MY_SWITCH:5.3L2 an, dass das Bandlaufwerk, das an Port 5 eines Switch namens MY_SWITCH angeschlossen ist, mit der Geräte-ID 3 gesetzt ist und die LUN 2 hat.

Die LUN (Logical Unit Number) wird durch das Laufwerk bestimmt. Fibre Channel, SCSI-Bandlaufwerke und Bibliotheken sowie Festplatten verfügen über PPNs.

PPNS von Bandlaufwerken und Bibliotheken ändern sich nicht, es sei denn, der Name des Switches ändert sich, das Bandlaufwerk oder die Bandbibliothek bewegt sich oder das Bandlaufwerk oder die Bandbibliothek wird neu konfiguriert. PPNS bleibt nach Neustart unverändert. Wenn zum Beispiel ein Bandlaufwerk namens MY_SWITCH:5.3L2 entfernt wird und ein neues Bandlaufwerk mit der gleichen Geräte-ID und LUN an Port 5 des Switch MY_SWITCH angeschlossen ist, würde das neue Bandlaufwerk über MY_SWITCH:5.3L2 zugänglich sein.

Erfahren Sie mehr über Seriennummern

Eine Seriennummer (SN) ist eine eindeutige Kennung für ein Bandlaufwerk oder einen Mittelwechsler. ONTAP generiert basierend auf SN anstelle des WWN Aliase.

Da die SN eine eindeutige Kennung für ein Bandlaufwerk oder einen Mittelwechsler ist, bleibt der Alias gleich, unabhängig von den mehreren Verbindungspfaden zum Bandlaufwerk oder zum Mittelwechsler. So können Storage-Systeme dasselbe Bandlaufwerk oder denselben Mediumwechsler in einer Bandbibliothek nachverfolgen.

Die SN eines Bandlaufwerks oder eines Mittelwechsels ändert sich nicht, auch wenn Sie den Fibre-Channel-Switch umbenennen, an den das Bandlaufwerk oder der Mittelwechsler angeschlossen ist. Wenn Sie jedoch in einer Bandbibliothek ein vorhandenes Bandlaufwerk durch ein neues ersetzen, generiert ONTAP neue Aliase, da sich die SN des Bandlaufwerks ändert. Wenn Sie ein vorhandenes Bandlaufwerk zu einem neuen Steckplatz in einer Bandbibliothek verschieben oder die LUN des Bandlaufwerks neu zuordnen, generiert ONTAP einen neuen Alias für das Bandlaufwerk.

Sie müssen die Backupanwendungen mit den neu erstellten Aliase aktualisieren.

Die Seriennummer eines Bandgeräts verwendet das folgende Format: `SN[xxxxxxxxxx]L[X]`

`x` Ist ein alphanumerisches Zeichen und L`X` ist die LUN des Bandgeräts. Wenn die LUN 0 ist,`X` wird der L-Teil der Zeichenfolge nicht angezeigt.

Jede SN besteht aus bis zu 32 Zeichen; das Format für die SN ist nicht Groß-/Kleinschreibung.

Überlegungen zur Konfiguration des ONTAP Multipath-Bandzugriffs

Sie können zwei Pfade vom Speichersystem konfigurieren, um auf die Bandlaufwerke in einer Bandbibliothek zuzugreifen. Falls ein Pfad ausfällt, kann das Storage-System die anderen Pfade für den Zugriff auf die Bandlaufwerke verwenden, ohne dass der ausgefallene Pfad sofort repariert werden muss. So wird sichergestellt, dass Tape-Vorgänge neu gestartet werden können.

Bei der Konfiguration von Multipath Tape-Zugriff über Ihr Storage-System müssen Sie Folgendes beachten:

- Bei Tape-Bibliotheken, die die LUN-Zuordnung unterstützen, muss die LUN-Zuordnung für den Multipath-Zugriff auf eine LUN-Gruppe symmetrisch für jeden Pfad sein.

  Bandlaufwerke und Medienwechsler werden LUN-Gruppen (Satz von LUNs, die sich denselben

Initiatorpfadsatz teilen) in einer Bandbibliothek zugewiesen. Alle Bandlaufwerke einer LUN-Gruppe müssen für Backup- und Restore-Vorgänge auf allen mehreren Pfaden verfügbar sein.

- Es können maximal zwei Pfade vom Speichersystem konfiguriert werden, um auf die Bandlaufwerke in einer Bandbibliothek zuzugreifen.
- Multipath Tape-Zugriff unterstützt die Lastverteilung. Der Lastenausgleich ist standardmäßig deaktiviert.

Im folgenden Beispiel greift das Storage-System über zwei Initiator-Pfade auf die LUN-Gruppe 0 zu: 0b und 0d. In beiden Pfaden hat die LUN-Gruppe die gleiche LUN-Anzahl, 0 und LUN-Anzahl, 5. Das Storage-System greift über nur einen Initiator-Pfad, 3d auf die LUN-Gruppe 1 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

- "Speicherbandbibliothekskonfiguration anzeigen"

Erfahren Sie, wie Sie Bandlaufwerke und Bibliotheken zu ONTAP Speichersystemen hinzufügen

Sie können dem Storage-System dynamisch Bandlaufwerke und Bibliotheken hinzufügen (ohne das Storage-System offline schalten zu müssen).

Wenn Sie einen neuen Mittelwechsler hinzufügen, erkennt das Speichersystem seine Anwesenheit und fügt ihn der Konfiguration hinzu. Wenn der mittlere Wechsler bereits in der Alias-Information referenziert wird, werden keine neuen logischen Namen erstellt. Wenn auf die Bibliothek kein Verweis erfolgt, erstellt das Speichersystem einen neuen Alias für den Mediumwechsler.

In einer Konfiguration der Bandbibliothek müssen Sie ein Bandlaufwerk oder einen mittleren Wechsler auf LUN 0 eines Zielports für ONTAP konfigurieren, um alle Mittelwechsler und Bandlaufwerke auf diesem Zielport zu erkennen.

Erfahren Sie mehr über ONTAP -Bandreservierungen

Mehrere Speichersysteme können den Zugriff auf Bandlaufwerke, mittlere Wechsler, Brücken oder Bandbibliotheken gemeinsam nutzen. Durch die Reservierung von Bandgeräten wird sichergestellt, dass zu einem bestimmten Zeitpunkt nur ein Speichersystem auf ein Gerät zugreift, indem entweder der SCSI-Reserve-

/Freigabemechanismus oder SCSI Persistent Reservations für alle Bandlaufwerke, Mittelwechsler, Brücken und Bandbibliotheken ermöglicht wird.

> Alle Systeme, die Geräte in einer Bibliothek gemeinsam nutzen, unabhängig davon, ob Switches beteiligt sind oder nicht, müssen dieselbe Reservierungsmethode verwenden.

Der SCSI-Reserve-/Freigabemechanismus für die Reservierung von Geräten funktioniert unter normalen Bedingungen gut. Während der Recovery-Verfahren bei Schnittstellenfehlern können jedoch Reservierungen verloren gehen. In diesem Fall können andere Initiatoren als der reservierte Eigentümer auf das Gerät zugreifen.

Reservierungen, die mit SCSI Persistent Reservations vorgenommen werden, werden nicht durch Fehler-Recovery-Mechanismen wie Loop-Reset oder Ziel-Reset beeinflusst; jedoch implementieren nicht alle Geräte SCSI Persistent Reservations richtig.

Datentransfer zwischen Storage-Systemen

Übertragen Sie ONTAP -Daten mit ndmpcopy

Der `ndmpcopy` Befehl nodeshell überträgt Daten zwischen Storage-Systemen, die NDMP v4 unterstützen. Sie können vollständige und inkrementelle Datentransfers durchführen. Sie können komplette oder partielle Volumes, qtrees, Verzeichnisse oder einzelne Dateien übertragen.

Über diese Aufgabe

Bei Verwendung von ONTAP 8.x und früheren Versionen sind inkrementelle Transfers auf maximal zwei Ebenen begrenzt (ein vollständiger und bis zu zwei inkrementelle Backups).

Ab ONTAP 9.0 und neueren Versionen sind inkrementelle Transfers auf maximal neun Ebenen begrenzt (ein vollständiger und bis zu neun inkrementelle Backups).

Sie können `ndmpcopy` in der Nodeshell-Befehlszeile des Quell- und Ziel-Storage-Systems oder in einem Storage-System ausgeführt werden, das weder Quelle noch Ziel des Datentransfers ist. Sie können außerdem `ndmpcopy` auf einem einzigen Storage-System ausgeführt werden, das sowohl das Quell- als auch das Ziel des Datentransfers ist.

Im `ndmpcopy` Befehl können Sie IPv4- oder IPv6-Adressen der Quell- und Zielspeichersysteme verwenden. Das Pfadformat ist `/vserver_name/volume_name \[path\]`.

Schritte

1. Aktivieren des NDMP-Service auf Quell- und Ziel-Storage-Systemen:

Wenn Sie den Datentransfer an der Quelle oder am Ziel in durchführen…	Verwenden Sie den folgenden Befehl…

NDMP-Modus mit SVM-Umfang	`vserver services ndmp on` Für die NDMP-Authentifizierung in der Admin-SVM lautet das Benutzerkonto `admin` und die Benutzerrolle lautet `admin` oder `backup`. In der Daten-SVM lautet das Benutzerkonto `vsadmin` und die Benutzerrolle ist `vsadmin` bzw. `vsadmin-backup` Rolle.
Node-Scoped NDMP-Modus	`system services ndmp on`

2. Übertragen Sie Daten innerhalb eines Storage-Systems oder zwischen Storage-Systemen mit dem `ndmpcopy` Befehl in der Nodeshell:

```
::> 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. Sie müssen die IP-Adresse der Quelle und des Ziels angeben. Die Loopback-Adresse (127.0.0.1) wird für die Quell-IP-Adresse oder die Ziel-IP-Adresse nicht unterstützt.

- Der `ndmpcopy` Befehl bestimmt den Adressmodus für Steuerverbindungen wie folgt:
  - Der Adressmodus für die Steuerverbindung entspricht der angegebenen IP-Adresse.
  - Sie können diese Regeln mit den `-mcs -mcd` Optionen und überschreiben.
- Handelt es sich bei der Quelle oder dem Ziel um das ONTAP System, verwenden Sie abhängig vom NDMP-Modus (Node-Scoped oder SVM-Scoped) eine IP-Adresse, die den Zugriff auf das Ziel-Volume ermöglicht.
- `source_path` Und `destination_path` sind die absoluten Pfadnamen bis auf die granulare Ebene von Volume, qtree, Verzeichnis oder Datei.
- `-mcs` Gibt den bevorzugten Adressierungsmodus für die Steuerverbindung zum Quellspeichersystem an.

  `inet` Zeigt einen IPv4-Adressmodus an und `inet6` gibt einen IPv6-Adressmodus an.
- `-mcd` Gibt den bevorzugten Adressierungsmodus für die Steuerverbindung zum Zielspeichersystem an.

  `inet` Zeigt einen IPv4-Adressmodus an und `inet6` gibt einen IPv6-Adressmodus an.
- `-md` Gibt den bevorzugten Adressierungsmodus für Datentransfers zwischen Quell- und Zielspeichersystemen an.

  `inet` Zeigt einen IPv4-Adressmodus an und `inet6` gibt einen IPv6-Adressmodus an.

  Wenn Sie die `-md` Option im `ndmpcopy` Befehl nicht verwenden, wird der Adressierungsmodus für die

Datenverbindung wie folgt festgelegt:

- Wenn eine der für die Steuerverbindungen angegebenen Adressen eine IPv6-Adresse ist, ist der Adressmodus für die Datenverbindung IPv6.
- Wenn es sich bei den beiden für die Steuerverbindungen angegebenen Adressen um IPv4-Adressen handelt, `ndmpcopy` versucht der Befehl zunächst, einen IPv6-Adressmodus für die Datenverbindung zu verwenden.

  Wenn dies fehlschlägt, verwendet der Befehl einen IPv4-Adressmodus.

  > Eine IPv6-Adresse, falls angegeben, muss in eckigen Klammern eingeschlossen sein.

  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>
```

+
Mit diesem Beispielbefehl werden die Steuerverbindungen und die Datenverbindung explizit auf den IPv6-Adressmodus eingestellt:

```
> 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>
```

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Optionen für den Befehl ndmpcopy

Sie sollten die verfügbaren Optionen für den nodeshell-Befehl verstehen `ndmpcopy`, um erfolgreich zu "Datentransfer"sein.

In der folgenden Tabelle sind die verfügbaren Optionen aufgeführt.

Option	Beschreibung
`-sa username:[password]`	Mit dieser Option werden der Benutzername und das Passwort für die Quellauthentifizierung für die Verbindung zum Quell-Speichersystem festgelegt. Diese Option ist obligatorisch. Für einen Benutzer ohne Administratorberechtigung müssen Sie das vom System generierte NDMP-spezifische Passwort des Benutzers angeben. Das vom System generierte Passwort ist sowohl für Admin- als auch für nicht-Admin-Benutzer erforderlich.
`-da username:[password]`	Mit dieser Option werden der Benutzername und das Passwort für die Zielauthentifizierung für die Verbindung zum Zielspeichersystem festgelegt. Diese Option ist obligatorisch.
`-st {md5`	`text}`
Diese Option legt den Quellauthentifizierungstyp fest, der bei der Verbindung mit dem Quellspeichersystem verwendet werden soll.Dies ist eine obligatorische Option und daher sollte der Benutzer entweder die `text md5` Option oder angeben.	`-dt {md5`
`text}`	Mit dieser Option wird der Zielauthentifizierungstyp festgelegt, der bei der Verbindung mit dem Ziel-Speichersystem verwendet wird.
`-l`	Mit dieser Option wird die für die Übertragung verwendete Dump `0 1 9 0 1 9`-Ebene auf den angegebenen Wert von Level gesetzt.gültige Werte sind, , bis , wobei eine vollständige Übertragung angezeigt wird und bis eine inkrementelle Übertragung angibt. Der Standardwert ist `0`.
`-d`	Diese Option ermöglicht die Erstellung von NDMPcopy Debug-Protokollmeldungen. Die NDMPcopy Debug-Log-Dateien befinden sich im `/mroot/etc/log` Root-Volume. Die Namen der NDMPcopy-Debug-Log-Dateien liegen im `ndmpcopy.yyyymmdd` Format vor.
`-f`	Diese Option aktiviert den erzwungenen Modus. In diesem Modus können Systemdateien im `/etc` Stammverzeichnis des 7-Mode Volumes überschrieben werden.

Option	Beschreibung
`-h`	Mit dieser Option wird die Hilfemeldung gedruckt.
`-p`	Bei dieser Option werden Sie aufgefordert, das Kennwort für die Quell- und Zielautorisierung einzugeben. Dieses Kennwort setzt das für die `-sa -da` Optionen und angegebene Kennwort außer Kraft. Sie können diese Option nur verwenden, wenn der Befehl in einer interaktiven Konsole ausgeführt wird.
`-exclude`	Diese Option schließt angegebene Dateien oder Verzeichnisse aus dem für die Datenübertragung angegebenen Pfad aus. Der Wert kann eine kommagetrennte Liste von Verzeichnis- oder Dateinamen wie **`.pst`** `oder sein .txt`. Die maximale Anzahl unterstützter Ausschlussmuster beträgt 32 und die maximale Anzahl unterstützter Zeichen beträgt 255.

NDMP für FlexVol Volumes

Erfahren Sie mehr über NDMP für ONTAP FlexVol -Volumes

Das Network Data Management Protocol (NDMP) ist ein standardisiertes Protokoll für die Kontrolle von Backup, Recovery und anderen Arten des Datentransfers zwischen primären und sekundären Storage-Geräten, wie z. B. Storage-Systemen und Tape Libraries.

Durch Aktivierung der NDMP-Unterstützung auf einem Storage-System ermöglichen Sie, dass das Storage-System mit NDMP-fähigen, über das Netzwerk angeschlossenen Backup-Applikationen (auch *Data Management Applications* oder *DMAs*), Datenservern und Bandservern, die an Backup- oder Recovery-Vorgängen beteiligt sind, kommunizieren kann. Die gesamte Netzwerkkommunikation erfolgt über ein TCPIP- oder TCP/IPv6-Netzwerk. NDMP bietet darüber hinaus eine Low-Level-Kontrolle von Bandlaufwerken und Mediumchanger.

Sie können die Durchführung von Prozessen zur Tape-Sicherung und -Wiederherstellung entweder im NDMP-Modus mit Node-Umfang oder im NDMP-Modus mit dem Umfang von Storage Virtual Machines (SVM) durchführen.

Beachten Sie jedoch bei der Verwendung von NDMP, der Liste der Umgebungsvariablen und den unterstützten NDMP Tape-Backup-Topologien. Sie können auch die erweiterte DAR-Funktion aktivieren oder deaktivieren. ONTAP unterstützt die beiden von unterstützten Authentifizierungsmethoden zur Authentifizierung des NDMP-Zugriffs auf ein Storage-System: Klartext und Herausforderung.

Verwandte Informationen

Von ONTAP unterstützte Umgebungsvariablen

Allgemeines zum NDMP-Modus

Erfahren Sie mehr über die ONTAP NDMP-Betriebsmodi

Sie können Tape-Backup- und -Restore-Vorgänge entweder auf Node-Ebene oder auf SVM-Ebene (Storage Virtual Machine) durchführen. Damit diese Vorgänge auf SVM-Ebene erfolgreich durchgeführt werden können, muss der NDMP-Service auf der SVM aktiviert sein.

Wenn Sie ein Upgrade von Data ONTAP 8.2 auf Data ONTAP 8.3 durchführen, wird der in 8.2 verwendete NDMP-Betriebsmodus nach dem Upgrade von 8.2 auf 8.3 weiterhin beibehalten.

Bei der Installation eines neuen Clusters mit Data ONTAP 8.2 oder neuer befindet sich NDMP standardmäßig im NDMP-Modus mit SVM-Umfang. Zur Durchführung von Tape-Backup- und Restore-Vorgängen im NDMP-Modus mit Node-Umfang müssen Sie explizit den NDMP-Modus mit Node-Umfang aktivieren.

Erfahren Sie mehr über den knotenbezogenen ONTAP NDMP-Modus

Im NDMP-Modus mit Node-Umfang können Sie Tape-Backup- und Restore-Vorgänge auf Node-Ebene durchführen. Der in Data ONTAP 8.2 verwendete NDMP-Betriebsmodus wird nach dem Upgrade von 8.2 auf 8.3 weiterhin beibehalten.

Im NDMP-Modus mit Node-Umfang können Sie auf einem Node, der Eigentümer des Volume ist, Backup- und Restore-Vorgänge auf Band durchführen. Um diese Vorgänge auszuführen, müssen Sie NDMP-Steuerverbindungen auf einer logischen Schnittstelle einrichten, die auf dem Node gehostet wird, der Eigentümer des Volume- oder Bandgeräten ist.

Dieser Modus ist veraltet und wird in einer zukünftigen größeren Version entfernt.

Erfahren Sie mehr über den SVM-scoped ONTAP NDMP-Modus

Sie können Backup- und Restore-Vorgänge für Tapes auf der SVM-Ebene (Storage Virtual Machine) erfolgreich durchführen, wenn der NDMP-Service auf der SVM aktiviert ist. Wenn die Backup-Applikation die CAB-Erweiterung unterstützt, können Sie alle Volumes sichern und wiederherstellen, die über verschiedene Nodes in der SVM eines Clusters gehostet werden.

Eine NDMP-Steuerungsverbindung kann für verschiedene LIF-Typen hergestellt werden. Im NDMP-Modus mit SVM-Umfang gehören diese LIFs entweder der Daten-SVM oder der Admin-SVM. Die Verbindung kann auf einer logischen Schnittstelle nur dann hergestellt werden, wenn der NDMP-Service auf der SVM, der diese LIF ist, aktiviert ist.

Eine Daten-LIF gehört zur Daten-SVM, die Intercluster LIF, Node-Management-LIF und Cluster-Management-LIF gehören der Admin-SVM an.

Im SVM-Scoped NDMP-Modus hängt die Verfügbarkeit von Volumes und Bandgeräten für Backup- und Wiederherstellungsvorgänge vom LIF-Typ ab, von dem die NDMP-Steuerverbindung eingerichtet wurde, und vom Status der CAB-Erweiterung. Wenn Ihre Backup-Applikation die CAB-Erweiterung und ein Volume unterstützt und sich das Tape-Gerät dieselbe Affinität teilen, kann die Backup-Applikation einen lokalen Backup- oder Restore-Vorgang durchführen, anstatt drei Wege zu sichern oder wiederherzustellen.

Verwandte Informationen

Befehle für die Verwaltung des NDMP-Modus mit Node-Umfang

Überlegungen zur Verwendung des ONTAP NDMP-Dienstes

Beim Starten des NDMP-Dienstes auf Ihrem Storage-System müssen Sie einige Überlegungen beachten.

- Jeder Node unterstützt bei Nutzung angeschlossener Bandlaufwerke maximal 16 gleichzeitige Backups, Restores oder Kombinationen der beiden Nodes.
- NDMP Services können Dateiverläufe auf Anfrage von NDMP-Backup-Applikationen generieren.

  Der Dateiverlauf wird von Backup-Applikationen verwendet, um eine optimierte Recovery ausgewählter Datenuntergruppen aus einem Backup-Image zu ermöglichen. Die Erstellung und Verarbeitung von Dateiverläufe kann für das Storage-System und die Backup-Applikation zeitaufwendig und CPU-intensiv sein.

  SMTape unterstützt den Dateiverlauf nicht.

  Wenn Ihre Datensicherung für Disaster Recovery konfiguriert ist – wo das gesamte Backup-Image wiederhergestellt wird – können Sie die Erzeugung des Dateiverlaufs deaktivieren, um die Backup-Zeiten zu verkürzen. Prüfen Sie in der Dokumentation Ihrer Backup-Applikation, ob die Erzeugung des NDMP-Dateiverlaufs deaktiviert werden kann.

- Firewall-Richtlinie für NDMP ist standardmäßig bei allen LIF-Typen aktiviert.
- Im NDMP-Modus mit Node-Umfang muss die Sicherung eines FlexVol Volume mithilfe der Backup-Applikation ein Backup auf einem Node initiiert werden, der Eigentümer des Volume ist.

  Sie können jedoch kein Root-Volume des Nodes sichern.

- Sie können gemäß den Firewall-Richtlinien von jeder beliebigen logischen Schnittstelle NDMP-Backups durchführen.

  Wenn Sie eine Daten-LIF verwenden, müssen Sie ein LIF auswählen, das nicht für Failover konfiguriert ist. Wenn eine Daten-LIF während eines NDMP-Vorgangs ausfällt, fällt der NDMP-Vorgang aus und muss erneut ausgeführt werden.

- Im NDMP-Modus mit Node-Umfang und der SVM (Storage Virtual Machine) wird der NDMP-Modus ohne Unterstützung von CAB-Erweiterungen bereitgestellt. Die NDMP-Datenverbindung verwendet dieselbe LIF wie die NDMP-Steuerverbindung.
- Während der LIF-Migration werden laufende Backup- und Restore-Vorgänge unterbrochen.

  Sie müssen die Backup- und Restore-Vorgänge nach der LIF-Migration 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 Snapshot an.

- Wenn ein SnapMirror Ziel mithilfe der Dump-Engine auf Band gesichert wird, werden nur die Daten des Volume gesichert.

  Wenn jedoch ein SnapMirror Ziel mithilfe von SMTape auf Tape gesichert wird, werden die Metadaten auch gesichert. Die SnapMirror Beziehungen und die zugehörigen Metadaten werden nicht auf Tapes gesichert. Somit werden während der Wiederherstellung nur die Daten auf dem Volume wiederhergestellt, die zugehörigen SnapMirror Beziehungen sind aber nicht wiederhergestellt.

Verwandte Informationen

Was ist Cluster-bewusste Backup-Erweiterung

"Systemadministration"

Umgebungsvariable

Erfahren Sie mehr über die unterstützten Umgebungsvariablen für ONTAP NDMP

Umgebungsvariablen dienen der Kommunikation von Informationen zu Backup- oder Wiederherstellungsvorgang zwischen einer NDMP-fähigen Backup-Applikation und einem Storage-System.

Wenn ein Benutzer beispielsweise angibt, dass eine Backup-Anwendung gesichert werden soll `/vserver1/vol1/dir1`, setzt die Backup-Anwendung die Umgebungsvariable DATEISYSTEM auf `/vserver1/vol1/dir1`. Ebenso setzt die Backup-Anwendung die EBENE-Umgebungsvariable auf 1 (eins), wenn ein Benutzer angibt, dass ein Backup der Stufe 1 sein soll.

Die Festlegung und Untersuchung von Umgebungsvariablen ist für Backup-Administratoren in der Regel transparent. Das heißt, die Backup-Applikation legt sie automatisch fest.

Ein Backup-Administrator gibt Umgebungsvariablen selten an. Möglicherweise möchten Sie jedoch den Wert einer Umgebungsvariable von der Backup-Applikation ändern, um ein funktionales oder Performance-Problem zu charakterisieren oder zu umgehen. Beispielsweise möchte ein Administrator die Erzeugung des Dateiverlaufs vorübergehend deaktivieren, um festzustellen, ob die Verarbeitung der Dateiverlaufs-Informationen durch die Backup-Applikation zu Performance-Problemen oder zu Funktionsproblemen führt.

Viele Backup-Anwendungen bieten Mittel zum Überschreiben oder Ändern von Umgebungsvariablen oder zum Festlegen zusätzlicher Umgebungsvariablen. Weitere Informationen finden Sie in der Dokumentation Ihrer Backup-Anwendung.

Von ONTAP unterstützte Umgebungsvariablen

ONTAP unterstützt Umgebungsvariablen, denen ein Standardwert zugeordnet ist. Sie können diese Standardwerte jedoch manuell ändern.

Wenn Sie die von der Backup-Anwendung festgelegten Werte manuell ändern, verhält sich die Anwendung möglicherweise unvorhersehbar. Dies liegt daran, dass die Sicherungs- oder Wiederherstellungsvorgänge möglicherweise nicht das tun, was die Backup-Anwendung von ihnen erwartet hatte. In einigen Fällen kann jedoch eine vernünftige Änderung dazu beitragen, Probleme zu erkennen oder zu umgehen.

In den folgenden Tabellen sind die Umgebungsvariablen aufgeführt, deren Verhalten bei Dump und SMTape häufig der Einsatz ist, sowie die Variablen, die nur für Dump und SMTape unterstützt werden. Die Tabellen enthalten zudem eine Beschreibung der Arbeitsweise der durch ONTAP unterstützten Umgebungsvariablen, wenn diese verwendet werden:

In den meisten Fällen, Variablen, die den Wert haben, `Y` auch `T` `N` akzeptieren und auch akzeptieren `F`.

Umgebungsvariablen werden für Dump und SMTape unterstützt

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
DEBUGGEN	`Y` Oder `N`	`N`	Gibt an, dass Debugging-Informationen gedruckt werden.
DATEISYSTEM	`string`	`none`	Gibt den Pfadnamen des Stammes der zu sichernden Daten an.
NDMP_VERSION	`return_only`	`none`	Die Variable NDMP_VERSION sollte nicht geändert werden. Die durch den Backup-Vorgang erstellte Variable NDMP_VERSION liefert die NDMP-Version zurück. ONTAP legt die Variable NDMP_VERSION während eines Backups zur internen Verwendung fest und gibt die Variable zu Informationszwecken an eine Backup-Applikation weiter. Die NDMP-Version einer NDMP-Sitzung ist nicht mit dieser Variable festgelegt.
PFADNAME_TRENNZEICHEN	`return_value`	`none`	Gibt das Trennzeichen für den Pfadnamen an. Dieses Zeichen hängt vom zu sichernden Dateisystem ab. Bei ONTAP wird dieser Variable das Zeichen „`/`“ zugewiesen. Der NDMP-Server setzt diese Variable vor dem Start einer Bandsicherung.
TYP	`dump` Oder `smtape`	`dump`	Gibt den Typ der unterstützten Sicherung an, der die Sicherung und Wiederherstellung von Bandmedien durchführen soll.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
VERBOSE	`Y` Oder `N`	`N`	Erhöht die Protokollmeldungen bei einer Bandsicherung oder -Wiederherstellung.

Umgebungsvariablen werden für Dump unterstützt

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
ACL_START	`return_only`	`none`	Die Variable ACL_START wird durch den Backup-Vorgang erstellt und ist ein Offset-Wert, der von einer Wiederherstellung durch direkten Zugriff oder einer erneuerbaren NDMP-Sicherungsoperation verwendet wird. Der Offset-Wert ist der Byte-Offset in der Dump-Datei, in der die ACL-Daten (Pass V) beginnen und am Ende einer Sicherung zurückgegeben werden. Für eine Wiederherstellung der gesicherten Daten durch direkten Zugriff muss der ACL_START-Wert beim Start an den Wiederherstellungsvorgang übergeben werden. Ein neu startbarer NDMP-Backup-Vorgang verwendet den ACL_START-Wert, um mit der Backup-Applikation zu kommunizieren, wo der Einwegteil des Backup-Streams beginnt.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
BASE_DATE	`0`, `-1` Oder `DUMP_DATE` Wert	`-1`	Gibt das Startdatum für inkrementelle Backups an. Wenn auf festgelegt `-1`, ist der inkrementelle Spezifikator BASE_DATE deaktiviert. Wenn Sie auf `0` ein Backup der Ebene 0 setzen, werden inkrementelle Backups aktiviert. Nach der ersten Sicherung wird der Wert der DUMP_DATE-Variable aus dem vorherigen inkrementellen Backup der VARIABLE BASE_DATE zugewiesen. Diese Variablen sind eine Alternative zu DEN LEVEL-/UPDATE-basierten inkrementellen Backups.
DIREKT	`Y` Oder `N`	`N`	Gibt an, dass ein Restore schnell direkt an den Speicherort auf dem Band weiterleiten soll, in dem sich die Dateidaten befinden, anstatt das gesamte Tape zu scannen. Damit die direkte Wiederherstellung des Zugriffs funktioniert, muss die Backup-Anwendung Informationen zur Positionierung bereitstellen. Wenn diese Variable auf eingestellt `Y` ist, gibt die Backup-Anwendung die Datei- oder Verzeichnisnamen und die Positionierungsinformationen an.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
DMP_NAME	`string`	`none`	Gibt den Namen für eine Sicherung mehrerer Unterstrukturen an. Diese Variable ist für mehrere Unterbaumsicherungen obligatorisch.
DUMP_DATE	`return_value`	`none`	Diese Variable wird nicht direkt geändert. Sie wird durch das Backup erzeugt, wenn die Variable BASE_DATE auf einen anderen Wert als gesetzt ist `-1`. Die DUMP_DATE-Variable wird abgeleitet, indem der 32-Bit-Wert auf einen 32-Bit-Zeitwert vorsteht, der von der Dump-Software berechnet wird. Der Level wird von dem letzten Level-Wert erhöht, der in DIE VARIABLE BASE_DATE übergeben wurde. Der resultierende Wert wird als BASIS_DATE-Wert für ein nachfolgender inkrementeller Backup verwendet.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
ENHANCED_DAR_ENABLED	`Y` Oder `N`	`N`	Gibt an, ob die erweiterte DAR-Funktion aktiviert ist. Die verbesserte DAR-Funktion unterstützt das Verzeichnis DAR und DAS DATEN von Dateien mit NT-Streams. Sie bietet Performance-Verbesserungen. Verbessertes DAR während der Wiederherstellung ist nur möglich, wenn die folgenden Bedingungen erfüllt sind: • ONTAP unterstützt erweiterte DAR-Funktionen. • Der Dateiverlauf ist während der Sicherung aktiviert (HIST=Y). • Die `ndmpd.offset_map.enable` Option ist auf eingestellt `on`. • DIE Variable ENHANCED_DAR_ENABLED wird `Y` während der Wiederherstellung auf festgelegt.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
AUSSCHLIESSEN	`pattern_string`	`none`	Gibt Dateien oder Verzeichnisse an, die beim Sichern von Daten ausgeschlossen sind. Die Ausschlussliste ist eine kommagetrennte Liste von Datei- oder Verzeichnisnamen. Wenn der Name einer Datei oder eines Verzeichnisses mit einer der Namen in der Liste übereinstimmt, wird sie von der Sicherung ausgeschlossen. Beim Angeben von Namen in der Ausschlussliste gelten die folgenden Regeln: • Der genaue Name der Datei oder des Verzeichnisses muss verwendet werden. • Das Sternchen (*), ein Platzhalterzeichen, muss entweder das erste oder das letzte Zeichen des Strings sein. Jeder String kann bis zu zwei Sternchen haben. • Einem Komma in einem Datei- oder Verzeichnisnamen muss ein umgekehrter Schrägstrich vorangestellt werden. • Die Ausschlussliste kann bis zu 32 Namen enthalten.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
EXTRAHIEREN	`Y`, `N` Oder `E`	`N`	Gibt an, dass Substrukturen eines gesicherten Datensatzes wiederhergestellt werden sollen. Die Backup-Anwendung gibt die Namen der zu extrahierenden Unterstrukturen an. Wenn eine angegebene Datei einem Verzeichnis entspricht, 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, müssen Sie die Umgebungsvariable EXTRAHIEREN auf einstellen `E`.
EXTRAHIEREN_ACL	`Y` Oder `N`	`Y`	Gibt an, dass ACLs aus der gesicherten Datei bei einem Wiederherstellungsvorgang wiederhergestellt werden. Standardmäßig werden ACLs beim Wiederherstellen von Daten wiederhergestellt, mit Ausnahme von DARS (DIRECT=Y).

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
ERZWINGEN	`Y` Oder `N`	`N`	Legt fest, ob der Wiederherstellungsvorgang auf Volume-Speicherplatz und Inode-Verfügbarkeit auf dem Ziel-Volume überprüfen muss. Wenn diese Variable auf gesetzt `Y` wird, überspringt der Wiederherstellungsvorgang Prüfungen für den Volume-Speicherplatz und die Inodes-Verfügbarkeit auf dem Zielpfad. Wenn auf dem Ziel-Volume nicht genügend Volume-Speicherplatz oder Inodes verfügbar sind, stellt der Wiederherstellungsvorgang so viele Daten wieder her, wie von dem Ziel-Volume-Speicherplatz und der Inode-Verfügbarkeit zulässig. Der Wiederherstellungsvorgang wird beendet, wenn kein Volume-Speicherplatz oder -Inodes verfügbar sind.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
HIST	`Y` Oder `N`	`N`	Gibt an, dass Informationen zum Dateiverlauf an die Backup-Anwendung gesendet werden. Die meisten kommerziellen Backup-Anwendungen setzen die Variable HIST auf `Y`. Wenn Sie die Geschwindigkeit eines Backup-Vorgangs erhöhen möchten oder ein Problem mit der Dateihistorie-Sammlung beheben möchten, können Sie diese Variable auf einstellen `N`. Sie sollten die Variable HIST nicht auf einstellen `Y`, wenn die Backup-Anwendung den Dateiverlauf nicht unterstützt.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
IGNORIEREN_CTIME	`Y` Oder `N`	`N`	Gibt an, dass eine Datei nicht inkrementell gesichert wird, wenn sich der Ctime-Wert seit dem letzten inkrementellen Backup geändert hat. Bei einigen Anwendungen, wie z. B. bei der Virenscan-Software, wird der Ctime-Wert einer Datei innerhalb des Inode geändert, obwohl sich die Datei oder ihre Attribute nicht geändert haben. Aus diesem Grund sichert ein inkrementeller Backup Dateien, die sich nicht geändert haben. Die `IGNORE_CTIME` Variable sollte nur angegeben werden, wenn inkrementelle Backups eine nicht akzeptable Zeit- oder Speicherplatzmenge erfordern, da der ctime-Wert geändert wurde. Der `NDMP dump` Befehl wird `IGNORE_CTIME false` standardmäßig auf festgelegt. Die Einstellung auf `true` kann zu folgendem Datenverlust führen: 1. Wenn `IGNORE_CTIME` bei einem inkrementellen Volume-Level auf

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
IGNORE_QTREES	`Y` Oder `N`	`N`	Gibt an, dass der Wiederherstellungsvorgang keine qtree-Informationen aus gesicherten qtrees wiederherstellt.
EBENE	`0-31`	`0`	Gibt die Sicherungsebene an. Ebene 0 kopiert den gesamten Datensatz. Inkrementelle Backup-Level, angegeben durch Werte über 0, kopieren Sie alle Dateien (neu oder geändert) seit der letzten inkrementellen Sicherung. Ein Level 1 sichert zum Beispiel neue oder geänderte Dateien seit der Sicherung von Ebene 0, sichert ein Level 2 neue oder geänderte Dateien seit der Sicherung der Ebene 1 usw.
LISTE	`Y` Oder `N`	`N`	Listet die gesicherten Dateinamen und Inode-Nummern auf, ohne die Daten wiederherstellen zu müssen.
LIST_QTREES	`Y` Oder `N`	`N`	Listet die gesicherten qtrees auf, ohne die Daten wiederherstellen zu müssen.
			Löschen von Dateien, die während der inkrementellen Wiederherstellung in qtrees über die Quelle verschoben

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
MULTI_SUBTREE_ NAMEN	`string`	`none`	Gibt an, dass das Backup ein Backup mit mehreren Unterstrukturen ist. In der Zeichenfolge werden mehrere Unterbäume angegeben, die eine neu getrennte, Null-terminierte Liste von Unterbaumnamen ist. Subtrees 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 DMP_NAME-Variable verwenden.
NDMP_UNICODE_ FH	`Y` Oder `N`	`N`	Gibt an, dass zusätzlich zum NFS-Namen der Datei in den Dateiverlaufs-Informationen ein Unicode-Name enthalten ist. Diese Option wird von den meisten Backup-Anwendungen nicht verwendet und sollte erst dann eingestellt werden, wenn die Backup-Anwendung diese zusätzlichen Dateinamen erhalten soll. Die HIST-Variable muss ebenfalls eingestellt werden.
NEIN_ACLS	`Y` Oder `N`	`N`	Gibt an, dass ACLs beim Sichern von Daten nicht kopiert werden dürfen.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
NICHT_QUOTA_TREE	`Y` Oder `N`	`N`	Gibt an, dass Dateien und Verzeichnisse in qtrees beim Daten-Backup ignoriert werden müssen. Wenn auf festgelegt `Y`, werden Elemente in qtrees im von der DATEISYSTEMVARIABLE angegebenen Datensatz nicht gesichert. Diese Variable hat nur dann Wirkung, wenn die DATEISYSTEMVARIABLE ein ganzes Volume angibt. DIE Variable NON_QUOTA_TREE funktioniert nur bei Backups der Ebene 0 und funktioniert nicht, wenn DIE Variable MULTI_SUBTREE_NAMES angegeben wird. Dateien oder Verzeichnisse, die für die Sicherung ausgeschlossen werden sollen, werden nicht ausgeschlossen, wenn Sie NON_QUOTA_TREE auf `Y` gleichzeitig setzen.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
NOWRITE	`Y` Oder `N`	`N`	Gibt an, dass der Wiederherstellungsvorgang keine Daten auf die Festplatte schreiben darf. Diese Variable wird zum Debuggen verwendet.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
REKURSIV	`Y` Oder `N`	`Y`	Gibt an, dass Verzeichniseinträge während einer DAR-Wiederherstellung erweitert werden. Die DIREKTEN und ERWEITERTEN_DAR_ENABLED Umgebungsvariablen müssen `Y` ebenfalls aktiviert sein (gesetzt auf). Wenn die REKURSIVE Variable deaktiviert ist (gesetzt auf `N`), werden nur die Berechtigungen und ACLs für alle Verzeichnisse im ursprünglichen Quellpfad vom Band wiederhergestellt, nicht der Inhalt der Verzeichnisse. Wenn die REKURSIVE Variable auf gesetzt ist `N` oder die Variable RECOVER_FULL_PATHS auf gesetzt `Y` ist, muss der Wiederherstellungspfad mit dem ursprünglichen Pfad enden.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
WIEDERHERSTELLUNG_FULL_PATHS	`Y` Oder `N`	`N`	Gibt an, dass der vollständige Recovery-Pfad ihre Berechtigungen und ACLs nach DEM DAR wiederhergestellt hat. DIRECT und ENHANCED_DAR_ENABLED müssen `Y` ebenfalls aktiviert sein (gesetzt auf). Wenn RECOVER_FULL_PATHS auf gesetzt `Y` ist, muss der Wiederherstellungspfad mit dem ursprünglichen Pfad enden. Sind Verzeichnisse bereits auf dem Ziel-Volume vorhanden, werden ihre Berechtigungen und ACLs nicht vom Band wiederhergestellt.
AKTUALISIERUNG	`Y` Oder `N`	`Y`	Aktualisiert die Metadateninformationen, um EIN LEVEL-basiertes, inkrementelles Backup zu ermöglichen.

Für SMTape unterstützte Umgebungsvariablen

folgenden gültigen Wiederherstellungspfade, da sich alle Wiederherstellungspfade befinden `foo/dir1/deepdir/myfile`:

- `/foo`
- `/foo/dir`
- `/foo/dir1/deepdir`
- `/foo/dir1/deepdir/myfile`

Die folgenden sind ungültige Recovery-Pfade:

`/foo`

`/foo/dir`

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
BASE_DATE	`DUMP_DATE`	`-1`	Gibt das Startdatum für inkrementelle Backups an. `BASE_DATE` Ist eine String-Darstellung der Referenz-Snapshot-IDs. Mithilfe der `BASE_DATE` Zeichenfolge sucht SMTape den Referenz-Snapshot. `BASE_DATE` Ist bei Basis-Backups nicht erforderlich. Für ein inkrementelles Backup `DUMP_DATE` wird der Wert der Variable aus der vorherigen Basislinie oder dem inkrementellen Backup der `BASE_DATE` Variablen zugewiesen. Die Backup-Applikation weist den `DUMP_DATE` Wert einer früheren SMTape Baseline oder eines inkrementellen Backups zu.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
DUMP_DATE	`return_value`	`none`	Am Ende eines SMTape-Backups enthält DUMP_DATE eine String-ID, die den für dieses Backup verwendeten Snapshot identifiziert. Dieser Snapshot kann als Referenz-Snapshot für eine nachfolgende inkrementelle Sicherung 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 Reihenfolge der inkrementellen Backups, die mit dem Basistransfer verbunden sind. Die Backup-Set-ID ist eine eindeutige 128-Bit-ID, die während eines Basissicherung generiert wird. Die Backup-Anwendung weist diese ID der `SMTAPE_BACKUP_SET_ID` Variablen während einer inkrementellen Sicherung als Eingabe zu.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
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 Band gesichert. Für inkrementelle Backups gibt diese Variable einen inkrementellen Snapshot an. Die Variable BASE_DATE stellt den Baseline-Snapshot bereit.
SMTAPE_DELETE_SNAPSHOT	`Y` Oder `N`	`N`	Wenn die Variable SMTAPE_DELETE_SNAPSHOT für einen automatisch von SMTape erstellten SNAPSHOT auf gesetzt ist `Y`, löscht SMTape nach Abschluss des Sicherungsvorgangs diesen Snapshot. Ein von der Sicherungsanwendung erstellter Snapshot wird jedoch nicht gelöscht.
SMTAPE_BREAK_MIRROR	`Y` Oder `N`	`N`	Wenn die Variable SMTAPE_BREAK_MIRROR auf gesetzt `Y` ist, `DP` wird das Volume des Typs `RW` nach einer erfolgreichen Wiederherstellung in ein Volume geändert.

Erfahren Sie mehr über gängige ONTAP NDMP-Bandsicherungstopologien

NDMP unterstützt verschiedene Topologien und Konfigurationen zwischen Backup-Anwendungen und Speichersystemen oder anderen NDMP-Servern, die Daten (Dateisysteme) und Tape-Services bereitstellen.

Storage-System auf lokales Band

In der einfachsten Konfiguration sichert eine Backup-Applikation die Daten eines Storage-Systems auf ein mit dem Storage-System verbundenes Tape-Subsystem. Die NDMP-Steuerungsverbindung besteht über die Netzwerkgrenze hinweg. Die innerhalb des Storage-Systems zwischen den Daten- und Tape-Services

vorhandene NDMP-Datenverbindung wird als lokale NDMP-Konfiguration bezeichnet.

Storage-System-to-Tape, der an ein anderes Storage-System angeschlossen ist

Eine Backup-Anwendung kann auch Daten aus einem Speichersystem auf einer Bandbibliothek sichern (ein mittlerer Wechsler mit einem oder mehreren Bandlaufwerken), die an ein anderes Speichersystem angeschlossen ist. In diesem Fall erfolgt die NDMP-Datenverbindung zwischen den Daten- und Banddiensten über eine TCP- oder TCP/IPv6-Netzwerkverbindung. Dies wird als NDMP-Konfiguration für drei-Wege-Storage-Systeme bezeichnet.

Tape Library mit Storage-System zu Network-Attached Storage

NDMP-fähige Tape Libraries bieten eine Variante der drei-Wege-Konfiguration. In diesem Fall wird die Bandbibliothek direkt mit dem TCP/IP-Netzwerk verbunden und kommuniziert über einen internen NDMP-Server mit der Backup-Applikation und dem Storage-System.

Storage-System-to-Data-Server-to-Tape oder Datenserver-to-Storage-System-to-Tape

NDMP unterstützt darüber hinaus drei-Wege-Konfigurationen für das Storage-System und den Daten-Server-zu-Storage-System, obwohl diese Varianten weniger verbreitet sind. Mit dem Storage-System-to-Server können Storage-Systemdaten in einer Tape Library gesichert werden, die mit dem Host der Backup-Applikation oder einem anderen Datenserversystem verbunden ist. Die Konfiguration des Server-to-Storage-Systems ermöglicht die Sicherung von Serverdaten in einer über das Storage-System angeschlossenen Tape Library.

Von ONTAP unterstützte NDMP-Authentifizierungsmethoden

Sie können eine Authentifizierungsmethode angeben, um NDMP-Verbindungsanforderungen zuzulassen. ONTAP unterstützt zwei Methoden zur Authentifizierung des NDMP-Zugriffs auf ein Storage-System: Klartext und Herausforderung.

Im NDMP-Modus mit Node-Scoped sind Challenge und Klartext standardmäßig aktiviert. Sie können die Herausforderung jedoch nicht deaktivieren. Sie können Klartext aktivieren und deaktivieren. In der Klartext-Authentifizierungsmethode wird das Anmeldepasswort als Klartext übertragen.

Im NDMP-Modus mit festgelegtem Umfang der Storage Virtual Machine (SVM) ist die Authentifizierungsmethode standardmäßig schwierig. Im Gegensatz zum NDMP-Modus mit Node-Scoped können Sie in diesem Modus sowohl Klartext- als auch Challenge-Authentifizierungsmethoden aktivieren und deaktivieren.

Verwandte Informationen

Benutzerauthentifizierung in einem NDMP-Modus mit Node-Umfang

Benutzerauthentifizierung im NDMP-Modus mit SVM-Umfang

NDMP-Erweiterungen unterstützt von ONTAP

NDMP v4 bietet einen Mechanismus für die Erstellung von NDMP v4 Protokollerweiterungen ohne Änderung des Kernprotokolls NDMP v4. Sie sollten die NDMP v4 Erweiterungen kennen, die von ONTAP unterstützt werden.

Die folgenden NDMP v4 Erweiterungen werden von ONTAP unterstützt:

- Cluster-sensibles Backup (CAB)

  Diese Erweiterung wird nur im NDMP-Modus mit SVM-Umfang unterstützt.

- Connection Address Extension (CAE) für IPv6-Unterstützung
- Erweiterungsklasse 0x2050

  Diese Erweiterung unterstützt nicht starrbare Backup-Vorgänge und Snapshot Management-Erweiterungen.

  Die `NDMP_SNAP_RECOVER` Meldung, die Teil der Snapshot Management Extensions ist, wird verwendet, um einen Wiederherstellungsvorgang zu starten und die wiederhergestellten Daten von einem lokalen Snapshot an einen lokalen Dateisystemspeicherort zu übertragen. In ONTAP ermöglicht diese Meldung die Wiederherstellung von Volumes und regulären Dateien nur.

  Die `NDMP_SNAP_DIR_LIST` Meldung ermöglicht Ihnen das Durchsuchen der Snapshots eines Volumes. Falls während des Surfvorgangs ein unterbrechungsfreier Vorgang ausgeführt wird, muss die Backup-Applikation den Browservorgang erneut initiieren.

- NDMP-Erweiterung für neustartbare Sicherungen

  Sie können die Funktion NDMP Restartable Backup Extension (RBE) verwenden, um ein Backup von einem bekannten Checkpoint im Daten-Stream vor dem Ausfall neu zu starten.

Erfahren Sie mehr über die erweiterte DAR-Funktionalität für ONTAP NDMP

Sie können die erweiterte Funktion zur Wiederherstellung von Daten über Direktzugriff (Direct Access Recovery, DAR) für Verzeichnis-DAR und DAR von Dateien und NT-Streams nutzen. Standardmäßig ist die erweiterte DAR-Funktion aktiviert.

Die Aktivierung der erweiterten DAR-Funktionalität kann sich auf die Backup-Performance auswirken, da eine Offsetzuordnung erstellt und auf Tapes geschrieben werden muss. Im NDMP-Modus mit Node-Umfang und SVM-Umfang (Storage Virtual Machine) können Sie das erweiterte DAR aktivieren oder deaktivieren.

ONTAP Skalierbarkeitsgrenzen für NDMP-Sitzungen

Sie müssen die maximale Anzahl von NDMP-Sitzungen kennen, die gleichzeitig auf Speichersystemen mit unterschiedlichen Systemspeicherkapazitäten eingerichtet werden können. Diese maximale Zahl hängt vom Systemspeicher eines Storage-Systems ab.

Die in der folgenden Tabelle aufgeführten Einschränkungen gelten für den NDMP Server. Die im Abschnitt „`Scalability Limits for Dump Backup and Restore Sessions`“ genannten Einschränkungen gelten für die Dump- und Restore-Sitzung.

Skalierbarkeitsgrenzen für Dump Backup und Restore-Sessions

Systemspeicher eines Storage-Systems	Maximale Anzahl von NDMP-Sitzungen
Weniger als 16 GB	8

Systemspeicher eines Storage-Systems	Maximale Anzahl von NDMP-Sitzungen
Größer oder gleich 16 GB, aber kleiner als 24 GB	20
Größer oder gleich 24 GB	36

Sie können den Systemspeicher Ihres Speichersystems mit dem `sysconfig -a` Befehl (verfügbar über die nodeshell) abrufen. Erfahren Sie mehr über `sysconfig -a` in der "ONTAP-Befehlsreferenz".

Erfahren Sie mehr über die NDMP-Unterstützung mit ONTAP FlexGroup -Volumes

Ab ONTAP 9.7 wird NDMP auf FlexGroup Volumes unterstützt.

Ab ONTAP 9.7 wird der NDMPcopy Befehl für den Datentransfer zwischen FlexVol und FlexGroup Volumes unterstützt.

Wenn Sie von ONTAP 9.7 auf eine frühere Version zurücksetzen, werden die inkrementellen Transfer-Informationen der vorherigen Transfers nicht beibehalten. Daher müssen Sie nach dem Zurücksetzen eine Basiskopie durchführen.

Ab ONTAP 9.8 werden auf FlexGroup Volumes die folgenden NDMP-Funktionen unterstützt:

- Die NDMP_SNAP_RECOVERY-Nachricht in der Erweiterungsklasse 0x2050 kann für die Wiederherstellung einzelner Dateien in einem FlexGroup-Volume verwendet werden.
- NDMP Restartable Backup Extension (RBE) wird für FlexGroup Volumes unterstützt.
- Umgebungsvariablen EXCLUDE und MULTI_SUBTREE_NAMES werden für FlexGroup-Volumes unterstützt.

Erfahren Sie mehr über NDMP mit ONTAP SnapLock -Volumes

Die Erstellung mehrerer Kopien von Daten, die der Regulierung unterworfen sind, bietet Ihnen redundante Recovery-Szenarien. So können Sie die WORM-Merkmale (Write Once, Read Many) von Quelldateien auf einem SnapLock Volume aufbewahren.

WORM-Attribute für die Dateien in einem SnapLock Volume werden beim Backup, Restore und Kopieren von Daten beibehalten. WORM-Attribute sind jedoch nur bei der Wiederherstellung auf ein SnapLock Volume durchgesetzt. Wenn ein Backup aus einem SnapLock Volume auf ein anderes Volume als ein SnapLock Volume wiederhergestellt wird, werden DIE WORM-Attribute erhalten bleiben, aber ignoriert und nicht durch ONTAP durchgesetzt.

Verwaltung des Node-Scoped NDMP-Modus für FlexVol Volumes

Erfahren Sie mehr über die Verwaltung des ONTAP -Node-Scoped-NDMP-Modus für FlexVol -Volumes

Sie können NDMP auf Node-Ebene mit NDMP-Optionen und -Befehlen verwalten. Sie können die NDMP-Optionen mit dem `options` Befehl ändern. Für den Zugriff auf ein Speichersystem müssen NDMP-spezifische Anmeldedaten zum Durchführen von Bandsicherungs- und Wiederherstellungsvorgängen verwendet werden.

Erfahren Sie mehr über `options` in der "ONTAP-Befehlsreferenz".

Befehle zum Verwalten des ONTAP -Node-Scoped-NDMP-Modus

Sie können `system services ndmp` NDMP mit diesen Befehlen auf Node-Ebene verwalten. Einige dieser Befehle sind veraltet und werden in einer zukünftigen größeren Version entfernt.

Sie können die folgenden NDMP-Befehle nur auf der erweiterten Berechtigungsebene verwenden:

- `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`

Ihr Ziel ist	Befehl
Aktivieren des NDMP-Service	`system services ndmp on*`
Deaktivieren des NDMP-Dienstes	`system services ndmp off*`
Zeigt die NDMP-Konfiguration an	`system services ndmp show*`
NDMP-Konfiguration ändern	`system services ndmp modify*`
Zeigt die Standard-NDMP-Version an	`system services ndmp version*`
Zeigt die Konfiguration des NDMP-Dienstes an	`system services ndmp service show`
Konfiguration des NDMP-Dienstes ändern	`system services ndmp service modify`
Zeigt alle NDMP-Sitzungen an	`system services ndmp status`
Anzeigen detaillierter Informationen zu allen NDMP-Sitzungen	`system services ndmp probe`
Beenden Sie die angegebene NDMP-Sitzung	`system services ndmp kill`
Beenden Sie alle NDMP-Sitzungen	`system services ndmp kill-all`
Ändern Sie das NDMP-Passwort	`system services ndmp password*`
Aktivieren des NDMP-Modus mit Node-Umfang	`system services ndmp node-scope-mode on*`

Ihr Ziel ist	Befehl
Deaktivieren Sie den NDMP-Modus mit Node-Umfang	`system services ndmp node-scope-mode off*`
Zeigen den Status des NDMP-Modus mit Node-Umfang an	`system services ndmp node-scope-mode status*`
Alle NDMP-Sitzungen mit Nachdruck beenden	`system services ndmp service terminate`
Starten Sie den NDMP-Service-Daemon	`system services ndmp service start`
Beenden Sie den NDMP-Service-Daemon	`system services ndmp service stop`
Starten Sie die Protokollierung für die angegebene NDMP-Sitzung	`system services ndmp log start*`
Beenden der Protokollierung für die angegebene NDMP-Sitzung	`system services ndmp log stop*`

- Diese Befehle sind veraltet und werden in einer zukünftigen größeren Version entfernt.

Erfahren Sie mehr über `system services ndmp` in der "ONTAP-Befehlsreferenz".

Benutzerauthentifizierung in einem NDMP-Modus mit Node-Umfang

Im NDMP-Modus mit Node-Umfang müssen Sie für den Zugriff auf ein Storage-System NDMP-spezifische Anmeldedaten verwenden, um die Backup- und Restore-Vorgänge auf Tape durchzuführen.

Die Standard-Benutzer-ID lautet „`root`“. Bevor Sie NDMP auf einem Node verwenden, müssen Sie sicherstellen, dass Sie das dem NDMP-Benutzer zugeordnete Standardpasswort ändern. Sie können auch die Standard-NDMP-Benutzer-ID ändern.

Verwandte Informationen

Befehle für die Verwaltung des NDMP-Modus mit Node-Umfang

Welcher Node-Scoped NDMP-Modus ist

Managen des SVM-Scoped NDMP-Modus für FlexVol Volumes

Erfahren Sie mehr über die Verwaltung des ONTAP SVM-bezogenen NDMP-Modus für FlexVol -Volumes

Sie können NDMP auf Basis pro SVM mit den NDMP-Optionen und -Befehlen verwalten. Sie können die NDMP-Optionen mit dem `vserver services ndmp modify` Befehl ändern. Im SVM-Scoped NDMP-Modus ist die Benutzerauthentifizierung in den rollenbasierten Zugriffssteuerungsmechanismus integriert.

Sie können NDMP in der Liste zulässige oder unzulässige Protokolle mit dem `vserver modify` Befehl hinzufügen. Standardmäßig befindet sich NDMP in der Liste der zugelassenen Protokolle. Wenn der Liste der

nicht zulässigen Protokolle NDMP hinzugefügt wird, können NDMP-Sitzungen nicht erstellt werden.

Sie können den LIF-Typ steuern, auf dem eine NDMP-Datenverbindung hergestellt wird `-preferred -interface-role`, indem Sie die Option verwenden. Während einer NDMP-Datenverbindung wählt NDMP eine IP-Adresse aus, die zum von dieser Option angegebenen LIF-Typ gehört. Wenn die IP-Adressen keiner dieser LIF-Typen angehören, kann die NDMP-Datenverbindung nicht hergestellt werden. Erfahren Sie mehr über `vserver services ndmp modify` in der "ONTAP-Befehlsreferenz".

Befehle zum Verwalten des ONTAP SVM-bezogenen NDMP-Modus

Sie können mit diesen `vserver services ndmp` Befehlen NDMP auf jeder Storage Virtual Machine (SVM, ehemals Vserver) managen.

Ihr Ziel ist	Befehl
Aktivieren des NDMP-Service	`vserver services ndmp on` Der NDMP-Service muss immer auf allen Nodes in einem Cluster aktiviert sein. Sie können den NDMP-Service auf einem Node mit dem `system services ndmp on` Befehl aktivieren. Standardmäßig ist der NDMP-Service immer auf einem Node aktiviert.
Deaktivieren des NDMP-Dienstes	`vserver services ndmp off`
Zeigt die NDMP-Konfiguration an	`vserver services ndmp show`
NDMP-Konfiguration ändern	`vserver services ndmp modify`
Zeigt die Standard-NDMP-Version an	`vserver services ndmp version`
Zeigt alle NDMP-Sitzungen an	`vserver services ndmp status`
Anzeigen detaillierter Informationen zu allen NDMP-Sitzungen	`vserver services ndmp probe`
Beenden Sie eine angegebene NDMP-Sitzung	`vserver services ndmp kill`
Beenden Sie alle NDMP-Sitzungen	`vserver services ndmp kill-all`
Erstellen Sie das NDMP-Passwort	`vserver services ndmp generate-password`

Ihr Ziel ist	Befehl
Zeigt den NDMP-Erweiterungsstatus an	`vserver services ndmp extensions show` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.
Ändern Sie den NDMP-Verlängerungsstatus (aktivieren oder deaktivieren)	`vserver services ndmp extensions modify` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.
Starten Sie die Protokollierung für die angegebene NDMP-Sitzung	`vserver services ndmp log start` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.
Beenden der Protokollierung für die angegebene NDMP-Sitzung	`vserver services ndmp log stop` Dieser Befehl ist auf der erweiterten Berechtigungsebene verfügbar.

Erfahren Sie mehr über `vserver services ndmp` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Befehle für die Verwaltung des SVM-Scoped NDMP-Modus

Was ist Cluster-bewusste Backup-Erweiterung

Welcher SVM-Scoped NDMP-Modus ist

"Systemadministration"

Erfahren Sie mehr über die Cluster Aware Backup-Erweiterung für ONTAP NDMP

CAB (Cluster Aware Backup) ist eine NDMP v4 Protokollerweiterung. Mit dieser Erweiterung kann der NDMP-Server eine Datenverbindung auf einem Knoten einrichten, der ein Volume besitzt. So kann die Backup-Applikation auch ermitteln, ob sich Volumes und Tape-Geräte auf demselben Node in einem Cluster befinden.

Damit der NDMP-Server den Knoten identifizieren kann, der ein Volume besitzt, und eine Datenverbindung zu einem solchen Knoten hergestellt werden kann, muss die Backup-Anwendung die CAB-Erweiterung unterstützen. CAB-Erweiterung erfordert, dass die Backup-Anwendung den NDMP-Server über das zu sichernde Volume informiert oder wiederhergestellt, bevor die Datenverbindung hergestellt wird. So kann der NDMP-Server den Node ermitteln, der das Volume hostet, und die Datenverbindung entsprechend herstellen.

Mit der von der Backup-Applikation unterstützten CAB-Erweiterung bietet der NDMP-Server Affinitätsdaten zu Volumes und Bandgeräten. Mithilfe dieser Affinitätsdaten kann die Backup-Applikation ein lokales Backup durchführen, statt eines Dreiwege-Backups durchzuführen, wenn sich ein Volume- und ein Tape-Gerät auf demselben Node eines Clusters befinden.

Verfügbarkeit von ONTAP -Volumes und Bandgeräten für Backup und Wiederherstellung auf verschiedenen LIF-Typen

Sie können eine Backup-Applikation konfigurieren, um eine NDMP-Steuerverbindung auf einem der LIF-Typen in einem Cluster herzustellen. Im NDMP-Modus mit Storage Virtual Machine (SVM) können Sie die Verfügbarkeit von Volumes und Tape-Geräten für Backup- und Restore-Vorgänge bestimmen, abhängig von diesen LIF-Typen und dem Status der CAB-Erweiterung.

In der folgenden Tabelle sind die Verfügbarkeit von Volumes und Bandgeräten für NDMP Control Connection LIF-Typen und der Status der CAB-Erweiterung aufgeführt:

Verfügbarkeit von Volumes und Bandgeräten, wenn CAB-Erweiterung von der Backup-Anwendung nicht unterstützt wird

NDMP-Steuerverbindung – LIF-Typ	Volumes verfügbar für Backup und Restore	Bandgeräte für Backup oder Restore verfügbar
Node-Management-LIF	Alle Volumes werden von einem Node gehostet	Mit dem Node, der die Node-Management-LIF hostet, verbundene Tape-Geräte
Data LIF	Nur Volumes, die zu der SVM gehören, die von einem Node gehostet wird, der die Daten-LIF hostet	Keine
Cluster-Management-LIF	Alle Volumes werden von einem Node gehostet, der die LIF zum Cluster-Management hostet	Keine
Intercluster LIF	Alle Volumes werden von einem Node gehostet, der die Intercluster LIF hostet	Mit dem Node, der die Intercluster-LIF hostet, verbundene Bandgeräte

Verfügbarkeit von Volumes und Bandgeräten, wenn die CAB-Erweiterung von der Backup-Anwendung unterstützt wird

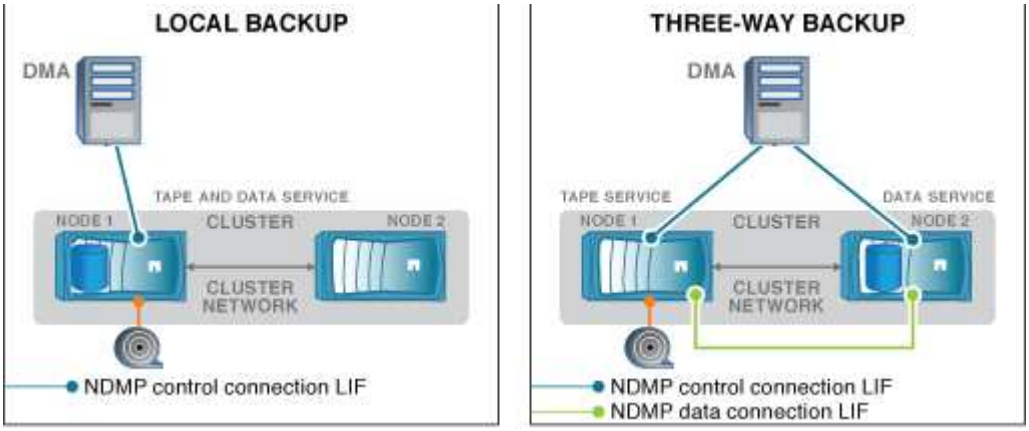
NDMP-Steuerverbindung – LIF-Typ	Volumes verfügbar für Backup und Restore	Bandgeräte für Backup oder Restore verfügbar
Node-Management-LIF	Alle Volumes werden von einem Node gehostet	Mit dem Node, der die Node-Management-LIF hostet, verbundene Tape-Geräte
Data LIF	Alle Volumes, die zu der SVM gehören, die die Daten-LIF hostet	Keine
Cluster-Management-LIF	Alle Volumes im Cluster	Alle Bandgeräte im Cluster
Intercluster LIF	Alle Volumes im Cluster	Alle Bandgeräte im Cluster

Erfahren Sie mehr über Affinitätsinformationen für ONTAP NDMP

Da die Backup-Applikation CAB-orientiert ist, bietet der NDMP-Server einzigartige Speicherinformationen über Volumes und Tape-Geräte. Mithilfe dieser Affinitätsdaten kann die Backup-Applikation ein lokales Backup durchführen, statt eines Backups der drei Wege, wenn sich ein Volume und ein Tape-Gerät dieselbe Affinität teilen.

Wenn die NDMP-Steuerverbindung auf einer Node-Management-LIF aufgebaut ist, Clustermanagement-LIF, Oder eine Intercluster-LIF: Die Backup-Applikation kann die Affinitätsdaten nutzen, um festzustellen, ob sich ein Volume und ein Tape-Gerät auf demselben Node befinden, und kann anschließend ein lokales oder dreistuges Backup oder eine Wiederherstellung durchführen. Wenn die NDMP-Steuerverbindung auf einer Daten-LIF aufgebaut ist, führt die Backup-Applikation immer ein drei-Wege-Backup durch.

Lokales NDMP-Backup und drei-Wege-NDMP-Backup



Unter Verwendung der Affinitätsdaten zu Volumes und Bandgeräten führt der DMA (Backup-Applikation) eine lokale NDMP-Sicherung auf dem Volume und dem Bandgerät durch, das sich auf Node 1 im Cluster befindet. Wenn das Volume von Node 1 zu Node 2 verschoben wird, ändert sich die Affinität über das Volume und das Tape-Gerät. Daher führt der DMA für ein nachfolgender Backup einen dreistufenden NDMP-Backup-Vorgang durch. Dadurch wird unabhängig vom Node, auf den das Volume verschoben wird, Continuity der Backup-Richtlinie für das Volume sichergestellt.

Verwandte Informationen

Was ist Cluster-bewusste Backup-Erweiterung

Der NDMP-Server unterstützt sichere ONTAP Steuerverbindungen im SVM-Bereichsmodus

Eine sichere Steuerungsverbindung zwischen der Data Management Application (DMA) und dem NDMP-Server kann über Secure Sockets (SSL/TLS) als Kommunikationsmechanismus hergestellt werden. Diese SSL-Kommunikation basiert auf den Serverzertifikaten. Der NDMP-Server wartet auf Port 30000 (von der IANA zugewiesen für den „`ndmps`“-Service).

Nach dem Herstellen der Verbindung vom Client auf diesem Port erfolgt der Standard-SSL-Handshake, in dem der Server das Zertifikat dem Client vorstellt. Wenn der Client das Zertifikat akzeptiert, ist der SSL-Handshake abgeschlossen. Nach Abschluss dieses Prozesses wird die gesamte Kommunikation zwischen Client und Server verschlüsselt. Der NDMP-Protokoll-Workflow bleibt exakt wie zuvor. Für die sichere NDMP-Verbindung ist nur eine serverseitige Zertifikatauthentifizierung erforderlich. Ein DMA kann eine Verbindung herstellen, indem er eine Verbindung zum sicheren NDMP-Dienst oder dem Standard-NDMP-Dienst herstellt.

Standardmäßig ist der sichere NDMP-Service für eine Storage Virtual Machine (SVM) deaktiviert. Sie können den sicheren NDMP-Service auf einer bestimmten SVM mit dem `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` Befehl aktivieren oder deaktivieren.

NDMP ONTAP Datenverbindungstypen

Im NDMP-Modus (Storage Virtual Machine) mit Scoped (SVM) hängen die unterstützten NDMP-Datenverbindungstypen vom LIF-Steuerverbindung-Typ und dem Status der CAB-Erweiterung ab. Dieser NDMP-Datenverbindungstyp gibt an, ob Sie ein lokales oder dreistuges NDMP-Backup oder eine Wiederherstellung durchführen können.

Sie können eine dreiseitige NDMP-Sicherung oder Wiederherstellung über ein TCP- oder TCP/IPv6-Netzwerk durchführen. In den folgenden Tabellen werden die NDMP-Datenverbindungsarten auf Basis des LIF-Typs NDMP-Steuerverbindung und des Status der CAB-Erweiterung angezeigt.

NDMP-Datenverbindungstyp, wenn CAB-Erweiterung von der Backup-Applikation unterstützt wird

NDMP-Steuerverbindung – LIF-Typ	NDMP-Datenverbindungsart
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 CAB-Erweiterung von der Backup-Anwendung nicht unterstützt wird

NDMP-Steuerverbindung – LIF-Typ	NDMP-Datenverbindungsart
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 ist Cluster-bewusste Backup-Erweiterung

"Netzwerkmanagement"

ONTAP Benutzerauthentifizierung im SVM-Bereich NDMP-Modus

Die NDMP-Benutzerauthentifizierung ist im NDMP-Modus (Storage Virtual Machine) mit Scoped integriert in die rollenbasierte Zugriffssteuerung. Im SVM-Kontext muss der

NDMP-Benutzer entweder über die Rolle „vsadmin“ oder „vsadmin-Backup“ verfügen. In einem Cluster-Kontext muss der NDMP-Benutzer entweder über die Rolle „admin“ oder „Backup“ verfügen.

Neben diesen vordefinierten Rollen kann ein Benutzerkonto, das einer benutzerdefinierten Rolle zugeordnet ist, auch für die NDMP-Authentifizierung verwendet werden, vorausgesetzt, dass die benutzerdefinierte Rolle den Ordner „vserver Services ndmp“ in ihrem Befehlsverzeichnis hat und die Zugriffsebene des Ordners nicht „none“ ist. In diesem Modus müssen Sie ein NDMP-Passwort für ein bestimmtes Benutzerkonto generieren, das über die rollenbasierte Zugriffssteuerung erstellt wird. Cluster-Benutzer in einer Administrator- 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 kann die Verfügbarkeit von Volumes und Bandgeräten für Backup- und Wiederherstellungsvorgänge je nach Benutzerrolle unterschiedlich sein.

Dieser Modus unterstützt auch die Benutzerauthentifizierung für NIS- und LDAP-Benutzer. Daher können NIS- und LDAP-Benutzer mit einer gemeinsamen Benutzer-ID und einem gemeinsamen Passwort auf mehrere SVMs zugreifen. Allerdings unterstützt die NDMP-Authentifizierung Active Directory-Benutzer nicht.

In diesem Modus muss ein Benutzerkonto mit der SSH-Anwendung und der Authentifizierungsmethode „User password“ verknüpft sein.

Verwandte Informationen

Befehle für die Verwaltung des SVM-Scoped NDMP-Modus

"Systemadministration"

Generieren Sie ein NDMP-spezifisches Passwort für ONTAP NDMP-Benutzer

Im NDMP-Modus (Storage Virtual Machine) mit Scoped (SVM) müssen Sie ein Passwort für eine bestimmte Benutzer-ID generieren. Das generierte Passwort basiert auf dem tatsächlichen Login-Passwort für den NDMP-Benutzer. Wenn sich das tatsächliche Anmeldepasswort ändert, müssen Sie das NDMP-spezifische Passwort erneut generieren.

Schritte

1. `vserver services ndmp generate-password`Erstellen Sie mit dem Befehl ein NDMP-spezifisches Passwort.

   Sie können dieses Passwort bei jedem aktuellen oder zukünftigen NDMP-Vorgang verwenden, der die Passworteingabe erfordert.

   > Im Kontext der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) können Sie NDMP-Passwörter für Benutzer generieren, die nur der SVM angehören.

   Das folgende Beispiel zeigt, wie ein NDMP-spezifisches Passwort für einen Benutzer-ID-Benutzer1 generiert wird:

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. Wenn Sie das Passwort auf Ihr reguläres Speichersystem-Konto ändern, wiederholen Sie dieses Verfahren, um Ihr neues NDMP-spezifisches Passwort zu erhalten.

Auswirkungen der Disaster Recovery auf Bandsicherungs- und Wiederherstellungsvorgänge in ONTAP MetroCluster -Konfigurationen

Sie können Tape-Backup und Restore-Vorgänge gleichzeitig während des Disaster Recovery in einer MetroCluster-Konfiguration durchführen. Die Auswirkungen dieser Vorgänge auf das Disaster Recovery müssen klar sein.

Wenn Backup- und Restore-Prozesse auf Tape auf einem Volume einer SVM in einer Disaster-Recovery-Beziehung durchgeführt werden, können Sie nach einem Switchover und einem Switchback weiterhin inkrementelle Tape-Backups durchführen und Vorgänge wiederherstellen.

Info über Dump Engine für FlexVol-Volumes

Erfahren Sie mehr über die ONTAP Dump Engine für FlexVol -Volumes

Dump ist eine Snapshot-basierte Backup- und Recovery-Lösung von ONTAP, mit der Sie Dateien und Verzeichnisse von einem Snapshot auf einem Bandgerät sichern und die gesicherten Daten auf einem Speichersystem wiederherstellen können.

Sie können Ihre Dateisystemdaten, wie Verzeichnisse, Dateien und deren zugehörigen Sicherheitseinstellungen, auf einem Bandgerät sichern, indem Sie den Backup-Speicherauszug verwenden. Sie können ein gesamtes Volume, einen vollständigen qtree oder Subbaum sichern, der weder ein gesamtes Volume noch ein vollständiger qtree ist.

Mithilfe von NDMP-konformen Backup-Applikationen können Sie eine Backup-Dump-Funktion oder -Wiederherstellung durchführen.

Wenn Sie ein Dump-Backup durchführen, können Sie den Snapshot angeben, der für ein Backup verwendet werden soll. Wenn Sie keinen Snapshot für das Backup angeben, erstellt die Dump-Engine einen Snapshot für das Backup. Nach Abschluss des Sicherungsvorgangs löscht die Dump-Engine diesen Snapshot.

Sie können Level-0, inkrementelle oder differenzielle Backups auf Band durch Verwendung der Dump-Engine durchführen.

> Nach dem Zurücksetzen auf eine Version vor Data ONTAP 8.3 müssen Sie einen Basistransfer durchführen, bevor Sie eine inkrementelle Backup-Operation durchführen.

Verwandte Informationen

"Upgrade, Zurücksetzen oder Downgrade"

So funktioniert ein Dump-Backup mit ONTAP NDMP

Ein Dump Backup schreibt mithilfe eines vordefinierten Prozesses Daten des Dateisystems von der Festplatte auf das Band. Sie können ein Backup eines Volumes, eines qtree oder Subbaums erstellen, der weder ein gesamtes Volume noch ein ganzer qtree ist.

In der folgenden Tabelle wird der Vorgang beschrieben, den ONTAP zum Backup des Objekts verwendet, das vom Dump-Pfad angegeben wird:

Stufe	Aktion
1	Bei weniger als vollständigen Volume oder vollständigen qtree Backups durchläuft ONTAP Verzeichnisse, um die zu sichernden Dateien zu identifizieren. Wenn Sie ein ganzes Volume oder einen gesamten qtree sichern, kombiniert ONTAP diese Phase mit Phase 2.
2	Bei einem vollständigen Volume oder vollständigen qtree-Backup identifiziert ONTAP die Verzeichnisse in den Volumes oder in den zu sichernden qtrees.
3	ONTAP schreibt die Verzeichnisse auf Band.
4	ONTAP schreibt die Dateien auf das Band.
5	ONTAP schreibt die ACL-Informationen (falls zutreffend) auf Tapes.

Das Dump Backup verwendet einen Snapshot Ihrer Daten für das Backup. Daher müssen Sie das Volume vor dem Start des Backups nicht offline schalten.

Der Dump Backup benennt jeden Snapshot, den er erstellt als `snapshot_for_backup.n`, wobei `n` eine Ganzzahl ist, die bei 0 beginnt. Jedes Mal, wenn das Dump-Backup einen Snapshot erstellt, wird die Ganzzahl um 1 erhöht. Die Ganzzahl wird nach dem Neustart des Speichersystems auf 0 zurückgesetzt. Nach Abschluss des Sicherungsvorgangs löscht die Dump-Engine diesen Snapshot.

Wenn ONTAP mehrere Dump-Backups gleichzeitig durchführt, erstellt die Dump-Engine mehrere Snapshots. Wenn ONTAP beispielsweise zwei Dump-Backups gleichzeitig ausführt, finden Sie die folgenden Snapshots in den Volumes, von denen Daten gesichert werden: `snapshot_for_backup.0` Und `snapshot_for_backup.1`.

> Wenn Sie ein Backup von einem Snapshot erstellen, erstellt die Dump-Engine keinen zusätzlichen Snapshot.

Arten von Daten, die die Dump-Engine sichert

Die Dump-Engine ermöglicht es Ihnen, Daten-Backups auf Tape zu erstellen, um sie vor Ausfällen oder Controller-Unterbrechungen zu schützen. Zusätzlich zum Backup von Datenobjekten wie Dateien, Verzeichnisse, qtrees oder ganzen Volumes kann die Dump-Engine viele Arten von Informationen zu jeder Datei sichern. Wenn Sie wissen, welche Daten von der Dump-Engine gesichert werden können und welche Einschränkungen berücksichtigt werden müssen, können Sie Ihren Ansatz für die Disaster Recovery planen.

Zusätzlich zum Sichern von Daten in Dateien kann die Dump-Engine die folgenden Informationen über jede

Datei sichern, falls zutreffend:

- UNIX GID, Besitzer-UID und Dateiberechtigungen
- Zugriff, Erstellung und Änderung für UNIX-Systeme
- Dateityp
- Dateigröße
- DOS-Name, DOS-Attribute und Erstellungszeit
- Zugriffssteuerungslisten (ACLs) mit 1,024 Einträgen (Aces)
- Qtree Informationen
- Verbindungspfade

Verbindungspfade werden als symbolische Links gesichert.

- Klone zu LUNs und LUNs

  Sie können ein vollständiges LUN-Objekt sichern. Sie können jedoch keine einzelne Datei innerhalb des LUN-Objekts sichern. Auf ähnliche Weise können Sie ein gesamtes LUN-Objekt, jedoch keine einzelne Datei in der LUN wiederherstellen.

  Die Dump-Engine sichert LUN-Klone als unabhängige LUNs.

- VM-bezogene Dateien

  Das Backup von VM-ausgerichteten Dateien wird in Versionen vor Data ONTAP 8.1 nicht unterstützt.

Wenn ein Snapshot-gesicherter LUN-Klon von Data ONTAP 7-Mode auf ONTAP migriert wird, ist dies eine inkonsistente LUN. Die Dump-Engine führt nicht zu einem Backup inkonsistenter LUNs.

Wenn Sie Daten auf einem Volume wiederherstellen, sind die Client-I/O-Vorgänge auf die wiederherzustellenden LUNs beschränkt. Die LUN-Einschränkung wird nur entfernt, wenn der Dump-Wiederherstellungsvorgang abgeschlossen ist. Ebenso beschränkt sich der Client-I/O während einer Wiederherstellung einzelner Dateien oder LUNs auf die wiederherzustellenden Dateien und LUNs. Diese Einschränkung wird nur entfernt, wenn die einzelne Datei oder die LUN-Wiederherstellung abgeschlossen ist. Wenn auf einem Volume, auf dem eine Dump-Wiederherstellung oder eine einzelne SnapMirror-Datei oder eine LUN-Wiederherstellung durchgeführt wird, ein Dump-Backup durchgeführt wird, werden die Dateien oder LUNs, die eine Client-I/O-Einschränkung aufweisen, nicht in das Backup einbezogen. Diese Dateien oder LUNs sind in einem nachfolgenden Backup-Vorgang enthalten, wenn die Client-I/O-Einschränkung entfernt wird.

Eine LUN, die auf Data ONTAP 8.3 ausgeführt wird und auf Tape gesichert wird, kann nur in 8.3 oder späteren Versionen wiederhergestellt werden, und nicht in einer früheren Version. Wenn die LUN auf eine frühere Version wiederhergestellt wird, wird die LUN als Datei wiederhergestellt.

Wenn Sie ein sekundäres SnapVault Volume oder ein Ziel-SnapMirror Volume auf Band sichern, werden nur die Daten auf dem Volume gesichert. Die zugehörigen Metadaten werden nicht gesichert. Wenn Sie also versuchen, das Volume wiederherzustellen, werden nur die Daten auf diesem Volume wiederhergestellt. Informationen über die Volume SnapMirror-Beziehungen sind im Backup nicht verfügbar und werden daher nicht wiederhergestellt.

Wenn Sie eine Datei abladen, die nur Windows NT Berechtigungen hat und sie auf einen UNIX-Stil qtree oder Volume wiederherstellen, erhält die Datei die standardmäßigen UNIX Berechtigungen für diesen qtree oder Volume.

Wenn Sie eine Datei abspeichern, die nur UNIX Berechtigungen hat und sie auf einen NTFS-Stil qtree oder Volume wiederherstellen, erhält die Datei die standardmäßigen Windows Berechtigungen für diesen qtree oder Volume.

Bei anderen Dumps und Wiederherstellungen werden die Berechtigungen beibehalten.

Sie können neben den Dateien, die an VMs ausgerichtet `vm-align-sector` sind, auch Backups erstellen. Weitere Informationen zu VM-ausgerichteten Dateien finden Sie unter "Logisches Storage-Management".

Erfahren Sie mehr über Inkrementketten und ONTAP NDMP

Eine Inkrementkette ist eine Reihe von inkrementellen Backups desselben Pfades. Da Sie jederzeit jedes beliebige Backup-Level angeben können, müssen Sie die Inkrementenketten verstehen, um Backups und Wiederherstellungen effektiv durchführen zu können. Sie können 31 Stufen inkrementeller Backup-Vorgänge durchführen.

Es gibt zwei Arten von Inkrementenketten:

- Eine aufeinander folgende Schrittkette, eine Sequenz von inkrementellen Backups, die mit Ebene 0 beginnt und bei jedem nachfolgenden Backup um 1 erhöht wird.
- Eine nicht aufeinanderfolgende Schrittkette, in der inkrementelle Backups Level überspringen oder Ebenen aufweisen, die nicht in der Reihenfolge sind, wie z. B. 0, 2, 3, 1 4 oder häufiger 0, 1, 1, 1 oder 0, 1, 2, 1, 2.

Inkrementelle Backups basieren auf dem letzten Backup auf niedrigerer Ebene. Die Reihenfolge der Backup-Level 0, 2, 3, 1, 4 bietet beispielsweise zwei Schrittketten: 0, 2, 3 und 0, 1, 4. Die folgende Tabelle erläutert die Grundlagen der inkrementellen Backups:

Sicherungsauftrag	Stufe erhöhen	Kette erhöhen	Basis	Gesicherte Dateien
1	0	Beides	Dateien auf dem Speichersystem	Alle Dateien im Backup-Pfad
2	2	0, 2, 3	Backup auf Ebene 0	Dateien im Sicherungspfad, die seit der Sicherung der Stufe 0 erstellt wurden
3	3	0, 2, 3	Level-2-Backup	Dateien im Backup-Pfad, die seit dem Level-2-Backup erstellt wurden

Sicherungsauftrag	Stufe erhöhen	Kette erhöhen	Basis	Gesicherte Dateien
4	1	0, 1, 4	Backup auf Ebene 0, da es sich um die aktuellste Ebene handelt, die niedriger ist als das Backup der Ebene 1	Dateien im Backup-Pfad, die seit dem Backup der Ebene 0 erstellt wurden, einschließlich Dateien, die sich in den Backups der Ebene 2 und Ebene 3 befinden
5	4	0, 1, 4	Das Backup auf Ebene 1 ist, da es eine niedrigere Ebene ist und aktueller als die Backups der Ebene 0, Ebene 2 oder Ebene-3 ist	Dateien, die seit dem Level-1-Backup erstellt wurden

Erfahren Sie mehr über den Blockierungsfaktor und ONTAP NDMP

Ein Bandblock besteht aus 1,024 Byte an Daten. Während eines Tape Backups oder einer Wiederherstellung können Sie die Anzahl der Bandblöcke angeben, die bei jedem Lese-/Schreibvorgang übertragen werden. Diese Zahl wird als *blockierfaktor* bezeichnet.

Sie können einen Sperrfaktor von 4 bis 256 verwenden. Wenn Sie ein Backup in einem anderen System als dem System wiederherstellen möchten, das das Backup durchgeführt hat, muss das Wiederherstellungssystem den Sperrfaktor unterstützen, den Sie für das Backup verwendet haben. Wenn Sie beispielsweise einen Sperrfaktor von 128 verwenden, muss das System, auf dem Sie dieses Backup wiederherstellen, einen Sperrfaktor von 128 unterstützen.

Während einer NDMP-Sicherung bestimmt der MOVER_RECORD_SIZE den Sperrfaktor. ONTAP ermöglicht einen Maximalwert von 256 KB für MOVER_RECORD_SIZE.

Wann muss ein ONTAP Dump-Backup neu gestartet werden?

Ein Dump-Backup wird manchmal nicht beendet, weil interne oder externe Fehler wie Tape-Schreibfehler, Stromausfälle, versehentliche Unterbrechungen der Benutzer oder interne Inkonsistenzen im Storage-System auftreten. Wenn Ihr Backup aus einem der folgenden Gründe ausfällt, können Sie es neu starten.

Sie können das Backup unterbrechen und neu starten, um Zeiten mit hohem Datenverkehr im Storage-System zu vermeiden oder um Mitbewerber wegen begrenzter Ressourcen auf dem Storage-System, wie beispielsweise eines Bandlaufwerks, zu vermeiden. Sie können ein langes Backup unterbrechen und es später neu starten, wenn für eine dringendere Wiederherstellung (oder Sicherung) dasselbe Bandlaufwerk erforderlich ist. Neu startbare Backups bleiben bei einem Neustart erhalten. Sie können eine abgebrochene Sicherung auf Band nur dann neu starten, wenn die folgenden Bedingungen erfüllt sind:

- Die abgebrochene Sicherung befindet sich in Phase IV

- Alle zugehörigen Snapshots, die durch den Dump-Befehl gesperrt wurden, sind verfügbar.
- Der Dateiverlauf muss aktiviert sein.

Wenn ein solcher Dump-Vorgang abgebrochen und in einem neu startbaren Zustand belassen wird, werden die zugehörigen Snapshots gesperrt. Diese Snapshots werden freigegeben, nachdem der Backup-Kontext gelöscht wurde. Sie können die Liste der Backup-Kontexte mit dem `vserver services ndmp restartable backup show` Befehl anzeigen.

```
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::>"
```

So funktioniert eine Dump-Wiederherstellung mit ONTAP NDMP

Eine Dump-Wiederherstellung schreibt mithilfe eines vordefinierten Prozesses File-Systemdaten von Band auf Festplatte.

Der Prozess in der folgenden Tabelle zeigt, wie die Dump-Wiederherstellung 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 setzt die Berechtigungen (einschließlich ACLs) darauf.
4	ONTAP wiederholt die Stufen 2 und 3, bis alle angegebenen Dateien vom Band kopiert werden.

Datentypen, die von der Dump-Engine wiederhergestellt werden

Bei einem Ausfall oder einer Controller-Unterbrechung bietet die Dump Engine verschiedene Methoden für Sie, um alle von Ihnen gesicherten Daten wiederherzustellen – von einzelnen Dateien über Dateiattribute bis hin zu ganzen Verzeichnissen. Wenn man weiß, welche Datentypen vom Dump Engine wiederhergestellt werden können und wann welche Recovery-Methode verwendet werden kann, kann dies zur Minimierung der Ausfallzeiten beitragen.

Sie können Daten einer Online-zugeordneten LUN wiederherstellen. Host-Applikationen können jedoch erst dann auf diese LUN zugreifen, wenn der Wiederherstellungsvorgang abgeschlossen ist. Nach Abschluss des Restore-Vorgangs sollte der Host-Cache der LUN-Daten gespeichert werden, um die Kohärenz mit den wiederhergestellten Daten zu gewährleisten.

Die Dump-Engine kann die folgenden Daten wiederherstellen:

- Inhalt von Dateien und Verzeichnissen
- UNIX-Dateiberechtigungen
- ACLs

  Wenn Sie eine Datei wiederherstellen, die nur UNIX-Dateiberechtigungen auf einen NTFS-qtree oder Datenträger hat, hat die Datei keine Windows NT-ACLs. Das Speichersystem verwendet nur die UNIX-Dateiberechtigungen auf dieser Datei, bis Sie eine Windows NT-ACL darauf erstellen.

  > Wenn Sie gesicherte ACLs von Storage-Systemen mit Data ONTAP 8.2 auf Storage-Systeme mit Data ONTAP 8.1.x und früher wiederherstellen, die ein ACE-Limit unter 1,024 haben, wird eine Standard-ACL wiederhergestellt.

- Qtree Informationen

  Qtree-Informationen werden nur verwendet, wenn ein qtree im Root-Verzeichnis eines Volume wiederhergestellt wird. Qtree-Informationen werden nicht verwendet, wenn ein qtree in einem niedrigeren Verzeichnis wiederhergestellt wird, `/vs1/vol1/subdir/lowerdir` z. B., und es hört auf, ein qtree zu sein.

- Alle anderen Datei- und Verzeichnisattribute
- Windows NT-Streams
- LUNs
  - Eine LUN muss auf Volume-Ebene oder qtree Ebene wiederhergestellt werden, damit sie als LUN

bleibt.

Wenn es in einem Verzeichnis wiederhergestellt wird, wird es als Datei wiederhergestellt, da es keine gültigen Metadaten enthält.

- Eine 7-Mode LUN wird als LUN auf einem ONTAP Volume wiederhergestellt.

- Ein 7-Mode Volume kann auf einem ONTAP Volume wiederhergestellt werden.
- VM-bezogene Dateien, die auf einem Ziel-Volume wiederhergestellt werden, übernehmen die VM-Ausrichten-Eigenschaften des Ziel-Volume.
- Auf dem Ziel-Volume für einen Wiederherstellungsvorgang sind möglicherweise Dateien mit obligatorischen oder beratenden Sperren vorhanden.

  Während eines Wiederherstellungsvorgangs auf einem solchen Ziel-Volume, ignoriert die Dump-Engine diese Sperren.

Überlegungen vor der Wiederherstellung von Daten mit ONTAP NDMP

Sie können gesicherte Daten auf ihrem ursprünglichen Pfad oder auf einem anderen Ziel wiederherstellen. Wenn Sie gesicherte Daten auf ein anderes Ziel wiederherstellen, müssen Sie das Ziel für die Wiederherstellung vorbereiten.

Bevor Sie Daten entweder in ihren ursprünglichen Pfad oder zu einem anderen Ziel wiederherstellen, müssen Sie über die folgenden Informationen verfügen und die folgenden Anforderungen erfüllen:

- Stufe der Wiederherstellung
- Der Pfad, auf den Sie die Daten wiederherstellen
- Der Blockierungsfaktor, der während des Backups verwendet wird
- Bei einem inkrementellen Restore müssen sich alle Tapes in der Backup-Kette befinden
- Ein Bandlaufwerk, das verfügbar ist und mit dem Band kompatibel ist, von dem wiederhergestellt werden soll

Bevor Sie Daten auf ein anderes Ziel wiederherstellen, müssen Sie die folgenden Vorgänge ausführen:

- Wenn Sie ein Volume wiederherstellen, müssen Sie ein neues Volume erstellen.
- Wenn Sie einen qtree oder ein Verzeichnis wiederherstellen, müssen Sie Dateien umbenennen oder verschieben, deren Namen wahrscheinlich die gleichen Dateien haben wie die von Ihnen wiederherzustellende Dateien.

> In ONTAP 9 unterstützen qtree-Namen das Unicode-Format. Die früheren Versionen von ONTAP unterstützen dieses Format nicht. Wird ein qtree mit Unicode-Namen in ONTAP 9 mithilfe des `ndmpcopy` Befehls oder durch Wiederherstellung von einem Backup Image auf einem Band in ein früheres Release von ONTAP kopiert, wird der qtree als reguläres Verzeichnis und nicht als qtree mit Unicode-Format wiederhergestellt.

> Wenn eine wiederhergestellte Datei denselben Namen hat wie eine vorhandene Datei, 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, müssen Sie die Umgebungsvariable EXTRAHIEREN auf einstellen `E`.

Erforderlicher Speicherplatz auf dem Ziel-Storage-System

Sie benötigen ca. 100 MB mehr Speicherplatz auf dem Ziel-Speichersystem als die wiederherzustellende Datenmenge.

> Der Wiederherstellungsvorgang überprüft beim Start der Wiederherstellung auf Volume-Fläche und Inode-Verfügbarkeit auf dem Ziel-Volume. Wenn die Umgebungsvariable ERZWINGEN auf `Y` aktiviert wird, überspringt der Wiederherstellungsvorgang die Prüfungen für den Volume-Speicherplatz und die Inopodes-Verfügbarkeit auf dem Zielpfad. Falls auf dem Ziel-Volume nicht genügend Volume-Speicherplatz oder Inodes verfügbar sind, stellt der Wiederherstellungsvorgang so viele Daten wieder her, wie vom Ziel-Volume-Speicherplatz und der Inode-Verfügbarkeit zulässig. Der Wiederherstellungsvorgang wird angehalten, wenn kein Volume-Speicherplatz oder Inodes mehr vorhanden ist.

Skalierbarkeitsgrenzen für ONTAP Dump-Sicherungs- und Wiederherstellungssitzungen

Sie müssen die maximale Anzahl von Dump Backup- und Restore-Sessions kennen, die gleichzeitig auf Speichersystemen mit unterschiedlichen Systemspeicherkapazitäten ausgeführt werden können. Diese maximale Zahl hängt vom Systemspeicher eines Storage-Systems ab.

Die in der folgenden Tabelle aufgeführten Grenzwerte gelten für die Dump- oder Wiederherstellungs-Engine. Die in den Skalierbarkeitslimits für NDMP-Sitzungen genannten Grenzwerte gelten für den NDMP-Server, die höher sind als die Engine-Limits.

Systemspeicher eines Storage-Systems	Gesamtzahl der Backup- und Restore-Sessions für Dump
Weniger als 16 GB	4
Größer oder gleich 16 GB, aber kleiner als 24 GB	16
Größer oder gleich 24 GB	32

> Wenn Sie `ndmpcopy` Befehl zum Kopieren von Daten innerhalb von Storage-Systemen verwenden, werden zwei NDMP-Sitzungen eingerichtet: Eine für Dump Backup und die andere für Dump Restore.

Sie können den Systemspeicher Ihres Speichersystems mit dem `sysconfig -a` Befehl (verfügbar über die nodeshell) abrufen. Erfahren Sie mehr über `sysconfig -a` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

Obergrenzen für Skalierbarkeit bei NDMP-Sitzungen

Löschen Sie neustartbare Kontexte, indem Sie den ONTAP SVM-Namen und die Kontext-ID angeben

Wenn Sie ein Backup starten möchten, anstatt einen Kontext neu zu starten, können Sie den Kontext löschen.

Über diese Aufgabe

Sie können mit dem `vserver services ndmp restartable-backup delete` Befehl einen neu startbaren Kontext löschen, indem Sie den SVM-Namen und die Kontext-ID angeben.

Schritte

1. Löschen eines neu startbaren 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::>"
```

So funktioniert der Dump auf einem sekundären ONTAP SnapVault -Volume

Sie können Tape-Backup-Vorgänge für Daten durchführen, die auf dem sekundären SnapVault Volume gespiegelt werden. Sie können nur die auf dem sekundären SnapVault Volume gespiegelten Daten auf Band sichern, nicht jedoch die SnapVault Beziehungs-Metadaten.

Wenn Sie die Datenschutz-Spiegelbeziehung unterbrechen (`snapmirror break`) oder wenn eine SnapMirror-Neusynchronisierung stattfindet, müssen Sie immer ein Basis-Backup durchführen.

Verwandte Informationen

- "Snapmirror-Pause"

Funktionsweise von Dump mit ONTAP -Speicher-Failover und ARL-Vorgängen

Bevor Sie Backup- oder Restore-Vorgänge für Dump durchführen, sollten Sie verstehen,

wie diese Vorgänge mit Storage-Failover (Takeover und Giveback) bzw. ARL (Aggregate Relocation) funktionieren. Die `-override-vetoes` Option bestimmt das Verhalten einer Dump Engine während eines Storage Failover- oder ARL-Vorgangs.

Wenn ein Dump-Backup- oder -Wiederherstellungsvorgang ausgeführt `-override-vetoes false` wird und die Option auf eingestellt ist, wird ein vom Benutzer initiierter Speicher-Failover oder ARL-Vorgang angehalten. Wenn die `-override-vetoes` Option jedoch auf eingestellt ist `true`, wird der Speicher-Failover oder ARL-Vorgang fortgesetzt und der Dump-Backup- oder Wiederherstellungsvorgang abgebrochen. Wenn das Storage-System automatisch ein Storage-Failover oder einen ARL-Vorgang initiiert, wird immer ein aktiver Dump-Backup oder -Restore-Vorgang abgebrochen. Sie können Backup- und Restore-Vorgänge nicht neu starten, selbst wenn ein Storage-Failover oder ARL-Vorgänge abgeschlossen sind.

Dump-Vorgänge, wenn CAB-Erweiterung unterstützt wird

Wenn die Backup-Applikation die CAB-Erweiterung unterstützt, können Sie weiterhin inkrementelle Dump-Backup- und Restore-Vorgänge durchführen, ohne Backup-Richtlinien nach einem Storage Failover oder ARL-Vorgang neu zu konfigurieren.

Dump-Vorgänge, wenn CAB-Erweiterung nicht unterstützt wird

Wenn die Backup-Anwendung keine CAB-Erweiterung unterstützt, können Sie weiterhin inkrementelle Dump-Backup- und Wiederherstellungsvorgänge durchführen, wenn Sie die in der Backup-Richtlinie konfigurierte LIF auf den Node migrieren, der das Zielaggregat hostet. Anderenfalls müssen Sie nach dem Storage-Failover und dem ARL-Betrieb ein Basis-Backup durchführen, bevor Sie das inkrementelle Backup durchführen.

> Für Storage-Failover-Vorgänge muss die in der Backup-Richtlinie konfigurierte LIF auf den Partner-Node migriert werden.

Verwandte Informationen

"Hochverfügbarkeit"

So funktioniert der Dump mit der ONTAP -Volume-Verschiebung

Tape-Backup- und Restore-Vorgänge sowie Volume-Verschiebung können parallel ausgeführt werden, bis die letzte Umstellungsphase vom Storage-System versucht wird. Nach dieser Phase sind neue Backup- und Restore-Vorgänge auf Tape auf dem zu verschiebenden Volume nicht zulässig. Die aktuellen Vorgänge werden jedoch bis zum Abschluss fortgesetzt.

In der folgenden Tabelle wird das Verhalten von Tape-Backup- und Restore-Vorgängen nach dem Verschieben eines Volumes beschrieben:

Wenn Sie Tape-Backup- und Restore-Vorgänge im ausführen…	Dann…
Der NDMP-Modus im Umfang der Storage Virtual Machine (SVM) wird bereitgestellt, wenn die CAB-Erweiterung von der Backup-Applikation unterstützt wird	Sie können weiterhin inkrementelle Backup- und Restore-Vorgänge auf Lese-/Schreib- und schreibgeschützten Volumes durchführen, ohne die Backup-Richtlinien neu zu konfigurieren.

Wenn Sie Tape-Backup- und Restore-Vorgänge im ausführen…	Dann…
SVM-Scoped NDMP-Modus, wenn CAB-Erweiterung nicht von der Backup-Applikation unterstützt wird	Sie können weiterhin inkrementelle Tape-Backups und Restore-Vorgänge bei Lese-/Schreib- und schreibgeschützten Volumes durchführen, wenn Sie die in der Backup-Richtlinie konfigurierte LIF auf den Node migrieren, der das Zielaggregat hostet. Andernfalls müssen Sie nach der Verschiebung eines Volumes ein Basis-Backup durchführen, bevor Sie den inkrementellen Backup-Vorgang durchführen.

Wenn das Volume, das zu einer anderen SVM auf dem Ziel-Node gehört, denselben Namen wie das verschobene Volume hat, können Sie bei der Verschiebung keine inkrementellen Backup-Vorgänge durchführen.

So funktioniert der Dump, wenn ein ONTAP FlexVol volume voll ist

Bevor Sie eine inkrementelle Dump-Sicherungsoperation durchführen, müssen Sie sicherstellen, dass genügend freier Speicherplatz im FlexVol-Volume vorhanden ist.

Wenn der Vorgang fehlschlägt, müssen Sie den freien Speicherplatz im Flex-Vol-Volume erhöhen, indem Sie entweder seine Größe erhöhen oder die Snapshots löschen. Dann führen Sie den inkrementellen Backup-Vorgang erneut aus.

Funktionsweise des Dumps bei Änderung des Zugriffstyps eines ONTAP Volumes

Wenn in einem SnapMirror Ziel-Volume oder einem sekundären SnapVault-Volume der Status von Lese-/Schreibzugriff auf schreibgeschützt oder vom schreibgeschützten Volume zu Lese-/Schreibzugriff geändert wird, müssen Sie ein Basis-Backup oder einen Restore-Vorgang durchführen.

SnapMirror Ziel und sekundäre SnapVault Volumes sind schreibgeschützte Volumes. Wenn Sie Tape-Backup- und Restore-Vorgänge für solche Volumes durchführen, müssen Sie einen Basis-Backup- oder Wiederherstellungsvorgang durchführen, wenn sich der Status des Volumes von schreibgeschützt auf Lesen/Schreiben oder vom Lesen/Schreiben auf schreibgeschützt ändert.

So funktioniert der Dump mit einer ONTAP SnapMirror Einzeldatei oder LUN-Wiederherstellung

Bevor Sie Dump-Backup oder -Restore-Vorgänge auf einem Volume ausführen, auf das eine einzelne Datei oder LUN mithilfe der SnapMirror Technologie wiederhergestellt wird, müssen Sie verstehen, wie Dump-Vorgänge mit einer einzelnen Datei oder einer LUN-Wiederherstellung funktionieren.

Bei einer einzelnen SnapMirror Datei oder einem LUN-Restore sind die Client-I/O-Vorgänge auf die Datei oder das wiederherzustellende LUN beschränkt. Sobald die Wiederherstellung einer einzelnen Datei oder eines LUN abgeschlossen ist, wird die I/O-Einschränkung für die Datei oder LUN entfernt. Wenn ein Dump-Backup auf einem Volume ausgeführt wird, auf das eine einzelne Datei oder eine LUN wiederhergestellt wird, dann ist die Datei oder die LUN, die die Client-I/O-Einschränkung aufweist, nicht in das Dump-Backup enthalten. Bei einem nachfolgenden Backup-Vorgang wird diese Datei oder dieses LUN nach dem Entfernen der I/O-Einschränkung auf Tape gesichert.

Sie können keine Dump-Wiederherstellung und keine SnapMirror-Wiederherstellung gleichzeitig auf demselben Volume durchführen.

Auswirkungen von Dump-Backup- und Wiederherstellungsvorgängen in einer ONTAP MetroCluster -Konfiguration

Bevor Sie in einer MetroCluster Konfiguration Dump-Backup- und Restore-Vorgänge durchführen, müssen Sie verstehen, wie Dump-Vorgänge beim Switchover oder Switchback beeinträchtigt werden.

Dump-Backup oder Restore-Vorgang gefolgt von Switchover

Ziehen Sie zwei Cluster in Betracht: Cluster 1 und Cluster 2. Wenn während eines Backup-Dump oder einer Wiederherstellung von Cluster 1 ein Switchover von Cluster 1 zu Cluster 2 initiiert wird, erfolgt Folgendes:

- Wenn der Wert der `override-vetoes` Option `false` , ist, wird die Umschaltung abgebrochen und der Sicherungs- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option `true` , ist, wird der Dump-Backup- oder Wiederherstellungsvorgang abgebrochen und die Umschaltung wird fortgesetzt.

Dump-Backup- oder Restore-Vorgang, gefolgt von einem Wechsel zurück

Eine Umschaltung wird von Cluster 1 auf Cluster 2 durchgeführt. Auf Cluster 2 wird ein Backup- oder Restore-Vorgang für Dump gestartet. Der Speicherabdump-Vorgang sichert ein auf Cluster 2 gelegenes Volume oder stellt es wieder her. Wenn an diesem Punkt ein Switchback von Cluster 2 auf Cluster 1 initiiert wird, erfolgt Folgendes:

- Wenn der Wert der `override-vetoes` Option `false` , dann wird der Switchback abgebrochen und der Sicherungs- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option `true` , dann wird der Sicherungs- oder Wiederherstellungsvorgang abgebrochen und der Switchback wird fortgesetzt.

Während eines Switchover oder einer Switchover-Funktion für den Backup- oder Restore-Vorgang gestartet

Wenn während einer Umschaltung von Cluster 1 auf Cluster 2 ein Backup- oder Restore-Vorgang für Dump auf Cluster 1 gestartet wird, schlägt der Backup- oder Restore-Vorgang fehl und die Umschaltung wird fortgesetzt.

Wenn während eines Umschalttasters von Cluster 2 auf Cluster 1 ein Dump-Backup oder Restore-Vorgang vom Cluster 2 initiiert wird, schlägt der Backup- oder Restore-Vorgang fehl und der Switchback wird fortgesetzt.

Über SMTape Engine für FlexVol Volumes

Erfahren Sie mehr über die ONTAP SMTape-Engine für FlexVol -Volumes

SMTape ist eine Disaster Recovery-Lösung von ONTAP, die Datenblöcke auf Tape sichert. Mit SMTape können Volume-Backups auf Tapes durchgeführt werden. Sie können jedoch keine Sicherung auf qtree- oder Subbaum-Ebene durchführen. SMTape unterstützt Basis-, Differenzial- und inkrementelle Backups. SMTape benötigt keine Lizenz.

Sie können eine Backup- und Restore-Operation mit SMTape über eine NDMP-kompatible Backup-Applikation durchführen. Sie können SMTape auswählen, um Backup- und Restore-Vorgänge nur im NDMP-Modus mit dem Umfang der Storage Virtual Machine (SVM) durchzuführen.

> Der Reversionsvorgang wird nicht unterstützt, wenn eine SMTape-Backup- oder Wiederherstellungssitzung läuft. Sie müssen warten, bis die Sitzung beendet ist, oder Sie müssen die NDMP-Sitzung abbrechen.

Mit SMTape können Sie 255 Snapshots sichern. Für nachfolgende Basis-, inkrementelle oder differenzielle Backups müssen Sie ältere gesicherte Snapshots löschen.

Vor einer Basis-Wiederherstellung muss das Volume, auf dem Daten wiederhergestellt werden, vom Typ sein `DP` und dieses Volume muss sich im eingeschränkten Zustand befinden. Nach einem erfolgreichen Restore wird dieses Volume automatisch online geschaltet. Sie können nachfolgende inkrementelle oder differenzielle Wiederherstellungen auf diesem Volume in der Reihenfolge durchführen, in der die Backups durchgeführt wurden.

Erfahren Sie mehr über die Verwendung von ONTAP -Snapshots während der SMTape-Sicherung

Sie sollten verstehen, wie Snapshots während eines SMTape Basis-Backups und eines inkrementellen Backups verwendet werden. Bedenken Sie auch bei der Durchführung eines Backups mit SMTape.

Basis-Backup

Während eines Basis-Backups können Sie den Namen des auf Tape zu sichernden Snapshots angeben. Wenn kein Snapshot angegeben wird, wird je nach Zugriffstyp des Volumes (Lese-/Schreibzugriff oder schreibgeschützt) entweder automatisch ein Snapshot erstellt oder vorhandene Snapshots verwendet. Wenn Sie einen Snapshot für das Backup angeben, werden alle Snapshots, die älter als der angegebene Snapshot sind, ebenfalls auf Band gesichert.

Wenn Sie keinen Snapshot für das Backup angeben, geschieht Folgendes:

- Für ein Lese-/Schreibvolume wird automatisch ein Snapshot erstellt.

  Der neu erstellte Snapshot und alle älteren Snapshots werden auf Band gesichert.

- Bei einem schreibgeschützten Volume werden alle Snapshots, einschließlich des neuesten Snapshots, auf Band gesichert.

  Neue Snapshots, die nach dem Start der Sicherung erstellt wurden, werden nicht gesichert.

Inkrementelles Backup

Für inkrementelle oder differenzielle Backup-Vorgänge von SMTape erstellen und verwalten die NDMP-konformen Backup-Anwendungen die Snapshots.

Sie müssen während eines inkrementellen Backup-Vorgangs immer einen Snapshot angeben. Für einen erfolgreichen inkrementellen Backup-Vorgang muss sich der während des vorherigen Backup-Vorgangs (Basis- oder inkrementell) gesicherte Snapshot auf dem Volume befinden, von dem aus das Backup durchgeführt wird. Um sicherzustellen, dass Sie diesen gesicherten Snapshot verwenden, müssen Sie die Snapshot-Richtlinie berücksichtigen, die auf diesem Volume zugewiesen ist, während Sie die Backup-Richtlinie konfigurieren.

Überlegungen zu SMTape Backups auf SnapMirror Zielen

- Eine Datensicherungsspiegelungsbeziehung erstellt temporäre Snapshots auf dem Ziel-Volume für die Replizierung.

  Sie sollten diese Snapshots nicht für SMTape Backups verwenden.

- Wenn während eines SMTape Backups auf demselben Volume eine SnapMirror-Aktualisierung auf einem Ziel-Volume in einer Datensicherungsmirror-Beziehung stattfindet, darf der von SMTape gesicherte Snapshot nicht auf dem Quell-Volume gelöscht werden.

  Während des Backup-Vorgangs sperrt SMTape den Snapshot auf dem Ziel-Volume, und wenn der entsprechende Snapshot auf dem Quell-Volume gelöscht wird, schlägt die nachfolgende SnapMirror-Aktualisierung fehl.

- Sie sollten diese Snapshots nicht während der inkrementellen Sicherung verwenden.

SMTape-Funktionen zur Optimierung von ONTAP -Bandsicherungs- und -wiederherstellungsvorgängen

SMTape-Funktionen wie Backup von Snapshots, inkrementelle und differenzielle Backups, Erhalt von Deduplizierungs- und Komprimierungsfunktionen auf wiederhergestellten Volumes und Tape-Seeding helfen Ihnen bei der Optimierung Ihrer Tape-Backup- und -Restore-Vorgänge.

SMTape bietet die folgenden Funktionen:

- Bietet eine Disaster Recovery-Lösung
- Ermöglicht inkrementelle und differenzielle Backups
- Sichert Snapshots
- Ermöglicht Backups und Restores deduplizierter Volumes und erhält die Deduplizierung auf den wiederhergestellten Volumes aufrecht
- Sichert komprimierte Volumes und erhält die Komprimierung auf den wiederhergestellten Volumes aufrecht
- Ermöglicht das Tape Seeding

SMTape unterstützt den Blockierfaktor in Vielfachen von 4 KB im Bereich von 4 KB bis 256 KB.

Sie können Daten auf Volumes wiederherstellen, die nur in bis zu zwei aufeinanderfolgenden ONTAP Versionen erstellt wurden.

ONTAP -Skalierbarkeitsgrenzen für SMTape-Sicherungs- und Wiederherstellungssitzungen

Bei Backup- und Restore-Vorgängen mit SMTape über NDMP oder CLI (Tape Seeding) müssen Sie jedoch die maximale Anzahl von SMTape Backup- und Restore-Sessions kennen, die gleichzeitig auf Storage-Systemen mit unterschiedlichen Systemspeicherkapazitäten ausgeführt werden können. Diese maximale Zahl hängt vom Systemspeicher eines Storage-Systems ab.

Einschränkungen bei SMTape-Backup- und Restore-Sessions unterscheiden sich von Einschränkungen durch NDMP-Sitzungsgrenzen und Einschränkungen bei Dump-Sitzungen.

Systemarbeitsspeicher des Storage-Systems	Gesamtzahl der SMTape Backup- und Restore-Sessions
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 mit dem `sysconfig -a` Befehl (verfügbar über die nodeshell) abrufen. Erfahren Sie mehr über `sysconfig -a` in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- Obergrenzen für Skalierbarkeit bei NDMP-Sitzungen
- Skalierbarkeitsgrenzen für Dump Backup und Restore-Sessions

Erfahren Sie mehr über ONTAP Tape Seeding

Bei der Tape Seeding handelt es sich um eine SMTape-Funktionalität, mit der Sie ein FlexVol Ziel-Volume in einer Datensicherungs-Spiegelbeziehung initialisieren können.

Mit Tape Seeding können Sie eine Datensicherungs-Spiegelbeziehung zwischen einem Quellsystem und einem Zielsystem über eine Verbindung mit niedriger Bandbreite herstellen.

Die inkrementelle Spiegelung von Snapshots von der Quelle zum Ziel ist über eine Verbindung mit niedriger Bandbreite möglich. Eine erste Spiegelung des Basis-Snapshots dauert jedoch über eine Verbindung mit niedriger Bandbreite lange. In solchen Fällen können Sie ein SMTape Backup des Quell-Volumes auf ein Band durchführen und den ersten Basis-Snapshot mithilfe des Tapes auf das Ziel übertragen. Anschließend können Sie über die Verbindung mit niedriger Bandbreite inkrementelle SnapMirror Updates auf das Zielsystem einrichten.

Funktionsweise von SMTape mit ONTAP -Speicher-Failover und ARL-Vorgängen

Bevor Sie SMTape Backup- oder Restore-Vorgänge durchführen, sollten Sie verstehen, wie diese Vorgänge mit Storage Failover (Übernahme und Rückgabe) oder ARL (Aggregate Relocation) funktionieren. Die `-override-vetoes` Option bestimmt das Verhalten der SMTape Engine während eines Storage Failover oder ARL-Vorgangs.

Wenn ein SMTape-Backup- oder -Wiederherstellungsvorgang ausgeführt `-override-vetoes` wird und die Option auf eingestellt `false` ist, wird ein benutzerinitiierter Speicher-Failover- oder ARL-Vorgang angehalten und der Sicherungs- oder Wiederherstellungsvorgang abgeschlossen. Wenn die Backup-Applikation CAB-Erweiterung unterstützt, können Sie mit inkrementellen Backup- und Restore-Vorgängen bei SMTape fortfahren, ohne Backup-Richtlinien neu zu konfigurieren. Wenn die `-override-vetoes` Option jedoch auf eingestellt ist `true`, wird das Speicher-Failover oder der ARL-Vorgang fortgesetzt und der SMTape-Backup- oder Wiederherstellungsvorgang abgebrochen.

Verwandte Informationen

"Netzwerkmanagement"

"Hochverfügbarkeit"

So funktioniert SMTape mit ONTAP -Volume-Verschiebung

Backup-Vorgänge von SMTape und Volume-Verschiebung können parallel ausgeführt werden, bis das Storage-System eine letzte Umstellungsphase versucht. Nach dieser Phase können neue SMTape Backup-Vorgänge auf dem zu verschiebenden Volume nicht ausgeführt werden. Die aktuellen Vorgänge werden jedoch bis zum Abschluss fortgesetzt.

Bevor die Umstellungsphase für ein Volume gestartet wird, wird während der Volume-Ververschiebt auf aktive SMTape Backup-Vorgänge auf demselben Volume überprüft. Wenn SMTape Backup-Vorgänge aktiv sind, wird die Verschiebung des Volumes in einen verzögerten Zustand verschoben und die Ausführung von SMTape Backup-Vorgängen ermöglicht. Nach Abschluss dieser Backup-Vorgänge müssen Sie die Volume-Verschiebung manuell neu starten.

Wenn die Backup-Anwendung CAB-Erweiterung unterstützt, können Sie weiterhin inkrementelle Tape-Backup- und Wiederherstellungsvorgänge für Lese-/Schreib- und schreibgeschützte Volumes durchführen, ohne Backup-Richtlinien neu zu konfigurieren.

Basis-Restore und Volume-Verschiebung sind nicht gleichzeitig möglich. Allerdings kann parallel zu Volume-Ververschiebungsvorgängen ein inkrementeller Restore durchgeführt werden, wobei das Verhalten wie bei SMTape Backup-Vorgängen während Volume-Ververschiebungsvorgänge ähnlich ist.

Funktionsweise von SMTape mit ONTAP Volume-Rehosting-Vorgängen

SMTape-Vorgänge können nicht gestartet werden, wenn auf einem Volume ein Rehosting durchgeführt wird. Wenn ein Volume an einer Rehosting eines Volumes beteiligt ist, sollten SMTape-Sitzungen nicht auf diesem Volume gestartet werden.

Wenn gerade ein Rehosting eines Volumes ausgeführt wird, schlägt das Backup oder die Wiederherstellung von SMTape fehl. Wenn ein Backup oder eine Wiederherstellung mit SMTape ausgeführt wird, schlägt das erneute Host von Volumes mit einer entsprechenden Fehlermeldung fehl. Dies gilt sowohl für NDMP- als auch für CLI-basierte Backup- oder Restore-Vorgänge.

Auswirkungen auf eine ONTAP NDMP-Sicherungsrichtlinie während ADB

Wenn der automatische Daten-Balancer (ADB) aktiviert ist, analysiert der Balancer die Nutzungsstatistiken von Aggregaten, um das Aggregat zu identifizieren, das den konfigurierten prozentualen Anteil der hohen Schwellenwertnutzung überschritten hat.

Nach der Identifizierung des Aggregats, das den Schwellenwert überschritten hat, identifiziert der Balancer ein Volume, das zu Aggregaten verschoben werden kann, die sich in einem anderen Node im Cluster befinden, und versucht, das Volume zu verschieben. Diese Situation wirkt sich auf die für dieses Volume konfigurierte Backup-Richtlinie aus, da die Datenmanagement-Applikation (DMA) keine CAB-Lösung erkennt, dann muss der Benutzer die Backup-Richtlinie neu konfigurieren und den Baseline-Backup-Vorgang ausführen.

Wenn der DMA CAB-fähig ist und die Backup-Richtlinie über eine bestimmte Schnittstelle konfiguriert wurde, ist die ADB davon nicht betroffen.

Auswirkungen auf SMTape-Sicherungs- und Wiederherstellungsvorgänge in ONTAP MetroCluster -Konfigurationen

Bevor Sie in einer MetroCluster Konfiguration SMTape Backup- und Restore-Vorgänge durchführen, müssen Sie verstehen, wie sich SMTape-Vorgänge bei einem Switchover- oder Switchback-Vorgang auswirken.

Backup- oder Restore-Vorgänge bei SMTape gefolgt von Switchover

Ziehen Sie zwei Cluster in Betracht: Cluster 1 und Cluster 2. Wenn während eines SMTape Backups oder Wiederherstellungsvorgangs auf Cluster 1 eine Umschaltung von Cluster 1 auf Cluster 2 initiiert wird, geschieht Folgendes:

- Wenn der Wert der `-override-vetoes` Option `false` , ist, wird die Umschaltung abgebrochen und der Sicherungs- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option ist `true`, dann wird der SMTape-Backup- oder Wiederherstellungsvorgang abgebrochen und der Umschaltvorgang wird fortgesetzt.

SMTape-Backup- oder Restore-Vorgang und anschließend Wechsel zurück

Eine Umschaltung wird von Cluster 1 auf Cluster 2 durchgeführt und ein SMTape Backup- oder Restore-Vorgang wird auf Cluster 2 initiiert. Der SMTape Vorgang sichert ein auf Cluster 2 gelegenes Volume oder stellt es wieder her. Wenn an diesem Punkt ein Switchback von Cluster 2 auf Cluster 1 initiiert wird, erfolgt Folgendes:

- Wenn der Wert der `-override-vetoes` Option `false` , dann wird der Switchback-Vorgang abgebrochen und der Backup- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option `true` , dann wird der Sicherungs- oder Wiederherstellungsvorgang abgebrochen und der Switchback-Prozess wird fortgesetzt.

SMTape-Backup- oder Restore-Vorgang während eines Switchover oder Switchover-Switch initiiert

Wenn während eines Umschalungsprozesses von Cluster 1 auf Cluster 2 ein SMTape Backup- oder Restore-Vorgang für Cluster 1 initiiert wird, schlägt der Backup- oder Restore-Vorgang fehl und die Umschaltung wird fortgesetzt.

Wenn während eines Switch-Back-Prozesses von Cluster 2 zu Cluster 1 ein SMTape Backup- oder Restore-Vorgang vom Cluster 2 initiiert wird, schlägt der Backup- oder Restore-Vorgang fehl und der Switchback wird fortgesetzt.

Überwachen von Tape-Backup- und Restore-Vorgängen für FlexVol Volumes

Überwachen Sie ONTAP -Bandsicherungs- und Wiederherstellungsvorgänge für FlexVol -Volumes

Sie können die Ereignisprotokolldateien anzeigen, um die Tape-Backup- und Restore-Vorgänge zu überwachen. ONTAP protokolliert automatisch wichtige Backup- und Restore-Ereignisse und die Zeit, zu der sie in einer Protokolldatei mit dem Namen `backup` im `/etc/log/` Verzeichnis des Controllers auftreten. Standardmäßig ist die Ereignisprotokollierung auf eingestellt `on`.

Die Ereignisprotokolldateien können aus folgenden Gründen angezeigt werden:

- Überprüfung, ob ein nächtliches Backup erfolgreich war
- Sammeln von Statistiken zu Backup-Vorgängen
- Zur Verwendung der Informationen in früheren Ereignisprotokolldateien, um bei der Diagnose von Problemen mit Backup- und Restore-Vorgängen zu helfen

Einmal wöchentlich werden die Ereignisprotokolldateien gedreht. Die `/etc/log/backup` Datei wird umbenannt in `/etc/log/backup.0`, die `/etc/log/backup.0` Datei wird umbenannt in `/etc/log/backup.1`, und so weiter. Das System speichert die Protokolldateien für bis zu sechs Wochen; Sie können also bis zu sieben Nachrichtendateien (`/etc/log/backup.[0-5]` und die aktuelle `/etc/log/backup` Datei haben).

Greifen Sie auf die ONTAP Ereignisprotokolldateien für Bandsicherungs- und Wiederherstellungsvorgänge zu

Sie können auf die Ereignisprotokolldateien für Bandsicherungs- und Wiederherstellungsvorgänge im `/etc/log/` Verzeichnis zugreifen `rdfile`, indem Sie den Befehl im nodeshell verwenden. Sie können diese Ereignisprotokolldateien anzeigen, um Tape-Backup- und Restore-Vorgänge zu überwachen.

Über diese Aufgabe

Mit zusätzlichen Konfigurationen, wie einer Zugriffskontrollrolle mit Zugriff auf den `spi` Webdienst oder einem Benutzerkonto, das mit der `http` Zugriffsmethode eingerichtet wurde, können Sie auch einen Webbrowser verwenden, um auf diese Protokolldateien zuzugreifen.

Schritte

1. Geben Sie den folgenden Befehl ein, um auf den nodeshell zuzugreifen:

   `node run -node` *`node_name`*

   `node_name` Ist der Name des Node.

2. Geben Sie den folgenden Befehl ein, um auf die Ereignisprotokolldateien für Backup- und Restore-Vorgänge auf Band zuzugreifen:

   `rdfile /etc/log/backup`

Verwandte Informationen

"Systemadministration"

Das Nachrichtenformat für die Speicherauszug und Wiederherstellung des Ereignisprotokolls lautet

ONTAP Dump- und Wiederherstellungsereignisprotokollnachrichtenformat

Für jedes Dump- und Wiederherstellungsereignis wird eine Meldung in die Backup-Protokolldatei geschrieben.

Das Format der Dump- und Restore-Meldung des Ereignisprotokolls lautet wie folgt:

`type timestamp identifier event (event_info)`

In der folgenden Liste werden die Felder im Meldungsformat des Ereignisprotokolls beschrieben:

- Jede Protokollmeldung beginnt mit einer der in der folgenden Tabelle beschriebenen Typanzeigen:

Typ	Beschreibung
Protokoll	Protokollieren des Ereignisses
dmp	Dump-Ereignis
rst	Ereignis wiederherstellen

- `timestamp` Zeigt das Datum und die Uhrzeit des Ereignisses an.
- Das `identifier` Feld für ein Dump-Ereignis enthält den Dump-Pfad und die eindeutige ID für den Dump. Im `identifier` Feld für ein Wiederherstellungsereignis wird nur der Name des Wiederherstellungspfads als eindeutige Kennung verwendet. Protokollierungsbezogene Ereignismeldungen enthalten kein `identifier` Feld.

Erfahren Sie mehr über ONTAP -Protokollierungsereignisse

Das Ereignisfeld einer Nachricht, die mit einem Protokoll beginnt, gibt den Beginn einer Protokollierung oder das Ende einer Protokollierung an.

Er enthält eines der in der folgenden Tabelle aufgeführten Ereignisse:

Ereignis	Beschreibung
Start_Protokollierung	Zeigt den Beginn der Protokollierung an oder dass die Protokollierung nach der Deaktivierung wieder eingeschaltet wurde.
Stop_Logging	Zeigt an, dass die Protokollierung deaktiviert wurde.

Erfahren Sie mehr über ONTAP Dump-Ereignisse

Das Ereignisfeld für ein Dump-Ereignis enthält einen Ereignistyp, gefolgt von ereignisspezifischen Informationen in Klammern.

In der folgenden Tabelle werden die Ereignisse, ihre Beschreibungen und verwandte Ereignisinformationen beschrieben, die für einen Dump-Vorgang aufgezeichnet werden können:

Ereignis	Beschreibung	Ereignisinformationen
Starten	NDMP Dump wird gestartet	Dump-Ebene und die Art von Dump
Beenden	Speicherabbilder erfolgreich abgeschlossen	Menge der verarbeiteten Daten
Abbrechen	Der Vorgang wird abgebrochen	Menge der verarbeiteten Daten

Ereignis	Beschreibung	Ereignisinformationen
Optionen	Die angegebenen Optionen sind aufgelistet	Alle Optionen und die zugehörigen Werte, einschließlich NDMP-Optionen
Tape_öffnen	Das Band ist für Lese-/Schreibzugriff geöffnet	Der neue Name des Bandgeräts
Tape_close	Das Band ist für Lese-/Schreibzugriff geschlossen	Der Name des Bandgeräts
Phasenänderung	Ein Dump wird in eine neue Verarbeitungsphase eingegeben	Der neue Phasenname
Fehler	In einem Dump ist ein unerwartetes Ereignis aufgetreten	Fehlermeldung
Snapshot	Ein Snapshot wird erstellt oder befindet sich	Name und Uhrzeit des Snapshots
Base_dump	Ein Base Dump-Eintrag in der internen Metadatei wurde gefunden	Level und Zeit des Basis-Dump (nur für inkrementelle Dumps)

Erfahren Sie mehr über ONTAP -Wiederherstellungsereignisse

Das Ereignisfeld für ein Wiederherstellungsereignis enthält einen Ereignistyp, gefolgt von ereignisspezifischen Informationen in Klammern.

Die folgende Tabelle enthält Informationen zu Ereignissen, deren Beschreibungen und den zugehörigen Ereignisinformationen, die für einen Wiederherstellungsvorgang aufgezeichnet werden können:

Ereignis	Beschreibung	Ereignisinformationen
Starten	NDMP-Wiederherstellung wird gestartet	Restore-Ebene und Art der Wiederherstellung
Beenden	Wiederherstellungen erfolgreich abgeschlossen	Anzahl der Dateien und Menge der verarbeiteten Daten
Abbrechen	Der Vorgang wird abgebrochen	Anzahl der Dateien und Menge der verarbeiteten Daten
Optionen	Die angegebenen Optionen sind aufgelistet	Alle Optionen und die zugehörigen Werte, einschließlich NDMP-Optionen
Tape_öffnen	Das Band ist für Lese-/Schreibzugriff geöffnet	Der neue Name des Bandgeräts

Ereignis	Beschreibung	Ereignisinformationen
Tape_close	Das Band ist für Lese-/Schreibzugriff geschlossen	Der Name des Bandgeräts
Phasenänderung	Wiederherstellung wird in eine neue Verarbeitungsphase eingegeben	Der neue Phasenname
Fehler	Wiederherstellung findet ein unerwartetes Ereignis	Fehlermeldung

Aktivieren oder Deaktivieren der Ereignisprotokollierung für ONTAP Bandsicherungs- und -wiederherstellungsvorgänge

Sie können die Ereignisprotokollierung ein- oder ausschalten.

Schritte

1. Geben Sie zum Aktivieren oder Deaktivieren der Ereignisprotokollierung den folgenden Befehl in der Clustershell ein:

   `options -option_name backup.log.enable -option-value {on | off}`

   `on` Aktiviert die Ereignisprotokollierung.

   `off` Deaktiviert die Ereignisprotokollierung.

   Die Ereignisprotokollierung ist standardmäßig aktiviert.

Fehlermeldungen beim Tape Backup und Restore von FlexVol Volumes

Fehlermeldungen sichern und wiederherstellen

Ressourcenbegrenzung: Kein verfügbarer Thread

- **Nachricht**

  `Resource limitation: no available thread`

- **Ursache**

  Die maximale Anzahl der aktiven lokalen I/O-Threads auf Band wird derzeit verwendet. Sie können maximal 16 aktive lokale Bandlaufwerke nutzen.

- **Korrekturmaßnahmen**

  Warten Sie, bis einige Bandjobs abgeschlossen sind, bevor Sie einen neuen Backup- oder Wiederherstellungsauftrag starten.

Die Tape-Reservierung wurde vorweggestellt

- **Nachricht**

  `Tape reservation preempted`

- **Ursache**

  Das Bandlaufwerk wird von einem anderen Vorgang verwendet oder das Band wurde vorzeitig geschlossen.

- **Korrekturmaßnahmen**

  Stellen Sie sicher, dass das Bandlaufwerk nicht von einem anderen Vorgang verwendet wird und dass die DMA-Anwendung den Job nicht abgebrochen hat und versuchen Sie es dann erneut.

Medien konnten nicht initialisiert werden

- **Nachricht**

  `Could not initialize media`

- **Ursache**

  Sie könnten diesen Fehler aus einem der folgenden Gründe bekommen:

  - Das Bandlaufwerk, das für das Backup verwendet wird, ist beschädigt oder beschädigt.
  - Das Band enthält nicht die vollständige Sicherung oder ist beschädigt.
  - Die maximale Anzahl der aktiven lokalen I/O-Threads auf Band wird derzeit verwendet.

    Sie können maximal 16 aktive lokale Bandlaufwerke nutzen.

- **Korrekturmaßnahmen**
  - Wenn das Bandlaufwerk beschädigt oder beschädigt ist, versuchen Sie, den Vorgang mit einem gültigen Bandlaufwerk erneut auszuführen.
  - Wenn das Band nicht das vollständige Backup enthält oder beschädigt ist, können Sie den Wiederherstellungsvorgang nicht ausführen.
  - Wenn keine Bandressourcen verfügbar sind, warten Sie, bis einige Backup- oder Wiederherstellungsaufträge abgeschlossen sind, und wiederholen Sie den Vorgang.

Maximale Anzahl an erlaubten Dumps oder Wiederherstellungen (Maximum Session-Limit) wird ausgeführt

- **Nachricht**

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- **Ursache**

  Die maximale Anzahl von Backup- oder Wiederherstellungsjobs wird bereits ausgeführt.

- **Korrekturmaßnahmen**

Wiederholen Sie den Vorgang, nachdem einige der aktuell ausgeführten Jobs abgeschlossen sind.

Medienfehler beim Schreiben auf Band

- **Nachricht**

  ```
  Media error on tape write
  ```

- **Ursache**

  Das für das Backup verwendete Band ist beschädigt.

- **Korrekturmaßnahmen**

  Ersetzen Sie das Band, und versuchen Sie es erneut.

Bandschreibfehler

- **Nachricht**

  ```
  Tape write failed
  ```

- **Ursache**

  Das für das Backup verwendete Band ist beschädigt.

- **Korrekturmaßnahmen**

  Ersetzen Sie das Band, und versuchen Sie es erneut.

Schreiben auf Band fehlgeschlagen – Fehler beim neuen Band

- **Nachricht**

  ```
  Tape write failed - new tape encountered media error
  ```

- **Ursache**

  Das für das Backup verwendete Band ist beschädigt.

- **Korrekturmaßnahmen**

  Ersetzen Sie das Band, und versuchen Sie es erneut.

Bandschreiben fehlgeschlagen - neues Band ist beschädigt oder schreibgeschützt

- **Nachricht**

  ```
  Tape write failed - new tape is broken or write protected
  ```

- **Ursache**

  Das für das Backup verwendete Band ist beschädigt oder schreibgeschützt.

- **Korrekturmaßnahmen**

  Ersetzen Sie das Band, und versuchen Sie es erneut.

Bandschreiben fehlgeschlagen - neues Band befindet sich bereits am Ende des Mediums

- **Nachricht**

  ```
  Tape write failed - new tape is already at the end of media
  ```

- **Ursache**

  Es ist nicht genügend Speicherplatz auf dem Band vorhanden, um das Backup abzuschließen.

- **Korrekturmaßnahmen**

  Ersetzen Sie das Band, und versuchen Sie es erneut.

Fehler beim Schreiben auf Band

- **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 reicht nicht aus, um die Backup-Daten zu enthalten.

- **Korrekturmaßnahmen**

  Verwenden Sie Bänder mit größerer Kapazität und versuchen Sie den Backup-Job erneut.

Medienfehler auf Band-Lesevorgang

- **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.

- **Korrekturmaßnahmen**

  Wenn Sie sicher sind, dass das Band das vollständige Backup enthält, versuchen Sie den Wiederherstellungsvorgang erneut. Wenn das Band nicht das vollständige Backup enthält, können Sie den Wiederherstellungsvorgang nicht ausführen.

Lesefehler beim Band

- **Nachricht**

  ```
  Tape read error
  ```

- **Ursache**

  Das Bandlaufwerk ist beschädigt, oder das Band enthält nicht die vollständige Sicherung.

- **Korrekturmaßnahmen**

  Wenn das Bandlaufwerk beschädigt ist, verwenden Sie ein anderes Bandlaufwerk. Wenn das Band nicht das vollständige Backup enthält, können Sie die Daten nicht wiederherstellen.

Bereits am Ende des Bandes

- **Nachricht**

  ```
  Already at the end of tape
  ```

- **Ursache**

  Das Band enthält keine Daten oder muss neu aufgewickelt werden.

- **Korrekturmaßnahmen**

  Wenn das Band keine Daten enthält, verwenden Sie das Band, das die Sicherung enthält, und versuchen Sie den Wiederherstellungsauftrag erneut. Andernfalls wird das Band neu gepumst und der Wiederherstellungsauftrag erneut durchgeführt.

Bandaufzeichngröße ist zu klein. Versuchen Sie es mit einer größeren Größe.

- **Nachricht**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Ursache**

  Der für den Wiederherstellungsvorgang angegebene Sperrfaktor ist kleiner als der Blockierungsfaktor, der während des Backups verwendet wurde.

- **Korrekturmaßnahmen**

  Verwenden Sie denselben Sperrfaktor, den Sie während des Backups angegeben haben.

Die Datensatzgröße des Tape sollte Block_size1 und nicht Block_size2 sein

- **Nachricht**

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- **Ursache**

Der für die lokale Wiederherstellung angegebene Sperrfaktor ist falsch.

- **Korrekturmaßnahmen**

  Wiederholen Sie den Wiederherstellungsauftrag mit `block_size1` als Blockierungsfaktor.

Die Größe des Bandauftrags 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 Backup- oder Wiederherstellungsvorgang angegebene Sperrfaktor liegt nicht im zulässigen Bereich.

- **Korrekturmaßnahmen**

  Geben Sie einen Sperrfaktor im Bereich von 4 KB bis 256 KB an.

NDMP-Fehlermeldungen

Fehler bei der Netzwerkkommunikation

- **Nachricht**

  ```
  Network communication error
  ```

- **Ursache**

  Die Kommunikation zu einem Remote-Band in einer NDMP-Dreiwege-Verbindung ist fehlgeschlagen.

- **Korrekturmaßnahmen**

  Überprüfen Sie die Netzwerkverbindung mit dem Remote Mover.

Nachricht von Read Socket: Error_string

- **Nachricht**

  ```
  Message from Read Socket: error_string
  ```

- **Ursache**

  Stellen Sie die Kommunikation von der Remote-Band in der NDMP 3-Wege Verbindung wieder her weist Fehler auf.

- **Korrekturmaßnahmen**

  Überprüfen Sie die Netzwerkverbindung mit dem Remote Mover.

Nachricht von Write Dirnet: Error_string

- **Nachricht**

  ```
  Message from Write Dirnet: error_string
  ```

- **Ursache**

  Die Backup-Kommunikation auf einem Remote Band in einer NDMP-Dreiwege-Verbindung hat einen Fehler.

- **Korrekturmaßnahmen**

  Überprüfen Sie die Netzwerkverbindung mit dem Remote Mover.

Lesen Sie die Buchse, die EOF erhalten hat

- **Nachricht**

  ```
  Read Socket received EOF
  ```

- **Ursache**

  Der Versuch, mit einem Remote-Band in einer NDMP-Verbindung zu kommunizieren, hat das Ende der Dateimarkierung erreicht. Möglicherweise versuchen Sie, eine dreistuseitige Wiederherstellung von einem Backup-Image mit einer größeren Blockgröße durchzuführen.

- **Korrekturmaßnahmen**

  Geben Sie die korrekte Blockgröße an, und versuchen Sie den Wiederherstellungsvorgang erneut.

NDMPD ungültige Versionsnummer: Version_Nummer ``

- **Nachricht**

  ```
  ndmpd invalid version number: version_number
  ```

- **Ursache**

  Die angegebene NDMP-Version wird vom Speichersystem nicht unterstützt.

- **Korrekturmaßnahmen**

  Angabe der NDMP-Version 4.

NDMPD Session Session_ID nicht aktiv

- **Nachricht**

  ```
  ndmpd session session_ID not active
  ```

- **Ursache**

  Die NDMP-Sitzung ist möglicherweise nicht vorhanden.

- **Korrekturmaßnahmen**

  Verwenden Sie den `ndmpd status` Befehl, um die aktiven NDMP-Sitzungen anzuzeigen.

Volume-Ref. Für Volume Volume Volume_Name konnte nicht erhalten werden

- **Nachricht**

  ```
  Could not obtain vol ref for Volume vol_name
  ```

- **Ursache**

  Die Volumenreferenz konnte nicht abgerufen werden, da das Volume möglicherweise von anderen Operationen verwendet wird.

- **Korrekturmaßnahmen**

  Wiederholen Sie den Vorgang später.

Datenverbindungstyp [„NDMP4_ADDR_TCP“ „NDMP4_ADDR_TCP_IPv6“] wird für Steuerverbindungen [„IPv6“ „ IPv4“] nicht unterstützt

- **Nachricht**

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- **Ursache**

  Im Node-Scoped NDMP-Modus muss die etablierte NDMP-Datenverbindung vom gleichen Netzwerkaddress-Typ (IPv4 oder IPv6) wie die NDMP-Steuerverbindung sein.

- **Korrekturmaßnahmen**

  Wenden Sie sich an den Anbieter Ihrer Backup-Applikation.

DATENHÖREN: CAB-Datenverbindung Precondition error

- **Nachricht**

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- **Ursache**

  NDMP-Datenhören schlägt fehl, wenn die Backup-Anwendung die CAB-Erweiterung mit dem NDMP-Server ausgehandelt hat und es im angegebenen NDMP-Datenverbindungsaddress Typ zwischen den NDMP_CAB_DATA_CONN_PREPARE und den NDMP_DATA_LISTEN Nachrichten eine Diskrepanz gibt.

- **Korrekturmaßnahmen**

  Wenden Sie sich an den Anbieter Ihrer Backup-Applikation.

DATENVERBINDUNG: CAB-Datenverbindung Vorbedingung-Fehler vorbereiten

- **Nachricht**

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- **Ursache**

  Die Verbindung zu NDMP-Daten schlägt fehl, wenn die Backup-Anwendung die CAB-Erweiterung mit dem NDMP-Server ausgehandelt hat und es im angegebenen NDMP-Datenverbindungsaddungstyp zwischen den NDMP_CAB_DATA_CONN_PREPARE und den NDMP_DATA_CONNECT Meldungen eine Diskrepanz gibt.

- **Korrekturmaßnahmen**

  Wenden Sie sich an den Anbieter Ihrer Backup-Applikation.

Fehler:Show failed: Kennwort für Benutzer '<username>' kann nicht abgerufen werden

- **Nachricht**

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- **Ursache**

  Unvollständige Benutzerkontenkonfiguration für NDMP

- **Korrekturmaßnahmen**

  Stellen Sie sicher, dass das Benutzerkonto mit der SSH-Zugriffsmethode verknüpft ist und dass die Authentifizierungsmethode das Benutzerpasswort ist.

Dump-Fehlermeldungen

Zielvolume ist schreibgeschützt

- **Nachricht**

  ```
  Destination volume is read-only
  ```

- **Ursache**

  Der Pfad, zu dem der Wiederherstellungsvorgang versucht wird, ist schreibgeschützt.

- **Korrekturmaßnahmen**

  Versuchen Sie, die Daten an einem anderen Speicherort wiederherzustellen.

Ziel-qtree ist schreibgeschützt

- **Nachricht**

  ```
  Destination qtree is read-only
  ```

- **Ursache**

  Der qtree, zu dem die Wiederherstellung versucht wird, ist schreibgeschützt.

- **Korrekturmaßnahmen**

  Versuchen Sie, die Daten an einem anderen Speicherort wiederherzustellen.

Dumps wurde auf dem Volume vorübergehend deaktiviert. Versuchen Sie es erneut

- **Nachricht**

  ```
  Dumps temporarily disabled on volume, try again
  ```

- **Ursache**

  Ein NDMP Dump-Backup wird auf einem SnapMirror-Ziel-Volume versucht `snapmirror break` `snapmirror resync`, das Teil eines oder eines Vorgangs ist.

- **Korrekturmaßnahmen**

  Warten Sie, bis der `snapmirror break` oder `snapmirror resync`-Vorgang abgeschlossen ist, und führen Sie dann den Dump-Vorgang aus.

  > Wenn der Status eines SnapMirror Ziel-Volumes von Lese-/Schreibzugriff auf schreibgeschützt oder von schreibgeschützt auf Schreib-/Lesezugriff wechselt, müssen Sie ein Basis-Backup durchführen.

Verwandte Informationen

- "Snapmirror-Pause"
- "SnapMirror-Neusynchronisierung"

NFS-Labels wurden nicht erkannt

- **Nachricht**

  ```
  Error: Aborting: dump encountered NFS security labels in the file system
  ```

- **Ursache**

  NFS-Sicherheitsetiketten werden ab ONTAP 9.9.1 unterstützt, wenn NFSv4.2 aktiviert ist. NFS-Sicherheitsetiketten werden jedoch derzeit nicht durch das Dump-Engine erkannt. Wenn auf NFS-Sicherheitsetiketten der Dateien, Verzeichnisse oder spezielle Dateien in einem Speicherauszug stößt, schlägt der Dump fehl.

- **Korrekturmaßnahmen**

  Vergewissern Sie sich, dass keine Dateien oder Verzeichnisse über NFS-Sicherheitsetiketten verfügen.

Es wurden keine Dateien erstellt

- **Nachricht**

```
No files were created
```

- **Ursache**

  Ein Verzeichnis DAR wurde versucht, ohne die erweiterte DAR-Funktionalität zu aktivieren.

- **Korrekturmaßnahmen**

  Aktivieren Sie die verbesserte DAR-Funktion, und versuchen Sie es erneut.

Wiederherstellung der Datei <Dateiname> fehlgeschlagen

- **Nachricht**

  ```
  Restore of the file file name failed
  ```

- **Ursache**

  Wenn eine DATEN-DAR (Direct Access Recovery) einer Datei durchgeführt wird, deren Dateiname mit der einer LUN auf dem Ziel-Volume identisch ist, schlägt das DAR fehl.

- **Korrekturmaßnahmen**

  WIEDERHOLEN SIE DAS DAR der Datei.

Die Kürzung für src Inode <Inode number>… ist fehlgeschlagen

- **Nachricht**

  ```
  Truncation failed for src inode <inode number>. Error <error number>. Skipping
  inode.
  ```

- **Ursache**

  Inode einer Datei wird gelöscht, wenn die Datei wiederhergestellt wird.

- **Korrekturmaßnahmen**

  Warten Sie, bis der Wiederherstellungsvorgang auf einem Volume abgeschlossen ist, bevor Sie dieses Volume verwenden.

Ein durch Dump benötigter Snapshot konnte nicht gesperrt werden

- **Nachricht**

  ```
  Unable to lock a snapshot needed by dump
  ```

- **Ursache**

  Der für das Backup angegebene Snapshot ist nicht verfügbar.

- **Korrekturmaßnahmen**

  Wiederholen Sie das Backup mit einem anderen Snapshot.

Mit dem `snap list` Befehl wird eine Liste der verfügbaren Snapshots angezeigt.

Erfahren Sie mehr über `snap list` in der "ONTAP-Befehlsreferenz".

Bitmap-Dateien konnten nicht gefunden werden

- **Nachricht**

  `Unable to locate bitmap files`

- **Ursache**

  Die für den Sicherungsvorgang erforderlichen Bitmap-Dateien wurden möglicherweise gelöscht. In diesem Fall kann das Backup nicht neu gestartet werden.

- **Korrekturmaßnahmen**

  Führen Sie das Backup erneut aus.

Das Volumen befindet sich vorübergehend im Übergangszustand

- **Nachricht**

  `Volume is temporarily in a transitional state`

- **Ursache**

  Das zu sichernde Volume befindet sich vorübergehend in einem nicht abgehängt Status.

- **Korrekturmaßnahmen**

  Warten Sie einige Zeit, und führen Sie die Sicherung erneut aus.

SMTape-Fehlermeldungen

Blöcke sind nicht in der Reihenfolge

- **Nachricht**

  `Chunks out of order`

- **Ursache**

  Die Sicherungsbänder werden nicht in der richtigen Reihenfolge wiederhergestellt.

- **Korrekturmaßnahmen**

  Wiederholen Sie den Wiederherstellungsvorgang, und laden Sie die Bänder in der richtigen Reihenfolge.

Das Chunk-Format wird nicht unterstützt

- **Nachricht**

```
Chunk format not supported
```

- **Ursache**

  Das Backup-Image ist nicht von SMTape.

- **Korrekturmaßnahmen**

  Wenn das Backup-Image nicht von SMTape ist, versuchen Sie den Vorgang mit einem Band, das über das SMTape-Backup verfügt, erneut.

Fehler beim Zuweisen des Arbeitsspeichers

- **Nachricht**

```
Failed to allocate memory
```

- **Ursache**

  Der Arbeitsspeicher des Systems ist nicht mehr verfügbar.

- **Korrekturmaßnahmen**

  Versuchen Sie den Job später erneut, wenn das System nicht zu beschäftigt ist.

Fehler beim Abrufen des Datenpuffer

- **Nachricht**

```
Failed to get data buffer
```

- **Ursache**

  Es wurden nicht mehr Puffer im Storage-System bereitgestellt.

- **Korrekturmaßnahmen**

  Warten Sie, bis einige Storage-Systemvorgänge abgeschlossen sind, und wiederholen Sie den Job.

Der Snapshot konnte nicht gefunden werden

- **Nachricht**

```
Failed to find snapshot
```

- **Ursache**

  Der für das Backup angegebene Snapshot ist nicht verfügbar.

- **Korrekturmaßnahmen**

  Überprüfen Sie, ob der angegebene Snapshot verfügbar ist. Wenn nicht, versuchen Sie es mit dem richtigen Snapshot.

Snapshot konnte nicht erstellt werden

- **Nachricht**

  `Failed to create snapshot`

- **Ursache**

  Das Volume enthält bereits die maximale Anzahl an Snapshots.

- **Korrekturmaßnahmen**

  Löschen Sie einige Snapshots, und versuchen Sie den Sicherungsvorgang erneut.

Snapshot konnte nicht gesperrt werden

- **Nachricht**

  `Failed to lock snapshot`

- **Ursache**

  Der Snapshot wird verwendet oder wurde gelöscht.

- **Korrekturmaßnahmen**

  Wenn der Snapshot von einem anderen Vorgang verwendet wird, warten Sie, bis dieser Vorgang abgeschlossen ist, und wiederholen Sie dann die Sicherung. Wenn der Snapshot gelöscht wurde, können Sie die Sicherung nicht durchführen.

Snapshot konnte nicht gelöscht werden

- **Nachricht**

  `Failed to delete snapshot`

- **Ursache**

  Der automatische Snapshot konnte nicht gelöscht werden, da er von anderen Vorgängen verwendet wird.

- **Korrekturmaßnahmen**

  Verwenden Sie den `snap` Befehl, um den Status des Snapshots zu bestimmen. Wenn der Snapshot nicht benötigt wird, löschen Sie ihn manuell.

Der neueste Snapshot konnte nicht abgerufen werden

- **Nachricht**

  `Failed to get latest snapshot`

- **Ursache**

  Der neueste Snapshot ist möglicherweise nicht vorhanden, da das Volume von SnapMirror initialisiert wird.

- **Korrekturmaßnahmen**

  Versuchen Sie es nach Abschluss der Initialisierung erneut.

Fehler beim Laden des neuen Bandes

- **Nachricht**

  ```
  Failed to load new tape
  ```

- **Ursache**

  Fehler beim Bandlaufwerk oder Datenträger.

- **Korrekturmaßnahmen**

  Tauschen Sie das Band aus, und wiederholen Sie den Vorgang.

Fehler beim Initialisieren des Tapes

- **Nachricht**

  ```
  Failed to initialize tape
  ```

- **Ursache**

  Sie könnten diese Fehlermeldung aus einem der folgenden Gründe erhalten:

  - Das Backup-Image ist nicht von SMTape.
  - Der angegebene Tape-Blockierfaktor ist falsch.
  - Das Band ist beschädigt oder beschädigt.
  - Das falsche Band wird zur Wiederherstellung geladen.

- **Korrekturmaßnahmen**
  - Wenn das Backup-Image nicht von SMTape ist, versuchen Sie den Vorgang mit einem Band mit SMTape-Backup erneut.
  - Wenn der Sperrfaktor nicht korrekt ist, geben Sie den korrekten Sperrfaktor an, und wiederholen Sie den Vorgang.
  - Wenn das Band beschädigt ist, können Sie den Wiederherstellungsvorgang nicht ausführen.
  - Wenn das falsche Band geladen ist, wiederholen Sie den Vorgang mit dem richtigen Band.

Fehler beim Initialisieren des Wiederherstellungsstroms

- **Nachricht**

  ```
  Failed to initialize restore stream
  ```

- **Ursache**

  Sie könnten diese Fehlermeldung aus einem der folgenden Gründe erhalten:

- Das Backup-Image ist nicht von SMTape.
- Der angegebene Tape-Blockierfaktor ist falsch.
- Das Band ist beschädigt oder beschädigt.
- Das falsche Band wird zur Wiederherstellung geladen.

- **Korrekturmaßnahmen**
  - Wenn das Backup-Image nicht von SMTape ist, versuchen Sie den Vorgang mit einem Band, das über das SMTape-Backup verfügt, erneut.
  - Wenn der Sperrfaktor nicht korrekt ist, geben Sie den korrekten Sperrfaktor an, und wiederholen Sie den Vorgang.
  - Wenn das Band beschädigt ist, können Sie den Wiederherstellungsvorgang nicht ausführen.
  - Wenn das falsche Band geladen ist, wiederholen Sie den Vorgang mit dem richtigen Band.

Fehler beim Lesen des Backup-Images

- **Nachricht**

  ```
  Failed to read backup image
  ```

- **Ursache**

  Das Band ist beschädigt.

- **Korrekturmaßnahmen**

  Wenn das Band beschädigt ist, können Sie den Wiederherstellungsvorgang nicht ausführen.

Bildkopf fehlt oder ist beschädigt

- **Nachricht**

  ```
  Image header missing or corrupted
  ```

- **Ursache**

  Das Band enthält kein gültiges SMTape Backup.

- **Korrekturmaßnahmen**

  Versuchen Sie es mit einem Band, das ein gültiges Backup enthält, erneut.

Interne Assertion

- **Nachricht**

  ```
  Internal assertion
  ```

- **Ursache**

  Es liegt ein interner SMTape-Fehler vor.

- **Korrekturmaßnahmen**

  Melden `etc/log/backup` Sie den Fehler, und senden Sie die Datei an den technischen Support.

Ungültige Magic-Nummer für das Backup-Image

- **Nachricht**

  ```
  Invalid backup image magic number
  ```

- **Ursache**

  Das Backup-Image ist nicht von SMTape.

- **Korrekturmaßnahmen**

  Wenn das Backup-Image nicht von SMTape ist, versuchen Sie den Vorgang mit einem Band, das über das SMTape-Backup verfügt, erneut.

Ungültige Prüfsumme für Backup-Images

- **Nachricht**

  ```
  Invalid backup image checksum
  ```

- **Ursache**

  Das Band ist beschädigt.

- **Korrekturmaßnahmen**

  Wenn das Band beschädigt ist, können Sie den Wiederherstellungsvorgang nicht ausführen.

Ungültiges Eingabeband

- **Nachricht**

  ```
  Invalid input tape
  ```

- **Ursache**

  Die Signatur des Backup-Images ist im Bandkopf nicht gültig. Das Band enthält beschädigte Daten oder enthält kein gültiges Backup-Image.

- **Korrekturmaßnahmen**

  Wiederholen Sie den Wiederherstellungsauftrag mit einem gültigen Backup-Image.

Ungültiger Volume-Pfad

- **Nachricht**

  ```
  Invalid volume path
  ```

- **Ursache**

  Das angegebene Volume für den Backup- oder Wiederherstellungsvorgang wurde nicht gefunden.

- **Korrekturmaßnahmen**

  Wiederholen Sie den Job mit einem gültigen Volume-Pfad und einem Volume-Namen.

Diskrepanz bei der Backup-Satz-ID

- **Nachricht**

  ```
  Mismatch in backup set ID
  ```

- **Ursache**

  Das während einer Bandänderung geladene Band ist nicht Teil des Backup-Satzes.

- **Korrekturmaßnahmen**

  Legen Sie das richtige Band ein, und versuchen Sie es erneut.

Nicht übereinstimmende Backup-Zeitstempel

- **Nachricht**

  ```
  Mismatch in backup time stamp
  ```

- **Ursache**

  Das während einer Bandänderung geladene Band ist nicht Teil des Backup-Satzes.

- **Korrekturmaßnahmen**

  ```
  `smtape restore -h`Überprüfen Sie mit dem Befehl die
  Kopfzeileninformationen eines Bandes.
  ```

Job wurde aufgrund des Herunterfahrens abgebrochen

- **Nachricht**

  ```
  Job aborted due to shutdown
  ```

- **Ursache**

  Das Storage-System wird neu gestartet.

- **Korrekturmaßnahmen**

  Versuchen Sie den Job nach dem Neustart des Speichersystems erneut.

Job wurde aufgrund des automatischen Löschvorgangs von Snapshots abgebrochen

- **Nachricht**

  ```
  Job aborted due to snapshot autodelete
  ```

- **Ursache**

  Das Volume verfügt nicht über genügend Speicherplatz und hat das automatische Löschen von Snapshots ausgelöst.

- **Korrekturmaßnahmen**

  Geben Sie Speicherplatz im Volume frei, und versuchen Sie den Job erneut.

Das Tape wird derzeit in anderen Vorgängen verwendet

- **Nachricht**

  ```
  Tape is currently in use by other operations
  ```

- **Ursache**

  Das Bandlaufwerk wird von einem anderen Job verwendet.

- **Korrekturmaßnahmen**

  Versuchen Sie die Sicherung erneut, nachdem der aktuell aktive Job abgeschlossen ist.

Bänder sind nicht in Ordnung

- **Nachricht**

  ```
  Tapes out of order
  ```

- **Ursache**

  Das erste Band der Bandsequenz für den Wiederherstellungsvorgang besitzt nicht den Bildkopf.

- **Korrekturmaßnahmen**

  Legen Sie das Band mit der Bildkopfzeile ein, und versuchen Sie den Job erneut.

Übertragung fehlgeschlagen (abgebrochen wegen MetroCluster-Vorgang)

- **Nachricht**

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- **Ursache**

  Der SMTape-Vorgang wird aufgrund eines Switchover- oder Switchback-Vorgangs abgebrochen.

- **Korrekturmaßnahmen**

Führen Sie den SMTape-Vorgang durch, nachdem der Switchover- oder Switch-Back-Vorgang abgeschlossen ist.

Übertragung fehlgeschlagen (ARL wird abgebrochen)

- **Nachricht**

  ```
  Transfer failed (ARL initiated abort)
  ```

- **Ursache**

  Obwohl gerade ein SMTape-Vorgang ausgeführt wird, wenn eine Aggregatverschiebung initiiert wird, wird der SMTape-Vorgang abgebrochen.

- **Korrekturmaßnahmen**

  Führen Sie den SMTape-Vorgang durch, nachdem die Aggregatverschiebung abgeschlossen ist.

Übertragung fehlgeschlagen (CFO wird abgebrochen)

- **Nachricht**

  ```
  Transfer failed (CFO initiated abort)
  ```

- **Ursache**

  Der SMTape-Vorgang wird abgebrochen, weil ein Storage Failover-Vorgang (Übernahme und Rückgabe) eines CFO-Aggregats durchgeführt wird.

- **Korrekturmaßnahmen**

  Führen Sie den SMTape-Vorgang durch, nachdem das Storage Failover des CFO-Aggregats abgeschlossen ist.

Übertragung fehlgeschlagen (SFO wird abgebrochen)

- **Nachricht**

  ```
  Transfer failed (SFO initiated abort)
  ```

- **Ursache**

  Der SMTape-Vorgang wird abgebrochen, da ein Storage Failover-Vorgang (Übernahme und Rückgabe) durchgeführt wird.

- **Korrekturmaßnahmen**

  Führen Sie den SMTape-Vorgang durch, nachdem der Storage Failover-Vorgang (Übernahme und Rückgabe) abgeschlossen ist.

Zugrunde liegendes Aggregat wird migriert

- **Nachricht**

```
Underlying aggregate under migration
```

- **Ursache**

  Falls ein SMTape-Vorgang auf einem Aggregat initiiert wird, das derzeit migriert wird (Storage Failover oder Aggregatverschiebung), schlägt der SMTape-Vorgang fehl.

- **Korrekturmaßnahmen**

  Führen Sie den SMTape-Vorgang durch, nachdem die Migration des Aggregats abgeschlossen ist.

Volume wird derzeit migriert

- **Nachricht**

  ```
  Volume is currently under migration
  ```

- **Ursache**

  Die Volume-Migration und das SMTape Backup können nicht gleichzeitig ausgeführt werden.

- **Korrekturmaßnahmen**

  Versuchen Sie es erneut, den Backup-Auftrag auszuführen, nachdem die Volume-Migration abgeschlossen ist.

Volume ist offline

- **Nachricht**

  ```
  Volume offline
  ```

- **Ursache**

  Das zu sichernde Volume ist offline.

- **Korrekturmaßnahmen**

  Schalten Sie das Volume online, und versuchen Sie es erneut.

Volume nicht eingeschränkt

- **Nachricht**

  ```
  Volume not restricted
  ```

- **Ursache**

  Das Ziel-Volume, auf das die Daten wiederhergestellt werden, ist nicht beschränkt.

- **Korrekturmaßnahmen**

  Beschränken Sie das Volume, und wiederholen Sie den Wiederherstellungsvorgang.

NDMP-Konfiguration

Erfahren Sie mehr über die ONTAP-NDMP-Konfiguration

ONTAP 9-Cluster können mithilfe des Network Data Management Protocol (NDMP) schnell und einfach konfiguriert werden, um Daten mithilfe einer Backup-Applikation eines Drittanbieters direkt auf Tape zu sichern.

Falls die Backup-Applikation Cluster Aware Backup (CAB) unterstützt, können Sie NDMP als *SVM-Scoped* oder *Node-Scoped* konfigurieren:

- Mit dem SVM-Umfang auf Cluster-Ebene (Admin SVM) können Sie alle Volumes sichern, die auf verschiedenen Nodes des Clusters gehostet werden. SVM-Scoped NDMP wird empfohlen, sofern möglich.
- Mit Node-Scoped NDMP können Sie ein Backup aller auf diesem Node gehosteten Volumes erstellen.

Falls die Backup-Anwendung CAB nicht unterstützt, müssen Sie den Node-Scoped NDMP verwenden.

SVM-Scoped und Node-Scoped NDMP schließen sich gegenseitig aus; sie können nicht auf demselben Cluster konfiguriert werden.

Node-Scoped NDMP ist veraltet in ONTAP 9.

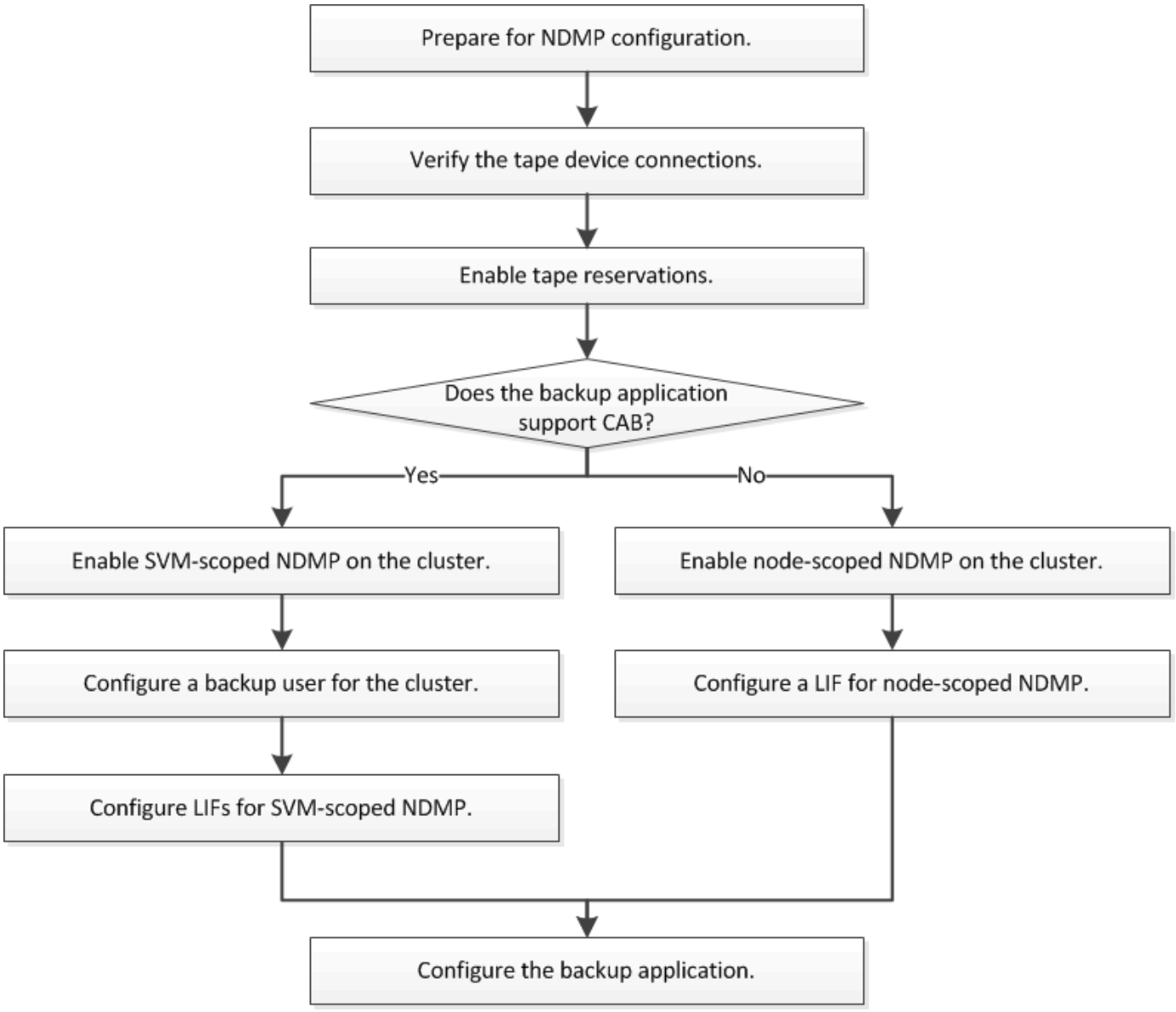
Erfahren Sie mehr über "Cluster-sensibles Backup (CAB)".

Überprüfen Sie vor dem Konfigurieren von NDMP Folgendes:

- Sie verfügen über eine Backup-Applikation eines Drittanbieters (auch als Datenmanagement-Applikation oder DMA bezeichnet).
- Sie sind ein Cluster-Administrator.
- Bandgeräte und ein optionaler Medienserver sind installiert.
- Bandgeräte sind über einen Fibre Channel-Switch (FC) mit dem Cluster verbunden oder lokal verbunden.
- Mindestens ein Bandgerät verfügt über eine Logical Unit Number (LUN) von 0.

Erfahren Sie mehr über den ONTAP NDMP-Konfigurationsworkflow

Die Einrichtung von Tape Backups über NDMP umfasst die Vorbereitung der NDMP-Konfiguration, die Überprüfung der Verbindungen zwischen Tape-Geräten, Aktivierung von Tape-Reservierungen, Konfiguration von NDMP auf SVM- oder Node-Ebene, Aktivierung von NDMP auf dem Cluster, die Konfiguration eines Backup-Benutzers, die Konfiguration von LIFs sowie die Konfiguration der Backup-Applikation.



Vorbereiten von ONTAP NDMP-Konfigurationen

Bevor Sie den Zugriff auf Tape-Backups über das Network Data Management Protocol (NDMP) konfigurieren, müssen Sie überprüfen, ob die geplante Konfiguration unterstützt wird. Vergewissern Sie sich, dass Ihre Bandlaufwerke auf jedem Node als qualifizierte Laufwerke aufgeführt sind. Vergewissern Sie sich, dass alle Nodes über Intercluster LIFs verfügen. Und ermitteln, ob die Backup-Applikation die Cluster-Aware-Backup-Erweiterung (CAB) unterstützt.

Schritte

1. ONTAP-Unterstützung finden Sie in der Kompatibilitätsmatrix des Providers Ihrer Backup-Applikation (NetApp ist nicht als Backup-Applikationen anderer Anbieter mit ONTAP oder NDMP qualifiziert).

   Sie sollten überprüfen, ob die folgenden NetApp Komponenten kompatibel sind:

   - Die Version von ONTAP 9, die auf dem Cluster ausgeführt wird.
   - Anbieter und Version der Backup-Applikation, beispielsweise Veritas NetBackup 8.2 oder CommVault.

- Die Bandgeräte enthalten Details wie Hersteller, Modell und Schnittstelle der Bandlaufwerke, z. B. IBM Ultrium 8 oder HPE StoreEver Ultrium 30750 LTO-8.
- Die Plattformen der Nodes im Cluster, z. B. FAS8700 oder A400.

> Sie finden ältere ONTAP-Kompatibilitätsmatrizen für Backup-Anwendungen in der "NetApp Interoperabilitäts-Matrix-Tool".

2. Vergewissern Sie sich, dass Ihre Bandlaufwerke in der integrierten Tape-Konfigurationsdatei jedes Node als qualifizierte Laufwerke aufgeführt sind:

   a. Zeigen Sie auf der Befehlszeilenschnittstelle die integrierte Tape-Konfigurationsdatei mit dem `storage tape show-supported-status` Befehl an.

```
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 Bandlaufwerke mit der Liste der qualifizierten Laufwerke in der Ausgabe.

> Die Namen der Bandgeräte in der Ausgabe können geringfügig von den Namen auf dem Geräteetikett oder in der Interoperabilitäts-Matrix abweichen. Beispielsweise kann Digital DLT2000 auch als DLT2K bezeichnet werden. Sie können diese geringfügigen Benennungsunterschiede ignorieren.

   c. Wenn ein Gerät in der Ausgabe nicht als qualifiziert aufgeführt wird, obwohl das Gerät gemäß der Interoperabilitäts-Matrix qualifiziert ist, können Sie eine aktualisierte Konfigurationsdatei für das Gerät herunterladen und mithilfe der Anweisungen auf der NetApp Support Site installieren.

      "NetApp Downloads: Konfigurationsdateien für Bandgeräte"

   In der integrierten Bandkonfigurationsdatei wird möglicherweise kein qualifiziertes Gerät aufgeführt, wenn das Bandgerät nach dem Versand des Knotens qualifiziert war.

3. Überprüfen Sie, ob jeder Node im Cluster über eine Intercluster-LIF verfügt:

   a. Über den `network interface show -role intercluster` Befehl können Sie sich die Intercluster LIFs auf den Nodes anzeigen lassen.

```
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
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

b. Wenn auf keinem Node eine Intercluster LIF vorhanden ist, erstellen Sie mithilfe des `network interface create` Befehls eine Intercluster LIF.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
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 -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
```

Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

"Netzwerkmanagement"

4. Ermitteln Sie, ob die Backup-Applikation Cluster-Aware Backup (CAB) unterstützt, indem Sie die mit der Backup-Applikation bereitgestellte Dokumentation verwenden.

   DIE CAB-Unterstützung ist ein entscheidender Faktor bei der Ermittlung der Art der Datensicherung, die Sie durchführen können.

Verwandte Informationen

- "Speicherband-Show"
- "Speicherband zeigt den unterstützten Status an"

Überprüfen Sie die ONTAP NDMP-Bandgeräteverbindungen

Sie müssen sicherstellen, dass alle Laufwerke und Medienwechsler in ONTAP als Geräte sichtbar sind.

Schritte

1. Mit dem `storage tape show` Befehl können Sie Informationen zu allen Laufwerken und Medienwechslern 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 kein Bandlaufwerk angezeigt wird, beheben Sie das Problem.
3. Wenn kein Medienwechsler angezeigt wird, können Sie mit dem `storage tape show-media-changer` Befehl Informationen zu Medienwechslern anzeigen und das Problem beheben.

```
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

- "Speicherband Show-Media-Changer"

Aktivieren Sie Bandreservierungen für ONTAP NDMP-Sicherungsvorgänge

Sie müssen sicherstellen, dass Bandlaufwerke für Backup-Anwendungen für NDMP-Backup-Vorgänge reserviert sind.

Über diese Aufgabe

Die Reservierungseinstellungen variieren in unterschiedlichen Backup-Anwendungen, und diese Einstellungen müssen mit der Backup-Anwendung und den Nodes oder Servern übereinstimmen, die die gleichen Laufwerke verwenden. Die richtigen Reservierungseinstellungen finden Sie in der Anbieterdokumentation der Backup-Anwendung.

Schritte

1. Aktivieren Sie Reservierungen mit dem `options -option-name tape.reservations -option -value persistent` Befehl.

   Mit dem folgenden Befehl werden Reservierungen mit dem `persistent` Wert aktiviert:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Überprüfen Sie mit dem `options tape.reservations` Befehl, ob Reservierungen auf allen Nodes aktiviert sind, und überprüfen Sie dann die Ausgabe.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                persistent

cluster1-2
    tape.reservations                persistent
2 entries were displayed.
```

Konfigurieren Sie SVM-Scoped NDMP

Aktivieren Sie SVM-bezogenes NDMP auf dem ONTAP-Cluster

Wenn der DMA die Erweiterung Cluster-Aware Backup (CAB) unterstützt, können Sie alle Volumes, die auf verschiedenen Nodes in einem Cluster gehostet werden, sichern, indem Sie SVM-Scoped NDMP aktivieren, den NDMP-Service auf dem Cluster aktivieren (admin SVM) und LIFs für die Daten- und Kontrollverbindung konfigurieren.

Bevor Sie beginnen

Die CAB-Erweiterung muss vom DMA unterstützt werden.

Über diese Aufgabe

Durch die Aktivierung des Node-Scoped NDMP-Modus wird der SVM-Scoped NDMP-Modus auf dem Cluster aktiviert.

Schritte

1. NDMP-Modus mit SVM-Umfang aktivieren:

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   Der NDMP-Modus mit SVM-Umfang ist aktiviert.

2. NDMP-Service auf der Admin-SVM aktivieren:

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   Der Authentifizierungstyp ist `challenge` standardmäßig auf festgelegt und die Klartext-Authentifizierung ist deaktiviert.

   Für eine sichere Kommunikation sollten Sie die Klartext-Authentifizierung deaktivieren.

3. Überprüfen Sie, ob der NDMP-Dienst 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-Applikation muss ein administrativer Benutzer mit ausreichenden Berechtigungen und einem NDMP-Passwort eingerichtet werden.

Über diese Aufgabe

Sie müssen ein NDMP-Passwort für Backup-Admin-Benutzer generieren. Sie können Backup-Admin-Benutzer auf Cluster- oder SVM-Ebene aktivieren und bei Bedarf einen neuen Benutzer erstellen. Standardmäßig können sich Benutzer mit den folgenden Rollen beim NDMP-Backup authentifizieren:

- Cluster-weit: `admin` Oder `backup`
- Einzelne SVMs: `vsadmin` Oder `vsadmin-backup`

Wenn Sie einen NIS- oder LDAP-Benutzer verwenden, muss der Benutzer auf dem jeweiligen Server vorhanden sein. Sie können keinen Active Directory-Benutzer verwenden.

Schritte

1. Aktuelle Admin-Benutzer und -Berechtigungen anzeigen:

   ```
   security login show
   ```

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

2. Erstellen Sie bei Bedarf einen neuen NDMP-Backup-Benutzer mit dem `security login create` Befehl und der entsprechenden Rolle für den gesamten Cluster oder einzelne SVM-Privileges.

   Sie können einen lokalen Backup-Benutzernamen oder einen NIS- oder LDAP-Benutzernamen für den `-user-or-group-name` Parameter angeben.

   Mit dem folgenden Befehl wird der Backup-Benutzer `backup_admin1` mit der `backup` Rolle für den gesamten Cluster erstellt:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   Mit dem folgenden Befehl wird der Backup-Benutzer `vsbackup_admin1` mit der `vsadmin-backup` Rolle für eine einzelne SVM erstellt:

   ```
   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.

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

3. Generieren Sie mit dem `vserver services ndmp generate password` Befehl ein Passwort für die Admin-SVM.

   Das generierte Passwort muss verwendet werden, um die NDMP-Verbindung durch die Backup-Anwendung zu authentifizieren.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Konfigurieren Sie ONTAP LIFs für SVM-bezogenes NDMP

Sie müssen die LIFs identifizieren, die für die Einrichtung einer Datenverbindung zwischen den Daten- und Tape-Ressourcen verwendet werden, und für die Kontrollverbindung zwischen der Admin-SVM und der Backup-Applikation. Nach der Identifizierung der LIFs müssen Sie überprüfen, ob die Service- und Failover-Richtlinien festgelegt sind.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Unterstützter Datenverkehr verwalten".

ONTAP 9.10.1 oder höher

Schritte

1. Identifizieren Sie die Intercluster LIF, die auf den Nodes gehostet wird `network interface show -service-policy`, indem Sie den Befehl mit dem Parameter verwenden.

   ```
   network interface show -service-policy default-intercluster
   ```

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

2. Identifizieren Sie die auf den Nodes gehostete Management-LIF mit dem `network interface show` Befehl mit dem `-service-policy` Parameter.

   ```
   network interface show -service-policy default-management
   ```

3. Stellen Sie sicher, dass die Intercluster LIF den Service umfasst `backup-ndmp-control`:

   ```
   network interface service-policy show
   ```

   Erfahren Sie mehr über `network interface service-policy show` in der "ONTAP-Befehlsreferenz".

4. Vergewissern Sie sich, dass die Failover-Richtlinie für alle LIFs ordnungsgemäß festgelegt ist:

   a. Überprüfen Sie, ob die Failover-Richtlinie für die Cluster-Management-LIF auf festgelegt ist `broadcast-domain-wide` und ob die Richtlinie für die Intercluster- und Node-Management-LIFs `local-only` über den `network interface show -failover` Befehl auf festgelegt ist.

      Mit dem folgenden Befehl wird die Failover-Richtlinie für die LIFs für das Cluster-Management, die Intercluster und die Node-Management angezeigt:

```
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. Wenn die Failover-Richtlinien nicht ordnungsgemäß festgelegt wurden, ändern Sie die Failover-Richtlinie mithilfe des `network interface modify` Befehls mit dem `-failover-policy` Parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

5. Geben Sie die LIFs an, die für die Datenverbindung erforderlich sind, indem `vserver services ndmp modify` `preferred-interface-role` Sie den Befehl mit dem Parameter verwenden.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Überprüfen Sie mit dem `vserver services ndmp show` Befehl, ob die bevorzugte Schnittstellenrolle für das Cluster 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. Intercluster-, Cluster-Management- und Node-Management-LIFs identifizieren, indem Sie den `network interface show` Befehl mit dem `-role` Parameter verwenden.

   Mit dem folgenden Befehl werden die Intercluster-LIFs angezeigt:

```
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
```

   Mit dem folgenden Befehl wird die Cluster-Management-LIF angezeigt:

```
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
```

Mit dem folgenden Befehl werden die Node-Management-LIFs angezeigt:

```
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
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

2. Stellen Sie sicher, dass die Firewallrichtlinie für NDMP auf den Intercluster, Cluster-Management (`cluster-mgmt`) und Node-Management aktiviert ist(`node-mgmt`) LIFs:

   a. Überprüfen Sie mit dem `system services firewall policy show` Befehl, ob die Firewallrichtlinie für NDMP aktiviert ist.

      Mit dem folgenden Befehl wird die Firewallrichtlinie für die Cluster-Management-LIF angezeigt:

```
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.
```

Mit dem folgenden Befehl wird die Firewallrichtlinie für die Intercluster-LIF angezeigt:

```
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.
```

Mit dem folgenden Befehl wird die Firewallrichtlinie für die Node-Management-LIF angezeigt:

```
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. Wenn die Firewallrichtlinie nicht aktiviert ist, aktivieren Sie die Firewallrichtlinie, indem Sie den `system services firewall policy modify` Befehl mit dem `-service` Parameter verwenden.

   Mit dem folgenden Befehl wird eine Firewall-Richtlinie für die Intercluster LIF aktiviert:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Vergewissern Sie sich, dass die Failover-Richtlinie für alle LIFs ordnungsgemäß festgelegt ist:

   a. Überprüfen Sie, ob die Failover-Richtlinie für die Cluster-Management-LIF auf festgelegt ist `broadcast-domain-wide` und ob die Richtlinie für die Intercluster- und Node-Management-LIFs `local-only` über den `network interface show -failover` Befehl auf festgelegt ist.

      Mit dem folgenden Befehl wird die Failover-Richtlinie für die LIFs für das Cluster-Management, die Intercluster und die Node-Management angezeigt:

```
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. Wenn die Failover-Richtlinien nicht ordnungsgemäß festgelegt wurden, ändern Sie die Failover-Richtlinie mithilfe des `network interface modify` Befehls mit dem `-failover-policy` Parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

4. Geben Sie die LIFs an, die für die Datenverbindung erforderlich sind, indem `vserver services ndmp modify` `preferred-interface-role` Sie den Befehl mit dem Parameter verwenden.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Überprüfen Sie mit dem `vserver services ndmp show` Befehl, ob die bevorzugte Schnittstellenrolle für das Cluster festgelegt ist.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

Konfigurieren Sie NDMP mit Node-Umfang

Aktivieren Sie knotenbezogenes NDMP auf dem ONTAP-Cluster

Sie können Backups von Volumes, die auf einem einzelnen Node gehostet werden, durch die Aktivierung von NDMP mit Node-Umfang, die Aktivierung des NDMP-Service und die Konfiguration einer logischen Schnittstelle für die Daten- und Kontrollverbindung erstellen. Dies kann für alle Nodes des Clusters durchgeführt werden.

Node-Scoped NDMP ist veraltet in ONTAP 9.

Über diese Aufgabe

Bei Verwendung von NDMP im Node-Scope-Modus muss die Authentifizierung pro Node konfiguriert werden. Weitere Informationen finden Sie unter "Der Knowledge Base-Artikel „How to configure NDMP Authentication in the ‘Node-scope’ Mode“".

Schritte

1. NDMP-Modus mit Knotenbereich aktivieren:

```
cluster1::> system services ndmp node-scope-mode on
```

Der NDMP Node-scope-Modus ist aktiviert.

2. Aktivieren Sie den NDMP-Dienst auf allen Nodes im Cluster:

   Mit dem Platzhalter „*“ wird der NDMP-Service auf allen Nodes gleichzeitig aktiviert.

   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. Deaktivieren Sie die `-clear-text` Option für die sichere Kommunikation des NDMP-Passworts:

   Verwenden der*" `disables the `-clear-text` Option Platzhalter „`“ auf allen Knoten gleichzeitig.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Überprüfen Sie, ob der NDMP-Dienst 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.
```

Konfigurieren Sie ONTAP LIFs für knotenbezogenes NDMP

Sie müssen ein LIF angeben, das zur Einrichtung einer Datenverbindung und zur Steuerung der Verbindung zwischen dem Node und der Backup-Applikation verwendet wird. Nach der Identifizierung der LIF müssen Sie überprüfen, ob für die LIF Firewall- und Failover-Richtlinien festgelegt sind.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Unterstützter Datenverkehr verwalten".

ONTAP 9.10.1 oder höher

Schritte

1. Identifizieren Sie die Intercluster LIF, die auf den Nodes gehostet wird `network interface show -service-policy`, indem Sie den Befehl mit dem Parameter verwenden.

   ```
   network interface show -service-policy default-intercluster
   ```

2. Stellen Sie sicher, dass die Intercluster LIF den Service umfasst `backup-ndmp-control`:

   ```
   network interface service-policy show
   ```

3. Vergewissern Sie sich, dass die Failover-Richtlinie für die Intercluster LIFs ordnungsgemäß festgelegt ist:

   a. Überprüfen Sie `local-only` mithilfe des `network interface show -failover` Befehls, ob die Failover-Richtlinie für die Intercluster-LIFs auf festgelegt ist.

   ```
   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 festgelegt ist, ändern Sie die Failover-Richtlinie mithilfe des `network interface modify` Befehls mit dem `-failover-policy` Parameter.

   ```
   cluster1::> network interface modify -vserver cluster1 -lif IC1
   -failover-policy local-only
   ```

Erfahren Sie mehr über `network interface show`, `network interface service-policy show` und `network interface modify` in der "ONTAP-Befehlsreferenz".

ONTAP 9.9 oder früher

Schritte

1. Identifizieren Sie die Intercluster LIF, die auf den Nodes gehostet wird `network interface show -role`, indem Sie den Befehl mit dem Parameter verwenden.

```
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. Vergewissern Sie sich, dass die Firewallrichtlinie für NDMP auf den intercluster LIFs aktiviert ist:

   a. Überprüfen Sie mit dem `system services firewall policy show` Befehl, ob die Firewallrichtlinie für NDMP aktiviert ist.

   Mit dem folgenden Befehl wird die Firewallrichtlinie für die Intercluster-LIF angezeigt:

```
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. Wenn die Firewallrichtlinie nicht aktiviert ist, aktivieren Sie die Firewallrichtlinie, indem Sie den

`system services firewall policy modify` Befehl mit dem `-service` Parameter verwenden.

Mit dem folgenden Befehl wird eine Firewall-Richtlinie für die Intercluster LIF aktiviert:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Vergewissern Sie sich, dass die Failover-Richtlinie für die Intercluster LIFs ordnungsgemäß festgelegt ist:

   a. Überprüfen Sie `local-only` mithilfe des `network interface show -failover` Befehls, ob die Failover-Richtlinie für die Intercluster-LIFs auf festgelegt ist.

```
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 festgelegt ist, ändern Sie die Failover-Richtlinie mithilfe des `network interface modify` Befehls mit dem `-failover-policy` Parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Erfahren Sie mehr über `network interface show` und `network interface modify` in der "ONTAP-Befehlsreferenz".

Konfigurieren von Backup-Anwendungen für die ONTAP NDMP-Konfiguration

Nachdem das Cluster für den NDMP-Zugriff konfiguriert ist, müssen Sie Informationen aus der Cluster-Konfiguration erfassen und dann den Rest des Backup-Prozesses in der Backup-Applikation konfigurieren.

Schritte

1. Stellen Sie die folgenden Informationen zusammen, die Sie zuvor in ONTAP konfiguriert haben:
   - Der Benutzername und das Passwort, den die Backup-Anwendung zum Erstellen der NDMP-Verbindung benötigt
   - Die IP-Adressen der Intercluster LIFs, die die Backup-Applikation zur Verbindung mit dem Cluster benötigt
2. Zeigen Sie in ONTAP die Aliase an, die ONTAP jedem Gerät mit dem `storage tape alias show` Befehl zugewiesen hat.

   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. Konfigurieren Sie in der Backup-Applikation den Rest des Backup-Prozesses mithilfe der Dokumentation der Backup-Applikation.

Nachdem Sie fertig sind

Falls ein Ereignis der Datenmobilität eintritt, wie z. B. eine Volume-Verschiebung oder LIF-Migration, müssen Sie bereit sein, alle unterbrochenen Backup-Vorgänge erneut zu initialisieren.

Verwandte Informationen

- "Speicherbandalias anzeigen"

Übersicht über die Replizierung zwischen NetApp Element Software und ONTAP

Mit SnapMirror können Sie Snapshots eines Element Volumes auf einem ONTAP Ziel replizieren und damit Business Continuity auf einem Element System sicherstellen. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element System anschließend nach Wiederherstellung des Service wieder aktivieren.

Ab ONTAP 9.4 können Sie Snapshots einer auf einem ONTAP Node erstellten LUN zurück in ein Element System replizieren. Möglicherweise haben Sie während eines Ausfalls am Element Standort eine LUN erstellt oder eine LUN verwenden, um Daten von ONTAP auf Element Software zu migrieren.

"Konfiguration der Replizierung von NetApp Element Software und ONTAP".