



Datensicherung und Disaster Recovery

System Manager Classic

NetApp
June 22, 2024

Inhalt

- Datensicherung und Disaster Recovery 1
 - Konfiguration des Cluster- und SVM-Peering 1
 - Volume Disaster Recovery 12
 - Vorbereitung der Volume Disaster Recovery 24
 - Volume Backup mit SnapVault 33
 - Management von Volume-Wiederherstellungen mit SnapVault 41

Datensicherung und Disaster Recovery

Konfiguration des Cluster- und SVM-Peering

Übersicht über Cluster- und SVM-Peering

Cluster-Administratoren können authentifizierte Peer-Beziehungen zwischen Clustern und SVMs erstellen, sodass die Cluster miteinander kommunizieren können, sodass Daten zwischen Volumes in unterschiedlichen Clustern repliziert werden. Sie können die Verfahren mit der ONTAP-Benutzeroberfläche „System Manager *classic*“ ausführen, die mit ONTAP 9.7 und früheren Versionen von ONTAP 9 verfügbar ist.

Verwenden Sie die Schnittstelle „ONTAP System Manager_classic_“ zum Erstellen von Cluster-Peer-Beziehungen und SVM-Peer-Beziehungen, wenn Folgendes gilt:

- Sie arbeiten mit Clustern mit ONTAP 9.7 oder älteren ONTAP 9 Versionen.
- Sie möchten authentifizierte Cluster-Peering-Beziehungen.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie möchten System Manager verwenden, nicht die ONTAP Befehlszeilenschnittstelle (CLI) oder ein automatisiertes Scripting Tool.

Weitere Möglichkeiten dies in ONTAP zu tun

ONTAP System Manager in ONTAP 9.3 vereinfacht die Konfiguration von Peer-Beziehungen zwischen Clustern und zwischen SVMs. Für alle Versionen von ONTAP 9 können das Cluster-Peering-Verfahren und das SVM-Peering-Verfahren verwendet werden. Sie sollten das entsprechende Verfahren für Ihre ONTAP-Version verwenden.

So führen Sie diese Aufgaben durch:	Siehe...
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	<ul style="list-style-type: none">• "Cluster-Management mit System Manager"
Die ONTAP Befehlszeilenschnittstelle (CLI)	<ul style="list-style-type: none">• "Übersicht über Cluster- und SVM-Peering mit der CLI" <p>Verwenden Sie die Befehlszeilenschnittstelle, um Cluster-Peering-Beziehungen und SVM-Peering-Beziehungen einzurichten.</p> <ul style="list-style-type: none">• "Netzwerkmanagement" <p>Verwenden Sie die Befehlszeilenschnittstelle, um Subnetze, LIFs zwischen Clustern, Routen, Firewall-Richtlinien und andere Netzwerkkomponenten zu konfigurieren</p>

Voraussetzungen für Cluster-Peering

Bevor Sie Cluster-Peering über die ONTAP System Manager *classic* -Schnittstelle mit ONTAP 9.7 oder früher einrichten, sollten Sie bestätigen, dass Konnektivität, Port, IP-Adresse, Subnetz, Firewall, Und die Anforderungen für die Cluster-Benennung erfüllen.

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 über genügend IP-Adressen verfügen, um einer Intercluster LIF pro Node zuzuweisen.

In einem Cluster mit sechs Nodes muss das für die Kommunikation zwischen Clustern verwendete Subnetz sechs 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.



ONTAP 9 ermöglicht Ihnen die Migration Ihrer Peering-Netzwerke von IPv4 zu IPv6, indem Sie optional zulassen, dass beide Protokolle gleichzeitig auf den Intercluster LIFs vorhanden sind. 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

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

- ICMP-Dienst
- TCP auf die IP-Adressen aller Cluster-LIFs über die Ports 10000, 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 ONTAP System Manager konfigurieren.

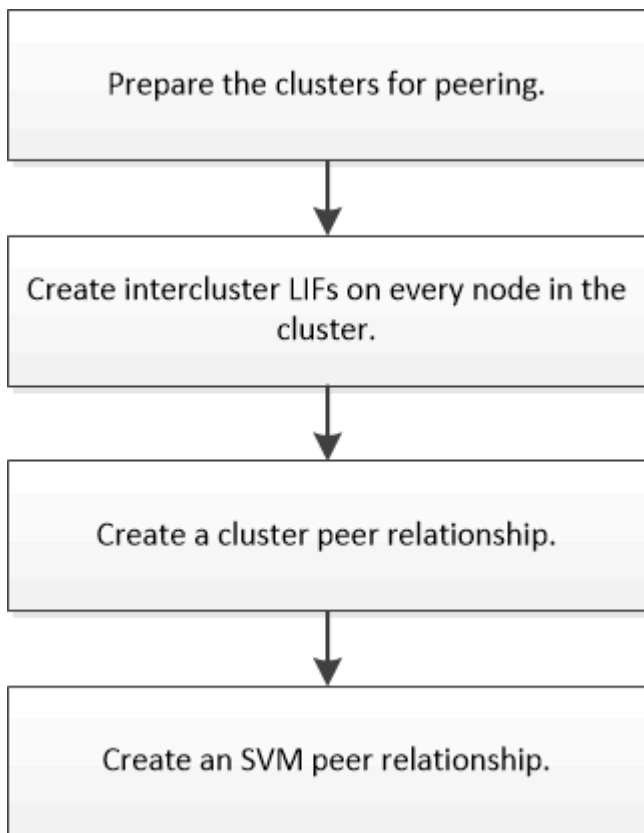
Der Standardwert `intercluster` Firewall-Richtlinie ermöglicht den Zugriff über das HTTPS-Protokoll und über alle IP-Adressen (0.0.0.0/0). Sie können die Richtlinie bei Bedarf ändern oder ersetzen.

Verwandte Informationen

["Datensicherung"](#)

Workflow für Cluster- und SVM-Peering

Sie können eine Peering-Beziehung mithilfe des ONTAP System Managers mit ONTAP 9.7 oder früher einrichten. Das Einrichten einer Peering-Beziehung umfasst die Vorbereitung jedes Clusters für Peering, die Erstellung von Intercluster Logical Interfaces (LIFs) auf jedem Node jedes Clusters, die Einrichtung einer Cluster-Peer-Beziehung und die Einrichtung einer SVM Peering-Beziehung.



Wenn Sie ONTAP 9.2 oder älter ausführen, erstellen Sie eine SVM Peering-Beziehung und erstellen eine Datensicherungsbeziehung zwischen dem Quell-Volumen und dem Ziel-Volumen.

Cluster-Peering vorbereiten

Bevor Sie eine Cluster-Peering-Beziehung mithilfe der ONTAP System Manager *classic* -Schnittstelle mit ONTAP 9.7 oder einer älteren Version erstellen, müssen Sie überprüfen, ob die Zeit auf jedem Cluster mit einem externen NTP-Server (Network Time Protocol) synchronisiert wird, und ermitteln Sie die Subnetze, Ports und Passphrases, die Sie verwenden möchten.

Schritte

1. Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, bestimmen Sie die Passphrase, die Sie für jede Cluster-Peer-Beziehung verwenden möchten.

Die Passphrase muss mindestens acht Zeichen enthalten.

Für die Beziehung zwischen...	Die Passphrase lautet...
Cluster A und Cluster B	

Ab ONTAP 9.3 können Sie die Passphrase aus dem Remote-Cluster generieren und gleichzeitig die Cluster-Peer-Beziehung erstellen.

["Erstellen einer Cluster-Peer-Beziehung \(Beginn: ONTAP 9.3\)"](#)

2. Identifizieren Sie die Subnetze, IP-Adressen und Ports, die Sie für Intercluster-LIFs verwenden.

Standardmäßig wird die IP-Adresse automatisch aus dem Subnetz ausgewählt. Wenn Sie die IP-Adresse manuell angeben möchten, müssen Sie sicherstellen, dass die IP-Adresse entweder bereits im Subnetz verfügbar ist oder später dem Subnetz hinzugefügt werden kann. Informationen zu Subnetzen finden Sie auf der Registerkarte Netzwerk.

Erstellen Sie eine Tabelle ähnlich der folgenden Tabelle, um Informationen zu den Clustern zu erfassen. In der folgenden Tabelle wird davon ausgegangen, dass jedes Cluster vier Nodes hat. Wenn ein Cluster mehr als vier Nodes hat, fügen Sie für die zusätzlichen Informationen Zeilen hinzu.

	Cluster A	Cluster B
Subnetz (ONTAP 9.2 oder früher)		
IP-Adresse (ab ONTAP 9.3, optional für ONTAP 9.2 oder älter)		
Node 1-Port		
Node 2-Port		
Node 3-Port		
Node 4-Port		

Konfiguration von Peer-Beziehungen (beginnend mit ONTAP 9.3)

Eine Peer-Beziehung definiert die Netzwerkverbindungen, mit denen Cluster und SVMs einen sicheren Datenaustausch ermöglichen. Ab ONTAP 9.3 können Sie bis ONTAP 9.7 mithilfe der Benutzeroberfläche des ONTAP System Manager *classic* eine vereinfachte Methode zum Konfigurieren von Peer-Beziehungen zwischen Clustern und zwischen SVMs ausführen.

Intercluster-LIFs erstellen (beginnend mit ONTAP 9.3)

Ab ONTAP 9.3 können Sie bis ONTAP 9.7 über die ONTAP System Manager *classic* Schnittstelle Cluster-übergreifende logische Schnittstellen (LIFs) erstellen, sodass das Cluster-Netzwerk mit einem Node kommunizieren kann. Sie müssen innerhalb jedes IPspaces, der für Peering verwendet wird, eine Intercluster LIF erstellen, auf jedem Node in jedem Cluster, für den Sie eine Peer-Beziehung erstellen möchten.

Über diese Aufgabe

Wenn Sie beispielsweise ein Cluster mit vier Nodes haben, das Sie mit Cluster X über IPspace A Peer mit Cluster Y über IPspace Y erstellen möchten, benötigen Sie insgesamt acht Intercluster-LIFs. Vier auf IPspace A (einer pro Knoten) und vier auf IPspace Y (einer pro Knoten).

Sie müssen dieses Verfahren auf beiden Clustern durchführen, für die Sie eine Peer-Beziehung erstellen möchten.

Schritte

1. Klicken Sie Auf **Konfiguration > Erweitertes Cluster-Setup**.
2. Klicken Sie im Fenster **Setup Advanced Cluster Features** neben der Option **Cluster Peering** auf **Proceed**.
3. Wählen Sie einen IPspace aus der Liste **IPspace** aus.
4. Geben Sie für jeden Node die IP-Adresse, den Port, die Netzwerkmaske und das Gateway ein.

	IP Address	Port	Netmask	Gateway (Optional)
sti50-vsrm-ucs103a	10.53.32.1	e0d	255.255.240.0	
sti50-vsrm-ucs103b	10.53.32.2	e0d		

5. Klicken Sie auf **Absenden und fortfahren**.

Nächste Schritte

Sie sollten die Cluster-Details im Cluster-Peering-Fenster eingeben, um mit Cluster-Peering fortzufahren.

Cluster-Peer-Beziehung erstellen (beginnend mit ONTAP 9.3)

Ab ONTAP 9.3 können Sie bis ONTAP 9.7 die ONTAP System Manager *classic* Schnittstelle verwenden, um eine Cluster-Peer-Beziehung zwischen zwei Clustern zu

erstellen. Dazu wird eine vom System generierte Passphrase und die IP-Adressen der Intercluster-LIFs des Remote-Clusters bereitgestellt.

Über diese Aufgabe

Ab ONTAP 9.6 ist die Cluster-Peering-Verschlüsselung bei allen neu erstellten Cluster-Peering-Beziehungen standardmäßig aktiviert. Die Cluster-Peering-Verschlüsselung muss manuell aktiviert werden, damit die vor dem Upgrade auf ONTAP 9.6 erstellte Peering-Beziehung Peering durchgeführt wird. Die Cluster-Peering-Verschlüsselung ist nicht für Cluster verfügbar, auf denen ONTAP 9.5 oder eine frühere Version ausgeführt wird. Daher müssen beide Cluster in der Peering-Beziehung ONTAP 9.6 ausführen, um die Verschlüsselung von Cluster-Peering zu ermöglichen.

Die Cluster-Peering-Verschlüsselung verwendet die Transport Security Layer (TLS) zum sicheren Cluster-übergreifenden Peering von Kommunikation für ONTAP Funktionen wie SnapMirror und FlexCache.

Schritte

1. Geben Sie im Feld **Target Cluster Intercluster LIF IP Addresses** die IP Adressen der Intercluster LIFs des Remote Clusters ein.
2. Generieren einer Passphrase aus dem Remote-Cluster.
 - a. Geben Sie die Managementadresse des Remote-Clusters an.
 - b. Klicken Sie auf **Management URL**, um ONTAP System Manager auf dem Remote-Cluster zu starten.
 - c. Melden Sie sich beim Remote-Cluster an.
 - d. Klicken Sie im Fenster **Cluster Peers** auf **Peering Passphrase generieren**.
 - e. Wählen Sie das IPspace, die Gültigkeit der Passphrase und die SVM-Berechtigungen aus.

Sie können alle SVMs oder ausgewählte SVMs für Peering zulassen. Wenn eine SVM-Peer-Anfrage generiert wird, werden die zulässigen SVMs automatisch mit den Quell-SVMs Peering durchgeführt, ohne dass Sie die Peer-Beziehung der Remote-SVMs akzeptieren müssen.

- f. Klicken Sie Auf **Erzeugen**.

Die Passphrase-Informationen werden angezeigt.

Generate Peering Passphrase



Passphrase generated successfully

Use the following information for peering based on the IPspace "Default":

Intercluster LIF IP Address 172.21.91.12

Passphrase QS7k+laFYJzclV9UMPXvHgWd

Passphrase Validity Valid Until Mon Nov... America/New_Y

SVM Permissions All

Email passphrase details

Copy passphrase details

Done

- a. Klicken Sie auf **Passphrase-Details kopieren** oder **E-Mail-Passphrase-Details**.
- b. Klicken Sie Auf **Fertig**.
3. Geben Sie im Quellcluster die generierte Passphrase ein, die Sie in erhalten haben [Schritt 2](#).
4. Klicken Sie Auf **Cluster Peering Initiieren**.
Die Cluster-Peer-Beziehung wurde erfolgreich erstellt.
5. Klicken Sie Auf **Weiter**.

Nächste Schritte

Sie sollten die SVM-Details im SVM-Peering-Fenster angeben, um den Peering-Prozess fortzusetzen.

Erstellung von SVM-Peer-Beziehungen

Beginnend mit ONTAP 9.3 bis ONTAP 9.7 können Sie die ONTAP System Manager *classic* Schnittstelle zum Erstellen von SVM-Peer-Beziehungen verwenden. Das Storage Virtual Machine (SVM)-Peering ermöglicht Ihnen die Einrichtung einer Peer-Beziehung zwischen zwei SVMs zur Datensicherung.

Schritte

1. Wählen Sie die Initiator-SVM aus.

2. Wählen Sie die Ziel-SVM aus der Liste zulässiger SVMs aus.
3. Klicken Sie auf **SVM-Peering initiieren**.
4. Klicken Sie Auf **Weiter**.

Nächste Schritte

Im Fenster „Zusammenfassung“ können die Clusterschnittstellen, die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung angezeigt werden.

Konfiguration von Peer-Beziehungen (ONTAP 9.2 und früher)

Erstellen Sie mithilfe der Schnittstelle ONTAP System Manager *classic* mit ONTAP 9.2 oder einer früheren ONTAP 9 Version SVM Peer-Beziehungen.

Eine Peer-Beziehung definiert Netzwerkverbindungen, mit denen Cluster und SVMs einen sicheren Datenaustausch ermöglichen. Sie müssen eine Cluster-Peer-Beziehung erstellen, bevor Sie eine SVM-Peer-Beziehung erstellen können.

Erstellen von Intercluster-Schnittstellen auf allen Nodes (ONTAP 9.2 oder früher)

Über die Schnittstelle ONTAP System Manager *classic* zu ONTAP 9.2 oder einer früheren Version von ONTAP 9 können Sie Intercluster LIFs erstellen, die für das Peering verwendet werden.

Cluster kommunizieren miteinander über logische Schnittstellen (LIFs), die für die Kommunikation zwischen Clustern dediziert sind. Sie müssen innerhalb jedes IPspace, der für Peering verwendet wird, eine Intercluster LIF erstellen. Die LIFs müssen auf jedem Node in jedem Cluster erstellt werden, für das Sie eine Peer-Beziehung erstellen möchten.

Bevor Sie beginnen

Sie müssen das Subnetz und die Ports und optional die IP-Adressen identifiziert haben, die Sie für die Intercluster LIFs verwenden möchten.

Über diese Aufgabe

Sie müssen dieses Verfahren auf beiden Clustern durchführen, für die Sie eine Peer-Beziehung erstellen möchten. Wenn Sie beispielsweise ein Cluster mit vier Nodes haben, das Sie mit Cluster X über IPspace A Peer mit Cluster Y über IPspace Y erstellen möchten, benötigen Sie insgesamt acht Intercluster-LIFs. Vier auf IPspace A (einer pro Knoten) und vier auf IPspace Y (einer pro Knoten).

Schritte

1. Erstellen einer intercluster LIF auf einem Knoten des Quellclusters:
 - a. Navigieren Sie zum Fenster **Netzwerkschnittstellen**.
 - b. Klicken Sie Auf **Erstellen**.

Das Dialogfeld Netzwerkschnittstelle erstellen wird angezeigt.

- c. Geben Sie einen Namen für die Intercluster LIF ein.

Sie können „ic01“ für die Intercluster-LIF auf dem ersten Knoten und „ic02“ für die Intercluster-LIF auf dem zweiten Knoten verwenden.

- d. Wählen Sie als Schnittstellenrolle * Intercluster Connectivity* aus.
- e. Wählen Sie das IPspace aus.
- f. Wählen Sie im Dialogfeld **Details hinzufügen** in der Dropdown-Liste **IP-Adresse zuweisen** die Option **über ein Subnetz** aus, und wählen Sie dann das Subnetz aus, das Sie für die Kommunikation zwischen Clustern verwenden möchten.

Standardmäßig wird die IP-Adresse automatisch aus dem Subnetz ausgewählt, nachdem Sie auf **Erstellen** geklickt haben. Wenn Sie die automatisch ausgewählte IP-Adresse nicht verwenden möchten, müssen Sie manuell die IP-Adresse angeben, die der Knoten für die Kommunikation zwischen Clustern verwendet.

- g. Wenn Sie die IP-Adresse, die der Knoten für die Intercluster-Kommunikation verwendet, manuell angeben möchten, wählen Sie **Diese IP-Adresse verwenden** aus, und geben Sie die IP-Adresse ein.
 Sie müssen sicherstellen, dass die IP-Adresse, die Sie verwenden möchten, bereits im Subnetz verfügbar ist oder später dem Subnetz hinzugefügt werden kann.
- h. Klicken Sie im Bereich **Ports** auf den Knoten, den Sie konfigurieren, und wählen Sie den Port aus, den Sie für diesen Knoten verwenden möchten.
- i. Wenn Sie sich entschieden haben, Ports für die Kommunikation zwischen Clustern und Daten nicht gemeinsam zu nutzen, bestätigen Sie, dass der ausgewählte Port in der Spalte **Hosted Interface Count** „0“ anzeigt.

Specify the following details to add a new network interface for data and management access of the chosen SVM.

Name:

Interface Role: Serves Data Intercluster Connectivity

SVM:

Protocol Access: CIFS NFS ISCSI FC/FCoE

Management Access: Enable Management Access

Subnet:

The IP address is selected from this subnet.

Use this IP Address:

i This IP address will be added to the chosen subnet if the address is not already present in the subnet available range.

Ports or Adapters	Hosted Interface Count	Speed
▲ clusterA-node1		
e0c	3	1000 Mbps
e0d	0	1000 Mbps
e0e	0	1000 Mbps

- j. Klicken Sie Auf **Erstellen**.

2. Wiederholen [Schritt 1](#) Für jeden Node im Cluster.


Jeder Node im Cluster verfügt über eine Intercluster-LIF.

3. Notieren Sie sich die IP-Adressen der Intercluster LIFs, sodass Sie sie später verwenden können, wenn Sie Peer-Beziehungen mit anderen Clustern erstellen:

- a. Klicken Sie im Fenster **Netzwerkschnittstellen** in der Spalte **Role** auf Deaktivieren Sie das Kontrollkästchen * All*, und wählen Sie dann **Intercluster** aus.

Im Fenster Netzwerkschnittstellen werden nur LIFs zwischen Clustern angezeigt.

- b. Notieren Sie sich die IP-Adressen, die in der Spalte **IP-Adressen/WWPN** aufgeführt sind, oder lassen Sie das Fenster **Netzwerkschnittstellen** geöffnet, damit Sie die IP-Adressen später abrufen können.

Sie können auf das Spaltenanzeigesymbol  klicken, um die Spalten auszublenden, die nicht angezeigt werden sollen.

Ergebnisse

Alle Nodes in jedem Cluster verfügen über Intercluster LIFs, die alle miteinander kommunizieren können.

Cluster-Peer-Beziehung erstellen (ONTAP 9.2 oder älter)

Mithilfe der ONTAP System Manager *classic*-Schnittstelle mit ONTAP 9.2 oder einer früheren Version von ONTAP 9 können Sie eine Cluster-Peer-Beziehung zwischen zwei Clustern erstellen, indem Sie eine vorab festgelegte Passphrase und die IP-Adressen der Intercluster-LIFs des Remote-Clusters eingeben, Und dann überprüfen, ob die Beziehung erfolgreich erstellt wurde.

Bevor Sie beginnen

- Sie müssen die IP-Adressen aller Cluster-Intercluster LIFs der Cluster kennen, die Sie Peer-to-Peer möchten.
- Sie müssen die Passphrase kennen, die Sie für jede Peer-Beziehung verwenden.

Über diese Aufgabe

Sie müssen dieses Verfahren für jedes Cluster durchführen.

Schritte

1. Erstellen Sie aus dem Quell-Cluster eine Cluster-Peer-Beziehung mit dem Ziel-Cluster.
 - a. Klicken Sie auf die Registerkarte **Konfigurationen**.
 - b. Klicken Sie im Fensterbereich **Cluster-Einstellungen** auf **Cluster-Peers**.
 - c. Klicken Sie Auf **Erstellen**.

Das Dialogfeld * Cluster-Peer erstellen* wird angezeigt.

- d. Geben Sie im Bereich **Details des zu Peering** des Remote-Clusters die Passphrase an, die beide Peers verwenden werden, um eine authentifizierte Cluster-Peer-Beziehung sicherzustellen.
- e. Geben Sie die IP-Adressen aller Cluster-Intercluster LIFs des Ziel-Clusters ein (eine pro Node), getrennt durch Kommas.

f. Klicken Sie Auf **Erstellen**.

Der Authentifizierungsstatus lautet „ausstehend“, da nur ein Cluster konfiguriert wurde.

2. Wechseln Sie zum Ziel-Cluster, und erstellen Sie anschließend eine Cluster-Peer-Beziehung zum Quell-Cluster:

- a. Klicken Sie auf die Registerkarte **Konfigurationen**.
- b. Klicken Sie im Fensterbereich **Cluster-Einstellungen** auf **Cluster-Peers**.
- c. Klicken Sie Auf **Erstellen**.

Das Dialogfeld Cluster-Peer erstellen wird angezeigt.

d. Geben Sie im Bereich **Details des Remote-Clusters für Peered** die gleiche Passphrase ein, die Sie in angegeben haben [Schritt 1d](#) Und die IP-Adressen der Intercluster-LIFs des Quellclusters, und klicken Sie dann auf **Erstellen**.

3. Vergewissern Sie sich im Fenster * Cluster Peers* des Ziel-Clusters, dass das Quellcluster „Available“ ist und dass der Authentifizierungsstatus „OK“ lautet.

i 'Availability' and 'Authentication Status' information might be stale for up to several minutes.

Create Modify Passphrase Modify Peer Network Parameters Delete Refresh

Peer Cluster	Availability	Authentication Status
clusterA	available	ok

Sie müssen möglicherweise auf **Aktualisieren** klicken, um die aktualisierten Informationen anzuzeigen.

Die beiden Cluster sind in einer Peer-Beziehung.

4. Wechseln Sie zum Quell-Cluster, und bestätigen Sie, dass das Ziel-Cluster „Available“ ist und dass der Authentifizierungsstatus „OK“ lautet.

Sie müssen möglicherweise auf **Aktualisieren** klicken, um die aktualisierten Informationen anzuzeigen.

Nächste Schritte

SVM-Peer-Beziehung zwischen Quell- und Ziel-SVMs erstellen und gleichzeitig eine Datensicherungsbeziehung zwischen dem Quell-Volume und dem Ziel-Volume erstellen.

["Volume Backup mit SnapVault"](#)

["Vorbereitung der Volume Disaster Recovery"](#)

Volume Disaster Recovery

Übersicht über die Disaster Recovery von Volumes

Sie können nach einem Notfall schnell ein Ziel-Volume aktivieren und dann das Quell-Volume in ONTAP mithilfe der klassischen Schnittstelle des ONTAP System Managers (ONTAP 9.7 und früher) erneut aktivieren.

Gehen Sie folgendermaßen vor, wenn Sie eine Disaster Recovery auf Volume-Ebene auf folgende Weise durchführen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die SnapMirror-Beziehung wie folgt konfiguriert [Vorbereitung der Volume Disaster Recovery](#)
- Der Cluster-Administrator des Quell-Clusters hat erklärt, dass die Daten im Quell-Volume nicht verfügbar sind, weil Ereignisse wie Virusinfektion, die zu Datenbeschädigung oder versehentlichem Löschen von Daten führen.
- Sie möchten den System Manager verwenden, nicht die ONTAP Befehlszeilenschnittstelle oder ein automatisiertes Scripting Tool.
- Sie möchten die klassische Benutzeroberfläche des System Manager für ONTAP 9.7 und ältere Versionen verwenden, nicht die ONTAP System Manager Benutzeroberfläche für ONTAP 9.7 und höher.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.

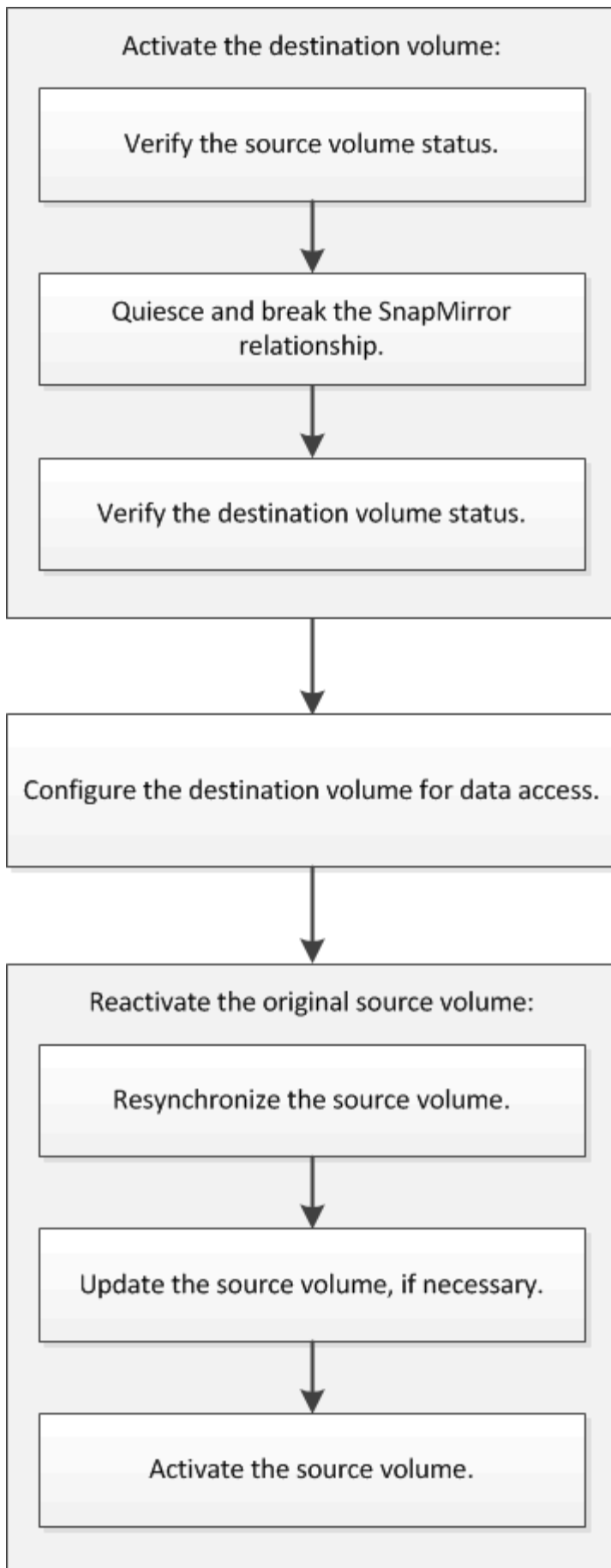
Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen...
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Stellen Sie Daten von einem SnapMirror Ziel bereit"

So führen Sie diese Aufgaben durch:	Inhalt anzeigen...
Die ONTAP Befehlszeilenschnittstelle	"Aktivieren Sie die Ziellautstärke"

Volume Disaster Recovery Workflow

Im Workflow für die Disaster Recovery von Volume müssen das Ziel-Volume aktiviert, das Ziel-Volume für den Datenzugriff konfiguriert und das ursprüngliche Quell-Volume neu aktiviert werden.



Darüber hinaus stehen Ihnen weitere Informationen zur Verfügung, mit denen Sie Disaster Recovery-Beziehungen auf Volume-Ebene managen können, und zudem weitere Disaster Recovery-Methoden zur Verfügung, um die Verfügbarkeit Ihrer Datenressourcen zu schützen.

- [Volume Backup mit SnapVault](#)

Beschreibt die schnelle Konfiguration von Backup-Vault-Beziehungen zwischen Volumes, die sich in verschiedenen ONTAP-Clustern befinden.

- [Management von Volume-Wiederherstellungen mit SnapVault](#)

Hier wird die schnelle Wiederherstellung eines Volumes aus einem Backup Vault in ONTAP beschrieben.

Aktivieren Sie die Ziellautstärke

Wenn das Quell-Volume aufgrund von Ereignissen wie Datenkorruption, versehentlichem Löschen oder offline-Status keine Daten bereitstellen kann, müssen Sie das Ziel-Volume aktivieren, um den Datenzugriff zu ermöglichen, bis Sie die Daten des Quell-Volume wiederherstellen. Die Aktivierung beinhaltet das Stoppen zukünftiger SnapMirror-Datentransfers und das Aufbrechen der SnapMirror Beziehung.

Überprüfen Sie den Status des Quell-Volume

Falls das Quell-Volume nicht verfügbar ist, müssen Sie sicherstellen, dass das Quell-Volume offline ist, und dann das Ziel-Volume identifizieren, das für den Datenzugriff aktiviert werden muss.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Wählen Sie das Quell-Volume aus, und überprüfen Sie dann, ob das Quell-Volume offline ist.
3. Identifizieren des Ziel-Volume in der SnapMirror Beziehung
 - Ab ONTAP 9.3: Doppelklicken Sie auf das Quell-Volume, um die Details anzuzeigen, und klicken Sie dann auf **PROTECTION**, um das Ziel-Volume in der SnapMirror-Beziehung und den Namen der SVM zu identifizieren, die das Volume enthält.

Health	Destination SVM	Destination Volume	Destination Clu...	Relations...	Transfer S...	Type	Lag Time	Policy
	svm2	vol_mirror_src_dst	cluster2	Snapmirrored	Idle	Version-Flexible ...	45 min(0)	Minor/Snap...

- ONTAP 9.2 oder früher: Klicken Sie auf die Registerkarte **Datensicherung** unten auf der Seite Volumes, um das Ziel-Volume in der SnapMirror-Beziehung und den Namen der SVM, die das Volume enthält, zu identifizieren.

The screenshot shows the NetApp System Manager interface. The top part displays a table of storage aggregates with columns: Name, Aggregate, Status, Thin Pro..., % Used, Availabl..., Total Sp..., Storage..., Is Volu..., and Encrypted. Below this is a table of volume relationships with columns: Destination St..., Destination Vo..., Is Healthy, Relationship St..., Transfer Status, Type, Lag Time, and Policy. At the bottom, there are tabs for Details, Space Allocation, Snapshot Copies, Storage Efficiency, Data Protection, Volume Move Det, and Performance.

Name	Aggregate	Status	Thin Pro...	% Used	Availabl...	Total Sp...	Storage...	Is Volu...	Encrypted
svm1_svm1_root...	aggr2	Online	No	5	970.48 MB	1 GB	Disabled	No	No
svm1_vol123_vault	aggr2	Online	No	5	121.35 MB	128.02 MB	Enabled	No	No
Vol1	aggr3	Offline	-NA-	-NA-	-NA-	-NA-	Disabled	No	No
svm2_root	aggr1	Online	No	5	971.12 MB	1 GB	Disabled	No	No

Destination St...	Destination Vo...	Is Healthy	Relationship St...	Transfer Status	Type	Lag Time	Policy
svm1	vol1	Yes	Snapmirrored	Idle	Mirror	7 day(s) 12 hr(s)...	DPDefault

SnapMirror Beziehung unterbrechen

Sie müssen die SnapMirror Beziehung stilllegen und unterbrechen, um das Ziel-Volumen zu aktivieren. Nach der Stilllegung werden zukünftige SnapMirror Datentransfers deaktiviert.

Bevor Sie beginnen

Das Ziel-Volumen muss auf dem Ziel-SVM-Namespace gemountet werden.

Über diese Aufgabe

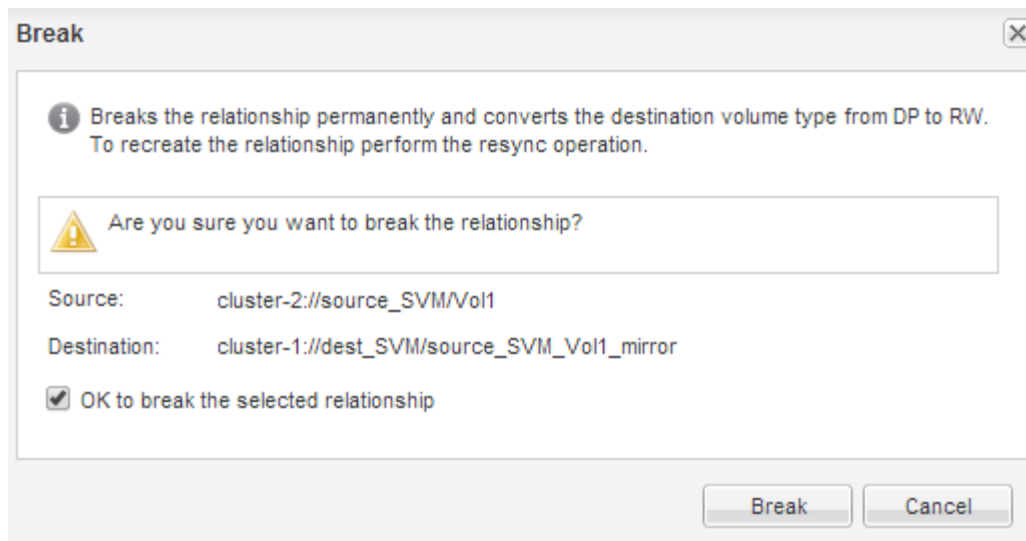
Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen dem Quell- und den Ziel-Volumen aus.
3. Klicken Sie auf **Operationen > Quiesce**, um zukünftige Datenübertragungen zu deaktivieren.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Quiesce**.

Der Vorgang zum quiesce könnte einige Zeit in Anspruch nehmen. Sie dürfen keine andere Operation an der SnapMirror-Beziehung durchführen, bis der Transferstatus als angezeigt wird **Quiesced**.

5. Klicken Sie Auf **Operationen > Pause**.
6. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **break**.



Die SnapMirror Beziehung ist in Broken Off Bundesland.

Source Siz	Source Vol	Destinatio	Destinatio	Is Healthy	Relationsh	Transfer St	Relationship	Lag Time	Policy Name	Policy Type
svm1	svm1_root	svm1_svm1_r...	svm2	Yes	Snapmirrored	Idle	Mirror	26 min(s)	DPDefault	Asynchronous
svm1	vol1	svm1_vol1_m...	svm2	Yes	Broken Off	idle	Mirror	None	DPDefault	Asynchronous

Source Location:	svm1:vol1	Is Healthy:	Yes	Transfer Status:	Idle
Destination Location:	svm2:svm1_vol1_mirror	Relationship State:	Broken Off	Current Transfer Type:	None
Source Cluster:	cluster-1	Network Compression Ratio:	Not Applicable	Current Transfer Error:	None
Destination Cluster:	cluster-1			Last Transfer Error:	None
Transfer Schedule:	hourly			Last Transfer Type:	Update
Data Transfer Rate:	Unlimited			Latest Snapshot Timestamp:	02/22/2017 13:05:00
Lag Time:	None			Latest Snapshot Copy:	snapmirror.9b4dae7c-e6d0-11e6-b44a-00a0981a1bda_2149622820_2017-

Überprüfen Sie den Status des Ziel-Volumes

Nach dem Brechen der SnapMirror Beziehung müssen Sie sicherstellen, dass das Ziel-Volumen über Lese-/Schreibzugriff verfügt und dass die Ziel-Volumen-Einstellungen den Einstellungen des Quell-Volumens entsprechen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Wählen Sie das Zielvolumen aus der Liste **Volumes** aus, und überprüfen Sie dann, ob der Zielvolumentyp lautet `rw`, Die Lese-/Schreibzugriff anzeigt.
3. Vergewissern Sie sich, dass die Volume-Einstellungen wie Thin Provisioning, Deduplizierung, Komprimierung und Autogrow auf dem Ziel-Volumen den Einstellungen des Quell-Volumens entsprechen.

Sie können die Informationen zu den Volume-Einstellungen verwenden, die Sie nach dem Erstellen der SnapMirror Beziehung angegeben haben, um die Einstellungen für das Ziel-Volumen zu überprüfen.

4. Wenn die Volume-Einstellungen nicht übereinstimmen, ändern Sie die Einstellungen auf dem Ziel-Volumen nach Bedarf:

- a. Klicken Sie Auf **Bearbeiten**.
- b. Sie können die allgemeinen Einstellungen, die Storage-Effizienz-Einstellungen und die erweiterten Einstellungen für Ihre Umgebung nach Bedarf ändern.
- c. Klicken Sie auf **Speichern und Schließen**.

Edit Volume

General | Storage Efficiency | Advanced

Name:

Security style:

Configure UNIX permissions (Optional)

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Thin Provisioned

When a volume is thin provisioned, space for the volume is not allocated in advance. Instead, space is allocated as data is written to the volume. The unused aggregate space is available to other thin provisioned volumes and LUNs.

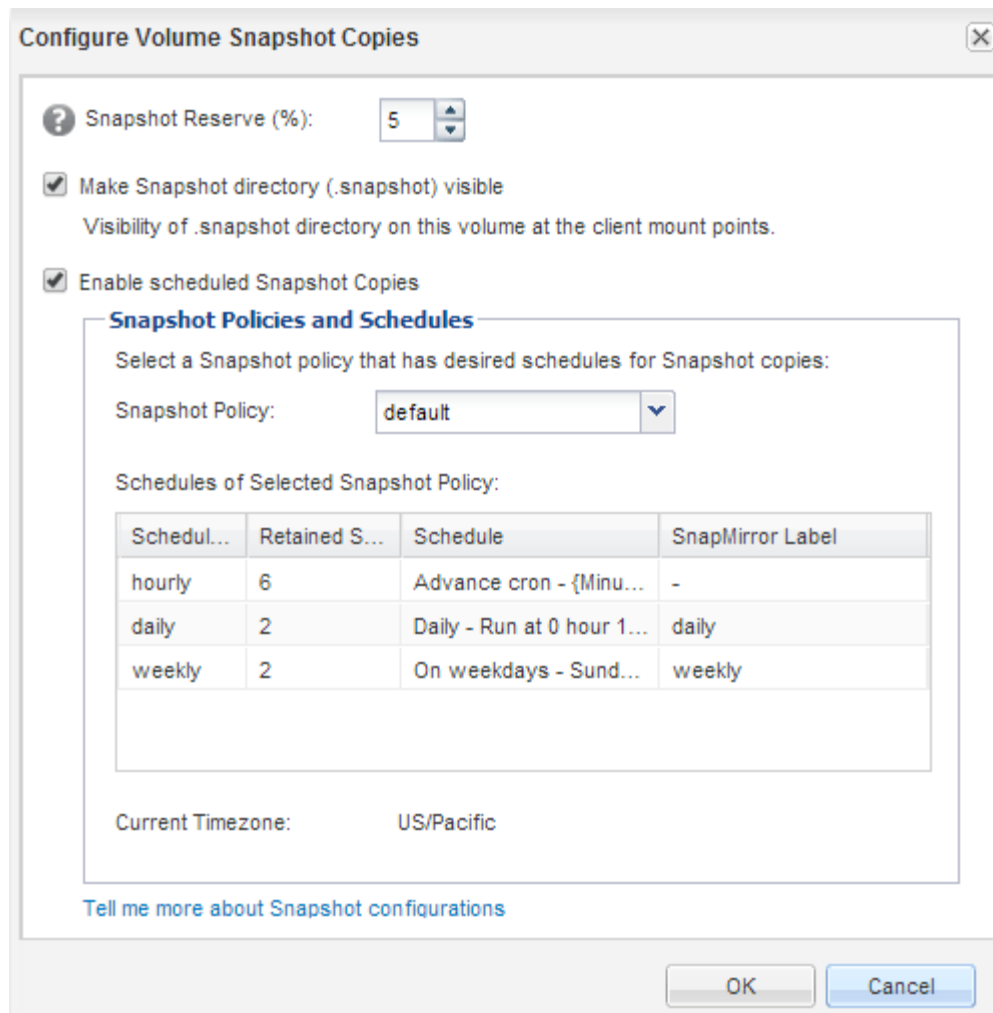
[Tell me more about Thin Provisioning](#)

Save Save and Close Cancel

- d. Stellen Sie sicher, dass die Spalten in der **Volumes**-Liste mit den entsprechenden Werten aktualisiert werden.
5. Aktivieren Sie die Erstellung von Snapshot Kopien für das Ziel-Volume.
- a. Navigieren Sie je nach ONTAP-Version zur Seite **Configure Volume Snapshot Copies** auf eine der folgenden Arten:

Ab ONTAP 9.3: Wählen Sie das Zielvolume aus und klicken Sie dann auf **Aktionen > Snapshots verwalten > Konfigurieren**.

ONTAP 9.2 oder früher: Wählen Sie das Ziel-Volume, und klicken Sie dann **Snapshot Kopien > Konfigurieren**.
 - b. Aktivieren Sie das Kontrollkästchen **geplante Snapshot-Kopien aktivieren** und klicken Sie dann auf **OK**.



Ziel-Volume für Datenzugriff konfigurieren

Nach Aktivierung des Ziel-Volume müssen Sie das Volume für den Datenzugriff konfigurieren. NAS-Clients und SAN-Hosts können auf die Daten vom Ziel-Volume zugreifen, bis das Quell-Volume erneut aktiviert ist.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Verfahren

- NAS-Umgebung:
 - a. Mounten Sie die NAS-Volumes mit dem Namespace über denselben Verbindungspfad, an den das Quell-Volume in der Quell-SVM angehängt war.
 - b. Wenden Sie die entsprechenden ACLs auf die CIFS-Freigaben am Ziel-Volume an.
 - c. Weisen Sie die NFS-Exportrichtlinien dem Ziel-Volume zu.
 - d. Wenden Sie die Kontingentregeln auf das Ziel-Volume an.
 - e. Leiten Sie die Clients an das Ziel-Volume weiter, indem Sie die erforderlichen Schritte durchführen, z. B. die DNS-Namensauflösung ändern.
 - f. NFS- und CIFS-Freigaben erneut auf den Clients einbinden.

- SAN-Umgebung:
 - a. Ordnen Sie die LUNs der entsprechenden Initiatorgruppe zu, um die LUNs im Volume den SAN-Clients zur Verfügung zu stellen.
 - b. Erstellen Sie für iSCSI-Sitzungen von den SAN-Host-Initiatoren zu den SAN-LIFs.
 - c. Führen Sie auf dem SAN-Client einen erneuten Speicherscan durch, um die verbundenen LUNs zu erkennen.

Nächste Schritte

Sie sollten das Problem beheben, das dazu geführt hat, dass das Quell-Volume nicht mehr verfügbar ist. Sie müssen das Quell-Volume nach Möglichkeit wieder online schalten, dann erneut synchronisieren und das Quell-Volume erneut aktivieren.

Verwandte Informationen

["ONTAP 9 Dokumentationszentrum"](#)

Aktivieren Sie das Quellvolumen erneut

Sobald das Quell-Volume verfügbar ist, müssen Sie die Daten vom Ziel-Volume zum Quell-Volume neu synchronisieren, nach der Neusynchronisierung Änderungen aktualisieren und das Quell-Volume aktivieren.

Synchronisieren Sie das Quell-Volume neu

Wenn das Quell-Volume online ist, müssen Sie die Daten zwischen dem Ziel-Volume und dem Quell-Volume neu synchronisieren, um die neuesten Daten vom Ziel-Volume zu replizieren.

Bevor Sie beginnen

Das Quell-Volume muss online sein.

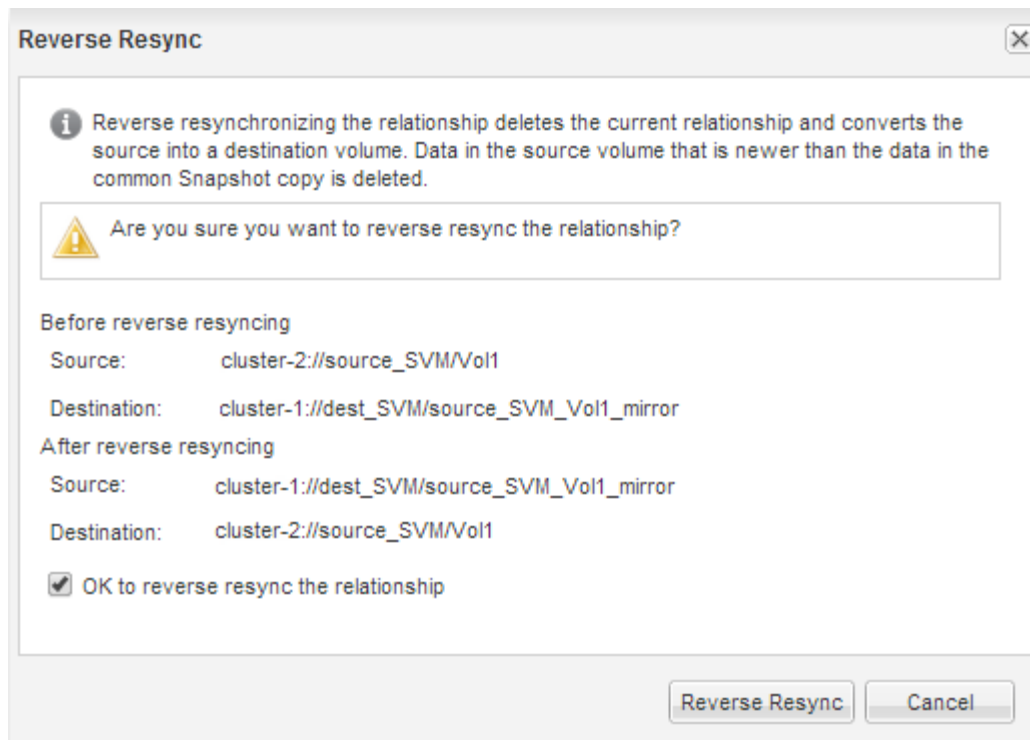
Über diese Aufgabe

Sie müssen die Aufgabe aus dem Cluster **Ziel** ausführen.

Die folgende Abbildung zeigt, dass die Daten vom aktiven Ziel-Volume auf das schreibgeschützte Quell-Volume repliziert werden:

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen den Quell- und Ziel-Volumes aus.
3. Notieren Sie sich den Übertragungszeitplan und die für die SnapMirror Beziehung konfigurierte Richtlinie.
4. Klicken Sie Auf **Operationen > Resync Rückwärts**.
5. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Resync rückwärts**.



Ab ONTAP 9.3 ist die SnapMirror Richtlinie der Beziehung auf festgelegt `MirrorAllSnapshots` Der Mirror-Zeitplan wird auf festgelegt `None`.

Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, wird die SnapMirror-Richtlinie für die Beziehung auf festgelegt `DPDefault` Der Mirror-Zeitplan wird auf festgelegt `None`.

6. Geben Sie im Quell-Cluster eine SnapMirror-Richtlinie an, die mit der Sicherheitskonfiguration der ursprünglichen SnapMirror Beziehung übereinstimmt.
 - a. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
 - b. Wählen Sie die SnapMirror Beziehung zwischen dem resynchronisierten Quell-Volume und dem Ziel-Volume aus, und klicken Sie dann auf **Bearbeiten**.
 - c. Wählen Sie die SnapMirror-Richtlinie und den Zeitplan aus, und klicken Sie dann auf **OK**.

Aktualisieren Sie das Quell-Volume

Nach der erneuten Synchronisierung des Quell-Volumes möchten Sie möglicherweise sicherstellen, dass alle neuesten Änderungen auf dem Quell-Volume aktualisiert werden, bevor Sie das Quell-Volume aktivieren.

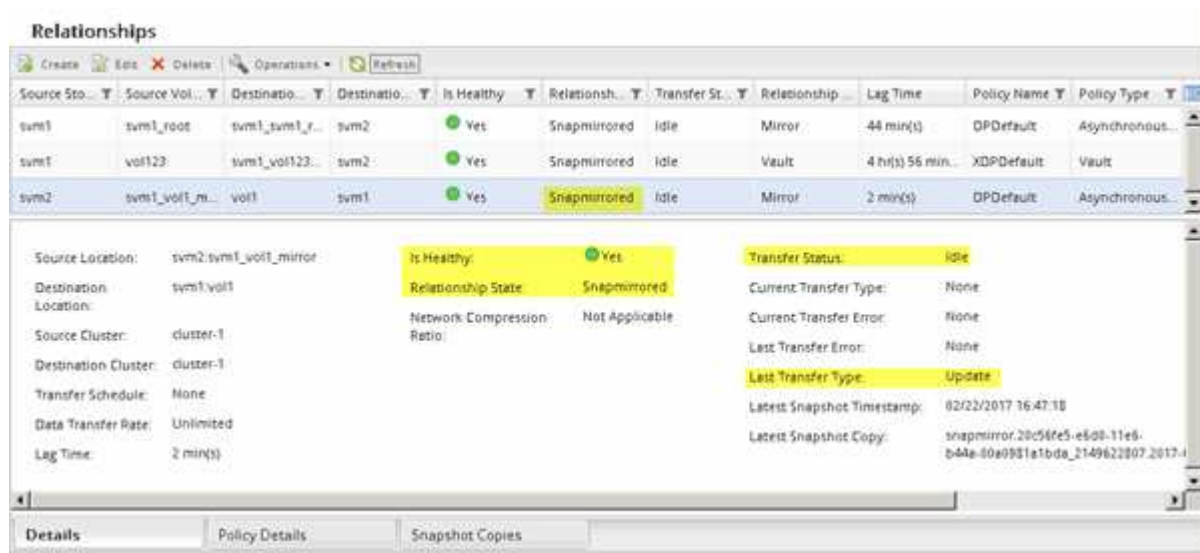
Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.

- Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen den Quell- und den Ziel-Volumes aus und klicken Sie dann auf **Operationen > Update**.
 3. Inkrementellen Transfer von der zuletzt verwendeten Snapshot Kopie zwischen den Quell- und Ziel-Volumes durchführen.
 - Ab ONTAP 9.3: Wählen Sie die Option **gemäß Richtlinie** aus.
 - ONTAP 9.2 oder früher: Wählen Sie die Option **On Demand**.
 4. **Optional:** Wählen Sie **Limit Transfer bandwidth to** aus, um die für Transfers verwendete Netzwerkbandbreite zu begrenzen und dann die maximale Übertragungsgeschwindigkeit anzugeben.
 5. Klicken Sie Auf **Aktualisieren**.
 6. Vergewissern Sie sich, dass der Übertragungsstatus lautet `Idle` Und der letzte Übertragungstyp lautet `Update` Klicken Sie auf der Registerkarte **Details** auf.



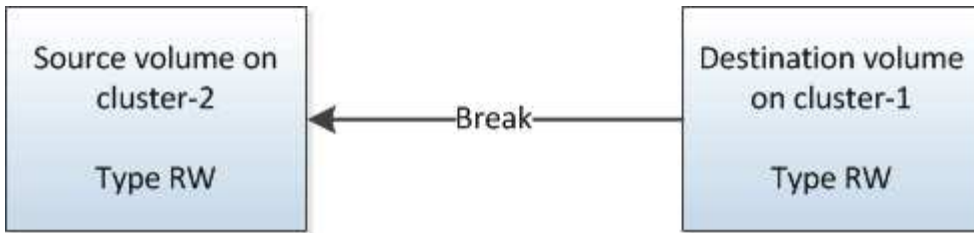
Aktivieren Sie das Quellvolumen erneut

Nachdem Sie die Daten vom Ziel-Volume zum Quell-Volume neu synchronisiert haben, müssen Sie das Quell-Volume aktivieren, indem Sie die SnapMirror Beziehung unterbrechen. Anschließend sollten Sie das Ziel-Volume neu synchronisieren, um das reaktivierte Quell-Volume zu schützen.

Über diese Aufgabe

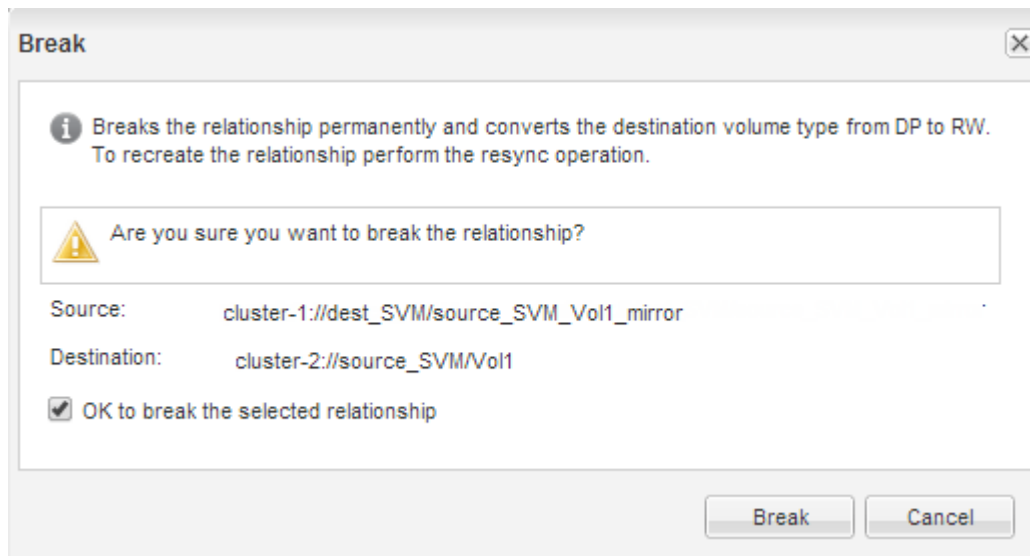
Die Break- und Reverse-Resynchronisierung wird vom * Source*-Cluster durchgeführt.

Die folgende Abbildung zeigt, dass die Quell- und Zieldatenträger gelesen/geschrieben werden, wenn Sie die SnapMirror Beziehung unterbrechen. Nach dem umgekehrten Resync-Vorgang werden die Daten vom aktiven Quell-Volume auf das schreibgeschützte Ziel-Volume repliziert.

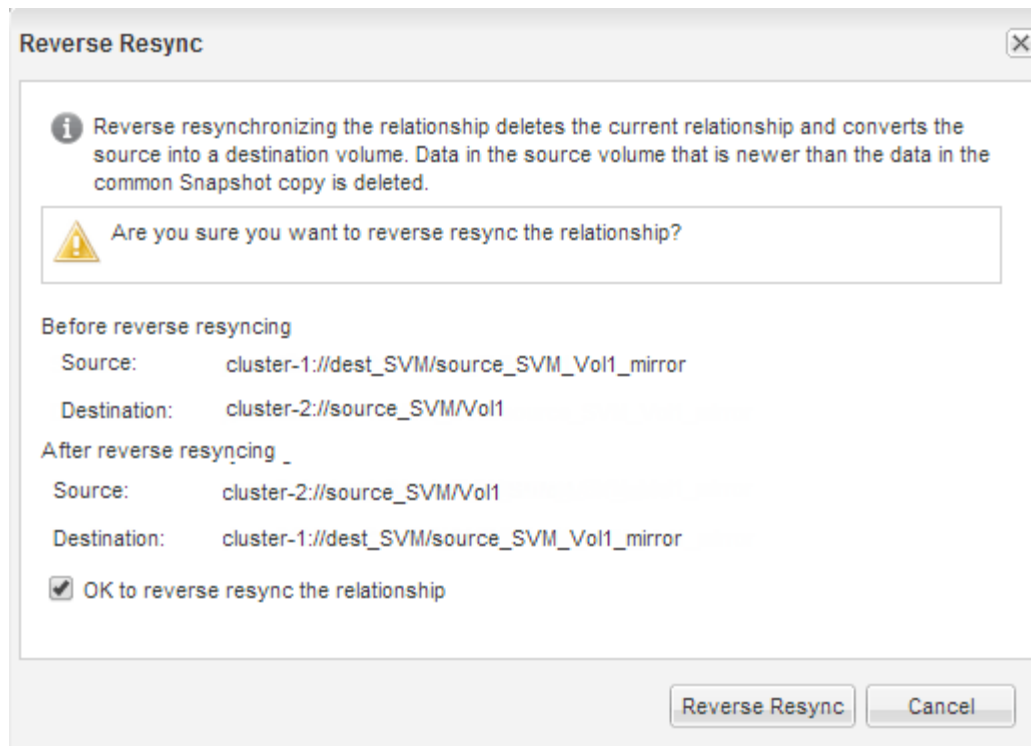


Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen dem Quell- und den Ziel-Volumes aus.
3. Klicken Sie Auf **Operationen > Quiesce**.
4. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Quiesce**.
5. Klicken Sie Auf **Operationen > Pause**.
6. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **break**.



7. Klicken Sie Auf **Operationen > Resync Rückwärts**.
8. Aktivieren Sie das Bestätigungsfeld, und klicken Sie dann auf **Resync rückwärts**.



Ab ONTAP 9.3 ist die SnapMirror Richtlinie der Beziehung auf festgelegt `MirrorAllSnapshots` Der SnapMirror Zeitplan ist auf festgelegt `None`.

Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, wird die SnapMirror-Richtlinie für die Beziehung auf festgelegt `DPDefault` Der SnapMirror Zeitplan ist auf festgelegt `None`.

9. Navigieren Sie auf der Seite Volumes zum Quell-Volumen, und vergewissern Sie sich, dass die erstellte SnapMirror Beziehung aufgeführt ist und der Beziehungsstatus lautet `Snapmirrored`.
10. Geben Sie auf dem Ziel-Cluster eine SnapMirror-Richtlinie und einen Zeitplan an, die der Sicherungskonfiguration der ursprünglichen SnapMirror Beziehung für die neue SnapMirror Beziehung entsprechen:
 - a. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
 - b. Wählen Sie die SnapMirror Beziehung zwischen den reaktivierten Quell- und den Ziel-Volumen aus und klicken Sie dann auf **Bearbeiten**.
 - c. Wählen Sie die SnapMirror-Richtlinie und den Zeitplan aus, und klicken Sie dann auf **OK**.

Ergebnisse

Das Quell-Volumen hat Lese-/Schreibzugriff und ist durch das Ziel-Volumen geschützt.

Vorbereitung der Volume Disaster Recovery

Überblick über die Vorbereitung der Volume Disaster Recovery

Zur Vorbereitung auf die Disaster Recovery können Sie ein Quell-Volumen auf einem ONTAP Cluster mit Peering schnell schützen. Sie sollten dieses Verfahren verwenden,

wenn Sie SnapMirror Beziehungen zwischen Peering Clustern für die Disaster Recovery von Volumes konfigurieren und überwachen möchten und keine großen konzeptionellen Hintergrundinformationen für diese Aufgaben benötigen.

SnapMirror bietet asynchrone Datensicherung auf Blockebene in Planung. SnapMirror repliziert Snapshot Kopien und kann NAS- oder SAN-Volumes replizieren, auf denen Deduplizierung, Datenkomprimierung oder beides ausgeführt wird – einschließlich Volumes mit qtrees und LUNs. SnapMirror Konfigurationsinformationen werden in einer Datenbank gespeichert, die ONTAP auf alle Knoten im Cluster repliziert.

Verwenden Sie diese Vorgehensweise, wenn Sie SnapMirror Beziehungen für die Disaster Recovery auf Volume-Ebene folgendermaßen erstellen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung konfiguriert.

["Konfiguration des Cluster- und SVM-Peering"](#)

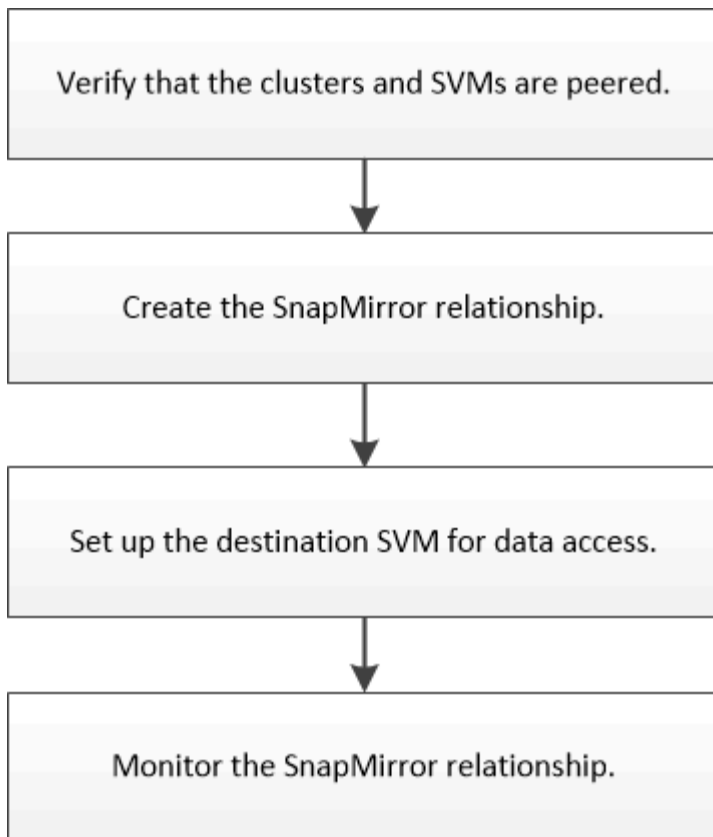
- Sie haben die SnapMirror Lizenz sowohl auf dem Quell- als auch auf den Ziel-Clustern aktiviert.
- Sie möchten Standardrichtlinien und -Zeitpläne verwenden und keine benutzerdefinierten Richtlinien erstellen.
- Sie möchten Best Practices verwenden, nicht alle verfügbaren Optionen erkunden (ONTAP 9.7 und älter).

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Siehe...
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Bereiten Sie sich auf Spiegelung und Vaulting vor"
Die ONTAP Befehlszeilenschnittstelle	"Cluster-Peer-Beziehung erstellen (ONTAP 9.3 und höher)"

Volume Workflow zur Vorbereitung der Disaster Recovery

Bei der Vorbereitung von Volumes für Disaster Recovery müssen die Cluster-Peer-Beziehung überprüft werden, die SnapMirror Beziehung zwischen Volumes auf Peering-Clustern erstellt, Ziel-SVM für den Datenzugriff festgelegt und die SnapMirror Beziehung regelmäßig überwacht werden.



Es stehen zusätzliche Dokumentation zur Verfügung, mit denen Sie das Ziel-Volume aktivieren können, um die Disaster Recovery-Einrichtung zu testen oder im Falle eines Ausfalls zu helfen. Weitere Informationen zur Reaktivierung des Quell-Volumes nach einem Ausfall finden Sie im Artikel.

Volume Disaster Recovery

+ Beschreibt, wie ein Ziel-Volume nach einem Ausfall schnell aktiviert und dann das Quell-Volume in ONTAP reaktiviert wird.

Überprüfung der Cluster-Peer-Beziehung und der SVM-Peer-Beziehung

Bevor Sie ein Volume für die Disaster Recovery einrichten, müssen Sie sicherstellen, dass die Quell- und Ziel-Cluster Peering durchgeführt werden und über die Peer-Beziehung miteinander kommunizieren.

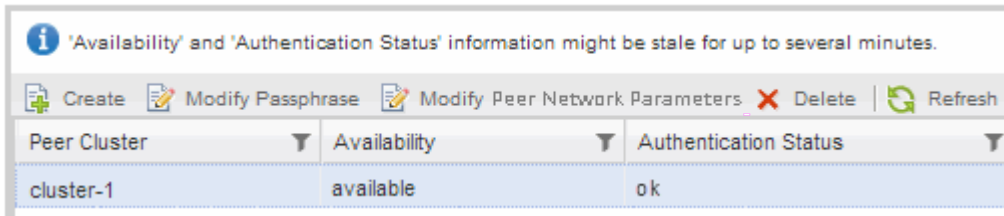
Verfahren

- Wenn ONTAP 9.3 oder höher ausgeführt wird, führen Sie die folgenden Schritte aus, um die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:
 - a. Klicken Sie Auf **Konfiguration > Cluster Peers**.
 - b. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.

<input checked="" type="checkbox"/>	Peer Cluster	Availability	Authentication Status	Local Cluster IPspace	Peer Cluster Intercluster IP Addresses	Last Updated Time
<input checked="" type="checkbox"/>	cluster2	Available	Ok	Default	10.237.213.119, 10.237.213.127	Nov 27, 2017, 2:13 PM

- c. Klicken Sie auf **Konfiguration > SVM-Peers**.

- d. Vergewissern Sie sich, dass die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.
- Wenn Sie ONTAP 9.2 oder eine frühere Version ausführen, führen Sie die folgenden Schritte aus, um die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:
 - a. Klicken Sie auf die Registerkarte **Konfigurationen**.
 - b. Klicken Sie im Fensterbereich **Cluster Details** auf **Cluster Peers**.
 - c. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.



Peer Cluster	Availability	Authentication Status
cluster-1	available	ok

- d. Klicken Sie auf die Registerkarte **SVMs** und wählen Sie die Quell-SVM aus.
- e. Überprüfen Sie im Bereich **Peer Storage Virtual Machines**, ob die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.

Wenn in diesem Bereich keine Peered SVM angezeigt wird, können Sie beim Erstellen der SnapMirror Beziehung die SVM-Peer-Beziehung erstellen.

Erstellung der SnapMirror Beziehung (ONTAP 9.2 oder älter)

SnapMirror Beziehung erstellen (beginnend mit ONTAP 9.3)

Sie müssen eine SnapMirror Beziehung zwischen dem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering Cluster erstellen, um die Daten für Disaster Recovery zu replizieren.

Bevor Sie beginnen

- Das Zielaggregat muss über verfügbaren Platz verfügen.
- Beide Cluster müssen entsprechend konfiguriert und eingerichtet werden, um die Anforderungen Ihrer Umgebung für Benutzerzugriff, Authentifizierung und Client-Zugriff zu erfüllen.


Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie Auf **Storage > Volumes**.
2. Wählen Sie das Volume aus, für das Sie eine Spiegelbeziehung erstellen möchten, und klicken Sie dann auf **Aktionen > schützen**.
3. Wählen Sie im Abschnitt **Beziehungstyp** aus der Dropdown-Liste **Beziehungstyp** die Option **Spiegel** aus.
4. Geben Sie auf der Seite **Bände: Protect Volumes** folgende Informationen ein:
 - a. Wählen Sie als Beziehungstyp * Mirror* aus.
 - b. Wählen Sie das Ziel-Cluster, die Ziel-SVM und das Suffix für den Namen des Ziel-Volume aus.

Es werden nur Peering SVMs und erlaubte SVMs unter Ziel-SVMs aufgeführt.

- c. Klicken Sie Auf .
- d. Überprüfen Sie das im Dialogfeld **Erweiterte Optionen** MirrorAllSnapshots Wird als Sicherungsrichtlinie festgelegt.

DPDefault Und MirrorLatest Die anderen standardmäßigen Sicherungsrichtlinien für SnapMirror Beziehungen sind verfügbar.

- e. Wählen Sie einen Schutzzeitplan aus.

Standardmäßig wird der verwendet hourly Der Zeitplan ist ausgewählt.

- f. Vergewissern Sie sich, dass **Ja** zur Initialisierung der SnapVault-Beziehung ausgewählt ist.

Alle Datensicherungsbeziehungen werden standardmäßig initialisiert. Durch Initialisieren der SnapMirror Beziehung wird sichergestellt, dass das Ziel-Volume über eine Baseline zum Sichern des Quell-Volume verfügt.

- g. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Advanced Options ✕

Protection Policy MirrorAllSnapshots ▼

SnapMirror Labels	Retention Count
sm_created	1
all_source_snapshots	1

Protection Schedule hourly ▼

Every hour at 05 minute(s)

i Initialize Protection Yes No

i SnapLock for SnapVault SnapLock for SnapVault is not supported for the selected destination or the selected relationship type.

i FabricPool There is no FabricPool assigned to the destination SVM.

Apply

5. Klicken Sie auf **Save**, um die SnapMirror Beziehung zu erstellen.
6. Vergewissern Sie sich, dass der Beziehungsstatus der SnapMirror-Beziehung im lautet Snapmirrored Bundesland.
- a. Navigieren Sie zum Fenster **Volumes** und wählen Sie dann den Datenträger aus, für den Sie die SnapMirror-Beziehung erstellt haben.

- b. Doppelklicken Sie auf das Volume, um die Volume-Details anzuzeigen, und klicken Sie dann auf **SCHUTZ**, um den Datenschutzstatus des Volumes anzuzeigen.



Nächste Schritte

Sie müssen die Einstellungen für das Quell-Volume wie Thin Provisioning, Deduplizierung, Komprimierung und Autogrow notieren. Sie können diese Informationen nutzen, um die Zielvolume-Einstellungen zu überprüfen, wenn Sie die SnapMirror-Beziehung unterbrechen.

SnapMirror Beziehung erstellen (ONTAP 9.2 oder älter)

Sie müssen eine SnapMirror Beziehung zwischen dem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering Cluster erstellen, um die Daten für Disaster Recovery zu replizieren.

Bevor Sie beginnen

- Sie müssen über den Benutzernamen und das Passwort des Cluster-Administrators für das Ziel-Cluster verfügen.
- Das Zielaggregat muss über verfügbaren Platz verfügen.
- Beide Cluster müssen entsprechend konfiguriert und eingerichtet werden, um die Anforderungen Ihrer Umgebung für Benutzerzugriff, Authentifizierung und Client-Zugriff zu erfüllen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie auf **Storage > SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Volumes**.
4. Wählen Sie das Volume aus, für das Sie eine Spiegelbeziehung erstellen möchten, und klicken Sie dann auf **Protect**.

Das Fenster Schutzbeziehung erstellen wird angezeigt.

5. Wählen Sie im Abschnitt **Beziehungstyp** aus der Dropdown-Liste **Beziehungstyp** die Option **Spiegel** aus.
6. Wählen Sie im Abschnitt **Zielvolume** den Peered Cluster aus.
7. Legen Sie die SVM für das Ziel-Volume fest:

Lautet die SVM...	Dann...
Peered	Wählen Sie aus der Liste die Peering SVM aus.

Lautet die SVM...	Dann...
Keine Peered	a. Wählen Sie die SVM aus. b. Klicken Sie Auf Authentifizieren . c. Geben Sie die Anmeldedaten des Clusteradministrators für den Peering Cluster ein, und klicken Sie dann auf Create .

8. Neues Ziel-Volume erstellen:

- Wählen Sie die Option **New Volume**.
- Verwenden Sie den Standard-Volume-Namen, oder geben Sie einen neuen Volume-Namen an.
- Wählen Sie das Zielaggregat aus.

Destination Volume

Cluster: cluster-1

Storage Virtual Machine: svm2(peered) [Browse...](#)

Volume: New Volume Select Volume

Volume name: svm1_svm1_root_mirror

Aggregate: aggr2 [Browse...](#)
387.19 GB available (of 390.21 GB)

Space Reserve (optional): Default

9. Wählen Sie im Abschnitt **Konfigurationsdetails** die Option **MirrorAllSnapshot** als Spiegelrichtlinie aus.

DPDefault Und MirrorLatest Sind die anderen standardmäßigen Spiegelungsrichtlinien, die für SnapMirror Beziehungen verfügbar sind.

10. Wählen Sie einen Schutzplan aus der Liste der Zeitpläne aus.

11. Stellen Sie sicher, dass das Kontrollkästchen **Beziehung initialisieren** aktiviert ist, und klicken Sie dann auf **Erstellen**.

Durch Initialisieren der SnapMirror Beziehung wird sichergestellt, dass das Ziel-Volume über eine Baseline zum Sichern des Quell-Volume verfügt.

Configuration Details

Mirror Policy: MirrorAllSnapshots [Browse...](#) [Create Policy](#)
SnapMirror labels: sm_created

Schedule: hourly [Browse...](#) [Create Schedule](#)
Every hour at 05 minute(s)

None

Initialize Relationship

Die Beziehung wird initialisiert durch einen Basistransfer der Daten vom Quell-Volume zum Ziel-Volume.

Der Initialisierungsvorgang kann einige Zeit in Anspruch nehmen. Im Abschnitt Status wird der Status jedes

Jobs angezeigt.

Create Protection Relationship

Source Volume

Cluster: cluster-1
Storage Virtual Machine: svm1
Volume: svm1_root { Used space 844 KB }

Destination Volume

Cluster: cluster-1
Storage Virtual Machine: svm2
Volume: svm1_svm1_root_mirror

Configuration Details

Mirror Policy: DPDefault
Schedule: hourly

Status

Create volume	✔ Completed successfully
Create relationship	✔ Completed successfully
Initialize relationship	✔ Started successfully

12. Überprüfen Sie den Beziehungsstatus der SnapMirror Beziehung:

- Wählen Sie das Volume aus, für das Sie die SnapMirror-Beziehung aus der Liste **Volumes** erstellt haben, und klicken Sie dann auf **Data Protection**.
- Überprüfen Sie auf der Registerkarte **Data Protection**, ob die von Ihnen erstellte SnapMirror-Beziehung aufgelistet ist und der Beziehungsstatus lautet `Snapmirrored`.

Nächste Schritte

Sie müssen die Einstellungen für das Quell-Volume wie Thin Provisioning, Deduplizierung, Komprimierung und Autogrow notieren. Sie können diese Informationen nutzen, um die Zielvolume-Einstellungen zu überprüfen, wenn Sie die SnapMirror-Beziehung unterbrechen.

Ziel-SVM für Datenzugriff einrichten

Sie können die Unterbrechung beim Datenzugriff minimieren, wenn Sie das Ziel-Volume aktivieren, indem Sie erforderliche Konfigurationen wie LIFs, CIFS-Freigaben und Exportrichtlinien für die NAS-Umgebung sowie LIFs und Initiatorgruppen für die SAN-Umgebung auf der SVM mit dem Ziel-Volume einrichten.

Über diese Aufgabe

Sie müssen diese Aufgabe auf dem **Ziel-Cluster** für die SVM mit dem Ziel-Volume ausführen.

Verfahren

- NAS-Umgebung:
 - a. Erstellen von NAS-LIFs
 - b. Erstellen Sie CIFS-Freigaben mit denselben Freigabenamen, die auf der Quelle verwendet wurden.
 - c. Erstellen Sie die entsprechenden NFS-Exportrichtlinien.
 - d. Geeignete Kontingentregeln erstellen.
- SAN-Umgebung:
 - a. Erstellung von SAN-LIFs.
 - b. **Optional:** Portsätze konfigurieren.
 - c. Konfigurieren von Initiatorgruppen.
 - d. Zonen Sie bei FC die FC-Switches, damit die SAN-Clients auf die LIFs zugreifen können.

Nächste Schritte

Wurden Änderungen an der SVM vorgenommen, die das Quell-Volume enthält, müssen die Änderungen manuell auf der SVM, die das Ziel-Volume enthält, repliziert werden.

Verwandte Informationen

["ONTAP 9 Dokumentationszentrum"](#)

Überwachen Sie den Status von SnapMirror Datentransfers

Sie sollten den Status der SnapMirror Beziehungen in regelmäßigen Abständen überwachen, um zu gewährleisten, dass die SnapMirror Datentransfers wie im angegebenen Zeitplan stattfinden.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
2. Wählen Sie die SnapMirror Beziehung zwischen dem Quell- und den Ziel-Volumes aus, und überprüfen Sie dann den Status auf der Registerkarte **Details** Bottom.

Die Registerkarte Details zeigt den Integritätsstatus der SnapMirror Beziehung sowie die Übertragungsfehler und die Verzögerungszeit an.

- Das Feld ist in Zustand muss angezeigt werden `Yes`.

Für die meisten SnapMirror Datentransferfehler wird das Feld angezeigt `No`. In einigen Fehlerfällen wird das Feld jedoch weiterhin angezeigt `Yes`. Sie müssen die Übertragungsfehler im Abschnitt Details überprüfen, um sicherzustellen, dass keine Datenübertragung fehlgeschlagen ist.

- Das Feld „Beziehungsstatus“ muss angezeigt werden `Snapmirrored`.

- Die Verzögerung darf nicht länger als das Transferzeitintervall sein.

Wenn der Transfer-Zeitplan beispielsweise stündlich ist, darf die Verzögerungszeit nicht mehr als eine Stunde sein.

Sie sollten alle Probleme in den SnapMirror Beziehungen beheben.

["Technischer Bericht 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2"](#)

Source Location:	source_SVM_Vol1	Is Healthy:	Yes	Transfer Status:	Idle
Destination Location:	dest_SVM_source_SVM_Vol1	Relationship State:	Snapshotred	Current Transfer Type:	None
Source Cluster:	cluster-2	Network Compression Ratio:	Not Applicable	Current Transfer Error:	None
Destination Cluster:	cluster-1			Last Transfer Error:	None
Transfer Schedule:	hourly			Last Transfer Type:	Initialize
Data Transfer Rate:	Unlimited			Latest Snapshot Timestamp:	09/16/2014 23:42:24
Lag Time:	None			Latest Snapshot Copy:	snapminor:3e51ed5f-31a3-11e4-98c7-005056974d2d_2147464686.2014-09-16_233526

Volume Backup mit SnapVault

Volume Backup mit SnapVault – Übersicht

SnapVault-Backup-Beziehungen können schnell zwischen Volumes konfiguriert werden, die sich in unterschiedlichen Clustern befinden. Das SnapVault Backup enthält eine Reihe schreibgeschützter Backup-Kopien, die sich auf einem Ziel-Volume befinden und zur Wiederherstellung von Daten genutzt werden können, wenn Daten beschädigt oder verloren gehen.

Verwenden Sie diese Prozedur, wenn Sie SnapVault-Backup-Beziehungen für Volumes auf folgende Weise erstellen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung konfiguriert.

["Konfiguration des Cluster- und SVM-Peering"](#)

- Sie müssen entweder die SnapMirror oder die SnapVault Lizenz aktivieren, nachdem alle Nodes im Cluster auf dieselbe Version von ONTAP 9 aktualisiert wurden.
- Sie möchten standardmäßige Sicherungsrichtlinien und -Zeitpläne verwenden und keine benutzerdefinierten Richtlinien erstellen.
- Sie möchten keine Daten für eine einzelne Datei oder eine LUN-Wiederherstellung sichern.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.
- Sie möchten den System Manager verwenden, nicht die ONTAP Befehlszeilenschnittstelle oder ein automatisiertes Scripting Tool.

- Sie möchten die klassische Benutzeroberfläche des System Manager für ONTAP 9.7 und ältere Versionen verwenden, nicht die ONTAP System Manager Benutzeroberfläche für ONTAP 9.7 und höher.

Wenn diese Annahmen nicht für Ihre Situation geeignet sind oder wenn Sie mehr konzeptionelle Hintergrundinformationen wünschen, sollten Sie die folgende Ressource finden:

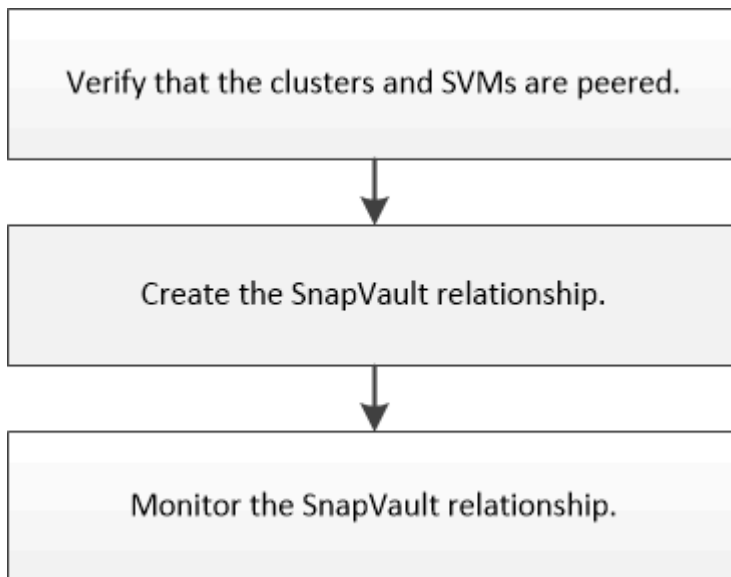
["Technischer Bericht 4183 zu SnapVault Best Practices"](#)

Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen...
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Konfigurieren von Spiegelungen und Vaults"
Die ONTAP Befehlszeilenschnittstelle	"Erstellen einer Replikationsbeziehung"

SnapVault Backup-Konfigurationsworkflow

Die Konfiguration einer SnapVault Backup-Beziehung umfasst die Überprüfung der Cluster Peer-Beziehung, die Erstellung der SnapVault Beziehung zwischen den Quell- und Ziel-Volumes und die Überwachung der SnapVault Beziehung.



Es steht zusätzliche Dokumentation zur Verfügung, mit der Sie Daten von einem Ziel-Volumen wiederherstellen können, um die gesicherten Daten zu testen oder wenn das Quell-Volumen verloren geht.

- [Management von Volume-Wiederherstellungen mit SnapVault](#)

Hier wird die schnelle Wiederherstellung eines Volumes aus einem SnapVault Backup in ONTAP beschrieben

Überprüfung der Cluster-Peer-Beziehung und der SVM-Peer-Beziehung

Bevor Sie ein Volume zur Datensicherung mit SnapVault Technologie einrichten, müssen Sie sicherstellen, dass das Quell-Cluster und das Ziel-Cluster Peered sind und über die

Peer-Beziehung miteinander kommunizieren. Es muss außerdem sichergestellt werden, dass die Quell-SVM und Ziel-SVM Peered sind und über die Peer-Beziehung miteinander kommunizieren.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

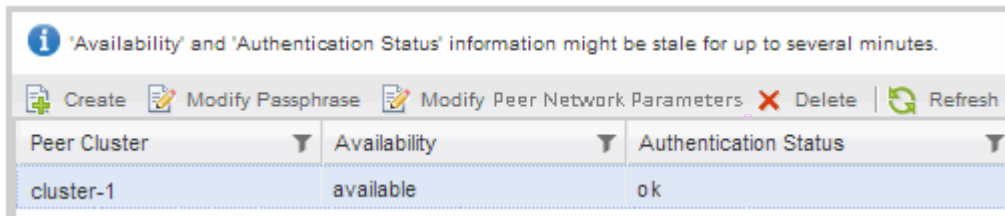
Verfahren

- Wenn ONTAP 9.3 oder höher ausgeführt wird, führen Sie die folgenden Schritte aus, um die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:
 - a. Klicken Sie Auf **Konfiguration > Cluster Peers**.
 - b. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.



<input checked="" type="checkbox"/>	Peer Cluster	Availability	Authentication Status	Local Cluster IPspace	Peer Cluster Intercluster IP Addresses	Last Updated Time
<input checked="" type="checkbox"/>	cluster2	Available	OK	Default	10.237.213.119, 10.237.213.127	Nov 27, 2017, 2:13 PM

- c. Klicken Sie auf **Konfiguration > SVM-Peers**.
 - d. Vergewissern Sie sich, dass die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.
- Wenn Sie ONTAP 9.2 oder eine frühere Version ausführen, führen Sie die folgenden Schritte aus, um die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung zu überprüfen:
 - a. Klicken Sie auf die Registerkarte **Konfigurationen**.
 - b. Klicken Sie im Fensterbereich **Cluster Details** auf **Cluster Peers**.
 - c. Vergewissern Sie sich, dass der Peering-Cluster authentifiziert und verfügbar ist.



<input type="checkbox"/>	Peer Cluster	Availability	Authentication Status
<input type="checkbox"/>	cluster-1	available	ok

- d. Klicken Sie auf die Registerkarte **SVMs** und wählen Sie die Quell-SVM aus.
- e. Überprüfen Sie im Bereich **Peer Storage Virtual Machines**, ob die Ziel-SVM mit der Quell-SVM Peering durchgeführt wird.

Wenn in diesem Bereich keine gleichgesinnten SVMs angezeigt werden, können Sie beim Erstellen der SnapVault-Beziehung die SVM-Peer-Beziehung erstellen.

[Erstellung der SnapVault Beziehung \(ONTAP 9.2 oder älter\)](#)

SnapVault-Beziehung erstellen (beginnend mit ONTAP 9.3)

Sie müssen eine SnapVault-Beziehung zwischen dem Quell-Volumen auf einem Cluster und dem Ziel-Volumen auf dem Peering Cluster erstellen, um ein SnapVault Backup zu erstellen.

Bevor Sie beginnen

- Sie müssen über den Benutzernamen und das Passwort des Cluster-Administrators für das Ziel-Cluster verfügen.
- Das Zielaggregat muss über verfügbaren Platz verfügen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie Auf **Storage > Volumes**.
2. Wählen Sie das Volumen aus, das Sie sichern möchten, und klicken Sie dann auf **Aktionen > Schützen**.


Es können auch mehrere Quell-Volumes ausgewählt und SnapVault Beziehungen mit einem einzelnen Ziel-Volume erstellt werden.

3. Geben Sie auf der Seite **Bände: Protect Volumes** folgende Informationen ein:

- a. Wählen Sie in der Dropdown-Liste **Beziehungstyp** * * * die Option **Vault** aus.
- b. Wählen Sie das Ziel-Cluster, Ziel-SVM und das Suffix für das Ziel-Volume aus.

Unter den Ziel-SVMs werden nur Peered SVMs und erlaubte SVMs aufgeführt.

Das Ziel-Volume wird automatisch erstellt. Der Name des Ziel-Volumes ist der Name des Quell-Volumes, der mit dem Suffix angehängt ist.

- a. Klicken Sie Auf .
- b. Überprüfen Sie im Dialogfeld **Erweiterte Optionen**, ob die **Schutzrichtlinie** als festgelegt ist `XDPDefault`.
- c. Wählen Sie den **Schutzplan** aus.

Standardmäßig wird der verwendet `daily` Der Zeitplan ist ausgewählt.

- d. Vergewissern Sie sich, dass **Ja** zur Initialisierung der SnapVault-Beziehung ausgewählt ist.

Alle Datensicherungsbeziehungen werden standardmäßig initialisiert.

- e. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Advanced Options



Protection Policy XDPDefault

SnapMirror Labels	Retention Count
daily	7
weekly	52

Protection Schedule daily

Every Night at 0:10 AM

i Initialize Protection Yes
 No

i SnapLock for SnapVault There are no SnapLock aggregates assigned to the destination SVM.

i FabricPool There is no FabricPool assigned to the destination SVM.

Apply

4. Klicken Sie auf der Seite **Volumes: Protect Volumes** auf **Validate**, um zu überprüfen, ob die Volumes mit den SnapMirror-Labels übereinstimmen.
5. Klicken Sie auf **Speichern**, um die SnapVault-Beziehung zu erstellen.
6. Vergewissern Sie sich, dass der Status der SnapVault-Beziehung im angezeigt wird `SnapshotMirrored` Bundesland.
 - a. Navigieren Sie zum Fenster **Volumes**, und wählen Sie dann das gesicherte Volume aus.
 - b. Erweitern Sie den Datenträger und klicken Sie auf **PROTECTION**, um den Datenschutzstatus des Volumes anzuzeigen.

Volumes on SVM All SVMs

Volume: vol_src [Back to All volumes](#) [Edit](#) [Cancel](#) [Actions](#) [Refresh](#)

Overview Snapshots Copies **Data Protection** Storage Efficiency Performance

[Refresh](#)

Health	Destination SVM	Destination Volume	Destination Clu...	Relationsh...	Transfer S...	Type	Lag Time	Policy
	vst	vol_src_dst	cluster1	SnapshotMirrored	SBF	Vault	29 min()	XDPDefault

SnapVault Beziehung erstellen (ONTAP 9.2 oder älter)

Sie müssen eine SnapVault-Beziehung zwischen dem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering Cluster erstellen, um ein SnapVault Backup zu erstellen.

Bevor Sie beginnen

- Sie müssen über den Benutzernamen und das Passwort des Cluster-Administrators für das Ziel-Cluster verfügen.
- Das Zielaggregat muss über verfügbaren Platz verfügen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Klicken Sie auf **Storage > SVMs**.
2. Wählen Sie die SVM aus, und klicken Sie dann auf **SVM Settings**.
3. Klicken Sie auf die Registerkarte **Volumes**.
4. Wählen Sie das Volumen aus, das Sie sichern möchten, und klicken Sie dann auf **schützen**.
5. Wählen Sie im Dialogfeld **Schutzbeziehung erstellen** aus der Dropdown-Liste **Beziehungstyp** die Option **Vault** aus.
6. Wählen Sie im Abschnitt **Zielvolume** den Peered Cluster aus.
7. Legen Sie die SVM für das Ziel-Volume fest:

Lautet die SVM...	Dann...
Peered	Wählen Sie aus der Liste die Peering SVM aus.
Keine Peered	<ol style="list-style-type: none"> a. Wählen Sie die SVM aus. b. Klicken Sie Auf Authentifizieren. c. Geben Sie die Anmeldedaten des Clusteradministrators für den Peering Cluster ein, und klicken Sie dann auf Create.

8. Neues Ziel-Volume erstellen:
 - a. Wählen Sie die Option **New Volume**.
 - b. Verwenden Sie den Standardnamen für das Volume, oder geben Sie einen neuen Volume-Namen ein.
 - c. Wählen Sie das Zielaggregat aus.
 - d. Vergewissern Sie sich, dass das Kontrollkästchen **Enable Dedupe** aktiviert ist.

Destination Volume

Cluster:

Storage Virtual Machine:

Volume: New Volume Select Volume

Volume name: Aggregate:

Enable dedupe 70.13 GB available (of 70.14 GB)

9. Wählen Sie im Abschnitt **Konfigurationsdetails** die Option **XDPDefault** Als Schutzrichtlinie.
10. Wählen Sie einen Schutzplan aus der Liste der Zeitpläne aus.
11. Stellen Sie sicher, dass das Kontrollkästchen **Beziehung initialisieren** aktiviert ist, um die Basis-Snapshot-Kopie zu übertragen, und klicken Sie dann auf **Erstellen**

Configuration Details

Vault Policy:
Snapshot with labels matching: daily, weekly

Schedule:
Every Sun at 0:15 am
 None

Initialize Relationship

Der Assistent erstellt die Beziehung zu der angegebenen Vault-Richtlinie und dem angegebenen Zeitplan. Die Beziehung wird initialisiert durch einen Basistransfer der Daten vom Quell-Volume zum Ziel-Volume.

Im Abschnitt Status wird der Status jedes Jobs angezeigt.

Create Protection Relationship [X]

Source Volume

Cluster: cluster-1
 Storage Virtual Machine: svm1
 Volume: vol_2 { Used space 292 KB }

Destination Volume

Cluster: cluster-1
 Storage Virtual Machine: vs0
 Volume: svm1_vol_2_vault

Configuration Details

Vault Policy: XDPDefault
 Schedule: weekly

Status

Create volume	✓ Completed successfully
Enable dedupe	✓ Completed successfully
Create relationship	✓ Completed successfully
Initialize relationship	✓ Started successfully

12. Vergewissern Sie sich, dass der Beziehungsstatus der SnapVault-Beziehung im angezeigt wird Snapmirrored Bundesland.

a. Wählen Sie das Volume aus der Liste Volumes aus und klicken Sie dann auf **Datenschutz**.

- b. Überprüfen Sie auf der Registerkarte **Data Protection** Bottom, ob die erstellte SnapMirror-Beziehung aufgelistet ist und der Beziehungsstatus lautet Snapmirrored Typ lautet Vault.

Name	Aggregate	Status	Thin Provi...	% Used	Available ...	Total Space	Storage Et...	Is Volume ...	Encrypted
svm1_root	aggr1	Online	No	5	979.56 MB	1 GB	Disabled	No	No
svm2_svm1_...	aggr2	Online	No	5	121.36 MB	128.92 MB	Enabled	No	No
vol1	aggr2	Online	No	0	1017.7 MB	1 GB	Disabled	No	No
vol123	aggr1	Online	Yes	5	1.9 GB	2 GB	Disabled	Yes	No

Destination Store...	Destination Volu...	Is Healthy	Relationship State	Transfer Status	Type	Lag Time	Policy
svm2	svm1_vol123_vault	Yes	Snapmirrored	Idle	Vault	4 hr(s) 21 min(s)	XDPDefault

Details Space Allocation Snapshot Copies Storage Efficiency **Data Protection** Volume Move Deta Performance

Überwachen der SnapVault Beziehung

Sie sollten den Status der SnapVault-Beziehungen regelmäßig überwachen, um sicherzustellen, dass die Daten gemäß dem festgelegten Zeitplan auf dem Ziel-Volume gesichert werden.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

- Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
- Wählen Sie die SnapVault-Beziehung zwischen Quell- und Ziel-Volumes aus, und überprüfen Sie dann den Status auf der Registerkarte **Details** Bottom.

Der Integritätsstatus der SnapVault-Beziehung, alle Übertragungsfehler und die Verzögerungszeit werden angezeigt:

- Das Feld ist in Zustand muss angezeigt werden **Yes**.

Bei den meisten Datenübertragungsfehlern wird das Feld angezeigt **No**. In einigen Fehlerfällen wird das Feld jedoch weiterhin angezeigt **Yes**. Sie müssen die Übertragungsfehler im Abschnitt **Details** überprüfen, um sicherzustellen, dass keine Datenübertragung fehlgeschlagen ist.

- Das Feld „Beziehungsstatus“ muss angezeigt werden **Snapmirrored**.
- Die Verzögerung darf nicht größer sein als das Transferplanintervall.

Wenn der Transferzeitplan z. B. täglich ist, darf die Verzögerungszeit nicht mehr als einen Tag lang sein.

Sie sollten Probleme in den SnapVault Beziehungen beheben. Die Fehlerbehebungsschritte für SnapMirror Beziehungen gelten auch für SnapVault Beziehungen.

Source Sv...	Source V...	Destinati...	Destinati...	Is Healthy	Relations...	Transfer...	Relationshi...	Lag Time	Policy Na...	Policy Type
svm1	svm1_root	svm1_svm1...	svm2	Yes	Snapmirror...	Idle	Mirror	33 min(s)	DPDefault	Asynchronous Mir...
svm1	vol123	svm1_vol12...	svm2	Yes	Snapmirror...	Idle	Vault	4 hr(s) 28 m...	XDPDefault	Vault

Source Location:	svm1:vol123	Is Healthy:	Yes	Transfer Status:	Idle
Destination Location:	svm2:svm1_vol123_vault	Relationship State:	Snapmirrored	Current Transfer Type:	None
Source Cluster:	cluster-1	Network Compression Ratio:	Not Applicable	Current Transfer Error:	None
Destination Cluster:	cluster-1			Last Transfer Error:	None
Transfer Schedule:	daily			Last Transfer Type:	Update
Data Transfer Rate:	Unlimited			Latest Snapshot Timestamp:	02/28/2017 00:10:00
Lag Time:	4 hr(s) 28 min(s)			Latest Snapshot Copy:	daily:2017-02-28_0010

Management von Volume-Wiederherstellungen mit SnapVault

Volume-Wiederherstellung mithilfe von SnapVault – Übersicht

Sie können bei einem Datenverlust ein Volume aus einem SnapVault Backup in ONTAP schnell wiederherstellen.

Gehen Sie folgendermaßen vor, wenn Sie die Daten aus der Sicherungskopie wiederherstellen möchten:

- Sie arbeiten mit Clustern, auf denen ONTAP 9 ausgeführt wird.
- Sie sind ein Cluster-Administrator.
- Sie haben die Vault-Beziehung gemäß dem in beschriebenen Verfahren konfiguriert [Volume Backup mit SnapVault](#)
- Sie möchten keine einzelne Datei oder kein LUN-Restore durchführen.
- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie wollen nicht viel konzeptuellen Hintergrund lesen.
- Sie möchten die klassische Benutzeroberfläche des System Manager für ONTAP 9.7 und ältere Versionen verwenden, nicht die ONTAP System Manager Benutzeroberfläche für ONTAP 9.7 und höher.

Wenn diese Annahmen nicht für Ihre Situation geeignet sind oder wenn Sie mehr konzeptionelle Hintergrundinformationen wünschen, sollten Sie die folgende Ressource finden:

["Technischer Bericht 4183 zu SnapVault Best Practices"](#)

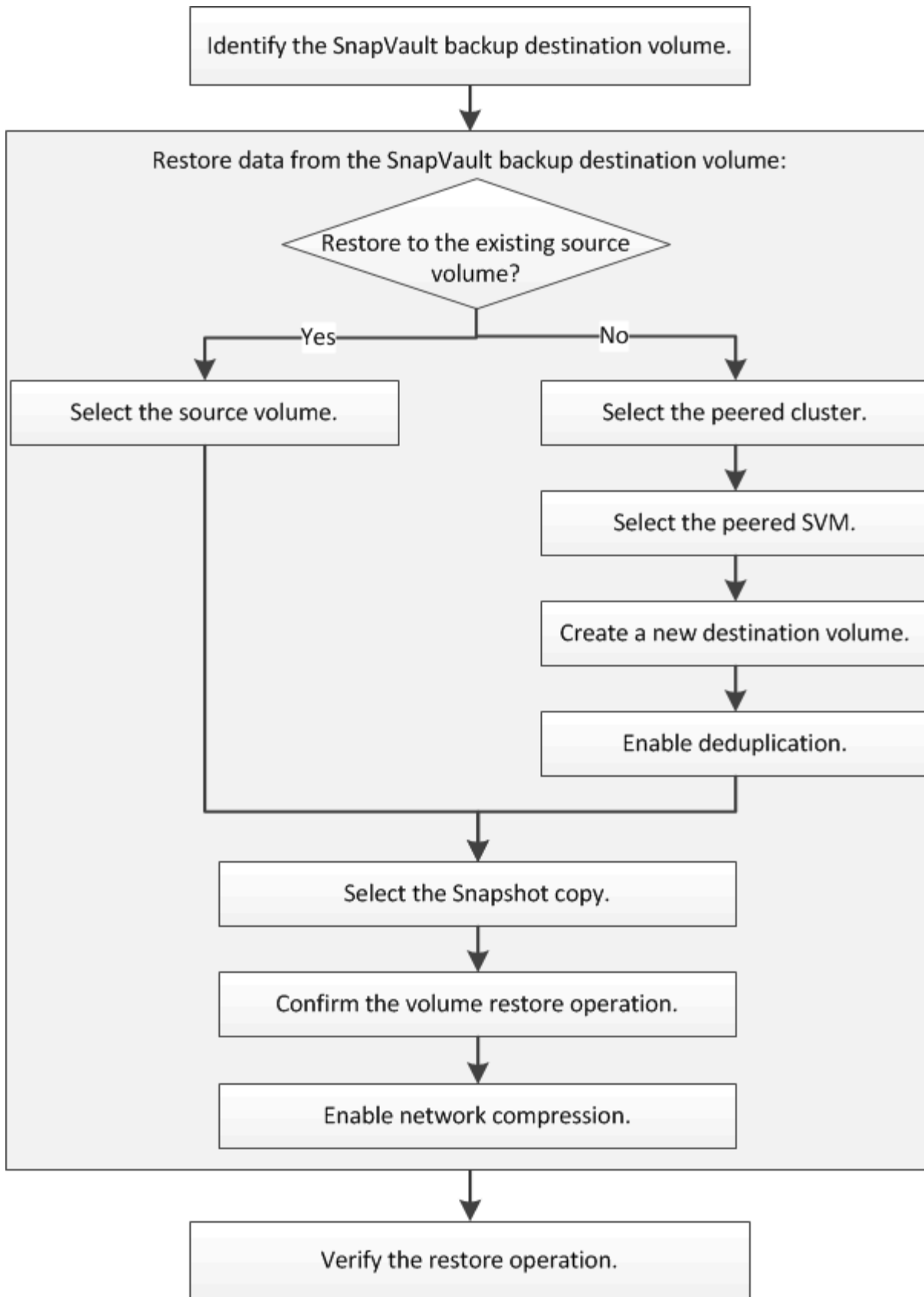
Weitere Möglichkeiten dies in ONTAP zu tun

So führen Sie diese Aufgaben durch:	Inhalt anzeigen...
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Wiederherstellung eines Volume aus einer früheren Snapshot Kopie"

So führen Sie diese Aufgaben durch:	Inhalt anzeigen...
Die ONTAP Befehlszeilenschnittstelle	"Stellen Sie den Inhalt eines Volumes von einem SnapMirror-Ziel wieder her"

Workflow zur Volume-Wiederherstellung

Falls Ihr Quell-Volume nicht verfügbar ist oder Daten beschädigt werden, können Sie die Wiederherstellung aus einem SnapVault Backup durchführen. Zur Wiederherstellung eines Volumes aus einem SnapVault Backup muss das SnapVault Ziel-Volume ausgewählt, entweder auf einem neuen Volume oder auf einem vorhandenen Volume wiederhergestellt und der Restore-Vorgang überprüft werden.



Weitere Informationen stehen Ihnen zum Management der SnapVault Backup-Beziehungen und zur Nutzung anderer Datensicherungsmethoden zur Verfügung, mit denen Sie die Verfügbarkeit Ihrer Datenressourcen sichern können.

- [Vorbereitung der Volume Disaster Recovery](#)

Beschreibt die schnelle Konfiguration eines Ziel-Volumes auf einem anderen ONTAP Cluster zur Vorbereitung der Disaster Recovery.

- [Volume Disaster Recovery](#)

Beschreibt die schnelle Aktivierung eines Ziel-Volumes aus einem anderen ONTAP Cluster nach einem Ausfall sowie die Wiederherstellung der SnapMirror Beziehung in den ursprünglichen Zustand durch erneute Aktivierung des Quell-Volume nach der Wiederherstellung.

Ermitteln des Ziel-Volume für das SnapVault Backup

Sie müssen das SnapVault Backup-Ziel-Volume identifizieren, von dem Sie Daten wiederherstellen möchten, wenn die Daten im Quell-Volume beschädigt sind oder verloren gehen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Geben Sie die URL ein `https://IP-address-of-cluster-management-LIF` Melden Sie sich in einem Webbrowser bei System Manager mit den Anmeldedaten für den Cluster-Administrator an.
2. Navigieren Sie zum Fenster **Volumes**.
3. Identifizieren des Ziel-Volume in der SnapVault Beziehung und des Namens der SVM, die den Volume enthält:
 - ONTAP 9.3 oder höher: Doppelklicken Sie auf den Datenträger, um die Details anzuzeigen, und klicken Sie dann auf **SCHUTZ**.
 - ONTAP 9.2 oder früher: Klicken Sie auf die Registerkarte **Datenschutz** unten im Fenster Volumen.

Wiederherstellung von Daten aus einem SnapVault-Backup

Nach Auswahl des SnapVault Backup-Ziel-Volume müssen Sie die Wiederherstellung entweder auf einem neuen Volume durchführen, um die gesicherten Daten zu testen, oder auf einem vorhandenen Volume, um die verlorenen oder beschädigten Daten wiederherzustellen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **Ziel** ausführen.

Schritte

1. Führen Sie je nach der verwendeten System Manager-Version einen der folgenden Schritte aus:
 - ONTAP 9.4 oder früher: Klicken Sie **Schutz > Beziehungen**.
 - Ab ONTAP 9.5: Klicken Sie **Schutz > Volume Relationships**.
2. Wählen Sie die SVM aus, die das Ziel-Volume für SnapVault-Backups enthält, und klicken Sie dann auf **Operationen > Wiederherstellen**.
3. Stellen Sie im Dialogfeld **Restore** die Daten auf dem ursprünglichen Quell-Volume oder einem neuen Volume wieder her:

Möchten Sie wiederherstellen auf...	Dann...
Das ursprüngliche Quell-Volumen	Wählen Sie Quellvolumen .
Ein neues Volume	<p>a. Wählen Sie anderes Volumen.</p> <p>b. Wählen Sie das Peering Cluster und die Peering SVM für das Volume aus.</p> <p>c. Wählen Sie aus der Liste eine Peering SVM aus.</p> <p>d. Wenn keine Peering-Punkte der SVM sind, erstellen Sie die SVM-Peer-Beziehung:</p> <ul style="list-style-type: none"> i. Wählen Sie die SVM aus. ii. Klicken Sie Auf Authentifizieren. iii. Geben Sie die Anmeldedaten des Clusteradministrators für den Peering Cluster ein, und klicken Sie dann auf Create. <p>e. Wählen Sie Neues Volume.</p> <p>f. Wenn Sie den Standardnamen ändern möchten, wird im Format angezeigt destination_SVM_name_destination_volume_name_restore, Geben Sie einen neuen Namen an und wählen Sie das zugehörige Aggregat für das Volume aus.</p> <p>g. Aktivieren Sie das Kontrollkästchen Deduplizierung aktivieren.</p>

Restore to _____

Source volume Other volume

Cluster:

Storage Virtual Machine:

Volume: New Volume Select Volume

Volume name: Aggregate:

Enable dedupe 517.22 GB available (of 520.28 GB)

4. Wählen Sie entweder die neueste Snapshot Kopie oder wählen Sie eine bestimmte Snapshot Kopie aus, die Sie wiederherstellen möchten.
5. Aktivieren Sie das Kontrollkästchen **OK, um das Volume aus der Snapshot-Kopie wiederherzustellen**.
6. Aktivieren Sie das Kontrollkästchen **Netzwerkkomprimierung aktivieren**, um die Daten zu komprimieren, die während des Wiederherstellungsvorgangs übertragen werden.
7. Klicken Sie Auf **Wiederherstellen**.

Während der Wiederherstellung wird das wiederherzustellende Volume in schreibgeschützt geändert. Nachdem der Wiederherstellungsvorgang abgeschlossen ist, wird die temporäre Beziehung entfernt und

das wiederhergestellte Volume wird in Lesen/Schreiben geändert.



8. Klicken Sie im Nachrichtefeld auf **OK**.

Überprüfen Sie den Wiederherstellungsvorgang

Nachdem Sie den Wiederherstellungsvorgang vom SnapVault Backup-Ziel-Volume durchgeführt haben, müssen Sie den Status des Wiederherstellungsvorgangs im Quell-Cluster überprüfen.

Über diese Aufgabe

Sie müssen diese Aufgabe aus dem Cluster **source** ausführen.

Schritte

1. Navigieren Sie zum Fenster **Volumes**.
2. Wählen Sie in der Liste Volumes das Quell-Volume aus und führen Sie abhängig von Ihrer ONTAP-Version eine der folgenden Aktionen durch:
 - Ab ONTAP 9.3: Doppelklicken Sie auf das Quell-Volume, um die Details anzuzeigen, und klicken Sie dann auf **PROTECTION**, um das Ziel-Volume in der SnapMirror-Beziehung und den Namen der SVM zu identifizieren, die das Volume enthält.
 - ONTAP 9.2 oder früher: Klicken Sie auf die Registerkarte **Data Protection** bottom, um das Ziel-Volume in der SnapMirror Beziehung und den Namen der SVM zu identifizieren, die das Volume enthält. Das Feld Typ wird angezeigt `Restore` Vorübergehend. Nach Abschluss des Wiederherstellungsvorgangs wird das Feld angezeigt `Vault`.

Sie sollten Probleme in den SnapVault Beziehungen beheben. Die Fehlerbehebungsschritte für SnapMirror Beziehungen gelten auch für SnapVault Beziehungen.

["Technischer Bericht 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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