Datensicherung und Disaster Recovery

ONTAP 9

NetApp
April 24, 2024

Inhalt

Datensicherung und Disaster Recovery

Datensicherung mit System Manager

Datensicherung mit System Manager im Überblick

Die Themen in diesem Abschnitt zeigen Ihnen, wie Sie Datensicherung mit System Manager in ONTAP 9.7 und neueren Versionen konfigurieren und managen.

Wenn Sie System Manager in ONTAP 9.7 oder früher verwenden, lesen Sie "Klassische Dokumentation des ONTAP System Manager"

Schützen Sie die Daten, indem Sie Snapshot Kopien, Spiegelungen, Vaults und Spiegel-und Vault-Beziehungen erstellen und managen.

SnapMirror ist eine Disaster Recovery-Technologie für den Failover von primärem Storage zu sekundärem Storage an einem geografisch verteilten Standort. Wie der Name schon sagt, erstellt SnapMirror eine Spiegelung Ihrer Arbeitsdaten im sekundären Storage, von dem aus Sie im K-Fall am primären Standort weiterhin Daten bereitstellen können.

A *Vault* wurde für Disk-to-Disk Snapshot Kopien zur Replizierung entwickelt, um Compliance-Standards und andere Governance-bezogene Zwecke zu erfüllen. Im Gegensatz zu einer SnapMirror Beziehung, in der das Ziel normalerweise nur die derzeit im Quell-Volume befindlichen Snapshot-Kopien enthält, speichert ein Vault-Ziel in der Regel zeitpunktgenaue Snapshot-Kopien, die über einen längeren Zeitraum erstellt wurden.

Ab ONTAP 9.10.1 können Sie Datensicherungsbeziehungen zwischen S3 Buckets mithilfe von S3 SnapMirror erstellen. Ziel-Buckets können sich auf lokalen oder Remote-ONTAP Systemen oder auf Systemen anderer Anbieter wie StorageGRID und AWS befinden. Weitere Informationen finden Sie unter "Übersicht über S3 SnapMirror".

Erstellen benutzerdefinierter Datensicherungsrichtlinien

Sie können in System Manager benutzerdefinierte Datensicherungsrichtlinien erstellen, wenn die vorhandenen Standardrichtlinien nicht für Ihre Anforderungen geeignet sind. Ab ONTAP 9.11.1 können Sie mit System Manager benutzerdefinierte Spiegelungs- 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.

Schritte

1. Klicken Sie Auf **Schutz > Lokale Richtlinieneinstellungen**.
2. Klicken Sie unter **Schutzrichtlinien** auf →.
3. Klicken Sie im Fensterbereich **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.

Konfigurieren von Snapshot Kopien

Sie können Richtlinien für Snapshot Kopien erstellen, um die maximale Anzahl an Snapshot Kopien anzugeben, die automatisch erstellt werden und wie oft sie erstellt werden. Die Richtlinie gibt an, wann Snapshot Kopien erstellt werden sollen, wie viele Kopien aufzubewahren sind und wie sie benannt werden.

Durch dieses Verfahren wird nur im lokalen Cluster eine Snapshot Kopie-Richtlinie erstellt.

Schritte

1. Klicken Sie Auf **Schutz > Übersicht > Lokale Richtlinieneinstellungen**.
2. Klicken Sie unter **Snapshot Policies** auf →, Und klicken Sie dann auf + Add .
3. Geben Sie den Richtliniennamen ein, wählen Sie den Richtlinienumfang aus, und klicken Sie unter **Zeitpläne** auf + Add Um die Terminplandetails einzugeben.

Berechnen Sie den nicht anforderbaren Speicherplatz, bevor Sie Snapshot Kopien löschen

Ab ONTAP 9.10.1 können Sie mit System Manager Snapshot Kopien 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 Snapshot Kopien löschen möchten.
3. Klicken Sie Auf **Snapshot Kopien**.
4. Wählen Sie eine oder mehrere Snapshot Kopien aus.
5. Klicken Sie Auf **Speicherplatz Berechnen**.

Aktivieren oder Deaktivieren des Client-Zugriffs auf das Verzeichnis der Snapshot Kopie

Ab ONTAP 9.10.1 können Sie mit System Manager Client-Systeme für den Zugriff auf ein Snapshot Kopie-Verzeichnis auf einem Volume aktivieren oder deaktivieren. Durch die Aktivierung des Zugriffs wird das Verzeichnis der Snapshot Kopie für Clients sichtbar. Windows Clients können ein Laufwerk dem Snapshot Kopien-Verzeichnis zuordnen, um seine Inhalte anzuzeigen und darauf zuzugreifen.

Sie können den Zugriff auf das Snapshot-Kopierverzeichnis eines Volumes aktivieren oder deaktivieren, indem Sie die Volume-Einstellungen bearbeiten oder die Freigabereinstellungen des Volumes bearbeiten.

Aktivieren oder deaktivieren Sie den Client-Zugriff auf das Verzeichnis der Snapshot-Kopien, indem Sie ein Volume bearbeiten

Das Verzeichnis der Snapshot-Kopie auf einem Volume ist standardmäßig für Clients verfügbar.

Schritte

1. Klicken Sie Auf **Storage > Volumes**.
2. Wählen Sie das Volume mit dem Verzeichnis Snapshot Kopien aus, das Sie anzeigen oder ausblenden möchten.
3. Klicken Sie Auf ⋮ Und wählen Sie **Bearbeiten**.
4. Wählen Sie im Abschnitt **Snapshot Kopien (Local) Settings** die Option oder deaktivieren Sie **das Verzeichnis der Snapshot Kopien für Clients anzeigen**.
5. Klicken Sie Auf **Speichern**.

Aktivieren oder deaktivieren Sie den Client-Zugriff auf das Verzeichnis der Snapshot-Kopie, indem Sie eine Freigabe bearbeiten

Das Verzeichnis der Snapshot-Kopie auf einem Volume ist standardmäßig für Clients verfügbar.

Schritte

1. Klicken Sie Auf **Storage > Shares**.
2. Wählen Sie das Volume mit dem Verzeichnis Snapshot Kopien aus, das Sie anzeigen oder ausblenden möchten.
3. Klicken Sie Auf ⋮ Und wählen Sie **Bearbeiten**.
4. Wählen Sie im Abschnitt **Share Properties** die Option **allow Clients to Access Snapshot Copies Directory** aus.
5. Klicken Sie Auf **Speichern**.

Bereiten Sie sich auf Spiegelung und Vaulting vor

Die Daten werden gesichert, indem sie zu Backup- und Disaster Recovery-Zwecken auf ein Remote-Cluster repliziert werden.

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

Schritte

1. Klicken Sie im lokalen Cluster auf **Schutz > Übersicht**.
2. Erweitern Sie **Intercluster-Einstellungen**. Klicken Sie auf **Netzwerkschnittstellen hinzufügen** und fügen Sie Intercluster-Netzwerkschnittstellen für den Cluster hinzu.

Wiederholen Sie diesen Schritt auf dem Remote-Cluster.

3. Klicken Sie im Remote-Cluster auf **Schutz > Übersicht**. Klicken Sie Auf ⋮ Klicken Sie im Abschnitt Cluster Peers auf **Passphrase generieren**.
4. Kopieren Sie die generierte Passphrase, und fügen Sie sie in das lokale Cluster ein.
5. Klicken Sie im lokalen Cluster unter Cluster Peers auf **Peer Clusters** und führen Sie die lokalen und Remote Cluster aus.
6. Klicken Sie optional unter Storage VM Peers auf ⋮ Und dann **Peer Storage VMs** um die Speicher-VMs zu nutzen.
7. Klicken Sie auf **Volumes schützen**, um Ihre Volumes zu schützen. Um Ihre LUNs zu schützen, klicken Sie auf **Speicher > LUNs**, wählen Sie eine zu schützenden LUN aus, und klicken Sie dann auf Protect.

   Wählen Sie die Sicherungsrichtlinie auf der Grundlage der Art der Datensicherung aus, die Sie benötigen.

8. Um zu überprüfen, ob die Volumes und LUNs erfolgreich aus dem lokalen Cluster geschützt sind, klicken Sie auf **Storage > Volumes** oder **Storage > LUNs** und erweitern Sie die Ansicht Volume/LUN.

Weitere Möglichkeiten dies in ONTAP zu tun

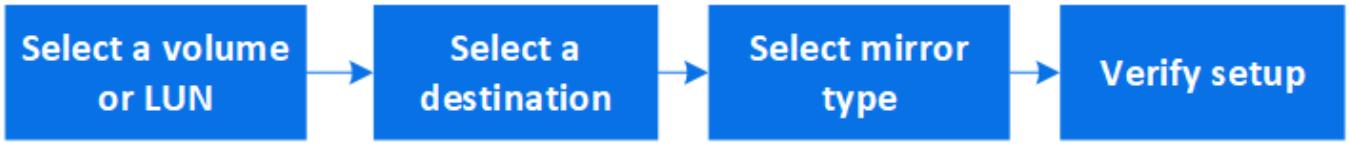
So führen Sie diese Aufgaben durch:	Inhalt anzeigen…
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Überblick über die Vorbereitung der Volume Disaster Recovery"
Die ONTAP Befehlszeilenschnittstelle	"Erstellen einer Cluster-Peer-Beziehung"

Konfigurieren von Spiegelungen und Vaults

Erstellen eines Spiegels und eines Volumes, um die Daten im Notfall zu sichern und mehrere archivierte Versionen von Daten zu haben, auf die Sie ein Rollback ausführen können. 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.

Durch dieses Verfahren wird eine Datenschutzrichtlinie in einem Remote-Cluster erstellt. Der Quell- und Ziel-Cluster verwenden Cluster-Netzwerkschnittstellen für den Datenaustausch. Die Vorgehensweise setzt voraus, dass die "Es werden Cluster-übergreifende Netzwerkschnittstellen erstellt, und die Cluster mit den Volumes werden Peering durchgeführt" (Gekoppelt). Sie können Storage VMs auch zur Datensicherung Peer nutzen. Wenn Storage VMs jedoch nicht Peering-Einheiten erfolgen, die Berechtigungen jedoch aktiviert sind, werden Storage-VMs automatisch durch die Erstellung der Sicherungsbeziehung wieder aktiviert.



Schritte

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.

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"
Die ONTAP Befehlszeilenschnittstelle	"Erstellen einer Replikationsbeziehung"

Synchronisieren Sie eine Schutzbeziehung neu

Wenn das ursprüngliche Quell-Volume nach einem Ausfall wieder verfügbar ist, können Sie die Daten vom Ziel-Volume neu synchronisieren und die Sicherungsbeziehung wiederherstellen.

Durch dieses Verfahren werden die Daten im ursprünglichen Quell-Volume in einer asynchronen Beziehung ersetzt, sodass Sie Daten vom ursprünglichen Quell-Volume erneut bereitstellen und die ursprüngliche Sicherungsbeziehung wieder aufnehmen können.

Schritte

1. Klicken Sie auf **Schutz > Beziehungen** und dann auf die unterbrochene Beziehung, die Sie neu synchronisieren möchten.
2. Klicken Sie Auf ⋮ Und wählen Sie dann **Resync**.
3. Überwachen Sie unter **Relationships** den Fortschritt der Neusynchronisierung, indem Sie den Beziehungsstatus überprüfen. Nach Abschluss der Resynchronisierung ändert sich der Status in „gespiegelt“.

Wiederherstellung eines Volume aus einer früheren Snapshot Kopie

Wenn Daten in einem Volume verloren gehen oder beschädigt werden, können Sie ein

Rollback Ihrer Daten durch eine frühere Snapshot Kopie durchführen.

Durch dieses Verfahren werden die aktuellen Daten des Quell-Volume durch Daten aus einer früheren Snapshot Kopierversion ersetzt. Sie sollten diese Aufgabe für das Ziel-Cluster ausführen.

Schritte

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 **Ziel** die Snapshot Kopie aus, die 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.

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"
Die ONTAP Befehlszeilenschnittstelle	"Stellen Sie den Inhalt eines Volumes von einem SnapMirror-Ziel wieder her"

Wiederherstellung aus Snapshot-Kopien

Sie können ein Volume auf einen früheren Zeitpunkt wiederherstellen, indem Sie es aus einer Snapshot Kopie wiederherstellen.

Durch dieses Verfahren wird ein Volume aus einer Snapshot Kopie wiederhergestellt.

Schritte

1. Klicken Sie auf **Storage** und wählen Sie ein Volume aus.
2. Klicken Sie unter **Snapshot Kopien** auf ⋮ Neben der Snapshot Kopie, die Sie wiederherstellen möchten, und wählen Sie **Wiederherstellen**.

Wiederherstellung auf einem neuen Volume

Ab ONTAP 9.8 können Sie mit System Manager gesicherte Daten auf dem Ziel-Volume in einem anderen Volume als der ursprünglichen Quelle wiederherstellen.

Wenn Sie ein anderes Volume wiederherstellen, können Sie ein vorhandenes Volume auswählen oder ein neues Volume erstellen.

Schritte

1. Wählen Sie die gewünschte Schutzbeziehung aus: Klicken Sie auf **Schutz > Beziehungen**.
2. Klicken Sie Auf ⋮ Und klicken Sie auf **Wiederherstellen**.
3. Wählen Sie im Abschnitt **Quelle** die Option **anderes Volume** aus, und wählen Sie den Cluster und die Storage VM aus.

4. Wählen Sie entweder **vorhandenes Volume** oder **Neues Volume erstellen**.
5. Wenn Sie ein neues Volume erstellen, geben Sie den Namen des Volumes ein.
6. Wählen Sie im Abschnitt **Ziel** die Snapshot Kopie aus, die wiederhergestellt werden soll.
7. Klicken Sie Auf **Speichern**.
8. Überwachen Sie unter **Relationships** den Fortschritt der Wiederherstellung, indem Sie **Transferstatus** für die Beziehung anzeigen.

Neusynchronisierung einer Schutzbeziehung rückgängig machen

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.

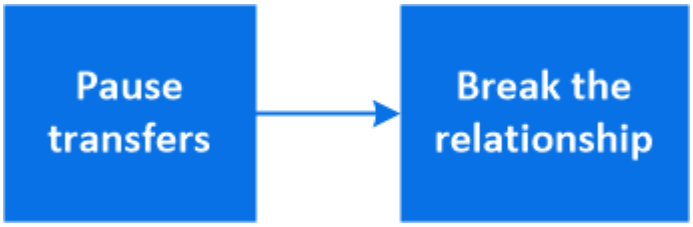
Wenn Sie einen umgekehrten Resynchronisierung durchführen, werden alle Daten auf dem Quell-Volume, die neuer sind als die Daten in der gemeinsamen Snapshot Kopie, gelöscht.

Schritte

1. Wählen Sie die gewünschte Schutzbeziehung aus: Klicken Sie auf **Schutz > Beziehungen**.
2. Klicken Sie Auf ⋮ Und klicken Sie auf **Resync rückwärts**.
3. Überwachen Sie unter **Relationships** den Fortschritt der umgekehrten Neusynchronisierung, indem Sie **Transferstatus** für die Beziehung anzeigen.

Stellen Sie Daten von einem SnapMirror Ziel bereit

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.



Schritte

1. Wählen Sie die gewünschte Schutzbeziehung aus: Klicken Sie auf **Schutz > Beziehungen** und klicken Sie dann auf den gewünschten Volumennamen.
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:

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. Bei diesem Vorgang werden die Daten auf dem ursprünglichen Quell-Volume ersetzt.

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"
Die ONTAP Befehlszeilenschnittstelle	"Aktivieren Sie die Ziellautstärke"

Disaster Recovery für Storage-VMs konfigurieren

Mit System Manager können Sie eine Storage VM Disaster Recovery-Beziehung (Storage VM DR) erstellen, um eine Storage-VM-Konfiguration auf eine andere zu replizieren. Bei einem Notfall am primären Standort können Sie die Ziel-Storage VM schnell aktivieren.

Führen Sie dieses Verfahren vom Ziel aus. Wenn Sie eine neue Schutzrichtlinie erstellen müssen, z. B. wenn Ihre Quell-Storage-VM SMB konfiguriert ist, sollten Sie die Richtlinie mit System Manager erstellen und im Fenster **Schutzrichtlinie hinzufügen** die Option **Identity Preserve** auswählen.
Weitere Details finden Sie unter "Erstellen benutzerdefinierter Datensicherungsrichtlinien".

Schritte

1. Klicken Sie auf dem Ziel-Cluster auf **Schutz > Beziehungen**.
2. Klicken Sie unter **Relationships** auf Protect und wählen Sie **Storage VMs (DR)** aus.
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. Klicken Sie Auf **Speichern**.

Bereitstellen von Daten von einem SVM DR-Ziel

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

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 SVM-Status der Quelle „ausgeführt“ lautet, beenden Sie ihn: Auswählen ⋮ Und wählen Sie **Stopp**.
3. Suchen Sie auf dem Ziel-Cluster die gewünschte Schutzbeziehung: Navigieren Sie zu **Schutz > Beziehungen**.
4. Klicken Sie Auf ⋮ Und wählen Sie **Ziel-Storage-VM aktivieren**.

Aktivieren Sie eine Quell-Storage-VM neu

Ab ONTAP 9.8 können Sie mit System Manager im Notfall eine Quell-Storage-VM erneut aktivieren. Durch die Reaktivierung der Quell-Storage-VM wird die Ziel-Storage-VM angehalten und die Replizierung von der Quelle zum Ziel wird erneut aktiviert.

Über diese Aufgabe

Wenn Sie die Quell-Storage-VM reaktivieren, führt System Manager im Hintergrund die folgenden Vorgänge aus:

- Erstellt eine Reverse-SVM-DR-Beziehung vom ursprünglichen Ziel zur ursprünglichen Quelle mithilfe von SnapMirror Resync
- Beendet die Ziel-SVM
- Aktualisiert die SnapMirror Beziehung
- Bricht die SnapMirror Beziehung auf
- Startet die ursprüngliche SVM neu
- Gibt eine SnapMirror-Neusynchronisierung der ursprünglichen Quelle zurück zum ursprünglichen Ziel vor
- Bereinigt die SnapMirror Beziehungen

Schritte

1. Wählen Sie die gewünschte Schutzbeziehung aus: Klicken Sie auf **Schutz > Beziehungen**.
2. Klicken Sie Auf ⋮ Und klicken Sie auf **Quell-Storage-VM reaktivieren**.
3. Überwachen Sie unter **Relationships** den Fortschritt der Reaktivierung der Quelle, indem Sie **Transferstatus** für die Schutzbeziehung anzeigen.

Synchronisieren Sie eine Ziel-Storage-VM erneut

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.

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.

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

1. Wählen Sie 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 ⋮ Und klicken Sie auf **Resync**.
4. Überwachen Sie unter **Relationships** den Fortschritt der Neusynchronisierung, indem Sie **Transferstatus** für die Beziehung anzeigen.

Daten mit SnapMirror in der Cloud sichern

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.

Bevor Sie die SnapMirror Cloud Funktion verwenden, sollten Sie einen SnapMirror Cloud API Lizenzschlüssel von der NetApp Support Site anfordern: "Fordern Sie den SnapMirror Cloud API-Lizenzschlüssel an". 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

Mithilfe der Cloud-Standardschutzrichtlinie 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 SnapMirror Cloud API Lizenzschlüssel wie dargestellt 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 die Standard-Cloud-Richtlinie von DailyBackup für Ihre SnapMirror Cloud-Backups nicht 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.

Schritte

1. Klicken Sie Auf **Storage > Volumes**.
2. Wählen Sie die Registerkarte * Backup to Cloud* aus.
3. Klicken Sie Auf ⋮ Neben dem Quellvolume, das wiederhergestellt werden soll, und wählen Sie **Wiederherstellen**.
4. Wählen Sie unter **Source** eine Speicher-VM aus und geben Sie dann den Namen des Volumes ein, auf dem die Daten wiederhergestellt werden sollen.
5. Wählen Sie unter **Ziel** die Snapshot Kopie aus, die Sie wiederherstellen möchten.
6. Klicken Sie Auf **Speichern**.

SnapMirror Cloud-Beziehung löschen

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 Auf ⋮ Neben dem Quellvolume 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 Objektspeicher aus, den Sie löschen möchten, und klicken Sie auf ⋮ Und wählen Sie **Löschen**.

Daten mit Cloud Backup sichern

Ab ONTAP 9.9 können Kunden mit System Manager Daten in der Cloud mithilfe von Cloud Backup sichern.

> Cloud Backup unterstützt FlexVol Volumes mit Schreibvorgängen und Datensicherung (DP) Volumes. FlexGroup Volumes und SnapLock-Volumes werden nicht unterstützt.

Bevor Sie beginnen

Führen Sie die folgenden Schritte durch, um ein Konto in BlueXP einzurichten. Für das Servicekonto müssen Sie die Rolle als „Account Admin“ erstellen. (Andere Service-Account-Rollen verfügen nicht über die erforderlichen Berechtigungen, die zum Herstellen einer Verbindung von System Manager erforderlich sind.)

1. "Erstellen Sie ein Konto in BlueXP".
2. "Erstellen Sie einen Anschluss in BlueXP" Nutzen Sie einen der folgenden Cloud-Provider:
   - 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-Provider auswählen, jedoch nur, wenn BlueXP vor Ort implementiert ist. Der BlueXP-Anschluss muss vor Ort installiert und über die BlueXP Software-as-a-Service (SaaS)-Anwendung verfügbar sein.

3. "Abonnieren Sie Cloud Backup Service unter BlueXP" (Erfordert die entsprechende Lizenz).
4. "Generieren Sie mithilfe von BlueXP einen Zugriffsschlüssel und einen geheimen Schlüssel".

Registrieren Sie den Cluster mit BlueXP

Sie können das Cluster mit BlueXP entweder über BlueXP oder über System Manager registrieren.

Schritte

1. Gehen Sie in System Manager zu **Protection Overview**.
2. Geben Sie unter **Cloud Backup Service** folgende Angaben an:
   - Client-ID

- Geheimschlüssel des Kunden

3. Wählen Sie **Registrieren und fortfahren**.

Cloud Backup Aktivieren

Nach der Registrierung des Clusters bei BlueXP müssen Sie das Cloud Backup aktivieren und das erste Backup in der Cloud starten.

Schritte

1. Klicken Sie in System Manager auf **Schutz > Übersicht** und scrollen 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 der Nutzung der Cloud, indem Sie auf **Erfahren Sie mehr über die Kosten der Cloud** klicken.

3. Klicken Sie auf **Verbinden und aktivieren Sie Cloud Backup Service**.
4. Geben Sie auf der Seite **Cloud Backup Service** aktivieren die folgenden Details an, je nachdem, welcher Anbieter Sie ausgewählt haben.

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 bei lokaler Implementierung von BlueXP)	• 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 bis zum letzten 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 der für Cloud-Backup verwendeten Sicherungsrichtlinie

Sie können die Sicherungsrichtlinie für Cloud Backup ändern.

Schritte

1. Klicken Sie in System Manager auf **Schutz > Übersicht** und scrollen Sie dann zum Abschnitt **Cloud Backup Service**.
2. Klicken Sie Auf ⋮, 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 bis zum letzten 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.
- Das Cluster muss ONTAP 9.9 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.
- FlexGroups können nicht über Cloud Backup 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 für Cloud-Backup aus.
3. Wenn der Cloud-Backup nicht aktiviert ist, wählen Sie **Cloud Backup Service aktivieren**.

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 klicken Sie auf **Protect**.
2. Geben Sie auf der Seite **Protect Volumes Sicherung mit Cloud Backup Service** für die Schutzpolitik an.
3. Klicken Sie Auf **Schutz**.
4. Aktivieren Sie auf der Seite **Schutz** das Kontrollkästchen **SnapMirror aktivieren (lokal oder Remote)**.
5. Wählen Sie **Cloud Backup Service Aktivieren**.

Wiederherstellung von Daten aus Backup-Dateien

Sie können Backup-Managementvorgänge ausführen, z. B. das Wiederherstellen von Daten, das Aktualisieren von Beziehungen und das Löschen von Beziehungen, nur wenn Sie die BlueXP-Schnittstelle verwenden. Siehe "Wiederherstellen von Daten aus Backup-Dateien" Finden Sie weitere Informationen.

Cluster- und SVM-Peering mit der CLI

Übersicht über Cluster- und SVM-Peering mit der CLI

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 Snapshot Kopien 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

Peering-Grundlagen

Sie müssen *Peer-Beziehungen* zwischen Quell- und Ziel-Clustern und zwischen Quell- und Ziel-SVMs erstellen, bevor Sie Snapshot Kopien mit SnapMirror replizieren können. 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
> ```

Voraussetzungen für Cluster-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-Peer-Verschlüsselung standardmäßig TLS 1.2 AES-256 GCM-Verschlüsselung für Datenreplizierung. Die Standard-Sicherheitskiffren („PSK-AES256-GCM-SHA364“) sind erforderlich, damit Cluster-Peering funktioniert, auch wenn die Verschlüsselung deaktiviert ist.
>
> Ab ONTAP 9.11.1 sind die DHE-PSK-Sicherheitsschlüssel standardmäßig verfügbar.

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.

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.

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 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.

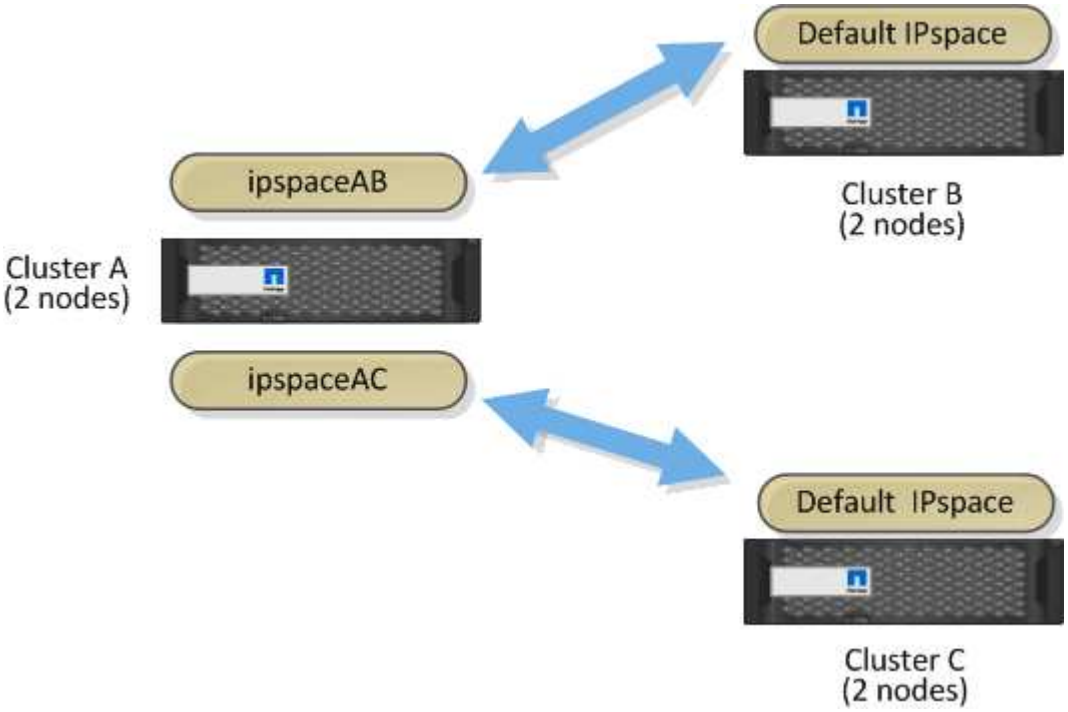
Sie können auch VLAN-Ports für die Replikation zuweisen. Die Bandbreite des Ports wird von allen VLANs und dem Basis-Port gemeinsam genutzt.

Verwenden Sie benutzerdefinierte IPspaces, um den Replikationsverkehr 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 den Replizierungsverkehr zwischen Cluster A und Cluster B vom Replizierungsdatenverkehr zwischen Cluster A und Cluster C trennen Hierzu können Sie auf Cluster A zwei IPspaces erstellen

Ein IPspace enthält die Intercluster LIFs, die Sie zur Kommunikation mit Cluster B. verwenden Die andere enthält die Intercluster-LIFs, die Sie für die Kommunikation mit Cluster C verwenden, wie in der folgenden Abbildung dargestellt.



Informationen zur benutzerdefinierten Konfiguration von IPspace finden Sie im Handbuch_Network Management_.

Konfigurieren Sie Intercluster LIFs

Konfigurieren Sie Intercluster-LIFs an gemeinsam genutzten Datenports

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
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in angezeigt `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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02`:

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

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

3. 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`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
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`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf dem `e0c` Ein Failover des Ports zum erfolgt `e0d` Port:

```
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 Intercluster-LIFs auf 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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in angezeigt `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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Ports angezeigt `e0e` Und `e0f` Es wurden 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`

Im folgenden Beispiel werden Ports zugewiesen `e0e` Und `e0f` Zur Failover-Gruppe `intercluster01` Auf der System-SVM `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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
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`

Option	Beschreibung
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`*

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02` In der Failover-Gruppe `intercluster01`:

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

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

6. 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`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
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`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf der SVM`e0e` Ein Failover des Ports zum erfolgt `e0f` Port:

```
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 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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerkports in angezeigt `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
```

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

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Ports angezeigt `e0e` Und `e0f` Es wurden 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. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden Ports entfernt `e0e` Und `e0f` In der Standard-Broadcast-Domäne:

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

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

   `network port show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Ports angezeigt `e0e` Und `e0f` Wurden aus der Standard-Broadcast-Domäne entfernt:

```
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-Domäne erstellt `ipspace-IC1-bd` Im IPspace `ipspace-IC1`:

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

7. Vergewissern Sie sich, dass die Broadcast-Domäne erstellt wurde:

   `network port broadcast-domain show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
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. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs erstellt `cluster01_icl01` Und `cluster01_icl02` In der Broadcast-Domäne `ipspace-IC1-bd`:

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

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

9. 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`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
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`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind `cluster01_icl01` Und `cluster01_icl02` Auf der SVM `e0e` Port-Failover zum Port`e0f`:

```
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

Erstellen einer Cluster-Peer-Beziehung

Sie können das verwenden `cluster peer create` Befehl zum Erstellen einer Peer-Beziehung zwischen einem lokalen und einem Remote-Cluster. Nachdem die Peer-Beziehung erstellt wurde, können Sie ausführen `cluster peer create` Im Remote-Cluster zur Authentifizierung beim lokalen Cluster.

Bevor Sie beginnen

- Sie müssen auf jedem Node in den Clustern, die Peering durchführen, Intercluster LIFs erstellt haben.
- Die Cluster müssen ONTAP 9.3 oder höher ausführen. (Wenn auf den Clustern ONTAP 9.2 oder eine frühere Version ausgeführt wird, lesen Sie die Verfahren in "Dieses archivierte Dokument".)

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 fügen Sie dem Cluster Intercluster-Netzwerkschnittstellen hinzu.

   Wiederholen Sie diesen Schritt auf dem Remote-Cluster.

3. Klicken Sie im Remote-Cluster auf **Cluster > Einstellungen**.
4. Klicken Sie Auf ⋮ Wählen Sie im Abschnitt **Cluster Peers** die Option **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**.
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 beides angeben `-generate-passphrase` Und `-peer-addrs`, Nur der Cluster, dessen Intercluster LIFs in angegeben sind `-peer-addrs` Kann das generierte Passwort verwenden.

   Sie können die ignorieren `-ipspace` Option, wenn kein benutzerdefinierter IPspace verwendet wird. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Wenn Sie die Peering-Beziehung in ONTAP 9.6 oder höher erstellen und keine clusterübergreifende Peering-Kommunikation verschlüsselt werden soll, müssen Sie den verwenden `-encryption -protocol-proposed none` Option zum Deaktivieren der Verschlüsselung.

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

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

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

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

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 mit einem nicht festgelegten Remote-Cluster erstellt und Peer-Beziehungen zu SVMs vorab autorisiert`vs1` Und `vs2` Auf dem lokalen Cluster:

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

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

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

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

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Bereiten Sie sich auf Spiegelung und Vaulting vor"
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Überblick über die Vorbereitung der Volume Disaster Recovery"

Erstellen einer Cluster-übergreifende SVM-Peer-Beziehung

Sie können das verwenden `vserver peer create` Befehl zum Erstellen einer Peer-Beziehung zwischen SVMs auf lokalen und Remote-Clustern.

Bevor Sie beginnen

- Die Quell- und Ziel-Cluster müssen Peering durchgeführt werden.
- Auf den Clustern muss ONTAP 9.3 ausgeführt werden. (Wenn auf den Clustern ONTAP 9.2 oder eine frühere Version ausgeführt wird, lesen Sie die Verfahren in "Dieses archivierte Dokument".)
- 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

In ONTAP 9.2 und älteren Versionen können Sie jeweils nur für eine SVM eine Peer-Beziehung autorisieren. Dies bedeutet, dass Sie das ausführen müssen `vserver peer accept` Führen Sie jedes Mal einen Befehl aus, wenn Sie eine ausstehende SVM-Peer-Beziehung autorisieren.

Ab ONTAP 9.3 können Sie Peer-Beziehungen für mehrere SVMs vorab autorisieren. Dazu müssen Sie die SVMs in der Liste auflisten `-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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird eine Peer-Beziehung zwischen der lokalen SVM erstellt `pvs1` Und der vorab autorisierten 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 eine Cluster-übergreifende SVM-Peer-Beziehung 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 das verwenden `vserver peer create` Befehl zum Erstellen einer Peer-Beziehung zwischen SVMs. Nachdem die Peer-Beziehung erstellt wurde, können Sie ausführen `vserver peer accept` Auf dem Remote-Cluster, 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. Weitere Informationen finden Sie im `vserver peer create` Man-Page.

Administratoren verwenden gelegentlich das `vserver peer reject` Befehl zum Ablehnen einer vorgeschlagenen SVM-Peer-Beziehung. Wenn die Beziehung zwischen SVMs sich in der befindet `rejected` Status: Sie müssen die Beziehung löschen, bevor Sie eine neue erstellen können. Weitere Informationen finden Sie im `vserver peer delete` Man-Page.

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 SVM erstellt`pvs1` Und die Remote-SVM`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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel zeigt die Peer-Beziehung zwischen SVM`pvs1` Und SVM`vs1` Wurde initiiert:

```
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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden 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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel autorisiert die Peer-Beziehung zwischen der lokalen SVM `vs1` Und die 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
```

Cluster-Peering-Verschlüsselung für vorhandene 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.

Entfernen Sie die Cluster-Peering-Verschlüsselung von einer vorhandenen Peer-Beziehung

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 Ziel-Cluster die Kommunikation mit dem Quell-Cluster, um die Verwendung von 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
     ```

   - Um Verschlüsselung und Authentifizierung zu entfernen, geben Sie Folgendes ein:

     ```
     cluster peer modify _source_cluster_ -auth-status no-authentication
     ```

2. Geben Sie bei Aufforderung eine Passphrase ein.
3. 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
     ```

   - Um Verschlüsselung und Authentifizierung zu entfernen, geben Sie Folgendes ein:

     ```
     cluster peer modify _destination_cluster_ -auth-status no-
     authentication
     ```

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

Managen Sie lokale Snapshot Kopien

Überblick: Managen von lokalen Snapshot Kopien

Eine *Snapshot Kopie* ist ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes. Das Image verbraucht nur wenig Storage und der Performance-Overhead ist zu vernachlässigen, da seit der letzten Snapshot Kopie nur Änderungen an Dateien aufgezeichnet werden.

Sie können eine Snapshot Kopie verwenden, um den gesamten Inhalt eines Volumes wiederherzustellen oder

einzelne Dateien oder LUNs wiederherzustellen. Snapshot-Kopien werden im Verzeichnis gespeichert `.snapshot` Auf dem Volume.

Ab ONTAP 9.3 und älteren Versionen kann ein Volume bis zu 255 Snapshot Kopien enthalten. Ab ONTAP 9.4 kann ein FlexVol Volume bis zu 1023 Snapshot Kopien enthalten.

> Ab ONTAP 9.8 können FlexGroup Volumes 1023 Snapshot Kopien enthalten. Weitere Informationen finden Sie unter "Schützen Sie FlexGroup Volumes mithilfe von Snapshot-Kopien".

Konfigurieren Sie benutzerdefinierte Snapshot Richtlinien

Konfigurieren Sie eine Übersicht über benutzerdefinierte Snapshot Richtlinien

Eine *Snapshot-Richtlinie* definiert, wie das System Snapshot Kopien erstellt. Die Richtlinie gibt an, wann Snapshot Kopien erstellt werden sollen, wie viele Kopien aufzubewahren sind und wie sie benannt werden. Ein System könnte beispielsweise jeden Tag um 12:10 Uhr eine Snapshot-Kopie erstellen, die beiden neuesten Kopien aufbewahren und die Kopien „`dalltäglich benennen.`*`timestamp`*`.`“

Die Standardrichtlinie für ein Volume erstellt automatisch Snapshot Kopien nach folgendem Zeitplan. Die ältesten Snapshot-Kopien werden gelöscht, um Platz für neuere Kopien zu schaffen:

- Maximal sechs stündliche Snapshot-Kopien wurden innerhalb von fünf Minuten nach der Stunde erstellt.
- Es werden maximal zwei tägliche Snapshot-Kopien erstellt, die von Montag bis Samstag um 10 Minuten nach Mitternacht erstellt wurden.
- Es sind maximal zwei wöchentliche Snapshot-Kopien erstellt jeden Sonntag um 15 Minuten nach Mitternacht.

Wenn Sie beim Erstellen eines Volumes keine Snapshot-Richtlinie angeben, übernimmt das Volume die ihm zugeordnete Snapshot-Richtlinie zur Storage Virtual Machine (SVM).

Zeitpunkt zum Konfigurieren einer benutzerdefinierten Snapshot-Richtlinie

Wenn sich die standardmäßige Snapshot-Richtlinie nicht für ein Volume eignet, können Sie eine benutzerdefinierte Richtlinie konfigurieren, die die Häufigkeit, Aufbewahrung und den Namen von Snapshot Kopien 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). Allgemein gesagt sollten Sie nur so viele Snapshot-Kopien wie nötig aufbewahren.

Erstellen eines Snapshot-Job-Zeitplans

Eine Snapshot-Richtlinie erfordert mindestens einen Zeitplan für Snapshot-Kopien. Sie

können das verwenden `job schedule cron create` Befehl zum Erstellen eines Jobplans.

Über diese Aufgabe

Standardmäßig erstellt ONTAP die Namen von Snapshot Kopien, indem ein Zeitstempel an den Namen des Job-Zeitplans angehängt wird.

Wenn Sie Werte sowohl für Tag des Monats als auch für Tag der Woche angeben, werden die Werte unabhängig betrachtet. Zum Beispiel ein Cron-Zeitplan mit der Tagesspezifikation `Friday` Und den Tag der Monatsangabe `13` Läuft jeden Freitag und am 13. Tag des Monats, nicht nur an jedem Freitag den 13.

Schritt

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`, Sie können angeben `all` Zum Ausführen des Jobs jeden Monat, Wochentag und Stunde.

   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 Job-Zeitplan mit dem Namen erstellt `myweekly` Das läuft samstags um 3:00 Uhr:

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

   Im folgenden Beispiel wird ein Zeitplan mit dem Namen erstellt `myweeklymulti` Das gibt mehrere Tage, Stunden und Minuten an:

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

Erstellen einer Snapshot-Richtlinie

Eine Snapshot-Richtlinie gibt an, wann Snapshot Kopien erstellt werden sollen, wie viele Kopien aufzubewahren sind und wie sie benannt werden sollen. Ein System könnte beispielsweise jeden Tag um 12:10 Uhr eine Snapshot-Kopie erstellen, die beiden neuesten Kopien aufbewahren und sie mit „`dalltäglich`" benennen.`*timestamp*.`" Eine Snapshot-Richtlinie kann bis zu fünf Zeitpläne für Jobs enthalten.

Über diese Aufgabe

Standardmäßig erstellt ONTAP die Namen von Snapshot Kopien, indem ein Zeitstempel an den Namen des

Job-Zeitplans angehängt wird:

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

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

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

Schritt

1. Erstellen einer Snapshot-Richtlinie:

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

   Im folgenden Beispiel wird eine Snapshot-Richtlinie mit dem Namen erstellt `snap_policy_daily` Das läuft auf einem `daily` Zeitplan: Die Richtlinie verfügt über maximal fünf Snapshot-Kopien, die jeweils mit dem Namen benannt sind `daily.`*`timestamp`* Und das SnapMirror-Etikett `daily`:

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

Managen Sie Snapshot Kopien manuell

Erstellen Sie Snapshot Kopien manuell und löschen Sie sie

Sie können Snapshot Kopien manuell erstellen, wenn Sie nicht warten können, bis eine geplante Snapshot Kopie erstellt wurde. Außerdem können Sie Snapshot Kopien löschen, wenn sie nicht mehr benötigt werden.

Erstellen Sie manuell eine Snapshot Kopie

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

System Manager

Schritte

1. Navigieren Sie zu **Storage > Volumes** und wählen Sie die Registerkarte **Snapshot Copies** aus.
2. Klicken Sie Auf + Add .
3. Akzeptieren Sie im Fenster **Snapshot Kopie hinzufügen** den Standardnamen der Snapshot Kopie oder bearbeiten Sie ihn, falls gewünscht.
4. **Optional**: Fügen Sie ein SnapMirror-Label hinzu.
5. Klicken Sie Auf **Hinzufügen**.

CLI

1. Erstellen einer Snapshot Kopie:

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

Löschen Sie eine Snapshot Kopie manuell

Sie können eine Snapshot Kopie manuell über System Manager oder die ONTAP CLI löschen.

System Manager

Schritte

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

CLI

1. Löschen einer Snapshot Kopie:

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

Managen Sie die Snapshot Kopie-Reserve

Managen Sie die Übersicht zur Snapshot Kopie-Reserve

Die *Snapshot Kopie Reserve* legt einen Prozentsatz des Speicherplatzes für Snapshot-Kopien beiseite, standardmäßig fünf Prozent. Da Snapshot-Kopien den Speicherplatz im aktiven File-System nutzen, wenn die Snapshot-Kopie-Reserve erschöpft ist, können Sie

die Snapshot-Kopie-Reserve je nach Bedarf erhöhen. Alternativ können Sie Snapshot-Kopien automatisches Löschen auch dann erstellen, wenn die Reserve voll ist.

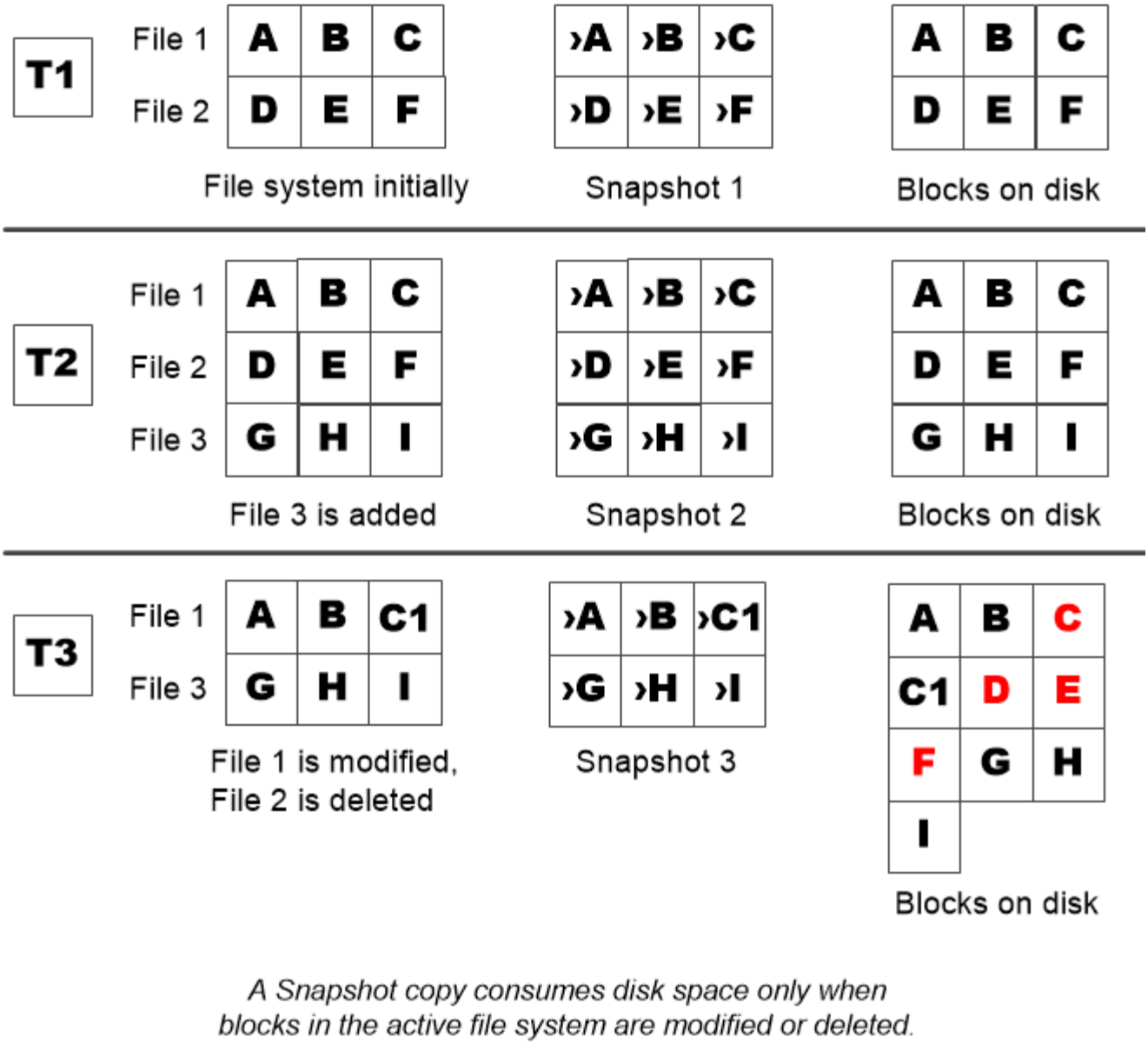
Vergrößern der Reserve für Snapshot Kopien

Bei der Entscheidung, ob die Snapshot Reserve erhöht werden soll, sollte nicht vergessen werden, dass eine Snapshot Kopie nur Änderungen an Dateien aufzeichnet, seit die letzte Snapshot Kopie erstellt wurde. Sie verbraucht nur dann Speicherplatz, wenn Blöcke im aktiven File-System geändert oder gelöscht werden.

Das bedeutet, dass die Änderungsrate des Dateisystems der Schlüsselfaktor bei der Bestimmung der Menge des Festplattenspeichers ist, der von Snapshot-Kopien verwendet wird. Unabhängig von der Anzahl der erstellten Snapshot-Kopien werden diese keinen Speicherplatz belegen, wenn sich das aktive Filesystem nicht geändert hat.

Ein FlexVol Volume mit Transaktions-Logs von Datenbanken könnte beispielsweise eine Snapshot-Kopie-Reserve von 20 % aufweisen, um die höhere Änderungsrate berücksichtigen zu können. Sie werden nicht nur mehr Snapshot Kopien erstellen möchten, um die häufigeren Updates für die Datenbank zu erfassen. Außerdem möchten Sie auch eine größere Snapshot-Kopie-Reserve erhalten, um den zusätzlichen Festplattenspeicher zu verarbeiten, den die Snapshot-Kopien belegen.

Eine Snapshot Kopie besteht aus Zeigern auf Blöcke statt Kopien von Blöcken. Denken Sie an einen Zeiger als „`Claim`“ auf einem Block: ONTAP „`Holds`“, bis die Snapshot Kopie gelöscht wird.



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

Eine Snapshot-Kopie verweist auf einen Block, sogar nachdem Sie die Datei gelöscht haben, die den Block verwendet hat. Dies erklärt, warum eine ausgeschöpfte Snapshot Kopie-Reserve zum gegenintuitiven Ergebnis führen könnte, wobei das Löschen eines gesamten File-Systems dazu führt, dass weniger Speicherplatz verfügbar ist als das belegte File-System.

Betrachten wir das folgende Beispiel. Bevor Sie Dateien löschen, wird der `df` Die Befehlsausgabe ist wie folgt:

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

Nach dem Löschen des gesamten Dateisystems und dem Erstellen einer Snapshot Kopie des Volume, wird

der angezeigt `df` Der Befehl generiert 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 jetzt zusätzlich zu den 0.5 GB vor dem Löschen auch die gesamten 3 GB, die zuvor vom aktiven File-System verwendet wurden, für Snapshot-Kopien verwendet.

Da der von den Snapshot-Kopien verwendete Festplattenspeicher nun die Snapshot-Kopie-Reserve überschreitet, erfolgt der Überlauf von 2.5 GB „`sPills`“ in den für aktive Dateien reservierten Speicherplatz. Dadurch verfügen Sie über 0.5 GB freien Speicherplatz für Dateien, bei denen Sie vernünftigerweise 3 GB erwartet haben.

Überwachen Sie den Festplattenverbrauch von Snapshot-Kopien

Sie können den Festplattenverbrauch von Snapshot-Kopien mit überwachen `df` Befehl. Der Befehl zeigt die Menge an freiem Speicherplatz im aktiven File-System und die Snapshot-Kopierreserve an.

Schritt

1. Zeigen Sie den Festplattenverbrauch der Snapshot-Kopie an: `df`

   Im folgenden Beispiel wird der Festplattenverbrauch von Snapshot-Kopien angezeigt:

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

Überprüfen Sie die verfügbare Snapshot-Kopie-Reserve auf einem Volume

Vielleicht möchten Sie überprüfen, wie viel Snapshot-Kopie-Reserve auf einem Volume verfügbar ist, indem Sie auf verwenden `snapshot-reserve-available` Parameter mit `volume show` Befehl.

Schritt

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

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die verfügbare Snapshot-Kopie-Reserve für angezeigt `vol1`:

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

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

Ändern Sie die Snapshot Kopie-Reserve

Es empfiehlt sich möglicherweise, eine größere Snapshot-Kopie-Reserve zu konfigurieren, um zu verhindern, dass Snapshot-Kopien den Speicherplatz nutzen, der für das aktive Dateisystem reserviert ist. Sie können die Snapshot Kopie-Reserve verringern, wenn Sie nicht mehr so viel Speicherplatz für Snapshot-Kopien benötigen.

Schritt

1. Ändern Sie die Snapshot Kopie-Reserve:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

Automatisches Löschen von Snapshot Kopien

Sie können das verwenden `volume snapshot autodelete modify` Befehl, um das automatische Löschen von Snapshot-Kopien auszulösen, wenn die Snapshot-Reserve überschritten wird. Standardmäßig werden die ältesten Snapshot Kopien zuerst gelöscht.

Über diese Aufgabe

LUN- und Dateiklone werden gelöscht, wenn keine weiteren Snapshot Kopien gelöscht werden müssen.

Schritt

1. Automatisches Löschen von Snapshot-Kopien:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden Snapshot Kopien für automatisch gelöscht `vol1` Wenn die Snapshot Kopie-Reserve erschöpft ist,

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

Wiederherstellung von Dateien aus Snapshot-Kopien

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

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

Jedes Verzeichnis im Dateisystem enthält ein Unterverzeichnis mit dem Namen `.snapshot` Zugriff für NFS- und SMB-Benutzer. Der `.snapshot` Unterverzeichnis enthält Unterverzeichnisse, die den Snapshot Kopien des Volume 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 die Snapshot Kopie verweist. Wenn Benutzer eine Datei versehentlich löschen oder überschreiben, kann sie die Datei in das übergeordnete Lese-/Schreibzugriff wiederherstellen, indem sie die Datei aus dem Snapshot Unterverzeichnis in das Lese-/Schreibzugriff-Verzeichnis kopiert.

```
$ 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 Verzeichnis für Snapshot-Kopien

Um zu ermitteln, ob das Verzeichnis der Snapshot Kopie für NFS- und SMB-Clients zum Wiederherstellen einer Datei oder eines LUN aus einer Snapshot Kopie sichtbar ist, können Sie den Zugriff auf das Snapshot Kopienverzeichnis über die aktivieren und deaktivieren `-snapdir-access` Option des `volume modify` Befehl.

Schritte

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
   ```

2. Aktivieren oder Deaktivieren des Verzeichniszugriffs für die Snapshot Kopie:

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

   Im folgenden Beispiel wird der Zugriff auf das Verzeichnis der Snapshot-Kopie auf vol1 aktiviert:

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

Wiederherstellen einer einzelnen Datei aus einer Snapshot Kopie

Sie können das verwenden `volume snapshot restore-file` Befehl zum Wiederherstellen einer einzelnen Datei oder einer LUN aus einer Snapshot Kopie. 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 in Form einer Snapshot Kopie erstellt und gesichert. Während des Wiederherstellungsvorgangs können Sie von lesen und auf die LUN schreiben.

Dateien mit Streams werden standardmäßig wiederhergestellt.

Schritte

1. Listen Sie die Snapshot Kopien in einem Volume auf:

   `volume snapshot show -vserver SVM -volume volume`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Snapshot Kopien in angezeigt `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 einer Snapshot Kopie:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Datei wiederhergestellt `myfile.txt`:

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

Wiederherstellen eines Teils einer Datei aus einer Snapshot Kopie

Sie können das verwenden `volume snapshot partial-restore-file` Befehl zum Wiederherstellen eines Datenbereichs von einer Snapshot Kopie auf eine LUN oder in eine NFS- oder SMB-Container-Datei, vorausgesetzt, Sie kennen den Start-Byte-Offset der Daten und die Anzahl des Bytes. 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 für Volumen in einer SM-BC-Beziehung eine partielle Wiederherstellung verfügbar.

Schritte

1. Listen Sie die Snapshot Kopien in einem Volume auf:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Snapshot Kopien in angezeigt `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 eines Teils einer Datei aus einer Snapshot Kopie:

   `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.

   Im folgenden Beispiel werden die ersten 4,096 Bytes der Datei wiederhergestellt `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
```

Wiederherstellung des Inhalts eines Volumes aus einer Snapshot Kopie

Sie können das verwenden `volume snapshot restore` Befehl zum Wiederherstellen des Inhalts eines Volumes aus einer Snapshot Kopie

Über diese Aufgabe

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

1. Listen Sie die Snapshot Kopien in einem Volume auf:

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

   Im folgenden Beispiel werden die Snapshot Kopien in angezeigt `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. Stellen Sie den Inhalt eines Volumes aus einer Snapshot Kopie wieder her:

   `volume snapshot restore -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`*

   Im folgenden Beispiel wird der Inhalt von wiederhergestellt `vol1`:

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

SnapMirror Volume-Replizierung

Grundlagen der asynchronen SnapMirror Disaster Recovery

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.

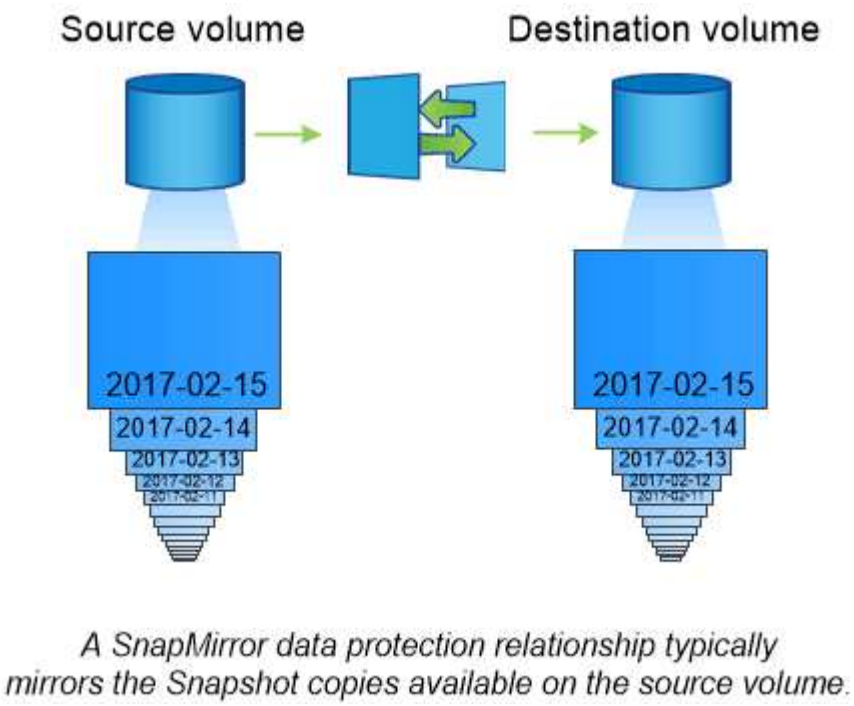
Wenn der primäre Standort weiterhin Daten versorgen kann, können Sie einfach alle benötigten Daten zurück darauf übertragen und nicht Clients vom Spiegel bedienen. Wie der Anwendungsfall für Failover impliziert, sollten die Controller auf dem sekundären System äquivalent oder fast vergleichbar mit den 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 *peering durchgeführt werden.* Eine Peer-Beziehung ermöglicht den Austausch von Clustern und SVMs Sicher aus Daten.

"Cluster- und SVM-Peering"

In der folgenden Abbildung werden SnapMirror Datensicherungsbeziehungen dargestellt.



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 asynchronen SnapMirror zum Schutz verwenden Konsistenzgruppen. Ab ONTAP 9.14.1 können Sie mithilfe von asynchronem SnapMirror Snapshots des Volumes mithilfe der Konsistenzgruppenbeziehung in den Ziel-Cluster replizieren. Weitere Informationen finden Sie unter Konfigurieren Sie den asynchronen SnapMirror Schutz.

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.

Basistransfer unter der Standard-SnapMirror-Richtlinie `MirrorAllSnapshots` Umfasst die folgenden Schritte:

- Erstellen einer Snapshot Kopie des Quell-Volume
- Übertragen Sie die Snapshot Kopie und alle Datenblöcke, auf die sie auf das Ziel-Volume verweist.
- Übertragen Sie die verbleibenden, weniger aktuellen Snapshot Kopien auf dem Quell-Volume auf das Ziel-Volume, falls die „`aktive`“-Spiegelung 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 jedem Update unter dem `MirrorAllSnapshots` Richtlinie: SnapMirror erstellt eine Snapshot Kopie des Quell-Volume und überträgt diese Snapshot Kopie sowie alle Snapshot Kopien, die seit der letzten Aktualisierung erstellt wurden. In der folgenden Ausgabe von der `snapmirror policy show` Befehl für das `MirrorAllSnapshots` Richtlinie, beachten Sie Folgendes:

- `Create Snapshot` Ist „`true`“, was darauf hinweist `MirrorAllSnapshots` Erstellt eine Snapshot Kopie, wenn SnapMirror die Beziehung aktualisiert.
- `MirrorAllSnapshots` Verfügt über Regeln „`sm_created`“ und „`all_source_Snapshots`“, die angeben, dass sowohl die von SnapMirror erstellte Snapshot Kopie als auch alle Snapshot Kopien, 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: Asynchronous SnapMirror 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

Der vorkonfigurierten `MirrorLatest` Politik funktioniert genau wie `MirrorAllSnapshots`, Außer dass nur die von SnapMirror erstellte Snapshot Kopie bei der Initialisierung und Aktualisierung übertragen wird.

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

Grundlagen von SnapMirror Synchronous Disaster Recovery

Ab ONTAP 9.5 wird SnapMirror Synchronous (SM-S) Technologie auf allen FAS und AFF Plattformen mit mindestens 16 GB Arbeitsspeicher sowie auf allen ONTAP Select Plattformen unterstützt. Die SnapMirror Synchronous Technologie ist eine pro Node lizenzierte Funktion zur synchronen Datenreplizierung auf Volume-Ebene.

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 pro HA-Paar entsprechend dem Plattformtyp und ONTAP Release zulässig sind.

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

Unterstützte Funktionen

In der folgenden Tabelle sind die Funktionen aufgeführt, die von SnapMirror Synchronous und den ONTAP Versionen unterstützt werden, in denen Unterstützung verfügbar ist.

Merkmal	Release wird zuerst unterstützt	Weitere Informationen
Antivirus auf dem primären Volume der SnapMirror Synchronous Beziehung	ONTAP 9.6	
Replizierung von applikationserstellten Snapshot Kopien	ONTAP 9.7	Wenn eine Snapshot Kopie zum Zeitpunkt der mit der entsprechenden Beschriftung versehen wird `snapshot create` Betrieb SnapMirror Synchronous repliziert über die CLI oder die ONTAP-API die Snapshot Kopien, sowohl von Benutzern als auch mit externen Skripts erstellt, nachdem die Applikationen stillgelegt wurden. Geplante Snapshot Kopien, die unter Verwendung einer Snapshot Richtlinie erstellt wurden, werden nicht repliziert. Weitere Informationen zum Replizieren von von durch Applikationen erstellten Snapshot-Kopien finden Sie im Knowledge Base-Artikel: "Wie repliziert man Snapshots von Anwendungen mit SnapMirror Synchronous".
Automatisches Löschen von Klonen	ONTAP 9.6	
FabricPool Aggregate mit einer Tiering-Richtlinie von „Keine“, „Snapshot“ oder „automatisch“ werden von SnapMirror Synchronous Quell- und Zielsystem 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 für das primäre Volume der SnapMirror Synchronous Beziehung	ONTAP 9.6	
Hard- und Soft-Quoten auf dem primären Volume der SnapMirror Synchronous 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 Beziehungen mit SnapMirror innerhalb eines Clusters tragen zur Obergrenze von gleichzeitig bei Beziehungen pro HA-Paar.
ISCSI	ONTAP 9.5	
LUN-Klone und NVMe Namespace-Klone	ONTAP 9.7	

LUN-Klone, die durch applikationserstellte Snapshot Kopien 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 SnapMirror Synchronous Operations (NDO) nur für 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 v4.3	ONTAP 9.5	
NFS Version 4.0	ONTAP 9.6	
NFS 4.1	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	
SnapMirror Kaskadenspiegelung mit synchroner Spiegelung	ONTAP 9.6	Die Beziehung zum Ziel-Volume der SnapMirror Synchronous Beziehung muss eine asynchrone SnapMirror-Beziehung sein.

Disaster Recovery für SVM	ONTAP 9.6	* Eine SnapMirror Synchronous Quelle kann auch eine SVM Disaster-Recovery-Quelle sein, zum Beispiel eine Fan-out-Konfiguration mit SnapMirror Synchronous als ein Bein und SVM Disaster Recovery als der andere. * Eine SnapMirror Synchronous Quelle kann kein SVM Disaster-Recovery-Ziel sein, da SnapMirror Synchronous keine Kaskadierung einer Datensicherungsquelle unterstützt. Sie müssen die synchrone Beziehung freigeben, bevor Sie eine SVM-Disaster-Recovery-Flip-Resynchronisierung im Ziel-Cluster durchführen. * Ein SnapMirror Synchronous Ziel kann keine SVM Disaster-Recovery-Quelle sein, da 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 nicht mit synchronen SnapMirror Beziehungen unterstützt:

- Konsistenzgruppen
- DP_Optimized (DPO)-Systeme
- FlexGroup Volumes
- FlexCache Volumes
- Globale Drosselung
- In einer Fan-out-Konfiguration kann nur eine Beziehung eine SnapMirror synchrone Beziehung sein. Alle anderen Beziehungen des Quell-Volumes 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 Snapshot Kopien
- 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 verfügt über zwei Betriebsmodi, abhängig vom Typ der verwendeten SnapMirror-Richtlinie:

- **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 die Fehlerbedingung korrigiert wird, werden SnapMirror Synchronous Technologie automatisch mit dem sekundären Storage neu synchronisiert und die Replizierung vom primären Speicher zum sekundären Storage im synchronen Modus fortgesetzt. 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.
- **StrictSync-Modus** SnapMirror Synchronous kann optional im StrictSync-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. Der Applikations-I/O zum primären System wird erst wieder aufgenommen, nachdem die SnapMirror Beziehung wieder auf zurückkehrt `InSync` Status: 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 SnapMirror Synchronous-Beziehung befindet sich immer im `InSync` Status während des normalen Betriebs. Wenn der SnapMirror Transfer aus irgendeinem Grund fehlschlägt, befindet sich das Ziel nicht im synchronen Modus mit der Quelle und kann mit dem fortfahren `OutofSync` Status:

Bei SnapMirror synchronen Beziehungen überprüft das System automatisch den Beziehungsstatus `InSync` Oder `OutofSync`) In einem festen Intervall. Wenn der Beziehungsstatus lautet `OutofSync`, ONTAP löst automatisch den automatischen Resync-Prozess, um die Beziehung auf die zurückzubringen `InSync` Status: 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 Funktionen wie z. B. `snapmirror quiesce` Und `snapmirror break` Führen Sie keine automatische Neusynchronisierung durch.

Wenn der Beziehungsstatus lautet `OutofSync` Für eine SnapMirror Synchronous-Beziehung im StrictSync-Modus werden alle I/O-Vorgänge zum primären Volume angehalten. Der `OutofSync` Status für SnapMirror Synchronous-Beziehung im Sync-Modus verursacht keine Unterbrechung für das primäre Volume und I/O-Vorgänge sind auf dem primären Volume zulässig.

Verwandte Informationen

"Technischer Bericht 4733 zu NetApp: Synchrone Konfiguration und Best Practices von SnapMirror"

Allgemeines zu Workloads, die von StrictSync- und Sync-Richtlinien unterstützt werden

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 Fileservices von Unternehmen wie Electronic Design Automation (EDA), Home Directories und Software-Build-Workloads 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 gehen diese Einschränkungen verloren und SnapMirror Synchronous kann für File Services-Workloads von Unternehmen mit Umgebungen für mehrere Benutzer eingesetzt werden, beispielsweise für Home Directorys und Software Build Workloads.

Verwandte Informationen

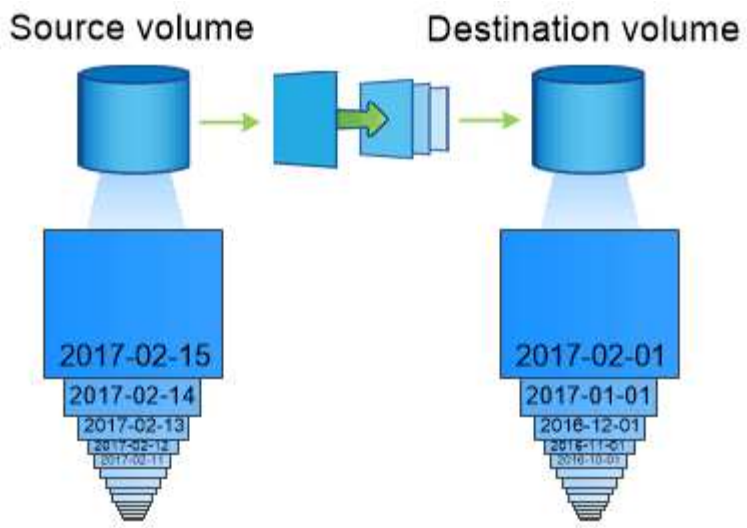
"SnapMirror Synchronous Configuration und Best Practices"

Vault-Archivierung mittels SnapMirror Technologie

Die Richtlinien von SnapMirror Vault ersetzen die SnapVault Technologie in ONTAP 9.3 und höher. Es wird eine SnapMirror Vault-Richtlinie für Disk-to-Disk Snapshot Kopien-Replizierung eingesetzt, um Compliance-Standards und andere Governance-bezogene Zwecke zu erfüllen. Im Gegensatz zu einer SnapMirror Beziehung, in der das Ziel normalerweise nur die derzeit im Quell-Volume befindlichen Snapshot-Kopien enthält, speichert ein Vault-Ziel in der Regel zeitpunktgenaue Snapshot-Kopien, die über einen längeren Zeitraum erstellt wurden.

Möglicherweise möchten Sie monatlich Snapshot Kopien Ihrer Daten über einen Zeitraum von 20 Jahren aufbewahren, um beispielsweise gesetzliche Buchhaltungsvorschriften für Ihr Unternehmen einzuhalten. 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.

Basistransfer unter der Standard-Vault-Richtlinie `XDPDefault` Erstellt eine Snapshot-Kopie des Quell-Volume und überträgt diese Kopie sowie die Datenblöcke, auf die sie auf das Ziel-Volume verweist. Im Gegensatz zu SnapMirror Beziehungen umfasst ein Vault-Backup keine älteren Snapshot-Kopien in der Baseline.

Aktualisierung von Vault-Datensicherungsbeziehungen

Updates werden asynchron und folgen dem von Ihnen konfigurierten Zeitplan. Die in der Richtlinie definierten Regeln für die Beziehung ermitteln, welche neuen Snapshot Kopien in Updates enthalten sein sollen, und wie viele Kopien sie aufbewahren sollen. Die in der Richtlinie definierten Labels (“monthly,” zum Beispiel) müssen mit einer oder mehreren in der Snapshot-Richtlinie auf der Quelle definierten Labels übereinstimmen. Andernfalls schlägt die Replizierung fehl.

Bei jedem Update unter dem `XDPDefault` Richtlinie: SnapMirror überträgt Snapshot Kopien, die seit der letzten Aktualisierung erstellt wurden, vorausgesetzt, sie verfügen über Labels, die mit den in den Richtlinienregeln definierten Beschriftungen übereinstimmen. In der folgenden Ausgabe von der `snapmirror policy show` Befehl für das `XDPDefault` Richtlinie, beachten Sie Folgendes:

- `Create Snapshot` Ist „`false`“, was darauf hinweist `XDPDefault` Erstellt keine Snapshot Kopie, wenn SnapMirror die Beziehung aktualisiert.
- `XDPDefault` Hat Regeln „`dily`“ und „`Weekly`“, die angeben, dass alle Snapshot-Kopien 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 -
-
```

Grundlagen der SnapMirror Unified Replication

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.

Basistransfer im Rahmen der Standard-Richtlinie für einheitliche Datensicherung `MirrorAndVault` Erstellt eine Snapshot-Kopie des Quell-Volume und überträgt diese Kopie sowie die Datenblöcke, auf die sie auf das Ziel-Volume verweist. Wie bei der Vault-Archivierung umfasst auch die Unified Data Protection keine älteren Snapshot-Kopien in der Basiskonfiguration.

Aktualisierung von Unified Datensicherungsbeziehungen

Bei jedem Update unter dem `MirrorAndVault` Richtlinie: SnapMirror erstellt eine Snapshot Kopie des Quell-Volume und überträgt diese Snapshot Kopie sowie alle Snapshot Kopien, die seit dem letzten Update erstellt

wurden, vorausgesetzt, sie verfügen über Labels, die mit den in den Snapshot-Richtlinienregeln definierten Labels definiert sind. In der folgenden Ausgabe von der `snapmirror policy show` Befehl für das `MirrorAndVault` Richtlinie, beachten Sie Folgendes:

- `Create Snapshot` Ist „`true`“, was darauf hinweist `MirrorAndVault` Erstellt eine Snapshot Kopie, wenn SnapMirror die Beziehung aktualisiert.
- `MirrorAndVault` Hat Regeln „`sm_created`“, „`dily`“ und „`Weekly`“, die angeben, dass sowohl die von SnapMirror erstellte Snapshot Kopie als auch die Snapshot Kopien mit übereinstimmenden Etiketten 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 Synchronous SnapMirror 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

Der vorkonfigurierten `Unified7year` Politik funktioniert genau wie `MirrorAndVault`, Außer dass eine vierte Regel monatliche Snapshot-Kopien überträgt und sie für sieben Jahre 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

Unified Replication beschränkt den Inhalt des Basistransfers auf die von SnapMirror bei der Initialisierung erstellte Snapshot Kopie. Bei jedem Update erstellt SnapMirror eine weitere Snapshot Kopie der Quelle und überträgt diese Snapshot Kopie sowie alle neuen Snapshot Kopien, deren Labels mit den in den Snapshot-Richtlinienregeln definiert sind.

Sie können sich gegen die Möglichkeit schützen, dass eine aktualisierte Snapshot-Kopie beschädigt wird, indem Sie eine Kopie der letzten übertragenen Snapshot-Kopie auf dem Zielsystem erstellen. Diese „`lokale Kopie`“ wird unabhängig von den Aufbewahrungsregeln auf der Quelle beibehalten. So wird auch wenn der ursprünglich von SnapMirror übertragene Snapshot nicht mehr auf der Quelle verfügbar ist, eine Kopie davon auf dem Ziel verfügbar.

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 herkömmliches Replikat könnte besser für ein Volume geeignet sein, das beispielsweise stündliche Snapshot Kopien von Datenbanktransaktionsprotokollen enthält.

XDP ersetzt DP als SnapMirror-Standard

Ab ONTAP 9.3 ersetzt der erweiterte Modus für Datensicherung (XDP) durch SnapMirror als SnapMirror Standard den SnapMirror Datensicherungs-Modus (DP).

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. Weitere Informationen finden Sie unter "Konvertieren einer bestehenden DP-Beziehung in XDP".

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. Ab ONTAP 9.5 ist MirrorAndVault die neue Standardrichtlinie, wenn kein Datenschutzmodus angegeben ist oder der XDP-Modus als Beziehungstyp angegeben wird. 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	MirrorAndVault (einheitliche Replizierung)
XDP	XDP	MirrorAndVault (einheitliche Replizierung)

Wie in der Tabelle dargestellt, stellen die XDP-Standardrichtlinien unter verschiedenen Umständen sicher, dass die Konvertierung die funktionale Äquivalenz der alten Typen bewahrt. 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.

Wenn ein Ziellaufwerk automatisch wächst

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.

Standardmäßig werden Datensicherungs-Volumes auf festgelegt `grow_shrink` autosize-Modus, der es ermöglicht, das Volumen als Reaktion auf die Menge des belegten Speicherplatzes zu vergrößern oder zu verkleinern. Die maximale automatische Größe für Datensicherungs-Volumes entspricht der maximalen FlexVol-Größe und ist plattformabhängig. Beispiel:

- FAS6220, standardmäßige max. Automatische DP-Volume-Größe = 70 TB
- FAS8200, Standard-max. Automatische Größe für DP Volume = 100 TB

Weitere Informationen finden Sie unter "NetApp Hardware Universe".

Fan-out- und kaskadierende Datensicherungsimplementierungen

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.

Sowohl Fan-out- als auch Kaskadenimplementierungen unterstützen eine beliebige Kombination aus SnapMirror DR, SnapVault oder einheitlicher Replizierung, allerdings unterstützen SnapMirror Synchronous Beziehungen (ab ONTAP 9.5 unterstützt) nur Fan-out-Implementierungen mit einer oder mehreren asynchronen SnapMirror Beziehungen und unterstützen keine Kaskadierung. Nur eine Beziehung in der Fan-out-Konfiguration kann eine SnapMirror synchrone Beziehung sein. Alle anderen Beziehungen des Quell-

Volumes müssen asynchrone SnapMirror Beziehungen sein. SnapMirror Business Continuity (Ab ONTAP 9.8 unterstützt) unterstützt auch Fan-out-Konfigurationen.

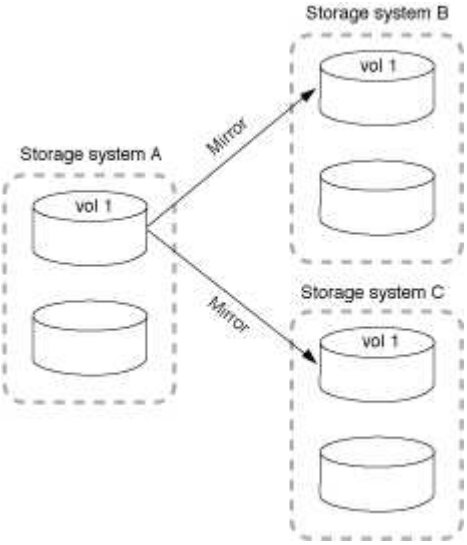
> Mithilfe einer *Fan-in*-Implementierung lassen sich Datensicherungsbeziehungen zwischen mehreren Primärsystemen und einem einzigen sekundären System erstellen. Für jede Beziehung muss auf dem sekundären System ein anderes Volume verwendet werden.

> 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.

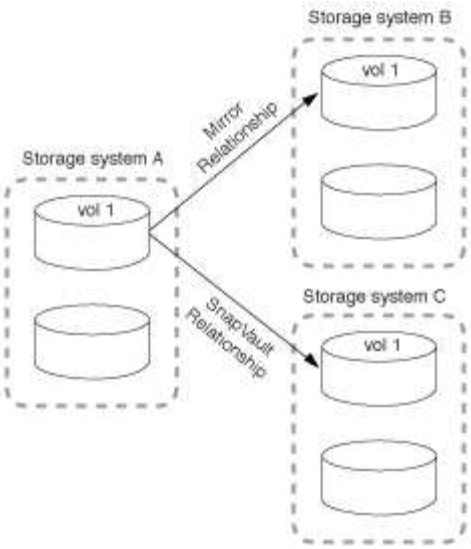
Funktionsweise von Fan-out-Implementierungen

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

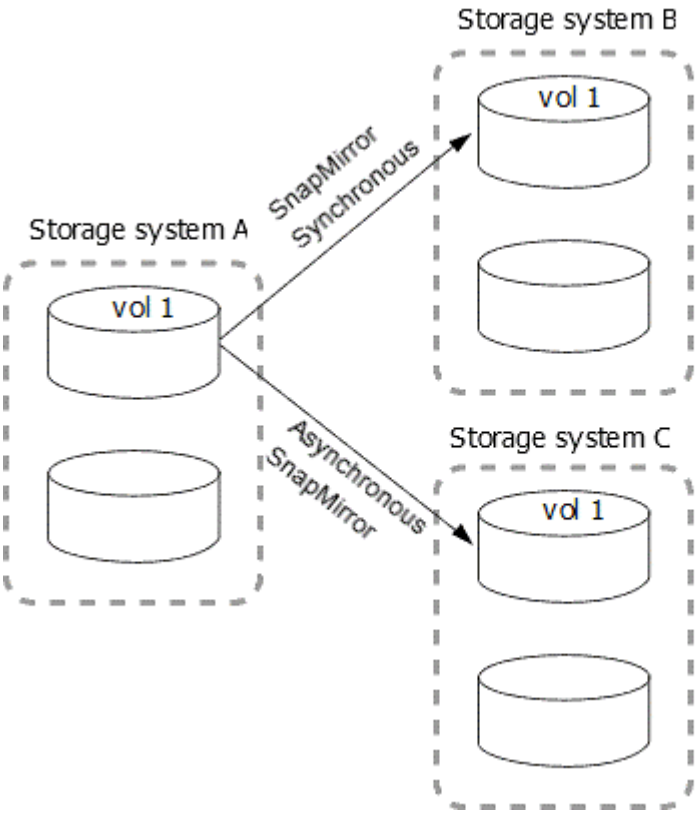
Eine Implementierung von Fan-out-Objekten aus mehreren Spiegelungen besteht aus einem Quell-Volume, das über eine Spiegelbeziehung zu mehreren sekundären Volumes verfügt.



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 genutzt werden. Allerdings kann nur eine Beziehung der Fan-out-Konfiguration eine synchrone SnapMirror Beziehung sein, alle anderen Beziehungen des Quell-Volume müssen asynchrone SnapMirror Beziehungen sein.

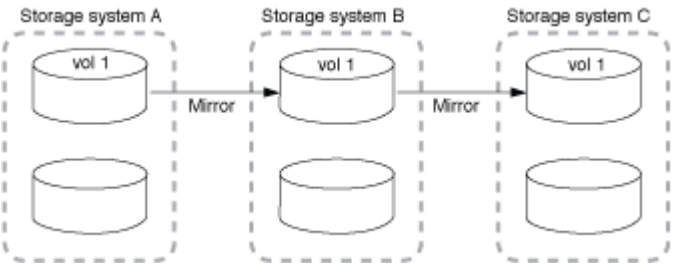


Funktionsweise der Kaskadierung

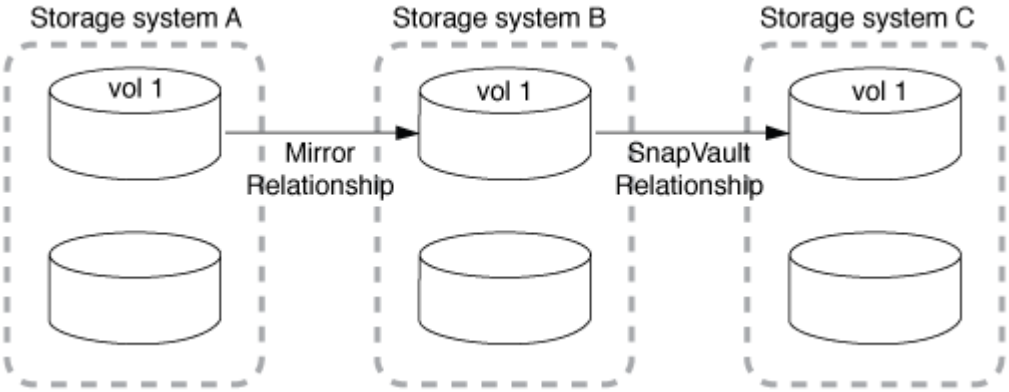
SnapMirror unterstützt *Mirror-Mirror*, *Mirror-Vault*, *Vault-Mirror* und *Vault-Vault* Kaskaden.

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.

Ab ONTAP 9.6 werden SnapMirror Synchronous Beziehungen in einer Kaskadierung mit Spiegelung unterstützt. Nur die primären und sekundären Volumes können sich in einer SnapMirror synchronen 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.



Auch Vault-Mirror und ab ONTAP 9.2 werden Vault-Kaskadierungs-Implementierungen 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.
- (Beginnend mit ONTAP 9.2) Eine Vault-Kaskadierung besteht aus einer Kette von Beziehungen, bei denen ein Quell-Volume auf ein sekundäres Volume verlagert wird und das sekundäre Volume auf ein tertiäres Volume verlagert wird.

Weitere Informationen

- Setzen Sie den Schutz in einer Fan-out-Konfiguration mit SM-BC fort

SnapMirror Lizenzierung

Übersicht über die 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 Version ONTAP 9.3 war eine separate SnapVault Lizenz erforderlich, um Vault Beziehungen zwischen ONTAP Instanzen zu konfigurieren, bei denen die DP-Instanz eine höhere Anzahl an Snapshot Kopien behalten konnte, um Backup-Anwendungsfälle mit längeren Aufbewahrungszeiten zu unterstützen. außerdem

wurde eine SnapMirror Lizenz benötigt, um Beziehungen zwischen ONTAP-Instanzen zu konfigurieren *mirror*, wobei jede ONTAP Instanz dieselbe Anzahl an Snapshot-Kopien beibehalten würde (d. h. ein *mirror* Image), um Disaster-Recovery-Anwendungsfälle zu unterstützen, um einen Cluster-Failover 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 Synchronous Lizenz

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

- Die SnapMirror Synchronous Lizenz ist sowohl auf dem Quell-Cluster 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 Bundle erworben wurde, können Sie einen NetApp Master Key herunterladen, um die erforderliche SnapMirror Synchronous Lizenz von der NetApp Support Website zu 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 ermöglicht die SnapMirror Cloud Lizenz die asynchrone Replizierung von Snapshot Kopien von ONTAP Instanzen in 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 auf vorkonfigurierte Objekt-Storage-Ziele 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.

Für den Aufbau einer SnapMirror Cloud-Beziehung benötigen Sie die folgenden Lizenzen:

- Sowohl eine SnapMirror Lizenz als auch eine SnapMirror Cloud Lizenz zur direkten Replizierung auf den Objektspeicher-Endpunkt.
- Bei der Konfiguration eines Workflows für die Replizierung mehrerer Richtlinien (z. B. Disk-to-Disk-to-Cloud) ist für alle ONTAP Instanzen eine SnapMirror Lizenz erforderlich, während die SnapMirror Cloud

Lizenz nur für das Quellcluster erforderlich ist, das sich direkt auf den Objekt-Storage-Endpunkt repliziert.

Ab ONTAP 9.9 ist dies möglich "Verwenden Sie System Manager für die SnapMirror Cloud-Replizierung".

Eine Liste autorisierter SnapMirror Cloud Applikationen von Drittanbietern wird 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".

SnapMirror Cloud Lizenzen installieren

SnapMirror Cloud-Beziehungen können über vorqualifizierte Backup-Applikationen von Drittanbietern orchestriert werden. Ab ONTAP 9.9 können Sie mit System Manager auch die SnapMirror Cloud Replizierung orchestrieren. Wenn Sie mit System Manager On-Premises-ONTAP über Objekt-Storage-Backups hinweg 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 S3 SnapMirror 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 erfordert die System Manager Orchestrierung von SnapMirror Cloud Backups in Objekt-Storage einen SnapMirror Cloud API-Schlüssel. 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 und 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. Folgen Sie den Anweisungen auf der NetApp Support-Website, um die SnapMirror Cloud API Lizenz anzufordern.

   "Fordern Sie den SnapMirror Cloud API-Lizenzschlüssel an"

4. Wenn Sie die Lizenzdateien erhalten und heruntergeladen haben, laden Sie die ONTAP Cloud

Compatibility NLF und die SnapMirror Cloud API-NLF mit System Manager auf den 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"

DPO-Systeme bieten Verbesserungen

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 der DPO-Lizenz das Zurückschalten von SnapMirror, die Volume-übergreifende Hintergrund-Deduplizierung, die Nutzung der Snapshot-Blöcke als Spender und die 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 dem aktiviert "DP_Optimized (DPO)-Lizenz". A "SnapMirror Lizenz" Ist weiterhin auf den Quell- und 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 die ausführen `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` Befehl zum Deduplizieren vorhandener Daten. Als Best Practice empfiehlt es sich, den Befehl in Zeiten geringerer Auslastung auszuführen, um die Auswirkungen auf die Performance zu verringern.

- Erhöhte Einsparungen durch Einsatz von Snapshot-Blöcken als Spender: Die Datenblöcke, die im aktiven File-System nicht verfügbar sind, aber in Snapshot-Kopien gefangen sind, werden als Spender für die Volume-Deduplizierung verwendet.

  Die neuen Daten können mit den Daten dedupliziert werden, die in Snapshot-Kopien gefangen sind, und zwar durch eine effektive gemeinsame Nutzung der Snapshot-Blöcke. Der größere Spenderbedarf sorgt für weitere Einsparungen, insbesondere wenn das Volume über eine große Anzahl von Snapshot-Kopien verfügt.

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

Managen Sie die SnapMirror Volume-Replizierung

SnapMirror Replizierungs-Workflow

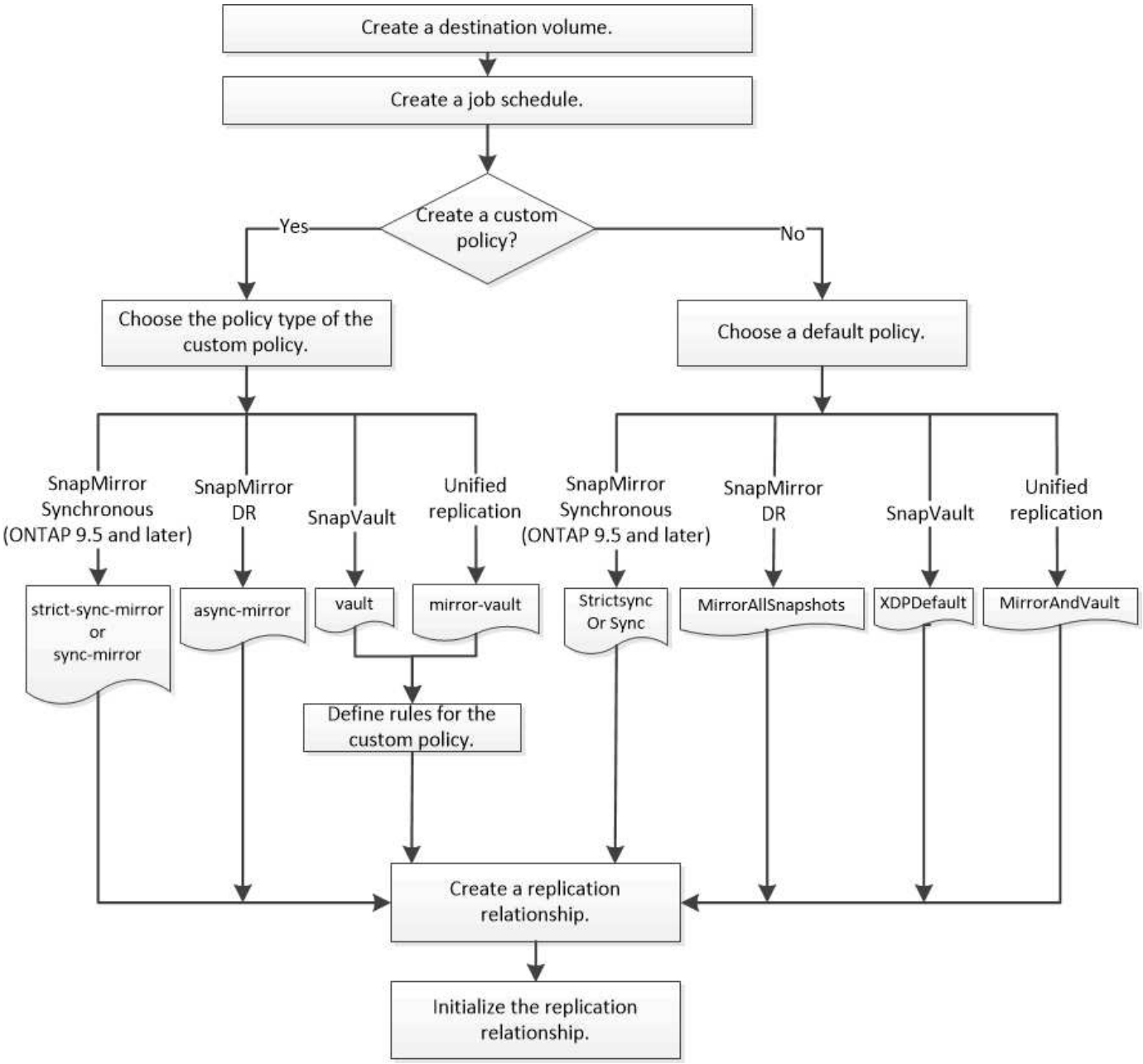
SnapMirror bietet drei Arten von Datensicherungsbeziehungen: SnapMirror DR, Archiv (ehemals SnapVault) und einheitliche Replizierung. Sie können denselben grundlegenden Workflow verwenden, um die einzelnen Beziehungstypen zu konfigurieren.

Ab der allgemeinen Verfügbarkeit ab ONTAP 9.9 bietet SnapMirror Business Continuity (SM-BC) eine Recovery Time Objective (Zero RTO) oder ein transparentes Applikations-Failover (TAF) für den automatischen Failover geschäftskritischer Applikationen in SAN-Umgebungen. SM-BC wird in einer Konfiguration von zwei AFF-Clustern oder zwei All-Flash SAN-Array (ASA)-Clustern unterstützt.

"NetApp Dokumentation: SnapMirror Business Continuity"

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 den verwenden `snapmirror protect` Befehl zum Konfigurieren einer Datensicherungsbeziehung in einem einzigen Schritt. Auch wenn Sie verwenden `snapmirror protect`, Sie müssen jeden Schritt im Workflow verstehen.



Konfigurieren Sie eine Replikationsbeziehung in einem Schritt

Ab ONTAP 9.3 können Sie den verwenden `snapmirror protect` Befehl zum Konfigurieren einer Datensicherungsbeziehung in einem einzigen Schritt. Sie legen eine Liste der zu replizierenden Volumes, eine SVM auf dem Ziel-Cluster, einen Job-Zeitplan und eine SnapMirror Richtlinie fest. `snapmirror protect` Erledigt den Rest.

Was Sie benötigen

- 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` Der 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 Ziel-Volume lautet des Formulars *`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 im Lieferumfang enthaltene `dst` Suffix:

Ab ONTAP 9.3 und älteren Versionen kann ein Ziel-Volume bis zu 251 Snapshot Kopien enthalten. Ab ONTAP 9.4 kann ein Ziel-Volume bis zu 1019 Snapshot Kopien enthalten.

> Initialisierung kann sehr zeitaufwendig sein. `snapmirror protect` Wartet nicht, bis die Initialisierung abgeschlossen ist, bevor der Job beendet wird. Aus diesem Grund sollten Sie die verwenden `snapmirror show` Befehl statt des `job show` Befehl zum Bestimmen, wann die Initialisierung abgeschlossen ist.

Ab ONTAP 9.5 können synchrone SnapMirror Beziehungen mithilfe der erstellt werden `snapmirror protect` Befehl.

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. Der `-auto -initialize` Die Option ist standardmäßig auf „`true`“ eingestellt.

   Das folgende Beispiel erstellt und initialisiert eine SnapMirror DR-Beziehung unter Verwendung der Standardeinstellung `MirrorAllSnapshots` Richtlinie:

   ```
   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 unter Verwendung der Standardeinstellung erstellt und initialisiert `XDPDefault` Richtlinie:

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

Das folgende Beispiel erstellt und initialisiert eine einheitliche Replikationsbeziehung unter Verwendung der Standardwerte `MirrorAndVault` Richtlinie:

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

Das folgende Beispiel erstellt und initialisiert eine SnapMirror synchrone Beziehung unter Verwendung der Standardeinstellung `Sync` Richtlinie:

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

> Bei SnapVault- und Unified Replication-Richtlinien kann es sich als nützlich erweisen, einen Zeitplan für die Erstellung einer Kopie der zuletzt übertragenen Snapshot Kopie auf dem Zielsystem zu definieren. Weitere Informationen finden Sie unter "Definieren eines Zeitplans zum Erstellen einer lokalen Kopie auf dem Ziel".

Nachdem Sie fertig sind

Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Konfigurieren Sie eine Replikationsbeziehung in einem Schritt nach dem anderen

Erstellen eines Ziel-Volumes

Sie können das verwenden `volume create` Befehl auf dem Ziel, ein Ziel-Volume zu erstellen. Das Zielvolumen sollte gleich oder größer sein als das Quellvolumen.

Schritt

1. Ziel-Volume erstellen:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

Erstellen eines Replikationsauftrags

Sie können das verwenden `job schedule cron create` Befehl zum Erstellen eines Replikationsauftragplans. Der Job-Zeitplan legt fest, wann SnapMirror die Datensicherungsbeziehung automatisch aktualisiert, denen der Zeitplan zugewiesen ist.

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.

Schritt

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`, Sie können angeben `all` Zum Ausführen des Jobs jeden Monat, Wochentag und Stunde.

   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 Job-Zeitplan mit dem Namen erstellt `my_weekly` Das läuft samstags um 3:00 Uhr:

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

Anpassen einer Replizierungsrichtlinie

Erstellen Sie eine benutzerdefinierte Replikationsrichtlinie

Sie können eine benutzerdefinierte Replikationsrichtlinie erstellen, wenn die Standardrichtlinie für eine Beziehung nicht geeignet ist. Möglicherweise möchten Sie z. B. Daten in einem Netzwerktransfer komprimieren oder die Anzahl der Versuche ändern,

wie SnapMirror Snapshot Kopien übertragen möchte.

Sie können eine Standard- oder benutzerdefinierte Richtlinie verwenden, wenn Sie eine Replikationsbeziehung erstellen. Bei einem benutzerdefinierten Archiv (früher SnapVault) oder einer einheitlichen Replizierungsrichtlinie müssen Sie ein oder mehrere *rules* definieren, die bestimmen, welche Snapshot Kopien während der Initialisierung und des Updates übertragen werden. Möglicherweise möchten Sie auch einen Zeitplan für das Erstellen lokaler Snapshot Kopien auf dem Ziel festlegen.

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 Synchronous im StrictSync-Modus (unterstützt ab ONTAP 9.5)
Synchrone Spiegelung	SnapMirror Synchronous im Sync-Modus (unterstützt ab ONTAP 9.5)

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

Schritt

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
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Ab ONTAP 9.5 können Sie den Zeitplan für das Erstellen eines gemeinsamen Zeitplans für SnapMirror Synchronous Beziehungen mit dem festlegen `-common-snapshot-schedule` Parameter. Standardmäßig beträgt der Zeitplan für synchrone Snapshot-Kopien für SnapMirror Beziehungen eine Stunde. Für den Zeitplan der Snapshot-Kopien für synchrone Beziehungen von SnapMirror können Sie einen Wert von 30 Minuten bis zwei Stunden 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 im StrictSync-Modus eine benutzerdefinierte Replizierungsrichtlinie für die SnapMirror Synchronous-Beziehung erstellt:

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

Nachdem Sie fertig sind

Bei den Richtlinientypen „`Vault`“ und „`mmirror-Vault`“ müssen Regeln definiert werden, die festlegen, welche Snapshot-Kopien während der Initialisierung und Aktualisierung übertragen werden.

Verwenden Sie die `snapmirror policy show` Befehl zur Überprüfung, ob die SnapMirror-Richtlinie erstellt wurde Eine vollständige Befehlssyntax finden Sie in der man-Page.

Definieren Sie eine Regel für eine Richtlinie

Für benutzerdefinierte Richtlinien mit dem Richtlinientyp „`Vault`“ oder „`mmirror-Vault`“ müssen Sie mindestens eine Regel definieren, die bestimmt, welche Snapshot-Kopien während der Initialisierung und Aktualisierung übertragen werden. Sie können auch Regeln für Standardrichtlinien mit dem Richtlinientyp „`Vault`“ oder „ `mmirror-Vault`“ definieren.

Über diese Aufgabe

Jede Richtlinie mit dem Richtlinientyp „`Vault`“ oder „`mMirror-Vault`“ muss über eine Regel verfügen, die festlegt, welche Snapshot Kopien repliziert werden sollen. Die Regel „`bi-monthly`“ gibt beispielsweise an, dass nur Snapshot Kopien, denen das SnapMirror Label „`bi-monthly`“ zugewiesen wurde, repliziert werden sollten. 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	Eine von SnapMirror erstellte Snapshot Kopie wird bei Initialisierung und Update übertragen.
All_Source_Snapshots	Asynchrone Spiegelung	Neue Snapshot Kopien auf der Quelle werden bei Initialisierung und Update übertragen.
Täglich	Vault, Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`dily`“ werden bei Initialisierung und Update übertragen.
Wöchentlich	Vault, Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`Weekly`“ werden bei Initialisierung und Update übertragen.
Monatlich	Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`monthly`“ werden bei Initialisierung und Update übertragen.
Applikationskonsistent	Sync, StrictSync	Snapshot-Kopien mit dem SnapMirror-Label „`App_konsistenter`“ auf der Quelle werden synchron zum 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 Standardeinstellung `MirrorAndVault` Richtlinie: Sie können eine Regel mit dem Namen „`bi-monthly`“ erstellen, die Snapshot-Kopien der Quelle mit dem „`bi-monthly`“ SnapMirror Label übereinstimmt.
- Für eine individuelle Policy mit dem Richtlinientyp „`mmirror-Vault`“ könnten Sie eine Regel namens „`bi-Weekly`“ erstellen, die Snapshot-Kopien auf der Quelle mit dem „`bi-Weekly`“ SnapMirror-Etikett übereinstimmt.

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`*

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird eine Regel mit dem SnapMirror-Label hinzugefügt `bi-monthly` Auf den Standardwert `MirrorAndVault` Richtlinie:

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

Im folgenden Beispiel wird eine Regel mit dem SnapMirror-Label hinzugefügt `bi-weekly` Auf den Benutzer `my_snapvault` Richtlinie:

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

Im folgenden Beispiel wird eine Regel mit dem SnapMirror-Label hinzugefügt `app_consistent` Auf den Benutzer `Sync` Richtlinie:

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

Sie können dann Snapshot Kopien aus dem Quell-Cluster replizieren, die mit diesem SnapMirror Etikett übereinstimmen:

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

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

Für SnapVault und einheitliche Replizierungsbeziehungen können Sie sich vor der Möglichkeit schützen, dass eine aktualisierte Snapshot Kopie beschädigt wird, indem Sie eine Kopie der zuletzt übertragenen Snapshot Kopie auf dem Zielsystem erstellen. Diese „`lokale Kopie`“ wird unabhängig von den Aufbewahrungsregeln auf der Quelle beibehalten. So wird auch wenn der ursprünglich von SnapMirror übertragene Snapshot nicht mehr auf der Quelle verfügbar ist, eine Kopie davon auf dem Ziel verfügbar.

Über diese Aufgabe

Sie legen den Zeitplan für das Erstellen einer lokalen Kopie in fest `-schedule` Option des `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`

Eine vollständige Befehlssyntax finden Sie in der man-Page. Informationen zum Erstellen eines Jobplans finden Sie unter "Erstellen eines Replikationsauftragplans".

Im folgenden Beispiel wird ein Zeitplan zum Erstellen einer lokalen Kopie zum Standard hinzugefügt `MirrorAndVault` Richtlinie:

```
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 zum benutzerdefinierten hinzugefügt `my_unified` Richtlinie:

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

Erstellen einer Replikationsbeziehung

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

Was Sie benötigen

- 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 Standardeinstellung zu erhalten `MirrorAllSnapshots` Richtlinie:

- 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 9.3 und älteren Versionen kann ein Ziel-Volume bis zu 251 Snapshot Kopien enthalten. Ab ONTAP 9.4 kann ein Ziel-Volume bis zu 1019 Snapshot Kopien enthalten.

Ab ONTAP 9.5 werden SnapMirror Synchronous Beziehungen unterstützt.

Schritt

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>
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

> Der `schedule` Der Parameter ist beim Erstellen von synchronen SnapMirror Beziehungen nicht anwendbar.

Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mit dem Standard erstellt `MirrorLatest` Richtlinie:

```
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 mit dem Standard erstellt `XDPDefault` Richtlinie:

```
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 eine einheitliche Replizierungsbeziehung mit dem Standard erstellt `MirrorAndVault` Richtlinie:

```
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 eine einheitliche Replikationsbeziehung mit dem benutzerdefinierten erstellt `my_unified` Richtlinie:

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

Das folgende Beispiel erstellt eine SnapMirror Synchronous-Beziehung unter Verwendung des Standards `Sync` Richtlinie:

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

Das folgende Beispiel erstellt eine SnapMirror Synchronous-Beziehung unter Verwendung des Standards `StrictSync` Richtlinie:

```
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 die Richtlinie standardmäßig auf das gesetzt `MirrorAllSnapshots` Richtlinie:

```
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 gesetzt `MirrorAllSnapshots` Richtlinie:

```
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 wurde, wird die Richtlinie standardmäßig auf das gesetzt `XDPDefault` Richtlinie:

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

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

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

> Die vordefinierte Richtlinie `SnapCenterSync` Ist des Typs `Sync`. Diese Richtlinie repliziert alle Snapshot Kopien, die zusammen mit erstellt werden `snapmirror-label` Von „App_konsistent“.

Nachdem Sie fertig sind

Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

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…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Konfigurieren von Spiegelungen und Vaults"
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Volume Backup mit SnapVault – Übersicht"

Initialisieren Sie eine Replikationsbeziehung

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

Was Sie benötigen

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 SnapMirror Synchronous Beziehungen unterstützt.

Schritt

1. Initialisieren einer Replikationsbeziehung:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

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

Beispiel: Konfiguration einer Vault-Vault-Kaskade

Ein Beispiel zeigt in konkreten Worten, wie Sie Replikationsbeziehungen nacheinander konfigurieren können. Sie können die im Beispiel konfigurierte Vault-Vault-Kaskadierung verwenden, um mehr als 251 Snapshot-Kopien mit der Bezeichnung „`my-Weekly`“ aufzubewahren.

Was Sie benötigen

- Quell- und Ziel-Cluster sowie SVMs müssen Peering durchgeführt werden.
- Sie müssen ONTAP 9.2 oder höher ausführen. Vault-Vault-Kaskaden werden in früheren ONTAP Versionen nicht unterstützt.

Über diese Aufgabe

Im Beispiel wird Folgendes vorausgesetzt:

- Sie haben Snapshot Kopien auf dem Quell-Cluster mit den SnapMirror-Labels „`my-Daily`“, „`my-Weekly`“ und „`my-monthly`“ konfiguriert.
- Sie haben Ziel-Volumes mit dem Namen „`Vola`“ auf den sekundären und tertiären Ziel-Clustern konfiguriert.
- Sie haben die Zeitpläne für Replikationsjobs mit dem Namen „`my_snapvault`“ auf den sekundären und tertiären Ziel-Clustern konfiguriert.

Das Beispiel zeigt, wie Replikationsbeziehungen auf Grundlage von zwei benutzerdefinierten Richtlinien erstellt werden:

- Die Richtlinie „`snapvault_secondary`“ speichert täglich 7, 52 wöchentlich und 180 monatliche Snapshot Kopien auf dem sekundären Ziel-Cluster.
- Die „`snapvault_tertiary Policy`“ speichert 250 wöchentliche Snapshot-Kopien auf dem tertiären Ziel-Cluster.

Schritte

1. Erstellen Sie auf dem sekundären Ziel-Cluster die Richtlinie „`snapVault_secondary`“:

   ```
   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 Regel „`my-Daily`“ für die Richtlinie:

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

3. Legen Sie auf dem sekundären Ziel-Cluster die Regel „`my-Weekly`“ für die Richtlinie fest:

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

4. Legen Sie auf dem sekundären Ziel-Cluster die Regel „`my-monthly`“ für die Richtlinie fest:

   ```
   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 Richtlinie „`snapVault_tertiary`“:

```
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 Regel „`my-Weekly`“ 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
```

Konvertieren einer bestehenden 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.

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. Hintergrundinformationen finden Sie unter "XDP ersetzt DP als SnapMirror-Standard".
- 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>
   ```

   Das folgende Beispiel zeigt die Ausgabe von im `snapmirror show` Befehl:

   ```
   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
   ```

> Sie könnten es hilfreich finden, eine Kopie des zu behalten `snapmirror show` Befehlsausgabe zum Verfolgen der Beziehungseinstellungen.

2. Von den Quell- und Ziel-Volumes aus, stellen Sie sicher, dass beide Volumes eine gemeinsame Snapshot Kopie aufweisen:

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

Das folgende Beispiel zeigt die `volume snapshot show` Ausgabe für die Quell- und Zielvolumes:

```
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>
```

Eine vollständige Befehlssyntax finden Sie im "Man-Page".

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

Das folgende Beispiel legt die Beziehung zwischen dem Quell-Volume fest `volA` Ein `svm1` Und dem Ziel-Volume `volA_dst` Ein `svm_backup`:

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

4. Bestehende DP-TYPE Beziehung aufbrechen:

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

Eine vollständige Befehlssyntax finden Sie im "Man-Page".

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

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

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

5. Wenn das automatische Löschen von Snapshot-Kopien auf dem Ziel-Volume aktiviert ist, deaktivieren Sie sie:

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

Im folgenden Beispiel wird das Löschen von Snapshot Kopien auf dem Ziel-Volume 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>
```

Eine vollständige Befehlssyntax finden Sie im "Man-Page".

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

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume gelöscht `volA` Ein `svm1` Und dem Ziel-Volume `volA_dst` Ein `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
```

8. Sie können die Ausgabe verwenden, die Sie im beibehalten haben `snapmirror show` Befehl zum Erstellen der neuen XDP-Typ-Beziehung:

```
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. Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

Im folgenden Beispiel wird eine Disaster Recovery-Beziehung zwischen dem Quell-Volume in SnapMirror erstellt `volA` Ein `svm1` Und dem Ziel-Volume `volA_dst` Ein `svm_backup` Die Standardeinstellung wird verwendet `MirrorAllSnapshots` Richtlinie:

```
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>
```

Zur Verbesserung der Neusynchronisierung können Sie das verwenden `-quick-resync` Option, aber Sie sollten beachten, dass Einsparungen durch Storage-Effizienz verloren gehen können. Eine vollständige Befehlssyntax finden Sie in der man-Page: "SnapMirror Resync-Befehl".

> 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 neu synchronisiert `volA` Ein `svm1` Und dem Ziel-Volume `volA_dst` Ein `svm_backup`:

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

10. Wenn Sie das automatische Löschen von Snapshot Kopien deaktiviert haben, aktivieren Sie sie erneut:

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

Nachdem Sie fertig sind

1. Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde.
2. Sobald das SnapMirror XDP Ziel-Volume mit der Aktualisierung von Snapshot Kopien gemäß den Definitionen in der SnapMirror Richtlinie beginnt, verwenden Sie die Ausgabe von `snapmirror list-destinations` Befehl aus dem Quell-Cluster, um die neue SnapMirror XDP-Beziehung anzuzeigen.

Konvertieren der Art einer SnapMirror Beziehung

Ab ONTAP 9.5 wird SnapMirror Synchronous unterstützt. Sie können eine asynchrone SnapMirror Beziehung in eine synchrone SnapMirror Beziehung umwandeln oder umgekehrt, ohne einen Basistransfer durchführen zu müssen.

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 zu einer SnapMirror Synchronous Beziehung**

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

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

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

b. Geben Sie die SnapMirror Beziehung aus dem Quell-Cluster frei, ohne die gemeinsamen Snapshot Kopien zu löschen:

   `snapmirror release -relationship-info-only true -destination-path` *`dest_SVM:dest_volume`*

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

c. Erstellen Sie aus dem Ziel-Cluster eine SnapMirror Synchronous-Beziehung:

   `snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path` *`dest_SVM:dest_volume`* `-policy sync-mirror`

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

d. SnapMirror Synchronous-Beziehung neu synchronisieren:

   `snapmirror resync -destination-path` *`dest_SVM:dest_volume`*

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

- **Umwandlung einer SnapMirror Synchronous Beziehung in eine asynchrone SnapMirror Beziehung**

a. Vom Ziel-Cluster aus, die bestehende SnapMirror Synchronous Beziehung stilllegen:

   `snapmirror quiesce -destination-path dest_SVM:dest_volume`

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

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

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

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

c. Geben Sie die SnapMirror Beziehung aus dem Quell-Cluster frei, ohne die gemeinsamen Snapshot Kopien zu löschen:

   `snapmirror release -relationship-info-only true -destination-path`

dest_SVM:dest_volume

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. Erstellen Sie im Ziel-Cluster eine asynchrone SnapMirror Beziehung:

   `snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path` *`dest_SVM:dest_volume`* `-policy MirrorAllSnapshots`

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. SnapMirror Synchronous-Beziehung neu synchronisieren:

   `snapmirror resync -destination-path` *`dest_SVM:dest_volume`*

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

Konvertieren Sie den Modus einer SnapMirror Synchronous Beziehung

Ab ONTAP 9.5 werden SnapMirror Synchronous Beziehungen unterstützt. Sie können den Modus einer SnapMirror Synchronous Beziehung von StrictSync in Sync konvertieren oder umgekehrt.

Über diese Aufgabe

Sie können die Richtlinie einer SnapMirror Synchronbeziehung nicht zur Konvertierung seines Modus ändern.

Schritte

1. Vom Ziel-Cluster aus, die bestehende SnapMirror Synchronous Beziehung stilllegen:

   `snapmirror quiesce -destination-path dest_SVM:dest_volume`

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

2. Löschen Sie im Zielcluster die vorhandene SnapMirror Synchronous Beziehung:

   `snapmirror delete -destination-path dest_SVM:dest_volume`

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

3. Geben Sie die SnapMirror Beziehung aus dem Quell-Cluster frei, ohne die gemeinsamen Snapshot Kopien zu löschen:

```
snapmirror release -relationship-info-only true -destination-path
dest_SVM:dest_volume
```

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. Erstellen Sie aus dem Ziel-Cluster eine SnapMirror Synchronous-Beziehung, indem Sie den Modus angeben, in den Sie die SnapMirror Synchronous-Beziehung konvertieren möchten:

   ```
   snapmirror create -source-path vs1:vol1 -destination-path dest_SVM:dest_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 dest_SVM:dest_volume
   ```

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

Erstellen und Löschen von 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 ⋮ Wählen Sie neben der Beziehungsquelle **Test Failover**.
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 > Share**.
6. Klicken Sie Auf + Add Und wählen Sie **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. Öffnen Sie die Freigabe auf dem Client, und überprüfen Sie, ob das Testvolume Lese- und Schreibfähigkeiten 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 ⋮ Wählen Sie neben der Beziehungsquelle **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 Zielvolumen schreibbar machen

Sie müssen das Ziel-Volume schreibbar machen, bevor Sie Daten vom Volume an die Clients bereitstellen können. Sie können das verwenden `snapmirror quiesce` Befehl zum Anhalten geplanter Transfers an das Ziel, das `snapmirror abort` Befehl zum Beenden laufender Transfers, und `snapmirror break` Befehl, um das Ziel beschreibbar zu machen.

Über diese Aufgabe

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

Schritte

1. Geplante Transfers zum Ziel anhalten:

   ```
   snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, …
   -destination-path SVM:volume|cluster://SVM/volume, …
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

2. Laufende Transfers zum Ziel anhalten:

   `snapmirror abort -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination -path` *`SVM:volume|cluster://SVM/volume, …`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

   Im folgenden Beispiel werden kontinuierliche Transfers zwischen dem Quell-Volume angehalten `volA` Ein `svm1` Und dem Ziel-Volume `volA_dst` Ein `svm_backup`:

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

3. SnapMirror DR-Beziehung unterbrechen:

   `snapmirror break -source-path` *`SVM:volume|cluster://SVM/volume, …`* `-destination -path` *`SVM:volume|cluster://SVM/volume, …`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

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"
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Übersicht über die Disaster Recovery von Volumes"

Ziel-Volume für Datenzugriff konfigurieren

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.

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

Aktivieren Sie das ursprüngliche Quellvolume 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
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > 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 eine allgemeine Snapshot Kopie nicht auf dem Quell- und Zielsystem vorhanden ist. Nutzung `snapmirror initialize` Um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Quell-Volume umkehren: `volA`

Ein `svm1`, Und dem Volumen, von dem Sie Daten bereitstellen, `volA_dst` Ein `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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > 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
   ```

3. Aktualisierung der umgekehrten Beziehung:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

   Im folgenden Beispiel wird die Beziehung zwischen dem Volume, von dem Sie Daten bereitstellen, aktualisiert. `volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `volA` Ein `svm1`:

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

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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

   Im folgenden Beispiel werden geplante Transfers zwischen dem ursprünglichen Ziel-Volume angehalten,

`volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `volA` Ein `svm1`:

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

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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

   Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Zielvolumen unterbrochen. `volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `volA` Ein `svm1`:

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

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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > 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 Quell-Volume gelöscht, `volA` Ein `svm1`, Und dem Volumen, von dem Sie Daten bereitstellen, `volA_dst` Ein `svm_backup`:

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

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 Ziel-Volume freigegeben. `volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `volA` Ein `svm1`:

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

8. Wiederherstellung der ursprünglichen Datensicherungsbeziehung vom ursprünglichen Zielort:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Quell-Volume wiederhergestellt. `volA` Ein `svm1`, Und das ursprüngliche Ziel Volumen, `volA_dst` Ein `svm_backup`:

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

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

   `vserver start -vserver` *`SVM`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die ursprüngliche Ziel-SVM gestartet:

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

Nachdem Sie fertig sind

Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Wiederherstellung von Dateien aus einem SnapMirror Ziel-Volume

Wiederherstellung einer einzelnen Datei, einer LUN oder eines NVMe Namespace von einem SnapMirror Ziel aus

Sie können eine einzelne Datei, eine LUN, eine Gruppe von Dateien oder LUNs aus einer Snapshot Kopie oder einen NVMe Namespace über ein SnapMirror Ziel-Volume wiederherstellen. Ab ONTAP 9.7 sind auch NVMe Namespaces von einem synchronen SnapMirror Ziel wiederhergestellt. Sie können Dateien auf dem ursprünglichen Quell-Volume oder auf einem anderen Volume wiederherstellen.

Was Sie benötigen

Um eine Datei oder LUN von einem synchronen SnapMirror Ziel (unterstützt ab ONTAP 9.5) wiederherzustellen, müssen Sie die Beziehung zuerst 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 eine gemeinsame Snapshot Kopie aufweisen (wie normalerweise bei der Wiederherstellung des ursprünglichen Quell-Volumes der Fall ist).
- Anderenfalls führt SnapMirror eine *Baseline Restore* durch, bei der die angegebene Snapshot Kopie und alle Datenblöcke, auf die sie Bezug nehmen, an das Ziel-Volume übertragen werden.

Schritte

1. Auflisten der Snapshot Kopien auf dem Ziel-Volume:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Snapshot Kopien auf der angezeigt `vserverB:secondary1` Ziel:

```
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. Wiederherstellung einer einzelnen Datei oder einer LUN oder eines Satzes von Dateien oder LUNs aus einer Snapshot Kopie in einem SnapMirror Ziel-Volume:

   `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`*

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

Mit dem folgenden Befehl werden die Dateien wiederhergestellt `file1` Und `file2` Aus der Snapshot Kopie `daily.2013-01-25_0010` Im ursprünglichen Ziel-Volume `secondary1`, An denselben Speicherort im aktiven Dateisystem des ursprünglichen Quell-Volume `primary1`:

```
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 wiederhergestellt `file1` Und `file2` Aus der Snapshot Kopie `daily.2013-01-25_0010` Im ursprünglichen Ziel-Volume `secondary1`, An einen anderen Speicherort im aktiven Dateisystem des ursprünglichen Quell-Volume `primary1`.

Der Zieldateipfad beginnt mit dem Symbol @, gefolgt vom Pfad der Datei aus dem Stammverzeichnis des ursprünglichen Quell-Volumes. In diesem Beispiel `file1` Wird auf wiederhergestellt `/dir1/file1.new` Und file2 wird auf wiederhergestellt `/dir2.new/file2` Ein `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 wiederhergestellt `file1` Und `file3` Aus der Snapshot Kopie `daily.2013-01-25_0010` Im ursprünglichen Ziel-Volume `secondary1`, Zu verschiedenen Speicherorten im aktiven Dateisystem des ursprünglichen Quell-Volume `primary1`, Und Wiederherstellung `file2` Von `snap1` An denselben Speicherort im aktiven Filesystem von `primary1`.

In diesem Beispiel wird die Datei angezeigt `file1` Wird auf wiederhergestellt `/dir1/file1.new` Und `file3` Wird auf wiederhergestellt `/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
```

Stellen Sie den Inhalt eines Volumes von einem SnapMirror-Ziel wieder her

Sie können den Inhalt eines gesamten Volumes von einer Snapshot Kopie in 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

Das Ziel-Volume für den Wiederherstellungsvorgang muss einer der folgenden Werte aufweisen:

- Ein Lese-Schreib-Volume, in diesem Fall führt SnapMirror eine *inkrementelle Wiederherstellung* durch, vorausgesetzt, dass die Quell- und Ziel-Volumes eine gemeinsame Snapshot Kopie haben (wie typischerweise bei der Wiederherstellung des ursprünglichen Quell-Volume).

  > Der Befehl schlägt fehl, wenn keine gemeinsame Snapshot-Kopie 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 dem die angegebene Snapshot Kopie und alle Datenblöcke, auf die er verweist, auf 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 das verwenden `volume quota modify` Befehl zum Reaktivieren von Quota-Regeln, nachdem der Wiederherstellungsvorgang abgeschlossen ist.

Schritte

1. Auflisten der Snapshot Kopien auf dem Ziel-Volume:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Snapshot Kopien auf der angezeigt `vserverB:secondary1` Ziel:

```
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 einer Snapshot Kopie in einem SnapMirror Ziel-Volume:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

   Mit dem folgenden Befehl wird der Inhalt des ursprünglichen Quell-Volume wiederhergestellt `primary1` Aus der Snapshot Kopie `daily.2013-01-25_0010` Im ursprünglichen Ziel-Volume `secondary1`:

```
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 copy 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…
Der neu gestaltete System Manager (verfügbar ab ONTAP 9.7)	"Wiederherstellung eines Volume aus einer früheren Snapshot Kopie"
System Manager Classic (verfügbar mit ONTAP 9.7 und älter)	"Volume-Wiederherstellung mithilfe von SnapVault – Übersicht"

Aktualisieren Sie eine Replikationsbeziehung manuell

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 SnapMirror Synchronous 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 die ausführen `snapmirror update` Befehl.

Schritt

1. Manuelles Aktualisieren einer Replikationsbeziehung:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

> Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen. Der Befehl schlägt fehl, wenn eine allgemeine Snapshot Kopie nicht auf dem Quell- und Zielsystem vorhanden ist. Nutzung `snapmirror initialize` Um die Beziehung neu zu initialisieren.

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume aktualisiert `volA` Ein `svm1` Und dem Ziel-Volume `volA_dst` Ein `svm_backup`:

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

Synchronisieren Sie eine Replikationsbeziehung neu

Sie müssen eine Replizierungsbeziehung neu synchronisieren, nachdem Sie ein Ziel-Volume schreibbar machen, nachdem ein Update fehlschlägt, weil eine gemeinsame Snapshot-Kopie nicht auf den Quell- und Ziel-Volumes vorhanden ist oder Sie die Replizierungsrichtlinie für die Beziehung ändern möchten.

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.

Schritt

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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

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

Löschen einer Volume-Replikationsbeziehung

Sie können das verwenden `snapmirror delete` Und `snapmirror release` Befehle zum Löschen einer Replikationsbeziehung für Volumes. Sie können dann nicht benötigte

Ziel-Volumes manuell löschen.

Über diese Aufgabe

Der `snapmirror release` Befehl löscht alle durch SnapMirror erstellten Snapshot Kopien aus der Quelle. Sie können das verwenden `-relationship-info-only` Option zum Bewahren der Snapshot Kopien.

Schritte

1. Replikationsbeziehung stilllegen:

   `snapmirror quiesce -destination-path` *`SVM:volume|cluster://SVM/volume`*

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

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
   ```

3. Löschen Sie die Replikationsbeziehung:

   `snapmirror delete -source-path` *`SVM:volume|cluster://SVM/volume`*`, … -destination -path` *`SVM:volume|cluster://SVM/volume`*`, …`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Sie müssen diesen Befehl vom Ziel-Cluster oder der Ziel-SVM ausführen.

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

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

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`*`, …`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Sie müssen diesen Befehl vom Quellcluster oder der Quell-SVM ausführen.

Das folgende Beispiel gibt Informationen für die angegebene Replizierungsbeziehung von der Quell-SVM frei `svm1`:

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

Management der Storage-Effizienz

SnapMirror erhält die Storage-Effizienz auf den Quell- und Ziel-Volumes mit einer Ausnahme, wenn die nachgelagerte Datenkomprimierung auf dem Zielsystem aktiviert ist. In diesem Fall gehen sämtliche Storage-Effizienz auf dem Zielsystem verloren. Um dieses Problem zu beheben, müssen Sie die nachgelagerte Komprimierung auf dem Ziel deaktivieren, die Beziehung manuell aktualisieren und die Storage-Effizienz erneut aktivieren.

Was Sie benötigen

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

  "Cluster- und SVM-Peering"

- Sie müssen die nachgelagerte Komprimierung auf dem Ziel deaktivieren.

Über diese Aufgabe

Sie können das verwenden `volume efficiency show` Befehl zum Bestimmen, ob Effizienz auf einem Volume aktiviert ist Weitere Informationen finden Sie auf den man-Pages.

Überprüfen Sie, ob SnapMirror die Storage-Effizienz aufrechtzuerhalten, indem Sie sich die SnapMirror Prüfprotokolle ansehen und die Übertragungsbeschreibung ermitteln. Wenn die Übertragungsbeschreibung angezeigt wird `transfer_desc=Logical Transfer`, SnapMirror aufrechterhalten der Storage-Effizienz nicht. Wenn die Übertragungsbeschreibung angezeigt wird `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror dient der Aufrechterhaltung der Storage-Effizienz. 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
```

Logischer Transfer mit Storage

Ab ONTAP 9.3 ist kein manuelles Update mehr nötig, um die Storage-Effizienz wieder zu steigern. 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 Zielvolumen mit der schreibbar gemacht haben `snapmirror break` Befehl, die Caching-Richtlinie auf dem Volume ist automatisch auf „`Auto`“ gesetzt (Standard).

  Dieses Verhalten gilt nur für FlexVol Volumes und nicht für FlexGroup Volumes.

- Bei Resynchronisierung wird die Caching-Richtlinie automatisch auf „`none`“ eingestellt. 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.

Schritt

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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Sie müssen diesen Befehl über die Ziel-SVM oder das Ziel-Cluster ausführen. Der Befehl schlägt fehl, wenn eine allgemeine Snapshot Kopie nicht auf dem Quell- und Zielsystem vorhanden ist. Nutzung `snapmirror initialize` Um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume aktualisiert `volA` Ein `svm1` Und dem Ziel-Volume `volA_dst` Ein `svm_backup`, Und ermöglicht eine erneute Steigerung der Storage-Effizienz:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

Globale Drosselung mit SnapMirror

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 Drosselklappe keine Auswirkungen auf `volume move` Übertragung oder Lastverteilung durch Spiegelungen Ab ONTAP 9.10.0 können Sie eine Option zur Drosselung von Volume-Move-Vorgängen angeben. Weitere Informationen finden Sie unter "Wie man die Volumenbewegung in ONTAP 9.10 und höher drosselt."

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 Drosselwert `0` Bedeutet, dass die globale Drosselung deaktiviert ist.

> Die globale Drosselung von SnapMirror hat keine Auswirkung auf die synchronen Beziehungen von SnapMirror, wenn sie in-Sync sind. Die Drosselung wirkt sich jedoch auf SnapMirror Synchronous Beziehungen aus, wenn sie eine asynchrone Übertragungsphase wie z. B. einen Initialisierungsvorgang oder nach einem Ereignis außerhalb der Synchronisierung durchführen. Aus diesem Grund wird die Aktivierung der globalen Drosselung mit SnapMirror Synchronous Beziehungen nicht empfohlen.

Schritte

1. Globale Drosselung aktivieren:

   `options -option-name replication.throttle.enable on|off`

   Das folgende Beispiel zeigt, wie die globale SnapMirror-Drosselung aktiviert wird `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 Drosselbandbreite beträgt 4 kbps und die maximale Bandbreite beträgt bis zu 2 Tbps. Der Standardwert für diese Option ist `unlimited`, Das heißt, es gibt keine Begrenzung der gesamten Bandbreite verwendet.

   Das folgende Beispiel zeigt, wie die maximale Bandbreite für eingehende Übertragungen auf 100 Mbit/s eingestellt wird:

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 Mbit/s = 12500 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`, Das heißt, es gibt keine Begrenzung der gesamten Bandbreite verwendet. Parameterwerte sind in Kbit/s 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

Allgemeines zur 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 der das Ziel normalerweise nur die Snapshot-Kopien enthält, die sich derzeit auf der Quelle befinden.

  Ab ONTAP 9.9 ändert sich dieses Verhalten, wenn Sie die Mirror-Vault-Richtlinie verwenden. Ab ONTAP 9.9 können Sie unterschiedliche Snapshot Richtlinien auf Quelle und Ziel erstellen. Die Snapshot Kopien auf dem Ziel werden nicht durch Snapshot Kopien 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 Richtlinien für Snapshot Kopien an der Quelle werden nicht auf das Ziel kopiert.
  - Systemdefinierte Snapshot Kopien werden nicht auf das Ziel kopiert.
  - Eine Volume-Zuordnung mit Benutzer- und systemdefinierten Snapshot-Richtlinien wird nicht auf das Ziel kopiert. + SVM.
- Beginnend mit ONTAP 9.2, *SnapMirror Unified Replication,* in der das Ziel für DR und langfristige Aufbewahrung konfiguriert ist.

Details zu diesen Beziehungstypen finden Sie hier: "Allgemeines zur Replizierung von SnapMirror Volumes".

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 sind von der neuen Standardeinstellung 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	MirrorAndVault (einheitliche Replizierung)

Details zu den Änderungen im Standard finden Sie hier: "XDP ersetzt DP als SnapMirror-Standard".

> 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:

- Der `-identity-preserve true` Option des `snapmirror create` Befehl repliziert die gesamte SVM-Konfiguration.

  Der `-identity-preserve false` Die Option repliziert nur die Volumes und die Authentifizierungs- und Autorisierungskonfigurationen der SVM sowie die in aufgeführten Protokoll- und Namensdiensteinstellungen "Konfigurationen, die in SVM-Disaster-Recovery-Beziehungen repliziert werden".

- Der `-discard-configs network` Option des `snapmirror policy create` Der Befehl schließt LIFs und zugehörige Netzwerkeinstellungen aus der SVM-Replizierung aus und kann dort verwendet werden, wo sich die Quell- und Ziel-SVMs in unterschiedlichen Subnetzen befinden.

- Der `-vserver-dr-protection unprotected` Option des `volume modify` Der Befehl schließt das angegebene Volume von der SVM-Replizierung 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 • Ab ONTAP 9.2 ist die einheitliche Replizierung mit SnapMirror möglich
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. Siehe "Sichern einer Konsistenzgruppe" Und "Einschränkungen für Konsistenzgruppen" Finden Sie weitere Informationen.
FabricPool	Ab ONTAP 9.6 wird die SnapMirror SVM-Replizierung mit FabricPool unterstützt.

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. • Ab ONTAP 9.10.1 kann eine MetroCluster-Konfiguration Ziel einer SVM-Disaster-Recovery-Beziehung ausschließlich zu Migrationszwecken sein und muss 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 die Interaktion des `snapmirror create -identity-preserve` Option und das `snapmirror policy create -discard-configs network` Option:

Konfiguration repliziert		**`-identity-preserve true`**		**`-identity-preserve false`**
		Richtlinie ohne `-discard-configs network` Set	**Richtlinien 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.	Snapshot Kopien, Snapshot-Richtlinien und Autodelete-Richtlinien	Ja.	Ja.	Ja.
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.

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. Siehe "Hardware Universe" Lernen Sie die Grenzen für Ihre spezifische Konfiguration kennen.

Storage Objekt	Grenze
SVM	300 flexible Volumes
HA-Paar	1,000 Flexible Volumes
Cluster	128 SVM-Disaster-Beziehungen

Replizieren der SVM -Konfigurationen

SnapMirror SVM-Replizierungs-Workflow

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 für die Platzierung von Volumes auf 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.
- Wenn der `-space-guarantee` Die Option für das zu replizierende Volume wird festgelegt `volume`, Nur Aggregate mit freiem Speicherplatz, der größer ist als die Volume-Größe, werden berücksichtigt.
- 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.

Wenn Sie ein Volume von einem Aggregat zu einem anderen verschieben möchten, können Sie das verwenden `volume move` Befehl auf der Ziel-SVM.

Replizierung einer gesamten SVM-Konfiguration

Sie können das verwenden `-identity-preserve true` Option des `snapmirror create` Befehl zum Replizieren einer gesamten SVM-Konfiguration

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".

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Über diese Aufgabe

Bei diesem Workflow wird vorausgesetzt, dass Sie bereits eine Standardrichtlinie oder eine benutzerdefinierte Replizierungsrichtlinie verwenden.

Ab ONTAP 9.9 können Sie bei Verwendung der Mirror-Vault-Richtlinie unterschiedliche Snapshot-Richtlinien auf der Quell- und Ziel-SVM erstellen. Die Snapshot Kopien auf dem Ziel werden nicht durch Snapshot Kopien auf dem Quellsystem überschrieben. Weitere Informationen finden Sie unter "Allgemeines zur Replizierung von SnapMirror SVMs".

Schritte

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
   ```

2. Erstellen Sie aus dem Ziel-Cluster eine SVM-Peer-Beziehung mit dem `vserver peer create` Befehl.

   Weitere Informationen finden Sie unter "Erstellen einer SVM-Peer-Beziehung".

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`, Sie können angeben `all` Zum Ausführen des Jobs jeden Monat, Wochentag und Stunde.

   > 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 Job-Zeitplan mit dem Namen erstellt `my_weekly` Das läuft samstags um 3:00 Uhr:

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

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`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen:

   Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mit dem Standard erstellt `MirrorAllSnapshots` Richtlinie:

   ```
   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 eine einheitliche Replizierungsbeziehung mit dem Standard erstellt `MirrorAndVault` Richtlinie:

   ```
   cluster_dst:> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
   -identity-preserve true
   ```

   Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt `async-mirror`, Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve true
```

Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt `mirror-vault`, Das folgende Beispiel erstellt eine einheitliche Replikationsbeziehung:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve true
```

5. Ziel-SVM stoppen:

   `vserver stop`

   `SVM name`

   Im folgenden Beispiel wird eine Ziel-SVM namens dvs1 angehalten:

```
cluster_dst::> vserver stop -vserver dvs1
```

6. Initialisieren Sie die SVM-Replizierungsbeziehung von der Ziel-SVM oder dem Ziel-Cluster: +

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

   Das folgende Beispiel initialisiert die Beziehung zwischen der Quell-SVM, `svm1`Und dem Ziel-SVM, `svm_backup`:

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

Schließt LIFs und zugehörige Netzwerkeinstellungen von der SVM-Replizierung aus

Wenn sich die Quell- und Ziel-SVMs in unterschiedlichen Subnetzen befinden, können Sie das verwenden `-discard-configs network` Option des `snapmirror policy create` Befehl zum Ausschließen von LIFs und zugehörigen Netzwerkeinstellungen von der SVM-Replizierung.

Was Sie benötigen

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

Der `-identity-preserve` Option des `snapmirror create` Der Befehl muss auf festgelegt sein `true` Wenn Sie die SVM-Replizierungsbeziehung erstellen.

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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 aus dem Ziel-Cluster eine SVM-Peer-Beziehung mit dem `vserver peer create` Befehl.

   Weitere Informationen finden Sie unter "Erstellen einer SVM-Peer-Beziehung".

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`, Sie können angeben `all` Zum Ausführen des Jobs jeden Monat, Wochentag und Stunde.

   > 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 Job-Zeitplan mit dem Namen erstellt `my_weekly` Das läuft samstags um 3:00 Uhr:

   ```
   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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   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
```

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`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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_daily -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_daily -policy unified_exclude_LIFs
-identity-preserve true
```

6. Ziel-SVM stoppen:

   `vserver stop`

   SVM name

   Im folgenden Beispiel wird eine Ziel-SVM namens dvs1 angehalten:

```
cluster_dst::> vserver stop -vserver dvs1
```

7. Initialisieren Sie von der Ziel-SVM oder dem Ziel-Cluster eine Replizierungsbeziehung:

   `snapmirror initialize -source-path SVM: -destination-path SVM:`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel initialisiert die Beziehung zwischen der Quelle, `svm1` Und dem Ziel, `svm_backup`:

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

Nachdem Sie fertig sind

Sie müssen das Netzwerk und die Protokolle auf der Ziel-SVM für den Datenzugriff bei einem Ausfall konfigurieren.

Schließen Sie Netzwerk-, Name-Service- und andere Einstellungen von der SVM-Replizierung aus

Sie können das verwenden `-identity-preserve false` Option des `snapmirror create` Befehl zum Replizieren nur der Volumes und Sicherheitskonfigurationen einer SVM 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".

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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 aus dem Ziel-Cluster eine SVM-Peer-Beziehung mit dem `vserver peer create` Befehl.

   Weitere Informationen finden Sie unter "Erstellen einer SVM-Peer-Beziehung".

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`, Sie können angeben `all` Zum Ausführen des Jobs jeden Monat, Wochentag und Stunde.

> 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 Job-Zeitplan mit dem Namen erstellt `my_weekly` Das läuft samstags um 3:00 Uhr:

```
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`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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 mit dem Standard erstellt `MirrorAllSnapshots` Richtlinie: 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 eine einheitliche Replizierungsbeziehung mit dem Standard erstellt `MirrorAndVault` Richtlinie: Die Beziehung schließt Netzwerk-, Namensdienst- und andere Konfigurationseinstellungen aus:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

   Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt `async-mirror`, Das folgende Beispiel erstellt eine SnapMirror DR-Beziehung. 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
```

Angenommen, Sie haben eine benutzerdefinierte Richtlinie mit dem Richtlinientyp erstellt `mirror-vault`, Das folgende Beispiel erstellt eine einheitliche Replikationsbeziehung. 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
```

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`*`:`

Nachdem Sie fertig sind

Sie müssen das Netzwerk und die Protokolle auf der Ziel-SVM für den Datenzugriff bei einem Ausfall konfigurieren.

Festlegen von Aggregaten, die für SVM-DR-Beziehungen verwendet werden sollen

Nachdem eine Disaster-Recovery-SVM erstellt wurde, können Sie den verwenden `aggr-list` Option mit `vserver modify` Befehl zum Limit, welche Aggregate zum Hosten von SVM-DR-Ziel-Volumes genutzt werden

Schritt

1. Ziel-SVM erstellen:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

2. Ändern Sie die Aggr-Liste der Disaster-Recovery-SVM, um die Aggregate zu begrenzen, die zum Hosten des SVM-Volumes der Disaster-Recovery verwendet werden:

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

Nur SMB: Erstellen Sie einen SMB-Server

Wenn die Quell-SVM über eine SMB-Konfiguration verfügt, haben Sie die Wahl, festzulegen `identity-preserve` Bis `false`, Sie müssen einen SMB-Server für die Ziel-SVM erstellen. SMB-Server ist für einige SMB-Konfigurationen erforderlich, z. B. Freigaben während der Initialisierung der SnapMirror Beziehung.

Schritte

1. Starten Sie die Ziel-SVM mit `vserver start` Befehl.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Vergewissern Sie sich, dass sich die Ziel-SVM im befindet `running` Status und Untertyp lautet `dp-destination` Durch Verwendung des `vserver show` Befehl.

```
destination_cluster::> vserver show
                                   Admin      Operational Root
Vserver  Type    Subtype           State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

3. Erstellen Sie mithilfe des ein LIF `network interface create` Befehl.

```
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
```

4. Erstellen Sie eine Route mit dem `network route create` Befehl.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Netzwerkmanagement"

5. Konfigurieren Sie DNS mit `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
```

6. Fügen Sie den bevorzugten Domänencontroller mithilfe des hinzu `vserver cifs domain preferred-dc add` Befehl.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

7. Erstellen Sie den SMB-Server mit `vserver cifs create` Befehl.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

8. Beenden Sie die Ziel-SVM mithilfe der `vserver stop` Befehl.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Schließen Sie Volumes von der SVM-Replizierung aus

Standardmäßig werden alle RW-Daten-Volumes der Quell-SVM repliziert. Wenn Sie nicht alle Volumes auf der Quell-SVM sichern möchten, können Sie die verwenden `-vserver -dr-protection unprotected` Option des `volume modify` Befehl zum Ausschließen von Volumes aus der SVM-Replizierung.

Schritte

1. Volume von SVM-Replizierung ausschließen:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das Volume ist im folgenden Beispiel nicht enthalten `volA_src` Über SVM-Replizierung:

```
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`

Das folgende Beispiel beinhaltet das Volume `volA_src` In der SVM-Replizierung:

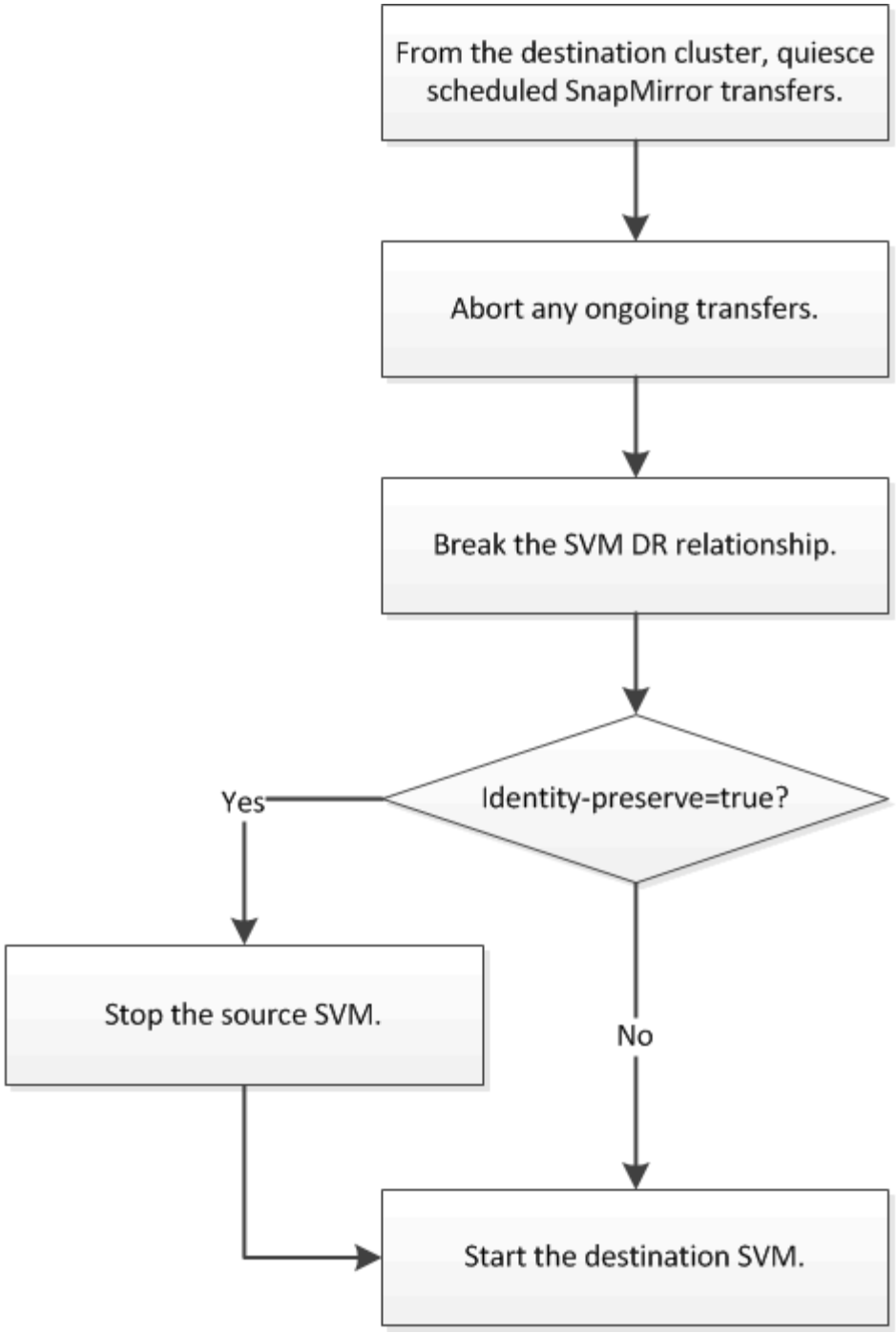
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Erstellen und Initialisieren der SVM-Replizierungsbeziehung, wie in beschrieben "Replizierung einer gesamten SVM-Konfiguration".

Bereitstellen von Daten von einem SVM DR-Ziel

SVM Disaster-Recovery-Workflow

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.



SVM Ziel-Volumes beschreibbar machen

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 die Einstellung festgelegt haben `-identity-preserve true` Beim Erstellen der SVM-Replizierungsbeziehung müssen Sie die Quell-SVM vor Aktivierung der Ziel-SVM beenden.

Über diese Aufgabe

Eine vollständige Befehlssyntax finden Sie in der man-Page.

> 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.

Schritte

1. Stoppen Sie die geplanten Transfers von der Ziel-SVM oder dem Ziel-Cluster auf das Ziel:

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

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel werden geplante Transfers zwischen der Quell-SVM angehalten `svm1` Und als Ziel-SVM zu definieren `svm_backup`:

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

2. Stoppen Sie den laufenden Transfer von der Ziel-SVM oder dem Ziel-Cluster zum Ziel:

   `snapmirror abort -source-path SVM: -destination-path SVM:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel werden kontinuierliche Transfers zwischen der Quell-SVM angehalten `svm1` Und als Ziel-SVM zu definieren `svm_backup`:

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

3. Unterbrechen Sie die Replizierungsbeziehung von der Ziel-SVM oder dem Ziel-Cluster:

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

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Das folgende Beispiel unterbricht die Beziehung zwischen der Quell-SVM `svm1` Und als Ziel-SVM zu definieren `svm_backup`:

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

4. Wenn Sie die Einstellung festgelegt haben `-identity-preserve true` Beenden Sie beim Erstellen der SVM-Replizierungsbeziehung die Quell-SVM:

   `vserver stop -vserver SVM`

   Im folgenden Beispiel wird die Quell-SVM angehalten `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
   ```

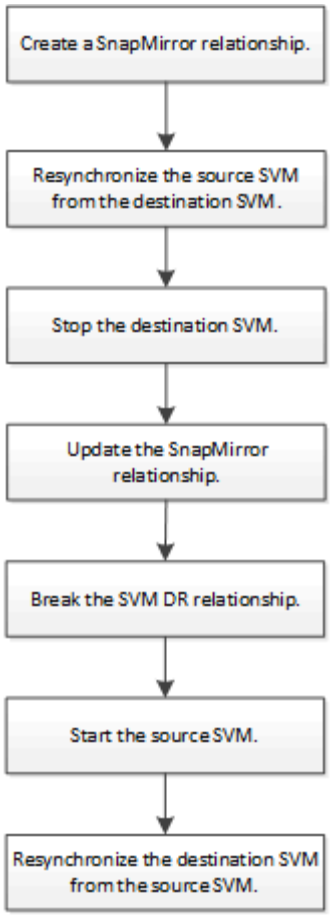
Nachdem Sie fertig sind

Konfigurieren von SVM Ziel-Volumes für Datenzugriff wie in beschrieben "Konfiguration des Ziel-Volume für den Datenzugriff".

Aktivieren Sie die Quell-SVM erneut

Umaktivierungs-Workflow für 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 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"

Über diese Aufgabe

Ab ONTAP 9.11.1 können Sie die Neusynchronisierung während einer Disaster Recovery-Probe mit dem verkürzen `-quick-resync true` Option des `snapmirror resync` Befehl während Durchführung einer Reverse-Resynchronisierung einer SVM-DR-Beziehung Durch eine schnelle Neusynchronisierung kann sich die Zeit bis zur Produktionsrückführung verkürzen, da das Data Warehouse neu aufgebaut und Vorgänge wiederhergestellt werden müssen.

> 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.

Eine vollständige Befehlssyntax für „Befehle“ finden Sie in der man-Page.

Schritte

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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird eine Beziehung zwischen der SVM erstellt, von der Sie Daten bereitstellen, `svm_backup`, Und der ursprünglichen Quelle SVM , `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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 eine allgemeine Snapshot Kopie nicht auf dem Quell- und Zielsystem vorhanden ist. Nutzung `snapmirror initialize` Um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Quell-SVM umkehren: `svm1`Und der SVM, von der aus Sie Daten bereitstellen, `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. Überprüfen Sie, ob die ursprüngliche Ziel-SVM sich mithilfe von im Status „angehalten“ befindet `vserver show` Befehl.

```
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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, von der Sie Daten bereitstellen, aktualisiert,`svm_backup`, Und der ursprünglichen Quelle SVM , `svm1`:

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

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:`

> Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

Im folgenden Beispiel werden geplante Transfers zwischen der SVM, von der Sie Daten bereitstellen, angehalten. `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`*`:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, der Sie Daten bereitstellen, unterbrochen. `svm_backup`, Und der ursprünglichen Quelle SVM , `svm1`:

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

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`*`:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Quell-SVM wiederhergestellt. `svm1`, Und das ursprüngliche Ziel SVM, `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:`

    > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

    Im folgenden Beispiel wird die umgekehrte Beziehung zwischen der ursprünglichen Ziel-SVM gelöscht. `svm_backup`, Und der ursprünglichen Quelle 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:`

    > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

    Im folgenden Beispiel werden die umgekehrten Beziehungen zwischen der ursprünglichen Ziel-SVM, svm_Backup und der ursprünglichen Quell-SVM freigegeben. `svm1`

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

Nachdem Sie fertig sind

Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Reaktivierung der ursprünglichen Quell-SVM (nur 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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die ursprüngliche Beziehung zwischen der ursprünglichen Quell-SVM, svm1 und der ursprünglichen Ziel-SVM gelöscht. `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. Geben Sie ausgehend von der ursprünglichen Quell-SVM oder dem ursprünglichen Quell-Cluster die ursprüngliche Beziehung frei, während die Snapshot Kopien intakt bleiben:

   `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird eine Beziehung zwischen der SVM erstellt, von der Sie Daten bereitstellen, `svm_backup`, Und der ursprünglichen Quelle SVM , `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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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 eine allgemeine Snapshot Kopie nicht auf dem Quell- und Zielsystem vorhanden ist. Nutzung `snapmirror initialize` Um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Quell-SVM umkehren: `svm1`Und der SVM, von der aus Sie Daten bereitstellen, `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. Überprüfen Sie, ob die ursprüngliche Ziel-SVM sich mithilfe von im Status „angehalten“ befindet `vserver show` Befehl.

   ```
   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:`

> Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, von der Sie Daten bereitstellen, aktualisiert,`svm_backup`, Und der ursprünglichen Quelle SVM , `svm1`:

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

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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel werden geplante Transfers zwischen der SVM, von der Sie Daten bereitstellen, angehalten. `svm_backup`Und der ursprünglichen SVM, `svm1`:

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

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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Ziel-SVM, der Sie Daten bereitstellen, unterbrochen. `svm_backup`, Und der ursprünglichen Quelle SVM , `svm1`:

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

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:`

    > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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 Snapshot Kopien intakt bleiben:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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:`

    > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

    Im folgenden Beispiel wird eine Beziehung zwischen der ursprünglichen Quell-SVM, `svm1`, Und das ursprüngliche 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:`

    > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

    Im folgenden Beispiel wird die Beziehung zwischen der ursprünglichen Quell-SVM wiederhergestellt. `svm1`, Und das ursprüngliche Ziel SVM, `svm_backup`:

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

Konvertieren von Volume-Replizierungsbeziehungen in eine SVM-Replizierungsbeziehung

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 die `volume rename` Befehl, wenn die SnapMirror-Beziehung inaktiv ist, um ggf. Ziel-Volumes umzubenennen

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`

    Eine vollständige Befehlssyntax finden Sie in der man-Page.

    > 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 neu synchronisiert `volA` Ein `svm1` Und dem Ziel-Volume `volA` Ein `svm_backup`:

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

2. Erstellen einer SVM-Replizierungsbeziehung zwischen den Quell- und Ziel-SVMs, wie in beschrieben "Replizierung von SVM-Konfigurationen".

   Sie müssen den verwenden `-identity-preserve true` Option des `snapmirror create` Befehl beim Erstellen der Replikationsbeziehung.

3. Ziel-SVM stoppen:

   `vserver stop -vserver` *`SVM`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Ziel-SVM angehalten `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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: 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 neu synchronisiert `svm1` Und als Ziel-SVM zu definieren `svm_backup`:

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

Löschen einer SVM-Replizierungsbeziehung

Sie können das verwenden `snapmirror delete` Und `snapmirror release` Befehle zum Löschen einer SVM-Replizierungsbeziehung. Sie können dann nicht benötigte Ziel-Volumes manuell löschen.

Über diese Aufgabe

Der `snapmirror release` Befehl löscht alle durch SnapMirror erstellten Snapshot Kopien aus der Quelle. Sie können das verwenden `-relationship-info-only` Option zum Bewahren der Snapshot Kopien.

Eine vollständige Befehlssyntax für „Befehle“ finden Sie in der man-Page.

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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Das folgende Beispiel unterbricht die Beziehung zwischen der Quell-SVM `svm1` Und als Ziel-SVM zu definieren `svm_backup`:

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

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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Im folgenden Beispiel wird die Beziehung zwischen der Quell-SVM gelöscht `svm1` Und als Ziel-SVM zu definieren `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

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:`

   > Sie müssen nach dem SVM-Namen in einen Doppelpunkt (:) eingeben `-source-path` Und `-destination-path` Optionen: Siehe das folgende Beispiel.

   Das folgende Beispiel gibt Informationen für die angegebene Replizierungsbeziehung von der Quell-SVM frei `svm1`:

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

Management der SnapMirror Root-Volume-Replizierung

Übersicht über die SnapMirror Root-Volume-Replizierung verwalten

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 Mirror-Beziehungen zur Lastverteilung

Sie sollten eine Load-Sharing-Spiegelung (LSM) für jedes SVM-Root-Volume erstellen, das NAS-Daten im Cluster bereitstellt. Bei Clustern mit zwei oder mehr HA-Paaren sollten Sie die Spiegelung der Lastverteilung von SVM-Root-Volumes in Erwägung ziehen, um sicherzustellen, dass der Namespace für Clients bei diesem Fall zugänglich bleibt Ein HA-Paar schlägt beide Nodes fehl. Die Load-Sharing-Spiegelung ist nicht für Cluster geeignet, die aus einem einzelnen HA-Paar bestehen.

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:

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

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

Das Zielvolumen sollte gleich oder größer sein als das Root-Volume.

Als Best Practice empfiehlt es sich, das Root- und Zielvolumen mit Suffixen wie z. B. zu benennen `_root` Und `_m1`.

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel erstellt ein Mirror-Volume zur Lastverteilung 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:

   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 LS -schedule <schedule>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel erstellt eine Mirror-Beziehung zur Lastverteilung zwischen dem Root-Volume `svm1_root` Und das Load-Sharing-Mirror-Volume `svm1_m1`:

   ```
   cluster_src::> snapmirror create -source-path svm1:svm1_root
   -destination-path svm1:svm1_m1 -type LS -schedule hourly
   ```

   Das Typ-Attribut der Load-Sharing-Spiegelung ändert sich von `DP` Bis `LS`.

4. Initialisieren Sie die Load-Sharing-Spiegelung:

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

   ```
   snapmirror initialize-ls-set -source-path <SVM:volume>
   ```

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

geringerer Auslastung durchführen.

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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
```

Aktualisierung einer Spiegelbeziehung mit Lastverteilung

LSM-Beziehungen (Load-Sharing Mirror) werden automatisch für SVM-Root-Volumes aktualisiert, nachdem ein Volume in der SVM gemountet oder abgehängt wurde, und während `volume create` Vorgänge, die die Option `Junction-Path`umfassen. 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` Der Befehl wird ausgegeben, der den enthält `juntion-path` Option

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>
   ```

   Im folgenden Beispiel wird die Mirror-Beziehung zur Lastverteilung für das Root-Volume aktualisiert `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

Hochstufen eines Spiegels 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.

Was Sie benötigen

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>
```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel gibt das Volumen an `svm1_m2` Als das neue SVM Root Volume:

```
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
```

   Eingabe `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.

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 hochgestuften Volume umbenannt `svm1_m2` Mit dem Namen `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".

Technische Details zu SnapMirror

Pfadnamenmuster verwenden

Sie können die Mustervergleich verwenden, um die Quell- und Zielpfade in festzulegen `snapmirror` Befehle.

```
`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, die `snapmirror` Der
Befehl nimmt den lokalen SVM-Kontext des Benutzers an.
```

Wenn die SVM „`vserver1`“ und der Name des Volumes „`vol1`“ heißt, lautet der vollständig qualifizierte Pfad `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*`	Abgleich aller SVMs und Volumes mit SVM-Namen beginnend mit `vs`.
`:*src`	Stimmt alle SVMs mit den Volume-Namen überein, die den enthalten `src` Text
`:vol`	Ordnet alle SVMs zunächst die Volume-Namen zu `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    -
```

Verwendung erweiterter Abfragen für viele SnapMirror Beziehungen

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 in einem initialisiert `Uninitialized` Bundesland:

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

Stellen Sie eine gemeinsame Snapshot Kopie in einer Implementierung von Spiegelgewölbe sicher

Sie können das verwenden `snapmirror snapshot-owner create` Befehl zum

Bewahren einer beschrifteten Snapshot Kopie auf dem sekundären System in einer Implementierung mit Spiegelgewölbe So wird sichergestellt, dass eine gemeinsame Snapshot Kopie für die Aktualisierung der Vault-Beziehung vorhanden ist.

Über diese Aufgabe

Wenn Sie eine Kombination aus Fan-out oder Kaskadierung verwenden, sollten Sie beachten, dass Updates fehlschlagen, wenn eine gemeinsame Snapshot-Kopie nicht auf den Quell- und Ziel-Volumes vorhanden ist.

Dies ist in einer Spiegelungs-Fan-out- oder Kaskadenbereitstellung niemals ein Problem für die Spiegelbeziehung, da SnapMirror immer eine Snapshot Kopie des Quell-Volume erstellt, bevor sie die Aktualisierung durchführt.

Es könnte ein Problem für die Vault-Beziehung sein, jedoch, da SnapMirror keine Snapshot Kopie des Quell-Volumes erstellt, wenn es eine Vault-Beziehung aktualisiert. Sie müssen den verwenden `snapmirror snapshot-owner create` Um sicherzustellen, dass mindestens eine gemeinsame Snapshot Kopie auf der Quelle und dem Ziel der Vault-Beziehung vorhanden ist.

Schritte

1. Weisen Sie auf dem Quell-Volume der beschrifteten Snapshot Kopie einen Eigentümer zu, die Sie erhalten möchten:

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

   Das folgende Beispiel wird zugewiesen `ApplicationA` Als Besitzer des `snap1` Snapshot Kopie:

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

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

   Alternativ können Sie auf die geplante Aktualisierung der Spiegelbeziehung warten.

3. Übertragen Sie die beschriftete Snapshot Kopie auf das Vault-Ziel:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird der übertragen `snap1` Snapshot Kopie

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

   Wenn die Tresor-Beziehung aktualisiert wird, bleibt die gekennzeichnete Snapshot-Kopie erhalten.

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

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

In den folgenden Beispielen wird entfernt `ApplicationA` Als Besitzer des `snap1` Snapshot Kopie:

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

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

> Interoperabilität ist bidirektional.

Interoperabilität für ONTAP Version 9.3 und höher

ONTAP-Version…	Interagiert mit diesen früheren ONTAP-Versionen…																	
	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4	9.3
9.14.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein	Nein	Nein
9.14.0*	**Ja**	**Ja**	**Ja**	Nein	**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**	Nein	Nein	Nein	Nein	Nein

9.13.0*	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	Nein	Nein	Nein	Nein
9.12.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein
9.12.0*	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	Nein	Nein	Nein	Nein
9.11.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.11.0*	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.10.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.10.0*	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.9.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.9.0*	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.8	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**
9.7	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**
9.6	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	**Ja**
9.5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9.4	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**
9.3	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**

SnapMirror – synchrone Beziehungen

SnapMirror Synchronous wird für ONTAP Cloud-Instanzen nicht unterstützt.

ONTAP-Version …	Interagiert mit diesen früheren ONTAP-Versionen…									
	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
9.14.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.13.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.12.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.11.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein	Nein
9.10.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein	Nein
9.9.1	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein	Nein
9.8	**Ja**	**Ja**	**Ja**	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**	Nein

9.7	Nein	**Ja**	**Ja**	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**	**Ja**
9.6	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**	**Ja**
9.5	Nein	Nein	Nein	Nein	Nein	Nein	Nein	**Ja**	**Ja**	**Ja**

SnapMirror SVM Disaster-Recovery-Beziehungen

- 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 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).

Quelle	Ziel																	
	9.3	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1
9.3	DR/Migration	Migration	Migration	Migration	Migration													
9.4		DR/Migration	Migration	Migration	Migration	Migration												
9.5			DR/Migration	Migration	Migration	Migration	Migration											
9.6				DR/Migration	Migration	Migration	Migration	Migration										

9.7					DR/ Migration	Migration	Migration	Migration	Migration									
9.8						DR/ Migration	Migration	Migration	Migration	Migration								
9.9.0*							DR/ Migration	Migration	Migration	Migration	Migration							
9.9.1								DR/ Migration	Migration	Migration	Migration	Migration						
9.10.0*									DR/ Migration	Migration	Migration	Migration	Migration					
9.10.1										DR/ Migration	Migration	Migration	Migration	Migration				
9.11.0*											DR/ Migration	Migration	Migration	Migration	Migration			
9.11.1												DR/ Migration	Migration	Migration	Migration	Migration		
9.12.0*													DR/ Migration	Migration	Migration	Migration	Migration	
9.12.1														DR/ Migration	Migration	Migration	Migration	Migration
9.13.0*															DR/ Migration	Migration	Migration	Migration

9.13.1																DR/Migration	Migration	Migration
9.14.0*																	DR/Migration	Migration
9.14.1																		DR/Migration

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	9.2	9.1	9
9.11.1	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.10.1	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.9.1	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.8	Nein	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.7	Nein	Nein	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein
9.6	Nein	Nein	Nein	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
9.5	Nein	Nein	Nein	Nein	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein
9.4	Nein	Nein	Nein	Nein	Nein	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
9.3	Nein	Nein	Nein	Nein	Nein	Nein	Ja.	Ja.	Ja.	Nein	Nein	Nein
9.2	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja.	Ja.	Ja.	Nein	Nein
9.1	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja.	Ja.	Ja.	Nein
9	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Nein	Ja.	Ja.	Ja.

> Interoperabilität ist nicht bidirektional.

Einschränkungen von SnapMirror

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. Siehe "Hardware Universe" Um Details zu Ihrer spezifischen Konfiguration zu erfahren.
- 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.

Archivierung und Compliance mit SnapLock Technologie

Was ist SnapLock

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

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

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

Mit einer Applikation LASSEN sich Dateien über NFS oder CIFS in WORM-FORMAT übersenden oder die automatische 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:

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

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

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

Ihre Möglichkeiten mit SnapLock

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

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

SnapLock Compliance und Enterprise Modi

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

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

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

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

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

Dar	SnapLock-Compliance	SnapLock Enterprise
Aktivieren und löschen Sie Dateien mit privilegierter Löschung	Nein	Ja.
Festplatten neu initialisieren	Nein	Ja.
Zerstören Sie SnapLock Aggregate und Volumes während der Aufbewahrungsdauer	Nein	Ja, mit Ausnahme des SnapLock Revisionsprotokoll-Volumes
Benennen Sie Aggregate oder Volumes um	Nein	Ja.
Verwenden Sie nicht NetApp Festplatten	Nein	Ja (mit "FlexArray Virtualisierung")
Verwenden Sie das SnapLock Volume zur Audit-Protokollierung	Ja.	Ja, ab ONTAP 9.5

Unterstützte und nicht unterstützte Funktionen in SnapLock

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

Merkmal	Unterstützt durch SnapLock Compliance	Unterstützt durch SnapLock Enterprise
Konsistenzgruppen	Nein	Nein
Verschlüsselte Volumes	Ja, ab ONTAP 9.2. Weitere Informationen zu Verschlüsselung und SnapLock.	Ja, ab ONTAP 9.2. Weitere Informationen zu Verschlüsselung und SnapLock.
FabricPool auf SnapLock Aggregaten	Nein	Ja, ab ONTAP 9.8. Weitere Informationen zu FabricPool auf SnapLock Enterprise-Aggregaten.
Flash Pool-Aggregate	Ja, ab ONTAP 9.1.	Ja, ab ONTAP 9.1.

FlexClone	Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen.	Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen.
FlexGroup Volumes	Ja, ab ONTAP 9.11.1. Weitere Informationen zu [flexgroup].	Ja, ab ONTAP 9.11.1. Weitere Informationen zu [flexgroup].
LUNs	Nein Weitere Informationen zu LUN-Unterstützung Mit SnapLock.	Nein Weitere Informationen zu LUN-Unterstützung Mit SnapLock.
MetroCluster Konfigurationen	Ja, ab ONTAP 9.3. Weitere Informationen zu MetroCluster Support.	Ja, ab ONTAP 9.3. Weitere Informationen zu MetroCluster Support.
Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV)	Ja, ab ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung.	Ja, ab ONTAP 9.13.1. Weitere Informationen zu MAV-Unterstützung.
San	Nein	Nein
SnapRestore mit einer Datei	Nein	Ja.
SnapMirror Business Continuity	Nein	Nein
SnapRestore	Nein	Ja.
SMTape	Nein	Nein
SnapMirror Synchronous	Nein	Nein
SSDs	Ja, ab ONTAP 9.1.	Ja, ab ONTAP 9.1.
Funktionen für effizienteren Storage	Ja, ab ONTAP 9.9.1. Weitere Informationen zu Support für Storage-Effizienz.	Ja, ab ONTAP 9.9.1. Weitere Informationen zu Support für Storage-Effizienz.

FabricPool auf SnapLock Enterprise-Aggregaten

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

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

FlexGroup Volumes

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

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

Sie sollten auch die folgenden Verhaltensweisen beachten:

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

LUN-Unterstützung

LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen auf einem nicht-SnapLock Volume erstellte Snapshot Kopien zur Sicherung im Rahmen der SnapLock Vault-Beziehung auf ein SnapLock Volume übertragen werden. LUNs werden in SnapLock-Volumes mit Lese-/Schreibzugriff nicht unterstützt. Manipulationssichere Snapshot Kopien werden jedoch auf SnapMirror Quell-Volumes und Ziel-Volumes unterstützt, die LUNs enthalten.

MetroCluster Support

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

SnapLock-Compliance

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

SnapLock Enterprise

- Ab ONTAP 9 werden SnapLock Enterprise Aggregate unterstützt.
- Ab ONTAP 9.3 werden SnapLock Enterprise-Aggregate mit privilegierten 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. Weitere Informationen zu "MAV".

Storage-Effizienz

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

Verschlüsselung

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

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

> Ab ONTAP 9.2 werden verschlüsselte Volumes von SnapLock Aggregaten unterstützt.

Umstieg Von 7-Mode

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

Konfigurieren Sie SnapLock

Konfigurieren Sie SnapLock

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

Und vieles mehr.

Initialisieren Sie die Compliance-Uhr

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

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

Bevor Sie beginnen

So initialisieren Sie die Compliance-Uhr neu:

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

Allgemeine Anforderungen für die Initialisierung der Compliance Clock:

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

Über diese Aufgabe

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

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

Schritte

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

System Manager

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

CLI

1. Initialisieren Sie die System-Compliance-Uhr:

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

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

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

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

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

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

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

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

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

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

Was Sie benötigen

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

Über diese Aufgabe

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

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

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

Schritte

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

   `snaplock compliance-clock ntp`

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

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

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

   `snaplock compliance-clock ntp show`

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

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

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

Erstellen Sie ein SnapLock Aggregat

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

Bevor Sie beginnen

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

Upgrade-Überlegungen

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

Überlegungen zurücksetzen

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

Über diese Aufgabe

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

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

Schritte

1. Erstellung eines SnapLock Aggregats:

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

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

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

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

SnapLock Volumes erstellen und mounten

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

> LUNs werden in SnapLock Volumes nicht unterstützt. LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen auf einem nicht-SnapLock Volume erstellte Snapshot Kopien zur Sicherung im Rahmen der SnapLock Vault-Beziehung auf ein SnapLock Volume übertragen werden. LUNs werden in SnapLock-Volumes mit Lese-/Schreibzugriff nicht unterstützt. Manipulationssichere Snapshot Kopien werden jedoch auf SnapMirror Quell-Volumes und Ziel-Volumes unterstützt, die LUNs enthalten.

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

System Manager

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

Schritte

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

CLI

1. SnapLock Volume erstellen:

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

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

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

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

Mounten Sie ein SnapLock Volume

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

Was Sie benötigen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

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

Schritte

1. Mounten eines SnapLock Volume:

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

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

   Mit dem folgenden Befehl wird ein SnapLock-Volume mit dem Namen gemountet `vol1` Zum Verbindungspfad `/sales` Im `vs1` Namespace:

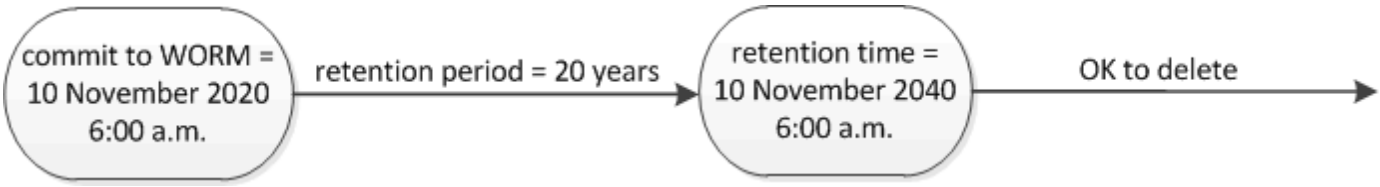
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Aufbewahrungszeit einstellen

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

Allgemeines zu Aufbewahrungszeitraum und Aufbewahrungszeit

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



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

Wichtige Überlegungen zur Replizierung

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

Wichtige Überlegungen zum Wechsel

ONTAP verhindert, dass Sie einen Cluster von ONTAP 9.10.1 auf eine frühere ONTAP-Version zurücksetzen,

wenn es Dateien mit einer Aufbewahrungsfrist später als „Januar 19, 2071 8:44:07“ gibt.

Die Aufbewahrungsfristen verstehen

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

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

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

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

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

Legen Sie den Standardaufbewahrungszeitraum fest

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

Was Sie benötigen

Das SnapLock Volume muss online sein.

Über diese Aufgabe

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

> Der Standardaufbewahrungszeitraum muss größer oder gleich (>=) dem Mindestaufbewahrungszeitraum und kleiner als oder gleich (<=) dem maximalen Aufbewahrungszeitraum sein.

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

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

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

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

Schritte

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

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

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

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

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

```
cluster1::> volume snaplock modify -vserver vs1 -volume 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 gespeichert `atime` Feld für die Datei.

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

Schritte

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

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

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

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

Legen Sie den Aufbewahrungszeitraum für die Datei nach einem Ereignis fest

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

Was Sie benötigen

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

  "Erstellen Sie ein SnapLock-Administratorkonto"

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

Über diese Aufgabe

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

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

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

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

Weitere Informationen zur erweiterten Verwendung finden Sie unter "Worm-Speicherung gemäß NetApp SnapLock".

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

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

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

Schritte

1. EBR-Richtlinie erstellen:

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

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

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

2. Anwenden einer EBR-Richtlinie:

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

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

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

Erstellen eines Prüfprotokolls

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

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

verwenden "Explizit ein SnapLock Volume erstellen" Indem Sie als SnapLock-Typ entweder Compliance oder Enterprise angeben.

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

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

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

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

Schritte

1. Erstellen Sie ein SnapLock Aggregat.

   Erstellen Sie ein SnapLock Aggregat

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

   SnapLock Volume erstellen

3. SVM für Audit-Protokollierung konfigurieren:

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

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

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

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

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

   Mounten Sie ein SnapLock Volume

Überprüfen Sie die SnapLock-Einstellungen

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

Schritte

1. Generieren eines Dateiprints:

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

   ```
   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 Eingaben in den verwenden können `volume file fingerprint dump` Befehl.

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

2. Zeigen Sie den Fingerabdruck für die Datei an:

volume file fingerprint dump -session-id *session_ID*

```
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

MANAGEN von WORM-Dateien

ES gibt folgende Möglichkeiten, WORM-Dateien zu verwalten:

- "Übertragung von Dateien an DIE WORM-Funktion"
- "Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel"
- "SPIEGELN VON WORM-Dateien für das Disaster Recovery"
- "Aufbewahrung VON WORM-Dateien bei Gerichtsverfahren"
- "LÖSCHEN SIE WORM-Dateien"

Übertragung von Dateien an DIE WORM-Funktion

Dateien können entweder manuell oder automatisch in DEN WORM-Modus verschoben werden (einmal schreiben, viele lesen). Sie können auch ANGEHÄNGBARE WORM-Dateien erstellen.

Manuelles Versetzen von Dateien in DIE WORM-FUNKTION

Sie übergeben eine Datei manuell in WORM, indem Sie die Datei schreibgeschützt machen. Sie können jeden geeigneten Befehl oder jedes Programm über NFS oder CIFS verwenden, um das Lese-/Schreibattribut einer Datei in schreibgeschützt zu ändern. Sie können Dateien manuell übergeben, wenn Sie sicherstellen möchten, dass eine Anwendung das Schreiben in eine Datei abgeschlossen hat, damit die Datei nicht vorzeitig beendet wird oder wenn aufgrund einer hohen Anzahl von Volumes Skalierungsprobleme für den Autocommit-Scanner auftreten.

Was Sie benötigen

- Die Datei, die Sie übertragen möchten, muss sich auf einem SnapLock-Volume befinden.
- Die Datei muss beschreibbar sein.

Über diese Aufgabe

Der Band ComplexanceClock Time wird in geschrieben `ctime` Feld der Datei, 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 zu erstellen `document.txt` Schreibgeschützt:

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

Verwenden Sie in einer Windows-Shell den folgenden Befehl, um eine Datei mit dem Namen zu erstellen `document.txt` Schreibgeschützt:

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

Automatisches Versetzen von Dateien in DIE WORM-FUNKTION

Mit der Funktion für automatische Verschiebungsfunktion von SnapLock können Sie Dateien automatisch in DIE WORM-FUNKTION übertragen. Die Funktion Autocommit begeht eine Datei in DEN WORM-Status auf einem SnapLock Volume, wenn sich die Datei während der Dauer des automatischen Commit-Zeitraums nicht geändert hat. Die Funktion Autocommit ist standardmäßig deaktiviert.

Was Sie benötigen

- Die Dateien, die automatisch übertragen werden sollen, müssen auf einem SnapLock-Volume gespeichert sein.
- Das SnapLock Volume muss online sein.
- Das SnapLock Volume muss ein Lese- und Schreib-Volume sein.

> Die Funktion Autocommit von SnapLock scannt alle Dateien auf dem Volume und begeht eine Datei, wenn sie die Anforderung für automatische Übertragung erfüllt. Es kann ein Zeitintervall zwischen dem Zeitpunkt geben, in dem die Datei für die automatische Übergabe bereit ist und dem SnapLock-Lesegerät für die automatische Übertragung tatsächlich gesetzt wird. Die Datei ist jedoch weiterhin vor Änderungen und Löschung durch das Dateisystem geschützt, sobald sie für die automatische Übertragung geeignet ist.

Über diese Aufgabe

Der Zeitraum *autocommit* gibt an, wie lange Dateien vor der automatischen Übergabe unverändert bleiben müssen. Durch Ändern einer Datei vor Ablauf des automatischen Verschiebungszeitraums wird der Zeitraum für die automatische Übertragung der Datei neu gestartet.

In der folgenden Tabelle sind die möglichen Werte für den automatischen Commit-Zeitraum aufgeführt:

Wert	Einheit	Hinweise
Keine	-	Der Standardwert.
5 - 5256000	Minuten	-
1 - 87600	Stunden	-
1 - 3650	Tage	-

Wert	Einheit	Hinweise
1 - 120	Monaten	-
1 - 10	Jahren	-

Der Mindestwert beträgt 5 Minuten und der Höchstwert beträgt 10 Jahre.

Schritte

1. Automatisches Versetzen von Dateien auf einem SnapLock Volume in DIE WORM-FUNKTION:

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

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

   Mit dem folgenden Befehl werden die Dateien auf dem Volume automatisch festgeschrieben `vol1` Der SVM vs1, sofern die Dateien 5 Stunden lang unverändert bleiben:

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

ERSTELLEN einer ANGEHÄNGBAREN WORM-Datei

In einer ANGEHÄNGBAREN WORM-Datei werden die Daten, die inkrementell geschrieben werden, wie Protokolleinträge. Sie können einen beliebigen geeigneten Befehl oder ein geeignetes Programm verwenden, um eine WORM-Datei zu erstellen, oder Sie können die Funktion SnapLock_Volume append Mode_ verwenden, um STANDARDMÄSSIG WORM-Dateien zu erstellen.

Verwenden Sie einen Befehl oder ein Programm, um eine WORM-Datei zu erstellen

Sie können jeden entsprechenden Befehl oder Programm über NFS oder CIFS verwenden, um eine WORM-Datei zu erstellen. In einer ANGEHÄNGBAREN WORM-Datei werden die Daten, die inkrementell geschrieben werden, wie Protokolleinträge. Die Daten werden in 256-KB-Blöcken an die Datei angehängt. Wenn jeder Datenblock geschrieben wird, wird der vorherige Datenblock ALS WORM-geschützt. Sie können die Datei erst löschen, wenn der Aufbewahrungszeitraum abgelaufen ist.

Was Sie benötigen

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

Über diese Aufgabe

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

Schritte

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

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Aufbewahrungszeit vom 21. November

2020 6:00 Uhr festzulegen In einer Datei mit dem Namen Null-Länge `document.txt`:

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

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

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Datei mit dem Namen zu erstellen `document.txt` Schreibgeschützt:

   ```
   chmod 444 document.txt
   ```

3. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um das Lese-Schreib-Attribut der Datei wieder in beschreibbar zu ändern.

   > Dieser Schritt gilt nicht als Compliance-Risiko, da sich keine Daten in der Datei befinden.

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um eine Datei mit dem Namen zu erstellen `document.txt` Beschreibbar:

   ```
   chmod 777 document.txt
   ```

4. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um mit dem Schreiben von Daten in die Datei zu beginnen.

   Verwenden Sie in einer UNIX-Shell den folgenden Befehl, um Daten in zu schreiben `document.txt`:

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

   > Ändern Sie die Dateiberechtigungen zurück in den schreibgeschützten Bereich, wenn Sie keine Daten mehr an die Datei anhängen müssen.

Verwenden Sie den Volume Appendable-Modus, um WORM-Dateien zu erstellen

Ab ONTAP 9.3 können Sie MIT der Funktion SnapLock_Volume Append Mode_ (VAM) STANDARDMÄSSIG WORM-Dateien erstellen. In einer ANGEHÄNGBAREN WORM-Datei werden die Daten, die inkrementell geschrieben werden, wie Protokolleinträge. Die Daten werden in 256-KB-Blöcken an die Datei angehängt. Wenn jeder Datenblock geschrieben wird, wird der vorherige Datenblock ALS WORM-geschützt. Sie können die Datei erst löschen, wenn der Aufbewahrungszeitraum abgelaufen ist.

Was Sie benötigen

- Die angehängbare WORM-Datei muss sich auf einem SnapLock Volume befinden.
- Das SnapLock Volume muss abgehängt und leer werden, ohne dass Snapshot Kopien und vom Benutzer erstellte Dateien enthalten sind.

Über diese Aufgabe

Die Daten müssen nicht sequenziell in den aktiven 256-KB-Datenblock geschrieben werden. Wenn Daten in Byte n×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`

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

   Mit dem folgenden Befehl wird VAM auf dem Volume aktiviert `vol1` Der SVM`vs1`:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
   -append-mode-enabled true
   ```

2. Verwenden Sie einen geeigneten Befehl oder ein geeignetes Programm, um Dateien mit Schreibberechtigungen zu erstellen.

   Die Dateien sind standardmäßig WORM-appensible.

Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel

Mit SnapLock für SnapVault können Snapshot Kopien IM Sekundärspeicher GESICHERT WERDEN. Sie führen alle grundlegenden SnapLock-Aufgaben auf dem Vault-Ziel aus. Das Ziel-Volume wird automatisch schreibgeschützt gemountet, sodass die Snapshot Kopien nicht explizit in WORM festgeschrieben werden müssen. Somit werden geplante Snapshot Kopien auf dem Ziel-Volume mithilfe von SnapMirror Richtlinien nicht unterstützt.

Bevor Sie beginnen

- Der Quell-Cluster muss ONTAP 8.2.2 oder höher ausführen.
- Die Quell- und Zielaggregate müssen 64 Bit sein.
- Das Quell-Volume kann kein SnapLock Volume sein.
- Die Quell- und Ziel-Volumes müssen in Peering-Clustern mit Peering SVMs erstellt werden.

  Weitere Informationen finden Sie unter "Cluster-Peering".

- Wenn Autogrow-Volume deaktiviert ist, muss der freie Speicherplatz auf dem Ziel-Volume mindestens fünf Prozent mehr als der verwendete Speicherplatz auf dem Quell-Volume sein.

Über diese Aufgabe

Das Quell-Volume kann Storage von NetApp oder anderen Herstellern verwenden. Für Storage anderer Anbieter als NetApp müssen Sie die FlexArray-Virtualisierung verwenden.

> Sie können eine Snapshot Kopie, die im WORM-Status übergeben ist, nicht umbenennen.

Sie können SnapLock Volumes klonen, aber Sie können keine Dateien auf einem SnapLock Volume klonen.

> LUNs werden in SnapLock Volumes nicht unterstützt. LUNs werden in SnapLock Volumes nur in Szenarien unterstützt, in denen auf einem nicht-SnapLock Volume erstellte Snapshot Kopien zur Sicherung im Rahmen der SnapLock Vault-Beziehung auf ein SnapLock Volume übertragen werden. LUNs werden in SnapLock-Volumes mit Lese-/Schreibzugriff nicht unterstützt. Manipulationssichere Snapshot Kopien werden jedoch auf SnapMirror Quell-Volumes und Ziel-Volumes unterstützt, die LUNs enthalten.

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

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

Bei MetroCluster Konfigurationen sollten Sie die folgenden Aspekte beachten:

- Sie können eine SnapVault-Beziehung nur zwischen den synchronen Quell-SVMs und nicht zwischen einer SVM mit Sync-Source-Synchronisierung und einer SVM erstellen.
- Sie können eine SnapVault-Beziehung von einem Volume auf einer Quell-SVM zu einer datenServing-SVM erstellen.
- Es ist möglich, eine SnapVault-Beziehung zwischen einem Volume auf einer Datenservice-SVM und einem DP-Volume auf einer SVM mit synchronem Quell-Volume zu erstellen.

In der folgenden Abbildung wird das Verfahren zum Initialisieren einer SnapLock Vault-Beziehung gezeigt:

Schritte

1. Ermitteln des Ziel-Clusters
2. Auf dem Ziel-Cluster "Installieren Sie die SnapLock-Lizenz", "Initialisieren Sie die Compliance Clock", Und wenn Sie eine ONTAP-Version vor 9.10.1 verwenden, "Erstellung eines SnapLock Aggregats".
3. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Ziel-Volume des Typs `DP` Das ist entweder die gleiche oder größer als das Quellvolumen:

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

> Ab ONTAP 9.10.1 können SnapLock- und nicht-SnapLock-Volumes auf demselben Aggregat vorhanden sein. Wenn Sie ONTAP 9.10.1 verwenden, sind Sie daher nicht mehr erforderlich, ein separates SnapLock Aggregat zu erstellen. Mithilfe der Option Volume -snaplock-TYPE können Sie einen Compliance- oder Enterprise SnapLock Volume-Typ festlegen. Bei älteren Versionen als ONTAP ONTAP 9.10.1 wird der SnapLock-Modus, Compliance oder Enterprise, vom Aggregat übernommen. Versionsflexible Ziel-Volumes werden nicht unterstützt. Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

Mit dem folgenden Befehl wird eine 2-GB-SnapLock erstellt `Compliance` Volume mit Namen `dstvolB` In `SVM2` Auf dem Aggregat `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Legen Sie auf dem Ziel-Cluster den Standardaufbewahrungszeitraum fest, wie in beschrieben Legen Sie den Standardaufbewahrungszeitraum fest.

> Einem SnapLock-Volume, das ein Vault-Ziel ist, ist ein Standardaufbewahrungszeitraum zugewiesen. Der Wert für diesen Zeitraum wird zunächst auf mindestens 0 Jahre für SnapLock Enterprise Volumes und maximal 30 Jahre für SnapLock Compliance Volumes festgelegt. Jede NetApp Snapshot-Kopie wird zunächst mit diesem standardmäßigen Aufbewahrungszeitraum festgelegt. Die Aufbewahrungsfrist kann bei Bedarf später verlängert werden. Weitere Informationen finden Sie unter Aufbewahrungszeit einstellen.

5. Erstellen einer neuen Replikationsbeziehung Zwischen der nicht-SnapLock-Quelle und dem neuen SnapLock-Ziel, den Sie in Schritt 3 erstellt haben.

   Dieses Beispiel erstellt eine neue SnapMirror Beziehung mit dem Ziel-SnapLock Volume `dstvolB` Verwenden einer Richtlinie von `XDPDefault` So speichern Sie Snapshot-Kopien, die täglich und wöchentlich nach einem stündlichen Zeitplan gekennzeichnet sind:

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

> Erstellen Sie eine benutzerdefinierte Replikationsrichtlinie Oder A Benutzerdefinierter Zeitplan Wenn die verfügbaren Standardeinstellungen nicht geeignet sind.

6. Initialisieren Sie auf der Ziel-SVM die SnapVault-Beziehung, die in Schritt 5 erstellt wurde:

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

   Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume initialisiert `srcvolA` Ein `SVM1` Und dem Ziel-Volume `dstvolB` Ein `SVM2`:

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

7. Nachdem die Beziehung initialisiert und inaktiv ist, verwenden Sie den `snapshot show` Befehl auf dem Ziel, um zu überprüfen, ob die SnapLock-Ablaufzeit auf die replizierten Snapshot Kopien angewendet wurde.

   Dieses Beispiel führt die Snapshot Kopien auf dem Volume auf `dstvolB` Die über das SnapMirror-Etikett und das SnapLock-Ablaufdatum verfügen:

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

Verwandte Informationen

"Cluster- und SVM-Peering"

"Volume Backup mit SnapVault"

SPIEGELN VON WORM-Dateien für das Disaster Recovery

AUSSERDEM KÖNNEN WORM-Dateien zur Disaster Recovery und zu anderen Zwecken an einem anderen geografischen Standort repliziert werden. Das Quell-Volume und das Ziel-Volume müssen für SnapLock konfiguriert werden. Dabei müssen beide Volumes denselben SnapLock-Modus, dieselbe Konformität oder ein Enterprise aufweisen. Alle wichtigen SnapLock Eigenschaften des Volume und der Dateien werden repliziert.

Voraussetzungen

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

Über diese Aufgabe

- Ab ONTAP 9.5 können Sie WORM-Dateien mit dem XDP-Typ (erweiterte Datensicherung) SnapMirror Beziehung replizieren, anstatt die DP-Beziehung (Datenschutz) zu verwenden. XDP-Modus ist unabhängig von der ONTAP-Version und ist in der Lage, Dateien im selben Block zu differenzieren, was die Resynchronisierung replizierter Compliance-Modus-Volumes erheblich erleichtert. Informationen zum Konvertieren einer bestehenden DP-Typ-Beziehung in eine XDP-Beziehung finden Sie unter "Datensicherung".
- Resync-Vorgang auf einer DP-Typ SnapMirror-Beziehung schlägt für ein Compliance-Modus-Volume fehl, wenn SnapLock feststellt, dass es zu einem Datenverlust führt. Falls ein Resynchronisierungsvorgang fehlschlägt, können Sie das verwenden `volume clone create` Befehl, um einen Klon des Ziel-Volume zu erstellen. Sie können dann das Quell-Volume mit dem Klon neu synchronisieren.
- Eine SnapMirror-Beziehung des Typs XDP zwischen SnapLock-konformen Volumes unterstützt eine Resynchronisierung nach einer Pause, auch wenn Daten auf dem Ziel von der Quelle nach der Pause umgeleitet wurden.

  Wenn bei einer Resynchronisierung Datendivergenz zwischen der Quelle, dem Ziel über den gemeinsamen Snapshot hinaus erkannt wird, wird ein neuer Snapshot auf das Ziel geschnitten, um diese Divergenz zu erfassen. Der neue Snapshot und der gemeinsame Snapshot sind mit einer Aufbewahrungszeit wie folgt gesperrt:

  - Die Verfallszeit des Zieldatums

- Wenn die Ablaufzeit des Datenträgers in der Vergangenheit liegt oder noch nicht eingestellt wurde, wird der Snapshot für einen Zeitraum von 30 Tagen gesperrt
- Wenn das Ziel gesetzliche Aufbewahrungspflichten hat, wird die tatsächliche Verfallszeit des Volumens maskiert und zeigt sich als ‘undefined’ an, der Snapshot ist jedoch für die Dauer des tatsächlichen Verfallszeitraums des Volumens gesperrt.

Wenn das Ziellaufwerk eine Ablauffrist hat, die später als das Quellvolumen ist, wird die Gültigkeitsdauer des Zieldatums beibehalten und wird nach der Resynchronisierung nicht durch den Ablaufzeitraum des Quellvolumens überschrieben.

Wenn auf dem Ziel gesetzliche Aufbewahrungspflichten liegen, die sich von der Quelle unterscheiden, ist eine Resynchronisierung nicht zulässig. Quelle und Ziel müssen identische gesetzlichen Aufbewahrungspflichten haben oder alle gesetzlichen Aufbewahrungspflichten auf dem Ziel müssen vor Beginn einer Neusynchronisierung freigegeben werden.

Eine gesperrte Snapshot Kopie auf dem Ziel-Volume, das zum Erfassen der divergenten Daten erstellt wurde, kann mithilfe der CLI auf die Quelle kopiert werden `snapmirror update -s snapshot` Befehl. Der nach dem Kopieren kopierte Snapshot wird weiterhin an der Quelle gesperrt.

- SVM-Datensicherungsbeziehungen werden nicht unterstützt.
- Beziehungen zur Lastverteilung für Daten werden nicht unterstützt.

Die folgende Abbildung zeigt das Verfahren zur Initialisierung einer SnapMirror Beziehung:

System Manager

Ab ONTAP 9.12.1 kann mit System Manager die SnapMirror Replizierung von WORM-Dateien eingerichtet werden.

Schritte

1. Navigieren Sie zu **Storage > Volumes**.
2. Klicken Sie auf **ein-/Ausblenden** und wählen Sie **SnapLock-Typ**, um die Spalte im Fenster **Volumen** anzuzeigen.
3. Suchen Sie ein SnapLock Volume.
4. Klicken Sie Auf ⋮ Und wählen Sie **Protect**.
5. Auswahl des Ziel-Clusters und der Ziel-Storage-VM
6. Klicken Sie Auf **Weitere Optionen**.
7. Wählen Sie **Legacy-Richtlinien anzeigen** und wählen Sie **DPDefault (Legacy)**.
8. Wählen Sie im Abschnitt **Zielkonfigurationsdetails** die Option **Transferzeitplan überschreiben** aus und wählen Sie **stündlich** aus.
9. Klicken Sie Auf **Speichern**.
10. Klicken Sie links vom Namen des Quell-Volumes auf den Pfeil, um die Volume-Details zu erweitern, und rechts auf der Seite sehen Sie die Remote SnapMirror Sicherungsdetails.
11. Navigieren Sie auf dem Remote-Cluster zu **Protection Relationships**.
12. Suchen Sie die Beziehung, und klicken Sie auf den Namen des Zielvolumes, um die Beziehungsdetails anzuzeigen.
13. Überprüfen Sie, ob der SnapLock-Typ des Ziel-Volumes und andere SnapLock-Informationen verwendet werden.

CLI

1. Ermitteln des Ziel-Clusters
2. Auf dem Ziel-Cluster "Installieren Sie die SnapLock-Lizenz", "Initialisieren Sie die Compliance Clock", Und wenn Sie eine ONTAP-Version vor 9.10.1 verwenden, "Erstellung eines SnapLock Aggregats".
3. Erstellen Sie auf dem Ziel-Cluster ein SnapLock Ziel-Volume des Typs `DP` Das ist entweder die gleiche Größe wie oder größer als das Quellvolumen:

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

   > Ab ONTAP 9.10.1 können SnapLock- und nicht-SnapLock-Volumes auf demselben Aggregat vorhanden sein. Wenn Sie ONTAP 9.10.1 verwenden, sind Sie daher nicht mehr erforderlich, ein separates SnapLock Aggregat zu erstellen. Mithilfe der Option Volume -snaplock-TYPE können Sie einen Compliance- oder Enterprise SnapLock Volume-Typ festlegen. In älteren Versionen als ONTAP ONTAP 9.10.1 übernimmt der SnapLock-Modus – Compliance oder Enterprise – das Aggregat. Versionsflexible Ziel-Volumes werden nicht unterstützt. Die Spracheinstellung des Zielvolumens muss mit der Spracheinstellung des Quellvolumens übereinstimmen.

   Mit dem folgenden Befehl wird eine 2-GB-SnapLock erstellt `Compliance` Volume mit Namen `dstvolB` In `SVM2` Auf dem Aggregat `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Erstellen Sie auf der Ziel-SVM eine SnapMirror Richtlinie:

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

   Mit dem folgenden Befehl wird die SVM-weite Richtlinie erstellt `SVM1-mirror`:

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

5. Erstellen Sie auf der Ziel-SVM einen SnapMirror Zeitplan:

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

   Mit dem folgenden Befehl wird ein SnapMirror Zeitplan mit dem Namen erstellt `weekendcron`:

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

6. Erstellen Sie auf der Ziel-SVM eine SnapMirror Beziehung:

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

   Mit dem folgenden Befehl wird eine SnapMirror Beziehung zwischen dem Quell-Volume erstellt `srcvolA` Ein `SVM1` Und dem Ziel-Volume `dstvolB` Ein `SVM2`, Und weist die Richtlinie zu `SVM1-mirror` Und Zeitplan `weekendcron`:

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

   Der XDP-Typ ist in ONTAP 9.5 und höher erhältlich. Sie müssen den DP-Typ in ONTAP 9.4 und früher verwenden.

7. Initialisieren Sie auf der Ziel-SVM die SnapMirror-Beziehung:

   snapmirror initialize -destination-path *destination_path*

   Der Initialisierungsvorgang führt einen *Baseline Transfer* zum Ziel-Volume durch. SnapMirror erstellt eine Snapshot-Kopie des Quell-Volume und überträgt dann die Kopie mit allen Datenblöcken, die er auf das Ziel-Volume verweist. Sie überträgt zudem alle anderen Snapshot Kopien auf dem Quell-Volume auf das Ziel-Volume.

Mit dem folgenden Befehl wird die Beziehung zwischen dem Quell-Volume initialisiert `srcvolA` Ein `SVM1` Und dem Ziel-Volume `dstvolB` Ein `SVM2`:

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

Verwandte Informationen

"Cluster- und SVM-Peering"

"Vorbereitung der Volume Disaster Recovery"

"Datensicherung"

BEWAHREN SIE WORM-Dateien bei Rechtsstreitigkeiten mithilfe der gesetzlichen Aufbewahrung auf

Ab ONTAP 9.3 können Sie WORM-Dateien im Compliance-Modus während der Dauer eines Rechtsstreits mithilfe der Funktion *Legal Hold* aufbewahren.

Was Sie benötigen

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

  "Erstellen Sie ein SnapLock-Administratorkonto"

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

Über diese Aufgabe

Eine Datei unter einer gesetzlichen Aufbewahrungspflichten, verhält sich wie EINE WORM-Datei mit einer unbestimmten Aufbewahrungsfrist. Es liegt in Ihrer Verantwortung anzugeben, wann die gesetzliche Haltefrist endet.

Die Anzahl der Dateien, die Sie unter einem Legal Hold platzieren können, hängt von dem verfügbaren Speicherplatz des Volume ab.

Schritte

1. Gesetzliche Aufbewahrungspflichten starten:

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

   Mit dem folgenden Befehl wird ein Legal Hold für alle Dateien in gestartet `vol1`:

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

2. Beenden einer gesetzlichen Aufbewahrungspflichten:

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

Mit dem folgenden Befehl wird ein Legal Hold für alle Dateien in beendet `vol1`:

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

ÜBERSICHT ZU WORM-Dateien löschen

SIE können WORM-Dateien im Enterprise-Modus während des Aufbewahrungszeitraums mit der Funktion Privileged delete löschen. Bevor Sie diese Funktion verwenden können, müssen Sie ein SnapLock-Administratorkonto erstellen und dann die Funktion mit dem Konto aktivieren.

Erstellen Sie ein SnapLock-Administratorkonto

Sie benötigen Administratorrechte von SnapLock, um ein privilegiertes Löschen durchführen zu können. Diese Berechtigungen werden in der Rolle vsadmin-snaplock definiert. Wenn Sie dieser Rolle noch nicht zugewiesen haben, können Sie den Cluster-Administrator bitten, ein SVM-Administratorkonto mit der SnapLock-Administratorrolle zu erstellen.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen sich mit einer sicheren Verbindung (SSH, Konsole oder ZAPI) angemeldet haben.

Schritte

1. SVM-Administratorkonto mit der SnapLock-Administratorrolle erstellen:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `SnapLockAdmin` Mit dem vordefinierten `vsadmin-snaplock` Rolle für den Zugriff `SVM1` Verwenden eines Passworts:

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

Aktivieren Sie die Funktion „privilegiertes Löschen“

Sie müssen das Priviledged delete-Feature auf dem Enterprise Volume, das die ZU löschenden WORM-Dateien enthält, explizit aktivieren.

Über diese Aufgabe

Der Wert des `-privileged-delete` Mit dieser Option wird festgelegt, ob das privilegierte Löschen aktiviert ist. Mögliche Werte sind `enabled`, `disabled`, und `permanently-disabled`.

`permanently-disabled` Ist der Terminalstatus. Sie können das privilegierte Löschen auf dem Volume nicht aktivieren, nachdem Sie den Status auf festgelegt haben `permanently-disabled`.

Schritte

1. Privilegiertes Löschen für ein SnapLock Enterprise Volume aktivieren:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   Mit dem folgenden Befehl wird die Privileged delete-Funktion für das Enterprise Volume aktiviert `dataVol` Ein `SVM1`:

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

LÖSCHEN SIE WORM-Dateien im Enterprise-Modus

Mit der Funktion Priviledged delete können SIE WORM-Dateien im Enterprise-Modus während des Aufbewahrungszeitraums löschen.

Was Sie benötigen

- Sie müssen ein SnapLock-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen ein SnapLock-Auditprotokoll erstellt und die Funktion zum Löschen von Berechtigungen auf dem Enterprise Volume aktiviert haben.

Über diese Aufgabe

Sie können eine abgelaufene WORM-Datei nicht mit einem privilegierten Löschvorgang löschen. Sie können das verwenden `volume file retention show` Befehl zum Anzeigen der Aufbewahrungszeit der WORM-Datei, die Sie löschen möchten. Weitere Informationen finden Sie auf der man-Page für den Befehl.

Schritt

1. LÖSCHEN EINER WORM-Datei auf einem Enterprise Volume:

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

   Mit dem folgenden Befehl wird die Datei gelöscht `/vol/dataVol/f1` Auf der SVM`SVM1`:

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

SnapLock Volumes werden verschoben

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

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

Erstellen Sie ein SnapLock-Sicherheitsadministratorkonto

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

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen sich mit einer sicheren Verbindung (SSH, Konsole oder ZAPI) angemeldet haben.

Über diese Aufgabe

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

Schritt

1. SVM-Administratorkonto mit der SnapLock-Administratorrolle erstellen:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Mit dem folgenden Befehl wird das SVM-Administratorkonto aktiviert `SnapLockAdmin` Mit dem vordefinierten `snaplock` Rolle für den Zugriff auf Admin-SVM `cluster1` Verwenden eines Passworts:

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

SnapLock Volumes werden verschoben

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

Was Sie benötigen

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

  "Erstellen eines Prüfprotokolls".

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

Schritte

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

   ```
   ssh snaplock_user@cluster_mgmt_ip
   ```

2. Verschieben eines SnapLock Volumes:

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

3. Prüfen Sie den Status der Volume-Verschiebung:

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

Sperren einer Snapshot Kopie zum Schutz vor Ransomware-Angriffen

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

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

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

Überlegungen und Überlegungen zu Snapshot Kopien vor Manipulationen

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

Spiegelungs-Vault festlegen. Der Aufbewahrungszeitraum wird für Snapshot Kopien, die auf dem Ziel-Volume repliziert werden, angewendet, wenn die Sperrung der Snapshot Kopien aktiviert ist. Der Aufbewahrungszeitraum hat Vorrang vor der Datenanzahl. Beispielsweise werden Snapshot Kopien, die ihren Ablaufdatum nicht bestanden haben, auch dann beibehalten, wenn die behalten wird.

- Sie können eine Snapshot-Kopie auf einem nicht-SnapLock-Volume umbenennen. Umbenennungsvorgänge für Snapshots auf dem primären Volume einer SnapMirror-Beziehung werden nur auf dem sekundären Volume wiedergegeben, wenn die Richtlinie MirrorAllSnapshots ist. Bei anderen Richtlinientypen wird die umbenannte Snapshot Kopie während Updates nicht propagiert.
- Wenn Sie die ONTAP CLI verwenden, können Sie eine gesperrte Snapshot Kopie mit dem wiederherstellen `volume snapshot restore` Befehl nur, wenn die gesperrte Snapshot Kopie das aktuellste ist. Wenn später noch nicht abgelaufene Snapshot Kopien als der wiederherzustellende Snapshot Kopie vorhanden sind, schlägt der Wiederherstellungsvorgang für die Snapshot Kopie fehl.

Funktionen, die durch manipulationssichere Snapshot Kopien unterstützt werden

- FlexGroup Volumes

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

- Konvertierung von FlexVol zu FlexGroup

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

- Volume-Klon und Dateiklon

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

Nicht unterstützte Funktionen

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

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

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

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

System Manager

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

CLI

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

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

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

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: Snapshot copy locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked Snapshot
   copies are past their expiry time. A volume with unexpired locked
   Snapshot copies cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Aktivieren Sie die Sperrung von Snapshot Kopien auf einem vorhandenen Volume

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

System Manager

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

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

CLI

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

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

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

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

Erstellen Sie eine Sperrrichtlinie für Snapshot Kopien

System Manager

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

CLI

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

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

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

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

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

Wenden Sie eine Sperrrichtlinie auf ein Volume an

System Manager

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

CLI

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

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

Wenden Sie den Aufbewahrungszeitraum während der Erstellung manueller Snapshot Kopien an

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

System Manager

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

CLI

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

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

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

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Wenden Sie den Aufbewahrungszeitraum auf eine vorhandene Snapshot Kopie an

System Manager

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

CLI

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

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

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

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -expiry-time "11/10/2022 09:00:00"
   ```

Ändern Sie eine vorhandene Richtlinie, um die langfristige Aufbewahrung anzuwenden

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

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

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

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

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

SnapLock APIs

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

Datei-Fingerabdruck-Abbruch

Abbrechen eines Fingerabdruckvorgangs für die Datei.

Datei-Fingerabdruck-Dump

Anzeigen von Fingerabdruckinformationen für Dateien

Datei-Fingerabdruck-get-iter

Zeigt den Status von Datei-Fingerabdruckoperationen an.

Starten von Datei-Fingerabdruck

Generieren eines DateiFingerabdrucks.

snaplock-ArchivvServer-Protokoll

Archivieren Sie die aktive Audit-Log-Datei.

snaplock-create-vserver-log

Erstellen einer Auditprotokollkonfiguration für eine SVM

snaplock-delete-vServer-Protokoll

Löschen einer Audit-Protokollkonfiguration für eine SVM

snaplock-Datei mit Privileged-delete

Führen Sie einen privilegierten Löschvorgang aus.

snaplock-Get-Retention

Erhalten Sie den Aufbewahrungszeitraum einer Datei.

snaplock-get-Node-Compliance-Clock

Abrufen des Knotens CompleanceClock Datum und Uhrzeit.

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

Zeigt den Status der aktiven Protokolldateien an.

snaplock-get-vserver-log-iter

Zeigt die Konfiguration des Prüfprotokolls an.

snaplock-modify-vserver-log

Ändern der Konfiguration des Prüfprotokolls für eine SVM

snaplock-Set-file-Retention

Aufbewahrungszeit für eine Datei festlegen.

snaplock-Set-Node-Compliance-Clock

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

snaplock-Volume-set-privilegiert-delete

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

Volume-get-snaplock-attrs

Erhalten Sie die Attribute eines SnapLock Volume.

Volume-Set-snaplock-attrs

Legen Sie die Attribute eines SnapLock-Volumes fest.

Konsistenzgruppen

Übersicht über Konsistenzgruppen

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.

Konsistenzgruppen erleichtern das Management von Applikations-Workloads, sorgen dabei für einfach konfigurierte lokale und Remote-Sicherungsrichtlinien sowie gleichzeitige absturzkonsistente oder applikationskonsistente Snapshot Kopien einer Sammlung von Volumes zu einem bestimmten Zeitpunkt. Snapshot Kopien einer Consistency Groups ermöglichen die Wiederherstellung eines gesamten Applikations-Workloads.

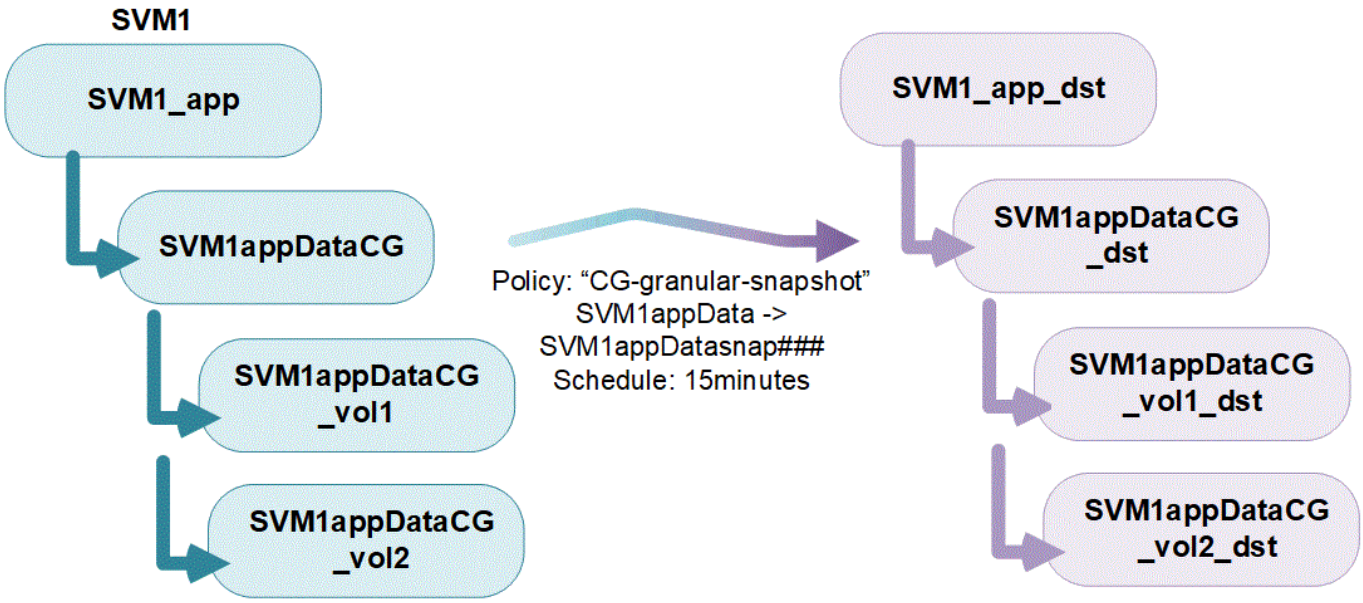
Erfahren Sie mehr über Konsistenzgruppen

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.

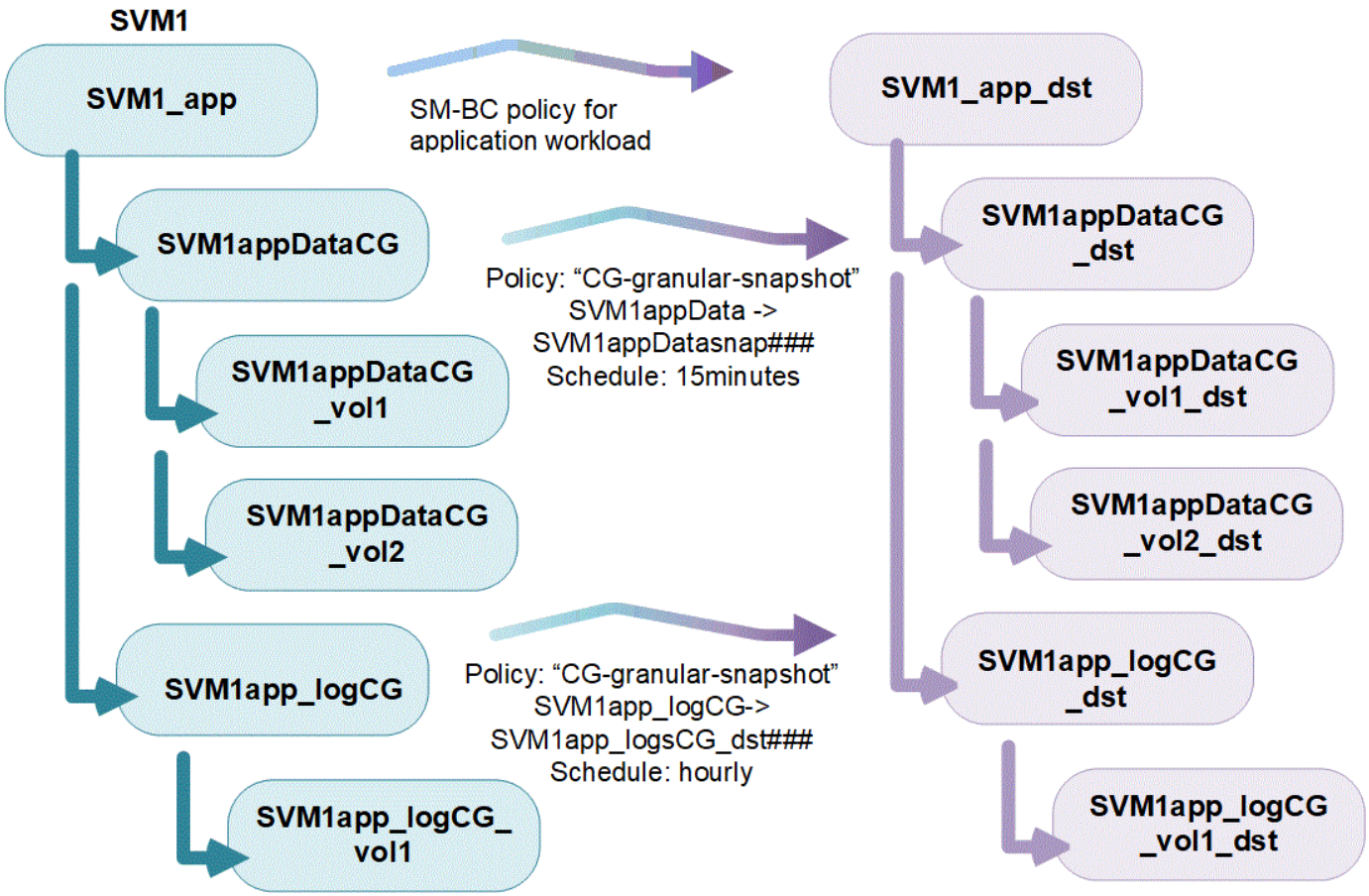
Consistency Groups können als einzelne Entitäten – als Sammlung von Volumes – oder in einer hierarchischen Beziehung existieren, die aus anderen Consistency Groups besteht. Einzelne Volumes können über eine eigene Snapshot-Richtlinie auf Volume-Granularität verfügen. Darüber hinaus kann es eine Snapshot Policy für die gesamte Konsistenzgruppe geben. Die Konsistenzgruppe kann nur eine SnapMirror Business Continuity (SM-BC) Beziehung und gemeinsame SM-BC Richtlinie haben, 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 auf gehostete Applikation `SVM1` Umfasst zwei Volumes: `vol1` Und `vol2`. Eine Snapshot-Richtlinie auf der Konsistenzgruppe erfasst alle 15 Minuten Snapshot-Kopien 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 eine Remote SM-BC-Sicherungsrichtlinie auf die gesamte Konfiguration von Konsistenzgruppen (übergeordnete und untergeordnete Elemente) angewendet werden, um den Applikations-Workload wiederherzustellen.

Im folgenden Beispiel wird eine Applikation auf gehostet `SVM1`. Der Administrator hat eine übergeordnete Konsistenzgruppe erstellt. `SVM1_app`, Die zwei Child-Konsistenzgruppen umfasst: `SVM1appDataCG` Für die Daten und `SVM1app_logCG` Für die Protokolle. Jede untergeordnete Konsistenzgruppe verfügt über eine eigene Snapshot-Richtlinie. Snapshot Kopien der Volumes in `SVM1appDataCG` Werden alle 15 Minuten gebraucht. Snapshots von `SVM1app_logCG` Werden stündlich genommen. Die übergeordnete Konsistenzgruppe `SVM1_app` Hat eine SM-BC-Richtlinie, die die Daten repliziert, um einen kontinuierlichen Service im Notfall zu gewährleisten.



Ab ONTAP 9.12.1 unterstützen Konsistenzgruppen Klonen Und die Mitglieder der Konsistenz durch ändern Hinzufügen oder Entfernen von Volumes Sowohl 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 Konsistenzgruppenmetriken mit der CLI mithilfe von anzeigen `consistency-group metrics show` Befehl.

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 bieten Schutz über:

- Snapshot-Richtlinien
- SnapMirror Business Continuity (SM-BC)
- [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 von Schutz für eine Konsistenzgruppe finden Sie unter "Sichern einer Konsistenzgruppe".

Um die Remote-Sicherung zu nutzen, müssen Sie die Anforderungen für erfüllen SnapMirror für Business Continuity-Implementierungen.

SM-BC-Beziehungen können nicht auf Volumes eingerichtet werden, die für den NAS-Zugriff gemountet sind.

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 Snapshot Kopien, die zu Konsistenzgruppen zugeordnet sind, 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 Snapshot Kopien von Konsistenzgruppen und System Manager auf Clustern zugreifen, auf denen ONTAP 9.11.1 oder höher ausgeführt wird. Ab ONTAP 9.14.1 können Sie auch über die ONTAP CLI auf Snapshot Kopien 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 Standort B ONTAP 9.10.1 oder eine frühere Version ausführt, werden nur die Volumes repliziert, die mit den Konsistenzgruppen in gespiegelten Aggregaten verknüpft sind Die Konfigurationen der Konsistenzgruppen

werden nur an Standort B repliziert, wenn auf beiden Standorten ONTAP 9.11.1 oder höher ausgeführt wird. 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, dass Sie für gespiegelte Aggregate mindestens 20 % freien Speicherplatz freihalten, um so optimale Storage Performance und Verfügbarkeit zu erzielen. Obwohl die Empfehlung 10 % für nicht gespiegelte Aggregate ist, können die zusätzlichen 10 % des Speicherplatzes vom Dateisystem verwendet werden, um inkrementelle Änderungen aufzunehmen. Inkrementelle Änderungen erhöhen die Speicherplatzauslastung für gespiegelte Aggregate aufgrund der Snapshot-basierten Architektur von ONTAP, die auf dem Copy-on-Write basiert. Die Nichteinhaltung dieser Best Practices kann sich negativ auf die Performance auswirken.

Upgrade-Überlegungen

Consistency Groups, die mit SM-BC in ONTAP 9.8 und 9.9.1 erstellt wurden, werden beim Upgrade auf ONTAP 9.10.1 oder höher automatisch aktualisiert und unter **Speicher > Consistency Groups** im System Manager oder der ONTAP REST API verwaltet. Weitere Informationen zum Upgrade von ONTAP 9.8 oder 9.9.1 finden Sie unter "SM-BC Upgrade und Überlegungen zurücksetzen".

In der REST-API erstellte Snapshot Kopien 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.

> Snapshot Kopien werden mit den ONTAPI Befehlen erstellt `cg-start` Und `cg-commit` Sie werden als Snapshots der Konsistenzgruppe erkannt und 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 Snapshot-Kopien unter Verwendung einer asynchronen SnapMirror Richtlinie auf das Ziel-Volume gespiegelt werden. Weitere Informationen finden Sie unter Konfigurieren Sie den asynchronen SnapMirror Schutz.

Unterstützte Funktionen von Version

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Hierarchische Konsistenzgruppen	✓	✓	✓	✓	✓
Lokale Sicherung durch Snapshot Kopien	✓	✓	✓	✓	✓
SnapMirror Business Continuity	✓	✓	✓	✓	✓
MetroCluster Support	✓	✓	✓	✓	
Zwei-Phasen-Commits (nur REST API)	✓	✓	✓	✓	
Applikations- und Komponenten-Tags	✓	✓	✓		
Klonen von Konsistenzgruppen	✓	✓	✓		
Hinzufügen und Entfernen von Volumes	✓	✓	✓		

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
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	✓	✓			
Asynchronous SnapMirror (nur einzelne Konsistenzgruppen)	✓	✓			
SVM-Disaster Recovery (nur einzelne Konsistenzgruppen)	✓				
CLI-Unterstützung	✓				

Weitere Informationen zu Konsistenzgruppen

Weitere Informationen

- "Dokumentation zur ONTAP-Automatisierung"
- SnapMirror Business Continuity
- Grundlagen der asynchronen SnapMirror Disaster Recovery
- "MetroCluster-Dokumentation"

Einschränkungen für Konsistenzgruppen

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 Business Continuity (SM-BC) verwenden, gelten gesonderte Einschränkungen. Weitere Informationen finden Sie unter "SM-BC Einschränkungen und Einschränkungen nach Limits".

Grenze	Umfang	Minimum	Maximal
Anzahl der Konsistenzgruppen	Cluster	0	Die maximale Anzahl der Volumes im Cluster entspricht
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 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

Nicht erzwungene Grenzwerte

Der Zeitplan für unterstützte Snapshot Kopien in Konsistenzgruppen beträgt mindestens 30 Minuten. Diese Grundlage basiert auf "Tests für FlexGroups", Die dieselbe Snapshot-Infrastruktur wie Konsistenzgruppen verwenden.

Konfigurieren einer einzelnen 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 Prozess finden Sie unter Ändern einer Konsistenzgruppe.

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

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 Tagging 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.

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.

Erstellen Sie eine Konsistenzgruppe mit NFS-Volumes

1. Erstellen Sie die Konsistenzgruppe:

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-
   group-name -volume volume-prefix -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 -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
   ```

Nachdem Sie fertig sind

1. Überprüfen Sie, ob Ihre Konsistenzgruppe mit erstellt wurde `consistency-group show` Befehl.

Erstellen einer Konsistenzgruppe mit vorhandenen Volumes

Sie können vorhandene Volumes zum Erstellen einer Konsistenzgruppe verwenden.

System Manager

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 Tagging von Konsistenz in Applikations- und Komponenten-Tags. Wenn die Konsistenzgruppe eine SM-BC Beziehung hat, müssen Sie **andere** verwenden.
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 asynchronen oder synchronen SnapMirror Beziehungen können zu Konsistenzgruppen hinzugefügt werden, sind aber nicht kompatibel mit Konsistenzgruppen. Konsistenzgruppen unterstützen keine S3-Buckets oder Storage-VMs mit SVMDR-Beziehungen.

5. Wählen Sie **Speichern**.
6. 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 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, Remote oder lokal, einen grünen Schild sehen.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der ONTAP CLI eine Konsistenzgruppe mit vorhandenen Volumes erstellen.

Schritte

1. Stellen Sie das aus `consistency-group create` Befehl. Der `-volumes` Der Parameter akzeptiert eine kommagetrennte Liste von Volume-Namen.

   ```
   consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
   ```

2. Zeigen Sie mithilfe der die Konsistenzgruppe an `consistency-group show` Befehl.

Nächste Schritte

- Sichern einer Konsistenzgruppe
- Ändern einer Konsistenzgruppe
- Klonen einer Konsistenzgruppe

Konfigurieren Sie eine hierarchische 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).

Ab ONTAP 9.13.1 ist dies möglich Ändern Sie die Geometrie der Konsistenzgruppen Und Verschieben Sie Volumes zwischen untergeordneten Konsistenzgruppen.

Informationen zu Objektbeschränkungen 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 Tagging 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

Ab ONTAP 9.14.1 können Sie mithilfe der CLI eine neue hierarchische Konsistenzgruppe erstellen.

Schritt

1. Erstellen Sie die neue Konsistenzgruppe mit `consistency-group create` Befehl.

   Der `volume-count` Parameter legt die Anzahl der Volumes in der jeweiligen untergeordneten Konsistenzgruppe fest. Sie können eine übergeordnete Konsistenzgruppe mit maximal fünf untergeordneten Konsistenzgruppen erstellen.

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -cg-count number_of_child_consistency_groups
-volume volume_prefix -volume-count number -size size -export-policy
policy_name -storage-service extreme
```

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 Tagging 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.

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. Eingabe `y` Bestätigen Sie, dass Sie eine neue übergeordnete und untergeordnete Konsistenzgruppe erstellen möchten.

Nächste Schritte

- Ändern Sie die Geometrie einer Konsistenzgruppen
- Ändern einer Konsistenzgruppe
- Sichern einer Konsistenzgruppe

Schützen Sie Konsistenzgruppen

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 Snapshot Kopien
- SnapMirror Business Continuity (SM-BC)
- 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 an Erstellung von Snapshots mit zwei Phasen einer Konsistenzgruppe. Bei dem Snapshot Vorgang in zwei Phasen wird eine Vorabprüfung durchgeführt, um sicherzustellen, dass die Snapshot Kopie erfolgreich erfasst wurde.

Die Wiederherstellung kann für eine gesamte Konsistenzgruppe, eine einzelne Konsistenzgruppe in einer hierarchischen Konfiguration oder für einzelne Volumes innerhalb der Konsistenzgruppe erfolgen. Das Recovery kann durch Auswahl der Konsistenzgruppe, von der Sie wiederherstellen möchten, durch Auswahl des Typs der Snapshot Kopie und dann durch Identifizieren der Snapshot Kopie auf der Basis der Wiederherstellung erfolgen. Weitere Informationen zu diesem Prozess finden Sie unter "Wiederherstellung eines Volume aus einer früheren Snapshot Kopie".

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 Zeitplan für unterstützte Snapshot Kopien in Konsistenzgruppen beträgt mindestens 30 Minuten. Diese Grundlage basiert auf "Tests für FlexGroups", 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 **Snapshot-Kopien 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 **Snapshot Kopien (lokal)** wird der Status neben geschützt angezeigt .

CLI

Ab ONTAP 9.14.1 können Sie die Schutzrichtlinie einer Konsistenzgruppe über die CLI ändern.

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 von identifizieren `-parent-consistency-group` *`parent_consistency_group_name`* Parameter.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Erstellung einer On-Demand Snapshot Kopie

Wenn Sie eine Snapshot-Kopie Ihrer Konsistenzgruppe außerhalb einer normalerweise geplanten Richtlinie erstellen müssen, können Sie eine On-Demand-Kopie erstellen.

System Manager

Schritte

1. Navigieren Sie zu **Storage** > **Consistency Groups**.
2. Wählen Sie die Konsistenzgruppe aus, für die Sie eine On-Demand-Snapshot Kopie 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 über die CLI eine On-Demand-Snapshot Kopie einer Konsistenzgruppe erstellen.

Schritt

1. Erstellen Sie die Snapshot Kopie:

   Standardmäßig ist der Snapshot-Typ absturzkonsistent. Sie können den Snapshot-Typ mit der optionalen Option ändern `-type` Parameter.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Erstellung von Snapshots von Konsistenzgruppen in zwei Phasen

Ab ONTAP 9.11.1 unterstützen Konsistenzgruppen die Snapshot-Erstellung von Konsistenzgruppen mit zwei-Phasen-Commits, die vor dem Übergeben der Snapshot Kopie 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, keine Konsistenzgruppen bereitstellen oder Konsistenzgruppen wiederherstellen.

Ein CG-Snapshot aus zwei Phasen unterbricht die Snapshot-Erstellung in zwei Phasen:

1. In der ersten Phase führt die API Vorabprüfungen aus und löst die Snapshot Erstellung aus. Die erste Phase umfasst einen Timeout-Parameter, der die Zeit angibt, für die die Snapshot Kopie erfolgreich übergeben werden konnte.
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 die Snapshot Kopie an den entsprechenden Endpunkt übergeben.

Bevor Sie beginnen

- Um Snapshots mit zwei Phasen zu verwenden, müssen alle Nodes im Cluster ONTAP 9.11.1 oder höher ausführen.
- Es wird jeweils nur ein aktiver Aufruf eines Snapshot-Vorgangs einer Konsistenzgruppe auf einer Konsistenzgruppe unterstützt, unabhängig davon, ob es sich um eine ein- oder zwei-Phasen-Instanz 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 Zeitüberschreitungswert 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 fest `action_timeout` Parameter. Verwenden Sie in der CLI die `-timeout` Flagge.

Schritte

Sie können einen zweiphasigen Snapshot mit der REST-API oder ab ONTAP 9.14.1 auch mit der ONTAP-CLI abschließen. Dieser Vorgang wird von System Manager nicht unterstützt.

> Wenn Sie die Snapshot Erstellung mit der API aufrufen, müssen Sie die Snapshot Kopie mit der API festschreiben. Wenn Sie die Snapshot Erstellung mit der CLI aufrufen, müssen Sie die Snapshot Kopie mit der CLI übertragen. Mischmethoden werden nicht unterstützt.

CLI

Ab ONTAP 9.14.1 können Sie mithilfe der CLI eine Snapshot Kopie mit zwei Phasen erstellen.

Schritte

1. Initiieren Sie den Snapshot:

   ```
   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. Festlegen des Snapshot:

   ```
   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 mithilfe von an den Endpunkt der Konsistenzgruppe `action=start` Parameter.

   ```
   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 zum Übergeben der Snapshot Kopie.

```
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 SM-BC und ab ONTAP 9.13.1 asynchronen SnapMirror.

Konfigurieren Sie den Schutz mit SM-BC

Sie können SM-BC verwenden, um sicherzustellen, dass Snapshot Kopien von Konsistenzgruppen, die in der Konsistenzgruppe erstellt werden, auf das Ziel kopiert werden. Weitere Informationen zu SM-BC oder zur Konfiguration von SM-BC mithilfe der CLI finden Sie unter Schutz für Business Continuity konfigurieren.

Bevor Sie beginnen

- SM-BC-Beziehungen können nicht auf Volumes eingerichtet werden, die für den NAS-Zugriff gemountet sind.
- Die Richtlinienbeschriftungen im Quell- und Ziel-Cluster müssen übereinstimmen.
- SM-BC repliziert Snapshot Kopien nicht standardmäßig, es sei denn, eine Regel mit einem SnapMirror-Label wird dem vordefinierten hinzugefügt `AutomatedFailOver` Richtlinie und die Snapshot Kopien werden mit diesem Etikett erstellt.

  Weitere Informationen zu diesem Prozess finden Sie unter "Schützen Sie mit SM-BC".

- Kaskadenimplementierungen Werden mit SM-BC nicht unterstützt.
- Ab ONTAP 9.13.1 ist dies unterbrechungsfrei Fügen Sie einer Konsistenzgruppe Volumes hinzu Mit einer aktiven SM-BC-Beziehung. Bei allen anderen Änderungen an einer Konsistenzgruppe müssen Sie die SM-BC-Beziehung unterbrechen, die Konsistenzgruppe ändern, dann die Beziehung wiederherstellen und neu synchronisieren.

> Informationen zum Konfigurieren von SM-BC mit der CLI finden Sie unter Schützen Sie mit SM-BC.

Schritte für System Manager

1. Stellen Sie sicher, dass Sie den erfüllt haben "Voraussetzungen für die Verwendung von SM-BC".
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 angezeigt `Protected` Neben .

Konfigurieren Sie den asynchronen SnapMirror Schutz

Ab ONTAP 9.13.1 können Sie asynchronen SnapMirror Schutz für eine einzelne Konsistenzgruppe konfigurieren. Ab ONTAP 9.14.1 können Sie mithilfe von asynchronem SnapMirror Replizierung von Volume-granularen Snapshot Kopien mithilfe der Konsistenzgruppenbeziehung in den Ziel-Cluster verwenden.

Über diese Aufgabe

Um Snapshot Kopien mit Volume-Granularität zu replizieren, muss ONTAP 9.14.1 oder höher ausgeführt werden. Bei MirrorAndVault- und Vault-Richtlinien muss das SnapMirror-Label der Snapshot-Richtlinie mit Volume-Granularität mit der SnapMirror-Richtlinienregel der Konsistenzgruppe übereinstimmen. Snapshots mit Volume-Granularität behalten den behalten-Wert der SnapMirror Richtlinie der Konsistenzgruppe bei, die unabhängig von den Snapshots der Konsistenzgruppe berechnet wird. Wenn Sie zum Beispiel die Richtlinie haben, zwei Snapshot Kopien auf dem Ziel zu behalten, können Sie über zwei Volume-granulare Snapshot Kopien und zwei Snapshot Kopien der Konsistenzgruppe verfügen.

Beim erneuten Synchronisieren der SnapMirror Beziehung mit Snapshot Kopien mit Volume-Granularität können Sie Snapshot Kopien mit der auf Volume-Ebene beibehalten `-preserve` Flagge. Snapshot Kopien mit Volume-Granularität, die neuer sind als Snapshot Kopien von Konsistenzgruppen, werden aufbewahrt. Wenn keine Snapshot-Kopie einer Konsistenzgruppe vorhanden ist, können während der Neusynchronisierung keine Snapshot-Kopien mit Volume-Granularität übertragen werden.

Bevor Sie beginnen

- Der asynchrone SnapMirror Schutz ist nur für einzelne Konsistenzgruppen 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.
- Unterbrechungsfrei Fügen Sie einer Konsistenzgruppe Volumes hinzu Mit einer aktiven asynchronen SnapMirror Beziehung. Bei allen anderen Änderungen an einer Konsistenzgruppe müssen Sie die SnapMirror Beziehung unterbrechen, die Konsistenzgruppe ändern, dann die Beziehung wiederherstellen und neu synchronisieren.
- Wenn Sie eine asynchrone SnapMirror-Sicherungsbeziehung für mehrere einzelne Volumes konfiguriert haben, können Sie diese Volumes in eine Konsistenzgruppe konvertieren, während die vorhandenen Snapshot Kopien beibehalten werden. So konvertieren Sie Volumes erfolgreich:
  - Es muss eine allgemeine Snapshot-Kopie der Volumes vorhanden sein.
  - Sie müssen die bestehende SnapMirror-Beziehung trennen, Fügen Sie die Volumes einer einzelnen Konsistenzgruppe hinzu, Und synchronisieren Sie die Beziehung anschließend mithilfe des folgenden Workflows erneut.

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 angezeigt `Protected` Neben .

SVM-Disaster Recovery konfigurieren

Ab ONTAP 9.14.1 Disaster Recovery für SVM Unterstützt Konsistenzgruppen, wodurch Sie Informationen zu Konsistenzgruppen von der Quelle auf das Ziel-Cluster spiegeln können.

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 im 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.
- Die 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 Snapshot Kopien"

- "Erstellen benutzerdefinierter Datensicherungsrichtlinien"
- "Wiederherstellung aus Snapshot-Kopien"
- "Wiederherstellung eines Volume aus einer früheren Snapshot Kopie"
- "SM-BC – Übersicht"
- "Dokumentation zur ONTAP-Automatisierung"
- Grundlagen der asynchronen SnapMirror Disaster Recovery

Ändern Sie Mitglieds-Volumes in einer 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 sich die Anpassungen insgesamt befinden Einschränkungen für Konsistenzgruppen.
- Ab ONTAP 9.13.1 können Sie einer Konsistenzgruppe mit einer aktiven SnapMirror Business Continuity (SM-BC) oder einer asynchronen SnapMirror Sicherungsrichtlinie Volumes unterbrechungsfrei hinzufügen.
- Wenn Sie Volumes zu einer durch SM-BC geschützten Konsistenzgruppe hinzufügen, ändert sich der Status der SM-BC-Beziehung 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 früheren Versionen können Sie Volumes nicht zu einer Konsistenzgruppe in einer SM-BC-Beziehung hinzufügen. Sie müssen zuerst die SM-BC-Beziehung unterbrechen, die Konsistenzgruppe ändern und dann den Schutz mit SM-BC 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.

- Wenn Sie eine Konsistenzgruppe erweitern, werden Snapshot Kopien der vor der Änderung erfassten Konsistenzgruppe als Teil betrachtet. Bei jedem auf dieser Snapshot Kopie basierenden Wiederherstellungsvorgang 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 asynchronem

SnapMirror in das Ziel-Cluster replizieren. Bei der Erweiterung einer Konsistenzgruppe mit Asynchronous SnapMirror werden Volume-granulare Snapshots erst nach Erweiterung der Konsistenzgruppe 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 nach dem erweitern der Konsistenzgruppe die SVM-Disaster-Recovery-Beziehung vom Ziel-Cluster aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Sie eine Replikationsbeziehung manuell.

Beispiel 1. 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. Wählen Sie die Schaltfläche **>** aus, um die untergeordneten Konsistenzgruppen anzuzeigen, und wählen Sie dann aus ⋮ Neben dem Namen der untergeordneten Konsistenzgruppe, 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.

Fügen Sie vorhandene Volumes hinzu

1. Geben Sie den folgenden Befehl ein. Der `-volumes` Der Parameter akzeptiert eine durch Kommas getrennte Liste von Volumes.

   > Schließen Sie nur die ein `-parent-consistency-group` Parameter, 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.

> Schließen Sie nur die ein `-parent-consistency-group` Parameter, wenn die Konsistenzgruppe sich in einer hierarchischen Beziehung befindet.

- 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 SM-BC- oder SVM-Disaster-Recovery-Beziehung entfernen. Sie müssen zuerst die SM-BC-Beziehung unterbrechen, um die Konsistenzgruppe zu ändern und dann die Beziehung wiederherzustellen.
- 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 bleiben 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 zur 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 Snapshot-Kopien der Konsistenzgruppe ungültig werden und wählen Sie **Entfernen** aus.

CLI

Ab ONTAP 9.14.1 können Sie Volumes mithilfe der CLI aus einer Konsistenzgruppe entfernen.

Schritt

1. Entfernen Sie die Volumes. Der `-volumes` Der Parameter akzeptiert eine durch Kommas getrennte Liste von Volumes.

   Schließen Sie nur die ein `-parent-consistency-group` Parameter, 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.
- Snapshot Kopien der übergeordneten Konsistenzgruppe bleiben gültig.
- Wenn Sie alle Volumes aus einer untergeordneten Konsistenzgruppe verschieben, wird diese Konsistenzgruppe gelöscht.
- Änderungen an einer Konsistenzgruppe müssen eingehalten werden Einschränkungen 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.

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` Der Parameter akzeptiert eine kommagetrennte 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 Geometrie der Konsistenzgruppe

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 Snapshot Kopien.

> 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.

Bevor Sie beginnen

- Eine übergeordnete Konsistenzgruppe kann maximal fünf untergeordnete Konsistenzgruppen enthalten. Siehe Einschränkungen für Konsistenzgruppen Für andere Grenzwerte.
- Sie können einer einzelnen Konsistenzgruppe keine untergeordnete Konsistenzgruppe hinzufügen. Zunächst müssen Sie [Werben] Die Konsistenzgruppe, dann können Sie eine untergeordnete Konsistenzgruppe hinzufügen.
- Vorhandene Snapshot Kopien der vor der Erweiterung erfassten Konsistenzgruppe gelten als Teil. Bei jedem auf dieser Snapshot Kopie basierenden Wiederherstellungsvorgang wird die Konsistenzgruppe zum Zeitpunkt der Snapshot Kopie wiedergegeben.

Beispiel 2. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

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.

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` Der Parameter akzeptiert eine kommagetrennte 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.

Bevor Sie beginnen

- Das Trennen einer untergeordneten Konsistenzgruppe führt dazu, dass die Snapshots der übergeordneten Konsistenzgruppe ungültig werden und auf sie nicht mehr zugegriffen werden kann. Granulare Volume-Snapshots sind weiterhin gültig.

- Vorhandene Snapshot Kopien 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 3. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

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.

1. Entfernen Sie die Konsistenzgruppe. Benennen Sie optional die getrennte Konsistenzgruppe mit dem um `-new-name` Parameter.

   ```
   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.

Bevor Sie beginnen

- Die übergeordnete Konsistenzgruppe muss vier oder weniger untergeordnete Elemente aufweisen. Eine übergeordnete Konsistenzgruppe kann maximal fünf untergeordnete Konsistenzgruppen enthalten. Siehe Einschränkungen für Konsistenzgruppen Für andere Grenzwerte.
- Vorhandene Snapshot-Kopien der vor diesem Vorgang erfassten *parent* Konsistenzgruppe gelten als teilweise. Bei jedem Wiederherstellungsvorgang, der auf einer dieser Snapshot Kopien basiert, wird die Konsistenzgruppe zum Zeitpunkt der Snapshot Kopie wiedergegeben.
- Vorhandene Snapshots der Konsistenzgruppe bleiben gültig.

Beispiel 4. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

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.

Verschieben Sie eine Konsistenzgruppe unter eine neue übergeordnete Konsistenzgruppe

1. Erstellen Sie die neue übergeordnete Konsistenzgruppe. Der `-consistency-groups` Mit dem 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.

Bevor Sie beginnen

- Wenn Sie eine untergeordnete Konsistenzgruppe in eine übergeordnete Konsistenzgruppe konvertieren möchten, müssen Sie zuerst [detach] Die untergeordnete Konsistenzgruppe führt dann dieses Verfahren aus.

- Vorhandene Snapshot Kopien der Konsistenzgruppe bleiben gültig, nachdem Sie die Konsistenzgruppe hochgestuft haben.

Beispiel 5. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

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.

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.

Bevor Sie beginnen

- Vorhandene Snapshot Kopien der übergeordneten Konsistenzgruppe bleiben gültig, nachdem Sie sie auf eine einzelne Konsistenz herabgestuft haben. Vorhandene Snapshot Kopien von einer der zugeordneten untergeordneten Konsistenzgruppen des übergeordneten Objekts werden ungültig, die einzelnen Volume-Snapshots in diesen Snapshots sind jedoch weiterhin als Volume-granulare Snapshots verfügbar.

Beispiel 6. Schritte

System Manager

Ab ONTAP 9.13.1 können Sie diesen Vorgang mit System Manager ausführen.

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.

1. Stufen Sie die Konsistenzgruppe zurück. Verwenden Sie das optionale `-new-name` Parameter, um die Konsistenzgruppe umzubenennen.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Anwendungs- und Komponenten-Tags ändern

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 Consistency Group eine SM-BC-Beziehung hat, müssen Sie **other** 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 die aus ⋮ Neben dem Namen der Konsistenzgruppe und dann **Edit**.
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.

Ändern Sie das Anwendungs-Tag

1. Anwendungs-Tags akzeptieren eine begrenzte Anzahl voreingestellter Zeichenfolgen. Um die Liste der akzeptierten Zeichenfolgen anzuzeigen, führen Sie den folgenden Befehl aus:
   `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 SM-BC verwenden, muss es „anders“ 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 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 ihrer aktuellen Konfiguration klonen, jedoch mit Volume-Inhalten, wenn sie sich befinden oder auf einem vorhandenen Snapshot einer Konsistenzgruppe basieren.

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 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.

  Siehe Zuordnen von Initiatorgruppen zu mehreren LUNs Oder Zuordnen eines NVMe Namespace zu einem Subsystem Finden Sie weitere Informationen.

- Das Klonen einer Konsistenzgruppe wird weder für eine Konsistenzgruppe in einer SnapMirror Business Continuity-Beziehung noch für zugehörige DP Volumes 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 aus, ob Sie die Option 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 Status zu klonen, wählen Sie **Neue Snapshot Kopie hinzufügen**.

   Um die Konsistenzgruppe auf der Grundlage eines Snapshots zu klonen, wählen Sie **Verwenden Sie eine vorhandene Snapshot Kopie**. Wenn Sie diese Option auswählen, wird ein neues Untermenü geöffnet. Wählen Sie den Snapshot aus, den Sie als Grundlage 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 über die CLI klonen.

Klonen einer Konsistenzgruppe

1. Der `consistency-group clone create` Der Befehl klont die Konsistenzgruppe im aktuellen Point-in-Time-Status. Um den Klonvorgang auf einem Snapshot zu basieren, schließen Sie das ein `-source-snapshot` Parameter.

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

Nächste Schritte

- Zuordnen von Initiatorgruppen zu mehreren LUNs
- Zuordnen eines NVMe Namespace zu einem Subsystem

Löschen einer 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 Snapshots, die auf jedem Volume vorhanden sind, jedoch sind sie nicht mehr als Snapshots von Konsistenzgruppen verfügbar. Die Snapshots können jedoch weiterhin als normale granulare Snapshots von Volumes 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 Prozess 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 aus ⋮ Dann **Löschen**.

CLI

Ab ONTAP 9.14.1 können Sie eine Konsistenzgruppe über die CLI löschen.

Löschen einer Konsistenzgruppe

1. Löschen Sie die Konsistenzgruppe:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror Business Continuity

Überblick über die Business Continuity in SnapMirror

SnapMirror Business Continuity (SM-BC), auch als SnapMirror Active Sync bekannt, ermöglicht es Business-Services, den Betrieb selbst bei einem vollständigen Standortausfall fortzusetzen. Applikationen können dank einer sekundären Kopie einen transparenten Failover durchführen. Zum Auslösen eines Failovers mit SM-BC sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich.

SM-BC ist ab ONTAP 9.8 verfügbar. SM-BC wird auf AFF Clustern oder All-Flash SAN Array (ASA) Clustern unterstützt, bei denen die primären und sekundären Cluster entweder AFF oder ASA sein können. SM-BC sichert Applikationen mit iSCSI oder FCP LUNs.

Vorteile

SM-BC bietet folgende Vorteile:

- Kontinuierliche Verfügbarkeit für geschäftskritische Applikationen

- Möglichkeit zum abwechselnd Hosten kritischer Applikationen vom primären und sekundären Standort aus
- Vereinfachtes Applikationsmanagement mit Konsistenzgruppen für abhängige Schreibreihenfolge
- Die Möglichkeit, für jede Applikation ein Failover zu testen
- Sofortige Erstellung von Spiegelklonen, ohne die Applikationsverfügbarkeit zu beeinträchtigen
- Ab ONTAP 9.11.1 unterstützt SM-BC SnapRestore mit einer Datei.
- Ab ONTAP 9.14.1 unterstützt SM-BC Windows-Failover-Clustering und "Persistente SCSI 3-Reservierungen", Verbesserung der Hochverfügbarkeit.

Anwendungsfälle

Applikationsimplementierung für Objekt mit null Recovery-Zeit (RTO)

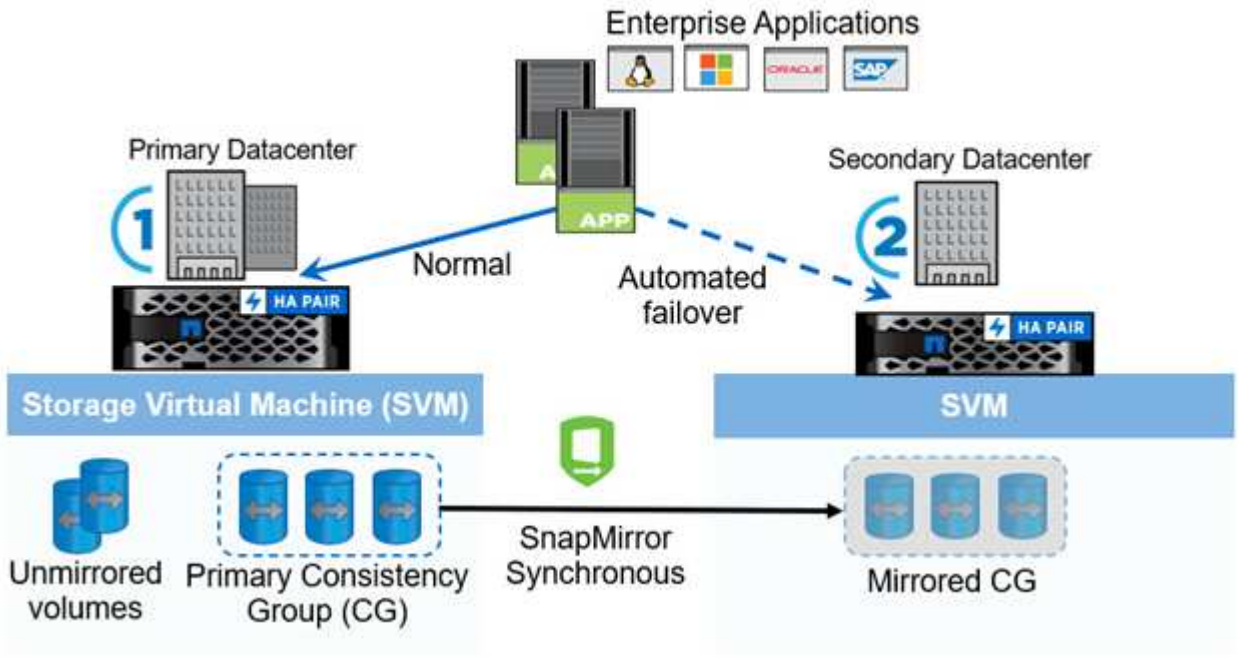
In einer SM-BC-Bereitstellung verfügen Sie über ein primäres und ein sekundäres Cluster. Eine LUN im primären Cluster `1LP`) Wird einen Spiegel haben (`L1s`) Auf der sekundären; beide LUNs teilen sich dieselbe serielle ID und werden als Lese-Schreib-LUNs an den Host gemeldet. Lese- und Schreibvorgänge werden jedoch nur auf der primären LUN gewartet. `1LP`. Alle Schreibvorgänge auf die Spiegelung `L1S` Werden von Proxy bedient.

Notfallszenario

Mit SM-BC können Sie mehrere Volumes synchron für eine Applikation zwischen Standorten an geografisch verteilten Standorten replizieren. Bei Unterbrechungen des primären Storage kann automatisch ein Failover auf die sekundäre Kopie durchgeführt werden. Dies ermöglicht Business Continuity für Tier-1-Applikationen.

Der Netapp Architektur Sind

Die folgende Abbildung zeigt den Betrieb der SnapMirror Business Continuity-Funktion auf hoher Ebene.



In Abschnitt 1 des Diagramms wird eine Applikation auf einer SVM im primären Datacenter implementiert. Die Volumes, die zur primären Konsistenzgruppe hinzugefügt wurden, sind mit SM-BC geschützt und werden auf die sekundäre Konsistenzgruppe in einem sekundären Rechenzentrum gespiegelt. Bei einer Unterbrechung erfolgt ein Failover der Volumes in der primären Konsistenzgruppe auf die gespiegelte Konsistenzgruppe.

Volumes, die sich nicht in einer gespiegelten Konsistenzgruppe befinden, werden im Falle eines Failovers nicht bedient.

Weitere Informationen

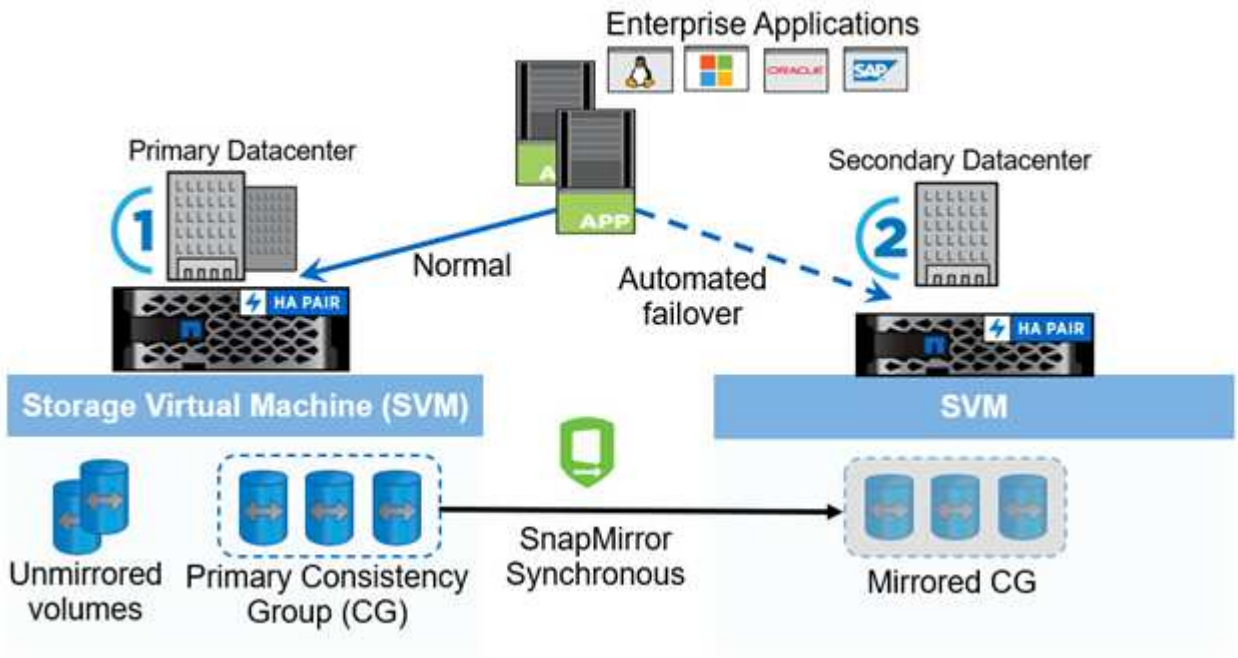
- "TR-4878: SnapMirror Business Continuity"

Schlüsselkonzepte

SnapMirror Business Continuity (SM-BC) nutzt Funktionen wie Konsistenzgruppen und den ONTAP Mediator, um sicherzustellen, dass Ihre Daten repliziert und auch im Notfall bereitgestellt werden. Bei der Planung Ihrer SM-BC-Implementierung ist es wichtig, die wesentlichen Konzepte in SM-BC und seiner Architektur zu verstehen.

Der Netapp Architektur Sind

Die folgende Abbildung zeigt eine allgemeine Übersicht über eine SM-BC-Bereitstellung.



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 Katastrophenfalls im primären Rechenzentrum leitet der ONTAP-Mediator das sekundäre Rechenzentrum als primäres Rechenzentrum an, das alle I/O-Operationen bedient. Es werden nur die Volumes bedient, die in der Konsistenzgruppe gespiegelt werden. Alle Vorgänge, die die anderen beiden Volumes auf der SVM betreffen, sind durch den Notfall betroffen.

Grundlegende Konzepte

Das Verständnis der folgenden Begriffe hilft Ihnen bei der Bereitstellung von SM-BC.

Konsistenzgruppe

Eine Konsistenzgruppe ist eine Sammlung von Volumes oder LUNs, die eine Garantie der Schreibreihenfolge für den Applikations-Workload bietet, der für Business Continuity gesichert werden muss. Eine Konsistenzgruppe stellt sicher, dass alle Volumes dieses Datensatzes stillgelegt und dann zum selben Zeitpunkt wieder eingesetzt werden. Dadurch wird ein datenkonsistenter Restore-Punkt über die Volumes hinweg für diesen Datensatz bereitgestellt.

In SM-BC erstellen Sie eine primäre und sekundäre Konsistenzgruppe für Replikation und Datenschutz. Die sekundäre Konsistenzgruppe stellt Ihre Daten im Falle einer Unterbrechung bereit.

Weitere Informationen zu Konsistenzgruppen finden Sie unter "Übersicht über Konsistenzgruppen".

Konstitutive

Ein einzelnes Volume oder LUN, die Teil einer Konsistenzgruppe ist, die durch die SM-BC-Beziehung geschützt ist.

ONTAP Mediator

Die ONTAP Mediatoren überwachen die beiden ONTAP-Cluster und orchestrieren das Failover für den Fall, dass Ihr primäres Speichersystem ausfällt. Mit dem ONTAP Mediator stellt Ihre Anwendung automatisch wieder eine Verbindung zu den Ressourcen im sekundären Speichersystem her.

Durch die Integritätsinformationen des ONTAP Mediators können Cluster zwischen einem Cluster-LIF-Ausfall und einem Standortausfall unterscheiden. Wenn der Standort ausfällt, leitet ONTAP Mediator die Integritätsinformationen bei Bedarf an den Peer-Cluster weiter, wodurch der Peer-Cluster ein Failover ermöglicht wird.

Erfahren Sie mehr über das "ONTAP Mediator".

Geplantes Failover

Ein manueller Vorgang zum Ändern der Rollen von Kopien in einer SM-BC-Beziehung. 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 von Mediator, um zu erkennen, dass die primäre Kopie nicht verfügbar ist.

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 Spiegelungsstatus lautet `Snapmirrored`Dies zeigt einen Übertragungsfehler oder einen Fehler aufgrund eines nicht unterstützten Vorgangs an.

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 als akzeptabel erachtet. Kein RTO bedeutet, dass keine Ausfallzeiten akzeptabel sind.

Planen

Voraussetzungen

Stellen Sie bei der Planung Ihrer SnapMirror Business Continuity-Implementierung sicher, dass Sie die verschiedenen Anforderungen an Hardware, Software und Systemkonfiguration erfüllt haben.

Trennt

- Es werden nur HA-Cluster mit zwei Nodes unterstützt
- Beide Cluster müssen entweder AFF (einschließlich AFF C-Serie) oder ASA (keine Mischung) sein.

Software

- ONTAP 9.8 oder höher
- ONTAP Mediator 1.2 oder höher
- Ein Linux-Server oder eine virtuelle Maschine für den ONTAP Mediator, auf dem einer der folgenden Komponenten ausgeführt wird:

Version des ONTAP Mediators	Unterstützte Linux-Versionen
1.7	• Red Hat Enterprise Linux: 8.5, 8.6, 8.7, 8.8, 8.9 9.0, 9.1, 9.2 und 9.3 • Rocky Linux 8 und 9
1.6	• Red Hat Enterprise Linux: 8.4, 8.5, 8.6, 8.7, 8.8 9.0, 9.1, 9.2 • Rocky Linux 8 und 9
1.5	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.4	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.3	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1.2	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

Lizenzierung

- Die SnapMirror Synchronous-Lizenz (SM-S) muss auf beiden Clustern angewendet werden
- SnapMirror Lizenz muss auf beiden Clustern angewendet werden

> Wenn Sie Ihre ONTAP Storage-Systeme vor Juni 2019 gekauft haben, finden Sie unter "Master-Lizenzschlüssel für NetApp ONTAP" Um die erforderliche SM-S Lizenz zu erhalten.

Die Lizenz für SnapMirror Synchronous und SnapMirror ist enthalten "ONTAP One".

Netzwerkumgebung

- Die Latenzzeit zwischen den Clustern muss weniger als 10 Millisekunden betragen.
- SCSI-3 persistente Reservierungen werden **nicht** mit SM-BC unterstützt.

Unterstützte Protokolle

- Nur SAN-Protokolle werden unterstützt (nicht NFS/SMB).
- Es werden nur die Protokolle Fibre Channel und iSCSI unterstützt.
- SM-BC benötigt den standardmäßigen IPspace für Cluster-Peer-Beziehungen. Benutzerdefinierter IPspace wird nicht unterstützt.

NTFS-Sicherheitsstil

NTFS Sicherheitsstil wird auf SM-BC-Volumes **nicht** unterstützt.

ONTAP Mediator

- Der ONTAP Mediator wird extern bereitgestellt und an ONTAP für transparentes Applikations-Failover angeschlossen.
- Um vollständig funktionsfähig zu sein und ein automatisches ungeplantes Failover zu ermöglichen, muss der externe ONTAP Mediator mit ONTAP Clustern bereitgestellt und konfiguriert werden.
- Der ONTAP-Mediator muss in einer dritten Fehlerdomäne, getrennt von den beiden ONTAP-Clustern, installiert werden.
- Bei der Installation des ONTAP Mediators sollten Sie das selbstsignierte Zertifikat durch ein gültiges Zertifikat ersetzen, das von einer zuverlässigen Standardzertifizierungsstelle signiert wurde.
- Weitere Informationen zum ONTAP Mediator finden Sie unter "Bereiten Sie die Installation des ONTAP Mediator-Dienstes vor".

Read-Write Ziel-Volumen

- SM-BC-Beziehungen werden auf Lese- und Schreib-Zielvolumen nicht unterstützt. Bevor Sie ein Lese- und Schreib-Volume verwenden können, müssen Sie es in ein DP-Volume konvertieren, indem Sie eine SnapMirror Beziehung auf Volume-Ebene erstellen und dann die Beziehung löschen. Weitere Informationen finden Sie unter "Bestehende Beziehungen in SM-BC-Beziehungen umwandeln"

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

- Für ONTAP 9.12.1 P2 und höher unterstützt SMBC große LUNs und große Volumes von mehr als 100 TB auf ASA und AFF (einschließlich C-Serie).

> 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 oder rein Flash-basierte Arrays 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 9.8 - 9.12.1P1

- Für ONTAP-Versionen zwischen ONTAP 9.8 und 9.12.1 P1 (inklusive) werden große LUNs und große Volumen über 100 TB nur auf rein Flash-basierten SAN-Arrays unterstützt.

> Bei ONTAP-Versionen zwischen ONTAP 9.8 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 9.8 oder höher installiert ist. Wenn auf dem sekundären Cluster eine ältere Version als ONTAP 9.8 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

- "Hardware Universe"
- "ONTAP Mediator Übersicht"

Unterstützte Konfigurationen und Funktionen

SnapMirror Business Continuity ist mit zahlreichen Betriebssystemen und Funktionen der ONTAP kompatibel. Hier finden Sie Details und empfohlene Konfigurationen.

Unterstützte Konfigurationen

SM-BC wird von zahlreichen Betriebssystemen unterstützt, darunter:

- AIX (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 SM-BC unterstützt. Mit einer AIX-Konfiguration ist der primäre Cluster der „aktive“ Cluster.

In einer AIX-Konfiguration ist ein Failover mit Unterbrechungen verbunden. Bei jedem Failover müssen Sie einen Re-Scan am Host durchführen, um I/O-Vorgänge wiederaufzunehmen.

Informationen zur Konfiguration für AIX-Host mit SM-BC finden Sie im Knowledge Base-Artikel "So konfigurieren Sie einen AIX Host für SnapMirror Business Continuity (SM-BC)".

HP-UX ERHÄLTLICH

Ab ONTAP 9.10.1 wird SM-BC für HP-UX unterstützt.

Einschränkungen bei HP-UX

Ein Ereignis für einen automatischen ungeplanten Failover (AUFO) auf dem isolierten Master-Cluster kann durch einen Dual-Event-Fehler verursacht werden, wenn die Verbindung zwischen dem primären und dem sekundären Cluster unterbrochen wird und auch die Verbindung zwischen dem primären Cluster und dem Mediator unterbrochen wird. Dies gilt im Gegensatz zu anderen AUFO-Ereignissen als ein 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.

Empfehlung für die Solaris Host-Einstellung

Ab ONTAP 9.10.1 unterstützt SM-BC Solaris 11.4.

Um sicherzustellen, dass die Solaris-Clientanwendungen bei einer ungeplanten Standortausfallumschaltung in einer SM-BC-Umgebung unterbrechungsfrei ausgeführt werden, ändern Sie die standardmäßigen Solaris-Betriebssystemeinstellungen. Informationen zum Konfigurieren von Solaris mit den empfohlenen Einstellungen finden Sie im Knowledge Base-Artikel "Solaris Host Support Empfohlene Einstellungen in SnapMirror Business Continuity (SM-BC)-Konfiguration".

Windows-Failover-Clustering

Ab ONTAP 9.14.1 wird Windows-Failover-Clustering mit SM-BC unterstützt. Weitere Informationen finden Sie unter "TR-4878: SnapMirror Business Continuity".

ONTAP Integrationen

SM-BC unterstützt weitere Funktionen von ONTAP, darunter:

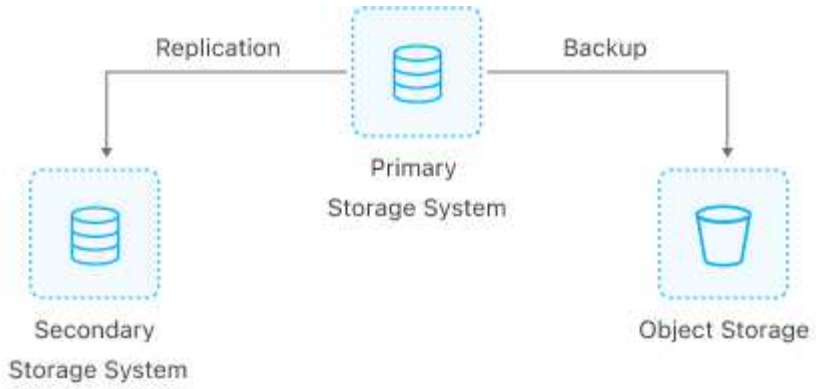
- Fan-out-Konfigurationen
- NDMP Kopie (ab ONTAP 9.13.1)
- Partieller File Restore (ab ONTAP 9.12.1)

FabricPool

SM-BC unterstützt Quell- und Ziel-Volumes auf FabricPool-Aggregaten mit der Tiering-Richtlinie „Keine“, „Snapshot“ oder „automatisch“. SM-S SM-BC unterstützt keine FabricPool-Aggregate mit einer Tiering Policy von allen.

Fan-out-Konfigurationen

In A Fan-out-Konfigurationen, Ihr Quell-Volume kann zu einem SM-BC Ziel-Endpunkt und zu einer oder mehreren asynchronen SnapMirror Beziehungen gespiegelt werden.



SM-BC unterstützt Fan-out-Konfigurationen Mit dem `MirrorAllSnapshots` Richtlinie und ab ONTAP 9.11.1 `MirrorAndVault` Richtlinie: Fan-out-Konfigurationen werden in SM-BC auf nicht unterstützt `XDPDefault` Richtlinie:

Wenn Sie ein Failover auf dem SM-BC-Ziel in einer Fan-out-Konfiguration erleben, müssen Sie dies manuell tun Setzen Sie den Schutz in der Fan-out-Konfiguration fort.

NDMP-Wiederherstellung

Ab ONTAP 9.13.1 können Sie NDMP verwenden, um Daten mit SM-BC zu kopieren und wiederherzustellen. Mithilfe von NDMP können Sie Daten auf die SM-BC Quelle verschieben, um eine Wiederherstellung durchzuführen, ohne den Schutz anzuhalten. Dies ist insbesondere bei Fan-out-Konfigurationen von Vorteil.

Weitere Informationen zu diesem Prozess finden Sie unter Datenübertragung mithilfe einer ndmp-Kopie.

Partielle Dateiwiederherstellung

Ab ONTAP 9.12.1 wird für SM-BC Volumes eine partielle LUN-Wiederherstellung unterstützt. Weitere Informationen zu diesem Prozess finden Sie unter "Wiederherstellen eines Teils einer Datei aus einer Snapshot Kopie".

Objektbeschränkungen für SnapMirror Business Continuity

Beachten Sie bei der Vorbereitung der Verwendung und Verwaltung von SnapMirror Business Continuity die folgenden Einschränkungen.

Konsistenzgruppen in einem Cluster

Die Einschränkungen der Konsistenzgruppen für ein Cluster mit SM-BC werden auf Basis von Beziehungen berechnet und hängen von der verwendeten ONTAP Version ab. Einschränkungen sind plattformunabhängig.

ONTAP-Version	Maximale Anzahl von Beziehungen
ONTAP 9.8-9.9.1	5
ONTAP 9.10.1	20
ONTAP 9.11.1 und höher	50

Volumes pro Konsistenzgruppe

Die maximale Anzahl von Volumes pro Konsistenzgruppe mit SM-BC ist plattformunabhängig.

ONTAP-Version	Maximale Anzahl von Volumes, die in einer Konsistenzgruppenbeziehung unterstützt werden
ONTAP 9.8-9.9.1	12
ONTAP 9.10.1 und höher	16

Volumes

Volumengrenzen in SM-BC werden auf der Grundlage der Anzahl der Endpunkte berechnet, nicht anhand der Anzahl der Beziehungen. Eine Konsistenzgruppe mit 12 Volumes steuert 12 Endpunkte auf dem primären und dem sekundären Cluster bei. Sowohl SM-BC als auch SnapMirror Synchronous Beziehungen tragen zur Gesamtzahl der Endpunkte bei.

Die maximale Anzahl der Endpunkte pro Plattform ist in der folgenden Tabelle enthalten.

S. Nein	Plattform	Endpunkte pro HA für SM-BC			Sync insgesamt und SM-BC Endpunkte pro HA		
		ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 und höher	ONTAP 9.8-9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 und höher
1	AFF	60	200	400	80	200	400
2	ASA	60	200	400	80	200	400

SAN-Objektbeschränkungen

Die EINSCHRÄNKUNGEN FÜR SAN-Objekte sind in der folgenden Tabelle enthalten. Die Grenzen gelten unabhängig von der Plattform.

Objekt in einer SM-BC-Beziehung	Zählen
LUNs pro Volume	256
LUN-Zuordnungen pro Node	• 4096 (ONTAP 9.10 und höher) • 2048 (ONTAP 9.9.1 und früher)
LUN-Zuordnungen pro Cluster	• 8192 (ONTAP 9.10 und höher) • 4096 (ONTAP 9.9.1 und früher)
LIFs pro SVM (mit mindestens einem Volume in einer SM-BC-Beziehung)	256
Inter-Cluster-LIFs pro Node	4
Inter-Cluster LIFs pro Cluster	8

Verwandte Informationen

- "Hardware Universe"
- "Einschränkungen für Konsistenzgruppen"

Installieren und einrichten

ONTAP Mediator und Cluster für SnapMirror Business Continuity konfigurieren

SnapMirror Business Continuity (SM-BC) nutzt Peering-Cluster, damit Ihre Daten im Fall eines Failover-Szenarios verfügbar sind. Der ONTAP Mediator ist eine wichtige Ressource, die Business Continuity gewährleistet und den Zustand jedes Clusters überwacht. Um SM-BC zu konfigurieren, müssen Sie zuerst den ONTAP Mediator installieren und sicherstellen, dass die primären und sekundären Cluster ordnungsgemäß konfiguriert sind.

Nachdem Sie den ONTAP Mediator installiert und die Cluster konfiguriert haben, müssen Sie dies tun [initialize-the-ontap-mediator] Der ONTAP Mediator für die Verwendung mit SM-BC. Dann müssen Sie Erstellen, initialisieren und zuordnen der Konsistenzgruppe für SM-BC

ONTAP Mediator

Der ONTAP Mediator stellt ein Quorum für die ONTAP Cluster in einer SM-BC Beziehung her. Es koordiniert das automatische Failover bei einem erkannten Ausfall, ermittelt, welches Cluster als primäres Cluster fungiert und stellt sicher, dass die Daten zum und vom korrekten Ziel bereitgestellt werden.

Voraussetzungen für den ONTAP Mediator

- Der ONTAP Mediator enthält eigene Voraussetzungen. Sie müssen diese Voraussetzungen erfüllen, bevor Sie den Mediator installieren.

  Weitere Informationen finden Sie unter "Bereiten Sie die Installation des ONTAP Mediator-Dienstes vor".

- Standardmäßig stellt der ONTAP Mediator den Dienst über TCP-Port 31784 bereit. Sie sollten sicherstellen, dass Port 31784 zwischen den ONTAP-Clustern und dem Mediator geöffnet und verfügbar ist.

Installieren Sie den ONTAP Mediator und bestätigen Sie die Clusterkonfiguration

Gehen Sie die folgenden Schritte durch. Bei jedem Schritt sollten Sie bestätigen, dass die spezifische Konfiguration durchgeführt wurde. Nutzen Sie den Link nach jedem Schritt, um weitere Informationen zu erhalten.

Schritte

1. Installieren Sie den ONTAP Mediator-Dienst, bevor Sie sicherstellen, dass Ihre Quell- und Zielcluster ordnungsgemäß konfiguriert sind.

   Bereiten Sie die Installation oder das Upgrade des ONTAP Mediatordienstes vor

2. Bestätigen Sie, dass zwischen den Clustern eine Cluster-Peering-Beziehung besteht.

   > SM-BC benötigt den standardmäßigen IPspace für Cluster-Peer-Beziehungen. Ein benutzerdefinierter IP-Bereich wird nicht unterstützt.

   Konfiguration von Peer-Beziehungen

3. Vergewissern Sie sich, dass die Storage VMs auf jedem Cluster erstellt werden.

   Erstellen einer SVM

4. Vergewissern Sie sich, dass zwischen den Storage-VMs auf jedem Cluster eine Peer-Beziehung besteht.

   Erstellen einer SVM-Peering-Beziehung

5. Vergewissern Sie sich, dass die Volumes für Ihre LUNs vorhanden sind.

   Erstellen eines Volumes

6. Vergewissern Sie sich, dass auf jedem Node im Cluster mindestens eine SAN-LIF erstellt wurde.

   "Überlegungen zu LIFs in einer Cluster-SAN-Umgebung"

   "Erstellen eines LIF"

7. Vergewissern Sie sich, dass die erforderlichen LUNs erstellt und einer Initiatorgruppe zugeordnet sind, die zum Zuordnen von LUNs zum Initiator auf dem Applikations-Host verwendet wird.

   LUNs erstellen und Initiatorgruppen zuordnen

8. Prüfen Sie den Applikations-Host erneut, um neue LUNs zu erkennen.

Initialisieren Sie den ONTAP Mediator für SM-BC

Nachdem Sie den ONTAP Mediator installiert und die Clusterkonfiguration bestätigt haben, müssen Sie den ONTAP Mediator für die Clusterüberwachung initialisieren. Sie können den ONTAP Mediator mit System Manager oder der ONTAP CLI initialisieren.

System Manager

Mit System Manager können Sie den ONTAP Mediator Server für automatisches 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.

Schritte

1. Navigieren Sie zu **Schutz > Übersicht > Mediator > Konfigurieren**.
2. Wählen Sie **Hinzufügen**, und geben Sie die folgenden ONTAP Mediatorserver-Informationen ein:
   - IPv4-Adresse
   - Benutzername
   - Passwort
   - Zertifikat

CLI

Sie können den ONTAP Mediator entweder vom primären oder sekundären Cluster mithilfe der ONTAP CLI initialisieren. Wenn Sie das ausgeben `mediator add` Befehl auf einem Cluster wird der ONTAP Mediator automatisch auf dem anderen Cluster hinzugefügt.

Schritte

1. Mediator auf einem der Cluster initialisieren:

   ```
   snapmirror mediator add -mediator-address IP_Address -peer-cluster
   cluster_name -username user_name
   ```

   Beispiel

   ```
   cluster1::> snapmirror mediator add -mediator-address 192.168.10.1
   -peer-cluster cluster2 -username mediatoradmin
   Notice: Enter the mediator password.

   Enter the password: ******
   Enter the password again: ******
   ```

2. Überprüfen Sie den Status der Mediator-Konfiguration:

   ```
   snapmirror mediator show
   ```

   ```
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   192.168.10.1     cluster-2        connected         true
   ```

   `Quorum Status` Gibt an, ob die Beziehungen der SnapMirror Konsistenzgruppe mit dem Mediator synchronisiert sind; einen Status von `true` Zeigt eine erfolgreiche Synchronisierung an.

Sicherung mit SnapMirror Business Continuity

Bei der Konfiguration der Sicherung mit SnapMirror Business Continuity werden LUNs auf dem ONTAP Quell-Cluster ausgewählt und einer Konsistenzgruppe hinzugefügt.

Bevor Sie beginnen

- Sie müssen eine haben "SnapMirror Synchronous Lizenz".
- 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 SM-BC-Beziehungen zu Konsistenzgruppen über ASA-Cluster und nicht-ASA-Cluster hinweg aufbauen.
- SM-BC benötigt den standardmäßigen IPspace für Cluster-Peer-Beziehungen. 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 Endpunkt und ein Menü für Konsistenzgruppen in System Manager, das zusätzliche Management Utilities bietet. Wenn Sie ONTAP 9.10.1 oder höher verwenden, finden Sie weitere Informationen unter "Konfigurieren einer Konsistenzgruppe" Dann "Schutz konfigurieren" Um eine SM-BC-Beziehung zu erstellen.

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 können Sie bis zu 12 zusammengehörige Volumes zuordnen `cg-item-mappings` Parameter auf dem `snapmirror create` Befehl.

   Im folgenden Beispiel werden zwei Konsistenzgruppen erstellt: `cg_src_ on the source with` `vol1` Und `vol2` Und einer gespiegelten Ziel-Konsistenzgruppe, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

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*`
5. Ordnen Sie auf jedem Cluster LUNs der Initiatorgruppe zu:

   ```
   lun map -path path_name -igroup igroup_name
   ```

6. Überprüfen Sie, ob die LUN-Zuordnung mit dem erfolgreich abgeschlossen wurde `lun map` Befehl. Anschließend können Sie die neuen LUNs auf dem Anwendungshost ermitteln.

SM-BC managen und Daten sichern

Erstellen einer gemeinsamen Snapshot Kopie

Zusätzlich zu den regelmäßig geplanten Snapshot Kopiervorgängen können Sie manuell eine gemeinsame erstellen "Snapshot Kopie" Zwischen den Volumes in der primären SnapMirror Konsistenzgruppe und den Volumes in der sekundären SnapMirror Konsistenzgruppe.

Über diese Aufgabe

- In ONTAP 9.8 beträgt die geplante Erstellung von Snapshots eine Stunde.

  Ab ONTAP 9.9 beträgt dieses Intervall 12 Stunden.

Bevor Sie beginnen

- Die SnapMirror-Gruppenbeziehung muss synchron sein.

Schritte

1. Erstellen einer gemeinsamen Snapshot Kopie:

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. Überwachen Sie den Fortschritt des Updates:

   ```
   destination::>snapmirror show -fields -newest-snapshot
   ```

Führen Sie ein geplantes Failover durch

Bei einem geplanten Failover wechseln Sie die Rollen der primären und sekundären Cluster, sodass das sekundäre Cluster vom primären Cluster übernommen wird. 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 SM-BC-Beziehung muss synchron sein.
- Sie können kein geplantes Failover initiieren, wenn gerade ein unterbrechungsfreier Betrieb läuft. Zu den unterbrechungsfreien Abläufen gehören Volume-Verschiebungen, aggregrate Standortwechsel und Storage-Failover.
- 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

1. Wählen Sie in System Manager **Schutz > Übersicht > Beziehungen**.
2. Identifizieren Sie die SM-BC-Beziehung, die Sie für ein Failover verwenden möchten. Wählen Sie neben dem Namen den aus … Wählen Sie neben dem Namen der Beziehung die Option **Failover**.
3. Um den Status des Failover zu überwachen, verwenden Sie die `snapmirror failover show` Über die 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. Wenn der Failover-Vorgang abgeschlossen ist, können Sie den Status der synchronen SnapMirror Schutzbeziehung vom Ziel aus überwachen:

   ```
   destination::>snapmirror show
   ```

Wiederherstellung nach automatischen ungeplanten Failover-Vorgängen

Ein automatischer ungeplanter Failover (AUFO) erfolgt, wenn das primäre Cluster ausgefallen ist oder isoliert ist. Der ONTAP Mediator erkennt, wenn ein Failover stattfindet, und führt einen automatischen ungeplanten Failover auf den sekundären Cluster aus. Der sekundäre Cluster wird in den primären Cluster konvertiert und beginnt mit der Bereitstellung von Clients. Dieser Vorgang wird nur mithilfe des ONTAP Mediators 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

1. Navigieren Sie zu **Schutz > Beziehungen** und warten Sie, bis der Beziehungsstatus „InSync“ anzeigt.
2. Um die Vorgänge auf dem ursprünglichen Quell-Cluster fortzusetzen, klicken Sie auf ⋮ Und wählen Sie **Failover**.

CLI

Sie können den Status des automatischen ungeplanten Failovers mit der überwachen `snapmirror failover show` Befehl.

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: -
```

Siehe "EMS-Referenz" Um Informationen zu Ereignismeldungen und zu Korrekturmaßnahmen zu erhalten.

Setzen Sie den Schutz in einer Fan-out-Konfiguration nach dem Failover fort

Wenn auf dem sekundären Cluster in der SM-BC-Beziehung ein Failover erfolgt, wird das asynchrone SnapMirror-Ziel als fehlerhaft betrachtet. Sie müssen den Schutz manuell wiederherstellen, indem Sie die Beziehung zum asynchronen SnapMirror-Endpunkt löschen und neu erstellen.

Schritte

1. Überprüfen Sie, ob der Failover erfolgreich abgeschlossen wurde:
   `snapmirror failover show`
2. Löschen Sie am asynchronen SnapMirror Endpunkt das Fan-out-Endpunkt:
   `snapmirror delete -destination-path` *`destination_path`*
3. Erstellen Sie am dritten Standort eine asynchrone SnapMirror Beziehungen zwischen dem neuen primären SM-BC Volume und dem asynchronen Fan-out-Ziel-Volume:
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*
4. Beziehung neu synchronisieren:
   `snapmirror resync -destination-path` *`destination_path`*

5. Überprüfen Sie den Beziehungsstatus und den Status „Systemzustand“:
   `snapmirror show`

Monitoring der SnapMirror Business Continuity Abläufe

Sie können die folgenden SnapMirror Business Continuity (SM-BC) Operationen überwachen, um den Zustand Ihrer SM-BC Konfiguration sicherzustellen:

- ONTAP Mediator
- Geplante Failover-Vorgänge
- Automatische ungeplante Failover-Vorgänge
- Verfügbarkeit von SM-BC

ONTAP Mediator

Während des normalen Betriebs sollte der ONTAP-Mediatorstatus verbunden sein. Wenn sie sich in einem anderen Status befindet, kann dies auf einen Fehler hinweisen. Sie können die überprüfen "EMS-Meldungen (Event Management System" Zur Bestimmung des Fehlers und der entsprechenden Korrekturmaßnahmen.

Geplante Failover-Vorgänge

Mit dem können Sie den Status und den Status eines geplanten Failover-Vorgangs überwachen `snapmirror failover show` Befehl. Beispiel:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Sobald der Failover-Vorgang abgeschlossen ist, können Sie den synchronen SnapMirror Sicherungsstatus aus dem neuen Ziel-Cluster überwachen. Beispiel:

```
ClusterA::> snapmirror show
```

Siehe "EMS-Referenz" Um Informationen zu Ereignismeldungen und Korrekturmaßnahmen zu erhalten.

Automatische ungeplante Failover-Vorgänge

Während eines ungeplanten automatischen Failover können Sie mithilfe von den den den Status des Vorgangs überwachen `snapmirror failover show` Befehl.

```
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: -
```

Siehe "EMS-Referenz" Um Informationen zu Ereignismeldungen und zu Korrekturmaßnahmen zu erhalten.

Verfügbarkeit von SM-BC

Sie können die Verfügbarkeit der SM-BC-Beziehung mit einer Reihe von Befehlen überprüfen, entweder im primären Cluster, im sekundären Cluster oder beiden.

Die Befehle, die Sie verwenden, enthalten `snapmirror mediator show` Befehl für das primäre und das sekundäre Cluster, um den Status der Verbindung und des Quorum zu überprüfen, der `snapmirror show` Befehl, und das `volume show` Befehl. Beispiel:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored InSync  -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored InSync    -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

Hinzufügen oder Entfernen von Volumes zu einer 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 SM-BC Beziehung hängt von der Version von ONTAP ab, die Sie verwenden.

In den meisten Fällen führt dies zu Unterbrechungen des Betriebs, die dazu führen, dass Sie die SnapMirror Beziehung unterbrechen, die Konsistenzgruppe ändern und den Schutz wieder aufnehmen. Ab ONTAP 9.13.1 ist das Hinzufügen von Volumes zu einer Konsistenzgruppe mit einer aktiven SM-BC-Beziehung ein

unterbrechungsfreier Vorgang.

Über diese Aufgabe

- In ONTAP 9.8 bis 9.9 können Sie einer Konsistenzgruppe über die ONTAP-CLI Volumes hinzufügen oder entfernen.
- Ab ONTAP 9.10.1 empfehlen wir Ihnen, das Management "Konsistenzgruppen" Über System Manager oder mit der ONTAP REST API.

  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 unterbrechungsfrei zu einer Konsistenzgruppe mit einer aktiven SM-BC-Beziehung von der Quelle oder dem Ziel hinzufügen.

  Das Entfernen von Volumes verursacht Unterbrechungen. Sie müssen die SnapMirror-Beziehung unterbrechen, bevor Sie mit dem Entfernen von Volumes fortfahren.

ONTAP 9.8-9.13.0

Bevor Sie beginnen

- Sie können nicht damit beginnen, die Konsistenzgruppe zu ändern, während sie sich im befindet `InSync` Bundesland.
- Das Ziel-Volume sollte vom Typ DP sein.
- Das neue Volumen, das Sie zur Erweiterung der Konsistenzgruppe hinzufügen, muss über zwei allgemeine Snapshot Kopien zwischen den Quell- und Ziel-Volumes verfügen.

Schritte

Die Beispiele in zwei Volume-Zuordnungen: `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. Falls keine gemeinsame Snapshot Kopie 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:vol_dst3
   ```

4. Geben Sie die SnapMirror Quellbeziehung wieder und behalten Sie die allgemeinen Snapshot Kopien 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 und recreate und die Consistency Group auf der Quelle mit der richtigen Zusammensetzung. Befolgen Sie die Schritte unter Löschen einer Konsistenzgruppe Und dann Konfigurieren einer einzelnen Konsistenzgruppe. In ONTAP 9.10.1 und höher müssen Sie die Löschvorgänge in System Manager oder mit der ONTAP REST API ausführen. Es gibt kein CLI-Verfahren.

   Wenn Sie ONTAP 9.8, 9.0 oder 9.9 verwenden, gehen sie zum nächsten Schritt.

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 SM-BC-Beziehung hinzufügen. SM-BC unterstützt das Hinzufügen von Volumes sowohl von der Quelle als auch vom Ziel.

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 SM-BC Beziehung, zu 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**.

Vorhandene Beziehungen in SM-BC-Beziehungen konvertieren

Wenn Sie eine bestehende synchrone SnapMirror-Beziehung zwischen einem Quell- und Ziel-Cluster haben, können Sie sie in eine SM-BC-Beziehung konvertieren. Auf diese Weise können Sie die gespiegelten Volumes einer Konsistenzgruppe zuordnen, um für einen Workload mit mehreren Volumes einen RPO von null zu gewährleisten. Außerdem können Sie vorhandene SnapMirror Snapshots behalten, wenn Sie zu einem bestimmten

Zeitpunkt vor dem Herstellen der SM-BC-Beziehung zurücksetzen müssen.

Bevor Sie beginnen

- Zwischen dem primären und dem sekundären Cluster muss eine synchrone SnapMirror Beziehung mit einem 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.
- SM-BC unterstützt nur SAN-Protokolle (keine NFS/CIFS). Stellen Sie sicher, dass für den NAS-Zugriff keine Komponente der Konsistenzgruppe bereitgestellt ist.

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 Zuordnung der LUNs aufgehoben wird, bevor Sie die ausgeben `snapmirror create` Befehl.

  Wenn vorhandene LUNs auf dem sekundären Volume zugeordnet sind, und der `AutomatedFailover` Policy wird konfiguriert, der `snapmirror create` Löst einen Fehler aus.

Schritte

1. Führen Sie aus dem sekundären Cluster ein SnapMirror Update der bestehenden Beziehung durch:

   ```
   destination::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Überprüfen Sie, ob das SnapMirror Update erfolgreich abgeschlossen wurde:

   ```
   destination::>snapmirror show
   ```

3. Stilllegung jeder der synchronen Beziehungen ohne RPO:

   ```
   destination::>snapmirror quiesce -destination-path vs1_dst:vol1

   destination::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Sie löschen jede der synchronen Beziehungen ohne RPO:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:vol1

   destination::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Geben Sie die SnapMirror Quellbeziehung frei, behalten Sie die gemeinsamen Snapshot Kopien jedoch bei:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Erstellen einer Gruppe null RTO synchrone SnapMirror Beziehung:

```
destination::> 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:

```
destination::> 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

Aktualisieren und Zurücksetzen von ONTAP mit SM-BC

SnapMirror Business Continuity (SM-BC) wird ab ONTAP 9.8 unterstützt. Das Aktualisieren und Zurücksetzen des ONTAP-Clusters hat Auswirkungen auf die SM-BC Beziehungen, abhängig von der ONTAP-Version, auf die Sie aktualisieren oder zurücksetzen.

Aktualisieren Sie ONTAP mit SM-BC

Um SM-BC zu verwenden, müssen alle Knoten auf den Quell- und Zielcluster ONTAP 9.8 oder höher ausführen.

Wenn Sie ONTAP mit aktiven SM-BC-Beziehungen aktualisieren, sollten Sie verwenden Automatisierte unterbrechungsfreie Upgrades (ANDU). Durch die Verwendung von ANDU wird sichergestellt, dass Ihre SM-BC-Beziehungen während des Upgrade-Prozesses synchron und fehlerfrei sind.

Es gibt keine Konfigurationsschritte, um SM-BC-Implementierungen für ONTAP-Upgrades vorzubereiten. Es wird jedoch empfohlen, vor und nach dem Upgrade Folgendes zu überprüfen:

- SM-BC-Beziehungen 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 9.8 oder 9.9.1 auf ONTAP 9.10.1 und höher aktualisieren, erstellt ONTAP neu Konsistenzgruppen Auf Quell- und Ziel-Clustern für SM-BC-Beziehungen, die mit System Manager konfiguriert werden können.

> Der `snapmirror quiesce` Und `snampirror resume` Befehle werden mit SM-BC nicht unterstützt.

Kehren Sie von ONTAP 9.10.1 zu ONTAP 9.9.1 zurück

Um Beziehungen von 9.10.1 auf 9.9 zurückzusetzen, müssen SM-BC-Beziehungen gelöscht werden, gefolgt von der Konsistenzgruppeinstanz 9.10.1. Konsistenzgruppen mit einer aktiven SM-BC-Beziehung 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. Siehe "Löschen einer Konsistenzgruppe" Weitere Informationen zu dieser Aufgabe finden Sie in ONTAP 9.10.1 und höher.

Kehren Sie von ONTAP 9.8 zu ONTAP 9.7 zurück

SM-BC wird nicht mit gemischten ONTAP 9.7 und ONTAP 9.8 Clustern unterstützt.

Wenn Sie von ONTAP 9.8 auf ONTAP 9.7 zurücksetzen, müssen Sie Folgendes beachten:

- Wenn der Cluster-Host ein SM-BC Ziel ist, kann das Zurücksetzen auf ONTAP 9.7 nicht zulässig, bis die Beziehung unterbrochen und gelöscht wird.
- Wenn der Cluster eine SM-BC Quelle hostet, ist das Zurücksetzen auf ONTAP 9.7 erst zulässig, wenn die Beziehung freigegeben ist.
- Alle benutzerdefinierten SM-BC SnapMirror-Richtlinien, die vom Benutzer erstellt wurden, müssen gelöscht werden, bevor Sie auf ONTAP 9.7 zurücksetzen.

Informationen zur Erfüllung dieser Anforderungen finden Sie unter "Entfernen Sie eine SM-BC-Konfiguration".

Schritte

1. Führen Sie einen Rückkehrcheck von einem der Cluster in der SM-BC Beziehung durch:

   ```
   cluster::*> system node revert-to -version 9.7 -check-only
   ```

   Beispiel:

   ```
   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 9.8"
    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>
```

Informationen zum Zurücksetzen von Clustern finden Sie unter "ONTAP zurücksetzen".

Entfernen Sie eine SM-BC-Konfiguration

Wenn Sie keinen RTO-Synchronous SnapMirror-Schutz mehr benötigen, können Sie Ihre SM-BC-Beziehung löschen.

Über diese Aufgabe

- Bevor Sie die SM-BC-Beziehung löschen, müssen alle LUNs im Ziel-Cluster nicht zugeordnet 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 die ausgeben `snapmirror break` Befehl zum Konvertieren in Lesen/Schreiben.
- 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 SM-BC-Konsistenzgruppenbeziehung zwischen dem Quellendpunkt und dem Zielendpunkt:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. Geben Sie aus dem primären Cluster die Konsistenzgruppenbeziehung und die Snapshot Kopien wieder, die für die Verbindung erstellt wurden:

   ```
   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. Siehe Löschen einer Konsistenzgruppe Finden Sie weitere Informationen.

Entfernen Sie den ONTAP Mediator

Wenn Sie eine vorhandene ONTAP Mediator-Konfiguration aus Ihren ONTAP Clustern entfernen möchten, verwenden Sie die `snapmirror mediator remove` Befehl.

Schritte

1. ONTAP-Mediator entfernen:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster
   cluster_xyz
   ```

Fehlerbehebung

Das Löschen von SnapMirror schlägt im Takover-Status fehl

Problem:

Wenn ONTAP 9.9.1 auf einem Cluster installiert ist, führen Sie die aus `snapmirror delete` Befehl schlägt fehl, wenn eine SM-BC Konsistenzgruppenbeziehung sich im Übernahmemodus befindet.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Nutzen

Wenn sich die Knoten in einer SM-BC Beziehung im Übernahmemodus befinden, führen Sie die SnapMirror

Lösch- und Freigabeoperation durch und die Option „-Force“ ist auf „true“ gesetzt.

```
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".
```

Das Erstellen einer SnapMirror-Beziehung und das Initialisieren der Konsistenzgruppe ist fehlgeschlagen

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 für Konsistenzgruppen in SM-BC sind plattformunabhängig und variieren je nach Version von ONTAP. Siehe "Zusätzliche Einschränkungen und Einschränkungen" Für Einschränkungen basierend auf der Version von ONTAP.

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`.

Lösung:

Wenn Konsistenzgruppen nicht initialisiert werden, entfernen Sie die SM-BC-Beziehung, löschen Sie die Konsistenzgruppe, erstellen Sie dann die Beziehung neu und initialisieren Sie sie. Dieser Workflow unterscheidet sich je nach der verwendeten ONTAP Version.

Bei Verwendung von ONTAP 9.8-9.9.1	Wenn Sie ONTAP 9.10.1 oder höher verwenden
1. "Entfernen Sie die SM-BC-Konfiguration" 2. "Erstellen einer Konsistenzgruppenbeziehung" 3. "Initialisieren Sie die Konsistenzgruppenbeziehung"	1. Finden Sie unter **Schutz > Beziehungen** die SM-BC Beziehung auf der Konsistenzgruppe. Wählen Sie ⋮, Dann **Löschen**, um die SM-BC-Beziehung zu entfernen. 2. "Löschen Sie die Konsistenzgruppe" 3. "Konfigurieren Sie die Konsistenzgruppe"

Ein geplantes Failover war nicht erfolgreich

Problem:

Nach Ausführung des `snapmirror failover start` Befehl, die Ausgabe für das `snapmirror failover show` Befehl zeigt eine Meldung an, dass 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.

Der ONTAP-Mediator ist nicht erreichbar oder der Mediator-Quorum-Status ist falsch

Problem:

Nach Ausführung des `snapmirror failover start` Befehl, die Ausgabe für das `snapmirror failover show` Der Befehl zeigt eine Meldung an, dass Mediator nicht konfiguriert ist.

Siehe "Initialisieren Sie den ONTAP-Mediator".

```
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 SM-BC-Beziehung aufbauen 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
```

Der automatische ungeplante Failover wird nicht an Standort B ausgelöst

Problem:

Ein Fehler an Standort A löst kein ungeplantes Failover auf Standort B aus

Mögliche Ursache #1:

Der ONTAP-Mediator ist nicht konfiguriert. Um festzustellen, ob dies die Ursache ist, geben Sie den ein `snapmirror mediator show` Befehl auf dem Cluster Standort B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Dieses Beispiel zeigt an, dass ONTAP Mediator nicht auf Standort B konfiguriert ist

Lösung:

Stellen Sie sicher, dass ONTAP Mediator auf beiden Clustern konfiguriert ist, dass der Status verbunden und Quorum auf wahr 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 Consistency Group-Beziehung mit dem `force` Option.
3. Geben Sie das ein `snapmirror break` Befehl für die Consistency Group -Teilvolume zum Konvertieren von Volumes von DP in R/W, 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 frei `relationship-info-only` An Standort A werden die allgemeine Snapshot Kopie beibehalten und die Zuordnung der LUNs zu der Konsistenzgruppe aufheben.
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. Stellen Sie das aus `snapmirror resync` So synchronisieren Sie die Beziehungen.
8. Löschen Sie die SnapMirror Beziehungen mit der Sync-Richtlinie auf Standort A
9. Lassen Sie die SnapMirror Beziehungen mit der Sync-Richtlinie los `relationship-info-only true` Vor Ort B.
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

Verbindung zwischen Standort B und Mediator Down und Standort A Down

Um die Verbindung des ONTAP Mediators zu überprüfen, verwenden Sie die `snapmirror mediator show` Befehl. Wenn der Verbindungsstatus nicht erreichbar ist und Standort B Standort A nicht erreichen kann, erhalten Sie eine Ausgabe ähnlich der unten stehenden. Befolgen Sie die Schritte in der Lösung, um die Verbindung wiederherzustellen

```
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 einen Failover, um I/O von Standort B zu aktivieren und dann eine RTO-Beziehung von Standort B zu Standort A ohne Recovery-Wert zu definieren 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 Consistency Group-Beziehung mit der Force-Option.
3. Geben Sie den SnapMirror Break-Befehl ein (`snapmirror break -destination_path` *`svm`*`:_volume_`) Auf den Volumes der Consistency Group, 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.

4. Starten Sie die Knoten Standort A, um eine RTO-Beziehung von Standort B zu Standort A zu erstellen
5. Freigabe der Konsistenzgruppe mit „nur Beziehung“ bei Standort A, um eine allgemeine Snapshot Kopie beizubehalten und die zu der Konsistenzgruppe gehörenden LUNs zu aufheben
6. 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.
7. Stellen Sie das aus `snapmirror resync` Befehl zum Synchronisieren der Beziehungen.
8. Löschen Sie die SnapMirror Beziehungen mit der Sync-Richtlinie auf Standort A
9. Lassen Sie die SnapMirror Beziehungen mit Sync-Richtlinie unter Verwendung von Relationship-info-only True auf Site B. frei
10. Erstellen Sie eine Konsistenzgruppenbeziehung zwischen Standort B und Standort A.
11. Synchronisieren Sie die Konsistenzgruppe aus dem Quell-Cluster neu. Überprüfen Sie, ob der Status der Konsistenzgruppe synchron ist.
12. Scannen Sie die Host-LUN-I/O-Pfade erneut, um alle Pfade zu den LUNs wiederherzustellen.

Verbindung zwischen Standort A und Mediator down und Standort B down

Bei Verwendung von SM-BC kann die Verbindung zwischen dem ONTAP Mediator oder Ihren Peered Clustern verloren gehen. Sie können das Problem diagnostizieren, indem Sie die Verbindung, Verfügbarkeit und den Konsensstatus der verschiedenen Teile der SM-BC-Beziehung prüfen und dann die Verbindung mit Nachdruck wieder aufnehmen.

Was zu prüfen ist	CLI-Befehl	Anzeige
Mediator von Standort A	`snapmirror mediator show`	Der Verbindungsstatus lautet `unreachable`
Anschluss an Standort B	`cluster peer show`	Die Verfügbarkeit ist möglich `unavailable`
Konsensstatus des SM-BC Volumens	`volume show` *`volume_name`* `-fields smbc-consensus`	Der `sm-bc consensus` Feld wird gelesen `Awaiting-consensus`

Weitere Informationen zur Diagnose und Lösung dieses Problems finden Sie im Artikel in der Knowledge Base "Verknüpfung zwischen Standort A und Mediator ab und Standort B unten bei Verwendung von SM-BC".

SM-BC SnapMirror Löschvorgang schlägt fehl, wenn Zaun auf dem Ziel-Volume eingestellt 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

Volume-Verschiebung bei Ausfall des primären Laufwerks nicht aktiviert

Problem:

Ein Vorgang zur Verschiebung eines Volumes ist unbegrenzt in einem verzögerten Zustand der Umstellung stecken, wenn der primäre Standort in einer SM-BC-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.

Der Release von SnapMirror schlägt fehl, wenn die Snapshot Kopie nicht gelöscht werden kann

Problem:

Der Release von SnapMirror schlägt fehl, wenn die Snapshot Kopie nicht gelöscht werden kann.

Lösung:

Die Snapshot-Kopie enthält ein vorübergehendes Tag. Verwenden Sie die `snapshot delete` Befehl mit dem `-ignore-owners` Option zum Entfernen der transienten Snapshot Kopie.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Wiederholen Sie den `snapmirror release` Befehl.

Die Snapshot Kopie der Verschiebung der Volume-Referenz wird als neueste angezeigt

Problem:

Nach einem Volume-Verschiebevorgang auf einem Konsistenzgruppenvolume wird möglicherweise die Snapshot Kopie zur Verschiebung des Volumes als neueste für die SnapMirror Beziehung angezeigt.

Sie können die neueste Snapshot Kopie mit dem folgenden Befehl anzeigen:

```
snapmirror show -fields newest-snapshot status -expand
```

Lösung:

Führen Sie manuell einen aus `snapmirror resync` Oder warten Sie, bis der nächste automatische Neusynchronisierung erfolgt, nachdem die Volume-Verschiebung abgeschlossen ist.

Mediator Service für MetroCluster und SnapMirror Business Continuity

ONTAP Mediator Übersicht

Der ONTAP Mediator bietet verschiedene Funktionen für ONTAP-Funktionen:

- 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.

Der ONTAP Mediator stellt zwei zusätzliche systemctl-Dienste zur Verfügung:

- **`ontap_mediator.service`**

  Verwaltet den REST-APIs-Server für das Management der ONAP-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 nutzt SCST für die iSCSI-Bereitstellung (siehe. 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 den ONTAP Mediator deinstallieren, dann neu installieren und dann die ONTAP-Beziehung neu konfigurieren.

> Alle Aktualisierungen des Server-OS-Kernels sollten mit einem Wartungsfenster in ONTAP koordiniert werden.

Was gibt es Neues beim ONTAP Mediator

Mit jeder Version werden neue Verbesserungen am ONTAP Mediator bereitgestellt. Was ist neu?

Vorgestellt Werden

Version des ONTAP Mediators	Vorgestellt Werden
1.7	• Unterstützung für RHEL 8.5, 8.6, 8.7, 8.8, 8.9 9.0, 9.1, 9.2 und 9.3 • Unterstützung für Rocky Linux 8 und 9
1.6	• Python 3.9-Updates. • Unterstützung für RHEL 8.4-8.8, 9.0-9.2, Rocky Linux 8 und 9. • Nicht mehr unterstützte RHEL 7.x/CentOS-Versionen.
1.5	• Optimiert die Geschwindigkeit für größere SMBC-Systeme. • Kryptografische Codesignatur wurde dem Installationsprogramm hinzugefügt. • Enthält Abschreibungswarnungen für RHEL 7.x / CentOS 7.x.
1.4	• Unterstützung für RHEL 8.4 und 8.5. • Enthält SCST Version 3.6.0. • Zusätzliche Unterstützung für Secure Boot (SB) der UFEI-basierten Firmware.
1.3	• Unterstützung für RHEL/CentOS 8.2 und 8.3. • Enthält SCST Version 3.5.0.
1.2	• Unterstützung für HTTPS-Mailboxen. • Zur Verwendung mit ONTAP 9.8+ MCC-IP AUSO und SM-BC ZRTO. • Enthält SCST Version 3.4.0.

1.1	• Unterstützung für RHEL/CentOS 7.6, 7.7, 8.0 und 8.1. • Eliminiert Perl-Abhängigkeiten. • Enthält SCST Version 3.4.0.
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	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1.0
7.6	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Ja.	Ja (nur RHEL)
7.7	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Nein	Nein
7.8	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Nein	Nein
7.9	Veraltet	Veraltet	Ja.	Ja.	Ja.	Implizit	Nein	Nein
RHEL 8.0	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Ja.	Nein
RHEL 8.1	Veraltet	Veraltet	Ja.	Ja.	Ja.	Ja.	Nein	Nein
RHEL 8.2	Veraltet	Veraltet	Ja.	Ja.	Ja.	Nein	Nein	Nein
RHEL 8.3	Veraltet	Veraltet	Ja.	Ja.	Ja.	Nein	Nein	Nein
RHEL 8.4	Veraltet	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
RHEL 8.5	Ja.	Ja.	Ja.	Ja.	Nein	Nein	Nein	Nein
RHEL 8.6	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8.7	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 8.8	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9.0	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein

RHEL 9.1	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9.2	Ja.	Ja.	Nein	Nein	Nein	Nein	Nein	Nein
RHEL 9.3	Ja.	Nein	Nein	Nein	Nein	Nein	Nein	Nein
CentOS 8 und Stream	Nein	Nein	Nein	Nein	Nein	1. A.	1. A.	1. A.
Rocky Linux 8	Ja.	Ja.	1. A.	1. A.	1. A.	1. A.	1. A.	1. A.
Rocky Linux 9	Ja.	Ja.	1. A.	1. A.	1. A.	1. A.	1. A.	1. A.

- OS bezieht sich auf RedHat- und CentOS-Versionen, sofern nicht anders angegeben.
- „Nein“ bedeutet, dass Betriebssystem und ONTAP Mediator nicht kompatibel sind.
- 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.
- ONTAP Mediator 1.5 war die letzte unterstützte Version für RHEL 7.x-Filialbetriebssysteme.
- ONTAP Mediator 1.6 bietet Unterstützung für Rocky Linux 8 und 9.

Behobene Probleme

Änderungsdatum	ID ändern	Beschreibung
Januar 2023, 10	6567145	Folgende Änderungen wurden vorgenommen: • Zusätzliche Unterstützung für zusätzliche Betriebssysteme für ONTAP Mediator: RHEL 9.6, 8.7, 9.0 und 9.1. • Neue SCST-Version 3.7.0 hinzugefügt, um die Blockierung von Problemen für neu unterstützte Betriebssysteme aufzuheben. • Zusätzliche Unterstützung für Rocky Linux: Rocky 8 und 9.
Januar 2023, 24	6621319	Zulässige vorinstallierte SCST-Bibliothek für ONTAP Mediator-Installationen.
27 Februar 2023	6623764	Änderungen wurden implementiert, um immer das Kernel-Modul scst_Disk zu laden, wenn der Mediator-scst-Dienst neu gestartet wird. Diese Änderungen stellen sicher, dass der Service immer bereit ist, neue iSCSI-Ziele unter Verwendung der Standardlogik zu erstellen.

28 Februar 2023	6625194	Dem Installationsprogramm für ONTAP Mediator wurde eine neue Option hinzugefügt: `--skip-yum-dependencies`
24 März 2023	6652840	Das Installationsprogramm für ONTAP Mediator wurde aktualisiert, damit es die SCST-Installation neu installieren oder reparieren kann.
27 März 2023	6655179	Es wurde ein Analyseproblem behoben, das beim Auslösen der Sammlung des Support-Pakets mit einem komplexen Kennwort aufgetreten war.
28 März 2023	6656739	Die SCST-Vergleichslogik wurde so geändert, dass die richtige Version installiert wird, wenn ONTAP Mediator aktualisiert wird.

Installation oder Upgrade

Bereiten Sie die Installation oder das Upgrade des ONTAP Mediatordienstes vor

Um den ONTAP Mediator-Dienst zu installieren, müssen Sie sicherstellen, dass alle Voraussetzungen erfüllt sind, das Installationspaket abrufen und das Installationsprogramm auf dem Host ausführen. Dieses Verfahren wird für eine Installation oder ein Upgrade einer vorhandenen Installation verwendet.

Über diese Aufgabe

- Ab ONTAP 9.7 können Sie eine beliebige Version des ONTAP Mediators verwenden, um eine MetroCluster IP-Konfiguration zu überwachen.
- Ab ONTAP 9.8 können Sie eine beliebige Version des ONTAP Mediators verwenden, um eine SM-BC-Beziehung zu überwachen.

Bevor Sie beginnen

Sie müssen die folgenden Voraussetzungen erfüllen.

Version des ONTAP Mediators	Unterstützte Linux-Versionen
1.7	• Red Hat Enterprise Linux: 8.5, 8.6, 8.7, 8.8, 8.9 9.0, 9.1, 9.2 und 9.3 • Rocky Linux 8 und 9
1.6	• Red Hat Enterprise Linux: 8.4, 8.5, 8.6, 8.7, 8.8 9.0, 9.1, 9.2 • Rocky Linux 8 und 9
1.5	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9
1.4	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3, 8.4, 8.5 • CentOS: 7.6, 7.7, 7.8, 7.9

1.3	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1 8.2, 8.3 • CentOS: 7.6, 7.7, 7.8, 7.9
1.2	• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1 • CentOS: 7.6, 7.7, 7.8

Die Kernel-Version muss mit der Betriebssystemversion übereinstimmen.

- 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

Alle Bibliothekspakete mit Ausnahme des Kernels können sicher aktualisiert werden, erfordern jedoch möglicherweise einen Neustart, um in der ONTAP Mediator-Anwendung wirksam zu werden. Wenn ein Neustart erforderlich ist, wird ein Service-Fenster empfohlen.

Wenn Sie den installieren `yum-utils` Die Sie verwenden können `needs-restarting` Befehl.

Der Kernelkern kann aktualisiert werden, wenn er auf eine Version aktualisiert wird, die noch von der ONTAP Mediator Versionsmatrix unterstützt wird. Ein Neustart ist obligatorisch, daher ist ein Service-Fenster erforderlich.

Das SCST-Kernelmodul muss vor dem Neustart deinstalliert und nach dem Neustart neu installiert werden.

Ein Upgrade auf einen Kernel, der über die unterstützte OS-Version für die spezifische ONTAP Mediator-Version hinausgeht, wird nicht unterstützt. (Dies deutet wahrscheinlich darauf hin, dass das getestete SCST-Modul nicht kompiliert).

Registrieren Sie einen Sicherheitsschlüssel, wenn UEFI Secure Boot aktiviert ist

Wenn UEFI Secure Boot aktiviert ist, müssen Sie zur Installation von ONTAP Mediator einen Sicherheitsschlüssel registrieren, bevor der ONTAP Mediator Dienst gestartet werden kann. So stellen Sie fest, ob das System UEFI-aktiviert und Secure Boot eingeschaltet ist:

Schritte

1. Wenn mokutil nicht installiert ist, führen Sie den folgenden Befehl aus:

   ```
   yum install mokutil
   ```

2. Führen Sie den folgenden Befehl aus, um zu ermitteln, ob UEFI Secure Boot auf Ihrem System aktiviert ist:

   ```
   mokutil --sb-state
   ```

   Die Ergebnisse zeigen, ob UEFI Secure Boot auf diesem System aktiviert ist.

   ONTAP Mediator 1.2.0 und frühere Versionen unterstützen diesen Modus nicht.

Deaktivieren Sie UEFI Secure Boot

Sie können auch den sicheren UEFI-Start deaktivieren, bevor Sie ONTAP Mediator installieren.

Schritte

1. Deaktivieren Sie in den BIOS-Einstellungen des physischen Computers die Option „UEFI Secure Boot“.
2. Deaktivieren Sie in den VMware-Einstellungen für die VM die Option „Sicherer Start“ für vSphere 6.x oder die Option „Sicherer Start“ für vSphere 7.x

Aktualisieren Sie das Host-Betriebssystem und anschließend den ONTAP Mediator

Um das Host-Betriebssystem für ONTAP Mediator auf eine neuere Version zu aktualisieren, müssen Sie ONTAP Mediator zuerst deinstallieren.

Bevor Sie beginnen

Die Best Practices für die Installation von Red hat Enterprise Linux oder Rocky Linux und den zugehörigen Repositorys auf Ihrem System sind unten aufgeführt. Eine andere Konfiguration oder Installation von Systemen erfordert möglicherweise zusätzliche Schritte.

- Sie müssen Red hat Enterprise Linux oder Rocky Linux gemäß den Best Practices von Red hat installieren. Da die CentOS 8.x-Versionen Unterstützung zum Ende der Lebensdauer bieten, werden kompatible Versionen von CentOS 8.x nicht empfohlen.
- Bei der Installation des ONTAP Mediator-Dienstes auf Red hat Enterprise Linux oder Rocky Linux muss das System Zugriff auf das entsprechende Repository haben, damit das Installationsprogramm auf alle erforderlichen Softwareabhängigkeiten zugreifen und diese installieren kann.
- Damit der yum-Installer nach abhängiger Software in den Red hat Enterprise Linux-Repositorys sucht, müssen Sie das System während der Red hat Enterprise Linux-Installation oder danach mit einem gültigen Red hat-Abonnement registriert haben.

  Informationen zum Red hat Subscription Manager finden Sie in der Red hat Dokumentation.

- Die folgenden Ports müssen nicht verwendet und für den Mediator verfügbar sein:
  - 31784
  - 3260
- Wenn Sie eine Firewall eines Drittanbieters verwenden, lesen Sie "Firewall-Anforderungen für ONTAP Mediator"
- Wenn sich der Linux-Host an einem Standort ohne Zugriff auf das Internet befindet, müssen Sie sicherstellen, dass die erforderlichen Pakete in einem lokalen Repository verfügbar sind.

  Wenn Sie das Link Aggregation Control Protocol (LACP) in einer Linux-Umgebung verwenden, müssen Sie den Kernel korrekt konfigurieren und sicherstellen, dass der `sysctl net.ipv4.conf.all.arp_ignore` Ist auf „2“ eingestellt.

Was Sie benötigen

Folgende Pakete werden vom ONTAP Mediator Service benötigt:

Alle RHEL/CentOS Versionen	Zusätzliche Pakete für RHEL 8.x / Rocky Linux 8	Zusätzliche Pakete für RHEL 9.x / Rocky Linux 9

• openssl • openssl-devel • Kernel-devel-€ (uname -r) • gcc • Make • Libselinux-utils • Patch • Bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeuMaker • Efibootmgr • Mokutil	• python3-Pip • Elfutils-libelf-devel • Politicoreutils-Python-utils • Redhat-lsb-Core • Python39 • Python39-devel	• python3-Pip • Elfutils-libelf-devel • Politicoreutils-Python-utils • python3 • python3-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.

Eine gültige SSL-Zertifizierung wird empfohlen.

Über diese Aufgabe

Wenn Sie das Host-Betriebssystem für ONTAP Mediator mit dem Leapp-Upgrade-Tool auf eine neuere Hauptversion (z. B. von 7.x auf 8.x) aktualisieren, Sie müssen ONTAP Mediator deinstallieren, da das Tool versucht, neue Versionen aller RPMs zu erkennen, die in den Repositories installiert sind, die beim System registriert sind.

Da eine rpm-Datei als Teil des Installationsprogramms für ONTAP Mediator installiert wurde, wird sie in diese Suche aufgenommen. Da diese rpm-Datei jedoch als Teil des Installers entpackt und nicht von einem registrierten Repository heruntergeladen wurde, kann kein Upgrade gefunden werden. In diesem Fall deinstalliert das Leapp-Upgrade-Tool das Paket.

Um die Protokolldateien zu erhalten, die zur Einstufung von Support-Fällen verwendet werden, sollten Sie die Dateien vor einem Betriebssystem-Upgrade sichern und nach einer Neuinstallation des ONTAP Mediator-Pakets wiederherstellen. Da der ONTAP Mediator neu installiert wird, müssen alle ONTAP-Cluster, die mit ihm verbunden sind, nach der neuen Installation erneut verbunden werden.

> Die folgenden Schritte sollten in der angegebenen Reihenfolge ausgeführt werden. Unmittelbar nach der Neuinstallation von ONTAP Mediator sollten Sie den ontap_Mediator Service beenden, die Protokolldateien ersetzen und den Service neu starten. Dadurch wird sichergestellt, dass keine Protokolle verloren gehen.

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. Upgrade mit leapp-Upgrade-Tool durchführen.

```
[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. Installieren Sie ONTAP Mediator neu.

> Führen Sie die restlichen Schritte unmittelbar nach der Neuinstallation von ONTAP Mediator aus, um einen Verlust von Protokolldateien zu verhindern.

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Stoppen Sie den ontap_Mediator Service.

```
[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. starten Sie den ontap_Mediator Service.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Schließen Sie alle ONTAP-Cluster wieder an den aktualisierten ONTAP Mediator an

```
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::>
```

Verfahren für SnapMirror Business Continuity

Wenn Sie Ihr TLS-Zertifikat außerhalb des /opt/netapp-Verzeichnisses installiert haben, müssen Sie es für SnapMirror Business Continuity nicht erneut installieren. Wenn Sie das automatisch generierte, selbstsignierte Standardzertifikat verwenden oder Ihr benutzerdefiniertes Zertifikat im Verzeichnis /opt/netapp ablegen, sollten Sie es sichern und wiederherstellen.

```
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::>
```

Aktivieren Sie den Zugriff auf die Repositorys

Sie sollten den Zugriff auf Repositories aktivieren, damit ONTAP Mediator während des Installationsprozesses auf die benötigten 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 7.x	• rhel-7-Server-fakultative-Rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-Rpms
RHEL 9.x	• rhel-9-für-x86_64-baseos-eff • rhel-9-für-x86_64-appstream-Effektivwert
CentOS 7.x	• C7.6.1810 - Basis-Repository
Rocky Linux 8	• appstream • Baseos
Rocky Linux 9	• 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.

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 die aus `yum repolist` Befehl.

   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 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 die aus `yum repolist` Befehl.

   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 die aus `yum repolist` Befehl.

   Die neu abonnierten Repositories sollten in der Liste angezeigt werden.

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 die aus `yum repolist` Befehl.

   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 ~]#
```

Verfahren für die Betriebssysteme Rocky Linux 8 oder 9

Verwenden Sie dieses Verfahren, wenn Ihr Betriebssystem **Rocky Linux 8** oder **Rocky Linux 9** 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 ein aus `clean` Betriebliche Gründe:

   ```
   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 8 - AppStream
baseos                         Rocky Linux 8 - 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 ~]#
```

Laden Sie das Mediator-Installationspaket herunter

Laden Sie das Mediator-Installationspaket im Rahmen des Installationsprozesses herunter.

Schritte

1. Laden Sie das Mediator-Installationspaket von der ONTAP Mediator-Seite herunter.

"Download-Seite für ONTAP Mediator"

2. Vergewissern Sie sich, dass sich das Mediator-Installationspaket im aktuellen Arbeitsverzeichnis befindet:

   `ls`

   ```
   [root@mediator-host ~]#ls
   ontap-mediator-1.7.0.tgz
   ```

   > Für ONTAP Mediator Versionen 1.4 und früher wird der Name des Installationsprogramms verwendet `ontap-mediator`.

   Wenn Sie sich an einem Ort ohne Zugang zum Internet befinden, müssen Sie sicherstellen, dass der Installer Zugriff auf die erforderlichen Pakete hat.

3. Verschieben Sie bei Bedarf das Mediator-Installationspaket aus dem Download-Verzeichnis in das Installationsverzeichnis auf dem Linux Mediator-Host.
4. Entpacken Sie das Installationspaket:

   `tar xvfz ontap-mediator-1.7.0.tgz`

   ```
   [root@scs000099753 ~]# tar xvfz ontap-mediator-1.7.0.tgz
   ontap-mediator-1.7.0/
   ontap-mediator-1.7.0/ONTAP-Mediator-production.pub
   ontap-mediator-1.7.0/tsa-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/tsa-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/csc-prod-chain-ONTAP-Mediator.pem
   ontap-mediator-1.7.0/ontap-mediator-1.7.0
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.tsr
   ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig
   ```

Überprüfen Sie die ONTAP Mediator-Code-Signatur

Vor der Installation des Mediator Installationspakets sollten Sie die Signatur des ONTAP Mediator-Codes überprüfen.

Bevor Sie beginnen

Bevor Sie die Signatur des Mediator-Codes überprüfen, muss Ihr System die folgenden Anforderungen erfüllen.

- 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

Die folgenden Dateien sind im Download-Paket enthalten:

Datei	Beschreibung
`ONTAP-Mediator-development.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-1.7.0`	Die ausführbare Produktinstallation für Version 1.7.0
`ontap-mediator-1.7.0.sig`	Der SHA-256 wurde gehasht, dann RSA-signiert mit dem csc-prod-Schlüssel, Signatur für das Installationsprogramm
`ontap-mediator-1.7.0.sig.tsr`	Die Annullierungsanfrage für die Verwendung durch OCSCP für die Unterschrift des Installers
`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. Überprüfen Sie den Widerruf `csc-prod-ONTAP-Mediator.pem` Mithilfe des Online Certificate Status Protocol (OCSP).
   a. Suchen Sie die OCSP-URL, die zum Registrieren des Zertifikats verwendet wird, da Entwicklerzertifikate möglicherweise keinen uri bereitstellen.

   ```
   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`

   > Der `openssl` Version vom PFAD muss gültig sein `cert.pem` (Nicht selbstsigniert).

   ```
   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-1.6.0.sig.tsr` Und `ontap-mediator-1.7.0.tsr` Dateien, die die zugehörigen Zertifikate verwenden:

   `openssl ts -verify`

   > `.tsr` Dateien enthalten die mit dem Installationsprogramm verknüpfte Antwort auf Zeitstempel und die Codesignatur. Die Verarbeitung bestätigt, dass der Zeitstempel eine gültige Signatur von TSA hat und dass Ihre Eingabedatei nicht geändert wurde. Die Überprüfung erfolgt lokal auf Ihrem Computer. Unabhängig davon ist kein Zugriff auf TSA-Server erforderlich.

   ```
   openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
   1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
   prod-ONTAP-Mediator.pem
   openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
   1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
   ONTAP-Mediator.pem
   ```

4. Überprüfen Sie die Signaturen gegen den Schlüssel:

   `openssl -dgst -verify`

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
```

Beispiel für die Überprüfung der ONTAP Mediator-Code-Signatur (Konsolenausgabe)

```
[root@scspa2695423001 ontap-mediator-1.7.0]# pwd
/root/ontap-mediator-1.7.0
[root@scspa2695423001 ontap-mediator-1.7.0]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.7.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.7.0.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.7.0.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.7.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.7.0]#
[root@scspa2695423001 ontap-mediator-1.7.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ 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
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

```
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
        Next Update: Mar  4 04:59:59 2023 GMT
```

```
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.7.0]#
```

Installieren Sie das Installationspaket für den ONTAP Mediator

Um den ONTAP Mediator-Dienst zu installieren, müssen Sie das Installationspaket abrufen und das Installationsprogramm auf dem Host ausführen.

Schritte

1. Führen Sie das Installationsprogramm aus, und reagieren Sie auf die Eingabeaufforderungen, falls erforderlich:

   ```
   ./ontap-mediator-1.7.0/ontap-mediator-1.7.0 -y
   ```

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.5.0/ontap-mediator-1.7.0 -y
   ```

   Der Installationsprozess führt die Erstellung der erforderlichen Konten und die Installation der erforderlichen Pakete durch. Wenn auf dem Host eine frühere Version von Mediator installiert ist, werden Sie aufgefordert, zu bestätigen, dass Sie ein Upgrade durchführen möchten.

2. 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 durchführen, um den Sicherheitsschlüssel zu registrieren:

   - 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
     ```

- Suchen Sie die erforderlichen Schlüssel:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

> Nach der Installation werden die README-Dateien und der Speicherort des Schlüssels ebenfalls in der Ausgabe des Systems bereitgestellt.

Beispiel für die Installation von ONTAP Mediator 1.6 (Konsolenausgang)

```
[root@scs000099753 ~]# ./ontap-mediator-1.6.0/ontap-mediator-1.6.0 -y
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

+ 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).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode


+ Checking for default Linux firewall
success
success
success


################################################################
Preparing for installation of ONTAP Mediator packages.


+ Installing required packages.


Last metadata expiration check: 0:25:24 ago on Fri 21 Oct 2022 04:00:13
PM EDT.
Package openssl-1:1.1.1k-4.el8.x86_64 is already installed.
Package gcc-8.4.1-1.el8.x86_64 is already installed.
Package python36-3.6.8-2.module+el8.1.0+3334+5cb623d7.x86_64 is already
installed.
Package libselinux-utils-2.9-5.el8.x86_64 is already installed.
Package perl-Data-Dumper-2.167-399.el8.x86_64 is already installed.
Package efibootmgr-16-1.el8.x86_64 is already installed.
Package mokutil-1:0.3.0-11.el8.x86_64 is already installed.
```

```
Package python3-pip-9.0.3-19.el8.noarch is already installed.
Package policycoreutils-python-utils-2.9-14.el8.noarch is already
installed.
Dependencies resolved.
=========================================================================
=========================================================================
========================================
 Package                                        Architecture
Version                                                   Repository
Size
=========================================================================
=========================================================================
========================================
Installing:
 bzip2                                          x86_64
1.0.6-26.el8                                              rhel-8-for-
x86_64-baseos-rpms                       60 k
 elfutils-libelf-devel                          x86_64
0.186-1.el8                                               rhel-8-for-
x86_64-baseos-rpms                       60 k
 kernel-devel                                   x86_64
4.18.0-348.el8                                            rhel-8-for-
x86_64-baseos-rpms                       20 M
 make                                           x86_64
1:4.2.1-11.el8                                            rhel-8-for-
x86_64-baseos-rpms                      498 k
 openssl-devel                                  x86_64
1:1.1.1k-7.el8_6                                          rhel-8-for-
x86_64-baseos-rpms                      2.3 M
 patch                                          x86_64
2.7.6-11.el8                                              rhel-8-for-
x86_64-baseos-rpms                      138 k
 perl-ExtUtils-MakeMaker                        noarch
1:7.34-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                   301 k
 python36-devel                                 x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                    rhel-8-for-
x86_64-appstream-rpms                    17 k
 redhat-lsb-core                                x86_64
4.1-47.el8                                                rhel-8-for-
x86_64-appstream-rpms                    45 k
Upgrading:
 cpp                                            x86_64
8.5.0-10.1.el8_6                                          rhel-8-for-
x86_64-appstream-rpms                    10 M
 elfutils-libelf                                x86_64
```

```
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      229 k
 elfutils-libs                                  x86_64
0.186-1.el8                                                 rhel-8-for-
x86_64-baseos-rpms                      295 k
 gcc                                            x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-appstream-rpms                    23 M
 libgcc                                         x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                       80 k
 libgomp                                        x86_64
8.5.0-10.1.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      207 k
 libsemanage                                    x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      168 k
 mokutil                                        x86_64
1:0.3.0-11.el8_6.1                                          rhel-8-for-
x86_64-baseos-rpms                       46 k
 openssl                                        x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      709 k
 openssl-libs                                   x86_64
1:1.1.1k-7.el8_6                                            rhel-8-for-
x86_64-baseos-rpms                      1.5 M
 platform-python-pip                            noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-baseos-rpms                      1.6 M
 policycoreutils                                x86_64
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      374 k
 policycoreutils-python-utils                   noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      253 k
 python3-libsemanage                            x86_64
2.9-8.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      128 k
 python3-pip                                    noarch
9.0.3-22.el8                                                rhel-8-for-
x86_64-appstream-rpms                    20 k
 python3-policycoreutils                        noarch
2.9-19.el8                                                  rhel-8-for-
x86_64-baseos-rpms                      2.2 M
 python36                                       x86_64
3.6.8-38.module+el8.5.0+12207+5c5719bc                      rhel-8-for-
```

```
x86_64-appstream-rpms                    19 k
Installing dependencies:
 annobin                                         x86_64
10.29-3.el8                                               rhel-8-for-
x86_64-appstream-rpms                   117 k
 at                                              x86_64
3.1.20-11.el8                                             rhel-8-for-
x86_64-baseos-rpms                       81 k
 bc                                              x86_64
1.07.1-5.el8                                              rhel-8-for-
x86_64-baseos-rpms                      129 k
 cups-client                                     x86_64
1:2.2.6-38.el8                                            rhel-8-for-
x86_64-appstream-rpms                   169 k
 dwz                                             x86_64
0.12-10.el8                                               rhel-8-for-
x86_64-appstream-rpms                   109 k
 ed                                              x86_64
1.14.2-4.el8                                              rhel-8-for-
x86_64-baseos-rpms                       82 k
 efi-srpm-macros                                 noarch
3-3.el8                                                   rhel-8-for-
x86_64-appstream-rpms                    22 k
 esmtp                                           x86_64
1.2-15.el8                                                EPEL-8
57 k
 ghc-srpm-macros                                 noarch
1.4.2-7.el8                                               rhel-8-for-
x86_64-appstream-rpms                   9.4 k
 go-srpm-macros                                  noarch
2-17.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    13 k
 keyutils-libs-devel                             x86_64
1.5.10-6.el8                                              rhel-8-for-
x86_64-baseos-rpms                       48 k
 krb5-devel                                      x86_64
1.18.2-14.el8                                             rhel-8-for-
x86_64-baseos-rpms                      560 k
 libcom_err-devel                                x86_64
1.45.6-2.el8                                              rhel-8-for-
x86_64-baseos-rpms                       38 k
 libesmtp                                        x86_64
1.0.6-18.el8                                              EPEL-8
70 k
 libkadm5                                        x86_64
1.18.2-14.el8                                             rhel-8-for-
```

```
x86_64-baseos-rpms                      187 k
 liblockfile                                    x86_64
1.14-1.el8                                              rhel-8-for-
x86_64-appstream-rpms                    32 k
 libselinux-devel                               x86_64
2.9-5.el8                                               rhel-8-for-
x86_64-baseos-rpms                      200 k
 libsepol-devel                                 x86_64
2.9-3.el8                                               rhel-8-for-
x86_64-baseos-rpms                       87 k
 libverto-devel                                 x86_64
0.3.0-5.el8                                             rhel-8-for-
x86_64-baseos-rpms                       18 k
 m4                                             x86_64
1.4.18-7.el8                                            rhel-8-for-
x86_64-baseos-rpms                      223 k
 mailx                                          x86_64
12.5-29.el8                                             rhel-8-for-
x86_64-baseos-rpms                      257 k
 ncurses-compat-libs                            x86_64
6.1-9.20180224.el8                                      rhel-8-for-
x86_64-baseos-rpms                      328 k
 ocaml-srpm-macros                              noarch
5-4.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   9.5 k
 openblas-srpm-macros                           noarch
2-2.el8                                                 rhel-8-for-
x86_64-appstream-rpms                   8.0 k
 pcre2-devel                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      605 k
 pcre2-utf16                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      229 k
 pcre2-utf32                                    x86_64
10.32-2.el8                                             rhel-8-for-
x86_64-baseos-rpms                      220 k
 perl-CPAN-Meta-YAML                            noarch
0.018-397.el8                                           rhel-8-for-
x86_64-appstream-rpms                    34 k
 perl-ExtUtils-Command                          noarch
1:7.34-1.el8                                            rhel-8-for-
x86_64-appstream-rpms                    19 k
 perl-ExtUtils-Install                          noarch
2.14-4.el8                                              rhel-8-for-
x86_64-appstream-rpms                    46 k
```

```
 perl-ExtUtils-Manifest                          noarch
1.70-395.el8                                             rhel-8-for-
x86_64-appstream-rpms                    37 k
 perl-ExtUtils-ParseXS                           noarch
1:3.35-2.el8                                             rhel-8-for-
x86_64-appstream-rpms                    83 k
 perl-JSON-PP                                    noarch
1:2.97.001-3.el8                                         rhel-8-for-
x86_64-appstream-rpms                    68 k
 perl-Math-BigInt                                noarch
1:1.9998.11-7.el8                                        rhel-8-for-
x86_64-baseos-rpms                      196 k
 perl-Math-Complex                               noarch
1.59-421.el8                                             rhel-8-for-
x86_64-baseos-rpms                      109 k
 perl-Test-Harness                               noarch
1:3.42-1.el8                                             rhel-8-for-
x86_64-appstream-rpms                   279 k
 perl-devel                                      x86_64
4:5.26.3-419.el8_4.1                                     rhel-8-for-
x86_64-appstream-rpms                   599 k
 perl-srpm-macros                                noarch
1-25.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    11 k
 perl-version                                    x86_64
6:0.99.24-1.el8                                          rhel-8-for-
x86_64-appstream-rpms                    67 k
 platform-python-devel                           x86_64
3.6.8-41.el8                                             rhel-8-for-
x86_64-appstream-rpms                   249 k
 python-rpm-macros                               noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python-srpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    15 k
 python3-pyparsing                               noarch
2.1.10-7.el8                                             rhel-8-for-
x86_64-baseos-rpms                      142 k
 python3-rpm-generators                          noarch
5-7.el8                                                  rhel-8-for-
x86_64-appstream-rpms                    25 k
 python3-rpm-macros                              noarch
3-41.el8                                                 rhel-8-for-
x86_64-appstream-rpms                    14 k
 qt5-srpm-macros                                 noarch
```

```
5.15.2-1.el8                                                rhel-8-for-
x86_64-appstream-rpms                   11 k
 redhat-lsb-submod-security                     x86_64
4.1-47.el8                                                  rhel-8-for-
x86_64-appstream-rpms                   22 k
 redhat-rpm-config                              noarch
125-1.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   87 k
 rust-srpm-macros                               noarch
5-2.el8                                                     rhel-8-for-
x86_64-appstream-rpms                  9.3 k
 spax                                           x86_64
1.5.3-13.el8                                                rhel-8-for-
x86_64-baseos-rpms                    217 k
 systemtap-sdt-devel                            x86_64
4.6-4.el8                                                   rhel-8-for-
x86_64-appstream-rpms                   86 k
 time                                           x86_64
1.9-3.el8                                                   rhel-8-for-
x86_64-baseos-rpms                      54 k
 unzip                                          x86_64
6.0-46.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    196 k
 util-linux-user                                x86_64
2.32.1-28.el8                                               rhel-8-for-
x86_64-baseos-rpms                    100 k
 zip                                            x86_64
3.0-23.el8                                                  rhel-8-for-
x86_64-baseos-rpms                    270 k
 zlib-devel                                     x86_64
1.2.11-17.el8                                               rhel-8-for-
x86_64-baseos-rpms                      58 k
Installing weak dependencies:
 perl-CPAN-Meta                                 noarch
2.150010-396.el8                                            rhel-8-for-
x86_64-appstream-rpms                   191 k
 perl-CPAN-Meta-Requirements                    noarch
2.140-396.el8                                               rhel-8-for-
x86_64-appstream-rpms                   37 k
 perl-Encode-Locale                             noarch
1.05-10.module+el8.3.0+6498+9eecfe51                        rhel-8-for-
x86_64-appstream-rpms                   22 k
 perl-Time-HiRes                                x86_64
4:1.9758-2.el8                                              rhel-8-for-
x86_64-appstream-rpms                   61 k
```

```
Transaction Summary
================================================================================
================================================================================
==========================================
Install  69 Packages
Upgrade  17 Packages

Total download size: 72 M
Is this ok [y/N]: y
Downloading Packages:
(1/86): perl-ExtUtils-Install-2.14-4.el8.noarch.rpm
735 kB/s |  46 kB     00:00
(2/86): libesmtp-1.0.6-18.el8.x86_64.rpm
1.0 MB/s |  70 kB     00:00
(3/86): esmtp-1.2-15.el8.x86_64.rpm
747 kB/s |  57 kB     00:00
(4/86): rust-srpm-macros-5-2.el8.noarch.rpm
308 kB/s | 9.3 kB     00:00
(5/86): perl-ExtUtils-Manifest-1.70-395.el8.noarch.rpm
781 kB/s |  37 kB     00:00
(6/86): perl-CPAN-Meta-2.150010-396.el8.noarch.rpm
2.7 MB/s | 191 kB     00:00
(7/86): ocaml-srpm-macros-5-4.el8.noarch.rpm
214 kB/s | 9.5 kB     00:00
(8/86): perl-JSON-PP-2.97.001-3.el8.noarch.rpm
1.2 MB/s |  68 kB     00:00
(9/86): perl-ExtUtils-MakeMaker-7.34-1.el8.noarch.rpm
5.8 MB/s | 301 kB     00:00
(10/86): ghc-srpm-macros-1.4.2-7.el8.noarch.rpm
317 kB/s | 9.4 kB     00:00
(11/86): perl-Test-Harness-3.42-1.el8.noarch.rpm
4.5 MB/s | 279 kB     00:00
(12/86): perl-ExtUtils-Command-7.34-1.el8.noarch.rpm
520 kB/s |  19 kB     00:00

...

15 MB/s | 1.5 MB     00:00
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------------------
Total
35 MB/s |  72 MB     00:02
Running transaction check
Transaction check succeeded.
Running transaction test
```

```
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/1
  Upgrading        : openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Upgrading        : libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Running scriptlet: libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Upgrading        : elfutils-libelf-0.186-1.el8.x86_64
3/103
  Installing       : perl-version-6:0.99.24-1.el8.x86_64
4/103
  Installing       : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
5/103
  Upgrading        : libsemanage-2.9-8.el8.x86_64
6/103
  Installing       : zlib-devel-1.2.11-17.el8.x86_64
7/103
  Installing       : python-srpm-macros-3-41.el8.noarch
8/103
  Installing       : python-rpm-macros-3-41.el8.noarch
9/103
  Installing       : python3-rpm-macros-3-41.el8.noarch
10/103
  Installing       : perl-Time-HiRes-4:1.9758-2.el8.x86_64
11/103
  Installing       : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
12/103
  Installing       : perl-Test-Harness-1:3.42-1.el8.noarch
13/103
  Upgrading        : python3-libsemanage-2.9-8.el8.x86_64
14/103
  Upgrading        : policycoreutils-2.9-19.el8.x86_64
15/103
  Running scriptlet: policycoreutils-2.9-19.el8.x86_64
15/103
  Upgrading        : python3-policycoreutils-2.9-19.el8.noarch
16/103
  Installing       : dwz-0.12-10.el8.x86_64
17/103
```

```
  Installing       : ncurses-compat-libs-6.1-9.20180224.el8.x86_64
18/103
  Installing       : libesmtp-1.0.6-18.el8.x86_64
19/103
  Installing       : mailx-12.5-29.el8.x86_64
20/103
  Installing       : libkadm5-1.18.2-14.el8.x86_64
21/103
  Upgrading        : libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Running scriptlet: libgomp-8.5.0-10.1.el8_6.x86_64
22/103
  Upgrading        : platform-python-pip-9.0.3-22.el8.noarch
23/103
  Upgrading        : python3-pip-9.0.3-22.el8.noarch
24/103
  Upgrading        : python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Running scriptlet: python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
  Upgrading        : cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Running scriptlet: cpp-8.5.0-10.1.el8_6.x86_64
26/103
  Upgrading        : gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Running scriptlet: gcc-8.5.0-10.1.el8_6.x86_64
27/103
  Installing       : annobin-10.29-3.el8.x86_64
28/103
  Installing       : unzip-6.0-46.el8.x86_64
29/103
  Installing       : zip-3.0-23.el8.x86_64
30/103
  Installing       : perl-Math-Complex-1.59-421.el8.noarch
31/103
  Installing       : perl-Math-BigInt-1:1.9998.11-7.el8.noarch
32/103
  Installing       : perl-JSON-PP-1:2.97.001-3.el8.noarch
33/103
  Installing       : make-1:4.2.1-11.el8.x86_64
34/103
  Running scriptlet: make-1:4.2.1-11.el8.x86_64
34/103
```

```
  Installing       : libcom_err-devel-1.45.6-2.el8.x86_64
35/103
  Installing       : util-linux-user-2.32.1-28.el8.x86_64
36/103
  Installing       : libsepol-devel-2.9-3.el8.x86_64
37/103
  Installing       : pcre2-utf32-10.32-2.el8.x86_64
38/103
  Installing       : pcre2-utf16-10.32-2.el8.x86_64
39/103
  Installing       : pcre2-devel-10.32-2.el8.x86_64
40/103
  Installing       : libselinux-devel-2.9-5.el8.x86_64
41/103
  Installing       : patch-2.7.6-11.el8.x86_64
42/103
  Installing       : python3-pyparsing-2.1.10-7.el8.noarch
43/103
  Installing       : systemtap-sdt-devel-4.6-4.el8.x86_64
44/103
  Installing       : spax-1.5.3-13.el8.x86_64
45/103
  Running scriptlet: spax-1.5.3-13.el8.x86_64
45/103
  Installing       : m4-1.4.18-7.el8.x86_64
46/103
  Running scriptlet: m4-1.4.18-7.el8.x86_64
46/103
  Installing       : libverto-devel-0.3.0-5.el8.x86_64
47/103
  Installing       : bc-1.07.1-5.el8.x86_64
48/103
  Running scriptlet: bc-1.07.1-5.el8.x86_64
48/103
  Installing       : at-3.1.20-11.el8.x86_64
49/103
  Running scriptlet: at-3.1.20-11.el8.x86_64
49/103
  Installing       : keyutils-libs-devel-1.5.10-6.el8.x86_64
50/103
  Installing       : krb5-devel-1.18.2-14.el8.x86_64
51/103
  Installing       : time-1.9-3.el8.x86_64
52/103
  Running scriptlet: time-1.9-3.el8.x86_64
52/103
```

```
  Upgrading        : policycoreutils-python-utils-2.9-19.el8.noarch
80/103
  Installing       : elfutils-libelf-devel-0.186-1.el8.x86_64
81/103
  Upgrading        : elfutils-libs-0.186-1.el8.x86_64
82/103
  Upgrading        : mokutil-1:0.3.0-11.el8_6.1.x86_64
83/103
  Upgrading        : openssl-1:1.1.1k-7.el8_6.x86_64
84/103
  Installing       : kernel-devel-4.18.0-348.el8.x86_64
85/103
  Running scriptlet: kernel-devel-4.18.0-348.el8.x86_64

  ...

85/103
  Installing       : bzip2-1.0.6-26.el8.x86_64
86/103
  Cleanup          : policycoreutils-python-utils-2.9-14.el8.noarch
87/103
  Cleanup          : python3-policycoreutils-2.9-14.el8.noarch
88/103
  Cleanup          : python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Running scriptlet: python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
  Cleanup          : elfutils-libs-0.185-1.el8.x86_64
90/103
  Cleanup          : openssl-1:1.1.1k-4.el8.x86_64
91/103
  Cleanup          : python3-libsemanage-2.9-6.el8.x86_64
92/103
  Running scriptlet: gcc-8.4.1-1.el8.x86_64
93/103
  Cleanup          : gcc-8.4.1-1.el8.x86_64
93/103
  Running scriptlet: policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : policycoreutils-2.9-14.el8.x86_64
94/103
  Cleanup          : mokutil-1:0.3.0-11.el8.x86_64
95/103
```

```
  Cleanup          : python3-pip-9.0.3-19.el8.noarch
96/103
  Cleanup          : platform-python-pip-9.0.3-19.el8.noarch
97/103
  Cleanup          : openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Running scriptlet: openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
  Cleanup          : libsemanage-2.9-6.el8.x86_64
99/103
  Running scriptlet: cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : cpp-8.4.1-1.el8.x86_64
100/103
  Cleanup          : libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgcc-8.5.0-3.el8.x86_64
101/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : libgomp-8.4.1-1.el8.x86_64
102/103
  Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
  Cleanup          : elfutils-libelf-0.185-1.el8.x86_64
103/103
  Running scriptlet: elfutils-libelf-0.185-1.el8.x86_64
103/103
  Verifying        : esmtp-1.2-15.el8.x86_64
1/103
  Verifying        : libesmtp-1.0.6-18.el8.x86_64

  ...

Upgraded:
  cpp-8.5.0-10.1.el8_6.x86_64                              elfutils-
libelf-0.186-1.el8.x86_64     elfutils-libs-0.186-1.el8.x86_64
gcc-8.5.0-10.1.el8_6.x86_64
  libgcc-8.5.0-10.1.el8_6.x86_64                           libgomp-
8.5.0-10.1.el8_6.x86_64        libsemanage-2.9-8.el8.x86_64
mokutil-1:0.3.0-11.el8_6.1.x86_64
  openssl-1:1.1.1k-7.el8_6.x86_64                          openssl-
libs-1:1.1.1k-7.el8_6.x86_64   platform-python-pip-9.0.3-22.el8.noarch
policycoreutils-2.9-19.el8.x86_64
  policycoreutils-python-utils-2.9-19.el8.noarch           python3-
libsemanage-2.9-8.el8.x86_64   python3-pip-9.0.3-22.el8.noarch
```

```
python3-policycoreutils-2.9-19.el8.noarch
  python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
Installed:
  annobin-10.29-3.el8.x86_64                                          at-
3.1.20-11.el8.x86_64                                bc-1.07.1-5.el8.x86_64
  bzip2-1.0.6-26.el8.x86_64
cups-client-1:2.2.6-38.el8.x86_64                     dwz-0.12-
10.el8.x86_64
  ed-1.14.2-4.el8.x86_64
efi-srpm-macros-3-3.el8.noarch                        elfutils-libelf-
devel-0.186-1.el8.x86_64
  esmtp-1.2-15.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch                    go-srpm-macros-2-
17.el8.noarch
  kernel-devel-4.18.0-348.el8.x86_64
keyutils-libs-devel-1.5.10-6.el8.x86_64               krb5-devel-1.18.2-
14.el8.x86_64
  libcom_err-devel-1.45.6-2.el8.x86_64
libesmtp-1.0.6-18.el8.x86_64                          libkadm5-1.18.2-
14.el8.x86_64
  liblockfile-1.14-1.el8.x86_64
libselinux-devel-2.9-5.el8.x86_64                     libsepol-devel-2.9-
3.el8.x86_64
  libverto-devel-0.3.0-5.el8.x86_64                                   m4-
1.4.18-7.el8.x86_64                                 mailx-12.5-
29.el8.x86_64
  make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-9.20180224.el8.x86_64         ocaml-srpm-macros-
5-4.el8.noarch
  openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-7.el8_6.x86_64                 patch-2.7.6-
11.el8.x86_64
  pcre2-devel-10.32-2.el8.x86_64
pcre2-utf16-10.32-2.el8.x86_64                        pcre2-utf32-10.32-
2.el8.x86_64
  perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch      perl-CPAN-Meta-
YAML-0.018-397.el8.noarch
  perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch             perl-ExtUtils-
Install-2.14-4.el8.noarch
  perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch            perl-ExtUtils-
ParseXS-1:3.35-2.el8.noarch
  perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Math-BigInt-1:1.9998.11-7.el8.noarch             perl-Math-Complex-
```

```
1.59-421.el8.noarch
  perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64               perl-devel-
4:5.26.3-419.el8_4.1.x86_64
  perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64                 platform-python-
devel-3.6.8-41.el8.x86_64
  python-rpm-macros-3-41.el8.noarch
python-srpm-macros-3-41.el8.noarch                  python3-pyparsing-
2.1.10-7.el8.noarch
  python3-rpm-generators-5-7.el8.noarch
python3-rpm-macros-3-41.el8.noarch                  python36-devel-
3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
  qt5-srpm-macros-5.15.2-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64                   redhat-lsb-submod-
security-4.1-47.el8.x86_64
  redhat-rpm-config-125-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch                     spax-1.5.3-
13.el8.x86_64
  systemtap-sdt-devel-4.6-4.el8.x86_64
time-1.9-3.el8.x86_64                               unzip-6.0-
46.el8.x86_64
  util-linux-user-2.32.1-28.el8.x86_64
zip-3.0-23.el8.x86_64                               zlib-devel-1.2.11-
17.el8.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /tmp/ontap_mediator.JixKGP/ontap-
mediator-1.6.0/ontap-mediator-1.6.0/install_20221021155929.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20221021155929.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 reboot will be
```

```
needed.
     SCST will not start automatically when Secure Boot is enabled and
not configured properly.
+ 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@scs000099753 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.5 (Ootpa)
[root@scs000099753 ~]#
```

Überprüfen Sie die Installation

Nach der Installation des ONTAP Mediators sollten Sie überprüfen, ob die ONTAP Mediatordienste ausgeführt werden.

Schritte

1. Den Status der ONTAP Mediatordienste anzeigen:
   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 Ports, die vom ONTAP Mediator-Dienst verwendet werden:

   `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 nach der Installation

Nach der Installation und Ausführung des ONTAP Mediator-Dienstes müssen im ONTAP-Speichersystem zusätzliche Konfigurationsaufgaben ausgeführt werden, um die Mediator-Funktionen nutzen zu können:

- Informationen zur Verwendung des ONTAP Mediator-Dienstes in einer MetroCluster-IP-Konfiguration finden Sie unter "Konfigurieren des ONTAP Mediator-Dienstes aus einer MetroCluster-IP-Konfiguration".
- Informationen zur Verwendung von SnapMirror Business Continuity finden Sie unter "Installieren Sie den ONTAP Mediator Service, und bestätigen Sie die ONTAP-Clusterkonfiguration".

Konfigurieren Sie die Sicherheitsrichtlinien von ONTAP Mediator

Der ONTAP Mediatorserver unterstützt mehrere konfigurierbare Sicherheitseinstellungen. Die Standardwerte für alle Einstellungen sind in einer low_space_threshold_mib: 10read-only Datei:

`/opt/netapp/lib/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Alle Werte, die in der platziert werden `ontap_mediator.user_config.yaml` Setzt die Standardwerte außer Kraft und wird bei allen ONTAP Mediator-Upgrades beibehalten.

Nach dem Ändern von `ontap_mediator.user_config.yaml`, Starten Sie den ONTAP Mediator-Dienst neu:

```
systemctl restart ontap_mediator
```

Attribute des ONTAP Mediators ändern

Folgende Attribute können konfiguriert werden:

> Andere Standardwerte im `ontap_mediator.config.yaml` Darf nicht geändert werden.

- **Einstellungen zur Installation von SSL-Zertifikaten von Drittanbietern als Ersatz für die selbstsignierten Standardzertifikate**

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_media
tor_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'                   # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap'             # passphrase for the signed
client cert
```

- **Einstellungen, die Schutz vor Brute-Force-Passwortraten bieten**

  Um die Funktion zu aktivieren, legen Sie einen Wert für den fest `window_seconds` Und das `retry_limit`

  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
  ```

- **Felder, die die Regeln für die Passwortkomplexität des ONTAP Mediator API-Benutzerkontos steuern**

  ```
  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)
  ```

- **Einstellung, die den erforderlichen freien Speicherplatz auf dem steuert `/opt/netapp/lib/ontap_mediator` Datenträger.**

  Wenn der Platz unter dem festgelegten Schwellenwert liegt, gibt der Dienst ein Warnungsereignis aus.

  ```
  low_space_threshold_mib: 10
  ```

- **Einstellung, die RESERVE_LOG_SPACE steuert.**

  Der ONTAP Mediatorserver erstellt standardmäßig einen separaten Speicherplatz für die Protokolle. Das Installationsprogramm erstellt eine neue Datei mit fester Größe mit insgesamt 700 MB Festplattenspeicher, die explizit für Mediator Logging verwendet werden soll.

  So deaktivieren Sie diese Funktion und verwenden den Standardspeicherplatz:

  a. Ändern Sie den Wert von RESERVE_LOG_SPACE von „`1`“ in „`0`“ in der folgenden Datei:

     `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

b. Mediator neu starten:

i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

ii. `systemctl restart ontap_mediator`

Um die Funktion wieder zu aktivieren, ändern Sie den Wert von „`0`“ in „`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.

Verwalten des ONTAP Mediators Service

Nach der Installation des ONTAP Mediator-Dienstes möchten Sie möglicherweise den Benutzernamen oder das Kennwort ändern. Sie können auch den ONTAP Mediatordienst deinstallieren.

Ändern Sie den Benutzernamen

Über diese Aufgaben

Diese Aufgabe wird auf dem Linux-Host ausgeführt, auf dem der ONTAP Mediator-Dienst installiert ist.

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
```

Verfahren

Ändern Sie den Benutzernamen durch Auswahl einer der folgenden Optionen:

- Führen Sie den Befehl Mediator_change_user aus, und reagieren 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 ~]#
```

- 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

Über diese Aufgabe

Diese Aufgabe wird auf dem Linux-Host ausgeführt, auf dem der ONTAP Mediator-Dienst installiert ist.

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
```

Verfahren

Ändern Sie das Passwort, indem Sie eine der folgenden Optionen auswählen:

- Führen Sie die aus `mediator_change_password` Befolgen Sie diesen Befehl 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 ~]#
  ```

- 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 ~]#
```

Beenden Sie den ONTAP Mediator-Dienst

So beenden Sie den ONTAP Mediator-Dienst:

Schritte

1. Stoppen Sie den ONTAP Mediator.

   ```
   systemctl stop ontap_mediator
   ```

2. SCST stoppen.

   ```
   systemctl stop mediator-scst
   ```

3. Deaktivieren Sie ONTAP Mediator und SCST.

   ```
   systemctl diable ontap_mediator mediator-scst
   ```

Aktivieren Sie den ONTAP Mediator-Dienst erneut

So aktivieren Sie den ONTAP Mediator-Dienst erneut:

Schritte

1. Aktivieren Sie ONTAP Mediator und SCST.

   ```
   systemctl enable ontap_mediator mediator-scst
   ```

2. SCST starten.

   ```
   systemctl start mediator-scst
   ```

3. Starten Sie den ONTAP Mediator.

   ```
   systemctl start ontap_mediator
   ```

Überprüfen Sie, ob der ONTAP Mediator ordnungsgemäß funktioniert

Nach der Installation des ONTAP Mediators sollten Sie überprüfen, ob die ONTAP Mediatordienste ausgeführt werden.

Schritte

1. Den Status der ONTAP Mediatordienste anzeigen:

   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 Ports, die vom ONTAP Mediator-Dienst verwendet werden:

   `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 SCST manuell, um die Hostwartung durchzuführen

Um SCST zu deinstallieren, benötigen Sie das SCST tar-Paket, das für die installierte Version von ONTAP Mediator verwendet wird.

Schritte

1. Laden Sie das entsprechende SCST-Paket herunter (wie in der folgenden Tabelle gezeigt) und enttar es.

Für diese Version …	Verwenden Sie dieses tar-Bündel…
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

2. Geben Sie die folgenden Befehle im Verzeichnis „scst“ ein:
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Installieren Sie SCST manuell, um die Hostwartung durchzuführen

Um SCST manuell zu installieren, benötigen Sie das SCST tar-Paket, das für die installierte Version von ONTAP Mediator verwendet wird (siehe Tabelle oben).

1. Geben Sie die folgenden Befehle im Verzeichnis „scst“ ein:
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`
   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
   i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`
2. (Optional) Wenn Secure Boot aktiviert ist, führen Sie vor dem Neustart die folgenden Schritte aus:
   a. Bestimmen Sie jeden Dateinamen für die Module „scst_vdisk“, „scst“ und „iscsi_scst“.

      ```
      [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 Datei 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_module_key.priv \
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der \
      _module-filename_
      ```

   d. Installieren Sie den richtigen Schlüssel mit der UEFI-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. Führen Sie einen Neustart durch.

```
reboot
```

Deinstallieren Sie den ONTAP Mediator-Dienst

Bevor Sie beginnen

Bei Bedarf können Sie den ONTAP Mediator-Dienst entfernen. Der Mediator muss von ONTAP getrennt werden, bevor Sie den Mediator-Dienst entfernen.

Über diese Aufgabe

Diese Aufgabe wird auf dem Linux-Host ausgeführt, auf dem der ONTAP Mediator-Dienst installiert ist.

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 den ONTAP Mediator-Dienst:

```
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

Über diese Aufgabe

- Sie führen diese Aufgabe auf dem Linux-Host aus, auf dem der ONTAP-Mediator-Dienst installiert ist.
- 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 des ONTAP Mediators 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 den 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
   ```

OS-Host für ONTAP Mediator warten

Für eine optimale Leistung sollten Sie das Host-Betriebssystem für ONTAP Mediator regelmäßig pflegen.

Starten Sie den Host neu

Starten Sie den Host neu, wenn sich die Cluster in einem ordnungsgemäßen Zustand befinden. Während der ONTAP-Mediator offline ist, besteht die Gefahr, dass die Cluster nicht ordnungsgemäß auf Ausfälle reagieren können. Wenn ein Neustart erforderlich ist, wird ein Service-Fenster empfohlen.

ONTAP Mediator wird während eines Neustarts automatisch wieder aufgenommen und gibt die Beziehungen wieder, die zuvor mit ONTAP-Clustern konfiguriert wurden.

Updates des Host-Pakets

Alle Bibliotheken oder yum-Pakete (außer dem Kernel) können sicher aktualisiert werden, erfordern aber möglicherweise einen Neustart, um wirksam zu werden. Wenn ein Neustart erforderlich ist, wird ein Service-Fenster empfohlen.

Wenn Sie den installieren `yum-utils` Verwenden Sie die `needs-restarting` Befehl, um zu erkennen, ob eine Paketänderung einen Neustart erfordert.

Sie sollten neu starten, wenn eine der Abhängigkeiten von ONTAP Mediator aktualisiert wird, da diese nicht sofort auf laufende Prozesse wirken.

Kleinere Kernel-Upgrades für das Host-Betriebssystem

SCST muss für den verwendeten Kernel kompiliert werden. Zum Aktualisieren des Betriebssystems ist ein Wartungsfenster erforderlich.

Schritte

Führen Sie die folgenden Schritte aus, um den Kernel des Host-Betriebssystems zu aktualisieren.

1. Stoppen Sie den ONTAP Mediator
2. Deinstallieren Sie das SCST-Paket. (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 die ONTAP Mediatordienste erneut.

Host ändert sich zum Hostnamen oder IP

Über diese Aufgabe

- Sie führen diese Aufgabe auf dem Linux-Host aus, auf dem der ONTAP-Mediator-Dienst installiert ist.
- 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 des ONTAP Mediators 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 den 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
```

Managen Sie MetroCluster Standorte mit System Manager

Überblick über das Management der MetroCluster Site mit System Manager

Ab ONTAP 9.8 können Sie System Manager als vereinfachte Benutzeroberfläche zum Management einer Konfiguration einer MetroCluster Einrichtung verwenden.

Eine MetroCluster Konfiguration ermöglicht es zwei Clustern, Daten aufeinander zu spiegeln, wenn ein Cluster ausfällt, gehen die Daten nicht verloren.

In der Regel richtet ein Unternehmen die Cluster an zwei verschiedenen geografischen Standorten ein. Ein Administrator an jedem Standort richtet ein Cluster ein und konfiguriert es. Anschließend kann ein Administrator das Peering zwischen den Clustern einrichten, um Daten gemeinsam zu nutzen.

Das Unternehmen kann auch einen ONTAP Mediator an einem dritten Standort installieren. Der ONTAP Mediator Service überwacht den Status jedes Clusters. Wenn eines der Cluster erkennt, dass es nicht mit dem Partner-Cluster kommunizieren kann, fragt es den Monitor ab, um zu ermitteln, ob der Fehler ein Problem mit

dem Cluster-System oder mit der Netzwerkverbindung ist.

Wenn das Problem mit der Netzwerkverbindung besteht, führt der Systemadministrator Fehlerbehebungsmethoden durch, um den Fehler zu beheben und die Verbindung wiederherzustellen. Wenn das Partner-Cluster ausfällt, initiiert das andere Cluster einen Switchover-Prozess, um den Daten-I/O für beide Cluster zu steuern.

Sie können auch eine Umschaltung durchführen, um eines der Cluster-Systeme für eine geplante Wartung herunterzufahren. Das Partner-Cluster übernimmt alle Daten-I/O-Vorgänge für beide Cluster, bis Sie das Cluster hochfahren, für das Sie Wartungsarbeiten durchgeführt und einen Switchback-Vorgang durchführen.

Sie können folgende Vorgänge verwalten:

- "Richten Sie eine IP MetroCluster-Site ein"
- "IP-MetroCluster-Peering einrichten"
- "Konfigurieren Sie einen IP MetroCluster-Standort"
- "IP MetroCluster-Umschaltung und zurückwechseln"
- "Fehlerbehebung mit IP MetroCluster-Konfigurationen"
- "Aktualisieren Sie ONTAP auf MetroCluster Clustern"

Richten Sie eine IP MetroCluster-Site ein

Ab ONTAP 9.8 können Sie mit System Manager eine IP-Konfiguration eines MetroCluster Standorts einrichten.

Ein MetroCluster-Standort besteht aus zwei Clustern. In der Regel befinden sich die Cluster an verschiedenen geografischen Standorten.

Bevor Sie beginnen

- Das System sollte bereits installiert und entsprechend dem verkabelt sein "Installations- und Setup-Anleitung" Das kam mit dem System.
- Clusternetzwerkschnittstellen sollten auf jedem Knoten eines jeden Clusters für die Kommunikation innerhalb des Clusters konfiguriert werden.

Weisen Sie eine Node-Management-IP-Adresse zu

Windows System

Sie sollten Ihren Windows-Computer mit dem Subnetz verbinden, mit dem die Controller verbunden sind. Sie weist Ihrem System automatisch eine Node-Management-IP-Adresse zu.

Schritte

1. Öffnen Sie vom Windows-System aus das Laufwerk **Network**, um die Knoten zu erkennen.
2. Doppelklicken Sie auf den Node, um den Cluster-Setup-Assistenten zu starten.

Andere Systeme

Sie sollten die Node-Management-IP-Adresse für einen der Nodes im Cluster konfigurieren. Sie können diese Node-Management-IP-Adresse verwenden, um den Setup-Assistenten für das Cluster zu starten.

Siehe "Erstellen des Clusters auf dem ersten Node" Informationen über das Zuweisen einer Node-

Management-IP-Adresse.

Initialisieren und konfigurieren Sie den Cluster

Sie initialisieren den Cluster, indem Sie ein Administratorpasswort für das Cluster festlegen und die Cluster-Management- und Node-Managementnetzwerke einrichten. Sie können auch Dienste wie einen DNS-Server konfigurieren, um Hostnamen aufzulösen und einen NTP-Server, um Zeit zu synchronisieren.

Schritte

1. Geben Sie in einem Webbrowser die IP-Adresse für die Node-Verwaltung ein, die Sie konfiguriert haben: "https://node-management-IP"

   System Manager erkennt die im Cluster verbliebenen Nodes automatisch.

2. Führen Sie im Fenster **Storage System initialisieren** folgende Schritte durch:
   a. Geben Sie die Netzwerkkonfigurationsdaten des Cluster-Managements ein.
   b. Geben Sie die Node-Management-IP-Adressen für alle Nodes ein.
   c. Geben Sie DNS-Details (Domain Name Server) an.
   d. Aktivieren Sie im Abschnitt **andere** das Kontrollkästchen **Zeitdienst verwenden (NTP)**, um die Zeitserver hinzuzufügen.

Wenn Sie auf **Absenden** klicken, warten Sie, bis der Cluster erstellt und konfiguriert wurde. Anschließend erfolgt ein Validierungsprozess.

Nächste Schritte

Nachdem beide Cluster eingerichtet, initialisiert und konfiguriert wurden, führen Sie das folgende Verfahren aus:

- "IP-MetroCluster-Peering einrichten"

Konfigurieren Sie ONTAP auf einem neuen Cluster-Video

IP-MetroCluster-Peering einrichten

Ab ONTAP 9.8 können Sie eine IP-Konfiguration eines MetroCluster-Vorgangs mit System Manager verwalten. Nachdem Sie zwei Cluster eingerichtet haben, richten Sie Peering zwischen ihnen ein.

Bevor Sie beginnen

Sie sollten das folgende Verfahren zum Einrichten von zwei Clustern abgeschlossen haben:

- "Richten Sie eine IP MetroCluster-Site ein"

Bestimmte Schritte dieses Prozesses werden von verschiedenen Systemadministratoren an den geografischen Standorten des jeweiligen Clusters ausgeführt. Zur Erläuterung dieses Verfahrens werden die Cluster „Standort A Cluster“ und „Standort B Cluster“ genannt.

Durchführen des Peering-Prozesses von Standort A

Dieser Prozess wird von einem Systemadministrator an Standort A durchgeführt

Schritte

1. Melden Sie sich bei Site A Cluster an.
2. Wählen Sie in System Manager in der linken Navigationsleiste **Dashboard** aus, um die Clusterübersicht anzuzeigen.

   Im Dashboard werden die Details zu diesem Cluster angezeigt (Standort A). Im Abschnitt **MetroCluster** wird Standort A Cluster auf der linken Seite angezeigt.

3. Klicken Sie Auf **Partner-Cluster Anhängen**.
4. Geben Sie die Details der Netzwerkschnittstellen ein, die es den Knoten in Standort-A-Cluster

ermöglichen, mit den Knoten im Standort-B-Cluster zu kommunizieren.

5. Klicken Sie auf **Speichern und fortfahren**.
6. Wählen Sie im Fenster **Partner-Cluster anhängen** die Option **Ich habe keine Passphrase**, mit der Sie eine Passphrase generieren können.
7. Kopieren Sie die generierte Passphrase, und teilen Sie sie mit dem Systemadministrator an Standort B
8. Wählen Sie **Schließen**.

Durchführen des Peering-Prozesses von Standort B

Dieser Prozess wird von einem Systemadministrator an Standort B durchgeführt

Schritte

1. Melden Sie sich bei Standort B-Cluster an.
2. Wählen Sie in System Manager **Dashboard** aus, um die Clusterübersicht anzuzeigen.

   Das Dashboard zeigt die Details zu diesem Cluster an (Standort B). Im Abschnitt MetroCluster wird links Standort-B-Cluster angezeigt.

3. Klicken Sie auf **Attach Partner Cluster**, um den Peering-Prozess zu starten.
4. Geben Sie die Details der Netzwerkschnittstellen ein, die es den Knoten im Cluster Standort B ermöglichen, mit den Knoten in Standort A zu kommunizieren.
5. Klicken Sie auf **Speichern und fortfahren**.
6. Wählen Sie im Fenster **Partner-Cluster anhängen** die Option **Ich habe eine Passphrase** aus, mit der Sie die Passphrase eingeben können, die Sie vom Systemadministrator an Standort A erhalten haben
7. Wählen Sie **Peer**, um den Peering-Prozess abzuschließen.

Was kommt als Nächstes?

Nachdem der Peering-Prozess erfolgreich abgeschlossen wurde, konfigurieren Sie die Cluster. Siehe "Konfigurieren Sie einen IP MetroCluster-Standort".

Konfigurieren Sie einen IP MetroCluster-Standort

Ab ONTAP 9.8 können Sie eine IP-Konfiguration eines MetroCluster-Vorgangs mit System Manager verwalten. Nachdem Sie zwei Cluster eingerichtet und Peering durchgeführt haben, konfigurieren Sie jedes Cluster.

Bevor Sie beginnen

Sie sollten die folgenden Verfahren durchgeführt haben:

- "Richten Sie eine IP MetroCluster-Site ein"
- "IP-MetroCluster-Peering einrichten"

Konfigurieren Sie die Verbindung zwischen Clustern

Schritte

1. Melden Sie sich an einem der Standorte bei System Manager an, und wählen Sie **Dashboard**.

   Im Abschnitt **MetroCluster** zeigt die Grafik die beiden Cluster, die Sie für die MetroCluster-Sites

eingerichtet und angepasst haben. Das Cluster, von dem Sie arbeiten (lokales Cluster), wird auf der linken Seite angezeigt.

2. Klicken Sie auf **MetroCluster konfigurieren**. In diesem Fenster können Sie die folgenden Aufgaben ausführen:
   a. Es werden die Nodes für jedes Cluster in der MetroCluster-Konfiguration dargestellt. Wählen Sie mithilfe der Dropdown-Listen aus, welche Nodes im lokalen Cluster Disaster-Recovery-Partner sind, mit welchen Nodes im Remote-Cluster.
   b. Aktivieren Sie das Kontrollkästchen, wenn Sie einen ONTAP-Mediator-Dienst konfigurieren möchten. Siehe Konfigurieren Sie den ONTAP Mediator-Dienst.
   c. Wenn beide Cluster über eine Lizenz zur Aktivierung der Verschlüsselung verfügen, wird der Abschnitt **Verschlüsselung** angezeigt.

      Geben Sie zum Aktivieren der Verschlüsselung eine Passphrase ein.

   d. Aktivieren Sie das Kontrollkästchen, wenn Sie MetroCluster mit Shared Layer 3-Netzwerk konfigurieren möchten.

      > Die HA-Partner-Nodes und die mit den Nodes verbundenen Netzwerk-Switches müssen über eine passende Konfiguration verfügen.

3. Klicken Sie auf **Speichern**, um die MetroCluster-Sites zu konfigurieren.

   Auf dem **Dashboard** im Abschnitt **MetroCluster** zeigt die Grafik ein Häkchen auf der Verbindung zwischen den beiden Clustern an, was auf eine gesunde Verbindung hinweist.

Konfigurieren Sie den ONTAP Mediator-Dienst

Der ONTAP Mediator Service wird normalerweise an einem geografischen Standort installiert, der sich von beiden Standorten der Cluster getrennt befindet. Die Cluster kommunizieren regelmäßig mit dem Service, um anzugeben, dass sie betriebsbereit sind. Wenn eines der Cluster in der MetroCluster Konfiguration feststellt, dass die Kommunikation mit dem Partner-Cluster ausgefallen ist, wird mit dem ONTAP Mediator geprüft, ob das Partner-Cluster selbst ausgefallen ist.

Bevor Sie beginnen

Beide Cluster an den MetroCluster Standorten sollten up und Peering durchgeführt werden.

Schritte

1. Wählen Sie unter System Manager in ONTAP 9.8 die Option **Cluster > Einstellungen** aus.
2. Klicken Sie im Abschnitt **Mediator** auf ⚙.
3. Klicken Sie im Fenster **Mediator konfigurieren** auf **Hinzufügen+**.
4. Geben Sie die Konfigurationsdetails für den ONTAP Mediator ein.

   Sie können die folgenden Details eingeben, während Sie einen ONTAP Mediator mit dem System Manager konfigurieren.

   - Die IP-Adresse des Mediators.
   - Der Benutzername.
   - Das Passwort.

Verwalten Sie den Mediator mit System Manager

Mit System Manager können Sie Aufgaben zur Verwaltung des Mediators ausführen.

Über diese Aufgaben

Ab ONTAP 9.8 können Sie System Manager als vereinfachte Schnittstelle zur Verwaltung einer IP-Konfiguration mit vier Knoten eines MetroCluster-Setups verwenden. Zu diesen kann auch ein ONTAP Mediator an einem dritten Standort gehören.

Ab ONTAP 9.14.1 können Sie die folgenden Vorgänge auch für eine IP-Konfiguration mit acht Nodes an einem MetroCluster Standort mit System Manager ausführen. Sie können zwar kein System mit acht Nodes mit System Manager einrichten oder erweitern, aber wenn Sie bereits ein IP MetroCluster-System mit acht Nodes eingerichtet haben, können diese Vorgänge trotzdem ausgeführt werden.

Führen Sie die folgenden Aufgaben aus, um den Mediator zu verwalten.

Aufgabe durchführen…	Ergreifen Sie diese Maßnahmen…
Konfigurieren Sie den Mediator-Dienst	Führen Sie die Schritte unter aus "Konfigurieren Sie den ONTAP Mediator-Dienst".
Aktivieren oder Deaktivieren der Mediator-gestützten automatischen Umschaltung (MAUSO)	1. Klicken Sie in System Manager auf **Dashboard**. 2. Blättern Sie zum Abschnitt „MetroCluster“. 3. Klicken Sie Auf ⋮ Neben dem Namen der MetroCluster-Site. 4. Wählen Sie **Enable** oder **Disable**. 5. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie dann auf **enable** oder **Disable**. ⓘ Sie können den Mediator aktivieren oder deaktivieren, wenn er erreicht werden kann und sich beide Standorte im Modus „`normal`“ befinden. Der Mediator ist weiterhin erreichbar, wenn MAUSO aktiviert oder deaktiviert ist, wenn das MetroCluster-System in einem ordnungsgemäßen Zustand ist.
Entfernen Sie den Mediator aus der MetroCluster-Konfiguration	1. Klicken Sie in System Manager auf **Dashboard**. 2. Blättern Sie zum Abschnitt „MetroCluster“. 3. Klicken Sie Auf ⋮ Neben dem Namen der MetroCluster-Site. 4. Wählen Sie **Mediator Entfernen**. 5. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie dann auf **Entfernen**.
Überprüfen Sie den Zustand des Mediators	Führen Sie die Schritte unter aus "Fehlerbehebung mit IP MetroCluster-Konfigurationen".
Durchführen einer Umschaltung und eines Switchback	Führen Sie die Schritte unter aus "IP MetroCluster-Umschaltung und zurückwechseln".

IP MetroCluster-Umschaltung und zurückwechseln

Sie können die Steuerung von einem IP MetroCluster-Standort zur anderen umschalten, um Wartungsarbeiten durchzuführen oder ein Problem wiederherzustellen.

> Umschalterungs- und Umschaltvorgänge werden nur für IP MetroCluster-Konfigurationen unterstützt.

Überblick über Umschaltung und zurückwechseln

Eine Umschaltung kann in zwei Fällen erfolgen:

- **Eine geplante Umschaltung**

  Diese Umschaltung wird von einem Systemadministrator über System Manager initiiert. Mit der geplanten Umschaltung kann ein Systemadministrator eines lokalen Clusters die Kontrolle wechseln, sodass die Datenservices des Remote-Clusters vom lokalen Cluster übernommen werden. Anschließend kann ein Systemadministrator am Remote-Cluster-Standort Wartungsarbeiten am Remote-Cluster durchführen.

- **Eine ungeplante Umschaltung**

  Wenn ein MetroCluster Cluster ausfällt oder die Verbindungen zwischen den Clustern ausfällt, initiiert ONTAP automatisch ein Switchover-Verfahren, sodass das Cluster, das noch läuft, die Datenhandhabungsaufgaben des down-Clusters übernimmt.

  Wenn ONTAP den Status eines der Cluster nicht bestimmen kann, leitet der Systemadministrator des Standorts, der gerade arbeitet, das Switchover-Verfahren ein, um die Verantwortlichkeiten für die Datenhandhabung des anderen Standorts zu kontrollieren.

Bei jedem Switch-Verfahren wird die Datenpflege mithilfe eines *switchback*-Prozesses an das Cluster zurückgegeben.

Für ONTAP 9.7 und 9.8 führen Sie verschiedene Switchover- und Switchback-Prozesse durch:

- Verwenden Sie in ONTAP 9.7 System Manager zum Umschalten und zurückwechseln
- Verwenden Sie in ONTAP 9.8 System Manager zum Umschalten und zurückwechseln

Verwenden Sie in ONTAP 9.7 System Manager zum Umschalten und zurückwechseln

Schritte

1. Melden Sie sich unter ONTAP 9.7 bei System Manager an.
2. Klicken Sie auf **(Zurück zur klassischen Version)**.
3. Klicken Sie auf **Konfiguration > MetroCluster**.

   System Manager überprüft, ob eine ausgehandelte Umschaltung möglich ist.

4. Führen Sie einen der folgenden Teilschritte durch, wenn der Validierungsprozess abgeschlossen ist:
   a. Wenn die Validierung fehlschlägt, Standort B jedoch aktiv ist, ist ein Fehler aufgetreten. Beispielsweise könnte ein Problem mit einem Subsystem auftreten, oder NVRAM-Spiegelung wird unter Umständen nicht synchronisiert.
      i. Beheben Sie das Problem, das den Fehler verursacht, klicken Sie auf **Schließen** und starten Sie

dann erneut bei Schritt 2.

ii. Stoppen Sie die Knoten Standort B, klicken Sie auf **Schließen** und führen Sie die Schritte unter aus "Durchführung einer ungeplanten Umschaltung".

b. Wenn die Validierung fehlschlägt und Standort B nicht verfügbar ist, liegt wahrscheinlich ein Verbindungsproblem vor. Überprüfen Sie, ob Standort B wirklich ausgefallen ist, und führen Sie die Schritte unter aus "Durchführung einer ungeplanten Umschaltung".

5. Klicken Sie auf **Umschaltung von Standort B zu Standort A**, um den Switchover-Prozess zu starten.
6. Klicken Sie auf **Wechseln Sie zum neuen Erlebnis**.

Verwenden Sie in ONTAP 9.8 System Manager zum Umschalten und zurückwechseln

Geplante Umschaltung durchführen (ONTAP 9.8)

Schritte

1. Melden Sie sich unter ONTAP 9.8 bei System Manager an.
2. Wählen Sie **Dashboard**. Im Abschnitt **MetroCluster** werden die beiden Cluster mit einer Verbindung angezeigt.
3. Klicken Sie im lokalen Cluster (links dargestellt) auf ⋮, Und wählen Sie **Umschalten Remote-Datendienste zum lokalen Standort**.

   Nach der Validierung der Switchover-Anfrage wird die Kontrolle vom Remote-Standort an den lokalen Standort übertragen, sodass Datenservice-Anfragen für beide Cluster durchgeführt werden.

   Das Remote Cluster wird neu gebootet, die Storage-Komponenten sind jedoch nicht aktiv, und das Cluster verarbeitet keine Datenanfragen. Es steht nun für die geplante Wartung zur Verfügung.

> Das Remote-Cluster sollte erst für die Datenpflege verwendet werden, wenn Sie einen Switchback durchführen.

Ungeplante Umschaltung durchführen (ONTAP 9.8)

Eine ungeplante Umschaltung kann automatisch von ONTAP initiiert werden. Wenn ONTAP nicht feststellen kann, ob ein Switchback erforderlich ist, so initiiert der Systemadministrator des noch aktiven MetroCluster Standorts die Umschaltung mit folgenden Schritten:

Schritte

1. Melden Sie sich unter ONTAP 9.8 bei System Manager an.
2. Wählen Sie **Dashboard**.

   Im Abschnitt **MetroCluster** wird die Verbindung zwischen den beiden Clustern mit einem "X" angezeigt, was bedeutet, dass eine Verbindung nicht erkannt werden kann. Die Verbindungen oder das Cluster ist ausgefallen.

3. Klicken Sie im lokalen Cluster (links dargestellt) auf ⋮, Und wählen Sie **Umschalten Remote-Datendienste zum lokalen Standort**.

   Falls die Umschaltung mit einem Fehler fehlschlägt, klicken Sie auf den Link „View Details“ in der Fehlermeldung und bestätigen Sie die ungeplante Umschaltung.

   Nach der Validierung der Switchover-Anfrage wird die Kontrolle vom Remote-Standort an den lokalen

Standort übertragen, sodass Datenservice-Anfragen für beide Cluster durchgeführt werden.

Das Cluster muss repariert werden, bevor es wieder online geschaltet wird.

> Nachdem das Remote-Cluster wieder online geschaltet wurde, sollte es erst für die Datenpflege verwendet werden, wenn Sie einen Switchback durchführen.

Zurückwechseln (ONTAP 9.8)

Bevor Sie beginnen

Ob das Remote Cluster aufgrund geplanter Wartungsarbeiten oder aufgrund eines Notfalls ausgefallen ist, sollte es nun betriebsbereit sein und auf den Switchback gewartet werden.

Schritte

1. Melden Sie sich beim lokalen Cluster bei System Manager in ONTAP 9.8 an.
2. Wählen Sie **Dashboard**.

   Im Abschnitt **MetroCluster** werden die beiden Cluster angezeigt.

3. Klicken Sie im lokalen Cluster (links dargestellt) auf ⋮, Und wählen Sie **Rücknehmen Kontrolle**.

   Die Daten werden zuerst *geheilt*, um sicherzustellen, dass die Daten zwischen beiden Clustern synchronisiert und gespiegelt werden.

4. Wenn die Datenheilung abgeschlossen ist, klicken Sie auf ⋮, Und wählen Sie **Umschalttack initiieren**.

   Nach Abschluss der zurückschalttaFunktionen sind beide Cluster aktiv und warten Datenanfragen. Außerdem werden die Daten zwischen den Clustern gespiegelt und synchronisiert.

Adresse, Netmask und Gateway in einer MetroCluster-IP ändern

Ab ONTAP 9.10.1 können Sie die folgenden Eigenschaften einer MetroCluster IP-Schnittstelle ändern: IP-Adresse und -Maske sowie Gateway. Sie können jede beliebige Kombination von Parametern zum Aktualisieren verwenden.

Möglicherweise müssen Sie diese Eigenschaften aktualisieren, z. B. wenn eine doppelte IP-Adresse erkannt wird oder wenn ein Gateway aufgrund von Änderungen der Routerkonfiguration im Fall eines Layer 3-Netzwerks geändert werden muss. Sie können jeweils nur eine Schnittstelle ändern. Es wird eine Verkehrsunterbrechung auf dieser Schnittstelle geben, bis die anderen Schnittstellen aktualisiert und Verbindungen wiederhergestellt sind.

> Sie müssen die Änderungen an jedem Port vornehmen. Auf ähnliche Weise müssen Netzwerk-Switches auch ihre Konfiguration aktualisieren. Wenn das Gateway beispielsweise aktualisiert wird, wird idealerweise auf beiden Knoten eines HA-Paares geändert, da sie identisch sind. Außerdem muss der mit diesen Nodes verbundene Switch auch sein Gateway aktualisieren.

Schritt

Aktualisieren Sie die IP-Adresse, die Netmask und das Gateway für jeden Node und jede Schnittstelle.

Fehlerbehebung mit IP MetroCluster-Konfigurationen

Ab ONTAP 9.8 überwacht System Manager den Systemzustand der IP MetroCluster-Konfigurationen und unterstützt Sie dabei, eventuell auftretende Probleme zu identifizieren und zu beheben.

Überblick über den MetroCluster Health Check

System Manager überprüft regelmäßig den Zustand Ihrer IP MetroCluster-Konfiguration. Wenn Sie den Abschnitt „MetroCluster“ auf dem Dashboard anzeigen, wird in der Regel die Meldung „MetroCluster-Systeme sind ordnungsgemäß“ ausgegeben.

Wenn jedoch ein Problem auftritt, wird in der Meldung die Anzahl der Ereignisse angezeigt. Sie können auf diese Meldung klicken und die Ergebnisse der Integritätsprüfung für die folgenden Komponenten anzeigen:

- Knoten
- Netzwerkschnittstelle
- Ebene (Storage)
- Cluster
- Verbindung
- Datenmenge
- Konfigurationsreplizierung

In der Spalte **Status** werden die Komponenten mit Problemen identifiziert, und in der Spalte **Details** wird erläutert, wie das Problem behoben werden kann.

MetroCluster Fehlerbehebung

Schritte

1. Wählen Sie in System Manager **Dashboard** aus.
2. Beachten Sie im Abschnitt **MetroCluster** die Meldung.
   a. Wenn die Meldung angibt, dass Ihre MetroCluster-Konfiguration ordnungsgemäß ist und die Verbindungen zwischen den Clustern und dem ONTAP Mediator in einem ordnungsgemäßen Zustand sind (siehe Häkchen), können Sie keine Probleme beheben.
   b. Wenn die Meldung die Anzahl der Ereignisse auflistet oder die Verbindungen (mit einem „X“ angezeigt) abwärts gegangen sind, fahren Sie mit dem nächsten Schritt fort.
3. Klicken Sie auf die Nachricht, die die Anzahl der Ereignisse anzeigt.

   Der MetroCluster-Integritätsbericht wird angezeigt.
4. Beheben Sie die im Bericht angezeigten Probleme mithilfe der Vorschläge in der Spalte **Details**.
5. Wenn alle Probleme behoben wurden, klicken Sie auf **MetroCluster-Zustand prüfen**.

   > Der MetroCluster Systemintegritätscheck verwendet intensive Ressourcen. Daher empfiehlt es sich, alle Fehlerbehebungsaufgaben auszuführen, bevor Sie die Prüfung durchführen.

   Die MetroCluster-Integritätsprüfung wird im Hintergrund ausgeführt. Sie können andere Aufgaben bearbeiten, während Sie warten, bis der Vorgang abgeschlossen ist.

Datensicherung mithilfe von Tape Backup

Tape Backup der FlexVol Volumes: Überblick

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-Kopie-basiertes Backup, in dem Ihre Dateisystem-Daten 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 auf Snapshot Kopien basierende 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-Backups mit SMTape SnapMirror Business Continuity.

Workflow für Tape-Backup und -Wiederherstellung

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 der ändern `system services ndmp modify` Befehl und auf SVM-Ebene mit dem `vserver services ndmp modify` Befehl. Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages.

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 die Wahl einer Tape-Backup-Engine

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

Managen von Bandlaufwerken – Übersicht

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.

Befehle für das Management 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.
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`

Ihr Ziel ist	Befehl
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 das verwenden `-v` Option, 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.

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages.

Verwenden Sie ein nicht qualifiziertes Bandlaufwerk

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 sich die nicht qualifizierten Bandlaufwerke an, die mit dem an ein Storage-System angeschlossen sind `storage tape show-supported-status` Befehl.

   Mit dem folgenden Befehl werden Bandlaufwerke angezeigt, die an das Speichersystem angeschlossen sind, sowie der Support und Qualifikationsstatus der einzelnen Bandlaufwerke. Darüber hinaus sind die

nicht qualifizierten Bandlaufwerke aufgeführt. `tape_drive_vendor_name` Es handelt sich um ein nicht qualifiziertes Bandlaufwerk, das an das Storage-System angeschlossen ist, jedoch 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

Zuweisen von Bandaliasen

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 mit dem einen Alias einem Bandlaufwerk oder einem Mittelwechsler zu `storage tape alias set` Befehl.

   Weitere Informationen zu diesem Befehl finden Sie in den man-Pages.

   Sie können die Seriennummern (SN) Informationen zu den Bandlaufwerken anzeigen, indem Sie die verwenden `system node hardware tape drive show` Führen Sie den Befehl und die Bandbibliotheken mithilfe von aus `system node hardware tape library show` Befehle.

   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

Entfernen Sie die Bandaliase

Sie können Aliase mithilfe des entfernen `storage tape alias clear` Befehl, wenn persistente Aliase für ein Bandlaufwerk oder einen Mediumwechsler nicht mehr erforderlich sind.

Schritte

1. Entfernen Sie mit dem einen Alias von einem Bandlaufwerk oder Mittelwechsler `storage tape alias clear` Befehl.

   Weitere Informationen zu diesem Befehl finden Sie in den man-Pages.

   Mit dem folgenden Befehl werden die Aliase aller Bandlaufwerke entfernt, indem der Umfang des Alias-Clear-Vorgangs 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

Aktivieren oder Deaktivieren von Bandreservierungen

Sie können steuern, wie ONTAP Reservierungen für Bandgeräte mit dem verwaltet `tape.reservations` Option. 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 persistente SCSI-Reservierungen aus.

   `off` Deaktiviert Bandreservierungen.

Verwandte Informationen

Welche Tape-Reservierungen sind

Befehle für das Überprüfen von Tape Library-Verbindungen

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`

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages.

Allgemeines zu Bandlaufwerken

Überblick über qualifizierte 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 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 gemeldeten Lieferanten-ID `SCSI Inquiry` Befehl.
`product_id`(Zeichenfolge)	Bis zu 16 Byte	Die Produkt-ID wie vom gemeldet `SCSI Inquiry` Befehl.

Element	Größe	Beschreibung
`id_match_size`(Anzahl)		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 mit dem vom Befehl angezeigten String angegeben. `storage tape show -device -names`; Andernfalls wird INQ_VENDOR_ID angezeigt.
`product_pretty`(Zeichenfolge)	Bis zu 16 Byte	Wenn dieser Parameter vorhanden ist, wird er mit dem vom Befehl angezeigten String angegeben. `storage tape show -device -names`; Andernfalls wird INQ_PRODUCT_ID angezeigt.

Der `vendor_pretty` Und `product_pretty` Felder 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 Density Code und der Komprimierungsalgorithmus für die verschiedenen Komprimierungsarten wie erläutert `l`, `m`, `h`, und `a`:

Element	Größe	Beschreibung
`{l	m	h
a}_description=(string)`	Bis zu 24 Byte	Die Zeichenkette, die für den Befehl nodeshell gedruckt werden soll, `sysconfig -t`, Das beschreibt Eigenschaften der besonderen Dichte Einstellung.
`{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

Element	Größe	Beschreibung
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 festgelegt `yes` Wenn das Bandlaufwerk über eine automatische Ladefunktion verfügt, d. h. nach dem Einsetzen der Bandkassette, wird das Bandlaufwerk bereit, ohne dass ein ausgeführt werden muss `SCSI load` (Start/STOP-Einheit), Befehl. Die Standardeinstellung für dieses Feld ist `no`.
`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"

Wie das Storage-System ein neues 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

Übersicht über 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 für Bandgerätenamen

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 Rückwind-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 Drive-spezifischer Code für die Dichte von Daten auf dem Band und den Komprimierungstyp.

In der folgenden Liste werden die verschiedenen Werte für beschrieben `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 simultaner 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.

Welche physischen Pfadnamen sind

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 direkt angeschlossenen Geräten verwenden das folgende Format: `host_adapter.device_id_lun`

> Der LUN-Wert wird nur für Band- und Mittelwechsler angezeigt, deren LUN-Werte nicht null sind. Das heißt, wenn der LUN-Wert null ist `lun` Ein Teil des PPN wird 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-Attached-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.

Um welche Seriennummern handelt es sich

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 SN eines Bandgeräts verwendet das folgende Format: `SN[xxxxxxxxxx]L[X]`

`x` Ist ein alphanumerisches Zeichen und `Lx` Ist die LUN des Bandgeräts. Wenn die LUN 0 ist, lautet `Lx` Ein Teil der Zeichenfolge wird nicht angezeigt.

Jede SN besteht aus bis zu 32 Zeichen; das Format für die SN ist nicht Groß-/Kleinschreibung.

Überlegungen bei der Konfiguration von Multipath Tape-Zugriffen

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
```

Weitere Informationen finden Sie auf den man-Pages.

So fügen Sie den Storage-Systemen Bandlaufwerke und Bibliotheken hinzu

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.

Welche Tape-Reservierungen sind

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.

Übertragen von Daten mit NDMPcopy

Übertragen Sie die Daten mit NDMPcopy Übersicht

Der `ndmpcopy` Der nodeshell Befehl 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 laufen `ndmpcopy` In der nodeshell Befehlszeile der Quell- und Ziel-Speichersysteme oder ein Speichersystem, das weder die Quelle noch das Ziel des Datentransfers ist. Sie können auch ausführen `ndmpcopy` Auf einem einzelnen Storage-System, das sowohl die Quelle als auch das Ziel des Datentransfers ist.

Sie können IPv4- oder IPv6-Adressen der Quell- und Zielspeichersysteme im verwenden `ndmpcopy` Befehl. Das Pfadformat lautet `/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 Administrator-SVM lautet das Benutzerkonto `admin` Und die Benutzerrolle lautet `admin` Oder `backup`. In der Daten-SVM lautet das Benutzerkonto `vsadmin` Und die Benutzerrolle lautet `vsadmin` Oder `vsadmin-backup` Rolle:
Node-Scoped NDMP-Modus	`system services ndmp on`

2. Übertragen von Daten innerhalb eines Storage-Systems oder zwischen Storage-Systemen mithilfe von `ndmpcopy` Befehl im 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 legt den Adressmodus für Steuerverbindungen wie folgt fest:
     - Der Adressmodus für die Steuerverbindung entspricht der angegebenen IP-Adresse.
     - Sie können diese Regeln mit der überschreiben `-mcs` Und `-mcd` Optionen:
   - 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 zur granularen Ebene von Volume, qtree, Verzeichnis oder Datei.
   - `-mcs` Gibt den bevorzugten Adressierungmodus für die Steuerverbindung zum Quell-Speichersystem an.

`inet` Zeigt den IPv4-Adressmodus und an `inet6` Zeigt einen IPv6-Adressmodus an.

- `-mcd` Gibt den bevorzugten Adressierungmodus für die Steuerverbindung zum Zielspeichersystem an.

  `inet` Zeigt den IPv4-Adressmodus und an `inet6` Zeigt einen IPv6-Adressmodus an.

- `-md` Gibt den bevorzugten Adressierungmodus für Datentransfers zwischen Quell- und Zielspeichersystemen an.

  `inet` Zeigt den IPv4-Adressmodus und an `inet6` Zeigt einen IPv6-Adressmodus an.

  Wenn Sie den nicht verwenden `-md` Wählen Sie im `ndmpcopy` Befehl, der Adressierungmodus für die Datenverbindung wird wie folgt bestimmt:

  - Wenn eine der für die Steuerverbindungen angegebenen Adressen eine IPv6-Adresse ist, ist der Adressmodus für die Datenverbindung IPv6.
  - Wenn die für die Steuerverbindungen angegebenen beiden Adressen IPv4-Adressen sind, liefert das `ndmpcopy` Befehl versucht zunächst einen IPv6-Adressmodus für die Datenverbindung.

    Wenn dies fehlschlägt, verwendet der Befehl einen IPv4-Adressmodus.

    > Eine IPv6-Adresse, falls angegeben, muss in eckigen Klammern eingeschlossen sein.

    Mit diesem Beispielbefehl werden Daten von einem Quellpfad migriert (`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>
```

Optionen für den Befehl ndmpcopy

Sie sollten die für das verfügbaren Optionen verstehen `ndmpcopy` Nodeshell Befehl, um erfolgreich Daten zu übertragen.

In der folgenden Tabelle sind die verfügbaren Optionen aufgeführt. Weitere Informationen finden Sie im `ndmpcopy` Man-Pages durch die nodeshell.

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`}
Mit dieser Option wird der Typ der Quellauthentifizierung festgelegt, der verwendet werden soll, wenn eine Verbindung zum Quellspeichersystem hergestellt wird.Dies ist eine obligatorische Option und daher sollte der Benutzer entweder die bereitstellen `text` Oder `md5` Option.	`-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-Ebene auf den angegebenen Wert von Level festgelegt.gültige Werte sind `0`, `1`, An `9`, Wo `0` Zeigt eine vollständige Übertragung und an `1` Bis `9` Gibt eine inkrementelle Übertragung an. Die Standardeinstellung lautet `0`.
`-d`	Diese Option ermöglicht die Erstellung von NDMPcopy Debug-Protokollmeldungen. Die Debug-Log-Dateien für die NDMPcopy befinden sich im `/mroot/etc/log` Root-Volume: Die Namen der ndmpcopy Debug-Log-Datei befinden sich im `ndmpcopy.yyyymmdd` Formatieren.
`-f`	Diese Option aktiviert den erzwungenen Modus. In diesem Modus können Systemdateien im überschrieben werden `/etc` Verzeichnis im Root-Verzeichnis des 7-Mode Volumes.

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 Passwort überschreibt das für angegebene Passwort `-sa` Und `-da` Optionen: 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 sein, z. B. **`.pst`** `Oder .txt.`

NDMP für FlexVol Volumes

Über NDMP für 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

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.

Verwandte Informationen

Befehle für die Verwaltung des NDMP-Modus mit Node-Umfang

Verwalten des NDMP-Modus mit Node-Umfang für FlexVol Volumes

Verwalten des SVM-Scoped NDMP-Modus für FlexVol Volumes

Welcher Node-Scoped NDMP-Modus ist

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.

Verwandte Informationen

Verwalten des NDMP-Modus mit Node-Umfang für FlexVol Volumes

Welcher SVM-Scoped NDMP-Modus ist

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

Verwalten des SVM-Scoped NDMP-Modus für FlexVol Volumes

Überlegungen bei der Verwendung von NDMP

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, einer Datei oder der Snapshot Kopie 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

"ONTAP-Konzepte"

"Systemadministration"

Umgebungsvariable

Übersicht über Umgebungsvariablen

Umgebungsvariablen dienen der Kommunikation von Informationen zu Backup- oder Wiederherstellungsvorgang zwischen einer NDMP-fähigen Backup-Applikation und einem Storage-System.

Beispiel: Wenn ein Benutzer angibt, dass eine Sicherungsanwendung gesichert werden soll `/vserver1/vol1/dir1`, Die Backup-Anwendung setzt die DATEISYSTEM-Umgebung Variable 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

Umgebungsvariablen dienen der Kommunikation von Informationen zu Backup- oder Wiederherstellungsvorgang zwischen einer NDMP-fähigen Backup-Applikation und einem Storage-System. ONTAP unterstützt Umgebungsvariablen, die einen zugeordneten Standardwert haben. Sie können diese Standardwerte jedoch manuell ändern.

Wenn Sie die von der Backup-Anwendung festgelegten Werte manuell ändern, verhält sich die Anwendung möglicherweise unvorhersehbar. Das liegt daran, dass die Backup- oder Restore-Vorgänge das tun, was die Backup-Applikation erwartet. Aber in einigen Fällen kann eine vernünftige Änderung helfen, Probleme zu

identifizieren 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 haben Variablen, die den Wert haben, `Y` Akzeptieren Sie auch `T` Und `N` Akzeptieren Sie auch `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.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
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.
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 Wiederherstellungsvorgan g 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 eingestellt auf `-1`, Der BASE_DATE-Inkremental-Spezifikator ist deaktiviert. Wenn eingestellt auf `0` Bei Backups auf Ebene 0 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 festgelegt ist `Y`, Die Backup-Anwendung gibt 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 vom Backup erstellt, wenn die VARIABLE BASE_DATE auf einen anderen Wert als gesetzt wird `-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). • Der `ndmpd.offset_map.enable` Die Option ist auf festgelegt `on`. • DIE VARIABLE ENHANCED_DAR_ENABLED ist auf festgelegt `Y` Während des Wiederherstellens.

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. Einstellung dieser Variable auf `Y` Bewirkt, dass der Wiederherstellungsvorgang die Prüfungen auf Volume-Speicherplatz und Inode-Verfügbarkeit auf dem Zielpfad überspringen kann. 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 HIST-Variable auf `Y`. Wenn Sie die Geschwindigkeit eines Backup-Vorgangs erhöhen oder ein Problem mit der Dateihistorie-Sammlung beheben möchten, können Sie diese Variable auf einstellen `N`. Sie sollten die HIST-Variable 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. Der `IGNORE_CTIME` Variable sollte nur angegeben werden, wenn inkrementelle Backups nicht genügend Zeit oder Speicherplatz beanspruchen, da der ctime-Wert geändert wurde. Der `NDMP dump` Befehlssätze `IGNORE_CTIME` Bis `false` Standardmäßig. Einstellen auf `true` Kann zu folgenden Datenverlusten führen: 1. Wenn `IGNORE_CTIME` Ist für eine inkrementelle Volume-Ebene

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.

n von Dateien, die während des inkrementellen Restores über qtrees auf die Quelle verschoben werden.

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 eingestellt auf `Y`, Objekte in qtrees im Datensatz, die von DER DATEISYSTEMVARIABLE angegeben sind, werden 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 NICHT_QUOTA_TREE auf setzen `Y` Gleichzeitig.

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 Umgebungsvariablen_DAR_ENABLED müssen aktiviert sein (auf festgelegt) `Y`) Auch. Wenn die REKURSIVE Variable deaktiviert ist (auf gesetzt `N`), nur die Berechtigungen und ACLs für alle Verzeichnisse im ursprünglichen Quellpfad werden von Band, nicht der Inhalt der Verzeichnisse wiederhergestellt. Wenn die REKURSIVE Variable auf festgelegt ist `N` Oder die Variable „RECOVER_FULL_PATHS“ ist auf festgelegt `Y`, Der Wiederherstellungspfad muss 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 muss aktiviert sein (auf eingestellt) `Y`) Auch. Wenn RECOVERY_FULL_PATHS auf festgelegt ist `Y`, Der Wiederherstellungspfad muss 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

Recovery-Pfade, da alle Recovery-Pfade innerhalb von vorhanden sind `foo/dir1/deepdir/myfile`:

- `/foo`
- `/foo/dir`
- `/foo/dir1/deepdir`
- `/foo/dir1/deepdir/myfile`

Die folgenden sind ungültige Recovery-Pfade:

- `/foo`

  `/foo/dir`

  `/foo/dir1/myfile`

Umgebungsvariable	Gültige Werte	Standard	Beschreibung

BASE_DATE	`DUMP_DATE`	`-1`	Gibt das Startdatum für inkrementelle Backups an.
			
			`` `BASE_DATE` Ist eine String-Darstellung der Snapshot Referenzkennungen. Verwenden der `BASE_DATE` Zeichenfolge, SMTape lokalisiert die Referenz-Snapshot Kopie. ``
			
			`` `BASE_DATE` Ist nicht für Basis-Backups erforderlich. Für ein inkrementelles Backup, der Wert des `DUMP_DATE` Die Variable aus dem vorherigen Basisplan oder dem inkrementellen Backup wird dem zugewiesen `BASE_DATE` Variabel. ``
			
			Die Backup-Anwendung weist den zu `DUMP_DATE` Mehrwert aus einer früheren SMTape-Basis oder einem inkrementellen Backup

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
DUMP_DATE	`return_value`	`none`	AM Ende eines SMTape Backups enthält DUMP_DATE eine String-Kennung, die die für das Backup verwendete Snapshot Kopie identifiziert. Diese Snapshot Kopie kann als Referenz-Snapshot für ein nachfolgender, inkrementeller Backup verwendet werden. Der resultierende Wert von DUMP_DATE wird als BASE_DATE-Wert für nachfolgende inkrementelle Backups verwendet.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifiziert die 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 als Eingabe an das zu `SMTAPE_BACKUP_SET_ID` Variable während eines inkrementellen Backups.

Umgebungsvariable	Gültige Werte	Standard	Beschreibung
SMTAPE_SNAPSHOT_NAME	Alle gültigen Snapshot Kopien, die im Volume verfügbar sind	`Invalid`	Wenn die Variable SMTAPE_SNAPSHOT_NAME auf eine Snapshot Kopie festgelegt ist, werden diese Snapshot Kopie und ihre älteren Snapshot Kopien auf Tape gesichert. Für inkrementelle Backups legt diese Variable die inkrementelle Snapshot Kopie fest. Die Variable „BASE_DATE“ stellt die Basis-Snapshot Kopie bereit.
SMTAPE_DELETE_SNAPSHOT	`Y` Oder `N`	`N`	Wenn die Variable SMTAPE_DELETE_SNAPSHOT auf festgelegt ist, wird für eine automatisch von SMTape erstellte Snapshot Kopie ausgewählt `Y`, Dann löscht SMTape nach Abschluss des Backup-Vorgangs diese Snapshot Kopie. Eine von der Backup-Applikation erstellte Snapshot Kopie wird jedoch nicht gelöscht.
SMTAPE_BREAK_MIRROR	`Y` Oder `N`	`N`	Wenn die Variable SMTAPE_BREAK_MIRROR auf festgelegt ist `Y`, Das Volumen des Typs `DP` Wird in A geändert `RW` Volume nach einem erfolgreichen Restore wiederherstellen.

Gängige NDMP Tape-Backup-Topologien

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.

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.

  Der `NDMP_SNAP_RECOVER` Nachricht, die Teil der Snapshot Management Extensions ist, wird verwendet, um eine Wiederherstellung zu starten und die wiederhergestellten Daten von einer lokalen Snapshot-Kopie zu einem lokalen Dateisystem-Speicherort zu übertragen. In ONTAP ermöglicht diese Meldung die Wiederherstellung von Volumes und regulären Dateien nur.

  Der `NDMP_SNAP_DIR_LIST` Nachricht ermöglicht Ihnen das Durchsuchen der Snapshot Kopien eines Volumes. Falls während des Surfvorgangs ein unterbrechungsfreier Vorgang ausgeführt wird, muss die Backup-Applikation den Browservorgang erneut initiieren.

NDMP nicht starrbare Backup-Erweiterung für einen Dump unterstützt von ONTAP

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.

Die verbesserte DAR-Funktionalität ist

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.

Obergrenzen für Skalierbarkeit bei 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
Größer oder gleich 16 GB, aber kleiner als 24 GB	20
Größer oder gleich 24 GB	36

Sie können den Systemspeicher Ihres Storage-Systems mit dem abrufen `sysconfig -a` Befehl (verfügbar über die nodeshell). Weitere Informationen über diese Verwendung dieses Befehls finden Sie in den man-Pages.

Über NDMP für 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.

Über NDMP mit 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

Überblick über den Node-Scoped NDMP-Modus für FlexVol Volumes managen

Sie können NDMP auf Node-Ebene mit NDMP-Optionen und -Befehlen verwalten. Sie

können die NDMP-Optionen mit dem ändern `options` Befehl. Für den Zugriff auf ein Speichersystem müssen NDMP-spezifische Anmeldedaten zum Durchführen von Bandsicherungs- und Wiederherstellungsvorgängen verwendet werden.

Weitere Informationen zum `options` Befehl, siehe die man-Pages.

Verwandte Informationen

Befehle für die Verwaltung des NDMP-Modus mit Node-Umfang

Welcher Node-Scoped NDMP-Modus ist

Befehle für die Verwaltung des NDMP-Modus mit Node-Umfang

Sie können das verwenden `system services ndmp` Befehle zum Managen von NDMP auf Node-Ebene. 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`

Ihr Ziel ist	Befehl
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*`
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.

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages für die `system services ndmp` Befehle.

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

Managen des SVM-Scoped NDMP-Modus für FlexVol Volumes

Überblick über das Managen des SVM-Scoped 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 ändern `vserver services ndmp modify` Befehl. Im SVM-Scoped NDMP-Modus ist die Benutzerauthentifizierung in den rollenbasierten Zugriffssteuerungsmechanismus integriert.

Sie können NDMP in die Liste der zugelassenen oder unzulässigen Protokolle hinzufügen, indem Sie das verwenden `vserver modify` Befehl. 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 mithilfe von hergestellt wird `-preferred-interface-role` Option. 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. Weitere Informationen zum `-preferred-interface-role` Weitere Informationen finden Sie auf den man-Pages.

Weitere Informationen zum `vserver services ndmp modify` Befehl, siehe die man-Pages.

Verwandte Informationen

Befehle für die Verwaltung des SVM-Scoped NDMP-Modus

Was ist Cluster-bewusste Backup-Erweiterung

"ONTAP-Konzepte"

Welcher SVM-Scoped NDMP-Modus ist

"Systemadministration"

Befehle für die Verwaltung des SVM-Scoped NDMP-Modus

Sie können das verwenden `vserver services ndmp` Befehle zum Managen von NDMP auf jeder Storage Virtual Machine (SVM, ehemals bekannt als Vserver)

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 aktivieren `system services ndmp on` Befehl. Standardmäßig ist der NDMP-Service immer auf einem Node aktiviert.

Ihr Ziel ist	Befehl
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`
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.

Weitere Informationen zu diesen Befehlen finden Sie in den man-Pages für die `vserver services ndmp` Befehle.

Was ist Cluster-bewusste Backup-Erweiterung

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 Volumes und Tape-Geräten für Backup und Restore bei unterschiedlichen 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
Daten-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

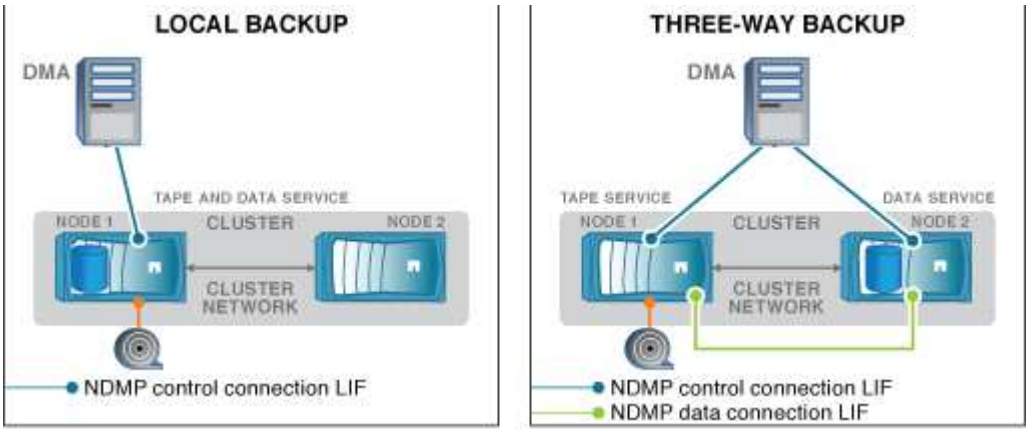
NDMP-Steuerverbindung – LIF-Typ	Volumes verfügbar für Backup und Restore	Bandgeräte für Backup oder Restore verfügbar
Node-Management-LIF	Alle Volumes werden von einem Node gehostet	Mit dem Node, der die Node-Management-LIF hostet, verbundene Tape-Geräte
Daten-LIF	Alle Volumes, die zu der SVM gehören, 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

Was ist Affinität Information

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

Der NDMP-Server unterstützt sichere Kontrollverbindungen im SVM-Scoped-Modus

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 für eine bestimmte SVM über die aktivieren oder deaktivieren `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` Befehl.

NDMP-Datenverbindungsarten

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
Daten-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
Daten-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"

Benutzerauthentifizierung im NDMP-Modus mit SVM-Umfang

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"

"ONTAP-Konzepte"

Erstellen Sie ein NDMP-spezifisches Passwort für 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. Verwenden Sie die `vserver services ndmp generate-password` Befehl zum Generieren eines NDMP-spezifischen Passworts.

   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 von Tape-Backup- und -Restore-Vorgängen bei Disaster Recovery in der MetroCluster Konfiguration

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

Info über Dump Engine für FlexVol-Volumes

Dump ist eine auf Snapshot-Kopien basierende Backup- und Recovery-Lösung von ONTAP. Sie hilft Ihnen beim Backup von Dateien und Verzeichnissen aus einer Snapshot-Kopie auf einem Bandgerät und beim Wiederherstellen der gesicherten Daten in einem Storage-System.

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 die Snapshot-Kopie angeben, die für ein Backup verwendet werden soll. Wenn Sie keine Snapshot Kopie für das Backup angeben, erstellt die Dump Engine eine Snapshot Kopie für das Backup. Nach Abschluss des Backup-Vorgangs wird diese Snapshot Kopie durch die Dump-Engine gelöscht.

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"

Wie ein Dump Backup funktioniert

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 eine Snapshot-Kopie Ihrer Daten für das Backup. Daher müssen Sie das Volume vor dem Start des Backups nicht offline schalten.

Der Dump Backup benennt jede Snapshot-Kopie, die es als erstellt `snapshot_for_backup.n`, Wo `n` Ist eine

Ganzzahl, die bei 0 beginnt. Jedes Mal, wenn die Dump-Datensicherung eine Snapshot-Kopie erstellt, erhöht sie die Ganzzahl um 1. Die Ganzzahl wird nach dem Neustart des Speichersystems auf 0 zurückgesetzt. Nach Abschluss des Backup-Vorgangs wird diese Snapshot Kopie durch die Dump-Engine gelöscht.

Wenn ONTAP mehrere Dump-Backups gleichzeitig ausführt, erstellt die Dump Engine mehrere Snapshot-Kopien. Wenn ONTAP beispielsweise zwei Dump-Backups gleichzeitig ausführt, finden Sie die folgenden Snapshot-Kopien in den Volumes, aus denen Daten gesichert werden: `snapshot_for_backup.0` Und `snapshot_for_backup.1`.

> Wenn Sie aus einer Snapshot Kopie sichern, erstellt die Dump-Engine keine zusätzliche Snapshot-Kopie.

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 VM-bezogene Dateien und die sichern `vm-align-sector` Option. Weitere Informationen zu VM-ausgerichteten Dateien finden Sie unter "Logisches Storage-Management".

Welche Inkrementenketten sind

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 Backup-Pfad, die seit dem Backup der Ebene 0 erstellt wurden
3	3	0, 2, 3	Level-2-Backup	Dateien im Backup-Pfad, die seit dem Level-2-Backup erstellt wurden
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

Was ist der Sperrfaktor

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 wird ein Speicherauszug neu gestartet

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
- Es sind alle zugehörigen Snapshot Kopien verfügbar, die durch den Dump-Befehl gesperrt wurden.
- Der Dateiverlauf muss aktiviert sein.

Wenn ein solcher Dump-Vorgang abgebrochen und wieder rückgängig gemacht wird, werden die zugehörigen Snapshot-Kopien gesperrt. Diese Snapshot Kopien werden freigegeben, nachdem der Backup-Kontext gelöscht wurde. Sie können die Liste der Backup-Kontexte anzeigen, indem Sie die verwenden `vserver services ndmp restartable backup show` Befehl.

```
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 Copy 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 Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Wie eine Dump-Wiederherstellung funktioniert

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.

Stufe	Aktion
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 wie beispielsweise wiederhergestellt wird `/vs1/vol1/subdir/lowerdir`, 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 dem Wiederherstellen der Daten

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. Wenn ein qtree mit Unicode-Namen in ONTAP 9 in eine frühere Version von ONTAP kopiert wird, verwendet das `ndmpcopy` Befehl oder durch Wiederherstellung von einem Backup-Image in einem Band wird der qtree als normales Verzeichnis wiederhergestellt und nicht als qtree mit Unicode-Format.

> 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. Festlegen der Umgebungsvariable KRAFT auf `Y` Bewirkt, dass der Wiederherstellungsvorgang die Prüfungen auf Volume-Speicherplatz und Inode-Verfügbarkeit auf dem Zielpfad überspringt. 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 Dump Backup und Restore-Sessions

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 verwenden `ndmpcopy` Befehl zum Kopieren von Daten in Storage-Systemen werden zwei NDMP-Sitzungen eingerichtet, eine für Dump-Backup und die andere für Dump-Wiederherstellung.

Sie können den Systemspeicher Ihres Storage-Systems mit dem abrufen `sysconfig -a` Befehl (verfügbar über die nodeshell). Weitere Informationen über diese Verwendung dieses Befehls finden Sie in den man-Pages.

Verwandte Informationen

Obergrenzen für Skalierbarkeit bei NDMP-Sitzungen

Unterstützung für Tape-Backup und Restore zwischen Data ONTAP im 7-Mode und ONTAP

Sie können gesicherte Daten von einem Storage-System mit 7-Mode wiederherstellen oder ONTAP auf einem Storage-System wiederherstellen, das entweder im 7-Mode oder mit ONTAP ausgeführt wird.

Die folgenden Backup- und Restore-Vorgänge auf Tape werden zwischen Data ONTAP 7-Mode und ONTAP unterstützt:

- Sichern eines 7-Mode Volumes auf ein Bandlaufwerk, das an ein Storage-System mit ONTAP angeschlossen ist
- Sichern eines ONTAP-Volumes auf einem Bandlaufwerk, das mit einem 7-Mode-System verbunden ist
- Wiederherstellen gesicherter Daten eines 7-Mode Volumes von einem Bandlaufwerk, das an ein Storage-System mit ONTAP angeschlossen ist
- Wiederherstellen gesicherter Daten eines ONTAP-Volumes von einem Bandlaufwerk, das mit einem 7-Mode-System verbunden ist
- Wiederherstellung eines 7-Mode Volumes auf ein ONTAP Volume

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Wiederherstellen eines ONTAP Volumes auf ein 7-Mode Volume

Eine ONTAP LUN wird als normale Datei auf einem 7-Mode Volume wiederhergestellt.

Löschen von neu startbaren Kontexten

Wenn Sie ein Backup starten möchten, anstatt einen Kontext neu zu starten, können Sie den Kontext löschen.

Über diese Aufgabe

Sie können einen neu startbaren Kontext mit dem löschen `vserver services ndmp restartable-backup delete` Geben Sie den SVM-Namen und die Kontext-ID ein.

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::>"
```

Wie Dump funktioniert auf einem sekundären 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 Datensicherungs-Spiegelbeziehung unterbrechen (`snapmirror break`) Oder wenn eine SnapMirror Neusynchronisierung eintritt, müssen Sie immer ein Baseline-Backup durchführen.

So funktioniert Dump mit Storage-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. Der `-override-vetoes` Die Option bestimmt das Verhalten der Dump-Engine während eines Storage-Failovers oder ARL-Vorgangs.

Wenn ein Dump-Backup oder -Restore ausgeführt wird und das `-override-vetoes` Die Option ist auf festgelegt `false`, Ein vom Benutzer initiiertes Storage-Failover oder ARL-Vorgang wird angehalten. Wenn der jedoch `-override-vetoes` Die Option ist auf festgelegt `true`, Dann wird das Storage-Failover oder der ARL-Vorgang fortgesetzt und der Dump-Backup- bzw. Restore-Vorgang wird 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

"ONTAP-Konzepte"

"Hochverfügbarkeit"

Wie Dump funktioniert mit 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.
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.

Verwandte Informationen

"ONTAP-Konzepte"

Wie Dump funktioniert, wenn ein 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 entweder durch eine Erhöhung seiner Größe oder durch Löschen der Snapshot Kopien erhöhen. Dann führen Sie den inkrementellen Backup-Vorgang erneut aus.

Wie Dump funktioniert, wenn sich der Volume-Zugriffstyp ändert

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.

Verwandte Informationen

"ONTAP-Konzepte"

Wie Dump funktioniert mit SnapMirror Single File- 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 Restore-Vorgängen in MetroCluster-Konfigurationen

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 des `override-vetoes` Option ist `false`, Dann wird die Umschaltung abgebrochen und der Backup- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option lautet `true`, Dann wird der Backup- oder Wiederherstellungsvorgang für Dump 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 des `override-vetoes` Option ist `false`, Dann wird der Wechsel abgebrochen und der Backup- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option lautet `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

Über 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 bis zu 255 Snapshot Kopien erstellen. Für nachfolgende Baseline-, inkrementelle oder differenzielle Backups müssen ältere gesicherte Snapshot Kopien gelöscht werden.

Vor dem Ausführen eines Basis-Restore muss das Volume, auf dem die Daten wiederhergestellt werden, vom Typ sein `DP` Und dieses Volumen 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.

Snapshot-Kopien während SMTape Backups nutzen

Sie sollten verstehen, wie Snapshot Kopien während eines Basis-Backups mit SMTape und einem inkrementellen Backup verwendet werden. Bedenken Sie auch bei der Durchführung eines Backups mit SMTape.

Basis-Backup

Während Sie ein Basis-Backup durchführen, können Sie den Namen der zu sichernden Snapshot Kopie angeben. Wenn keine Snapshot Kopie angegeben wird, wird abhängig vom Zugriffstyp des Volume (Lese-/Schreib- oder schreibgeschützt) entweder eine Snapshot Kopie automatisch erstellt oder vorhandene Snapshot Kopien verwendet. Wenn Sie eine Snapshot Kopie für das Backup angeben, werden alle Snapshot Kopien, die älter als die angegebene Snapshot Kopie sind, auch auf Tape gesichert.

Wenn Sie keine Snapshot Kopie für das Backup angeben, erfolgt die folgende Meldung:

- Für ein Lese-/Schreib-Volume wird automatisch eine Snapshot-Kopie erstellt.

  Die neu erstellte Snapshot Kopie und alle älteren Snapshot Kopien werden auf Tape gesichert.

- Bei einem schreibgeschützten Volume werden alle Snapshot Kopien, einschließlich der neuesten Snapshot Kopie, auf Tape gesichert.

  Neue Snapshot Kopien, die nach dem Starten des Backups erstellt wurden, werden nicht gesichert.

Inkrementelles Backup

Bei inkrementellen oder differenziellen Backup-Vorgängen mit SMTape erstellen und managen die NDMP-kompatiblen Backup-Applikationen die Snapshot Kopien.

Sie müssen immer eine Snapshot Kopie angeben, während Sie einen inkrementellen Backup-Vorgang durchführen. Für einen erfolgreichen, inkrementellen Backup-Vorgang muss sich die während des vorherigen Backup-Vorgangs (Baseline oder inkrementell) gesicherte Snapshot Kopie auf dem Volume befinden, von dem das Backup durchgeführt wird. Um sicherzustellen, dass Sie diese gesicherte Snapshot Kopie verwenden, müssen Sie während der Konfiguration der Backup-Richtlinie die auf diesem Volume zugewiesene Snapshot-Richtlinie berücksichtigen.

Überlegungen zu SMTape Backups auf SnapMirror Zielen

- Eine Datensicherungs-Spiegelbeziehung erstellt temporäre Snapshot Kopien auf dem Ziel-Volume zur

Replizierung.

Für SMTape-Backups sollten diese Snapshot Kopien nicht verwendet werden.

- Wenn ein SnapMirror Update auf einem Ziel-Volume in einer Datensicherungsspiegelbeziehung während eines SMTape Backups auf demselben Volume stattfindet, darf die von SMTape gesicherte Snapshot Kopie nicht auf dem Quell-Volume gelöscht werden.

  Während des Backups sperrt SMTape die Snapshot Kopie auf dem Ziel-Volume und wenn die entsprechende Snapshot Kopie auf dem Quell-Volume gelöscht wird, dann schlägt der nachfolgende SnapMirror Update fehl.

- Sie sollten diese Snapshot-Kopien nicht während des inkrementellen Backups verwenden.

SMTape Funktionen

SMTape-Funktionen wie das Backup von Snapshot-Kopien, inkrementelle und differenzielle Backups, Beibehaltung von Deduplizierungs- und Komprimierungsfunktionen auf wiederhergestellten Volumes und Tape Seeding helfen Ihnen bei der Optimierung von Tape-Backup- und Restore-Vorgängen.

SMTape bietet die folgenden Funktionen:

- Bietet eine Disaster Recovery-Lösung
- Ermöglicht inkrementelle und differenzielle Backups
- Sicherung von Snapshot Kopien
- 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.

Funktionen, die nicht in SMTape unterstützt werden

SMTape unterstützt keine neu startbaren Backups und keine Überprüfung der gesicherten Dateien.

Skalierbarkeitsbeschränkungen für SMTape Backup- und Restore-Sessions

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 Storage-Systems mit dem abrufen `sysconfig -a` Befehl (verfügbar über die nodeshell). Weitere Informationen über diese Verwendung dieses Befehls finden Sie in den man-Pages.

Verwandte Informationen

Obergrenzen für Skalierbarkeit bei NDMP-Sitzungen

Skalierbarkeitsgrenzen für Dump Backup und Restore-Sessions

Was ist das 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.

Eine inkrementelle Spiegelung von Snapshot Kopien vom Quell- zum Zielsystem ist über eine Verbindung mit niedriger Bandbreite realisierbar. Eine erste Spiegelung der Basis-Snapshot-Kopie dauert jedoch sehr lange über eine Verbindung mit einer niedrigen Bandbreite. In solchen Fällen können Sie ein SMTape Backup des Quell-Volume auf ein Tape durchführen und die Tapes zur Übertragung der ersten Basis-Snapshot Kopie an das Ziel verwenden. Anschließend können Sie über die Verbindung mit niedriger Bandbreite inkrementelle SnapMirror Updates auf das Zielsystem einrichten.

Verwandte Informationen

"ONTAP-Konzepte"

Funktionsweise von SMTape mit Storage-Failover und ARL-Betrieb

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. Der `-override-vetoes` Die Option bestimmt das Verhalten der SMTape Engine während eines Storage Failover oder eines ARL-Betriebs.

Wenn ein Backup- oder Wiederherstellungsvorgang mit SMTape ausgeführt wird, und `-override-vetoes` Die Option ist auf festgelegt `false`, Ein durch den Benutzer initiiertes Storage Failover oder ARL-Vorgang wird angehalten und der Backup- 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 der jedoch `-override-vetoes` Die Option ist auf festgelegt `true`, Dann wird das Storage-Failover oder der ARL-Vorgang fortgesetzt und der SMTape-Backup- oder Restore-Vorgang wird abgebrochen.

Verwandte Informationen

"Netzwerkmanagement"

"Hochverfügbarkeit"

Funktionsweise von SMTape mit der Verschiebung von Volumes

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.

Verwandte Informationen

"ONTAP-Konzepte"

Funktionsweise von SMTape mit Volume Rehosting

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 der NDMP-Backup-Richtlinie während der 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 von Backup- und Restore-Vorgängen mit SMTape in 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 des `-override-vetoes` Option ist `false`, Dann wird der Umschaltvorgang abgebrochen und der Backup- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option lautet `true`, Dann wird der SMTape-Backup- oder Restore-Vorgang abgebrochen und der Switchover-Prozess 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 des `-override-vetoes` Option ist `false`, Dann wird der Switchback-Prozess abgebrochen und der Backup- oder Wiederherstellungsvorgang wird fortgesetzt.
- Wenn der Wert der Option lautet `true`, Dann wird der Backup- oder Wiederherstellungsvorgang abgebrochen und der Switch-Back-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

Überwachung von Tape-Backup- und Restore-Vorgängen für FlexVol Volumes – Übersicht

Sie können die Ereignisprotokolldateien anzeigen, um die Tape-Backup- und Restore-

Vorgänge zu überwachen. ONTAP protokolliert wichtige Backup- und Restore-Ereignisse automatisch sowie die Zeit, zu der sie in einer Protokolldatei mit dem Namen auftreten `backup` In den Controllern `/etc/log/` Verzeichnis. Standardmäßig ist die Ereignisprotokollierung auf festgelegt `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. Der `/etc/log/backup` Datei wird in umbenannt `/etc/log/backup.0`, Das `/etc/log/backup.0` Datei wird in umbenannt `/etc/log/backup.1`, Und so weiter. Das System speichert die Protokolldateien bis zu sechs Wochen lang, sodass Sie bis zu sieben Nachrichtendateien haben können (`/etc/log/backup.[0-5]` Und den Strom `/etc/log/backup` Datei).

Greifen Sie auf die Ereignis-Log-Dateien zu

Sie können auf die Ereignisprotokolldateien für Bandsicherungs- und Wiederherstellungsvorgänge in zugreifen `/etc/log/` Verzeichnis mit verwenden `rdfile` Befehl im nodeshell. Sie können diese Ereignisprotokolldateien anzeigen, um Tape-Backup- und Restore-Vorgänge zu überwachen.

Über diese Aufgabe

Mit zusätzlichen Konfigurationen, wie z. B. eine Zugriffskontroll-Rolle mit Zugriff auf das `spi` Webdienst oder ein mit dem eingerichtet Benutzerkonto `http` Zugriffsmethode Sie können 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"

"ONTAP-Konzepte"

Das Nachrichtenformat für die Speicherauszug und Wiederherstellung des Ereignisprotokolls lautet

Dump bedeutet „Dump“ und Wiederherstellung des Nachrichtenformats des Ereignisprotokolls

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.
- Der `identifier` Feld für ein Dump-Ereignis enthält den Dump-Pfad und die eindeutige ID für den Dump. Der `identifier` Feld für ein Wiederherstellungsereignis verwendet nur den Namen des wiederherzustellenden Zielpfads als eindeutige Kennung. Protokollierende Ereignismeldungen enthalten keine `identifier` Feld.

Welche Protokollierungsereignisse sind

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.

Was sind 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
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	Eine Snapshot Kopie wird erstellt oder gefunden	Der Name und die Uhrzeit der Snapshot Kopie
Base_dump	Ein Base Dump-Eintrag in der internen Metadatei wurde gefunden	Level und Zeit des Basis-Dump (nur für inkrementelle Dumps)

Was sind 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

Ereignis	Beschreibung	Ereignisinformationen
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
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

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` Schaltet die Ereignisprotokollierung aus.

   > 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 Sperrfaktor.

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 die `ndmpd status` Befehl zum Anzeigen der aktiven NDMP-Sitzungen.

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**

  NDMP Dump Backup wird auf einem SnapMirror-Ziel-Volume versucht, das Teil entweder A ist `snapmirror break` Oder A `snapmirror resync` Betrieb.

- **Korrekturmaßnahmen**

  Warten Sie auf das `snapmirror break` Oder `snapmirror resync` Vorgang bis zum Abschluss und dann den Speicherauszugsvorgang durchführen.

  > 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.

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**

  Die für das Backup angegebene Snapshot-Kopie ist nicht verfügbar.

- **Korrekturmaßnahmen**

  Versuchen Sie das Backup mit einer anderen Snapshot Kopie erneut.

  Verwenden Sie die `snap list` Befehl, um die Liste der verfügbaren Snapshot Kopien anzuzeigen.

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**

  Die für das Backup angegebene Snapshot Kopie ist nicht verfügbar.

- **Korrekturmaßnahmen**

Prüfung, ob die angegebene Snapshot Kopie verfügbar ist Wenn nicht, versuchen Sie es mit der korrekten Snapshot Kopie.

Snapshot konnte nicht erstellt werden

- **Nachricht**

  ```
  Failed to create snapshot
  ```

- **Ursache**

  Das Volume enthält bereits die maximale Anzahl an Snapshot Kopien.

- **Korrekturmaßnahmen**

  Löschen Sie einige Snapshot Kopien, und versuchen Sie es dann erneut.

Snapshot konnte nicht gesperrt werden

- **Nachricht**

  ```
  Failed to lock snapshot
  ```

- **Ursache**

  Die Snapshot Kopie wird gerade verwendet oder wurde gelöscht.

- **Korrekturmaßnahmen**

  Wenn die Snapshot Kopie von einem anderen Vorgang verwendet wird, warten Sie, bis dieser Vorgang abgeschlossen ist, und versuchen Sie das Backup erneut. Wenn die Snapshot Kopie gelöscht wurde, können Sie das Backup nicht ausführen.

Snapshot konnte nicht gelöscht werden

- **Nachricht**

  ```
  Failed to delete snapshot
  ```

- **Ursache**

  Die automatische Snapshot-Kopie konnte nicht gelöscht werden, da sie von anderen Vorgängen verwendet wird.

- **Korrekturmaßnahmen**

  Verwenden Sie die `snap` Befehl zum Bestimmen des Status der Snapshot Kopie. Wenn die Snapshot Kopie nicht erforderlich ist, löschen Sie sie manuell.

Der neueste Snapshot konnte nicht abgerufen werden

- **Nachricht**

```
Failed to get latest snapshot
```

- **Ursache**

  Die neueste Snapshot Kopie 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 Sie den Fehler, und senden Sie den `etc/log/backup` Datei an 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**

  Verwenden Sie die `smtape restore -h` Befehl zum Überprüfen der Header-Informationen eines Bands.

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 Löschen von Snapshots abgebrochen

- **Nachricht**

  ```
  Job aborted due to Snapshot autodelete
  ```

- **Ursache**

  Das Volume verfügt nicht über genügend Speicherplatz und hat das automatische Löschen von Snapshot-Kopien 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

NDMP-Konfiguration – Überblick

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.

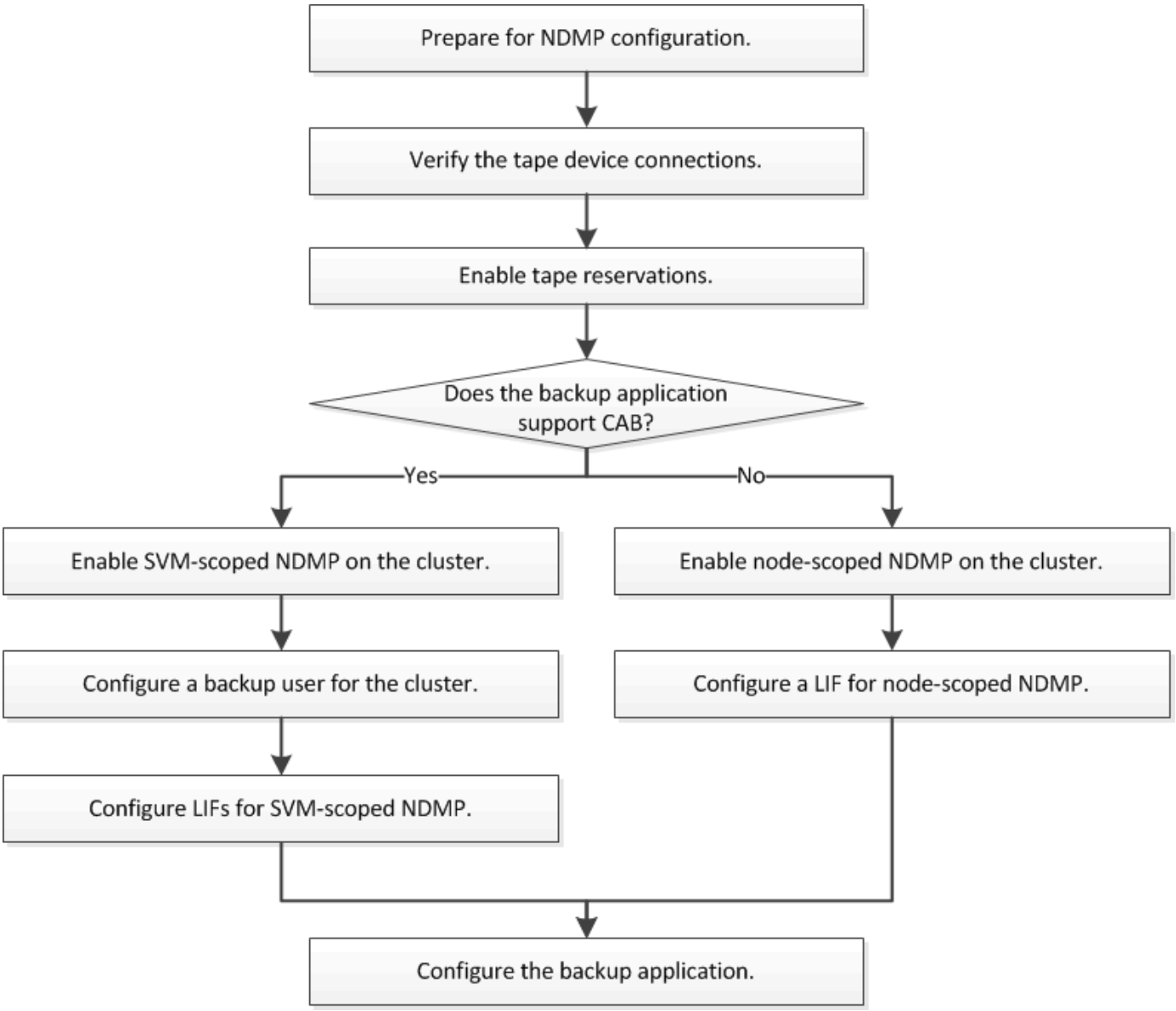
Weitere Informationen zu "Cluster-sensibles Backup (CAB)".

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.
- Tape-Geräte sind über einen FC-Switch (Fibre Channel) mit dem Cluster verbunden und nicht direkt verbunden.
- Mindestens ein Bandgerät verfügt über eine Logical Unit Number (LUN) von 0.

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.



Vorbereitung auf die NDMP-Konfiguration

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.

> Im finden Sie Legacy-Supportmatrizen zur ONTAP-Kompatibilität für Backup-Anwendungen "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 mithilfe von an `storage tape show-supported-status` Befehl.

```
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. Zeigen Sie die Intercluster-LIFs auf den Nodes mithilfe von an `network interface show -role intercluster` Befehl.

```
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
```

b. Wenn auf einem Node keine Intercluster-LIF vorhanden ist, erstellen Sie mithilfe der eine Intercluster-LIF `network interface create` Befehl.

```
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
```

"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.

Überprüfen Sie die Verbindungen des Bandgeräts

Sie müssen sicherstellen, dass alle Laufwerke und Medienwechsler in ONTAP als Geräte

sichtbar sind.

Schritte

1. Zeigen Sie Informationen zu allen Laufwerken und Medienschaltern an, indem Sie die verwenden `storage tape show` Befehl.

```
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, zeigen Sie Informationen über Medientauscher mithilfe des an `storage tape show-media-changer` Befehl und dann Fehlerbehebung.

```
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
...
```

Aktivieren Sie Tape-Reservierungen

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 mithilfe des `options -option-name tape.reservations -option -value persistent` Befehl.

   Mit dem folgenden Befehl werden Reservierungen mit aktiviert `persistent` Wert:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Überprüfen Sie mithilfe des, ob Reservierungen auf allen Knoten aktiviert sind `options tape.reservations` Befehl und dann überprüfen Sie 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 NDMP mit SVM-Umfang auf dem 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.

Was Sie benötigen

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 auf festgelegt `challenge` Standardmäßig ist die Klartext-Authentifizierung 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
```

Aktivieren Sie einen Backup-Benutzer für die NDMP-Authentifizierung

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
   ```

2. Erstellen Sie bei Bedarf einen neuen NDMP-Backup-Benutzer mit dem `security login create` Befehl und die entsprechende Rolle für Cluster-weite oder einzelne SVM-Berechtigungen.

   Sie können einen lokalen Backup-Benutzernamen oder einen NIS- oder LDAP-Benutzernamen für das angeben `-user-or-group-name` Parameter.

   Mit dem folgenden Befehl wird der Backup-Benutzer erstellt `backup_admin1` Mit dem `backup` Rolle für den gesamten Cluster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   Mit dem folgenden Befehl wird der Backup-Benutzer erstellt `vsbackup_admin1` Mit dem `vsadmin-backup` Rolle für eine einzelne SVM:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

Geben Sie ein Passwort für den neuen Benutzer ein und bestätigen Sie.

3. Generieren Sie mit ein Passwort für die Admin-SVM `vserver services ndmp generate password` Befehl.

   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 LIFs

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. Nachdem Sie die LIFs identifiziert haben, müssen Sie überprüfen, ob Firewall- und Failover-Richtlinien für die LIFs festgelegt wurden, und geben Sie die bevorzugte Schnittstellenrolle an.

Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "LIFs und Service-Richtlinien in ONTAP 9.6 und höher".

Schritte

1. Ermitteln Sie mithilfe des die Intercluster-, Cluster-Management- und Node-Management-LIFs `network interface show` Befehl mit dem `-role` Parameter.

   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
```

2. Vergewissern Sie sich, dass die Firewallrichtlinie für NDMP im Intercluster, Cluster-Management (Cluster-Management) und Node-Management-LIFs aktiviert ist:

   a. Überprüfen Sie mithilfe der, ob die Firewallrichtlinie für NDMP aktiviert ist `system services firewall policy show` Befehl.

      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 unter `system services firewall policy modify` Befehl mit dem `-service` Parameter.

   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 die Richtlinie für die Schnittstellen zwischen Clustern und Nodes-Management ist auf festgelegt `local-only` Durch Verwendung des `network interface show -failover` Befehl.

      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 entsprechend festgelegt sind, ändern Sie die Failover-Richtlinie mithilfe der `network interface modify` Befehl mit dem `-failover-policy` Parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Geben Sie die LIFs an, die mithilfe von für die Datenverbindung erforderlich sind `vserver services ndmp modify` Befehl mit dem `preferred-interface-role` Parameter.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Vergewissern Sie sich, dass die bevorzugte Schnittstellenrolle für das Cluster mithilfe von festgelegt wird `vserver services ndmp show` Befehl.

```
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 NDMP mit Node-Umfang auf dem 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 das `-clear-text` Option zur sicheren Kommunikation des NDMP-Passworts:

   Verwenden des Platzhalters „`*`" disables the `-clear-text` Auf allen Nodes gleichzeitig möglich.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Vergewissern Sie sich, dass der NDMP-Service aktiviert ist und der `-clear-text` Option ist deaktiviert:

```
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 ein LIF

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 "Konfigurieren Sie Firewallrichtlinien für LIFs".

Schritte

1. Identifizieren Sie die auf den Nodes gehostete Intercluster-LIF mithilfe des `network interface show` Befehl mit dem `-role` Parameter.

```
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 mithilfe der, ob die Firewallrichtlinie für NDMP aktiviert ist `system services firewall policy show` Befehl.

      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 unter `system services firewall policy modify` Befehl mit dem `-service` Parameter.

      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. Vergewissern Sie sich, dass die Failover-Richtlinie für die Intercluster LIFs auf festgelegt ist `local-only` Durch Verwendung des `network interface show -failover` Befehl.

```
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 entsprechend festgelegt ist, ändern Sie die Failover-Richtlinie mithilfe des `network interface modify` Befehl mit dem `-failover-policy` Parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Konfigurieren der Backup-Applikation

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 zugewiesen hat, indem Sie das verwenden `storage tape alias show` Befehl.

   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.

Replizierung zwischen NetApp Element Software und ONTAP

Übersicht über die Replizierung zwischen NetApp Element Software und ONTAP

Durch Verwendung von SnapMirror zur Replizierung von Snapshot Kopien eines Element Volume auf ein ONTAP Ziel wird die Business Continuity in einem Element System gewährleistet. 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 Snapshot Kopien 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.

Wenn Folgendes gilt, sollten Sie mit Element zu ONTAP Backups arbeiten:

- Sie möchten Best Practices verwenden und nicht alle verfügbaren Optionen erkunden.
- Sie möchten die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, nicht System Manager oder ein automatisiertes Scripting Tool.
- Sie verwenden iSCSI, um den Clients Daten bereitzustellen.

Falls Sie zusätzliche Konfigurations- oder konzeptionelle Informationen benötigen, lesen Sie bitte die folgende Dokumentation:

- Konfiguration von Elementen

  "NetApp Element Softwaredokumentation"

- SnapMirror Konzepte und Konfiguration

  "Datensicherung im Überblick"

Allgemeines zur Replizierung zwischen Element und ONTAP

Ab ONTAP 9.3 können Sie SnapMirror verwenden, um Snapshot Kopien eines Element Volume zu einem ONTAP Ziel zu replizieren. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element Quell-Volume nach Wiederherstellung des Service erneut aktivieren.

Ab ONTAP 9.4 können Sie Snapshot Kopien 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.

Arten von Datensicherungsbeziehungen

SnapMirror bietet zwei Arten von Datensicherungsbeziehungen. Für jeden Typ erstellt SnapMirror eine Snapshot Kopie des Quell-Volume des Element-Volumes, bevor die Beziehung initialisiert oder aktualisiert wird:

- In einer Datensicherungsbeziehung enthält das Ziel-Volume nur die von SnapMirror erstellte Snapshot Kopie, die im K-Fall am primären Standort weiterhin Daten bereitstellen kann.
- In einer Datensicherungsbeziehung enthält das Ziel-Volume zeitpunktgenaue Snapshot Kopien, die von Element Software erstellt wurden, sowie die von SnapMirror erstellte Snapshot Kopie. Es empfiehlt sich, beispielsweise monatliche Snapshot Kopien aufzubewahren, die über einen Zeitraum von 20 Jahren erstellt wurden.

Standardrichtlinien

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

Sie können eine Standard- oder benutzerdefinierte Richtlinie verwenden, wenn Sie eine Datensicherungsbeziehung erstellen. Der Typ_Policy_ bestimmt, welche Snapshot Kopien enthalten sollen und wie viele Kopien sie aufbewahren sollen.

Die folgende Tabelle zeigt die Standardrichtlinien. Verwenden Sie die `MirrorLatest` Richtlinie zur Erstellung einer herkömmlichen DR-Beziehung Verwenden Sie die `MirrorAndVault` Oder `Unified7year` Richtlinie zur Erstellung einer einheitlichen Replizierungsbeziehung, bei der DR und langfristige Aufbewahrung auf demselben Ziel-Volume konfiguriert werden

Richtlinie	Richtlinientyp	Verhalten aktualisieren
MirrorLatest	Asynchrone Spiegelung	Übertragen Sie die von SnapMirror erstellte Snapshot Kopie.
MirrorAndVault	Mirror-Vault	Übertragen Sie die von SnapMirror erstellte Snapshot Kopie mit den weniger aktuellen Snapshot-Kopien der letzten Aktualisierung, vorausgesetzt, sie haben SnapMirror-Labels „`dily`“ oder „`Weekly`“.

Unified7 Jahr	Mirror-Vault	Übertragen Sie die von SnapMirror erstellte Snapshot-Kopie mit noch weniger aktuellen Snapshot-Kopien seit dem letzten Update, vorausgesetzt, sie haben SnapMirror-Labels „`dily`“, „`Weekly`“ oder „`monthly`“.

Vollständige Hintergrundinformationen zu SnapMirror Richtlinien, einschließlich Anleitungen zur Verwendung von Richtlinien, finden Sie unter "Datensicherung".

Allgemeines zu SnapMirror-Beschriftungen

Jede Richtlinie mit dem Richtlinientyp „`mmirror-Vault`“ muss über eine Regel verfügen, die angibt, welche Snapshot Kopien repliziert werden sollen. Die Regel „`dallily`“ zeigt beispielsweise an, dass nur Snapshot-Kopien, die dem SnapMirror-Label „`dily`“ zugewiesen sind, repliziert werden sollten. Wenn Sie Element Snapshot Kopien konfigurieren, weisen Sie die SnapMirror-Bezeichnung zu.

Replizierung von einem Element Quell-Cluster zu einem ONTAP Ziel-Cluster

Mithilfe von SnapMirror werden Snapshot Kopien eines Element Volume in ein ONTAP Zielsystem repliziert. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element Quell-Volume nach Wiederherstellung des Service erneut aktivieren.

Ein Element Volume ist in etwa dem einer ONTAP LUN entsprechenden Modus. SnapMirror erstellt eine LUN mit dem Namen des Element-Volume, wenn eine Datensicherungsbeziehung zwischen Element Software und ONTAP initialisiert wird. SnapMirror repliziert Daten in eine vorhandene LUN, wenn die LUN die Anforderungen für Element zur ONTAP Replizierung erfüllt.

Replikationsregeln:

- Ein ONTAP Volume kann nur Daten aus einem Element Volume enthalten.
- Es können keine Daten von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Replizierung von einem ONTAP Quell-Cluster zu einem Element Ziel-Cluster

Ab ONTAP 9.4 können Sie Snapshot Kopien einer auf einem ONTAP System erstellten LUN zurück in ein Element Volume replizieren:

- Wenn bereits eine SnapMirror Beziehung zwischen einer Element Quelle und einem ONTAP Ziel vorhanden ist, wird eine beim Bereitstellen von Daten vom Ziel erstellte LUN automatisch repliziert, sobald die Quelle reaktiviert wird.
- Andernfalls müssen Sie eine SnapMirror Beziehung zwischen dem ONTAP Quell-Cluster und dem Element Ziel-Cluster erstellen und initialisieren.

Replikationsregeln:

- Die Replizierungsbeziehung muss über eine Richtlinie vom Typ „`async-Mirror`“ verfügen.

  Richtlinien vom Typ “mmirror-Vault” werden nicht unterstützt.

- Es werden nur iSCSI LUNs unterstützt.
- Es kann nicht mehr als eine LUN aus einem ONTAP Volume in ein Element Volume repliziert werden.

- Eine LUN kann nicht von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Voraussetzungen

Sie müssen die folgenden Aufgaben abgeschlossen haben, bevor Sie eine Datensicherungsbeziehung zwischen Element und ONTAP konfigurieren:

- Auf dem Element Cluster muss die NetApp Element Softwareversion 10.1 oder höher ausgeführt werden.
- Der ONTAP Cluster muss ONTAP 9.3 oder höher ausführen.
- SnapMirror muss auf dem ONTAP Cluster lizenziert sein.
- Sie müssen Volumes auf dem Element und ONTAP Cluster konfigurieren, die groß genug sind, um erwartete Datentransfers zu verarbeiten.
- Wenn Sie die Richtlinie „`mmirror-Vault`“ verwenden, muss ein SnapMirror Label konfiguriert worden sein, damit die Element Snapshot Kopien repliziert werden können.

> Diese Aufgabe kann nur in der Web-Benutzeroberfläche der Element Software ausgeführt werden. Weitere Informationen finden Sie im "NetApp Element Softwaredokumentation"

- Sie müssen sicherstellen, dass Port 5010 verfügbar ist.
- Wenn Sie bereits sehen, dass ein Ziel-Volume möglicherweise verschoben werden muss, müssen Sie sicherstellen, dass eine vollständige Mesh-Konnektivität zwischen Quelle und Ziel besteht. Jeder Node im Element Quell-Cluster muss in der Lage sein, mit jedem Node im ONTAP Ziel-Cluster zu kommunizieren.

Support-Details

Die folgende Tabelle enthält Support-Details für Element- zu ONTAP-Backups.

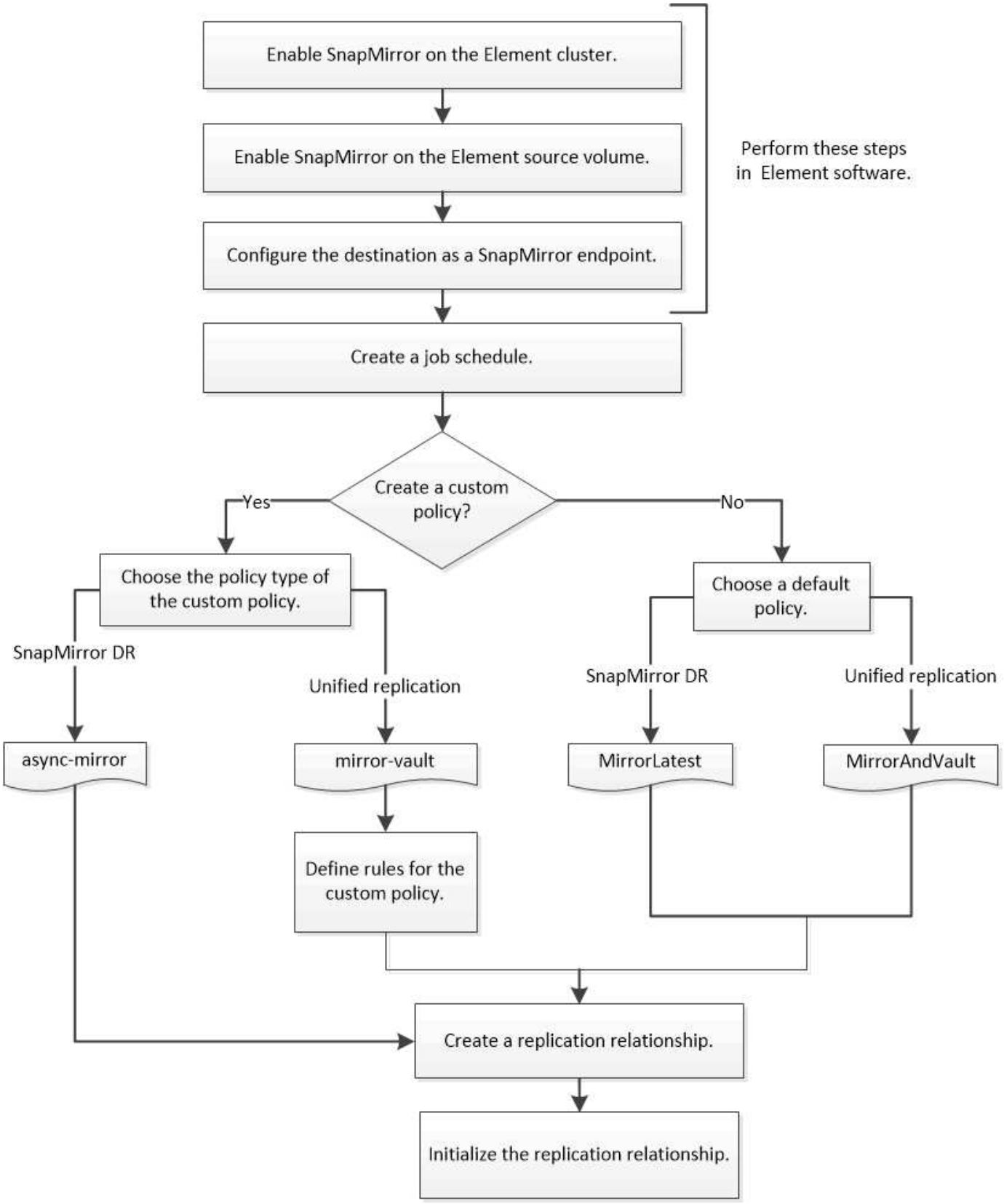
Ressource oder Funktion	Support-Details
SnapMirror	• Die SnapMirror Wiederherstellungsfunktion wird nicht unterstützt. • Der `MirrorAllSnapshots` Und `XDPDefault` Richtlinien werden nicht unterstützt. • Der Richtlinientyp „`Vault`“ wird nicht unterstützt. • Die systemdefinierte Regel „`all_Source_Snapshots`“ wird nicht unterstützt. • Der Richtlinientyp „`mmirror-Vault`“ wird nur zur Replikation von Element Software auf ONTAP unterstützt. Verwenden Sie „`Async-Mirror`“ für die Replizierung von ONTAP zu Element Software. • Der `-schedule` Und `-prefix` Optionen für `snapmirror policy add-rule` Werden nicht unterstützt. • Der `-preserve` Und `-quick-resync` Optionen für `snapmirror resync` Werden nicht unterstützt. • Storage-Effizienz bleibt erhalten. • Fan-out- und Kaskadenschutz-Implementierungen werden nicht unterstützt.

ONTAP	• ONTAP Select wird ab ONTAP 9.4 und Element 10.3 unterstützt. • Cloud Volumes ONTAP wird ab ONTAP 9.5 und Element 11.0 unterstützt.
Element	• Die maximale Volume-Größe beträgt 8 tib. • Die Volume-Blockgröße muss 512 Byte sein. Eine Blockgröße von 4 KB wird nicht unterstützt. • Die Volume-Größe muss ein Vielfaches von 1 MiB sein. • Volume-Attribute werden nicht erhalten. • 30 Snapshot Kopien, die repliziert werden sollen, sind maximal vorhanden.
Netzwerk	• Pro Übertragung ist eine einzelne TCP-Verbindung zulässig. • Der Element-Node muss als IP-Adresse angegeben werden. Die Suche nach DNS-Hostnamen wird nicht unterstützt. • IPspaces werden nicht unterstützt.
SnapLock	SnapLock Volumes werden nicht unterstützt.
FlexGroup	FlexGroup Volumes werden nicht unterstützt.
SVM-DR	ONTAP Volumes in einer SVM-DR-Konfiguration werden nicht unterstützt.
MetroCluster	ONTAP Volumes in einer MetroCluster Konfiguration werden nicht unterstützt.

Workflow für die Replizierung zwischen Element und ONTAP

Unabhängig davon, ob Daten von Element zu ONTAP oder von ONTAP zu Element repliziert werden, müssen Sie einen Job-Zeitplan konfigurieren, eine Richtlinie festlegen und die Beziehung erstellen und initialisieren. Sie können eine Standard- oder eine benutzerdefinierte Richtlinie verwenden.

Im Workflow wird davon ausgegangen, dass Sie die unter aufgeführten Aufgaben abgeschlossen haben Voraussetzungen. Vollständige Hintergrundinformationen zu SnapMirror Richtlinien, einschließlich Anleitungen zur Verwendung von Richtlinien, finden Sie unter "Datensicherung".



SnapMirror in Element Software aktivieren

Aktivieren Sie SnapMirror auf dem Element Cluster

Sie müssen SnapMirror auf dem Element-Cluster aktivieren, bevor Sie eine

Replizierungsbeziehung erstellen können. Diese Aufgabe kann nur in der Web-Benutzeroberfläche der Element Software ausgeführt werden.

Bevor Sie beginnen

- Auf dem Element Cluster muss die NetApp Element Softwareversion 10.1 oder höher ausgeführt werden.
- SnapMirror kann nur für Element Cluster aktiviert werden, die in NetApp ONTAP Volumes verwendet werden.

Über diese Aufgabe

Das Element System wird standardmäßig mit SnapMirror deaktiviert. SnapMirror wird im Rahmen einer neuen Installation oder eines Upgrades nicht automatisch aktiviert.

> Nach der Aktivierung kann SnapMirror nicht deaktiviert werden. Sie können die SnapMirror Funktion nur deaktivieren und die Standardeinstellungen wiederherstellen, indem Sie das Cluster wieder an das Werkseinstellungen zurücksetzen.

Schritte

1. Klicken Sie Auf **Cluster** > **Einstellungen**.
2. Suchen Sie die Cluster-spezifischen Einstellungen für SnapMirror.
3. Klicken Sie auf **SnapMirror aktivieren**.

Aktivieren Sie SnapMirror auf dem Element Quell-Volume

Sie müssen SnapMirror auf dem Element Quell-Volume aktivieren, bevor Sie eine Replizierungsbeziehung erstellen können. Diese Aufgabe kann nur in der Web-Benutzeroberfläche der Element Software ausgeführt werden.

Bevor Sie beginnen

- SnapMirror muss auf dem Element Cluster aktiviert sein.
- Die Volume-Blockgröße muss 512 Byte sein.
- Das Volume darf nicht an der Remote-Replizierung von Element beteiligt sein.
- Der Zugriffstyp des Volumes darf nicht „`Replikationsziel`“ sein.

Über diese Aufgabe

Für das folgende Verfahren wird vorausgesetzt, dass das Volume bereits vorhanden ist. Sie können SnapMirror auch beim Erstellen oder Klonen eines Volumes aktivieren.

Schritte

1. Wählen Sie **Management** > **Volumes**.
2. Wählen Sie die aus ⚙ Taste für die Lautstärke.
3. Wählen Sie im Dropdown-Menü die Option **Bearbeiten** aus.
4. Wählen Sie im Dialogfeld **Volume bearbeiten** die Option **SnapMirror aktivieren** aus.
5. Wählen Sie **Änderungen Speichern**.

Erstellen eines SnapMirror Endpunkts

Sie müssen einen SnapMirror Endpunkt erstellen, bevor Sie eine Replizierungsbeziehung erstellen können. Diese Aufgabe kann nur in der Web-Benutzeroberfläche der Element Software ausgeführt werden.

Bevor Sie beginnen

SnapMirror muss auf dem Element Cluster aktiviert sein.

Schritte

1. Klicken Sie auf **Datensicherung** > **SnapMirror Endpunkte**.
2. Klicken Sie Auf **Endpunkt Erstellen**.
3. Geben Sie im Dialogfeld **Neuen Endpunkt erstellen** die IP-Adresse für die ONTAP-Clusterverwaltung ein.
4. Geben Sie die Benutzer-ID und das Passwort des ONTAP Cluster-Administrators ein.
5. Klicken Sie Auf **Endpunkt Erstellen**.

Konfigurieren einer Replikationsbeziehung

Erstellen eines Replikationsauftrags

Unabhängig davon, ob Daten von Element zu ONTAP oder von ONTAP zu Element repliziert werden, müssen Sie einen Job-Zeitplan konfigurieren, eine Richtlinie festlegen und die Beziehung erstellen und initialisieren. Sie können eine Standard- oder eine benutzerdefinierte Richtlinie verwenden.

Sie können das verwenden `job schedule cron create` Befehl zum Erstellen eines Replikationsauftragplans. Der Job-Zeitplan legt fest, wann SnapMirror die Datensicherungsbeziehung automatisch aktualisiert, denen der Zeitplan zugewiesen ist.

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.

Schritt

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`, Sie können angeben `all` Zum Ausführen des Jobs jeden Monat, Wochentag und Stunde.

   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 Job-Zeitplan mit dem Namen erstellt `my_weekly` Das läuft samstags um 3:00 Uhr:

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

Anpassen einer Replizierungsrichtlinie

Erstellen Sie eine benutzerdefinierte Replikationsrichtlinie

Sie können eine Standard- oder benutzerdefinierte Richtlinie verwenden, wenn Sie eine Replikationsbeziehung erstellen. Bei einer benutzerdefinierten einheitlichen Replizierungsrichtlinie müssen Sie eine oder mehrere *rules* definieren, die festlegen, welche Snapshot Kopien während der Initialisierung und Aktualisierung übertragen werden.

Sie können eine benutzerdefinierte Replikationsrichtlinie erstellen, wenn die Standardrichtlinie für eine Beziehung nicht geeignet ist. Möglicherweise möchten Sie z. B. Daten in einem Netzwerktransfer komprimieren oder die Anzahl der Versuche ändern, wie SnapMirror Snapshot Kopien übertragen möchte.

Über diese Aufgabe

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

Schritt

1. Erstellen einer benutzerdefinierten Replizierungsrichtlinie:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Ab ONTAP 9.5 können Sie den Zeitplan für das Erstellen eines gemeinsamen Zeitplans für SnapMirror Synchronous Beziehungen mit dem festlegen `-common-snapshot-schedule` Parameter. Standardmäßig beträgt der Zeitplan für synchrone Snapshot-Kopien für SnapMirror Beziehungen eine Stunde. Für den Zeitplan der Snapshot-Kopien für synchrone Beziehungen von SnapMirror können Sie einen Wert von 30 Minuten bis zwei Stunden 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 einheitliche Replizierung erstellt:

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

Nachdem Sie fertig sind

Bei Richtlinientypen „`mmirror-Vault`“ müssen Regeln definiert werden, die bestimmen, welche Snapshot-Kopien während der Initialisierung und Aktualisierung übertragen werden.

Verwenden Sie die `snapmirror policy show` Befehl zur Überprüfung, ob die SnapMirror-Richtlinie erstellt wurde Eine vollständige Befehlssyntax finden Sie in der man-Page.

Definieren Sie eine Regel für eine Richtlinie

Für benutzerdefinierte Richtlinien mit dem Richtlinientyp „`mmirror-Vault`“ müssen Sie mindestens eine Regel definieren, die bestimmt, welche Snapshot-Kopien während der Initialisierung und Aktualisierung übertragen werden. Sie können auch Regeln für Standardrichtlinien mit dem Richtlinientyp „`mmirror-Vault`“ definieren.

Über diese Aufgabe

Jede Richtlinie mit dem Richtlinientyp „`mmirror-Vault`“ muss über eine Regel verfügen, die angibt, welche Snapshot Kopien repliziert werden sollen. Die Regel „`bi-monthly`“ gibt beispielsweise an, dass nur Snapshot Kopien, denen das SnapMirror Label „`bi-monthly`“ zugewiesen wurde, repliziert werden sollten. Wenn Sie Element Snapshot Kopien konfigurieren, weisen Sie die SnapMirror-Bezeichnung zu.

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/Vaulting	Eine von SnapMirror erstellte Snapshot Kopie wird bei Initialisierung und Update übertragen.
Täglich	Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`dily`“ werden bei Initialisierung und Update übertragen.

Wöchentlich	Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`Weekly`“ werden bei Initialisierung und Update übertragen.
Monatlich	Mirror-Vault	Neue Snapshot-Kopien auf der Quelle mit dem SnapMirror-Label „`monthly`“ werden bei Initialisierung und Update übertragen.

Sie können bei Bedarf zusätzliche Regeln für Standard- oder benutzerdefinierte Richtlinien festlegen. Beispiel:

- Für die Standardeinstellung `MirrorAndVault` Richtlinie: Sie können eine Regel mit dem Namen „`bi-monthly`“ erstellen, die Snapshot-Kopien der Quelle mit dem „`bi-monthly`“ SnapMirror Label übereinstimmt.
- Für eine individuelle Policy mit dem Richtlinientyp „`mmirror-Vault`“ könnten Sie eine Regel namens „`bi-Weekly`“ erstellen, die Snapshot-Kopien auf der Quelle mit dem „`bi-Weekly`“ SnapMirror-Etikett übereinstimmt.

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`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird eine Regel mit dem SnapMirror-Label hinzugefügt `bi-monthly` Auf den Standardwert `MirrorAndVault` Richtlinie:

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

   Im folgenden Beispiel wird eine Regel mit dem SnapMirror-Label hinzugefügt `bi-weekly` Auf den Benutzer `my_snapvault` Richtlinie:

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

   Im folgenden Beispiel wird eine Regel mit dem SnapMirror-Label hinzugefügt `app_consistent` Auf den Benutzer `Sync` Richtlinie:

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

Sie können dann Snapshot Kopien aus dem Quell-Cluster replizieren, die mit diesem SnapMirror Etikett übereinstimmen:

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

Erstellen einer Replikationsbeziehung

Erstellen einer Beziehung von einer Element Quelle zu einem ONTAP Ziel

Die Beziehung zwischen dem Quell-Volume im primären Storage und dem Ziel-Volume im sekundären Storage wird als „*Data Protection Relationship*“ bezeichnet. Sie können das verwenden `snapmirror create` Befehl zum Erstellen einer Datensicherungsbeziehung von einer Element Quelle zu einem ONTAP Ziel oder von einer ONTAP Quelle zu einem Element Ziel

Mithilfe von SnapMirror werden Snapshot Kopien eines Element Volume in ein ONTAP Zielsystem repliziert. Bei einem Ausfall am Element Standort können Sie Clients über das ONTAP System Daten bereitstellen und das Element Quell-Volume nach Wiederherstellung des Service erneut aktivieren.

Bevor Sie beginnen

- Der Element-Node, der das zu replizierende Volume enthält, muss ONTAP zugänglich gemacht werden.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.
- Wenn Sie die Richtlinie „`mmirror-Vault`“ verwenden, muss ein SnapMirror Label konfiguriert worden sein, damit die Element Snapshot Kopien repliziert werden können.

> Diese Aufgabe kann nur in der Web-Benutzeroberfläche der Element Software ausgeführt werden. Weitere Informationen finden Sie im "Dokumentation des Elements".

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben `hostip:/lun/name`, Wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ und ist `name` Ist der Name des Element Volume.

Ein Element Volume ist in etwa dem einer ONTAP LUN entsprechenden Modus. SnapMirror erstellt eine LUN mit dem Namen des Element-Volume, wenn eine Datensicherungsbeziehung zwischen Element Software und ONTAP initialisiert wird. SnapMirror repliziert Daten in eine vorhandene LUN, wenn die LUN die Anforderungen für die Replizierung von Element Software zu ONTAP erfüllt.

Replikationsregeln:

- Ein ONTAP Volume kann nur Daten aus einem Element Volume enthalten.
- Es können keine Daten von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Ab ONTAP 9.3 und älteren Versionen kann ein Ziel-Volume bis zu 251 Snapshot Kopien enthalten. Ab ONTAP 9.4 kann ein Ziel-Volume bis zu 1019 Snapshot Kopien enthalten.

Schritt

1. Erstellen Sie vom Ziel-Cluster eine Replizierungsbeziehung von einer Elementquelle zu einem ONTAP

Ziel:

```
snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume
|cluster://SVM/volume -type XDP -schedule schedule -policy policy
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mit dem Standard erstellt `MirrorLatest` Richtlinie:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

Im folgenden Beispiel wird eine einheitliche Replizierungsbeziehung mit dem Standard erstellt `MirrorAndVault` Richtlinie:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

Im folgenden Beispiel wird eine einheitliche Replizierungsbeziehung mit dem erstellt `Unified7year` Richtlinie:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

Im folgenden Beispiel wird eine einheitliche Replikationsbeziehung mit dem benutzerdefinierten erstellt `my_unified` Richtlinie:

```
cluster_dst::> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

Nachdem Sie fertig sind

Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Erstellen einer Beziehung von einer ONTAP Quelle zu einem Element Ziel

Ab ONTAP 9.4 können Sie SnapMirror verwenden, um Snapshot Kopien einer auf einer ONTAP Quelle erstellten LUN zurück zu einem Element Ziel zu replizieren. Möglicherweise verwenden Sie die LUN, um Daten von ONTAP zu Element Software zu

migrieren.

Bevor Sie beginnen

- Der Ziel-Node für Element muss ONTAP zugänglich gemacht worden sein.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.

Über diese Aufgabe

Sie müssen den Zielpfad für das Element im Formular angeben `hostip:/lun/name`, Wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ und ist `name` Ist der Name des Element Volume.

Replikationsregeln:

- Die Replizierungsbeziehung muss über eine Richtlinie vom Typ „`async-Mirror`“ verfügen.

  Sie können eine Standard- oder eine benutzerdefinierte Richtlinie verwenden.

- Es werden nur iSCSI LUNs unterstützt.
- Es kann nicht mehr als eine LUN aus einem ONTAP Volume in ein Element Volume repliziert werden.
- Eine LUN kann nicht von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Schritt

1. Replizierungsbeziehung von einer ONTAP-Quelle zu einem Element-Ziel erstellen:

   `snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -type XDP -schedule schedule -policy policy`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mit dem Standard erstellt `MirrorLatest` Richtlinie:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy MirrorLatest
   ```

   Im folgenden Beispiel wird eine SnapMirror DR-Beziehung mit dem benutzerdefinierten erstellt `my_mirror` Richtlinie:

   ```
   cluster_dst::> snapmirror create -source-path svm_1:volA_dst
   -destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
   -policy my_mirror
   ```

Nachdem Sie fertig sind

Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Initialisieren Sie eine Replikationsbeziehung

Bei allen Beziehungstypen führt die Initialisierung einen *Baseline Transfer* durch: Es erstellt eine Snapshot Kopie des Quell-Volume und überträgt dann die Kopie und alle Datenblöcke, auf die sie auf das Ziel-Volume verweist.

Bevor Sie beginnen

- Der Element-Node, der das zu replizierende Volume enthält, muss ONTAP zugänglich gemacht werden.
- Das Element Volume muss für die SnapMirror Replizierung aktiviert worden sein.
- Wenn Sie die Richtlinie „`mmirror-Vault`“ verwenden, muss ein SnapMirror Label konfiguriert worden sein, damit die Element Snapshot Kopien repliziert werden können.

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben *`hostip:`*`/lun/`*`name`*, Wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ und ist *`name`* Ist der Name des Element Volume.

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

> Wenn die Initialisierung einer Beziehung von einer ONTAP Quelle zu einem Element Ziel aus irgendeinem Grund fehlschlägt, wird sie weiterhin fehlschlagen, selbst wenn Sie das Problem behoben haben (z. B. ein ungültiger LUN-Name). Die Behelfslösung sieht wie folgt aus:
>
> 1. Löschen Sie die Beziehung.
> 2. Löschen Sie das Element Ziel-Volume.
> 3. Erstellung eines neuen Element Ziel-Volume
> 4. Erstellen und Initialisieren einer neuen Beziehung von der ONTAP Quelle auf das Ziel-Volume des Element

Schritt

1. Initialisieren einer Replikationsbeziehung:

   `snapmirror initialize -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume|cluster://SVM/volume`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume initialisiert `0005` An der IP-Adresse 10.0.0.11 und dem Zielvolume `volA_dst` Ein `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

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

Das Zielvolumen schreibbar machen

Wenn der primäre Standort für eine SnapMirror DR-Beziehung aufgrund einer Katastrophe deaktiviert wird, können Sie Daten vom Ziel-Volume mit minimaler Unterbrechung bereitstellen. Sie können das Quell-Volume neu aktivieren, wenn der Service am primären Standort wiederhergestellt ist.

Sie müssen das Ziel-Volume schreibbar machen, bevor Sie Daten vom Volume an die Clients bereitstellen können. Sie können das verwenden `snapmirror quiesce` Befehl zum Anhalten geplanter Transfers an das Ziel, das `snapmirror abort` Befehl zum Beenden laufender Transfers, und `snapmirror break` Befehl, um das Ziel beschreibbar zu machen.

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben *`hostip:`*`/lun/`*`name`*, Wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ und ist `name` Ist der Name des Element Volume.

Schritte

1. Geplante Transfers zum Ziel anhalten:

   `snapmirror quiesce -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|` *`cluster://SVM/volume`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden geplante Transfers zwischen dem Quell-Volume angehalten `0005` An der IP-Adresse 10.0.0.11 und dem Zielvolume `volA_dst` Ein `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

2. Laufende Transfers zum Ziel anhalten:

   `snapmirror abort -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|` *`cluster://SVM/volume`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden kontinuierliche Transfers zwischen dem Quell-Volume angehalten `0005` An der IP-Adresse 10.0.0.11 und dem Zielvolume `volA_dst` Ein `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005
   -destination-path svm_backup:volA_dst
   ```

3. SnapMirror DR-Beziehung unterbrechen:

   `snapmirror break -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`* `|` *`cluster://SVM/volume`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume unterbrochen `0005` An der IP-Adresse 10.0.0.11 und dem Zielvolume `volA_dst` Ein `svm_backup` Und dem Ziel-Volume `volA_dst` Ein `svm_backup`:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Ziel-Volume für Datenzugriff konfigurieren

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

1. Ordnen Sie die Element LUN der entsprechenden Initiatorgruppe zu.
2. Erstellen Sie iSCSI-Sitzungen von den SAN-Host-Initiatoren zu den SAN-LIFs.
3. Führen Sie auf dem SAN-Client einen erneuten Speicherscan durch, um die verbundene LUN zu erkennen.

Aktivieren Sie das ursprüngliche Quellvolume 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.

Sie müssen den Quellpfad des Elements im Formular angeben *`hostip:`*`/lun/`*`name`*, Wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ und ist `name` Ist der Name des Element Volume.

Ab ONTAP 9.4 werden Snapshot Kopien einer während der Datenbereitstellung erstellten LUN vom ONTAP Ziel automatisch repliziert, wenn die Element Quelle neu aktiviert wird.

Replikationsregeln:

- Es werden nur iSCSI LUNs unterstützt.
- Es kann nicht mehr als eine LUN aus einem ONTAP Volume in ein Element Volume repliziert werden.
- Eine LUN kann nicht von einem ONTAP Volume auf mehrere Element Volumes repliziert werden.

Schritte

1. Löschen Sie die ursprüngliche Datensicherungsbeziehung:

   `snapmirror delete -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`* `-policy` *`policy`*

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Quell-Volume gelöscht, `0005` Unter der IP-Adresse 10.0.0.11 und dem Volume, von dem Sie Daten bereitstellen, `volA_dst` Ein `svm_backup`:

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Umkehren der ursprünglichen Datensicherungsbeziehung:

   `snapmirror resync -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name -policy policy`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   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 ursprünglichen Quell-Volume umkehren: `0005` Unter der IP-Adresse 10.0.0.11 und dem Volume, von dem Sie Daten bereitstellen, `volA_dst` Ein `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Aktualisierung der umgekehrten Beziehung:

   `snapmirror update -source-path` *`SVM:volume|cluster://SVM/volume`* `-destination -path` *`hostip:`*`/lun/`*`name`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Der Befehl schlägt fehl, wenn eine allgemeine Snapshot Kopie nicht auf dem Quell- und Zielsystem vorhanden ist. Nutzung `snapmirror initialize` Um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen dem Volume, von dem Sie Daten bereitstellen, aktualisiert. `volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `0005` Unter der IP-Adresse 10.0.0.11:

```
cluster_dst::> snapmirror update -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

4. Geplante Transfers für die umgekehrte Beziehung stoppen:

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

`-path hostip:/lun/name`

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden geplante Transfers zwischen dem Volume, von dem Sie Daten bereitstellen, angehalten. `volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `0005` Unter der IP-Adresse 10.0.0.11:

```
cluster_dst::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

5. Laufende Transfers für die umgekehrte Beziehung stoppen:

   `snapmirror abort -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die laufenden Transfers zwischen dem Volume, von dem Sie Daten bereitstellen, angehalten. `volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `0005` Unter der IP-Adresse 10.0.0.11:

```
cluster_dst::> snapmirror abort -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

6. Zerbrechen der umgekehrten Beziehung:

   `snapmirror break -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel unterbricht die Beziehung zwischen dem Volume, aus dem Sie Daten bereitstellen, `volA_dst` Ein `svm_backup`, Und das ursprüngliche Quellvolumen, `0005` Unter der IP-Adresse 10.0.0.11:

```
cluster_dst::> snapmirror break -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005
```

7. Löschen Sie die umgekehrte Datensicherungsbeziehung:

   `snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination -path hostip:/lun/name -policy policy`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die umgekehrte Beziehung zwischen dem ursprünglichen Quell-Volume gelöscht, `0005` Unter der IP-Adresse 10.0.0.11 und dem Volume, von dem Sie Daten bereitstellen, `volA_dst` Ein `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Wiederherstellung der ursprünglichen Datensicherungsbeziehung:

   `snapmirror resync -source-path` *`hostip`*`:/lun/`*`name`* `-destination-path` *`SVM:volume`*`|`*`cluster://SVM/volume`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Beziehung zwischen dem ursprünglichen Quell-Volume wiederhergestellt. `0005` An der IP-Adresse 10.0.0.11 und dem ursprünglichen Ziel-Volume, `volA_dst` Ein `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Nachdem Sie fertig sind

Verwenden Sie die `snapmirror show` Befehl zur Überprüfung, ob die SnapMirror Beziehung erstellt wurde. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Aktualisieren Sie eine Replikationsbeziehung manuell

Möglicherweise müssen Sie eine Replikationsbeziehung manuell aktualisieren, wenn ein Update aufgrund eines Netzwerkfehlers fehlschlägt.

Über diese Aufgabe

Sie müssen den Quellpfad des Elements im Formular angeben *`hostip:`*`/lun/`*`name`*, Wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ und ist `name` Ist der Name des Element Volume.

Schritte

1. Manuelles Aktualisieren einer Replikationsbeziehung:

   `snapmirror update -source-path` *`hostip:`*`/lun/`*`name`* `-destination-path` *`SVM:volume`*`|`*`cluster://SVM/volume`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Der Befehl schlägt fehl, wenn eine allgemeine Snapshot Kopie nicht auf dem Quell- und Zielsystem vorhanden ist. Nutzung `snapmirror initialize` Um die Beziehung neu zu initialisieren.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume aktualisiert `0005` An der IP-Adresse 10.0.0.11 und dem Zielvolume `volA_dst` Ein `svm_backup`:

```
cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst
```

Synchronisieren Sie eine Replikationsbeziehung neu

Sie müssen eine Replizierungsbeziehung neu synchronisieren, nachdem Sie ein Ziel-Volume schreibbar machen, nachdem ein Update fehlschlägt, weil eine gemeinsame Snapshot-Kopie nicht auf den Quell- und Ziel-Volumes vorhanden ist oder Sie die Replizierungsrichtlinie für die Beziehung ändern möchten.

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.

Sie müssen den Quellpfad des Elements im Formular angeben `hostip:/lun/name`, Wobei „`lun`“ die tatsächliche Zeichenfolge „`lun`“ und ist `name` Ist der Name des Element Volume.

Schritt

1. Neusynchronisierung der Quell- und Ziel-Volumes:

   ```
   snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume
   |cluster://SVM/volume -type XDP -policy policy
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird die Beziehung zwischen dem Quell-Volume neu synchronisiert `0005` An der IP-Adresse 10.0.0.11 und dem Zielvolume `volA_dst` Ein `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005
   -policy MirrorLatest -destination-path svm_backup:volA_dst
   ```