TR-4931: Notfallwiederherstellung mit VMware Cloud auf Amazon Web Services und Guest Connect

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Inhalt

TR-4931: Notfallwiederherstellung mit VMware Cloud auf Amazon Web Services und Guest Connect 1
- Überblick 1
- Annahmen, Voraussetzungen und Komponentenübersicht 1
- Durchführen von DR mit SnapCenter 2
  - Konfigurieren Sie SnapMirror -Beziehungen und Aufbewahrungspläne 2
  - Stellen Sie den Windows SnapCenter -Server vor Ort bereit und konfigurieren Sie ihn. 11
  - Bereitstellen und Konfigurieren des Veeam Backup Servers 19
  - BlueXP backup and recovery und Wiederherstellungstools und -Konfiguration 30
  - SnapCenter -Datenbanksicherung für die Notfallwiederherstellung 31
  - Ausfallsicherung 39
  - Wiederherstellen von Anwendungs-VMs mit der vollständigen Wiederherstellung von Veeam 43
  - Wiederherstellen von SQL Server-Anwendungsdaten 56
  - Wiederherstellen von Oracle-Anwendungsdaten 65
  - Failback 71
- Abschluss 71

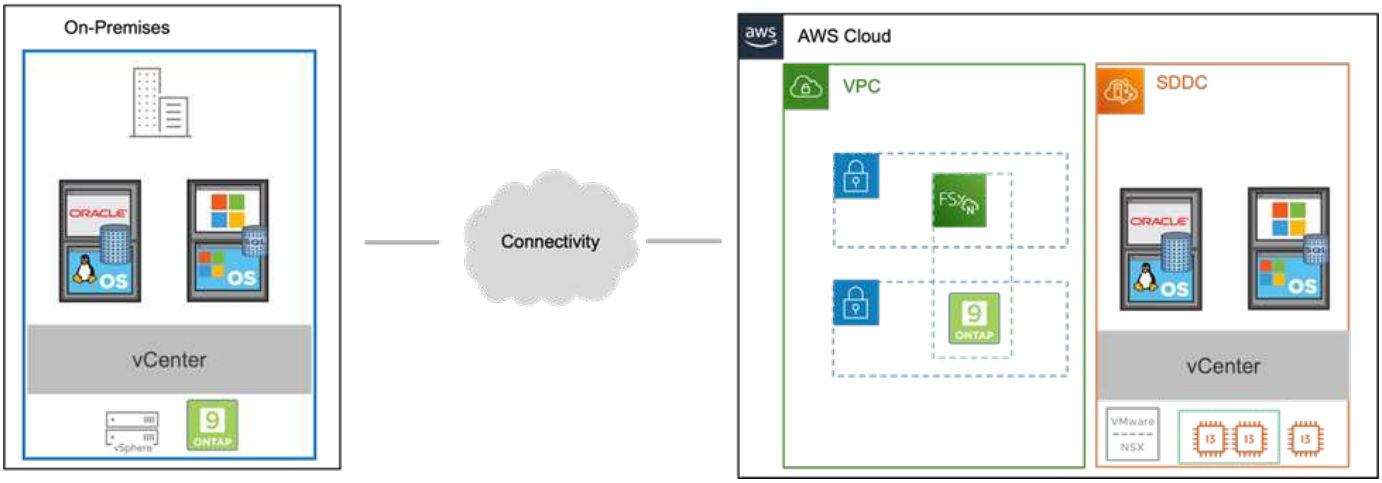
TR-4931: Notfallwiederherstellung mit VMware Cloud auf Amazon Web Services und Guest Connect

Eine bewährte Disaster Recovery-Umgebung (DR) und ein entsprechender Plan sind für Unternehmen von entscheidender Bedeutung, um sicherzustellen, dass geschäftskritische Anwendungen im Falle eines größeren Ausfalls schnell wiederhergestellt werden können. Diese Lösung konzentriert sich auf die Demonstration von DR-Anwendungsfällen mit Schwerpunkt auf VMware- und NetApp -Technologien, sowohl vor Ort als auch mit VMware Cloud auf AWS.

Überblick

NetApp verfügt über eine lange Tradition der Integration mit VMware, wie die Zehntausende von Kunden belegen, die sich für NetApp als Speicherpartner für ihre virtualisierte Umgebung entschieden haben. Diese Integration wird mit Gastverbindungsoptionen in der Cloud und kürzlichen Integrationen mit NFS-Datenspeichern fortgesetzt. Diese Lösung konzentriert sich auf den Anwendungsfall, der allgemein als gastverbundener Speicher bezeichnet wird.

Bei einem mit dem Gast verbundenen Speicher wird die Gast-VMDK auf einem von VMware bereitgestellten Datenspeicher bereitgestellt und Anwendungsdaten werden auf iSCSI oder NFS gespeichert und direkt der VM zugeordnet. Zur Demonstration eines DR-Szenarios werden Oracle- und MS SQL-Anwendungen verwendet, wie in der folgenden Abbildung dargestellt.



Annahmen, Voraussetzungen und Komponentenübersicht

Lesen Sie vor der Bereitstellung dieser Lösung die Übersicht über die Komponenten, die erforderlichen Voraussetzungen für die Bereitstellung der Lösung und die Annahmen, die bei der Dokumentation dieser Lösung getroffen wurden.

"Anforderungen, Voraussetzungen und Planung der DR-Lösung"

Durchführen von DR mit SnapCenter

In dieser Lösung bietet SnapCenter anwendungskonsistente Snapshots für SQL Server- und Oracle-Anwendungsdaten. Diese Konfiguration bietet zusammen mit der SnapMirror -Technologie eine Hochgeschwindigkeits-Datenreplikation zwischen unserem lokalen AFF und FSx ONTAP Cluster. Darüber hinaus bietet Veeam Backup & Replication Sicherungs- und Wiederherstellungsfunktionen für unsere virtuellen Maschinen.

In diesem Abschnitt behandeln wir die Konfiguration von SnapCenter, SnapMirror und Veeam für Sicherung und Wiederherstellung.

In den folgenden Abschnitten werden die Konfiguration und die Schritte beschrieben, die zum Durchführen eines Failovers am sekundären Standort erforderlich sind:

Konfigurieren Sie SnapMirror -Beziehungen und Aufbewahrungspläne

SnapCenter kann SnapMirror -Beziehungen innerhalb des primären Speichersystems (primär > Spiegel) und zu sekundären Speichersystemen (primär > Tresor) zum Zweck der langfristigen Archivierung und Aufbewahrung aktualisieren. Dazu müssen Sie mithilfe von SnapMirror eine Datenreplikationsbeziehung zwischen einem Zielvolume und einem Quellvolume herstellen und initialisieren.

Die Quell- und Ziel- ONTAP -Systeme müssen sich in Netzwerken befinden, die über Amazon VPC Peering, ein Transit Gateway, AWS Direct Connect oder ein AWS VPN verbunden sind.

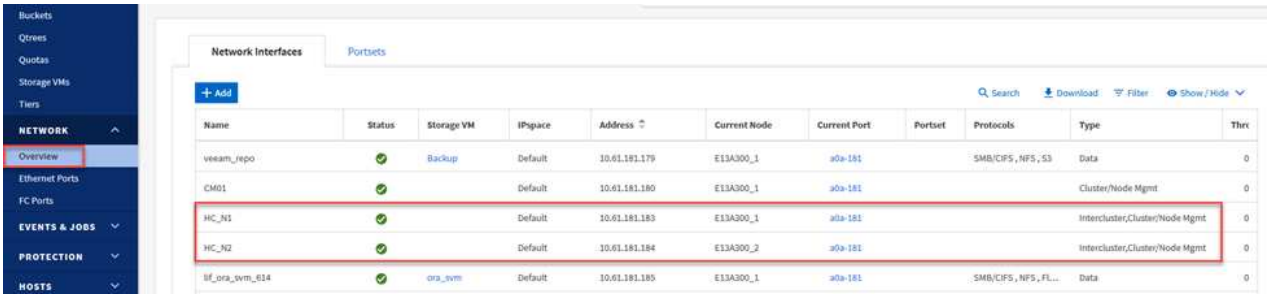
Zum Einrichten von SnapMirror -Beziehungen zwischen einem lokalen ONTAP System und FSx ONTAP sind die folgenden Schritte erforderlich:

Weitere Informationen finden Sie im "FSx ONTAP – ONTAP -Benutzerhandbuch" Weitere Informationen zum Erstellen von SnapMirror -Beziehungen mit FSx.

Notieren Sie die logischen Quell- und Zielschnittstellen zwischen Clustern.

Für das lokale ONTAP Quellsystem können Sie die LIF-Informationen zwischen den Clustern vom System Manager oder von der CLI abrufen.

1. Navigieren Sie im ONTAP System Manager zur Seite „Netzwerkübersicht“ und rufen Sie die IP-Adressen vom Typ „Intercluster“ ab, die für die Kommunikation mit dem AWS VPC konfiguriert sind, auf dem FSx installiert ist.



2. Um die Intercluster-IP-Adressen für FSx abzurufen, melden Sie sich bei der CLI an und führen Sie den folgenden Befehl aus:

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

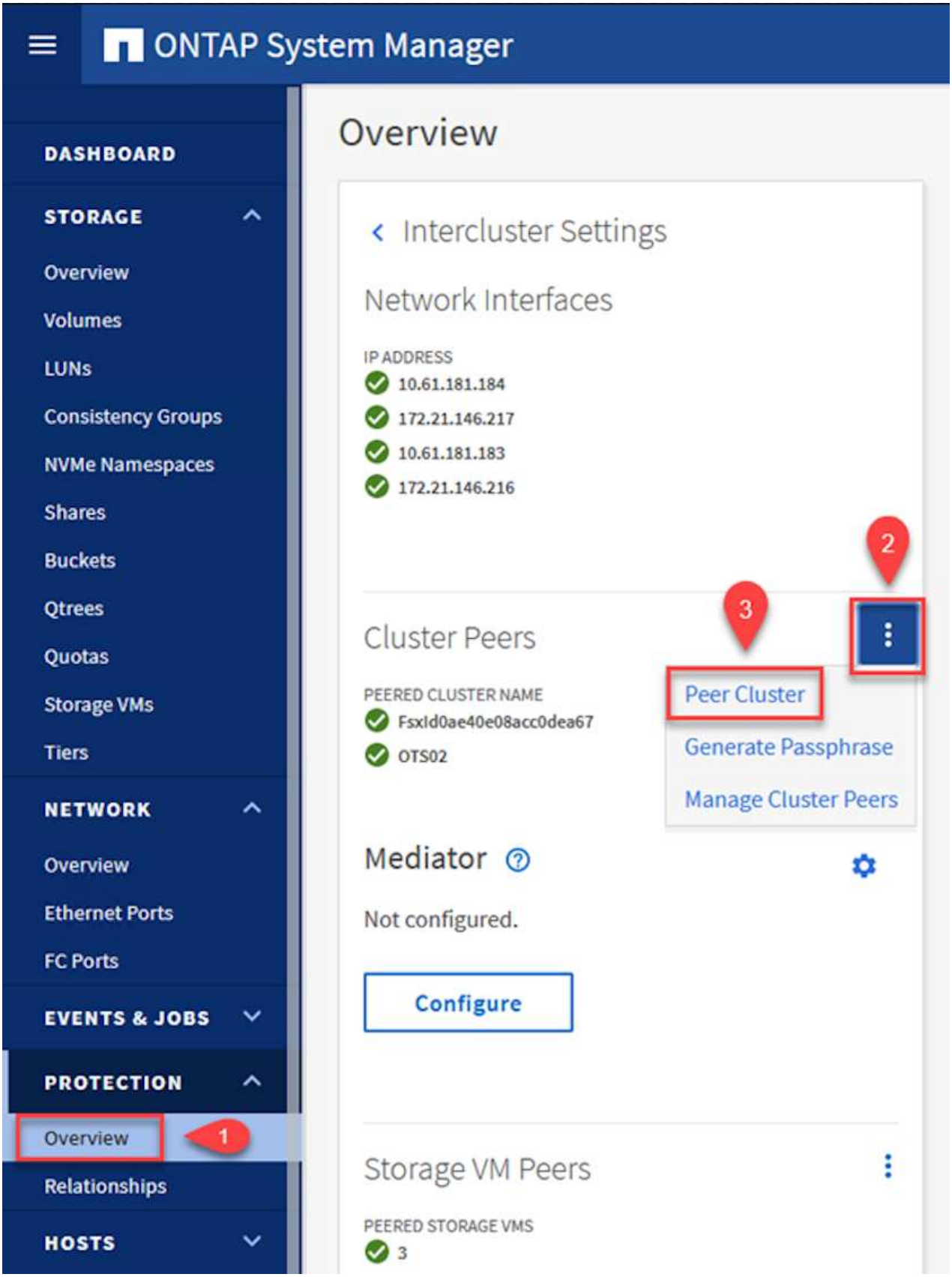
Cluster-Peering zwischen ONTAP und FSx einrichten

Um Cluster-Peering zwischen ONTAP Clustern herzustellen, muss eine eindeutige Passphrase, die im initiierenden ONTAP Cluster eingegeben wird, im anderen Peer-Cluster bestätigt werden.

1. Richten Sie Peering auf dem Ziel-FSx-Cluster mithilfe der `cluster peer create` Befehl. Geben Sie bei entsprechender Aufforderung eine eindeutige Passphrase ein, die später im Quellcluster verwendet wird, um den Erstellungsprozess abzuschließen.

   ```
   FSx-Dest::> cluster peer create -address-family ipv4 -peer-addrs
   source_intercluster_1, source_intercluster_2
   Enter the passphrase:
   Confirm the passphrase:
   ```

2. Im Quellcluster können Sie die Cluster-Peer-Beziehung entweder mit ONTAP System Manager oder der CLI herstellen. Navigieren Sie im ONTAP System Manager zu „Schutz > Übersicht“ und wählen Sie „Peer-Cluster“ aus.

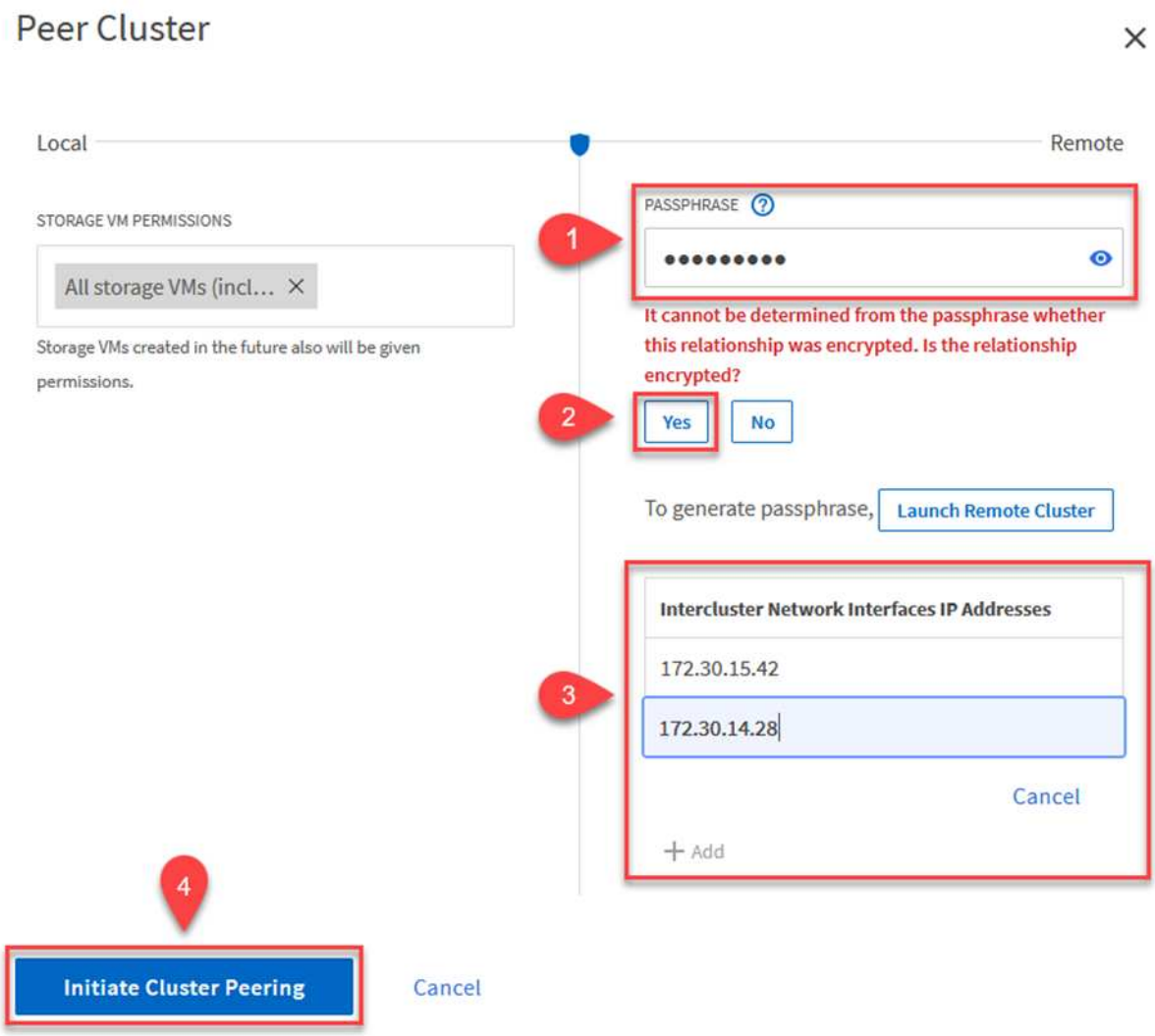


3. Geben Sie im Dialogfeld „Peer-Cluster“ die erforderlichen Informationen ein:
   a. Geben Sie die Passphrase ein, die zum Herstellen der Peer-Cluster-Beziehung im Ziel-FSx-Cluster verwendet wurde.

b. Wählen `Yes` um eine verschlüsselte Beziehung aufzubauen.

c. Geben Sie die Intercluster-LIF-IP-Adresse(n) des Ziel-FSx-Clusters ein.

d. Klicken Sie auf „Cluster-Peering starten“, um den Vorgang abzuschließen.



4. Überprüfen Sie den Status der Cluster-Peer-Beziehung vom FSx-Cluster mit dem folgenden Befehl:

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

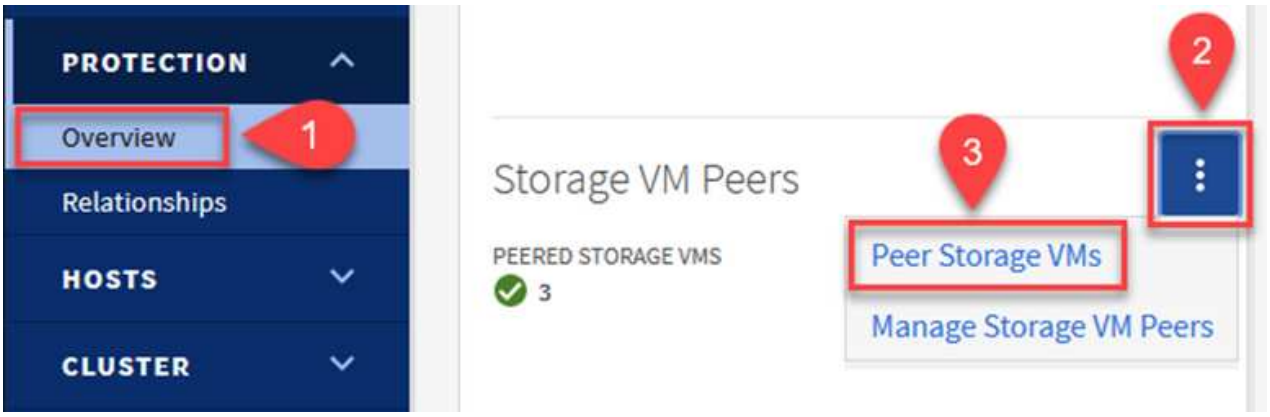
Herstellen einer SVM-Peering-Beziehung

Der nächste Schritt besteht darin, eine SVM-Beziehung zwischen den virtuellen Ziel- und Quellspeichermaschinen einzurichten, die die Volumes enthalten, die in SnapMirror -Beziehungen enthalten sein werden.

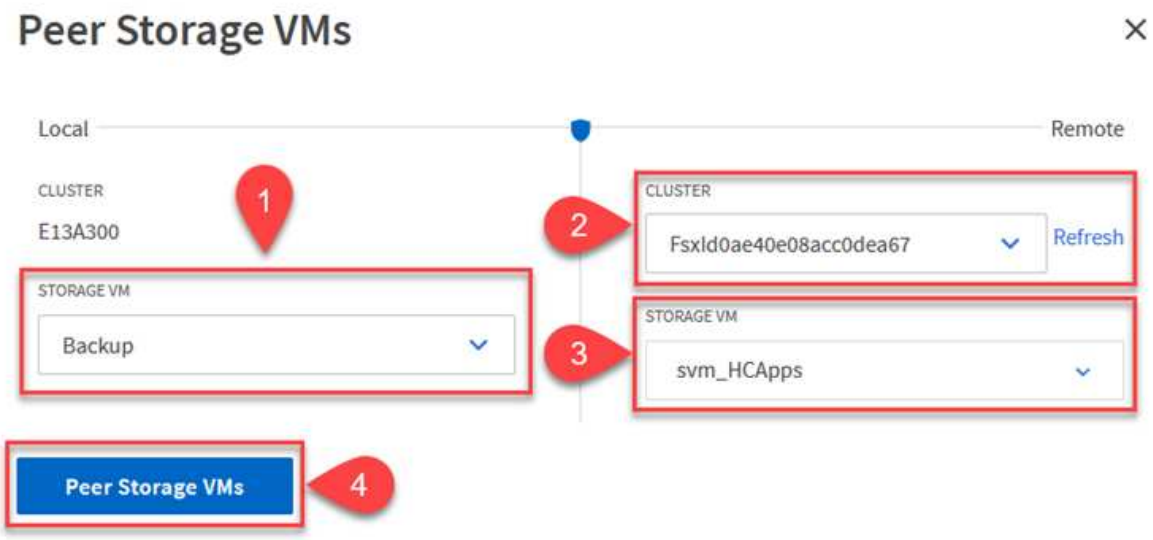
1. Verwenden Sie im Quell-FSx-Cluster den folgenden Befehl aus der CLI, um die SVM-Peer-Beziehung zu erstellen:

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. Akzeptieren Sie vom Quell ONTAP Cluster aus die Peering-Beziehung entweder mit dem ONTAP System Manager oder der CLI.
3. Gehen Sie im ONTAP System Manager zu „Schutz > Übersicht“ und wählen Sie unter „Storage VM Peers“ die Option „Peer Storage VMs“ aus.



4. Füllen Sie im Dialogfeld der Peer Storage-VM die erforderlichen Felder aus:
   - Die Quellspeicher-VM
   - Der Zielcluster
   - Die Zielspeicher-VM



5. Klicken Sie auf „Peer-Storage-VMs“, um den SVM-Peering-Prozess abzuschließen.

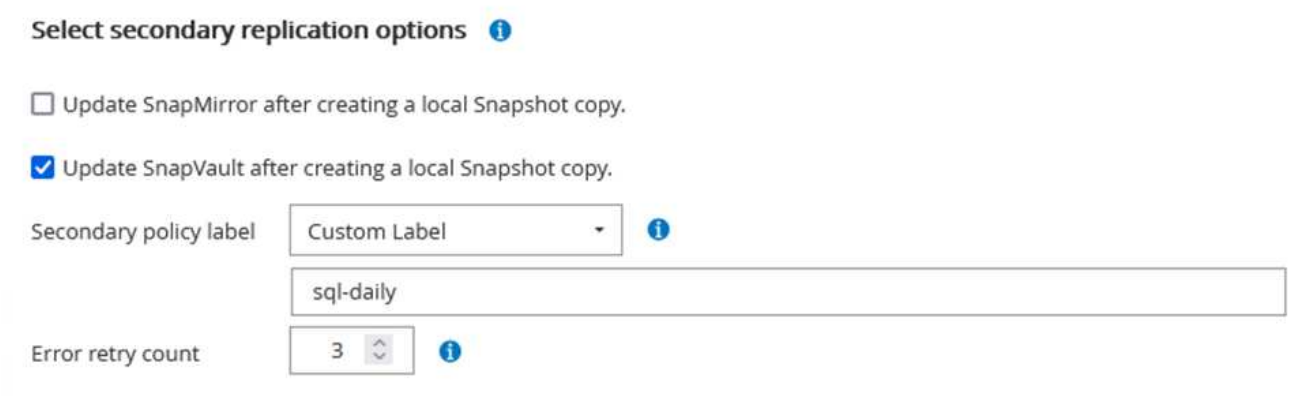
Erstellen einer Snapshot-Aufbewahrungsrichtlinie

SnapCenter verwaltet Aufbewahrungspläne für Backups, die als Snapshot-Kopien auf dem primären Speichersystem vorhanden sind. Dies wird beim Erstellen einer Richtlinie in SnapCenter festgelegt. SnapCenter verwaltet keine Aufbewahrungsrichtlinien für Backups, die auf sekundären Speichersystemen aufbewahrt werden. Diese Richtlinien werden separat über eine SnapMirror -Richtlinie verwaltet, die auf dem sekundären FSx-Cluster erstellt und den Zielvolumes zugeordnet wird, die in einer SnapMirror -Beziehung mit dem Quellvolume stehen.

Beim Erstellen einer SnapCenter -Richtlinie haben Sie die Möglichkeit, eine sekundäre Richtlinienbezeichnung anzugeben, die der SnapMirror Bezeichnung jedes Snapshots hinzugefügt wird, der beim Erstellen einer SnapCenter Sicherung generiert wird.

Auf dem sekundären Speicher werden diese Bezeichnungen mit den Richtlinienregeln des Zielvolumes abgeglichen, um die Aufbewahrung von Snapshots zu erzwingen.

Das folgende Beispiel zeigt ein SnapMirror -Label, das auf allen Snapshots vorhanden ist, die im Rahmen einer Richtlinie für tägliche Sicherungen unserer SQL Server-Datenbank und Protokollvolumes generiert werden.



Weitere Informationen zum Erstellen von SnapCenter -Richtlinien für eine SQL Server-Datenbank finden Sie im "SnapCenter -Dokumentation" .

Sie müssen zunächst eine SnapMirror -Richtlinie mit Regeln erstellen, die die Anzahl der aufzubewahrenden Snapshot-Kopien vorgeben.

1. Erstellen Sie die SnapMirror Richtlinie auf dem FSx-Cluster.

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Fügen Sie der Richtlinie Regeln mit SnapMirror -Beschriftungen hinzu, die den in den SnapCenter -Richtlinien angegebenen sekundären Richtlinienbezeichnungen entsprechen.

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

Das folgende Skript bietet ein Beispiel für eine Regel, die einer Richtlinie hinzugefügt werden könnte:

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

Erstellen Sie zusätzliche Regeln für jedes SnapMirror Label und die Anzahl der aufzubewahrenden Snapshots (Aufbewahrungszeitraum).

Zielvolumes erstellen

Um ein Zielvolume auf FSx zu erstellen, das Snapshot-Kopien von unseren Quellvolumes empfängt, führen Sie den folgenden Befehl auf FSx ONTAP aus:

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Erstellen Sie die SnapMirror -Beziehungen zwischen Quell- und Zielvolumes

Um eine SnapMirror -Beziehung zwischen einem Quell- und einem Zielvolume zu erstellen, führen Sie den folgenden Befehl auf FSx ONTAP aus:

```
FSx-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Initialisieren Sie die SnapMirror -Beziehungen

Initialisieren Sie die SnapMirror -Beziehung. Dieser Vorgang initiiert einen neuen Snapshot, der vom Quellvolume generiert wird, und kopiert ihn auf das Zielvolume.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Stellen Sie den Windows SnapCenter -Server vor Ort bereit und konfigurieren Sie ihn.

Bereitstellen von Windows SnapCenter Server vor Ort

Diese Lösung verwendet NetApp SnapCenter , um anwendungskonsistente Backups von SQL Server- und Oracle-Datenbanken zu erstellen. In Verbindung mit Veeam Backup & Replication zum Sichern von VMDKs virtueller Maschinen bietet dies eine umfassende Disaster-Recovery-Lösung für lokale und Cloud-basierte Rechenzentren.

Die SnapCenter software ist auf der NetApp Support-Site verfügbar und kann auf Microsoft Windows-Systemen installiert werden, die sich entweder in einer Domäne oder Arbeitsgruppe befinden. Eine ausführliche Planungshilfe und Installationsanleitung finden Sie auf der "NetApp Dokumentationscenter" .

Die SnapCenter software ist erhältlich unter "dieser Link" .

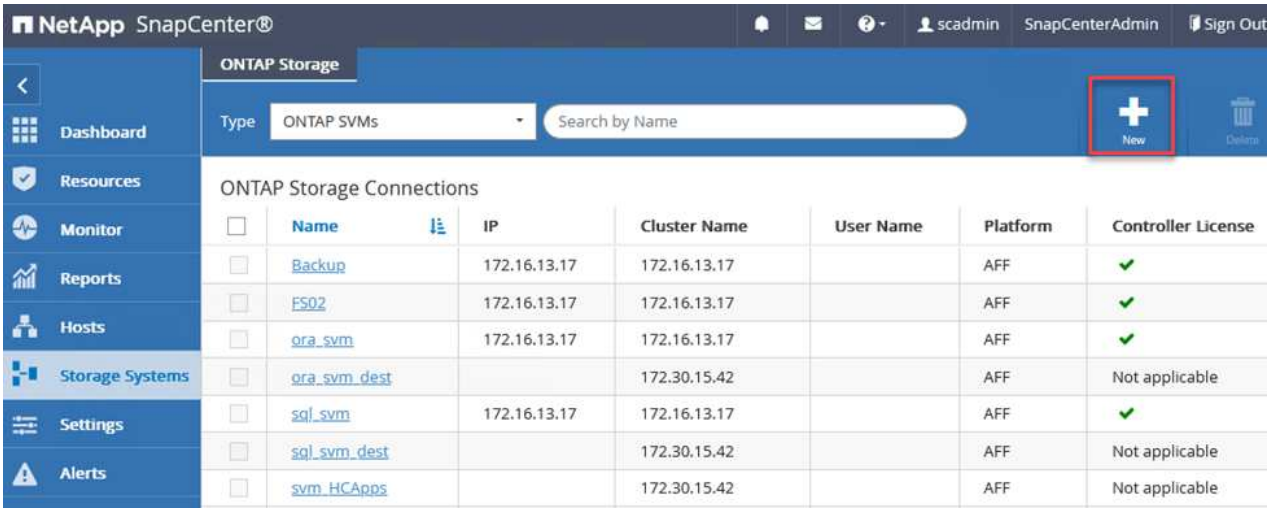
Nach der Installation können Sie über einen Webbrowser mit *https://Virtual_Cluster_IP_or_FQDN:8146* auf die SnapCenter -Konsole zugreifen.

Nachdem Sie sich bei der Konsole angemeldet haben, müssen Sie SnapCenter für die Sicherung von SQL Server- und Oracle-Datenbanken konfigurieren.

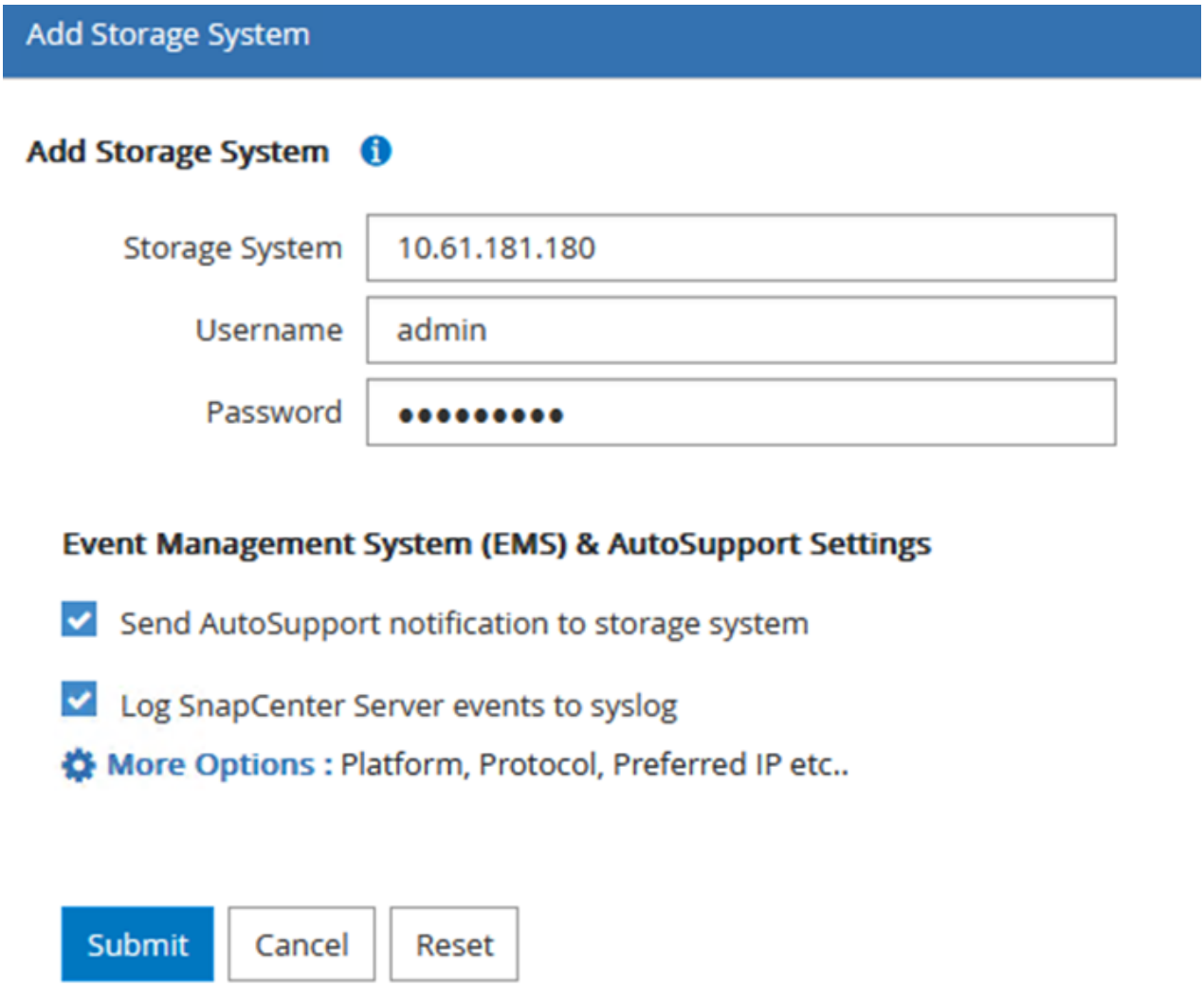
Speichercontroller zu SnapCenter hinzufügen

Führen Sie die folgenden Schritte aus, um Speichercontroller zu SnapCenter hinzuzufügen:

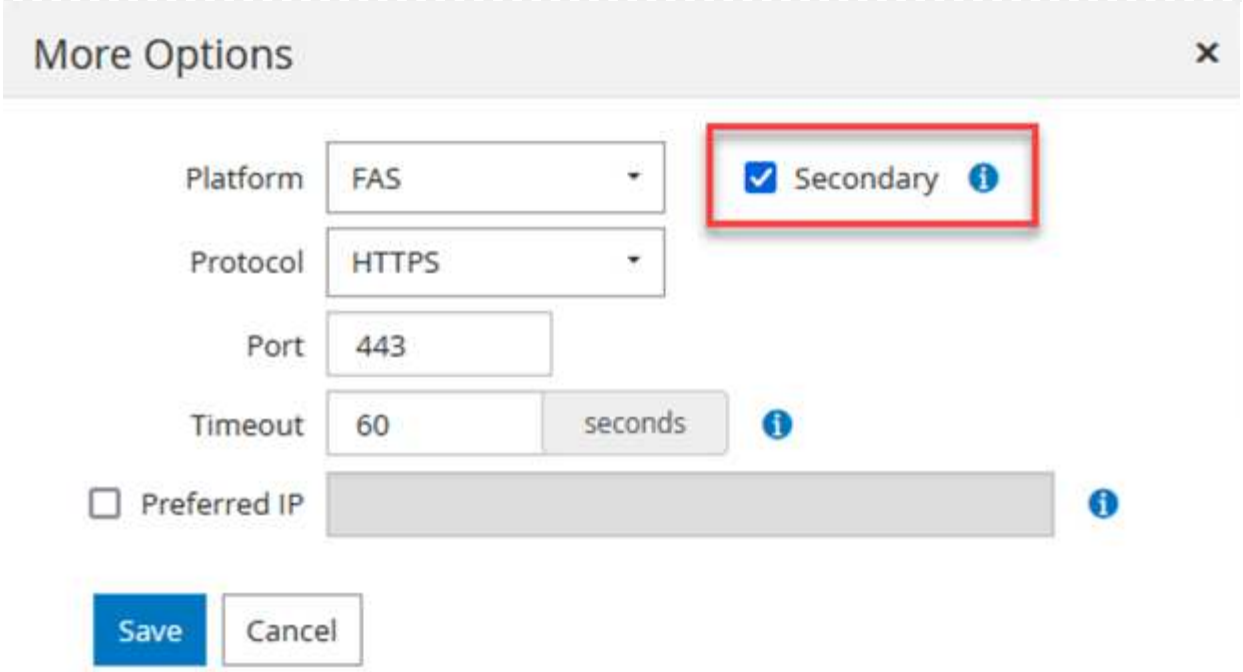
1. Wählen Sie im linken Menü „Speichersysteme“ aus und klicken Sie dann auf „Neu“, um mit dem Hinzufügen Ihrer Speichercontroller zu SnapCenter zu beginnen.



2. Fügen Sie im Dialogfeld „Speichersystem hinzufügen“ die Verwaltungs-IP-Adresse für den lokalen ONTAP -Cluster vor Ort sowie den Benutzernamen und das Kennwort hinzu. Klicken Sie dann auf „Senden“, um mit der Erkennung des Speichersystems zu beginnen.



3. Wiederholen Sie diesen Vorgang, um das FSx ONTAP -System zu SnapCenter hinzuzufügen. Wählen Sie in diesem Fall unten im Fenster „Speichersystem hinzufügen“ die Option „Weitere Optionen“ aus und aktivieren Sie das Kontrollkästchen für „Sekundär“, um das FSx-System als sekundäres Speichersystem festzulegen, das mit SnapMirror Kopien oder unseren primären Sicherungs-Snapshots aktualisiert wird.

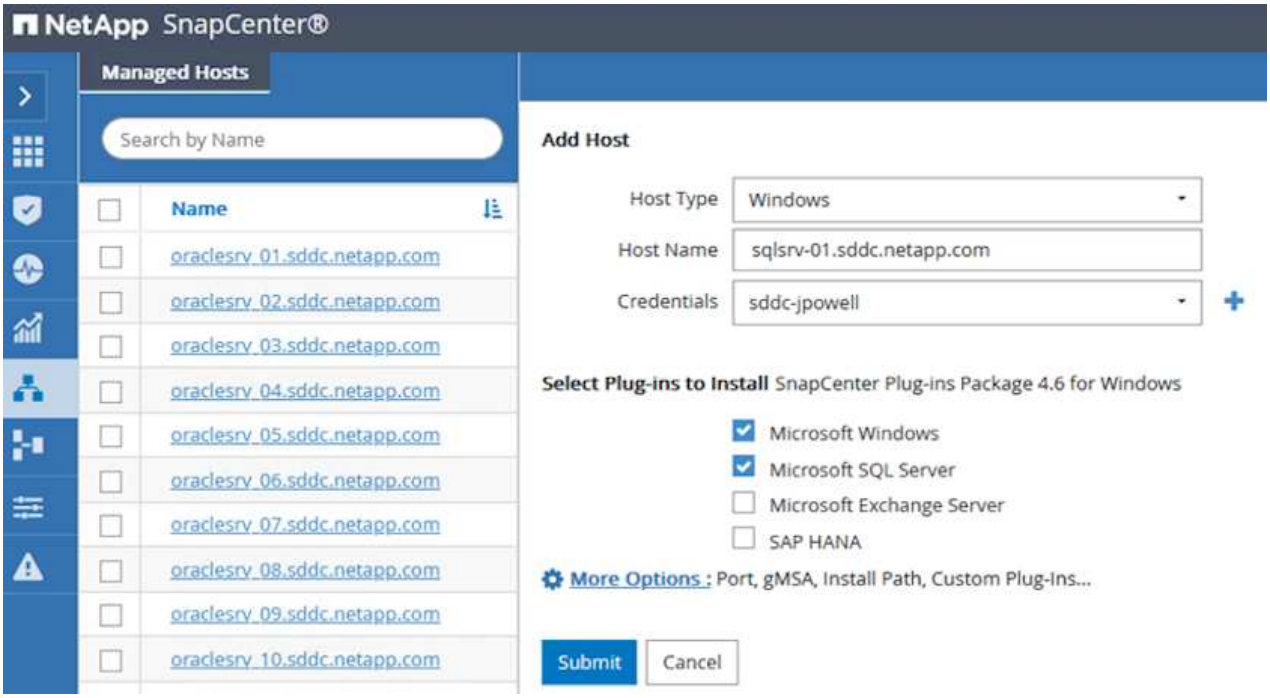


Weitere Informationen zum Hinzufügen von Speichersystemen zu SnapCenter finden Sie in der Dokumentation unter "dieser Link" .

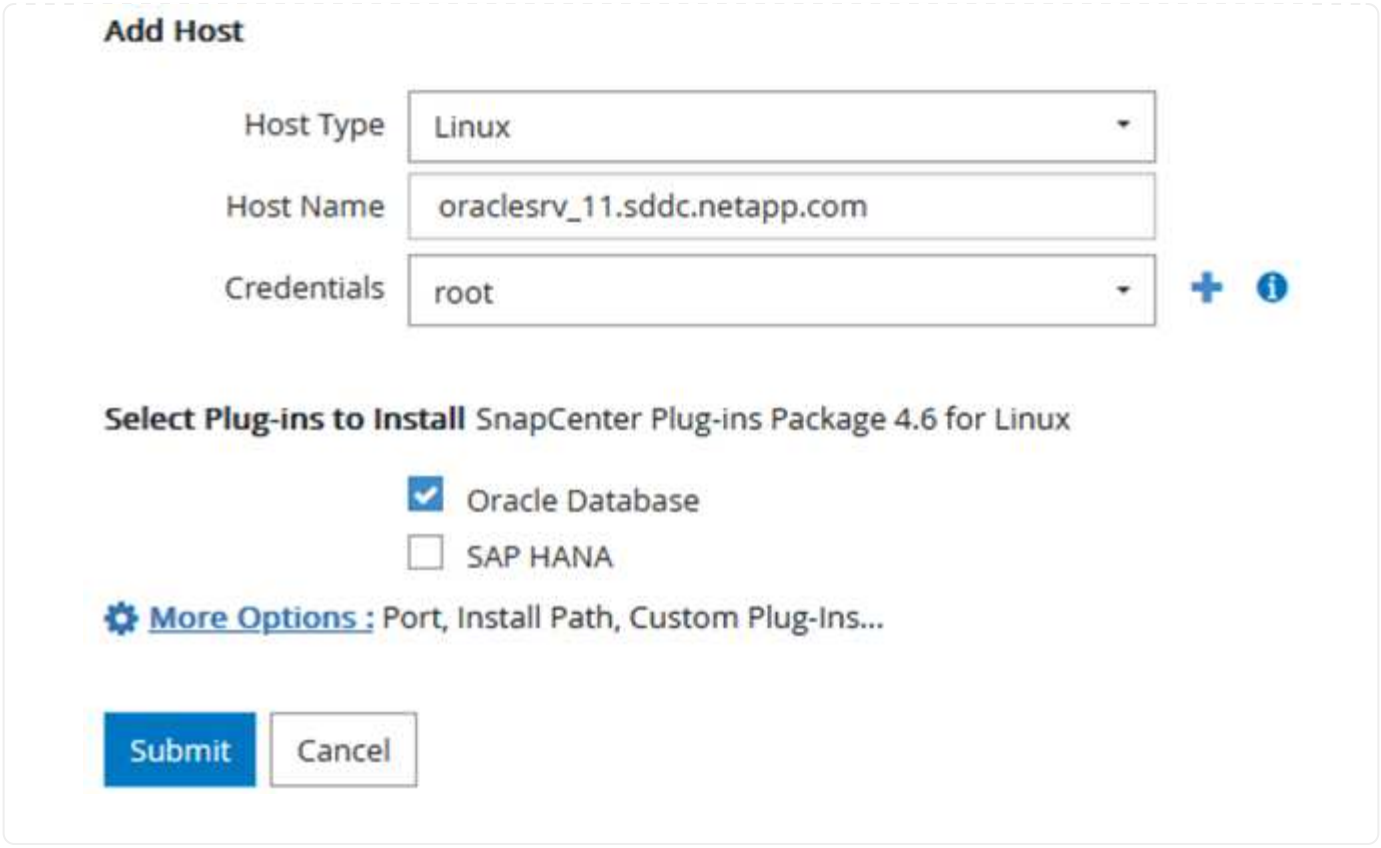
Hosts zu SnapCenter hinzufügen

Der nächste Schritt besteht darin, Hostanwendungsserver zu SnapCenter hinzuzufügen. Der Prozess ist für SQL Server und Oracle ähnlich.

1. Wählen Sie im linken Menü „Hosts“ aus und klicken Sie dann auf „Hinzufügen“, um mit dem Hinzufügen von Speichercontrollern zu SnapCenter zu beginnen.
2. Fügen Sie im Fenster „Hosts hinzufügen“ den Hosttyp, den Hostnamen und die Anmeldeinformationen des Hostsystems hinzu. Wählen Sie den Plug-In-Typ aus. Wählen Sie für SQL Server das Plug-In „Microsoft Windows und Microsoft SQL Server“ aus.



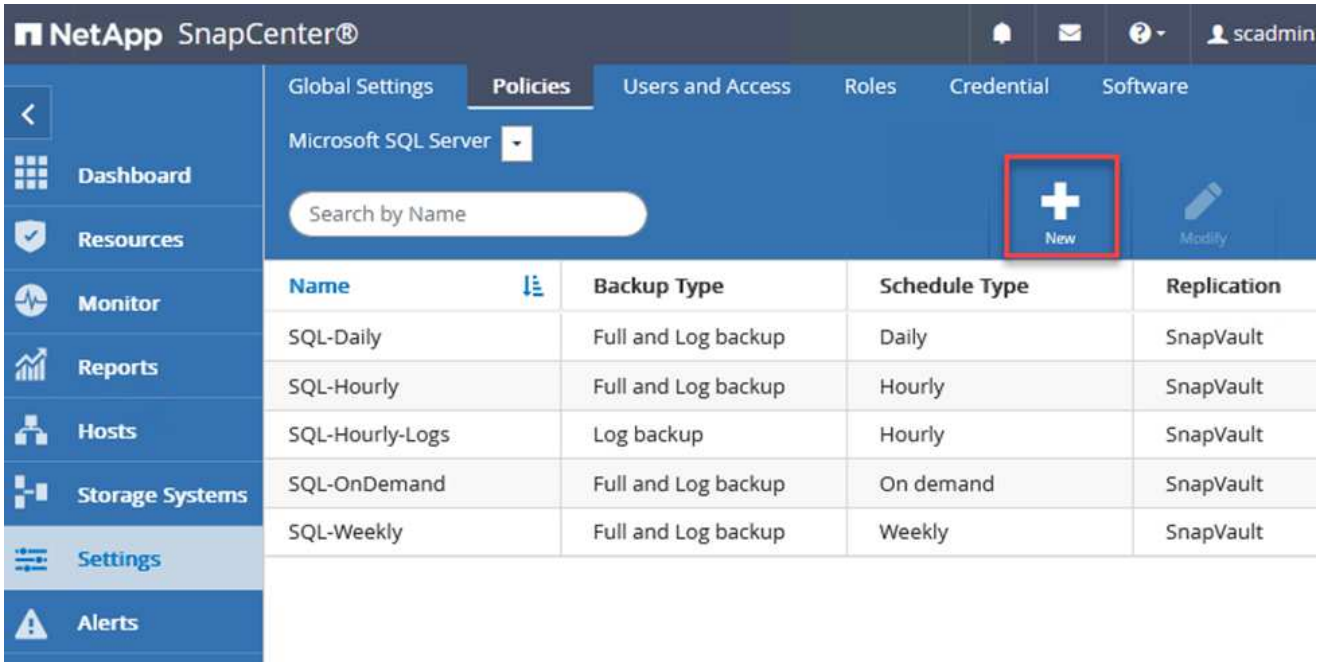
3. Füllen Sie für Oracle die erforderlichen Felder im Dialogfeld „Host hinzufügen“ aus und aktivieren Sie das Kontrollkästchen für das Oracle-Datenbank-Plug-In. Klicken Sie anschließend auf „Senden“, um den Erkennungsprozess zu starten und den Host zu SnapCenter hinzuzufügen.


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

Erstellen von SnapCenter -Richtlinien

Richtlinien legen die spezifischen Regeln fest, die für einen Sicherungsauftrag befolgt werden müssen. Hierzu gehören unter anderem der Sicherungszeitplan, der Replikationstyp und die Art und Weise, wie SnapCenter mit der Sicherung und Kürzung von Transaktionsprotokollen umgeht.

Sie können im Abschnitt „Einstellungen“ des SnapCenter Webclients auf Richtlinien zugreifen.



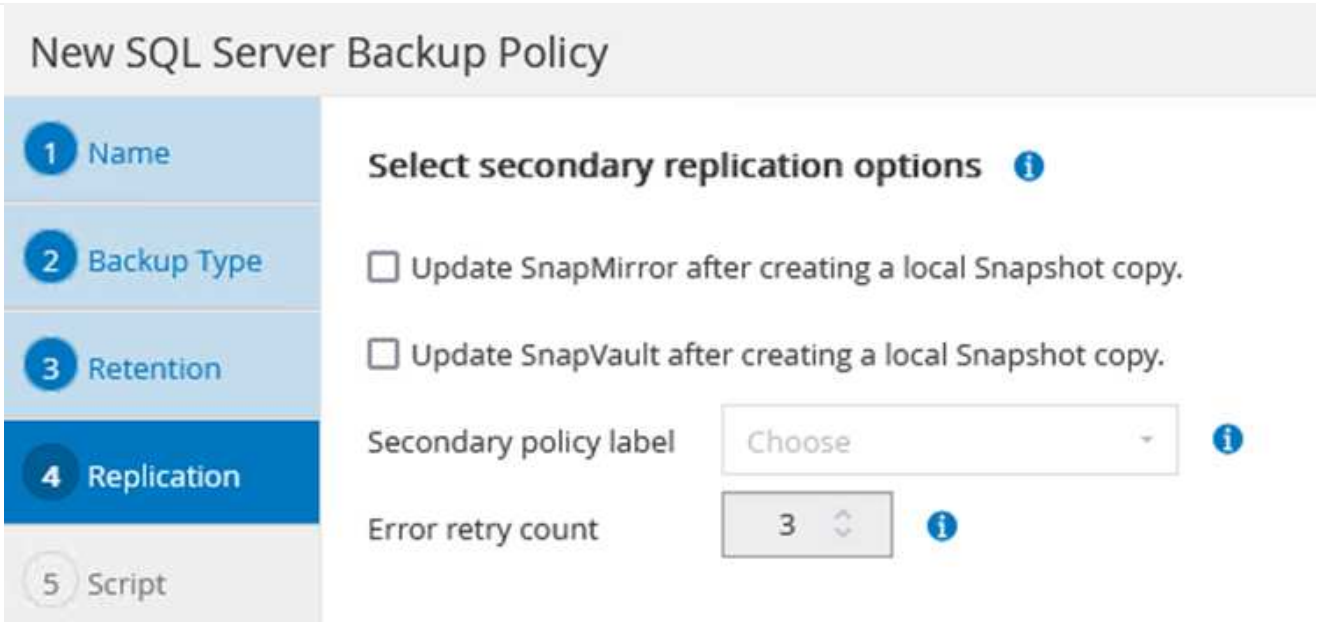
Ausführliche Informationen zum Erstellen von Richtlinien für SQL Server-Backups finden Sie im "SnapCenter -Dokumentation" .

Ausführliche Informationen zum Erstellen von Richtlinien für Oracle-Backups finden Sie im "SnapCenter -Dokumentation" .

Anmerkungen:

- Achten Sie beim Durchlaufen des Assistenten zur Richtlinienerstellung besonders auf den Abschnitt „Replikation“. In diesem Abschnitt legen Sie die Arten der sekundären SnapMirror -Kopien fest, die während des Sicherungsvorgangs erstellt werden sollen.
- Die Einstellung „ SnapMirror nach dem Erstellen einer lokalen Snapshot-Kopie aktualisieren“ bezieht sich auf die Aktualisierung einer SnapMirror Beziehung, wenn diese Beziehung zwischen zwei virtuellen Speichermaschinen besteht, die sich auf demselben Cluster befinden.
- Die Einstellung „ SnapVault nach dem Erstellen einer lokalen SnapShot-Kopie aktualisieren“ wird verwendet, um eine SnapMirror Beziehung zu aktualisieren, die zwischen zwei separaten Clustern und zwischen einem lokalen ONTAP System und Cloud Volumes ONTAP oder FSx ONTAP besteht.

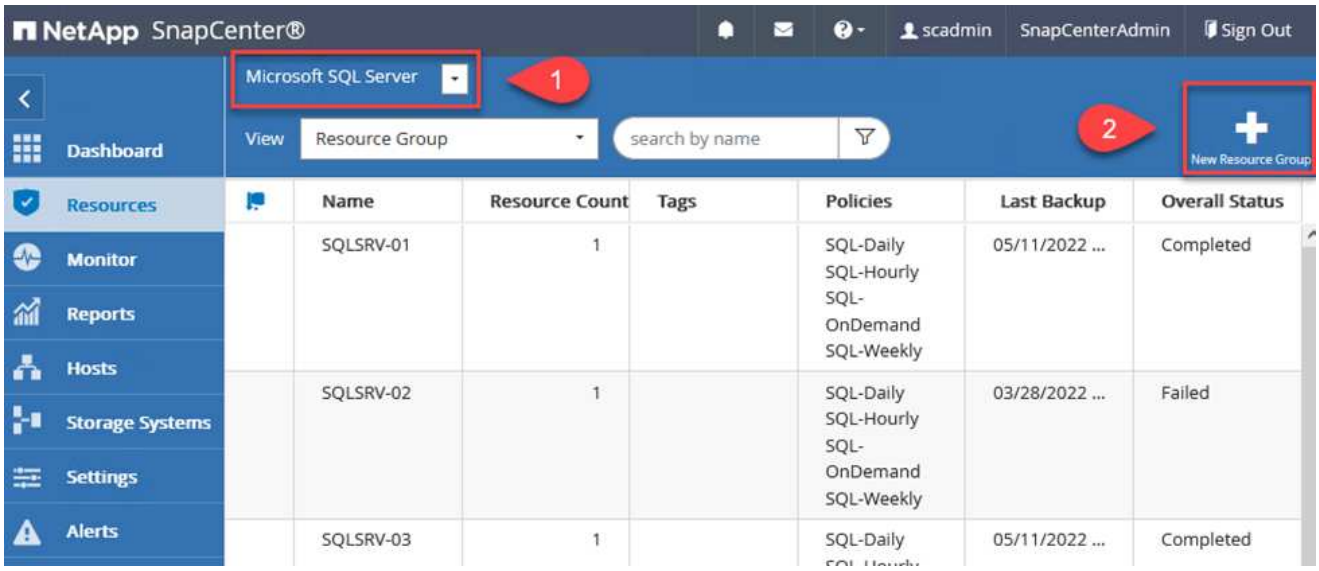
Das folgende Bild zeigt die vorhergehenden Optionen und wie sie im Assistenten für Sicherungsrichtlinien aussehen.



Erstellen von SnapCenter -Ressourcengruppen

Mithilfe von Ressourcengruppen können Sie die Datenbankressourcen auswählen, die Sie in Ihre Sicherungen einbeziehen möchten, sowie die für diese Ressourcen zu befolgenden Richtlinien.

1. Gehen Sie im linken Menü zum Abschnitt „Ressourcen“.
2. Wählen Sie oben im Fenster den Ressourcentyp aus, mit dem Sie arbeiten möchten (in diesem Fall Microsoft SQL Server), und klicken Sie dann auf Neue Ressourcengruppe.



Die SnapCenter -Dokumentation enthält schrittweise Details zum Erstellen von Ressourcengruppen für SQL Server- und Oracle-Datenbanken.

Um SQL-Ressourcen zu sichern, folgen Sie "dieser Link" .

Zum Sichern von Oracle-Ressourcen folgen Sie "dieser Link" .

Bereitstellen und Konfigurieren des Veeam Backup Servers

In der Lösung wird die Software Veeam Backup & Replication verwendet, um unsere virtuellen Anwendungsmaschinen zu sichern und eine Kopie der Sicherungen mithilfe eines Veeam Scale-Out Backup Repository (SOBR) in einem Amazon S3-Bucket zu archivieren. Veeam wird in dieser Lösung auf einem Windows-Server bereitgestellt. Spezifische Anleitungen zur Bereitstellung von Veeam finden Sie im "Veeam-Hilfecenter Technische Dokumentation" .

Konfigurieren des Veeam Scale-Out-Backup-Repository

Nachdem Sie die Software bereitgestellt und lizenziert haben, können Sie ein Scale-Out-Backup-Repository (SOBR) als Zielspeicher für Sicherungsaufträge erstellen. Sie sollten auch einen S3-Bucket als externes Backup der VM-Daten für die Notfallwiederherstellung einschließen.

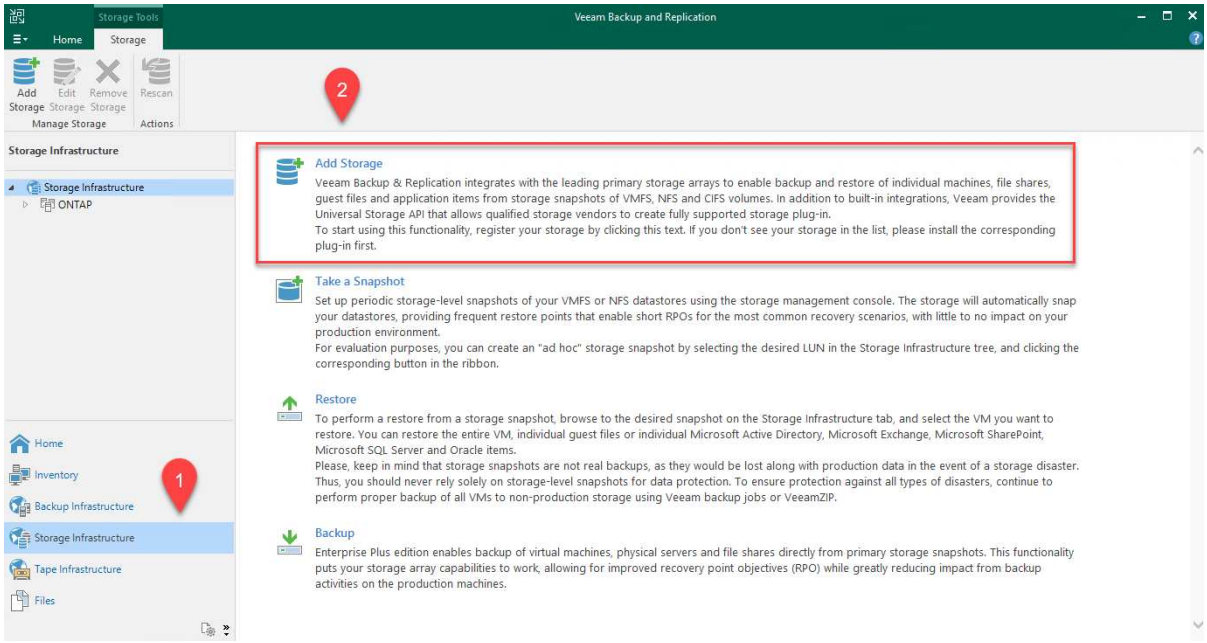
Sehen Sie sich die folgenden Voraussetzungen an, bevor Sie beginnen.

1. Erstellen Sie eine SMB-Dateifreigabe auf Ihrem lokalen ONTAP -System als Zielspeicher für Backups.
2. Erstellen Sie einen Amazon S3-Bucket, der in den SOBR aufgenommen werden soll. Dies ist ein Repository für die Offsite-Backups.

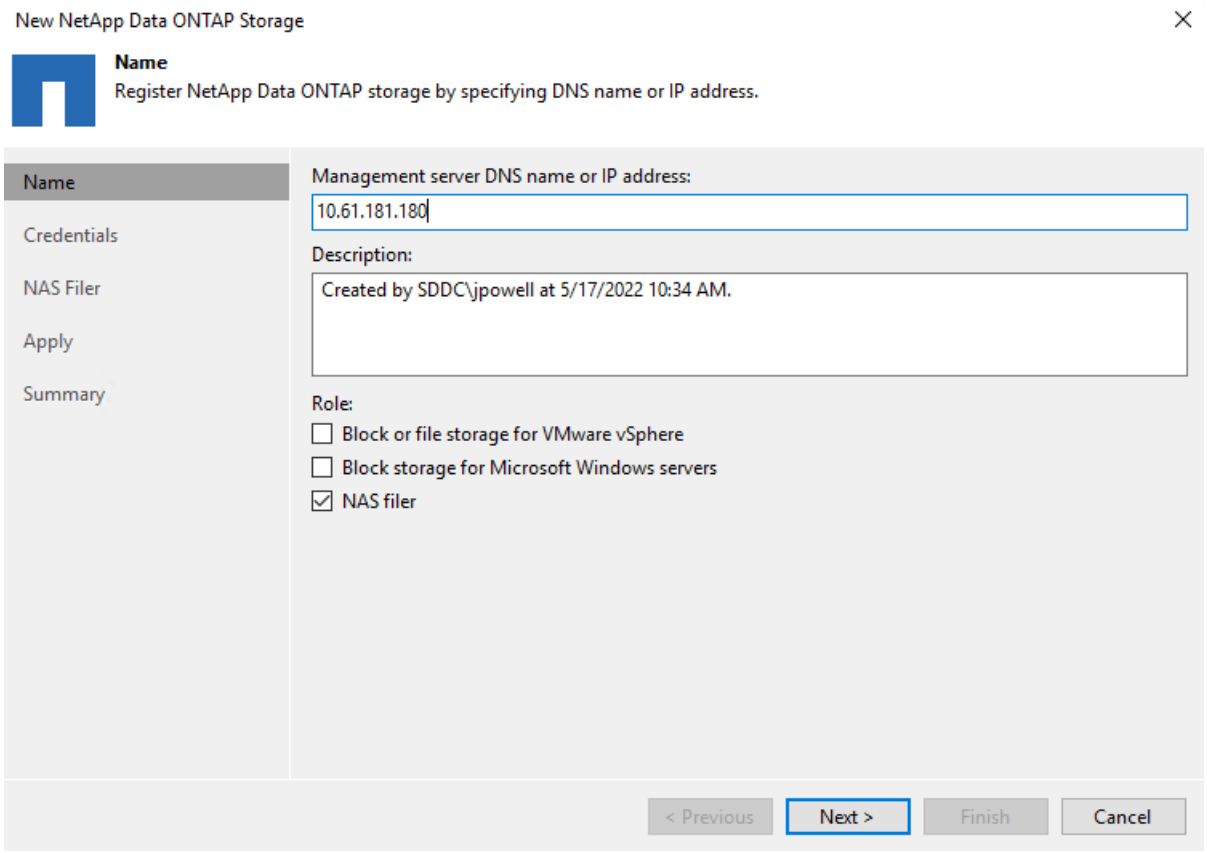
Fügen Sie ONTAP -Speicher zu Veeam hinzu

Fügen Sie zunächst den ONTAP -Speichercluster und das zugehörige SMB/NFS-Dateisystem als Speicherinfrastruktur in Veeam hinzu.

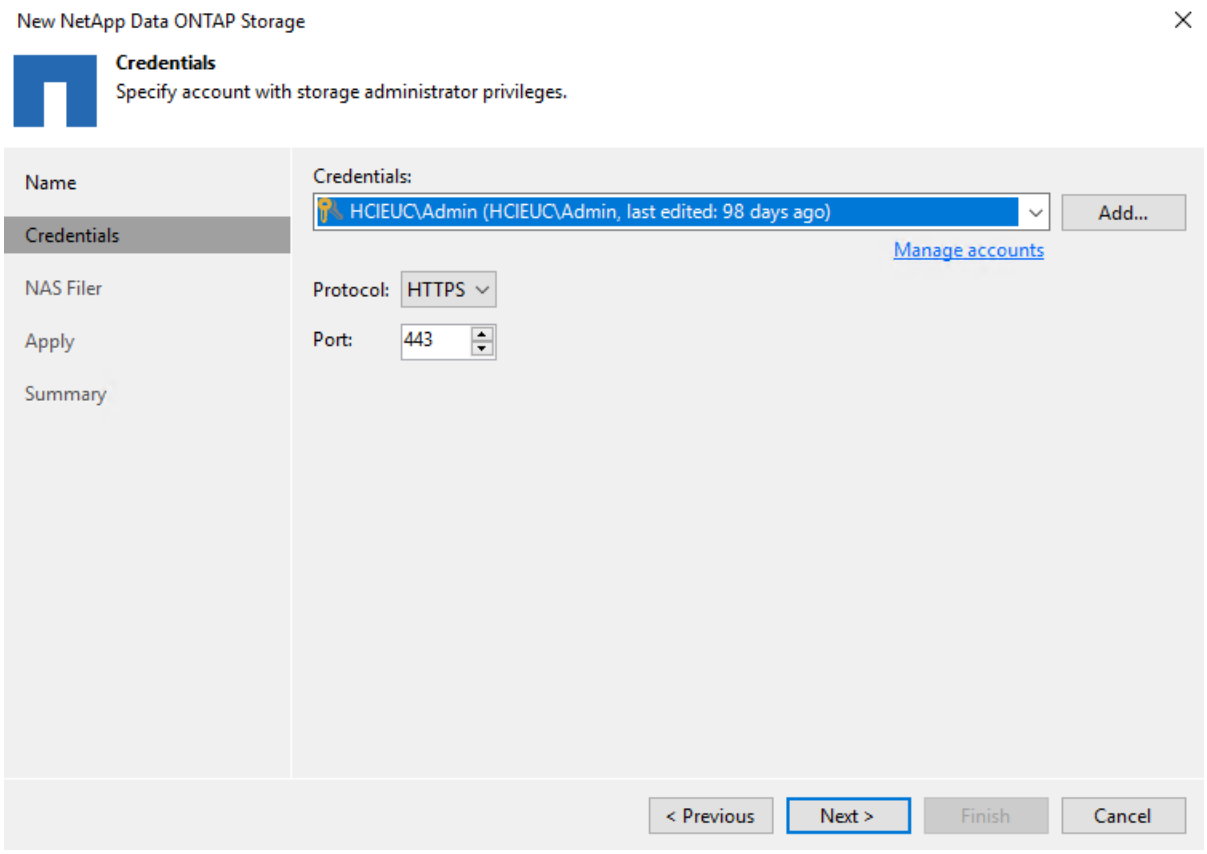
1. Öffnen Sie die Veeam-Konsole und melden Sie sich an. Navigieren Sie zu „Speicherinfrastruktur“ und wählen Sie dann „Speicher hinzufügen“ aus.



2. Wählen Sie im Assistenten „Speicher hinzufügen“ NetApp als Speicheranbieter und dann Data ONTAP aus.
3. Geben Sie die Verwaltungs-IP-Adresse ein und aktivieren Sie das Kontrollkästchen „NAS-Filer“. Klicken Sie auf Weiter.

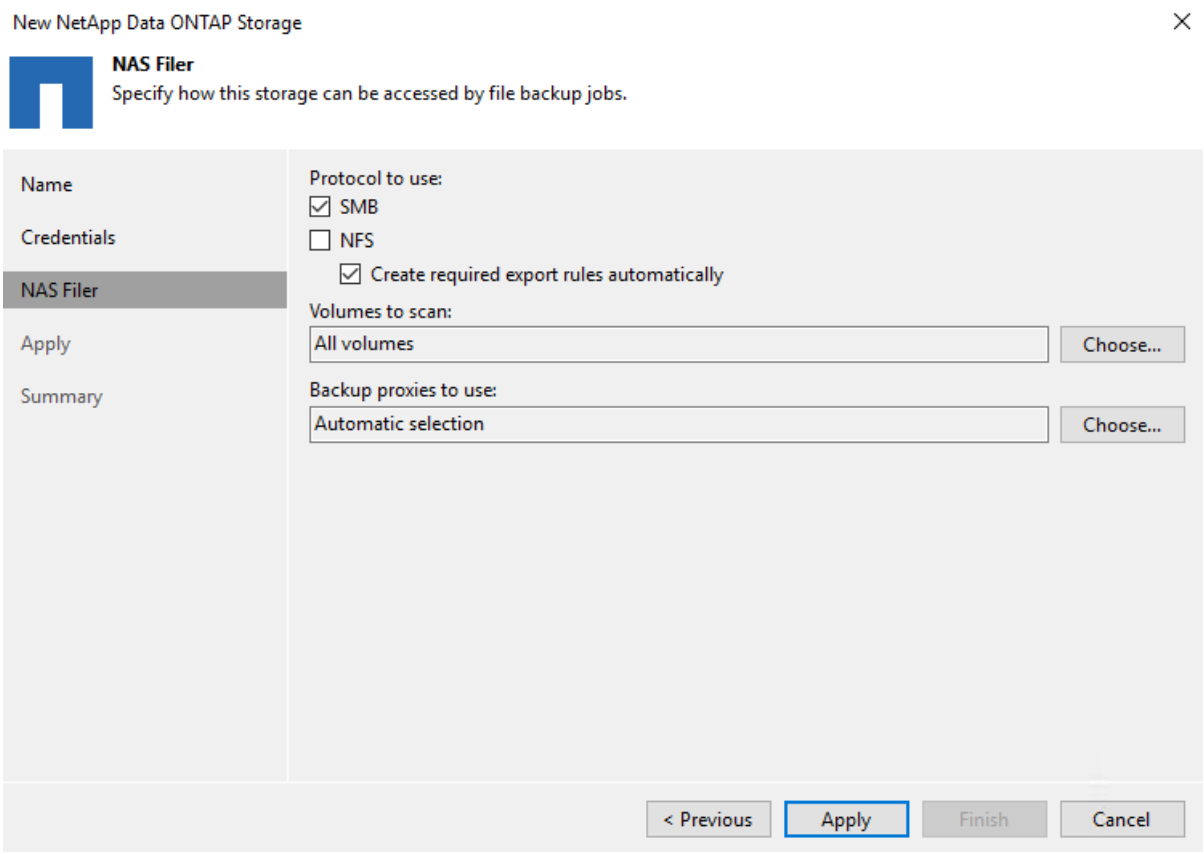


4. Fügen Sie Ihre Anmeldeinformationen hinzu, um auf den ONTAP Cluster zuzugreifen.

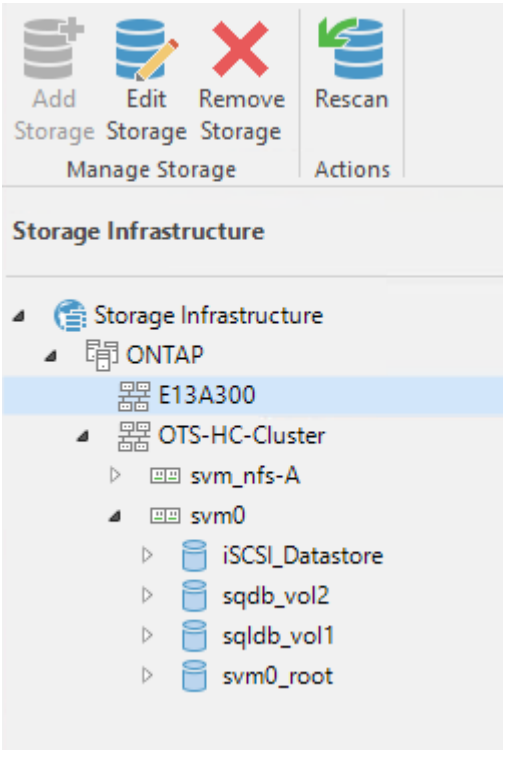


5. Wählen Sie auf der NAS-Filer-Seite die gewünschten Protokolle zum Scannen aus und klicken

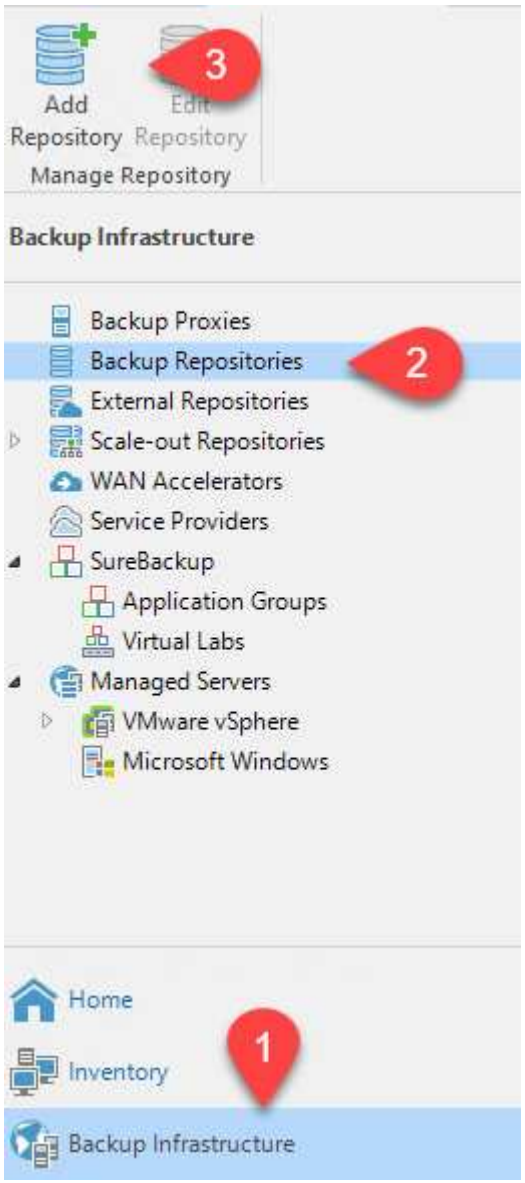
Sie auf „Weiter“.



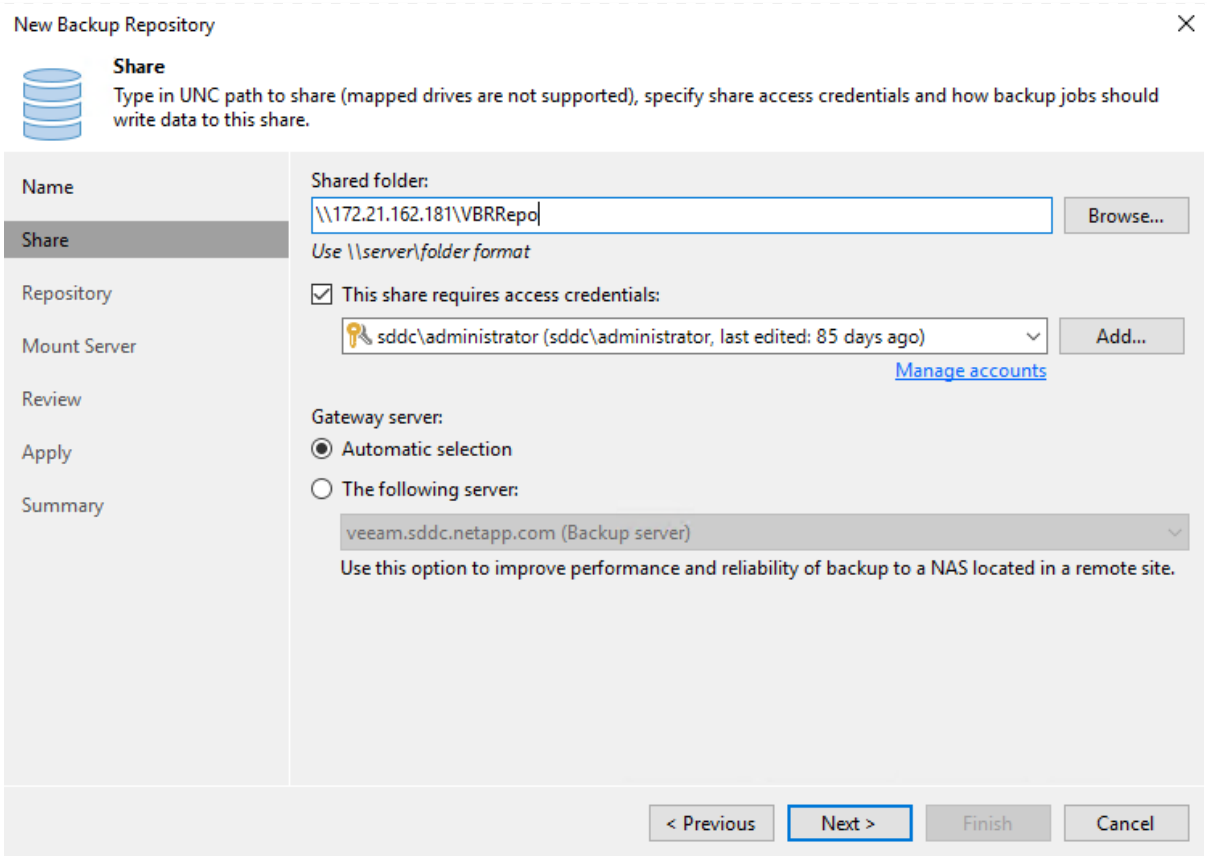
6. Füllen Sie die Seiten „Übernehmen“ und „Zusammenfassung“ des Assistenten aus und klicken Sie auf „Fertig stellen“, um mit der Speichererkennung zu beginnen. Nach Abschluss des Scans wird der ONTAP Cluster zusammen mit den NAS-Filern als verfügbare Ressourcen hinzugefügt.



7. Erstellen Sie ein Sicherungsrepository mit den neu erkannten NAS-Freigaben. Wählen Sie unter „Backup-Infrastruktur“ „Backup-Repositorys“ aus und klicken Sie auf das Menüelement „Repository hinzufügen“.



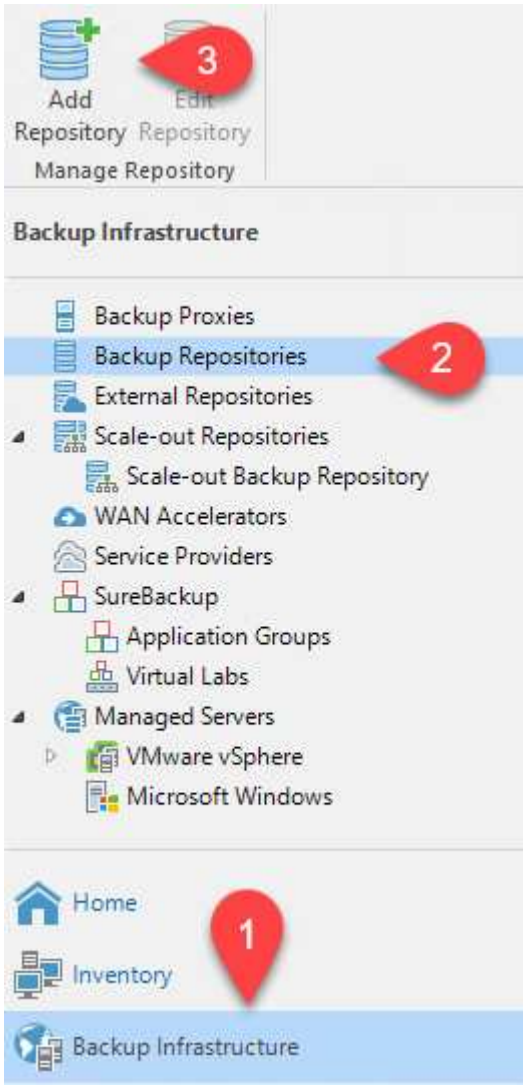
8. Befolgen Sie alle Schritte im Assistenten „Neues Sicherungsrepository“, um das Repository zu erstellen. Ausführliche Informationen zum Erstellen von Veeam Backup Repositories finden Sie im "Veeam-Dokumentation" .


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

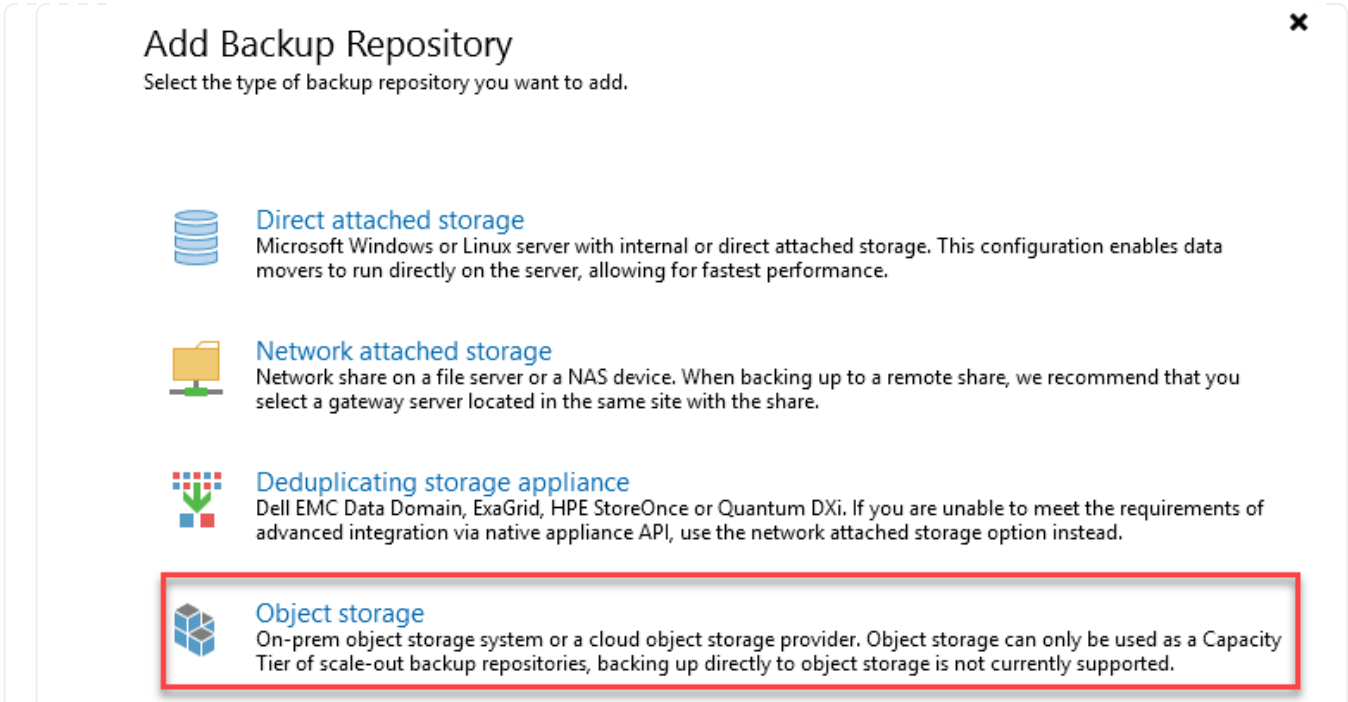
Fügen Sie den Amazon S3-Bucket als Backup-Repository hinzu

Der nächste Schritt besteht darin, den Amazon S3-Speicher als Backup-Repository hinzuzufügen.

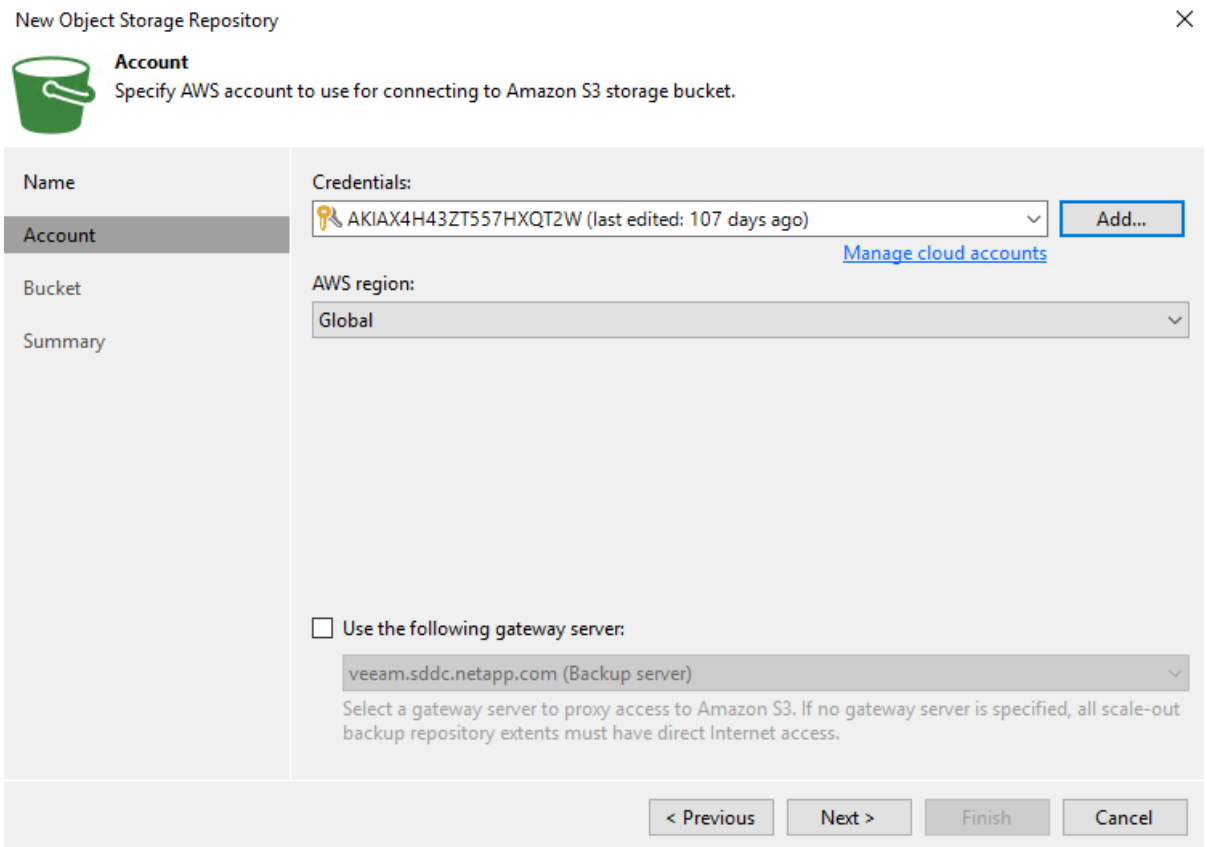
1. Navigieren Sie zu Backup-Infrastruktur > Backup-Repositorys. Klicken Sie auf Repository hinzufügen.



2. Wählen Sie im Assistenten „Backup-Repository hinzufügen“ Object Storage und dann Amazon S3 aus. Dadurch wird der Assistent „Neues Object Storage-Repository“ gestartet.



3. Geben Sie einen Namen für Ihr Objektspeicher-Repository ein und klicken Sie auf „Weiter“.
4. Geben Sie im nächsten Abschnitt Ihre Anmeldeinformationen ein. Sie benötigen einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel.

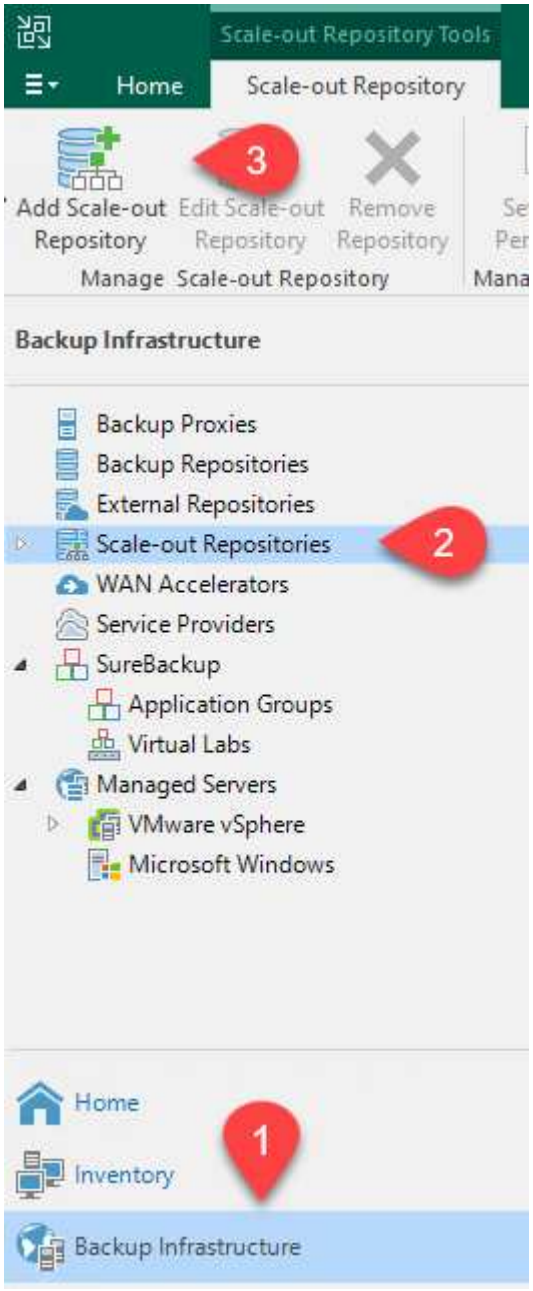


5. Nachdem die Amazon-Konfiguration geladen wurde, wählen Sie Ihr Rechenzentrum, Ihren Bucket und Ihren Ordner aus und klicken Sie auf „Übernehmen“. Klicken Sie abschließend auf „Fertig stellen“, um den Assistenten zu schließen.

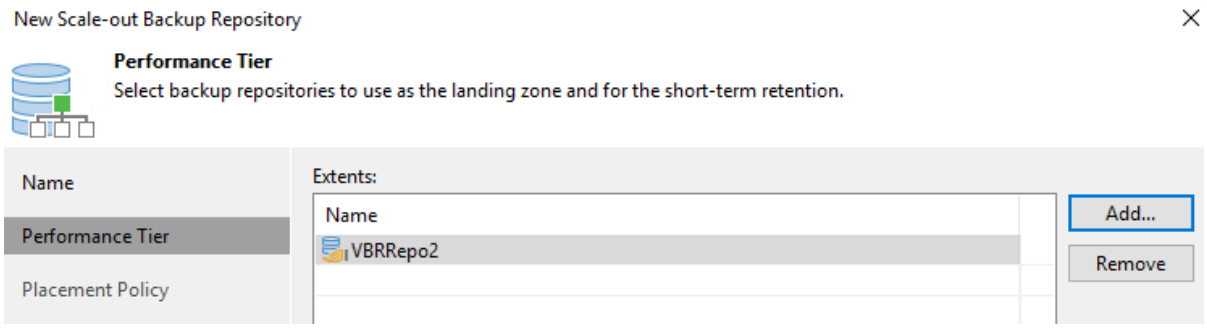
Erstellen eines Scale-Out-Sicherungsrepositorys

Nachdem wir nun unsere Speicher-Repositories zu Veeam hinzugefügt haben, können wir den SOBR erstellen, um Sicherungskopien zur Notfallwiederherstellung automatisch in unseren externen Amazon S3-Objektspeicher zu verschieben.

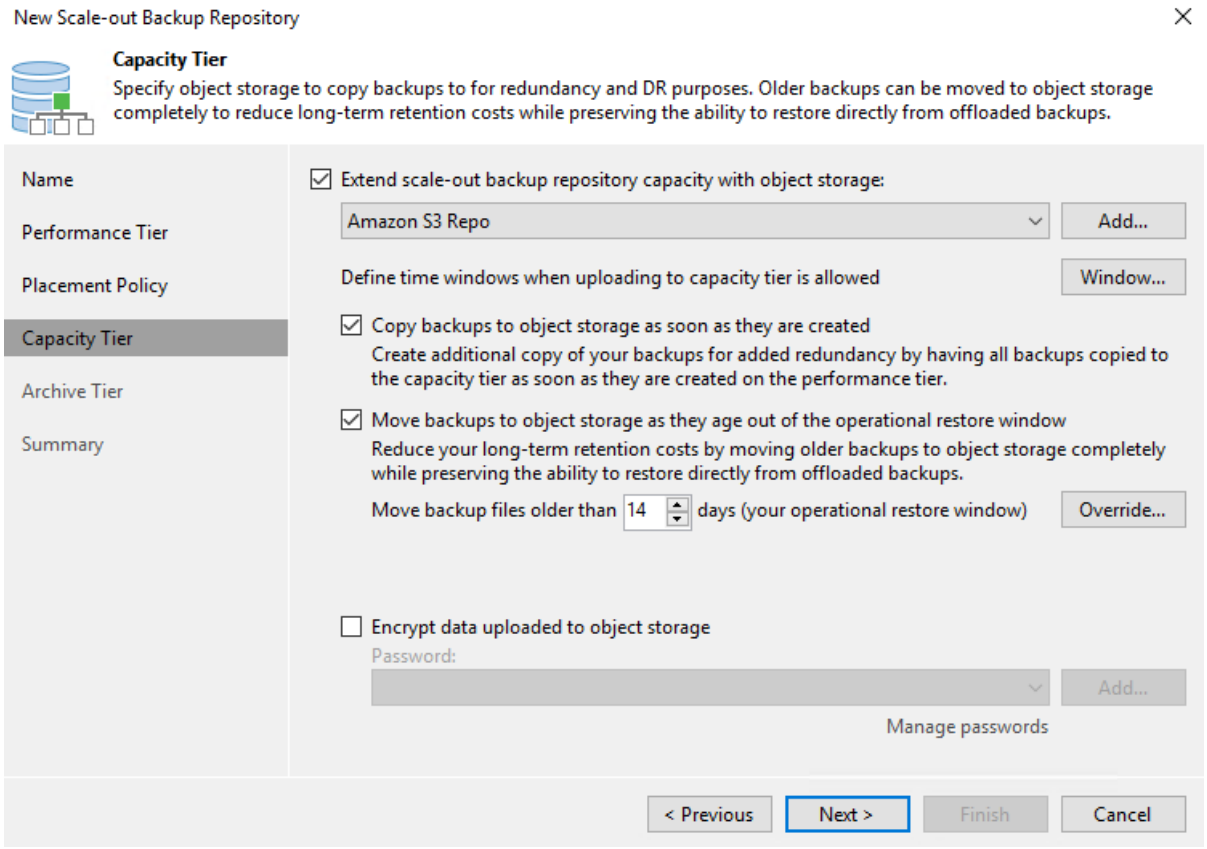
1. Wählen Sie unter „Backup-Infrastruktur“ die Option „Scale-out-Repositorys“ aus und klicken Sie dann auf das Menüelement „Scale-out-Repository hinzufügen“.



2. Geben Sie im neuen Scale-Out-Backup-Repository einen Namen für das SOBR ein und klicken Sie auf „Weiter“.
3. Wählen Sie für die Leistungsstufe das Sicherungsrepository aus, das die SMB-Freigabe enthält, die sich auf Ihrem lokalen ONTAP Cluster befindet.



4. Wählen Sie für die Platzierungsrichtlinie je nach Ihren Anforderungen entweder „Datenlokalität“ oder „Leistung“ aus. Wählen Sie „Weiter“ aus.
5. Für die Kapazitätsstufe erweitern wir den SOBR mit Amazon S3-Objektspeicher. Wählen Sie für die Notfallwiederherstellung „Backups sofort nach ihrer Erstellung in den Objektspeicher kopieren“ aus, um eine rechtzeitige Bereitstellung unserer sekundären Backups sicherzustellen.



6. Wählen Sie abschließend „Übernehmen und Fertigstellen“ aus, um die Erstellung des SOBR abzuschließen.

Erstellen der Scale-Out-Backup-Repository-Jobs

Der letzte Schritt zur Konfiguration von Veeam besteht darin, Sicherungsaufträge mit dem neu erstellten SOBR als Sicherungsziel zu erstellen. Das Erstellen von Sicherungsaufträgen gehört zum normalen Repertoire eines jeden Speicheradministrators und wir gehen hier nicht auf die einzelnen Schritte ein. Ausführlichere Informationen zum Erstellen von Sicherungsaufträgen in Veeam finden Sie im "Veeam Help Center Technische Dokumentation" .

BlueXP backup and recovery und Wiederherstellungstools und -Konfiguration

Um ein Failover von Anwendungs-VMs und Datenbank-Volumes auf VMware Cloud Volume-Dienste durchzuführen, die in AWS ausgeführt werden, müssen Sie eine laufende Instanz von SnapCenter Server und Veeam Backup and Replication Server installieren und konfigurieren. Nachdem das Failover abgeschlossen ist, müssen Sie diese Tools auch so konfigurieren, dass der normale Sicherungsvorgang fortgesetzt wird, bis ein Failback zum lokalen Rechenzentrum geplant und ausgeführt wird.

Bereitstellen eines sekundären Windows SnapCenter -Servers

SnapCenter Server wird im VMware Cloud SDDC bereitgestellt oder auf einer EC2-Instanz installiert, die sich in einem VPC mit Netzwerkkonnektivität zur VMware Cloud-Umgebung befindet.

Die SnapCenter software ist auf der NetApp Support-Site verfügbar und kann auf Microsoft Windows-Systemen installiert werden, die sich entweder in einer Domäne oder Arbeitsgruppe befinden. Eine ausführliche Planungshilfe und Installationsanleitung finden Sie auf der "NetApp Dokumentationszentrum" .

Sie finden die SnapCenter software unter "dieser Link" .

Konfigurieren des sekundären Windows SnapCenter -Servers

Um eine Wiederherstellung der auf FSx ONTAP gespiegelten Anwendungsdaten durchzuführen, müssen Sie zunächst eine vollständige Wiederherstellung der lokalen SnapCenter Datenbank durchführen. Nachdem dieser Vorgang abgeschlossen ist, wird die Kommunikation mit den VMs wiederhergestellt und Anwendungssicherungen können nun mit FSx ONTAP als primärem Speicher fortgesetzt werden.

Um dies zu erreichen, müssen Sie die folgenden Elemente auf dem SnapCenter -Server ausführen:

1. Konfigurieren Sie den Computernamen so, dass er mit dem ursprünglichen SnapCenter -Server vor Ort identisch ist.
2. Konfigurieren Sie das Netzwerk für die Kommunikation mit VMware Cloud und der FSx ONTAP Instanz.
3. Schließen Sie das Verfahren zum Wiederherstellen der SnapCenter -Datenbank ab.
4. Bestätigen Sie, dass sich SnapCenter im Disaster Recovery-Modus befindet, um sicherzustellen, dass FSx jetzt der primäre Speicher für Backups ist.
5. Bestätigen Sie, dass die Kommunikation mit den wiederhergestellten virtuellen Maschinen wiederhergestellt ist.

Bereitstellen eines sekundären Veeam Backup & Replication-Servers

Sie können den Veeam Backup & Replication-Server auf einem Windows-Server in der VMware Cloud auf AWS oder auf einer EC2-Instanz installieren. Ausführliche Anleitungen zur Implementierung finden Sie im "Veeam Help Center Technische Dokumentation" .

Konfigurieren Sie den sekundären Veeam Backup & Replication-Server

Um eine Wiederherstellung von virtuellen Maschinen durchzuführen, die im Amazon S3-Speicher gesichert wurden, müssen Sie den Veeam-Server auf einem Windows-Server installieren und ihn für die Kommunikation mit VMware Cloud, FSx ONTAP und dem S3-Bucket konfigurieren, der das ursprüngliche Sicherungsrepository enthält. Außerdem muss auf FSx ONTAP ein neues Backup-Repository konfiguriert sein, um nach der Wiederherstellung neue Backups der VMs durchzuführen.

Um diesen Vorgang durchzuführen, müssen die folgenden Punkte abgeschlossen sein:

1. Konfigurieren Sie das Netzwerk für die Kommunikation mit VMware Cloud, FSx ONTAP und dem S3-Bucket, das das ursprüngliche Sicherungsrepository enthält.
2. Konfigurieren Sie eine SMB-Freigabe auf FSx ONTAP als neues Backup-Repository.
3. Mounten Sie den ursprünglichen S3-Bucket, der als Teil des Scale-Out-Backup-Repositorys vor Ort verwendet wurde.
4. Richten Sie nach der Wiederherstellung der VM neue Sicherungsaufträge ein, um SQL- und Oracle-VMs zu schützen.

Weitere Informationen zum Wiederherstellen von VMs mit Veeam finden Sie im Abschnitt"Wiederherstellen von Anwendungs-VMs mit Veeam Full Restore" .

SnapCenter -Datenbanksicherung für die Notfallwiederherstellung

SnapCenter ermöglicht die Sicherung und Wiederherstellung der zugrunde liegenden MySQL-Datenbank und Konfigurationsdaten, um den SnapCenter -Server im Katastrophenfall wiederherzustellen. Für unsere Lösung haben wir die SnapCenter -Datenbank und -Konfiguration auf einer AWS EC2-Instanz wiederhergestellt, die sich in unserem VPC befindet. Weitere Informationen zur Notfallwiederherstellung von SnapCenter finden Sie unter "dieser Link" .

Voraussetzungen für SnapCenter -Backups

Für die SnapCenter Sicherung sind die folgenden Voraussetzungen erforderlich:

- Ein Volume und eine SMB-Freigabe, die auf dem lokalen ONTAP System erstellt wurden, um die gesicherte Datenbank und die Konfigurationsdateien zu finden.
- Eine SnapMirror -Beziehung zwischen dem lokalen ONTAP -System und FSx oder CVO im AWS-Konto. Diese Beziehung wird zum Transportieren des Snapshots verwendet, der die gesicherte SnapCenter Datenbank und die Konfigurationsdateien enthält.
- Im Cloud-Konto installierter Windows Server, entweder auf einer EC2-Instanz oder auf einer VM im VMware Cloud SDDC.
- SnapCenter ist auf der Windows EC2-Instanz oder VM in VMware Cloud installiert.

Zusammenfassung des SnapCenter -Sicherungs- und Wiederherstellungsprozesses

- Erstellen Sie auf dem lokalen ONTAP -System ein Volume zum Hosten der Sicherungsdatenbank und der Konfigurationsdateien.
- Richten Sie eine SnapMirror -Beziehung zwischen On-Premises und FSx/CVO ein.
- Mounten Sie die SMB-Freigabe.
- Rufen Sie das Swagger-Autorisierungstoken zum Ausführen von API-Aufgaben ab.
- Starten Sie den Datenbankwiederherstellungsprozess.
- Verwenden Sie das Dienstprogramm xcopy, um das lokale Verzeichnis der Datenbank- und Konfigurationsdateien in die SMB-Freigabe zu kopieren.
- Erstellen Sie auf FSx einen Klon des ONTAP Volumes (vom lokalen Standort über SnapMirror kopiert).
- Mounten Sie die SMB-Freigabe von FSx in EC2/VMware Cloud.
- Kopieren Sie das Wiederherstellungsverzeichnis von der SMB-Freigabe in ein lokales Verzeichnis.
- Führen Sie den SQL Server-Wiederherstellungsprozess von Swagger aus.

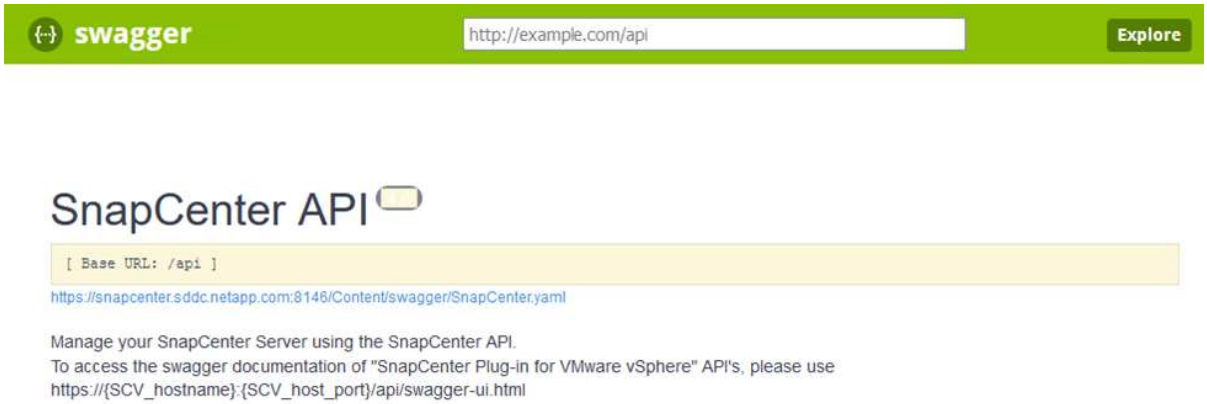
Sichern Sie die SnapCenter -Datenbank und -Konfiguration

SnapCenter bietet eine Webclient-Schnittstelle zum Ausführen von REST-API-Befehlen. Informationen zum Zugriff auf die REST-APIs über Swagger finden Sie in der SnapCenter -Dokumentation unter "dieser Link" .

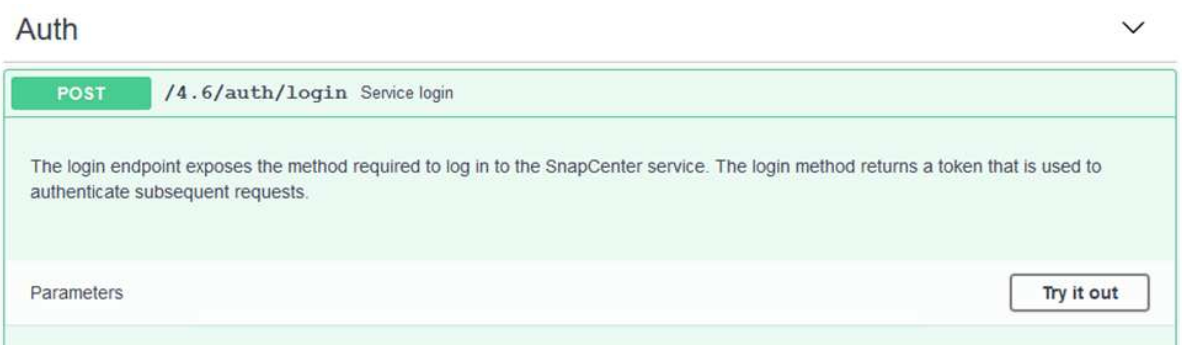
Melden Sie sich bei Swagger an und erhalten Sie ein Autorisierungstoken

Nachdem Sie zur Swagger-Seite navigiert sind, müssen Sie ein Autorisierungstoken abrufen, um den Datenbankwiederherstellungsprozess zu starten.

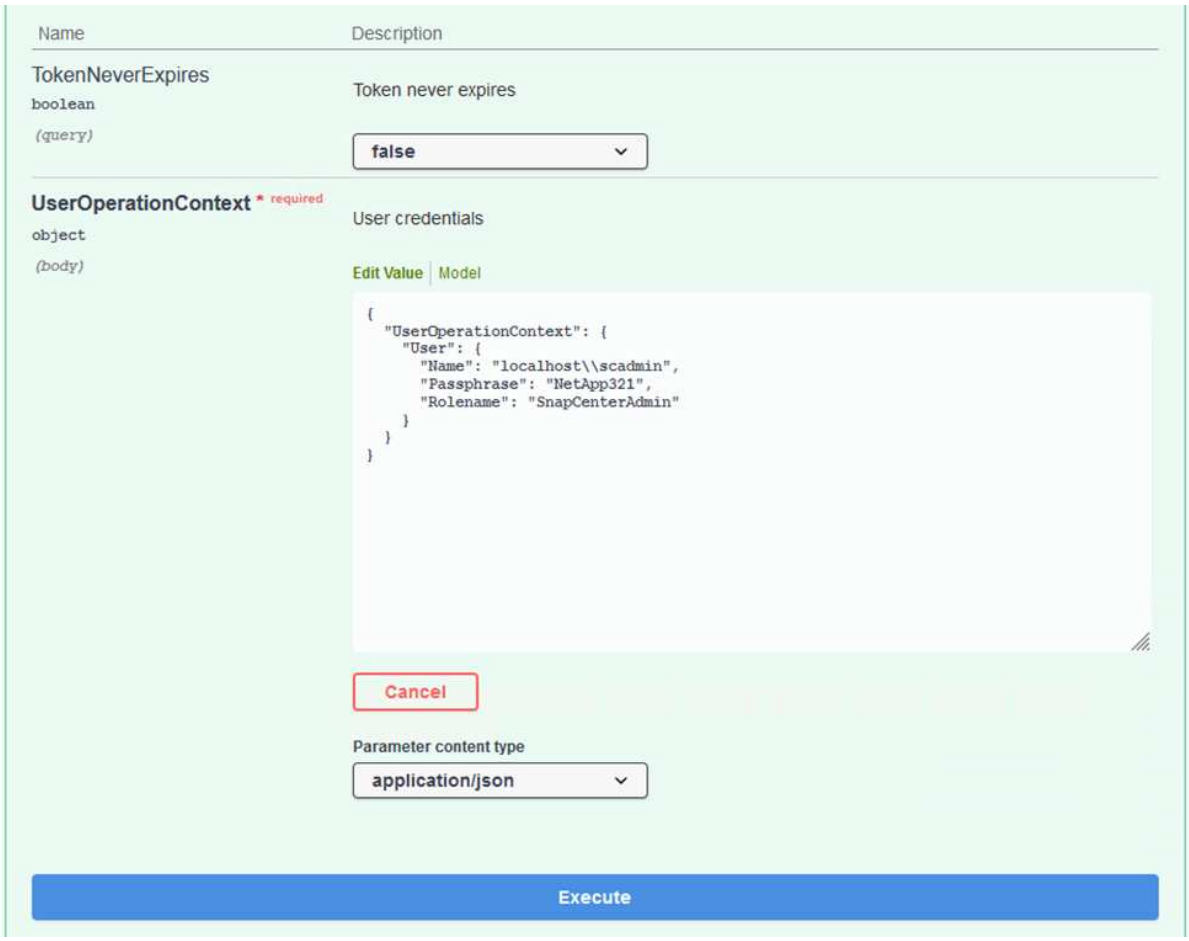
1. Greifen Sie auf die SnapCenter Swagger API-Webseite unter *https://< SnapCenter Server IP>:8146/swagger/* zu.



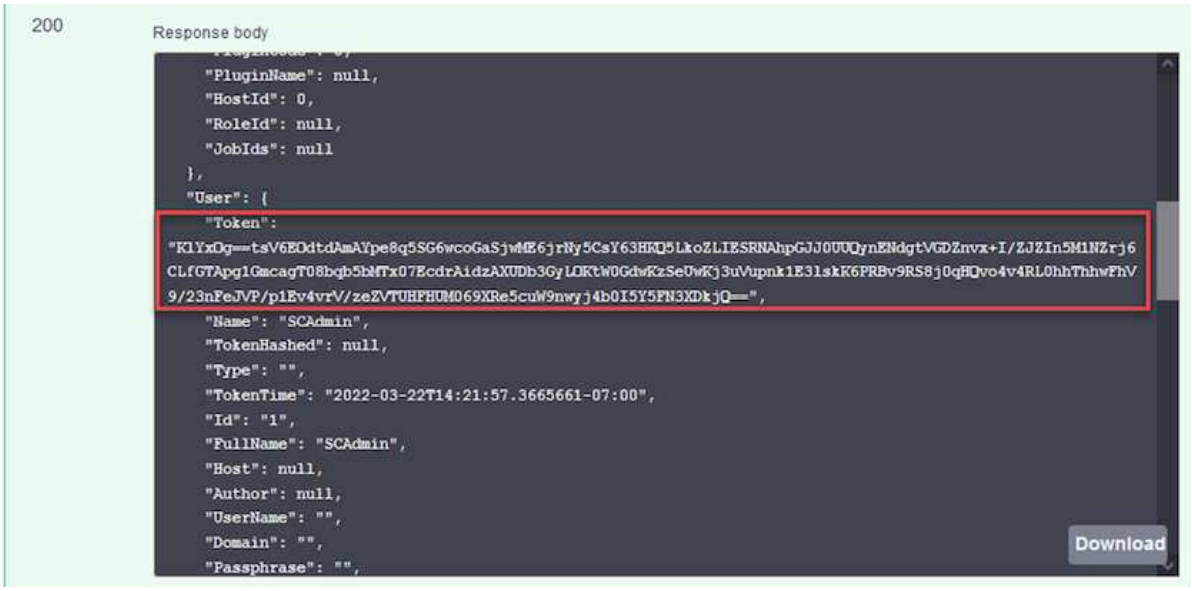
2. Erweitern Sie den Abschnitt „Auth“ und klicken Sie auf „Ausprobieren“.



3. Geben Sie im Bereich „UserOperationContext“ die SnapCenter -Anmeldeinformationen und -Rolle ein und klicken Sie auf „Ausführen“.



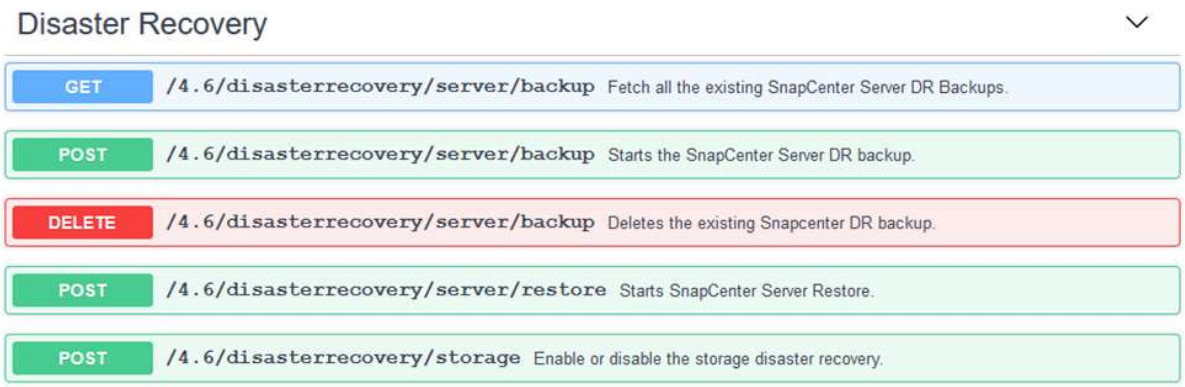
4. Im Antworttext unten können Sie das Token sehen. Kopieren Sie den Token-Text zur Authentifizierung beim Ausführen des Sicherungsvorgangs.



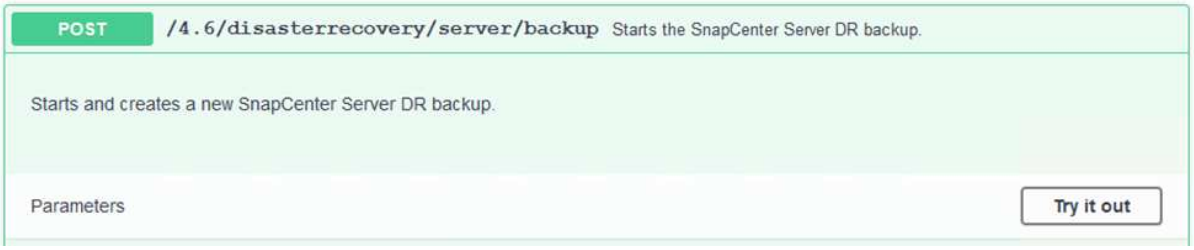
Führen Sie eine SnapCenter -Datenbanksicherung durch

Gehen Sie als Nächstes zum Bereich „Notfallwiederherstellung“ auf der Swagger-Seite, um den SnapCenter -Sicherungsprozess zu starten.

1. Erweitern Sie den Bereich „Disaster Recovery“, indem Sie darauf klicken.

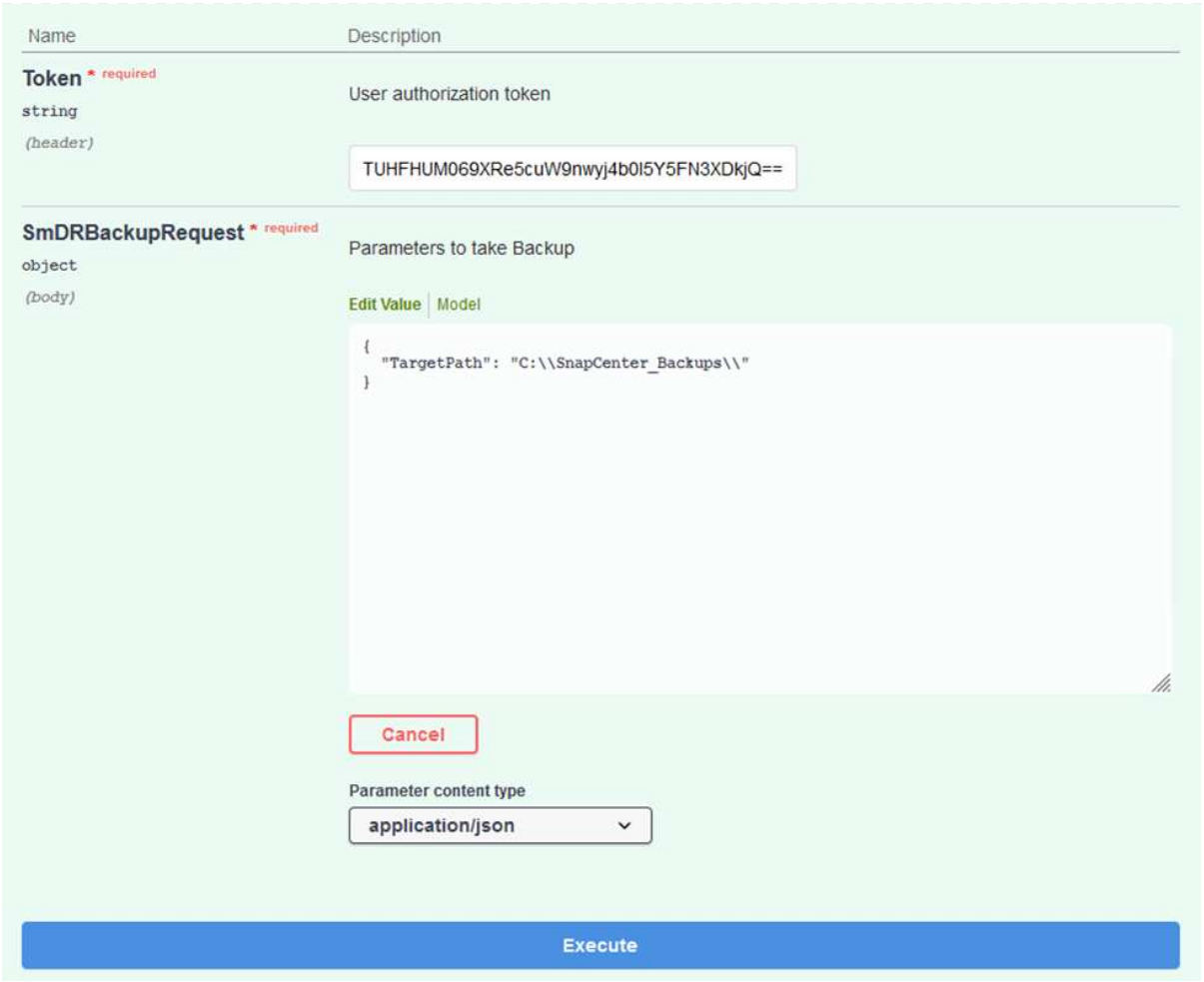


2. Erweitern Sie die `/4.6/disasterrecovery/server/backup` und klicken Sie auf „Ausprobieren“.



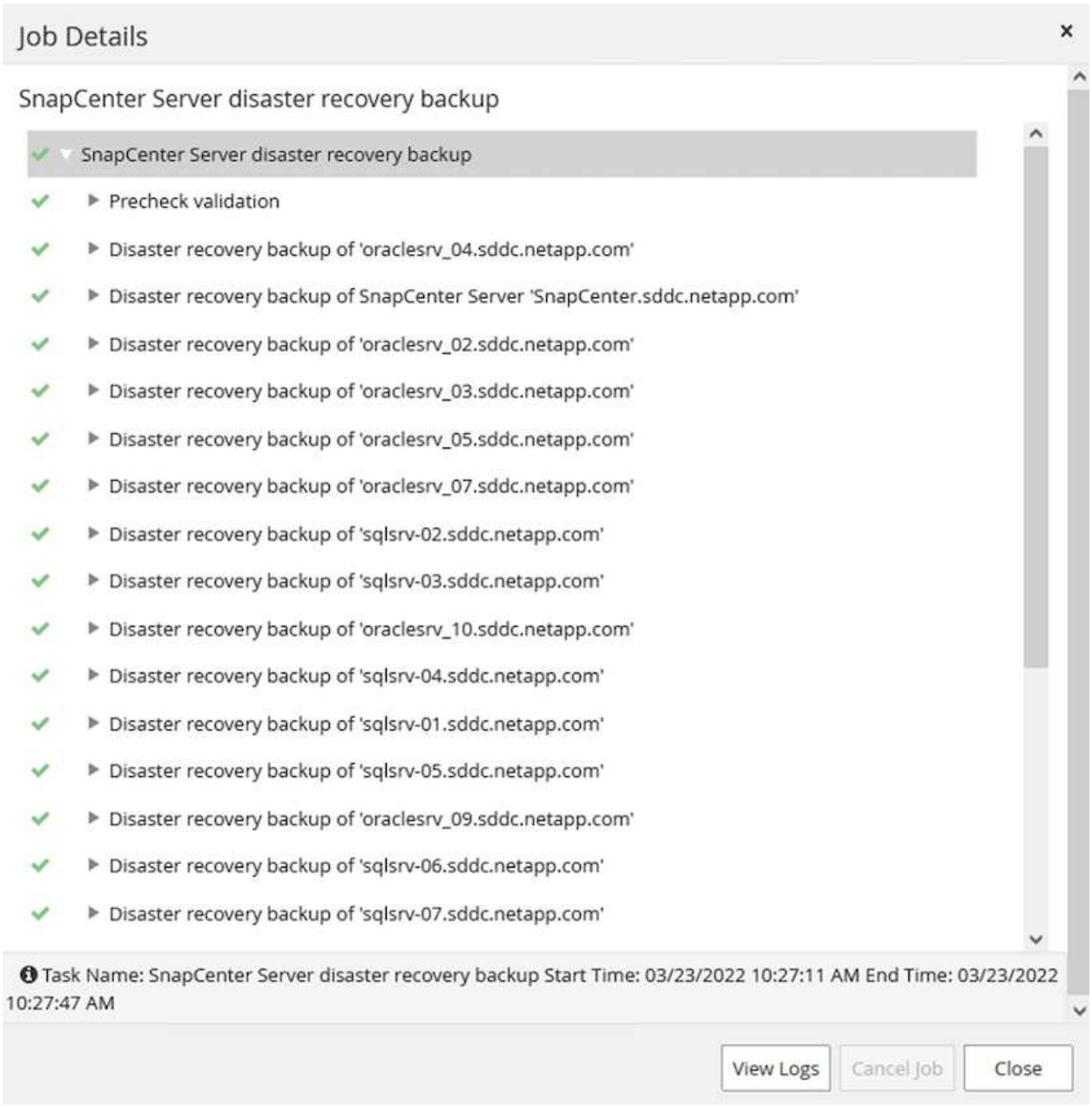
3. Fügen Sie im Abschnitt „SmDRBackupRequest“ den richtigen lokalen Zielpfad hinzu und wählen Sie „Ausführen“, um die Sicherung der SnapCenter -Datenbank und -Konfiguration zu starten.

> ⓘ Der Sicherungsvorgang ermöglicht keine direkte Sicherung auf eine NFS- oder CIFS-Dateifreigabe.


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

Überwachen Sie den Sicherungsauftrag von SnapCenter

Melden Sie sich bei SnapCenter an, um die Protokolldateien zu überprüfen, wenn Sie den Datenbankwiederherstellungsprozess starten. Im Abschnitt „Überwachen“ können Sie die Details der Notfallwiederherstellungssicherung des SnapCenter -Servers anzeigen.



Verwenden Sie das Dienstprogramm XCOPY, um die Datenbanksicherungsdatei auf die SMB-Freigabe zu kopieren

Als Nächstes müssen Sie die Sicherung vom lokalen Laufwerk auf dem SnapCenter -Server auf die CIFS-Freigabe verschieben, die zum Kopieren der Daten per SnapMirror an den sekundären Speicherort auf der FSx-Instanz in AWS verwendet wird. Verwenden Sie xcopy mit bestimmten Optionen, die die Berechtigungen der Dateien beibehalten.

Öffnen Sie eine Eingabeaufforderung als Administrator. Geben Sie in der Eingabeaufforderung die folgenden Befehle ein:

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

Ausfallsicherung

Katastrophe am Primärstandort

Für einen Notfall, der im primären Rechenzentrum vor Ort auftritt, umfasst unser Szenario ein Failover auf einen sekundären Standort, der sich auf der Amazon Web Services-Infrastruktur befindet und VMware Cloud auf AWS verwendet. Wir gehen davon aus, dass die virtuellen Maschinen und unser On-Premises ONTAP Cluster nicht mehr erreichbar sind. Darüber hinaus sind die virtuellen Maschinen von SnapCenter und Veeam nicht mehr zugänglich und müssen an unserem sekundären Standort neu erstellt werden.

In diesem Abschnitt geht es um das Failover unserer Infrastruktur in die Cloud. Dabei werden die folgenden Themen behandelt:

- SnapCenter -Datenbankwiederherstellung. Nachdem ein neuer SnapCenter -Server eingerichtet wurde, stellen Sie die MySQL-Datenbank und die Konfigurationsdateien wieder her und schalten Sie die Datenbank in den Notfallwiederherstellungsmodus, damit der sekundäre FSx-Speicher zum primären Speichergerät wird.
- Stellen Sie die virtuellen Anwendungsmaschinen mit Veeam Backup & Replication wieder her. Verbinden Sie den S3-Speicher, der die VM-Backups enthält, importieren Sie die Backups und stellen Sie sie in VMware Cloud auf AWS wieder her.
- Stellen Sie die SQL Server-Anwendungsdaten mit SnapCenter wieder her.
- Stellen Sie die Oracle-Anwendungsdaten mit SnapCenter wieder her.

SnapCenter -Datenbankwiederherstellungsprozess

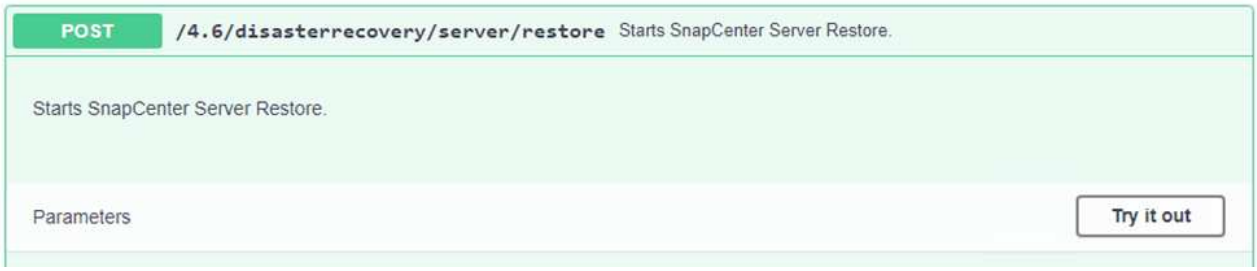
SnapCenter unterstützt Notfallwiederherstellungsszenarien, indem es die Sicherung und Wiederherstellung seiner MySQL-Datenbank und Konfigurationsdateien ermöglicht. Auf diese Weise kann ein Administrator regelmäßige Sicherungen der SnapCenter -Datenbank im lokalen Rechenzentrum durchführen und diese Datenbank später in einer sekundären SnapCenter Datenbank wiederherstellen.

Um auf die SnapCenter -Sicherungsdateien auf dem Remote- SnapCenter -Server zuzugreifen, führen Sie die folgenden Schritte aus:

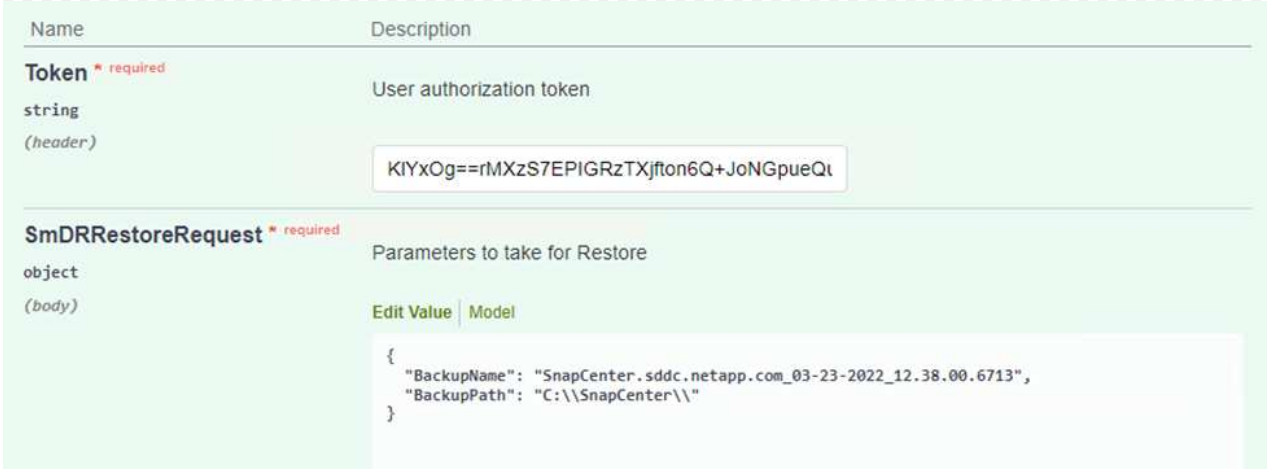
1. Unterbrechen Sie die SnapMirror -Beziehung zum FSx-Cluster, wodurch das Volume Lese-/Schreibzugriff erhält.
2. Erstellen Sie einen CIFS-Server (falls erforderlich) und erstellen Sie eine CIFS-Freigabe, die auf den Verbindungspfad des geklonten Volumes verweist.
3. Verwenden Sie xcopy, um die Sicherungsdateien in ein lokales Verzeichnis auf dem sekundären SnapCenter -System zu kopieren.
4. Installieren Sie SnapCenter v4.6.
5. Stellen Sie sicher, dass der SnapCenter -Server denselben FQDN wie der ursprüngliche Server hat. Dies ist erforderlich, damit die Datenbankwiederherstellung erfolgreich ist.

Führen Sie die folgenden Schritte aus, um den Wiederherstellungsvorgang zu starten:

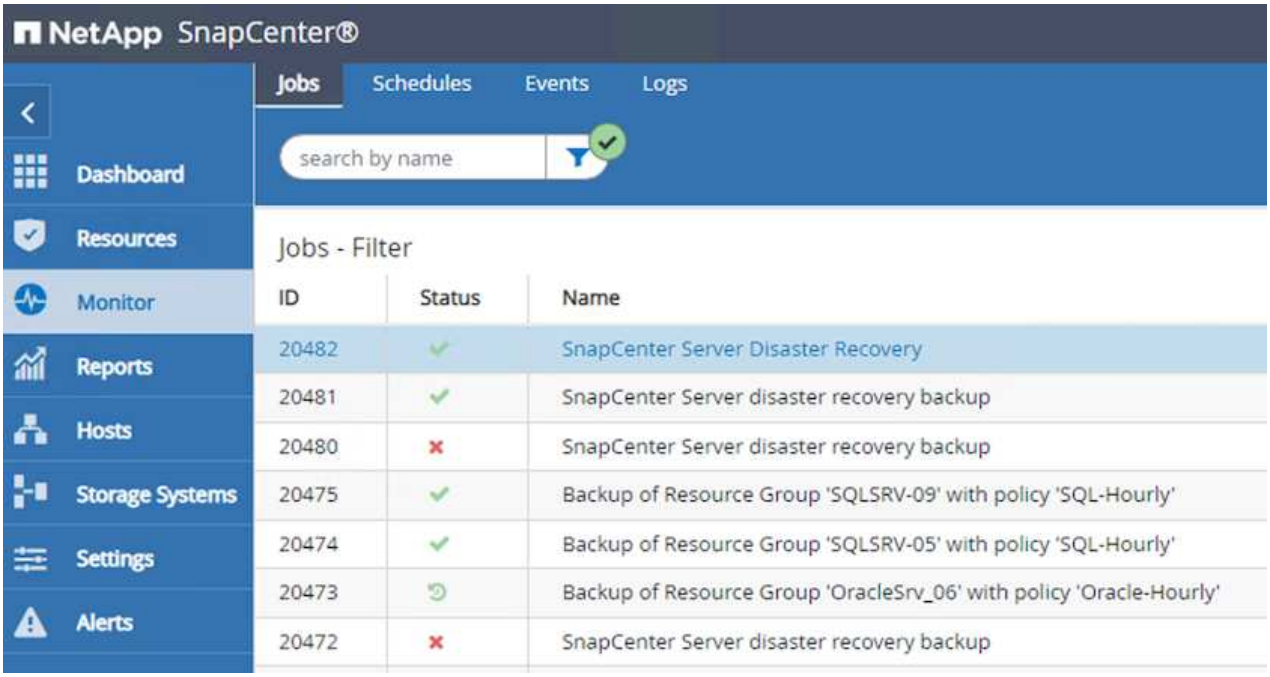
1. Navigieren Sie zur Swagger-API-Webseite für den sekundären SnapCenter Server und befolgen Sie die vorherigen Anweisungen, um ein Autorisierungstoken zu erhalten.
2. Navigieren Sie zum Abschnitt Disaster Recovery der Swagger-Seite, wählen Sie `/4.6/disasterrecovery/server/restore` und klicken Sie auf „Ausprobieren“.

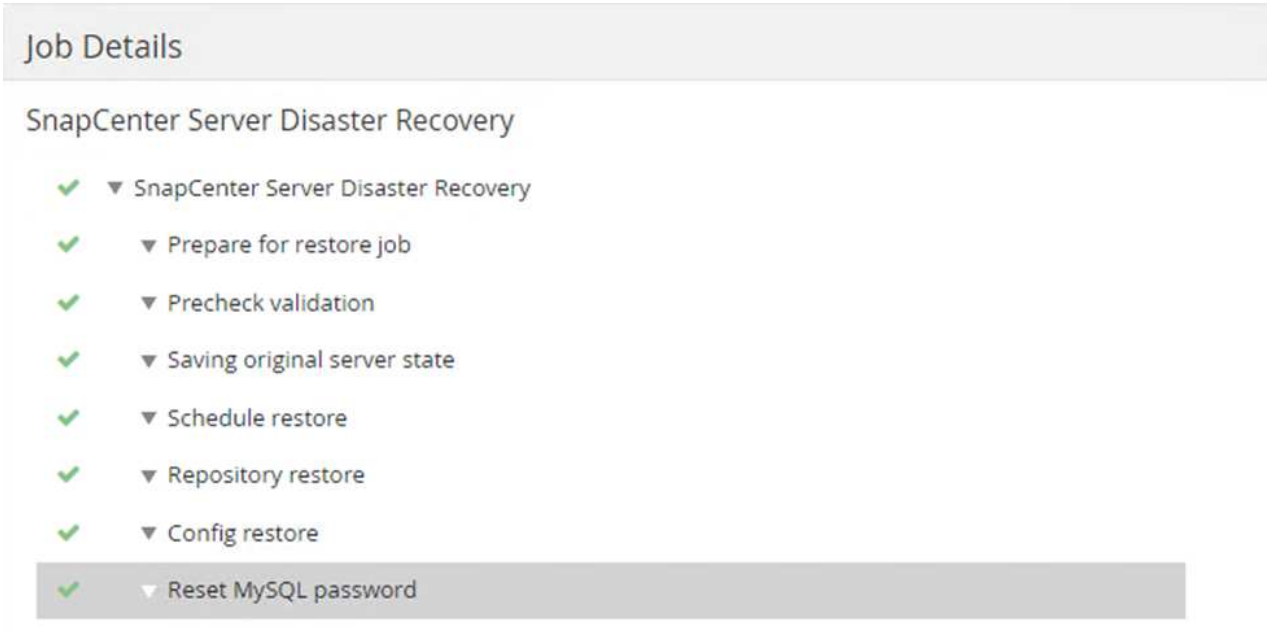


3. Fügen Sie Ihr Autorisierungstoken ein und fügen Sie im Abschnitt „SmDRResterRequest“ den Namen des Backups und des lokalen Verzeichnisses auf dem sekundären SnapCenter -Server ein.



4. Wählen Sie die Schaltfläche „Ausführen“, um den Wiederherstellungsvorgang zu starten.
5. Navigieren Sie in SnapCenter zum Abschnitt „Monitor“, um den Fortschritt des Wiederherstellungsauftrags anzuzeigen.





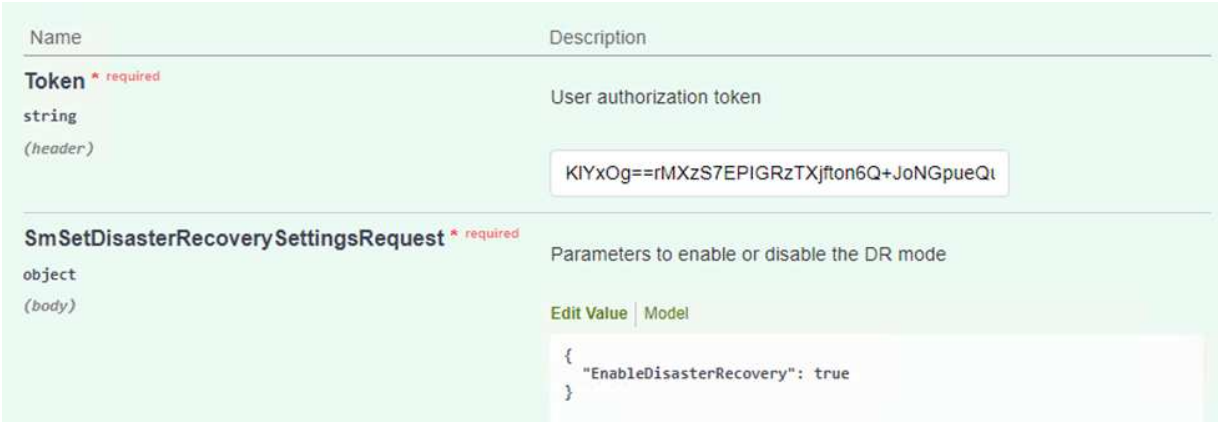
6. Um SQL Server-Wiederherstellungen vom sekundären Speicher zu aktivieren, müssen Sie die SnapCenter Datenbank in den Disaster Recovery-Modus schalten. Dies wird als separater Vorgang durchgeführt und auf der Swagger-API-Webseite initiiert.

   a. Navigieren Sie zum Abschnitt „Notfallwiederherstellung“ und klicken Sie auf `/4.6/disasterrecovery/storage` .

   b. Fügen Sie das Benutzerautorisierungstoken ein.

   c. Ändern Sie im Abschnitt „SmSetDisasterRecoverySettingsRequest“ `EnableDisasterRecover` Zu `true` .

   d. Klicken Sie auf „Ausführen“, um den Notfallwiederherstellungsmodus für SQL Server zu aktivieren.



Siehe Kommentare zu zusätzlichen Verfahren.

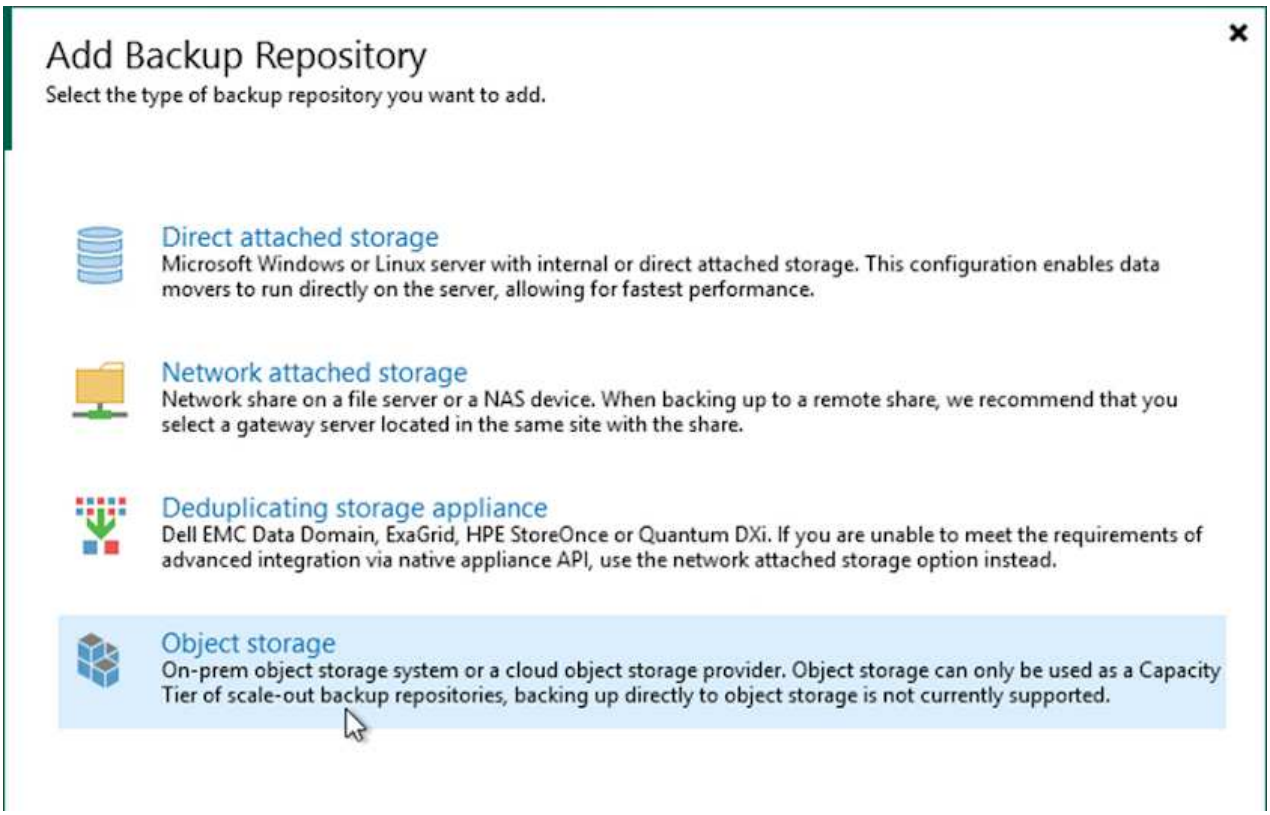
Wiederherstellen von Anwendungs-VMs mit der vollständigen Wiederherstellung von Veeam

Erstellen Sie ein Backup-Repository und importieren Sie Backups von S3

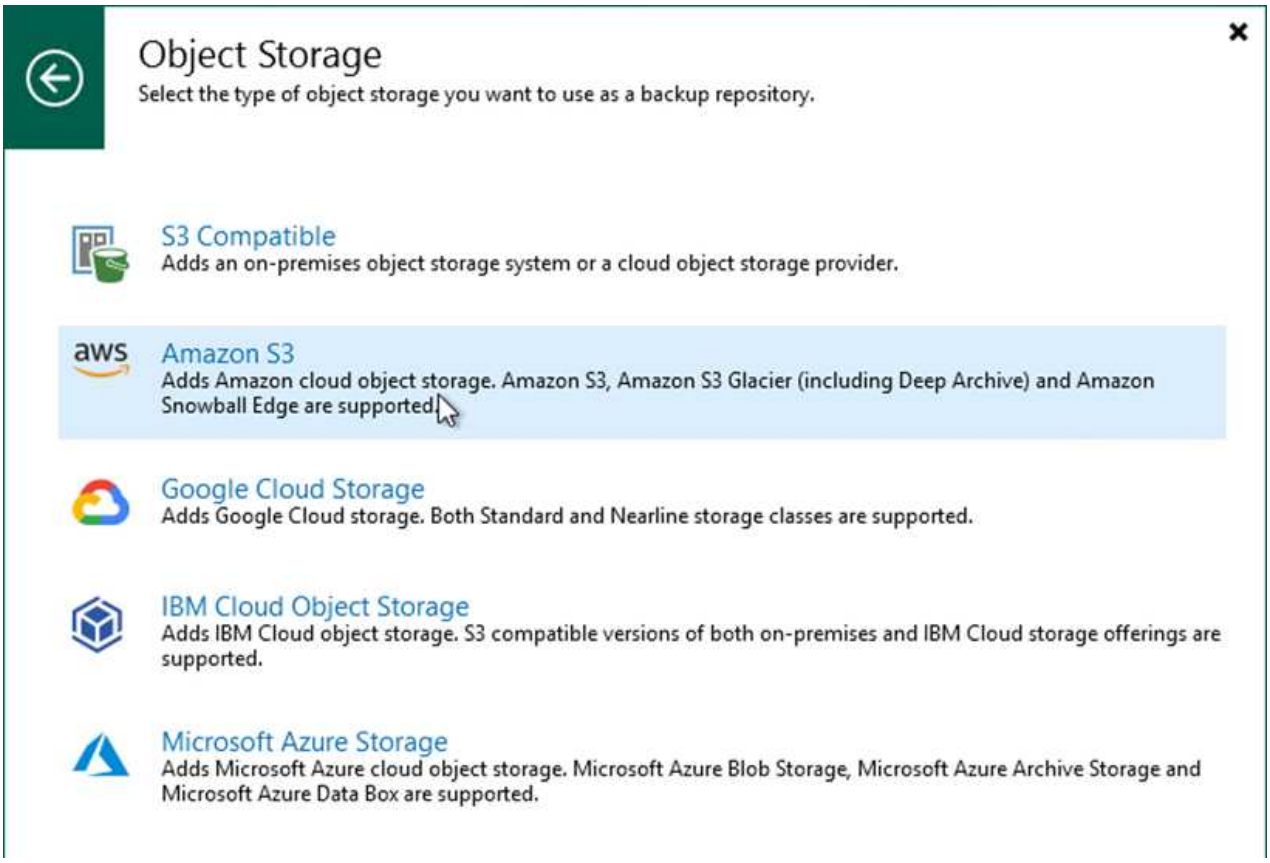
Importieren Sie vom sekundären Veeam-Server die Sicherungen aus dem S3-Speicher und stellen Sie die SQL Server- und Oracle-VMs in Ihrem VMware Cloud-Cluster wieder her.

Führen Sie die folgenden Schritte aus, um die Sicherungen aus dem S3-Objekt zu importieren, das Teil des lokalen Scale-Out-Sicherungsrepositorys war:

1. Gehen Sie zu „Backup-Repositorys“ und klicken Sie im oberen Menü auf „Repository hinzufügen“, um den Assistenten „Backup-Repository hinzufügen“ zu starten. Wählen Sie auf der ersten Seite des Assistenten „Object Storage“ als Sicherungsrepository-Typ aus.

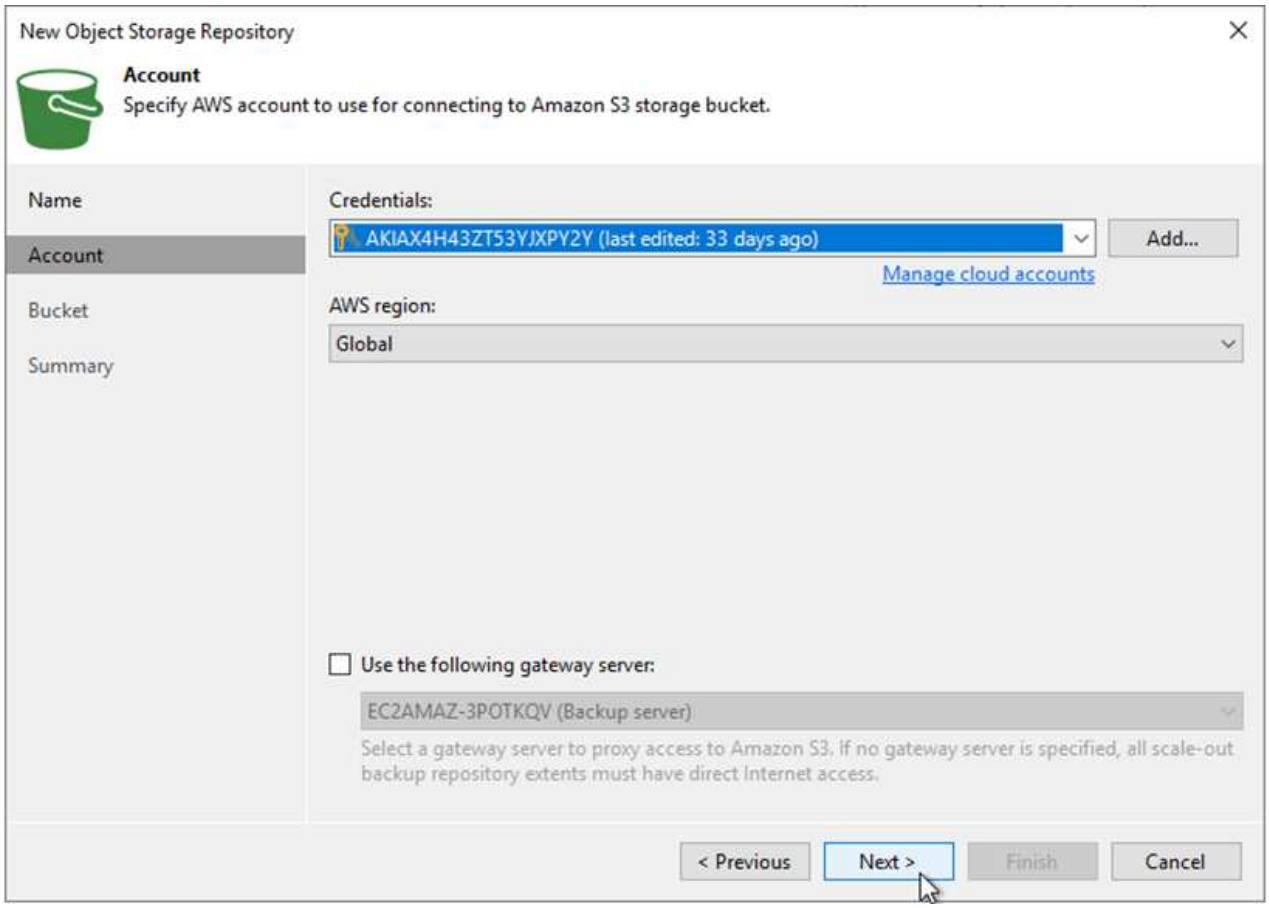


2. Wählen Sie Amazon S3 als Objektspeichertyp aus.

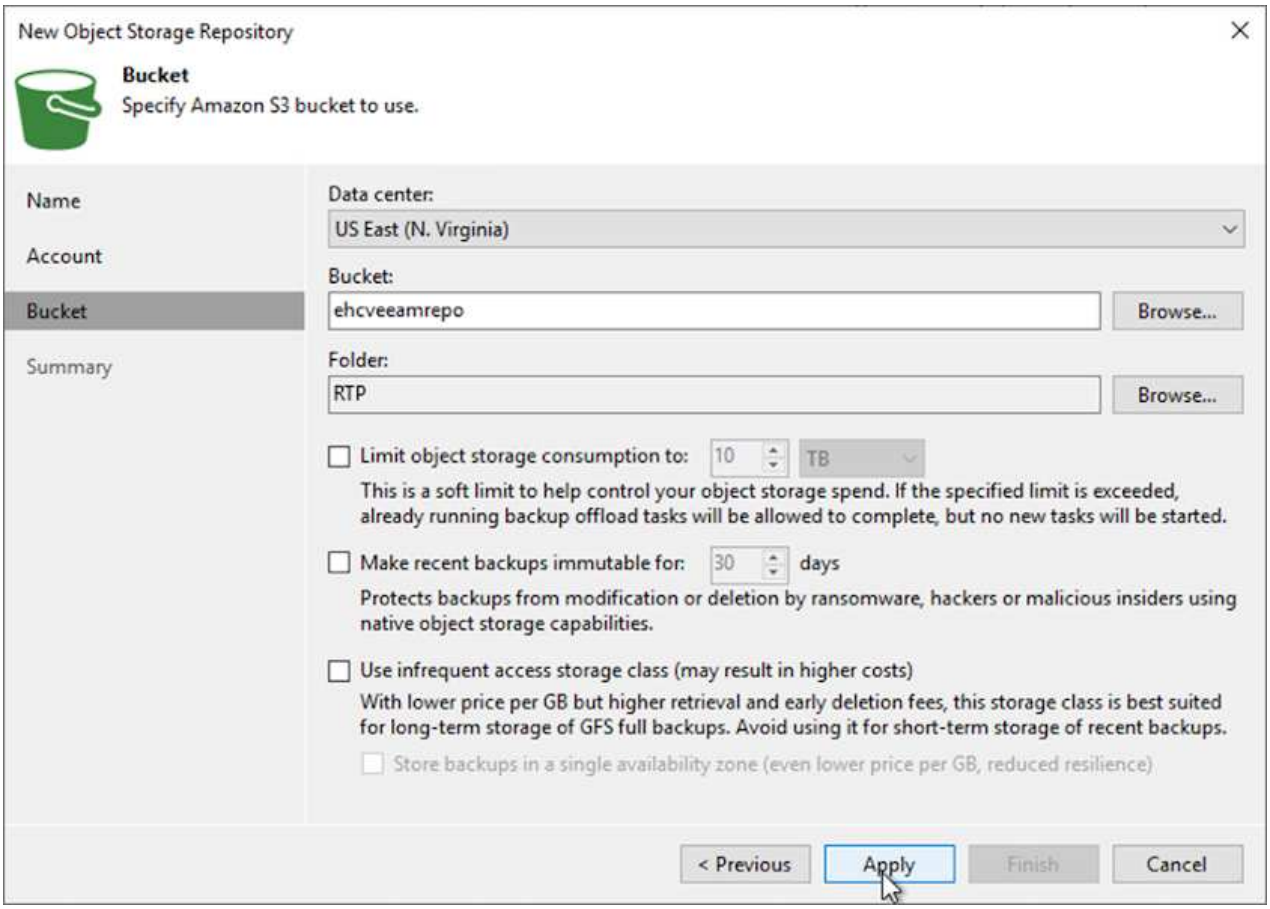


3. Wählen Sie aus der Liste der Amazon Cloud Storage Services Amazon S3 aus.

4. Wählen Sie Ihre vorab eingegebenen Anmeldeinformationen aus der Dropdown-Liste aus oder fügen Sie neue Anmeldeinformationen für den Zugriff auf die Cloud-Speicherressource hinzu. Klicken Sie auf Weiter, um fortzufahren.



5. Geben Sie auf der Bucket-Seite das Rechenzentrum, den Bucket, den Ordner und alle gewünschten Optionen ein. Klicken Sie auf „Übernehmen“.

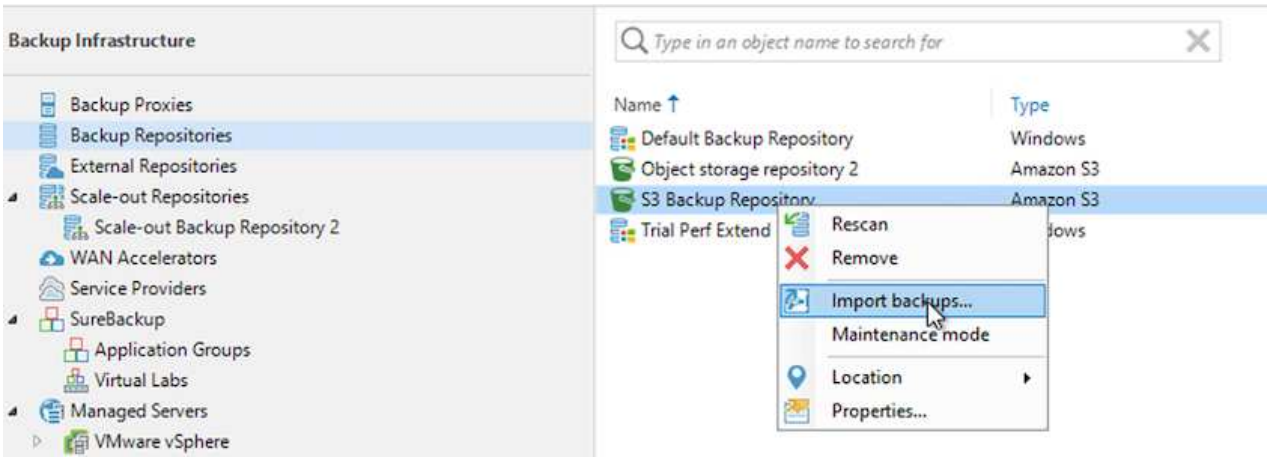


6. Wählen Sie abschließend „Fertig stellen“, um den Vorgang abzuschließen und das Repository hinzuzufügen.

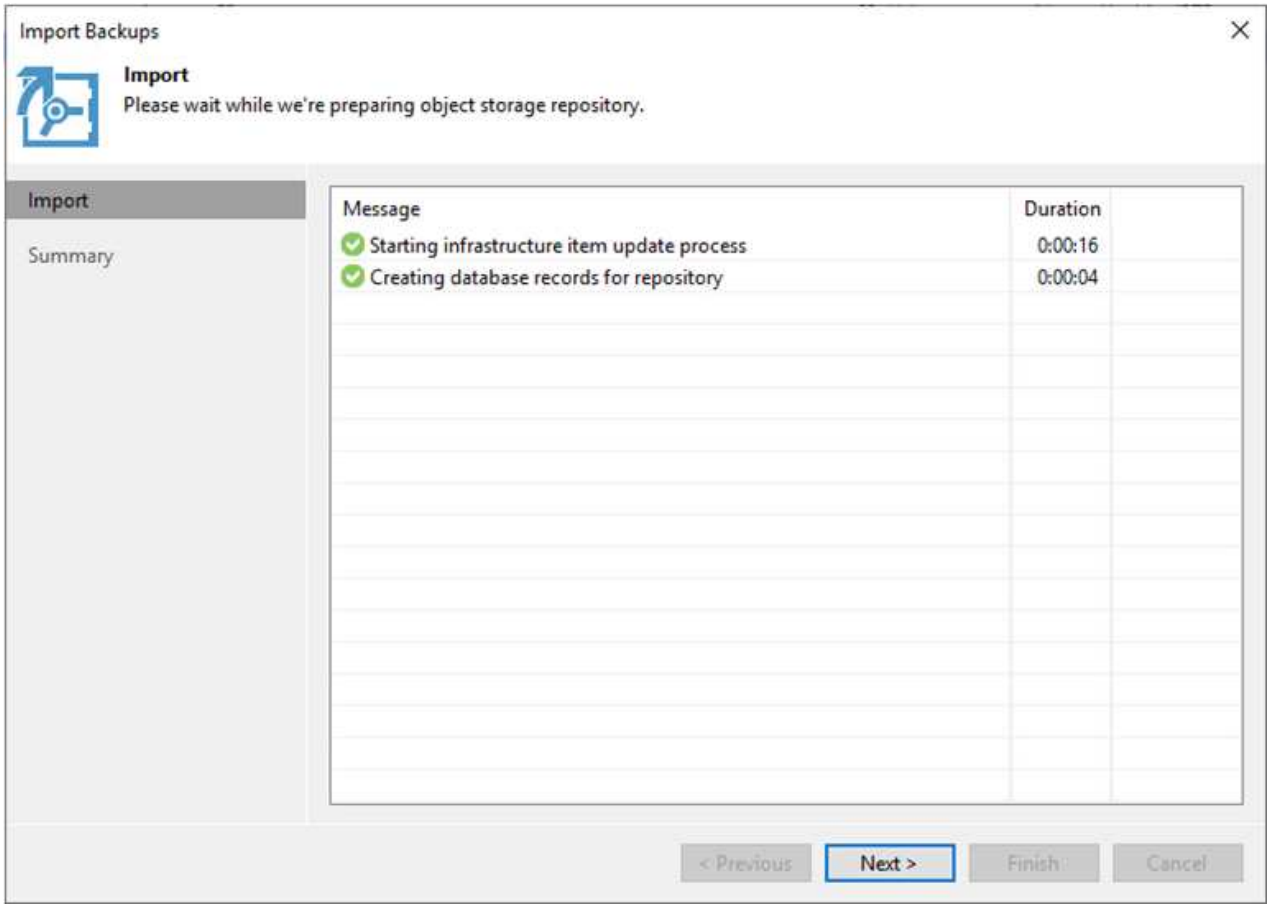
Importieren von Backups aus dem S3-Objektspeicher

Führen Sie die folgenden Schritte aus, um die Sicherungen aus dem S3-Repository zu importieren, das im vorherigen Abschnitt hinzugefügt wurde.

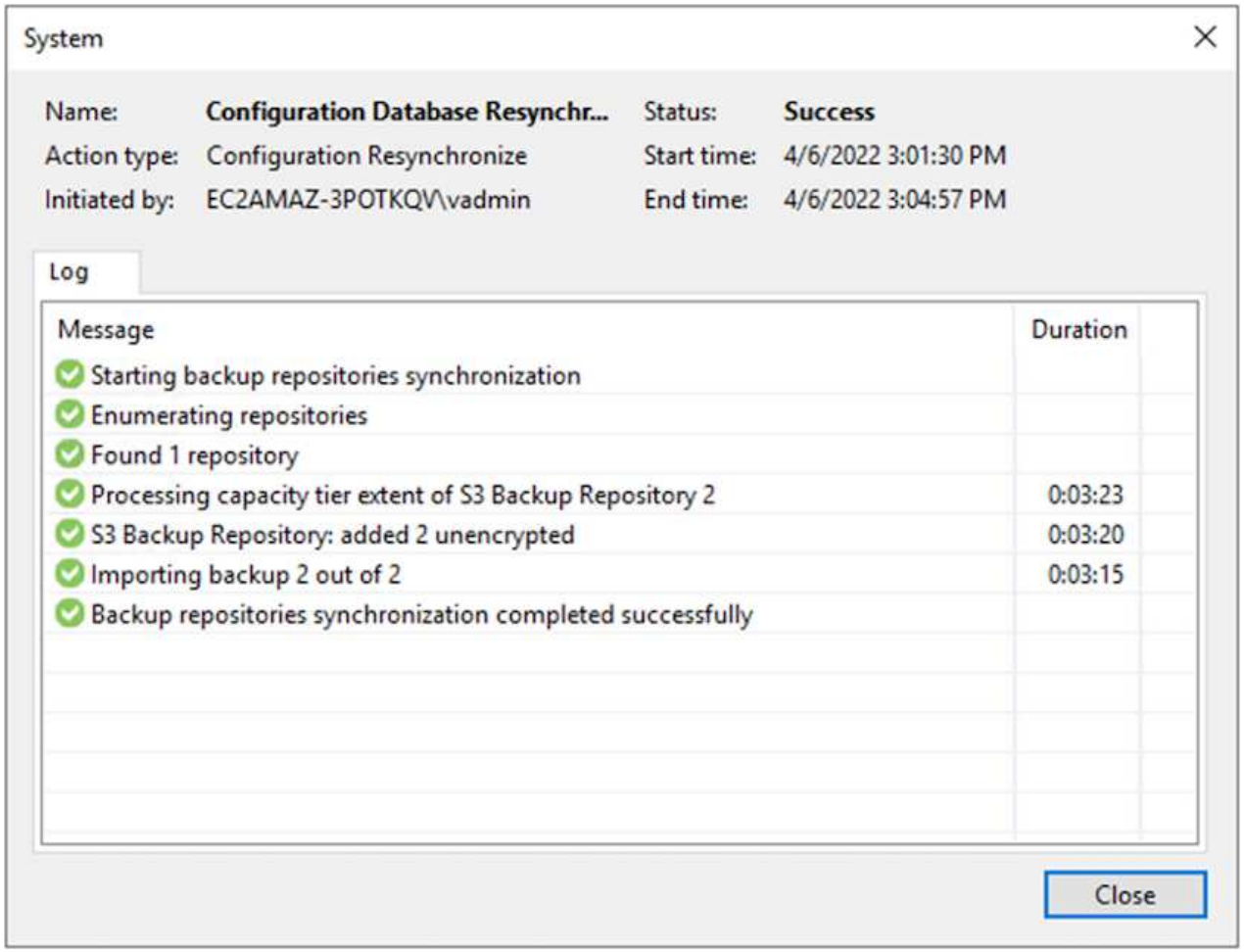
1. Wählen Sie im S3-Sicherungsrepository „Sicherungen importieren“ aus, um den Assistenten „Sicherungen importieren“ zu starten.



2. Nachdem die Datenbankeinträge für den Import erstellt wurden, wählen Sie auf dem Übersichtsbildschirm „Weiter“ und dann „Fertig stellen“, um den Importvorgang zu starten.



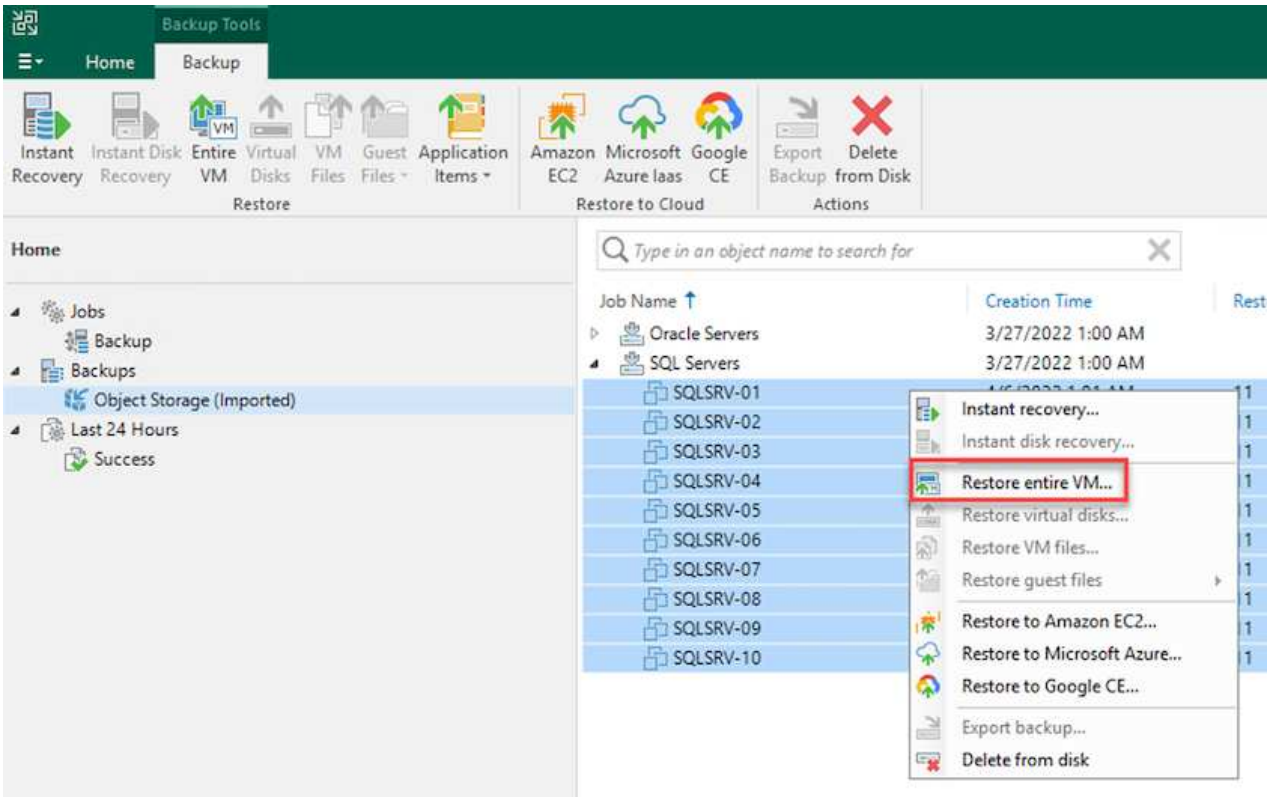
3. Nachdem der Import abgeschlossen ist, können Sie VMs im VMware Cloud-Cluster wiederherstellen.


System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

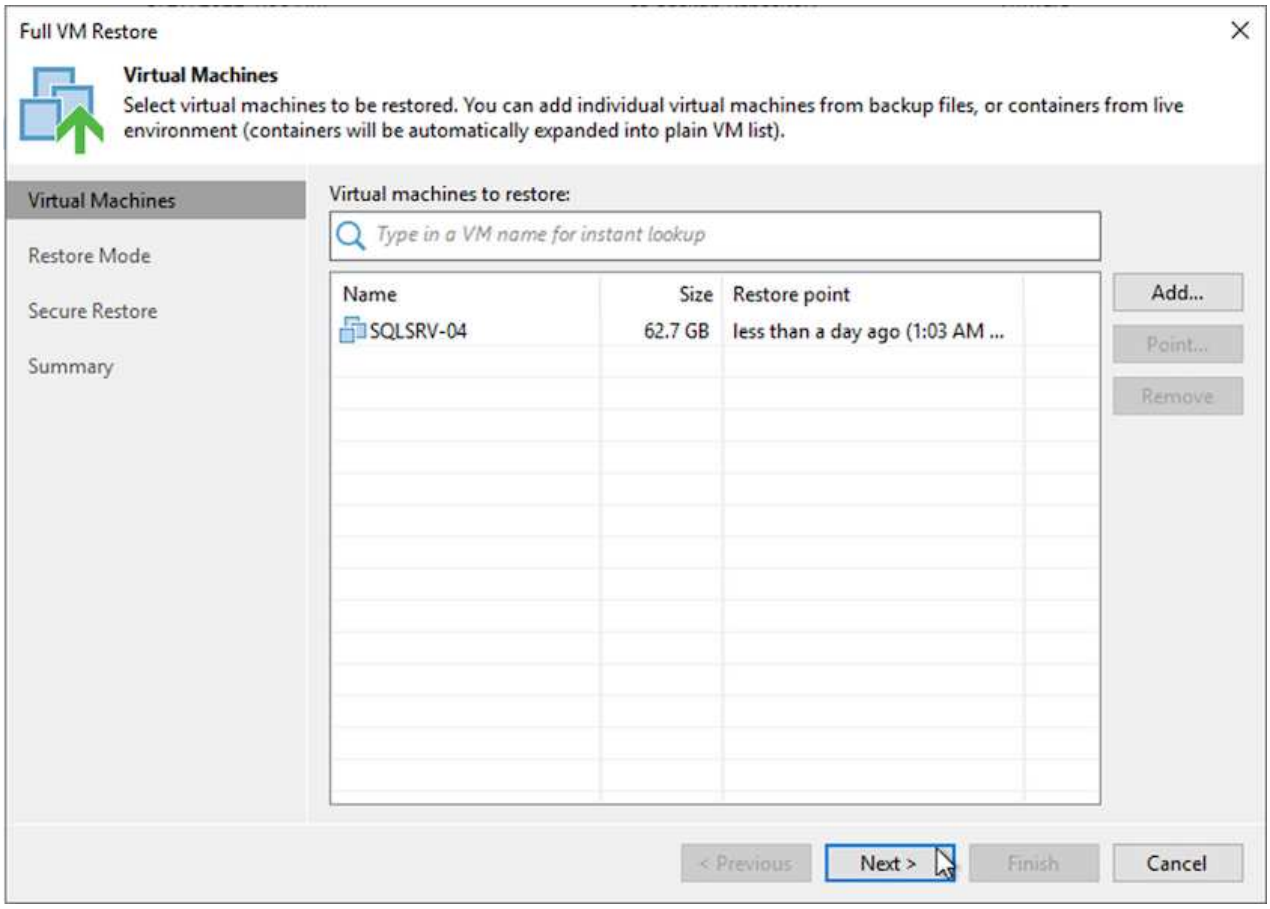
Stellen Sie Anwendungs-VMs mit der vollständigen Wiederherstellung von Veeam in der VMware Cloud wieder her

Führen Sie die folgenden Schritte aus, um SQL- und Oracle-VMs in der VMware Cloud on AWS-Workloaddomäne/dem -Cluster wiederherzustellen.

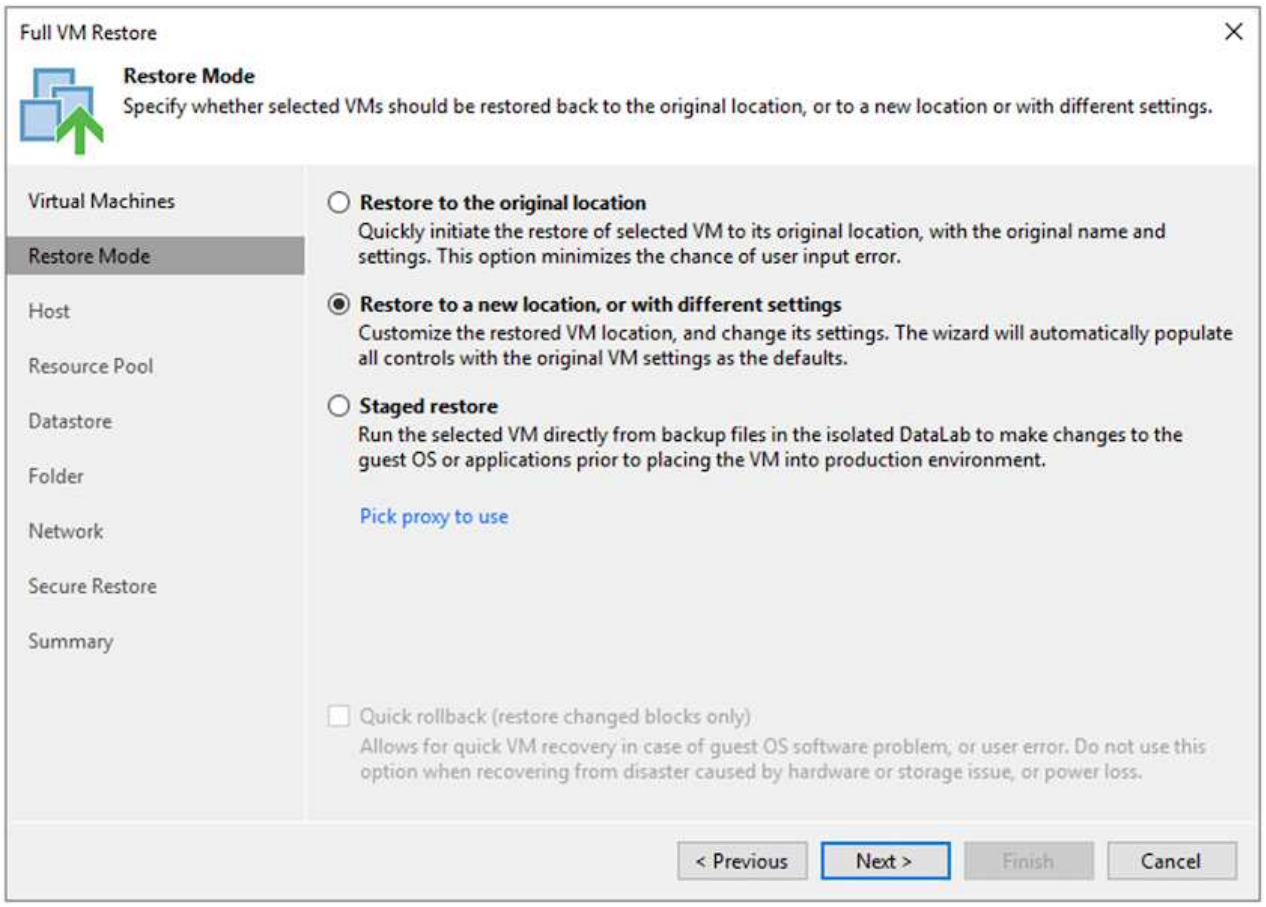
1. Wählen Sie auf der Veeam-Startseite den Objektspeicher mit den importierten Sicherungen aus, wählen Sie die wiederherzustellenden VMs aus, klicken Sie dann mit der rechten Maustaste und wählen Sie „Gesamte VM wiederherstellen“ aus.



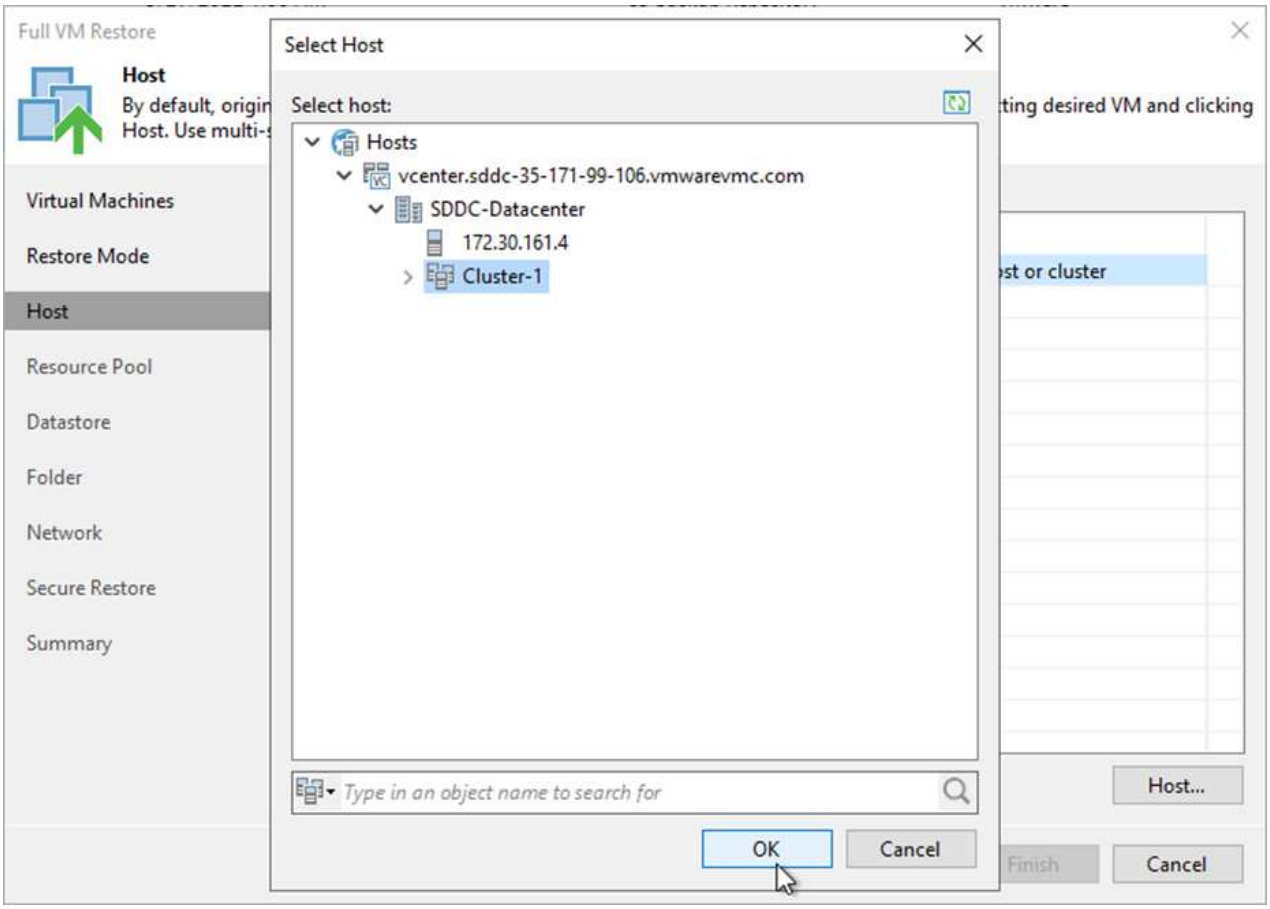
2. Ändern Sie auf der ersten Seite des Assistenten zur vollständigen VM-Wiederherstellung bei Bedarf die zu sichernden VMs und wählen Sie „Weiter“ aus.



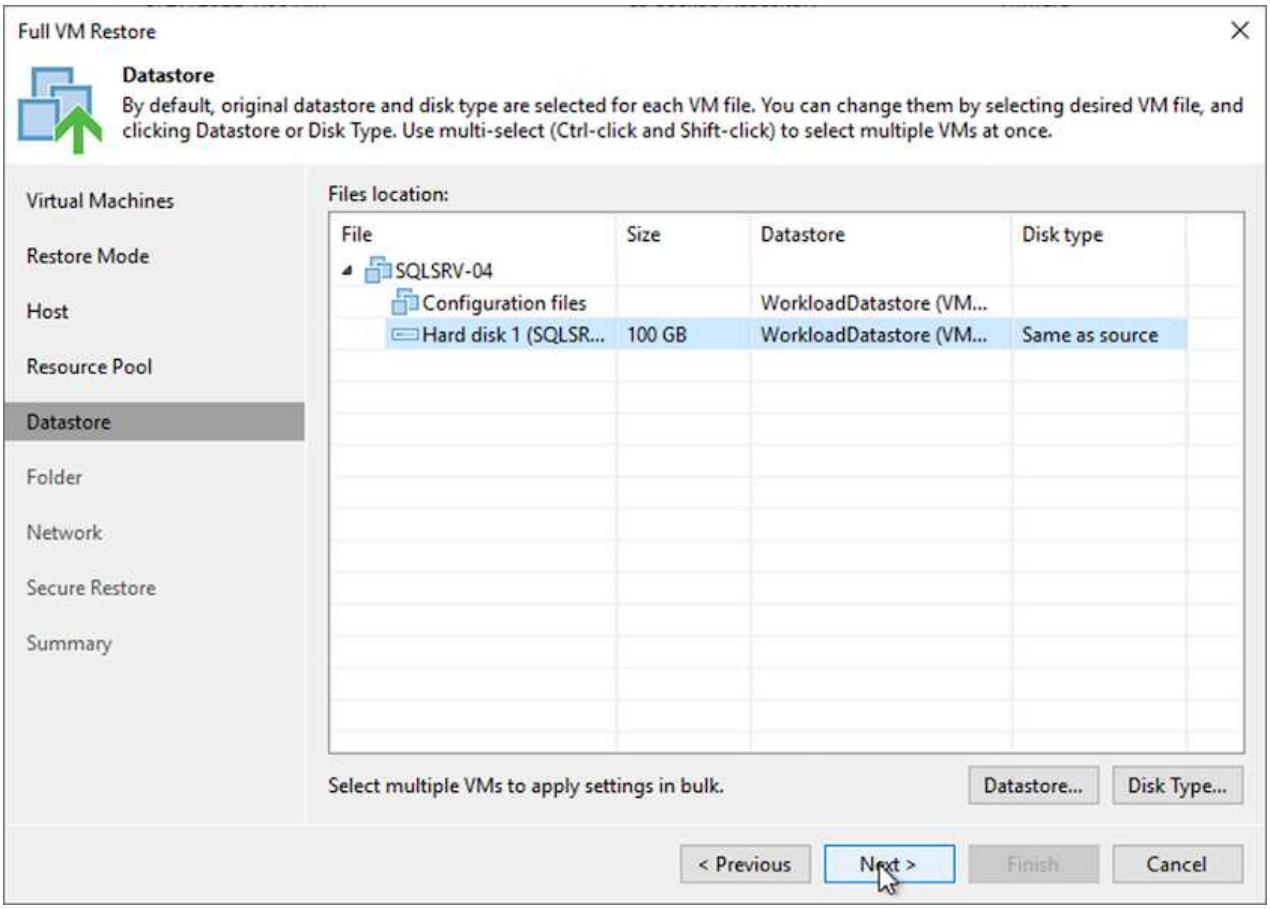
3. Wählen Sie auf der Seite „Wiederherstellungsmodus“ die Option „An einem neuen Speicherort oder mit anderen Einstellungen wiederherstellen“ aus.



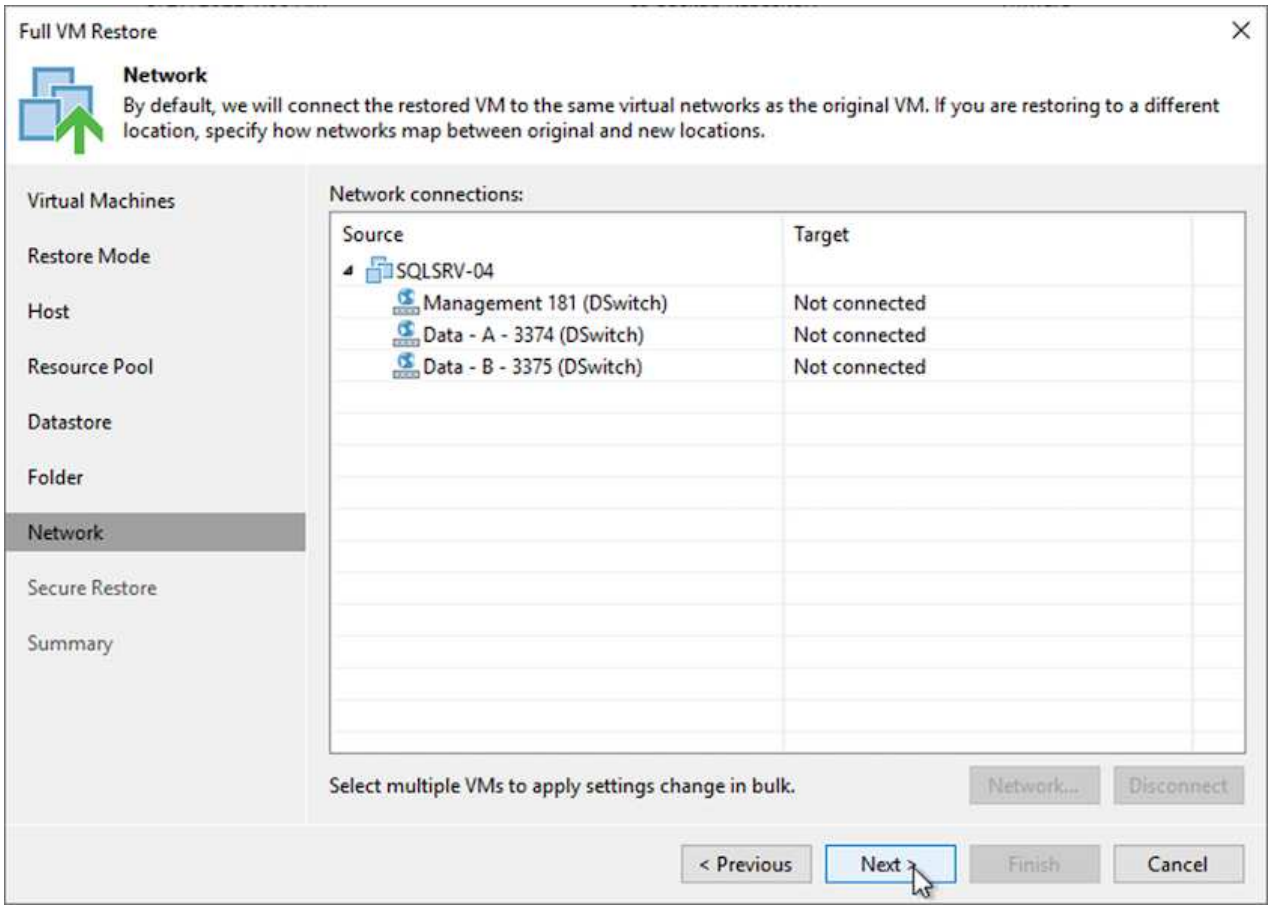
4. Wählen Sie auf der Hostseite den Ziel-ESXi-Host oder -Cluster aus, auf dem die VM wiederhergestellt werden soll.

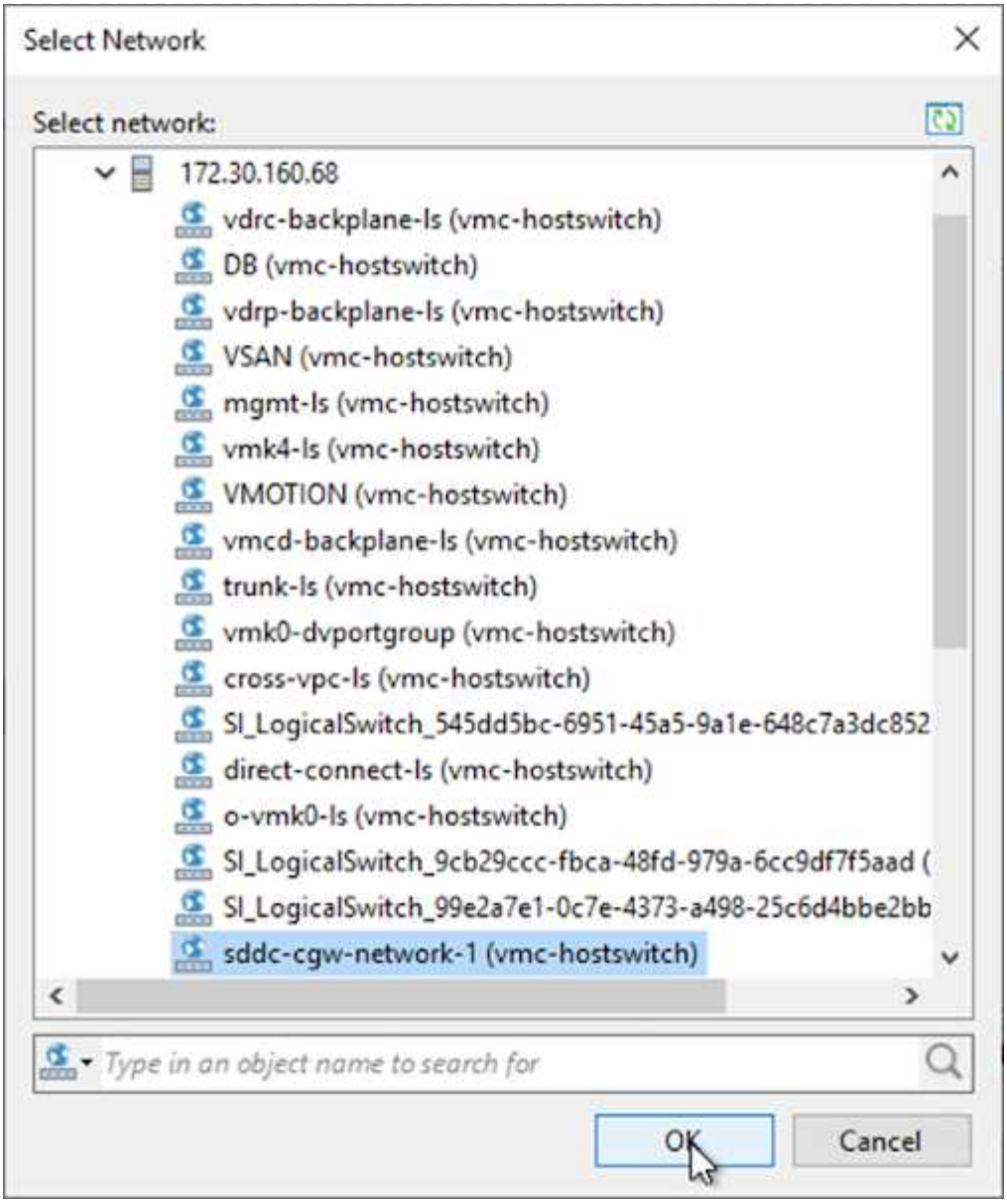


5. Wählen Sie auf der Seite „Datenspeicher“ den Zielspeicherort für die Konfigurationsdateien und die Festplatte aus.



6. Ordnen Sie auf der Seite „Netzwerk“ die ursprünglichen Netzwerke auf der VM den Netzwerken am neuen Zielstandort zu.


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. Wählen Sie aus, ob die wiederhergestellte VM auf Malware gescannt werden soll, überprüfen Sie die Übersichtsseite und klicken Sie auf „Fertig stellen“, um die Wiederherstellung zu starten.

Wiederherstellen von SQL Server-Anwendungsdaten

Der folgende Prozess enthält Anweisungen zum Wiederherstellen eines SQL-Servers in VMware Cloud Services in AWS im Falle einer Katastrophe, die den lokalen Standort funktionsunfähig macht.

Um mit den Wiederherstellungsschritten fortfahren zu können, wird davon ausgegangen, dass die folgenden Voraussetzungen erfüllt sind:

1. Die Windows Server-VM wurde mithilfe von Veeam Full Restore im VMware Cloud SDDC wiederhergestellt.
2. Ein sekundärer SnapCenter -Server wurde eingerichtet und die Wiederherstellung und Konfiguration der SnapCenter Datenbank wurde mit den im Abschnitt beschriebenen Schritten abgeschlossen"Zusammenfassung des SnapCenter -Sicherungs- und Wiederherstellungsprozesses."

VM: Konfiguration nach der Wiederherstellung für SQL Server-VM

Nachdem die Wiederherstellung der VM abgeschlossen ist, müssen Sie das Netzwerk und andere Elemente konfigurieren, um die Host-VM in SnapCenter erneut zu erkennen.

1. Weisen Sie neue IP-Adressen für Management und iSCSI oder NFS zu.
2. Fügen Sie den Host der Windows-Domäne hinzu.
3. Fügen Sie die Hostnamen zum DNS oder zur Hosts-Datei auf dem SnapCenter -Server hinzu.

> Wenn das SnapCenter -Plug-In mit anderen Domänenanmeldeinformationen als der aktuellen Domäne bereitgestellt wurde, müssen Sie das Anmeldekonto für das Plug-In für den Windows-Dienst auf der SQL Server-VM ändern. Starten Sie nach dem Ändern des Anmeldekontos die Dienste SnapCenter SMCore, Plug-in für Windows und Plug-in für SQL Server neu.

> Um die wiederhergestellten VMs in SnapCenter automatisch wiederzuerkennen, muss der FQDN mit dem der VM identisch sein, die ursprünglich vor Ort zum SnapCenter hinzugefügt wurde.

Konfigurieren des FSx-Speichers für die SQL Server-Wiederherstellung

Um den Disaster Recovery-Wiederherstellungsprozess für eine SQL Server-VM durchzuführen, müssen Sie die bestehende SnapMirror -Beziehung zum FSx-Cluster trennen und Zugriff auf das Volume gewähren. Führen Sie dazu die folgenden Schritte aus.

1. Um die vorhandene SnapMirror -Beziehung für die SQL Server-Datenbank und die Protokollvolumes aufzuheben, führen Sie den folgenden Befehl von der FSx-CLI aus:

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. Gewähren Sie Zugriff auf die LUN, indem Sie eine Initiatorgruppe erstellen, die den iSCSI-IQN der SQL Server-Windows-VM enthält:

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

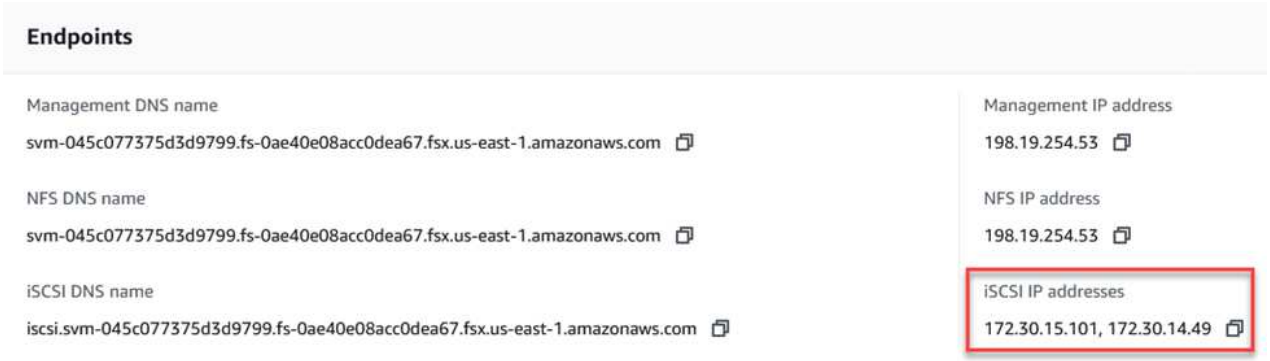
3. Ordnen Sie abschließend die LUNs der Initiatorgruppe zu, die Sie gerade erstellt haben:

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

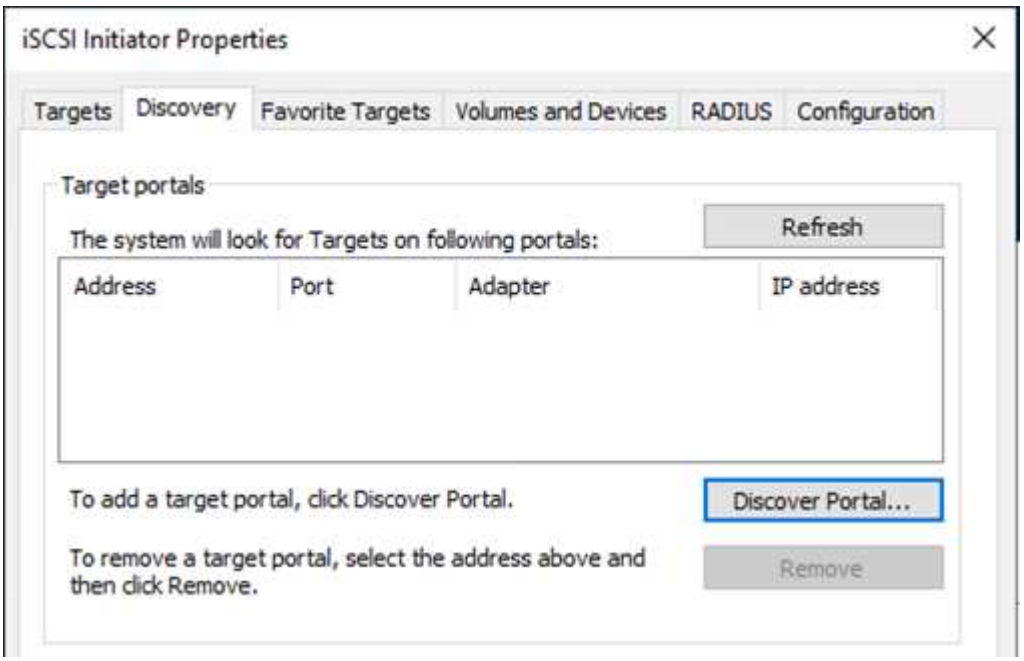
4. Um den Pfadnamen zu finden, führen Sie den `lun show` Befehl.

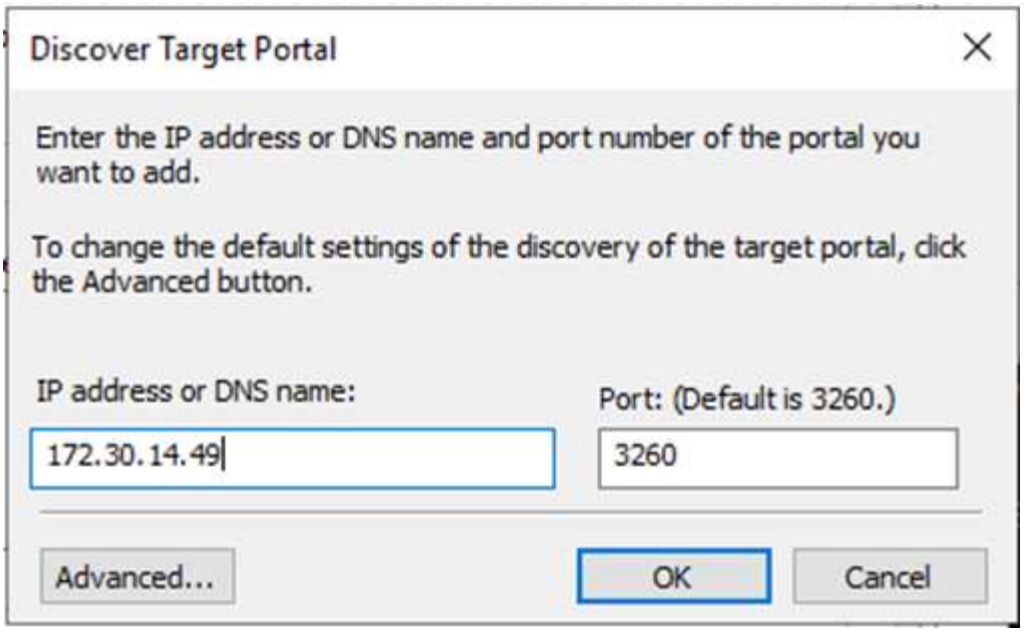
Einrichten der Windows-VM für den iSCSI-Zugriff und Ermitteln der Dateisysteme

1. Richten Sie von der SQL Server-VM aus Ihren iSCSI-Netzwerkadapter für die Kommunikation mit der VMware-Portgruppe ein, die mit Konnektivität zu den iSCSI-Zielschnittstellen auf Ihrer FSx-Instanz eingerichtet wurde.
2. Öffnen Sie das Dienstprogramm „iSCSI-Initiator-Eigenschaften“ und löschen Sie die alten Konnektivitätseinstellungen auf den Registerkarten „Erkennung“, „Favoritenziele“ und „Ziele“.
3. Suchen Sie die IP-Adresse(n) für den Zugriff auf die logische iSCSI-Schnittstelle auf der FSx-Instanz/dem FSx-Cluster. Dies finden Sie in der AWS-Konsole unter Amazon FSx > ONTAP > Storage Virtual Machines.

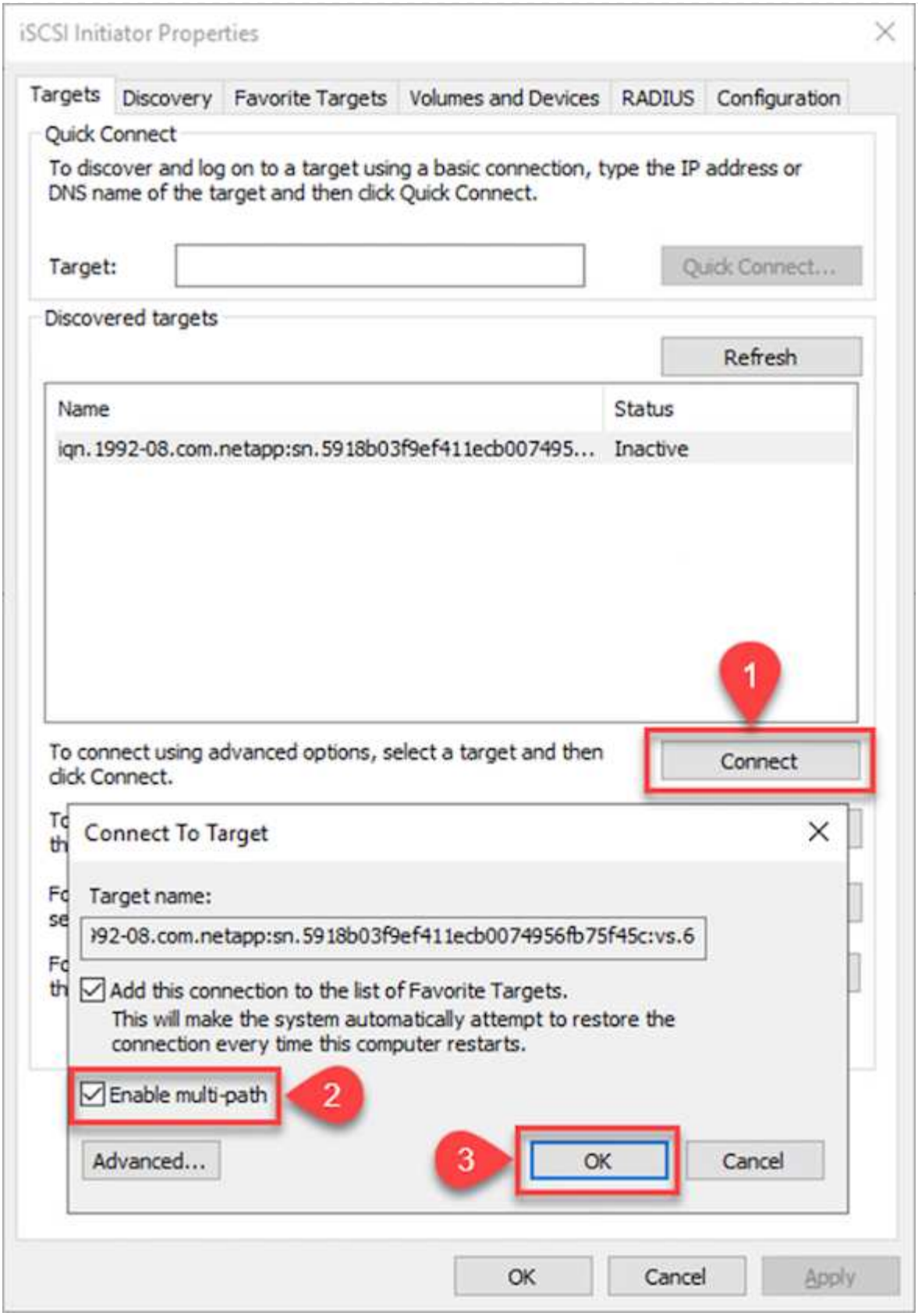


4. Klicken Sie auf der Registerkarte „Discovery“ auf „Discover Portal“ und geben Sie die IP-Adressen für Ihre FSx-iSCSI-Ziele ein.

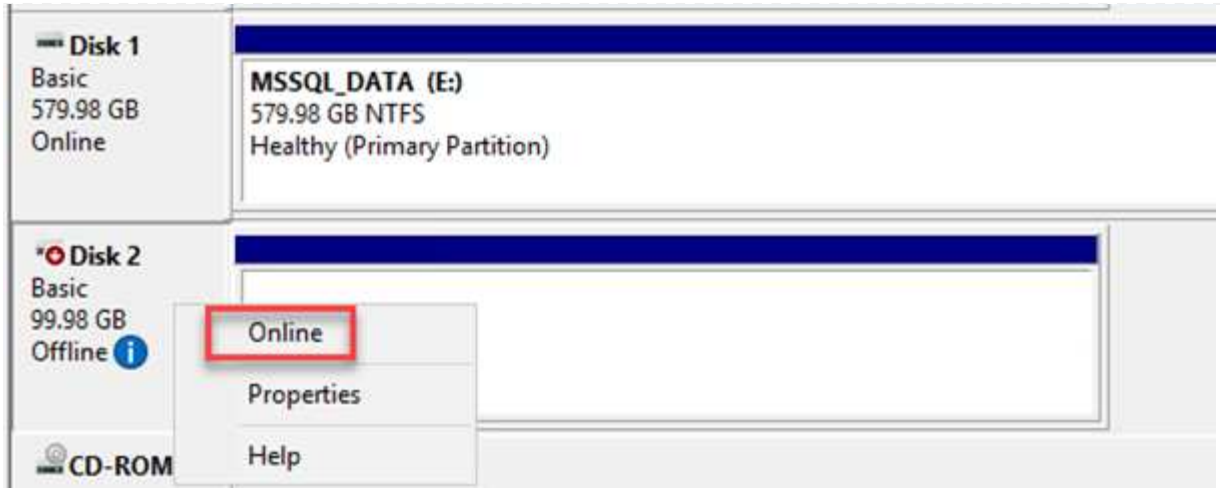




5. Klicken Sie auf der Registerkarte „Ziel“ auf „Verbinden“, wählen Sie „Mehrere Pfade aktivieren“ aus, falls dies für Ihre Konfiguration geeignet ist, und klicken Sie dann auf „OK“, um eine Verbindung mit dem Ziel herzustellen.

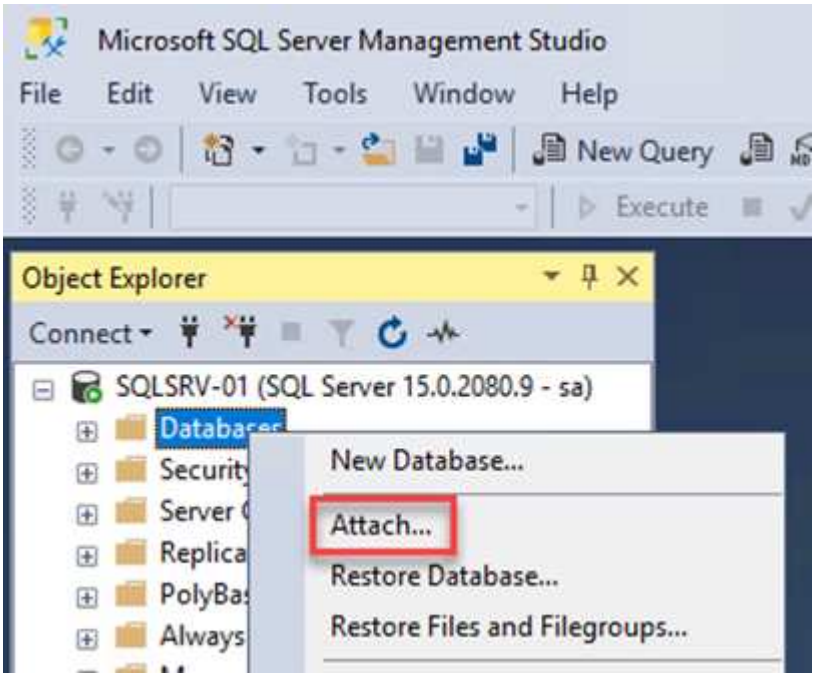


6. Öffnen Sie das Dienstprogramm „Computerverwaltung“ und schalten Sie die Festplatten online. Stellen Sie sicher, dass sie dieselben Laufwerksbuchstaben behalten, die sie zuvor hatten.

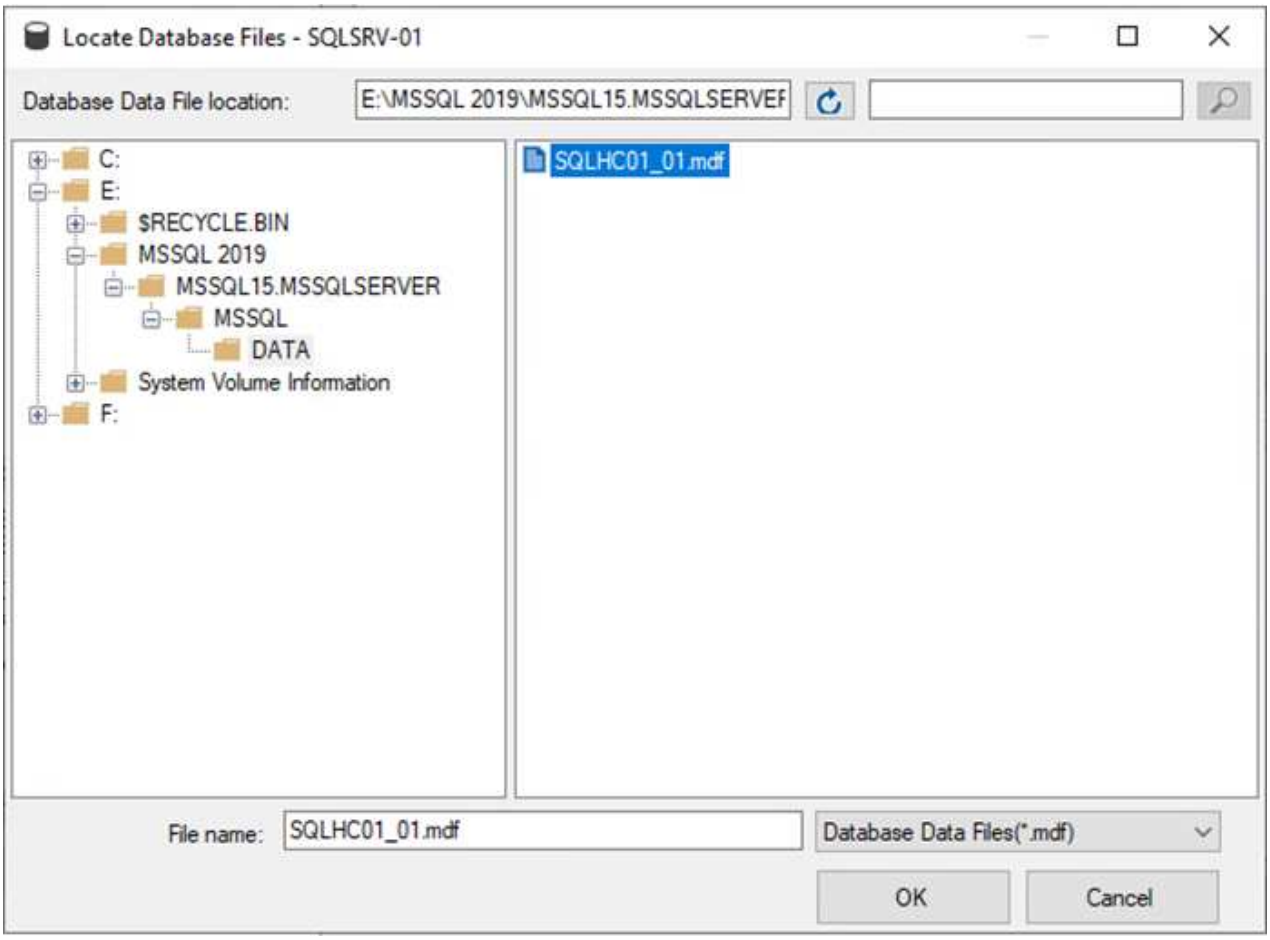

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Anfügen der SQL Server-Datenbanken

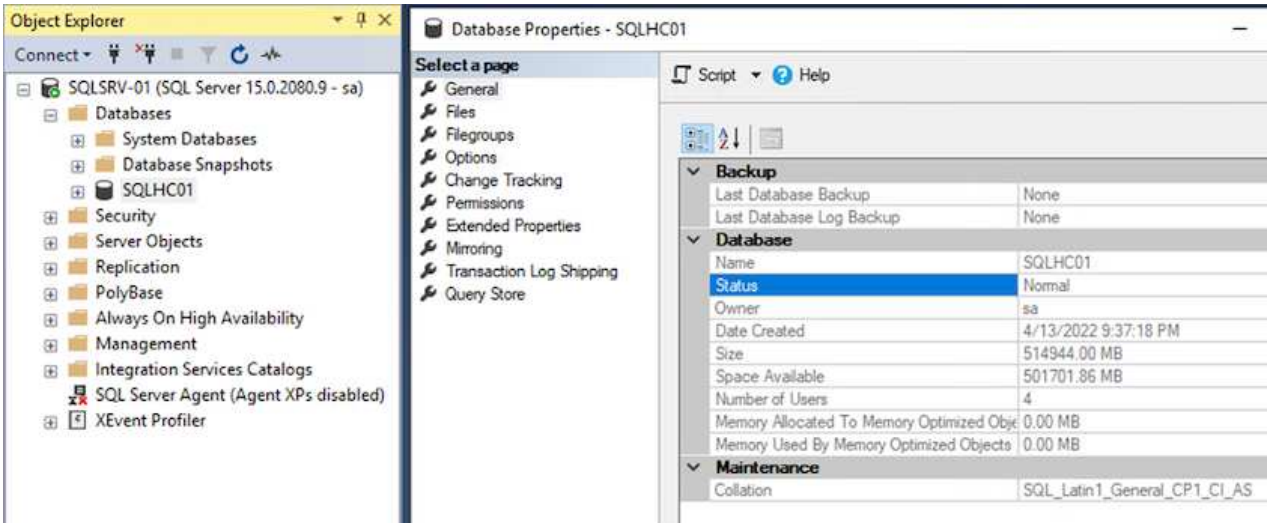
1. Öffnen Sie von der SQL Server-VM aus Microsoft SQL Server Management Studio und wählen Sie „Anhängen“ aus, um den Verbindungsvorgang mit der Datenbank zu starten.



2. Klicken Sie auf „Hinzufügen“, navigieren Sie zu dem Ordner, der die primäre SQL Server-Datenbankdatei enthält, wählen Sie sie aus und klicken Sie auf „OK“.



3. Wenn sich die Transaktionsprotokolle auf einem separaten Laufwerk befinden, wählen Sie den Ordner aus, der das Transaktionsprotokoll enthält.
4. Wenn Sie fertig sind, klicken Sie auf „OK“, um die Datenbank anzuhängen.

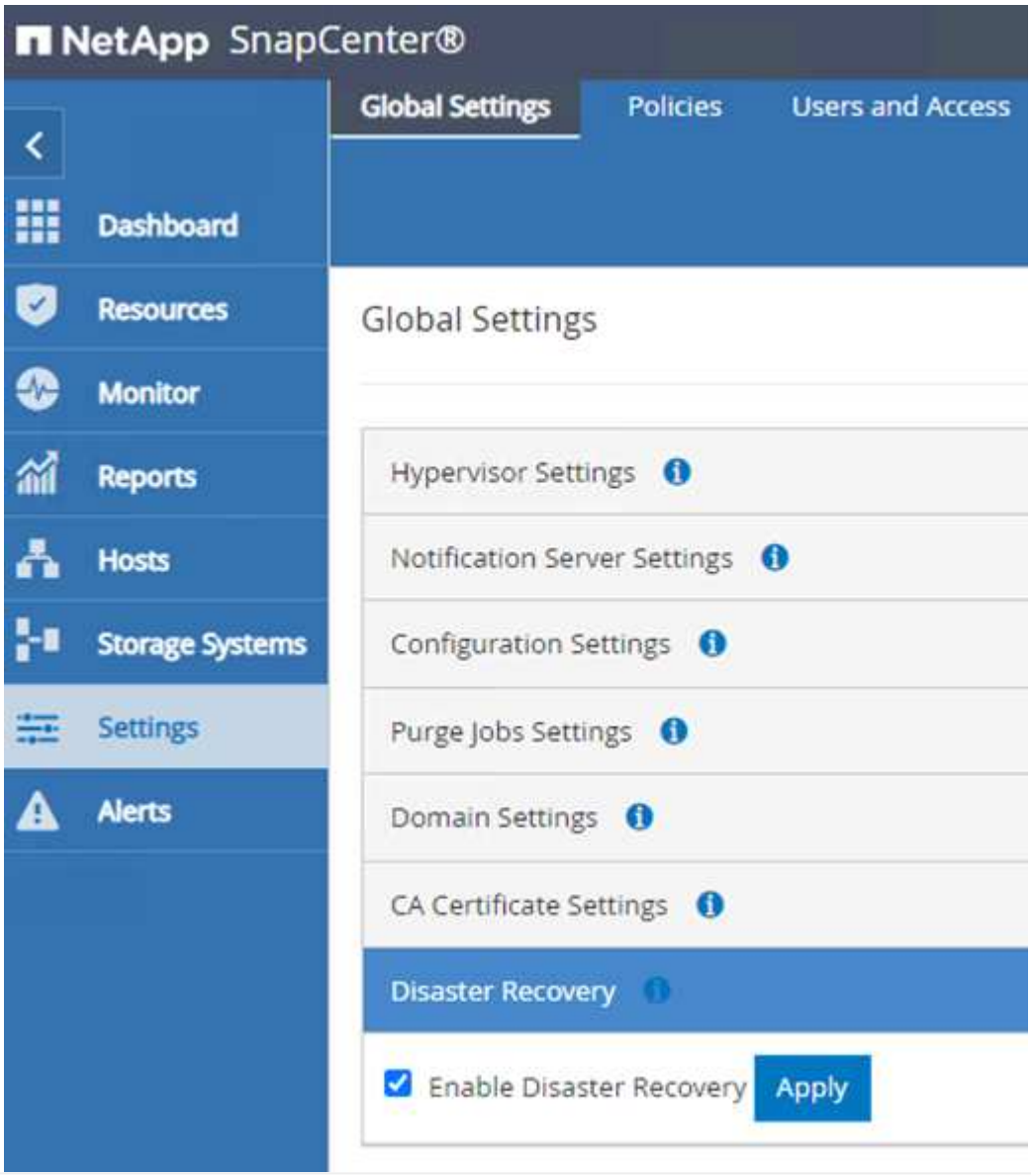


Bestätigen Sie die SnapCenter -Kommunikation mit dem SQL Server-Plug-in

Wenn die SnapCenter -Datenbank in ihren vorherigen Zustand zurückversetzt wird, werden die SQL Server-Hosts automatisch neu erkannt. Damit dies ordnungsgemäß funktioniert, beachten Sie die folgenden Voraussetzungen:

- SnapCenter muss in den Disaster-Recovery-Modus versetzt werden. Dies kann über die Swagger-API oder in den globalen Einstellungen unter „Disaster Recovery“ erreicht werden.
- Der FQDN des SQL-Servers muss mit der Instanz identisch sein, die im lokalen Rechenzentrum ausgeführt wurde.
- Die ursprüngliche SnapMirror Beziehung muss unterbrochen werden.
- Die LUNs, die die Datenbank enthalten, müssen in die SQL Server-Instanz eingebunden und die Datenbank angehängt werden.

Um zu bestätigen, dass sich SnapCenter im Disaster Recovery-Modus befindet, navigieren Sie im SnapCenter -Webclient zu „Einstellungen“. Gehen Sie zur Registerkarte „Globale Einstellungen“ und klicken Sie dann auf „Notfallwiederherstellung“. Stellen Sie sicher, dass das Kontrollkästchen „Notfallwiederherstellung aktivieren“ aktiviert ist.



Wiederherstellen von Oracle-Anwendungsdaten

Der folgende Prozess enthält Anweisungen zum Wiederherstellen von Oracle-Anwendungsdaten in VMware Cloud Services in AWS im Falle einer Katastrophe, die den lokalen Standort funktionsunfähig macht.

Erfüllen Sie die folgenden Voraussetzungen, um mit den Wiederherstellungsschritten fortzufahren:

1. Die Oracle Linux-Server-VM wurde mithilfe von Veeam Full Restore im VMware Cloud SDDC wiederhergestellt.
2. Ein sekundärer SnapCenter -Server wurde eingerichtet und die SnapCenter -Datenbank und Konfigurationsdateien wurden mit den in diesem Abschnitt beschriebenen Schritten wiederhergestellt"Zusammenfassung des SnapCenter -Sicherungs- und Wiederherstellungsprozesses."

Konfigurieren Sie FSx für die Oracle-Wiederherstellung – Unterbrechen Sie die SnapMirror -Beziehung

Um die auf der FSx ONTAP Instanz gehosteten sekundären Speichervolumes für die Oracle-Server zugänglich zu machen, müssen Sie zunächst die bestehende SnapMirror -Beziehung aufheben.

1. Führen Sie nach der Anmeldung bei der FSx-CLI den folgenden Befehl aus, um die nach dem richtigen Namen gefilterten Volumes anzuzeigen.

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

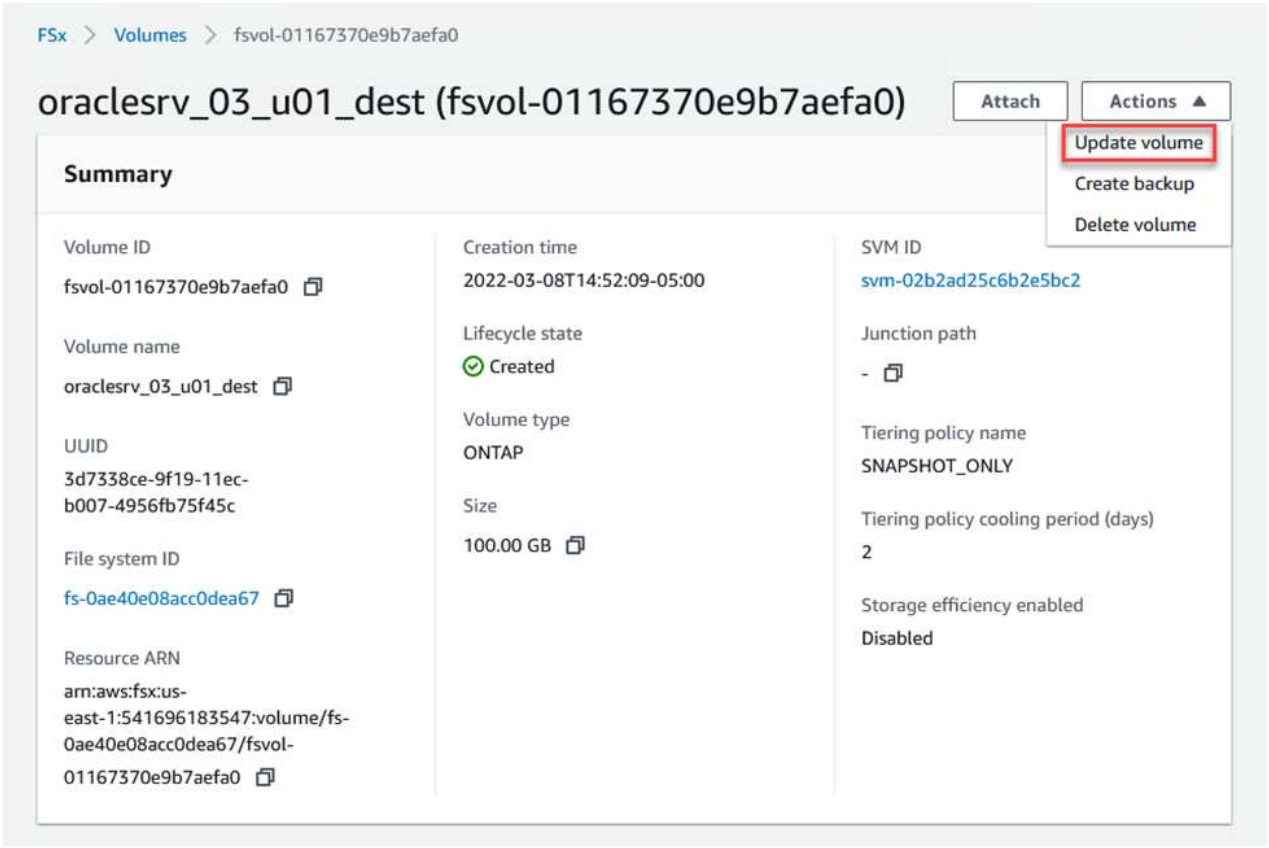
2. Führen Sie den folgenden Befehl aus, um die vorhandenen SnapMirror -Beziehungen aufzuheben.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

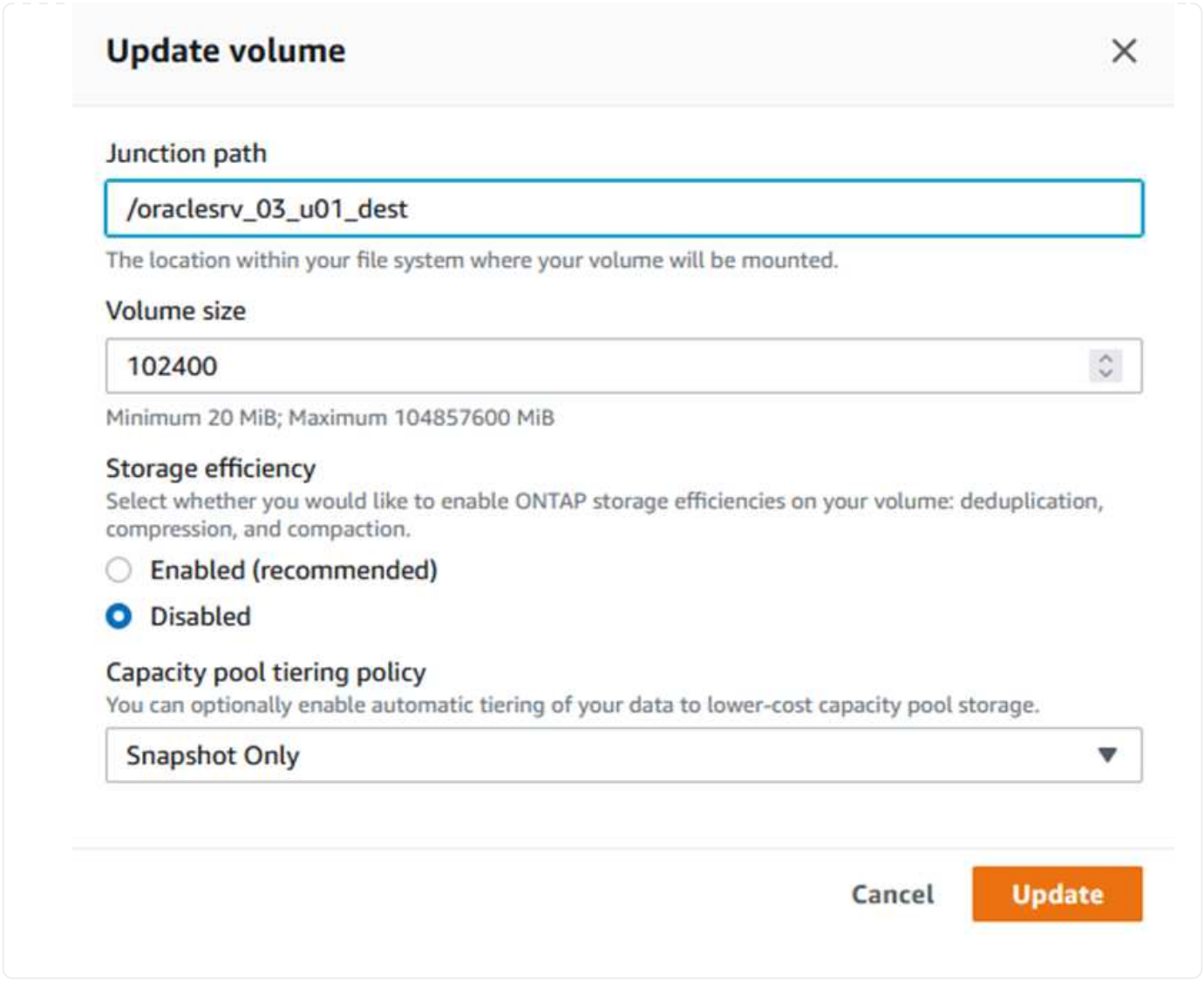
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Aktualisieren Sie den Junction-Pfad im Amazon FSx Webclient:



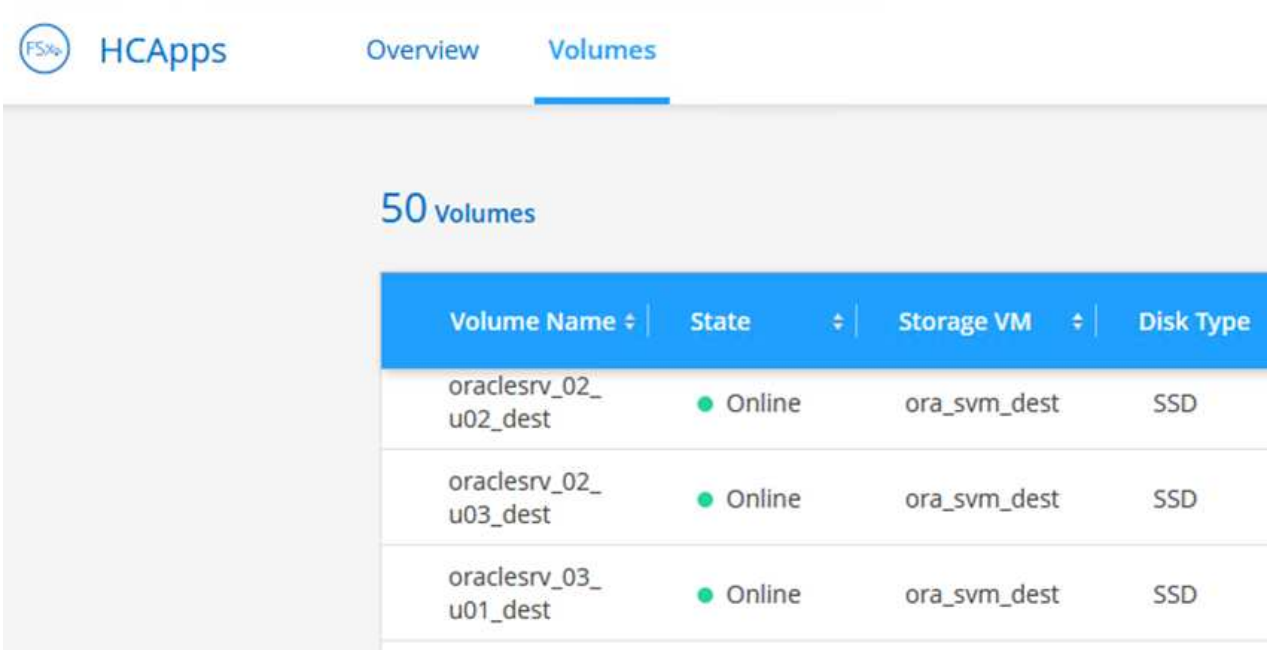
4. Fügen Sie den Namen des Kreuzungspfads hinzu und klicken Sie auf „Aktualisieren“. Geben Sie diesen Verbindungspfad an, wenn Sie das NFS-Volume vom Oracle-Server mounten.


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

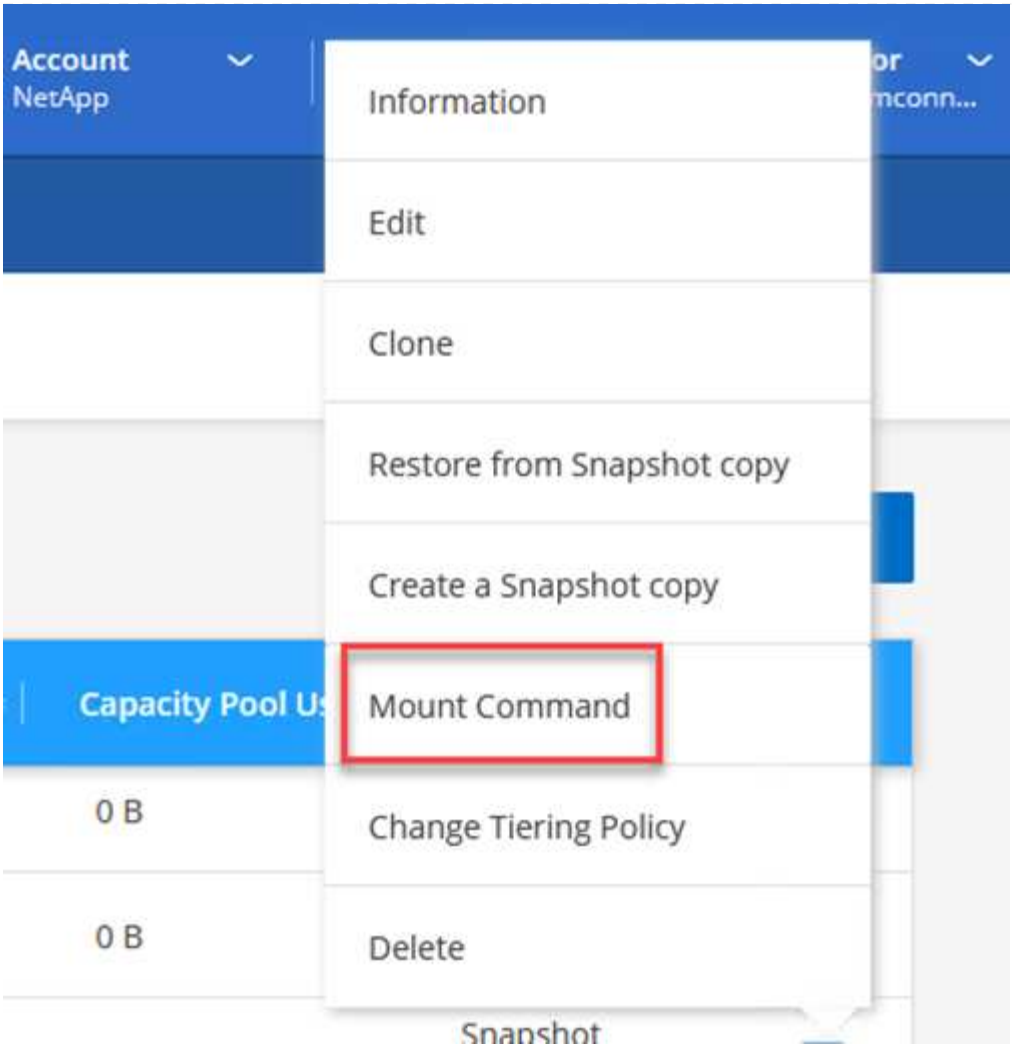
Mounten Sie NFS-Volumes auf Oracle Server

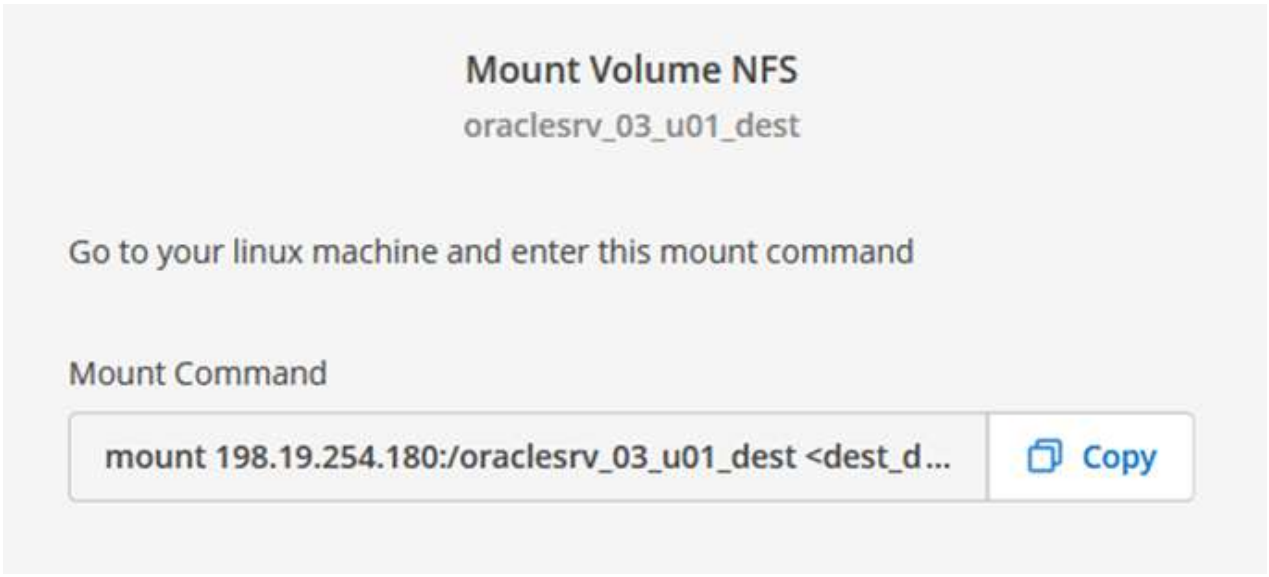
In Cloud Manager können Sie den Mount-Befehl mit der richtigen NFS-LIF-IP-Adresse zum Mounten der NFS-Volumes abrufen, die die Oracle-Datenbankdateien und -Protokolle enthalten.

1. Greifen Sie in Cloud Manager auf die Liste der Volumes für Ihren FSx-Cluster zu.



2. Wählen Sie im Aktionsmenü „Mount-Befehl“ aus, um den Mount-Befehl anzuzeigen und zu kopieren, der auf unserem Oracle Linux-Server verwendet werden soll.





3. Mounten Sie das NFS-Dateisystem auf dem Oracle Linux-Server. Die Verzeichnisse zum Einbinden der NFS-Freigabe sind auf dem Oracle Linux-Host bereits vorhanden.
4. Verwenden Sie vom Oracle Linux-Server aus den Mount-Befehl, um die NFS-Volumes zu mounten.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Wiederholen Sie diesen Schritt für jedes Volume, das mit den Oracle-Datenbanken verknüpft ist.

Um die NFS-Einbindung beim Neustart dauerhaft zu machen, bearbeiten Sie die `/etc/fstab` Datei, um die Mount-Befehle einzuschließen.

5. Starten Sie den Oracle-Server neu. Die Oracle-Datenbanken sollten normal starten und zur Verwendung verfügbar sein.

Failback

Nach erfolgreichem Abschluss des in dieser Lösung beschriebenen Failover-Prozesses nehmen SnapCenter und Veeam ihre in AWS ausgeführten Sicherungsfunktionen wieder auf und FSx ONTAP wird nun als primärer Speicher ohne bestehende SnapMirror Beziehungen mit dem ursprünglichen lokalen Rechenzentrum ausgewiesen. Nachdem der normale Betrieb vor Ort wieder aufgenommen wurde, können Sie einen Prozess verwenden, der mit dem in dieser Dokumentation beschriebenen identisch ist, um die Daten zurück auf das lokale ONTAP Speichersystem zu spiegeln.

Wie in dieser Dokumentation auch beschrieben, können Sie SnapCenter so konfigurieren, dass die Anwendungsdatenvolumes von FSx ONTAP auf ein ONTAP -Speichersystem vor Ort gespiegelt werden. Ebenso können Sie Veeam so konfigurieren, dass Sicherungskopien mithilfe eines Scale-Out-Backup-Repositorys auf Amazon S3 repliziert werden, sodass diese Sicherungen für einen Veeam-Backup-Server im lokalen Rechenzentrum zugänglich sind.

Failback liegt außerhalb des Rahmens dieser Dokumentation, unterscheidet sich jedoch kaum von dem hier ausführlich beschriebenen Prozess.

Abschluss

Der in dieser Dokumentation vorgestellte Anwendungsfall konzentriert sich auf bewährte Disaster Recovery-Technologien, die die Integration zwischen NetApp und VMware hervorheben. NetApp ONTAP Speichersysteme bieten bewährte Datenspiegelungstechnologien, mit denen Unternehmen Disaster Recovery-Lösungen entwickeln können, die sowohl lokale als auch ONTAP -Technologien der führenden Cloud-Anbieter umfassen.

FSx ONTAP auf AWS ist eine solche Lösung, die eine nahtlose Integration mit SnapCenter und SyncMirror zum Replizieren von Anwendungsdaten in die Cloud ermöglicht. Veeam Backup & Replication ist eine weitere bekannte Technologie, die sich gut in NetApp ONTAP Speichersysteme integrieren lässt und Failover für vSphere-nativen Speicher bereitstellen kann.

Diese Lösung stellte eine Notfallwiederherstellungslösung unter Verwendung von Gastverbindungsspeicher von einem ONTAP System dar, auf dem SQL Server- und Oracle-Anwendungsdaten gehostet werden. SnapCenter mit SnapMirror bietet eine einfach zu verwaltende Lösung zum Schutz von Anwendungsvolumes auf ONTAP -Systemen und deren Replikation auf FSx oder CVO in der Cloud. SnapCenter ist eine DR-fähige Lösung für das Failover aller Anwendungsdaten auf VMware Cloud auf AWS.