Schutz von Workloads auf AWS/VMC

NetApp Solutions

NetApp
April 26, 2024

Inhalt

Schutz von Workloads auf AWS/VMC

TR-4931: Disaster Recovery with VMware Cloud on Amazon Web Services and Guest Connect

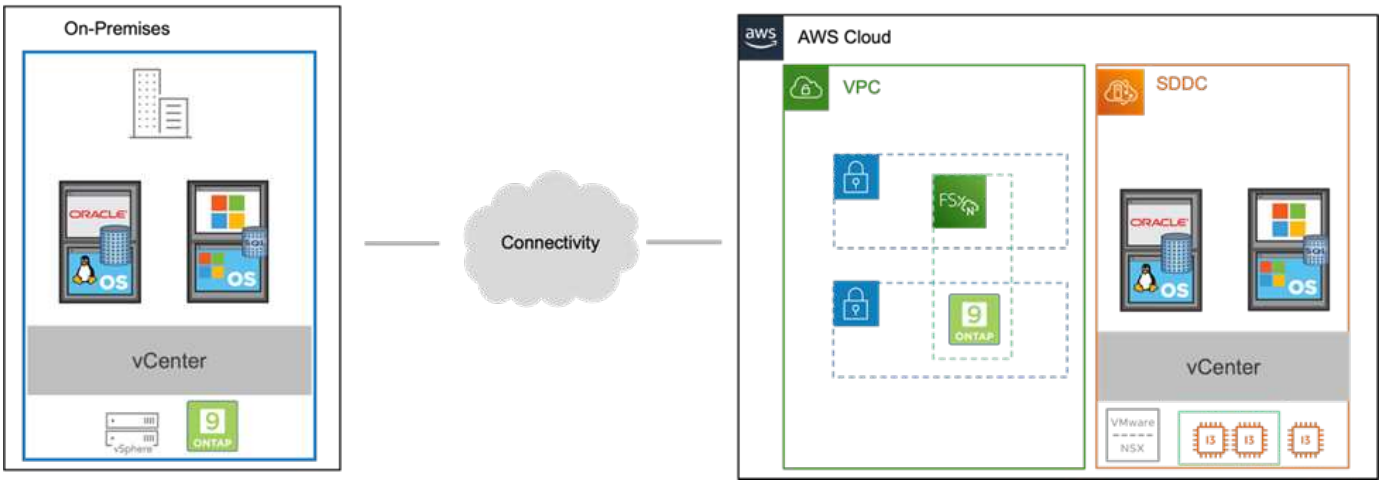
Autoren: Chris Reno, Josh Powell und Suresh ThopPay – NetApp Solutions Engineering

Überblick

Für Unternehmen ist eine bewährte Disaster Recovery-Umgebung (DR) und ein bewährter Plan unerlässlich, um sicherzustellen, dass geschäftskritische Applikationen bei einem schwerwiegenden Ausfall schnell wiederhergestellt werden können. Der Schwerpunkt dieser Lösung liegt auf der Demonstration von DR-Anwendungsfällen. Der Schwerpunkt liegt dabei auf VMware und NetApp Technologien, sowohl vor Ort als auch mit VMware Cloud auf AWS.

NetApp blickt auf langjährige Erfahrungen in der Integration mit VMware zurück. Zehntausende von Kunden haben sich für NetApp als Storage-Partner für ihre virtualisierte Umgebung entschieden. Diese Integration setzt die Optionen fort, die mit dem Gast in der Cloud verbunden sind, sowie die Integration von aktuellen NFS-Datenspeichern. Die Lösung konzentriert sich auf den Anwendungsfall, der als Gast-vernetzter Storage bezeichnet wird.

Im mit dem Gast verbundenen Storage wird die Gast-VMDK auf einem von VMware bereitgestellten Datastore bereitgestellt und die Applikationsdaten werden auf iSCSI oder NFS gespeichert und direkt der VM zugeordnet. Oracle und MS SQL Applikationen werden verwendet, um ein DR-Szenario zu demonstrieren, wie in der folgenden Abbildung dargestellt.



Annahmen, Voraussetzungen und Komponentenübersicht

Lesen Sie sich vor der Bereitstellung dieser Lösung die Übersicht über die Komponenten durch, welche Voraussetzungen für die Implementierung der Lösung und die Annahmen erfüllt sind, die bei der Dokumentation dieser Lösung zu beachten sind.

"Anforderungen FÜR DR-Lösung, Anforderungen und Planung"

DR mit SnapCenter

In dieser Lösung bietet SnapCenter applikationskonsistente Snapshots für SQL Server und Oracle Applikationsdaten. Diese Konfiguration sorgt in Kombination mit der SnapMirror Technologie für ultraschnelle Datenreplizierung zwischen unserem lokalen AFF und FSX ONTAP Cluster. Darüber hinaus bietet Veeam Backup & Replication Backup- und Restore-Funktionen für unsere Virtual Machines.

In diesem Abschnitt werden die Konfiguration von SnapCenter, SnapMirror und Veeam für Backups und auch für Restores erläutert.

In den folgenden Abschnitten werden die Konfiguration und die erforderlichen Schritte zum Abschluss eines Failover am sekundären Standort behandelt:

SnapMirror Beziehungen und Aufbewahrungszeitpläne konfigurieren

SnapCenter kann SnapMirror Beziehungen innerhalb des primären Storage-Systems (primär > Spiegel) und auf sekundäre Storage-Systeme (primär > Vault) aktualisieren, um langfristige Archivierung und Aufbewahrung zu ermöglichen. Hierfür müssen eine Datenreplizierungsbeziehung zwischen einem Ziel-Volume und einem Quell-Volume mithilfe von SnapMirror festgelegt und initialisiert werden.

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 Peering durchgeführt werden.

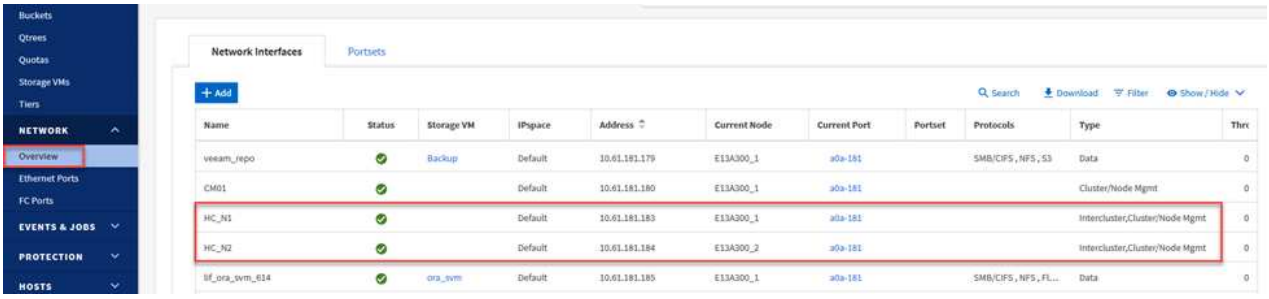
Die folgenden Schritte sind zum Einrichten von SnapMirror Beziehungen zwischen einem lokalen ONTAP System und FSX ONTAP erforderlich:

> Siehe "FSX für ONTAP – ONTAP-Benutzerhandbuch" Weitere Informationen zum Erstellen von SnapMirror Beziehungen mit FSX.

Zeichnen Sie die logischen Schnittstellen von Intercluster und Ziel auf

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

1. Wechseln Sie in ONTAP System Manager zur Seite „Netzwerkübersicht“ und rufen Sie die IP-Adressen des Typs „Intercluster“ ab, die für die Kommunikation mit der AWS VPC konfiguriert sind, bei der FSX installiert ist.



2. Um die Intercluster-IP-Adressen für FSX abzurufen, melden Sie sich in 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.
```

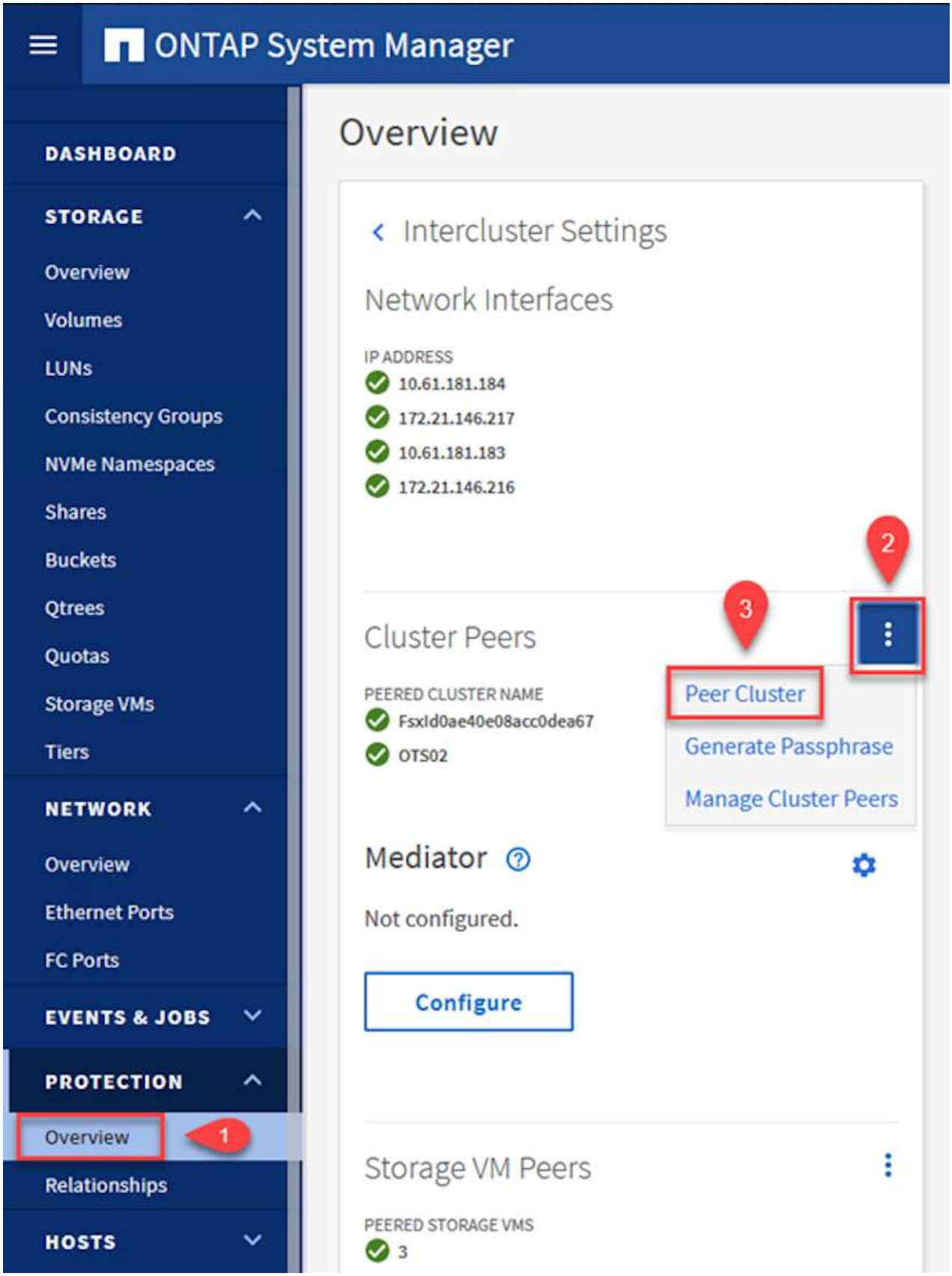
Cluster-Peering zwischen ONTAP und FSX einrichten

Zum Erstellen von Cluster-Peering zwischen ONTAP Clustern muss im anderen Peer-Cluster eine eindeutige Passphrase bestätigt werden, die beim Initiierung des ONTAP-Clusters eingegeben wurde.

1. Richten Sie mithilfe des Peering auf dem Ziel-FSX-Cluster ein `cluster peer create` Befehl. Wenn Sie dazu aufgefordert werden, geben Sie 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 Quell-Cluster können Sie die Cluster-Peer-Beziehung entweder mit ONTAP System Manager oder der CLI einrichten. Navigieren Sie im ONTAP System Manager zu Schutz > Übersicht, und wählen Sie Peer Cluster aus.

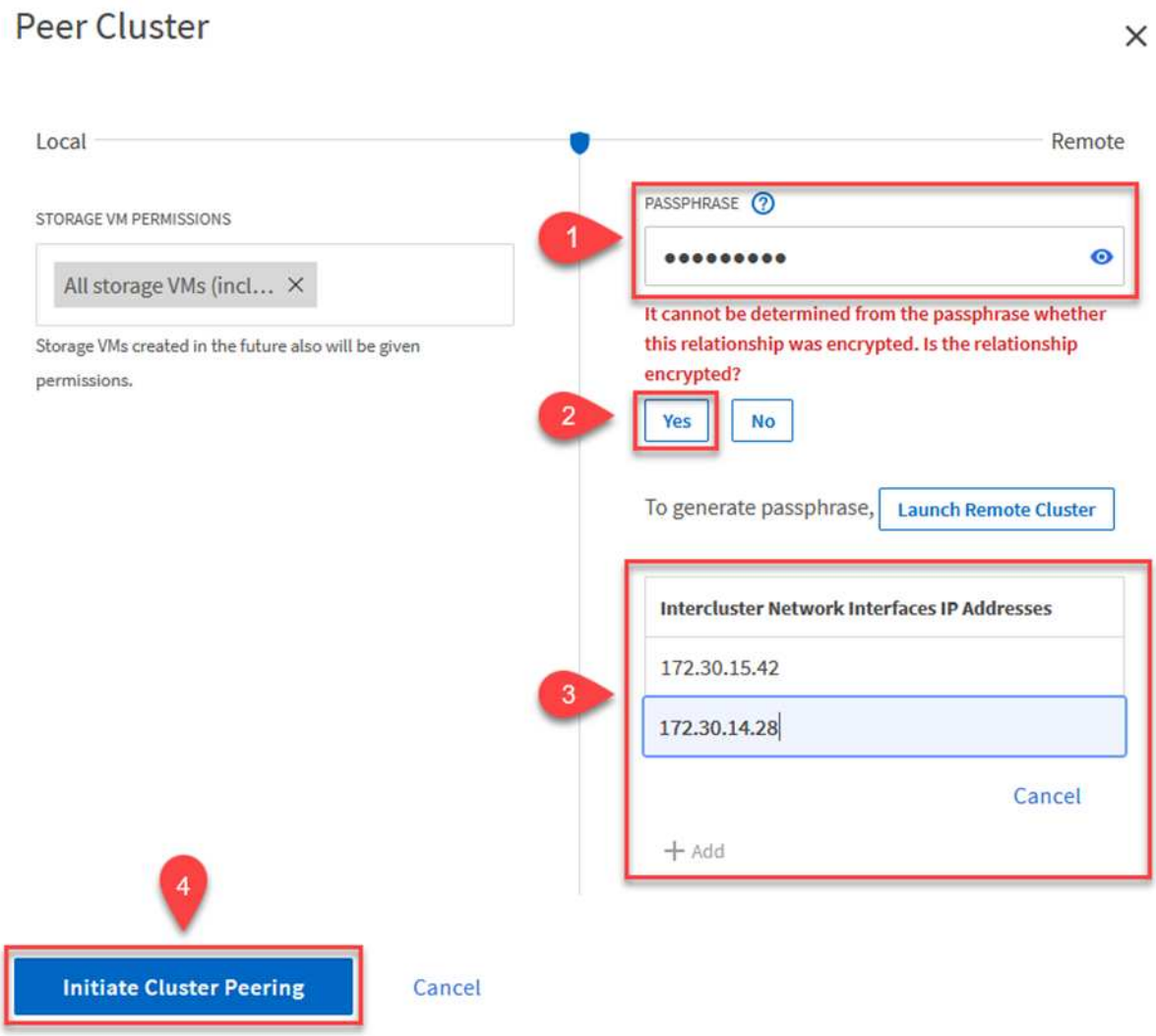


3. Füllen Sie im Dialogfeld Peer Cluster die erforderlichen Informationen aus:
   a. Geben Sie die Passphrase ein, die zum Erstellen der Peer-Cluster-Beziehung auf dem Ziel-FSX-Cluster verwendet wurde.

b. Wählen Sie `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 initiieren, um den Prozess 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
```

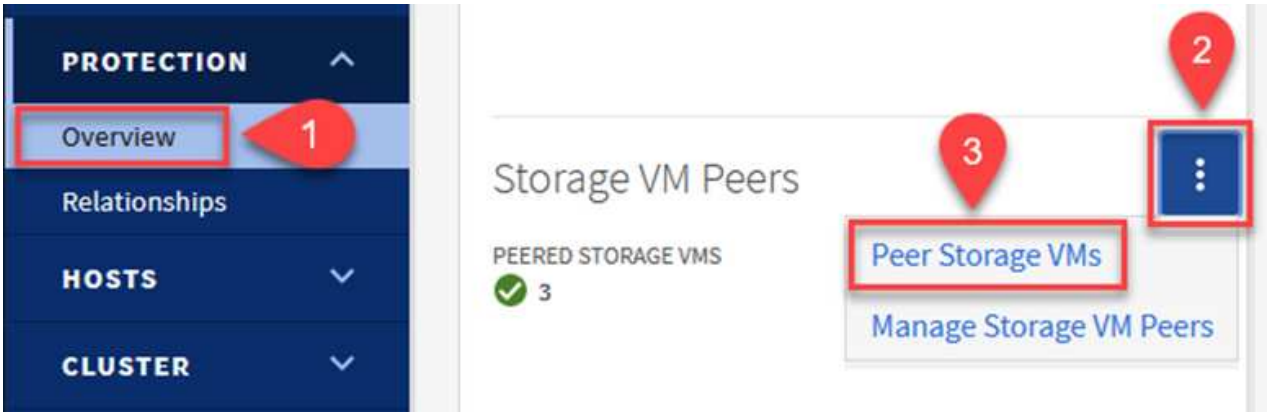
SVM-Peering-Beziehung einrichten

Im nächsten Schritt werden eine SVM-Beziehung zwischen den Ziel- und Quell-Storage Virtual Machines eingerichtet, die die Volumes enthalten, die sich in den SnapMirror Beziehungen befinden.

1. Verwenden Sie für den 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 ONTAP-Quellcluster die Peering-Beziehung entweder mit dem ONTAP System Manager oder der CLI.
3. Wählen Sie im ONTAP System Manager unter „Protection > Overview“ die Option „Peer Storage VMs“ unter „Storage VM Peers“ aus.



4. Füllen Sie im Dialogfeld Peer Storage VM die erforderlichen Felder aus:
   - Der Quell-Storage-VM
   - Dem Ziel-Cluster
   - Der Ziel-Storage-VM

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

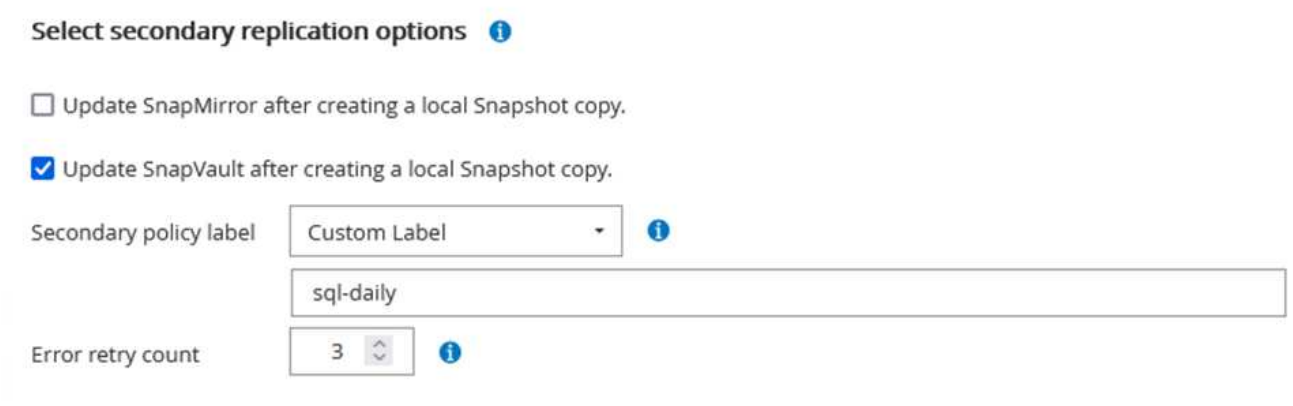
Erstellen einer Snapshot Aufbewahrungsrichtlinie

SnapCenter managt Aufbewahrungszeitpläne für Backups, die als Snapshot Kopien auf dem primären Storage-System existieren. Dies wird beim Erstellen einer Richtlinie in SnapCenter festgelegt. SnapCenter managt keine Aufbewahrungsrichtlinien für Backups, die in sekundären Storage-Systemen aufbewahrt werden. Diese Richtlinien werden separat durch eine SnapMirror Richtlinie gemanagt, die auf dem sekundären FSX-Cluster erstellt wurde und mit den Ziel-Volumes in einer SnapMirror Beziehung zum Quell-Volume verknüpft ist.

Beim Erstellen einer SnapCenter-Richtlinie haben Sie die Möglichkeit, ein sekundäres Richtlinienetikett anzugeben, das der SnapMirror-Kennzeichnung von jedem Snapshot hinzugefügt wird, der beim Erstellen eines SnapCenter-Backups generiert wird.

> Auf dem sekundären Storage werden diese Kennungen mit Richtliniensegeln abgeglichen, die mit dem Ziel-Volume verbunden sind, um die Aufbewahrung von Snapshots zu erzwingen.

Das folgende Beispiel zeigt ein SnapMirror-Etikett, das an allen Snapshots vorhanden ist, die im Rahmen einer Richtlinie erzeugt wurden, die für die täglichen Backups unserer SQL Server-Datenbank und der Protokoll-Volumes verwendet wird.



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

Sie müssen zuerst eine SnapMirror-Richtlinie mit Regeln erstellen, die die Anzahl der beizubehaltenden Snapshot-Kopien vorschreiben.

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-Labels hinzu, die zu den in den SnapCenter-Richtlinien angegebenen sekundären Richtlinienbezeichnungen passen.

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

Das folgende Skript enthält ein Beispiel für eine Regel, die einer Richtlinie hinzugefügt werden kann:

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

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

Erstellung von Ziel-Volumes

Führen Sie den folgenden Befehl auf FSX ONTAP aus, um ein Ziel-Volume auf FSX zu erstellen, das den Empfänger von Snapshot-Kopien aus unseren Quell-Volumes erhält:

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

SnapMirror Beziehungen zwischen Quell- und Ziel-Volumes erstellen

Führen Sie den folgenden Befehl auf FSX ONTAP aus, um eine SnapMirror Beziehung zwischen einem Quell- und Ziel-Volume zu erstellen:

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

SnapMirror Beziehungen initialisieren

Initialisieren Sie die SnapMirror-Beziehung. Bei diesem Prozess wird ein neuer Snapshot initiiert, der vom Quell-Volume erzeugt wird und in das Ziel-Volume kopiert.

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

Implementieren und konfigurieren Sie Windows SnapCenter Server vor Ort.

Implementieren Sie Windows SnapCenter Server vor Ort

Diese Lösung verwendet NetApp SnapCenter zur Erstellung applikationskonsistenter Backups von SQL Server und Oracle Datenbanken. Zusammen mit Veeam Backup & Replication zum Backup von VMDKs für Virtual Machines stellt dies eine umfassende Disaster-Recovery-Lösung für lokale und Cloud-basierte Datacenter bereit.

SnapCenter Software ist über die NetApp Support Site erhältlich und kann auf Microsoft Windows Systemen installiert werden, die sich entweder in einer Domäne oder Arbeitsgruppe befinden. Ein detaillierter Planungsleitfaden und Installationsanweisungen finden Sie unter "NetApp Documentation Center".

Die SnapCenter-Software ist erhältlich unter "Dieser Link".

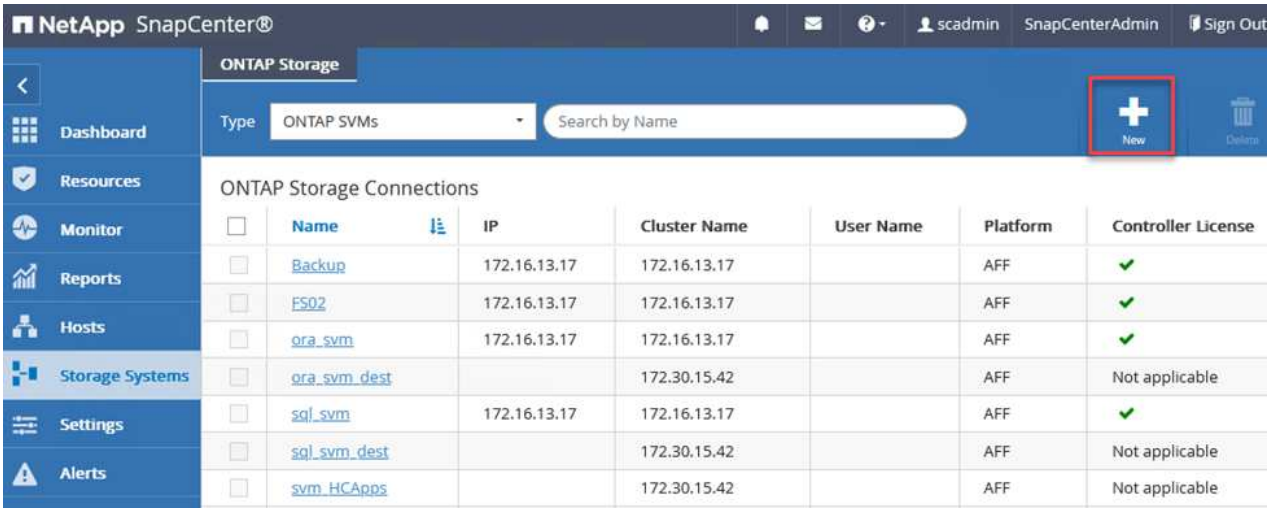
Nach der Installation können Sie über einen Webbrowser mit *https://Virtual_Cluster_IP_or_FQDN:8146* auf die SnapCenter Konsole zugreifen.

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

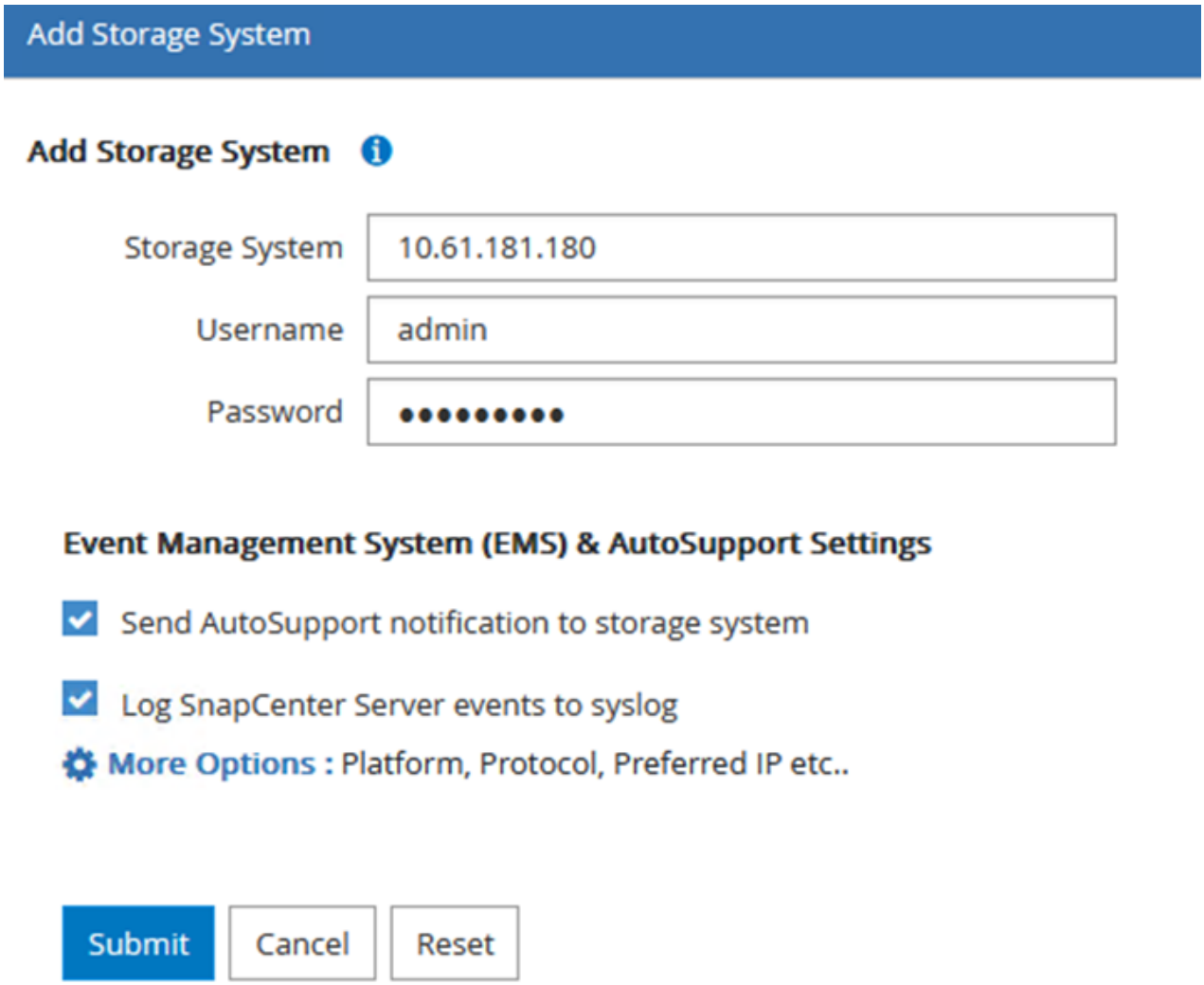
Hinzufügen von Storage-Controllern zu SnapCenter

Gehen Sie wie folgt vor, um SnapCenter Storage-Controller hinzuzufügen:

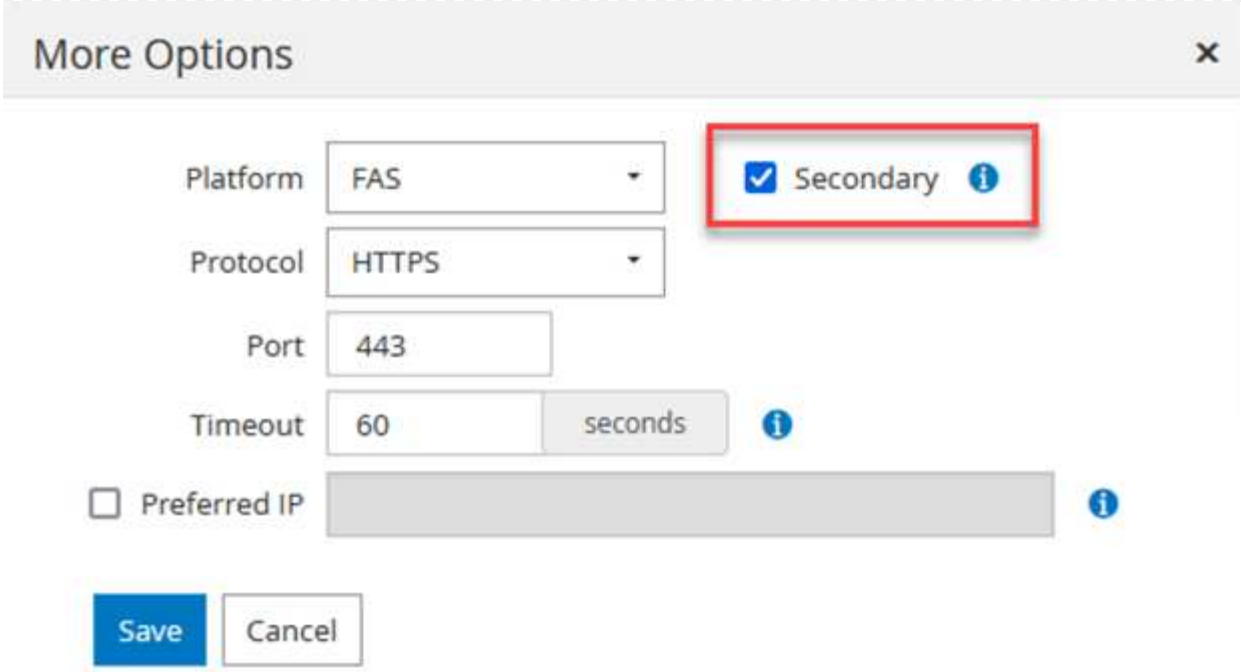
1. Wählen Sie im linken Menü Storage Systems aus und klicken Sie dann auf Neu, um mit dem Hinzufügen Ihrer Storage Controller zu SnapCenter zu beginnen.



2. Fügen Sie im Dialogfeld Add Storage System die Management-IP-Adresse für den lokalen ONTAP-Cluster sowie den Benutzernamen und das Passwort hinzu. Klicken Sie dann auf Senden, um die Erkennung des Speichersystems zu starten.



3. Wiederholen Sie diesen Vorgang, um dem SnapCenter das FSX ONTAP-System hinzuzufügen. Wählen Sie in diesem Fall unten im Fenster „Add Storage System“ die Option „More Options“ (Weitere Optionen) aus und klicken Sie auf das Kontrollkästchen für „Secondary“ (sekundär), um das FSX-System als sekundäres Storage-System zu bezeichnen, das mit SnapMirror Kopien oder unseren primären Backup Snapshots aktualisiert wird.

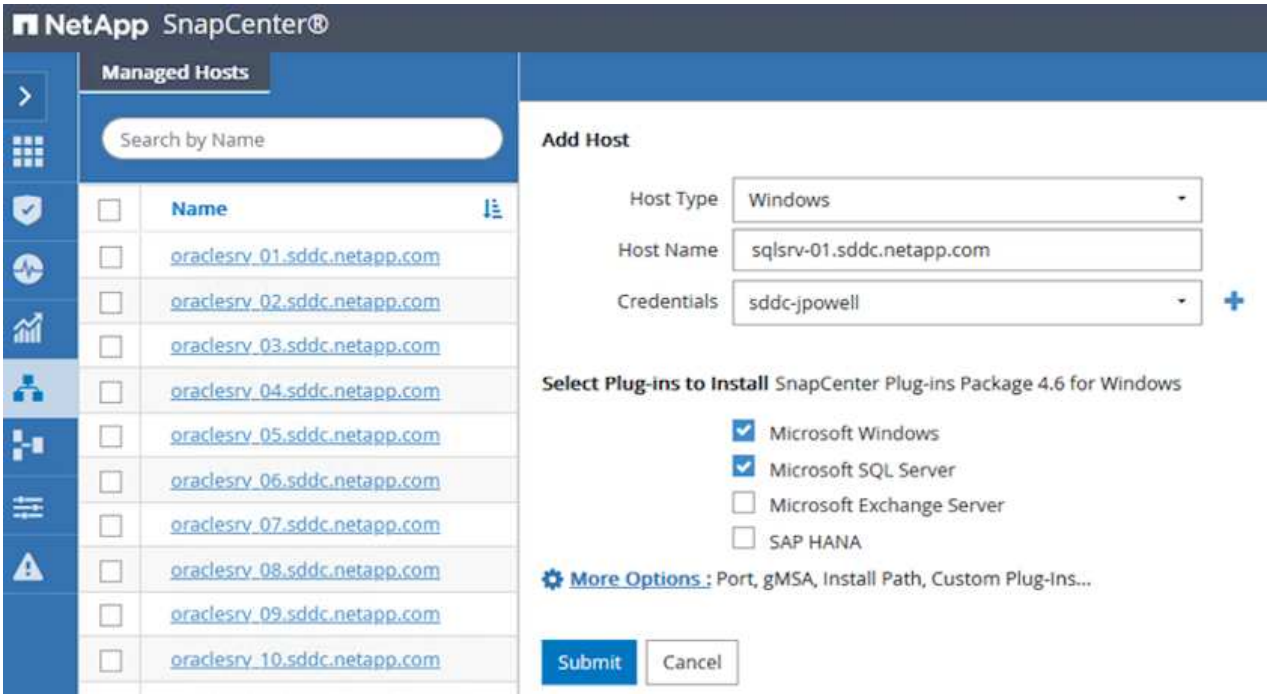


Weitere Informationen zum Hinzufügen von Storage-Systemen zum SnapCenter finden Sie in der Dokumentation unter "Dieser Link".

Fügen Sie Hosts zum SnapCenter hinzu

Der nächste Schritt ist das Hinzufügen von Host-Applikations-Servern zu SnapCenter. Der Prozess ist sowohl für SQL Server als auch für Oracle ähnlich.

1. Wählen Sie im linken Menü Hosts aus und klicken Sie dann auf Hinzufügen, um mit dem Hinzufügen von Speicher-Controllern zu SnapCenter zu beginnen.
2. Fügen Sie im Fenster Hosts hinzufügen den Host-Typ, den Hostnamen und die Anmeldedaten des Host-Systems hinzu. Wählen Sie den Plug-in-Typ aus. Wählen Sie für SQL Server das Plug-in für 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 Database Plug-in. Klicken Sie dann auf Senden, um den Erkennungsvorgang 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

- [x] Oracle Database
- [ ] SAP HANA

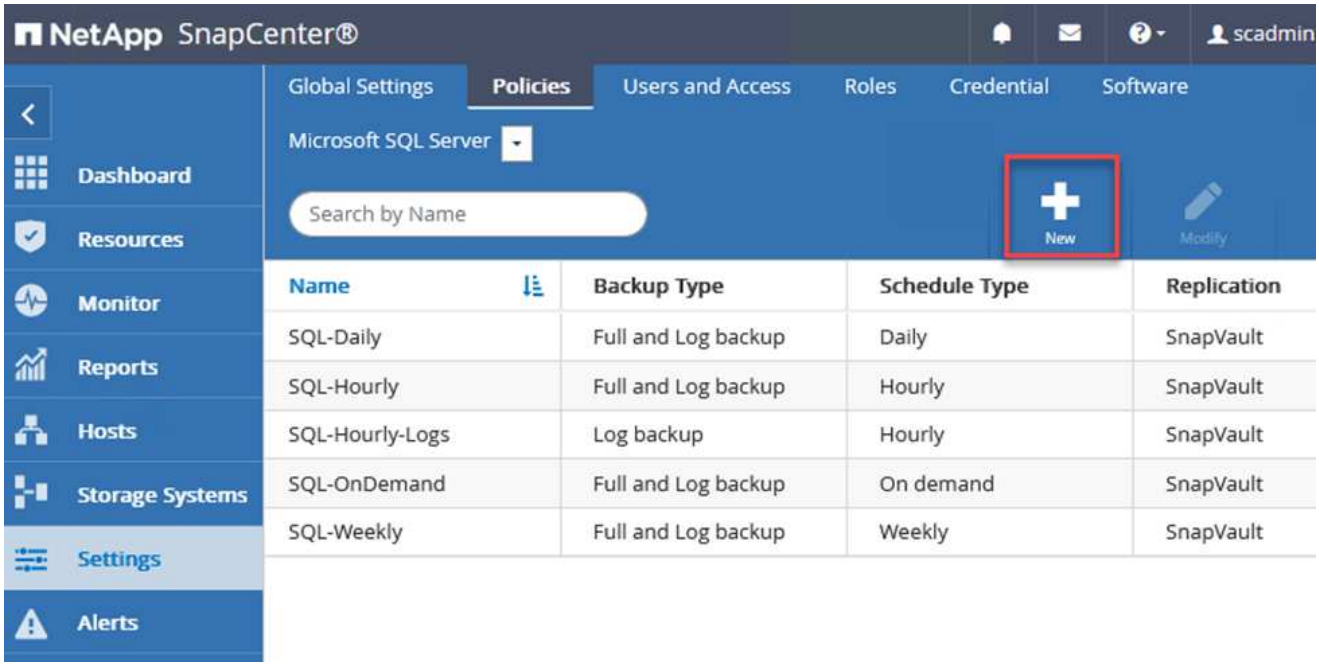
More Options : Port, Install Path, Custom Plug-Ins...

Submit Cancel

SnapCenter-Richtlinien erstellen

Richtlinien legen die spezifischen Regeln fest, die für einen Backup-Job zu beachten sind. Dazu gehören u. a. der Backup-Zeitplan, der Replizierungstyp und die Handhabung von SnapCenter für Backup und Verkürzung der Transaktions-Logs.

Sie können auf die Richtlinien im Abschnitt Einstellungen des SnapCenter-Webclients zugreifen.



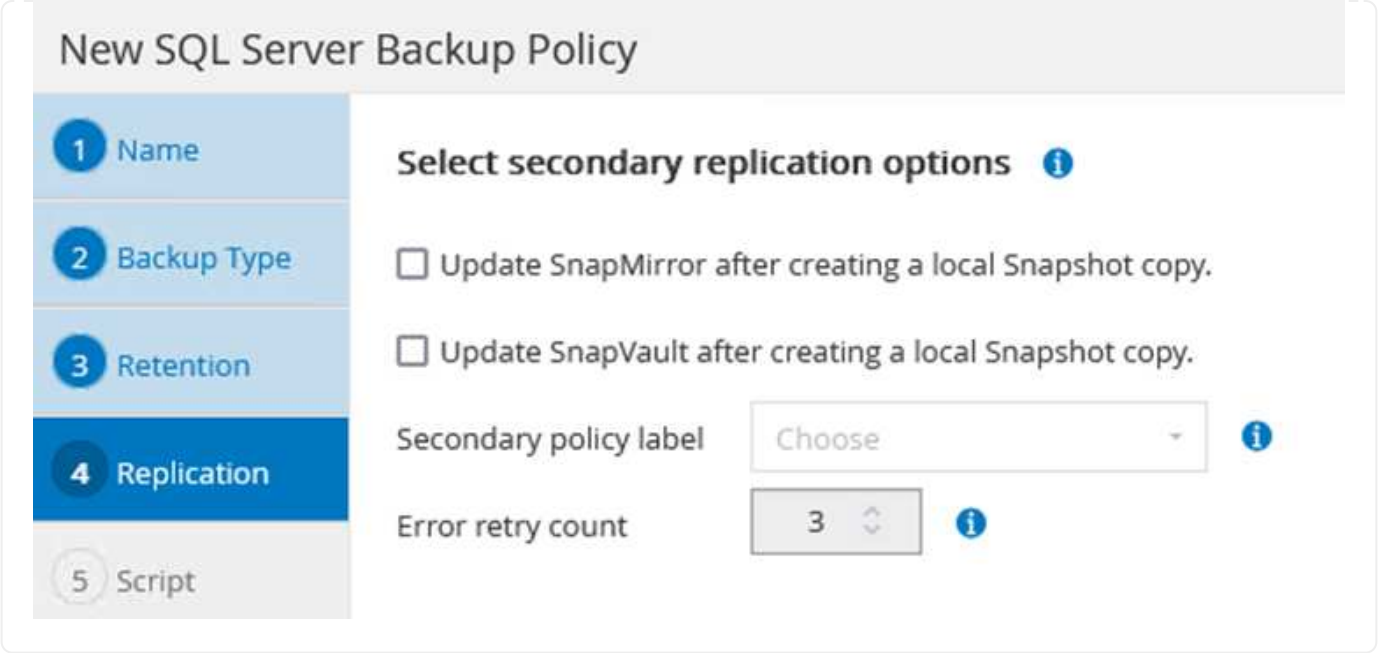
Vollständige Informationen zum Erstellen von Richtlinien für SQL Server-Backups finden Sie im "SnapCenter-Dokumentation".

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

Hinweise:

- Wenn Sie den Assistenten zur Erstellung von Richtlinien durchlaufen, beachten Sie den Abschnitt „Replikation“ besonders. In diesem Abschnitt werden die Arten von sekundären SnapMirror Kopien festgelegt, die während des Backup-Prozesses erstellt werden sollen.
- Die Einstellung „SnapMirror aktualisieren nach dem Erstellen einer lokalen Snapshot Kopie“ bezieht sich auf die Aktualisierung einer SnapMirror Beziehung, wenn diese Beziehung zwischen zwei Storage Virtual Machines besteht, die sich auf dem gleichen Cluster befinden.
- Die Einstellung „SnapVault aktualisieren nach Erstellen einer lokalen Snapshot Kopie“ wird verwendet, um eine SnapMirror Beziehung zu aktualisieren, die zwischen zwei separaten Clustern und zwischen einem On-Premises ONTAP System und Cloud Volumes ONTAP oder FSxN besteht.

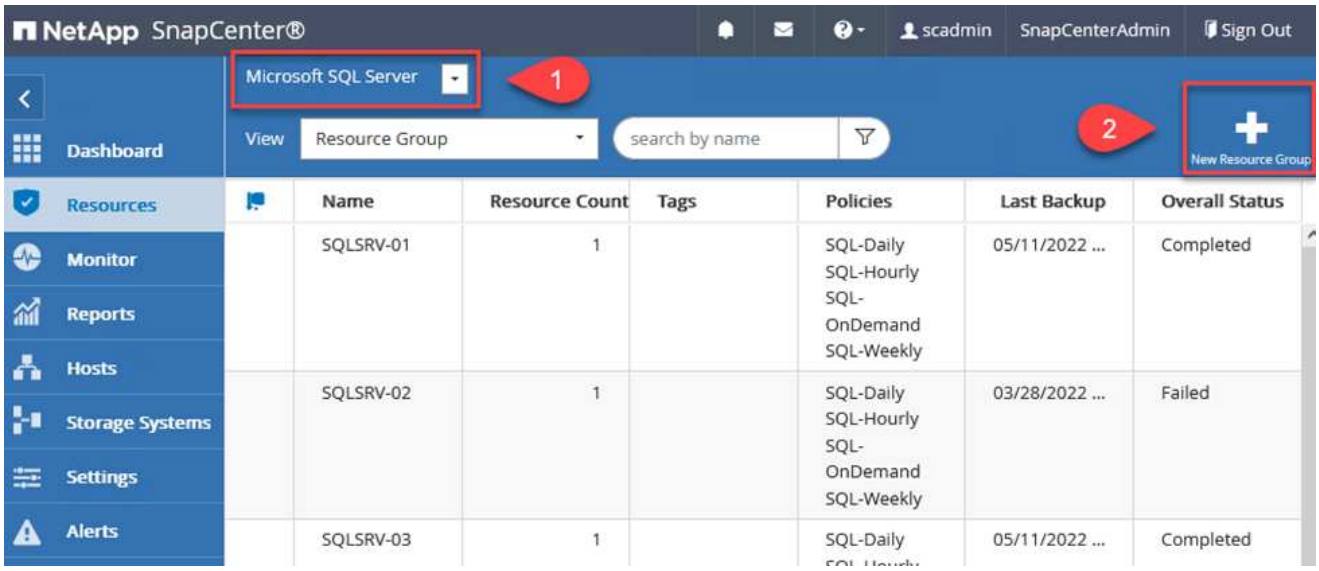
Die folgende Abbildung zeigt die vorhergehenden Optionen und deren Aussehen im Backup Policy Wizard.



Erstellen Sie SnapCenter-Ressourcengruppen

Mit Ressourcengruppen können Sie die Datenbankressourcen auswählen, die Sie in Ihre Backups aufnehmen möchten, und die Richtlinien für diese Ressourcen.

1. Wechseln 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 umfasst Schritt-für-Schritt-Details zum Erstellen von Ressourcengruppen für SQL Server und Oracle-Datenbanken.

Folgen Sie zum Backup von SQL-Ressourcen "Dieser Link".

Folgen Sie zum Backup von Oracle Ressourcen "Dieser Link".

Bereitstellung und Konfiguration von Veeam Backup Server

Veeam Backup & Replication Software verwendet in dieser Lösung das Backup unserer Virtual Machines für Applikationen und die Archivierung einer Kopie der Backups in einem Amazon S3 Bucket mithilfe eines Veeam Scale-Out-Backup-Repositorys (SOBR). Veeam wird auf einem Windows-Server in dieser Lösung implementiert. Eine Anleitung zur Implementierung von Veeam finden Sie im "Technische Dokumentation des Veeam Help Center".

Veeam Scale-out-Backup-Repository konfigurieren

Nachdem Sie die Software implementiert und lizenziert haben, können Sie ein Scale-out Backup Repository (SOBR) als Ziel-Storage für Backup-Jobs erstellen. Außerdem sollten Sie einen S3-Bucket als Backup von VM-Daten für die Disaster Recovery extern berücksichtigen.

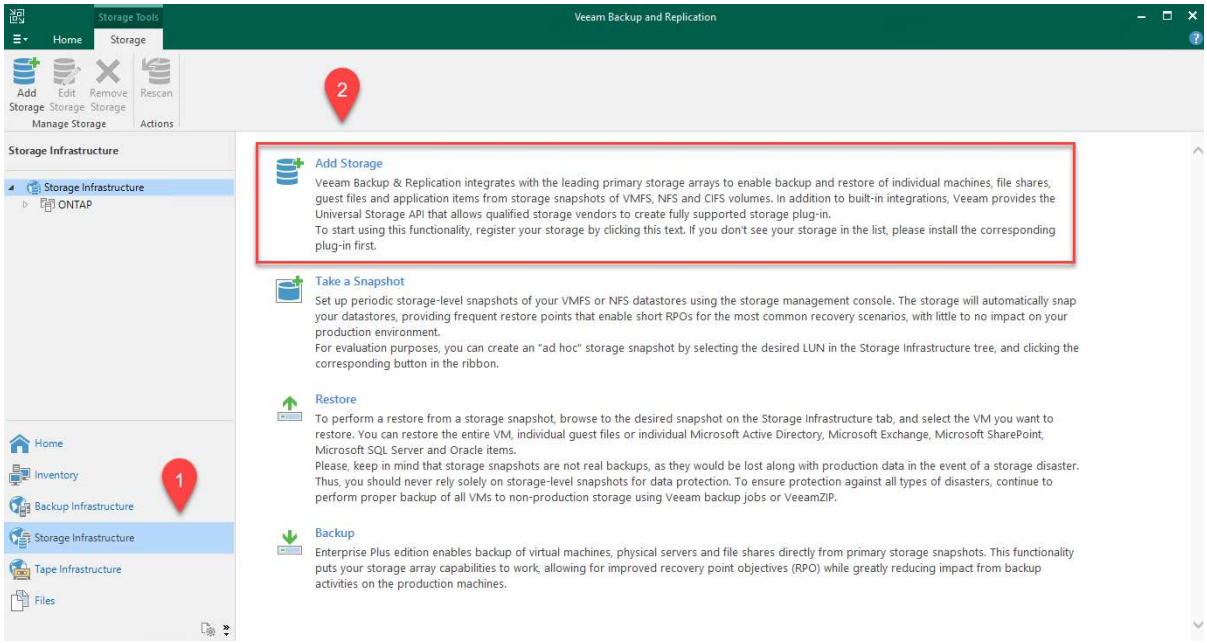
Lesen Sie die folgenden Voraussetzungen, bevor Sie beginnen.

1. Erstellen einer SMB-Dateifreigabe auf Ihrem lokalen ONTAP System als Ziel-Storage für Backups
2. Erstellen eines Amazon S3-Buckets, der in den SOBR aufgenommen werden soll Es handelt sich um ein Repository für die externen Backups.

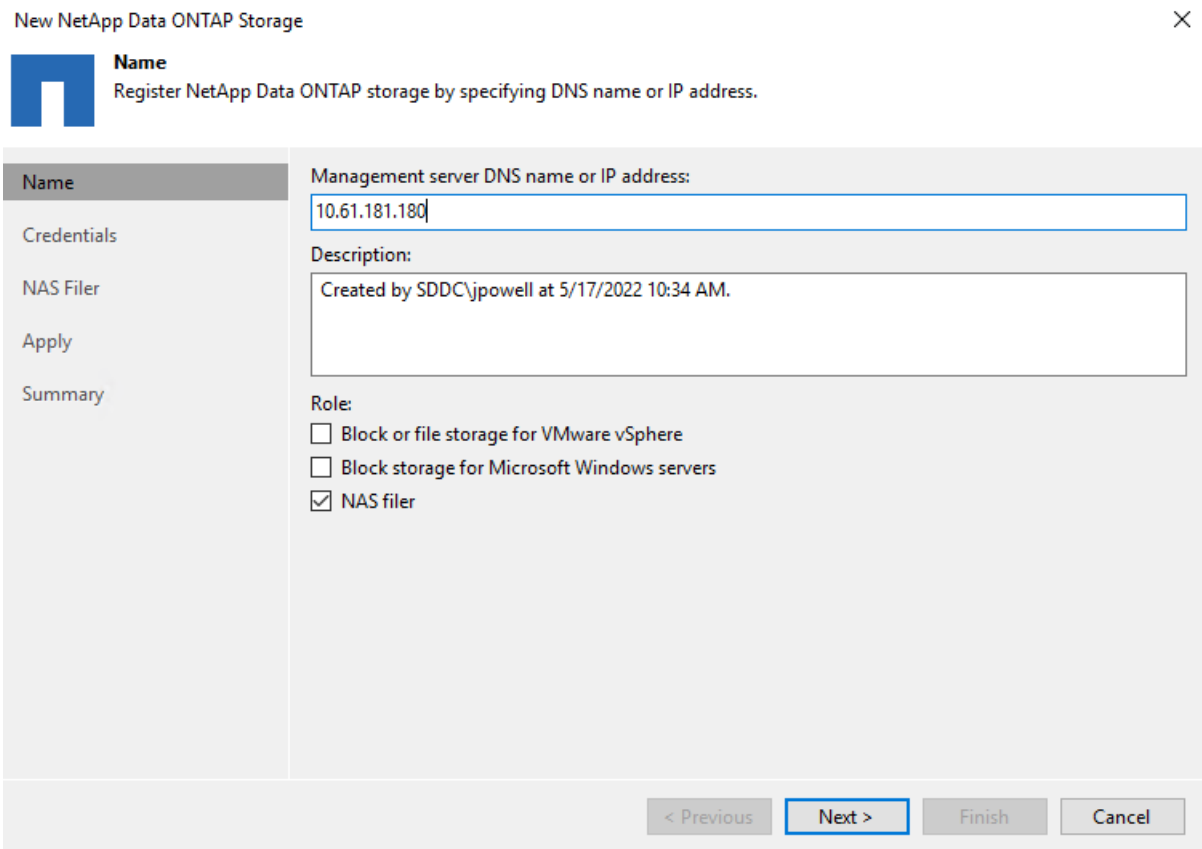
Fügen Sie ONTAP Storage zu Veeam hinzu

Zunächst fügen Sie den ONTAP Storage-Cluster und das zugehörige SMB/NFS-Dateisystem als Storage-Infrastruktur in Veeam hinzu.

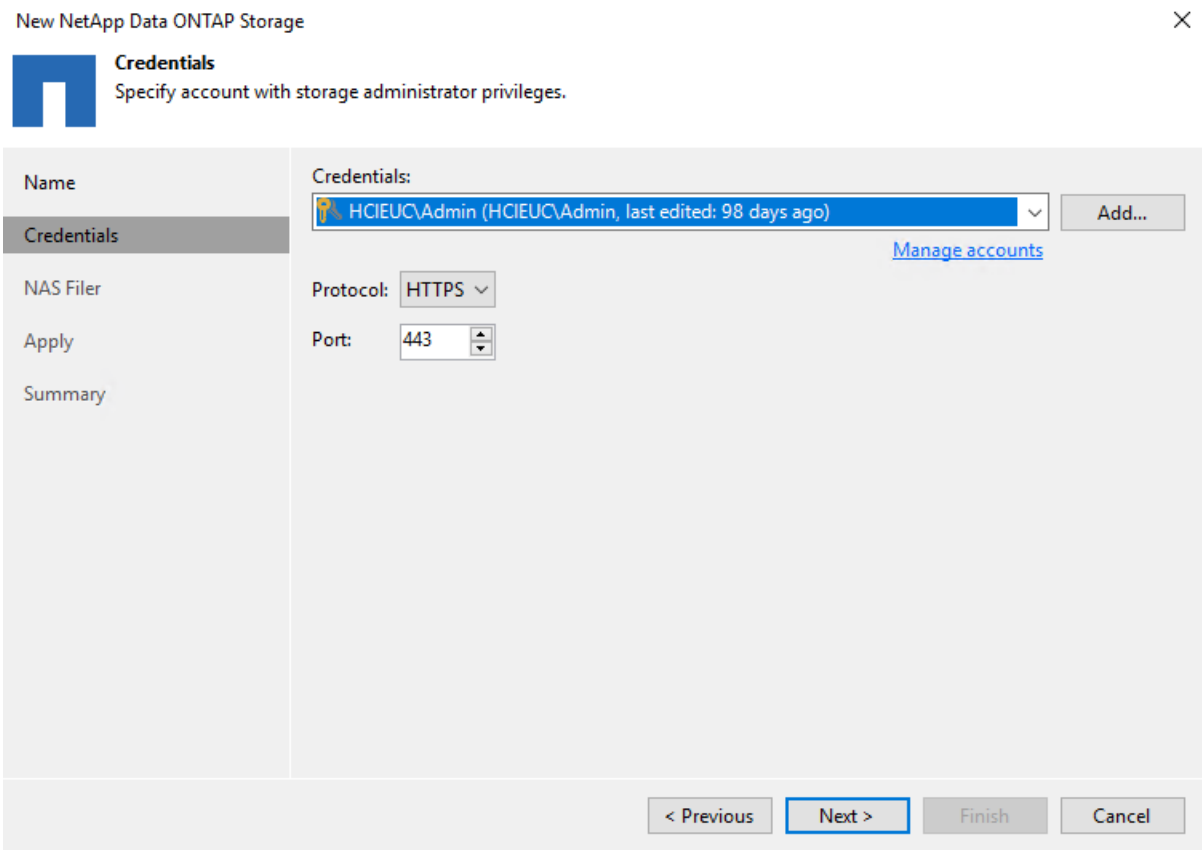
1. Öffnen Sie die Veeam-Konsole, und melden Sie sich an. Navigieren Sie zu Storage Infrastructure, und wählen Sie Add Storage aus.



2. Wählen Sie im Assistenten zum Hinzufügen von Storage NetApp als Storage-Anbieter aus, und wählen Sie dann Data ONTAP aus.
3. Geben Sie die Management-IP-Adresse ein und aktivieren Sie das Kontrollkästchen NAS-Filer. Klicken Sie Auf Weiter.

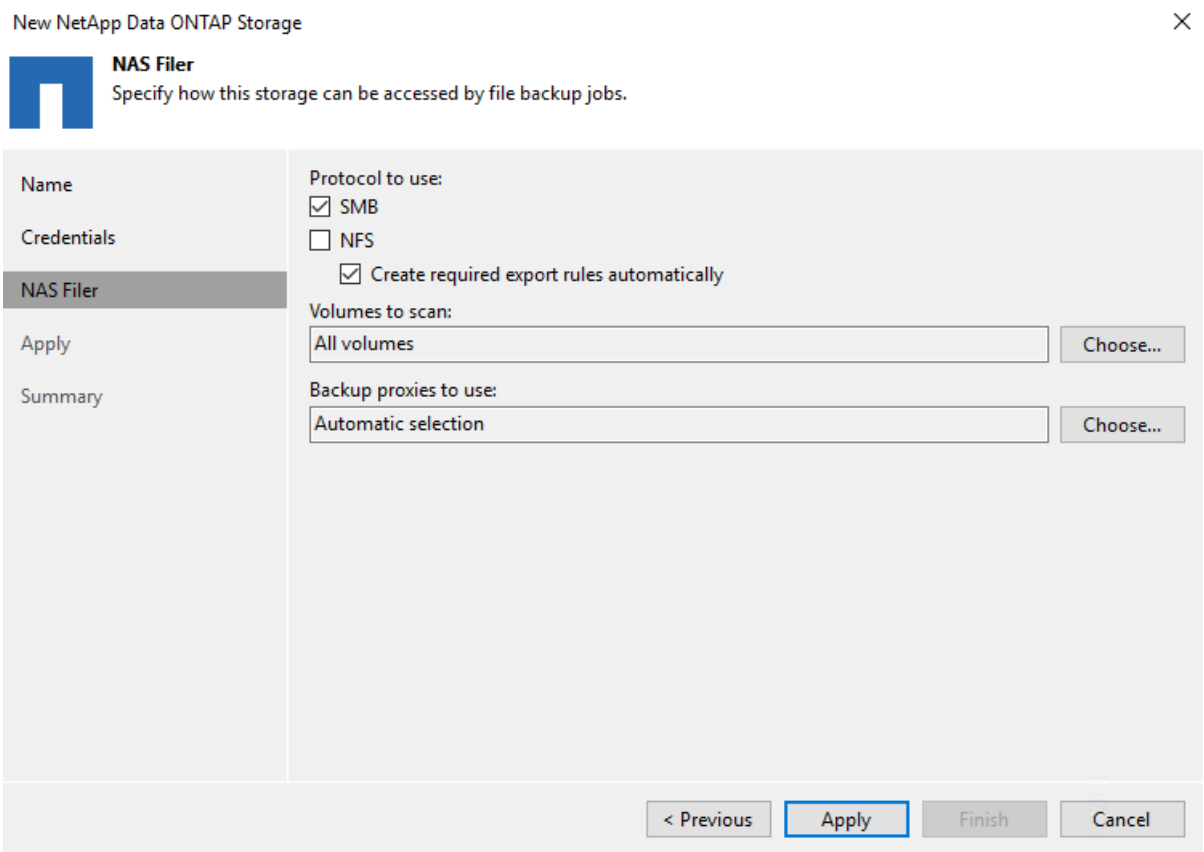


4. Fügen Sie Ihre Zugangsdaten ein, um auf das ONTAP Cluster zuzugreifen.

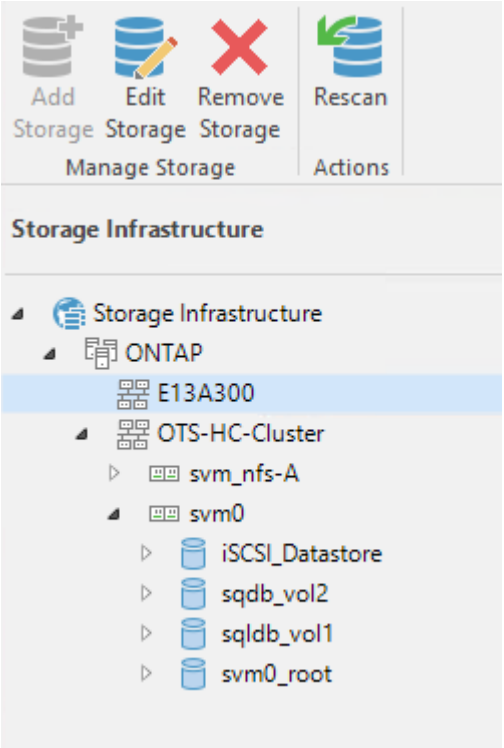


5. Wählen Sie auf der Seite NAS Filer die gewünschten Protokolle zum Scannen aus und wählen

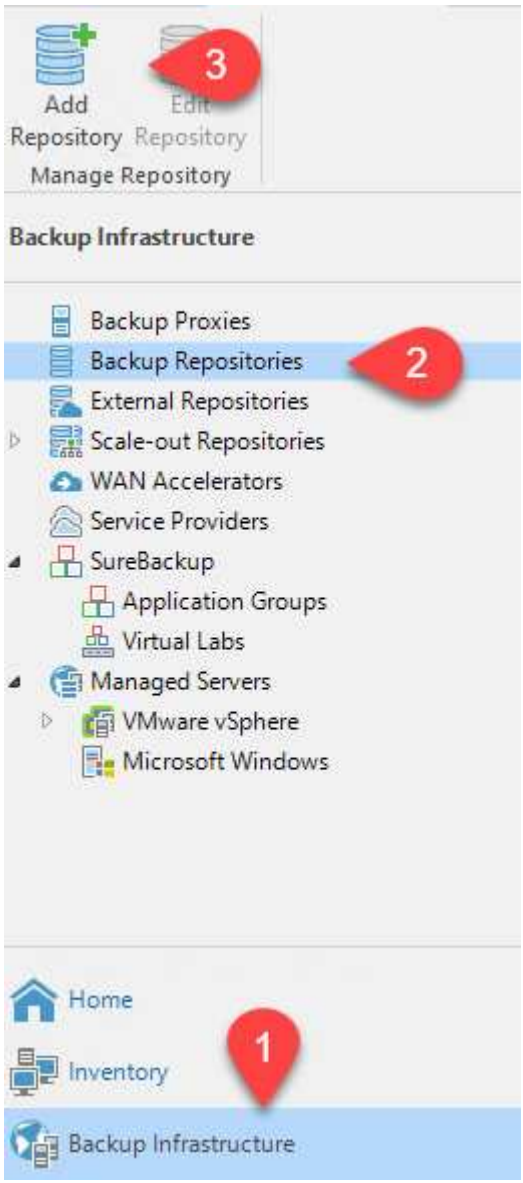
Sie Weiter.



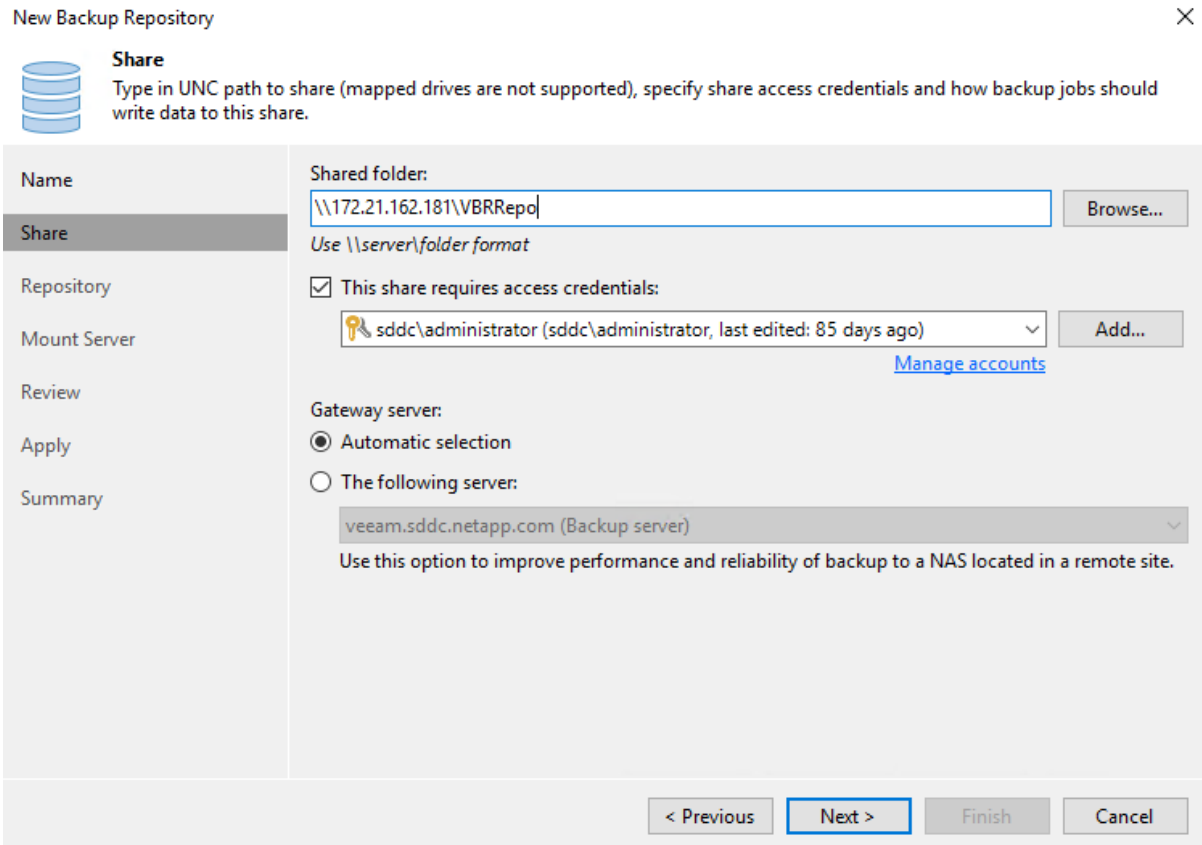
6. Schließen Sie die Seiten „Übernehmen“ und „Zusammenfassung“ des Assistenten ab, und klicken Sie auf „Fertig stellen“, um den Speicherermittlungsprozess zu starten. Nach Abschluss des Scans wird das ONTAP-Cluster zusammen mit den NAS-Filern als verfügbare Ressourcen hinzugefügt.



7. Erstellen Sie ein Backup-Repository mithilfe der neu erkannten NAS-Freigaben. Wählen Sie in Backup Infrastructure die Option Backup Repositories aus, und klicken Sie auf das Menüelement Add Repository.



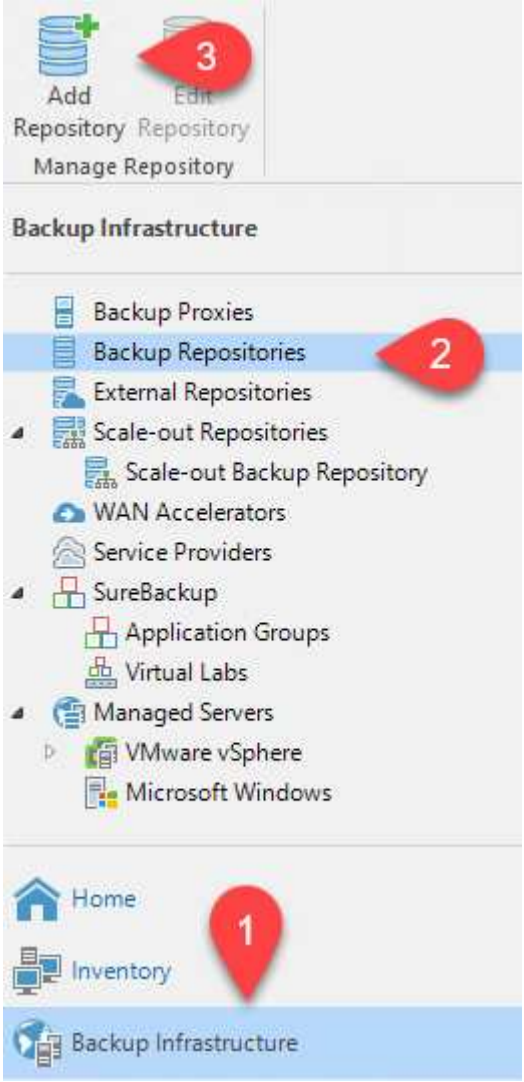
8. Führen Sie alle Schritte im Assistenten für das Neue Backup-Repository aus, um das Repository zu erstellen. Detaillierte Informationen zum Erstellen von Veeam Backup Repositorys finden Sie im "Veeam-Dokumentation".


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

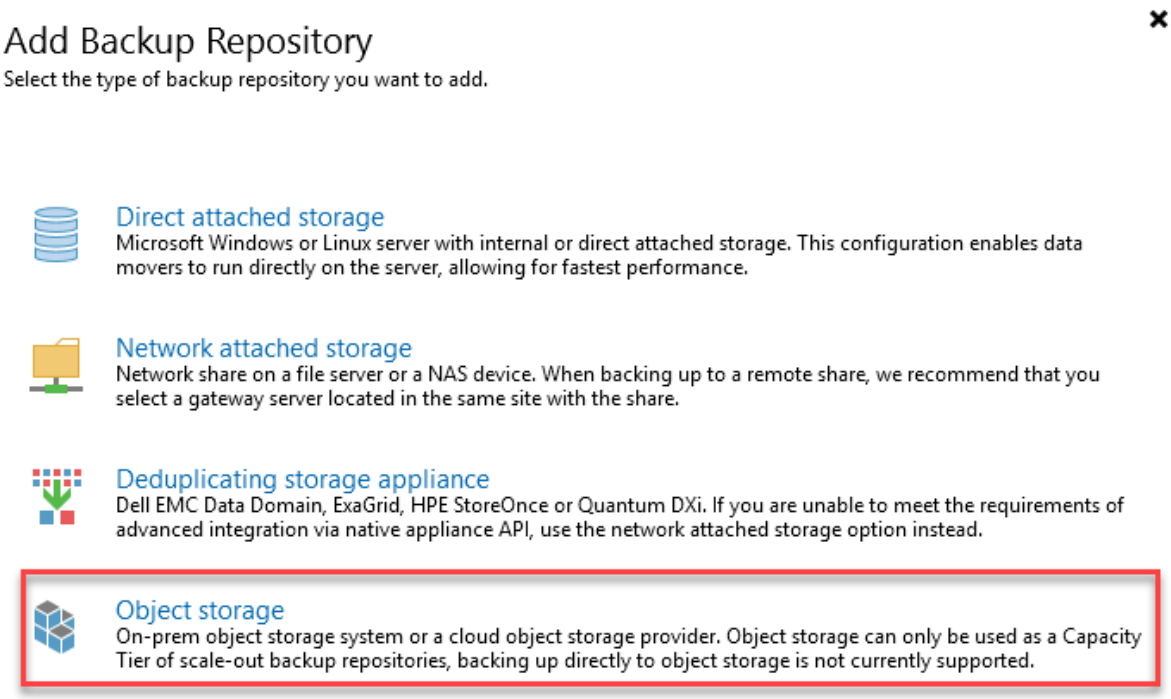
Fügen Sie den Amazon S3-Bucket als Backup-Repository hinzu

Im nächsten Schritt wird der Amazon S3-Storage als Backup-Repository hinzugefügt.

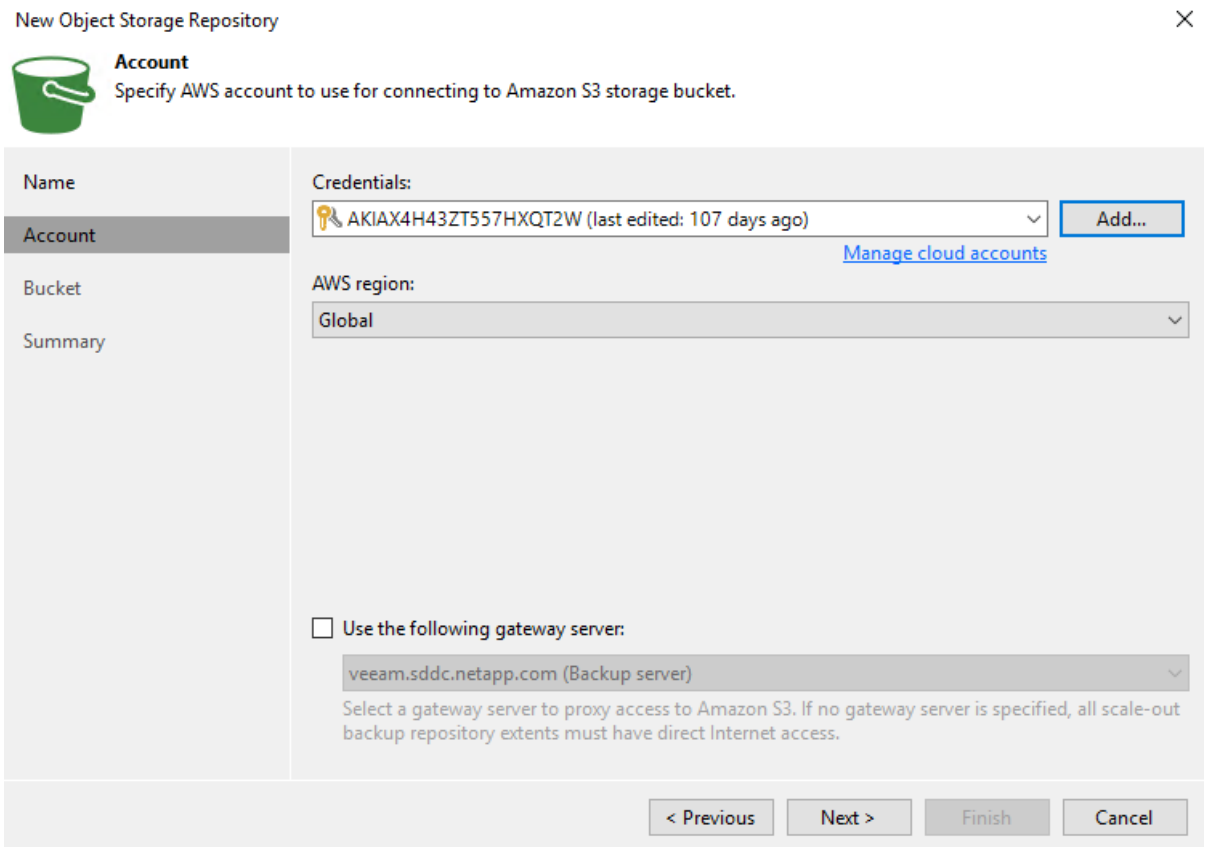
1. Navigieren Sie zu Backup Infrastructure > Backup Repositorys. Klicken Sie Auf Repository Hinzufügen.



2. Wählen Sie im Assistenten zum Hinzufügen von Backup-Repositorys Objekt-Storage und anschließend Amazon S3 aus. Daraufhin wird der Assistent für das Neue Objekt-Speicher-Repository gestartet.



3. Geben Sie einen Namen für das Objekt-Storage-Repository an, und klicken Sie auf Weiter.
4. Geben Sie im nächsten Abschnitt Ihre Anmeldedaten ein. Sie benötigen einen AWS-Zugriffsschlüssel und einen geheimen Schlüssel.

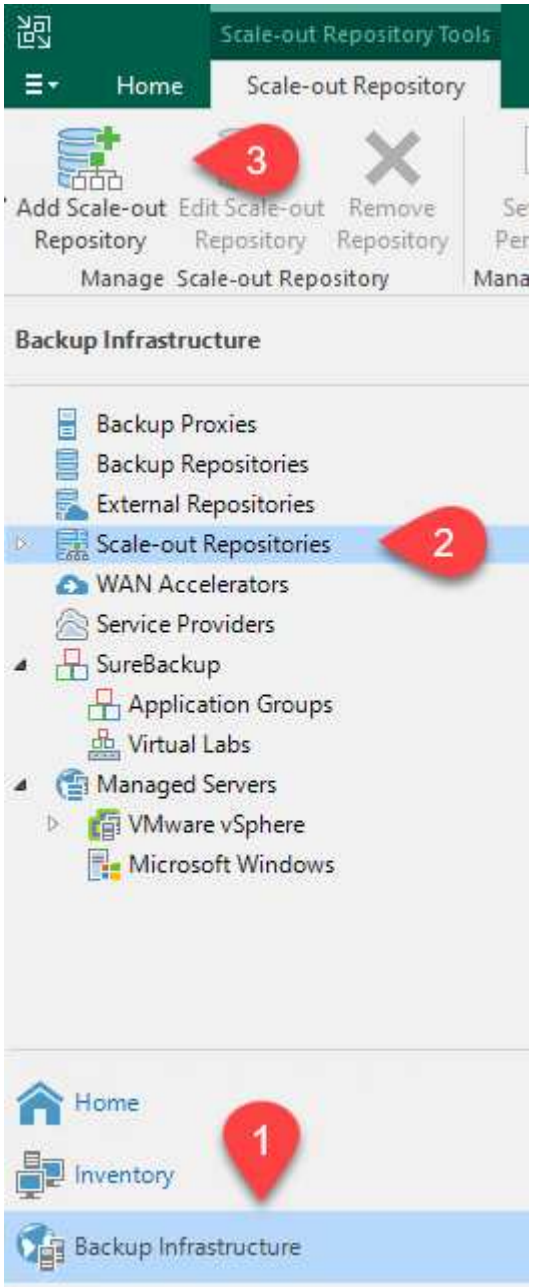


5. Wählen Sie nach dem Laden der Amazon Konfiguration Ihr Datacenter, Ihren Bucket und den Ordner aus und klicken Sie auf Anwenden. Klicken Sie abschließend auf Fertig stellen, um den Assistenten zu schließen.

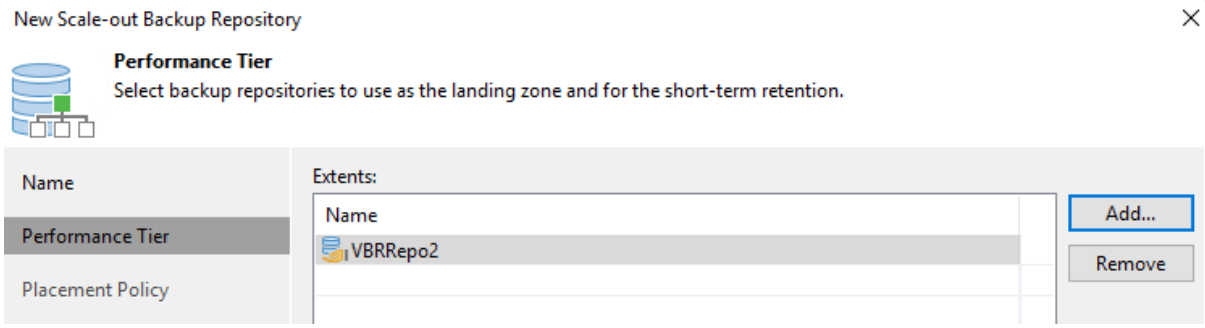
Scale-out-Backup-Repository erstellen

Nachdem wir jetzt unsere Storage Repositorys zu Veeam hinzugefügt haben, können wir das SOBR erstellen, um Backup-Kopien automatisch in unseren externen Amazon S3 Objekt-Storage zu Disaster Recovery-Zwecken zu verschieben.

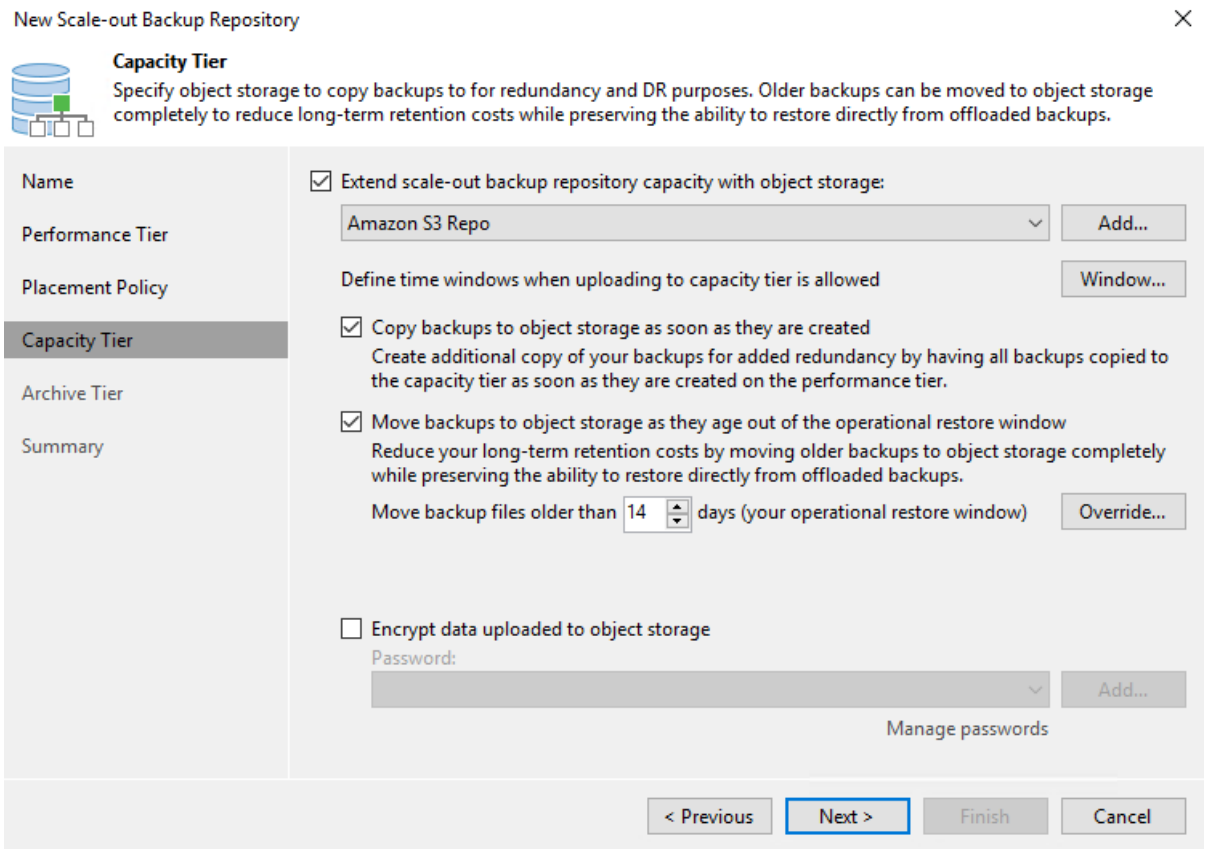
1. Wählen Sie in Backup Infrastructure die Option Scale-Out Repositorys aus, und klicken Sie dann auf das Menüelement Scale-Out Repository hinzufügen.



2. Geben Sie im neuen Scale-Out Backup Repository einen Namen für den SOBR ein, und klicken Sie auf Weiter.
3. Wählen Sie für die Performance-Ebene das Backup-Repository mit der SMB-Freigabe in Ihrem lokalen ONTAP Cluster aus.



4. Wählen Sie für die Richtlinie zur Platzierung entweder Data Locality oder Performance basierend auf Ihren Anforderungen aus. Wählen Sie weiter.
5. Für Kapazitäts-Tiers erweitern wir den SOBR auf Amazon S3 Objekt-Storage. Für Disaster Recovery wählen Sie „Copy Backups to Object Storage“, sobald sie erstellt werden, um unsere sekundären Backups rechtzeitig bereitzustellen.



6. Wählen Sie schließlich Übernehmen und Beenden, um die Erstellung des SOBR abzuschließen.

Erstellen Sie die Scale-out-Backup-Repository-Jobs

Der letzte Schritt zur Konfiguration von Veeam ist die Erstellung von Backup-Jobs anhand des neu erstellten SOBR als Backup-Ziel. Das Erstellen von Backupjobs ist ein normaler Teil des Repertoires eines Speicheradministrators und wir decken die einzelnen Schritte hier nicht ab. Nähere Informationen zum Erstellen von Backup-Jobs in Veeam finden Sie auf der "Technische Dokumentation Des Veeam Help Center".

BlueXP Backup- und Recovery-Tools sowie -Konfiguration

Um ein Failover von Applikations-VMs und Datenbank-Volumes auf VMware Cloud Volume-Services durchzuführen, die in AWS ausgeführt werden, müssen Sie eine laufende Instanz von SnapCenter Server sowie Veeam Backup and Replication Server installieren und konfigurieren. Nach Abschluss des Failover müssen diese Tools auch so konfiguriert werden, dass sie den normalen Backup-Betrieb fortsetzen, bis ein Failback zum lokalen Datacenter geplant und ausgeführt wird.

Implementieren Sie sekundären Windows SnapCenter Server

SnapCenter Server wird im VMware Cloud SDDC implementiert oder auf einer EC2 Instanz in einer VPC mit Netzwerkkonnektivität für die VMware Cloud-Umgebung installiert.

SnapCenter Software ist über die NetApp Support Site erhältlich und kann auf Microsoft Windows Systemen installiert werden, die sich entweder in einer Domäne oder Arbeitsgruppe befinden. Ein detaillierter Planungsleitfaden und Installationsanweisungen finden Sie unter "NetApp Dokumentationszentrum".

Die Software von SnapCenter finden Sie unter "Dieser Link".

Konfigurieren Sie den sekundären Windows SnapCenter-Server

Zur Wiederherstellung der Applikationsdaten, die auf FSX ONTAP gespiegelt werden, müssen Sie zuerst eine vollständige Wiederherstellung der lokalen SnapCenter-Datenbank durchführen. Nach Abschluss dieses Prozesses wird die Kommunikation mit den VMs wieder hergestellt, und Backups von Applikationen können nun mithilfe von FSX ONTAP als Primär-Storage wieder aufgenommen werden.

Dazu müssen Sie die folgenden Elemente auf dem SnapCenter-Server ausführen:

1. Konfigurieren Sie den Computernamen so, dass er mit dem ursprünglichen lokalen SnapCenter-Server identisch ist.
2. Konfigurieren Sie das Networking für die Kommunikation mit VMware Cloud und der FSX ONTAP-Instanz.
3. Führen Sie das Verfahren aus, um die SnapCenter-Datenbank wiederherzustellen.
4. Vergewissern Sie sich, dass sich SnapCenter im Disaster Recovery-Modus befindet, um sicherzustellen, dass FSX jetzt der primäre Storage für Backups ist.
5. Vergewissern Sie sich, dass die Kommunikation mit den wiederhergestellten virtuellen Maschinen wiederhergestellt wird.

Weitere Informationen zum Durchführen dieser Schritte finden Sie im Abschnitt "SnapCenter Datenbankwiederherstellungsvorgang".

Bereitstellung eines sekundären Veeam Backup & Amp; Replication Servers

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

Konfigurieren Sie den sekundären Veeam Backup & Replication Server

Zum Wiederherstellen von Virtual Machines, die auf Amazon S3 Storage gesichert wurden, müssen Sie den Veeam Server auf einem Windows Server installieren und für die Kommunikation mit VMware Cloud, FSX ONTAP und dem S3-Bucket konfigurieren, der das ursprüngliche Backup-Repository enthält. Außerdem muss auf FSX ONTAP ein neues Backup Repository konfiguriert werden, um nach der Wiederherstellung neue Backups der VMs durchzuführen.

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

1. Konfigurieren Sie das Networking für die Kommunikation mit VMware Cloud, FSX ONTAP und dem S3 Bucket mit dem ursprünglichen Backup-Repository.
2. Konfigurieren Sie eine SMB-Freigabe auf FSX ONTAP als neues Backup Repository.
3. Binden Sie den ursprünglichen S3-Bucket ein, der als Teil des Scale-out-Backup-Repositorys vor Ort verwendet wurde.
4. Nach dem Restore der VM neue Backup-Jobs zum Schutz von SQL und Oracle VMs einrichten.

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

Backup von SnapCenter Datenbanken für Disaster Recovery

SnapCenter ermöglicht das Backup und Recovery seiner zugrunde liegenden MySQL Datenbank und Konfigurationsdaten, um bei einem Ausfall den SnapCenter Server wiederherzustellen. Für unsere Lösung haben wir die SnapCenter-Datenbank und die Konfiguration auf einer AWS EC2 Instanz in unserer VPC wiederhergestellt. Weitere Informationen zu diesem Schritt finden Sie unter "Dieser Link".

Voraussetzungen für SnapCenter-Backup

Für die SnapCenter-Sicherung sind folgende Voraussetzungen erforderlich:

- Eine auf dem lokalen ONTAP-System erstellte Volume- und SMB-Freigabe, um die gesicherten Datenbank- und Konfigurationsdateien zu lokalisieren.
- Eine SnapMirror Beziehung zwischen dem lokalen ONTAP System und FSX oder CVO im AWS-Konto Über diese Beziehung wird der Snapshot mit der gesicherten SnapCenter-Datenbank und den Konfigurationsdateien transportiert.
- Windows Server wird im Cloud-Konto installiert, entweder auf einer EC2 Instanz oder auf einer VM im VMware Cloud SDDC.
- SnapCenter installiert auf der Windows EC2 Instanz oder VM in VMware Cloud.

Zusammenfassung des SnapCenter-Backup- und Restore-Prozesses

- Erstellen Sie ein Volume auf dem lokalen ONTAP System zum Hosten der Backup-db und Konfigurationsdateien.
- Einrichten einer SnapMirror Beziehung zwischen On-Premises- und FSX/CVO
- Mounten Sie den SMB-Share.
- Rufen Sie das Swagger-Autorisierungs-Token zum Ausführen von API-Aufgaben ab.
- starten sie den db-Wiederherstellungsprozess.
- Verwenden Sie das xcopy-Dienstprogramm, um das lokale Verzeichnis der db- und Konfigurationsdatei in die SMB-Freigabe zu kopieren.
- Erstellen Sie auf FSX einen Klon des ONTAP Volumes (kopiert über SnapMirror aus dem lokalen Datacenter).
- Installieren Sie den SMB-Share von FSX zu EC2/VMware Cloud.
- Kopieren Sie das Wiederherstellungsverzeichnis aus der SMB-Freigabe in ein lokales Verzeichnis.
- Führen Sie den Wiederherstellungsprozess für SQL Server aus Swagger aus.

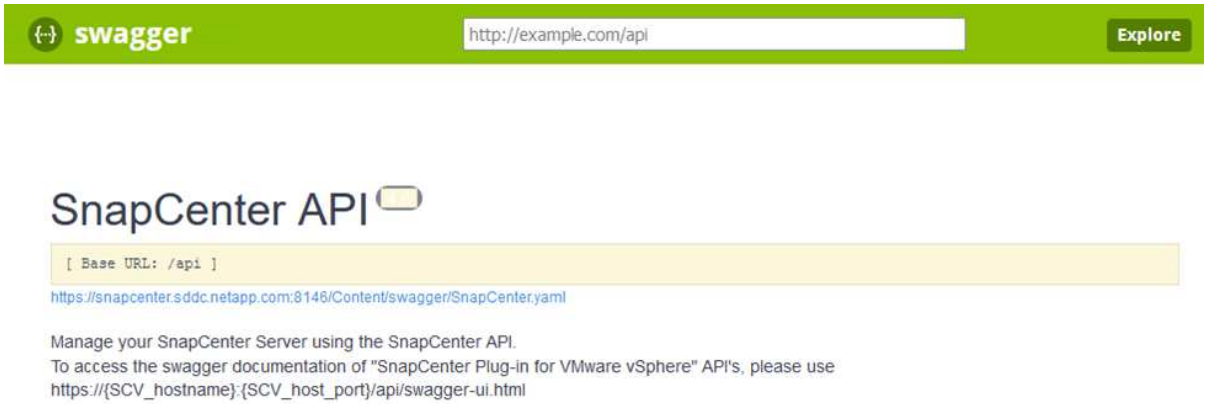
Backup der SnapCenter-Datenbank und -Konfiguration

SnapCenter stellt eine Web-Client-Schnittstelle zum Ausführen VON REST-API-Befehlen bereit. Weitere Informationen zum Zugriff auf DIE REST-APIs über Swagger finden Sie in der SnapCenter-Dokumentation unter "Dieser Link".

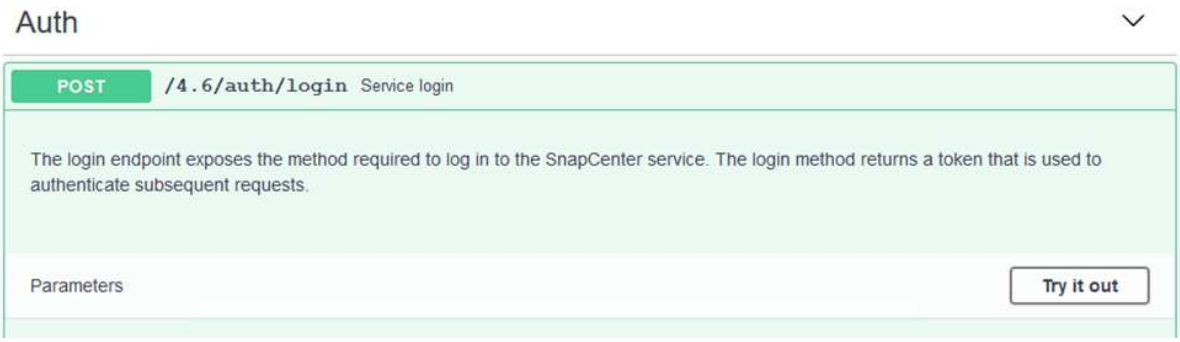
Melden Sie sich bei Swagger an und erhalten Sie ein Autorisierungs-Token

Nachdem Sie die Seite Swagger aufgerufen haben, müssen Sie ein Autorisierungs-Token abrufen, um den Wiederherstellungsprozess der Datenbank zu starten.

1. Rufen Sie die Webseite der SnapCenter Swagger API auf unter *https://<SnapCenter Server IP>:8146/Swagger/*.



2. Erweitern Sie den Abschnitt „Auth“, und klicken Sie auf „Probieren Sie es aus“.



3. Geben Sie im Bereich BenutzerbetriebContext die SnapCenter-Anmeldeinformationen und -Rolle ein, und klicken Sie auf Ausführen.

Name	Description
TokenNeverExpires boolean (query)	Token never expires false
UserOperationContext * required object (body)	User credentials Edit Value | Model

```
{
  "UserOperationContext": {
    "User": {
      "Name": "localhost\\scadmin",
      "Passphrase": "NetApp321",
      "Rolename": "SnapCenterAdmin"
    }
  }
}
```

Cancel

Parameter content type

application/json

Execute

4. Im unten stehenden Antwortkörper können Sie das Token sehen. Kopieren Sie den Token-Text zur Authentifizierung, wenn Sie den Backup-Prozess ausführen.

200

Response body

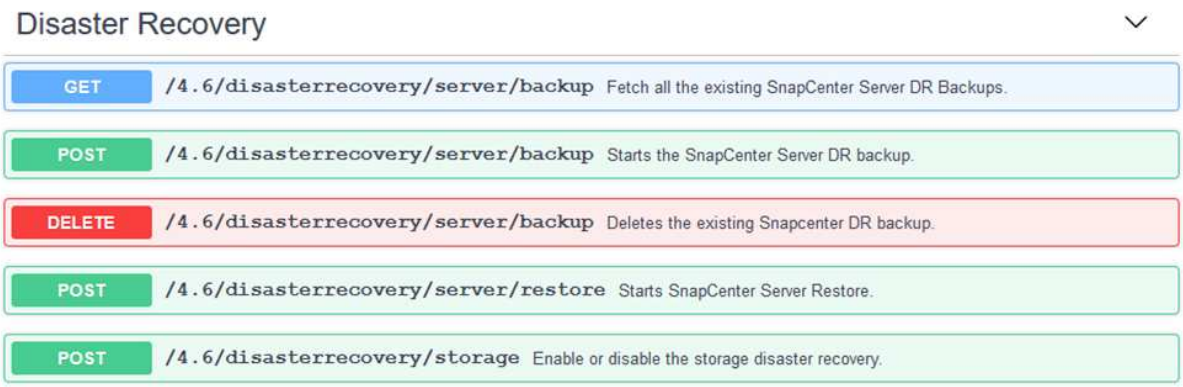

```
    "PluginName": null,
    "HostId": 0,
    "RoleId": null,
    "JobIds": null
  },
  "User": {
    "Token":
"KlYxOg==tsV6EOdtdAmAYpe8q5SG6wcoGaSjwME6jrNy5CsY63HKD5LkoZLIESRNAhpGJJ0UUQynENdgtVGDZnvx+I/ZJZIn5M1NZrj6
CLfGTApg1GmcagT08bqb5bMTx07EcdrAidzAXUDb3GyLOKtW0GdwKzSeOwKj3uVupnk1E3lskK6PRBv9RS8j0qHQvo4v4RL0hhThhwFhV
9/23nFeJVP/p1Ev4vrV/zeZVTUHPHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==",
    "Name": "SCAdmin",
    "TokenHashed": null,
    "Type": "",
    "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
    "Id": "1",
    "FullName": "SCAdmin",
    "Host": null,
    "Author": null,
    "UserName": "",
    "Domain": "",
    "Passphrase": "",
```


Download

Backup einer SnapCenter-Datenbank durchführen

Gehen Sie dann auf der Seite „Swagger“ auf den Bereich „Disaster Recovery“, um den SnapCenter-Backup-Prozess zu starten.

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



2. Erweitern Sie den `/4.6/disasterrecovery/server/backup` Und klicken Sie auf „Probieren“.

3. Fügen Sie im Abschnitt SmDRBackupRequest den korrekten lokalen Zielpfad hinzu und wählen Sie Ausführen, um das Backup der SnapCenter-Datenbank und -Konfiguration zu starten.

> Der Backup-Prozess erlaubt keine direkte Sicherung in einer NFS- oder CIFS-Dateifreigabe.

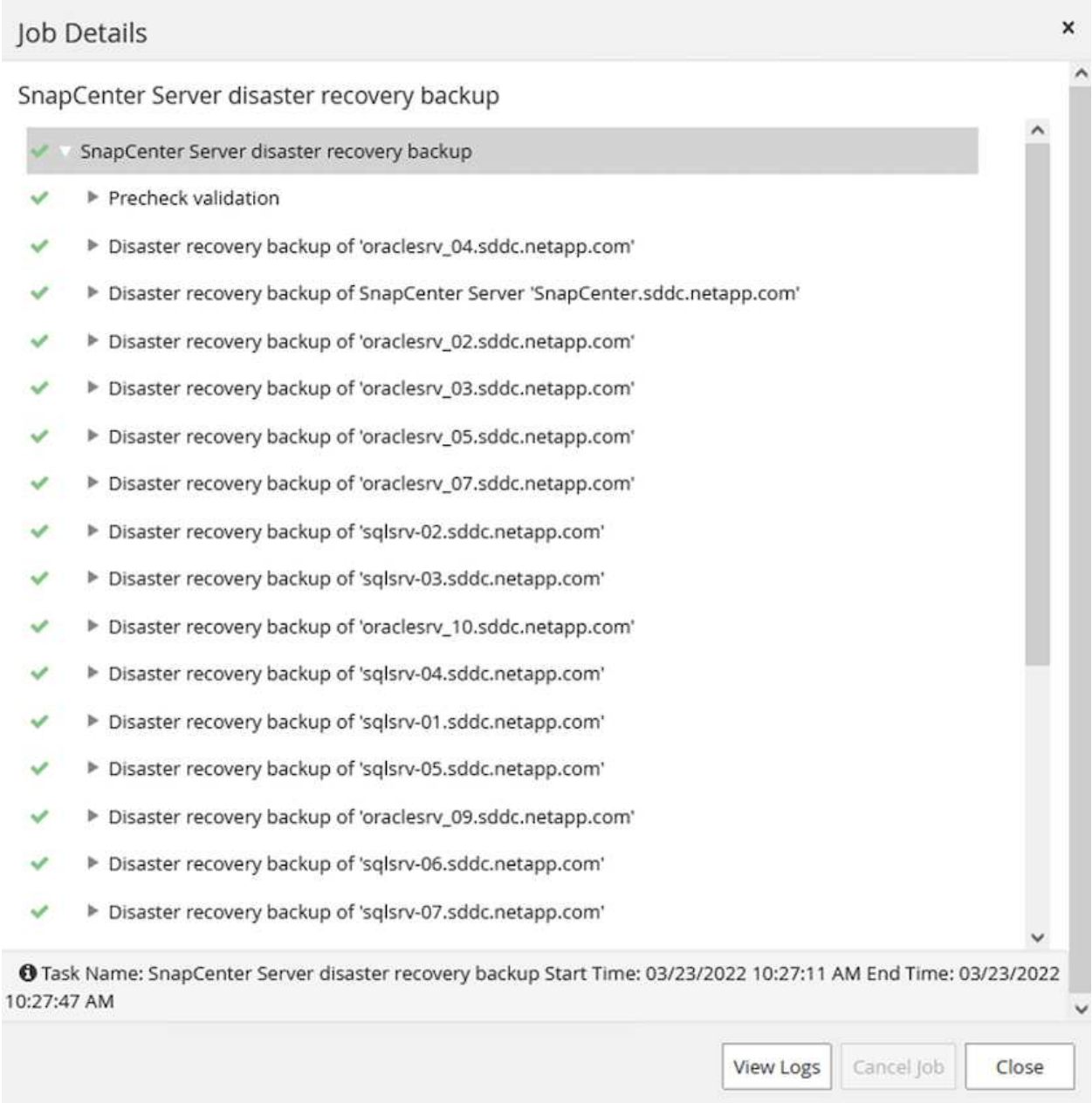
Name	Description
Token * required string *(header)*	User authorization token TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==

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 Backup-Job von SnapCenter

Melden Sie sich bei SnapCenter an, um Protokolldateien beim Starten der Datenbankwiederherstellung zu überprüfen. Im Abschnitt „Überwachen“ können Sie Details zum Disaster-Recovery-Backup des SnapCenter Servers anzeigen.



Verwenden Sie das XCOPY-Dienstprogramm, um die Datenbank-Sicherungsdatei in die SMB-Freigabe zu kopieren

Als Nächstes müssen Sie das Backup vom lokalen Laufwerk auf dem SnapCenter Server in die CIFS-Freigabe verschieben, die zum Kopieren der Daten durch SnapMirror an den sekundären Speicherort auf der FSX Instanz in AWS verwendet wird. Verwenden Sie xcopy mit spezifischen Optionen, die die Berechtigungen der Dateien behalten.

Öffnen Sie eine Eingabeaufforderung als Administrator. Geben Sie an 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
```

Failover

Ausfall am primären Standort

Für einen Ausfall im primären Datacenter vor Ort umfasst unser Szenario ein Failover an einen sekundären Standort in einer Amazon Web Services Infrastruktur mit VMware Cloud on AWS. Wir gehen davon aus, dass auf die Virtual Machines und unser On-Premises-ONTAP-Cluster nicht mehr zugegriffen werden kann. Darüber hinaus sind die SnapCenter und Veeam Virtual Machines nicht mehr zugänglich und müssen an unserem sekundären Standort neu erstellt werden.

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

- Wiederherstellung der SnapCenter-Datenbank. Nach dem Einrichten eines neuen SnapCenter Servers stellen Sie die MySQL-Datenbank und die Konfigurationsdateien wieder her und schalten die Datenbank in den Disaster-Recovery-Modus um, damit der sekundäre FSX-Storage zum primären Speichergerät wird.
- Stellen Sie die Virtual Machines der Applikationen mit Veeam Backup & Replication wieder her. Verbinden Sie den S3-Storage mit den VM-Backups, importieren Sie die Backups und stellen Sie sie in VMware Cloud auf AWS wieder her.
- Stellen Sie die SQL Server Applikationsdaten mithilfe von SnapCenter wieder her.
- Stellen Sie die Oracle Applikationsdaten mit SnapCenter wieder her.

Wiederherstellung der SnapCenter Datenbanken

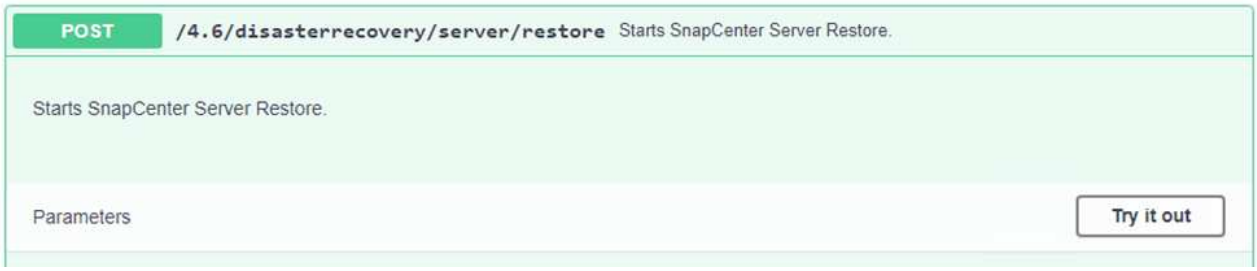
SnapCenter unterstützt Disaster Recovery-Szenarien, da das Backup und Restore seiner MySQL Datenbank und Konfigurationsdateien gestattet werden. So kann ein Administrator regelmäßige Backups der SnapCenter Datenbank im lokalen Datacenter durchführen und diese Datenbank später in einer sekundären SnapCenter Datenbank wiederherstellen.

Führen Sie die folgenden Schritte aus, um auf die SnapCenter Backup-Dateien auf dem Remote-SnapCenter-Server zuzugreifen:

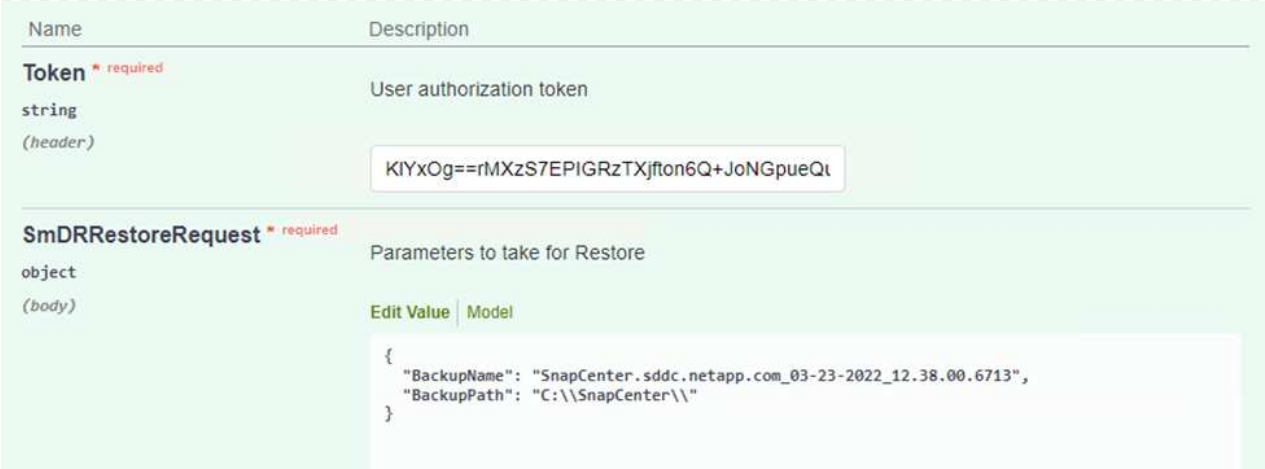
1. SnapMirror Beziehung vom FSX Cluster lösen, wodurch das Volume Lese-/Schreibzugriff ermöglicht.
2. Erstellen Sie (falls erforderlich) einen CIFS-Server und erstellen Sie eine CIFS-Freigabe, die zum Verbindungspfad des geklonten Volume führt.
3. Verwenden Sie xcopy, um die Sicherungsdateien in ein lokales Verzeichnis auf dem sekundären SnapCenter-System zu kopieren.
4. Installieren Sie SnapCenter v4.6.
5. Stellen Sie sicher, dass der SnapCenter-Server über denselben FQDN wie der ursprüngliche Server verfügt. Dies ist erforderlich, damit die datenbankwiederherstellung erfolgreich durchgeführt werden kann.

Um den Wiederherstellungsprozess zu starten, führen Sie die folgenden Schritte aus:

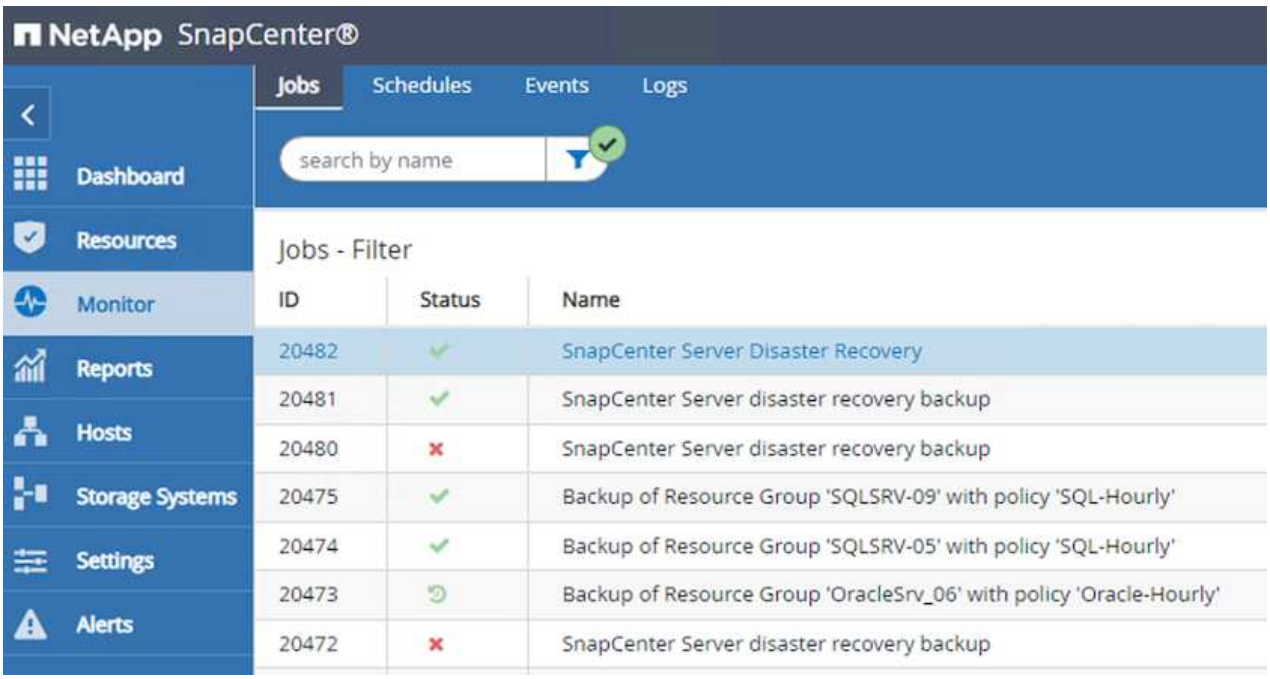
1. Navigieren Sie zur Swagger API-Webseite für den sekundären SnapCenter-Server, und folgen Sie den vorherigen Anweisungen, um ein Autorisierungs-Token zu erhalten.
2. Navigieren Sie auf der Seite Swagger zum Abschnitt Disaster Recovery, und wählen Sie `/4.6/disasterrecovery/server/restore`, Und klicken Sie auf Probieren Sie es aus.

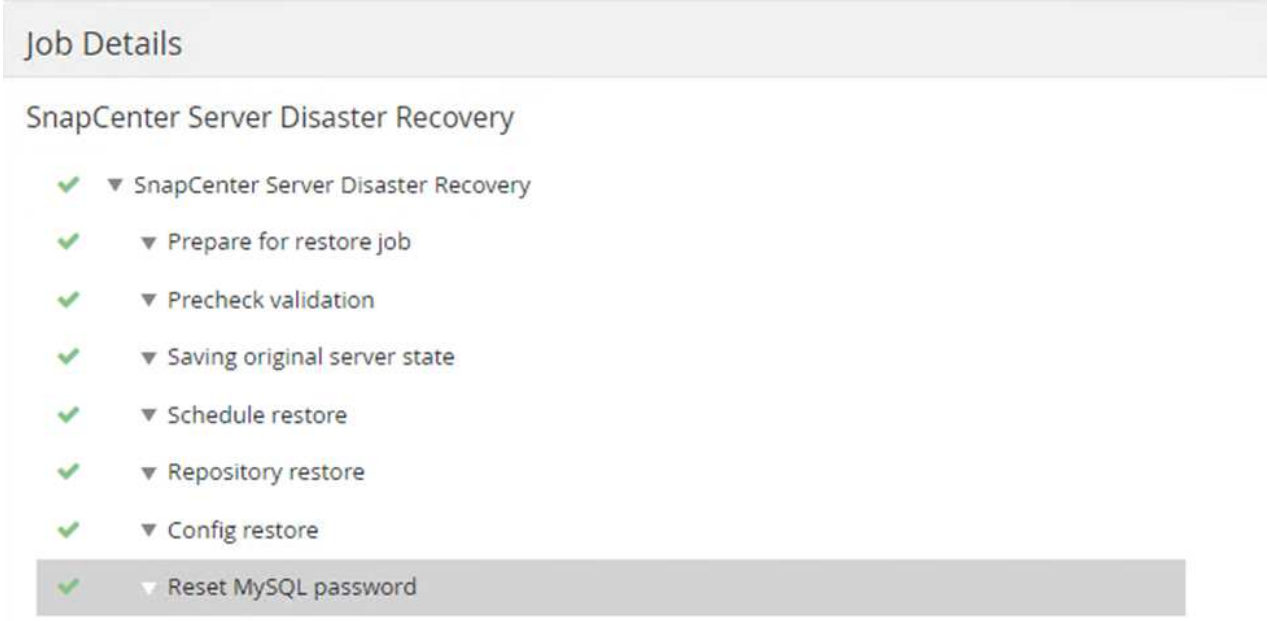


3. Fügen Sie das Autorisierungs-Token ein, und fügen Sie im Abschnitt SmDRResterRequest den Namen des Backups und das lokale Verzeichnis auf dem sekundären SnapCenter-Server ein.



4. Wählen Sie die Schaltfläche Ausführen, um den Wiederherstellungsvorgang zu starten.
5. Navigieren Sie in SnapCenter zum Abschnitt Überwachung, um den Fortschritt des Wiederherstellungsjobs anzuzeigen.





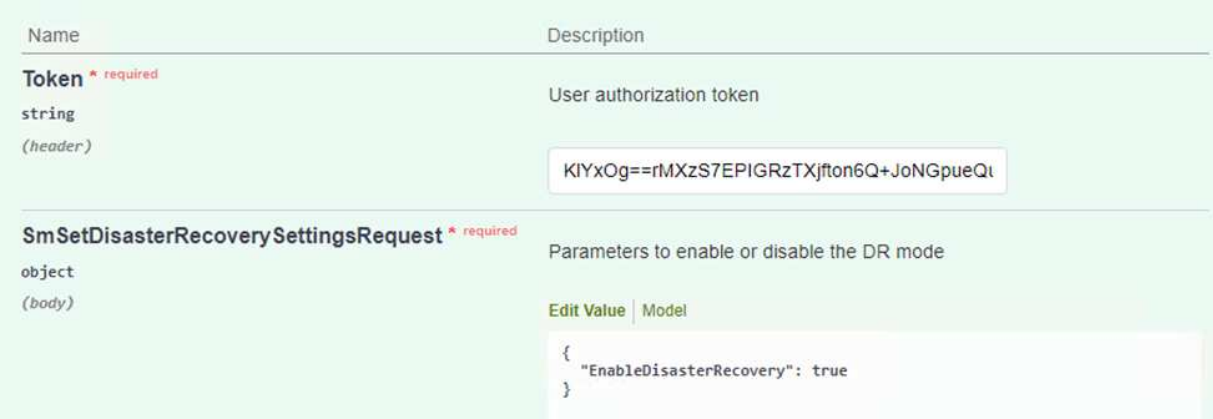
6. Um SQL Server Restores von einem sekundären Storage zu aktivieren, müssen Sie die SnapCenter-Datenbank in den Disaster Recovery-Modus schalten. Dies wird als separate Operation durchgeführt und auf der Swagger API Webseite initiiert.

   a. Navigieren Sie zum Abschnitt Disaster Recovery, und klicken Sie auf `/4.6/disasterrecovery/storage`.

   b. Fügen Sie das Benutzerautorisierungs-Token ein.

   c. Ändern Sie im Abschnitt SmSetDistasterRecoverySettingsRequest `EnableDisasterRecover` Bis `true`.

   d. Klicken Sie auf Ausführen, um den Disaster Recovery-Modus für SQL Server zu aktivieren.



Siehe Anmerkungen zu weiteren Verfahren.

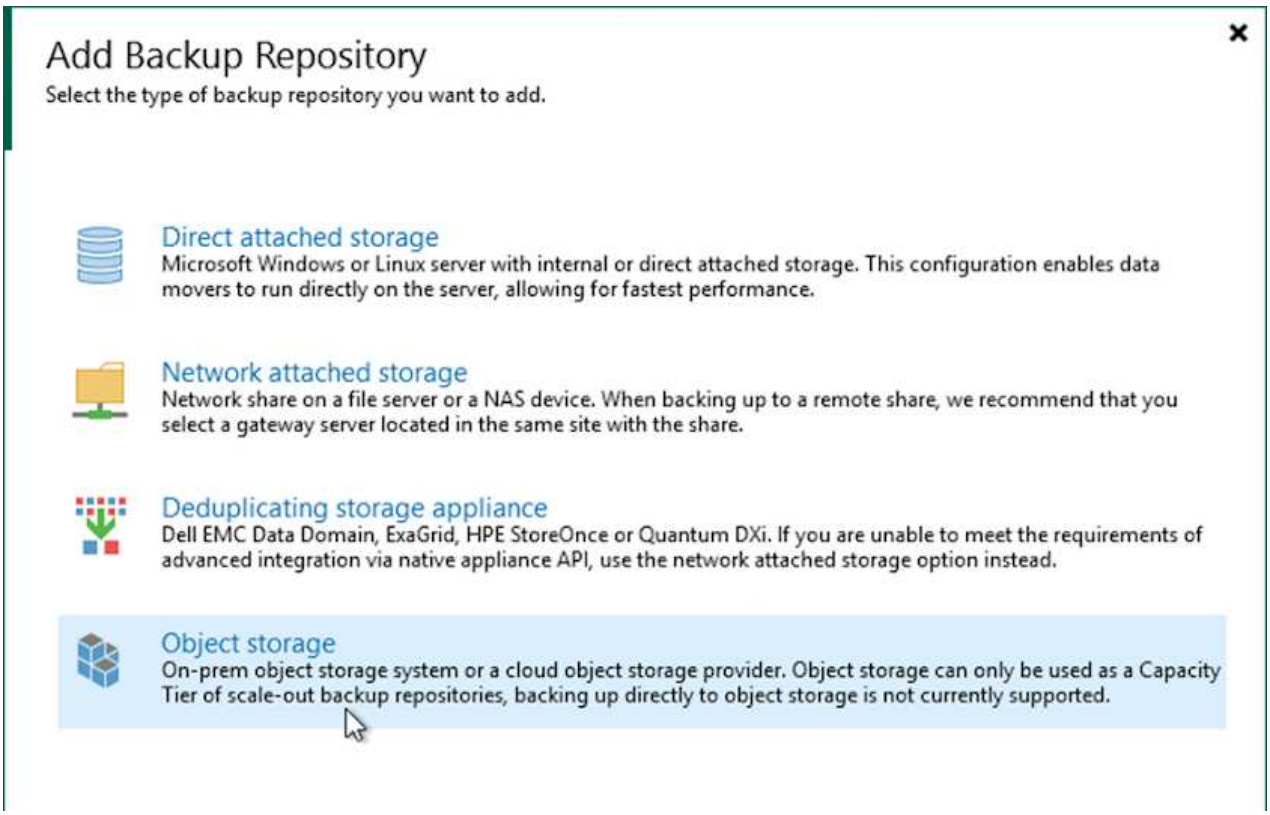
Wiederherstellung von Applikations-VMs mit vollständiger Veeam-Wiederherstellung

Backup-Repository erstellen und Backups aus S3 importieren

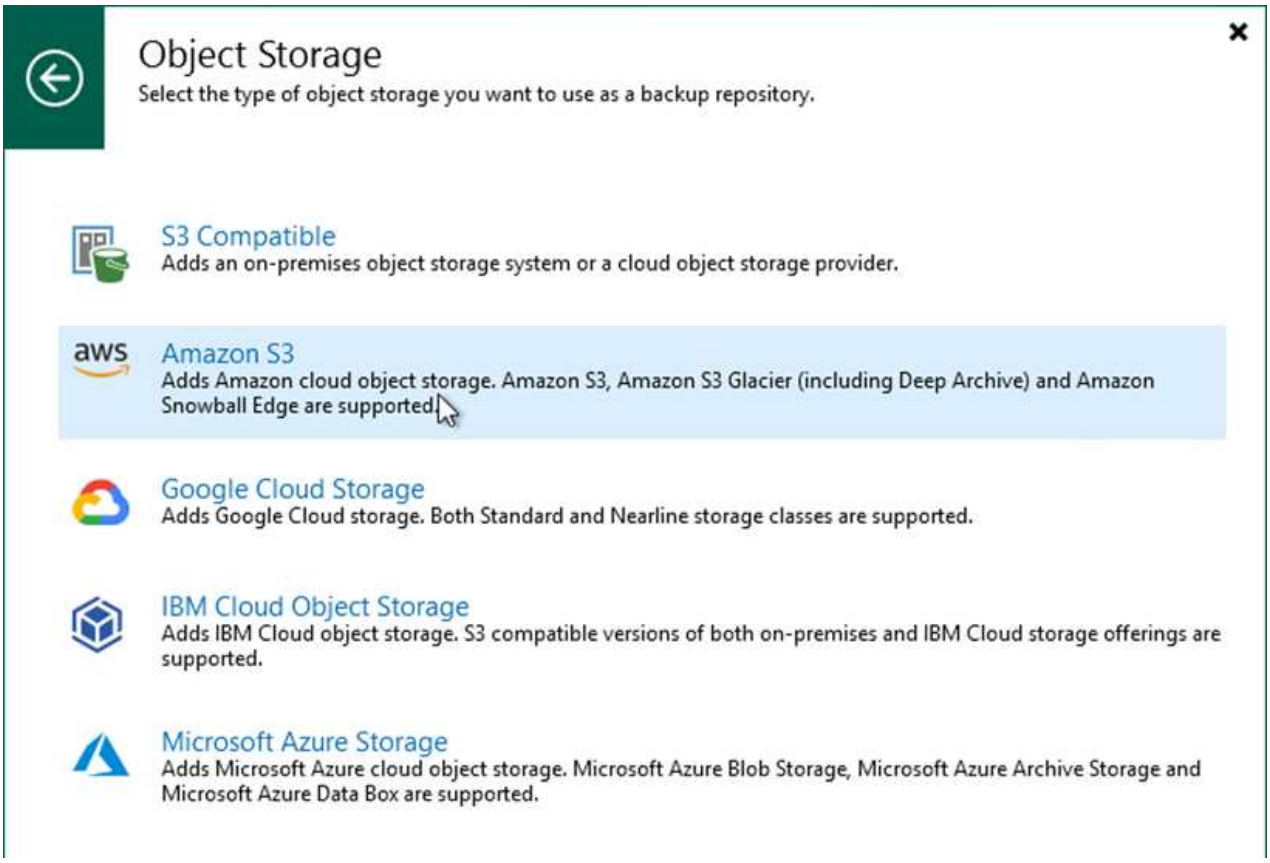
Importieren Sie vom sekundären Veeam-Server die Backups aus S3 Storage und stellen Sie SQL Server und Oracle VMs in Ihr VMware Cloud-Cluster wieder her.

So importieren Sie die Backups aus dem S3-Objekt, das Teil des Scale-out-Backup-Repositorys vor Ort war:

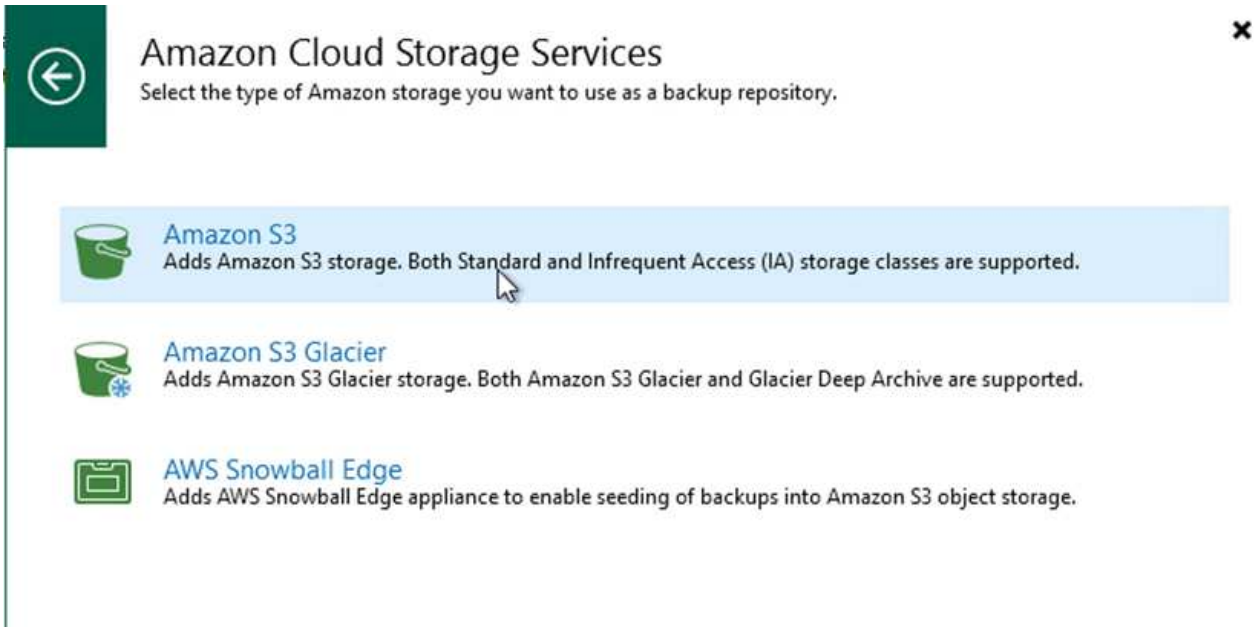
1. Gehen Sie zu Backup Repositories und klicken Sie im oberen Menü auf Repository hinzufügen, um den Assistenten zum Hinzufügen von Backup-Repositorys zu starten. Wählen Sie auf der ersten Seite des Assistenten als Backup-Repository-Typ Objekt-Storage aus.



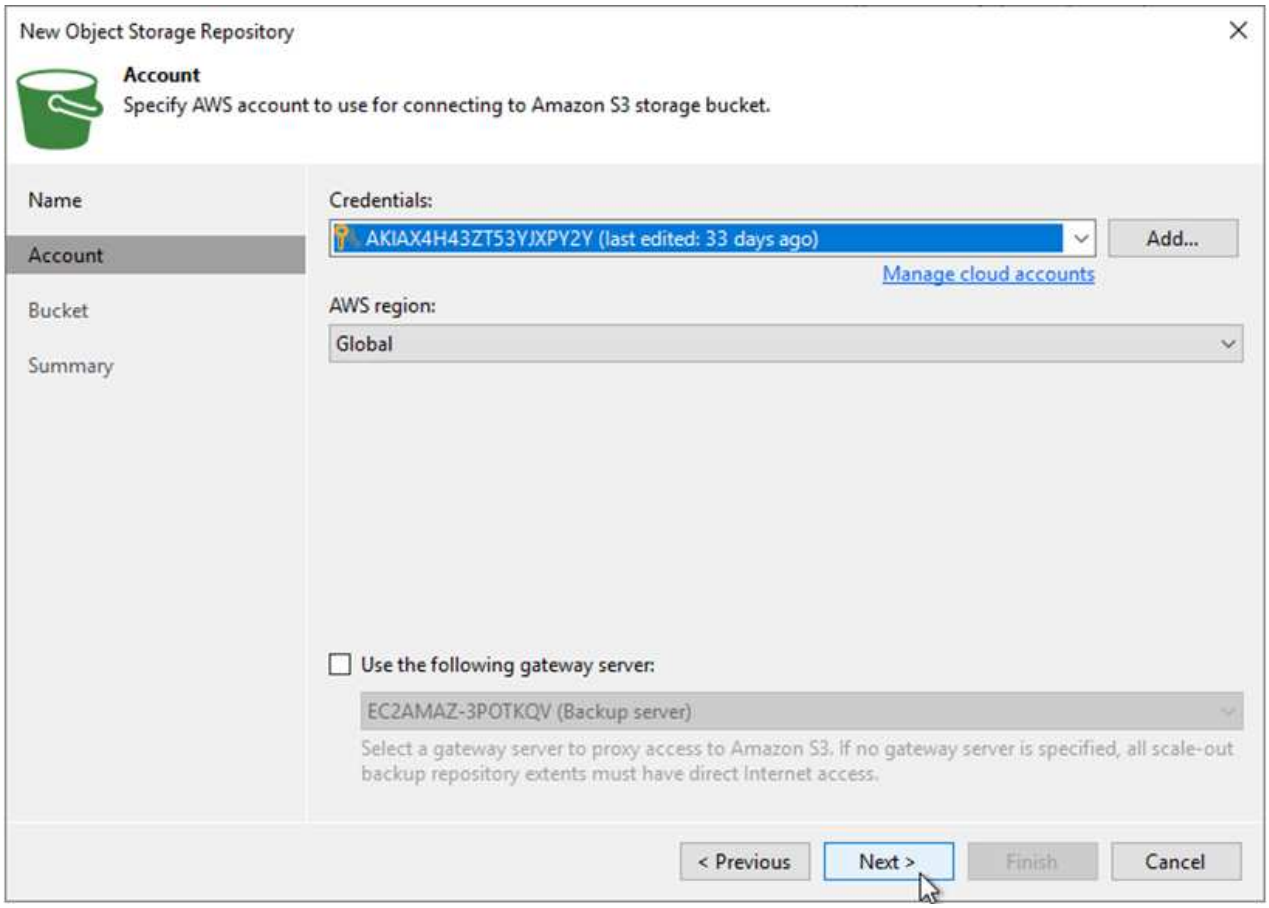
2. Wählen Sie Amazon S3 als Objektspeichertyp aus.



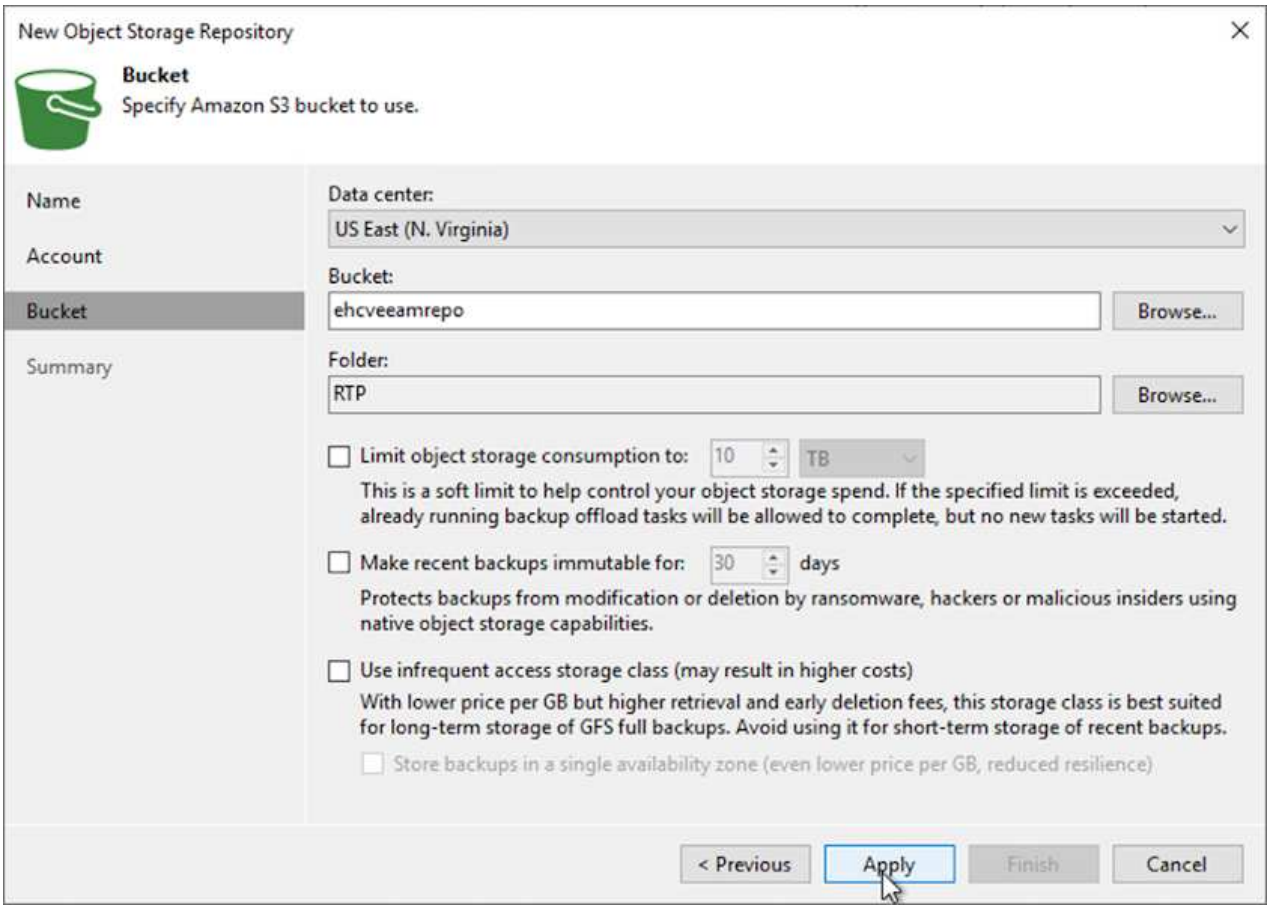
3. Wählen Sie aus der Liste der Amazon Cloud Storage Services Amazon S3 aus.



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



5. Geben Sie auf der Bucket-Seite Datacenter, Bucket, Ordner und gewünschte Optionen ein. Klicken Sie Auf Anwenden.

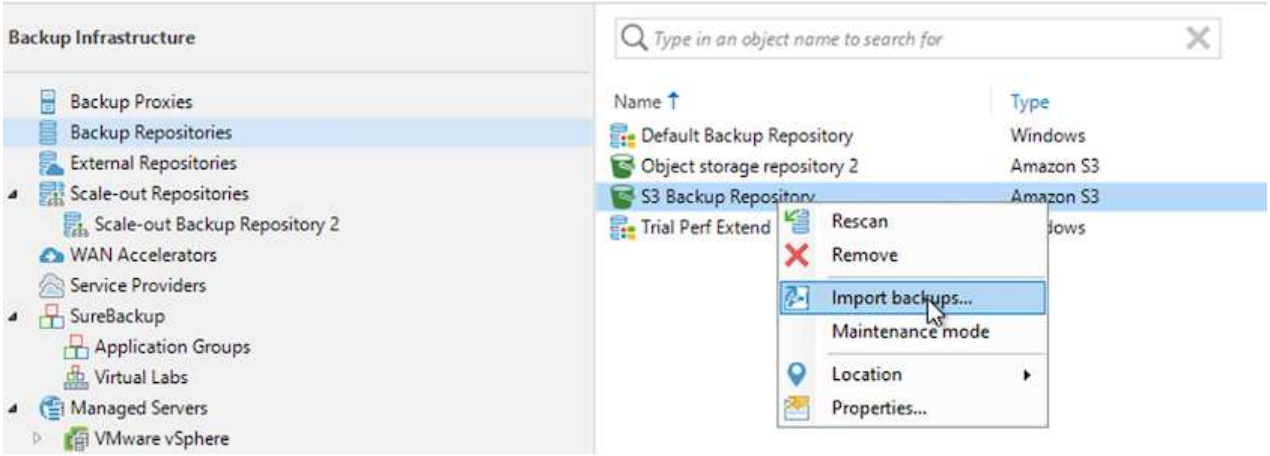


6. Wählen Sie abschließend Fertigstellen aus, um den Prozess abzuschließen und das Repository hinzuzufügen.

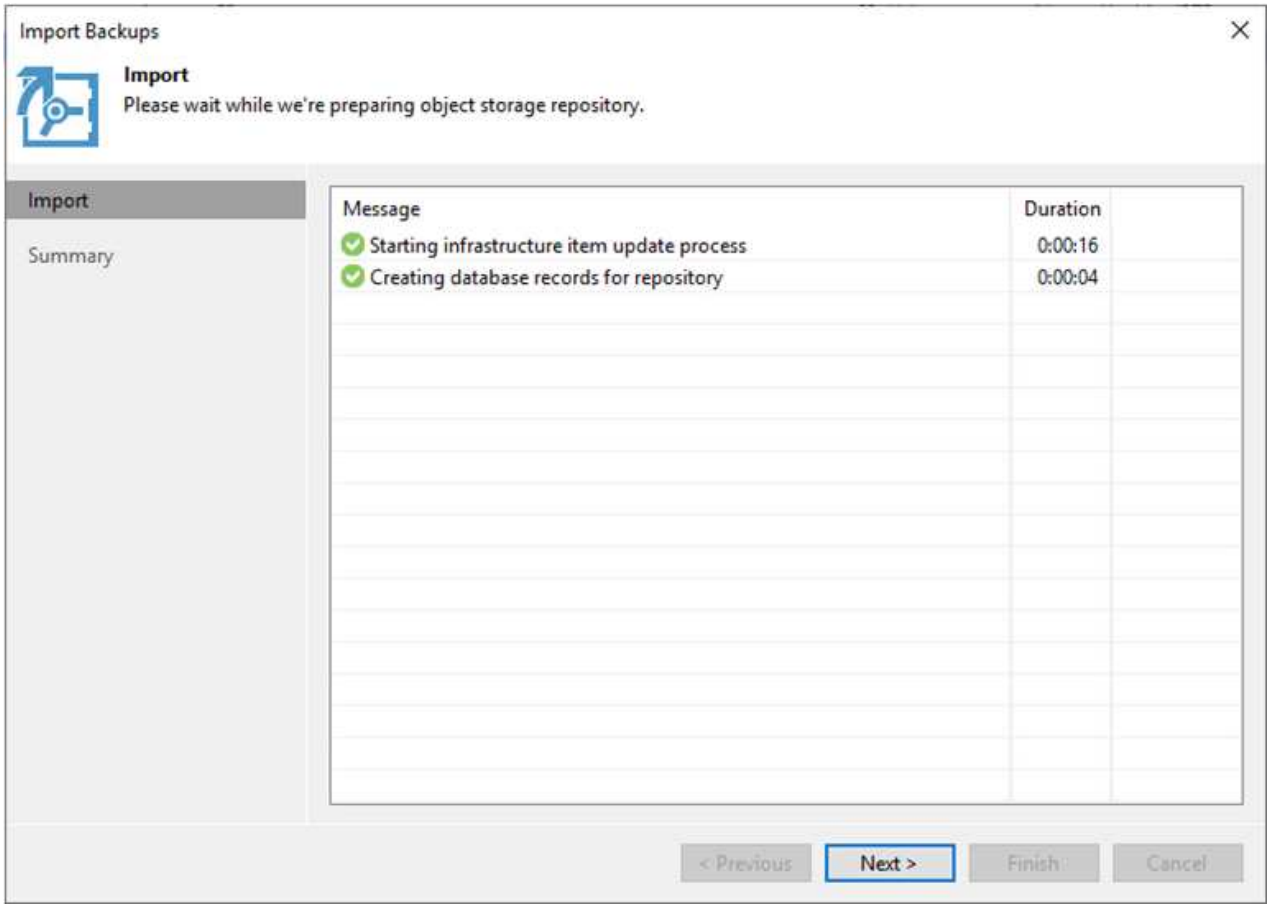
Backups aus S3 Objekt-Storage importieren

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

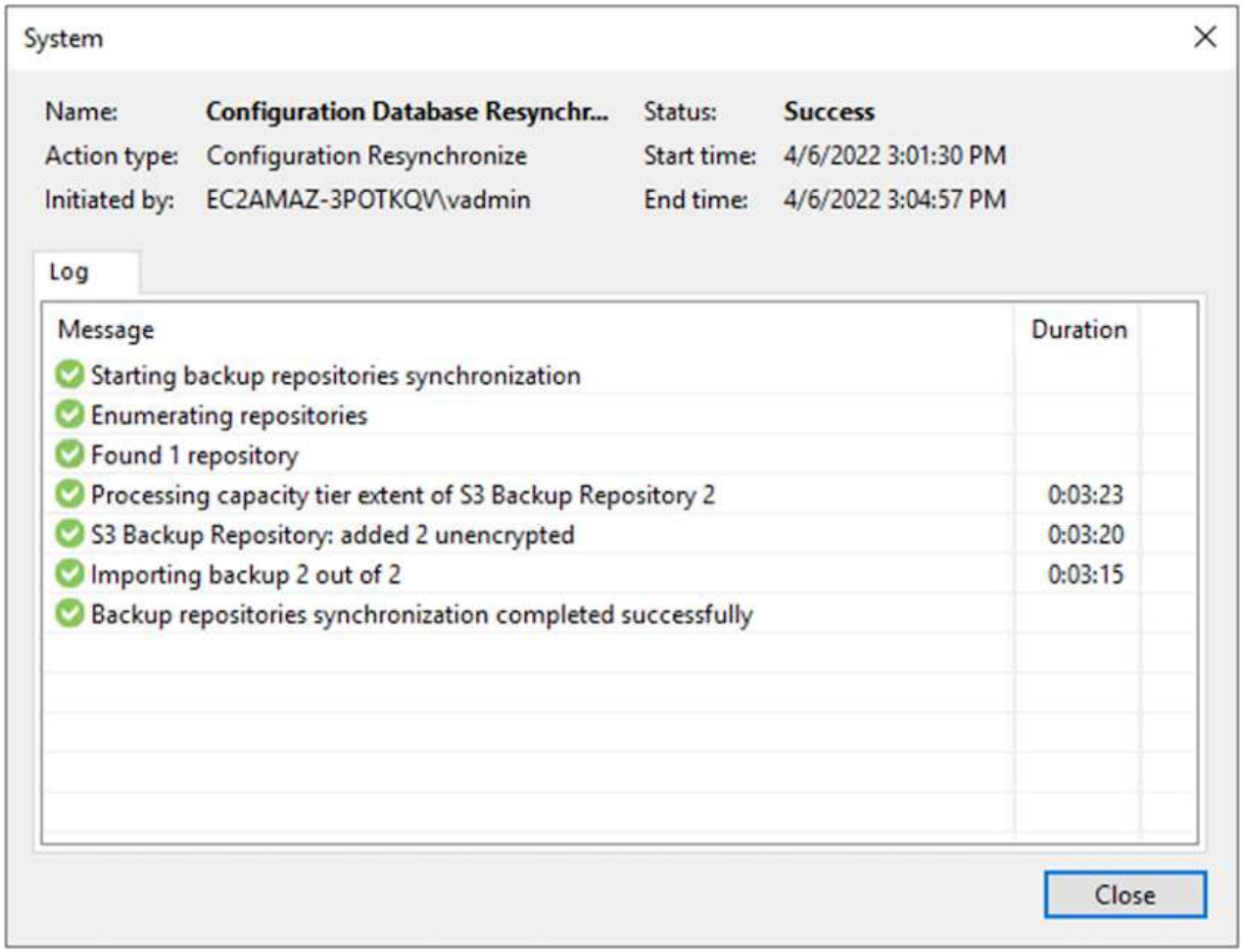
1. Wählen Sie aus dem S3-Backup-Repository die Option Backups importieren aus, um den Assistenten zum Importieren von Backups zu starten.



2. Nachdem die Datenbankdatensätze für den Import erstellt wurden, wählen Sie Weiter und dann auf dem Übersichtsbildschirm Beenden, um den Importvorgang zu starten.



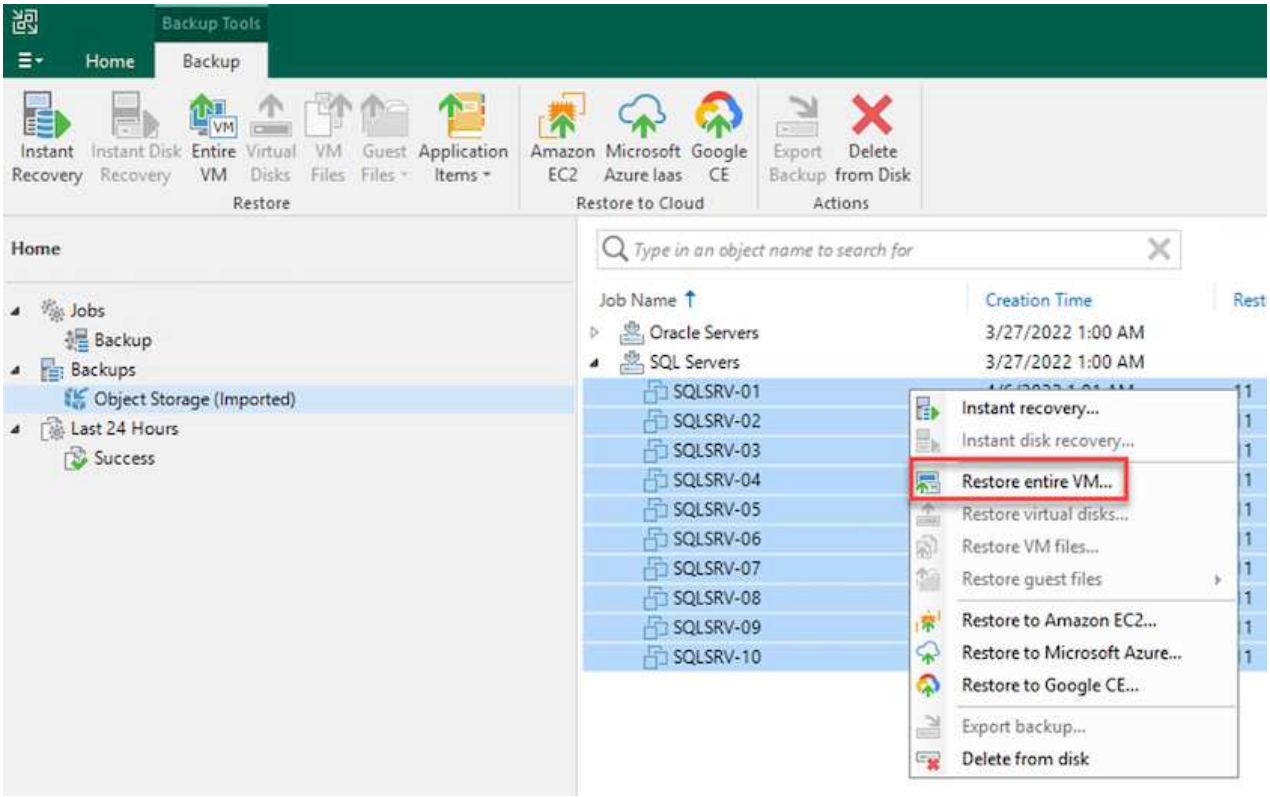
3. Nach Abschluss des Imports können Sie die VMs in das VMware Cloud Cluster wiederherstellen.


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

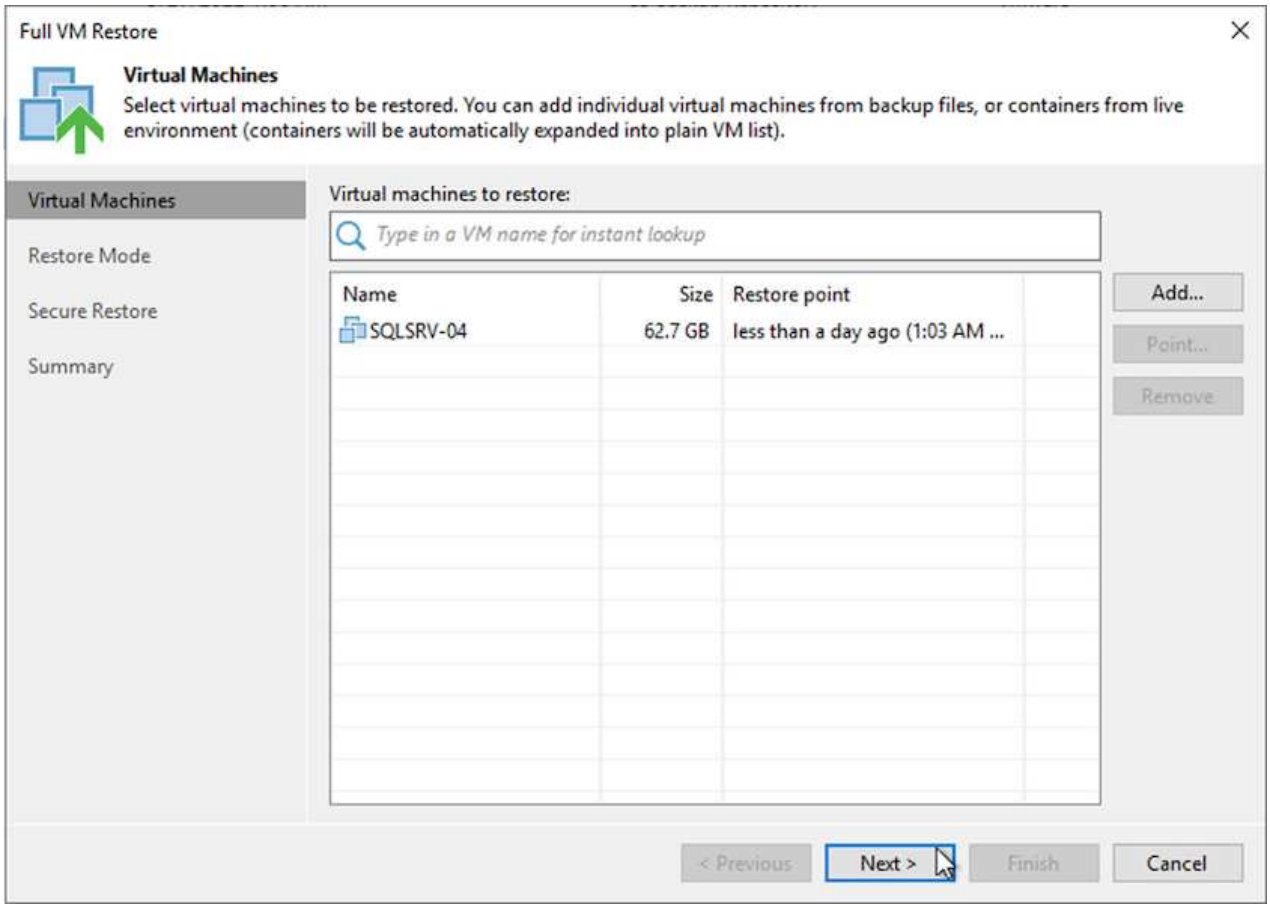
Wiederherstellung von Applikations-VMs mit vollständiger Wiederherstellung durch Veeam in VMware Cloud

Um SQL und Oracle Virtual Machines in VMware Cloud auf AWS Workload Domain/Cluster wiederherzustellen, führen Sie die folgenden Schritte aus.

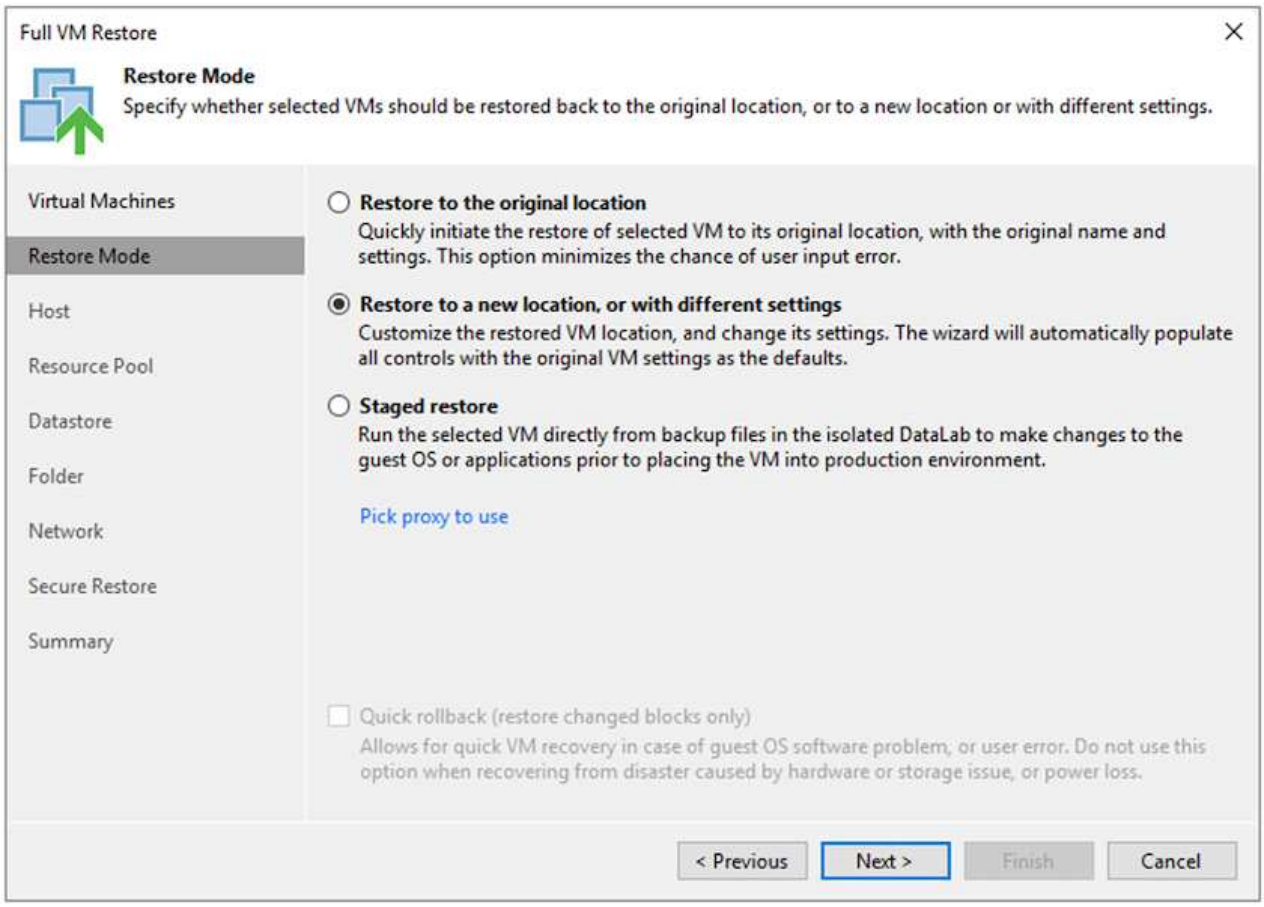
1. Wählen Sie auf der Veeam-Startseite den Objektspeicher aus, der die importierten Backups enthält, wählen Sie die wiederherzustellenden VMs aus, und klicken Sie dann mit der rechten Maustaste, und wählen Sie die Option gesamte VM wiederherstellen aus.



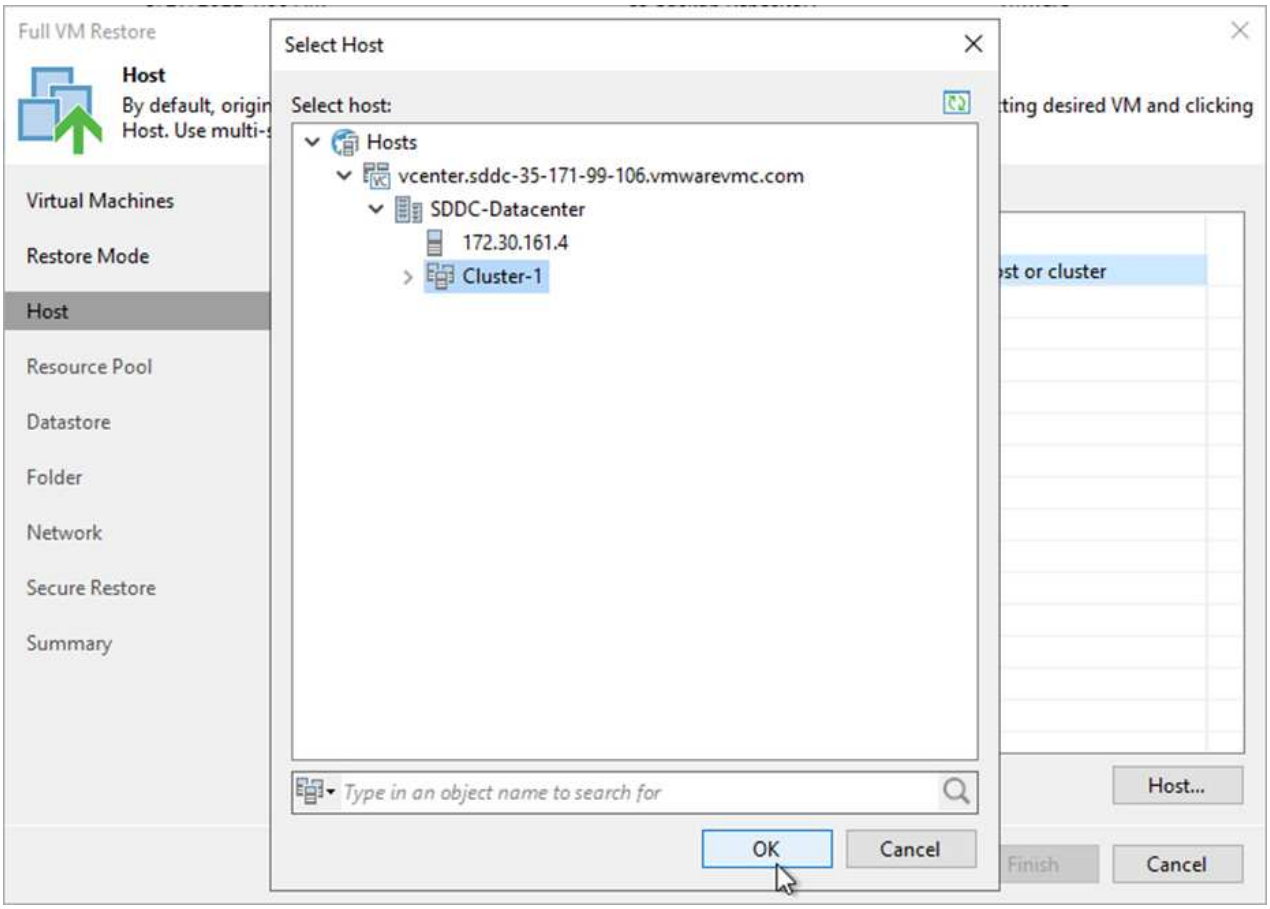
2. Ändern Sie auf der ersten Seite des Assistenten zur vollständigen VM-Wiederherstellung die VMs, die gesichert werden sollen, falls gewünscht, und wählen Sie Weiter.



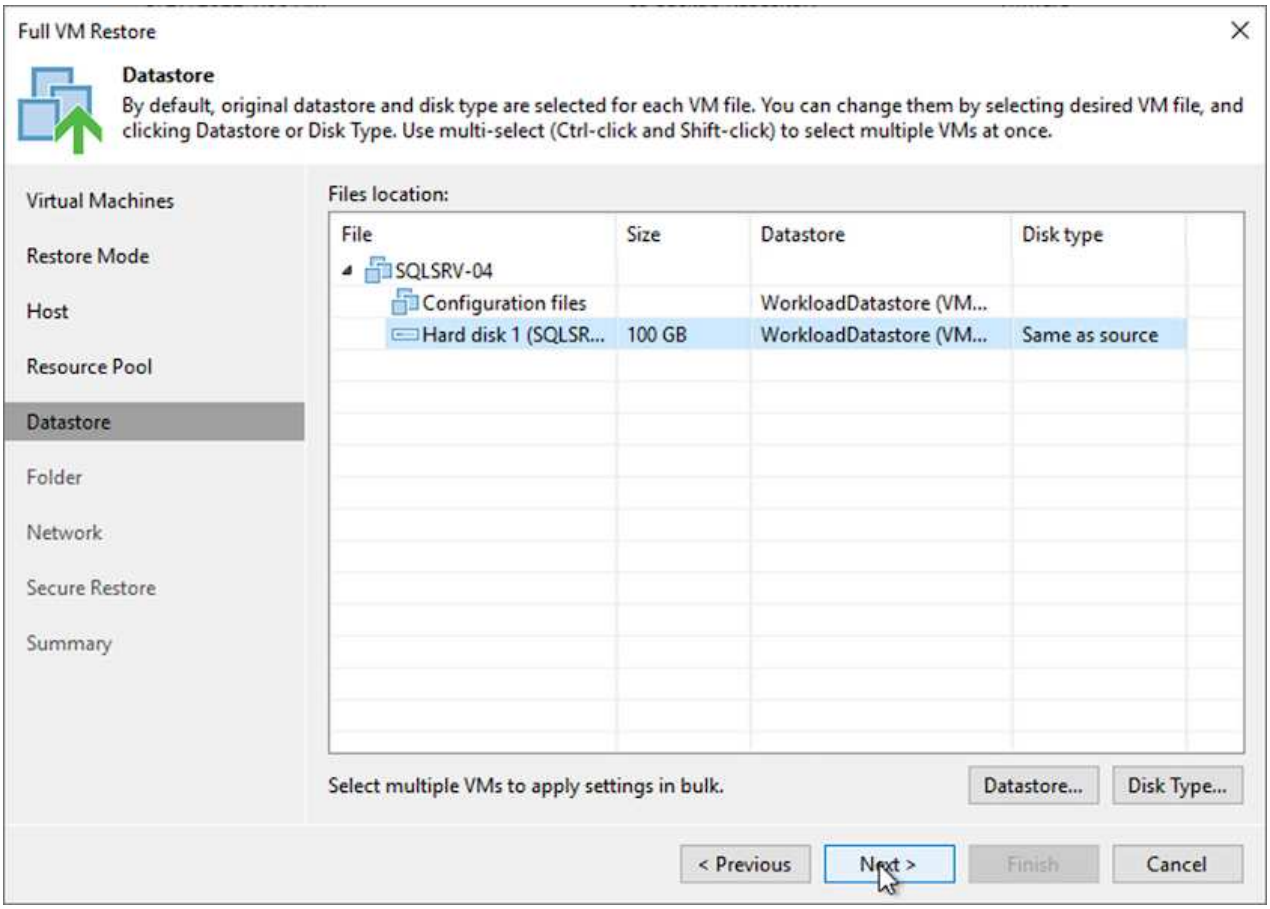
3. Wählen Sie auf der Seite Wiederherstellungsmodus die Option Wiederherstellen an einem neuen Speicherort oder mit anderen Einstellungen.



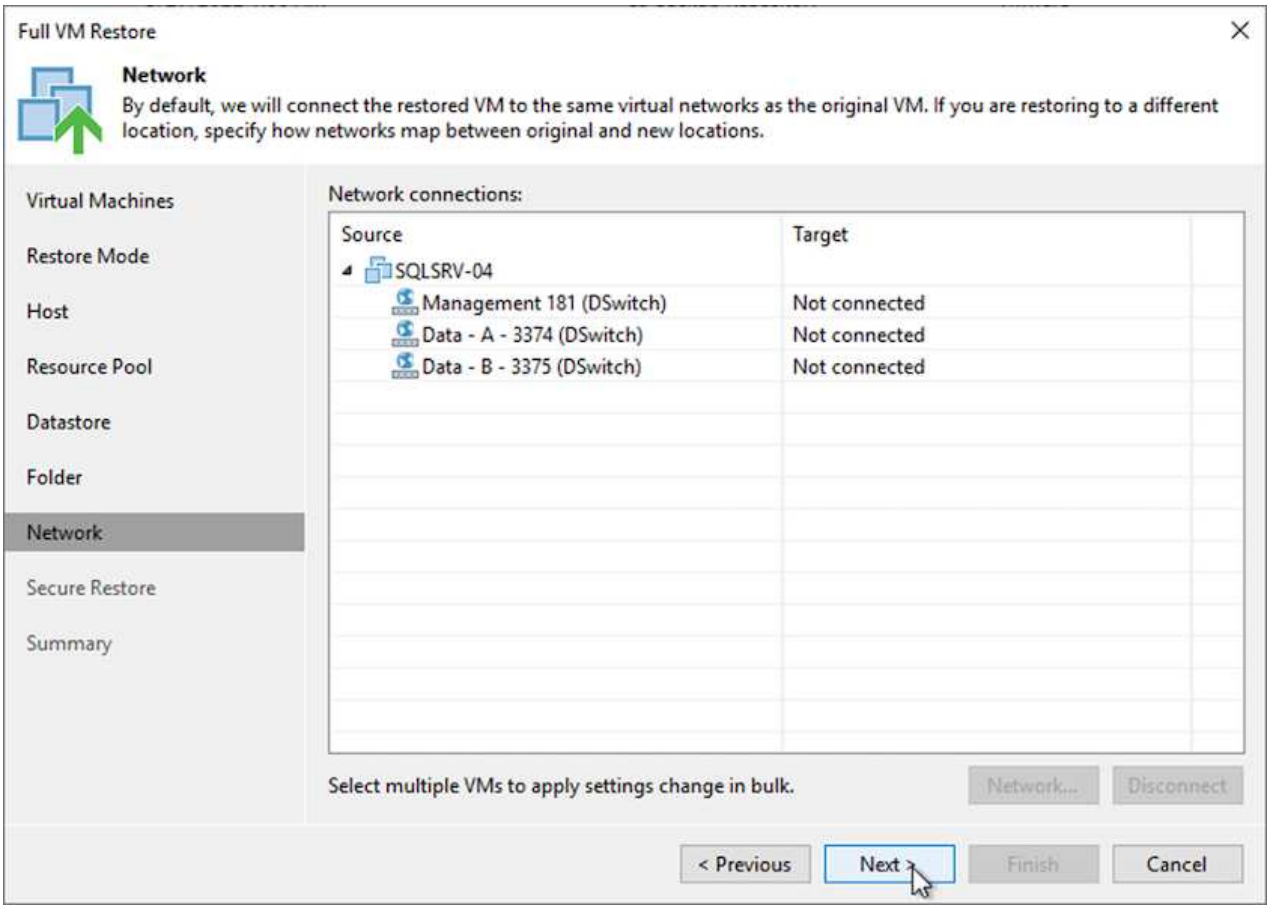
4. Wählen Sie auf der Host-Seite den Ziel-ESXi-Host oder das Ziel-Cluster aus, auf dem die VM wiederhergestellt werden soll.

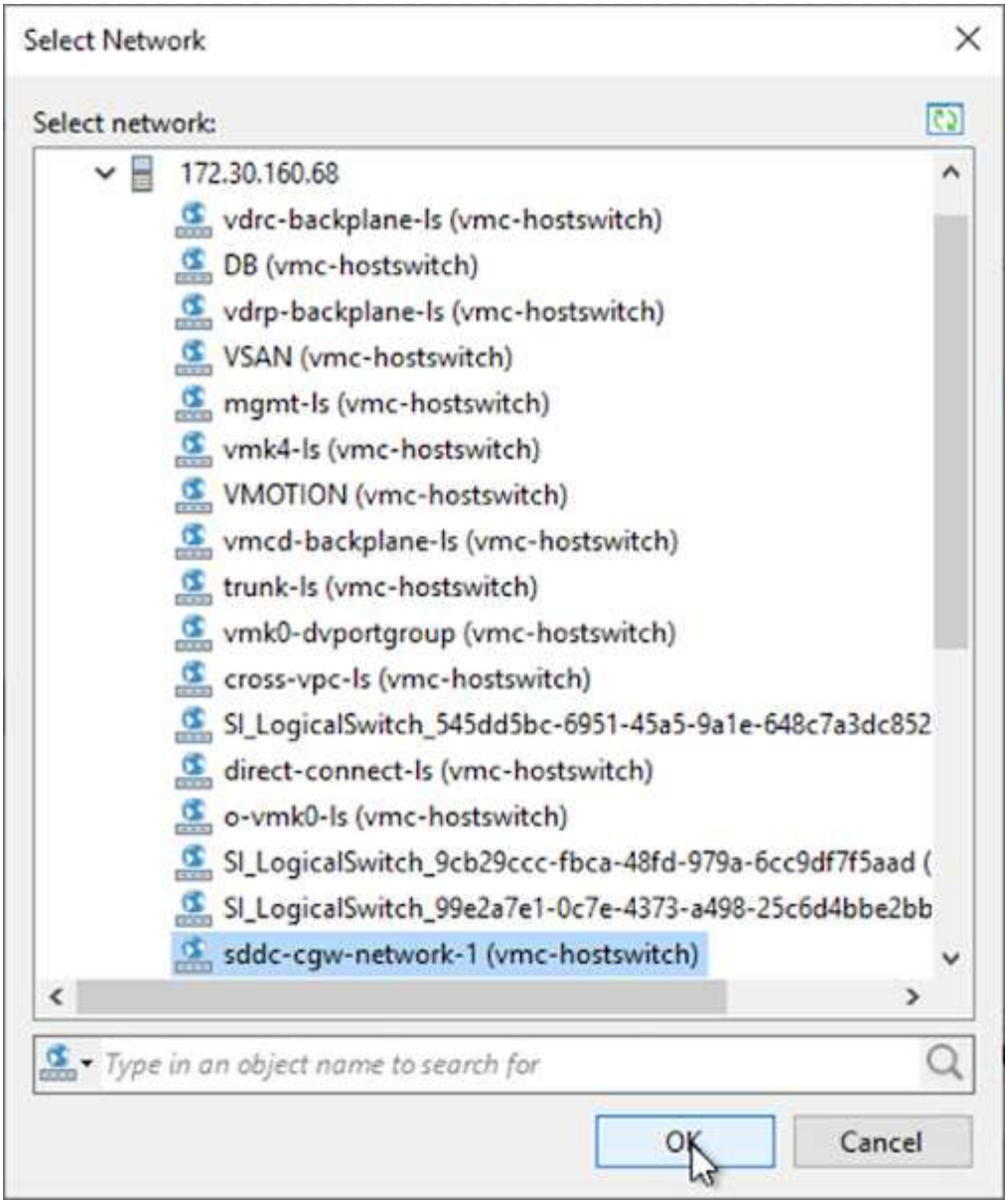


5. Wählen Sie auf der Seite Datastores den Speicherort des Ziel-Datenspeichers für die Konfigurationsdateien und die Festplatte aus.



6. Ordnen Sie auf der Seite Netzwerk die ursprünglichen Netzwerke auf der VM den Netzwerken im neuen Zielverzeichnis 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 nach Malware gescannt werden soll, überprüfen Sie die Übersichtsseite, und klicken Sie auf Fertig stellen, um die Wiederherstellung zu starten.

Stellen Sie SQL Server Applikationsdaten wieder her

Das folgende Verfahren enthält Anweisungen zur Wiederherstellung eines SQL Servers in VMware Cloud Services in AWS im Falle eines Ausfalls, durch den der Betrieb des lokalen Standorts gewährleistet wird.

Es wird davon ausgegangen, dass die folgenden Voraussetzungen abgeschlossen sind, um mit den Wiederherstellungsschritten fortzufahren:

1. Die Windows-Server-VM wurde mithilfe von Veeam Full Restore in VMware Cloud SDDC wiederhergestellt.
2. Es wurde ein sekundärer SnapCenter-Server eingerichtet, und die Wiederherstellung und Konfiguration von SnapCenter Datenbanken wurden anhand der im Abschnitt beschriebenen Schritte abgeschlossen "Zusammenfassung des SnapCenter-Backup- und Restore-Prozesses"

VM: Post-Restore-Konfiguration für SQL Server VM

Nach Abschluss der Wiederherstellung der VM müssen Sie Netzwerke und andere Elemente konfigurieren, die für die erneute Erkennung der Host-VM in SnapCenter konfiguriert werden.

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

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

> Damit die wiederhergestellten VMs in SnapCenter automatisch wieder aufgeermittelt werden können, muss der FQDN mit der VM übereinstimmen, die ursprünglich der SnapCenter vor Ort hinzugefügt wurde.

Konfigurieren Sie FSX-Speicher für SQL Server Restore

Um den Disaster Recovery-Prozess für eine SQL Server VM durchzuführen, müssen Sie die bestehende SnapMirror Beziehung vom FSX Cluster durchbrechen und den Zugriff auf das Volume gewähren. Um das zu tun, führen Sie folgende Schritte durch.

1. Um die vorhandene SnapMirror Beziehung für die SQL Server-Datenbank und Protokoll-Volumes zu unterbrechen, führen Sie den folgenden Befehl aus der FSX-CLI aus:

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

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

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

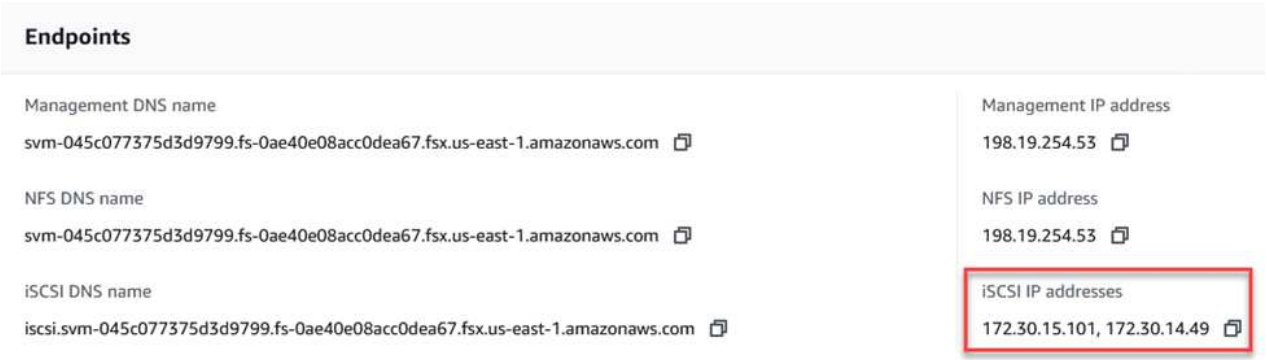
3. Schließlich ordnen Sie die LUNs der Initiatorgruppe zu, die Sie gerade erstellt haben:

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

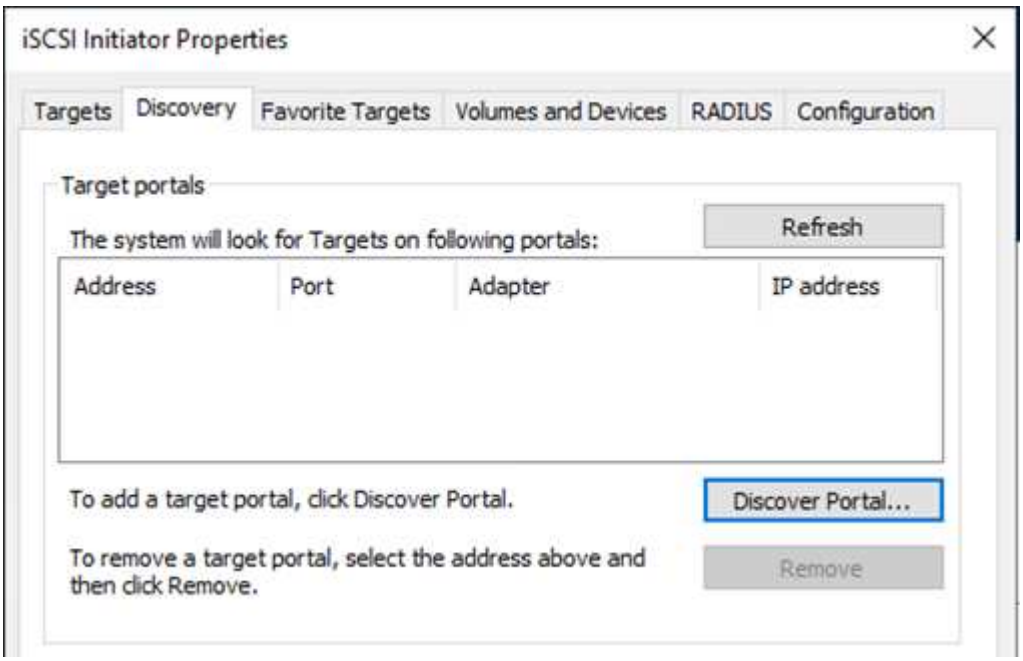
4. Um den Namen des Pfads zu finden, führen Sie den aus `lun show` Befehl.

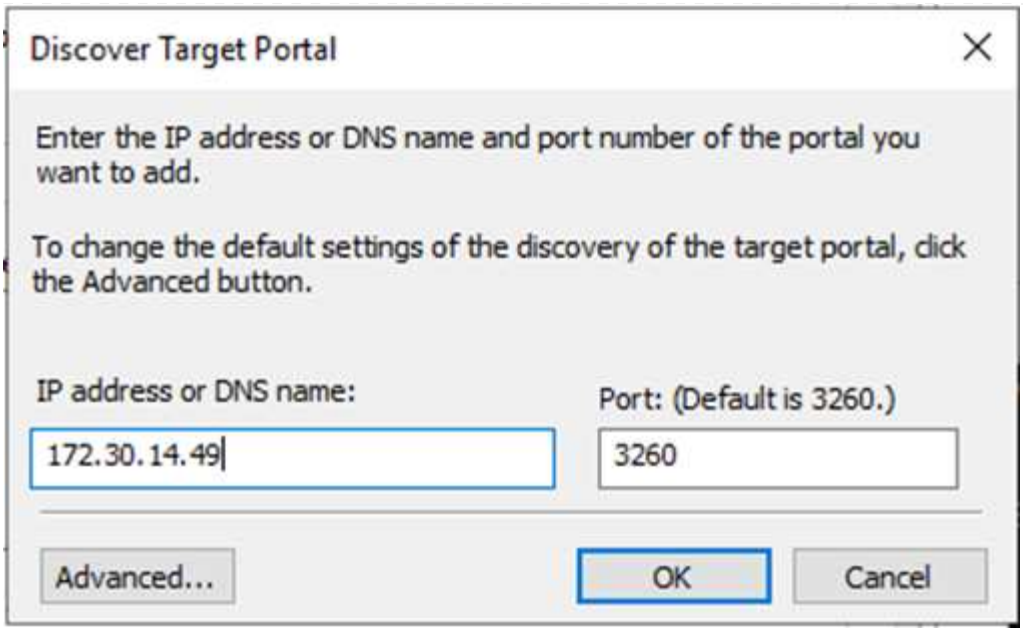
Richten Sie Windows VM für iSCSI-Zugriff ein und ermitteln Sie die Dateisysteme

1. Richten Sie von der SQL Server-VM aus Ihren iSCSI-Netzwerkadapter ein, um mit der VMware-Portgruppe zu kommunizieren, die mit Konnektivität zu den iSCSI-Zielschnittstellen auf Ihrer FSX-Instanz eingerichtet wurde.
2. Öffnen Sie das Dienstprogramm iSCSI Initiator Properties, und löschen Sie die alten Verbindungseinstellungen auf den Registerkarten Discovery, Favorite Targets und Targets.
3. Suchen Sie die IP-Adresse(n) für den Zugriff auf die logische iSCSI-Schnittstelle auf der FSX-Instanz/dem FSX-Cluster. Sie finden sie in der AWS Konsole unter Amazon FSX > ONTAP > Storage Virtual Machines.

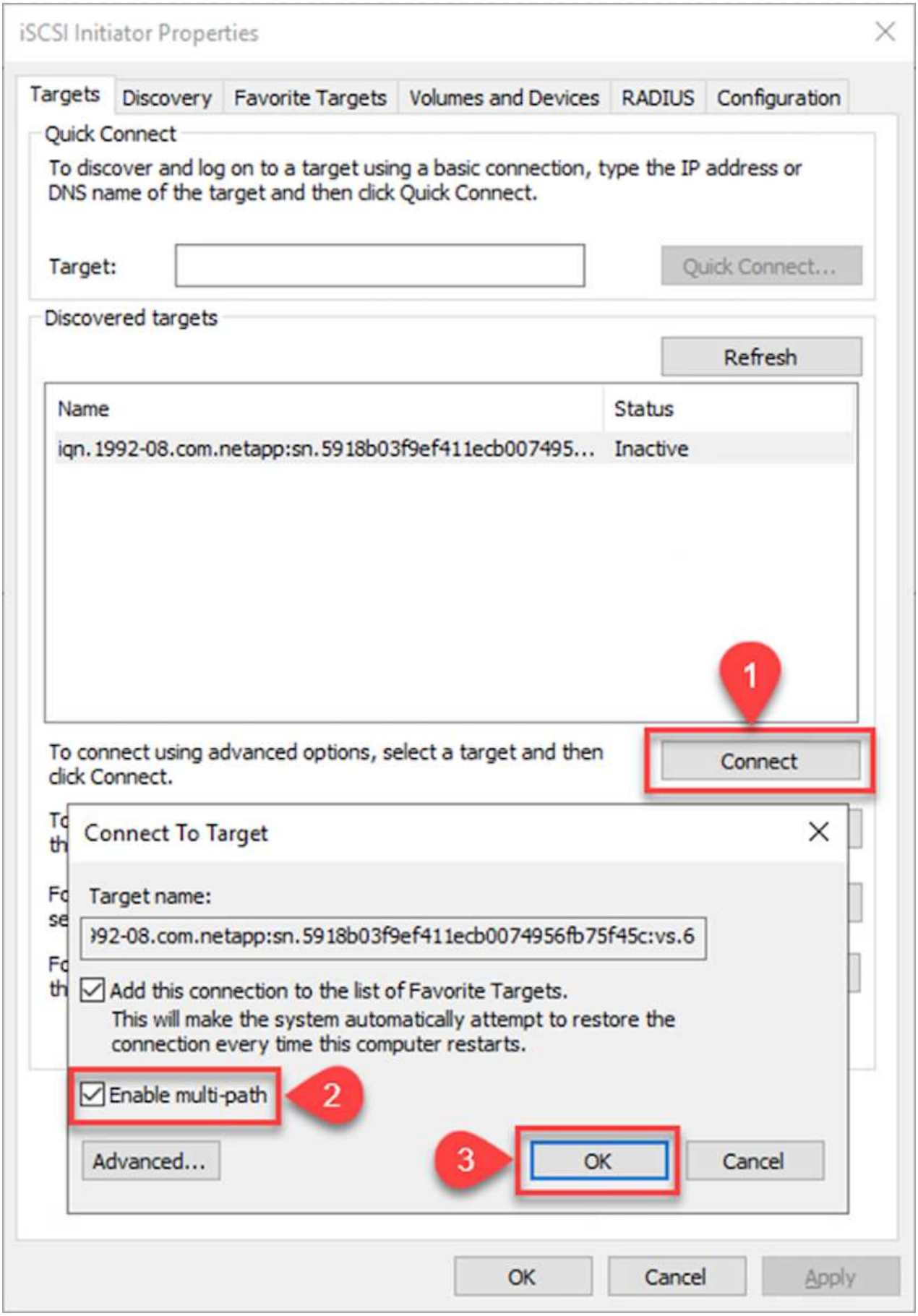


4. Klicken Sie auf der Registerkarte Erkennung auf Portal ermitteln, und geben Sie die IP-Adressen für Ihre FSX-iSCSI-Ziele ein.

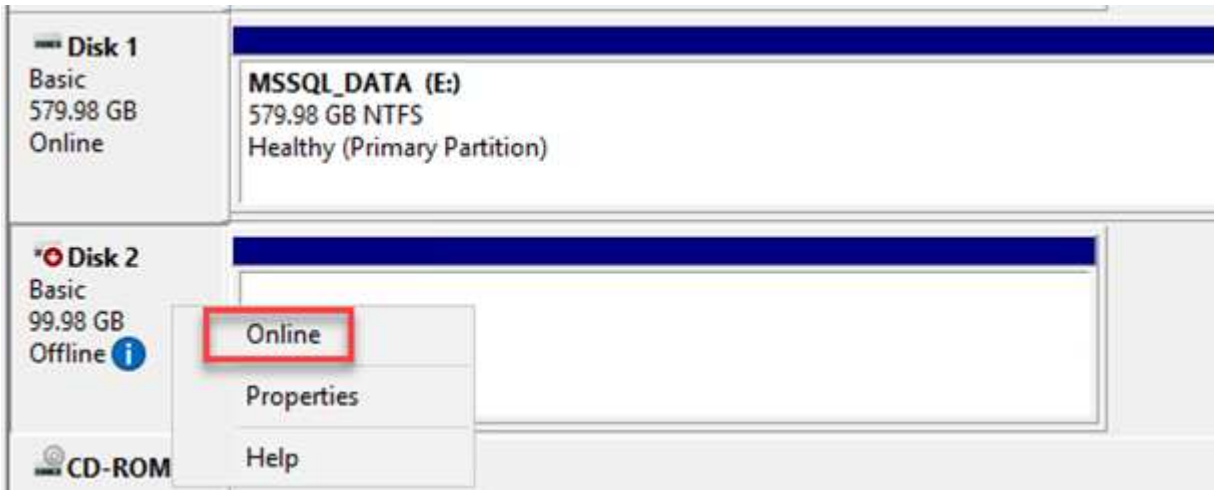




5. Klicken Sie auf der Registerkarte Ziel auf Verbinden, wählen Sie gegebenenfalls Multi-Path aktivieren für Ihre Konfiguration aus, und klicken Sie dann auf OK, um eine Verbindung zum Ziel herzustellen.

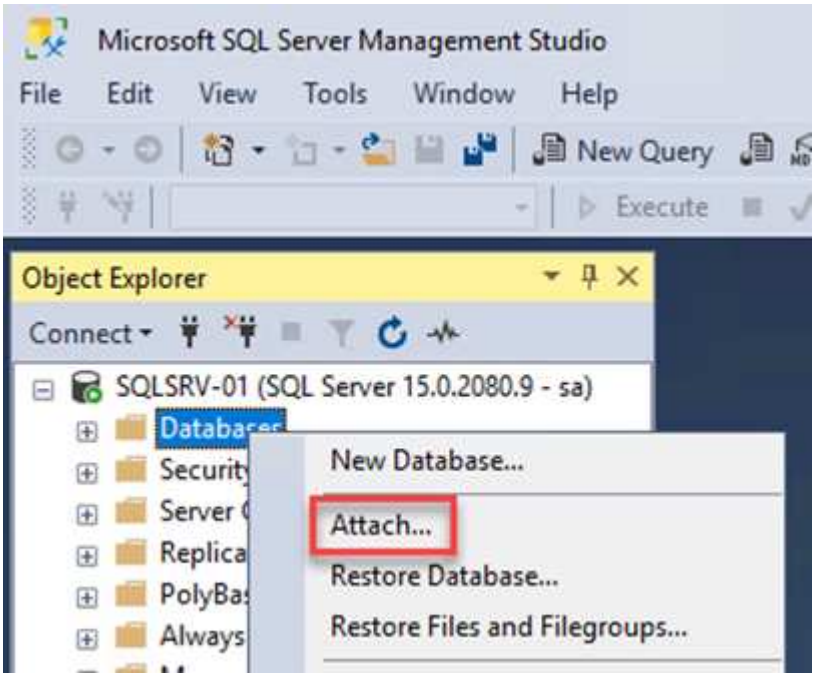

iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
Target:
Quick Connect...
Discovered targets
Refresh
Name
Status
iqn.1992-08.com.netapp:sn.5918b03f9ef411ecb007495...
Inactive
1
To connect using advanced options, select a target and then click Connect.
Connect
Connect To Target
Target name:
92-08.com.netapp:sn.5918b03f9ef411ecb0074956fb75f45c:vs.6
Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.
Enable multi-path
2
Advanced...
3
OK
Cancel
OK
Cancel
Apply

6. Öffnen Sie das Computer Management-Dienstprogramm, und bringen Sie die Laufwerke online. Vergewissern Sie sich, dass sie die gleichen Laufwerksbuchstaben wie zuvor gehalten haben.

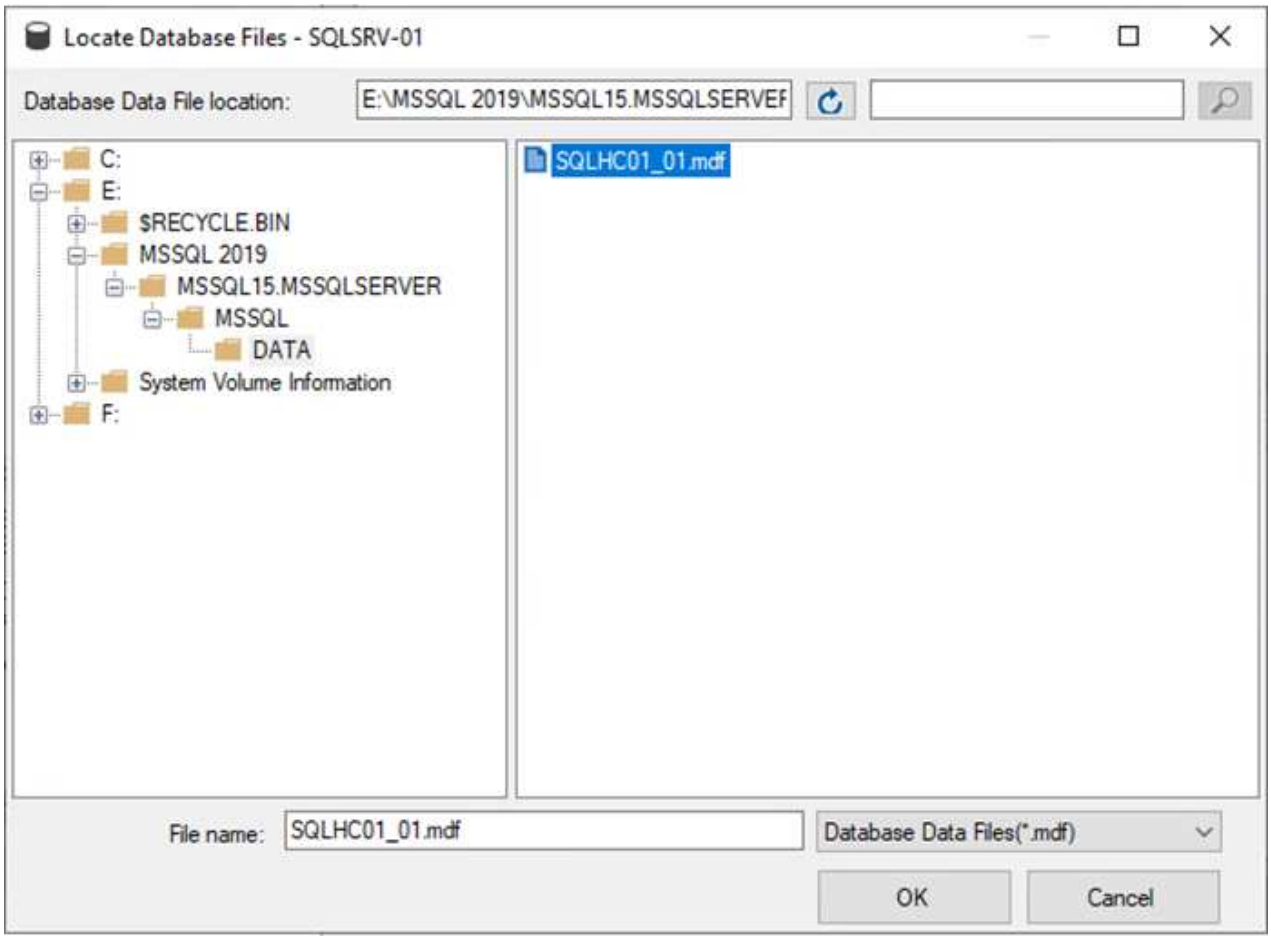


Verbinden Sie die SQL Server-Datenbanken

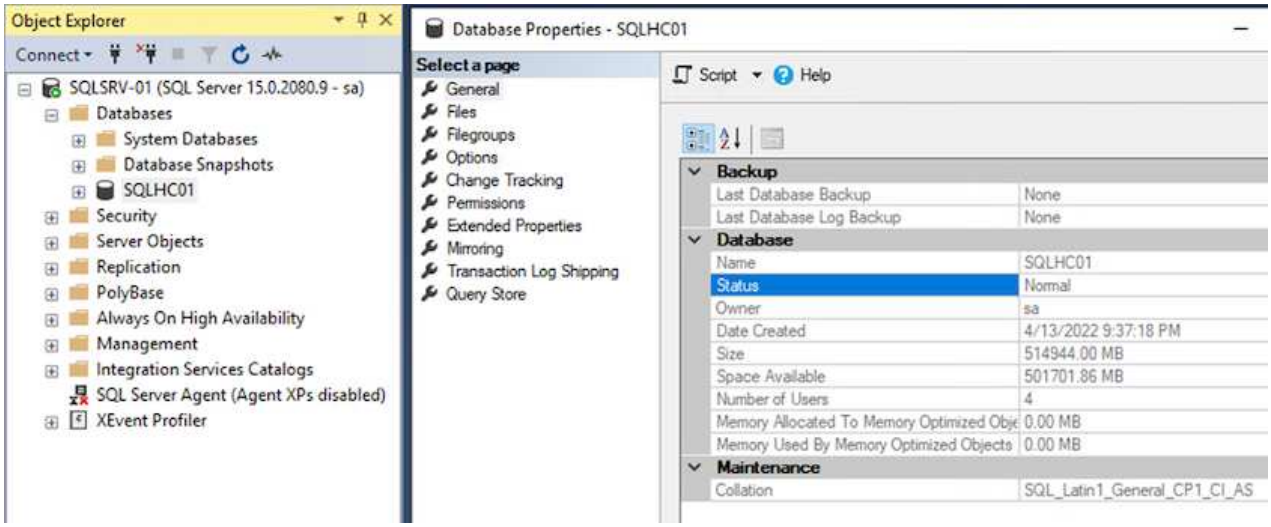
1. Öffnen Sie in der SQL Server VM Microsoft SQL Server Management Studio, und wählen Sie Attach aus, um den Prozess der Verbindung zur Datenbank zu starten.



2. Klicken Sie auf Hinzufügen, und 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.

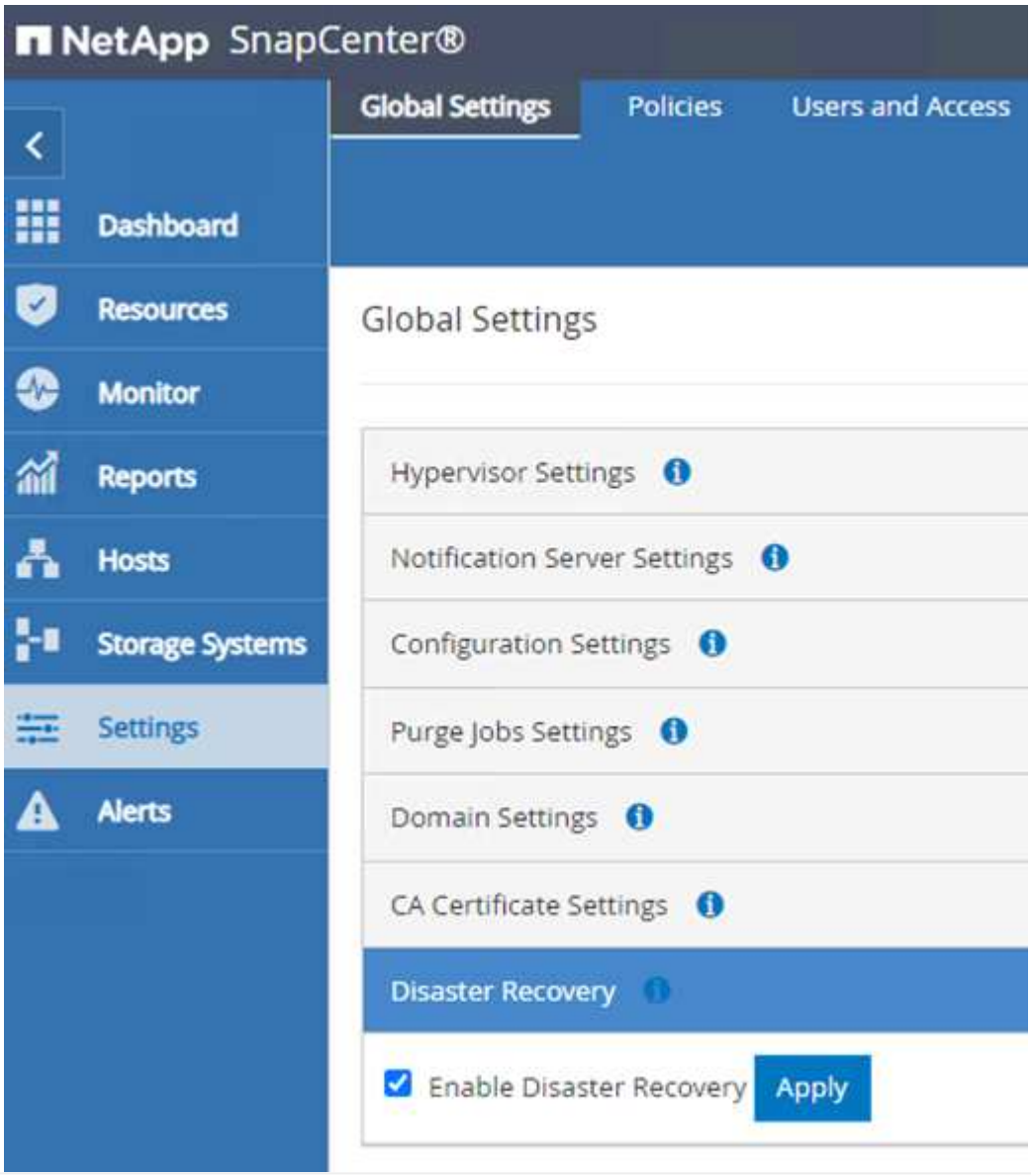


Bestätigen Sie die SnapCenter-Kommunikation mit dem SQL Server-Plug-in

Wenn die SnapCenter Datenbank wieder in den vorherigen Status zurückversetzt wurde, werden die SQL Server Hosts automatisch erneut erkannt. Damit dies korrekt funktioniert, beachten Sie die folgenden Voraussetzungen:

- SnapCenter muss im Disaster Recovery-Modus platziert 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 Datacenter ausgeführt wurde.
- Die ursprüngliche SnapMirror Beziehung muss unterbrochen werden.
- Die LUNs, die die Datenbank enthalten, müssen auf die SQL Server-Instanz und die angehängte Datenbank eingebunden werden.

Um zu überprüfen, ob sich SnapCenter im Disaster Recovery-Modus befindet, navigieren Sie über den SnapCenter Web-Client zu Einstellungen. Wechseln Sie zur Registerkarte Globale Einstellungen und klicken Sie dann auf Disaster Recovery. Stellen Sie sicher, dass das Kontrollkästchen Disaster Recovery aktivieren aktiviert ist.



Stellen Sie Oracle Applikationsdaten wieder her

Das folgende Verfahren enthält Anweisungen zur Wiederherstellung von Oracle Applikationsdaten in VMware Cloud Services in AWS bei einem Ausfall, der den Betrieb des lokalen Standorts erübrigt.

Führen Sie die folgenden Voraussetzungen aus, um mit den Wiederherstellungsschritten fortzufahren:

1. Die Oracle Linux-Server-VM wurde mithilfe von Veeam Full Restore in VMware Cloud SDDC wiederhergestellt.
2. Es wurde ein sekundärer SnapCenter-Server erstellt, und die SnapCenter-Datenbank und -Konfigurationsdateien wurden anhand der in diesem Abschnitt beschriebenen Schritte wiederhergestellt "Zusammenfassung des SnapCenter-Backup- und Restore-Prozesses"

FSX für Oracle Restore konfigurieren – Unterbrechung der SnapMirror Beziehung

Damit die sekundären Storage-Volumes, die auf der FSxN-Instanz gehostet werden, auf die Oracle Server zugreifen können, müssen Sie die bestehende SnapMirror-Beziehung unterbrechen.

1. Nach der Anmeldung bei der FSX-CLI führen Sie den folgenden Befehl aus, um die Volumes anzuzeigen, die nach dem richtigen Namen gefiltert wurden.

```
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::>
```

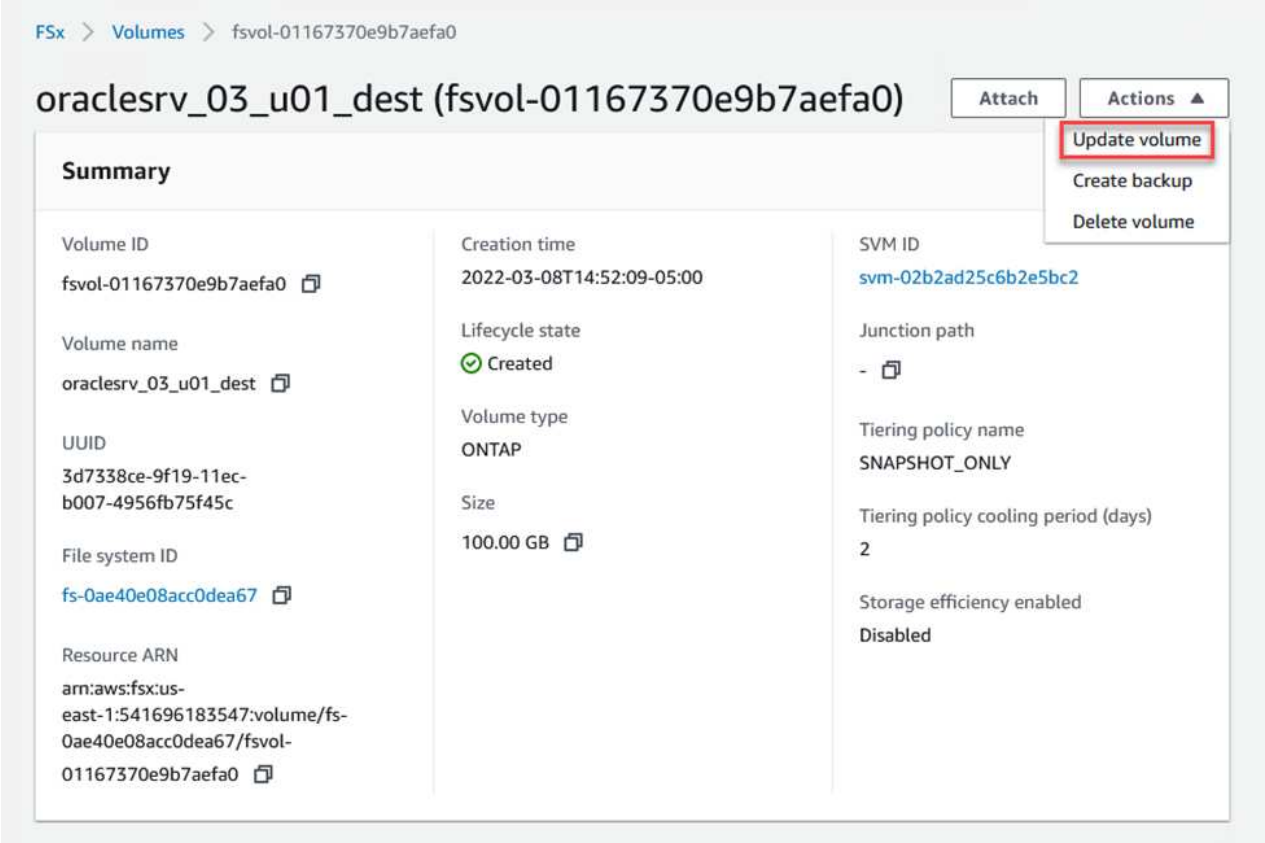
2. Führen Sie den folgenden Befehl aus, um die bestehenden SnapMirror Beziehungen zu unterbrechen.

```
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 Verbindungspfad im Amazon FSX Web-Client:



4. Fügen Sie den Namen des Verbindungspfads 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.

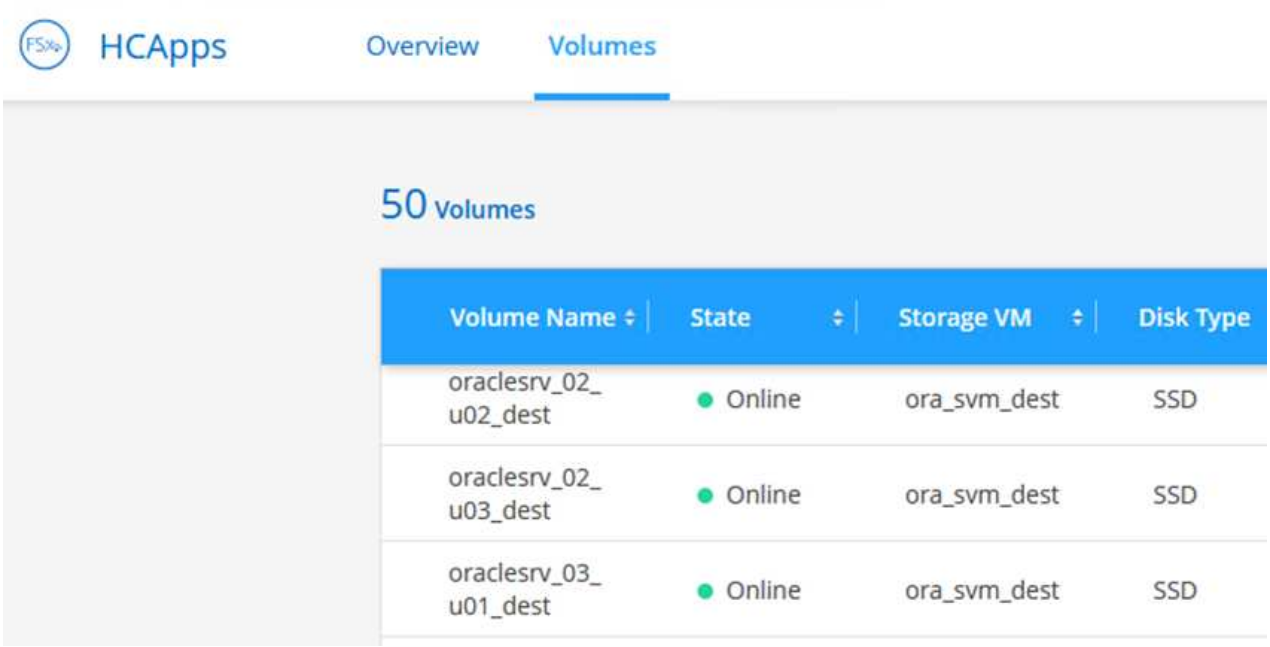
Snapshot Only

Cancel | Update

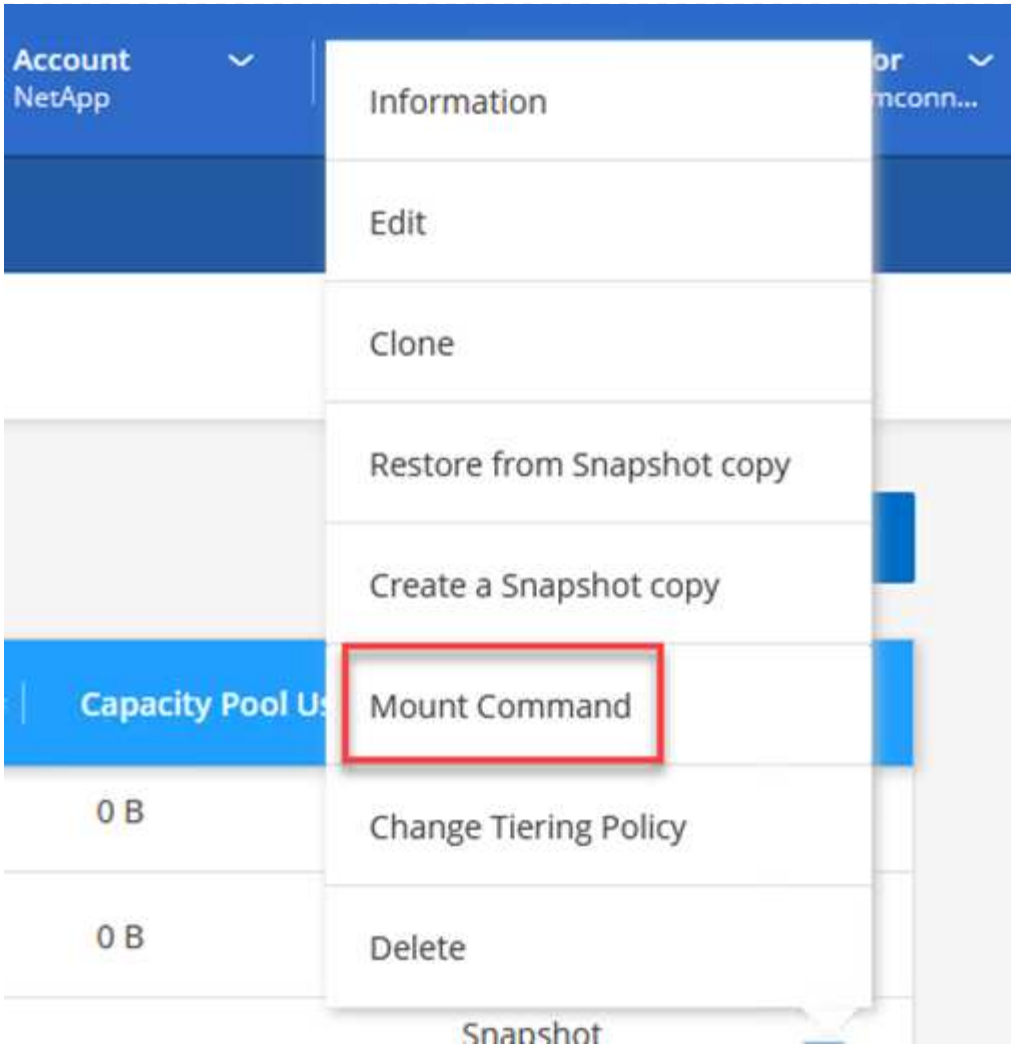
Mounten Sie NFS Volumes auf Oracle Server

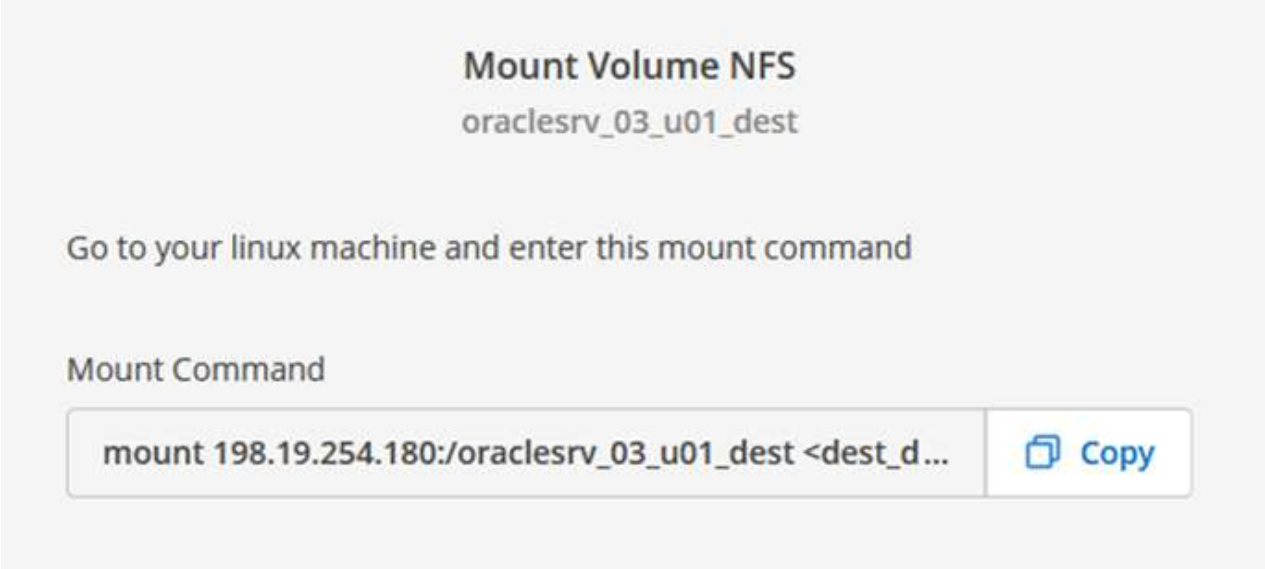
In Cloud Manager erhalten Sie den Mount-Befehl mit der richtigen NFS-LIF-IP-Adresse zum Mounten der NFS-Volumes, die die Oracle-Datenbankdateien und -Protokolle enthalten.

1. Rufen Sie in Cloud Manager die Liste der Volumes für Ihr FSX-Cluster auf.



2. Wählen Sie im Aktivitätsmenü Mount Command 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 Mounten des NFS-Shares sind bereits auf dem Oracle Linux-Host vorhanden.
4. Verwenden Sie auf dem Oracle Linux-Server den Mount-Befehl, um die NFS-Volumes zu mounten.

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

Wiederholen Sie diesen Schritt für jedes mit den Oracle Datenbanken verbundene Volume.

> Um den NFS-Mount beim Neustart persistent zu machen, bearbeiten Sie den `/etc/fstab` Datei zum Einschließen der Mount-Befehle.

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

Failback

Sobald der in dieser Lösung beschriebene Failover-Prozess erfolgreich abgeschlossen ist, setzen SnapCenter und Veeam ihre Backup-Funktionen in AWS wieder ein. FSX für ONTAP ist jetzt als primärer Storage vorgesehen und keine bestehenden SnapMirror Beziehungen zum ursprünglichen lokalen Datacenter vorhanden. Nachdem die normale Funktion wieder aufgenommen wurde, können Daten mit einem Prozess wie in dieser Dokumentation beschrieben in das lokale ONTAP Storage-System gespiegelt werden.

Wie in dieser Dokumentation auch dargestellt, können Sie SnapCenter so konfigurieren, dass die Applikationsdaten-Volumes von FSX für ONTAP auf ein ONTAP Storage-System vor Ort gespiegelt werden. Ähnlich lässt sich Veeam für die Replizierung von Backup-Kopien in Amazon S3 konfigurieren. Dazu wird ein Scale-out-Backup-Repository verwendet, damit diese Backups einem Veeam Backup-Server im lokalen Datacenter zugänglich sind.

Failback liegt außerhalb des Umfangs dieser Dokumentation, aber Failback unterscheidet sich wenig von dem hier beschriebenen Prozess.

Schlussfolgerung

Der in dieser Dokumentation vorgestellte Anwendungsfall konzentriert sich auf bewährte Disaster-Recovery-Technologien, die die Integration von NetApp und VMware hervorheben. NetApp ONTAP Storage-Systeme bieten bewährte Technologien zur Datenspiegelung. Damit können Unternehmen Disaster-Recovery-Lösungen entwerfen, die sich sowohl vor Ort als auch ONTAP Technologien in Verbindung mit den führenden Cloud-Providern befinden.

FSX für ONTAP auf AWS ermöglicht eine nahtlose Integration in SnapCenter und SyncMirror zur Replizierung von Applikationsdaten in die Cloud. Veeam Backup & Replication ist eine weitere bekannte Technologie, die sich gut in NetApp ONTAP Storage-Systeme integrieren lässt und Failover auf nativen vSphere Storage bietet.

Diese Lösung stellte eine Disaster-Recovery-Lösung dar, bei der Storage von einem ONTAP-System, das SQL Server und Oracle-Applikationsdaten hostet, verwendet wurde. SnapCenter mit SnapMirror ist eine benutzerfreundliche Lösung für den Schutz von Applikations-Volumes auf ONTAP Systemen und die Replizierung auf FSX oder CVO in der Cloud. SnapCenter ist eine DR-fähige Lösung für den Failover aller Applikationsdaten zu VMware Cloud auf AWS.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Links zur Lösungsdokumentation

"NetApp Hybrid-Multi-Cloud mit VMware Lösungen"

"NetApp Lösungen"

Veeam Backup & Restore in VMware Cloud mit Amazon FSX for ONTAP

Autor: Josh Powell – NetApp Solutions Engineering

Überblick

Veeam Backup & Replication ist eine effektive und zuverlässige Lösung für den Schutz von Daten in der VMware Cloud. Diese Lösung zeigt die ordnungsgemäße Einrichtung und Konfiguration für den Einsatz von Veeam Backup and Replication für das Backup und die Wiederherstellung von Applikations-VMs auf FSX für ONTAP-NFS-Datastores in VMware Cloud.

VMware Cloud (in AWS) unterstützt die Verwendung von NFS-Datastores als ergänzenden Storage und FSX für NetApp ONTAP ist eine sichere Lösung für Kunden, die große Datenmengen für ihre Cloud-Applikationen speichern müssen, die unabhängig von der Anzahl der ESXi-Hosts im SDDC-Cluster skalierbar sind. Dieser integrierte AWS Storage-Service bietet hocheffizienten Storage mit allen herkömmlichen NetApp ONTAP Funktionen.

Anwendungsfälle

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Backup und Restore von Windows und Linux Virtual Machines, die in VMC gehostet werden, mithilfe von FSX für NetApp ONTAP als Backup-Repository
- Backup und Restore von Applikationsdaten von Microsoft SQL Server mithilfe von FSX für NetApp ONTAP als Backup-Repository.
- Backup und Restore von Oracle Applikationsdaten mit FSX für NetApp ONTAP als Backup-Repository.

NFS-Datastores mit Amazon FSX for ONTAP

Alle Virtual Machines in dieser Lösung befinden sich in ergänzenden NFS-Datastores für FSX for ONTAP. Die Verwendung von FSX for ONTAP als ergänzender NFS-Datastore bringt mehrere Vorteile mit sich. Sie können beispielsweise:

- Erstellen Sie ein skalierbares und hochverfügbares Filesystem in der Cloud, ohne dass aufwändige Einrichtung und Verwaltung erforderlich sind.
- Die Integration in Ihre bestehende VMware-Umgebung ermöglicht Ihnen, vertraute Tools und Prozesse für das Management Ihrer Cloud-Ressourcen zu verwenden.
- ONTAP bietet erweiterte Datenmanagementfunktionen wie Snapshots und Replizierung, die zur Sicherung und Verfügbarkeit der Daten genutzt werden können.

Übersicht Zur Lösungsimplementierung

Diese Liste enthält die allgemeinen Schritte, die erforderlich sind, um Veeam Backup & Replication zu konfigurieren, Backup- und Restore-Jobs mithilfe von FSX für ONTAP als Backup-Repository auszuführen und Restores von SQL Server- und Oracle-VMs und -Datenbanken durchzuführen:

1. Das FSX für ONTAP-Dateisystem erstellen, das als iSCSI-Backup-Repository für Veeam Backup & Replication verwendet werden kann
2. Einsatz von Veeam Proxy zur Verteilung von Backup-Workloads und zum Mounten von iSCSI-Backup-Repositorys auf FSX für ONTAP
3. Konfigurieren Sie Veeam Backup Jobs für die Sicherung virtueller SQL Server-, Oracle-, Linux- und Windows-Maschinen.
4. Stellen Sie Virtual Machines und einzelne Datenbanken von SQL Server wieder her.
5. Stellen Sie Oracle Virtual Machines und individuelle Datenbanken wieder her.

Voraussetzungen

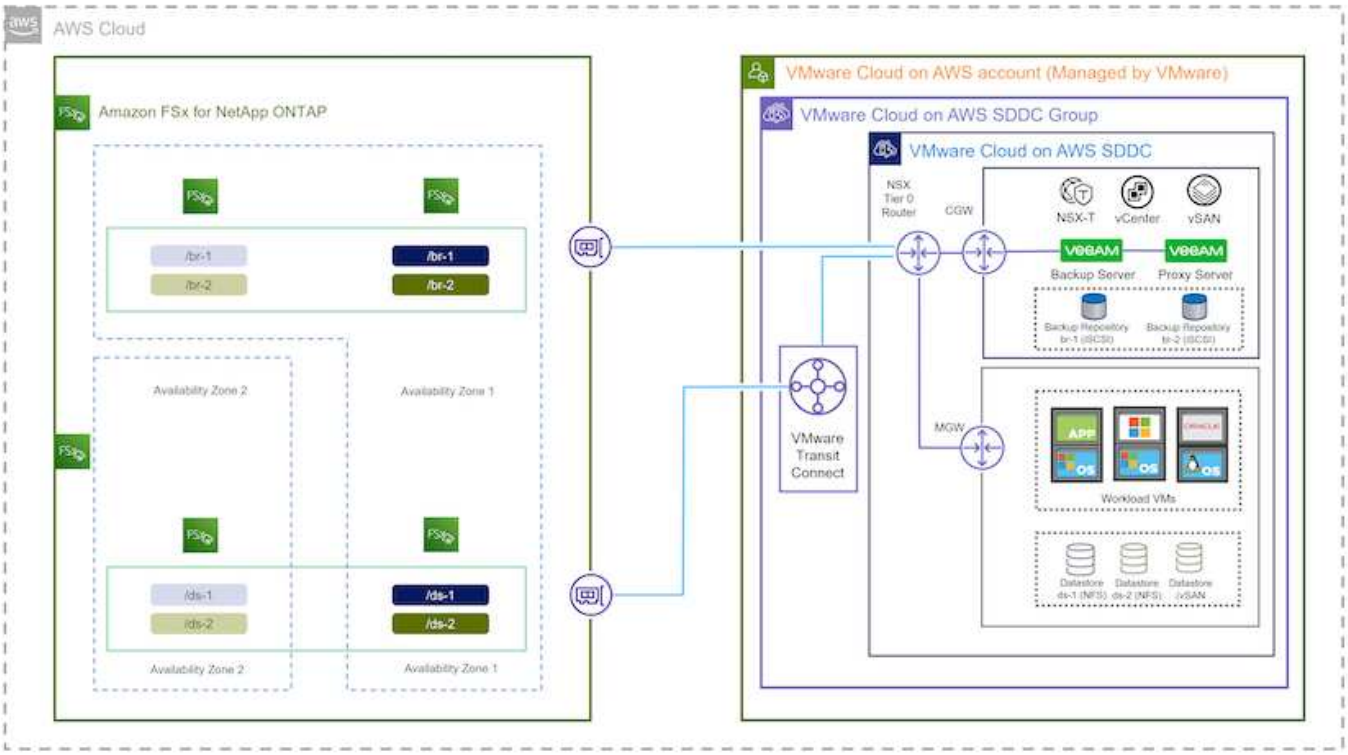
Der Zweck dieser Lösung besteht darin, die Datensicherung von Virtual Machines zu demonstrieren, die in der VMware Cloud ausgeführt werden und sich in NFS-Datenspeichern befinden, die von FSX for NetApp ONTAP gehostet werden. Bei dieser Lösung wird vorausgesetzt, dass die folgenden Komponenten konfiguriert und einsatzbereit sind:

1. FSX für ONTAP-Dateisystem mit einem oder mehreren NFS-Datastores verbunden mit VMware-Cloud.
2. Microsoft Windows Server VM mit installierter Veeam Backup & Replication Software
   - Der vCenter-Server wurde vom Veeam Backup & Replication-Server unter Verwendung seiner IP-Adresse oder eines vollständig qualifizierten Domänennamens erkannt.
3. Microsoft Windows Server VM, die während der Lösungsbereitstellung mit Veeam Backup Proxy-Komponenten installiert werden soll.
4. Microsoft SQL Server VMs mit VMDKs und Applikationsdaten auf FSX für ONTAP NFS-Datastores. Für diese Lösung hatten wir zwei SQL-Datenbanken auf zwei separaten VMDKs.
   - Hinweis: Als Best Practice werden Datenbank- und Transaktions-Log-Dateien auf separaten Laufwerken platziert, da dies die Performance und Zuverlässigkeit verbessert. Dies liegt zum Teil daran, dass Transaktions-Logs sequenziell geschrieben werden, während Datenbankdateien zufällig geschrieben werden.
5. Oracle Database VMs mit VMDKs und Applikationsdaten auf FSX für ONTAP NFS-Datastores.
6. Linux- und Windows-File-Server-VMs mit VMDKs, die auf FSX für ONTAP-NFS-Datastores liegen.
7. Veeam benötigt spezielle TCP Ports für die Kommunikation zwischen Servern und den Komponenten in der Backup-Umgebung. Auf den Komponenten der Veeam Backup-Infrastruktur werden automatisch die erforderlichen Firewall-Regeln erstellt. Eine vollständige Liste der Anforderungen an den Netzwerkport finden Sie im Abschnitt Ports des "Veeam Backup and Replication User Guide for VMware vSphere".

Übergeordnete Architektur

Die Test-/Validierung dieser Lösung wurde in einem Labor durchgeführt, das in der endgültigen Implementierungsumgebung eventuell nicht übereinstimmt. Weitere Informationen finden Sie in den folgenden

Abschnitten.



Hardware-/Software-Komponenten

Der Zweck dieser Lösung besteht darin, die Datensicherung von Virtual Machines zu demonstrieren, die in der VMware Cloud ausgeführt werden und sich in NFS-Datenspeichern befinden, die von FSX for NetApp ONTAP gehostet werden. Bei dieser Lösung wird davon ausgegangen, dass die folgenden Komponenten bereits konfiguriert und einsatzbereit sind:

- Microsoft Windows VMs auf einem FSX für ONTAP NFS Datastore
- Linux (CentOS) VMs auf einem FSX für ONTAP NFS-Datenspeicher
- Microsoft SQL Server VMs auf einem FSX für ONTAP NFS-Datastore
  - Zwei Datenbanken, die auf separaten VMDKs gehostet werden
- Oracle VMs auf einem FSX für ONTAP-NFS-Datastore

Lösungsimplementierung

In dieser Lösung stellen wir detaillierte Anweisungen für die Implementierung und Validierung einer Lösung bereit, die Veeam Backup and Replication verwendet, um Backup und Recovery von virtuellen File-Server-Maschinen mit SQL Server, Oracle und Windows und Linux in einem VMware Cloud SDDC on AWS durchzuführen. Die Virtual Machines in dieser Lösung befinden sich in einem ergänzenden NFS-Datastore, der von FSX for ONTAP gehostet wird. Darüber hinaus wird ein separates Filesystem für FSX für ONTAP verwendet, um iSCSI-Volumes zu hosten, die für Veeam Backup-Repositorys verwendet werden.

Wir werden FSX für die Erstellung von ONTAP-Dateisystemen durchgehen, iSCSI-Volumes für die Verwendung als Backup-Repositorys mounten, Backup-Jobs erstellen und ausführen und VM- und Datenbank-Restores durchführen.

Nähere Informationen zu FSX für NetApp ONTAP finden Sie im "FSX for ONTAP Benutzerhandbuch".

Detaillierte Informationen zu Veeam Backup and Replication finden Sie im "Technische Dokumentation Des Veeam Help Center" Standort.

Hinweise zu Überlegungen und Einschränkungen bei der Verwendung von Veeam Backup and Replication mit VMware Cloud on AWS finden Sie unter "VMware Cloud on AWS und VMware Cloud on Dell EMC Support. Überlegungen und Einschränkungen".

Implementieren des Veeam Proxy-Servers

Ein Veeam-Proxyserver ist eine Komponente der Veeam Backup & Replication-Software, die als Vermittler zwischen der Quelle und dem Backup- oder Replikationsziel fungiert. Der Proxy-Server hilft bei der Optimierung und Beschleunigung der Datenübertragung während von Backup-Jobs durch lokale Verarbeitung von Daten und kann verschiedene Transportmodi nutzen, um über VMware vStorage APIs for Data Protection oder über direkten Speicherzugriff auf Daten zuzugreifen.

Bei der Auswahl eines Veeam Proxy-Server-Designs müssen die Anzahl der gleichzeitigen Aufgaben und der gewünschte Transportmodus oder die Art des Storage-Zugriffs berücksichtigt werden.

Informationen zur Dimensionierung der Anzahl von Proxy-Servern und zu deren Systemanforderungen finden Sie im "Veeam VMware vSphere Best Practice Guide".

Der Veeam Data Mover ist eine Komponente des Veeam Proxy Servers und verwendet einen Transport Mode als Methode, um VM-Daten von der Quelle zu erhalten und an das Ziel zu übertragen. Der Transportmodus wird während der Konfiguration des Backup-Jobs festgelegt. Mithilfe des direkten Storage-Zugriffs ist es möglich, die Effizienz von Backups von NFS-Datenspeichern zu erhöhen.

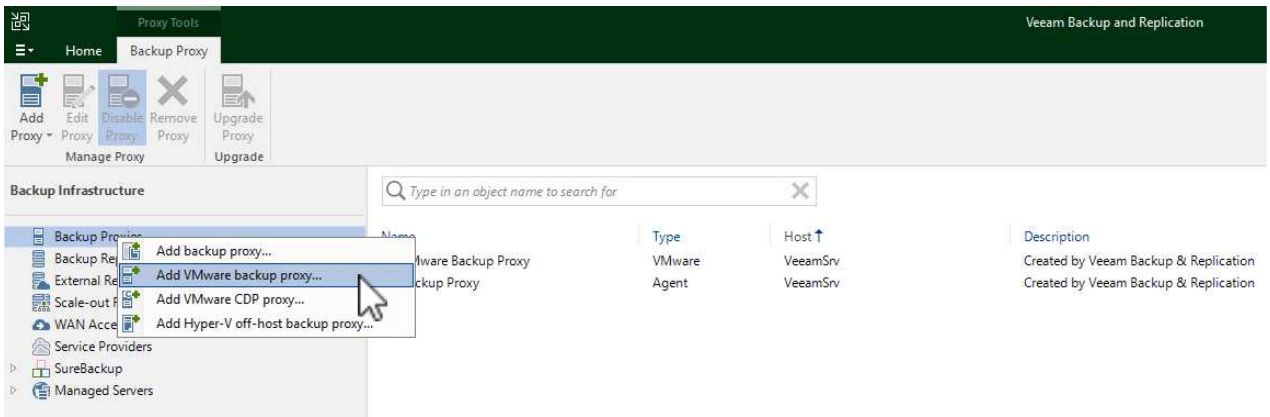
Weitere Informationen zu den Transportmodi finden Sie im "Veeam Backup and Replication User Guide for VMware vSphere".

Im folgenden Schritt behandeln wir die Bereitstellung des Veeam Proxy Servers auf einer Windows VM im VMware Cloud SDDC.

Implementieren Sie Veeam Proxy für die Verteilung von Backup-Workloads

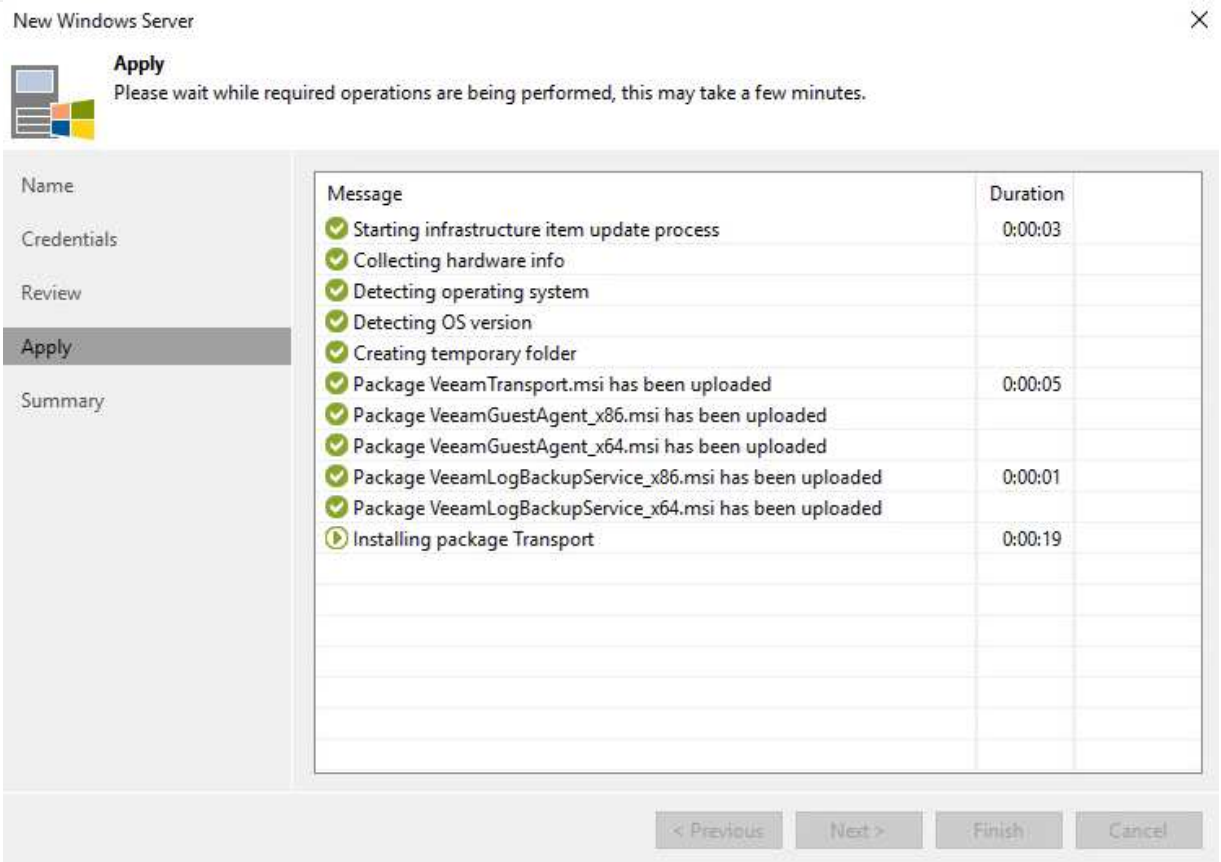
In diesem Schritt wird der Veeam Proxy auf einer vorhandenen Windows-VM bereitgestellt. So können Backup-Jobs zwischen dem primären Veeam Backup-Server und dem Veeam Proxy verteilt werden.

1. Öffnen Sie auf dem Veeam Backup and Replication Server die Administrationskonsole und wählen Sie im unteren linken Menü **Backup Infrastructure** aus.
2. Klicken Sie mit der rechten Maustaste auf **Backup-Proxies** und klicken Sie auf **Add VMware Backup Proxy…**, um den Assistenten zu öffnen.

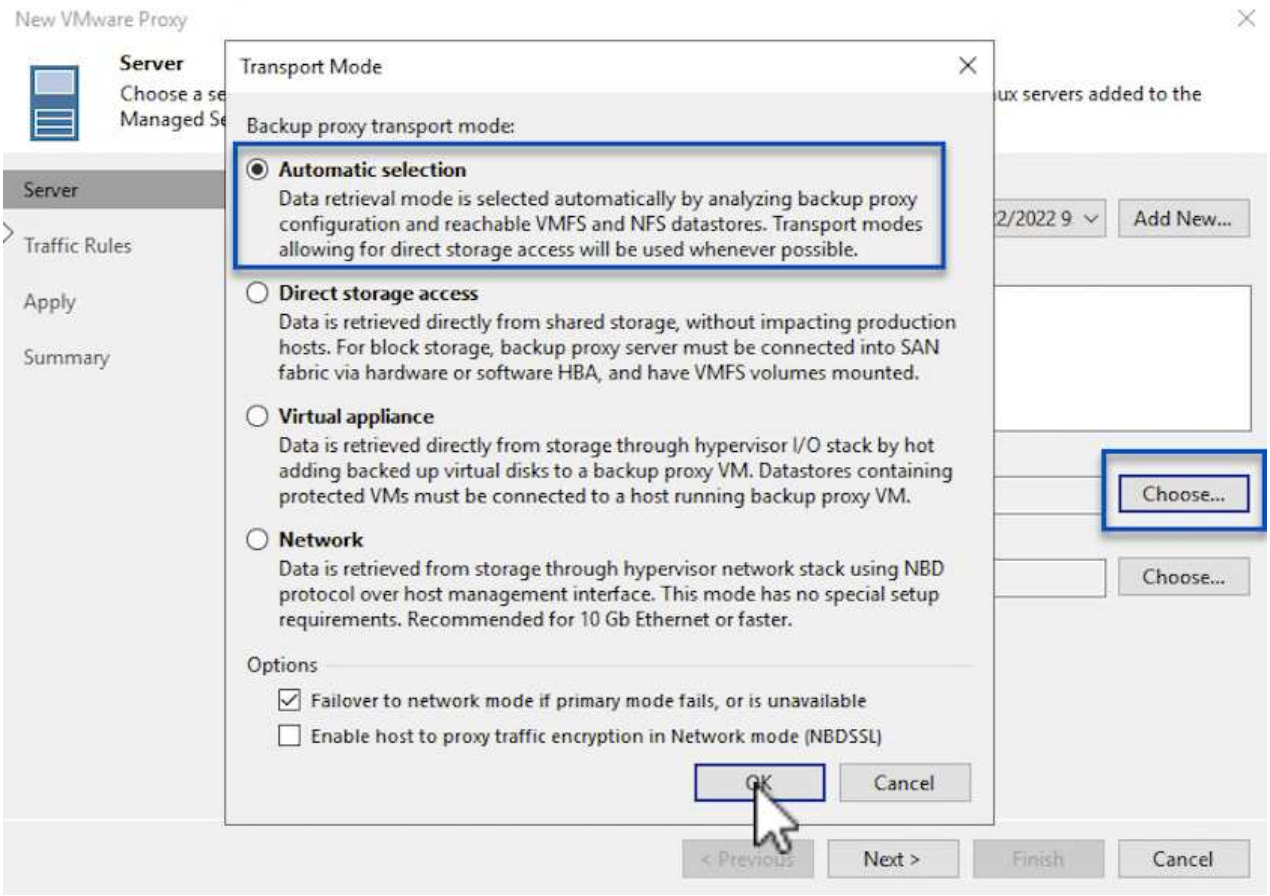


3. Klicken Sie im **Add VMware Proxy** Wizard auf die Schaltfläche **Add New…**, um einen neuen Proxyserver hinzuzufügen.

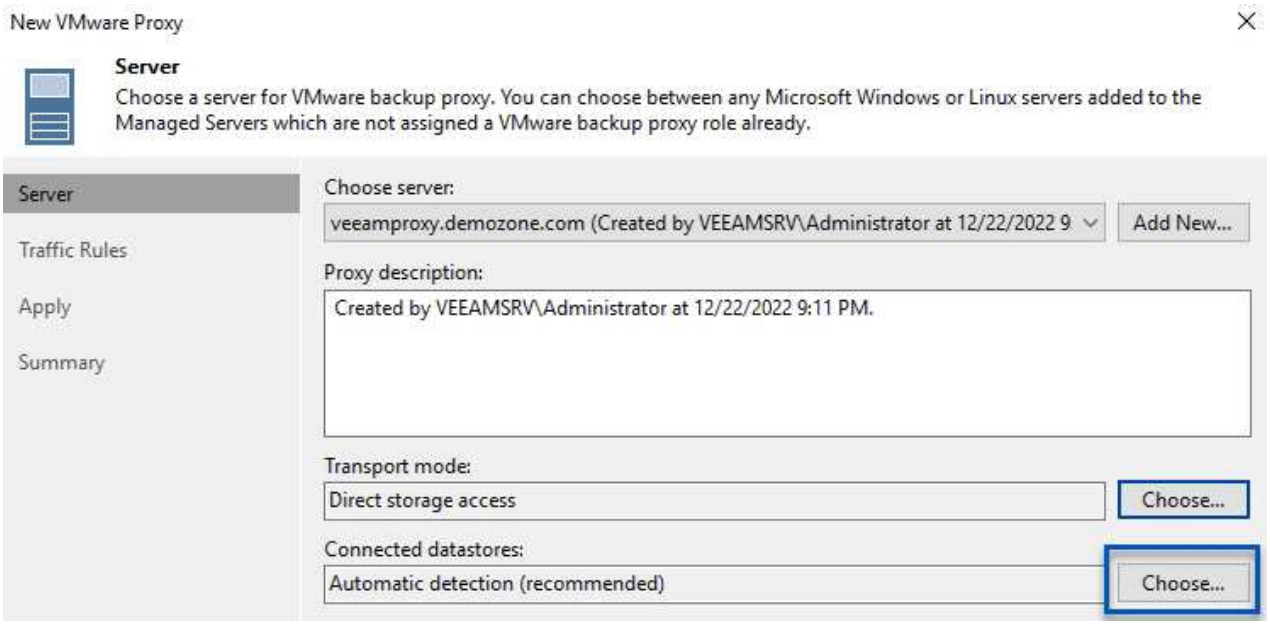
4. Wählen Sie diese Option, um Microsoft Windows hinzuzufügen, und befolgen Sie die Anweisungen zum Hinzufügen des Servers:
   - Geben Sie den DNS-Namen oder die IP-Adresse ein
   - Wählen Sie ein Konto aus, das für Anmeldeinformationen auf dem neuen System verwendet werden soll, oder fügen Sie neue Anmeldeinformationen hinzu
   - Überprüfen Sie die zu installierenden Komponenten und klicken Sie dann auf **Apply**, um die Bereitstellung zu starten

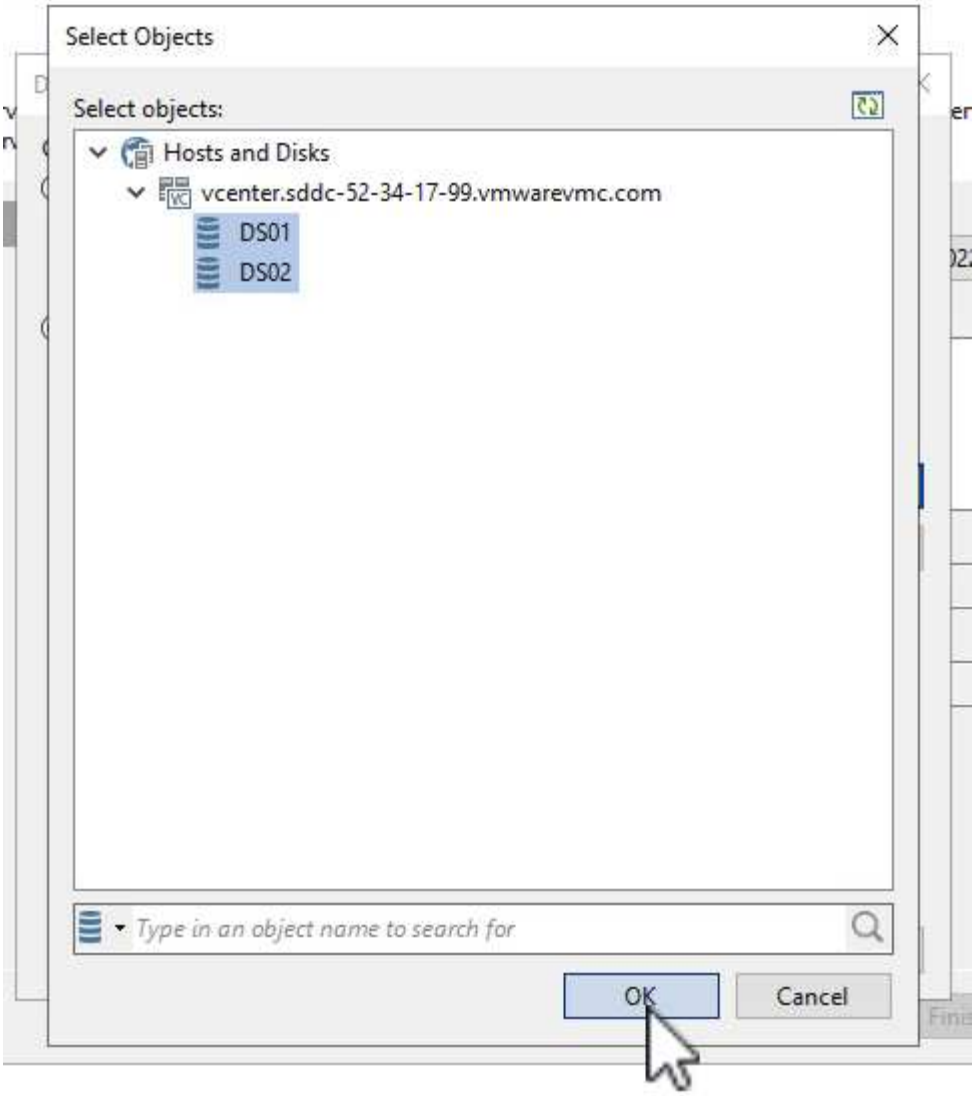


5. Wählen Sie im Assistenten **New VMware Proxy** einen Transportmodus aus. In unserem Fall haben wir uns für **Automatische Auswahl** entschieden.

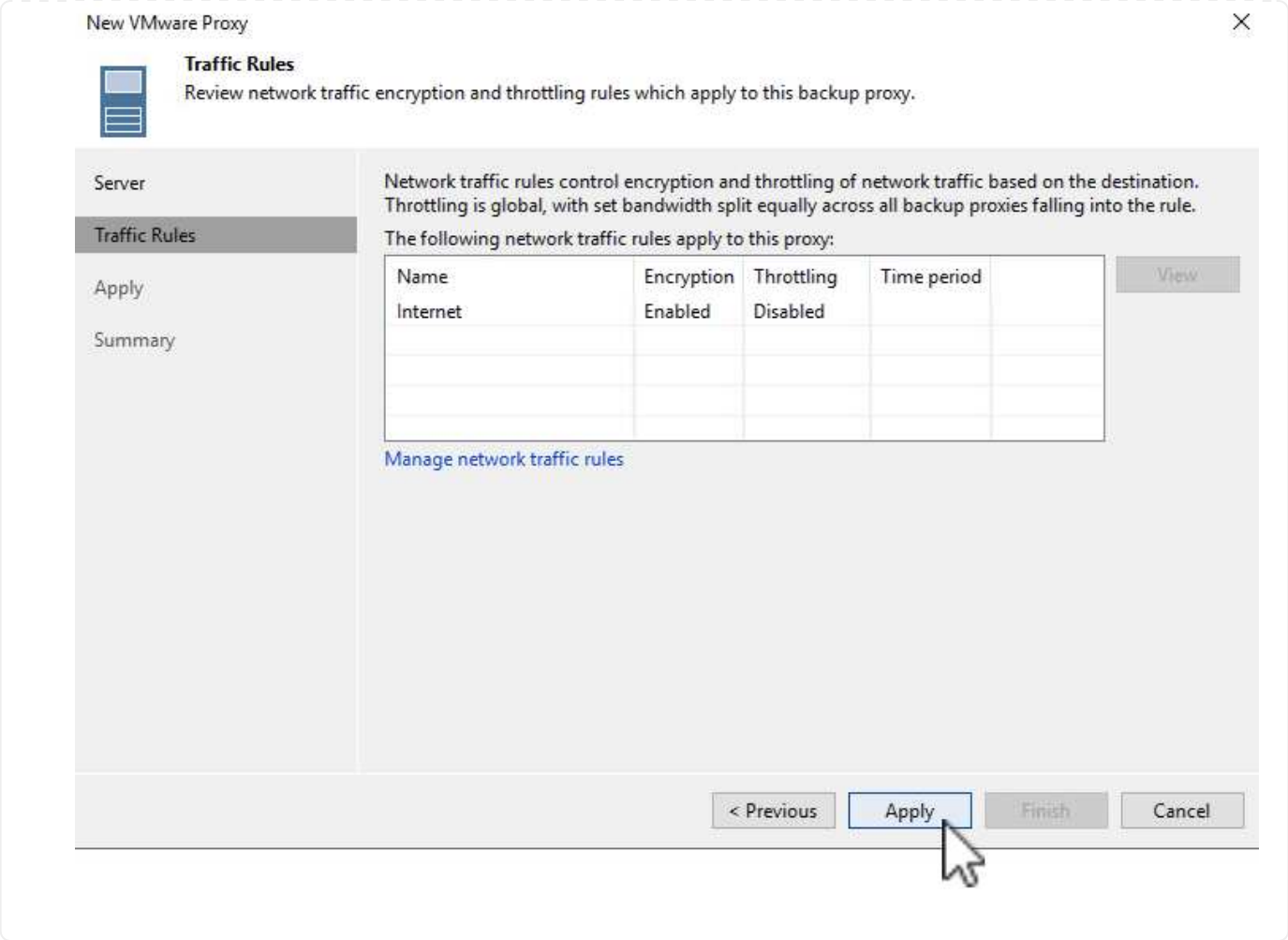


6. Wählen Sie die verbundenen Datastores aus, auf die der VMware Proxy direkten Zugriff haben soll.





7. Konfigurieren und wenden Sie alle gewünschten Regeln für den Netzwerkverkehr an, z. B. Verschlüsselung oder Drosselung. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche **Anwenden**, um die Bereitstellung abzuschließen.



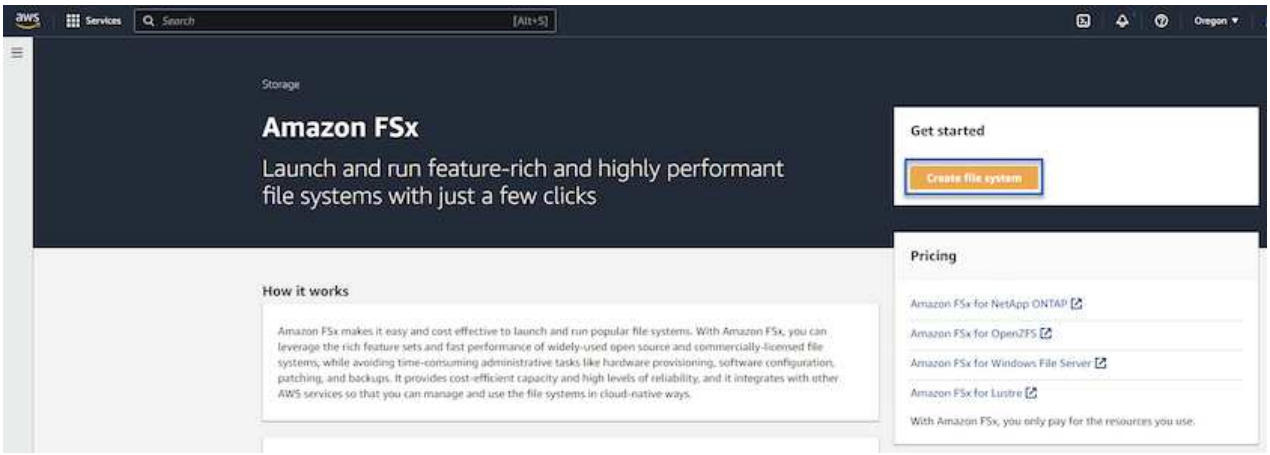
Konfiguration von Storage- und Backup-Repositorys

Der primäre Veeam Backup-Server und der Veeam Proxy-Server haben Zugriff auf ein Backup-Repository in Form eines direkt verbundenen Speichers. In diesem Abschnitt werden die Erstellung eines FSX für ONTAP-Dateisystems, das Mounten von iSCSI-LUNs auf den Veeam-Servern und die Erstellung von Backup-Repositorys behandelt.

Erstellen Sie FSX für ONTAP-Dateisystem

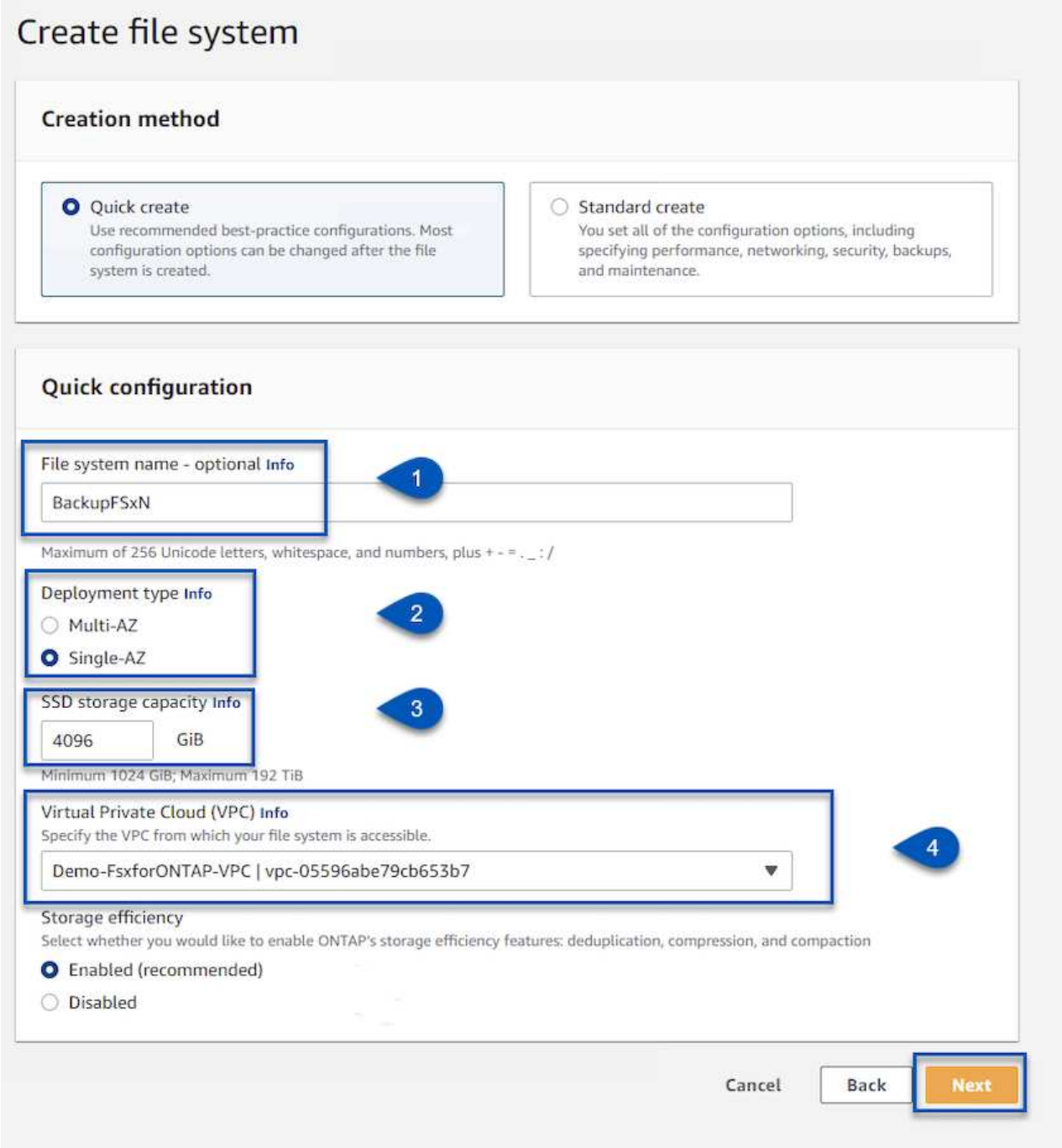
Erstellen Sie ein FSX für ONTAP-Dateisystem, das zum Hosten der iSCSI-Volumes für die Veeam Backup-Repositorys verwendet wird.

1. Gehen Sie in der AWS-Konsole zu FSX und dann zu **Dateisystem erstellen**



2. Wählen Sie **Amazon FSX for NetApp ONTAP** und dann **Weiter**, um fortzufahren.

3. Geben Sie den Namen des Filesystems, den Implementierungstyp, die SSD-Storage-Kapazität und die VPC ein, in der sich das FSX für das ONTAP-Cluster befinden soll. Bei dieser VPC muss die Kommunikation mit dem Virtual Machine-Netzwerk in VMware Cloud erfolgen. Klicken Sie auf **Weiter**.



4. Überprüfen Sie die Bereitstellungsschritte und klicken Sie auf **Dateisystem erstellen**, um den Dateisystemerstellungsprozess zu starten.

Konfigurieren und Mounten von iSCSI-LUNs

Erstellen und konfigurieren Sie die iSCSI-LUNs auf FSX für ONTAP und mounten Sie sie auf den Veeam Backup- und Proxy-Servern. Diese LUNs werden später zur Erstellung von Veeam Backup-Repositorys verwendet.

> Das Erstellen einer iSCSI-LUN auf FSX für ONTAP ist ein mehrstufiger Prozess. Der erste Schritt zur Erstellung der Volumes kann über die Amazon FSX-Konsole oder über die NetApp ONTAP-CLI durchgeführt werden.

> Weitere Informationen zur Verwendung von FSX für ONTAP finden Sie im "FSX for ONTAP Benutzerhandbuch".

1. Erstellen Sie über die NetApp ONTAP CLI die anfänglichen Volumes mit dem folgenden Befehl:

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. Erstellen Sie LUNs mithilfe der Volumes, die im vorherigen Schritt erstellt wurden:

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Gewähren Sie Zugriff auf die LUNs, indem Sie eine Initiatorgruppe erstellen, die den iSCSI-IQN der Veeam Backup- und Proxyserver enthält:

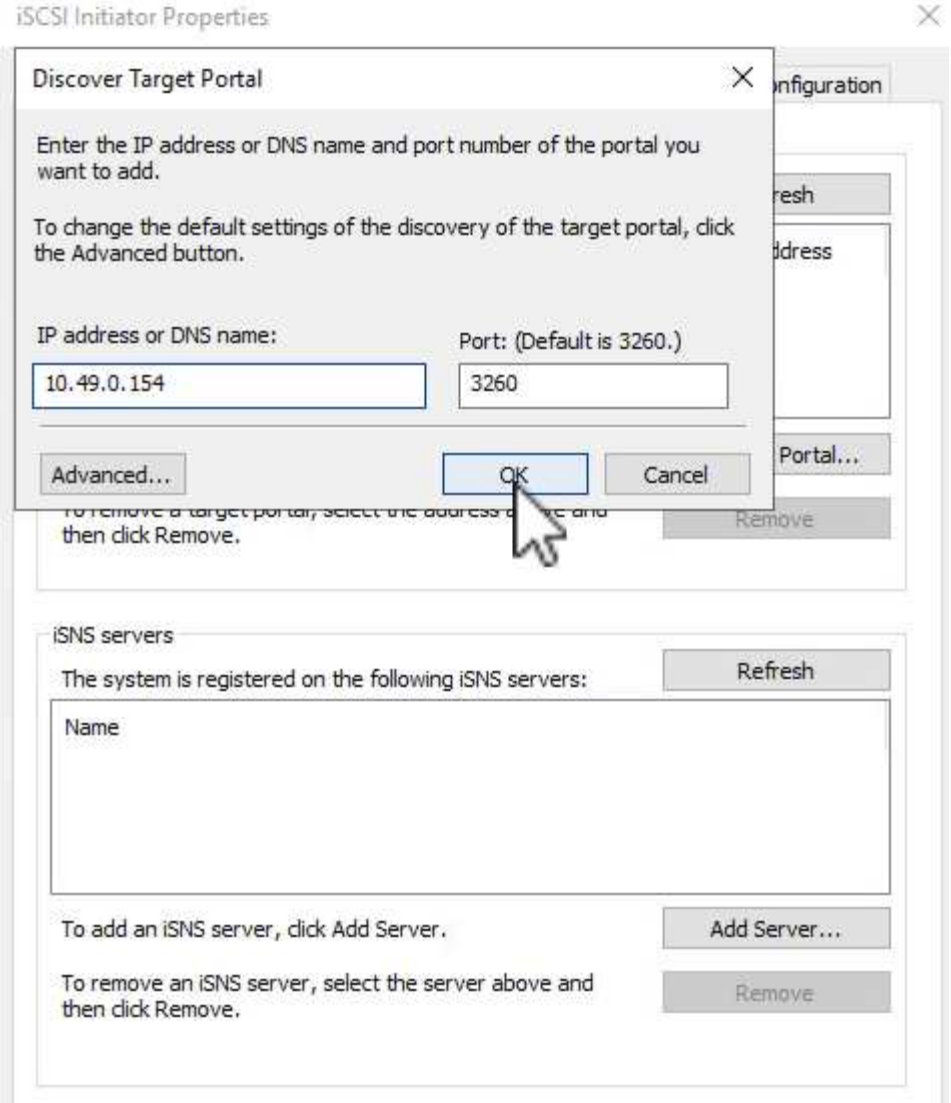
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

> Um den vorherigen Schritt abzuschließen, müssen Sie zuerst den IQN aus den iSCSI-Initiatoreigenschaften auf den Windows-Servern abrufen.

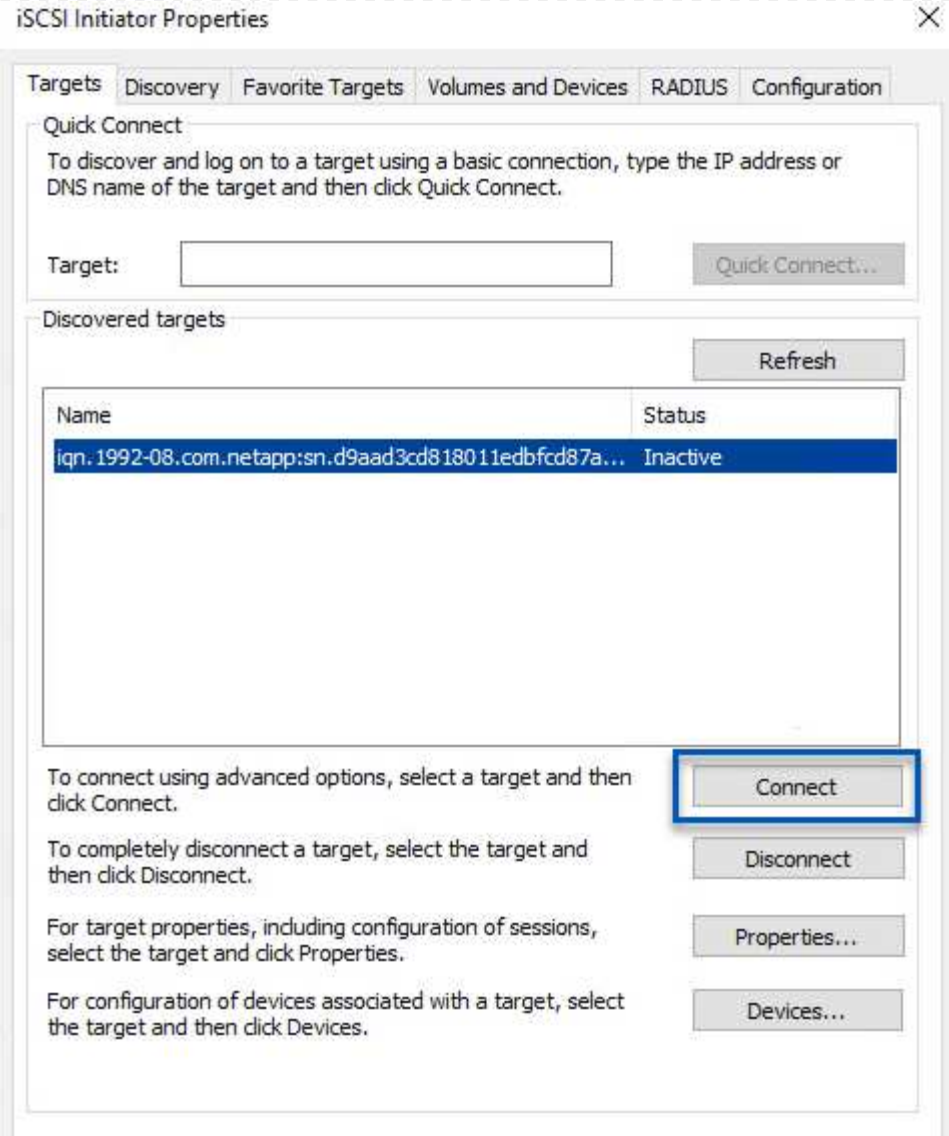
4. Schließlich ordnen Sie die LUNs der Initiatorgruppe zu, die Sie gerade erstellt haben:

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

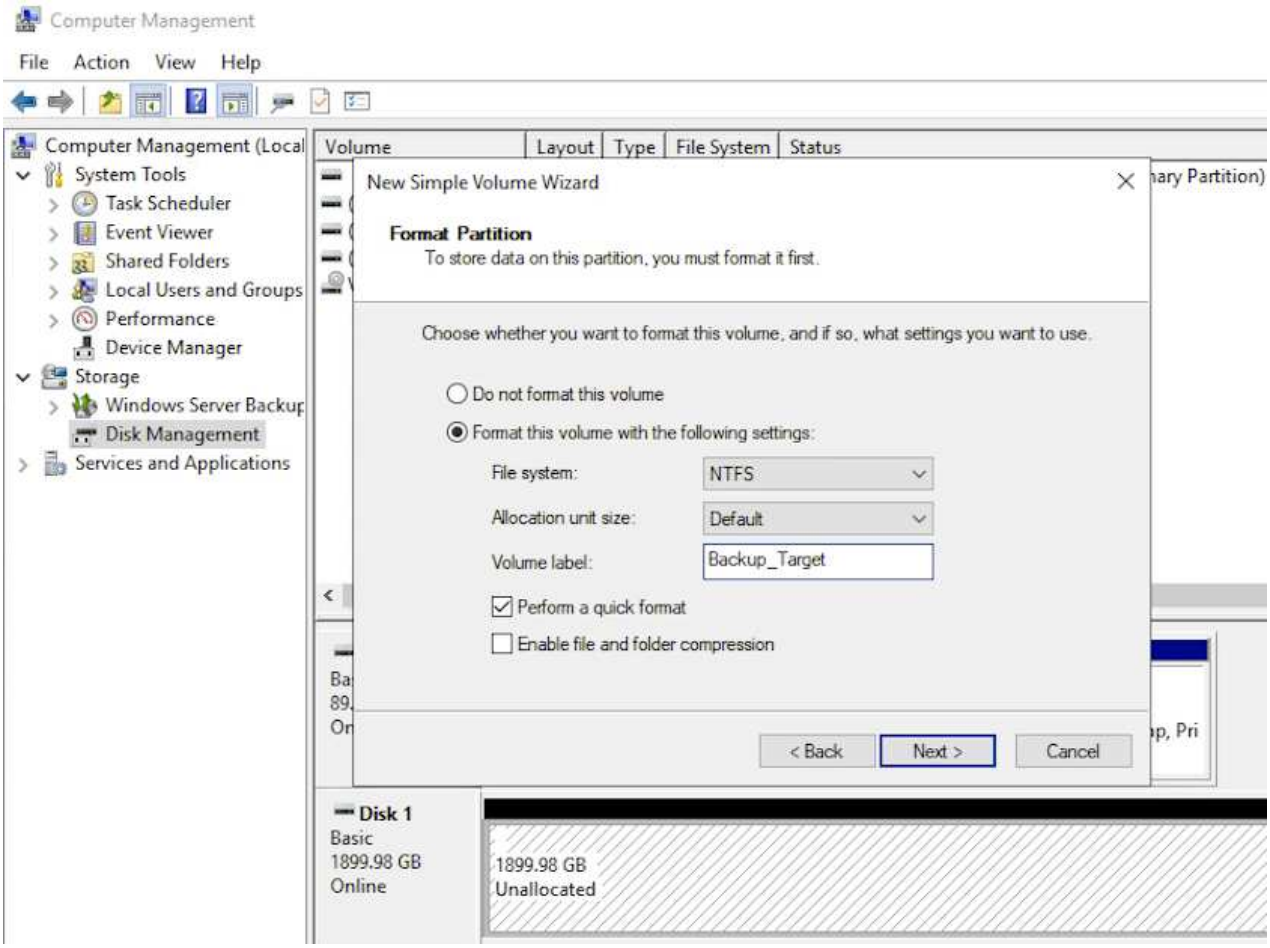
5. Melden Sie sich zum Mounten der iSCSI-LUNs beim Veeam Backup & Replication Server an, und öffnen Sie die iSCSI-Initiatoreigenschaften. Gehen Sie auf die Registerkarte **Discover** und geben Sie die iSCSI-Ziel-IP-Adresse ein.



6. Markieren Sie auf der Registerkarte **targets** die inaktive LUN und klicken Sie auf **Connect**. Aktivieren Sie das Kontrollkästchen **enable multi-path** und klicken Sie auf **OK**, um eine Verbindung zur LUN herzustellen.



7. Initialisieren Sie im Disk Management Utility die neue LUN und erstellen Sie ein Volume mit dem gewünschten Namen und Laufwerksbuchstaben. Aktivieren Sie das Kontrollkästchen **enable multi-path** und klicken Sie auf **OK**, um eine Verbindung zur LUN herzustellen.

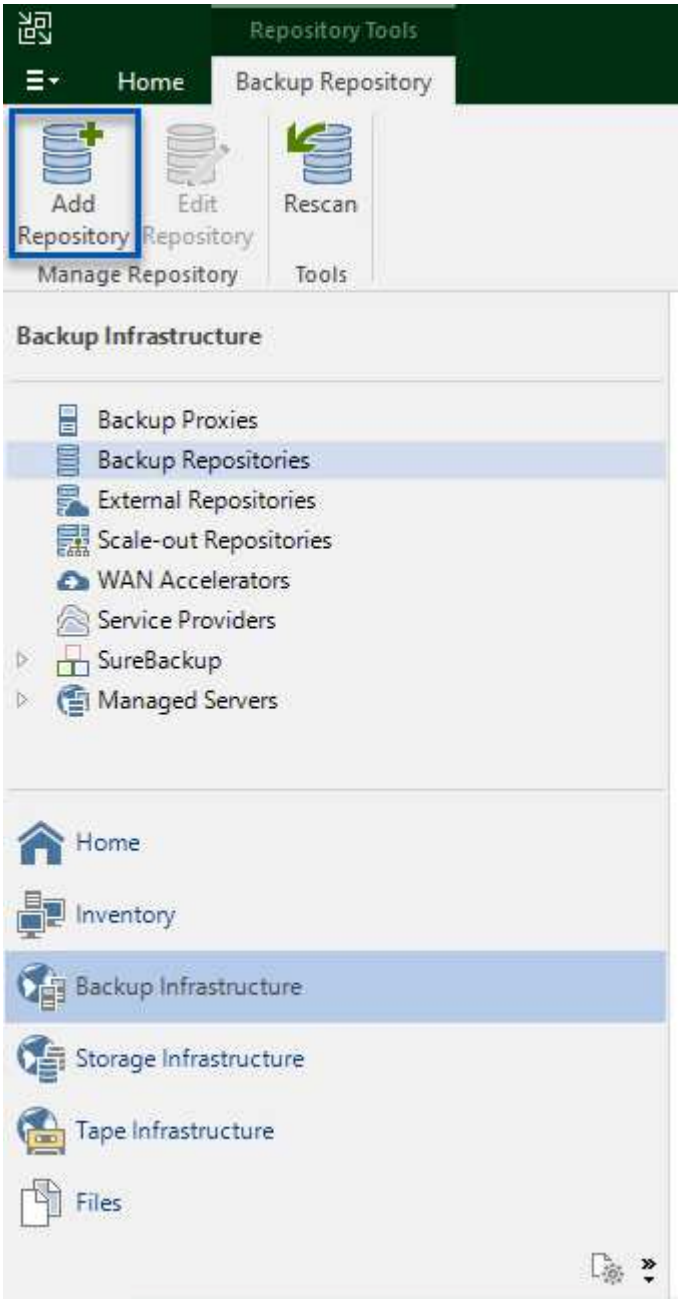


8. Wiederholen Sie diese Schritte, um die iSCSI-Volumes auf den Veeam Proxy-Server zu mounten.

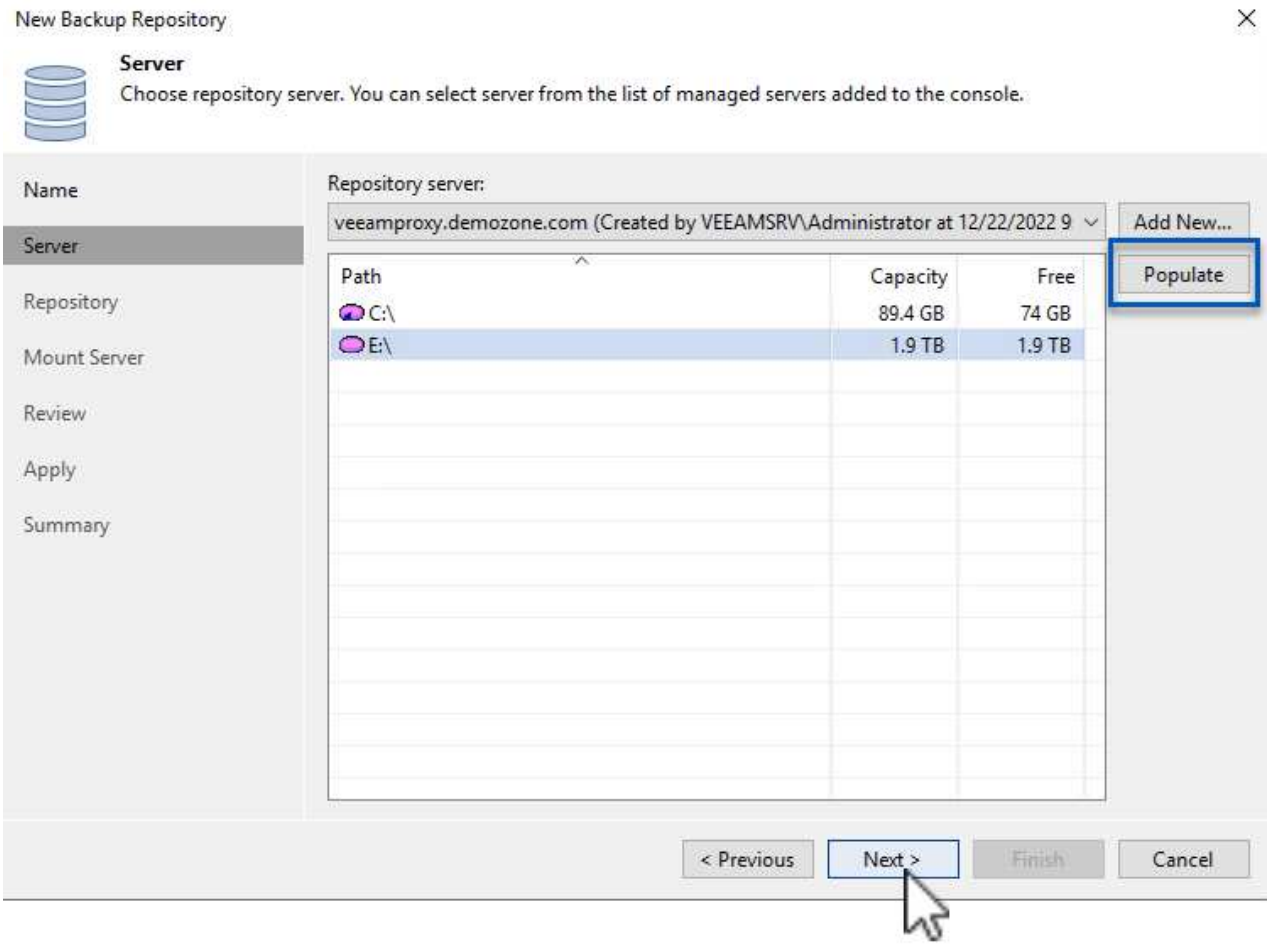
Veeam Backup Repositorys Erstellen

Erstellen Sie in der Veeam Backup and Replication-Konsole Backup-Repositorys für die Veeam Backup- und Veeam Proxy-Server. Diese Repositorys werden als Backup-Ziele für die Backups virtueller Maschinen verwendet.

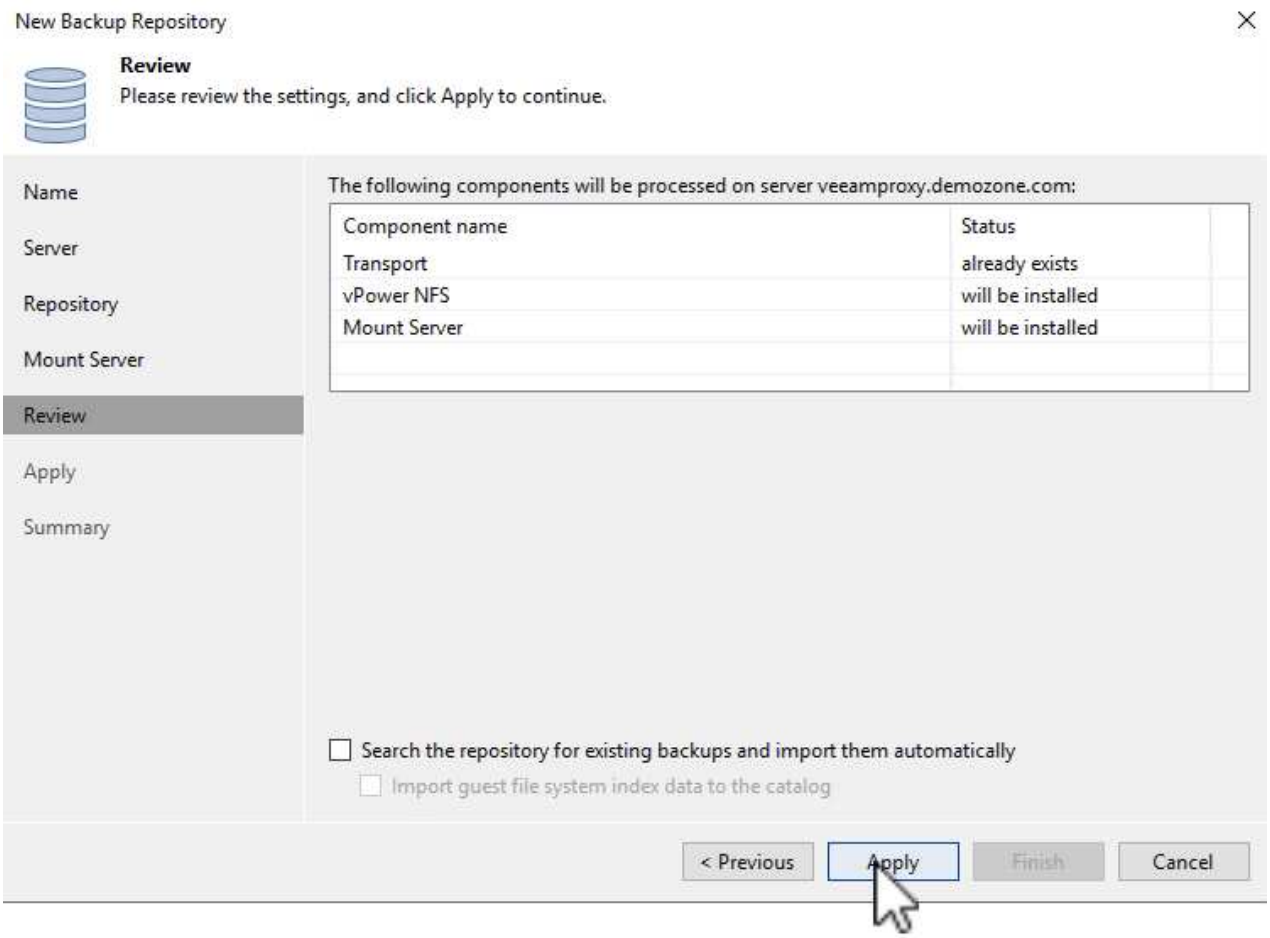
1. Klicken Sie in der Veeam Backup and Replication Konsole unten links auf **Backup Infrastructure** und wählen Sie dann **Add Repository**



2. Geben Sie im Assistenten Neues Backup-Repository einen Namen für das Repository ein, wählen Sie dann den Server aus der Dropdown-Liste aus und klicken Sie auf die Schaltfläche **ausfüllen**, um das zu verwendende NTFS-Volume auszuwählen.



3. Wählen Sie auf der nächsten Seite einen Mount-Server aus, der zum Mounten von Backups verwendet wird, wenn erweiterte Wiederherstellungen durchgeführt werden. Standardmäßig ist dies derselbe Server, mit dem der Repository-Speicher verbunden ist.
4. Überprüfen Sie Ihre Auswahl und klicken Sie auf **Apply**, um die Erstellung des Backup-Repository zu starten.



5. Wiederholen Sie diese Schritte für alle weiteren Proxy-Server.

Veeam Backup-Jobs konfigurieren

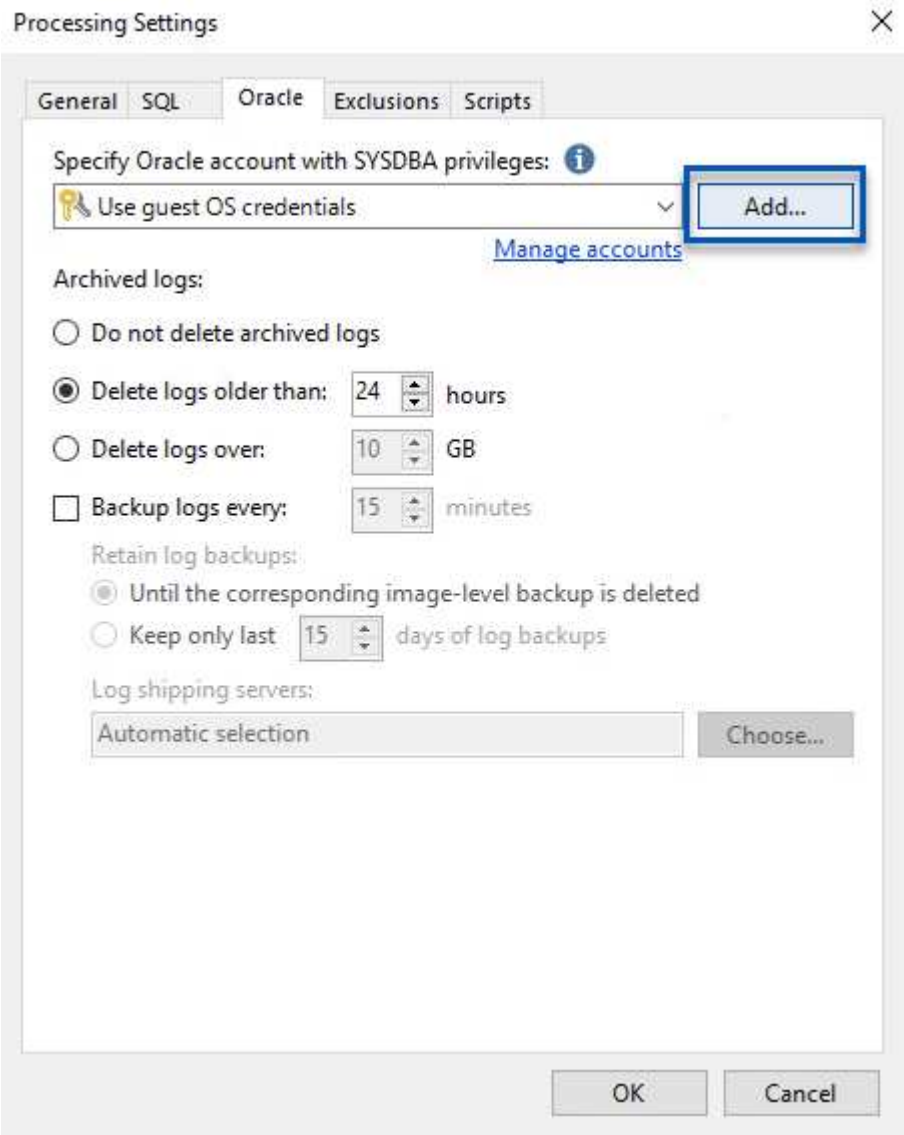
Backup-Jobs sollten mithilfe der Backup-Repositorys im vorherigen Abschnitt erstellt werden. Die Erstellung von Backup-Jobs gehört normalerweise zum Repertoire eines Storage-Administrators und wir werden hier nicht alle Schritte besprechen. Nähere Informationen zum Erstellen von Backup-Jobs in Veeam finden Sie auf der "Technische Dokumentation Des Veeam Help Center".

In dieser Lösung wurden separate Backup-Jobs erstellt für:

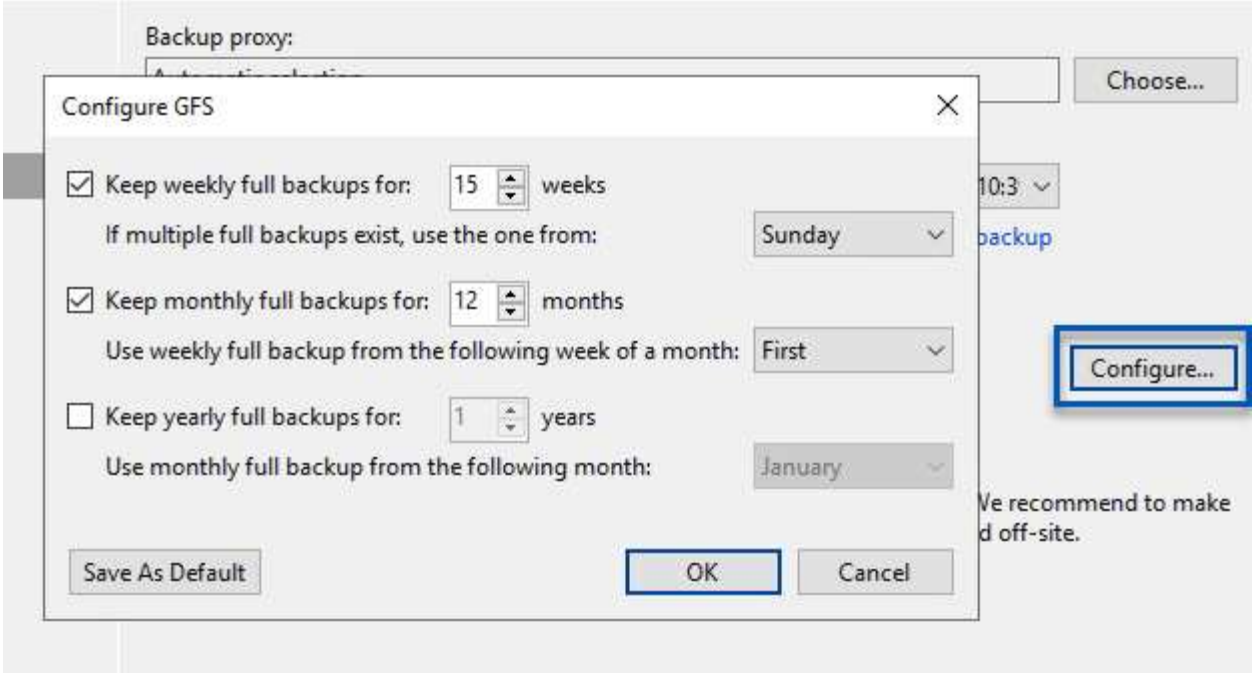
- Microsoft Windows SQL Server
- Oracle Database Server
- Windows File-Server
- Linux-File-Server

Allgemeine Überlegungen beim Konfigurieren von Veeam Backup-Jobs

1. Ermöglichen Sie eine applikationsgerechte Verarbeitung, um konsistente Backups zu erstellen und Transaktions-Log-Verarbeitung durchzuführen.
2. Nach Aktivierung der anwendungsorientierten Verarbeitung fügen Sie der Anwendung die richtigen Anmeldeinformationen mit Administratorrechten hinzu, da diese sich von den Anmeldedaten des Gastbetriebssystems unterscheiden können.



3. Um die Aufbewahrungsrichtlinie für das Backup zu verwalten, überprüfen Sie die Option **bestimmte vollständige Backups länger für Archivierungszwecke behalten** und klicken Sie auf die Schaltfläche **Configure…**, um die Richtlinie zu konfigurieren.



Stellen Sie Applikations-VMs mit der vollständigen Wiederherstellung von Veeam wieder her

Der erste Schritt zur Wiederherstellung einer Applikation ist die vollständige Wiederherstellung mit Veeam. Wir validierten, dass vollständige Restores unserer VMs eingeschaltet waren und alle Services normal liefen.

Die Wiederherstellung von Servern ist normalerweise Teil des Repertoires eines Storage-Administrators und wir decken nicht alle hier aufgeführten Schritte ab. Weitere Informationen zur Durchführung vollständiger Wiederherstellungen in Veeam finden Sie im "Technische Dokumentation Des Veeam Help Center".

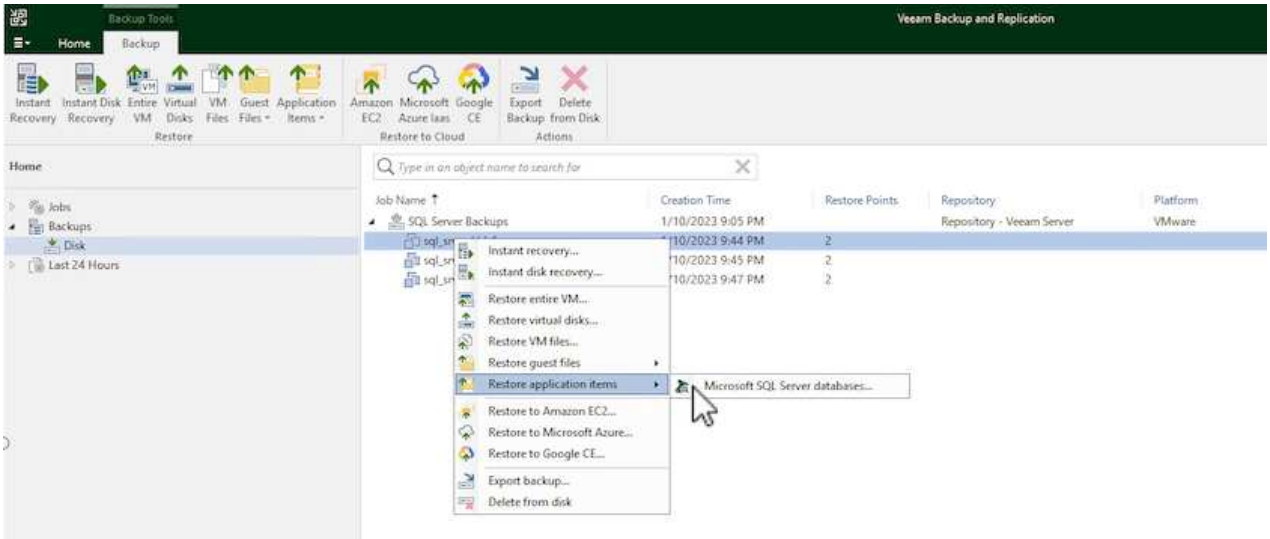
SQL Server-Datenbanken wiederherstellen

Veeam Backup & Replication bietet mehrere Optionen für die Wiederherstellung von SQL Server Datenbanken. Für diese Validierung haben wir mit dem Veeam Explorer für SQL Server mit Instant Recovery Restores unserer SQL Server Datenbanken durchgeführt. SQL Server Instant Recovery ist eine Funktion, mit der Sie SQL Server Datenbanken schnell wiederherstellen können, ohne auf eine vollständige Wiederherstellung der Datenbank warten zu müssen. Durch diesen schnellen Recovery-Prozess werden Ausfallzeiten minimiert und Business Continuity sichergestellt. Und so funktioniert's:

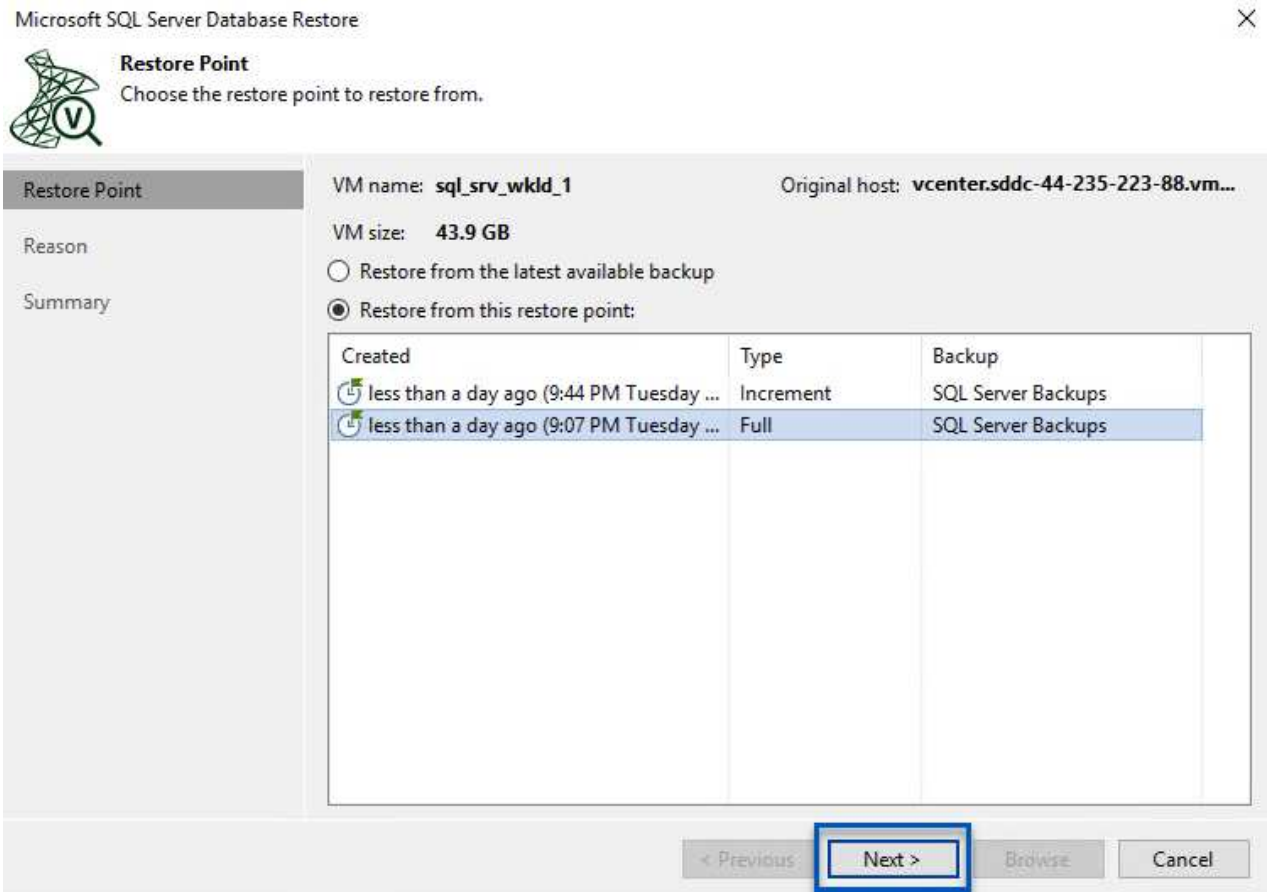
- Veeam Explorer **mountet das Backup** mit der zu wiederherzufüenden SQL Server Datenbank.
- Die Software **veröffentlicht die Datenbank** direkt aus den gemounteten Dateien und macht sie als temporäre Datenbank auf der SQL Server-Zielinstanz zugänglich.
- Während die temporäre Datenbank verwendet wird, leitet Veeam Explorer **Benutzerabfragen** an diese Datenbank weiter, um sicherzustellen, dass Benutzer weiterhin auf die Daten zugreifen und mit ihnen arbeiten können.
- Im Hintergrund führt Veeam **eine vollständige Datenbankwiederherstellung** durch und überträgt Daten aus der temporären Datenbank an den ursprünglichen Speicherort der Datenbank.
- Sobald die vollständige Wiederherstellung der Datenbank abgeschlossen ist, schaltet Veeam Explorer **Benutzeranfragen zurück in die ursprüngliche** Datenbank und entfernt die temporäre Datenbank.

Stellen Sie die SQL Server Datenbank mit Veeam Explorer Instant Recovery wieder her

1. Navigieren Sie in der Veeam Backup and Replication-Konsole zur Liste der SQL Server-Backups, klicken Sie mit der rechten Maustaste auf einen Server und wählen Sie **Restore Application items** und dann **Microsoft SQL Server-Datenbanken…** aus.



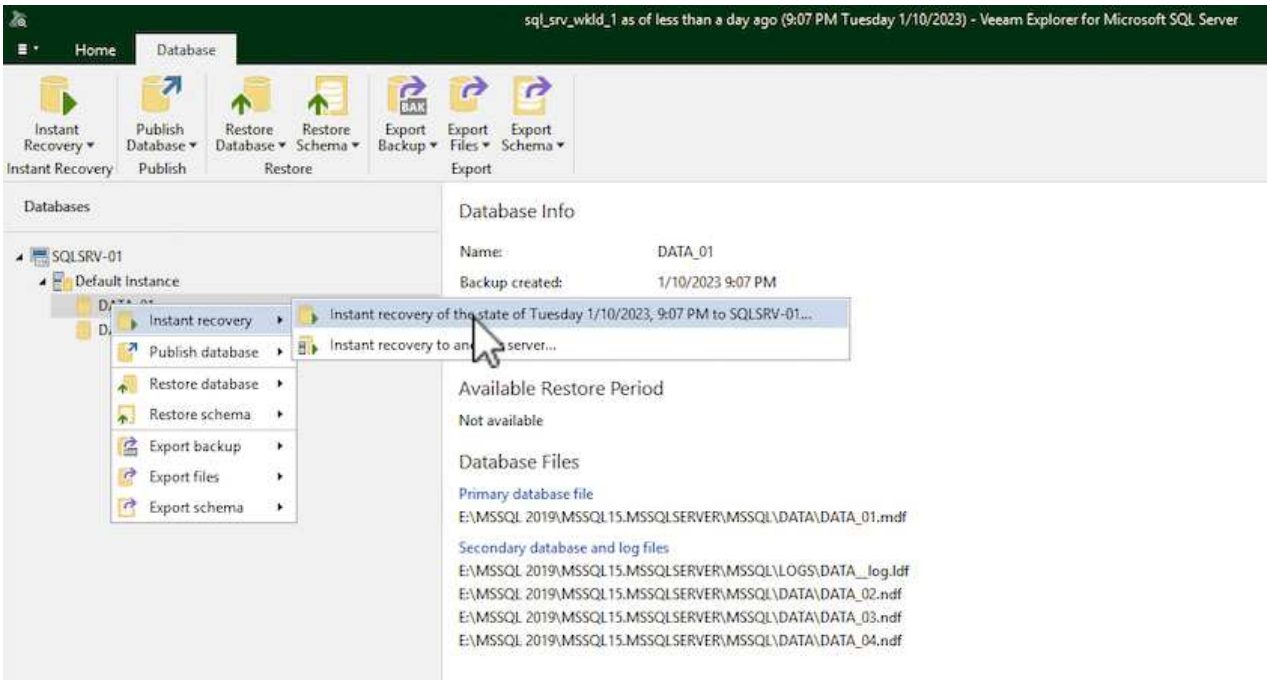
2. Wählen Sie im Microsoft SQL Server Datenbankwiederherstellungsassistenten einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.



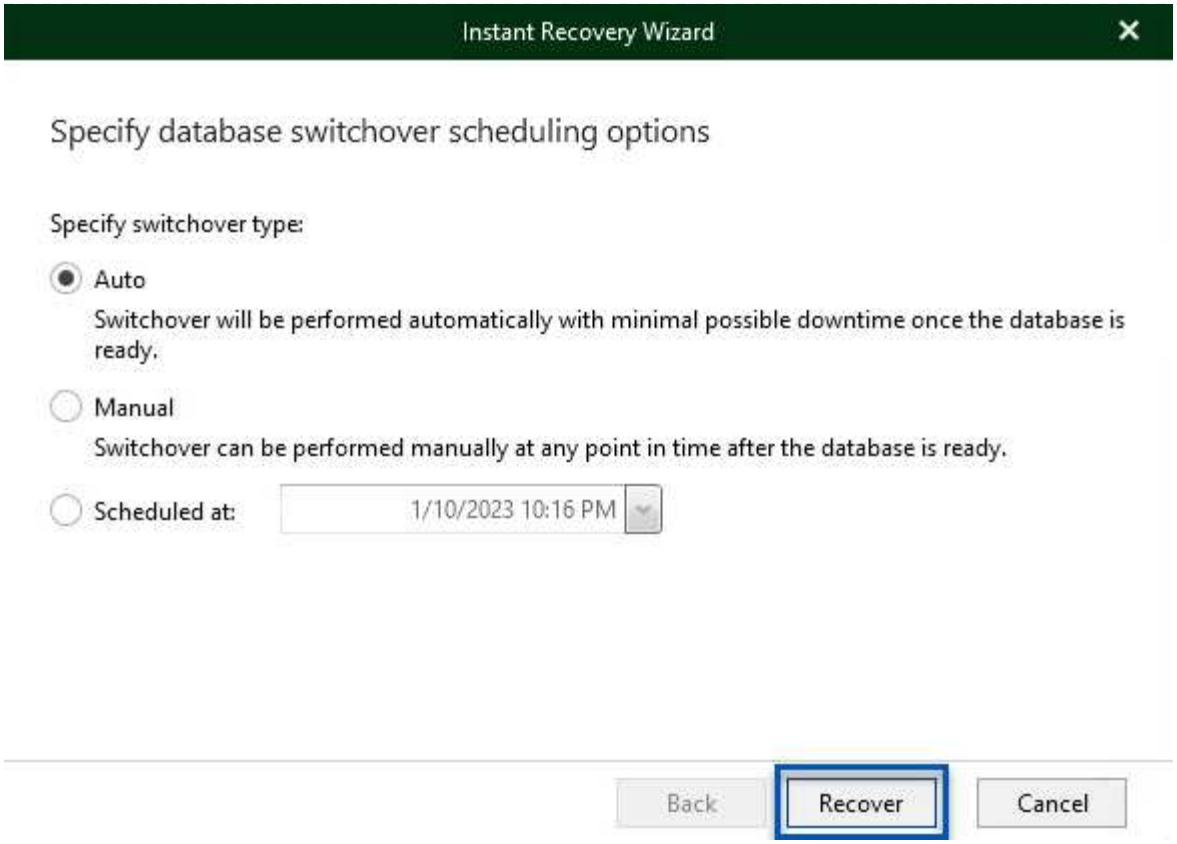
3. Geben Sie bei Bedarf einen * Wiederherstellungsgrund* ein, und klicken Sie dann auf der Übersichtsseite auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Microsoft SQL Server zu

starten.

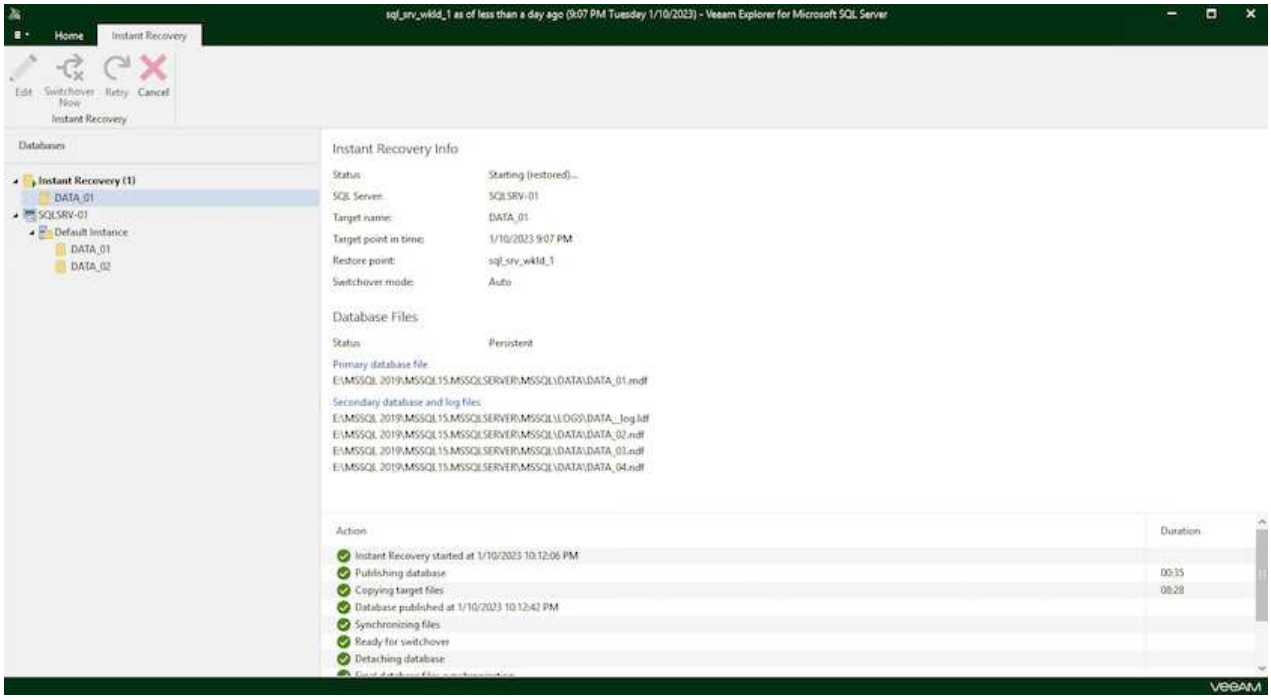
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie mit der rechten Maustaste und wählen Sie * sofortige Wiederherstellung * und dann den spezifischen Wiederherstellungspunkt für die Wiederherstellung.



5. Geben Sie im Assistenten für sofortige Wiederherstellung den Umschalttyp an. Dies kann entweder automatisch mit minimaler Ausfallzeit erfolgen, manuell oder zu einem festgelegten Zeitpunkt. Klicken Sie dann auf die Schaltfläche **Recover**, um den Wiederherstellungsprozess zu starten.



6. Der Recovery-Prozess kann über den Veeam Explorer überwacht werden.



Weitere Informationen zum Durchführen von SQL Server-Wiederherstellungsvorgängen mit Veeam Explorer finden Sie im Abschnitt Microsoft SQL Server in der "Benutzerhandbuch Für Veeam Explorers".

Stellen Sie Oracle Datenbanken mit Veeam Explorer wieder her

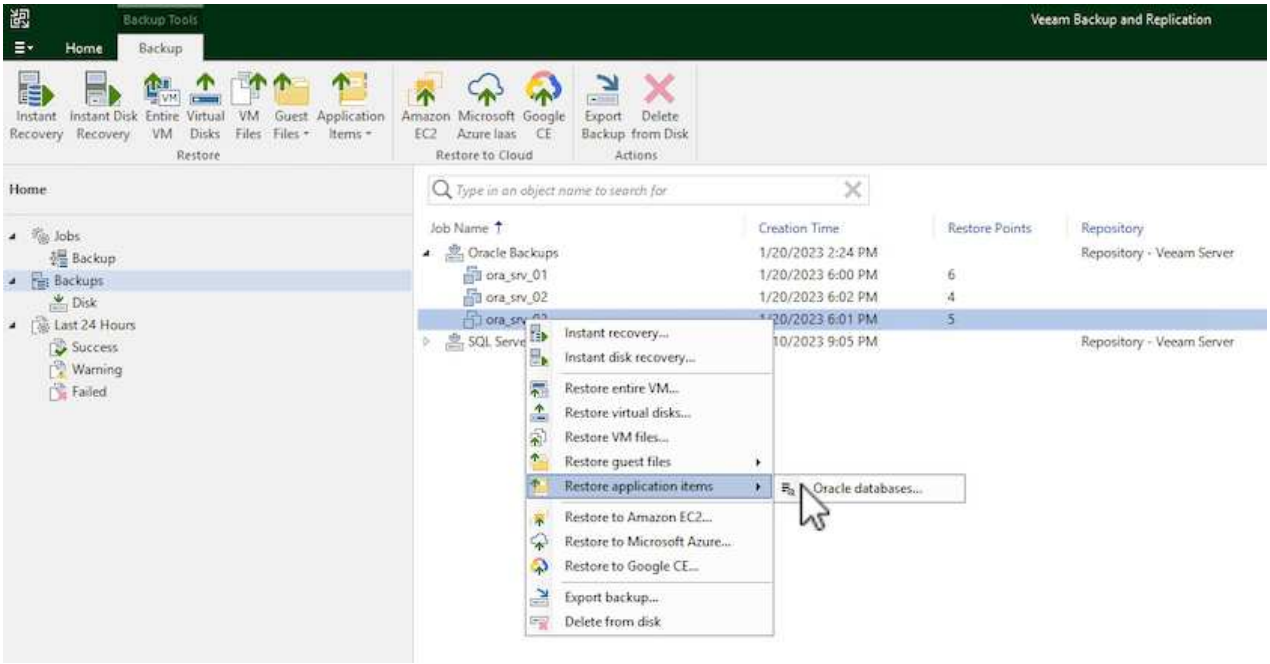
Mit dem Veeam Explorer für Oracle Database können Sie eine standardmäßige Wiederherstellung von Oracle-Datenbanken oder eine unterbrechungsfreie Wiederherstellung mithilfe von Instant Recovery durchführen. Es unterstützt auch die Veröffentlichung von Datenbanken für schnellen Zugriff, Recovery von Data Guard-Datenbanken und Wiederherstellungen von RMAN-Backups.

Weitere Informationen zur Wiederherstellung von Oracle-Datenbanken mit Veeam Explorer finden Sie im Abschnitt Oracle in der "Benutzerhandbuch Für Veeam Explorers".

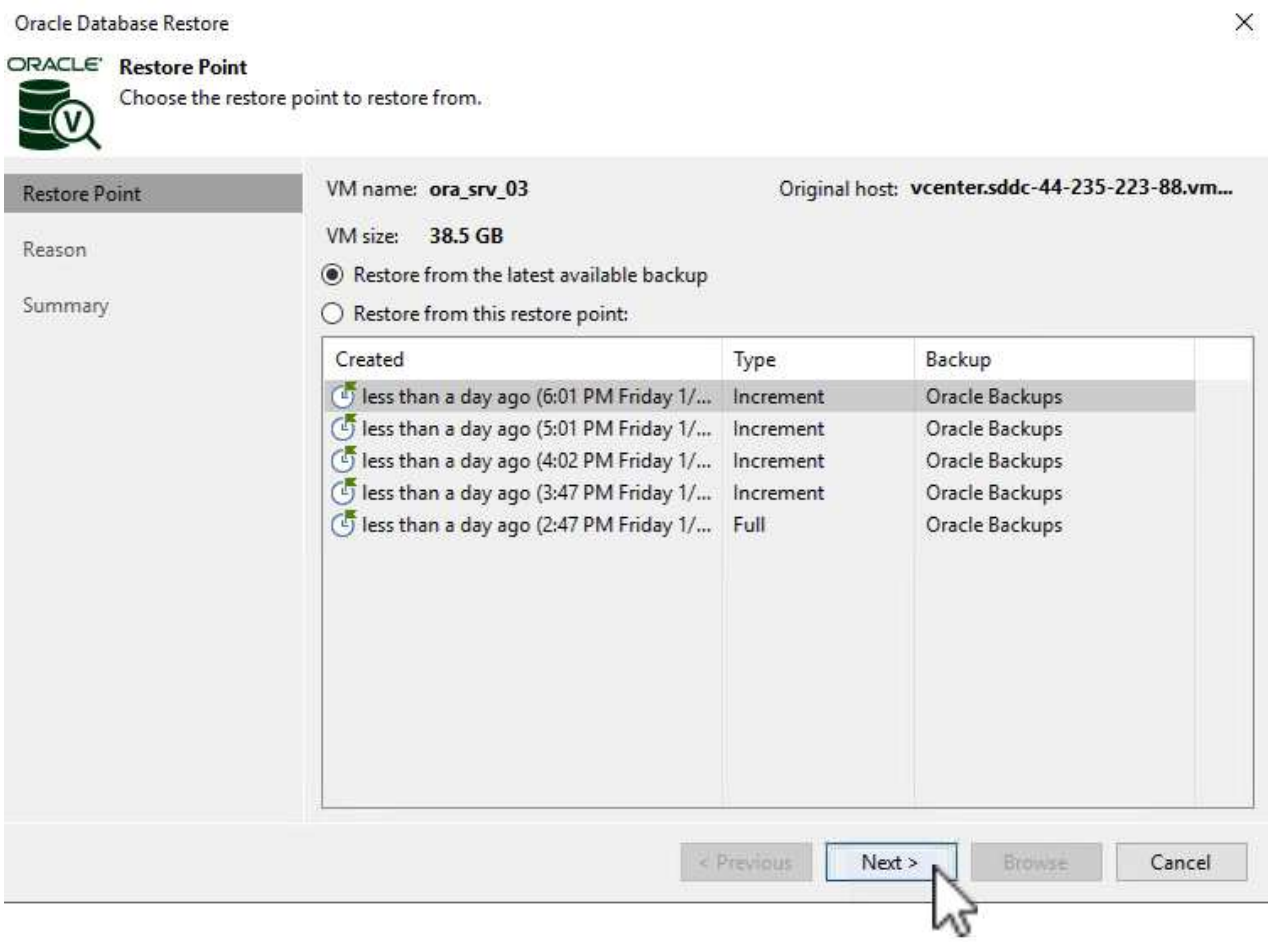
Stellen Sie Oracle Datenbanken mit Veeam Explorer wieder her

In diesem Abschnitt wird die Wiederherstellung einer Oracle-Datenbank auf einem anderen Server mit Veeam Explorer behandelt.

1. Navigieren Sie in der Veeam Backup and Replication-Konsole zur Liste der Oracle-Backups, klicken Sie mit der rechten Maustaste auf einen Server und wählen Sie **Restore Application items** und dann **Oracle Databases…** aus.

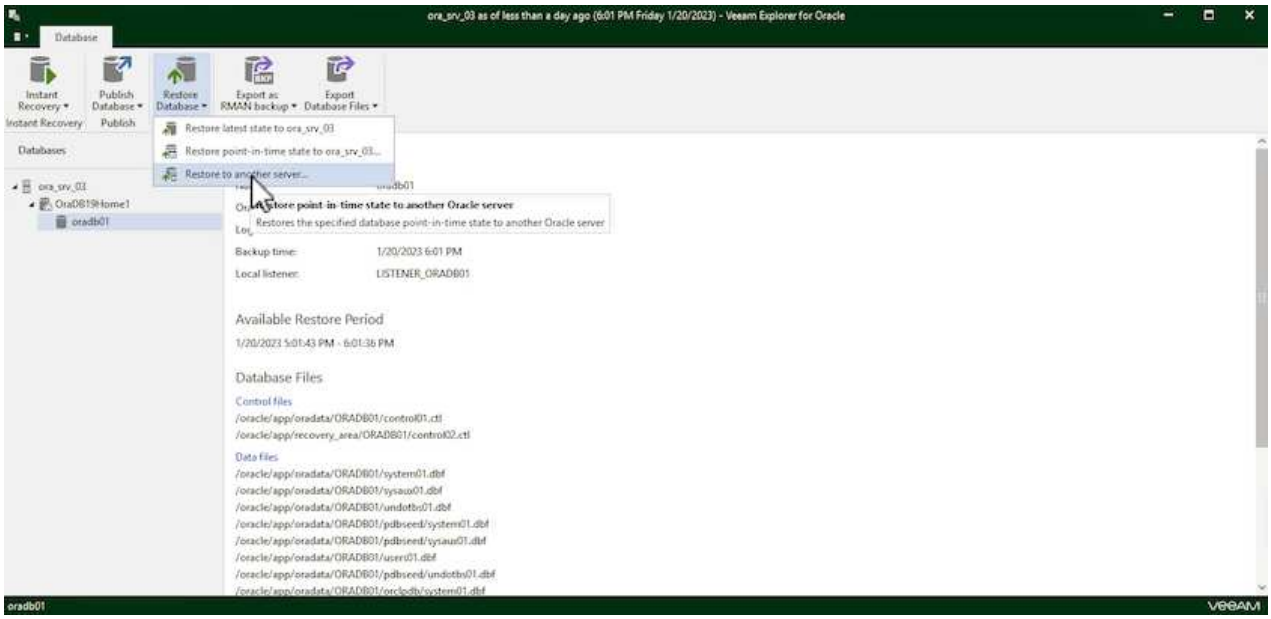


2. Wählen Sie im Oracle Database Restore Wizard einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.

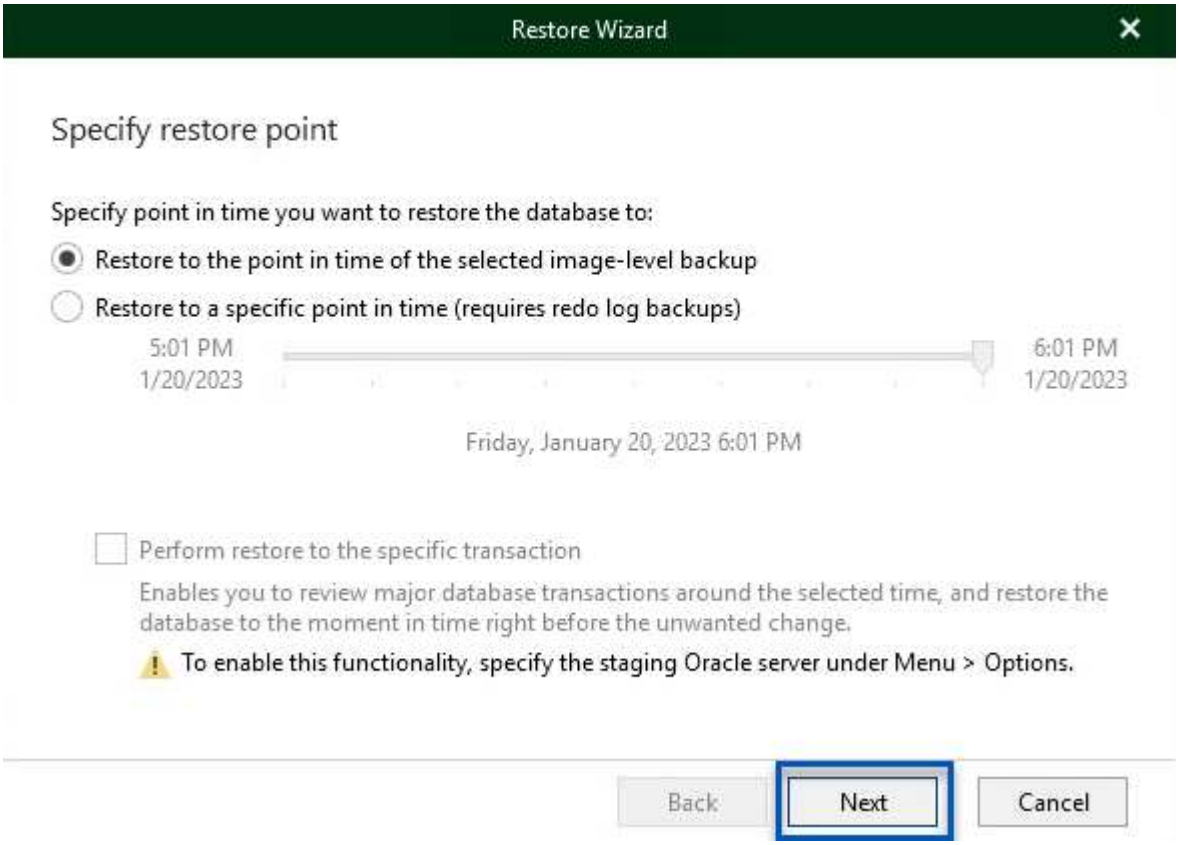


3. Geben Sie bei Bedarf einen * Wiederherstellungsgrund* ein, und klicken Sie dann auf der Übersichtsseite auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Oracle zu starten.

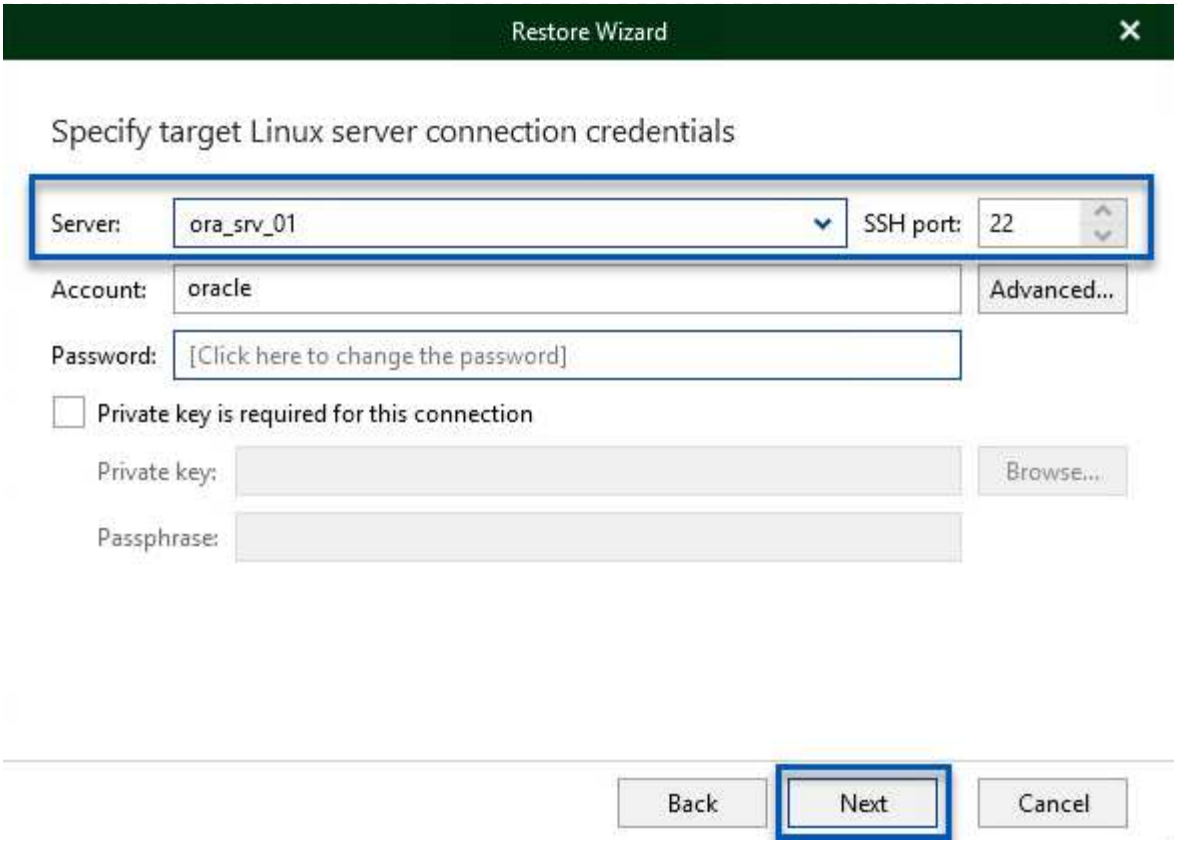
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie auf die Datenbank, die wiederhergestellt werden soll, und wählen Sie dann aus dem Dropdown-Menü **Datenbank wiederherstellen** oben **auf einem anderen Server wiederherstellen…**.



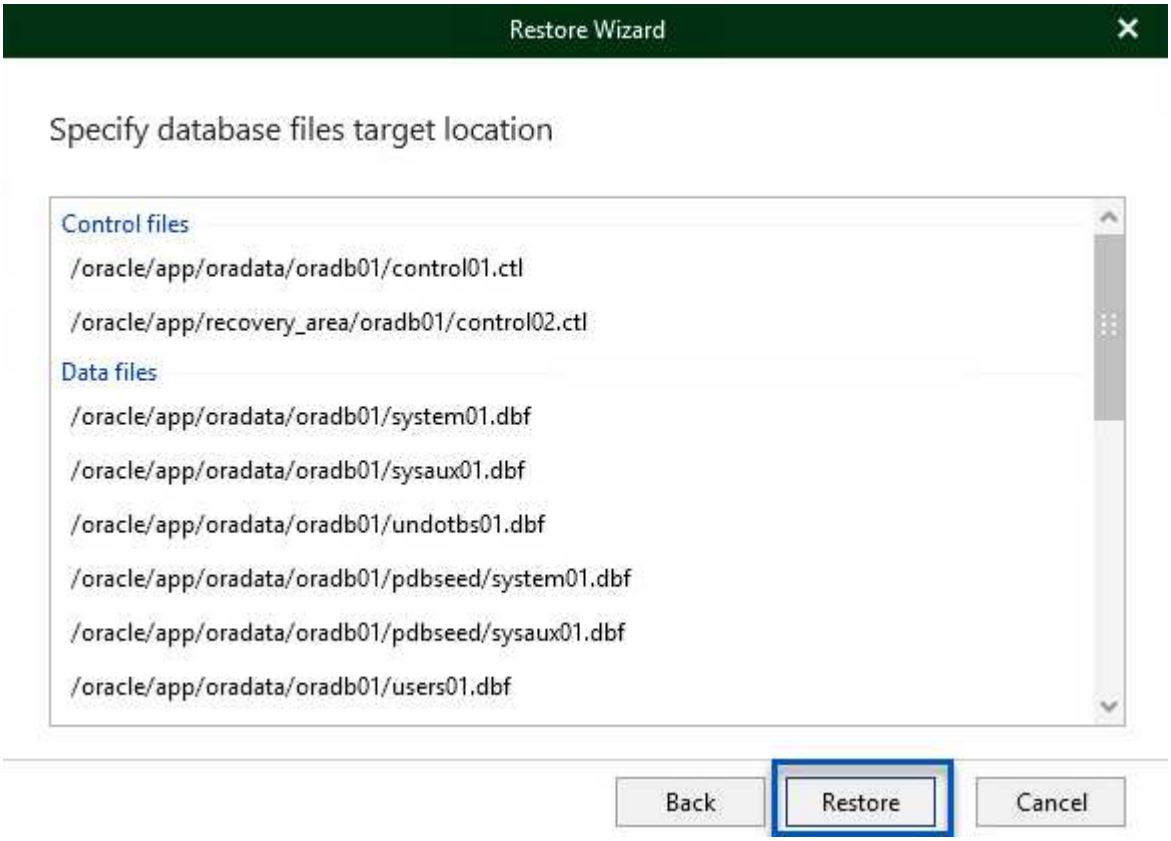
5. Geben Sie im Wiederherstellungsassistenten den Wiederherstellungspunkt an, von dem aus wiederhergestellt werden soll, und klicken Sie auf **Weiter**.



6. Geben Sie den Zielserver an, auf dem die Datenbank wiederhergestellt werden soll, und klicken Sie auf **Weiter**.



7. Geben Sie schließlich den Zielspeicherort der Datenbankdateien an und klicken Sie auf die Schaltfläche **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.



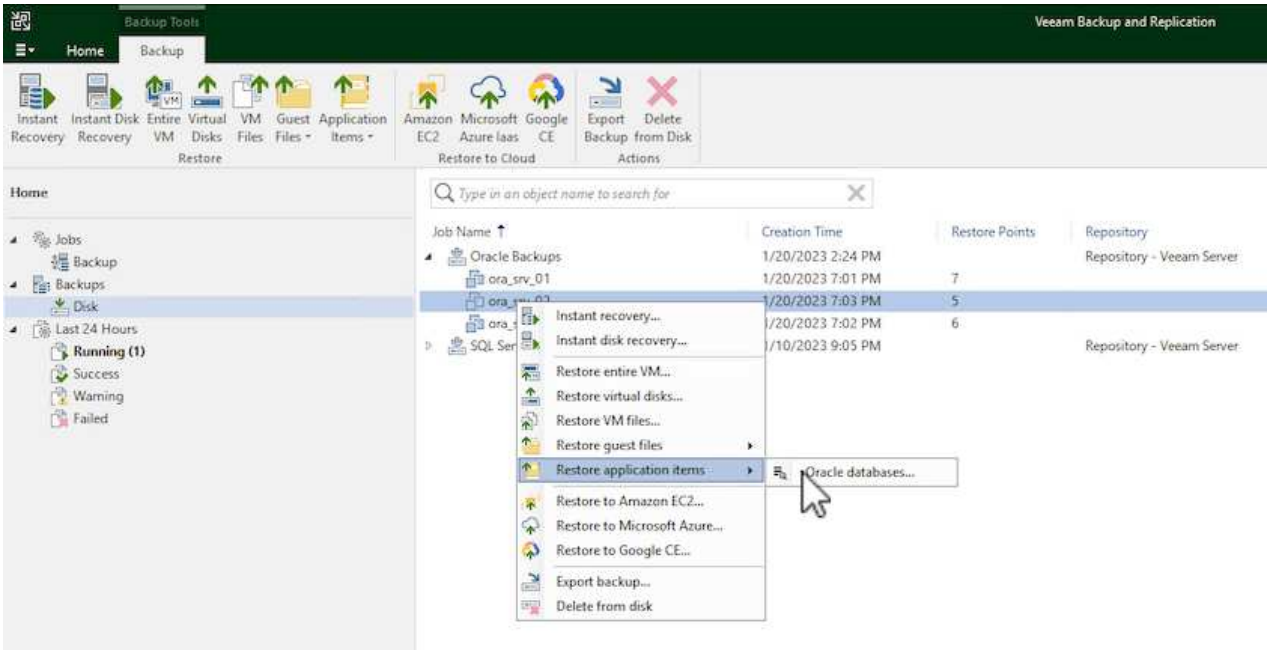
8. Sobald die Wiederherstellung der Datenbank abgeschlossen ist, überprüfen Sie, ob die Oracle-

Datenbank ordnungsgemäß auf dem Server gestartet wird.

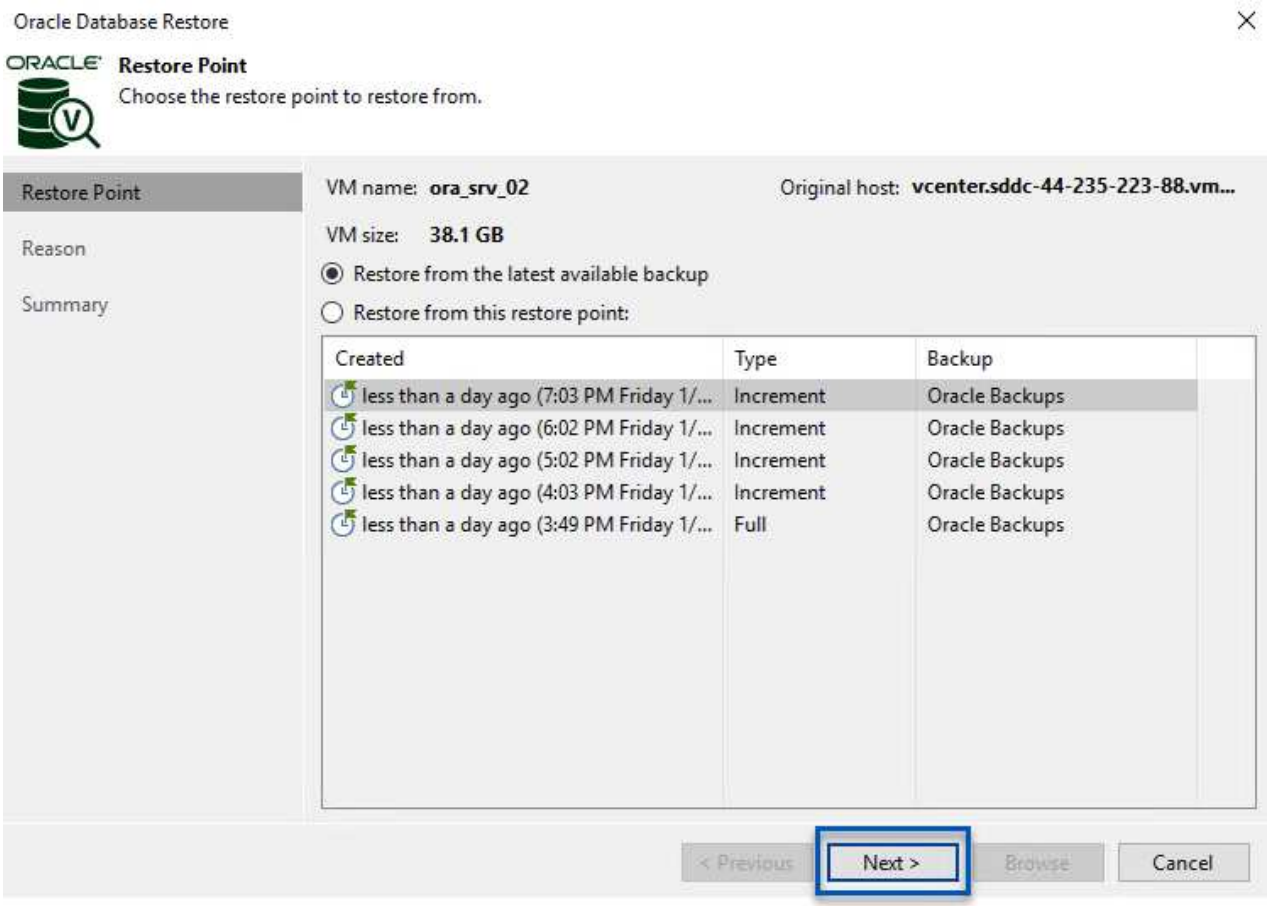
Veröffentlichen der Oracle-Datenbank auf einem alternativen Server

In diesem Abschnitt wird eine Datenbank für einen schnellen Zugriff auf einen alternativen Server veröffentlicht, ohne eine vollständige Wiederherstellung zu starten.

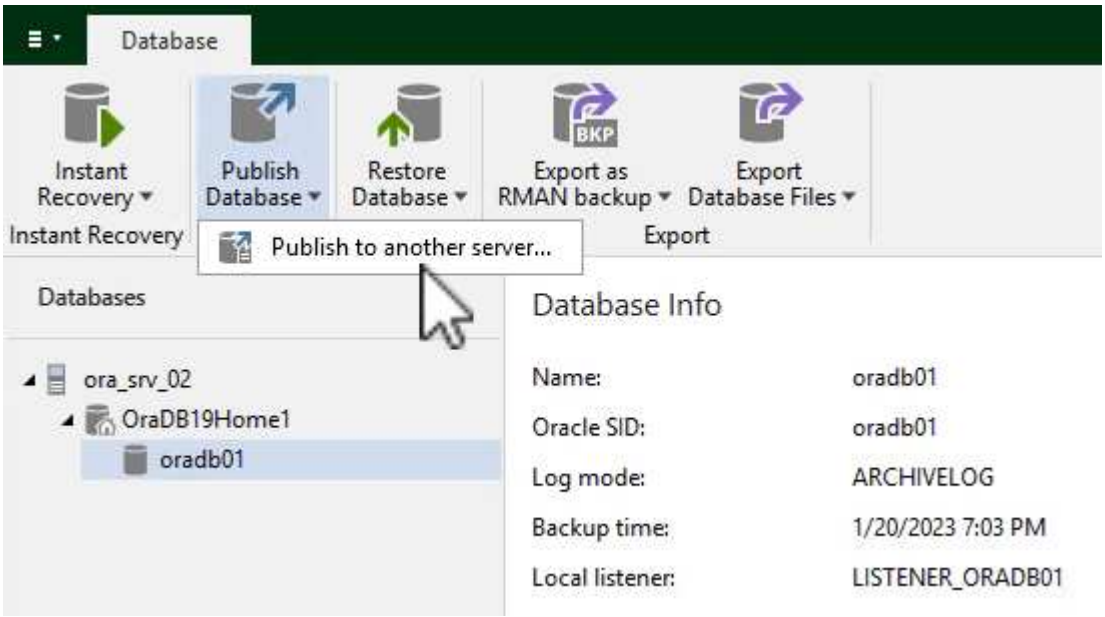
1. Navigieren Sie in der Veeam Backup and Replication-Konsole zur Liste der Oracle-Backups, klicken Sie mit der rechten Maustaste auf einen Server und wählen Sie **Restore Application items** und dann **Oracle Databases…** aus.



2. Wählen Sie im Oracle Database Restore Wizard einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.

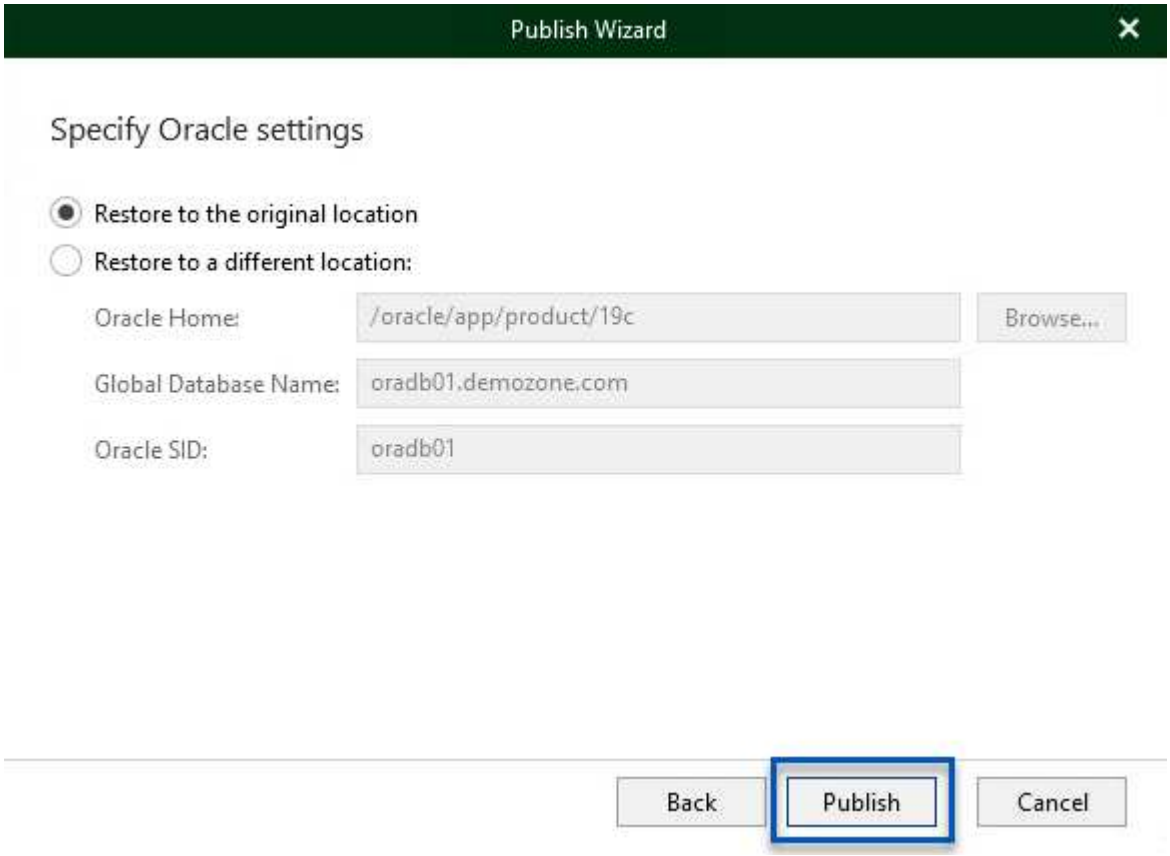


3. Geben Sie bei Bedarf einen * Wiederherstellungsgrund* ein, und klicken Sie dann auf der Übersichtsseite auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Oracle zu starten.
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie auf die Datenbank, die wiederhergestellt werden soll, und wählen Sie dann aus dem Dropdown-Menü **Datenbank veröffentlichen** oben **auf einem anderen Server veröffentlichen…**.



5. Geben Sie im Veröffentlichungsassistenten den Wiederherstellungspunkt an, von dem die Datenbank veröffentlicht werden soll, und klicken Sie auf **Weiter**.

6. Geben Sie schließlich den Speicherort des Linux-Dateisystems an und klicken Sie auf **Veröffentlichen**, um den Wiederherstellungsprozess zu starten.



7. Melden Sie sich nach Abschluss der Veröffentlichung beim Zielserver an und führen Sie die folgenden Befehle aus, um sicherzustellen, dass die Datenbank ausgeführt wird:

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```

```
oracle@ora_srv_01:~
File  Edit  View  Search  Terminal  Help
[oracle@ora_srv_01 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Jan 20 16:46:39 2023
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select name, open_mode from v$database;

NAME      OPEN_MODE
--------- --------------------
ORADB01   READ WRITE
```

Schlussfolgerung

VMware Cloud ist eine leistungsstarke Plattform, mit der Sie geschäftskritische Applikationen ausführen und sensible Daten speichern. Für Unternehmen, die sich auf VMware Cloud verlassen, ist eine sichere Datensicherungslösung unabdingbar, um die Business Continuity sicherzustellen und vor Cyberbedrohungen und Datenverlust zu schützen. Unternehmen, die sich für eine zuverlässige und robuste Datensicherungslösung entscheiden, können sich darauf verlassen, dass ihre geschäftskritischen Daten in jedem Fall sicher und geschützt sind.

Der in dieser Dokumentation präsentierte Anwendungsfall konzentriert sich auf bewährte Datensicherungstechnologien, bei denen die Integration von NetApp, VMware und Veeam hervorzuheben ist. FSX for ONTAP wird als ergänzende NFS-Datastores für VMware Cloud in AWS unterstützt und für alle Virtual Machine- und Applikationsdaten verwendet. Veeam Backup & Replication ist eine umfassende Datensicherungslösung, die Unternehmen bei der Verbesserung, Automatisierung und Optimierung ihrer Backup- und Recovery-Prozesse unterstützt. Veeam wird in Verbindung mit iSCSI-Backup-Ziel-Volumes verwendet, die auf FSX für ONTAP gehostet werden, um eine sichere und einfach zu managende Datensicherungslösung für Applikationsdaten in VMware Cloud bereitzustellen.

Weitere Informationen

Weitere Informationen zu den in dieser Lösung vorgestellten Technologien finden Sie in den folgenden zusätzlichen Informationen.

- "FSX for ONTAP Benutzerhandbuch"
- "Technische Dokumentation Des Veeam Help Center"
- "VMware Cloud auf AWS Unterstützung: Überlegungen und Einschränkungen"

TR-4955: Disaster Recovery mit FSX für ONTAP und VMC (AWS VMware Cloud)

Niyaz Mohamed, NetApp

Überblick

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz der Workloads vor Standortausfällen und Datenbeschädigungen (z. B. Ransomware). Dank der NetApp SnapMirror Technologie können lokale VMware Workloads auf FSX für ONTAP repliziert werden, die in AWS ausgeführt werden.

Disaster Recovery Orchestrator (DRO, eine skriptbasierte Lösung mit UI) kann verwendet werden, um Workloads, die von lokalen Systemen auf FSX für ONTAP repliziert werden, nahtlos wiederherzustellen. DRO automatisiert die Recovery von SnapMirror Ebene durch VM-Registrierung zu VMC und Netzwerkzuordnungen direkt auf NSX-T. Diese Funktion ist in allen VMC Umgebungen enthalten.

Erste Schritte

Implementieren und Konfigurieren von VMware Cloud auf AWS

"VMware Cloud auf AWS" Cloud-native Arbeitsumgebung für VMware-basierte Workloads im AWS Ecosystem Jedes softwaredefinierte VMware Datacenter (SDDC) wird in einer Amazon Virtual Private Cloud (VPC) ausgeführt und bietet einen vollständigen VMware Stack (einschließlich vCenter Server), softwaredefiniertes NSX-T Networking, softwaredefinierten vSAN Storage sowie einen oder mehrere ESXi Hosts, die Computing- und Storage-Ressourcen für die Workloads bereitstellen. Gehen Sie folgendermaßen vor, um eine VMC-Umgebung auf AWS zu konfigurieren "Verlinken". Ein Pilot-Light-Cluster kann auch für DR-Zwecke verwendet werden.

> In der ersten Version unterstützt DRO einen vorhandenen Pilot-Light-Cluster. Die Erstellung eines On-Demand SDDC wird in einer kommenden Version verfügbar sein.

Provisionieren und konfigurieren Sie FSX für ONTAP

Amazon FSX für NetApp ONTAP ist ein vollständig gemanagter Service, der zuverlässigen, skalierbaren, hochperformanten und funktionsreichen File Storage auf dem beliebten NetApp ONTAP Filesystem bietet. Befolgen Sie die Schritte unter diesem "Verlinken" Zur Bereitstellung und Konfiguration von FSX für ONTAP.

SnapMirror wird auf FSX für ONTAP implementiert und konfiguriert

Im nächsten Schritt werden NetApp BlueXP verwendet, um die bereitgestellte FSX für ONTAP auf AWS Instanzen zu ermitteln und die gewünschten Datastore-Volumes aus einer lokalen Umgebung mit der entsprechenden Häufigkeit und mit der Aufbewahrung von NetApp Snapshot Kopien in FSX für ONTAP zu replizieren:

Befolgen Sie die Schritte in diesem Link, um BlueXP zu konfigurieren. Sie können die NetApp ONTAP CLI auch verwenden, um die Replikation über diesen Link zu planen.

> Eine SnapMirror Beziehung ist Voraussetzung und muss im Vorfeld erstellt werden.

DRO-Installation

Um mit DRO zu beginnen, verwenden Sie das Betriebssystem Ubuntu auf einer dafür vorgesehenen EC2-Instanz oder virtuellen Maschine, um sicherzustellen, dass Sie die Voraussetzungen erfüllen. Installieren Sie dann das Paket.

Voraussetzungen

- Stellen Sie sicher, dass Konnektivität mit dem Quell- und Ziel-vCenter und den Storage-Systemen vorhanden ist.
- DNS-Auflösung sollte vorhanden sein, wenn Sie DNS-Namen verwenden. Andernfalls sollten Sie IP-Adressen für vCenter und Storage-Systeme verwenden.
- Erstellen Sie einen Benutzer mit Root-Berechtigungen. Sie können auch sudo mit einer EC2-Instanz verwenden.

Anforderungen an das Betriebssystem

- Ubuntu 20.04 (LTS) mit mindestens 2 GB und 4 vCPUs
- Die folgenden Pakete müssen auf der zugewiesenen Agent-VM installiert werden:
  - Docker
  - Docker-komponieren
  - Jq.

Berechtigungen ändern auf `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.

> Der `deploy.sh` Skript führt alle erforderlichen Voraussetzungen aus.

Installieren Sie das Paket

1. Laden Sie das Installationspaket auf der angegebenen virtuellen Maschine herunter:

   ```
   git clone https://github.com/NetApp/DRO-AWS.git
   ```

   > Der Agent kann lokal oder in einem AWS VPC installiert werden.

2. Entpacken Sie das Paket, führen Sie das Bereitstellungsskript aus, und geben Sie die Host-IP ein (z. B. 10.10.10.10).

   ```
   tar xvf DRO-prereq.tar
   ```

3. Navigieren Sie zum Verzeichnis, und führen Sie das Skript Bereitstellen wie folgt aus:

   ```
   sudo sh deploy.sh
   ```

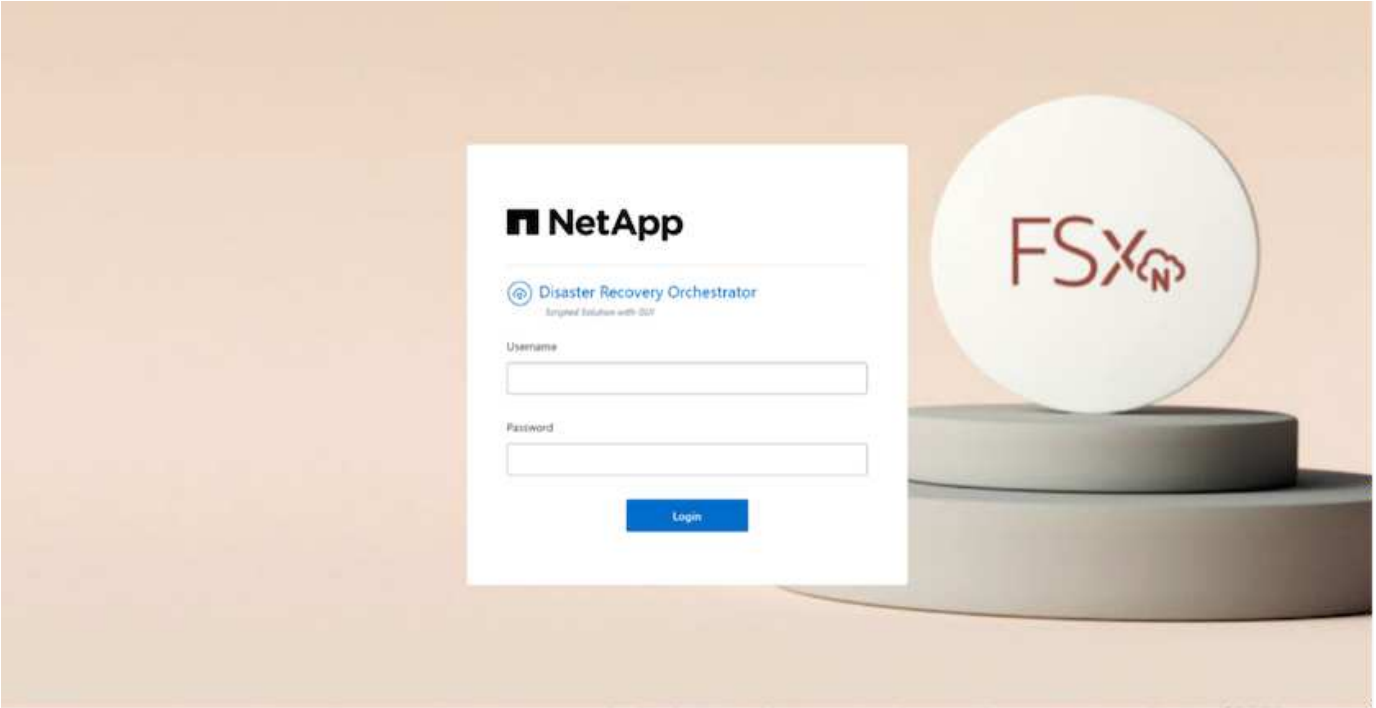
4. Greifen Sie über folgende Funktionen auf die UI zu:

```
https://<host-ip-address>
```

Mit den folgenden Standardanmeldeinformationen:

```
Username: admin
Password: admin
```

Das Passwort kann mit der Option „Passwort ändern“ geändert werden.



DRO-Konfiguration

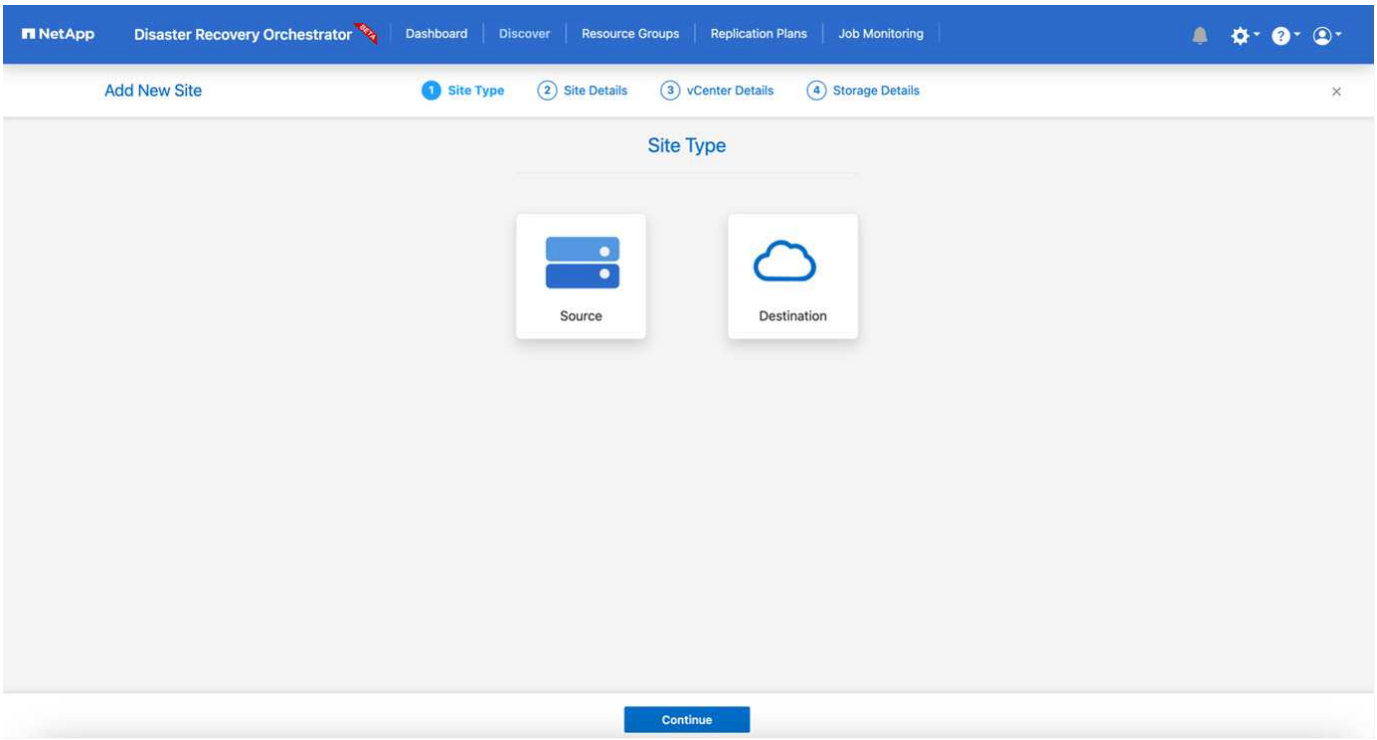
Nachdem FSX für ONTAP und VMC ordnungsgemäß konfiguriert wurden, können Sie DRO konfigurieren, um die Wiederherstellung lokaler Workloads auf VMC zu automatisieren. Dazu werden die schreibgeschützten SnapMirror Kopien auf FSX für ONTAP verwendet.

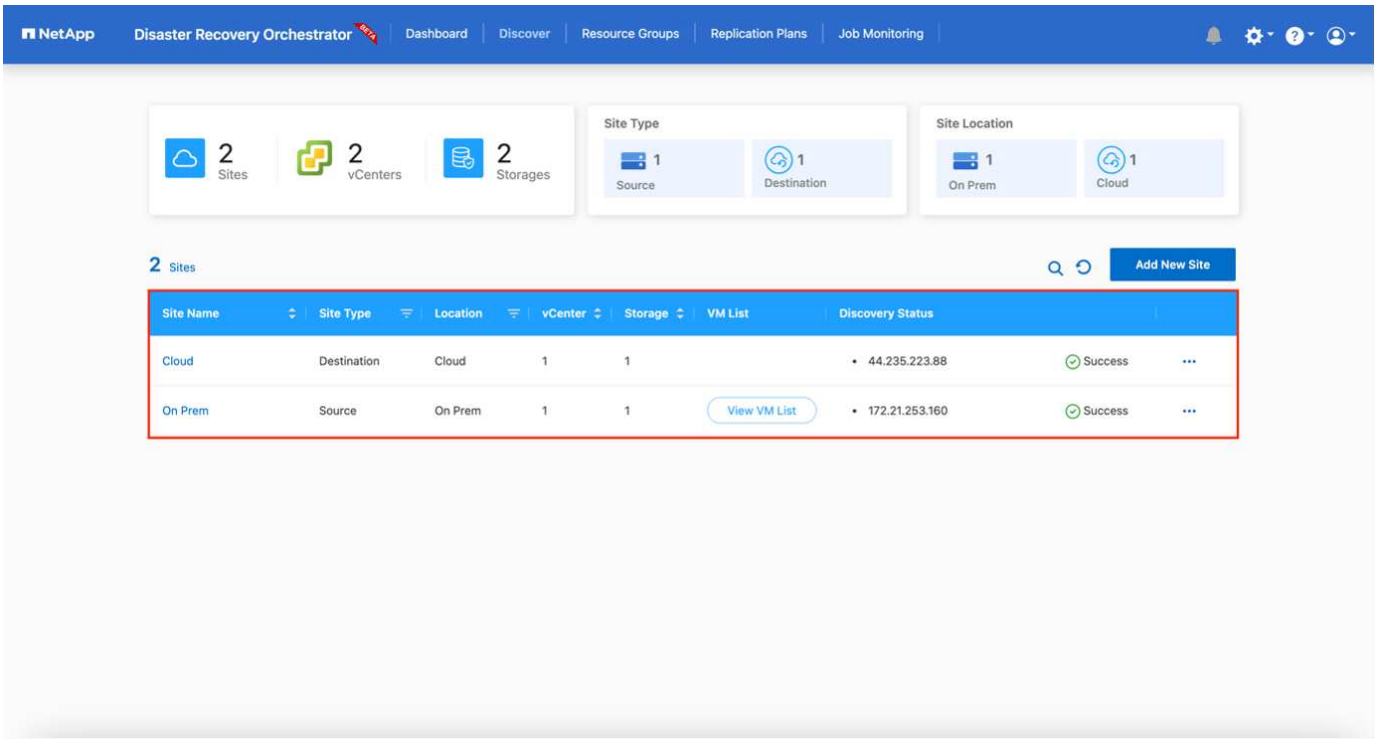
NetApp empfiehlt, den DRO-Agent in AWS und auch auf die gleiche VPC zu implementieren, bei dem FSX für ONTAP eingesetzt wird (es kann auch Peer-Verbindung bestehen) Damit der DRO-Agent über das Netzwerk mit Ihren On-Premises-Komponenten sowie mit den FSX für ONTAP- und VMC-Ressourcen kommunizieren kann.

Im ersten Schritt werden lokale und Cloud-Ressourcen (vCenter und Storage) zu DRO hinzugefügt. Öffnen Sie DRO in einem unterstützten Browser, und verwenden Sie den Standardbenutzernamen und das Standardpasswort (admin/admin) und Add Sites. Standorte können auch mithilfe der Option Entdecken hinzugefügt werden. Fügen Sie die folgenden Plattformen hinzu:

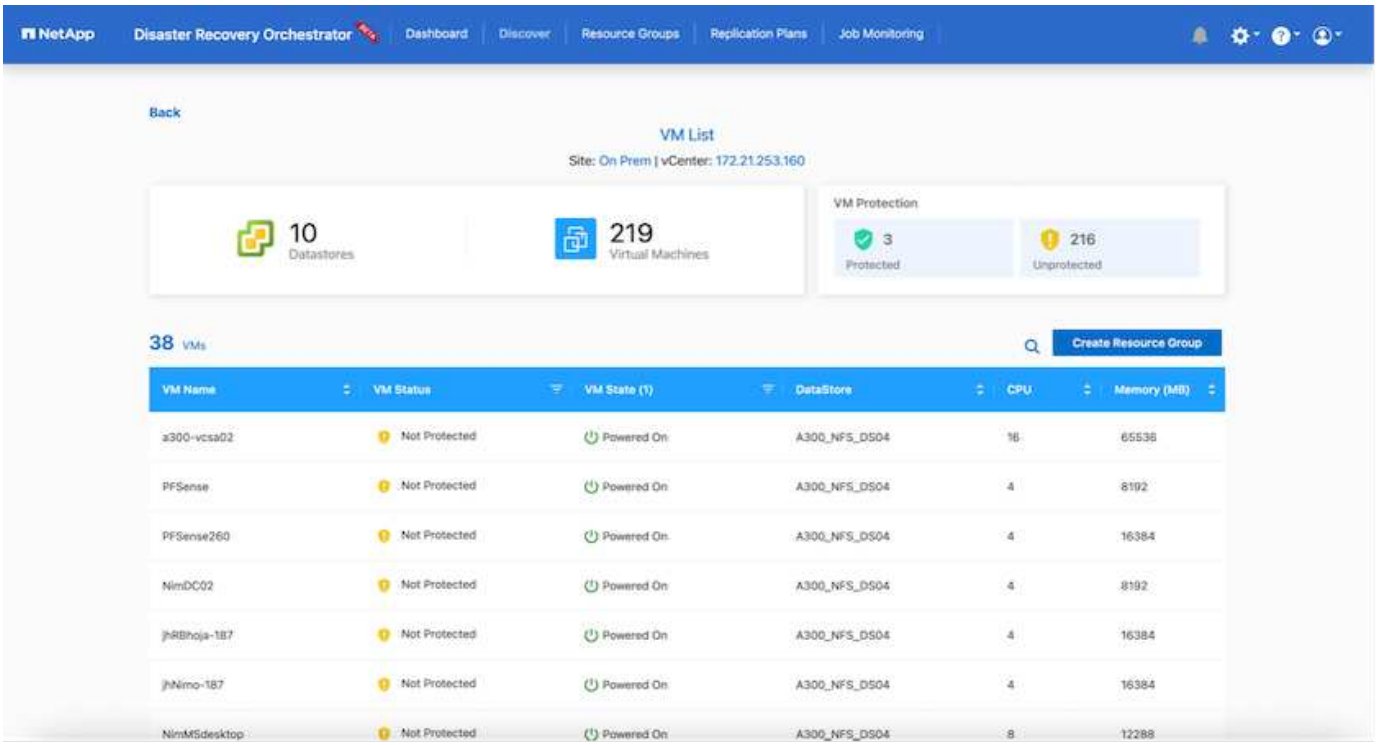
- On-Premises
  - VCenter vor Ort

    - ONTAP Storage-System
- Cloud
    - VMC vCenter
    - FSX für ONTAP





Sobald DRO hinzugefügt wurde, führt die automatische Erkennung durch und zeigt die VMs mit entsprechenden SnapMirror Replikaten vom Quell-Storage auf FSX für ONTAP an. DRO erkennt automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie aus.



Im nächsten Schritt werden die erforderlichen VMs in funktionale Gruppen zusammengefasst, die als Ressourcengruppen dienen.

Ressourcen-Gruppierungen

Nachdem die Plattformen hinzugefügt wurden, können Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen gruppieren. MIT DRO-Ressourcengruppen können Sie eine Gruppe abhängiger VMs zu logischen Gruppen gruppieren, die ihre Boot-Aufträge, Boot-Verzögerungen und optionale Applikationsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

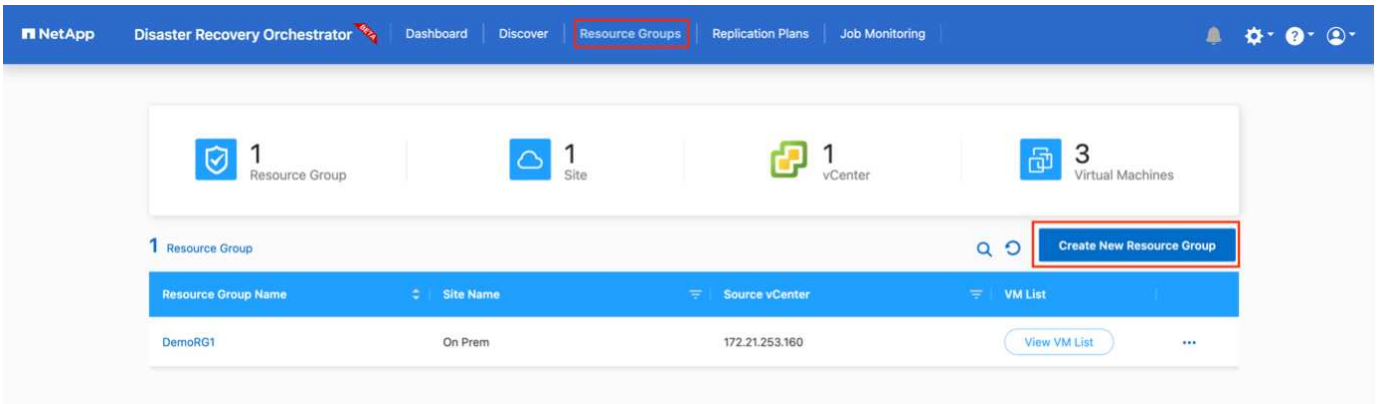
Gehen Sie wie folgt vor, um mit dem Erstellen von Ressourcengruppen zu beginnen:

1. Öffnen Sie **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.
2. Wählen Sie unter **Neue Ressourcengruppe** den Quellstandort aus der Dropdown-Liste aus und klicken Sie auf **Erstellen**.
3. Geben Sie **Ressourcengruppendetails** an und klicken Sie auf **Weiter**.
4. Wählen Sie über die Suchoption die entsprechenden VMs aus.
5. Wählen Sie die Startreihenfolge und die Boot-Verzögerung (Sek.) für die ausgewählten VMs aus. Legen Sie die Reihenfolge des Einschaltvorgangs fest, indem Sie jede VM auswählen und deren Priorität festlegen. Drei ist der Standardwert für alle VMs.

   Folgende Optionen stehen zur Verfügung:

   1 – die erste virtuelle Maschine, die 3 – Standard 5 – die letzte virtuelle Maschine, die eingeschaltet werden soll

6. Klicken Sie Auf **Ressourcengruppe Erstellen**.

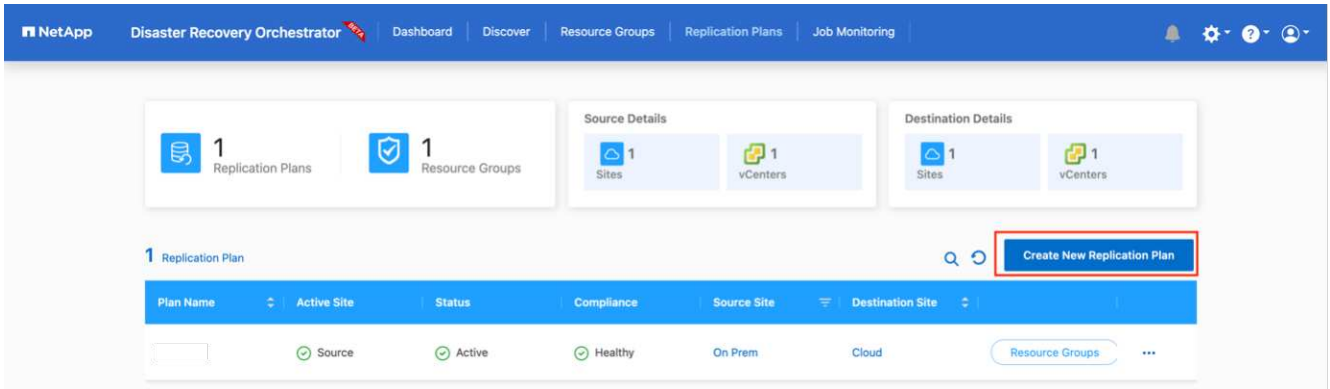


Replizierungspläne

Sie benötigen einen Plan für die Wiederherstellung von Applikationen bei einem Ausfall. Wählen Sie in der Dropdown-Liste die Quell- und Ziel-vCenter Plattformen aus und wählen Sie die Ressourcengruppen aus, die in diesen Plan enthalten sein sollen. Außerdem werden die Gruppen gruppiert, wie Applikationen wiederhergestellt und eingeschaltet werden sollen (z. B. Domänencontroller, dann Tier-1, dann Tier-2 usw.). Solche Pläne werden manchmal auch als Blueprints bezeichnet. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Neuer Replikationsplan**.

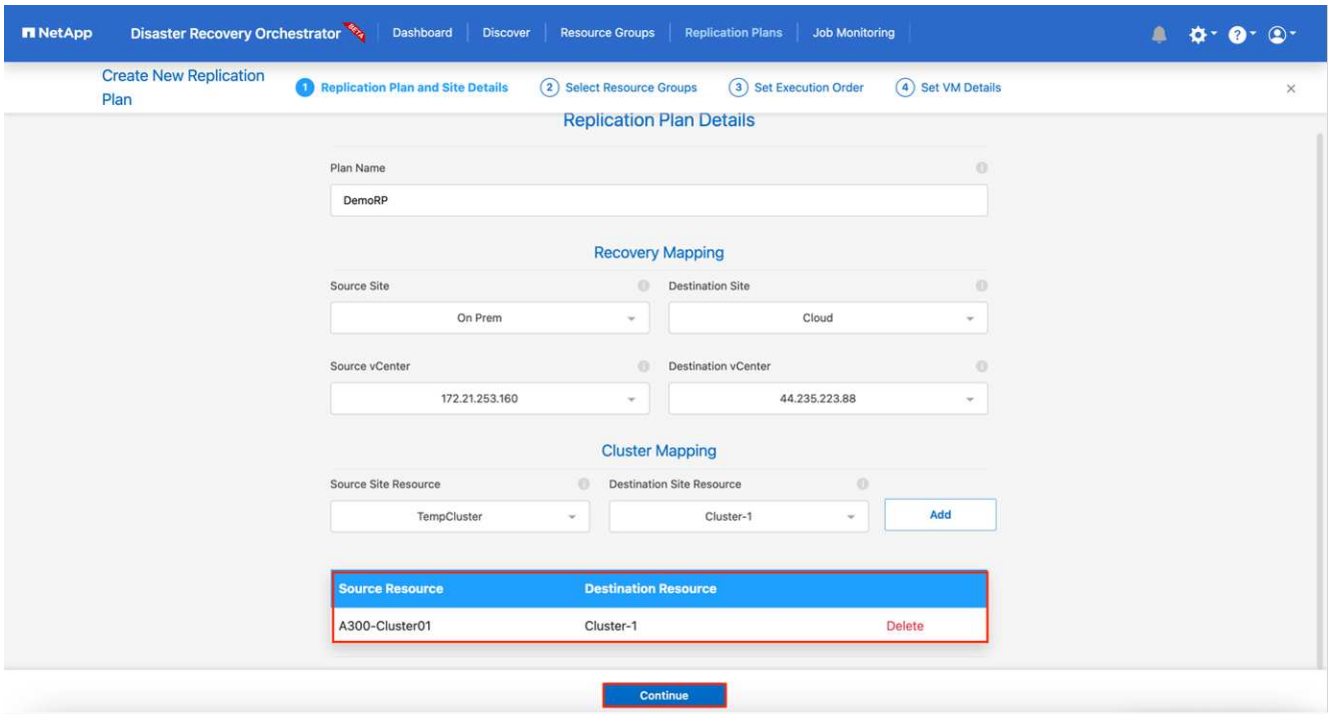
Gehen Sie wie folgt vor, um mit der Erstellung eines Replikationsplans zu beginnen:

1. Öffnen Sie **Replikationspläne**, und klicken Sie auf **Neuen Replikationsplan erstellen**.



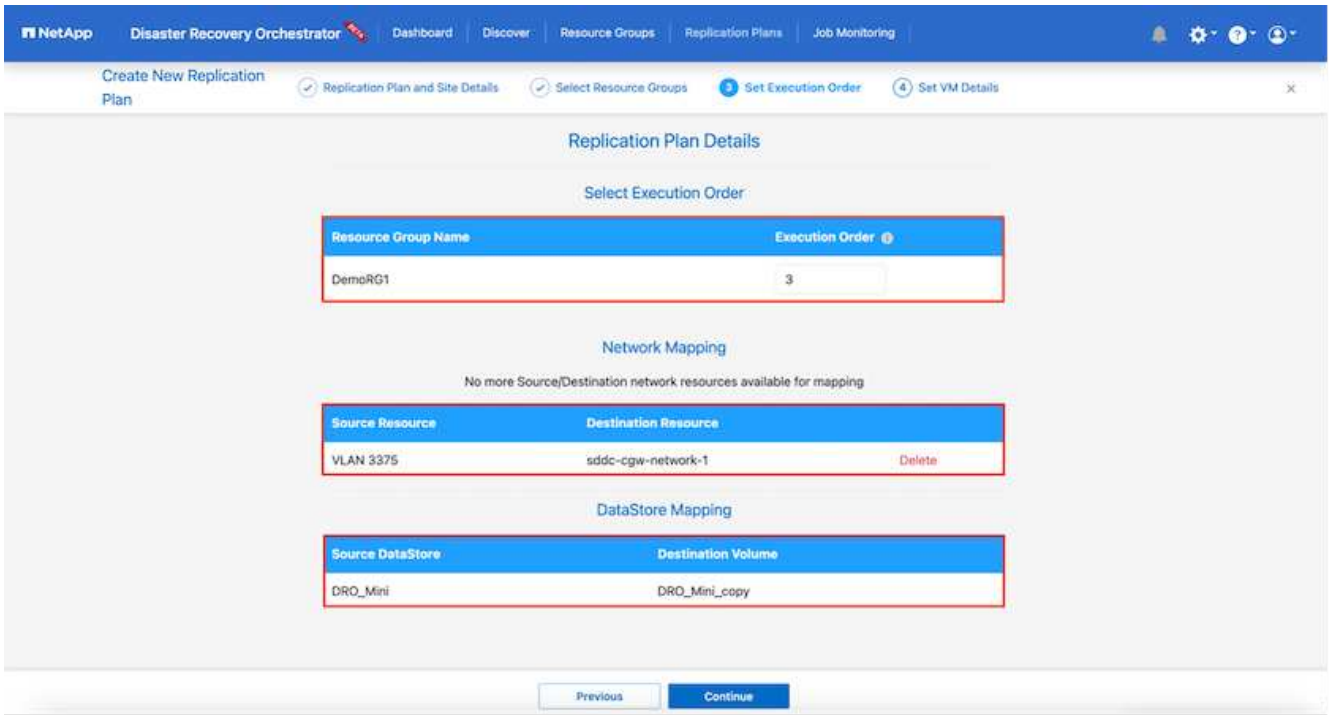
2. Geben Sie unter **New Replication Plan** einen Namen für den Plan ein und fügen Sie Recovery Mappings hinzu, indem Sie den Quellstandort, das zugehörige vCenter, den Zielstandort und das zugehörige vCenter auswählen.

3. Wählen Sie nach Abschluss der Recovery-Zuordnung die Cluster-Zuordnung aus.

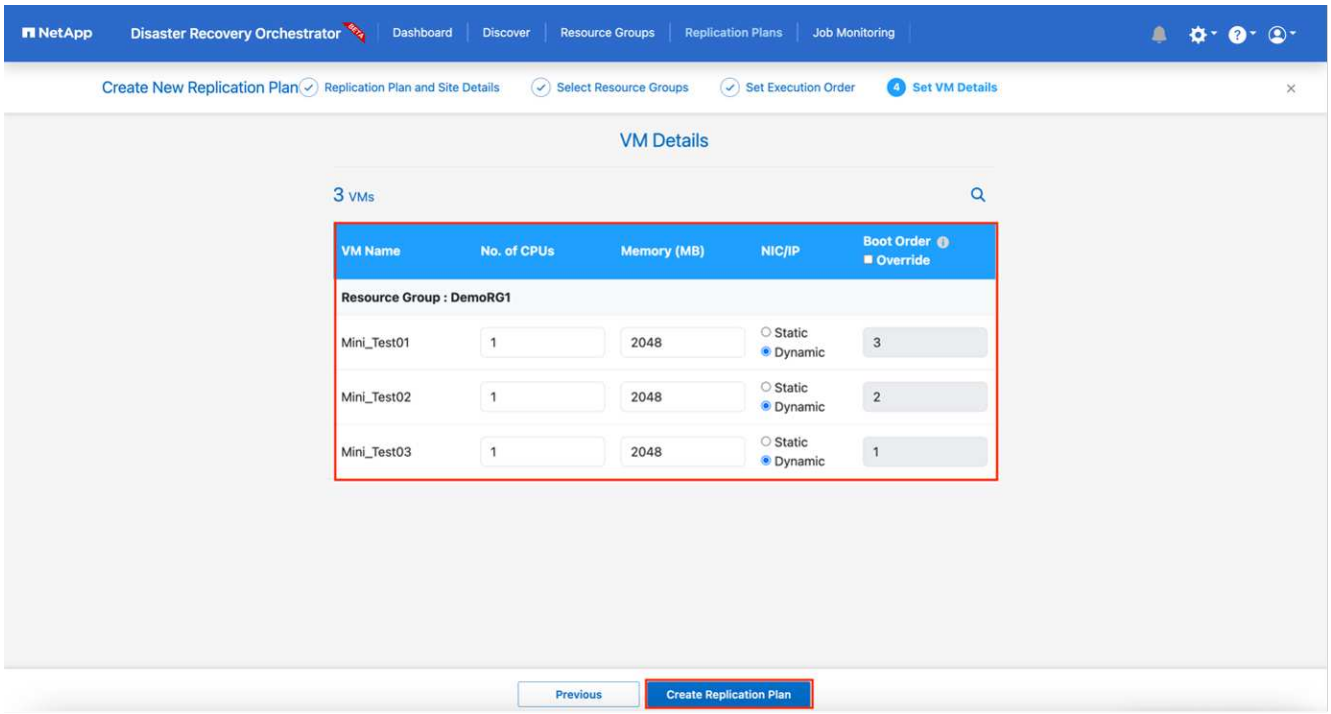


4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
6. Wählen Sie nach dem Beenden die Netzwerkzuordnung zum entsprechenden Segment aus. Die Segmente sollten bereits innerhalb des VMC bereitgestellt werden, wählen Sie also das entsprechende Segment aus, um die VM zuzuordnen.
7. Je nach Auswahl der VMs werden automatisch Datastore-Zuordnungen ausgewählt.

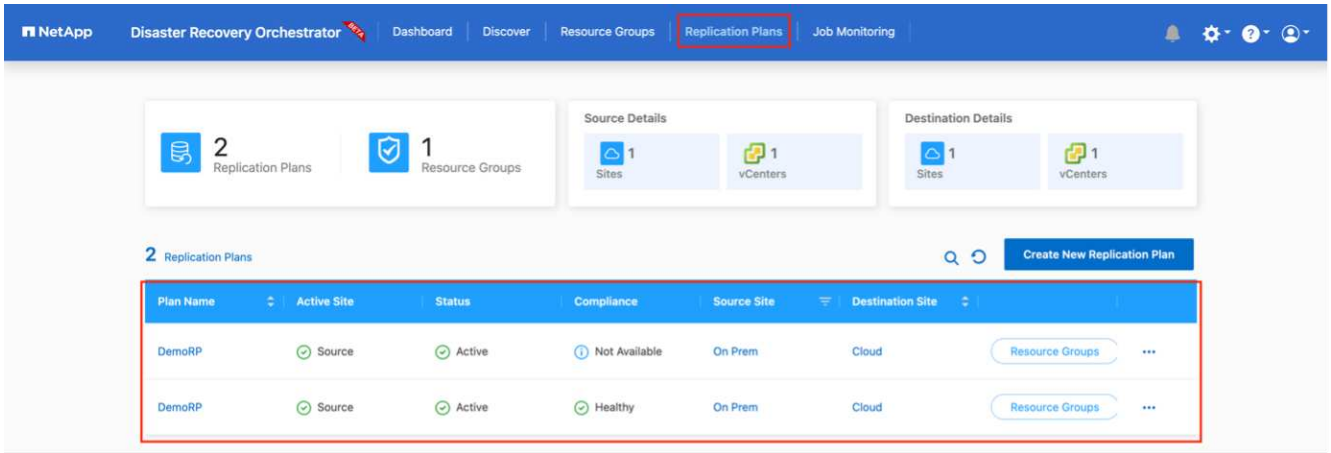
> SnapMirror befindet sich auf Volume-Ebene. Daher werden alle VMs zum Replizierungsziel repliziert. Vergewissern Sie sich, dass alle VMs ausgewählt sind, die Teil des Datastores sind. Sind sie nicht ausgewählt, werden nur die VMs verarbeitet, die Teil des Replikationsplans sind.



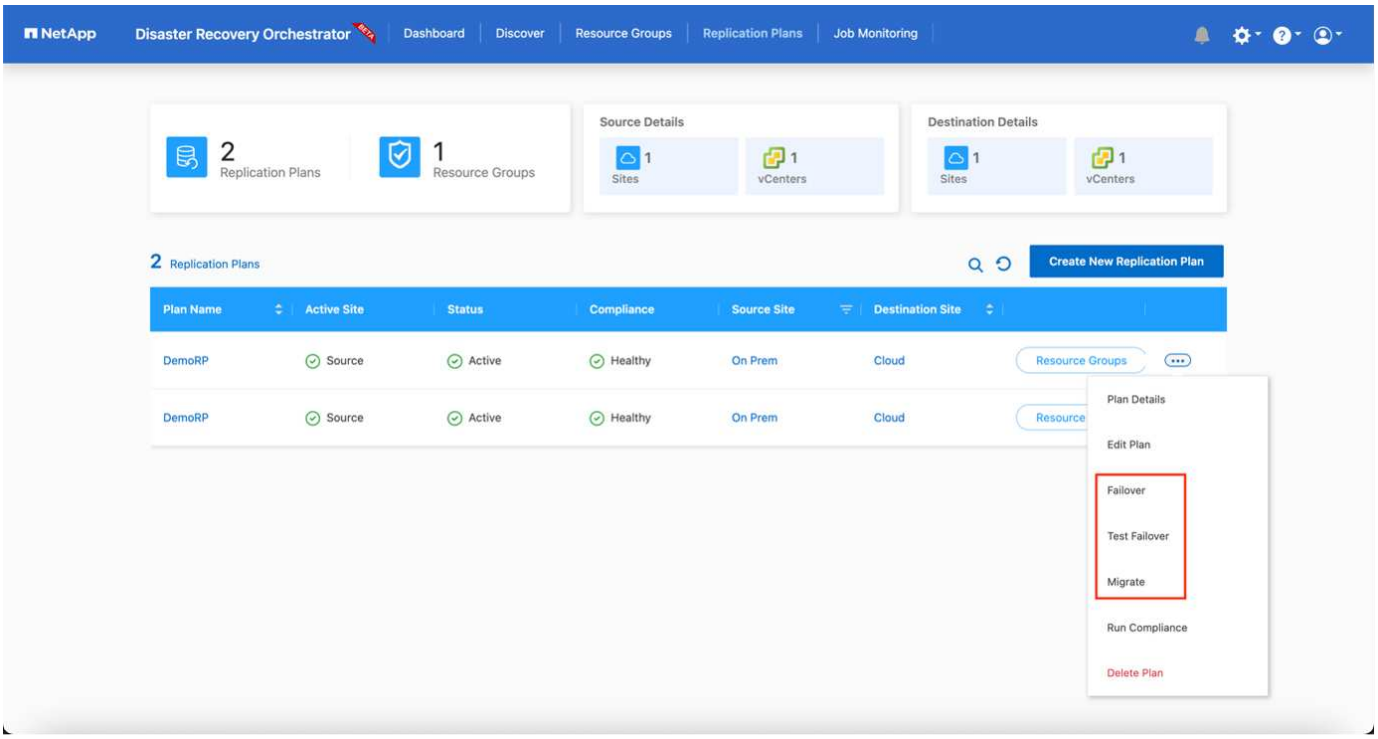
8. Unter den VM-Details können Sie optional die Größe der CPU- und RAM-Parameter der VM ändern. Dies kann sich sehr hilfreich erweisen, wenn Sie große Umgebungen auf kleinere Zielcluster wiederherstellen oder DR-Tests durchführen möchten, ohne eine eineineineineinone physische VMware-Infrastruktur bereitstellen zu müssen. Zudem können Sie die Boot-Reihenfolge und die Boot-Verzögerung (Sekunden) für alle ausgewählten VMs innerhalb der Ressourcengruppen ändern. Es gibt eine zusätzliche Option, um die Startreihenfolge zu ändern, wenn Änderungen von den während der Auswahl der Ressourcengruppe ausgewählten Änderungen erforderlich sind. Standardmäßig wird die während der Ressourcengruppenauswahl ausgewählte Startreihenfolge verwendet. Änderungen können jedoch in dieser Phase vorgenommen werden.

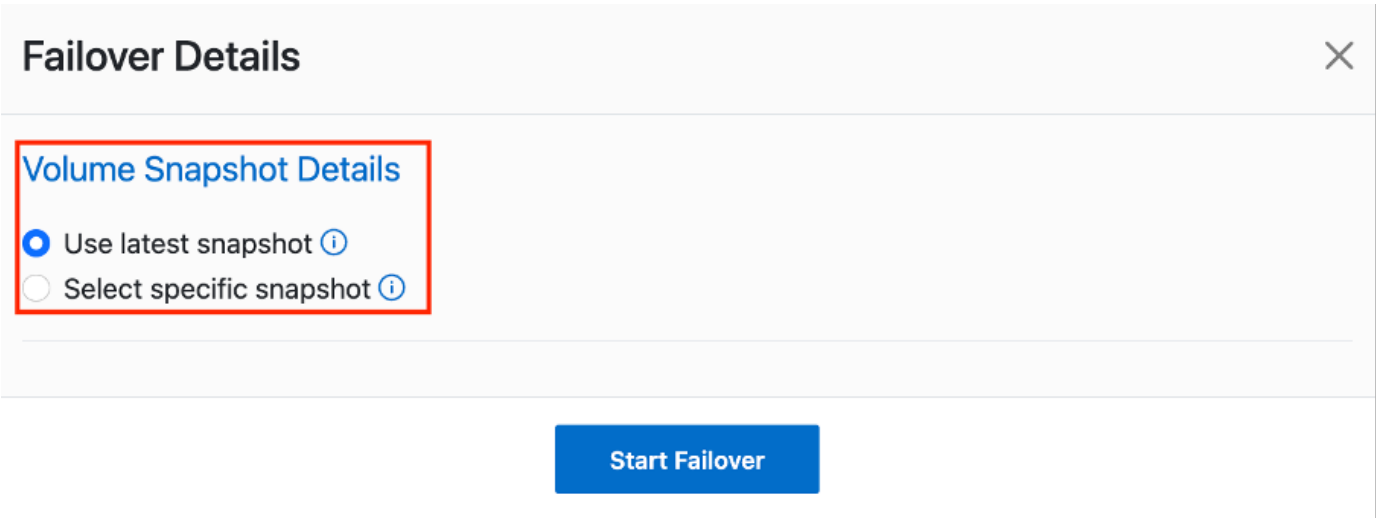


9. Klicken Sie Auf **Replikationsplan Erstellen**.

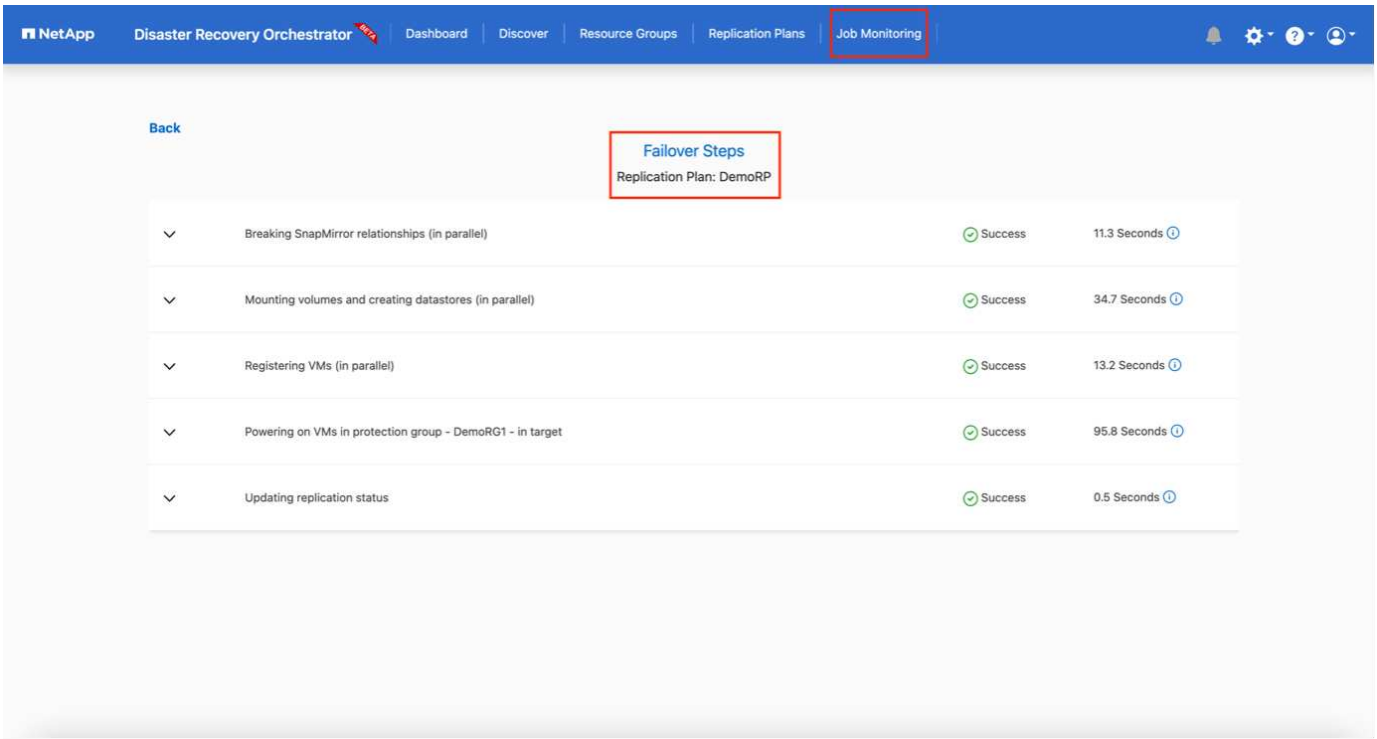


Nach dem Erstellen des Replizierungsplans können je nach Anforderungen die Failover-Option, die Test-Failover-Option oder die Migrationsoption ausgeübt werden. Während der Failover- und Test-Failover-Optionen wird die aktuellste SnapMirror Snapshot Kopie verwendet. Zudem kann aus einer zeitpunktgenauen Snapshot Kopie (gemäß der Aufbewahrungsrichtlinie von SnapMirror) eine bestimmte Snapshot Kopie ausgewählt werden. Die Point-in-Time-Option ist besonders dann hilfreich, wenn ein Korruptionsereignis wie Ransomware anfällt, wenn die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. DRO zeigt alle verfügbaren Punkte in der Zeit an. Um Failover oder Failover-Tests mit der im Replikationsplan angegebenen Konfiguration auszulösen, können Sie auf **Failover** oder **Test Failover** klicken.

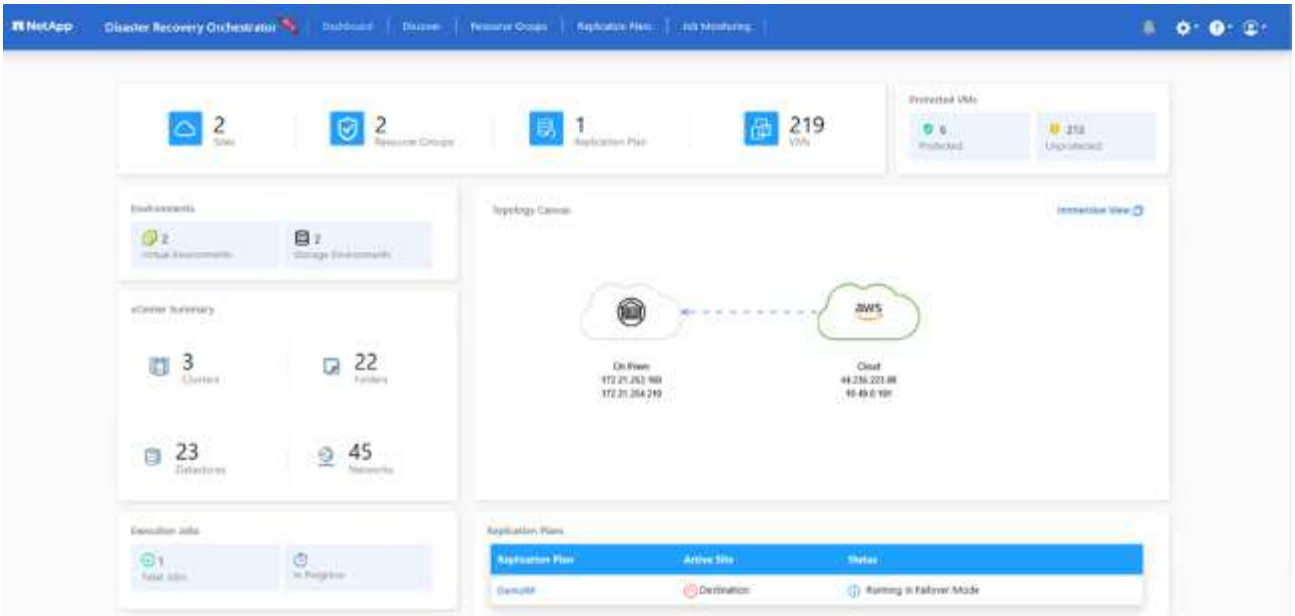




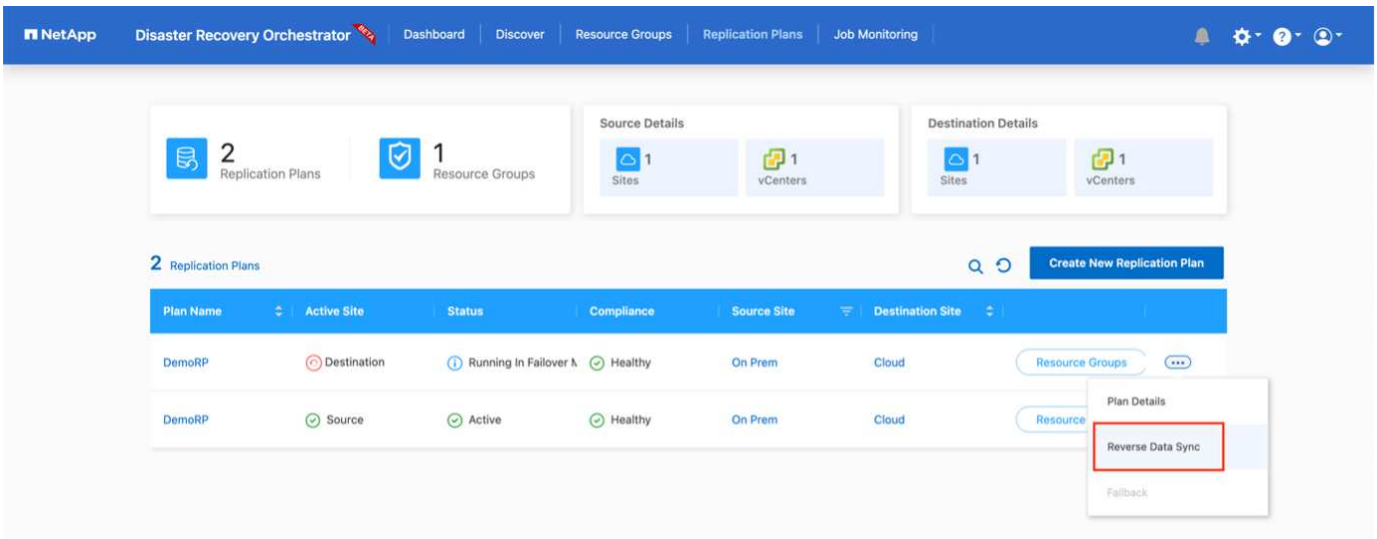
Der Replikationsplan kann im Aufgabenmenü überwacht werden:

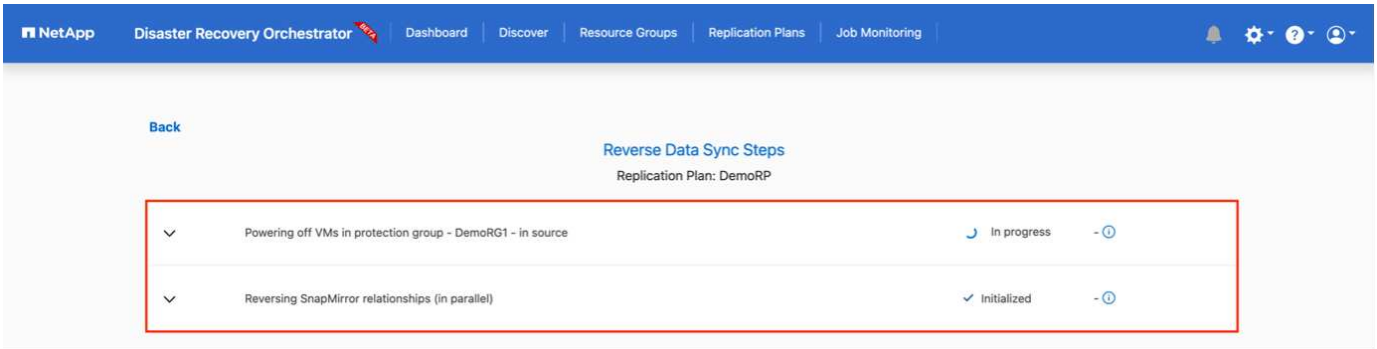


Nach der Auslösung des Failover sind die wiederhergestellten Elemente in VMC vCenter (VMs, Netzwerke, Datastores) ersichtlich. Standardmäßig werden die VMs in den Workload-Ordner wiederhergestellt.

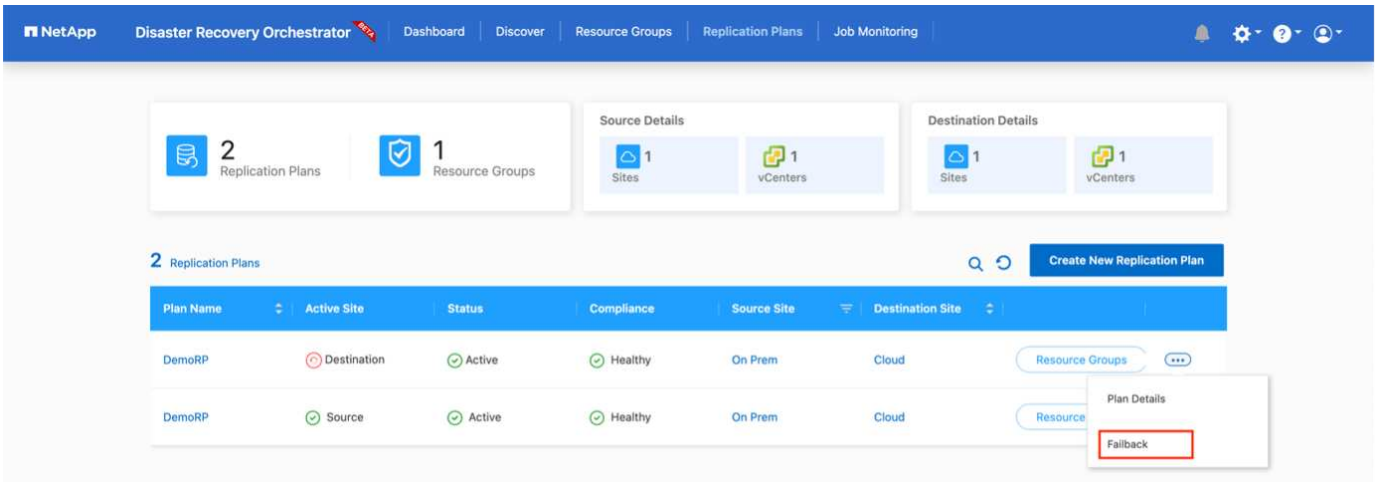


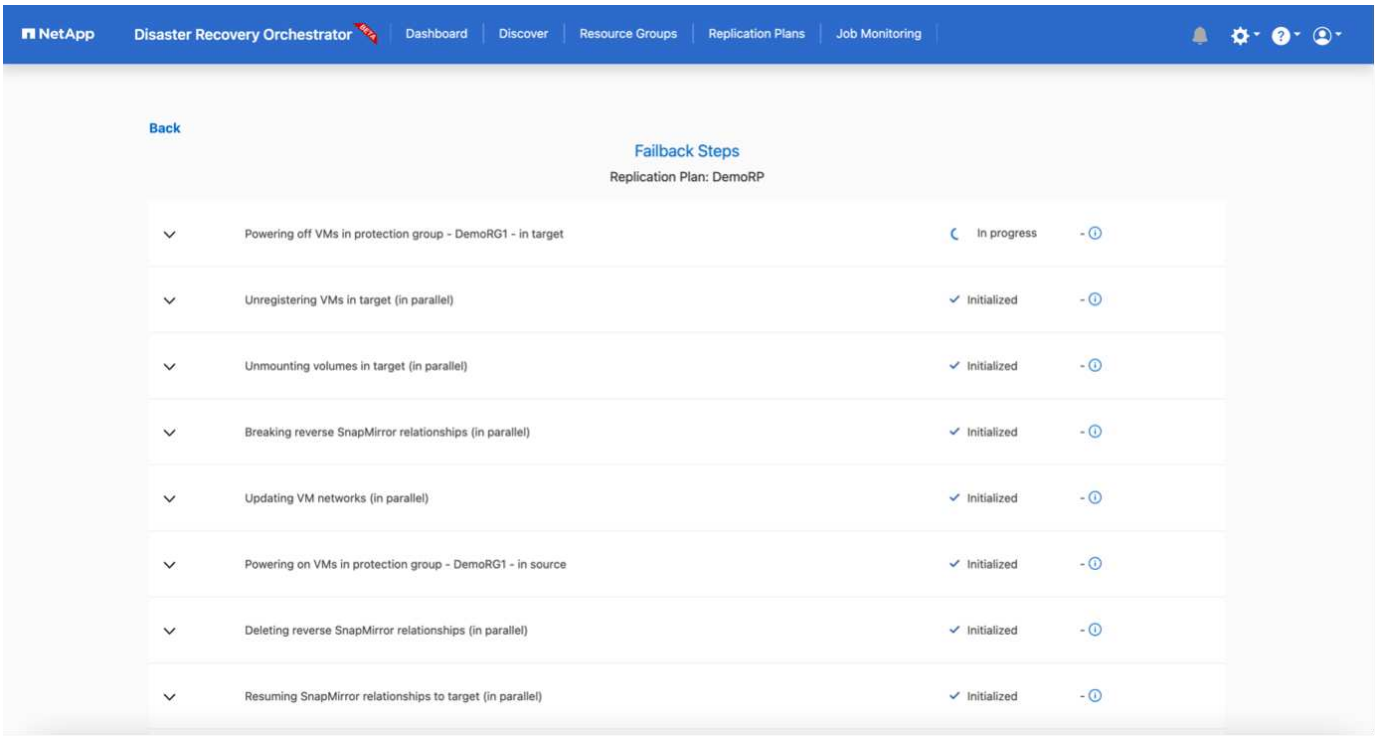
Failback kann auf der Ebene des Replikationsplans ausgelöst werden. Bei einem Test-Failover kann mit der Option „Tear-Down“ ein Rollback der Änderungen durchgeführt und die FlexClone Beziehung entfernt werden. Failback ist in Verbindung mit Failover ein Prozess in zwei Schritten. Wählen Sie den Replikationsplan aus und wählen Sie **Datensynchronisation umkehren**.



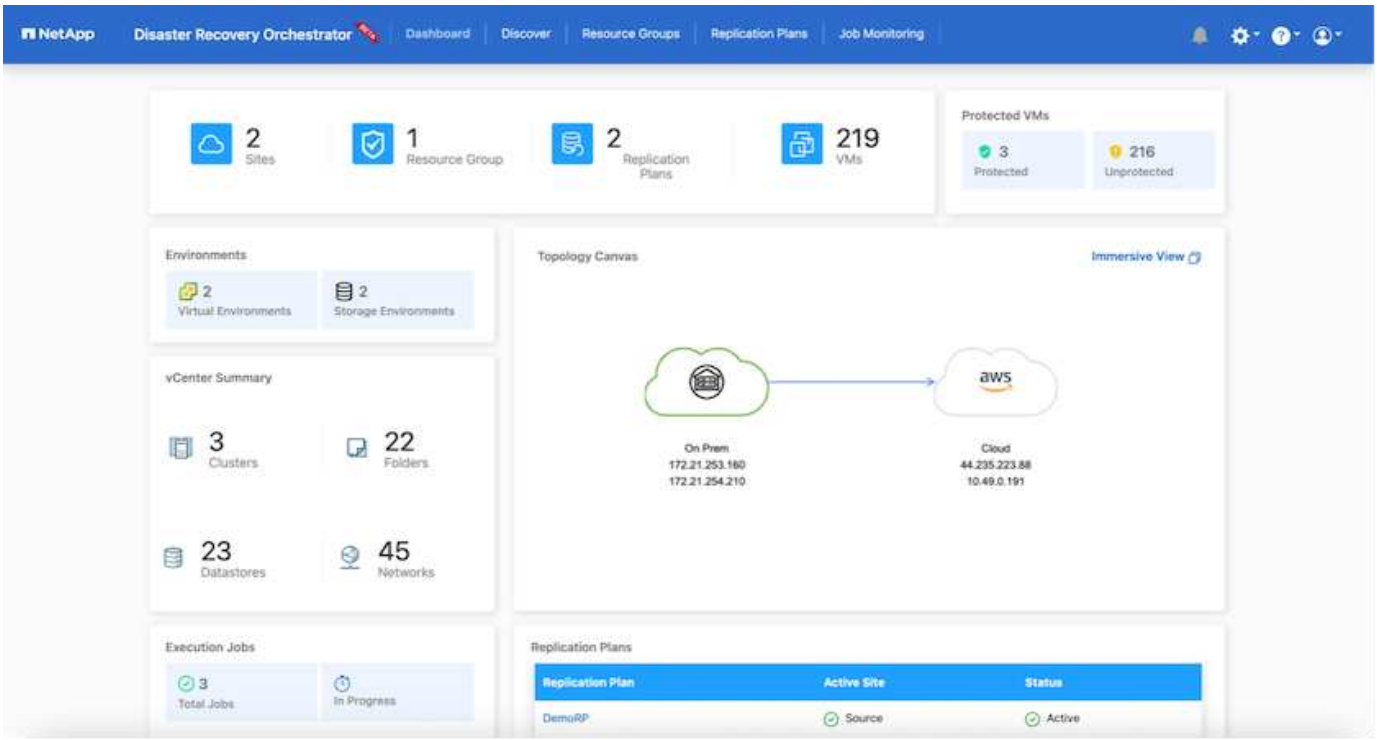


Wenn dieser Vorgang abgeschlossen ist, können Sie ein Failback auslösen und zum ursprünglichen Produktionsstandort zurückkehren.





Aus NetApp BlueXP können wir sehen, dass die Replikationsintegrität für die entsprechenden Volumes (die auf VMC als Read-Write-Volumes zugeordnet wurden) aufgebrochen ist. Beim Test-Failover weist DRO nicht das Ziel- oder Replikatvolume zu. Stattdessen wird eine FlexClone Kopie der erforderlichen SnapMirror Instanz (oder Snapshot) erstellt und die FlexClone Instanz offenlegt, die keine zusätzliche physische Kapazität für FSX für ONTAP beansprucht. Dadurch wird sichergestellt, dass das Volume nicht geändert wird und Replikatjobs sogar während DR-Tests oder während der Triage-Workflows fortgesetzt werden können. Darüber hinaus stellt dieser Prozess sicher, dass bei Auftreten von Fehlern oder beschädigten Daten die Wiederherstellung bereinigt werden kann, ohne dass das Replikat zerstört werden könnte.



Recovery durch Ransomware

Die Wiederherstellung von Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Abteilungen schwierig sein, einen Punkt zu bestimmen, an dem sich der sichere Rückgabepunkt befindet und nach dem wir festgestellt haben, dass sie wiederhergestellte Workloads vor erneuten Angriffen, beispielsweise durch schlafende Malware oder anfällige Anwendungen, schützen.

DRO behebt diese Bedenken, indem Sie Ihr System von jedem beliebigen verfügbaren Zeitpunkt wiederherstellen können. Zudem können Sie Workloads in funktionellen und dennoch isolierten Netzwerken wiederherstellen, damit Applikationen an einem Standort ohne North-South-Datenverkehr miteinander kommunizieren und arbeiten können. So erhält Ihr Sicherheitsteam einen sicheren Ort, um Forensik durchzuführen und sicherzustellen, dass keine verborgene oder schlafende Malware vorhanden ist.

Vorteile

- Nutzung der effizienten und robusten SnapMirror Replizierung.
- Recovery zu jedem verfügbaren Zeitpunkt mit Aufbewahrung von Snapshot Kopien
- Vollständige Automatisierung aller erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden VMs in den Schritten für Storage, Computing, Netzwerk und Applikationen
- Workload Recovery mit ONTAP FlexClone Technologie mit einer Methode, bei der das replizierte Volume nicht geändert wird.
  - Vermeidung des Risikos einer Beschädigung von Daten bei Volumes oder Snapshot Kopien
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Potenzielle Nutzung von DR-Daten mit Cloud-Computing-Ressourcen für Workflows über DR hinaus, wie z. B. DevTest, Sicherheitstests, Patch- oder Upgrade-Tests und Korrekturtests
- CPU- und RAM-Optimierung zur Senkung der Cloud-Kosten durch Recovery auf kleinere Computing-Cluster.

Verwenden von Veeam Replizierung und FSX for ONTAP für die Disaster Recovery in VMware Cloud on AWS

Autor: Niyaz Mohamed - NetApp Solutions Engineering

Überblick

Amazon FSX for NetApp ONTAP-Integration in VMware Cloud on AWS ist ein von AWS gemanagter externer NFS-Datastore, der auf dem NetApp ONTAP-Filesystem basiert und mit einem Cluster im SDDC verbunden werden kann. Sie bietet Kunden eine flexible, hochperformante virtualisierte Storage-Infrastruktur, die unabhängig von den Compute-Ressourcen skaliert werden kann.

Für Kunden, die VMware Cloud on AWS SDDC als Disaster-Recovery-Ziel verwenden möchten, können FSX für ONTAP-Datastores verwendet werden, um Daten aus On-Premises-Umgebungen mithilfe einer beliebigen validierten Drittanbieterlösung mit VM-Replizierungsfunktionen zu replizieren. Durch das Hinzufügen von FSX for ONTAP Datastore wird eine kostenoptimierte Implementierung ermöglicht als die Einrichtung einer VMware Cloud auf AWS SDDC mit einer enormen Menge an ESXi-Hosts, die nur den Storage beherbergen.

Dieser Ansatz hilft Kunden auch, Pilot-Light-Cluster in VMC zusammen mit FSX für ONTAP-Datastores zu verwenden, um VM-Replikate zu hosten. Derselbe Prozess kann auch als Migrationsoption in VMware Cloud on AWS durch ein ordnungsgemäges Failover des Replizierungsplans erweitert werden.

Problemstellung

In diesem Dokument wird beschrieben, wie Sie FSX für ONTAP-Datastore und Veeam Backup and Replication verwenden, um die Disaster-Recovery für lokale VMware-VMs zu VMware Cloud on AWS mithilfe der VM-Replizierungsfunktion einzurichten.

Veeam Backup & Replication ermöglicht On-Site- und Remote-Replizierung für Disaster Recovery (DR). Wenn Virtual Machines repliziert werden, erstellt Veeam Backup & Replication eine exakte Kopie der VMs im nativen VMware vSphere-Format auf dem Ziel-VMware Cloud auf dem AWS SDDC-Cluster und sorgt dafür, dass die Kopie mit der ursprünglichen VM synchronisiert wird.

Die Replizierung bietet den besten RTO-Wert (Recovery Time Objective), da sich eine Kopie einer VM im Bereitschaftszustand befindet. Dieser Replizierungsmechanismus sorgt dafür, dass die Workloads bei einem Ausfall schnell in VMware Cloud on AWS SDDC gestartet werden können. Die Veeam Backup & Replication Software optimiert darüber hinaus die Datenübertragung zur Replizierung über WAN und für langsame Verbindungen. Darüber hinaus werden doppelte Datenblöcke herausgefiltert und keine Datenblöcke eliminiert. Außerdem lassen sich Dateien auslagern und VM Gast-OS-Dateien ausschließen sowie der Daten-Traffic von Replikaten komprimiert.

Um zu verhindern, dass Replikationsjobs die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Regeln zur Netzwerkdrosselung eingerichtet werden. Der Replizierungsprozess in Veeam Backup & Replication ist auftraggesteuert, d. h. die Replizierung wird durch Konfiguration von Replizierungsjobs durchgeführt. Bei einem Ausfall kann ein Failover zur Wiederherstellung der VMs durch einen Failover auf die Replikatkopie ausgelöst werden.

Wenn ein Failover durchgeführt wird, übernimmt eine replizierte VM die Rolle der ursprünglichen VM. Ein Failover kann auf den neuesten Status eines Replikats oder auf einen der bekannten Wiederherstellungspunkte erfolgen. Dies ermöglicht bei Bedarf eine Wiederherstellung nach Ransomware-Angriffen oder isolierte Tests. In Veeam Backup & Replication sind Failover und Failback temporäre Zwischenschritte, die weiter abgeschlossen werden sollten. Veeam Backup & Replication bietet mehrere Optionen für unterschiedliche Disaster-Recovery-Szenarien.

[Diagramm des DR-Szenarios mit Veeam Replizierung und FSX ONTAP für VMC]

Lösungsimplementierung

Übergeordnete Schritte

1. Die Veeam Backup & Replication-Software wird in der On-Premises-Umgebung mit entsprechender Netzwerkkonnektivität ausgeführt.
2. Konfigurieren Sie VMware Cloud on AWS, lesen Sie den Artikel zur VMware Cloud Tech Zone "Implementierungs-Leitfaden zur Integration von VMware Cloud on AWS in Amazon FSX for NetApp ONTAP" Konfigurieren Sie zur Implementierung VMware Cloud on AWS SDDC und FSX for ONTAP als NFS-Datastore. (Für DR-Zwecke kann eine Pilotumgebung mit minimaler Konfiguration verwendet werden. Bei einem Vorfall erfolgt ein Failover von VMs auf dieses Cluster, und es können weitere Nodes hinzugefügt werden).
3. Richten Sie Replikationsjobs ein, um VM-Replikate mit Veeam Backup and Replication zu erstellen.
4. Erstellen eines Failover-Plans und Durchführen eines Failover
5. Wechseln Sie zurück zu den Produktions-VMs, sobald der Notfall abgeschlossen und der primäre Standort eingerichtet ist.

Voraussetzungen für die Veeam VM Replication to VMC und FSX for ONTAP Datastores

1. Stellen Sie sicher, dass die Backup-VM von Veeam Backup & Replication mit dem Quell-vCenter sowie der Ziel-VMware-Cloud auf AWS SDDC-Clustern verbunden ist.
2. Der Backup-Server muss in der Lage sein, Kurznamen aufzulösen und eine Verbindung zu Quell- und Ziel-vCenter herzustellen.
3. Das Ziel-FSX für ONTAP Datastore muss über genügend freien Speicherplatz verfügen, um VMDKs von replizierten VMs zu speichern

Weitere Informationen finden Sie unter „Überlegungen und Einschränkungen“ "Hier".

Einzelheiten Zur Bereitstellung

Schritt: Replizierung von VMs

Veeam Backup & Replication nutzt VMware vSphere Snapshot-Funktionen. Veeam Backup & Replication fordert während der Replizierung VMware vSphere zur Erstellung eines VM-Snapshots an. Der VM-Snapshot ist die zeitpunktgenaue Kopie einer VM, die virtuelle Festplatten, Systemstatus, Konfiguration usw. umfasst. Veeam Backup & Replication verwendet den Snapshot als Datenquelle für die Replizierung.

Gehen Sie wie folgt vor, um VMs zu replizieren:

1. Öffnen Sie die Veeam Backup & Replication Console.
2. Wählen Sie in der Home-Ansicht Replikationsjob > Virtuelle Maschine > VMware vSphere aus.
3. Geben Sie einen Jobnamen an, und aktivieren Sie das entsprechende Kontrollkästchen für die erweiterte Steuerung. Klicken Sie Auf Weiter.
   - Aktivieren Sie das Kontrollkästchen Replikat-Seeding, wenn bei der Verbindung zwischen On-Premises und AWS eine eingeschränkte Bandbreite vorhanden ist.
   - Aktivieren Sie das Kontrollkästchen Network Remapping (für AWS VMC-Standorte mit unterschiedlichen Netzwerken), wenn Segmente auf VMware Cloud on AWS SDDC nicht mit denen auf lokalen Standortnetzwerken übereinstimmen.
   - Wenn sich das IP-Adressierungsschema am Produktionsstandort vor Ort vom Schema am AWS VMC-Standort unterscheidet, aktivieren Sie das Kontrollkästchen Replica RE-IP (für DR-Standorte mit unterschiedlichem IP-Adressierungsschema).

     [dr veeam fsx image2] | *dr-veeam-fsx-image2.png*
4. Wählen Sie im Schritt **Virtual Machines** die VMs aus, die zum FSX for ONTAP-Datastore repliziert werden müssen, der mit VMware Cloud on AWS SDDC verbunden ist. Die Virtual Machines können auf vSAN platziert werden, um die verfügbare vSAN Datastore-Kapazität zu füllen. In einem Pilotcluster wird die nutzbare Kapazität eines 3-Knoten-Clusters begrenzt. Die restlichen Daten können auf FSX für ONTAP-Datenspeicher repliziert werden. Klicken Sie auf **Hinzufügen**, wählen Sie dann im Fenster **Objekt hinzufügen** die erforderlichen VMs oder VM-Container aus und klicken Sie auf **Hinzufügen**. Klicken Sie Auf **Weiter**.

   [dr veeam fsx image3] | *dr-veeam-fsx-image3.png*
5. Wählen Sie anschließend das Ziel als VMware Cloud on AWS SDDC Cluster/Host und den entsprechenden Ressourcen-Pool, VM-Ordner und FSX for ONTAP Datastore für VM-Replikate aus. Klicken Sie Dann Auf **Weiter**.

   [dr veeam fsx image4] | *dr-veeam-fsx-image4.png*
6. Erstellen Sie im nächsten Schritt die Zuordnung zwischen dem virtuellen Quell- und Zielnetzwerk nach Bedarf.

   [dr veeam fsx image5] | *dr-veeam-fsx-image5.png*
7. Geben Sie im Schritt **Job-Einstellungen** das Backup-Repository an, in dem Metadaten für VM-Replikate, Aufbewahrungsrichtlinien usw. gespeichert werden.
8. Aktualisieren Sie die Proxy-Server **Source** und **Target** im Schritt **Data Transfer** und lassen Sie die Option **Automatic** (Standard) und halten Sie die Option **Direct** ausgewählt und klicken Sie auf **Next**.
9. Wählen Sie im Schritt **Gastverarbeitung** die Option **anwendungsorientierte Verarbeitung aktivieren** nach Bedarf aus. Klicken Sie Auf **Weiter**.

[dr veeam fsx image6] | *dr-veeam-fsx-image6.png*

10. Wählen Sie den Replikationszeitplan aus, um den Replikationsjob regelmäßig auszuführen.
11. Überprüfen Sie im Schritt **Zusammenfassung** des Assistenten die Details des Replikationsjobs. Um den Job direkt nach dem Schließen des Assistenten zu starten, aktivieren Sie das Kontrollkästchen **Job ausführen, wenn ich auf Fertig stellen klicke**, andernfalls lassen Sie das Kontrollkästchen deaktiviert. Klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.

    [dr veeam fsx image7] | *dr-veeam-fsx-image7.png*

Sobald der Replikationsjob gestartet wurde, werden die VMs mit dem angegebenen Suffix auf dem Ziel-VMC SDDC-Cluster/Host gefüllt.

[dr veeam fsx image8] | *dr-veeam-fsx-image8.png*

Weitere Informationen zur Veeam-Replizierung finden Sie unter "Funktionsweise Der Replikation".

Schritt 2: Erstellen eines Failover-Plans

Erstellen Sie nach Abschluss der ersten Replikation oder des Seeding den Failover-Plan. Mithilfe des Failover-Plans können Sie ein Failover für abhängige VMs einzeln oder als Gruppe automatisch durchführen. Der Failover-Plan ist das Modell für die Reihenfolge, in der die VMs verarbeitet werden, einschließlich der Boot-Verzögerungen. Der Failover-Plan trägt außerdem dazu bei, sicherzustellen, dass kritische abhängige VMs bereits laufen.

Um den Plan zu erstellen, navigieren Sie zum neuen Unterabschnitt „Replikate“, und wählen Sie „Failover-Plan“ aus. Wählen Sie die entsprechenden VMs aus. Veeam Backup & Replication sucht nach den nächstgelegenen Wiederherstellungspunkten zu diesem Zeitpunkt und verwendet diese, um VM-Replikate zu starten.

> Der Failover-Plan kann nur hinzugefügt werden, wenn die erste Replikation abgeschlossen ist und sich die VM-Replikate im Bereitschaftszustand befinden.

> Es können maximal 10 VMs gleichzeitig gestartet werden, wenn ein Failover-Plan ausgeführt wird.

> Während des Failover-Prozesses werden die Quell-VMs nicht ausgeschaltet.

Um den **Failover Plan** zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Home-Ansicht **Failover-Plan > VMware vSphere** aus.
2. Geben Sie als Nächstes einen Namen und eine Beschreibung für den Plan ein. Pre- und Post-Failover-Skript können bei Bedarf hinzugefügt werden. Führen Sie beispielsweise ein Skript aus, um die VMs vor dem Starten der replizierten VMs herunterzufahren.

   [dr veeam fsx image9] | *dr-veeam-fsx-image9.png*

3. Fügen Sie die VMs zum Plan hinzu und ändern Sie die VM-Startreihenfolge und die Boot-Verzögerungen, um die Applikationsabhängigkeiten zu erfüllen.

   [dr veeam fsx image10] | *dr-veeam-fsx-image10.png*

Weitere Informationen zum Erstellen von Replikationsjobs finden Sie unter "Erstellen Von Replikationsjobs".

Schritt 3: Führen Sie den Failover-Plan aus

Bei einem Failover wird die Quell-VM am Produktionsstandort auf ihr Replikat am Disaster-Recovery-Standort umgeschaltet. Im Rahmen des Failover-Prozesses stellt Veeam Backup & Replication das VM-Replikat zum erforderlichen Wiederherstellungspunkt wieder her und verschiebt alle I/O-Aktivitäten von der Quell-VM auf das Replikat. Replikate können nicht nur im Notfall verwendet werden, sondern auch DR-Übungen simulieren. Während der Failover-Simulation bleibt die Quell-VM aktiv. Sobald alle erforderlichen Tests durchgeführt wurden, können Sie das Failover rückgängig machen und zum normalen Betrieb zurückkehren.

> Stellen Sie sicher, dass eine Netzwerksegmentierung vorhanden ist, um IP-Konflikte während des DR-Bohrvorgangs zu vermeiden.

Um den Failover Plan zu starten, klicken Sie einfach auf die Registerkarte **Failover Plans** und klicken Sie mit der rechten Maustaste auf den Failover Plan. Wählen Sie **Start**. Dabei wird ein Failover mit den neuesten Wiederherstellungspunkten der VM-Replikate durchgeführt. Um ein Failover zu bestimmten Wiederherstellungspunkten von VM-Replikaten durchzuführen, wählen Sie **Start to** aus.

[dr veeam fsx image11] | *dr-veeam-fsx-image11.png*

[dr veeam fsx image12] | *dr-veeam-fsx-image12.png*

Der Status der VM-Replikate ändert sich von „bereit“ zu „Failover“, und die VMs werden auf dem Ziel VMware Cloud auf dem AWS SDDC-Cluster/Host gestartet.

[dr veeam fsx image13] | *dr-veeam-fsx-image13.png*

Sobald der Failover abgeschlossen ist, ändert sich der Status der VMs in „Failover“.

[dr veeam fsx image14] | *dr-veeam-fsx-image14.png*

> Veeam Backup & Replication hält alle Replikationsaktivitäten für die Quell-VM an, bis das Replikat in den Bereitschaftszustand zurückkehrt.

Ausführliche Informationen zu Failover-Plänen finden Sie unter "Failover-Pläne".

Schritt 4: Failback zum Produktionsstandort

Wenn der Failover-Plan ausgeführt wird, gilt er als Zwischenschritt und muss basierend auf den Anforderungen abgeschlossen werden. Folgende Optionen stehen zur Verfügung:

- **Failback zur Produktion** - Wechseln Sie zurück zur ursprünglichen VM und übertragen Sie alle Änderungen, die während des VM-Replikats auf die ursprüngliche VM ausgeführt wurden.

> Wenn Sie ein Failback durchführen, werden die Änderungen nur übertragen, aber nicht veröffentlicht. Wählen Sie **commit Failback** (sobald bestätigt wurde, dass die ursprüngliche VM wie erwartet funktioniert) oder **Undo Failback**, um zum VM-Replikat zurückzukehren, wenn die ursprüngliche VM nicht wie erwartet funktioniert.

- **Rückgängigmachen des Failover** - Wechseln Sie zurück zur ursprünglichen VM und verwerfen Sie alle Änderungen, die während der Ausführung am VM-Replikat vorgenommen wurden.
- **Permanent Failover** - Wechseln Sie dauerhaft von der ursprünglichen VM auf ein VM-Replikat und verwenden Sie dieses Replikat als ursprüngliche VM.

In dieser Demo wurde „Failback zur Produktion“ gewählt. Failback auf die ursprüngliche VM wurde während des Zielschritts des Assistenten ausgewählt und das Kontrollkästchen „VM nach der Wiederherstellung einschalten“ war aktiviert.

[dr veeam fsx image15] | *dr-veeam-fsx-image15.png*

[dr veeam fsx image16] | *dr-veeam-fsx-image16.png*

Failback-Commit ist eine der Möglichkeiten, den Failback-Vorgang abzuschließen. Wenn Failback durchgeführt wird, wird bestätigt, dass die an die zurückgeschickte VM (die Produktions-VM) gesendeten Änderungen wie erwartet funktionieren. Nach dem Commit-Vorgang setzt Veeam Backup & Replication die Replizierungsaktivitäten für die Produktions-VM fort.

Detaillierte Informationen zum Failback-Prozess finden Sie in der Veeam-Dokumentation für "Failover und Failback für die Replikation".

[dr veeam fsx image17] | *dr-veeam-fsx-image17.png*

[dr veeam fsx image18] | *dr-veeam-fsx-image18.png*

Nach einem erfolgreichen Failback zur Produktion werden die VMs alle auf den ursprünglichen Produktionsstandort zurückgestellt.

[dr veeam fsx image19] | *dr-veeam-fsx-image19.png*

Schlussfolgerung

Mit der Funktion FSX for ONTAP Datastore kann Veeam oder jedes beliebige validierte Drittanbieter-Tool eine kostengünstige DR-Lösung mit Pilot Light-Cluster bereitstellen, ohne eine große Anzahl von Hosts im Cluster einzurichten, nur um die VM-Replikatkopie aufzunehmen. Dies bietet eine leistungsstarke Lösung für einen individuellen Disaster-Recovery-Plan und ermöglicht zudem die interne Wiederverwendung vorhandener Backup-Produkte zur Erfüllung der DR-Anforderungen. Auf diese Weise ist eine Cloud-basierte Disaster Recovery durch das Beenden von DR-Datacentern vor Ort möglich. Failover lässt sich als geplanter Failover oder Failover mit einem Mausklick durchführen, wenn ein Notfall eintritt, und es wird entschieden, den DR-Standort zu aktivieren.

Wenn Sie mehr über diesen Prozess erfahren möchten, folgen Sie bitte dem detaillierten Video zum Rundgang.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a