Öffentliche und hybride Cloud

NetApp Solutions

NetApp
May 10, 2024

Inhalt

Öffentliche und hybride Cloud

NetApp Hybrid-Multi-Cloud mit VMware Lösungen

VMware für Public Cloud

Überblick über NetApp Hybrid-Multi-Cloud mit VMware

Die meisten IT-Abteilungen verfolgen den Hybrid-Cloud-First-Ansatz. Diese Unternehmen befinden sich in einer Transformationsphase, und Kunden bewerten ihre aktuelle IT-Umgebung und migrieren ihre Workloads anschließend anhand des Assessments und der Bestandsaufnahme in die Cloud.

Zu den Faktoren für Kunden, die eine Migration zur Cloud durchführen, gehören Flexibilität und Burst, der Ausstieg aus dem Datacenter, die Datacenter-Konsolidierung, End-of-Life-Szenarien, Fusionen, Firmenübernahmen usw. Der Grund für diese Migration kann je nach Unternehmen und ihren jeweiligen Geschäftsprioritäten variieren. Beim Wechsel in die Hybrid Cloud ist die Wahl des richtigen Storage in der Cloud sehr wichtig, um die Vorteile der Cloud-Implementierung und -Flexibilität auszuschöpfen.

VMware Cloud-Optionen in der Public Cloud

In diesem Abschnitt wird beschrieben, wie jeder der Cloud-Provider innerhalb ihrer jeweiligen Public-Cloud-Angebote ein VMware SDDC (Software Defined Data Center) und/oder VMware Cloud Foundation (VCF) Stack unterstützt.

Azure VMware Lösung

Azure VMware Lösung ist ein Hybrid-Cloud-Service, der VMware SDDC innerhalb der Public Cloud Microsoft Azure vollständig nutzt. Azure VMware Solution ist eine Komplettlösung, die vollständig von Microsoft gemanagt und unterstützt wird und die von VMware unter Verwendung der Azure Infrastruktur verifiziert wurde. Das heißt, Unternehmen können bei der Implementierung der Azure VMware Lösung ESXi für Computing-Virtualisierung nutzen, vSAN für hyperkonvergenten Storage. NSX für Networking und Sicherheit, gleichzeitig aber auch die globale Präsenz von Microsoft Azure, erstklassige Datacenter-Einrichtungen und die Nähe zum umfassenden Ecosystem aus nativen Azure-Services und -Lösungen.

VMware Cloud auf AWS

VMware Cloud auf AWS ermöglicht die Software SDDC der Enterprise-Klasse von VMware in der AWS Cloud mit optimiertem Zugriff auf native AWS Services. VMware Cloud auf AWS basiert auf VMware Cloud Foundation und integriert die Computing-, Storage- und Netzwerkvirtualisierungsprodukte von VMware (VMware vSphere, VMware vSAN und VMware NSX) in Kombination mit dem VMware vCenter Server-Management, das für die Ausführung auf einer dedizierten, flexiblen Bare-Metal-Infrastruktur von AWS optimiert ist.

Google Cloud VMware Engine

Google Cloud VMware Engine ist ein IaaS-Angebot (Infrastruktur als Service), das auf der enorm performanten skalierbaren Infrastruktur von Google Cloud und dem VMware Cloud Foundation Stack – VMware vSphere, vCenter, vSAN und NSX-T. – basiert Dieser Service ermöglicht einen schnellen Pfad zur Cloud und eine nahtlose Migration oder Erweiterung vorhandener VMware Workloads von On-Premises-Umgebungen auf die Google Cloud Platform – ohne die Kosten, den Aufwand oder das Risiko einer Umstrukturierung von Applikationen oder Neuwerkzeugen. Es handelt sich um einen Service, der von Google vertrieben und unterstützt wird und eng mit VMware zusammenarbeitet.

Die Private Cloud SDDC und NetApp Cloud Volumes Colocation bieten optimale Performance bei minimaler Netzwerklatenz.

Wussten Sie schon?

Unabhängig von der verwendeten Cloud umfasst der erste Cluster bei Implementierung eines VMware SDDC die folgenden Produkte:

- VMware ESXi Hosts für die Computing-Virtualisierung mit einer vCenter Server Appliance zum Management
- VMware vSAN hyperkonvergenter Storage mit den physischen Storage-Ressourcen des jeweiligen ESXi Hosts
- VMware NSX für virtuelles Networking und Sicherheit mit einem NSX Manager Cluster für Management

Storage-Konfiguration

Wenn Kunden planen, Storage-intensive Workloads zu hosten und horizontal auf jeder Cloud-gehosteten VMware Lösung zu skalieren, schreibt die hyperkonvergente Standardinfrastruktur vor, dass die Erweiterung sowohl auf die Computing- als auch auf die Storage-Ressourcen erfolgen sollte.

Durch die Integration mit NetApp Cloud Volumes, z. B. Azure NetApp Files, Amazon FSX für NetApp ONTAP, Cloud Volumes ONTAP (verfügbar für alle drei gängigen Hyperscaler) und Cloud Volumes Service für Google Cloud, haben Kunden nun die Möglichkeit, ihren Storage unabhängig voneinander zu skalieren. Sie fügen dann nach Bedarf nur noch Computing-Nodes zum SDDC-Cluster hinzu.

Hinweise:

- VMware empfiehlt keine unausgeglichenen Cluster-Konfigurationen, daher bedeutet Erweiterung des Storage das Hinzufügen weiterer Hosts, was zu höheren TCO führt.
- Es ist nur eine vSAN Umgebung möglich. Der gesamte Storage Traffic steht somit direkt mit den Produktions-Workloads im Wettbewerb.
- Es besteht keine Option, mehrere Performance-Tiers bereitzustellen, um Applikationsanforderungen, Performance und Kosten anzupassen.
- Es ist sehr einfach, die Storage-Kapazitäten von vSAN, das auf den Cluster-Hosts aufgebaut ist, zu erreichen. Verwenden Sie NetApp Cloud Volumes, um Storage zu skalieren, um entweder aktive Datensätze zu hosten oder kühlere Daten auf persistenten Storage zu verschieben.

Azure NetApp Files, Amazon FSX für NetApp ONTAP, Cloud Volumes ONTAP (verfügbar für alle drei gängigen

Hyperscaler) und Cloud Volumes Service für Google Cloud können zusammen mit Gast-VMs verwendet werden. Diese Hybrid-Storage-Architektur besteht aus einem vSAN Datastore, der das Gastbetriebssystem und Binärdaten der Applikationen enthält. Die Applikationsdaten sind über einen Gast-basierten iSCSI-Initiator oder die NFS/SMB-Mounts mit der VM verbunden, die direkt mit Amazon FSX für NetApp ONTAP, Cloud Volume ONTAP, Azure NetApp Files und Cloud Volumes Service für Google Cloud kommunizieren. Mit dieser Konfiguration lassen sich Herausforderungen mit Storage-Kapazität wie mit vSAN bewältigen. Der verfügbare freie Speicherplatz hängt von den eingesetzten Rack-Flächen und Storage-Richtlinien ab.

Betrachten wir ein SDDC-Cluster mit drei Nodes auf VMware Cloud auf AWS:

- Die gesamte Rohkapazität eines SDDC mit drei Nodes = 31,1 TB (ca. 10 TB pro Node).
- Der zu pflegende Slack-Platz bevor zusätzliche Hosts hinzugefügt werden = 25% = (0,25 x 31,1 TB) = 7,7 TB.
- Die nutzbare Bruttokapazität nach Abzug des Speicherplatzes = 22,4 TB
- Der verfügbare effektive freie Speicherplatz hängt von der angewandten Storage-Richtlinie ab.

  Beispiel:

  - RAID 0 = effektiver freier Speicherplatz = 22,4 TB (nutzbare Bruttokapazität/1)
  - RAID 1 = effektiver freier Speicherplatz = 11,7 TB (nutzbare Rohkapazität/2)
  - RAID 5 = effektiver freier Speicherplatz = 17,5 TB (nutzbare Bruttokapazität/1.33)

Daher würde eine Nutzung von NetApp Cloud Volumes als Storage mit Gastverbunden helfen, den Storage zu erweitern und die TCO zu optimieren, während gleichzeitig die Anforderungen an Performance und Datensicherung erfüllt werden.

Die Option in-Guest Storage war zum Zeitpunkt der Erstellung dieses Dokuments die einzige verfügbare. Sobald eine zusätzliche Unterstützung für einen NFS-Datastore verfügbar wird, wird eine zusätzliche Dokumentation verfügbar sein "Hier".

Wichtige Hinweise

- Platzieren Sie in Hybrid-Storage-Modellen Tier-1- oder Workloads mit hoher Priorität auf vSAN Datastore, um alle spezifischen Latenzanforderungen abzudecken, da diese Teil des Hosts selbst und in der Nähe sind. Nutzung von in-Guest-Mechanismen für alle Workload-VMs, für die transaktionsorientierte Latenzen akzeptabel sind
- NetApp SnapMirror Technologie ermöglicht die Replizierung der Workload-Daten vom lokalen ONTAP System auf Cloud Volumes ONTAP oder Amazon FSX für NetApp ONTAP, um die Migration mithilfe von Mechanismen auf Blockebene zu vereinfachen. Dies gilt nicht für Azure NetApp Files und Cloud Volumes Services. Für die Migration von Daten zu Azure NetApp Files oder Cloud Volumes Services verwenden Sie je nach verwendetem Dateiprotokoll NetApp XCP, BlueXP Copy und Sync, rysnc oder robocopy.
- Bei den Tests wird eine zusätzliche Latenz von 2 bis 4 ms angezeigt, während der Zugriff auf Storage von den jeweiligen SDDCs erfolgt. Berücksichtigen Sie diese zusätzliche Latenz bei der Zuordnung des Storage in die Applikationsanforderungen.
- Um mit dem Gast verbundenen Storage während des Test Failover und des tatsächlichen Failover zu mounten, stellen Sie sicher, dass iSCSI-Initiatoren neu konfiguriert sind, DNS für SMB-Freigaben aktualisiert wird und die NFS-Mount-Punkte in fstab aktualisiert werden.
- Vergewissern Sie sich, dass die Registry-Einstellungen für Microsoft Multipath I/O (MPIO), Firewall und Festplatten-Timeout innerhalb der VM ordnungsgemäß konfiguriert sind.

Dies bezieht sich ausschließlich auf den zu Gast verbundenen Speicher.

Vorteile von NetApp Cloud Storage

NetApp Cloud Storage bietet folgende Vorteile:

- Verbessert die Dichte von Computing zu Storage durch Skalierung des Storage unabhängig vom Computing.
- Ermöglicht Ihnen eine Verringerung der Host-Anzahl und somit eine Reduzierung der TCO insgesamt.
- Ein Ausfall des Computing-Nodes hat keine Auswirkungen auf die Storage-Performance.
- Mit der Volume-Umgestaltung und den dynamischen Service Level-Funktionen von Azure NetApp Files können Sie die Kosten optimieren, indem Sie die Größe für stabilen Workloads dimensionieren und so die Überprovisionierung verhindern.
- Die Cloud Volumes ONTAP Funktionen für Storage-Effizienz, Cloud-Tiering und Instanztypen erlauben das optimale Hinzufügen und Skalieren von Storage.
- Verhindert, dass überprovisioniert wird, dass Storage-Ressourcen nur bei Bedarf hinzugefügt werden.
- Mit effizienten Snapshot-Kopien und Klonen können Sie schnell und ohne Performance-Einbußen Kopien erstellen.
- Ransomware-Angriffe werden mit einer schnellen Recovery aus Snapshot-Kopien beheben.
- Effizientes, inkrementelles, blockbasiertes regionales Disaster Recovery und integrierte Backup-Blockebene über Regionen hinweg sorgen für bessere RPO und RTOs.

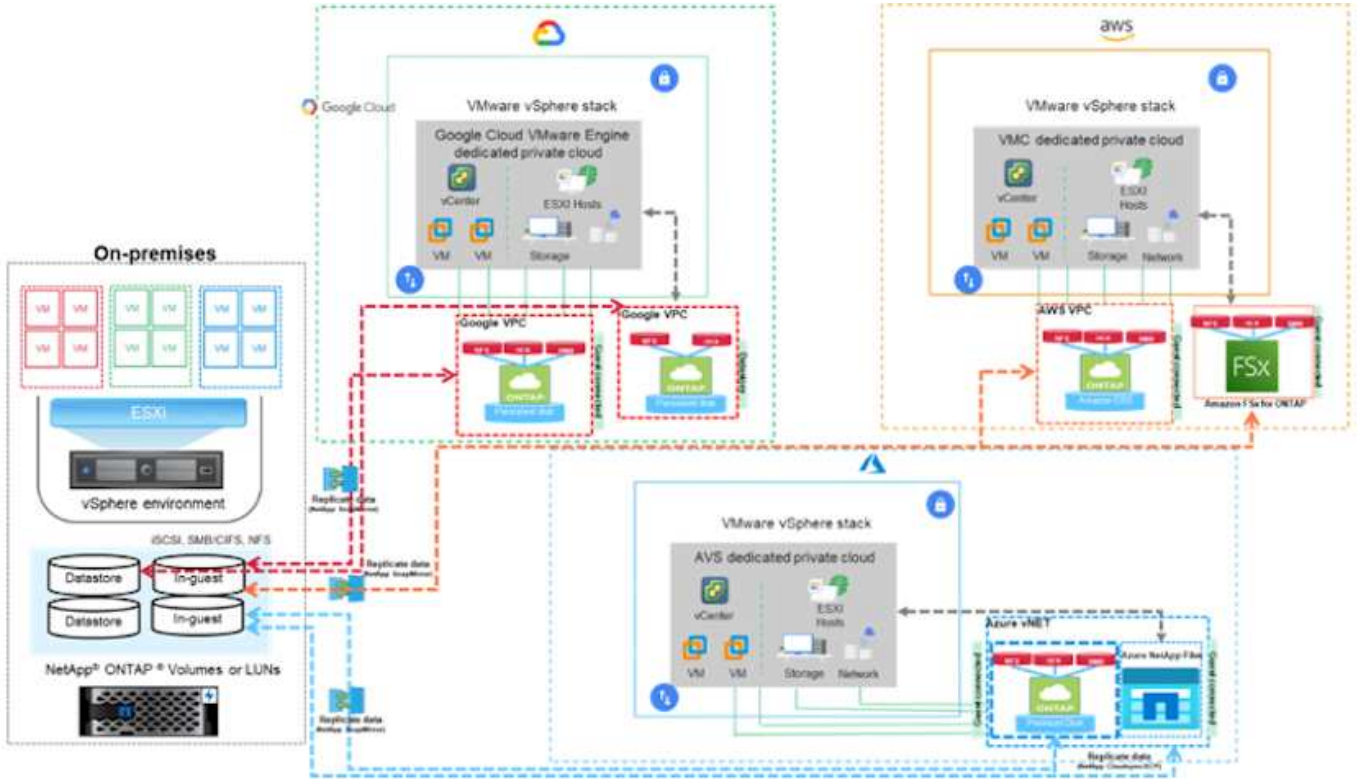
Voraussetzungen

- SnapMirror Technologie oder andere relevante Datenmigrationsmechanismen werden aktiviert. Es gibt viele Konnektivitätsoptionen – vor Ort und in beliebigen Hyperscaler-Clouds. Verwenden Sie den entsprechenden Pfad, und arbeiten Sie mit den entsprechenden Netzwerkteams zusammen.
- Die Option in-Guest Storage war zum Zeitpunkt der Erstellung dieses Dokuments die einzige verfügbare. Sobald eine zusätzliche Unterstützung für einen NFS-Datastore verfügbar wird, wird eine zusätzliche Dokumentation verfügbar sein "Hier".

Wenden Sie sich an NetApp Solution Architects und zugehörige Hyperscaler-Cloud-Architekten, um Storage und die erforderliche Anzahl von Hosts zu planen und zu dimensionieren. NetApp empfiehlt die Ermittlung der Anforderungen an die Storage-Performance, bevor das Cloud Volumes ONTAP-Sizer verwendet wird, um den Instanztyp oder das entsprechende Service Level mit dem richtigen Durchsatz abzuschließen.

Detaillierte Architektur

Im allgemeinen wird mit dieser Architektur (in der Abbildung unten dargestellt) erläutert, wie sich Hybrid-Multi-Cloud-Konnektivität und App-Portabilität über diverse Cloud-Provider hinweg erreichen lässt, die NetApp Cloud Volumes ONTAP, Cloud Volumes Service für Google Cloud und Azure NetApp Files als zusätzliche Option für Gast-Storage verwenden.



NetApp Lösungen für VMware bei Hyperscalern

Erfahren Sie mehr über die Funktionen, die NetApp den drei primären Hyperscalern (3) bietet: Von NetApp als Gast-verbundenen Storage-Gerät oder einem zusätzlichen NFS Datastore zur Migration von Workflows, Erweiterung/Bursting in die Cloud, Backup/Restore und Disaster Recovery.

Entscheiden Sie sich für die Cloud und überlassen Sie NetApp den Rest.

Um die Funktionen für einen bestimmten Hyperscaler anzuzeigen, klicken Sie auf die entsprechende Registerkarte für diesen Hyperscaler.

Springen Sie zum Abschnitt zum gewünschten Inhalt, indem Sie eine der folgenden Optionen auswählen:

- "VMware in der Konfiguration von Hyperscalern"

- "NetApp Storage-Optionen"
- "NetApp/VMware Cloud-Lösungen"

VMware in der Konfiguration von Hyperscalern

Wie bei lokalen Systemen ist die Planung einer Cloud-basierten Virtualisierungsumgebung eine entscheidende Voraussetzung für eine erfolgreiche, sofort einsatzbereite Umgebung zum Erstellen von VMs und Migrationen.

AWS/VMC

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS SDDC einrichten und managen und es in Kombination mit den verfügbaren Optionen zur Verbindung von NetApp Storage nutzen.

> Der in-Guest Storage ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit AWS VMC.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Implementieren und Konfigurieren von VMware Cloud für AWS
- Verbinden Sie VMware Cloud mit FSX ONTAP

Details anzeigen "Konfigurationsschritte für VMC".

Azure/AVS

In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Lösung einrichten und managen und in Kombination mit den verfügbaren Optionen für die Verbindung von NetApp Storage verwenden.

> Der in-Guest-Speicher ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit Azure VMware-Lösung.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Registrieren Sie den Ressourcenanbieter und erstellen Sie eine Private Cloud
- Stellen Sie eine Verbindung zu einem neuen oder vorhandenen virtuellen ExpressRoute Netzwerk-Gateway her
- Netzwerkverbindung validieren und auf Private Cloud zugreifen

Details anzeigen "Konfigurationsschritte für AVS".

GCP/GCVE

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und managen und in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp Storage verwenden.

> Der in-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP und Cloud Volumes Services mit GCVE.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von GCVE
- Aktivieren Sie den privaten Zugriff auf GCVE

Details anzeigen "Konfigurationsschritte für GCVE".

NetApp Storage-Optionen

NetApp Storage kann in allen 3 großen Hyperscalern auf verschiedene Weise genutzt werden – entweder als mit dem Gast verbunden oder als ergänzender NFS-Datastore.

Besuchen Sie "Unterstützte NetApp Storage-Optionen" Finden Sie weitere Informationen.

AWS/VMC

AWS unterstützt NetApp Storage in den folgenden Konfigurationen:

- FSX ONTAP als Storage mit Gastverbunden
- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- FSX ONTAP als zusätzlichen NFS-Datastore

Details anzeigen "Storage-Optionen für VMC für Gastverbindung". Details anzeigen "Zusätzliche NFS-Datastore-Optionen für VMC".

Azure/AVS

Azure unterstützt NetApp Storage in den folgenden Konfigurationen:

- Azure NetApp Files (ANF) als Storage mit Gastverbunden
- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- Azure NetApp Files (ANF) als zusätzlicher NFS-Datastore

Details anzeigen "Gastanbindung Speicheroptionen für AVS". Details anzeigen "Zusätzliche NFS-Datastore-Optionen für AVS".

GCP/GCVE

Google Cloud unterstützt NetApp Storage in den folgenden Konfigurationen:

- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- Cloud Volumes Service (CVS) als Storage mit Gastverbunden
- Cloud Volumes Service (CVS) als zusätzlicher NFS Datastore

Details anzeigen "Speicheroptionen für die Gastverbindung für GCVE".

Weitere Informationen "Unterstützung von NetApp Cloud Volumes Service-Datastores für die Google Cloud VMware Engine (NetApp Blog)" Oder "Verwendung von NetApp CVS als Datastores für Google Cloud VMware Engine (Google Blog)"

NetApp/VMware Cloud-Lösungen

Bei Cloud-Lösungen von NetApp und VMware lassen sich viele Anwendungsfälle einfach in einem Hyperscaler nach Wahl implementieren. VMware definiert primäre Anwendungsfälle für Cloud-Workloads wie:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Migrieren
- Erweitern

AWS/VMC

"NetApp Lösungen für AWS/VMC"

Azure/AVS

"NetApp Lösungen für Azure/AVS"

GCP/GCVE

"Erfahren Sie mehr über die NetApp Lösungen für die Google Cloud Platform (GCP)/GCVE"

Unterstütze Konfigurationen für NetApp Hybrid-Multi-Cloud mit VMware

Verstehen der Kombinationen für den Support von NetApp Storage in den wichtigsten Hyperscalern.

	Gast Verbunden	Ergänzende NFS-Datastore
AWS	CVO FSX-ONTAP"Details"	FSX ONTAP"Details"
Azure	CVO ANF"Details"	ANF"Details"
GCP	CVO CVS"Details"	CVS"Details"

Konfiguration der Virtualisierungsumgebung beim Cloud-Provider

Im Folgenden werden Details zur Konfiguration der Virtualisierungsumgebung für jeden der unterstützten Hyperscaler erläutert.

AWS/VMC

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS SDDC einrichten und managen und es in Kombination mit den verfügbaren Optionen zur Verbindung von NetApp Storage nutzen.

> Der in-Guest Storage ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit AWS VMC.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Implementieren und Konfigurieren von VMware Cloud für AWS
- Verbinden Sie VMware Cloud mit FSX ONTAP

Details anzeigen "Konfigurationsschritte für VMC".

Azure/AVS

In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Lösung einrichten und managen und in Kombination mit den verfügbaren Optionen für die Verbindung von NetApp Storage verwenden.

> Der in-Guest-Speicher ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit Azure VMware-Lösung.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Registrieren Sie den Ressourcenanbieter und erstellen Sie eine Private Cloud
- Stellen Sie eine Verbindung zu einem neuen oder vorhandenen virtuellen ExpressRoute Netzwerk-Gateway her
- Netzwerkverbindung validieren und auf Private Cloud zugreifen

Details anzeigen "Konfigurationsschritte für AVS".

GCP/GCVE

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und managen und in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp Storage verwenden.

> Der in-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP und Cloud Volumes Services mit GCVE.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von GCVE
- Aktivieren Sie den privaten Zugriff auf GCVE

Details anzeigen "Konfigurationsschritte für GCVE".

Implementieren und Konfigurieren der Virtualisierungsumgebung auf AWS

Wie auch bei lokalen Systemen ist die Planung von VMware Cloud auf AWS von entscheidender Bedeutung für eine erfolgreiche produktionsbereite Umgebung zur

Erstellung von VMs und Migration.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS SDDC einrichten und managen und es in Kombination mit den verfügbaren Optionen zur Verbindung von NetApp Storage nutzen.

Im-Gast-Storage ist derzeit die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP (CVO) mit AWS VMC.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Implementieren und Konfigurieren von VMware Cloud for AWS

"VMware Cloud auf AWS" Für VMware-basierte Workloads im AWS Ecosystem bietet es ein Cloud-natives Arbeiten. 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 Ihre Workloads bereitstellen.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS einrichten und managen und in Kombination mit Amazon FSX für NetApp ONTAP und/oder Cloud Volumes ONTAP auf AWS mit in-Guest Storage verwenden.

Im-Gast-Storage ist derzeit die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP (CVO) mit AWS VMC.

Der Einrichtungsprozess kann in drei Teile unterteilt werden:

Für ein AWS Konto registrieren

Für ein registrieren "Amazon Web Services Konto".

Sie brauchen ein AWS-Konto, um zu beginnen, vorausgesetzt, es gibt nicht bereits erstellt. Neu oder bereits vorhanden, Sie benötigen Administratorrechte im Konto für viele Schritte in diesem Verfahren. Siehe das "Verlinken" Weitere Informationen zu AWS Zugangsdaten.

Für einen My VMware Account registrieren

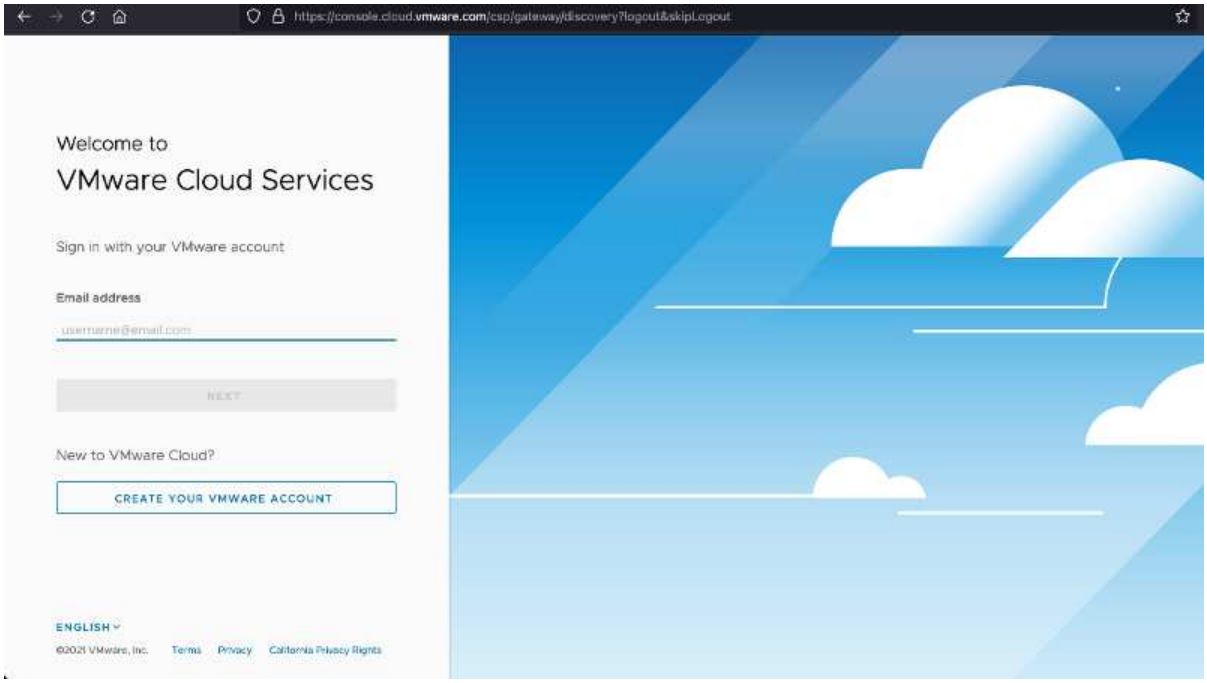
Für A registrieren "Meine VMware" Konto.

Für den Zugriff auf das Cloud-Portfolio von VMware (einschließlich VMware Cloud auf AWS) benötigen Sie ein VMware-Kundenkonto oder ein My VMware-Konto. Falls noch nicht geschehen, erstellen Sie ein VMware-Konto "Hier".

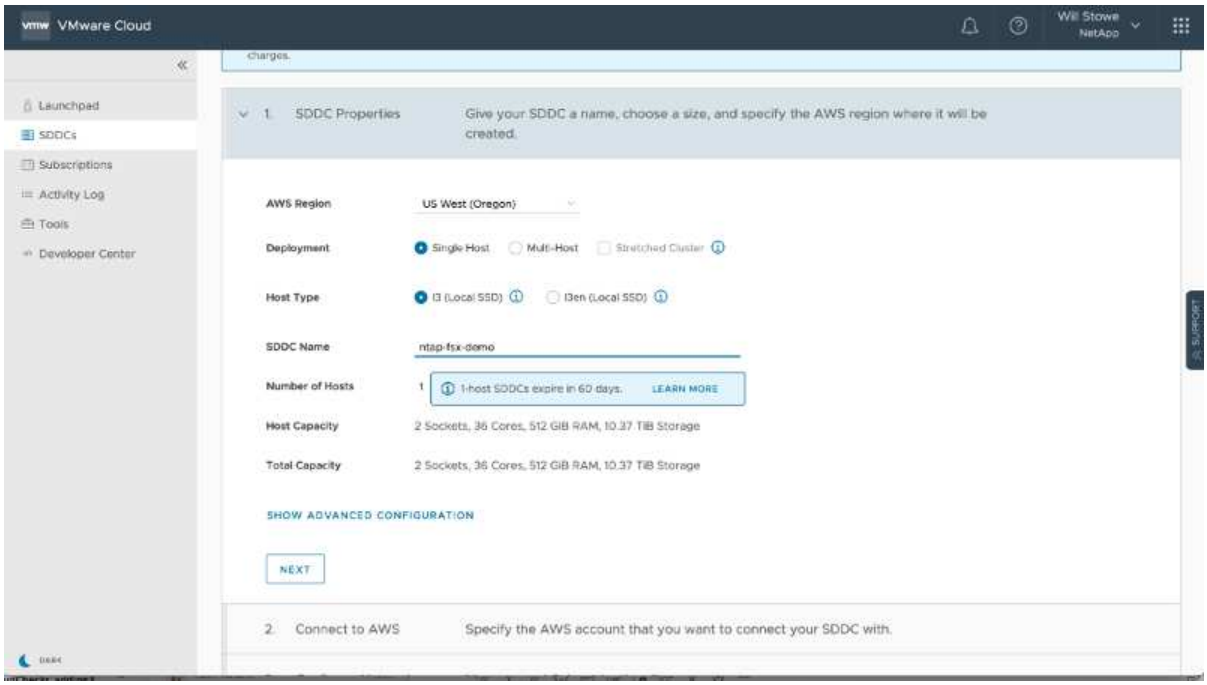
Bereitstellung von SDDC in VMware Cloud

Nach der Konfiguration des VMware Kontos und der ordnungsgemäßen Größenbestimmung ist die Implementierung eines softwaredefinierten Datacenters der nächste Schritt auf dem Weg zur Nutzung des VMware Cloud auf AWS Service. Wenn Sie ein SDDC erstellen möchten, wählen Sie eine AWS Region zum Hosten aus, geben Sie dem SDDC einen Namen und legen Sie fest, wie viele ESXi Hosts das SDDC enthalten soll. Wenn Sie noch kein AWS Konto haben, können Sie dennoch ein SDDC mit einer Starterkonfiguration erstellen, das einen einzelnen ESXi Host enthält.

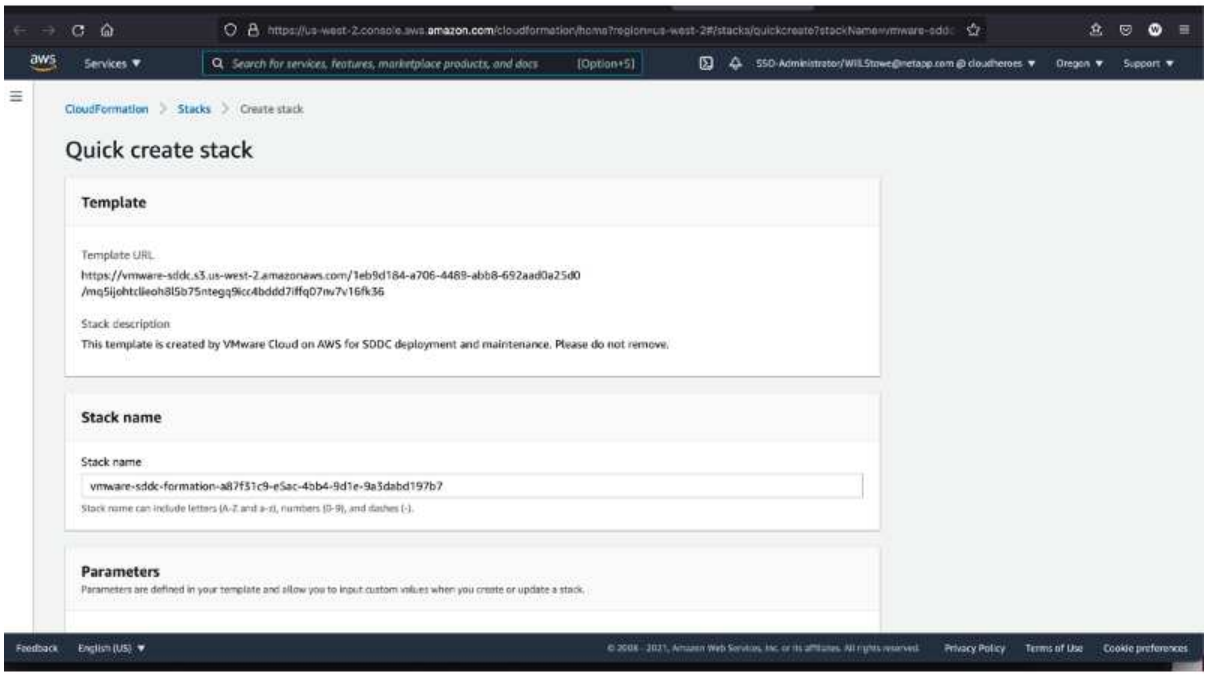
1. Melden Sie sich mit Ihren vorhandenen oder neu erstellten VMware Zugangsdaten bei der VMware Cloud Console an.

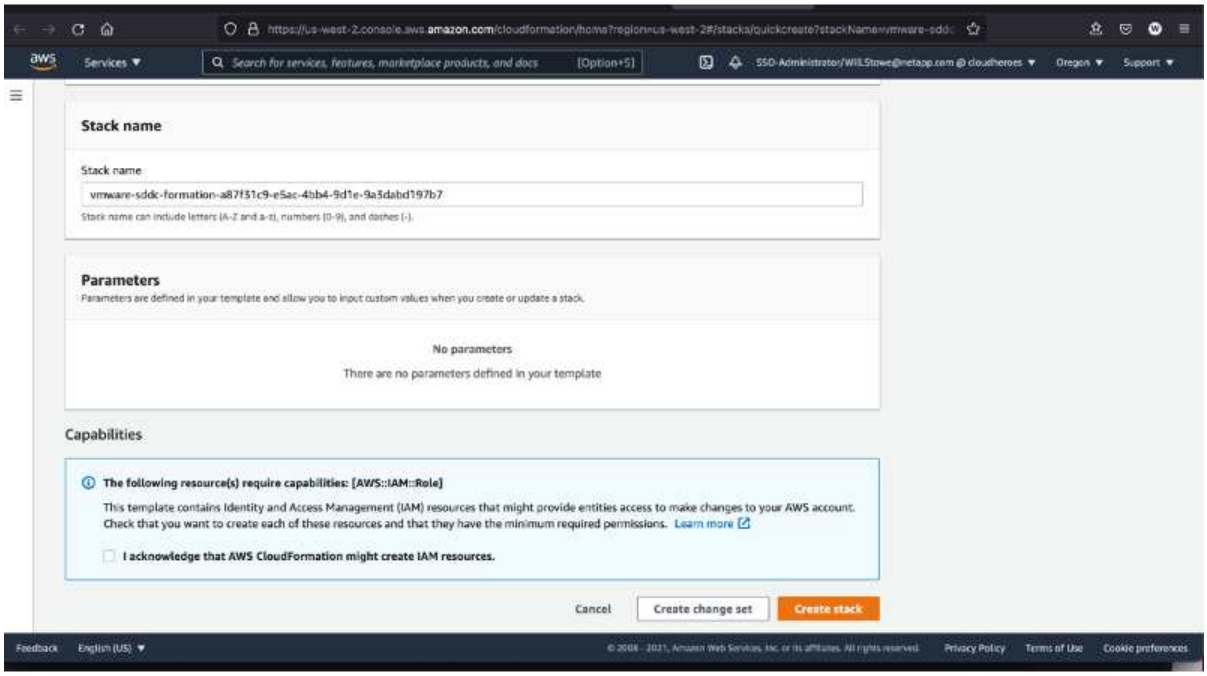


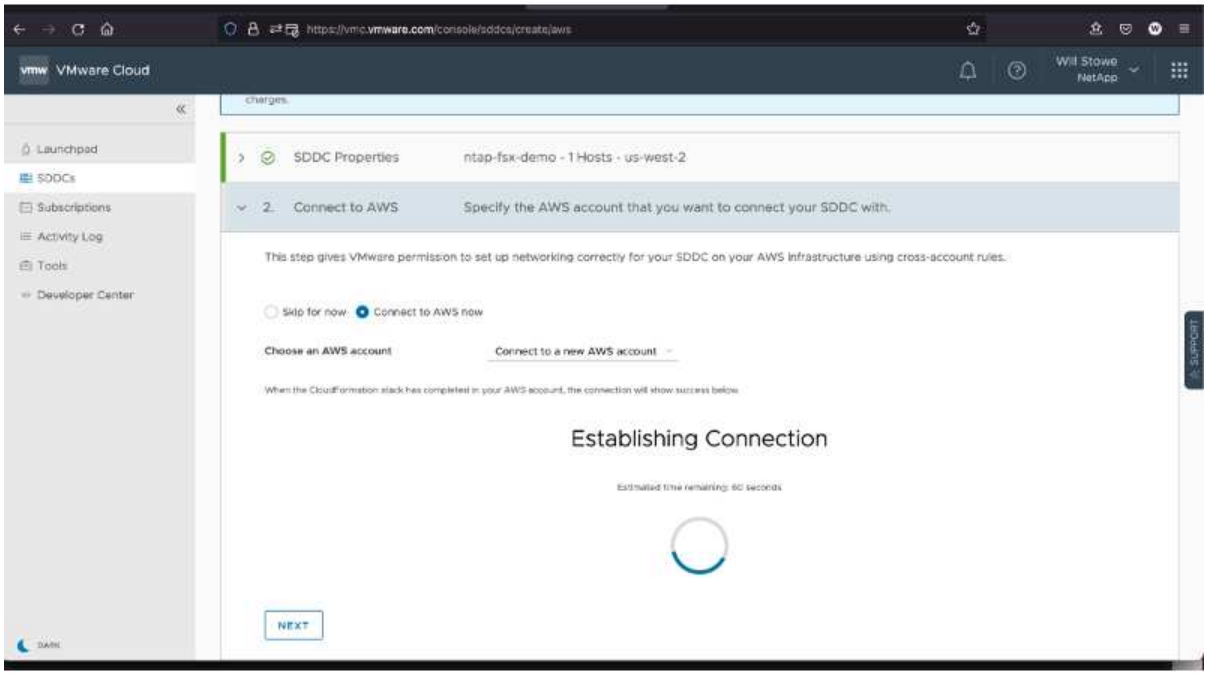
2. Konfigurieren Sie die AWS Region, die Implementierung und den Host-Typ sowie den SDDC-Namen:

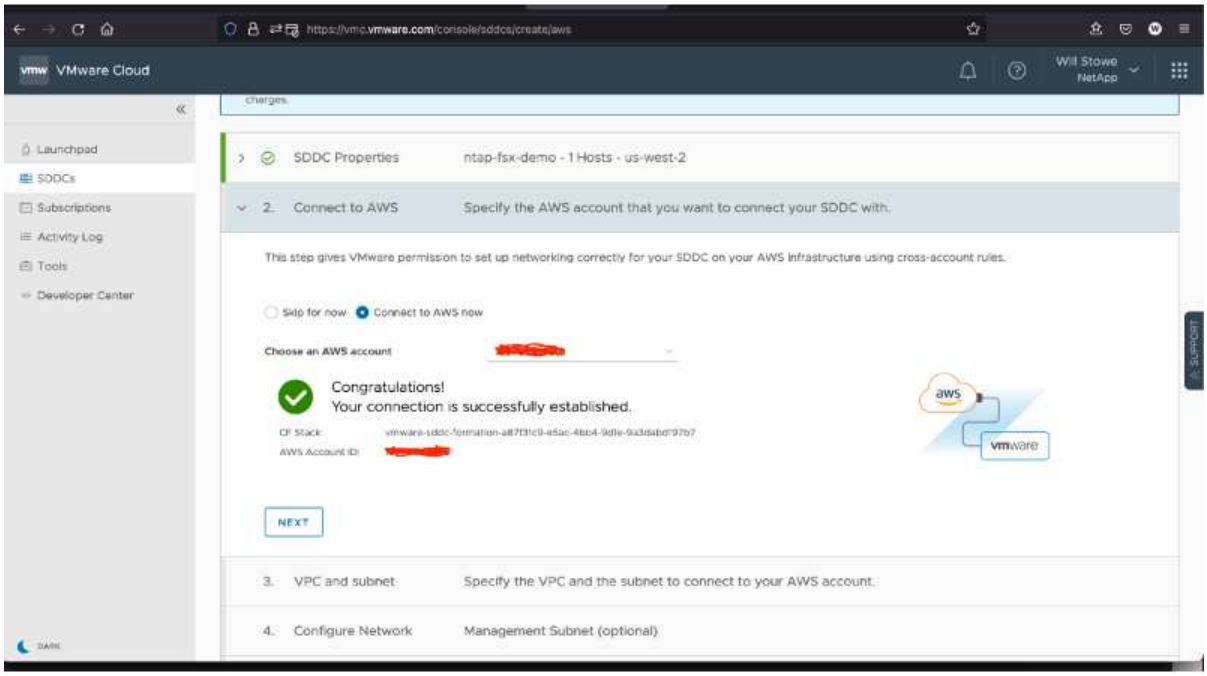


3. Stellen Sie eine Verbindung mit dem gewünschten AWS Konto her und führen Sie den AWS Cloud-Formationstack aus.



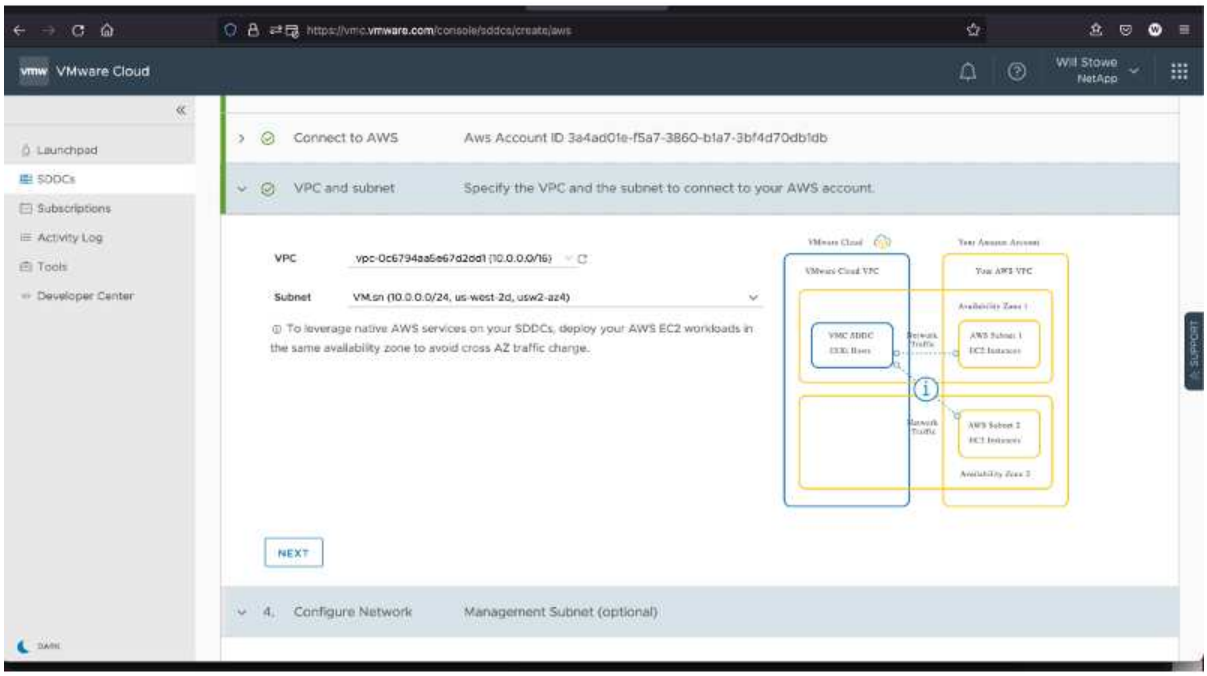

Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack


VMware Cloud
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
SDDC Properties
ntap-fsx-demo - 1 Hosts - us-west-2
2. Connect to AWS
Specify the AWS account that you want to connect your SDDC with.
This step gives VMware permission to set up networking correctly for your SDDC on your AWS infrastructure using cross-account rules.
Skip for now
Connect to AWS now
Choose an AWS account
Connect to a new AWS account
Establishing Connection
NEXT

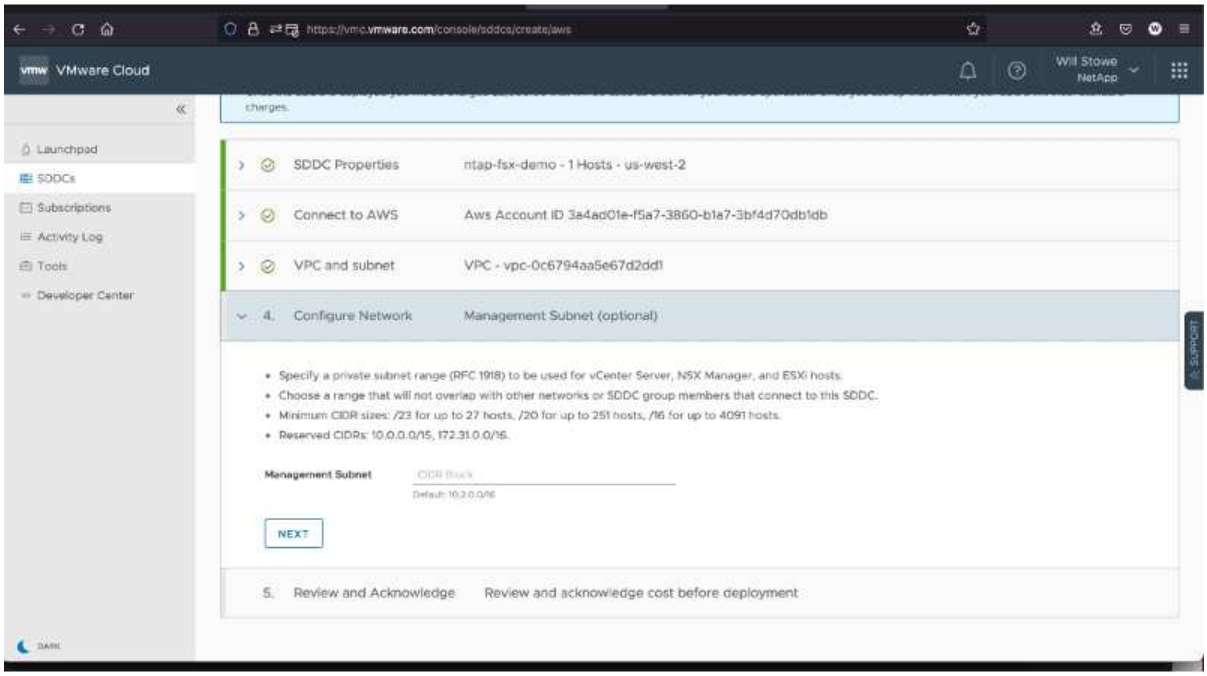


In dieser Validierung wird Single-Host-Konfiguration verwendet.

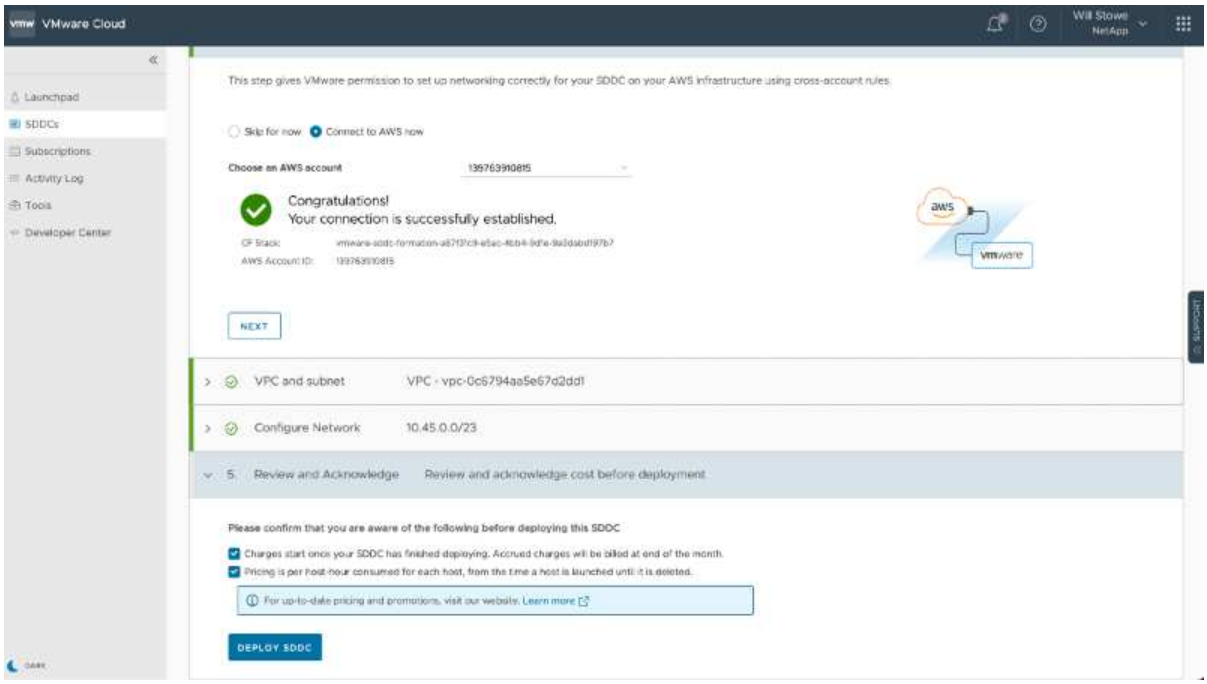
4. Wählen Sie die gewünschte AWS VPC aus, mit der die VMC-Umgebung verbunden werden soll.



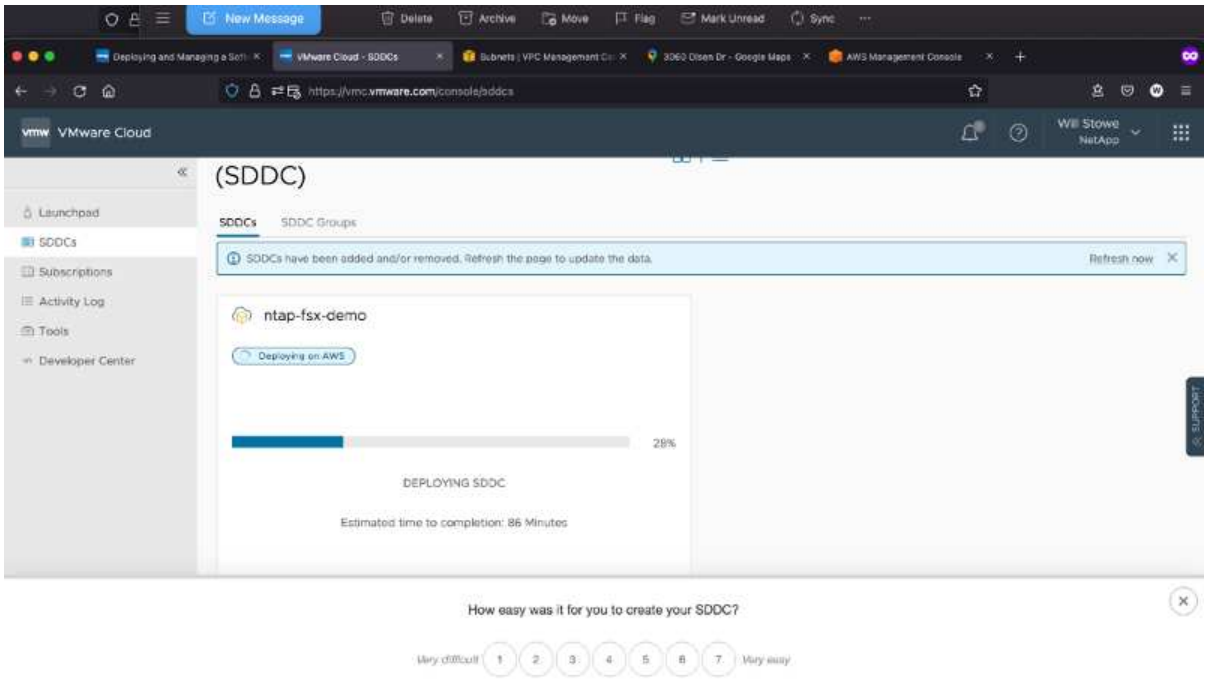
5. VMC-Managementsubnetz konfigurieren: Dieses Subnetz enthält von VMC gemanagte Services wie vCenter, NSX usw. Wählen Sie keinen überlappenden Adressraum mit anderen Netzwerken, die Verbindung zur SDDC-Umgebung benötigen. Folgen Sie abschließend den unten aufgeführten Empfehlungen für CIDR-Größe.



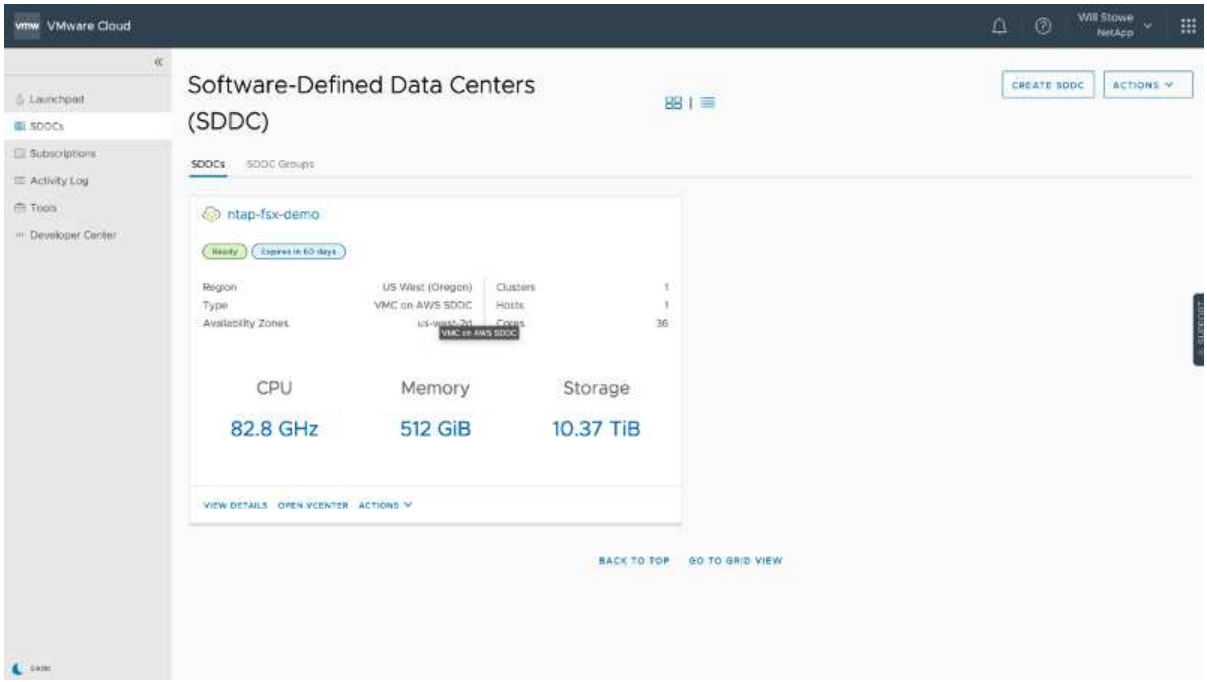
6. Prüfen und bestätigen Sie die SDDC-Konfiguration und klicken Sie dann auf Bereitstellen des SDDC.



Die Implementierung dauert normalerweise etwa zwei Stunden.



7. Nach Abschluss der Fertigstellung ist das SDDC einsatzbereit.

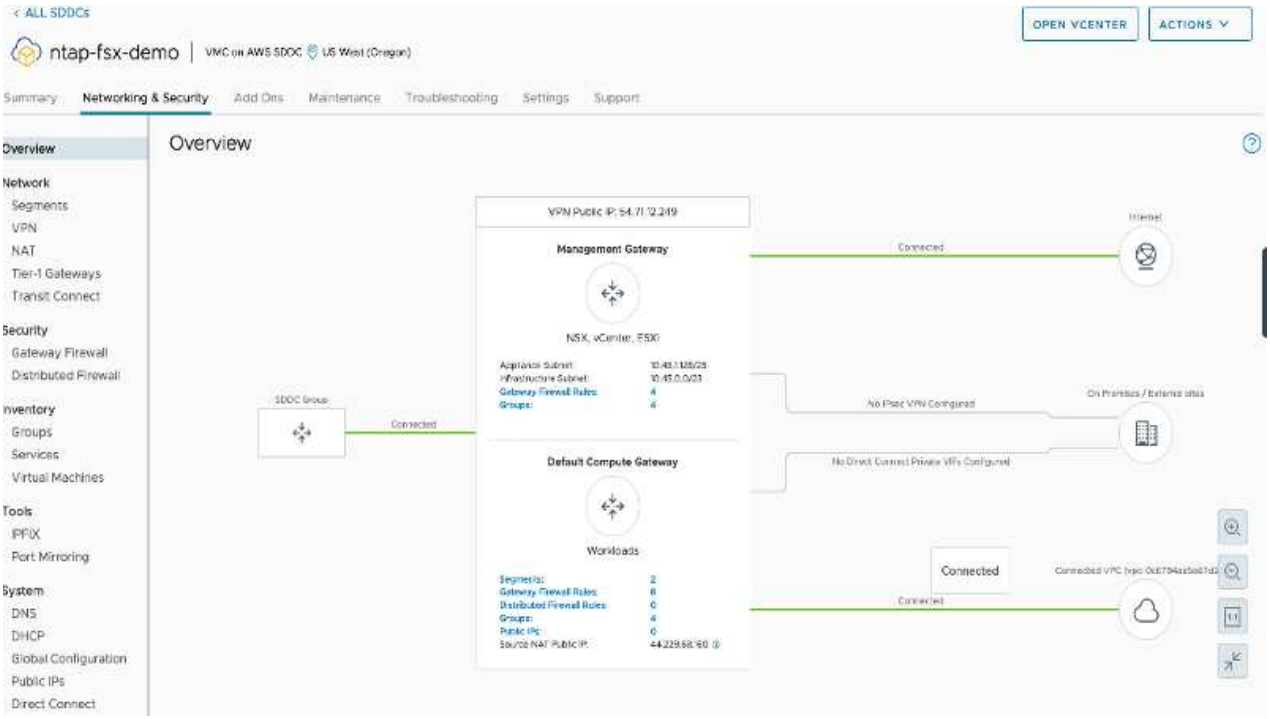


Einen Schritt-für-Schritt-Leitfaden zur SDDC-Implementierung finden Sie unter "Implementieren Sie ein SDDC über die VMC-Konsole".

Verbinden Sie VMware Cloud mit FSX ONTAP

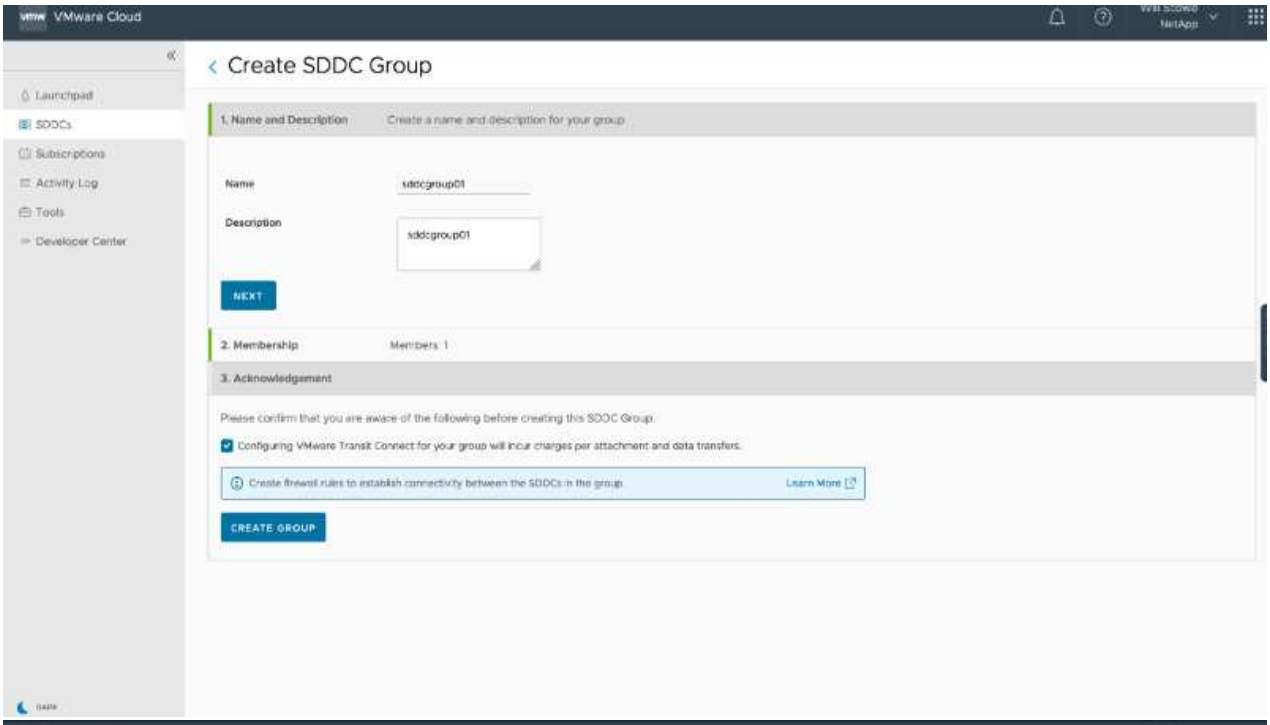
So verbinden Sie VMware Cloud mit FSX ONTAP:

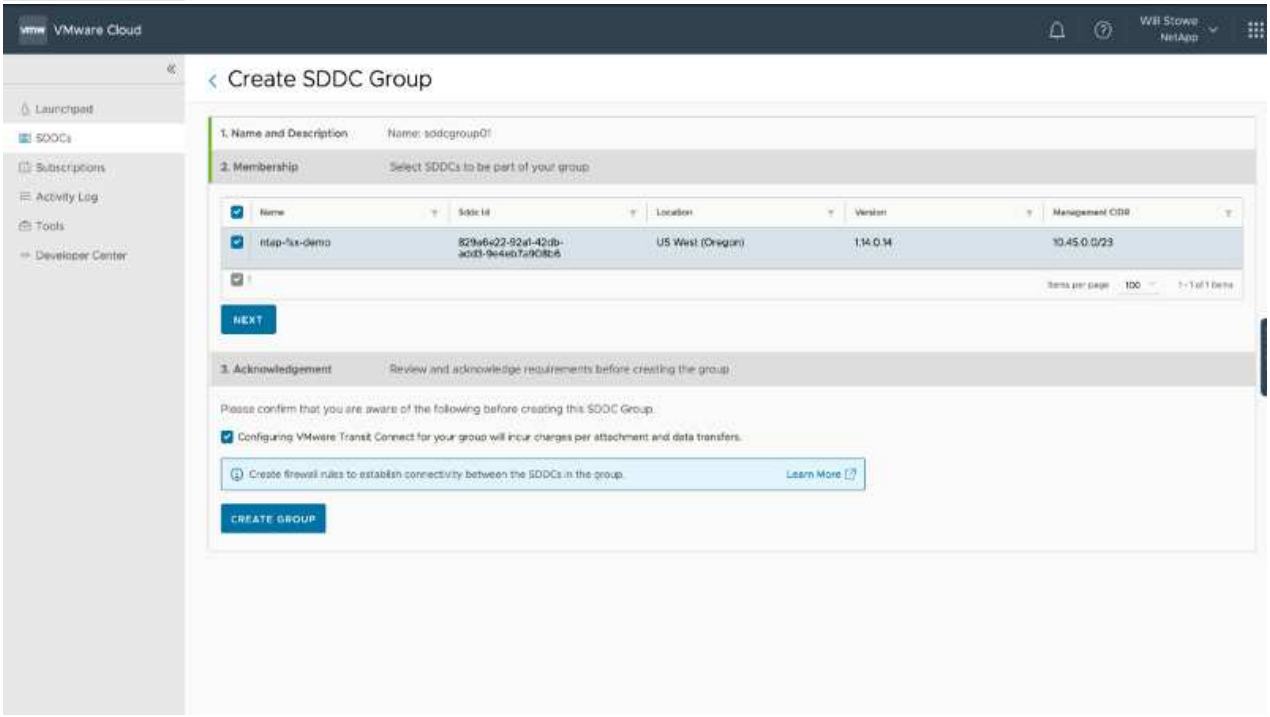
1. Wenn die VMware Cloud Implementierung abgeschlossen und mit AWS VPC verbunden ist, müssen Sie Amazon FSX für NetApp ONTAP in ein neues VPC anstatt in der mit der Integration verbundenen VPC implementieren (siehe Abbildung unten). FSX (NFS- und SMB-fließende IPs) ist nicht zugänglich, wenn sie in der verbundenen VPC implementiert werden. ISCSI-Endpunkte wie Cloud Volumes ONTAP funktionieren genauso gut wie die verbundene VPC.

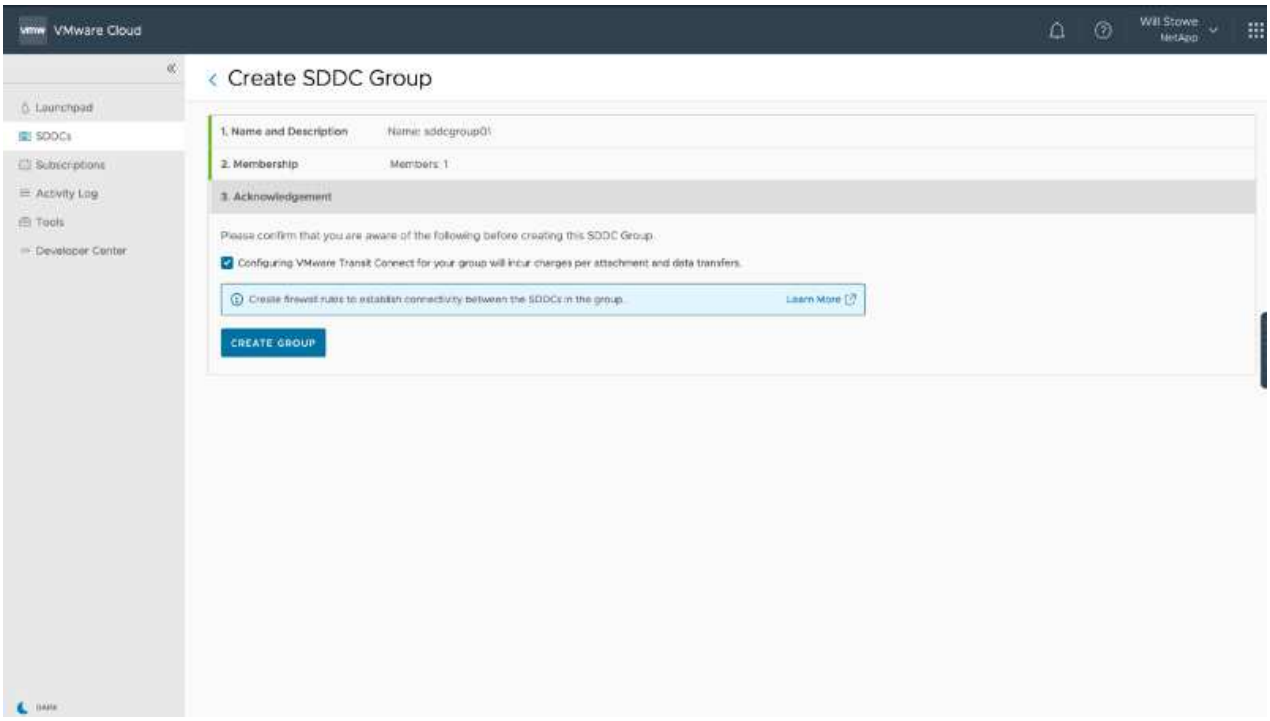


2. Eine zusätzliche VPC in derselben Region implementieren und dann Amazon FSX für NetApp ONTAP in die neue VPC implementieren.

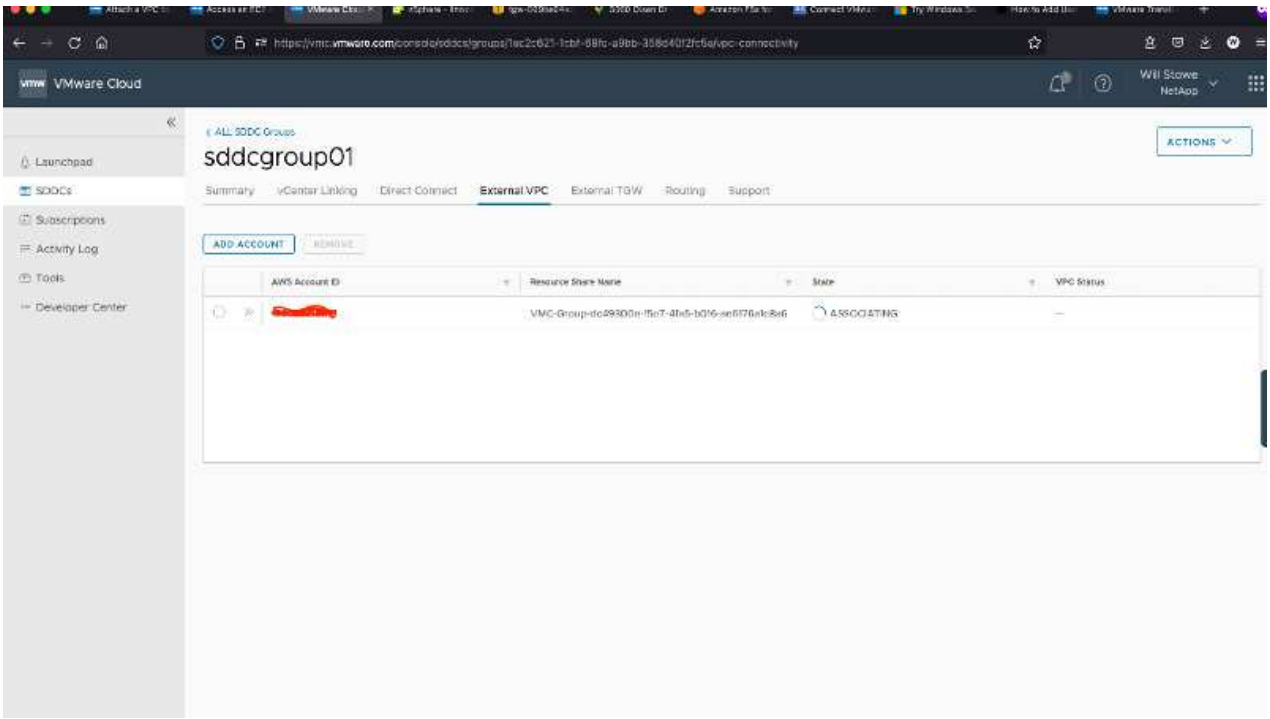
   Die Konfiguration einer SDDC-Gruppe in der VMware Cloud Konsole ermöglicht die erforderlichen Netzwerkkonfigurationsoptionen für die Verbindung zur neuen VPC, bei der FSX implementiert wird. Überprüfen Sie in Schritt 3, ob „VMware Transit Connect für Ihre Gruppe konfigurieren“ Gebühren pro Anlage und Datenübertragung anfällt und wählen Sie „Gruppe erstellen“. Dieser Vorgang kann einige Minuten dauern.

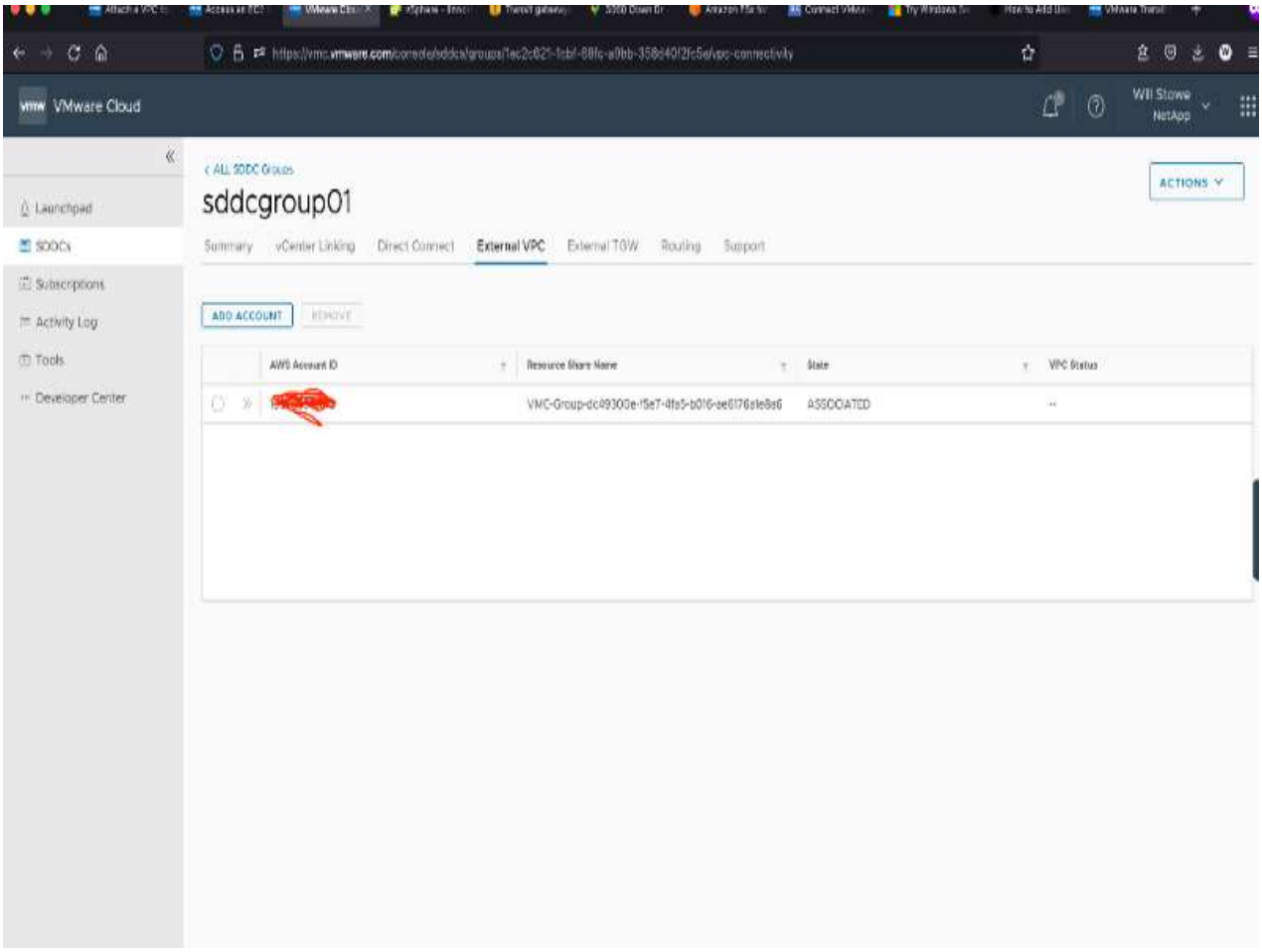

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP


VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6e22-92a1-42db-acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page
100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

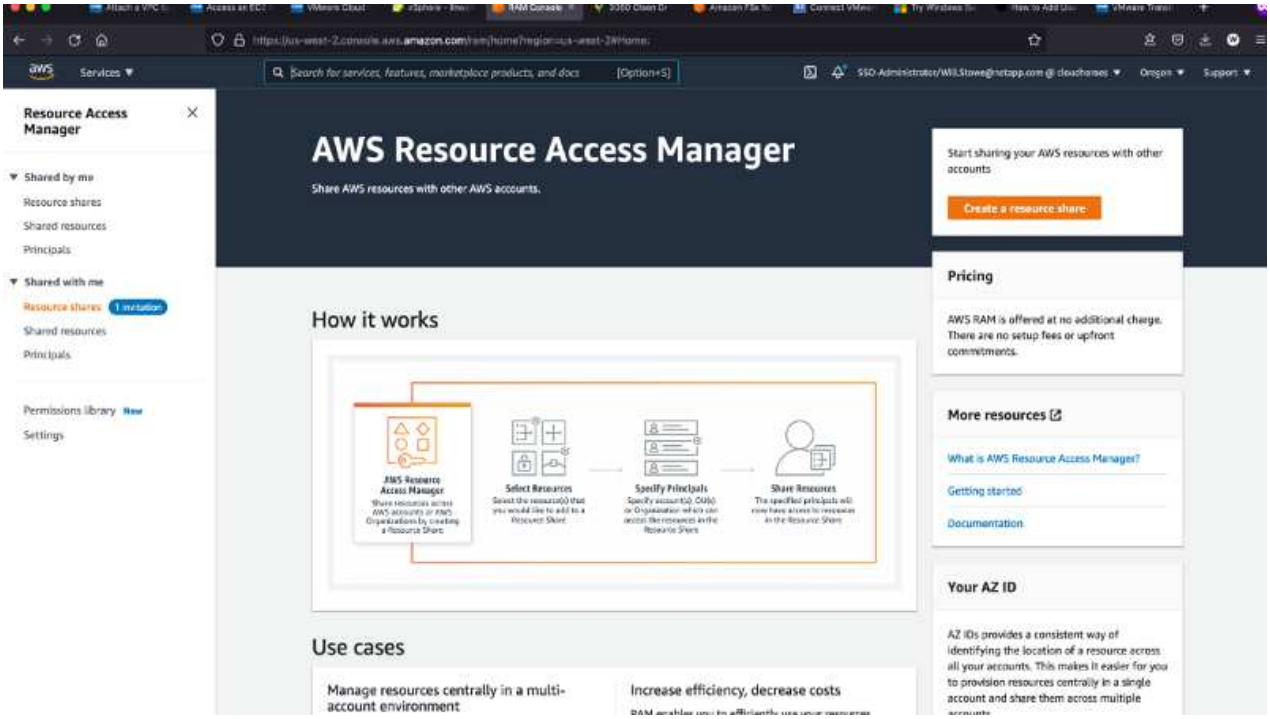


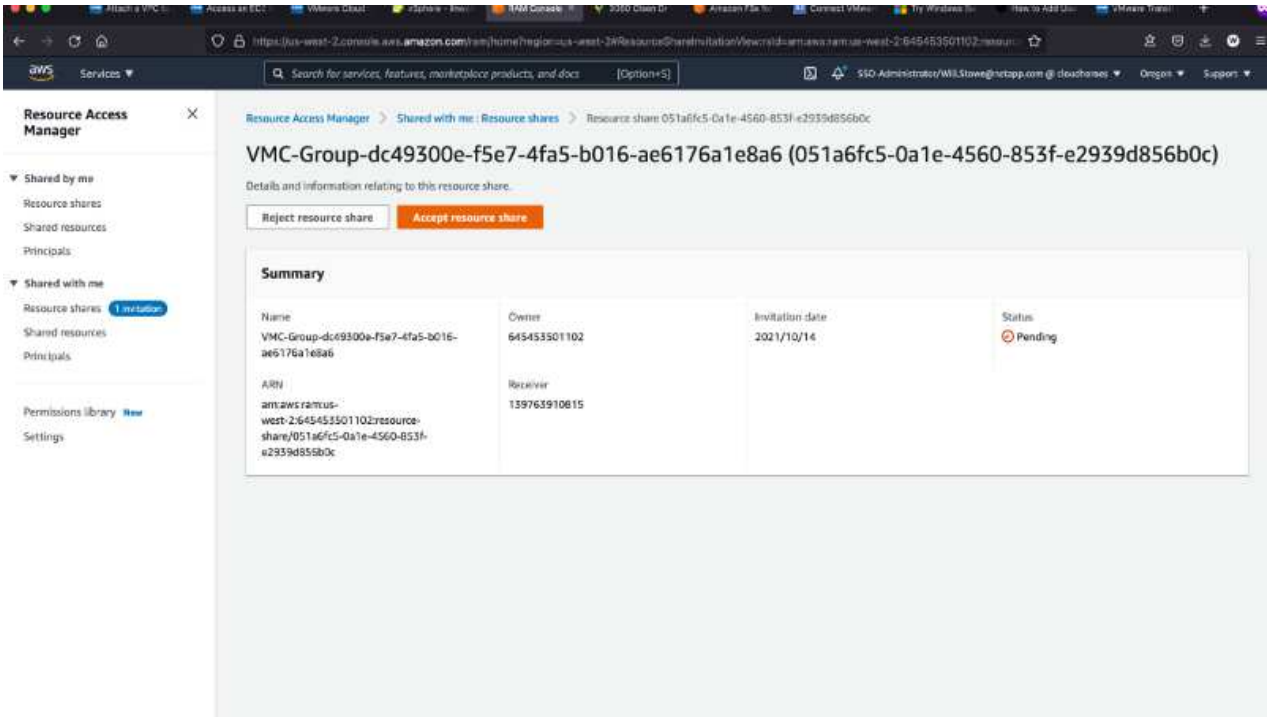
3. Binden Sie die neu erstellte VPC an die gerade erstellte SDDC-Gruppe. Wählen Sie die Registerkarte External VPC aus, und folgen Sie der "Anweisungen zum Anschließen eines externen VPC" Für die Gruppe. Dieser Vorgang kann 10 bis 15 Minuten in Anspruch nehmen.



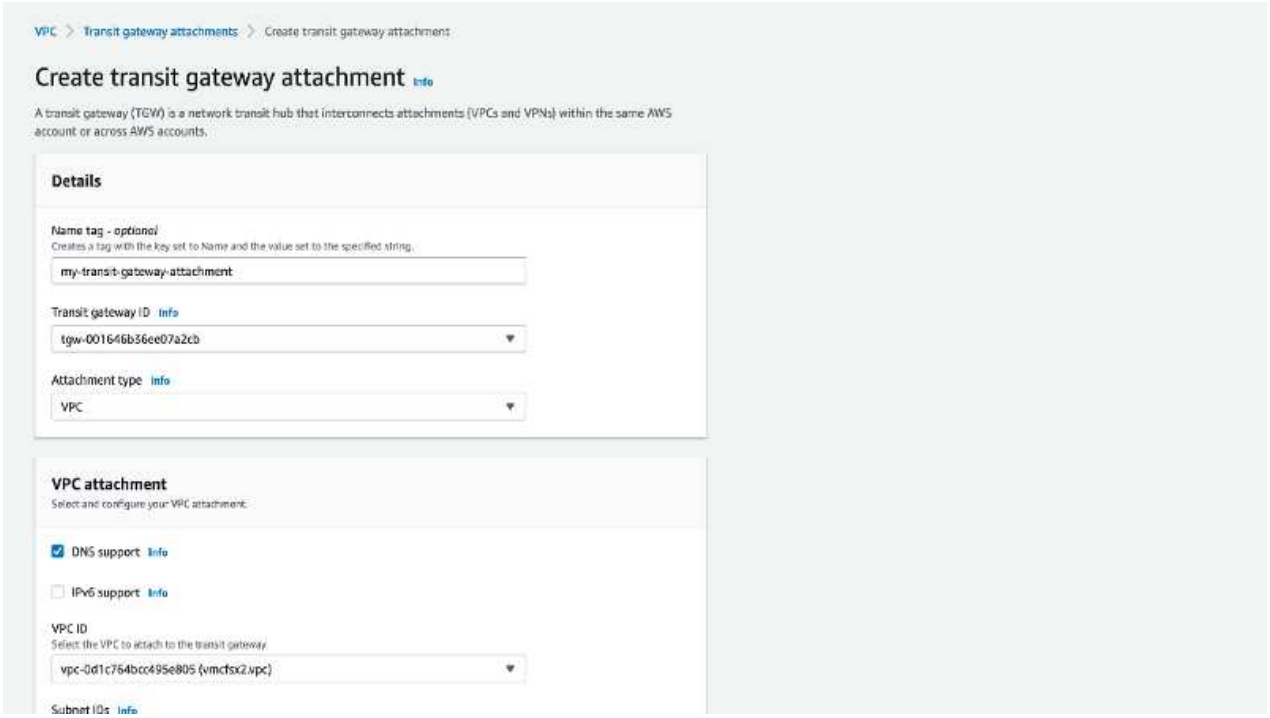


4. Im Rahmen des externen VPC-Prozesses werden Sie über die AWS-Konsole zu einer neuen, gemeinsam genutzten Ressource über den Resource Access Manager aufgefordert. Die gemeinsam genutzte Ressource ist die "AWS Transit Gateway" Management über VMware Transit Connect

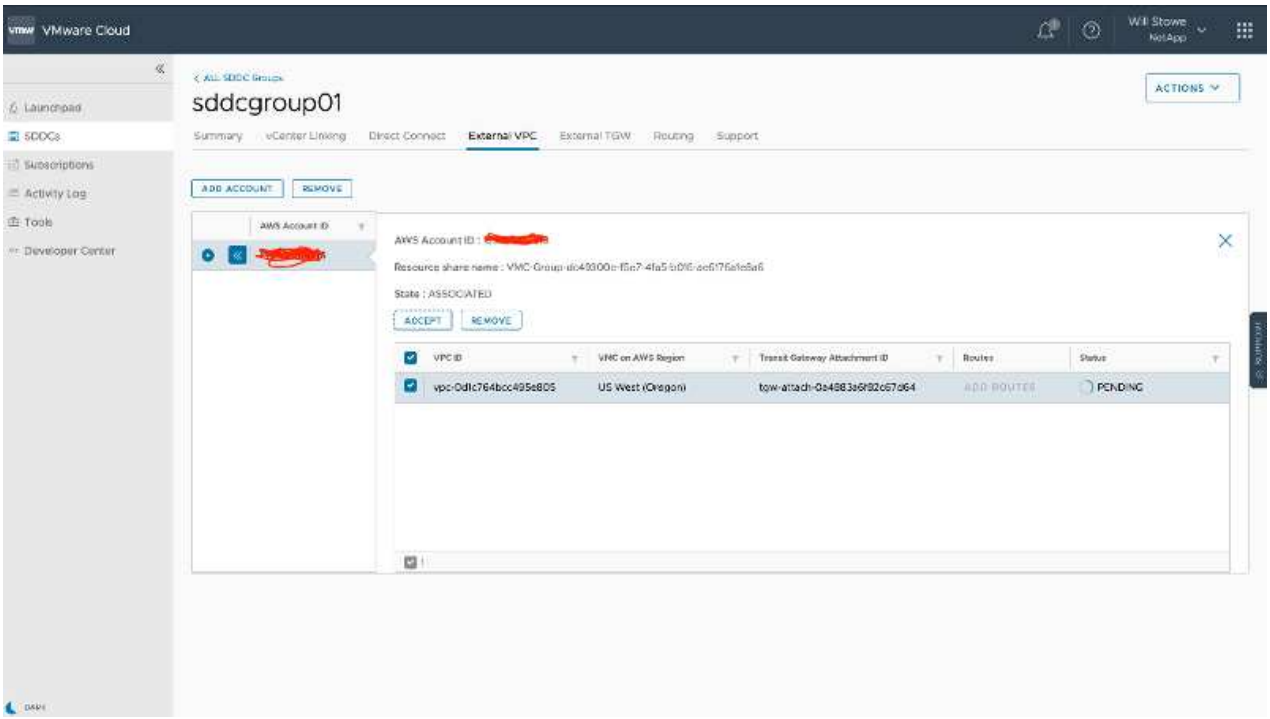




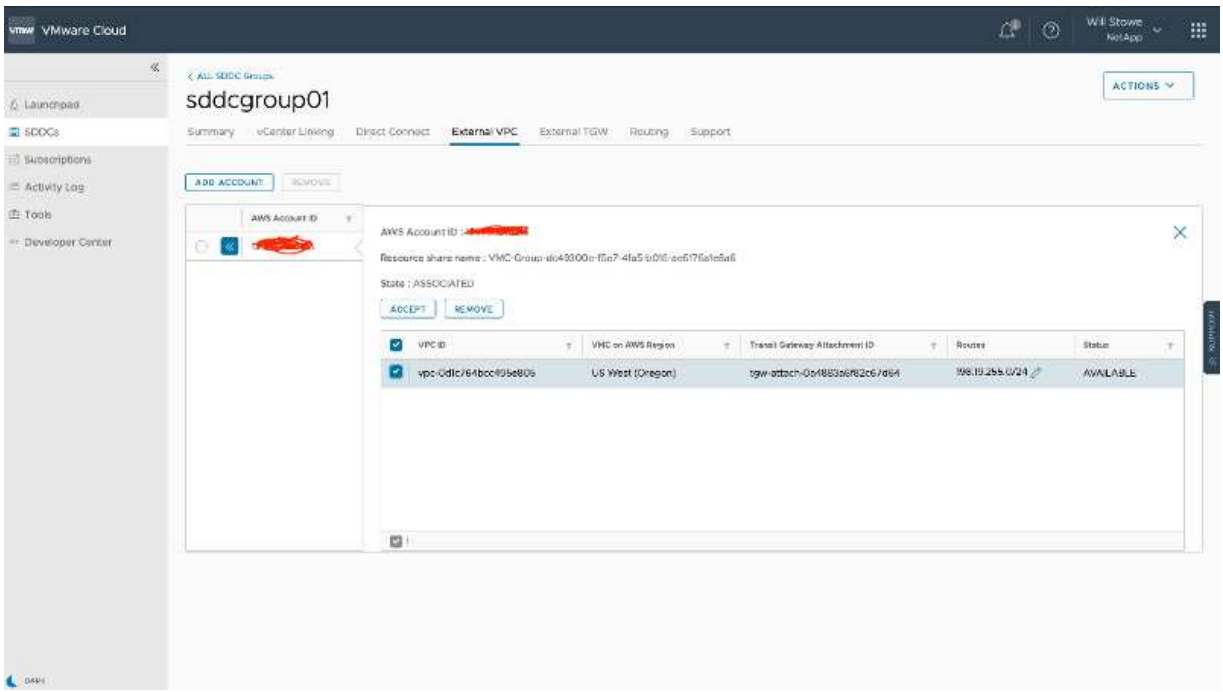
5. Erstellen Sie den Transit Gateway-Anhang.



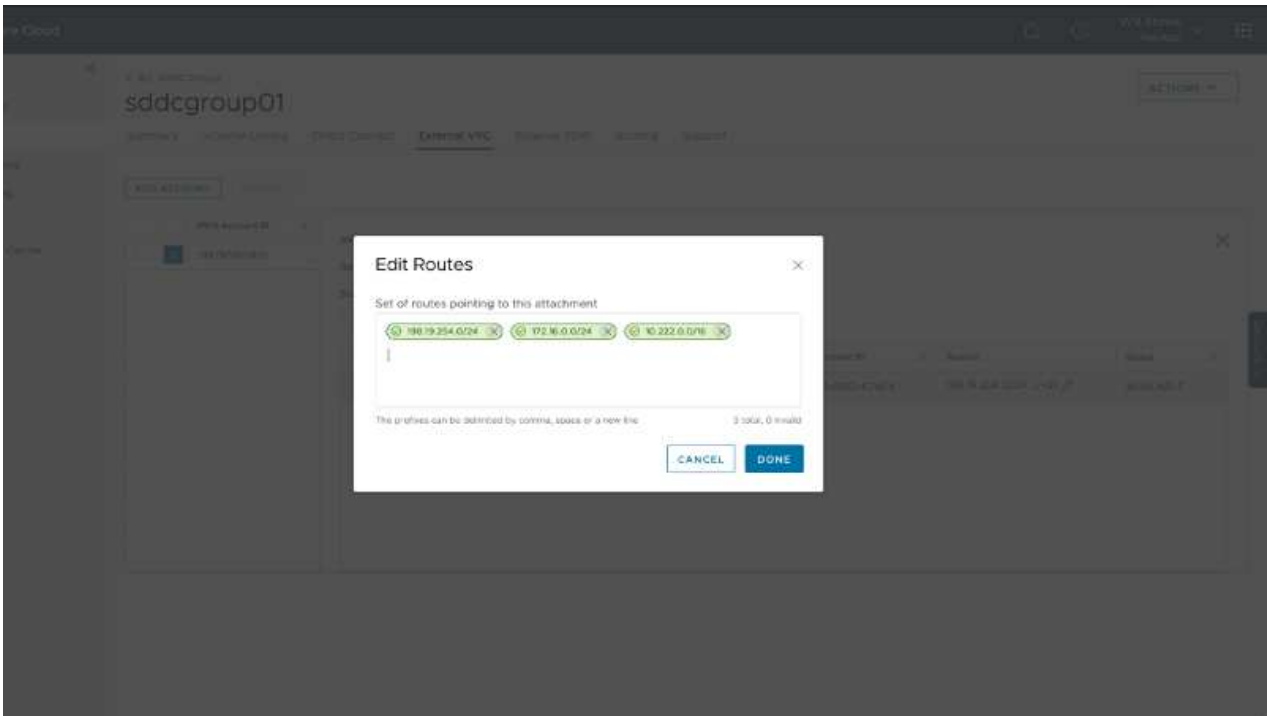
6. Nehmen Sie wieder an der VMC-Konsole die VPC-Anlage an. Dieser Vorgang dauert etwa 10 Minuten.



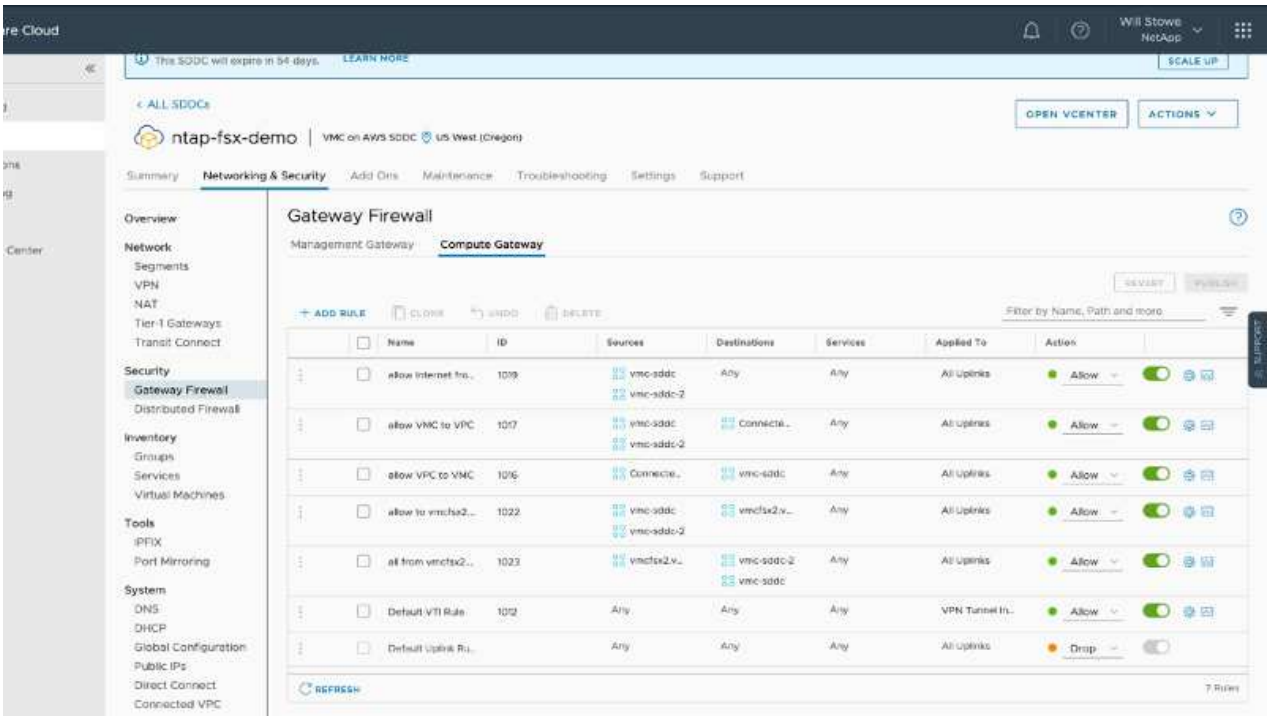
7. Klicken Sie auf der Registerkarte External VPC auf das Bearbeiten-Symbol in der Spalte Routen und fügen Sie die folgenden erforderlichen Routen hinzu:
   - Eine Route für den unverankerten IP-Bereich für Amazon FSX für NetApp ONTAP "Fließende IPs".
   - Eine Route für den unverankerten IP-Bereich für Cloud Volumes ONTAP (falls zutreffend).
   - Eine Route für den neu erstellten externen VPC-Adressraum.



8. Außerdem bidirektionalen Datenverkehr zulassen "Firewall-Regeln" Für den Zugriff auf FSX/CVO. Befolgen Sie diese "Detaillierte Schritte" Für die Firewall des Computing-Gateways für die SDDC-Workload-Konnektivität.



9. Nachdem die Firewall-Gruppen sowohl für das Management- als auch für das Computing-Gateway konfiguriert wurden, ist der Zugriff auf vCenter wie folgt möglich:



Als nächsten Schritt müssen Sie überprüfen, ob Amazon FSX ONTAP oder Cloud Volumes ONTAP je nach Ihren Anforderungen konfiguriert ist und dass die Volumes bereitgestellt werden, um Storage-Komponenten aus vSAN auszulagern, um die Implementierung zu optimieren.

Wie bei On-Premises-Systemen ist die Planung von Azure VMware Lösungen für eine erfolgreiche produktionsbereite Umgebung für das Erstellen von VMs und die Migration von großer Bedeutung.

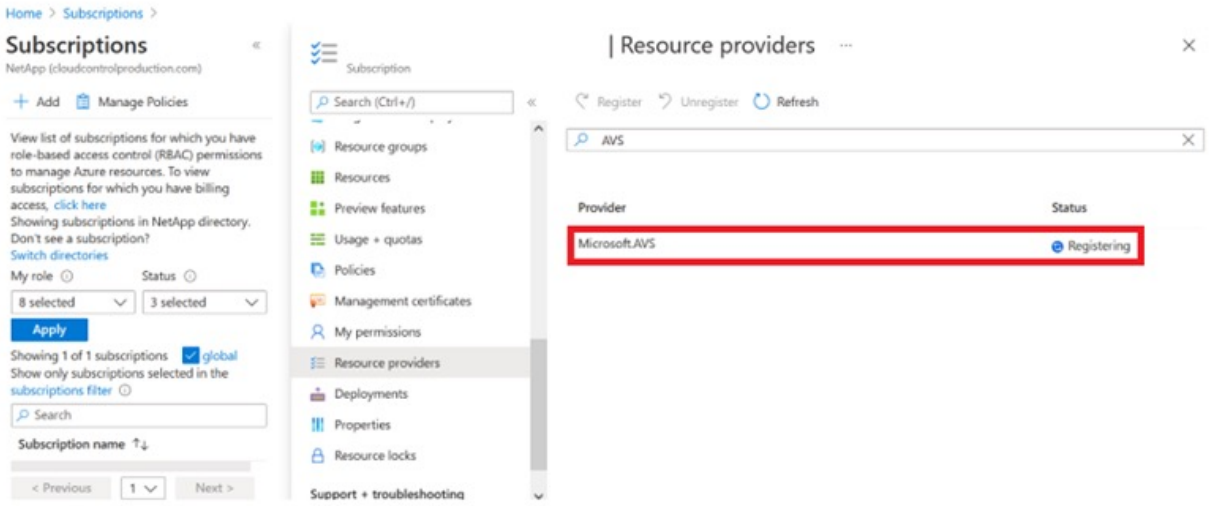
In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Lösung einrichten und managen und in Kombination mit den verfügbaren Optionen für die Verbindung von NetApp Storage verwenden.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Registrieren Sie den Ressourcenanbieter und erstellen Sie eine Private Cloud

Für die Nutzung der Azure VMware Lösung müssen Sie zunächst den Ressourcenanbieter im angegebenen Abonnement registrieren:

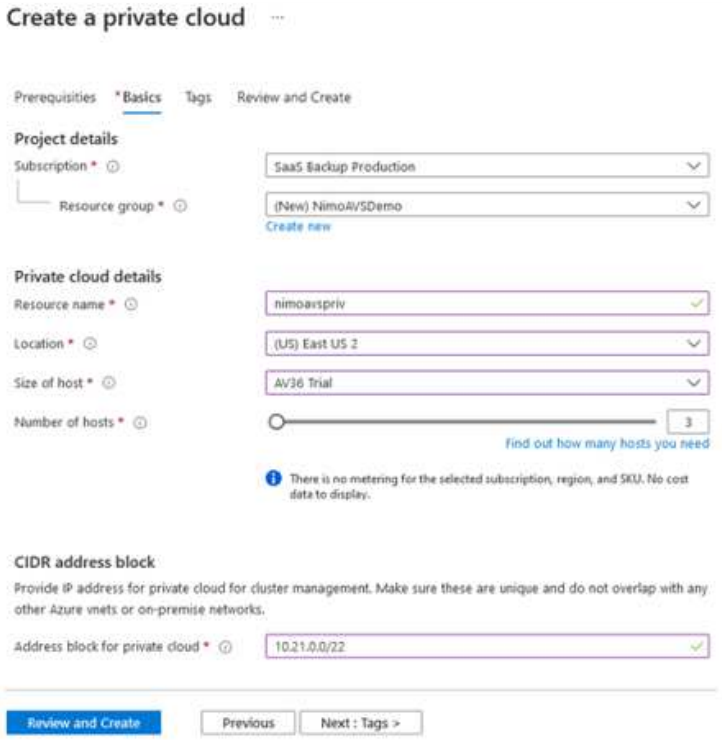
1. Melden Sie sich im Azure Portal an.
2. Wählen Sie im Menü Azure-Portal die Option Alle Services aus.
3. Geben Sie im Dialogfeld „Alle Services“ das Abonnement ein, und wählen Sie anschließend Abonnements aus.
4. Wählen Sie das Abonnement aus der Abonnementliste aus, um es anzuzeigen.
5. Wählen Sie Ressourcenanbieter aus, und geben Sie Microsoft.AVS in die Suche ein.
6. Wenn der Ressourcenanbieter nicht registriert ist, wählen Sie Registrieren.



7. Nachdem der Ressourcenanbieter registriert ist, erstellen Sie über das Azure-Portal eine Private Cloud für eine Azure VMware-Lösung.
8. Melden Sie sich im Azure Portal an.
9. Wählen Sie Neue Ressource erstellen.
10. Geben Sie im Textfeld „Search the Marketplace“ die Azure VMware Lösung ein und wählen Sie sie aus den Ergebnissen aus.
11. Wählen Sie auf der Seite Azure VMware Lösung die Option Erstellen.
12. Geben Sie auf der Registerkarte Grundlagen die Werte in die Felder ein, und wählen Sie Überprüfen + Erstellen.

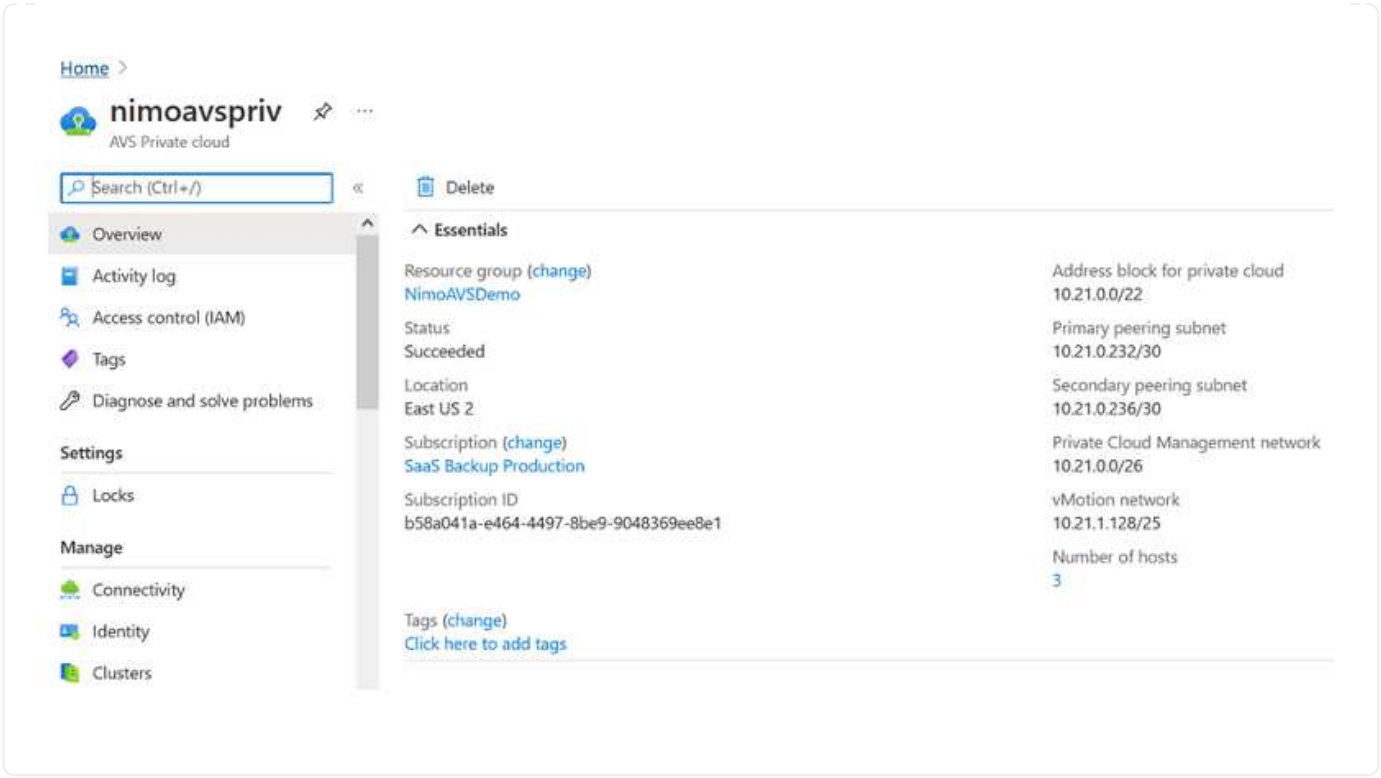
Hinweise:

- Für einen schnellen Start müssen Sie die erforderlichen Informationen während der Planungsphase erfassen.
- Wählen Sie eine vorhandene Ressourcengruppe aus oder erstellen Sie eine neue Ressourcengruppe für die private Cloud. Eine Ressourcengruppe ist ein logischer Container, in dem die Azure Ressourcen implementiert und gemanagt werden.
- Stellen Sie sicher, dass die CIDR-Adresse einzigartig ist und nicht mit anderen virtuellen Azure Netzwerken oder On-Premises-Netzwerken überlappt. Das CIDR stellt das private Cloud-Managementnetzwerk dar und wird für Cluster-Managementservices wie vCenter Server und NSX-T Manager verwendet. NetApp empfiehlt die Verwendung eines Adressspeichers unter /22. In diesem Beispiel wird 10.21.0.0/22 verwendet.



Die Bereitstellung dauert ungefähr 4 bis 5 Stunden. Nach Abschluss des Prozesses muss überprüft werden, ob die Implementierung erfolgreich war. Greifen Sie über das Azure-Portal auf die Private Cloud zu. Nach Abschluss der Bereitstellung wird ein Status von erfolgreich angezeigt.

Eine Private Cloud für eine Azure VMware Lösung erfordert ein virtuelles Azure Netzwerk. Da die Azure VMware Lösung vCenter vor Ort nicht unterstützt, sind für die Integration in eine vorhandene lokale Umgebung zusätzliche Schritte erforderlich. Zudem ist die Einrichtung einer ExpressRoute-Verbindung und eines virtuellen Netzwerk-Gateways erforderlich. Während Sie warten, bis die Cluster-Bereitstellung abgeschlossen ist, erstellen Sie ein neues virtuelles Netzwerk oder verwenden Sie ein vorhandenes für die Verbindung mit Azure VMware Lösung.


Home
nimoavspriv
AVS Private cloud
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Identity
Clusters
Delete
Essentials
Resource group (change)
NimoAVSDemo
Status
Succeeded
Location
East US 2
Subscription (change)
SaaS Backup Production
Subscription ID
b58a041a-e464-4497-8be9-9048369ee8e1
Tags (change)
Click here to add tags
Address block for private cloud
10.21.0.0/22
Primary peering subnet
10.21.0.232/30
Secondary peering subnet
10.21.0.236/30
Private Cloud Management network
10.21.0.0/26
vMotion network
10.21.1.128/25
Number of hosts
3

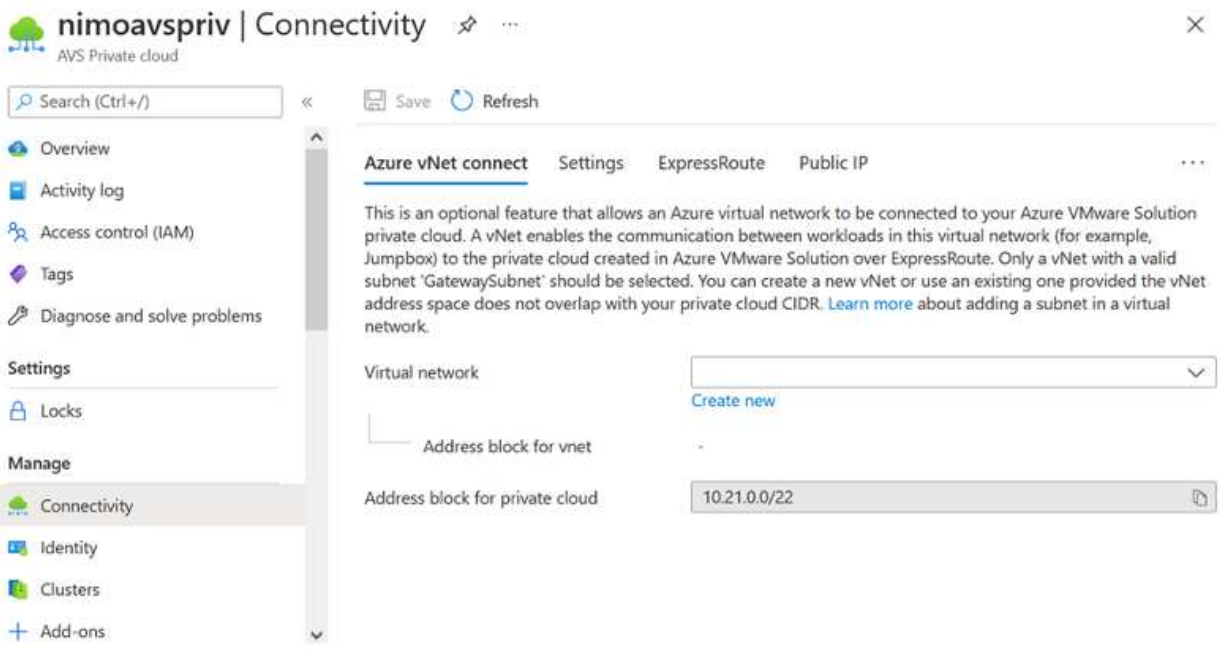
Stellen Sie eine Verbindung zu einem neuen oder vorhandenen virtuellen ExpressRoute Netzwerk-Gateway her

Um ein neues Azure Virtual Network (vnet) zu erstellen, wählen Sie die Registerkarte Azure vnet Connect aus. Alternativ können Sie aus dem Azure-Portal eine manuell erstellen mit dem Assistenten zum Erstellen von virtuellen Netzwerken:

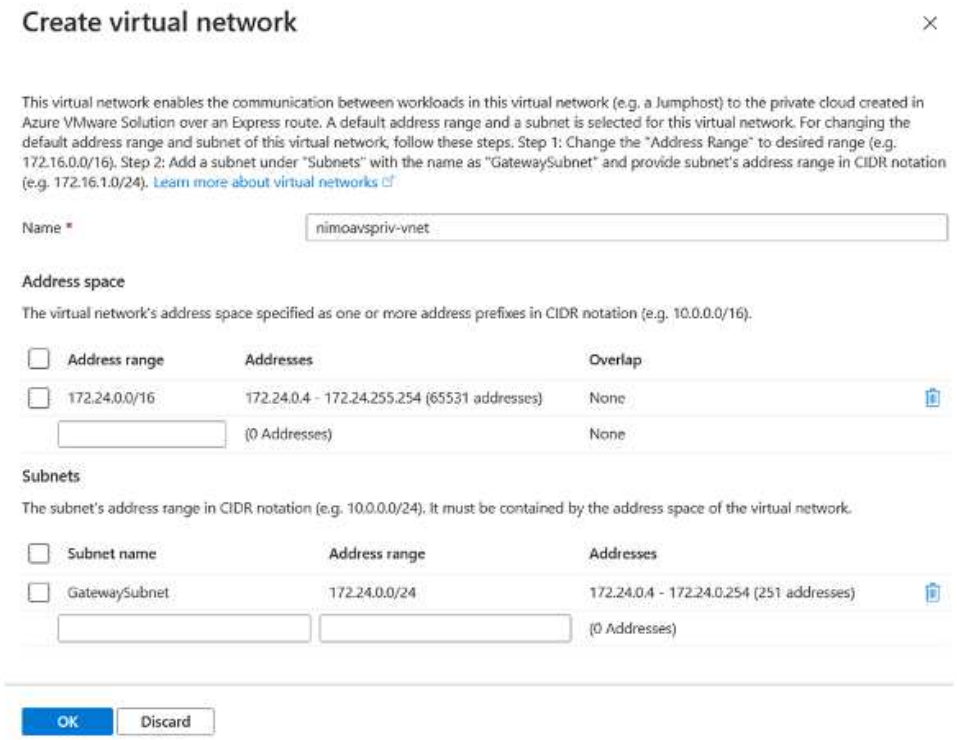
1. Gehen Sie zur Azure VMware Solution Private Cloud und greifen Sie unter Manage auf Konnektivität zu.
2. Wählen Sie Azure vnet Connect aus.
3. Um ein neues vnet zu erstellen, wählen Sie die Option Neue erstellen.

   Mit dieser Funktion kann ein vnet mit der Azure VMware-Lösung Private Cloud verbunden werden. Vnet ermöglicht die Kommunikation zwischen Workloads in diesem virtuellen Netzwerk, indem die erforderlichen Komponenten automatisch erstellt werden (z. B. Sprungbox, Shared Services wie Azure NetApp Files und Cloud Volume ONTAP) in der in Azure VMware Lösung erstellten Private Cloud über ExpressRoute.

   Hinweis: der vnet-Adressraum sollte sich nicht mit der privaten Cloud CIDR überschneiden.



4. Geben Sie die Informationen für die neue vnet ein, oder aktualisieren Sie sie, und wählen Sie OK.

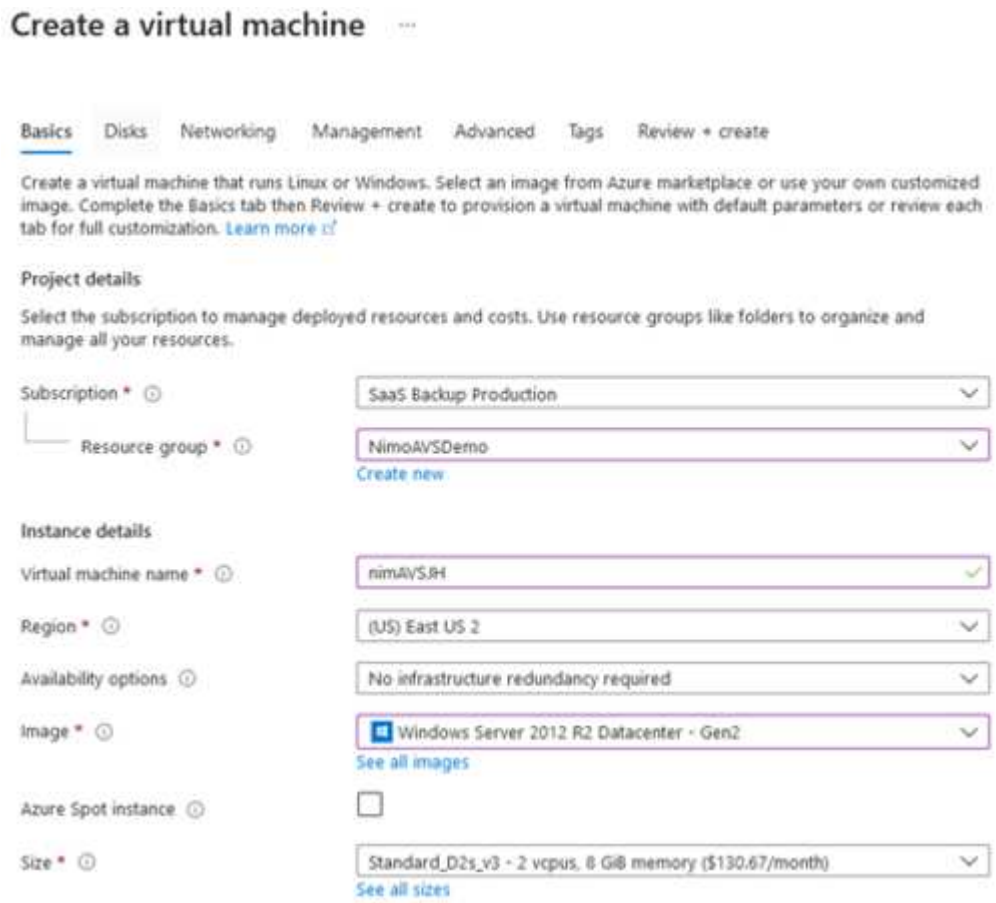


Das vnet mit dem angegebenen Adressbereich und Gateway Subnetz wird in der designierten Abonnement- und Ressourcengruppe erstellt.

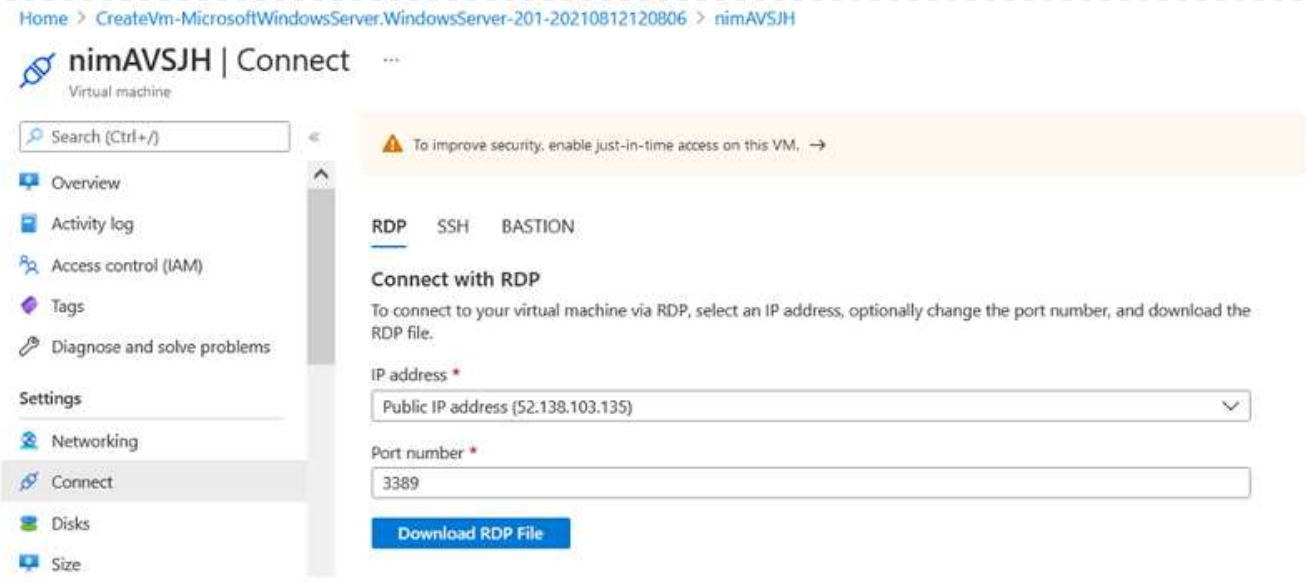
Wenn Sie ein vnet manuell erstellen, erstellen Sie ein virtuelles Netzwerk-Gateway mit der entsprechenden SKU und ExpressRoute als Gateway-Typ. Nach Abschluss der Implementierung verbinden Sie die ExpressRoute Verbindung mit dem virtuellen Netzwerk-Gateway mit der Private Cloud der Azure VMware Lösung über den Autorisierungsschlüssel. Weitere Informationen finden Sie unter "Konfigurieren Sie das Networking für Ihre VMware Private Cloud in Azure".

Netzwerkverbindung und Zugriff auf Azure VMware Solution Private Cloud validieren

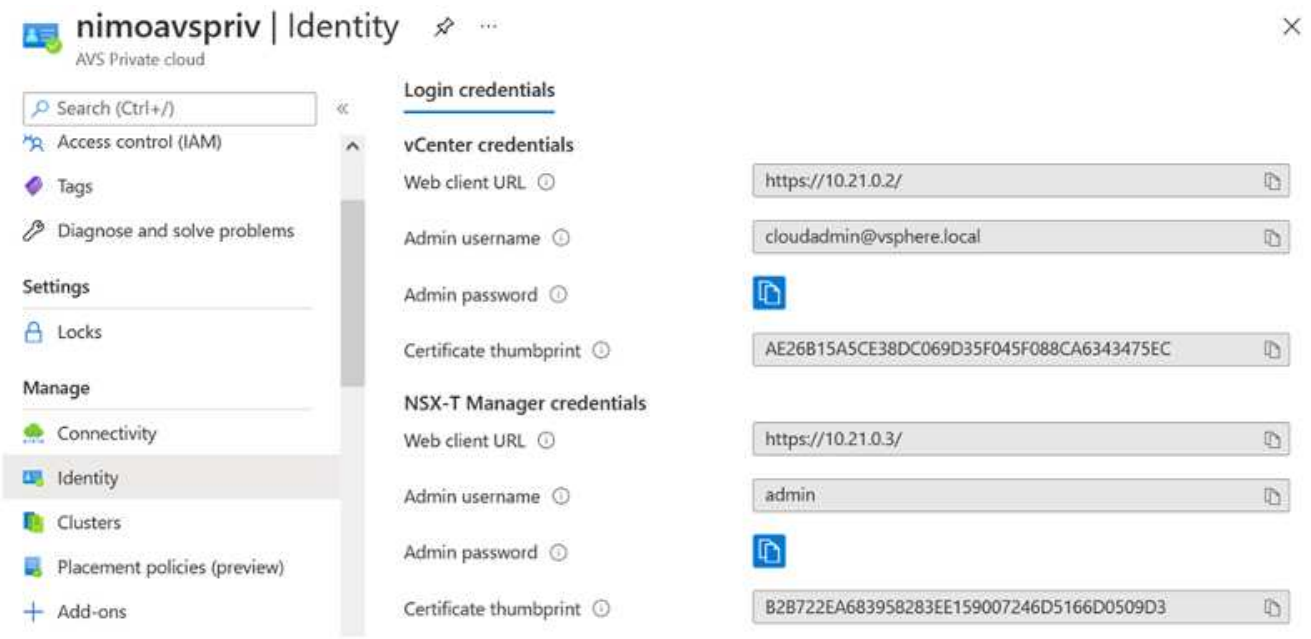
Mit der Azure VMware Lösung können Sie eine Private Cloud nicht über VMware vCenter vor Ort managen. Stattdessen ist zum Herstellen der Verbindung mit der vCenter Instanz der Azure VMware Lösung ein Sprunglink auf den Host erforderlich. Erstellen Sie einen Sprunghost in der angegebenen Ressourcengruppe und melden Sie sich bei Azure VMware Solution vCenter an. Dieser Jump-Host sollte eine Windows VM in demselben virtuellen Netzwerk sein, das für die Konnektivität erstellt wurde und sowohl vCenter als auch den NSX Manager nutzen sollte.



Nachdem die virtuelle Maschine bereitgestellt wurde, verwenden Sie die Option Verbinden, um auf RDP zuzugreifen.

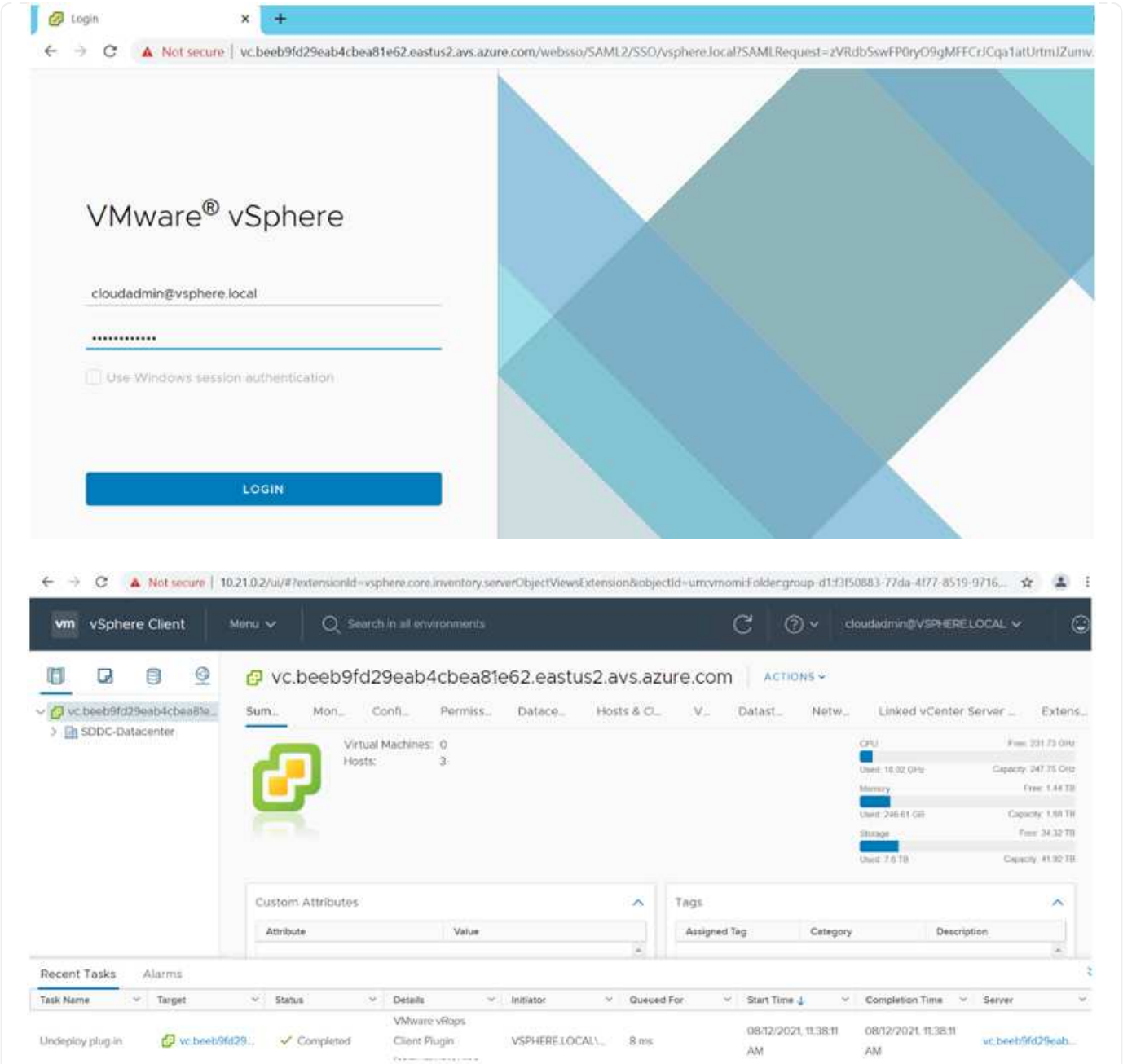


Melden Sie sich von dieser neu erstellten Jump-Host-virtuellen Maschine mit dem Cloud-Admin-Benutzer in vCenter an. Rufen Sie zum Zugreifen auf die Anmeldedaten im Azure-Portal auf und navigieren Sie zu „Identity“ (Identitäts-Management (über die Option „Manage“ in der Private Cloud). Die URLs und Benutzeranmeldeinformationen für die private Cloud vCenter und NSX-T Manager können hier kopiert werden.



Öffnen Sie in der virtuellen Windows-Maschine einen Browser, und navigieren Sie zur vCenter Web-Client-URL Und verwenden Sie den Admin-Benutzernamen als **cloudadmin@vsphere.local** und fügen Sie das kopierte Passwort ein. Auf ähnliche Weise kann auch NSX-T-Manager über die Web-Client-URL zugegriffen werden Und verwenden Sie den Admin-Benutzernamen und fügen Sie das kopierte Passwort ein, um neue Segmente zu erstellen oder die vorhandenen Tier-Gateways zu ändern.

Die Web-Client-URLs sind für jede bereitgestellte SDDC unterschiedlich.



Die Azure VMware Lösung SDDC ist jetzt implementiert und konfiguriert. Nutzung von ExpressRoute Global REACH zur Verbindung der lokalen Umgebung mit der Private Cloud der Azure VMware Lösung Weitere Informationen finden Sie unter "Erstellen Sie Peer-on-Premises-Umgebungen mit der Azure VMware Lösung".

Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)

Wie bei vor Ort ist die Planung der Google Cloud VMware Engine (GCVE) entscheidend für eine erfolgreiche produktionsbereite Umgebung für das Erstellen von VMs und die Migration.

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und managen und in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp Storage verwenden.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

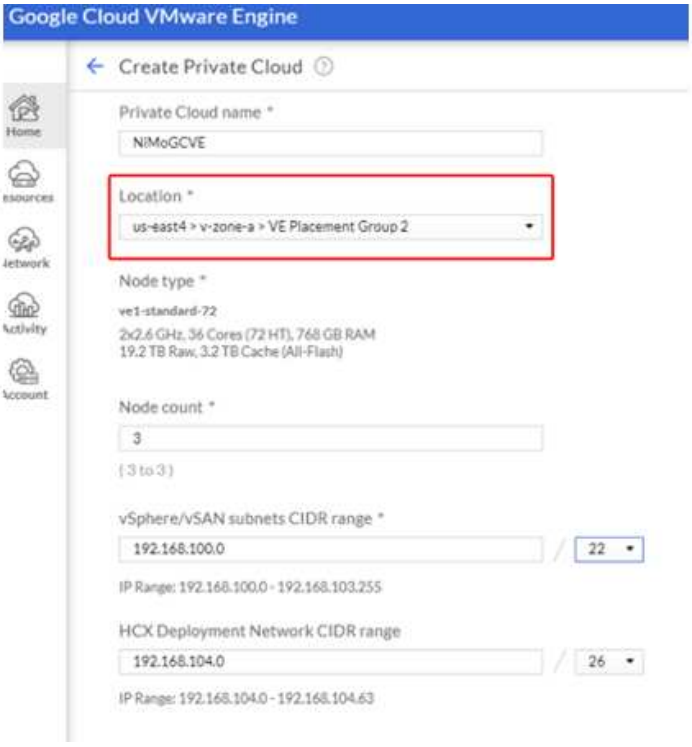
GCVE bereitstellen und konfigurieren

Um eine GCVE-Umgebung auf GCP zu konfigurieren, melden Sie sich bei der GCP-Konsole an und greifen Sie auf das VMware Engine-Portal zu.

Klicken Sie auf die Schaltfläche „Neue private Cloud“ und geben Sie die gewünschte Konfiguration für die GCVE Private Cloud ein. Achten Sie beim „Standort“ darauf, die Private Cloud in derselben Region/Zone, in der CVS/CVO implementiert wird, zu implementieren, um die beste Performance und die niedrigste Latenz zu gewährleisten.

Voraussetzungen:

- Einrichtung der IAM-Rolle des VMware Engine Service Admin
- "VMware Engine-API-Zugriff und Node-Kontingent aktivieren"
- Stellen Sie sicher, dass der CIDR-Bereich nicht mit Ihren lokalen oder Cloud-Subnetzen überlappt. Der CIDR-Bereich muss /27 oder höher sein.



Hinweis: Die Erstellung einer privaten Cloud kann zwischen 30 Minuten und 2 Stunden dauern.

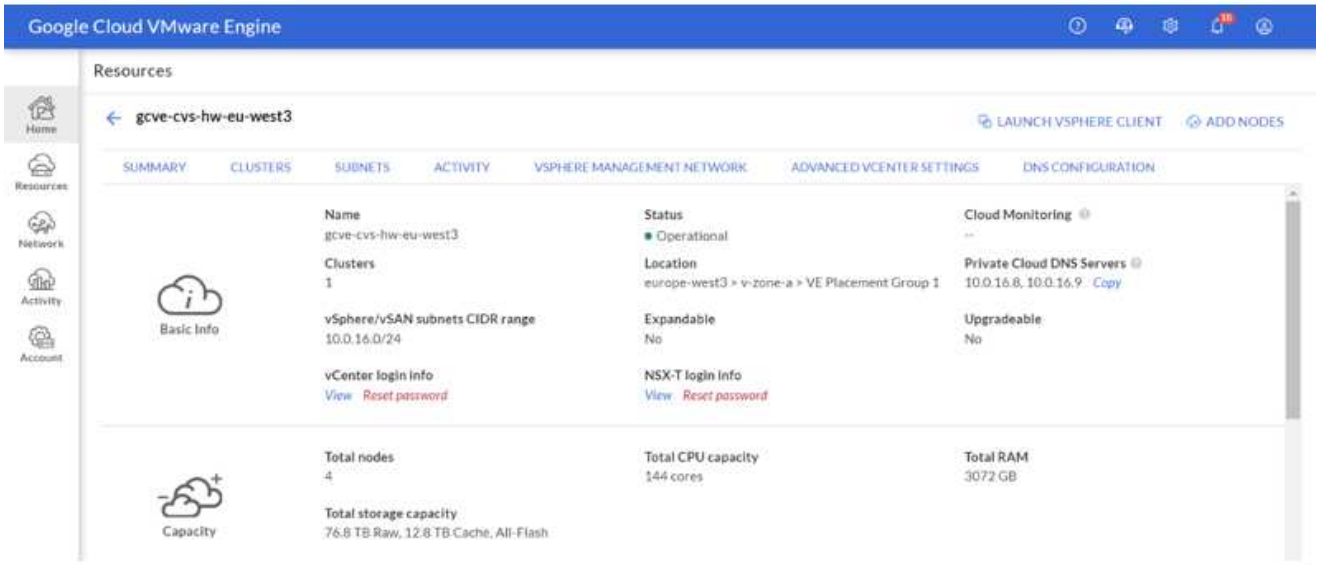
Aktivieren Sie den privaten Zugriff auf GCVE

Konfigurieren Sie nach der Bereitstellung der Private Cloud den privaten Zugriff auf die Private Cloud für eine Verbindung mit hohem Durchsatz und niedriger Latenz.

Dadurch wird sichergestellt, dass das VPC-Netzwerk, auf dem Cloud Volumes ONTAP-Instanzen ausgeführt werden, mit der GCVE Private Cloud kommunizieren kann. Folgen Sie dazu dem "GCP-Dokumentation". Richten Sie für den Cloud Volume Service eine Verbindung zwischen VMware Engine und Cloud Volumes Service ein, indem Sie einmalig zwischen den Mandanten-Host-Projekten Peering durchführen. Gehen Sie wie folgt vor, um ausführliche Schritte zu erhalten "Verlinken".

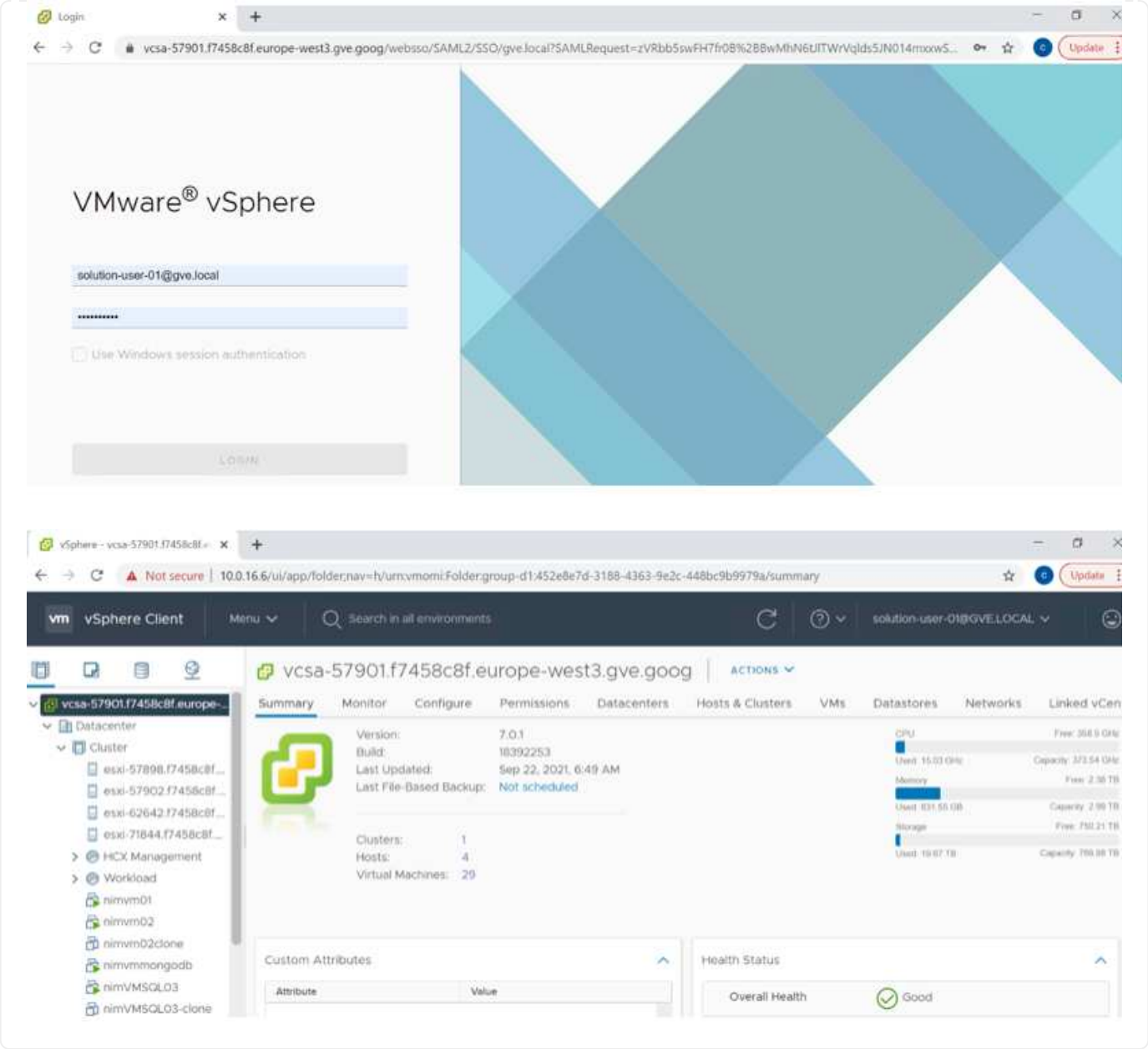
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

Melden Sie sich mit dem CloudOwner@gve.local-Benutzer bei vcenter an. Rufen Sie das VMware Engine Portal auf, rufen Sie zu Ressourcen auf und wählen Sie die entsprechende Private Cloud aus. Klicken Sie im Abschnitt grundlegende Informationen auf den Link Anzeigen, um die vCenter-Anmeldedaten (vCenter Server, HCX Manager) oder NSX-T-Anmeldeinformationen (NSX Manager) anzuzeigen.



Öffnen Sie in einer virtuellen Windows-Maschine einen Browser, und navigieren Sie zur vCenter Web-Client-URL Verwenden Sie dann den Admin-Benutzernamen als CloudOwner@gve.local, und fügen Sie das kopierte Passwort ein. Auf ähnliche Weise kann auch NSX-T-Manager über die Web-Client-URL zugegriffen werden Und verwenden Sie den Admin-Benutzernamen und fügen Sie das kopierte Passwort ein, um neue Segmente zu erstellen oder die vorhandenen Tier-Gateways zu ändern.

Wenn Sie ein lokales Netzwerk zur Private Cloud der VMware Engine verbinden möchten, nutzen Sie Cloud-VPN oder Cloud Interconnect, um entsprechende Konnektivität zu erhalten und stellen sicher, dass die erforderlichen Ports geöffnet sind. Gehen Sie wie folgt vor, um ausführliche Schritte zu erhalten "Verlinken".



Stellen Sie zusätzlichen Datastore für den NetApp-Cloud-Volume-Service in GCVE bereit

Siehe "Verfahren zum Bereitstellen von zusätzlichem NFS-Datastore mit NetApp CVS zu GCVE"

NetApp Storage-Optionen für Public-Cloud-Provider

Entdecken Sie die Optionen für NetApp als Storage in den drei wichtigsten Hyperscalern.

AWS/VMC

AWS unterstützt NetApp Storage in den folgenden Konfigurationen:

- FSX ONTAP als Storage mit Gastverbunden
- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- FSX ONTAP als zusätzlichen NFS-Datastore

Details anzeigen "Storage-Optionen für VMC für Gastverbindung". Details anzeigen "Zusätzliche NFS-Datastore-Optionen für VMC".

Azure/AVS

Azure unterstützt NetApp Storage in den folgenden Konfigurationen:

- Azure NetApp Files (ANF) als Storage mit Gastverbunden
- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- Azure NetApp Files (ANF) als zusätzlicher NFS-Datastore

Details anzeigen "Gastanbindung Speicheroptionen für AVS". Details anzeigen "Zusätzliche NFS-Datastore-Optionen für AVS".

GCP/GCVE

Google Cloud unterstützt NetApp Storage in den folgenden Konfigurationen:

- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- Cloud Volumes Service (CVS) als Storage mit Gastverbunden
- Cloud Volumes Service (CVS) als zusätzlicher NFS Datastore

Details anzeigen "Speicheroptionen für die Gastverbindung für GCVE".

Weitere Informationen "Unterstützung von NetApp Cloud Volumes Service-Datastores für die Google Cloud VMware Engine (NetApp Blog)" Oder "Verwendung von NetApp CVS als Datastores für Google Cloud VMware Engine (Google Blog)"

TR-4938: Mounten Sie Amazon FSX für ONTAP als NFS-Datenspeicher mit VMware Cloud auf AWS

Niyaz Mohamed, NetApp

Einführung

Alle erfolgreichen Unternehmen befinden sich auf dem Weg der Transformation und Modernisierung. Im Rahmen dieses Prozesses setzen Unternehmen in der Regel ihre vorhandenen VMware-Investitionen ein, um von den Cloud-Vorteilen zu profitieren und die Migration, den Burst, die Erweiterung und die Bereitstellung von Disaster Recovery für Prozesse so nahtlos wie möglich zu untersuchen. Kunden, die in die Cloud migrieren, müssen die Anwendungsfälle für Flexibilität und Burst, den Ausstieg aus dem Datacenter, die Datacenter-Konsolidierung, End-of-Life-Szenarien, Fusionen, Firmenübernahmen usw.

Obwohl VMware Cloud auf AWS die bevorzugte Option für die Mehrheit der Kunden ist, da es Kunden einzigartige Hybrid-Funktionen bietet, haben begrenzte native Storage-Optionen die Nützlichkeit für Unternehmen mit Storage-lastigen Workloads eingeschränkt. Da Storage direkt an Hosts gebunden ist, besteht

die einzige Möglichkeit zur Skalierung des Storage darin, weitere Hosts hinzuzufügen. Dadurch lassen sich die Kosten bei Storage-intensiven Workloads um 35 bis 40 % oder mehr senken. Diese Workloads benötigen zusätzlichen Storage und eine abgegrenzte Performance – keine zusätzliche Leistung, sondern die Kosten für zusätzliche Hosts. Hier ist der "Neueste Integration" Der FSX für ONTAP eignet sich mit VMware Cloud auf AWS für Storage- und Performance-intensive Workloads.

Betrachten wir einmal das folgende Szenario: Ein Kunde benötigt acht Hosts für mehr Performance (vCPU/Vmem), hat aber auch einen erheblichen Storage-Bedarf. Basierend auf ihrem Assessment benötigen sie 16 Hosts, um die Storage-Anforderungen zu erfüllen. Dies erhöht die Gesamtbetriebskosten, da diese zusätzliche Leistung anschaffen müssen, wenn überhaupt mehr Storage benötigt wird. Dies gilt für alle Anwendungsfälle, einschließlich Migration, Disaster Recovery, Bursting, Entwicklung/Test, Und so weiter.

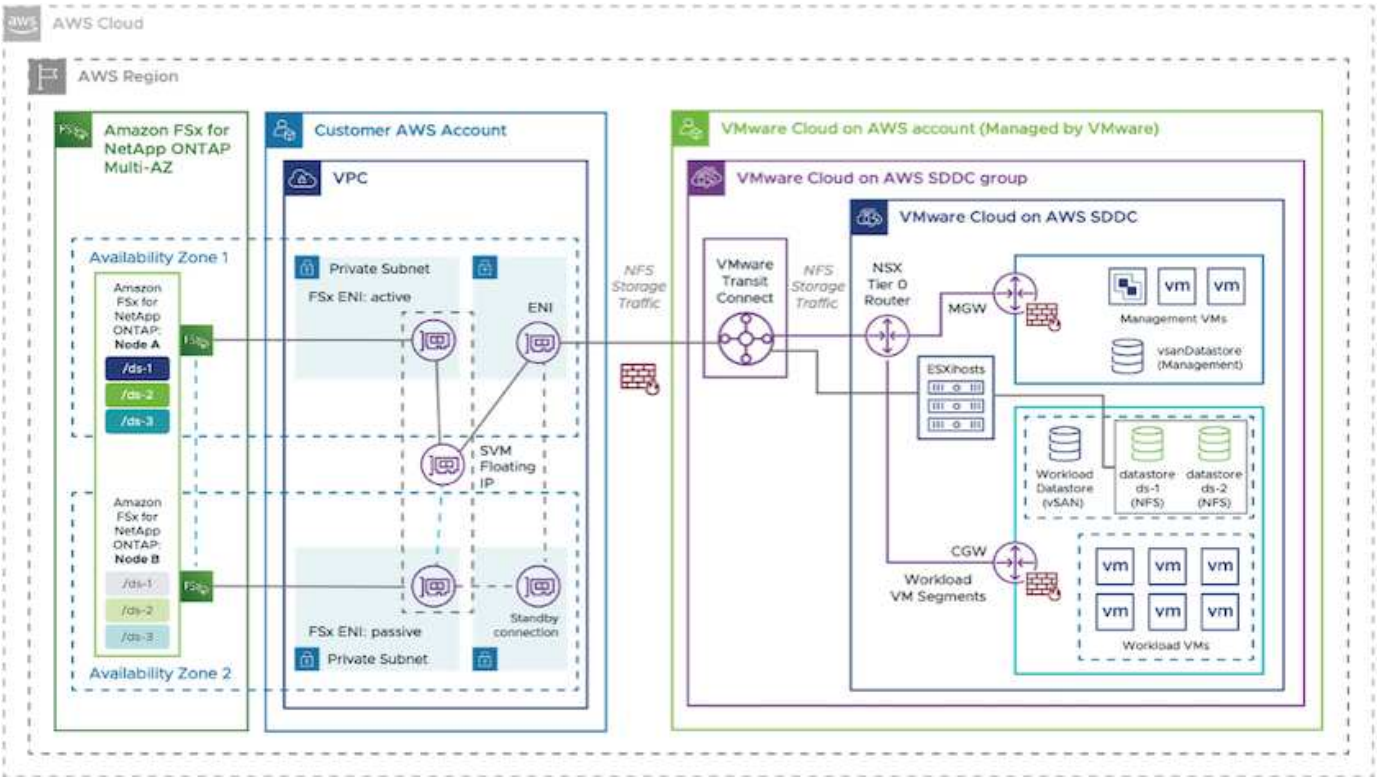
In diesem Dokument werden die Schritte aufgeführt, die erforderlich sind, um FSX für ONTAP als NFS-Datenspeicher für VMware Cloud auf AWS bereitzustellen und anzuhängen.

Diese Lösung ist auch bei VMware verfügbar. Besuchen Sie das "VMware Cloud Tech Zone" Finden Sie weitere Informationen.

Konnektivitätsoptionen

VMware Cloud auf AWS unterstützt sowohl Implementierungen mit mehreren Verfügbarkeitszonen als auch mit einer Verfügbarkeitszone von FSX für ONTAP.

In diesem Abschnitt wird die grundlegende Konnektivitätsarchitektur beschrieben sowie die nötigen Schritte zur Implementierung der Lösung zur Erweiterung des Storage in einem SDDC-Cluster ohne zusätzliche Hosts beschrieben.



Die grundlegenden Implementierungsschritte sind wie folgt:

1. Amazon FSX für ONTAP in einem neuen benannten VPC erstellen.

2. Erstellen einer SDDC-Gruppe
3. VMware Transit Connect und einen TGW-Anhang erstellen.
4. Konfigurieren von Routing (AWS VPC und SDDC) und Sicherheitsgruppen.
5. Verbinden Sie ein NFS-Volume als Datastore mit dem SDDC-Cluster.

Bevor Sie FSX für ONTAP als NFS-Datastore bereitstellen und anhängen, müssen Sie zuerst eine VMware auf Cloud SDDC-Umgebung einrichten oder ein vorhandenes SDDC-System mit Upgrade auf v1.20 oder höher installieren. Weitere Informationen finden Sie im "Erste Schritte mit VMware Cloud on AWS".

FSX für ONTAP wird derzeit nicht mit Stretch-Clustern unterstützt.

Schlussfolgerung

Dieses Dokument behandelt die Schritte, die zur Konfiguration von Amazon FSX für ONTAP mit VMware Cloud on AWS erforderlich sind. Amazon FSX für ONTAP bietet hervorragende Optionen zum Implementieren und Managen von Applikations-Workloads und Fileservices sowie zur Senkung der TCO, da die Datenanforderungen nahtlos auf die Applikationsebene reduziert werden. Wie auch immer der Anwendungsfall funktioniert: Wählen Sie VMware Cloud auf AWS zusammen mit Amazon FSX for ONTAP, um schnell von den Vorteilen der Cloud zu profitieren, konsistente Infrastruktur und Abläufe von On-Premises-Systemen zu AWS, bidirektionale Portabilität von Workloads und Kapazität und Performance der Enterprise-Klasse zu realisieren. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren für die Verbindung von Speicher. Denken Sie daran, dass nur die Position der geänderten Daten zusammen mit neuen Namen bekannt ist. Die Tools und Prozesse bleiben dieselben, und Amazon FSX für ONTAP trägt zur Optimierung der generellen Implementierung bei.

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

Amazon FSX für ONTAP VMware Cloud

NetApp Guest Connected Storage-Optionen für AWS

AWS unterstützt NetApp Storage mit Anbindung an Gäste über den nativen FSX-Service (FSX ONTAP) oder über Cloud Volumes ONTAP (CVO).

FSX ONTAP

Amazon FSX für NetApp ONTAP ist ein vollständig gemanagter Service, der zuverlässigen, skalierbaren, hochperformanten und funktionsreichen File Storage auf der Basis des beliebten ONTAP Filesystems von NetApp bietet. FSX für ONTAP kombiniert die bekannten Funktionen, Performance, Funktionen und API-Vorgänge von NetApp Filesystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig gemanagten AWS Service.

FSX für ONTAP bietet funktionsreichen, schnellen und flexiblen Shared-File-Storage, der weit über Linux-, Windows- und macOS-Computing-Instanzen zugänglich ist, die in AWS oder vor Ort ausgeführt werden. FSX für ONTAP bietet hochperformanten SSD-Storage (Solid State Drive) mit Latenzzeiten von unter einer Millisekunde. Mit FSX für ONTAP können Sie SSD-Performance-Level für Ihre Workloads erzielen und gleichzeitig die Kosten für SSD-Storage mit nur einem Bruchteil Ihrer Daten bezahlen.

Das Datenmanagement mit FSX für ONTAP gestaltet sich einfacher, da Sie Ihre Dateien mit nur einem Mausklick erstellen, klonen und replizieren können. Außerdem führt FSX für ONTAP automatisch ein Tiering Ihrer Daten auf kostengünstigeren, elastischen Storage durch. Dadurch reduzieren Sie die Bereitstellung oder

das Management von Kapazität.

FSX für ONTAP bietet außerdem hochverfügbaren und langlebigen Storage mit vollständig gemanagten Backups und unterstützt Disaster Recovery über mehrere Regionen hinweg. FSX für ONTAP unterstützt gängige Sicherheits- und Antivirenanwendungen für die Datensicherung und erleichtert so den Schutz und die Sicherung Ihrer Daten.

FSX ONTAP als Storage mit Gastverbunden

Konfiguration von Amazon FSX für NetApp ONTAP mit VMware Cloud auf AWS

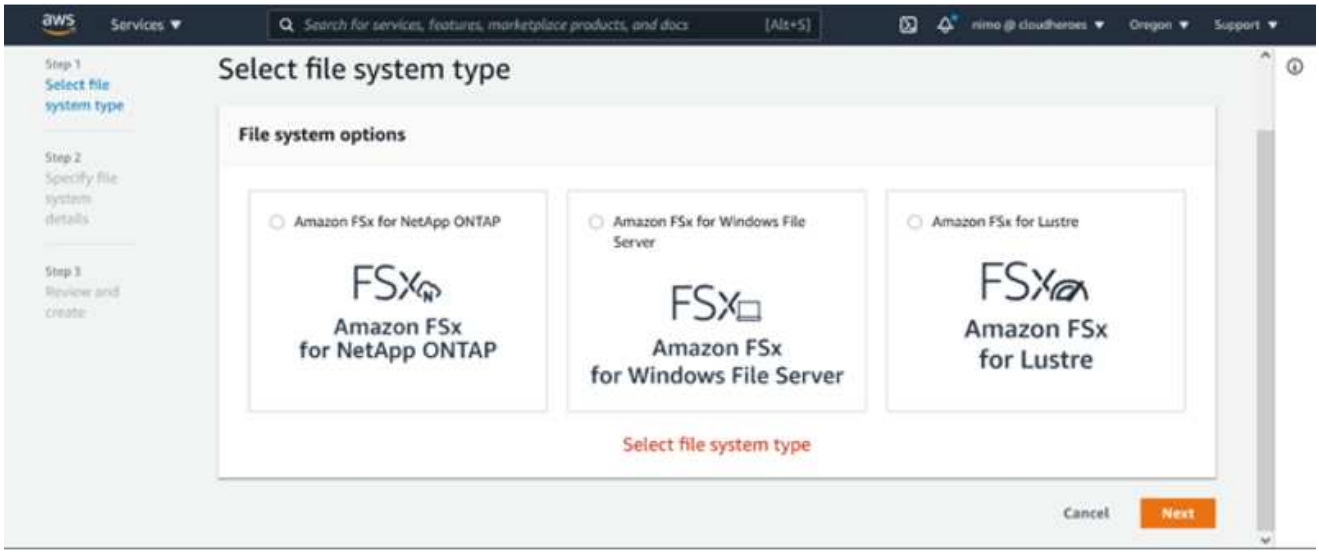
Amazon FSX für NetApp ONTAP Dateifreigaben und LUNs können von VMs gemountet werden, die in der VMware SDDC Umgebung bei VMware Cloud bei AWS erstellt wurden. Die Volumes können auch auf dem Linux-Client eingebunden und mithilfe des NFS- oder SMB-Protokolls auf dem Windows-Client abgebildet werden. LUNs sind unter Linux- oder Windows-Clients als Block-Geräte verfügbar, wenn sie über iSCSI eingebunden werden. Amazon FSX für das NetApp ONTAP Filesystem lässt sich mit den folgenden Schritten schnell einrichten.

Amazon FSX für NetApp ONTAP und VMware Cloud auf AWS müssen sich in derselben Verfügbarkeitszone befinden, um eine bessere Performance zu erzielen und Datenübertragungsgebühren zwischen Verfügbarkeitszonen zu vermeiden.

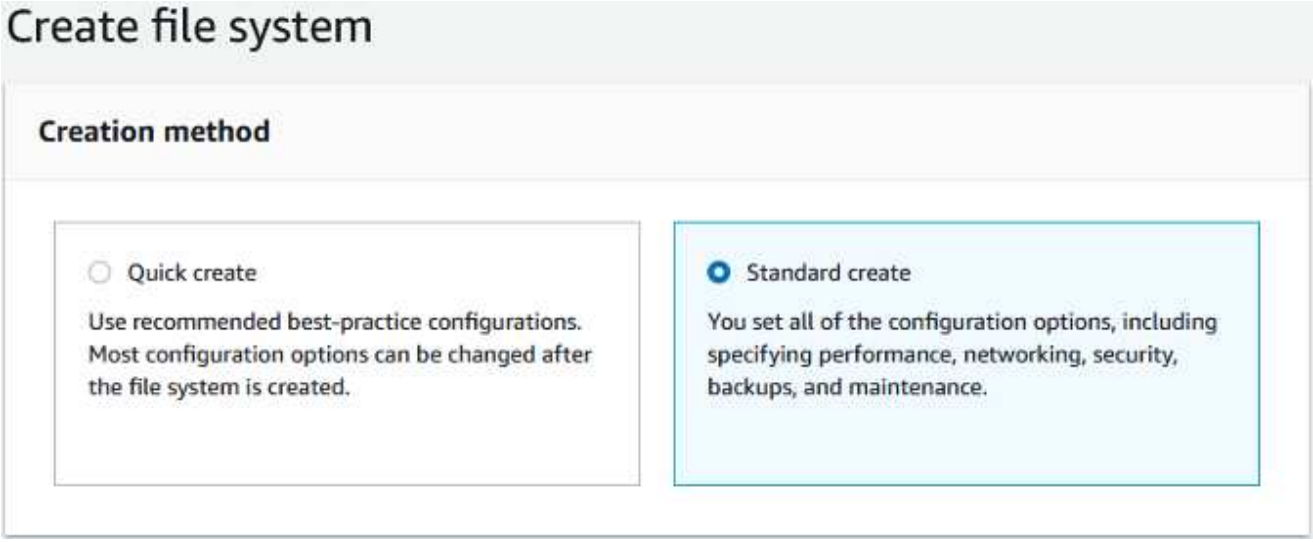
Amazon FSX für ONTAP Volumes erstellen und mounten

So erstellen und mounten Sie Amazon FSX für NetApp ONTAP Filesystem:

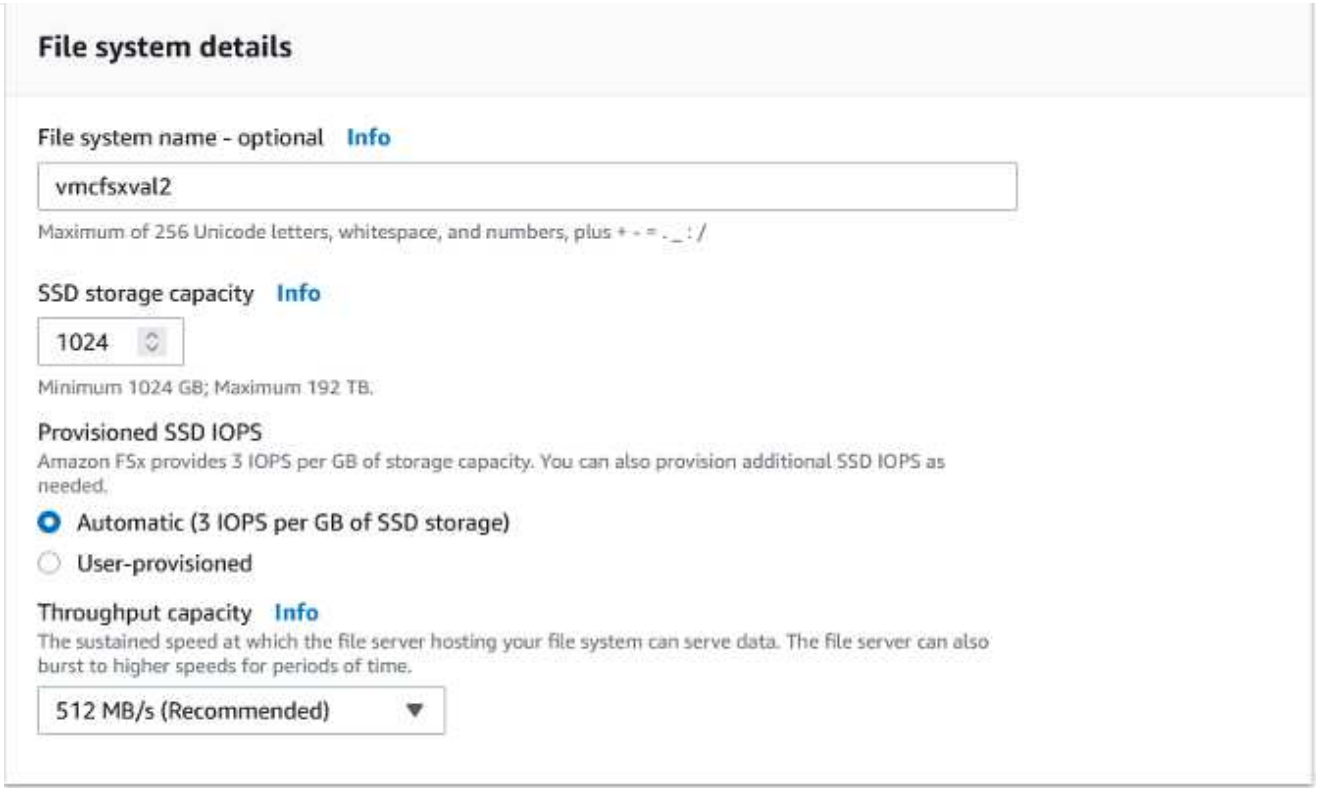
1. Öffnen Sie das "Amazon FSX-Konsole" Und wählen Sie Create File System, um den Assistenten zur Erstellung von Dateisystemen zu starten.
2. Wählen Sie auf der Seite Select File System Type „Amazon FSX for NetApp ONTAP“ und anschließend „Weiter“. Die Seite Dateisystem erstellen wird angezeigt.



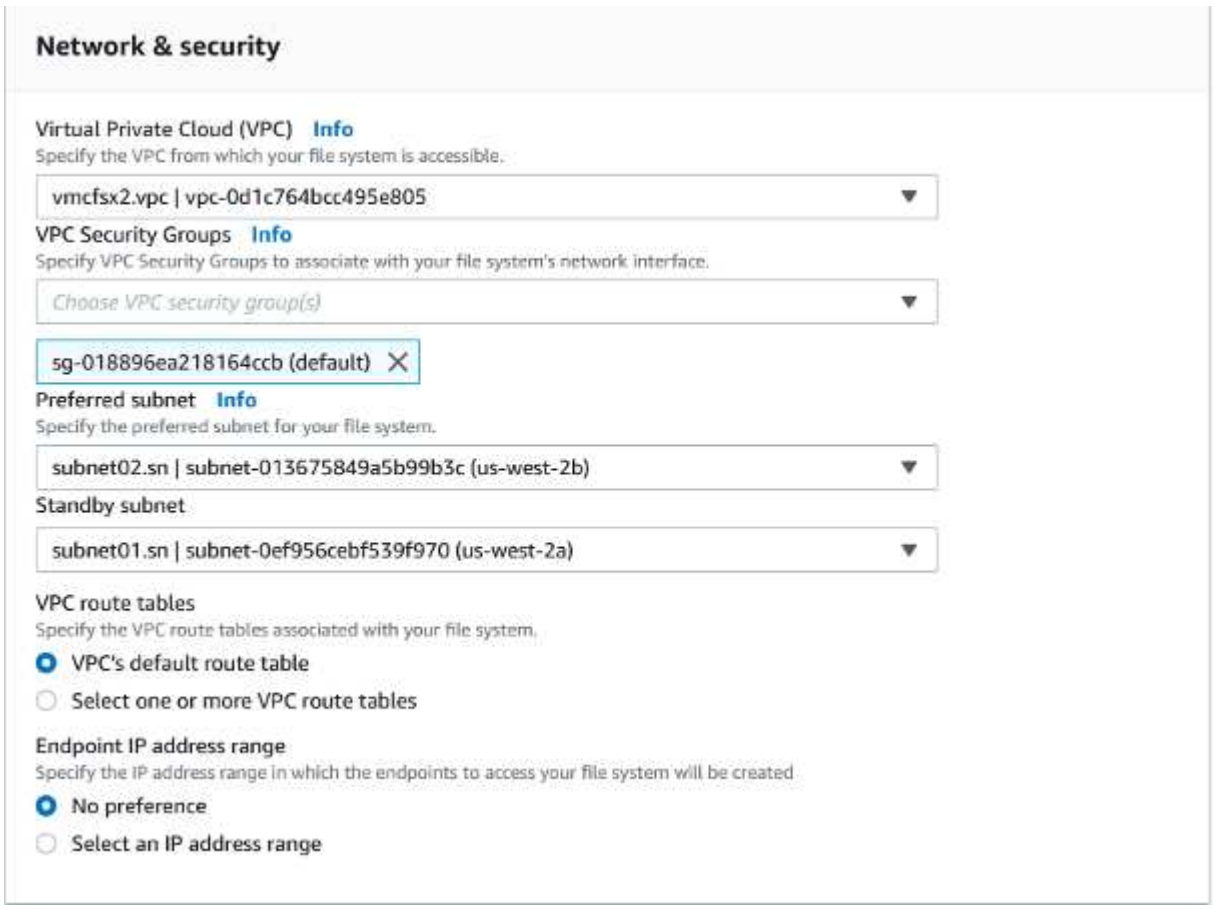
1. Wählen Sie im Abschnitt Networking für Virtual Private Cloud (VPC) die geeignete VPC und die bevorzugten Subnetze zusammen mit der Routing-Tabelle aus. In diesem Fall wird vmcfsx2.vpc aus dem Dropdown-Menü ausgewählt.



1. Wählen Sie für die Erstellungsmethode die Option Standarderstellung. Sie können auch schnell erstellen wählen, aber dieses Dokument verwendet die Option Standard create.

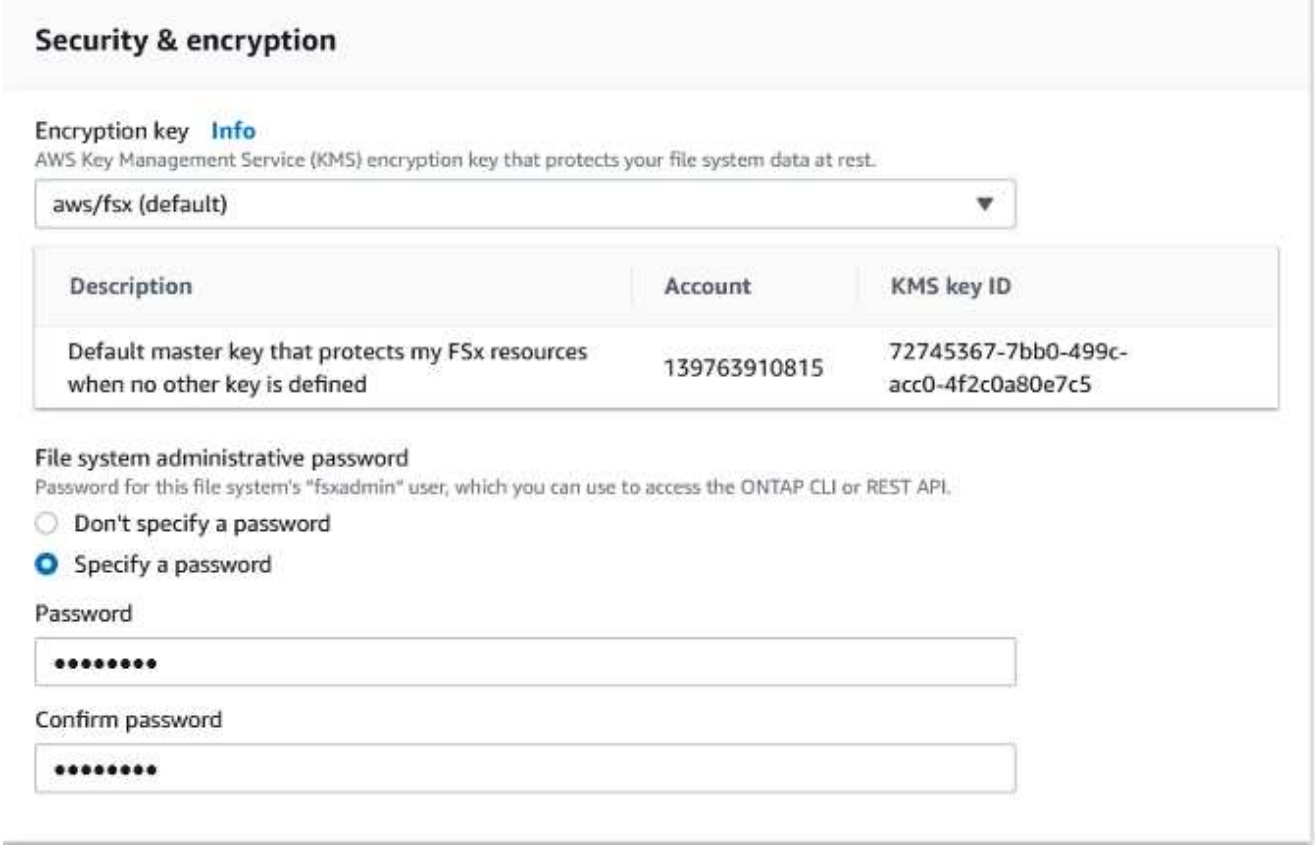


1. Wählen Sie im Abschnitt Networking für Virtual Private Cloud (VPC) die geeignete VPC und die bevorzugten Subnetze zusammen mit der Routing-Tabelle aus. In diesem Fall wird vmcfsx2.vpc aus dem Dropdown-Menü ausgewählt.

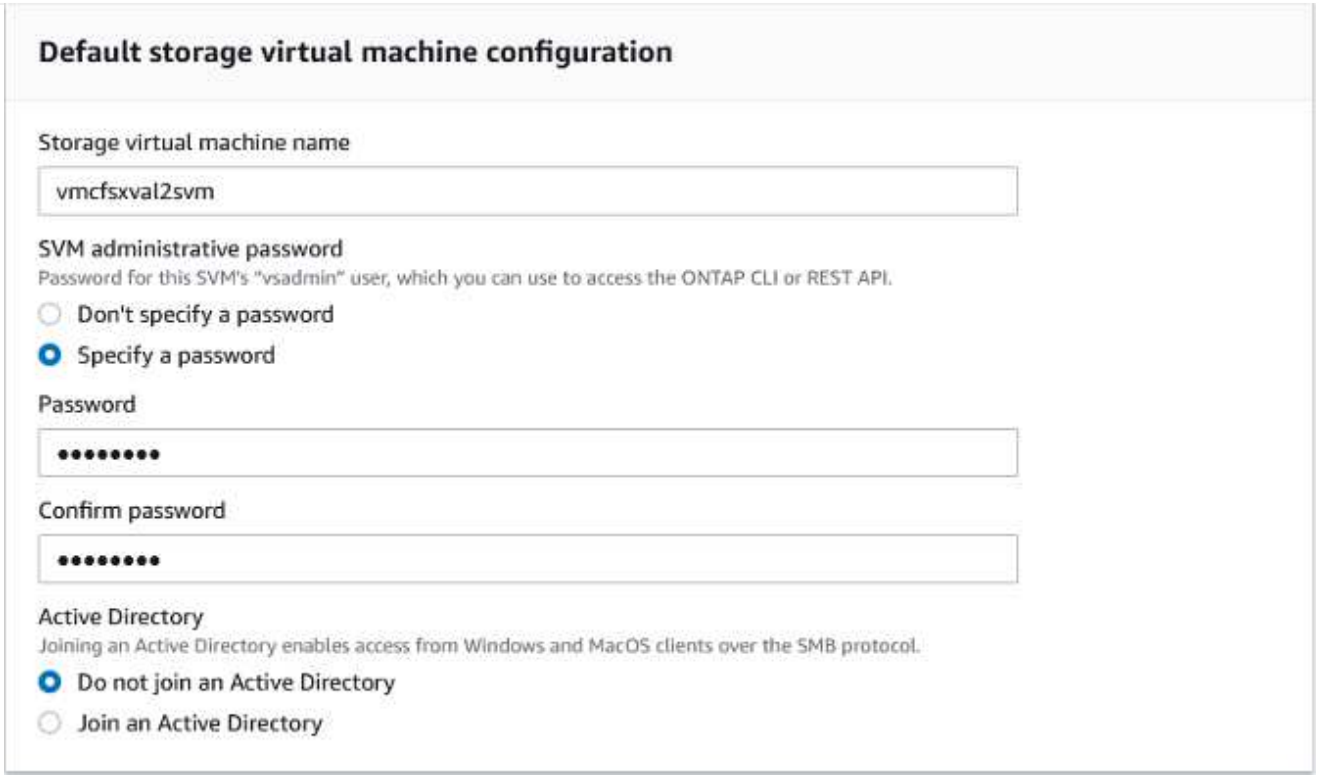


Wählen Sie im Abschnitt Networking für Virtual Private Cloud (VPC) die geeignete VPC und die bevorzugten Subnetze zusammen mit der Routing-Tabelle aus. In diesem Fall wird vmcfsx2.vpc aus dem Dropdown-Menü ausgewählt.

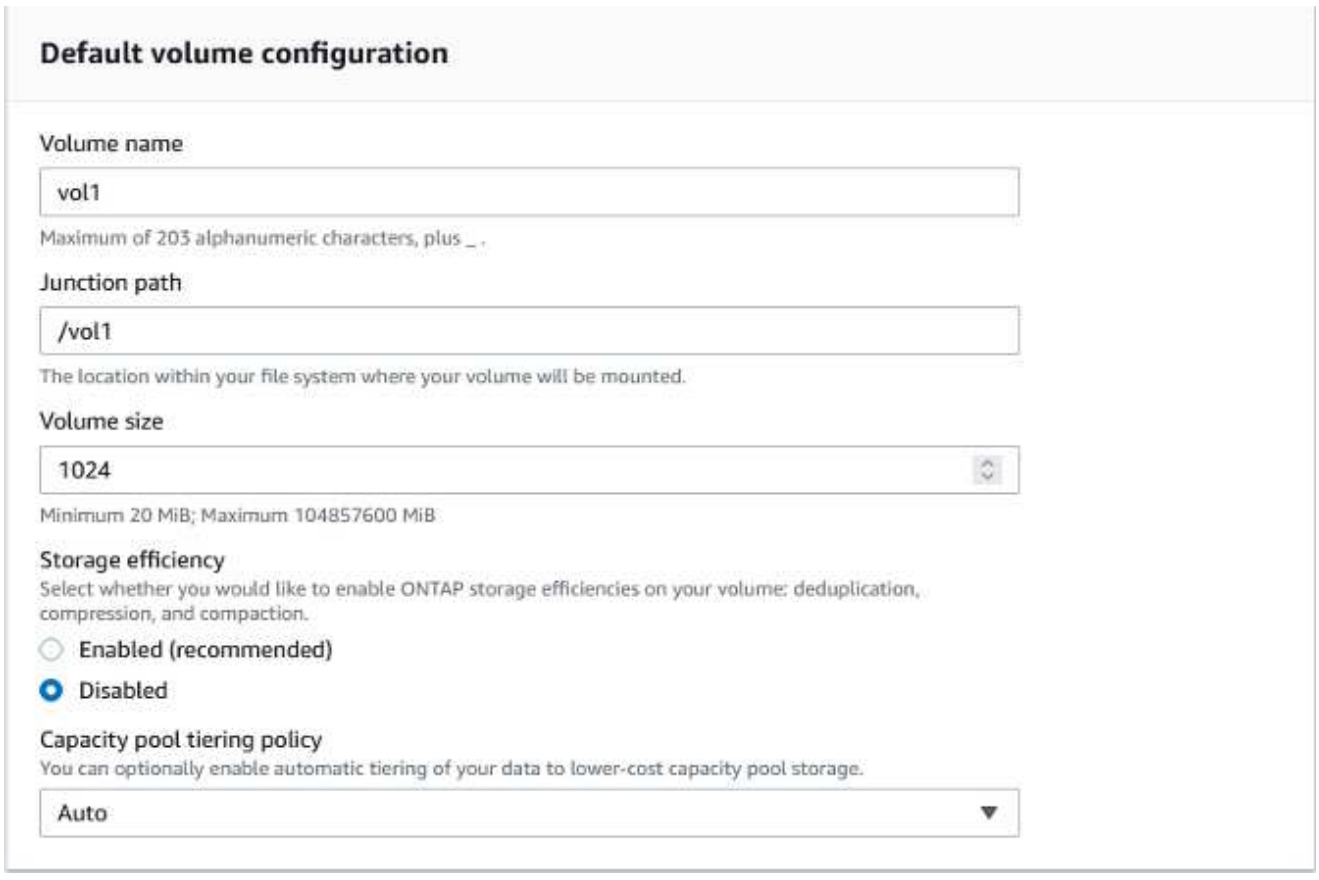
1. Wählen Sie im Abschnitt Sicherheit und Verschlüsselung für den Verschlüsselungsschlüssel den AWS KMS-Schlüssel (Key Management Service) aus, der die Daten des Filesystems im Ruhezustand schützt. Geben Sie für das Administratorkennwort des Dateisystems ein sicheres Kennwort für den Benutzer fsxadmin ein.



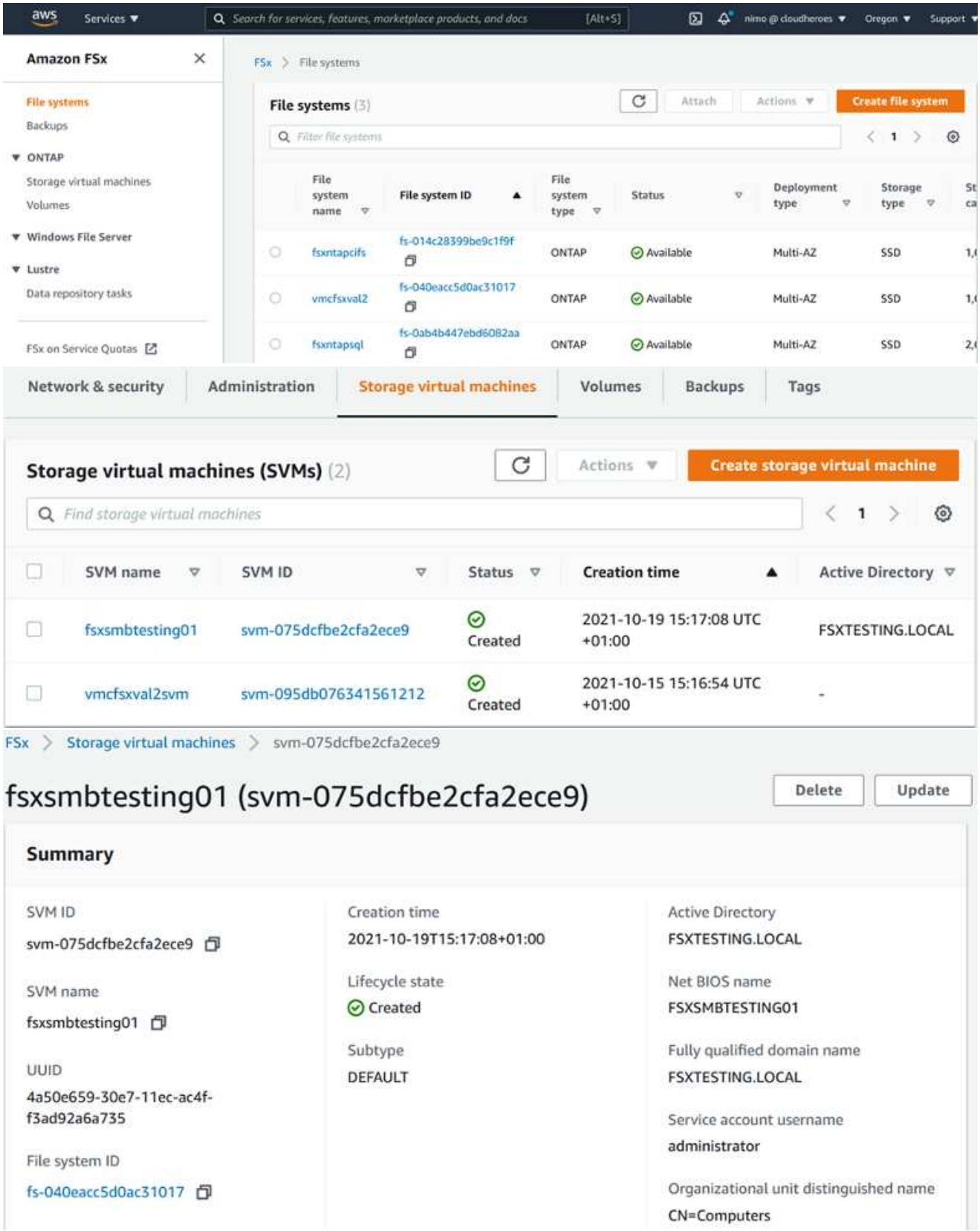
1. Geben Sie in der Virtual Machine das Passwort an, das mit vsadmin für die Administration von ONTAP mit REST-APIs oder der CLI verwendet werden soll. Wenn kein Passwort angegeben wird, kann ein fsxadmin-Benutzer für die Verwaltung der SVM verwendet werden. Stellen Sie im Abschnitt „Active Directory“ sicher, dass Sie Active Directory zur SVM zur Bereitstellung von SMB-Freigaben verbinden. Geben Sie im Abschnitt Konfiguration von Standardspeichern Virtual Machines einen Namen für den Storage ein. In dieser Validierung werden SMB-Freigaben über eine selbst gemanagte Active Directory-Domäne bereitgestellt.



1. Geben Sie im Abschnitt Standard-Volume-Konfiguration den Namen und die Größe des Volumes an. Dies ist ein NFS-Volume. Wählen Sie aus, um die ONTAP Storage-Effizienzfunktionen (Komprimierung, Deduplizierung und Data-Compaction) zu aktivieren oder zu deaktivieren.



1. Überprüfen Sie die Konfiguration des Dateisystems, die auf der Seite Dateisystem erstellen angezeigt wird.
2. Klicken Sie Auf Dateisystem Erstellen.

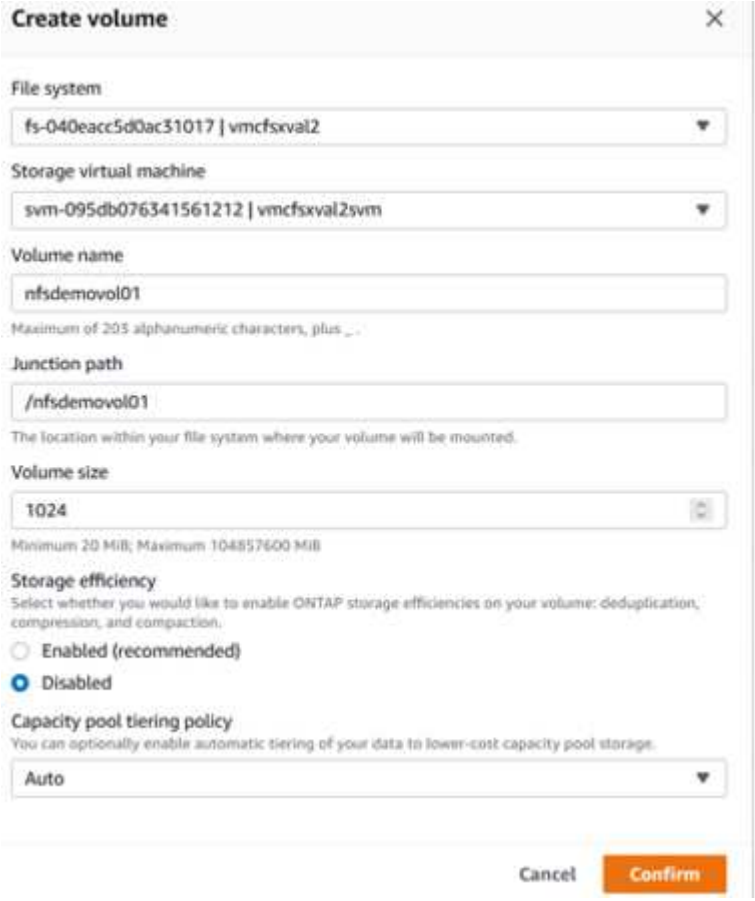


Weitere Informationen finden Sie unter "Erste Schritte mit Amazon FSX für NetApp ONTAP".

Nachdem das Filesystem wie oben erstellt wurde, erstellen Sie das Volume mit der erforderlichen Größe und dem erforderlichen Protokoll.

1. Öffnen Sie das "Amazon FSX-Konsole".
2. Wählen Sie im linken Navigationsbereich Dateisysteme und anschließend das ONTAP-Dateisystem aus, für das Sie ein Volume erstellen möchten.
3. Wählen Sie die Registerkarte Volumes aus.
4. Wählen Sie die Registerkarte Volume erstellen.
5. Das Dialogfeld Volume erstellen wird angezeigt.

Zu Demonstrationszwecken wird ein NFS-Volume in diesem Abschnitt erstellt, das leicht auf VMs eingebunden werden kann, die auf VMware Cloud auf AWS laufen. Nfsdemovol01 wird wie unten dargestellt erstellt:



Mounten Sie FSX ONTAP Volume auf dem Linux Client

So mounten Sie das im vorherigen Schritt erstellte FSX ONTAP-Volumen. Führen Sie von den Linux VMs innerhalb von VMC auf dem AWS SDDC folgende Schritte aus:

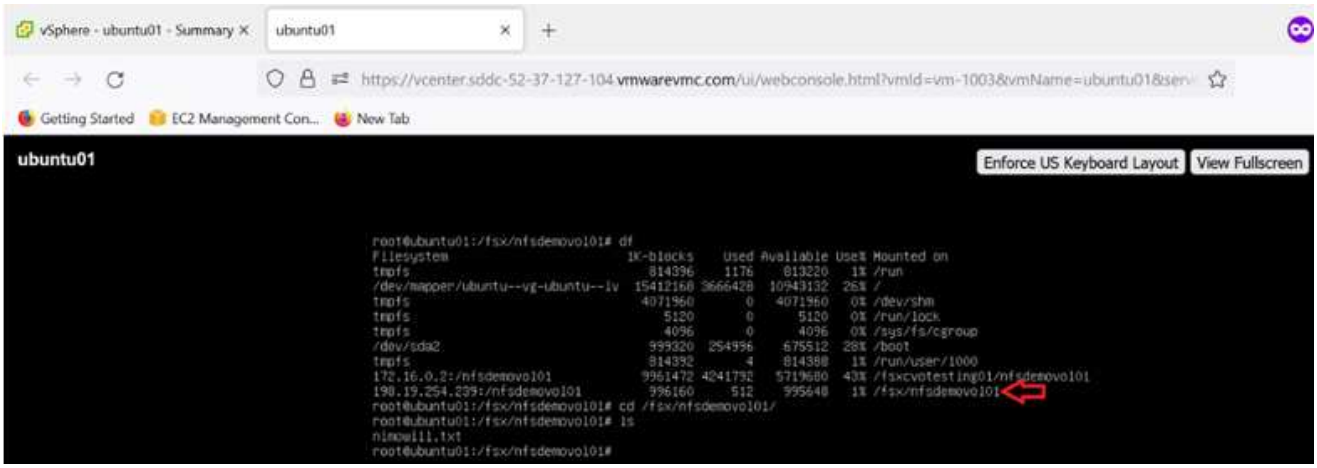
1. Stellen Sie eine Verbindung mit der angegebenen Linux-Instanz her.
2. Öffnen Sie ein Terminal auf der Instanz mithilfe von Secure Shell (SSH), und melden Sie sich mit den entsprechenden Anmeldedaten an.
3. Erstellen Sie mit dem folgenden Befehl ein Verzeichnis für den Mount-Punkt des Volumes:

```
 $ sudo mkdir /fsx/nfsdemovol01
. Mounten Sie das Amazon FSX für NetApp ONTAP NFS Volume in das
Verzeichnis, das im vorherigen Schritt erstellt wurde.
```

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01
/fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. Führen Sie einmal ausgeführt den df-Befehl aus, um den Mount zu überprüfen.



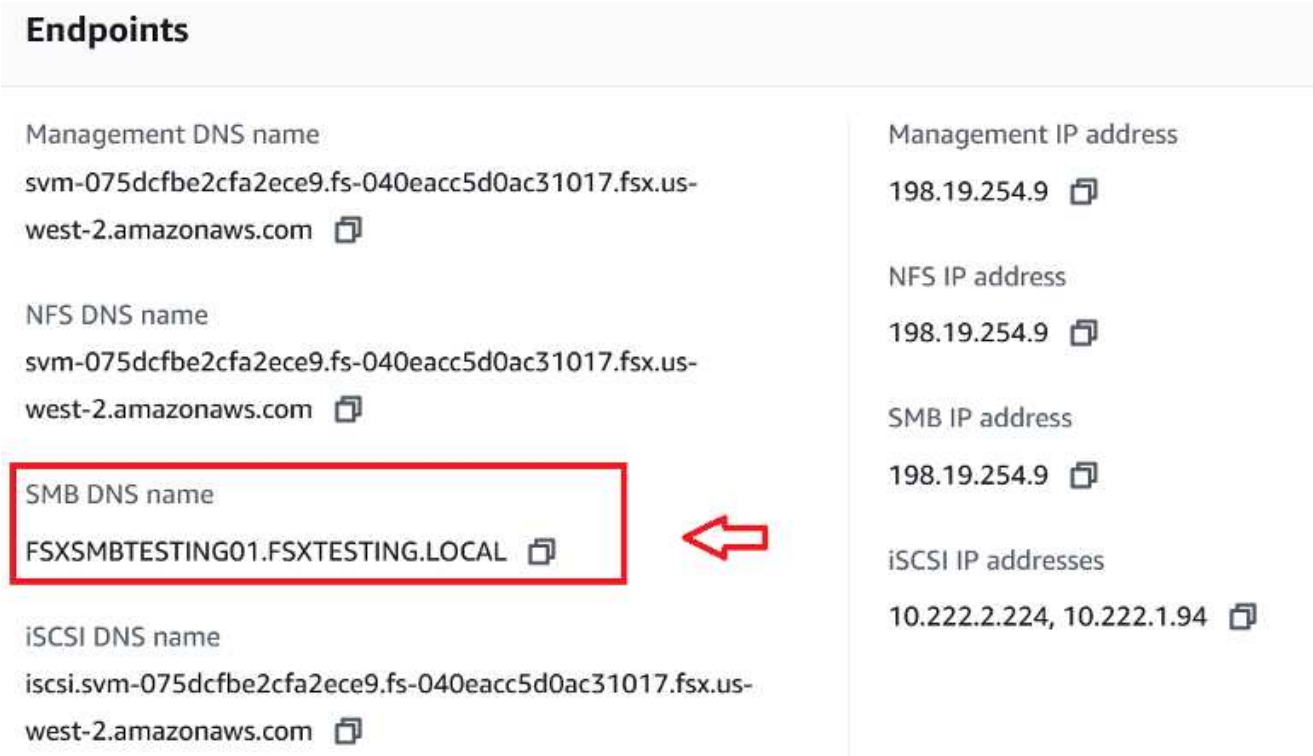
Mounten Sie FSX ONTAP Volume auf dem Linux Client

Hängen Sie FSX ONTAP Volumes an Microsoft Windows Clients an

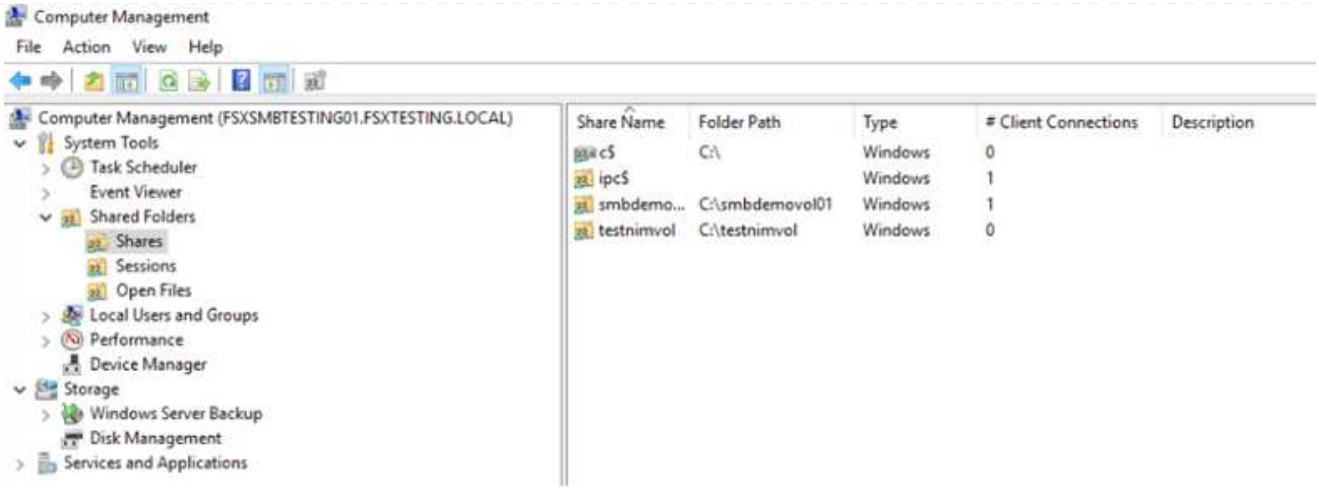
Um Dateifreigaben auf einem Amazon FSX-Dateisystem zu verwalten und zuzuordnen, muss die GUI für freigegebene Ordner verwendet werden.

1. Öffnen Sie das Startmenü, und führen Sie fsmgmt.msc mit Ausführen als Administrator aus. Dadurch wird das GUI-Tool für freigegebene Ordner geöffnet.
2. Klicken Sie auf Aktion > Alle Aufgaben, und wählen Sie mit einem anderen Computer verbinden.
3. Geben Sie für einen anderen Computer den DNS-Namen für die SVM (Storage Virtual Machine) ein. In diesem Beispiel wird beispielsweise FSXSMBTESTING01.FSXTESTING.LOCAL verwendet.

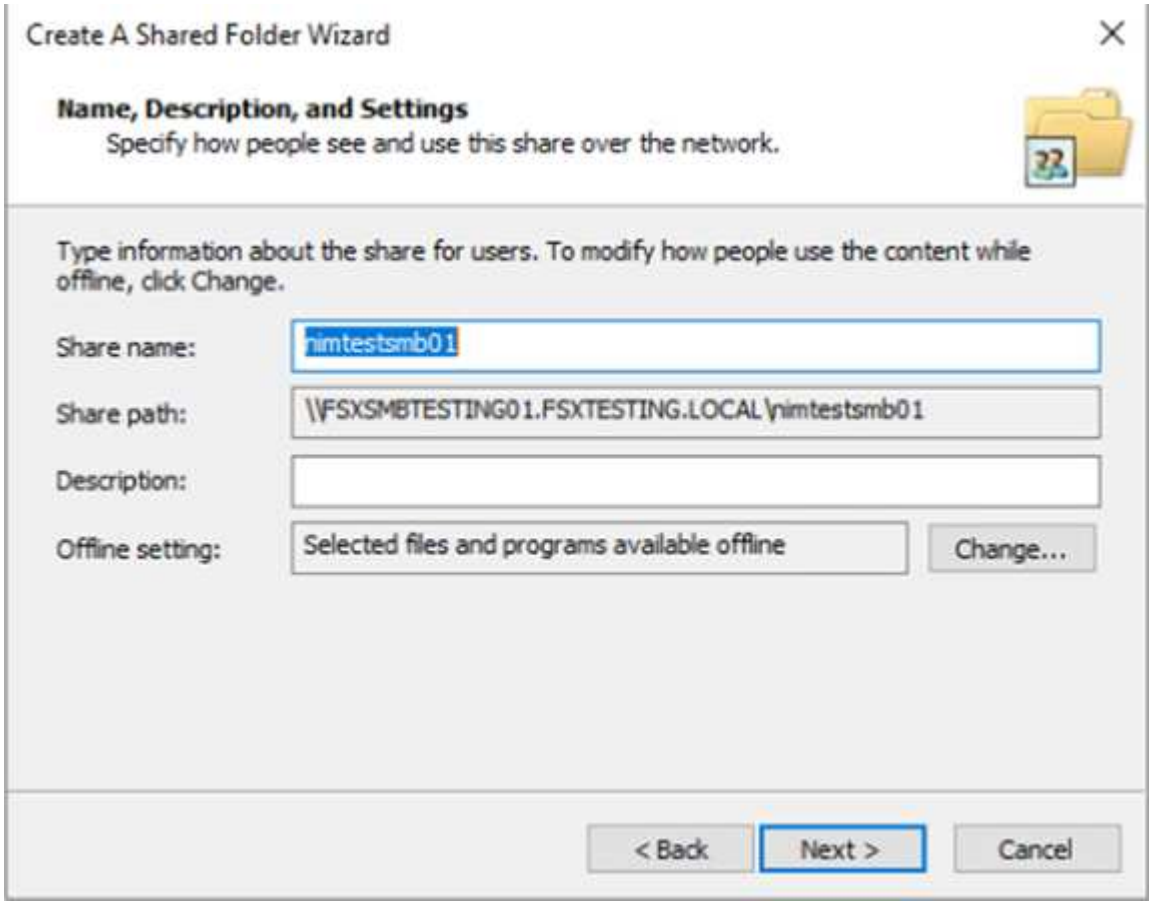
TP finden Sie den DNS-Namen der SVM in der Amazon FSX-Konsole. Wählen Sie Storage Virtual Machines, wählen Sie SVM aus, und blättern Sie dann zu Endpoints, um den SMB-DNS-Namen zu finden. Klicken Sie auf OK. Das Amazon FSX-Dateisystem wird in der Liste der freigegebenen Ordner angezeigt.



1. Wählen Sie im Tool freigegebene Ordner die Option Freigaben im linken Fensterbereich aus, um die aktiven Freigaben für das Amazon FSX-Dateisystem anzuzeigen.

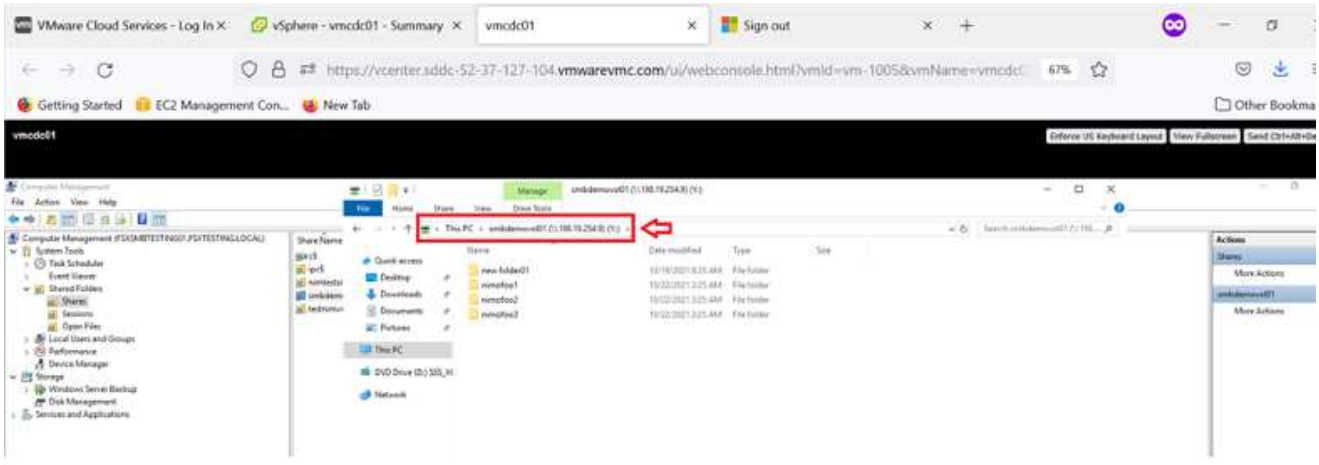


1. Wählen Sie nun eine neue Freigabe aus, und schließen Sie den Assistenten zum Erstellen eines freigegebenen Ordners ab.



Weitere Informationen zum Erstellen und Managen von SMB-Freigaben auf einem Amazon FSX-Dateisystem finden Sie unter "Erstellen von SMB-Freigaben".

1. Nach erfolgter Konnektivität kann die SMB-Freigabe angehängt und für Applikationsdaten verwendet werden. Um dies zu erreichen, kopieren Sie den Freigabepfad und verwenden Sie die Option Netzwerklaufwerk zuordnen, um das Volume auf der VM zu mounten, die auf VMware Cloud auf dem AWS SDDC ausgeführt wird.



Verbinden Sie FSX für NetApp ONTAP LUNs mit einem Host über iSCSI

Verbinden Sie FSX für NetApp ONTAP LUNs mit einem Host über iSCSI

ISCSI-Datenverkehr für FSX durchläuft das VMware Transit Connect/AWS Transit Gateway über die im vorherigen Abschnitt angegebenen Routen. Folgen Sie der Dokumentation, um eine LUN in Amazon FSX für NetApp ONTAP zu konfigurieren "Hier".

Stellen Sie auf Linux Clients sicher, dass der iSCSI-Daemon ausgeführt wird. Nachdem die LUNs bereitgestellt wurden, lesen Sie die detaillierte Anleitung zur iSCSI-Konfiguration mit Ubuntu (als Beispiel). "Hier".

In diesem Dokument wird die Verbindung der iSCSI-LUN mit einem Windows-Host dargestellt:

Bereitstellen eines LUNs in FSX für NetApp ONTAP:

1. Greifen Sie über den Management-Port des FSX für das Dateisystem ONTAP auf die NetApp ONTAP CLI zu.
2. Erstellen Sie die LUNs mit der erforderlichen Größe, wie durch die Ausgabe der Dimensionierung angegeben.

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

In diesem Beispiel haben wir eine LUN der Größe 5g (5368709120) erstellt.

1. Erstellen Sie die erforderlichen Initiatorgruppen, um zu steuern, welche Hosts auf bestimmte LUNs zugreifen können.

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators

--------- ------------ -------- --------
-----------------------------------

vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

Es wurden zwei Einträge angezeigt.

1. Ordnen Sie die LUNs Initiatorgruppen mit dem folgenden Befehl zu:

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------ ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

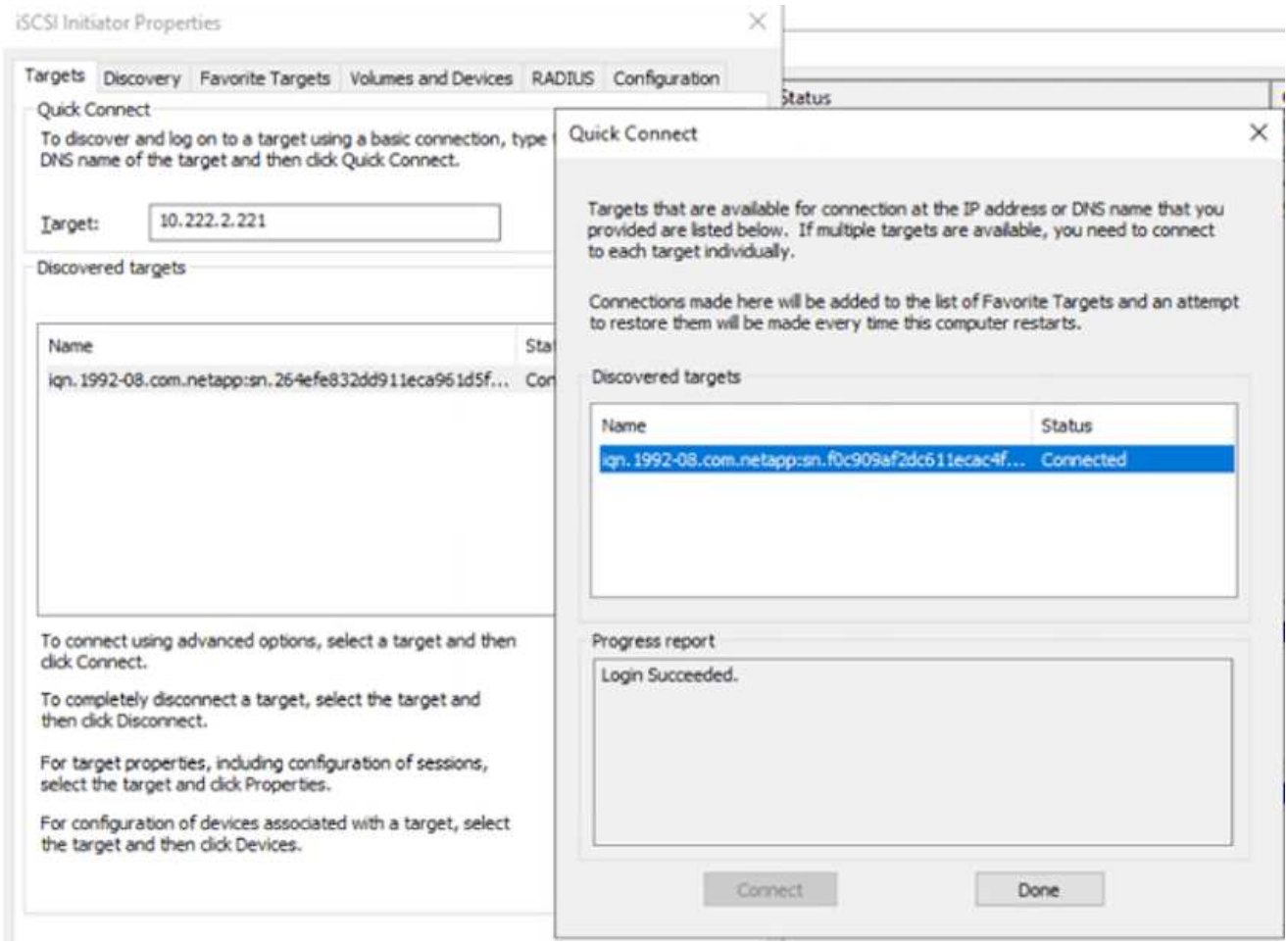
Es wurden zwei Einträge angezeigt.

1. Verbinden Sie die neu bereitgestellte LUN mit einer Windows VM:

Um den neuen LUN-Server auf einem Windows-Host in der VMware Cloud auf dem AWS SDDC zu verbinden, gehen Sie wie folgt vor:

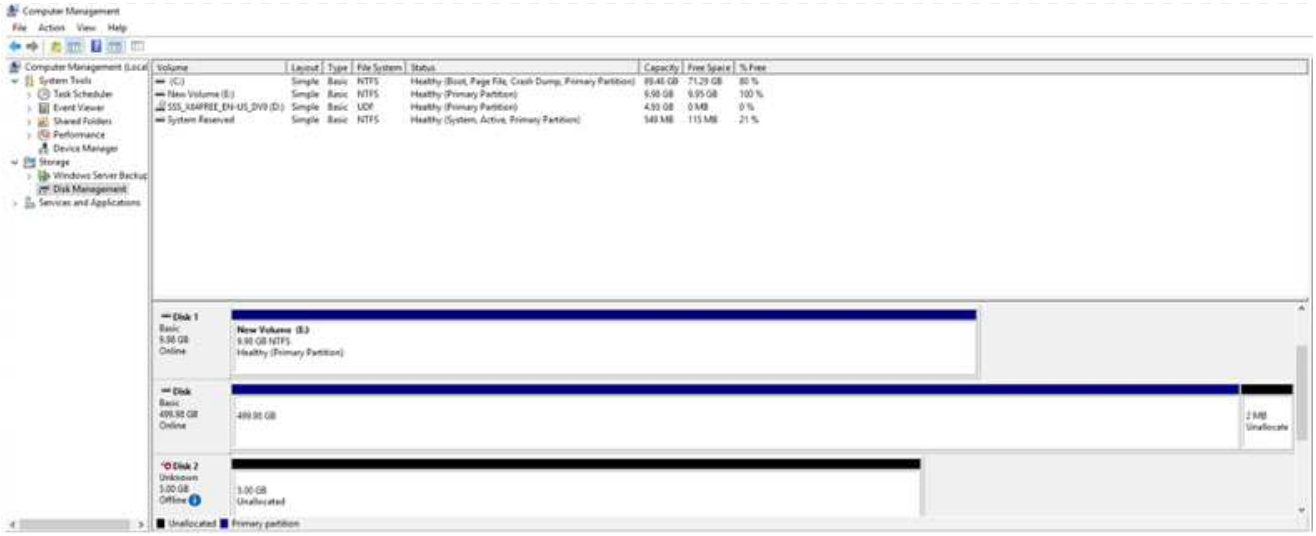
1. RDP auf die Windows VM gehostet auf der VMware Cloud auf AWS SDDC.
2. Navigieren Sie zu Server Manager > Dashboard > Tools > iSCSI Initiator, um das Dialogfeld iSCSI Initiator Properties zu öffnen.
3. Klicken Sie auf der Registerkarte Ermittlung auf Portal erkennen oder Portal hinzufügen, und geben Sie dann die IP-Adresse des iSCSI-Zielports ein.
4. Wählen Sie auf der Registerkarte Ziele das erkannte Ziel aus und klicken Sie dann auf Anmelden oder Verbinden.
5. Wählen Sie Multipath aktivieren, und wählen Sie dann „Diese Verbindung automatisch wiederherstellen, wenn der Computer startet“ oder „Diese Verbindung zur Liste der bevorzugten Ziele hinzufügen“. Klicken Sie Auf Erweitert.

Der Windows-Host muss über eine iSCSI-Verbindung zu jedem Knoten im Cluster verfügen. Das native DSM wählt die besten Pfade aus.



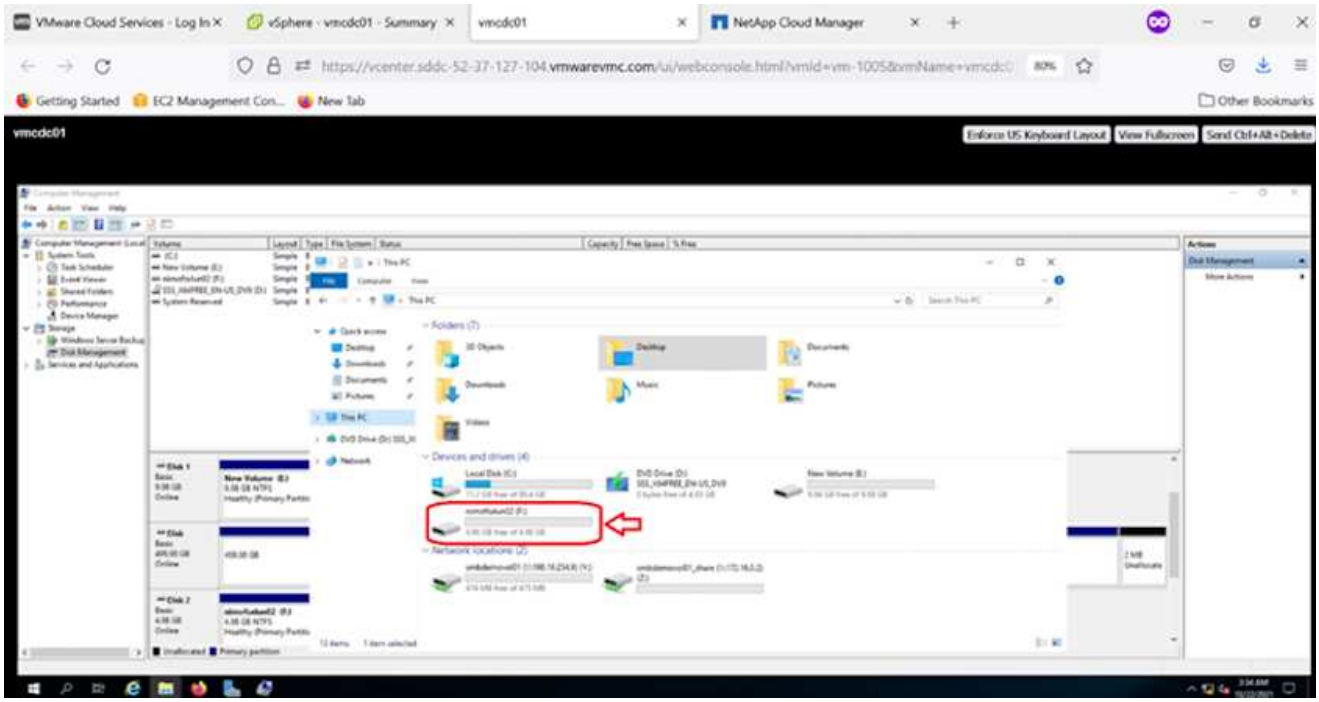
Die LUNs auf der Storage Virtual Machine (SVM) werden dem Windows Host als Festplatten angezeigt. Neue hinzugefügte Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen Rescan aus, um die Festplatten zu ermitteln, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie das Dienstprogramm Windows Computer Management: Start > Verwaltung > Computerverwaltung.
2. Erweitern Sie den Knoten Speicher in der Navigationsstruktur.
3. Klicken Sie Auf Datenträgerverwaltung.
4. Klicken Sie Auf Aktion > Datenträger Erneut Scannen.



Wenn der Windows-Host zum ersten Mal auf eine neue LUN zugreift, hat sie keine Partition oder kein Dateisystem. Initialisieren Sie die LUN und formatieren Sie optional die LUN mit einem Dateisystem, indem Sie die folgenden Schritte durchführen:

1. Starten Sie Windows Disk Management.
2. Klicken Sie mit der rechten Maustaste auf die LUN, und wählen Sie dann den erforderlichen Festplatten- oder Partitionstyp aus.
3. Befolgen Sie die Anweisungen im Assistenten. In diesem Beispiel ist Laufwerk F: Angehängt.



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenmanagement-Lösung auf Basis der Storage-Software ONTAP von NetApp. Sie ist nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar.

Es handelt sich um eine softwaredefinierte Version von ONTAP, die Cloud-nativen Storage nutzt, sodass Sie dieselbe Storage-Software in der Cloud und vor Ort nutzen können. Dadurch müssen SIE Ihre IT-Mitarbeiter nicht mehr in komplett neue Methoden zum Datenmanagement Schulen.

Mit CVO können Kunden Daten nahtlos vom Edge- zum Datacenter, zur Cloud und zurück verschieben und so Ihre Hybrid Cloud zusammen – all das wird über eine zentrale Managementkonsole, NetApp Cloud Manager, gemanagt.

CVO ist von Grund auf für beste Performance und erweiterte Datenmanagementfunktionen konzipiert, um auch die anspruchsvollsten Applikationen in der Cloud zu unterstützen

Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff

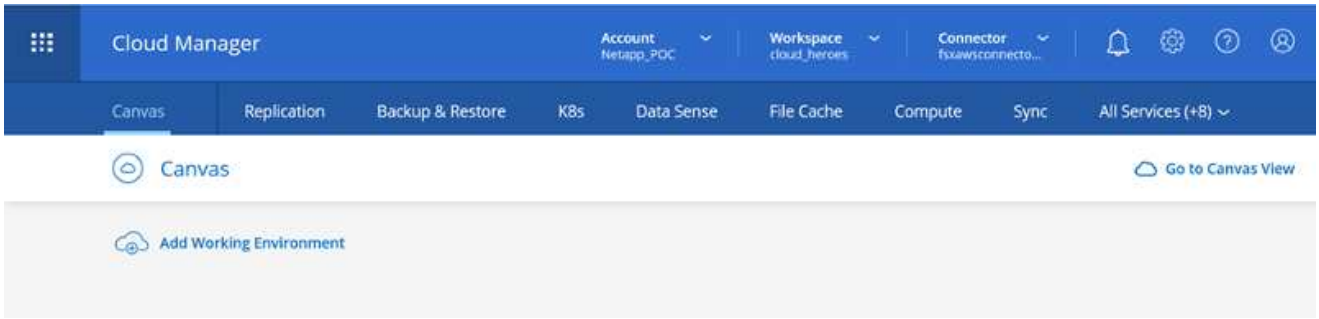
Neue Cloud Volumes ONTAP-Instanz in AWS implementieren (selbst übernehmen)

Cloud Volumes ONTAP-Freigaben und LUNs können von VMs gemountet werden, die in der VMware Cloud on AWS SDDC Umgebung erstellt wurden. Die Volumes können auch auf nativen AWS VM Linux Windows Clients eingebunden werden, und AUF LUNS kann bei Verwendung über iSCSI als Blockgeräte zugegriffen werden, da Cloud Volumes ONTAP iSCSI-, SMB- und NFS-Protokolle unterstützt. Cloud Volumes ONTAP Volumes lassen sich in wenigen einfachen Schritten einrichten.

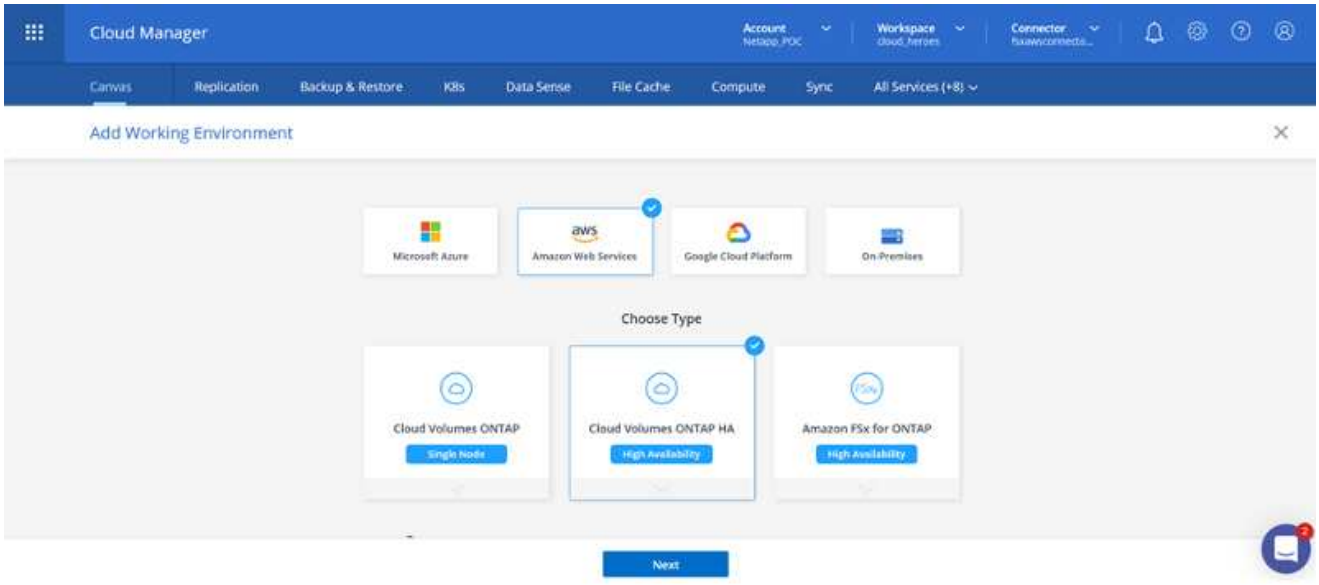
Um Volumes aus einer lokalen Umgebung für Disaster Recovery- oder Migrationszwecke in die Cloud zu replizieren, stellen Sie die Netzwerkverbindung zu AWS her, entweder über ein Site-to-Site-VPN oder DirectConnect. Die Replizierung von Daten zwischen On-Premises-Systemen und Cloud Volumes ONTAP ist im Rahmen dieses Dokuments nicht enthalten. Informationen zur Replizierung von Daten zwischen On-Premises- und Cloud Volumes ONTAP-Systemen finden Sie unter "Datenreplikation zwischen Systemen einrichten".

Verwenden Sie die "Cloud Volumes ONTAP-Dimensionierungstool" Und die präzise Größe der Cloud Volumes ONTAP-Instanzen. Überwachung der lokalen Performance als Eingänge im Cloud Volumes ONTAP Sizer

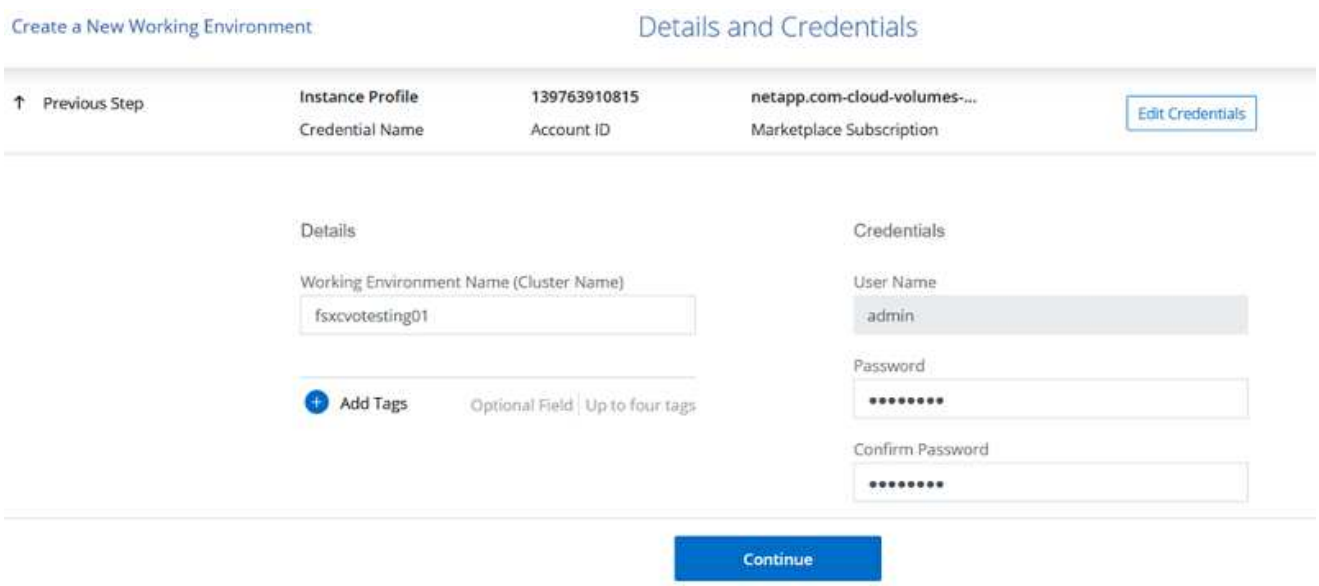
1. Melden Sie sich bei NetApp Cloud Central an. Der Bildschirm Fabric View wird angezeigt. Wählen Sie die Registerkarte Cloud Volumes ONTAP aus und wechseln Sie zu Cloud Manager. Nach der Anmeldung wird der Bildschirm Arbeitsfläche angezeigt.



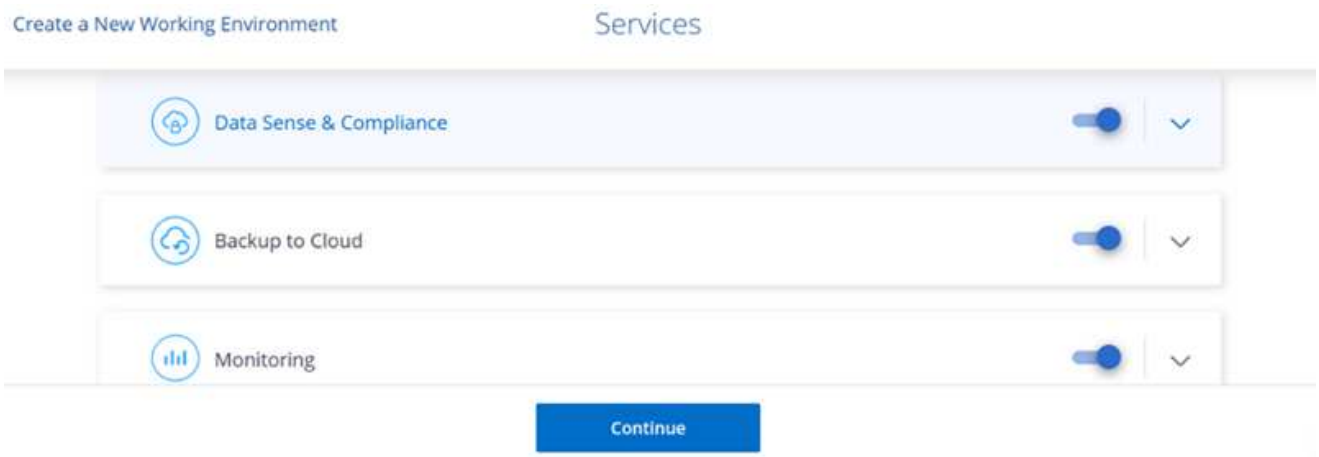
1. Klicken Sie auf der Cloud Manager-Startseite auf „Add a Working Environment“, und wählen Sie AWS als Cloud und den Typ der Systemkonfiguration aus.



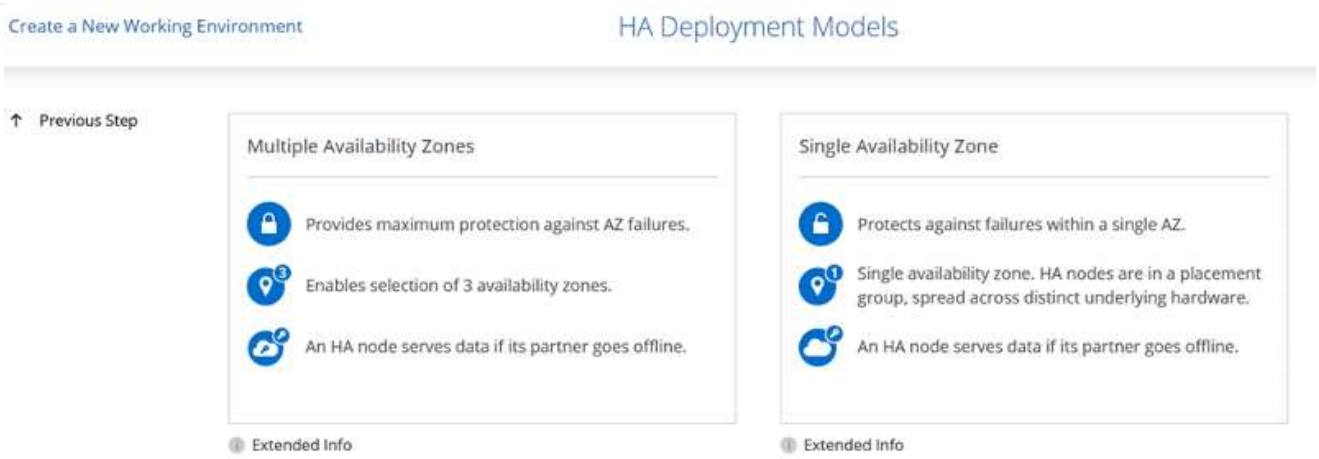
1. Geben Sie die Details zur zu erstellenden Umgebung an, einschließlich Name der Umgebung und Anmeldedaten des Administrators. Klicken Sie auf Weiter .



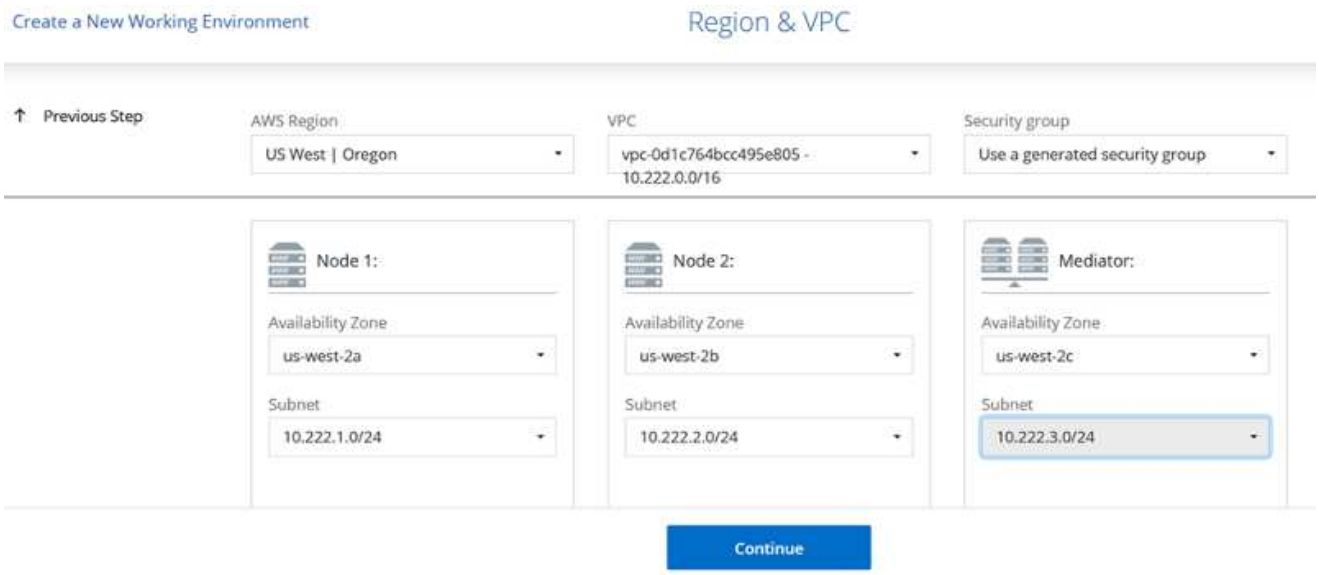
1. Wählen Sie die Add-on-Services für die Implementierung von Cloud Volumes ONTAP aus, darunter BlueXP Klassifizierung, BlueXP Backup und Recovery sowie Cloud Insights. Klicken Sie auf Weiter .



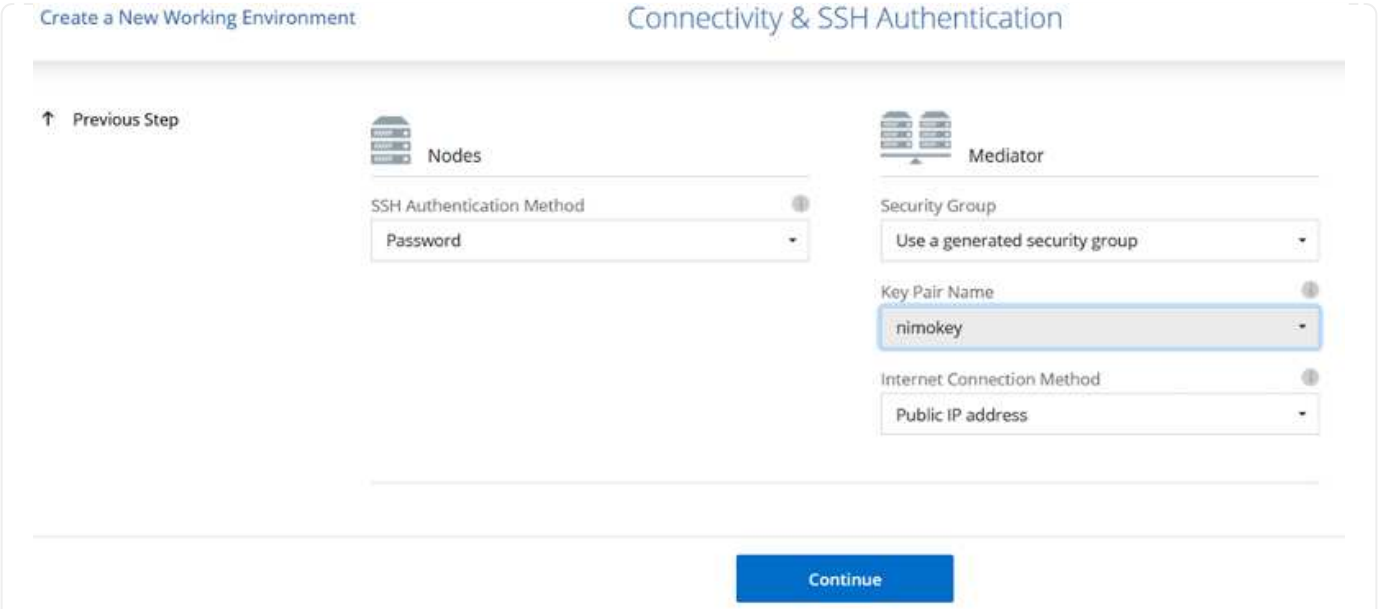
1. Wählen Sie auf der Seite HA-Bereitstellungsmodelle die Konfiguration mehrerer Verfügbarkeitszonen aus.



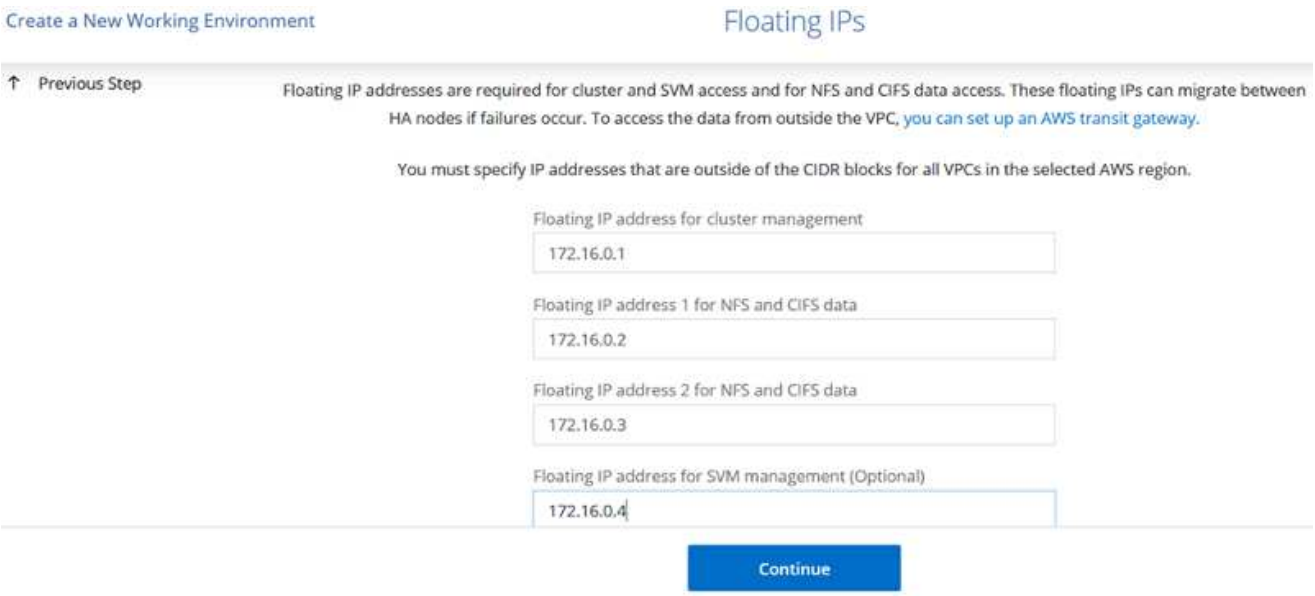
1. Geben Sie auf der Seite Region & VPC die Netzwerkinformationen ein, und klicken Sie dann auf Weiter.



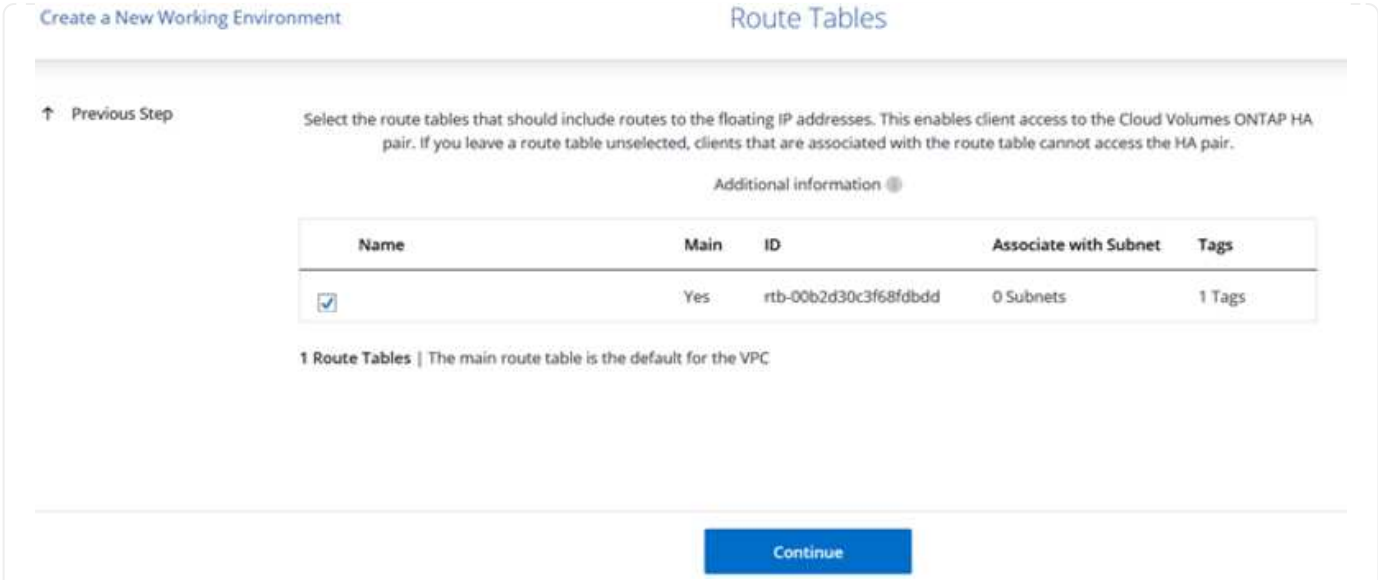
1. Wählen Sie auf der Seite Konnektivität und SSH-Authentifizierung Verbindungsmethoden für das HA-Paar und den Mediator aus.



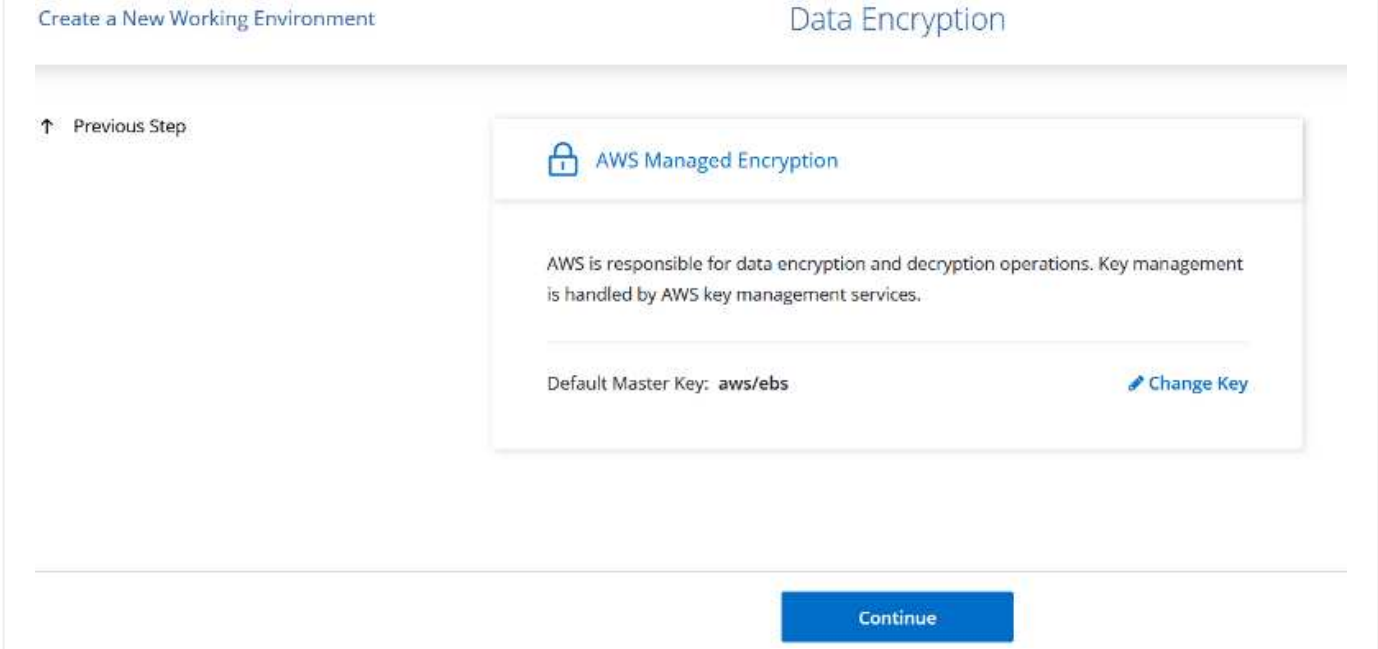
1. Geben Sie die unverankerten IP-Adressen an, und klicken Sie dann auf Weiter.



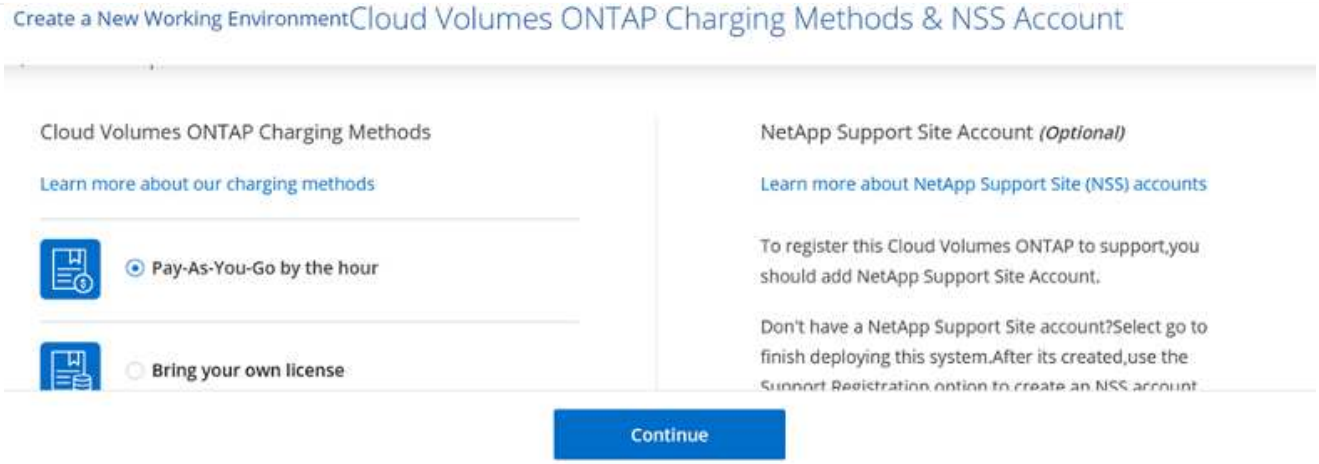
1. Wählen Sie die entsprechenden Routingtabellen aus, um Routen zu den unverankerten IP-Adressen einzuschließen, und klicken Sie dann auf Weiter.



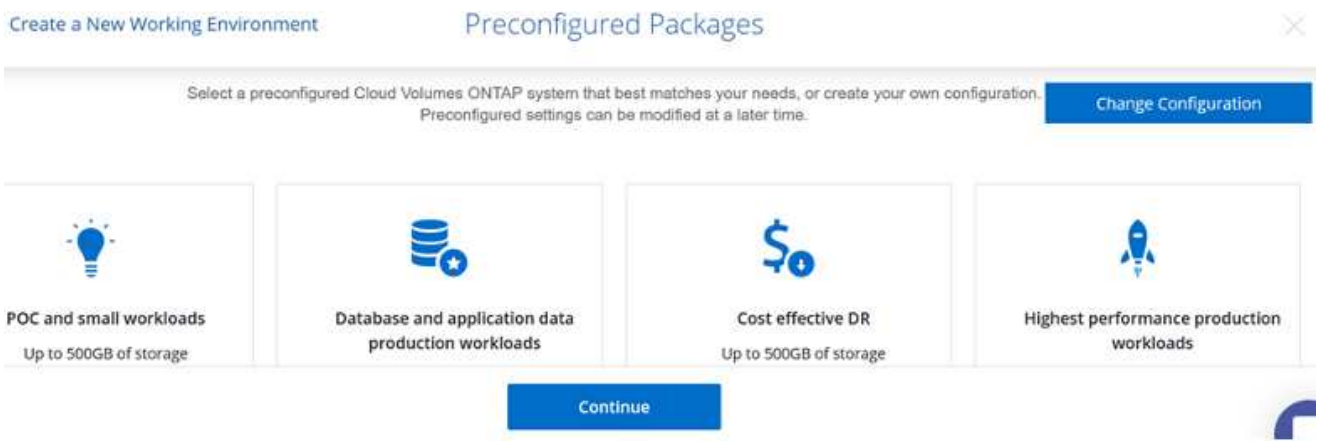
1. Wählen Sie auf der Seite Datenverschlüsselung die von AWS gemanagte Verschlüsselung aus.



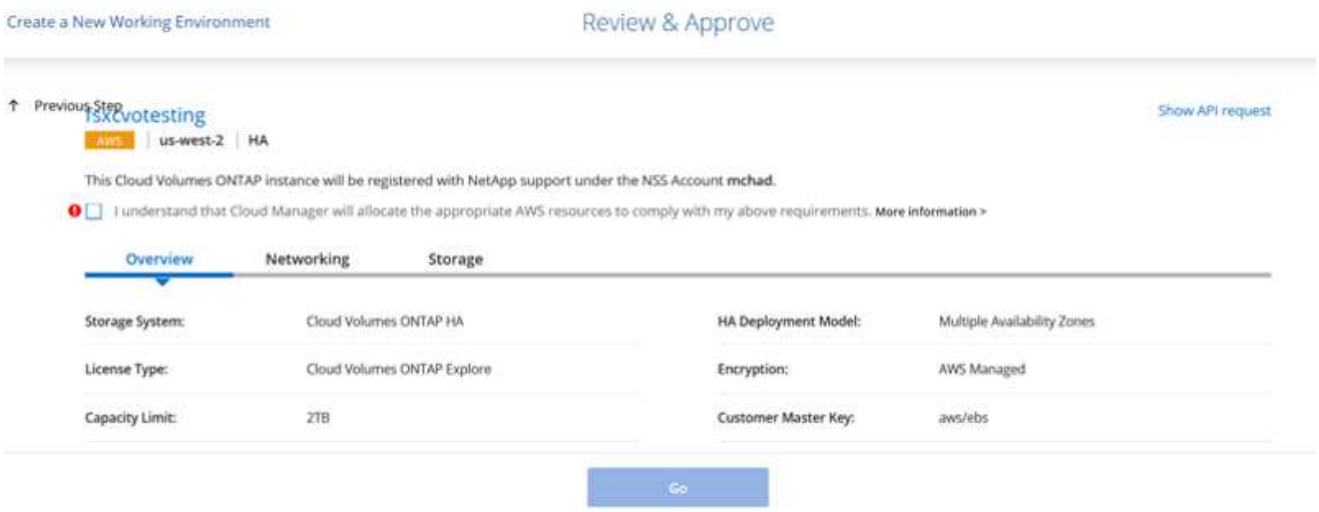
1. Wählen Sie die Lizenzoption: Pay-as-you-Go oder BYOL für die Nutzung einer vorhandenen Lizenz. In diesem Beispiel wird die Pay-as-you-Go-Option verwendet.



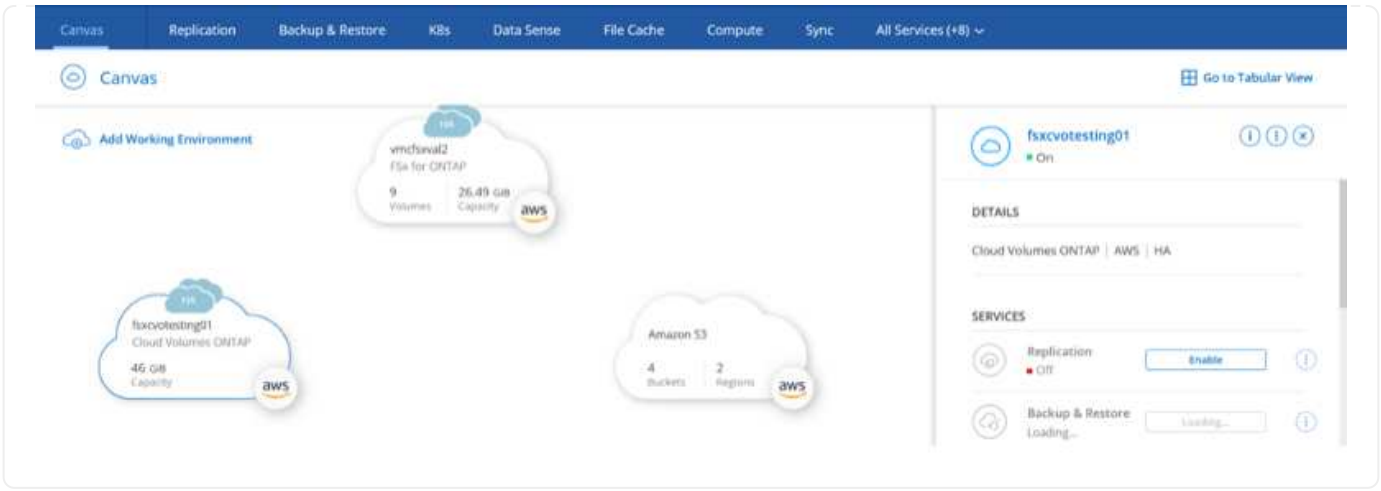
1. Wählen Sie zwischen mehreren vorkonfigurierten Paketen, die auf Grundlage des Workload-Typs verfügbar sind, die auf den VMs ausgeführt werden, die auf der VMware Cloud auf dem AWS SDDC ausgeführt werden.



1. Prüfen und bestätigen Sie die Auswahl auf der Seite Prüfen & Genehmigen.zum Erstellen der Cloud Volumes ONTAP-Instanz klicken Sie auf Los.

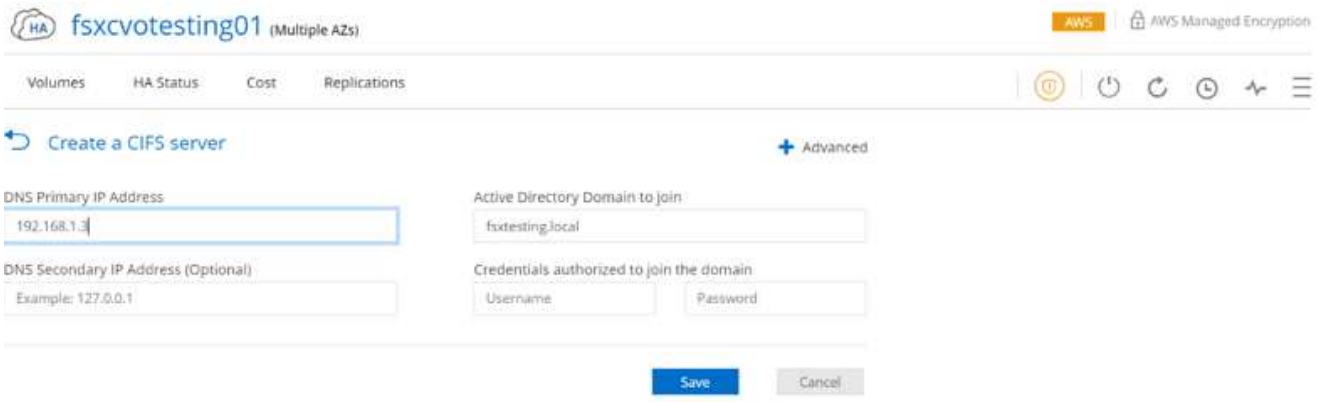


1. Nach der Bereitstellung von Cloud Volumes ONTAP wird es in den Arbeitsumgebungen auf der Seite Arbeitsfläche aufgelistet.

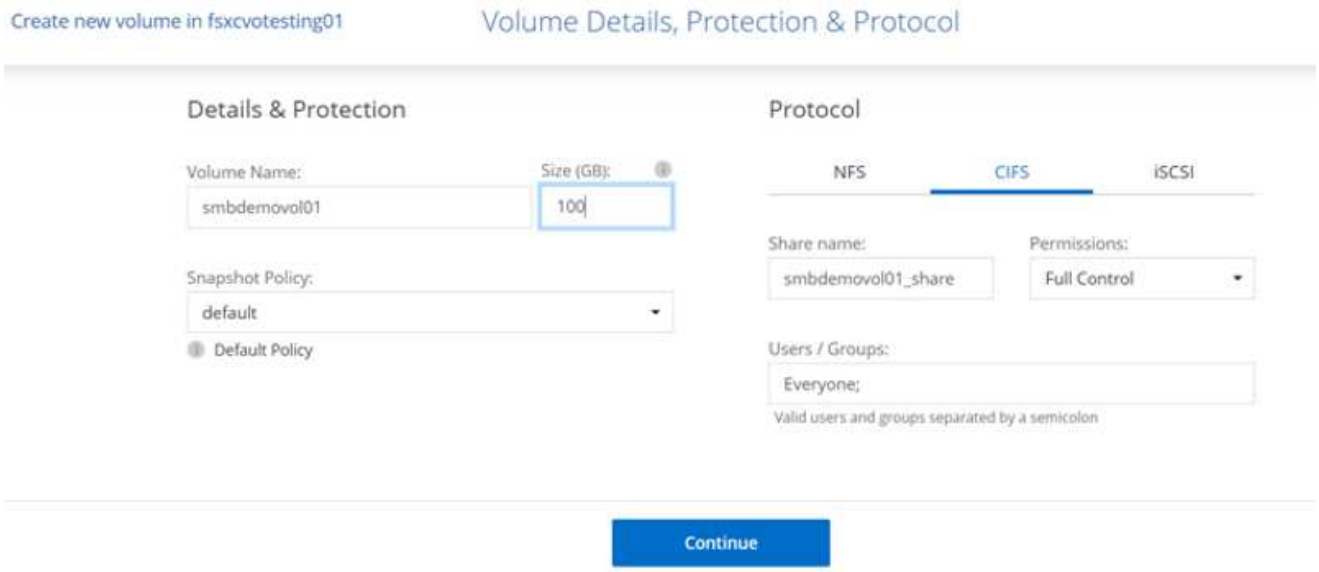

Canvas
Replication
Backup & Restore
K8s
Data Sense
File Cache
Compute
Sync
All Services (+8)
Canvas
Go to Tabular View
Add Working Environment
vmcfsaval2
FSx for ONTAP
9
Volumes
26.49 GiB
Capacity
fsxcvotesting01
Cloud Volumes ONTAP
46 GiB
Capacity
Amazon S3
4
Buckets
2
Regions
fsxcvotesting01
On
DETAILS
Cloud Volumes ONTAP | AWS | HA
SERVICES
Replication
Off
Enable
Backup & Restore
Loading...

Zusätzliche Konfigurationen für SMB Volumes

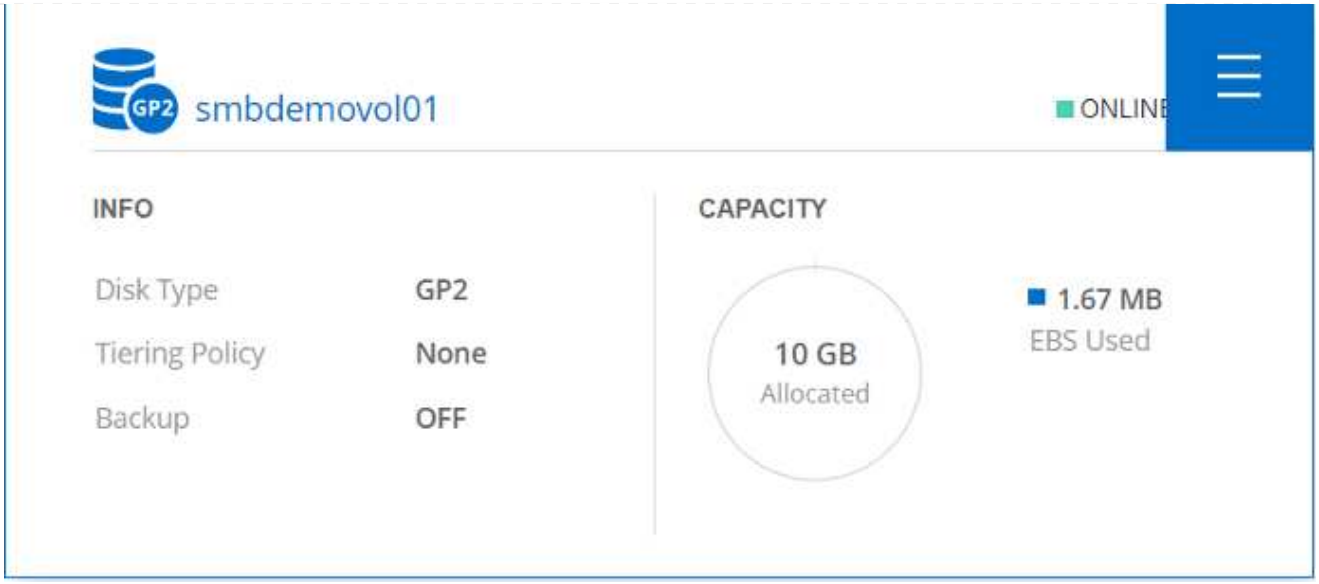
1. Stellen Sie nach der Arbeitsumgebung sicher, dass der CIFS-Server mit den entsprechenden DNS- und Active Directory-Konfigurationsparametern konfiguriert ist. Dieser Schritt ist erforderlich, bevor Sie das SMB-Volume erstellen können.



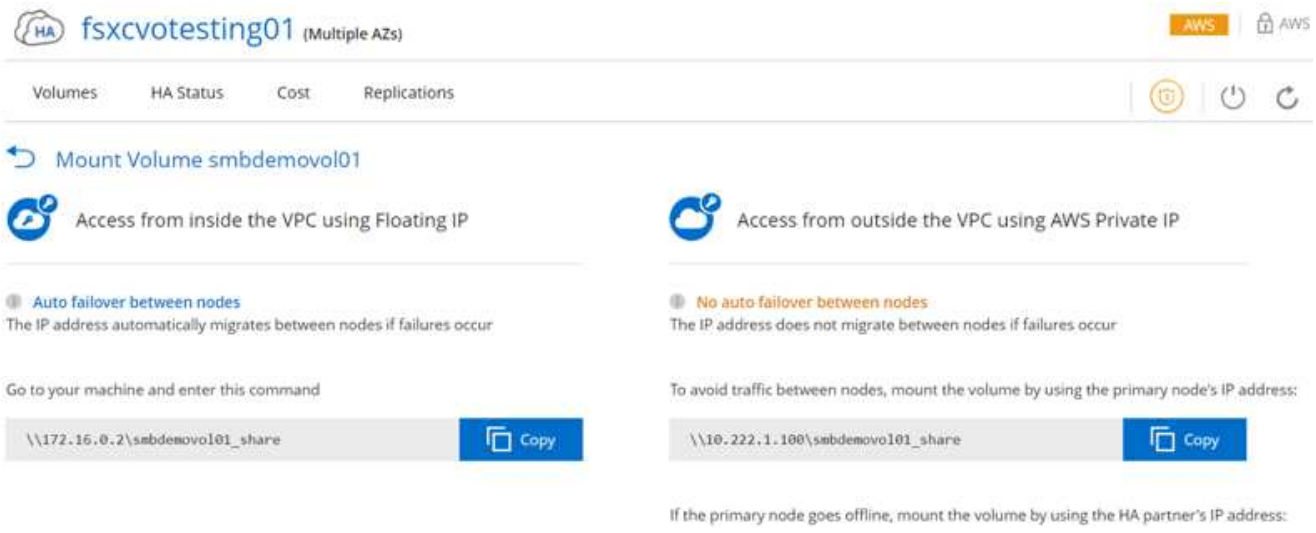
1. Wählen Sie die CVO-Instanz aus, um das Volume zu erstellen, und klicken Sie auf die Option Volume erstellen. Wählen Sie die entsprechende Größe und Cloud Manager wählt das Aggregat aus, das Sie enthalten, oder verwenden Sie den erweiterten Zuweisungsmechanismus auf einem bestimmten Aggregat. Für diese Demo wird SMB als Protokoll ausgewählt.

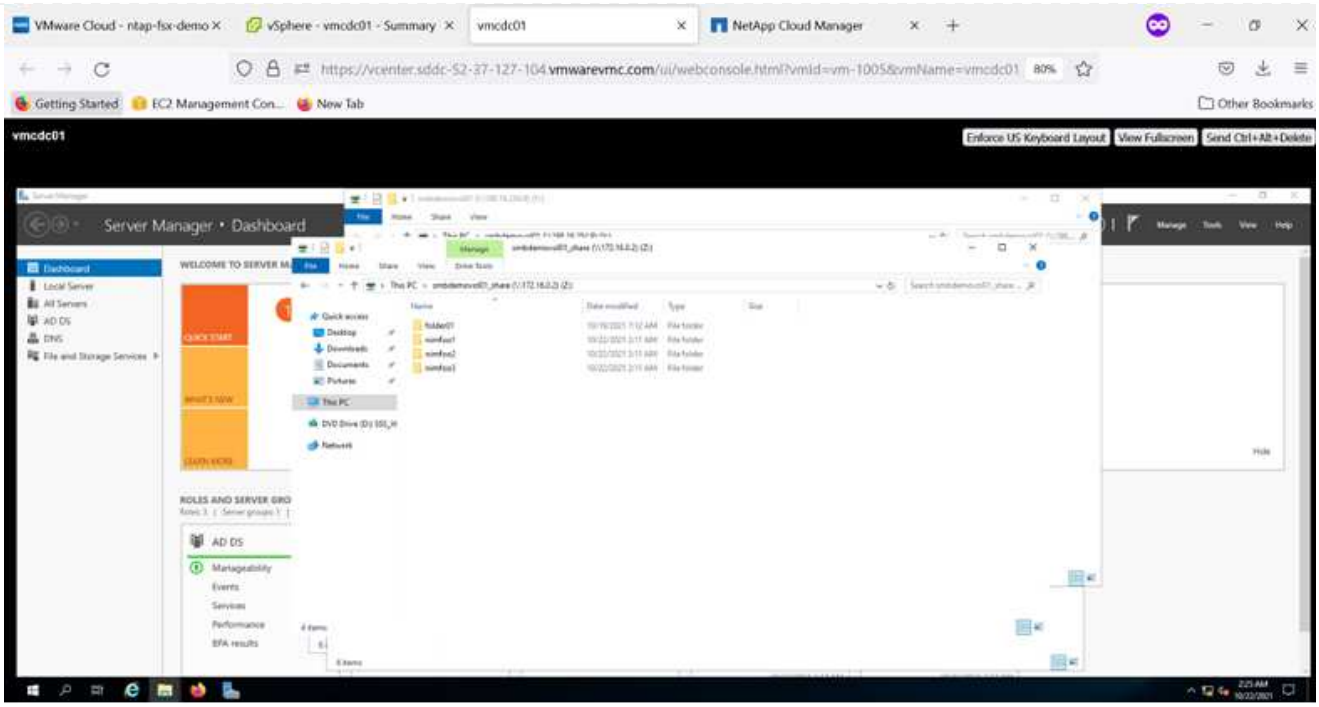


1. Nachdem das Volume bereitgestellt wurde, ist es unter dem Fensterbereich Volumes verfügbar. Da eine CIFS-Freigabe bereitgestellt wird, sollten Sie Ihren Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner gewähren und überprüfen, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.



1. Nachdem das Volume erstellt wurde, verwenden Sie den Mount-Befehl, um eine Verbindung zu dem Share von der VM herzustellen, die auf der VMware Cloud in AWS SDDC Hosts ausgeführt wird.
2. Kopieren Sie den folgenden Pfad und verwenden Sie die Option Netzwerklaufwerk zuordnen, um das Volume auf der VM zu mounten, die auf der VMware Cloud in AWS SDDC ausgeführt wird.

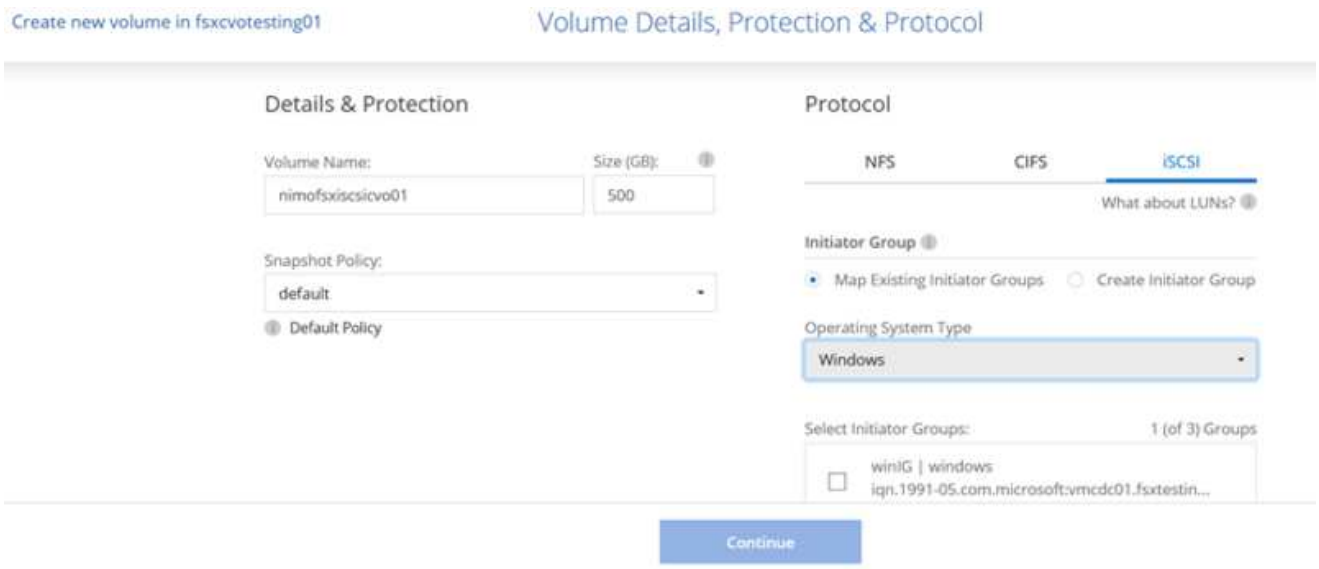


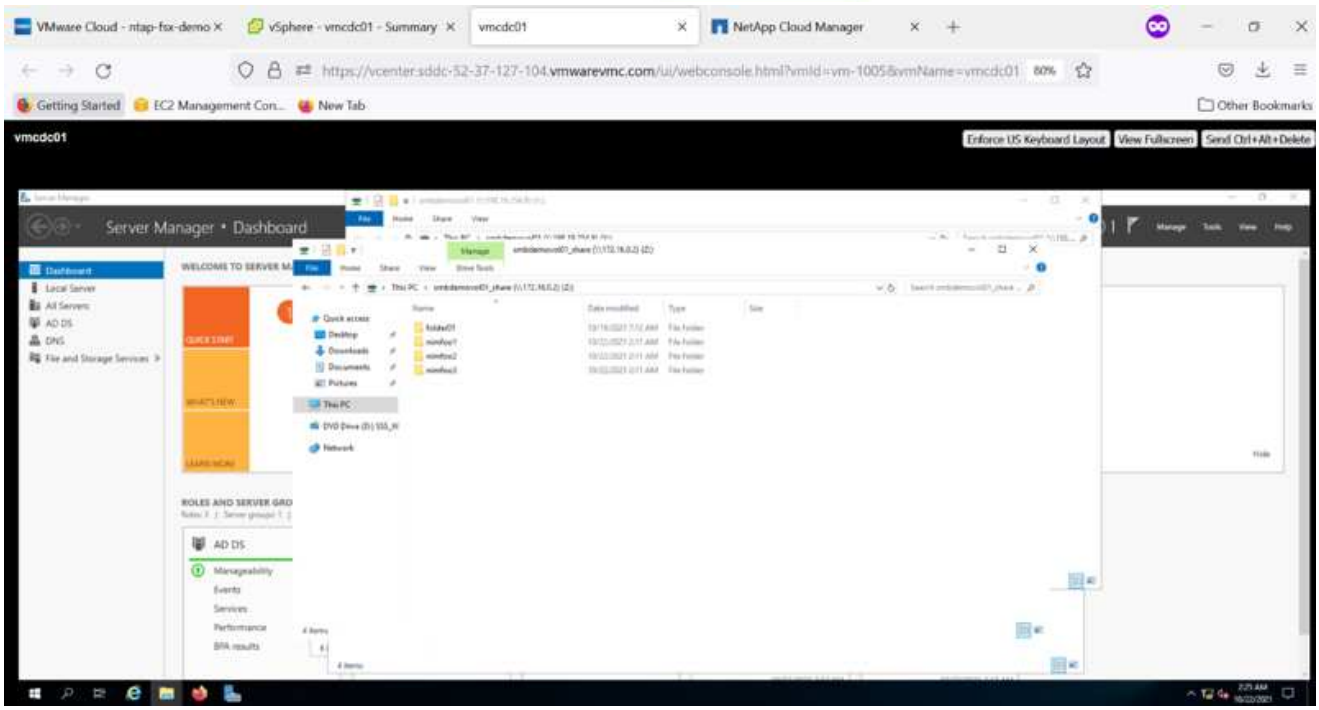

VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager • Dashboard

Verbinden Sie die LUN mit einem Host

Führen Sie die folgenden Schritte aus, um die Cloud Volumes ONTAP-LUN mit einem Host zu verbinden:

1. Doppelklicken Sie auf der Seite „Cloud Manager“ auf die Arbeitsumgebung von Cloud Volumes ONTAP, um Volumes zu erstellen und zu verwalten.
2. Klicken Sie auf Volume hinzufügen > Neues Volume, wählen Sie iSCSI aus und klicken Sie auf Initiatorgruppe erstellen. Klicken Sie auf Weiter .





1. Wählen Sie nach der Bereitstellung des Volumes das Volume aus, und klicken Sie dann auf Ziel-IQN. Um den iSCSI-qualifizierten Namen (IQN) zu kopieren, klicken Sie auf Kopieren. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.

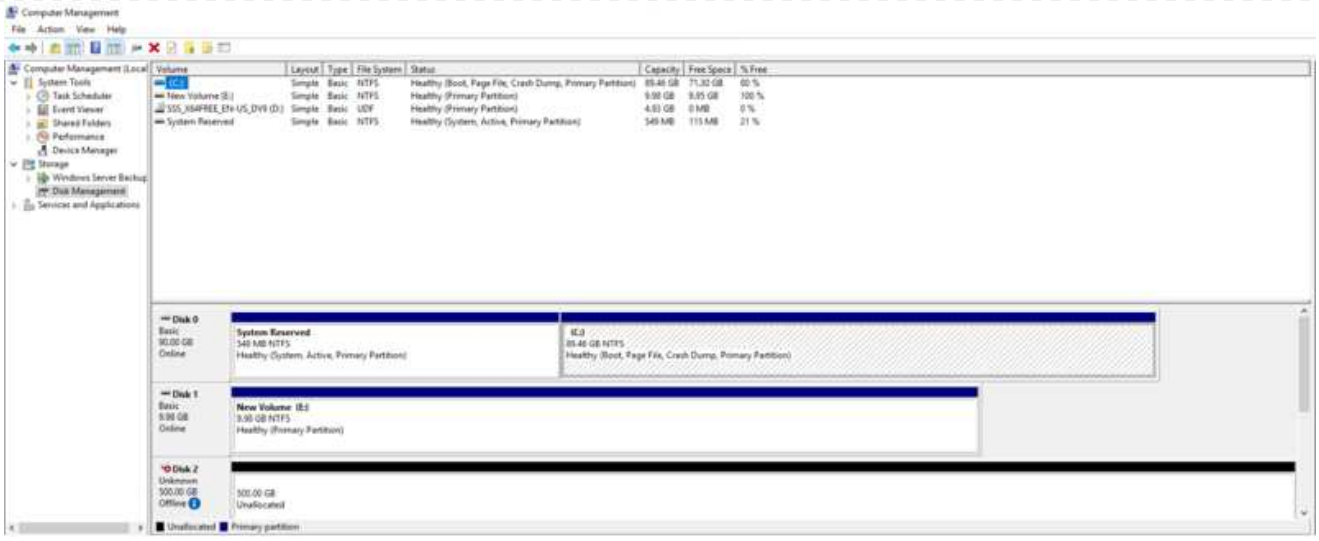
Um dies für den Host zu erreichen, der sich auf VMware Cloud auf AWS SDDC befindet, gehen Sie wie folgt vor:

1. RDP auf die VM, die auf VMware Cloud auf AWS gehostet wird.
2. Öffnen Sie das Dialogfeld iSCSI-Initiator-Eigenschaften: Server Manager > Dashboard > Tools > iSCSI-Initiator.
3. Klicken Sie auf der Registerkarte Ermittlung auf Portal erkennen oder Portal hinzufügen, und geben Sie dann die IP-Adresse des iSCSI-Zielports ein.
4. Wählen Sie auf der Registerkarte Ziele das erkannte Ziel aus und klicken Sie dann auf Anmelden oder Verbinden.
5. Wählen Sie Multipath aktivieren, und wählen Sie dann automatisch Diese Verbindung wiederherstellen, wenn der Computer startet oder Diese Verbindung zur Liste der bevorzugten Ziele hinzufügen. Klicken Sie Auf Erweitert.

Der Windows-Host muss über eine iSCSI-Verbindung zu jedem Knoten im Cluster verfügen. Das native DSM wählt die besten Pfade aus.

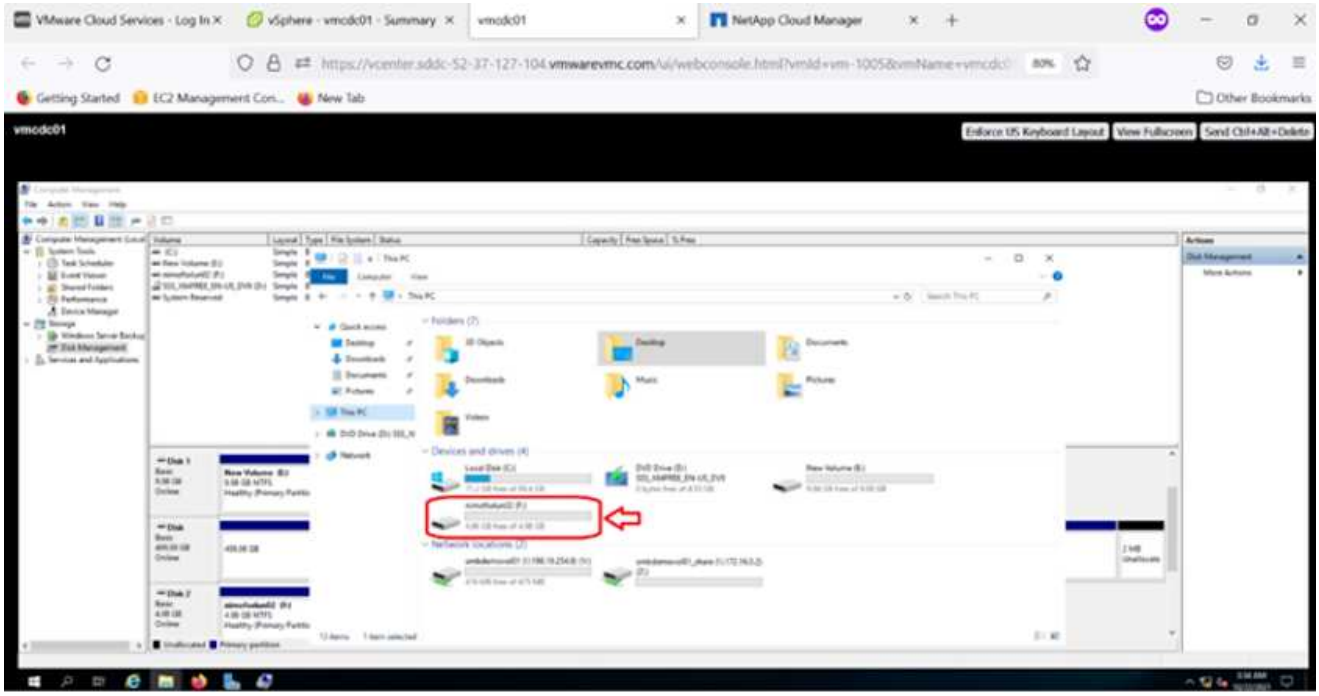
LUNs aus der SVM werden dem Windows-Host als Festplatten angezeigt. Neue hinzugefügte Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen Rescan aus, um die Festplatten zu ermitteln, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie das Dienstprogramm Windows Computer Management: Start > Verwaltung > Computerverwaltung.
2. Erweitern Sie den Knoten Speicher in der Navigationsstruktur.
3. Klicken Sie Auf Datenträgerverwaltung.
4. Klicken Sie Auf Aktion > Datenträger Erneut Scannen.



Wenn der Windows-Host zum ersten Mal auf eine neue LUN zugreift, hat sie keine Partition oder kein Dateisystem. Initialisieren Sie die LUN; und optional formatieren Sie die LUN mit einem Dateisystem, indem Sie die folgenden Schritte durchführen:

1. Starten Sie Windows Disk Management.
2. Klicken Sie mit der rechten Maustaste auf die LUN, und wählen Sie dann den erforderlichen Festplatten- oder Partitionstyp aus.
3. Befolgen Sie die Anweisungen im Assistenten. In diesem Beispiel ist Laufwerk F: Angehängt.



Stellen Sie auf den Linux-Clients sicher, dass der iSCSI-Daemon ausgeführt wird. Nachdem die LUNs bereitgestellt wurden, lesen Sie die detaillierte Anleitung zur iSCSI-Konfiguration für Ihre Linux-Distribution. Beispielsweise kann Ubuntu iSCSI-Konfiguration gefunden werden "Hier". Führen Sie zur Überprüfung lsblk cmd aus der Shell aus.

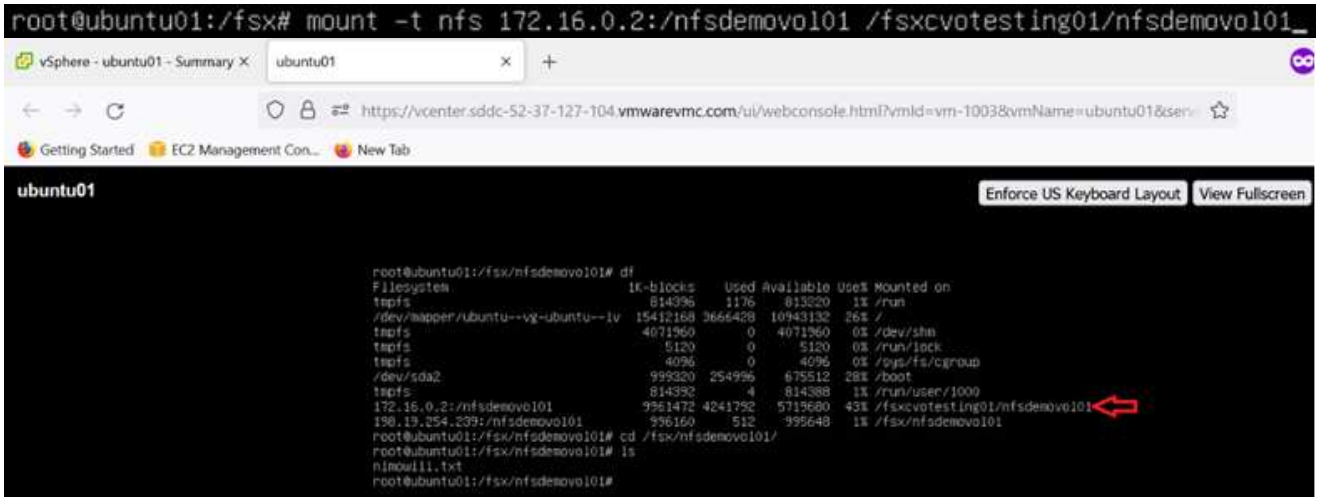
Mounten Sie das Cloud Volumes ONTAP NFS Volume auf dem Linux Client

So mounten Sie das Cloud Volumes ONTAP (DIY) Dateisystem von VMs innerhalb VMC auf AWS SDDC aus:

1. Stellen Sie eine Verbindung mit der angegebenen Linux-Instanz her.
2. Öffnen Sie ein Terminal auf der Instanz mithilfe von Secure Shell (SSH), und melden Sie sich mit den entsprechenden Anmeldedaten an.
3. Erstellen Sie mit dem folgenden Befehl ein Verzeichnis für den Mount-Punkt des Volumes.

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. Mounten Sie das Amazon FSX für NetApp ONTAP NFS Volume in das
Verzeichnis, das im vorherigen Schritt erstellt wurde.
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```



Überblick über ANF Datastore Solutions

Alle erfolgreichen Unternehmen befinden sich auf dem Weg der Transformation und Modernisierung. In diesem Prozess verwenden Unternehmen in der Regel ihre vorhandenen VMware-Investitionen, während sie gleichzeitig die Vorteile der Cloud nutzen und untersuchen, wie sich Migrations-, Burst-, Extend- und Disaster Recovery-Prozesse so nahtlos wie möglich gestalten lassen. Kunden, die zur Cloud migrieren, müssen die Aspekte Flexibilität und Burst, Datacenter-Ausstieg, Datacenter-Konsolidierung, End-of-Life-Szenarien, Fusionen, Übernahmen usw. bewerten. Der von den einzelnen Unternehmen angenommene Ansatz kann je nach Geschäftsprioritäten variieren. Bei der Auswahl der Cloud-basierten Prozesse ist die Auswahl eines kostengünstigen Modells mit angemessener Performance und minimaler Behinderung ein entscheidendes Ziel. Dabei ist es besonders wichtig, dass Sie die richtige Plattform

auswählen, sowie die Storage- und Workflow-Orchestrierung, um das Potenzial der Cloud-Implementierung und -Flexibilität auszuschöpfen.

Anwendungsfälle

Obwohl die Azure VMware Lösung Kunden einzigartige Hybrid-Funktionen bietet, haben begrenzte native Storage-Optionen jedoch ihre Nützlichkeit in Unternehmen mit speicherlastigen Workloads eingeschränkt. Da Storage direkt an Hosts gebunden ist, besteht die einzige Möglichkeit zur Skalierung des Storage darin, weitere Hosts hinzuzufügen. Dadurch lassen sich die Kosten bei Storage-intensiven Workloads um 35 bis 40 % oder mehr senken. Diese Workloads erfordern zusätzlichen Storage und keine zusätzliche Leistung, sondern die Kosten für zusätzliche Hosts.

Betrachten wir einmal das folgende Szenario: Ein Kunde benötigt sechs Hosts für mehr Performance (vCPU/Vmem), hat aber auch einen erheblichen Storage-Bedarf. Basierend auf ihrem Assessment benötigen sie 12 Hosts, um die Storage-Anforderungen zu erfüllen. Dies erhöht die Gesamtbetriebskosten, da diese zusätzliche Leistung anschaffen müssen, wenn überhaupt mehr Storage benötigt wird. Dies gilt für alle Anwendungsfälle, einschließlich Migration, Disaster Recovery, Bursting, Entwicklung/Test, Und so weiter.

Ein weiterer häufiger Anwendungsfall für Azure VMware Lösung ist Disaster Recovery (DR). Die meisten Unternehmen verfügen nicht über eine zukunftssichere DR-Strategie. Oder sie tun sich schwer damit, einen Geist nur für DR zu rechtfertigen. Administratoren prüfen möglicherweise in Verbindung mit einem Pilot-Light-Cluster oder On-Demand-Cluster DR-Optionen, die für keinerlei Stellfläche benötigen. Anschließend konnte der Storage ohne zusätzliche Hosts skaliert werden, was potenziell eine attraktive Option wäre.

Zusammengefasst können die Anwendungsfälle auf zwei Arten klassifiziert werden:

- Skalierung der Storage-Kapazität mithilfe von ANF Datastores
- Nutzung von ANF-Datastores als Disaster-Recovery-Ziel für einen kostenoptimierten Recovery-Workflow von lokalen oder Azure-Regionen zwischen den softwaredefinierten Datacentern (SDDC).dieser Leitfaden bietet Einblicke in die Verwendung von Azure NetApp Files für die Bereitstellung von optimiertem Storage für Datastores (derzeit in öffentlicher Vorschau). Neben erstklassigen Datensicherungs- und DR-Funktionen in einer Azure VMware Lösung können Sie Storage-Kapazität von vSAN Storage verlagern.

Weitere Informationen zur Verwendung von ANF-Datastores erhalten Sie bei NetApp oder Microsoft Solution Architects in Ihrer Region.

VMware Cloud Optionen in Azure

Azure VMware Lösung

Die Azure VMware Lösung (AVS) ist ein Hybrid-Cloud-Service, der VMware Datacenters in einer Public Cloud von Microsoft Azure vollständig nutzt. AVS ist eine Lösung eines Erstanbieters, die vollständig von Microsoft verwaltet und unterstützt wird und von VMware überprüft wurde, die eine Azure-Infrastruktur nutzt. Kunden entscheiden sich daher für VMware ESXi für Computing-Virtualisierung, vSAN für hyperkonvergenten Storage und NSX für Netzwerk und Sicherheit. Sie profitieren gleichzeitig von der globalen Präsenz von Microsoft Azure, den erstklassigen Datacenter-Einrichtungen und der Nähe zum umfassenden Ecosystem aus nativen Azure Services und Lösungen. Eine Kombination aus Azure VMware Solution SDDC und Azure NetApp Files bietet die beste Performance bei minimaler Netzwerklatenz.

Unabhängig vom verwendeten Cloud-Einsatz umfasst der anfängliche Cluster bei der Implementierung eines VMware SDDC die folgenden Komponenten:

- VMware ESXi Hosts für die Computing-Virtualisierung mit einer vCenter Server Appliance zum

Management

- VMware vSAN hyperkonvergenter Storage mit den physischen Storage-Ressourcen des jeweiligen ESXi Hosts.
- VMware NSX für virtuelles Networking und Sicherheit mit einem NSX Manager Cluster für Management.

Schlussfolgerung

Egal, ob Sie auf eine All-Cloud oder eine Hybrid Cloud abzielen – Azure NetApp Files bietet exzellente Optionen zur Implementierung und zum Management von Applikations-Workloads zusammen mit Fileservices und senkt gleichzeitig die TCO, da die Datenanforderungen nahtlos auf die Applikationsebene integriert werden. Wie auch immer der Anwendungsfall ist: Wählen Sie die Azure VMware Lösung zusammen mit Azure NetApp Files, um Cloud-Vorteile schnell zu realisieren, eine konsistente Infrastruktur und Abläufe vor Ort und in mehreren Clouds, bidirektionale Workload-Portabilität und Kapazität und Performance der Enterprise-Klasse. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, mit denen der Speicher verbunden wird. Denken Sie daran: Es ist nur die Position der geänderten Daten, die Tools und Prozesse bleiben dieselben, und Azure NetApp Files hilft bei der Optimierung der generellen Implementierung.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können Azure NetApp Files nun als Datastore auf dem AVS SDDC verwenden.
- Kürzere Reaktionszeiten von Applikationen und höhere Verfügbarkeit für den Zugriff auf Workload-Daten nach Bedarf
- Mit einfachen und sofortigen Funktionen zur Anpassung vereinfachen Sie die allgemeine Komplexität des vSAN-Storage.
- Garantierte Performance für geschäftskritische Workloads durch dynamische Umformungsfunktionen
- Wenn Azure VMware Solution Cloud Ziel ist, ist Azure NetApp Files die richtige Storage-Lösung für eine optimierte Implementierung.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie unter den folgenden Links:

- Dokumentation der Azure VMware Lösung

  "https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files-Dokumentation

  "https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- Azure NetApp Files-Datenspeicher an Hosts der Azure VMware Lösung anhängen (Vorschau)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

NetApp Guest Connected Storage Optionen für Azure

Azure unterstützt NetApp Storage mit Anbindung an den Gast-Storage über den nativen Azure NetApp Files-Service (ANF) oder über Cloud Volumes ONTAP (CVO).

Azure NetApp Dateien (ANF)

Azure NetApp Files ermöglicht Datenmanagement und Storage der Enterprise-Klasse in Azure, damit Sie Ihre Workloads und Applikationen komfortabel managen. Migrieren Sie Ihre Workloads in die Cloud und führen Sie sie ohne Performance-Einbußen aus.

Azure NetApp Files beseitigt Hindernisse, damit Sie alle dateibasierten Applikationen in die Cloud verschieben können. Zum ersten Mal müssen Sie Ihre Applikationen nicht umstrukturieren und Sie erhalten persistenten Storage für Ihre Applikationen ohne Komplexität.

Da der Service über das Microsoft Azure-Portal bereitgestellt wird, erhalten Benutzer einen vollständig gemanagten verwalteten Service als Teil ihres Microsoft Enterprise Agreements. Der von Microsoft gemanagte erstklassige Support nimmt Ihnen alle Sorgen. Durch diese einfache Lösung fügen Sie Multiprotokoll-Workloads mit Leichtigkeit schnell hinzu. Dateibasierte Applikationen für Windows und auch für Linux – sogar Applikationen für Legacy-Umgebungen – lassen sich erstellen und implementieren.

Azure NetApp Files (ANF) als Storage mit Gastverbunden

Konfiguration von Azure NetApp Files mit Azure VMware Lösung (AVS)

Azure NetApp Files Shares können von VMs gemountet werden, die in der SDDC Umgebung der Azure VMware Lösung erstellt wurden. Die Volumes können auch auf dem Linux-Client eingebunden und auf dem Windows-Client zugeordnet werden, da Azure NetApp Files SMB- und NFS-Protokolle unterstützt. Azure NetApp Files Volumes lassen sich in fünf einfachen Schritten einrichten.

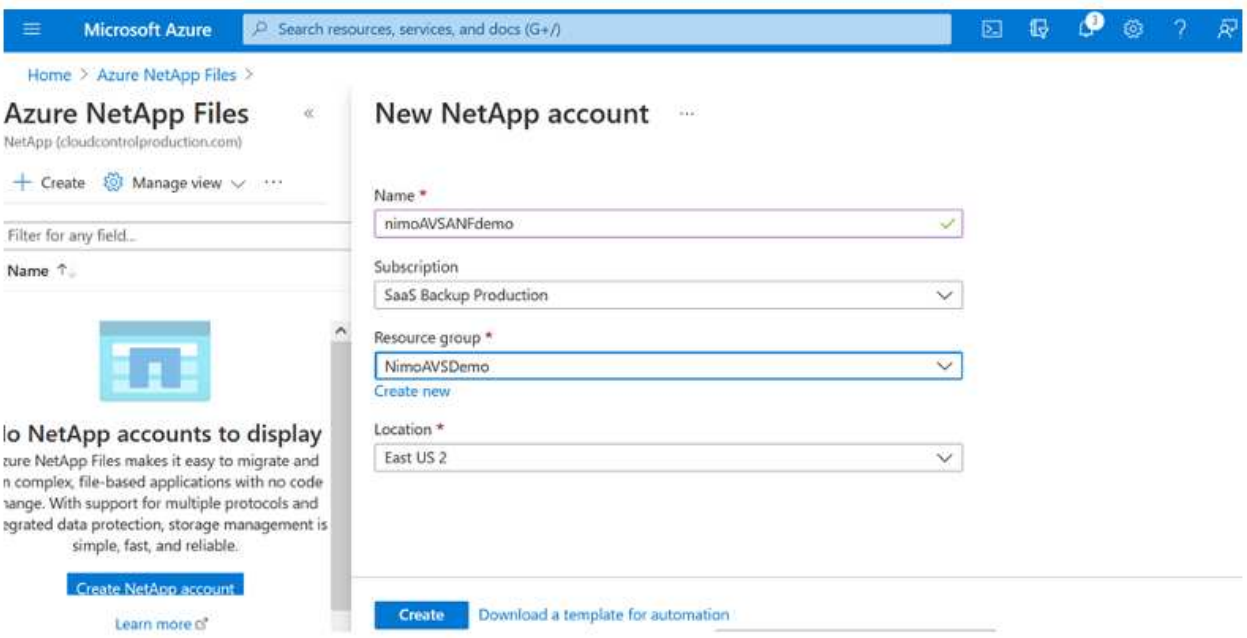
Azure NetApp Files und Azure VMware müssen sich in derselben Azure Region befinden.

Azure NetApp Files Volumes erstellen und mounten

Führen Sie folgende Schritte aus, um Azure NetApp Files Volumes zu erstellen und zu mounten:

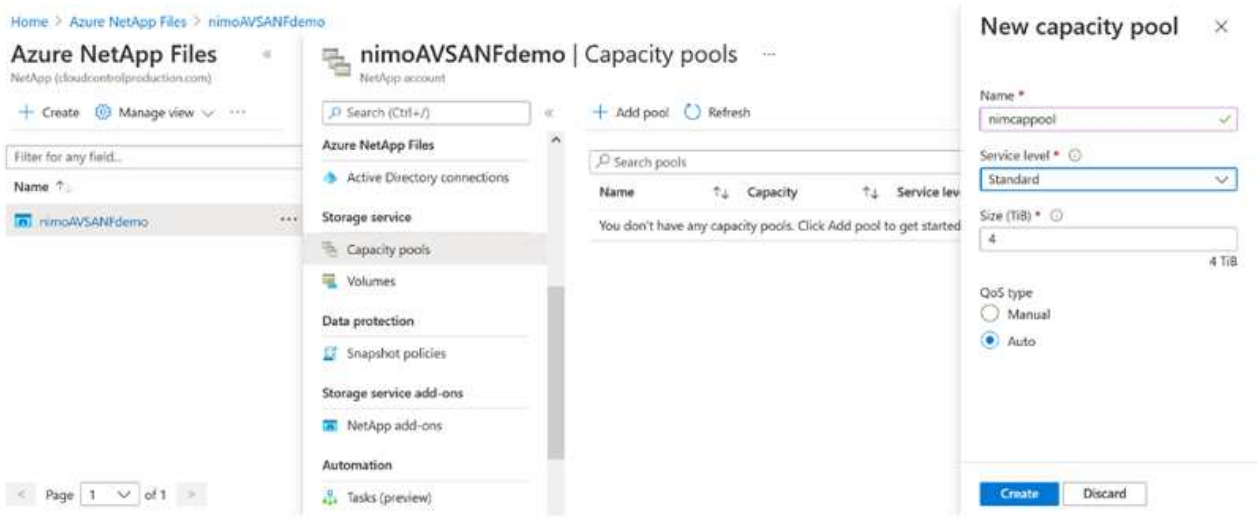
1. Melden Sie sich im Azure Portal an und greifen Sie auf Azure NetApp Files zu. Überprüfen Sie den Zugriff auf den Azure NetApp Files-Dienst und registrieren Sie den Azure NetApp Files-Ressourcenanbieter mit dem Befehl *az Provider Register --Namespace Microsoft.NetApp –wait*. Nach Abschluss der Registrierung erstellen Sie einen NetApp Account.

   Ausführliche Schritte finden Sie unter "Azure NetApp Files-Freigaben". Auf dieser Seite finden Sie einen Schritt-für-Schritt-Prozess.

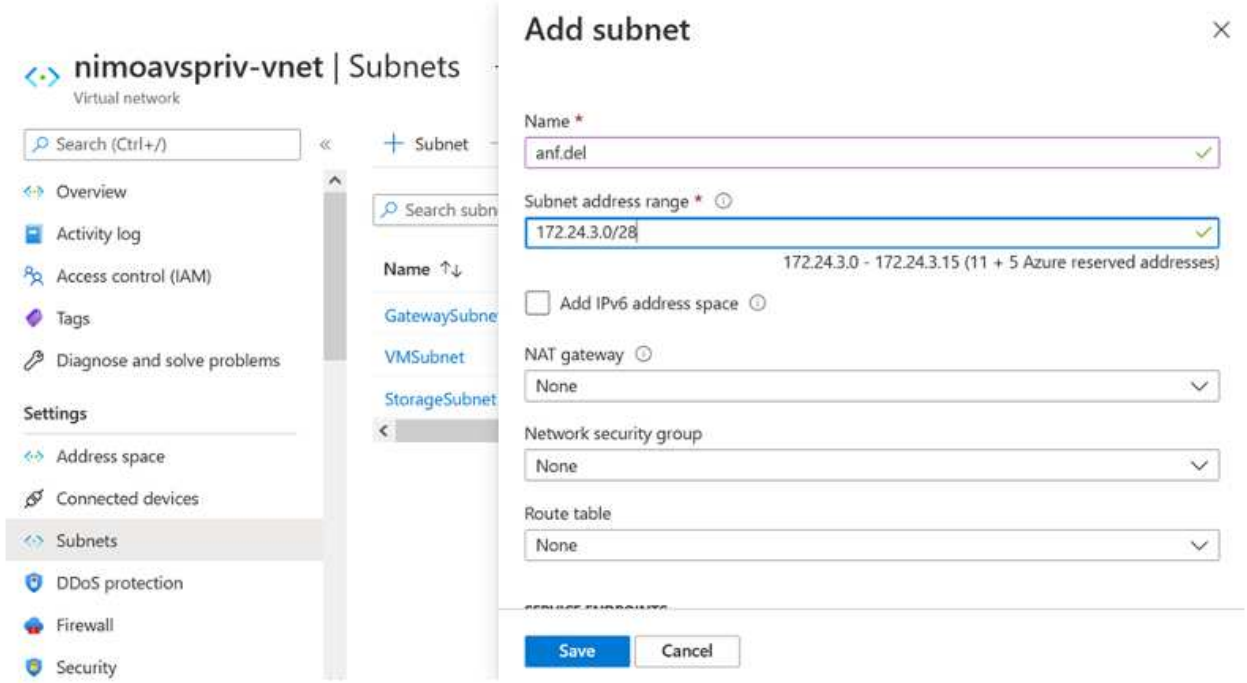


2. Nach der Erstellung des NetApp Accounts werden die Kapazitäts-Pools mit dem erforderlichen Service Level und der erforderlichen Größe eingerichtet.

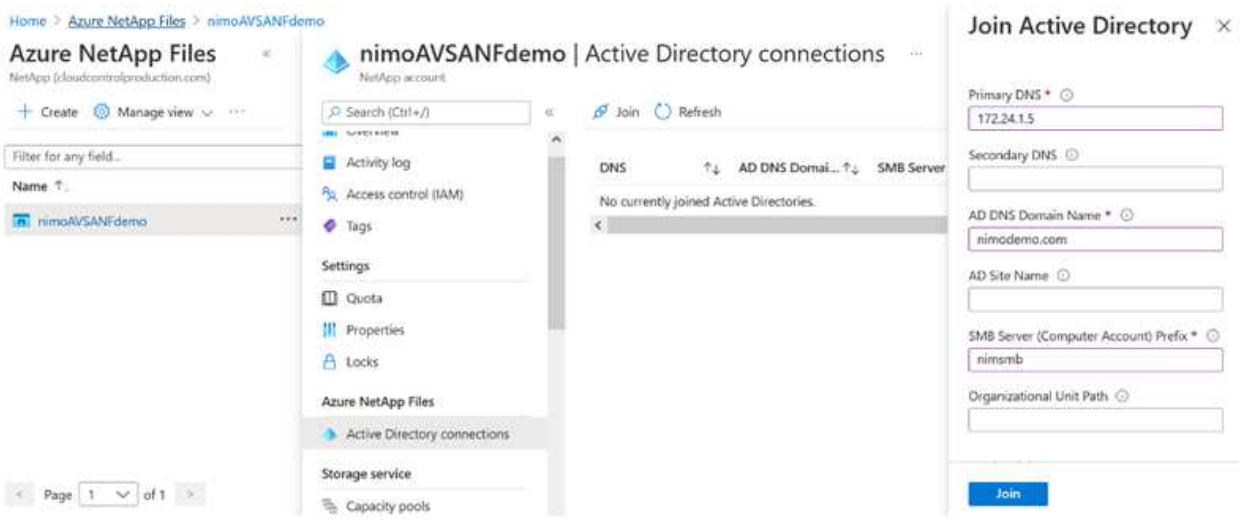
   Weitere Informationen finden Sie unter "Richten Sie einen Kapazitäts-Pool ein".



3. Konfigurieren Sie das delegierte Subnetz für Azure NetApp Files, und geben Sie dieses Subnetz an, während Sie die Volumes erstellen. Detaillierte Schritte zum Erstellen eines delegierten Subnetzes finden Sie unter "Delegieren eines Subnetzes an Azure NetApp Files".

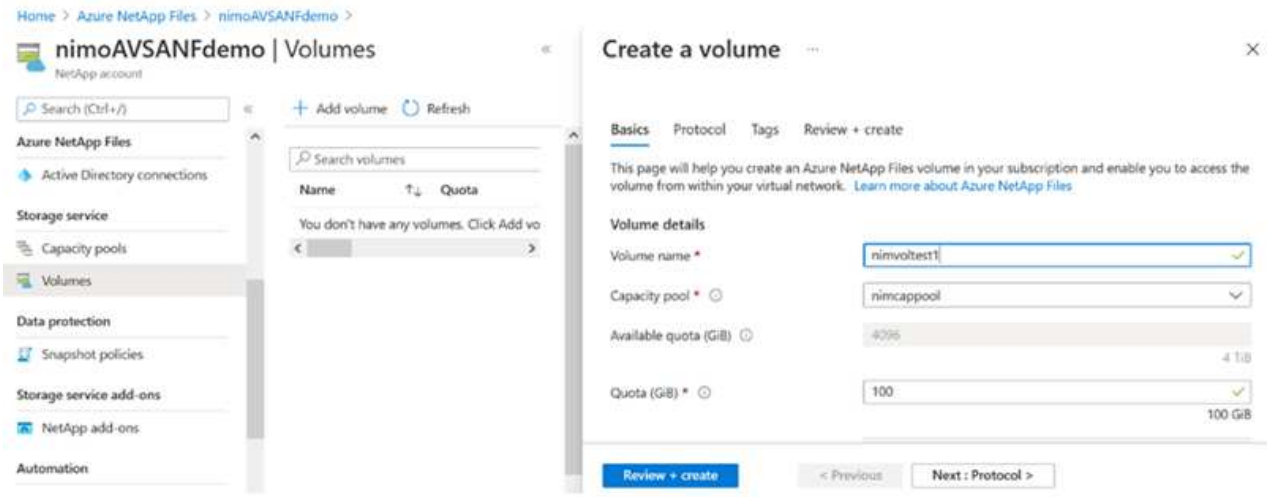


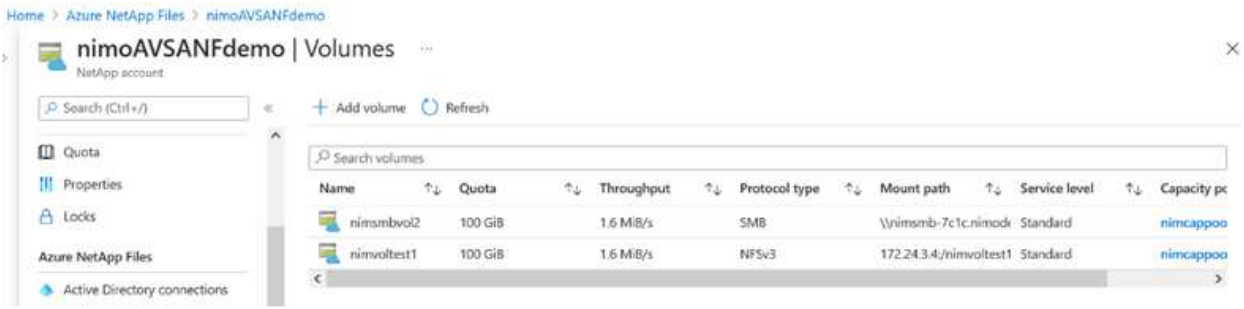
4. Fügen Sie ein SMB-Volume mithilfe des Volumes Blade unter dem Capacity Pools Blade hinzu. Stellen Sie sicher, dass der Active Directory-Konnektor konfiguriert ist, bevor Sie das SMB-Volume erstellen.



5. Klicken Sie auf Überprüfen + Erstellen, um das SMB-Volume zu erstellen.

   Wenn es sich bei der Applikation um SQL Server handelt, aktivieren Sie die kontinuierliche Verfügbarkeit von SMB.

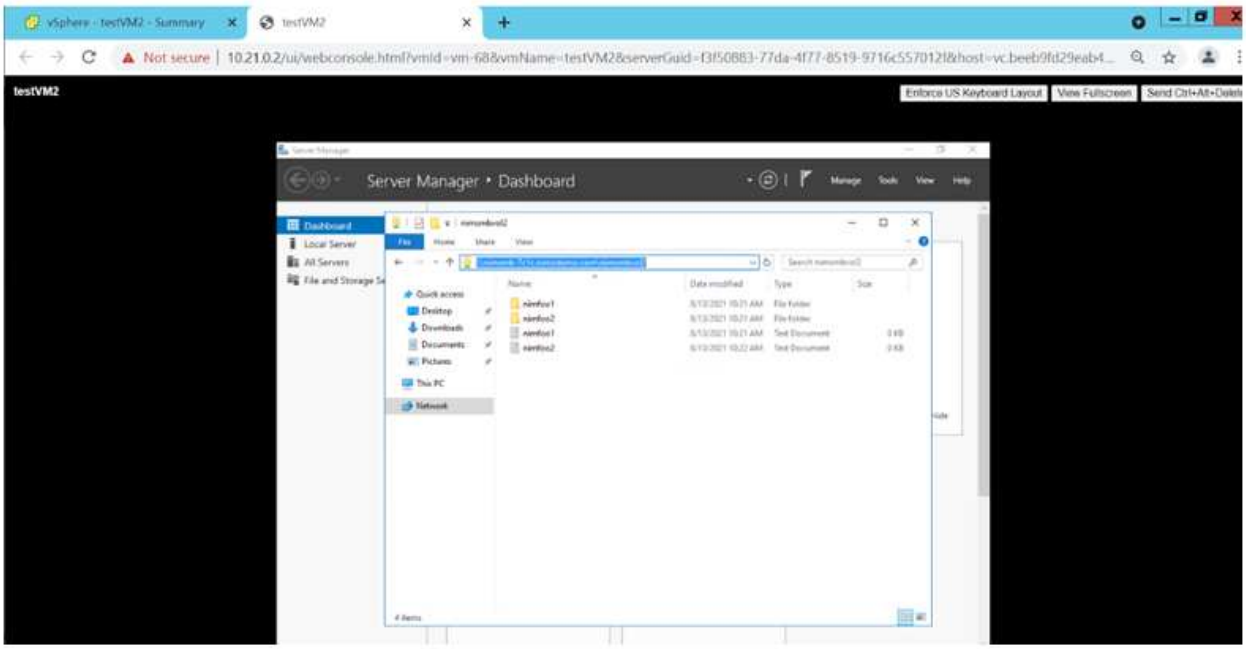


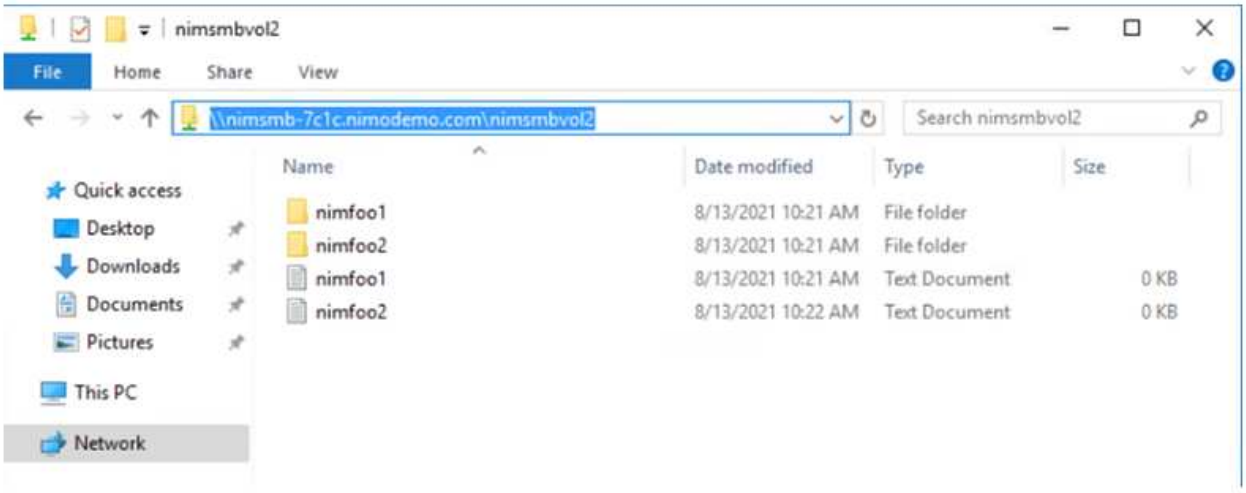


Weitere Informationen zur Azure NetApp Files Volume-Performance nach Größe oder Kontingent finden Sie unter "Überlegungen zur Performance von Azure NetApp Files".

6. Nach erfolgter Konnektivität kann das Volume gemountet und für Applikationsdaten verwendet werden.

   Dazu klicken Sie im Azure Portal auf das Volumes-Blade und wählen Sie dann das zu montierenden Volume aus und greifen Sie auf die Mount-Anweisungen zu. Kopieren Sie den Pfad und verwenden Sie die Option Map Network Drive, um das Volume auf der VM zu mounten, die auf der Azure VMware Solution SDDC ausgeführt wird.





7. Um NFS Volumes auf Linux VMs einzubinden, die auf dem Azure VMware Solution SDDC laufen, verwenden Sie denselben Prozess. Erfüllen Sie die Workload-Anforderungen mit Volume-Neustrukturierung oder dynamischen Service-Level-Funktionen.

```
nimoadmin@nimoadmin-virtual-machine:~$ sudo mount -t nfs -o rw,hard,tcp 172.24.
3.4:/nimodemonfsv1 /home/nimoadmin/nimodemo11
nimoadmin@nimoadmin-virtual-machine:~$ df
Filesystem                  1K-blocks     Used Available Use% Mounted on
udev                          8168112        0   8168112   0% /dev
tmpfs                         1639548     1488   1638060   1% /run
/dev/sda5                    50824704  7902752  40310496  17% /
tmpfs                         8197728        0   8197728   0% /dev/shm
tmpfs                            5120        0      5120   0% /run/lock
tmpfs                         8197728        0   8197728   0% /sys/fs/cgroup
/dev/loop0                      56832    56832         0 100% /snap/core18/2128
/dev/loop2                      66688    66688         0 100% /snap/gtk-common-the
mes/1515
/dev/loop1                     224256   224256         0 100% /snap/gnome-3-34-180
4/72
/dev/loop3                      52224    52224         0 100% /snap/snap-store/547
/dev/loop4                      33152    33152         0 100% /snap/snapd/12704
/dev/sda1                      523248        4    523244   1% /boot/efi
tmpfs                         1639544       52   1639492   1% /run/user/1000
/dev/sr0                        54738    54738         0 100% /media/nimoadmin/VMw
are Tools
172.24.3.4:/nimodemonfsv1 104857600        0 104857600   0% /home/nimoadmin/nimo
demo11
nimoadmin@nimoadmin-virtual-machine:~$
```

Weitere Informationen finden Sie unter "Profitieren Sie von einer dynamischen Änderung des Service-Levels eines Volumes".

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenmanagement-Lösung auf Basis der Storage-Software ONTAP von NetApp. Sie ist nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar.

Es handelt sich um eine softwaredefinierte Version von ONTAP, die Cloud-nativen Storage nutzt, sodass Sie

dieselbe Storage-Software in der Cloud und vor Ort nutzen können. Dadurch müssen SIE Ihre IT-Mitarbeiter nicht mehr in komplett neue Methoden zum Datenmanagement Schulen.

Mit CVO können Kunden Daten nahtlos vom Edge- zum Datacenter, zur Cloud und zurück verschieben und so Ihre Hybrid Cloud zusammen – all das wird über eine zentrale Managementkonsole, NetApp Cloud Manager, gemanagt.

CVO ist von Grund auf für beste Performance und erweiterte Datenmanagementfunktionen konzipiert, um auch die anspruchsvollsten Applikationen in der Cloud zu unterstützen

Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff

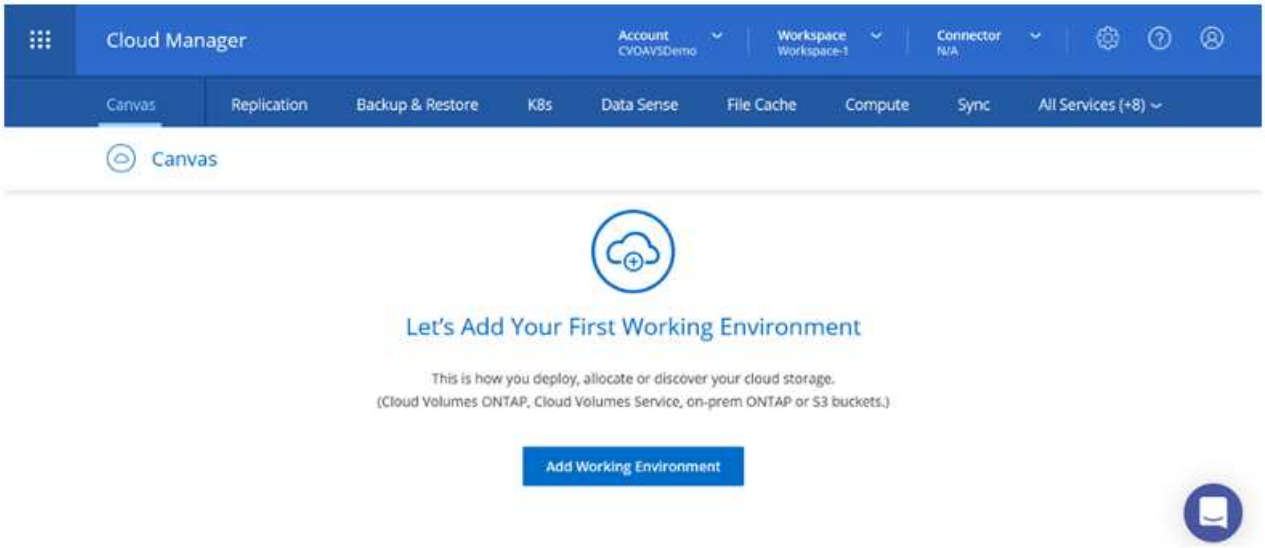
Implementieren Sie neue Cloud Volumes ONTAP in Azure

Cloud Volumes ONTAP-Freigaben und LUNs können von VMs gemountet werden, die in der SDDC Umgebung der Azure VMware Lösung erstellt wurden. Die Volumes können auch auf dem Linux-Client und auf dem Windows-Client eingebunden werden, da Cloud Volumes ONTAP iSCSI-, SMB- und NFS-Protokolle unterstützt. Cloud Volumes ONTAP Volumes lassen sich in wenigen einfachen Schritten einrichten.

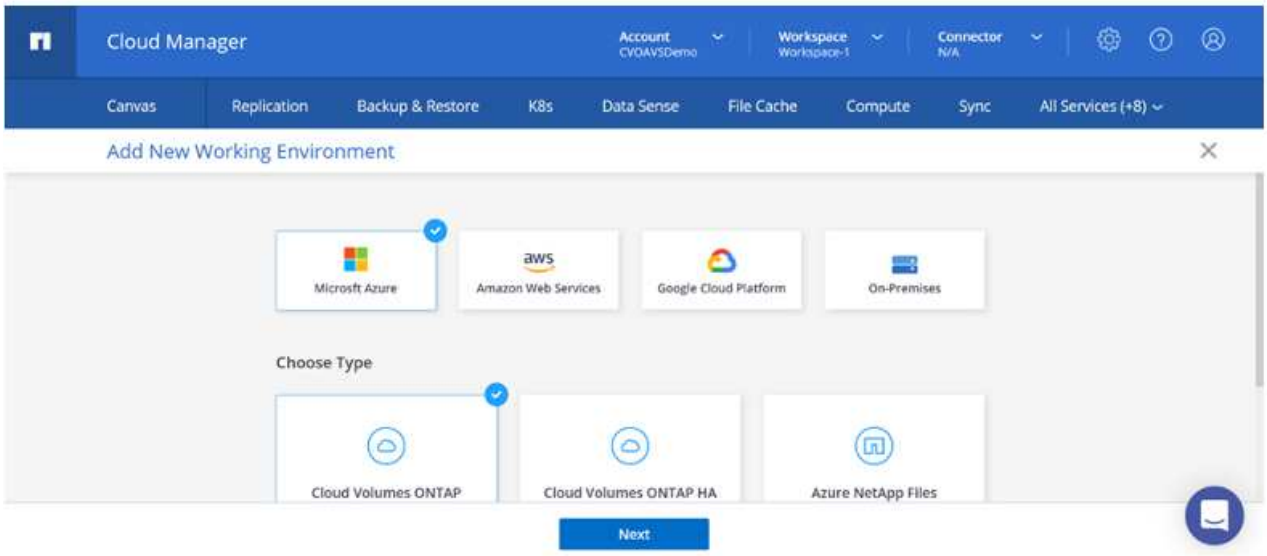
Um Volumes aus einer On-Premises-Umgebung zu Disaster-Recovery- oder Migrationszwecken in die Cloud zu replizieren, sollten Sie entweder über ein Site-to-Site-VPN oder ExpressRoute eine Netzwerkverbindung zu Azure herstellen. Die Replizierung von Daten zwischen On-Premises-Systemen und Cloud Volumes ONTAP ist im Rahmen dieses Dokuments nicht enthalten. Informationen zur Replizierung von Daten zwischen On-Premises- und Cloud Volumes ONTAP-Systemen finden Sie unter "Datenreplikation zwischen Systemen einrichten".

Nutzung "Cloud Volumes ONTAP-Dimensionierungstool" Und die präzise Größe der Cloud Volumes ONTAP-Instanzen. Monitoring der On-Premises-Performance als Eingaben im Cloud Volumes ONTAP Sizer.

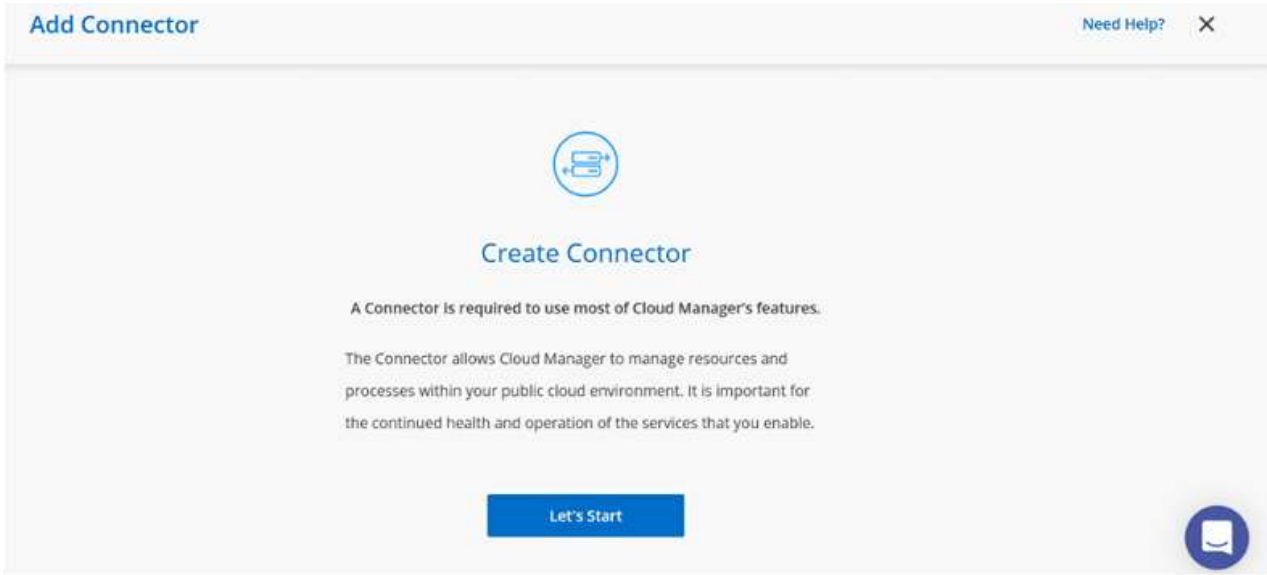
1. Bei NetApp Cloud Central anmelden – der Bildschirm Fabric View wird angezeigt. Wählen Sie die Registerkarte Cloud Volumes ONTAP aus und wechseln Sie zu Cloud Manager. Nach der Anmeldung wird der Bildschirm Arbeitsfläche angezeigt.



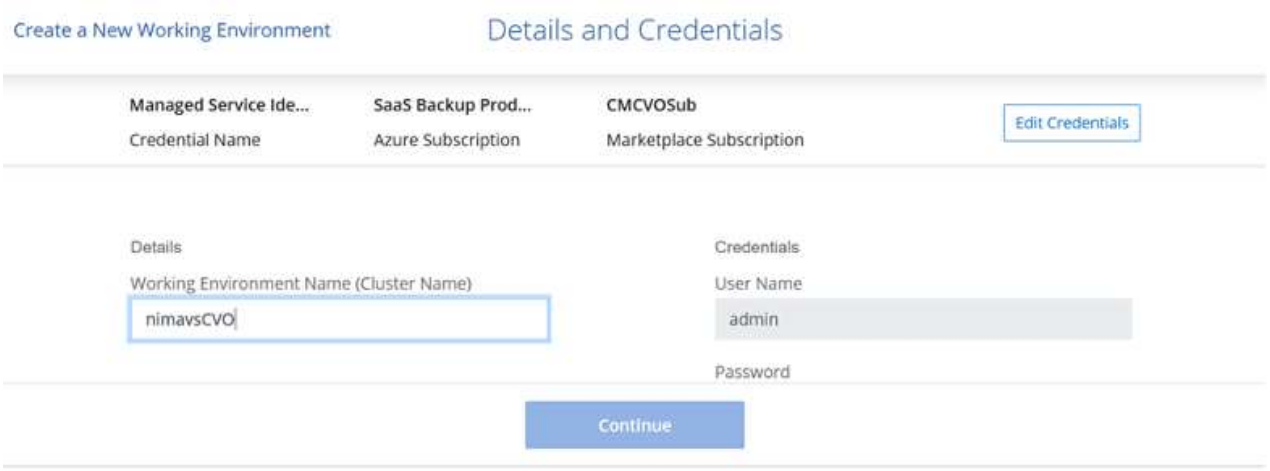
2. Klicken Sie auf der Cloud Manager-Startseite auf „Arbeitsumgebung hinzufügen“ und wählen Sie dann Microsoft Azure als Cloud und den Typ der Systemkonfiguration aus.



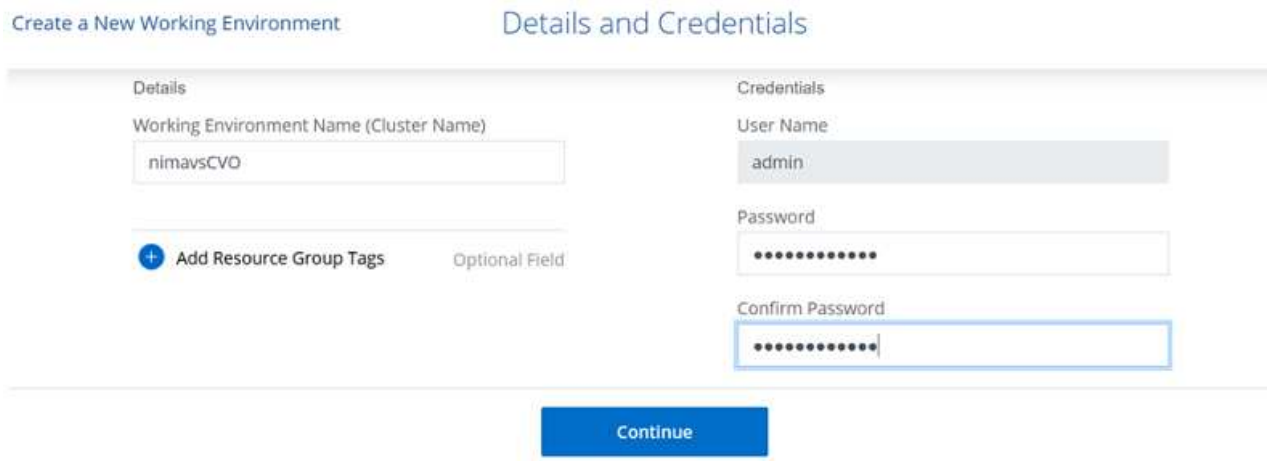
3. Beim Erstellen der ersten Cloud Volumes ONTAP-Arbeitsumgebung werden Sie von Cloud Manager aufgefordert, einen Connector bereitzustellen.



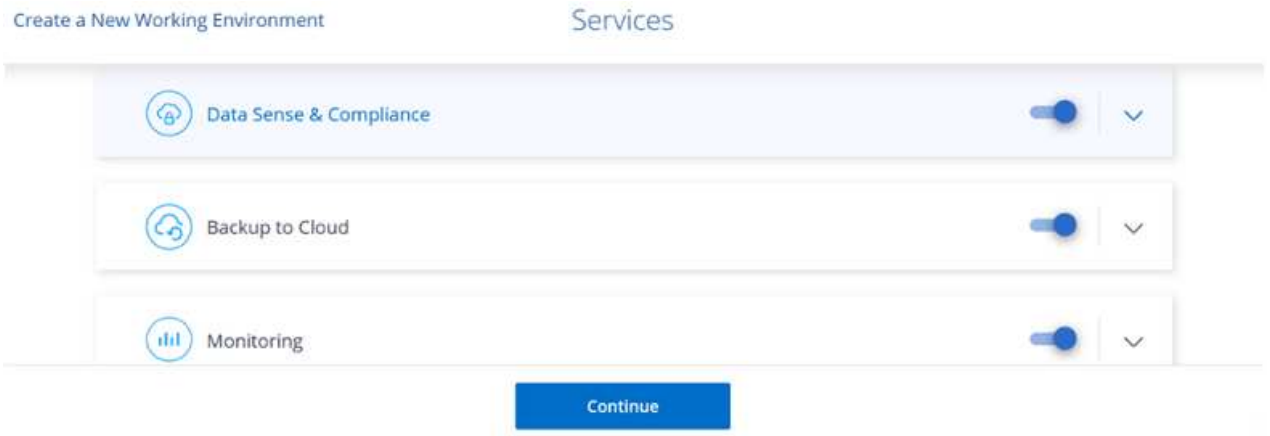
4. Aktualisieren Sie nach der Erstellung des Connectors die Felder Details und Anmeldeinformationen.



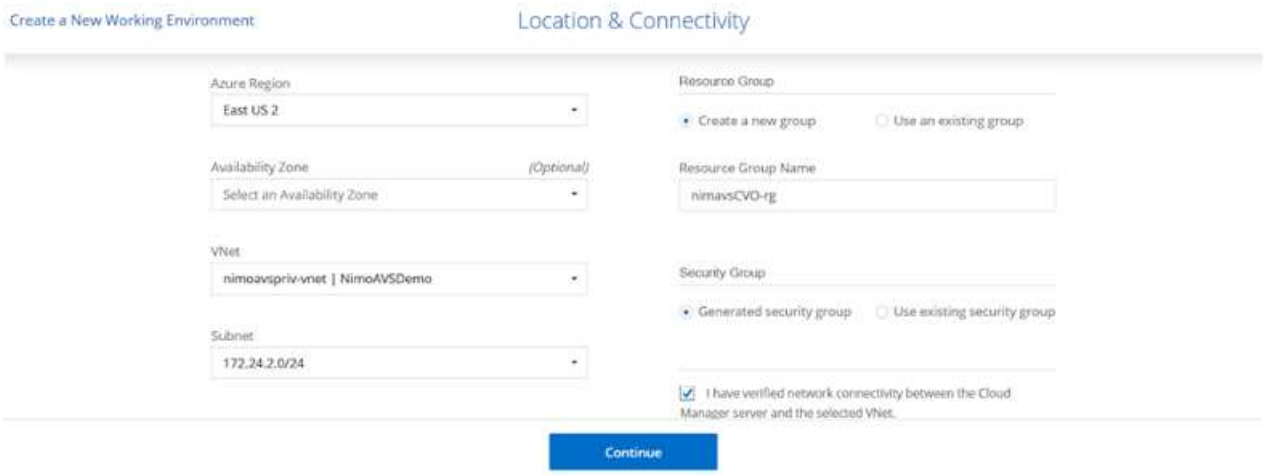
5. Geben Sie die Details zur zu erstellenden Umgebung an, einschließlich Name der Umgebung und Anmeldedaten des Administrators. Fügen Sie als optionaler Parameter Ressourcengruppen-Tags für die Azure-Umgebung hinzu. Klicken Sie nach dem Abschluss auf Weiter.



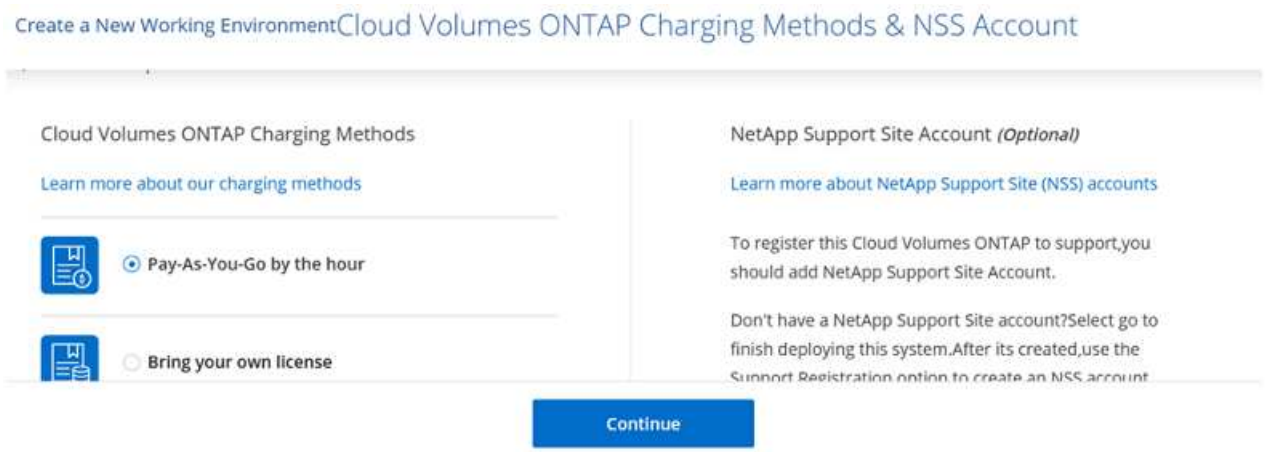
6. Wählen Sie die Add-on-Services für die Implementierung von Cloud Volumes ONTAP aus, darunter BlueXP Klassifizierung, BlueXP Backup und Recovery sowie Cloud Insights. Wählen Sie die Dienste aus, und klicken Sie dann auf Weiter.



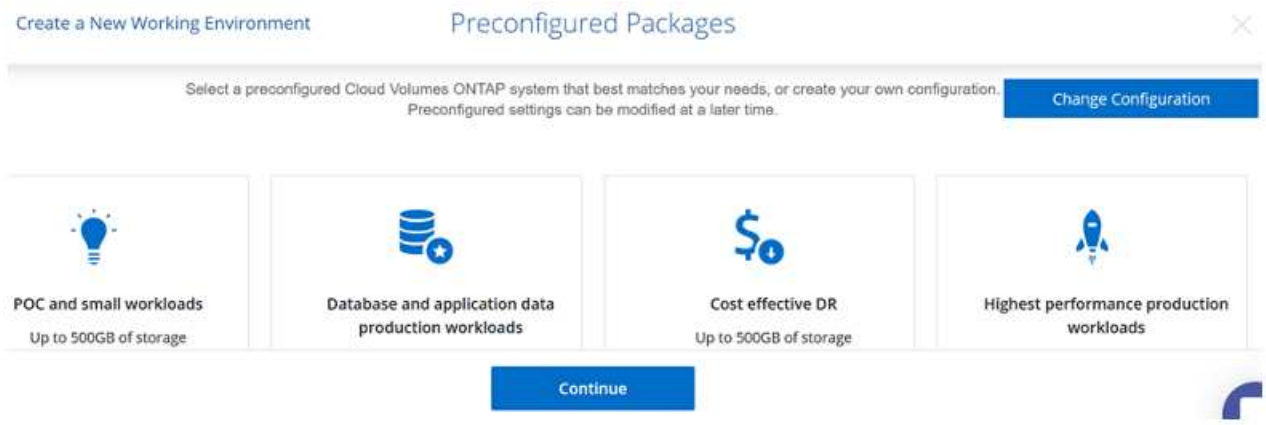
7. Konfigurieren Sie den Azure-Speicherort und die Konnektivität. Wählen Sie die Azure Region, Ressourcengruppe, vnet und Subnetz aus, die verwendet werden sollen.



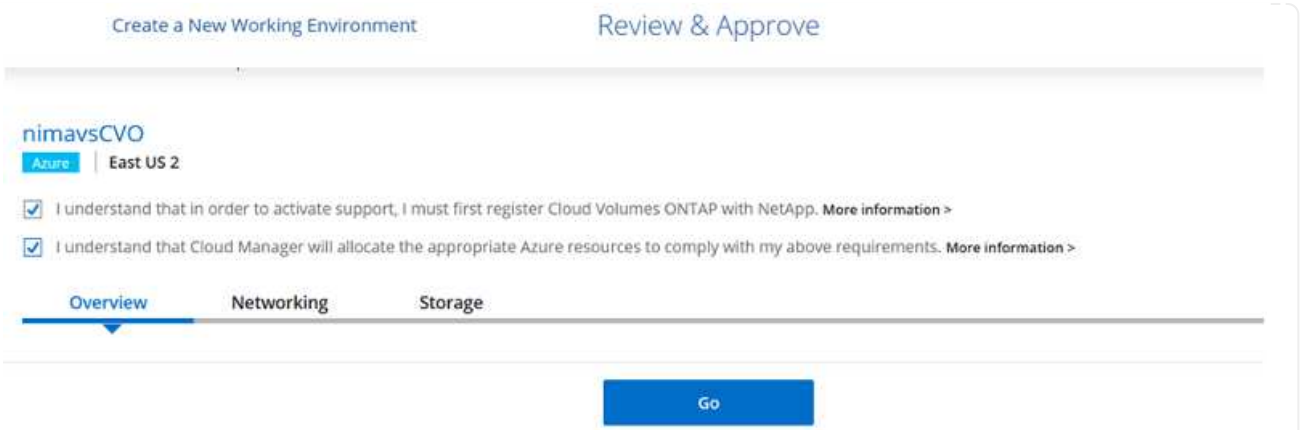
8. Wählen Sie die Lizenzoption: Pay-as-you-Go oder BYOL für die Nutzung vorhandener Lizenz. In diesem Beispiel wird die Pay-as-you-Go-Option verwendet.



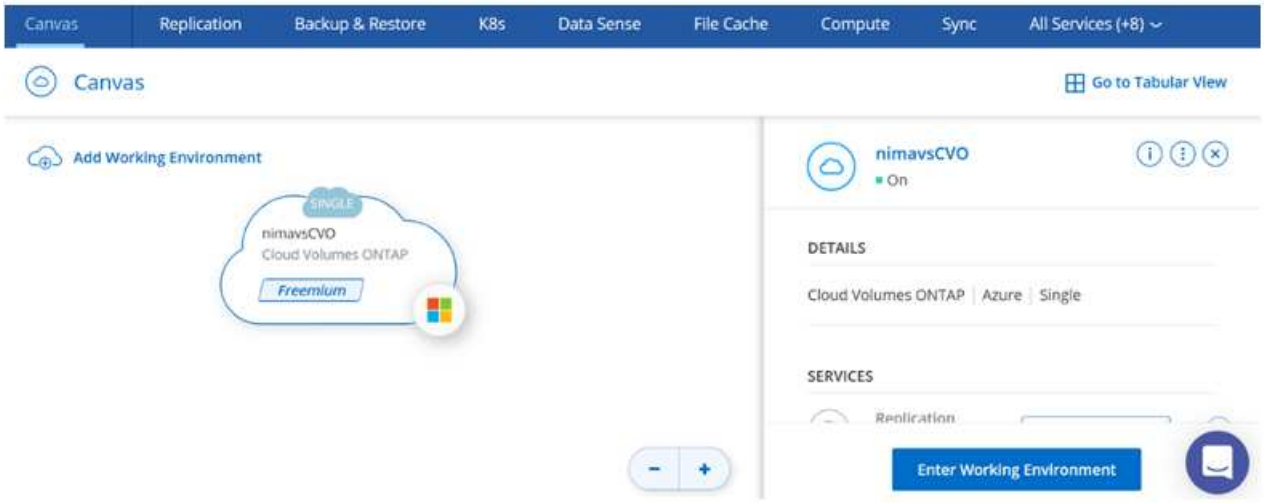
9. Wählen Sie zwischen mehreren vorkonfigurierten Paketen, die für die verschiedenen Workload-Typen verfügbar sind.



10. Akzeptieren Sie die beiden Vereinbarungen über die Aktivierung von Support und Zuweisung von Azure Ressourcen.zum Erstellen der Cloud Volumes ONTAP Instanz klicken Sie auf Go.

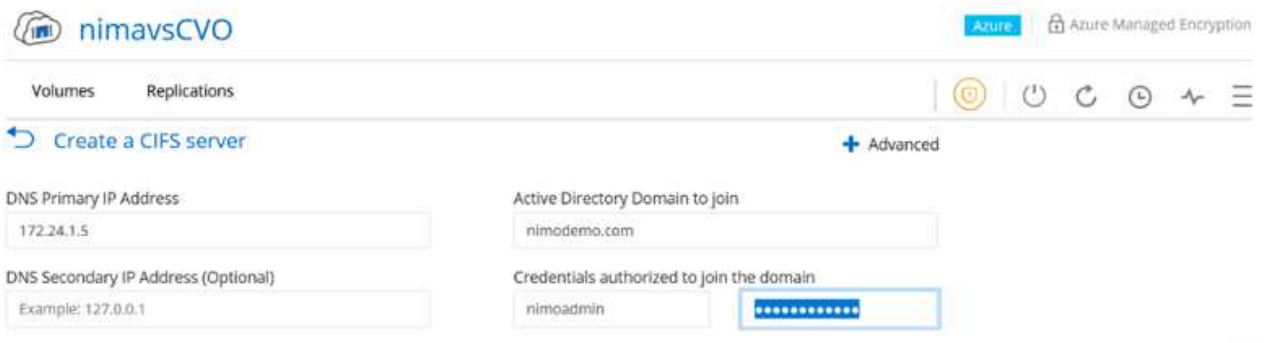


11. Nach der Bereitstellung von Cloud Volumes ONTAP wird es in den Arbeitsumgebungen auf der Seite Arbeitsfläche aufgelistet.

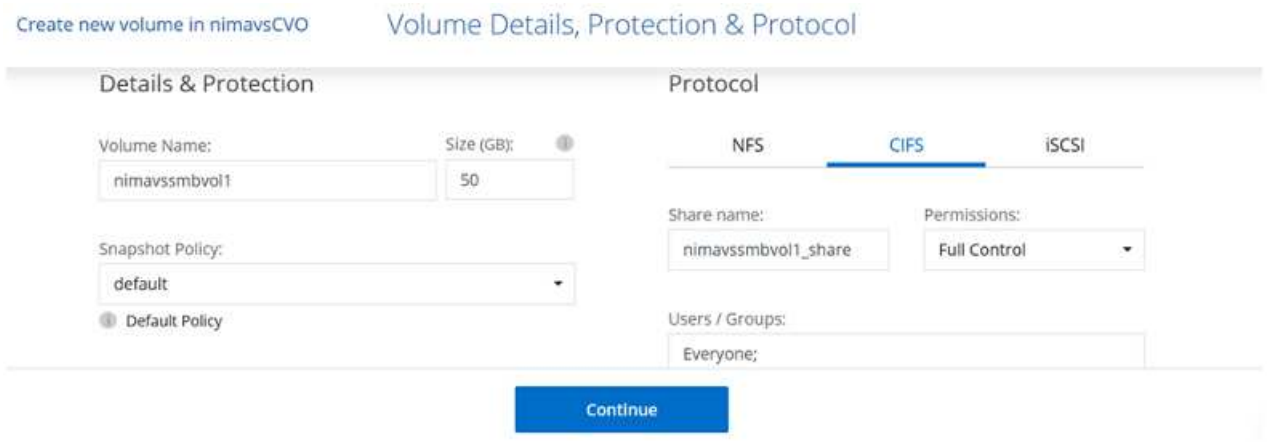


Zusätzliche Konfigurationen für SMB Volumes

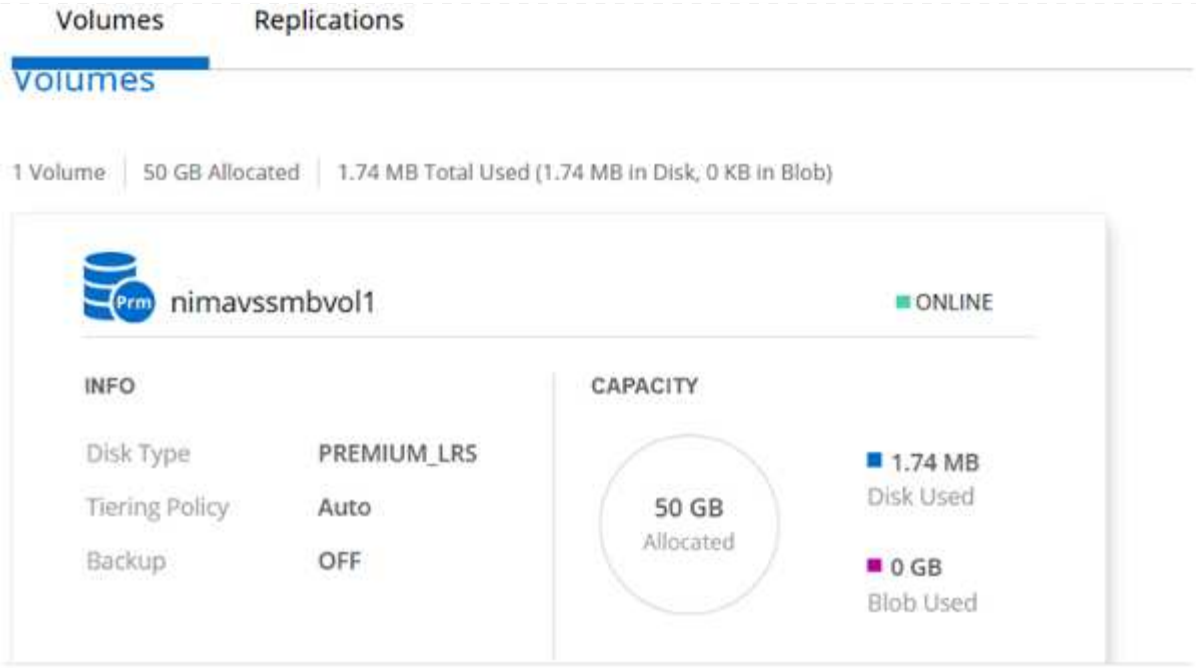
1. Stellen Sie nach der Arbeitsumgebung sicher, dass der CIFS-Server mit den entsprechenden DNS- und Active Directory-Konfigurationsparametern konfiguriert ist. Dieser Schritt ist erforderlich, bevor Sie das SMB-Volume erstellen können.



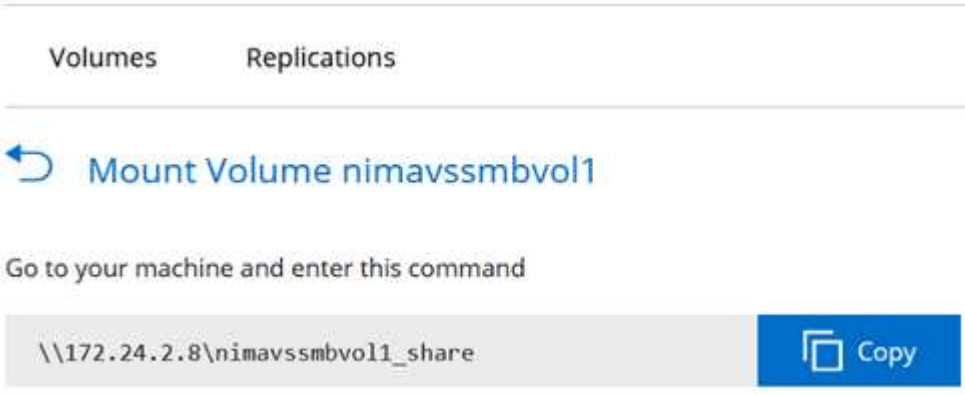
2. Das Erstellen des SMB Volume ist einfach. Wählen Sie die CVO-Instanz aus, um das Volume zu erstellen, und klicken Sie auf die Option Volume erstellen. Wählen Sie die entsprechende Größe und Cloud Manager wählt das Aggregat aus, das Sie enthalten, oder verwenden Sie den erweiterten Zuweisungsmechanismus auf einem bestimmten Aggregat. Für diese Demo wird SMB als Protokoll ausgewählt.

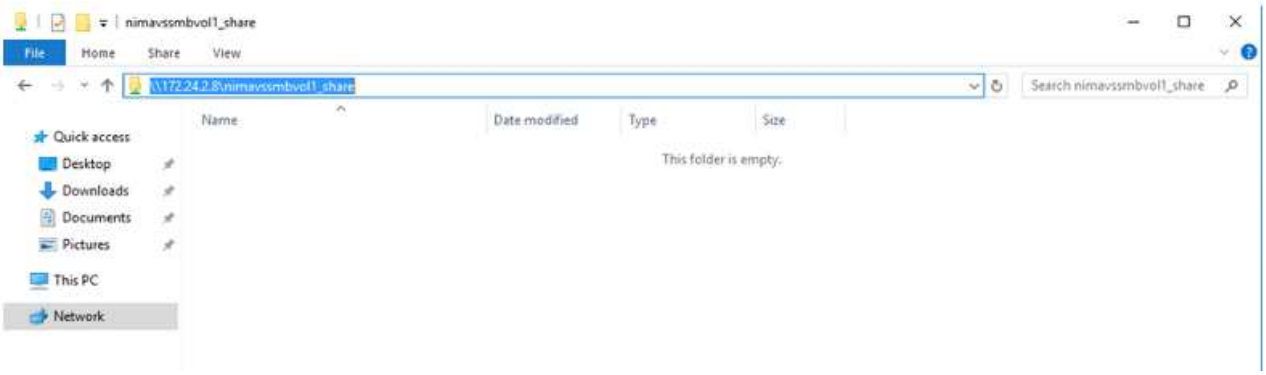


3. Nachdem das Volume bereitgestellt wurde, wird es unter dem Fensterbereich Volumes verfügbar sein. Da eine CIFS-Freigabe bereitgestellt wird, geben Sie Ihren Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können. Dieser Schritt ist nicht erforderlich, wenn das Volume aus einer lokalen Umgebung repliziert wird, da die Datei- und Ordnerberechtigungen im Rahmen der SnapMirror Replizierung beibehalten werden.



4. Nachdem das Volume erstellt wurde, verwenden Sie den Mount-Befehl, um eine Verbindung mit dem Share von der VM herzustellen, die auf den Azure VMware SDDC-Lösungen ausgeführt wird.
5. Kopieren Sie den folgenden Pfad und verwenden Sie die Option Netzwerklaufwerk zuordnen, um das Volume auf der VM zu mounten, die auf dem Azure VMware SDDC ausgeführt wird.

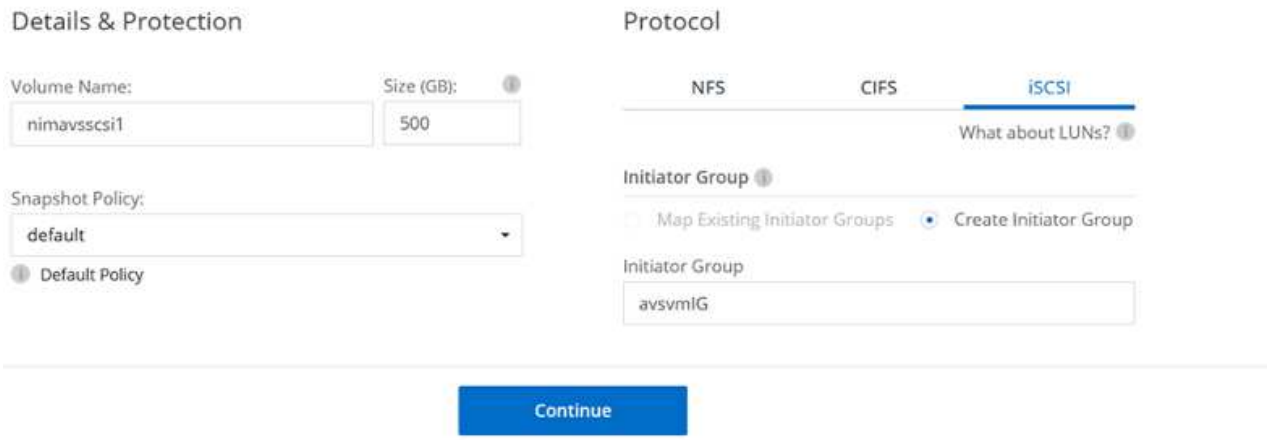




Verbinden Sie die LUN mit einem Host

Gehen Sie wie folgt vor, um die LUN mit einem Host zu verbinden:

1. Doppelklicken Sie auf der Seite Arbeitsfläche von Cloud Volumes ONTAP auf die Arbeitsumgebung, um Volumes zu erstellen und zu verwalten.
2. Klicken Sie auf Volume hinzufügen > Neues Volume, und wählen Sie iSCSI aus, und klicken Sie auf Initiatorgruppe erstellen. Klicken Sie auf Weiter .



3. Wählen Sie nach der Bereitstellung des Volumes das Volume aus, und klicken Sie dann auf Ziel-IQN. Um den iSCSI-qualifizierten Namen (IQN) zu kopieren, klicken Sie auf Kopieren. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.

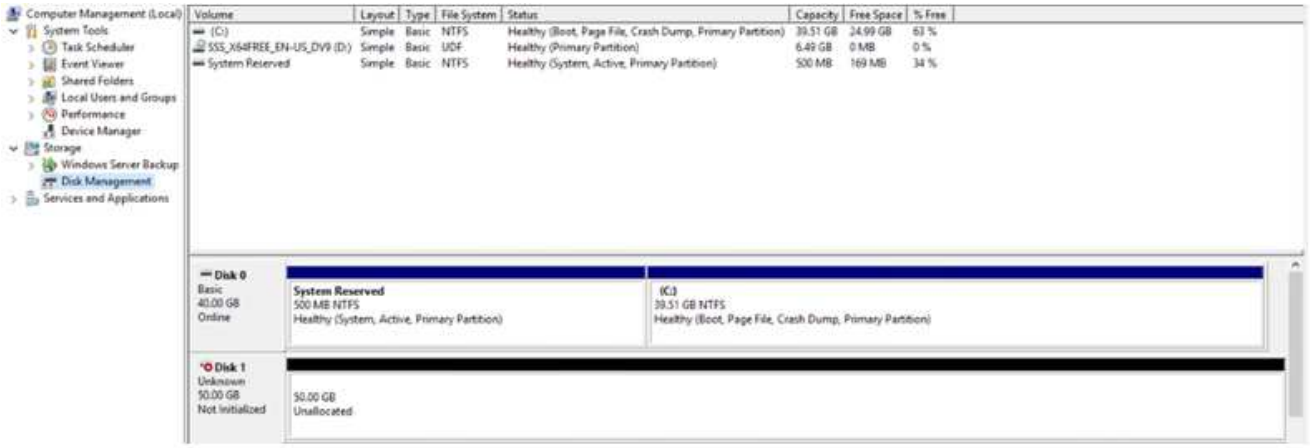
   Um dasselbe für den Host, der auf dem Azure VMware Solution SDDC liegt, zu erreichen:

   a. RDP auf die VM gehostet auf Azure VMware Solution SDDC.
   b. Öffnen Sie das Dialogfeld iSCSI-Initiator-Eigenschaften: Server Manager > Dashboard > Tools > iSCSI-Initiator.
   c. Klicken Sie auf der Registerkarte Ermittlung auf Portal erkennen oder Portal hinzufügen, und geben Sie dann die IP-Adresse des iSCSI-Zielports ein.
   d. Wählen Sie auf der Registerkarte Ziele das erkannte Ziel aus und klicken Sie dann auf Anmelden oder Verbinden.
   e. Wählen Sie Multipath aktivieren, und wählen Sie dann automatisch Diese Verbindung wiederherstellen, wenn der Computer startet oder diese Verbindung zur Liste der bevorzugten Ziele hinzufügen. Klicken Sie Auf Erweitert.

      Hinweis: der Windows-Host muss eine iSCSI-Verbindung zu jedem Knoten im Cluster haben. Das native DSM wählt die besten Pfade aus.

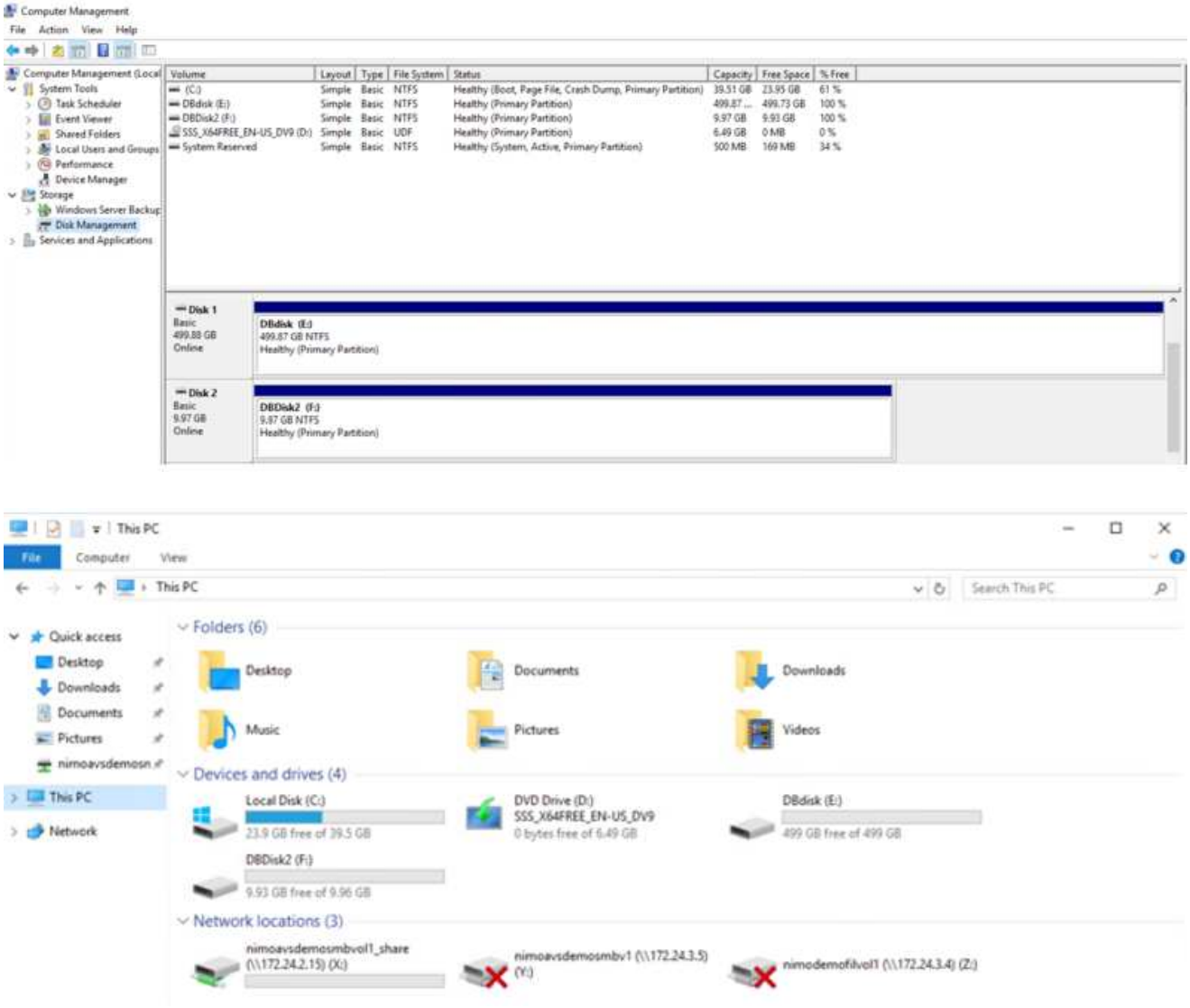
LUNs auf Storage Virtual Machine (SVM) werden dem Windows Host als Festplatten angezeigt. Neue hinzugefügte Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen Rescan aus, um die Festplatten zu ermitteln, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie das Dienstprogramm Windows Computer Management: Start > Verwaltung > Computerverwaltung.
2. Erweitern Sie den Knoten Speicher in der Navigationsstruktur.
3. Klicken Sie Auf Datenträgerverwaltung.
4. Klicken Sie Auf Aktion > Datenträger Erneut Scannen.



Wenn der Windows-Host zum ersten Mal auf eine neue LUN zugreift, hat sie keine Partition oder kein Dateisystem. Initialisieren Sie die LUN; und optional formatieren Sie die LUN mit einem Dateisystem, indem Sie die folgenden Schritte durchführen:

1. Starten Sie Windows Disk Management.
2. Klicken Sie mit der rechten Maustaste auf die LUN, und wählen Sie dann den erforderlichen Festplatten- oder Partitionstyp aus.
3. Befolgen Sie die Anweisungen im Assistenten. In diesem Beispiel ist Laufwerk E: Angehängt

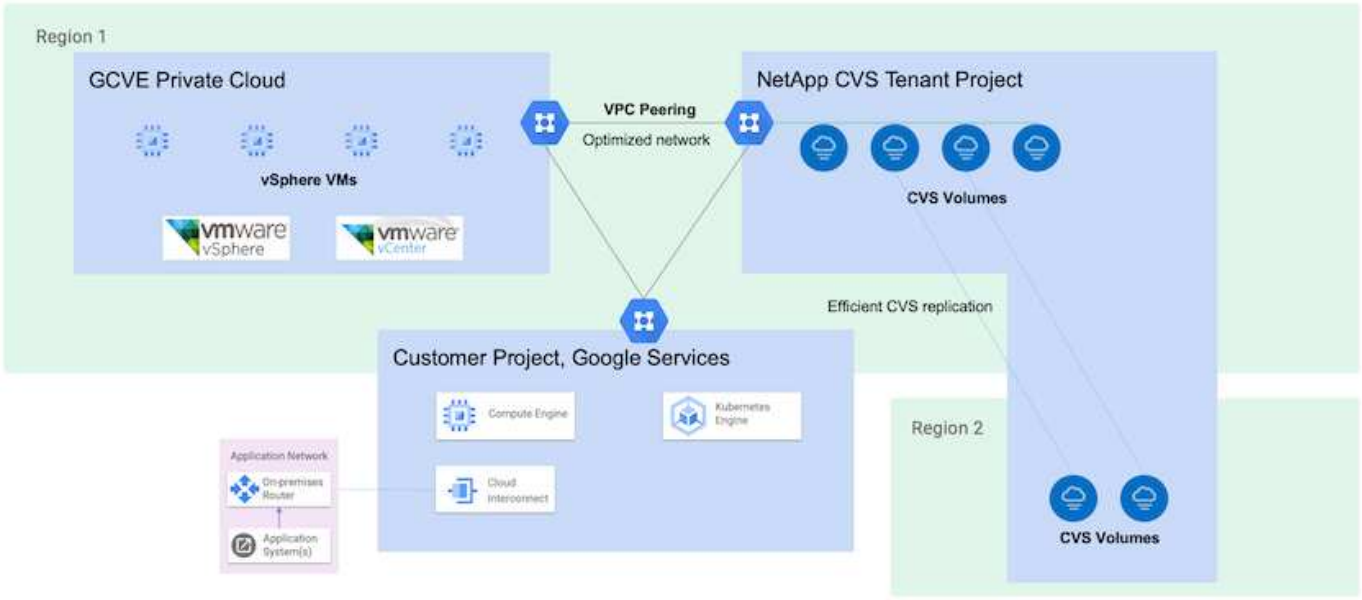


Ergänzender NFS-Datastore für die Google Cloud VMware Engine mit NetApp Cloud Volume Service

Überblick

Autoren: Suresh ThopPay, NetApp

Kunden, die in ihrer Google Cloud VMware Engine (GCVE) Umgebung zusätzliche Storage-Kapazität benötigen, können mithilfe des NetApp Cloud Volume Service als zusätzlichen NFS-Datastore mounten. Werden Daten in NetApp Cloud Volumes Service gespeichert, können Kunden zwischen Regionen replizieren, um sich vor Diastern zu schützen.



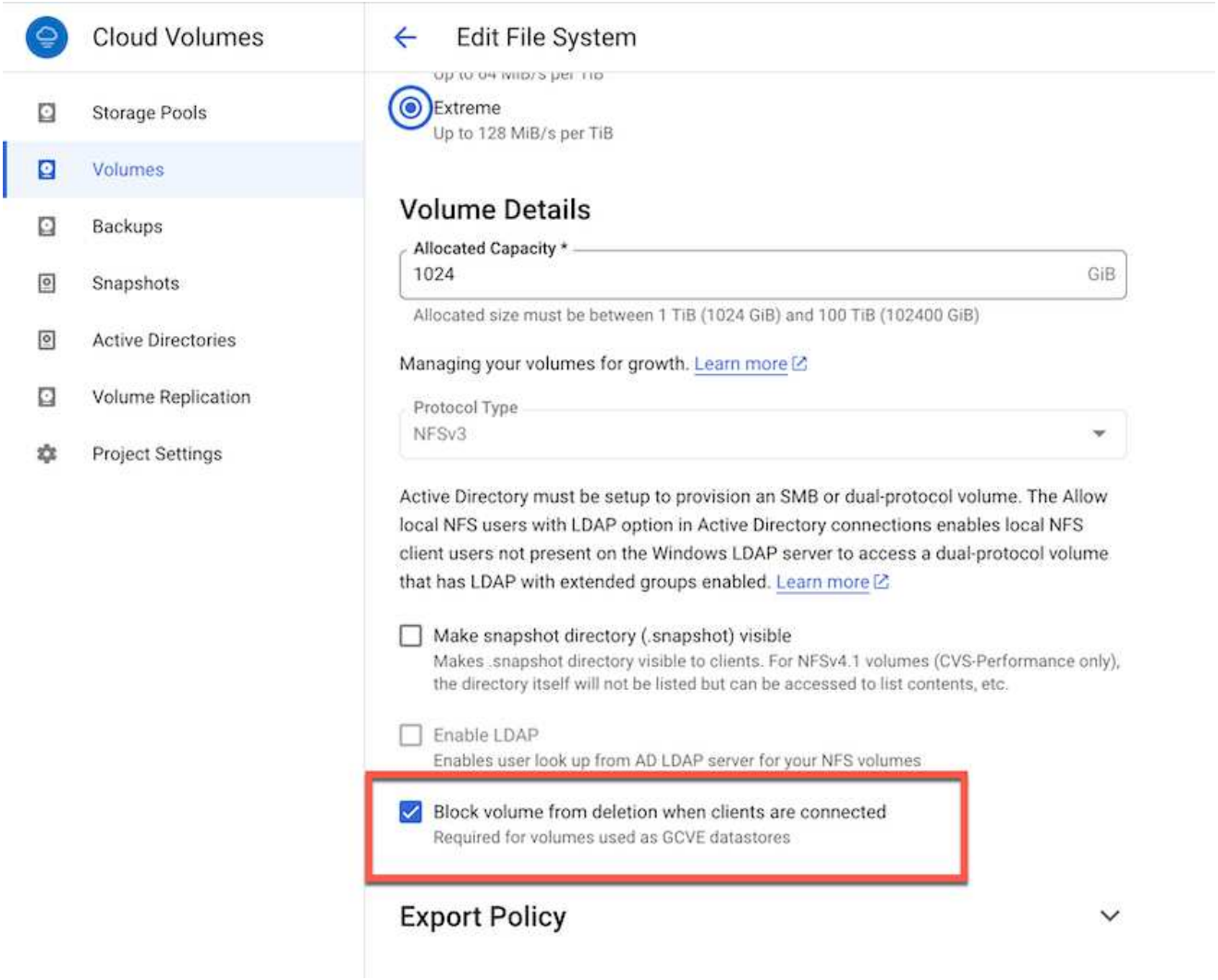
Bereitstellungsschritte zum Mounten von NFS-Datastore aus NetApp CVS auf GCVE

Bereitstellung von CVS-Performance Volume

Das NetApp Cloud Volume Service-Volume kann über bereitgestellt werden
"Verwenden Der Google Cloud Console"
"Sie nutzen das NetApp BlueXP Portal oder die API"

Markieren Sie das CVS-Volume als löschbar

Um versehentliches Löschen des Volumes während der Ausführung der VM zu vermeiden, stellen Sie sicher, dass das Volume als löschbar markiert ist, wie in der Abbildung unten gezeigt.



Weitere Informationen finden Sie unter "NFS-Volume wird erstellt" Dokumentation.

Stellen Sie sicher, dass für die NetApp CVS-Mandanten-VPC eine private Verbindung auf GCVE vorhanden ist.

Zum Mounten von NFS Datastore sollte eine private Verbindung zwischen GCVE und NetApp CVS-Projekt bestehen.
Weitere Informationen finden Sie unter "So richten Sie den Zugriff auf den privaten Dienst ein"

Mounten Sie den NFS-Datastore

Anweisungen zum Mounten von NFS-Datastore auf GCVE finden Sie unter "So erstellen Sie NFS Datastore mit NetApp CVS"

> Da vSphere-Hosts von Google gemanagt werden, haben Sie keinen Zugriff auf die Installation von NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB).
> Wenn Sie Unterstützung für Virtual Volumes (vVol) benötigen, lassen Sie es uns bitte wissen.
> Wenn Sie Jumbo Frames verwenden möchten, lesen Sie bitte nach "Maximal unterstützte MTU-Größen auf GCP"

Einsparungen mit NetApp Cloud Volume Service

Weitere Informationen zu Ihren potenziellen Einsparungen bei der Verwendung des NetApp Cloud Volume Service für Ihre Speicheranforderungen an GCVE finden Sie unter "ROI-Rechner von NetApp"

Referenzlinks

- "Google Blog - so verwenden Sie NetApp CVS als Datastores für Google Cloud VMware Engine"
- "NetApp-Blog – Eine bessere Möglichkeit, Ihre speicherintensiven Applikationen in Google Cloud zu migrieren"

NetApp Storage-Optionen für GCP

Die GCP unterstützt NetApp Storage mit Anbindung an den Gast-Storage über Cloud Volumes ONTAP (CVO) oder Cloud Volumes Service (CVS).

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenmanagement-Lösung auf Basis der Storage-Software ONTAP von NetApp. Sie ist nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar.

Es handelt sich um eine softwaredefinierte Version von ONTAP, die Cloud-nativen Storage nutzt, sodass Sie dieselbe Storage-Software in der Cloud und vor Ort nutzen können. Dadurch müssen SIE Ihre IT-Mitarbeiter nicht mehr in komplett neue Methoden zum Datenmanagement Schulen.

Mit CVO können Kunden Daten nahtlos vom Edge- zum Datacenter, zur Cloud und zurück verschieben und so Ihre Hybrid Cloud zusammen – all das wird über eine zentrale Managementkonsole, NetApp Cloud Manager, gemanagt.

CVO ist von Grund auf für beste Performance und erweiterte Datenmanagementfunktionen konzipiert, um auch die anspruchsvollsten Applikationen in der Cloud zu unterstützen

Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff

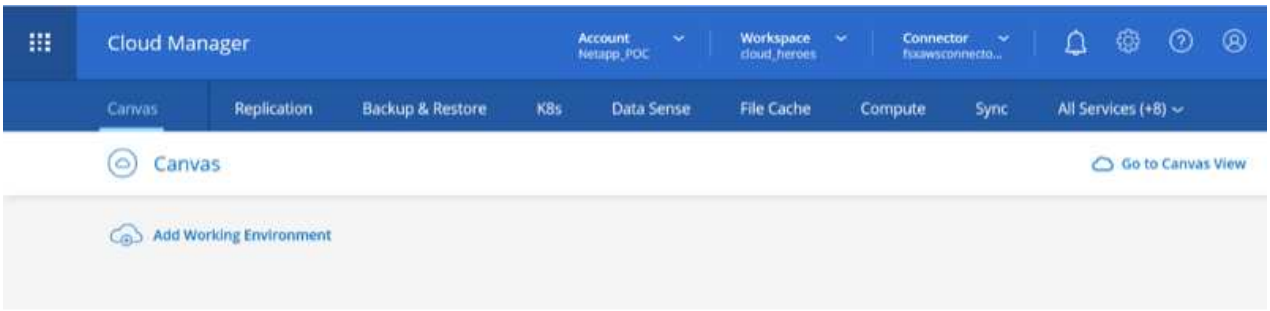
Implementierung von Cloud Volumes ONTAP in der Google Cloud (Do IT Yourself)

Cloud Volumes ONTAP-Freigaben und LUNs können von VMs gemountet werden, die in der GCVE Private Cloud-Umgebung erstellt wurden. Die Volumes können auch auf dem Linux-Client und auf dem Windows-Client eingebunden werden, wobei auf LUNS unter Linux- oder Windows-Clients als Blockgeräte zugegriffen werden kann, wenn sie über iSCSI gemountet werden, da Cloud Volumes ONTAP iSCSI-, SMB- und NFS-Protokolle unterstützt. Cloud Volumes ONTAP Volumes lassen sich in wenigen einfachen Schritten einrichten.

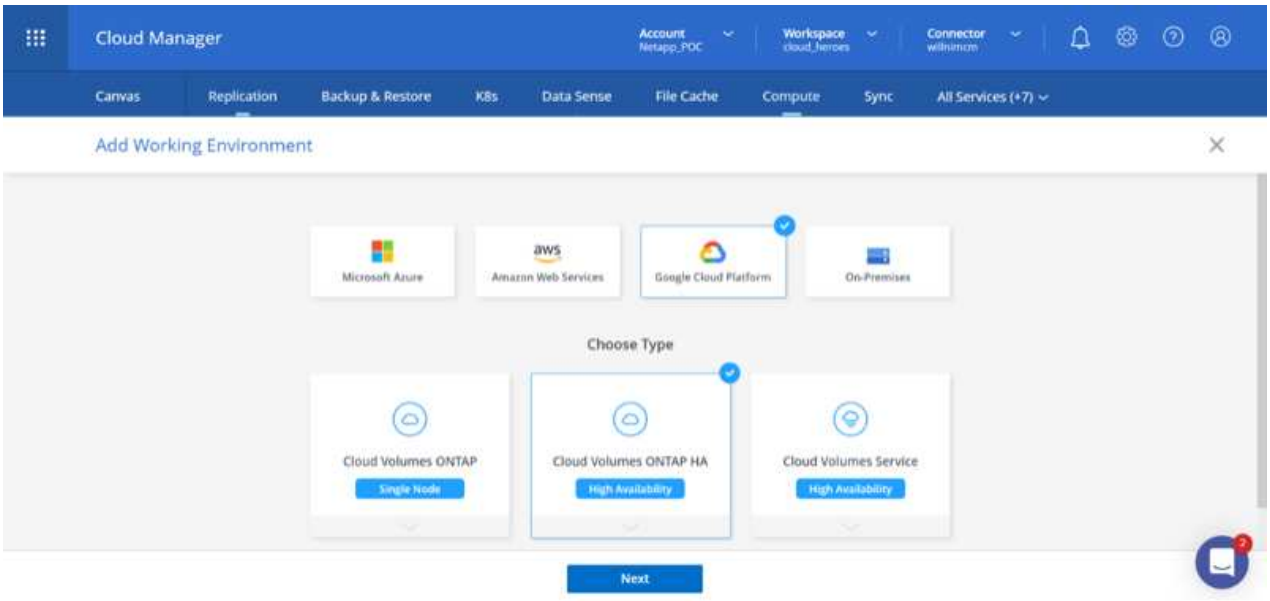
Wenn Sie Volumes aus einer lokalen Umgebung für Disaster Recovery- oder Migrationszwecke in die Cloud replizieren möchten, richten Sie Netzwerkkonnektivität mit Google Cloud ein, entweder über ein Site-to-Site VPN oder ein Cloud Interconnect. Die Replizierung von Daten zwischen On-Premises-Systemen und Cloud Volumes ONTAP ist im Rahmen dieses Dokuments nicht enthalten. Informationen zur Replizierung von Daten zwischen On-Premises- und Cloud Volumes ONTAP-Systemen finden Sie unter xref:./ehc/"Datenreplikation zwischen Systemen einrichten".

Nutzung "Cloud Volumes ONTAP-Dimensionierungstool" Und die präzise Größe der Cloud Volumes ONTAP-Instanzen. Monitoring der On-Premises-Performance als Eingaben im Cloud Volumes ONTAP Sizer.

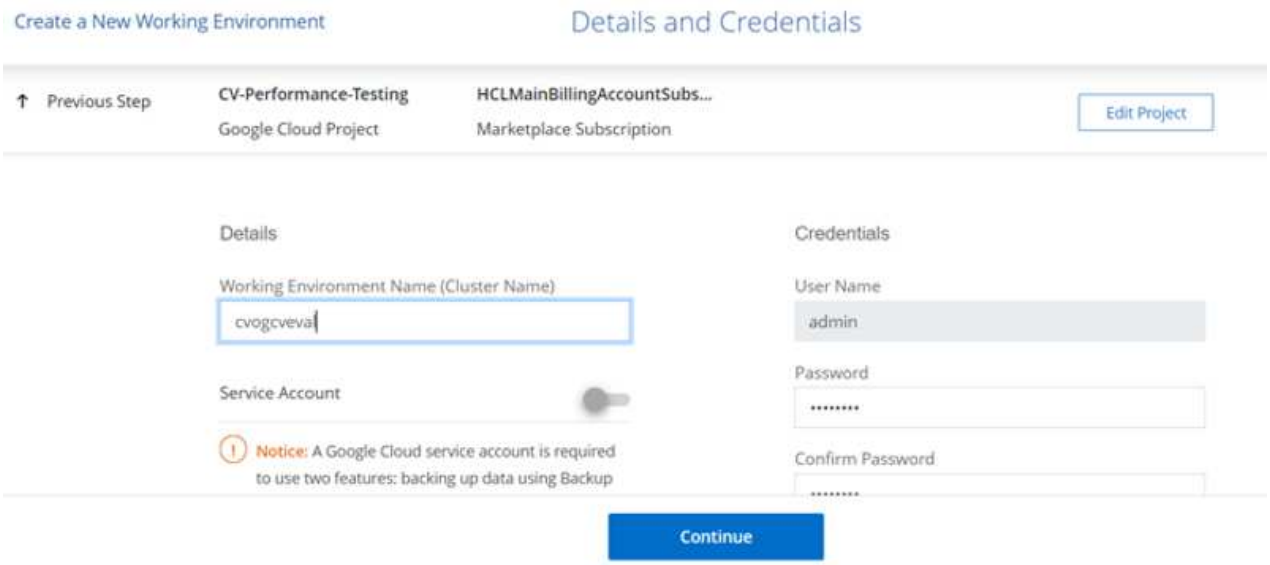
1. Bei NetApp Cloud Central anmelden – der Bildschirm Fabric View wird angezeigt. Wählen Sie die Registerkarte Cloud Volumes ONTAP aus und wechseln Sie zu Cloud Manager. Nach der Anmeldung wird der Bildschirm Arbeitsfläche angezeigt.



2. Klicken Sie auf der Registerkarte „Canvas“ auf „Arbeitsumgebung hinzufügen“ und wählen Sie dann Google Cloud Platform als Cloud und den Typ der Systemkonfiguration aus. Klicken Sie anschließend auf Weiter.

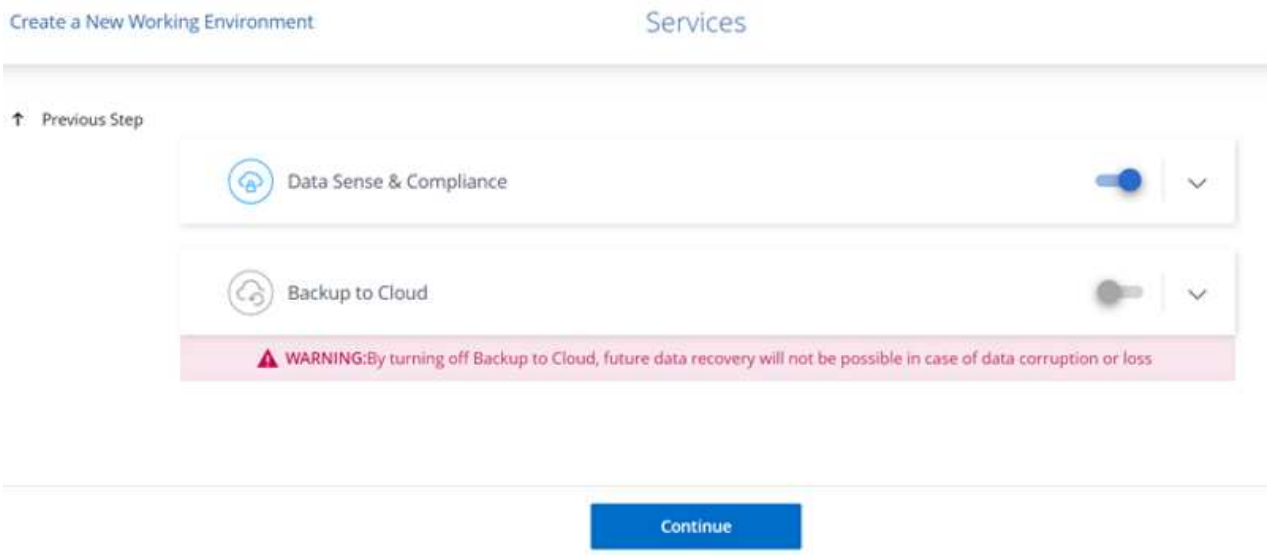


3. Geben Sie die Details zur zu erstellenden Umgebung an, einschließlich Name der Umgebung und Anmeldedaten des Administrators. Klicken Sie nach dem Abschluss auf Weiter.

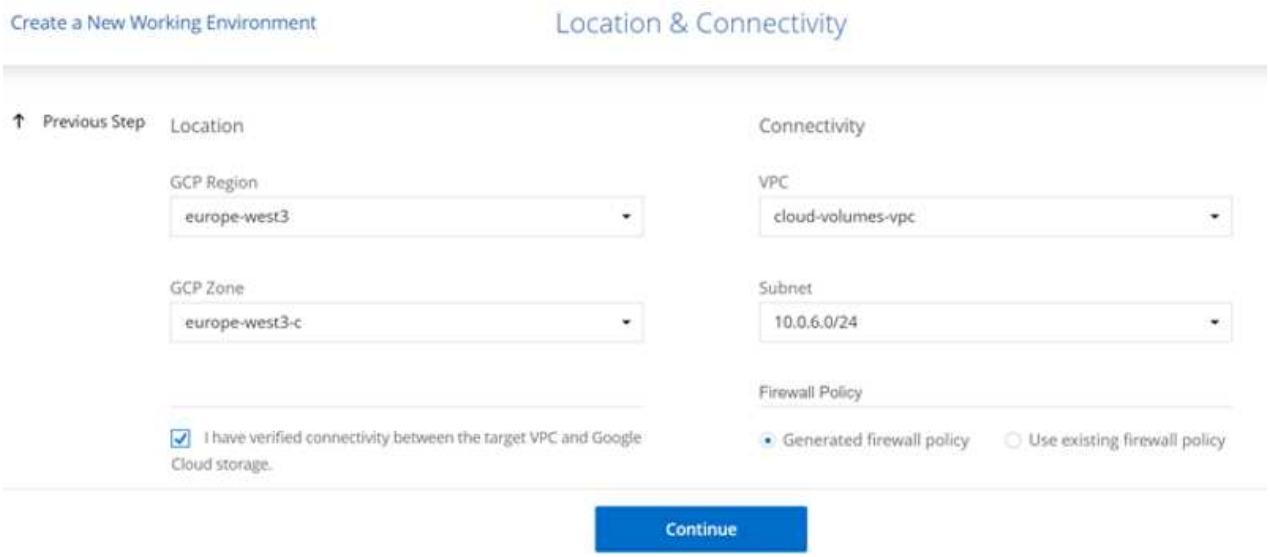


4. Wählen Sie die Add-on-Services für die Cloud Volumes ONTAP-Bereitstellung aus, einschließlich Data Sense & Compliance oder Backup in der Cloud. Klicken Sie anschließend auf Weiter.

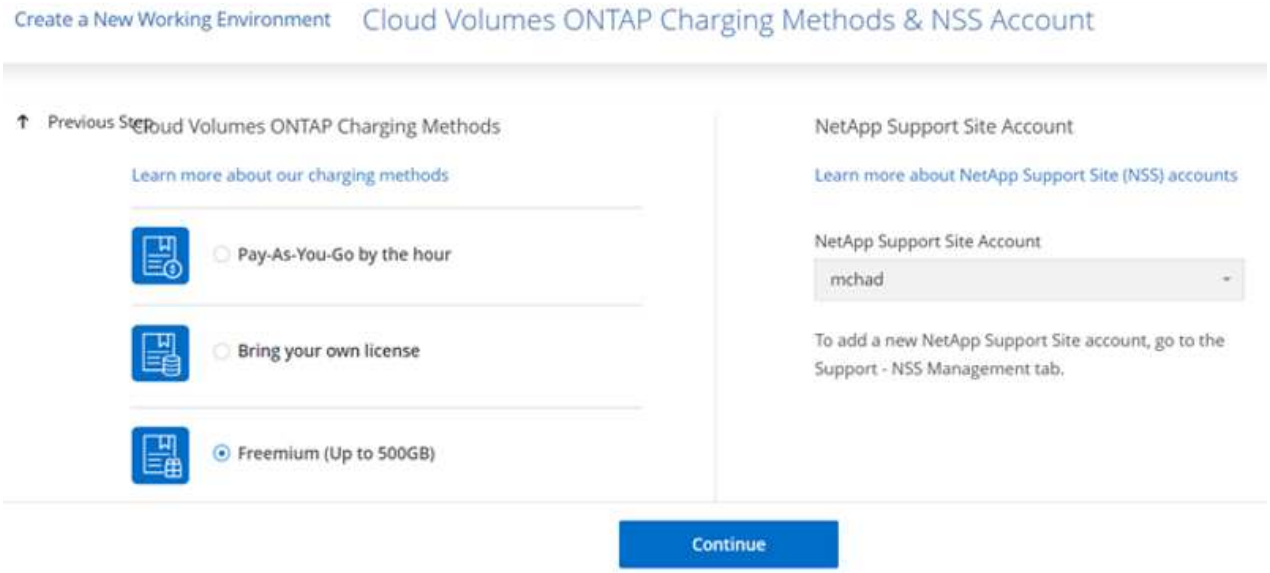
   HINWEIS: Beim Deaktivieren von Add-On-Diensten wird eine Pop-up-Meldung zur Überprüfung angezeigt. Add-on-Services können nach der CVO-Implementierung hinzugefügt/entfernt werden. Ziehen Sie in Erwägung, diese Services von Anfang an zu deaktivieren, wenn sie nicht benötigt werden, um Kosten zu vermeiden.



5. Wählen Sie einen Speicherort aus, wählen Sie eine Firewallrichtlinie aus und aktivieren Sie das Kontrollkästchen, um die Netzwerkverbindung zu Google Cloud Storage zu bestätigen.

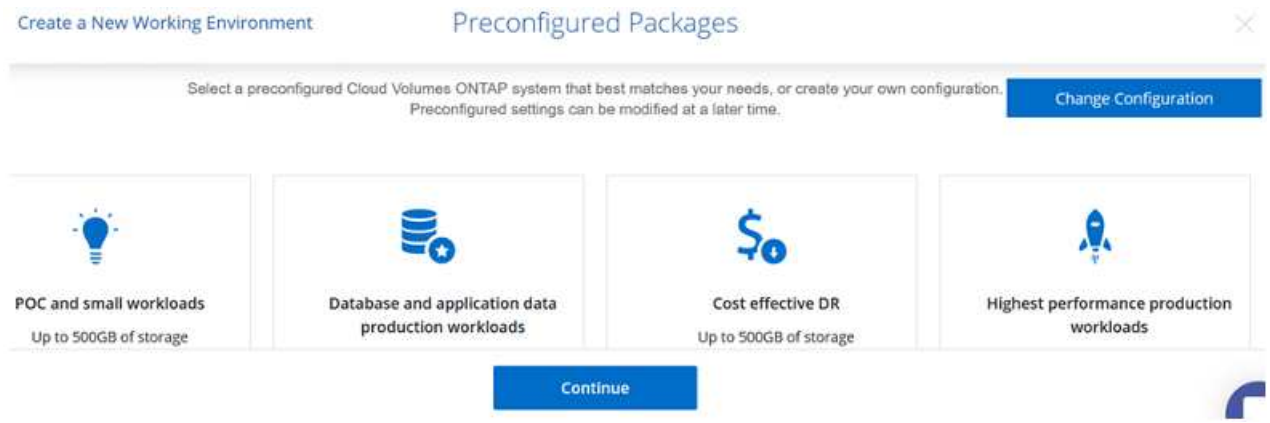


6. Wählen Sie die Lizenzoption: Pay-as-you-Go oder BYOL für die Nutzung vorhandener Lizenz. In diesem Beispiel wird die Freimium-Option verwendet. Klicken Sie anschließend auf Weiter.

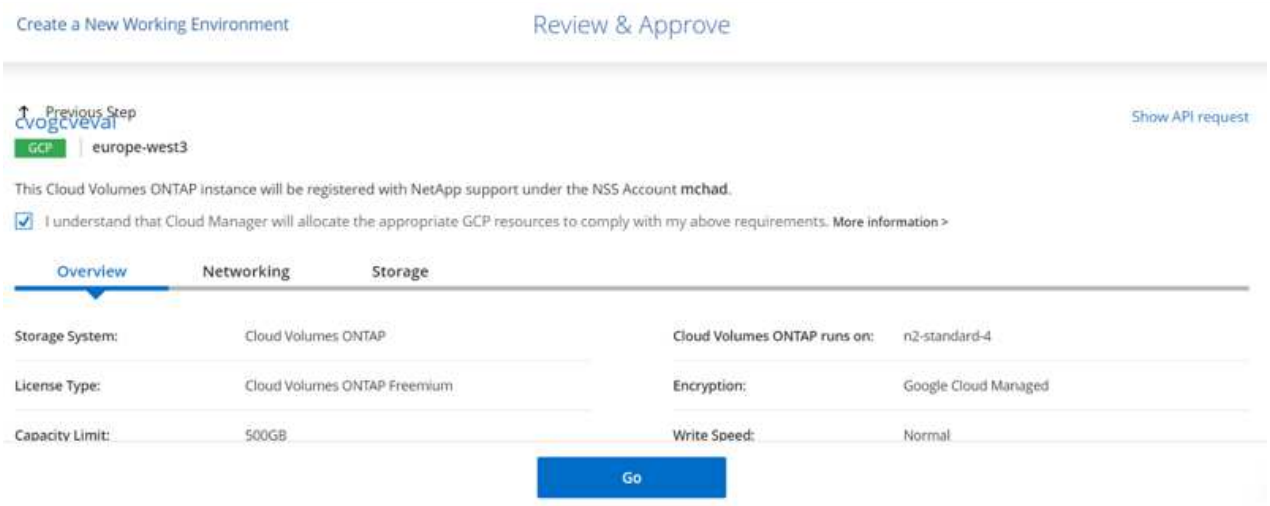


7. Wählen Sie zwischen mehreren vorkonfigurierten Paketen, die auf Grundlage des Workload-Typs verfügbar sind, die auf den VMs implementiert werden, die auf der VMware Cloud auf dem AWS SDDC ausgeführt werden.

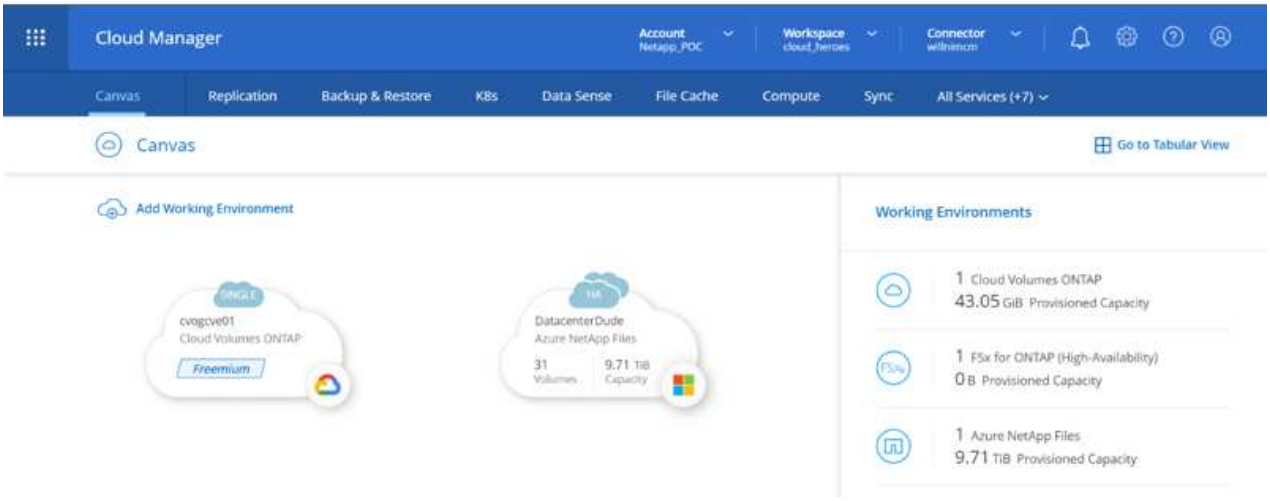
   HINWEIS: Ziehen Sie Ihre Maus über die Kacheln, um Details zu erhalten, oder passen Sie die CVO-Komponenten und die ONTAP-Version an, indem Sie auf Konfiguration ändern klicken.



8. Prüfen und bestätigen Sie die Auswahl auf der Seite Prüfen & Genehmigen.zum Erstellen der Cloud Volumes ONTAP-Instanz klicken Sie auf Los.



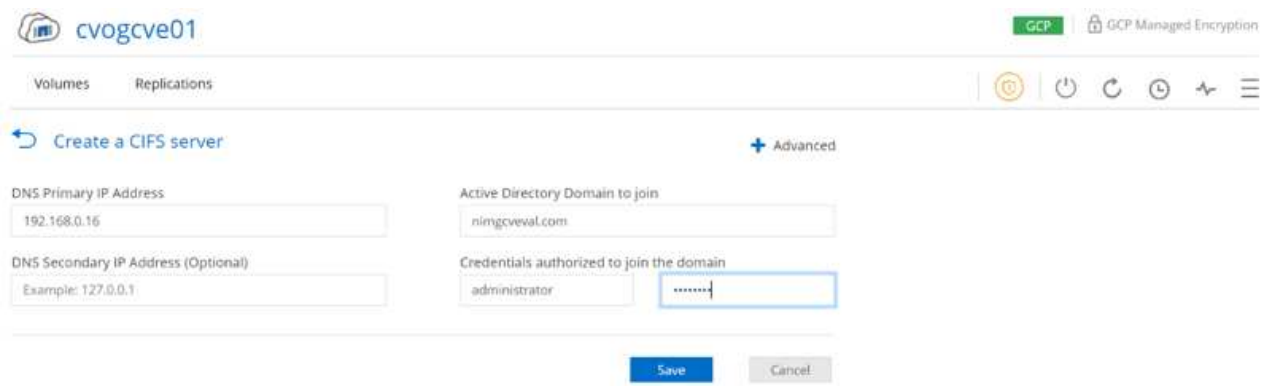
9. Nach der Bereitstellung von Cloud Volumes ONTAP wird es in den Arbeitsumgebungen auf der Seite Arbeitsfläche aufgelistet.



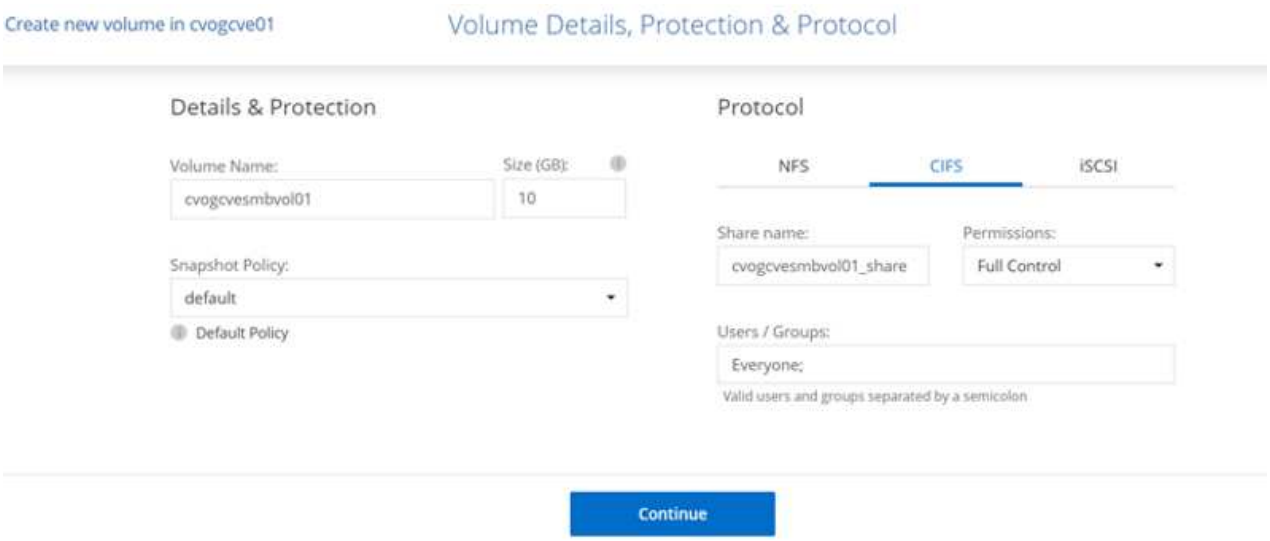
Zusätzliche Konfigurationen für SMB Volumes

1. Stellen Sie nach der Arbeitsumgebung sicher, dass der CIFS-Server mit den entsprechenden DNS- und Active Directory-Konfigurationsparametern konfiguriert ist. Dieser Schritt ist erforderlich, bevor Sie das SMB-Volume erstellen können.

   HINWEIS: Klicken Sie auf das Menü-Symbol (º), wählen Sie Erweitert, um weitere Optionen anzuzeigen, und wählen Sie CIFS-Setup.



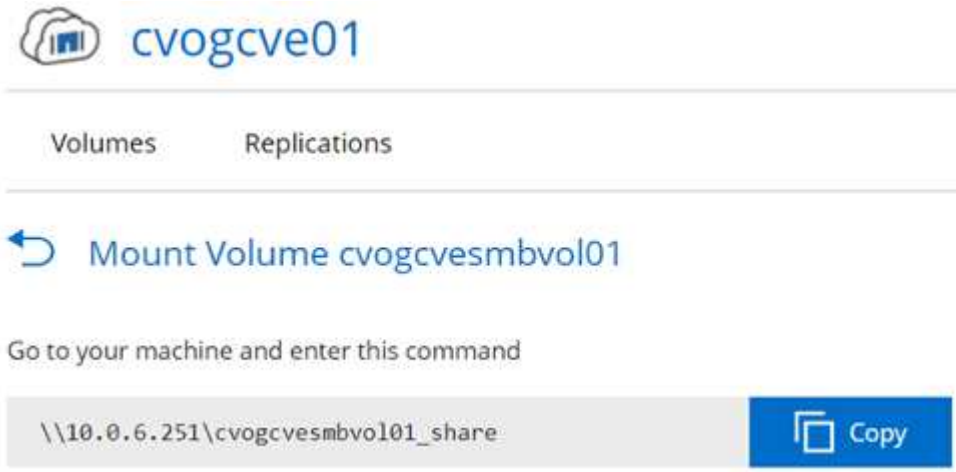
2. Das Erstellen des SMB Volume ist einfach. Doppelklicken Sie auf Canvas auf die Cloud Volumes ONTAP-Arbeitsumgebung, um Volumes zu erstellen und zu verwalten, und klicken Sie auf die Option „Volume erstellen“. Wählen Sie die entsprechende Größe und Cloud Manager wählt das Aggregat aus, das Sie enthalten, oder verwenden Sie den erweiterten Zuweisungsmechanismus auf einem bestimmten Aggregat. Für diese Demo wird CIFS/SMB als Protokoll ausgewählt.



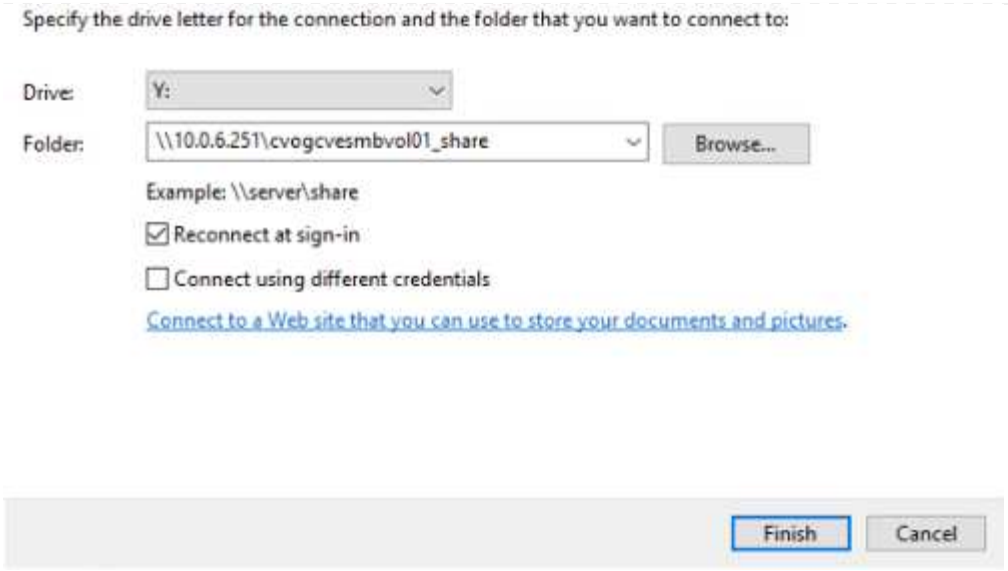
3. Nachdem das Volume bereitgestellt wurde, wird es unter dem Fensterbereich Volumes verfügbar sein. Da eine CIFS-Freigabe bereitgestellt wird, geben Sie Ihren Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner und überprüfen Sie, ob diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können. Dieser Schritt ist nicht erforderlich, wenn das Volume aus einer lokalen Umgebung repliziert wird, da die Datei- und Ordnerberechtigungen im Rahmen der SnapMirror Replizierung beibehalten werden.

   TIPP: Klicken Sie auf das Menü Volume (º), um seine Optionen anzuzeigen.

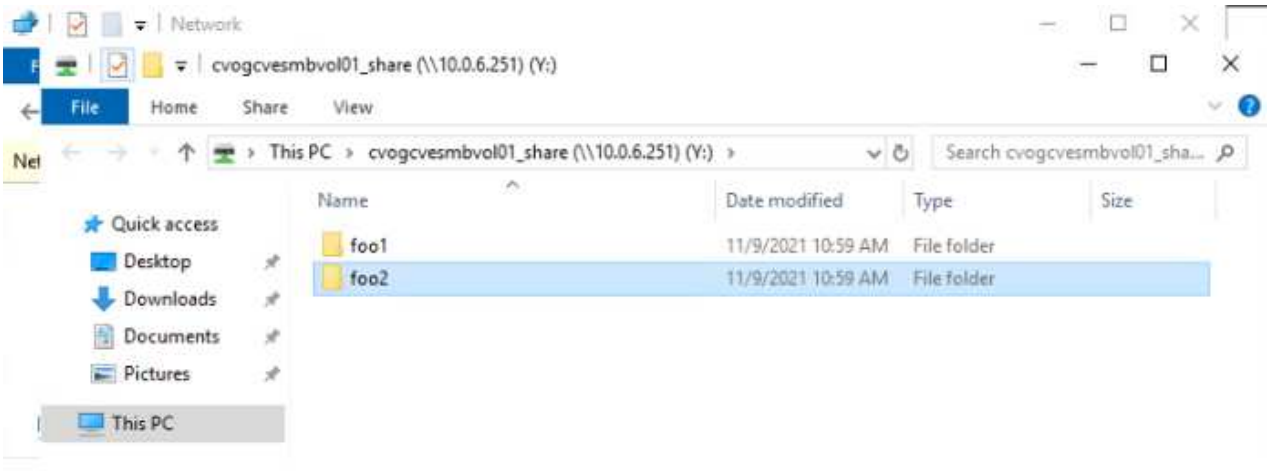
4. Nach der Erstellung des Volumes zeigen Sie mit dem Befehl Mount die Anweisungen zur Volume-Verbindung an und stellen dann eine Verbindung mit der Freigabe von den VMs auf der Google Cloud VMware Engine her.



5. Kopieren Sie den folgenden Pfad und verwenden Sie die Option Netzlaufwerk zuordnen, um das Volume auf der VM zu mounten, die auf der Google Cloud VMware Engine ausgeführt wird.



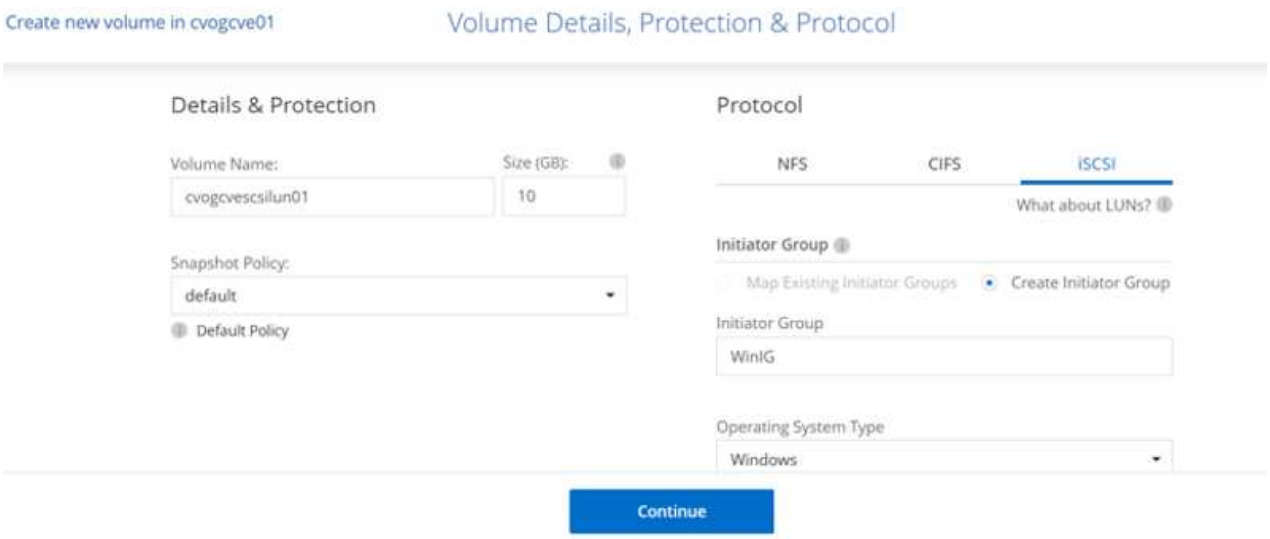
Nach dem Mapping kann man leicht darauf zugreifen, und die NTFS-Berechtigungen können entsprechend eingestellt werden.

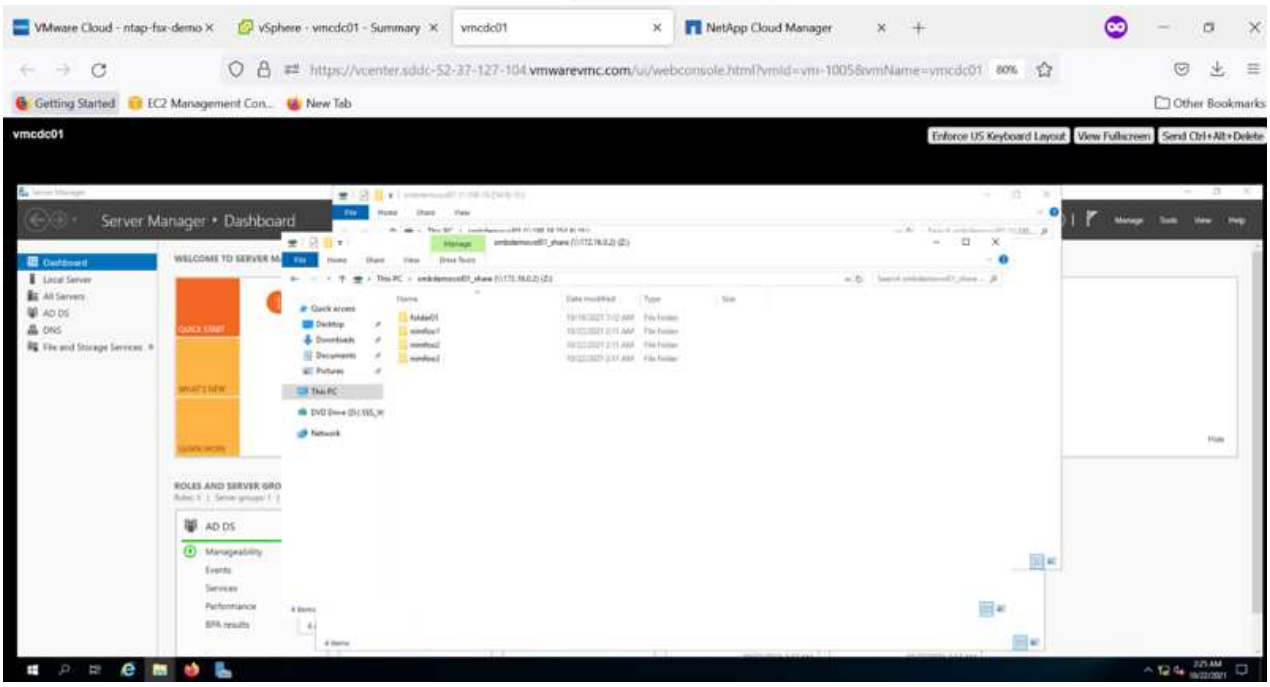


Verbinden Sie die LUN auf Cloud Volumes ONTAP mit einem Host

Führen Sie die folgenden Schritte aus, um die Cloud Volumes ONTAP-LUN mit einem Host zu verbinden:

1. Doppelklicken Sie auf der Seite Arbeitsfläche von Cloud Volumes ONTAP auf die Arbeitsumgebung, um Volumes zu erstellen und zu verwalten.
2. Klicken Sie auf Volume hinzufügen > Neues Volume, und wählen Sie iSCSI aus, und klicken Sie auf Initiatorgruppe erstellen. Klicken Sie auf Weiter .





3. Nachdem das Volume bereitgestellt wurde, wählen Sie das Menü Volume (º) aus, und klicken Sie dann auf Ziel-IQN. Um den iSCSI-qualifizierten Namen (IQN) zu kopieren, klicken Sie auf Kopieren. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.

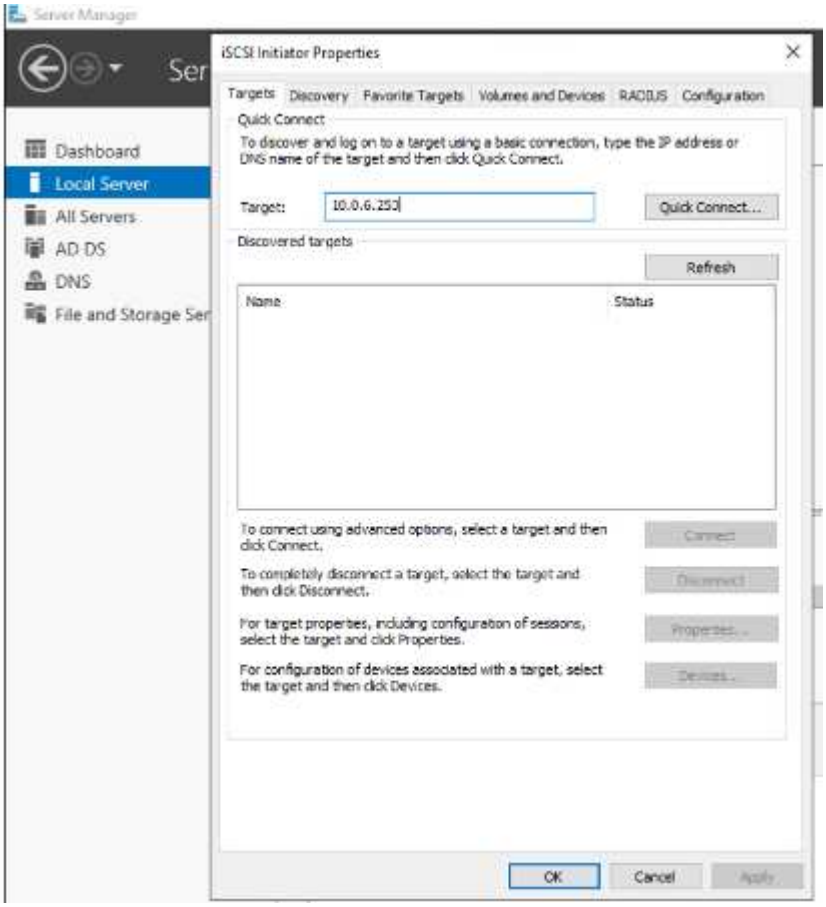
Für den Host, der sich auf der Google Cloud VMware Engine befindet, gilt dasselbe:

1. RDP auf die VM gehostet auf Google Cloud VMware Engine.
2. Öffnen Sie das Dialogfeld iSCSI-Initiator-Eigenschaften: Server Manager > Dashboard > Tools >

iSCSI-Initiator.

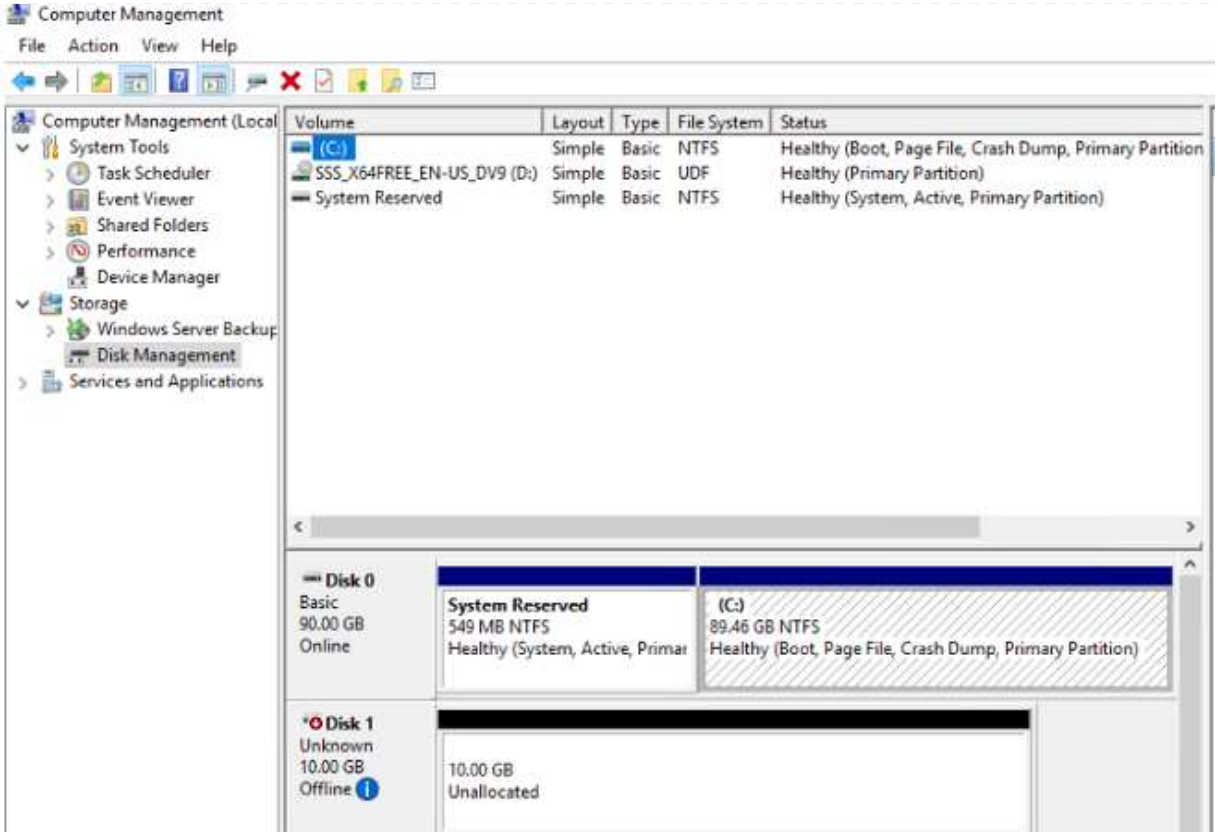
3. Klicken Sie auf der Registerkarte Ermittlung auf Portal erkennen oder Portal hinzufügen, und geben Sie dann die IP-Adresse des iSCSI-Zielports ein.
4. Wählen Sie auf der Registerkarte Ziele das erkannte Ziel aus und klicken Sie dann auf Anmelden oder Verbinden.
5. Wählen Sie Multipath aktivieren, und wählen Sie dann automatisch Diese Verbindung wiederherstellen, wenn der Computer startet oder diese Verbindung zur Liste der bevorzugten Ziele hinzufügen. Klicken Sie Auf Erweitert.

> Der Windows-Host muss über eine iSCSI-Verbindung zu jedem Knoten im Cluster verfügen. Das native DSM wählt die besten Pfade aus.



LUNs auf Storage Virtual Machine (SVM) werden dem Windows Host als Festplatten angezeigt. Neue hinzugefügte Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen Rescan aus, um die Festplatten zu ermitteln, indem Sie die folgenden Schritte ausführen:

a. Öffnen Sie das Dienstprogramm Windows Computer Management: Start > Verwaltung > Computerverwaltung.
b. Erweitern Sie den Knoten Speicher in der Navigationsstruktur.
c. Klicken Sie Auf Datenträgerverwaltung.
d. Klicken Sie Auf Aktion > Datenträger Erneut Scannen.

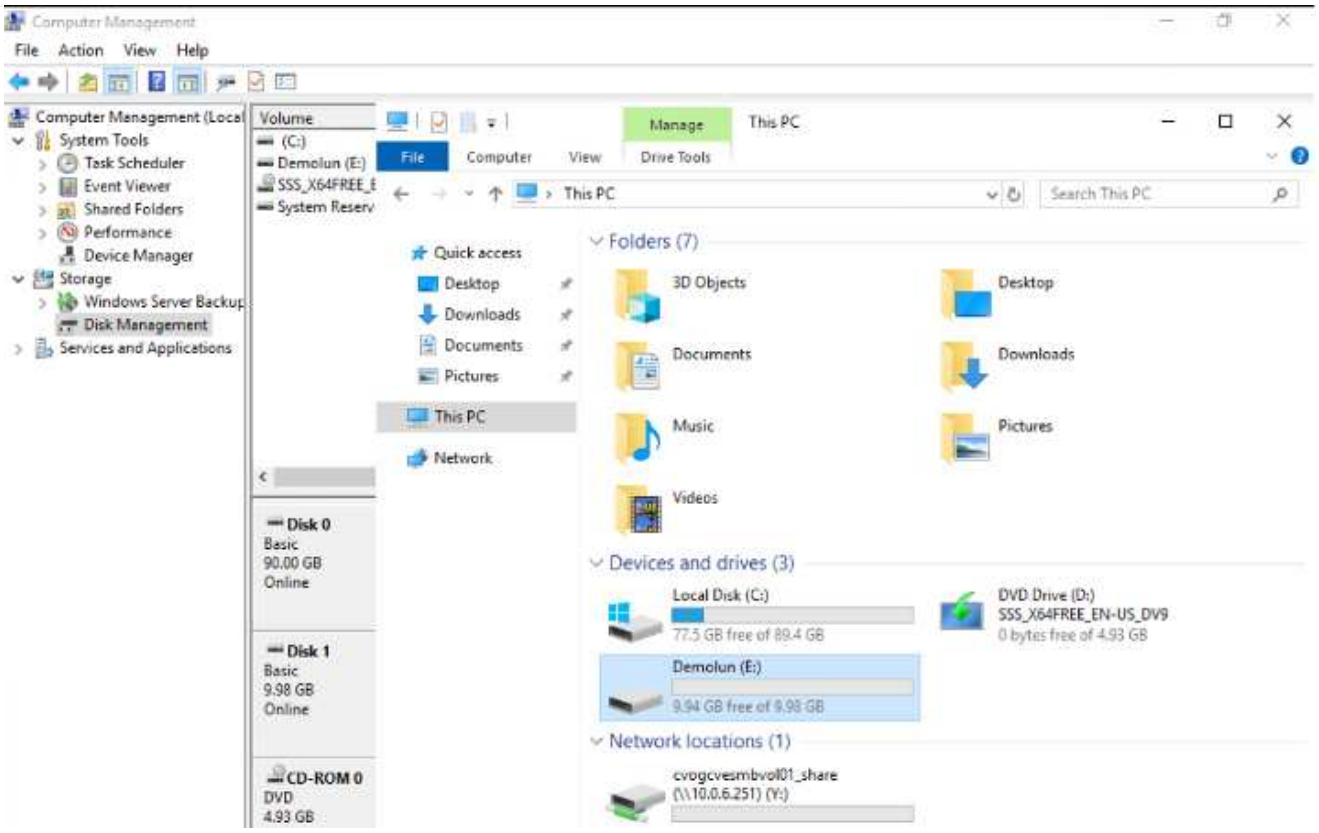


Wenn der Windows-Host zum ersten Mal auf eine neue LUN zugreift, hat sie keine Partition oder kein Dateisystem. Initialisieren Sie die LUN; und optional formatieren Sie die LUN mit einem Dateisystem, indem Sie die folgenden Schritte durchführen:

a. Starten Sie Windows Disk Management.

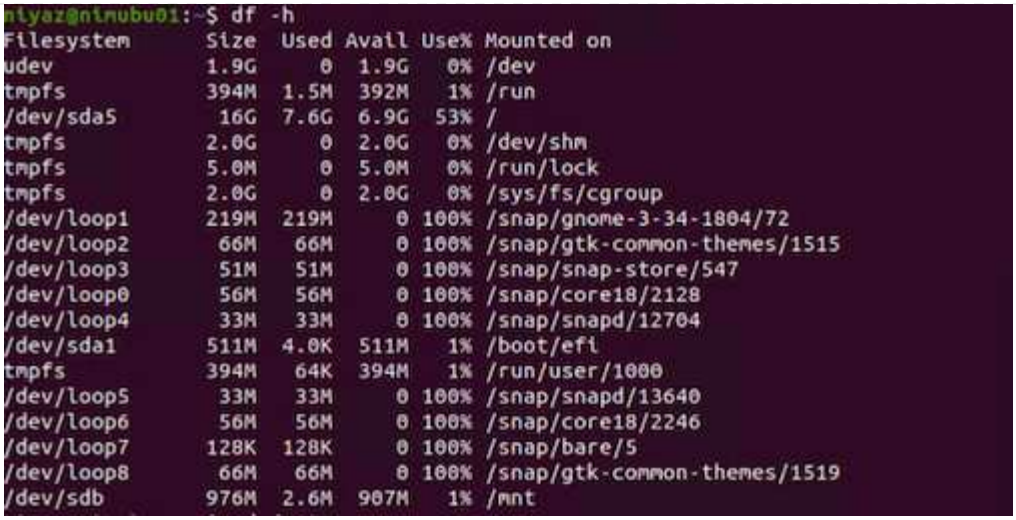
b. Klicken Sie mit der rechten Maustaste auf die LUN, und wählen Sie dann den erforderlichen Festplatten- oder Partitionstyp aus.

c. Befolgen Sie die Anweisungen im Assistenten. In diesem Beispiel ist Laufwerk F: Angehängt.



Stellen Sie auf den Linux-Clients sicher, dass der iSCSI-Daemon ausgeführt wird. Sobald die LUNs bereitgestellt sind, lesen Sie als Beispiel hier die detaillierte Anleitung zur iSCSI-Konfiguration mit Ubuntu. Führen Sie zur Überprüfung lsblk cmd aus der Shell aus.

```
niyaz@nimubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

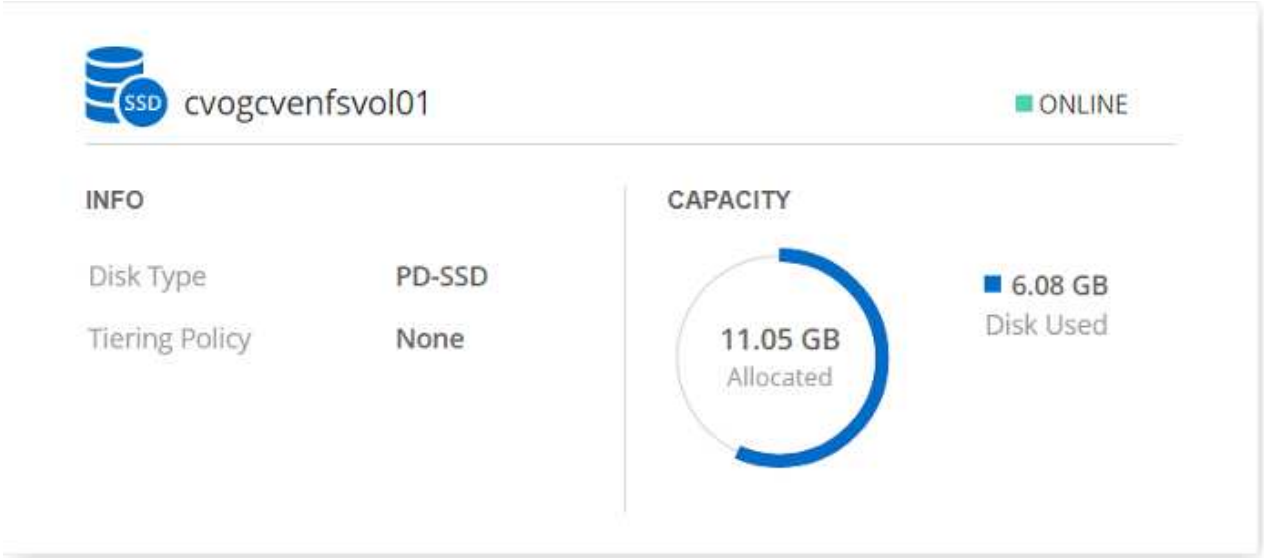

niyaz@ninubu01:~$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 1.9G 0 1.9G 0% /dev
tmpfs 394M 1.5M 392M 1% /run
/dev/sda5 16G 7.6G 6.9G 53% /
tmpfs 2.0G 0 2.0G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/loop1 219M 219M 0 100% /snap/gnome-3-34-1804/72
/dev/loop2 66M 66M 0 100% /snap/gtk-common-themes/1515
/dev/loop3 51M 51M 0 100% /snap/snap-store/547
/dev/loop0 56M 56M 0 100% /snap/core18/2128
/dev/loop4 33M 33M 0 100% /snap/snapd/12704
/dev/sda1 511M 4.0K 511M 1% /boot/efi
tmpfs 394M 64K 394M 1% /run/user/1000
/dev/loop5 33M 33M 0 100% /snap/snapd/13640
/dev/loop6 56M 56M 0 100% /snap/core18/2246
/dev/loop7 128K 128K 0 100% /snap/bare/5
/dev/loop8 66M 66M 0 100% /snap/gtk-common-themes/1519
/dev/sdb 976M 2.6M 907M 1% /mnt

Mounten Sie das Cloud Volumes ONTAP NFS Volume auf dem Linux Client

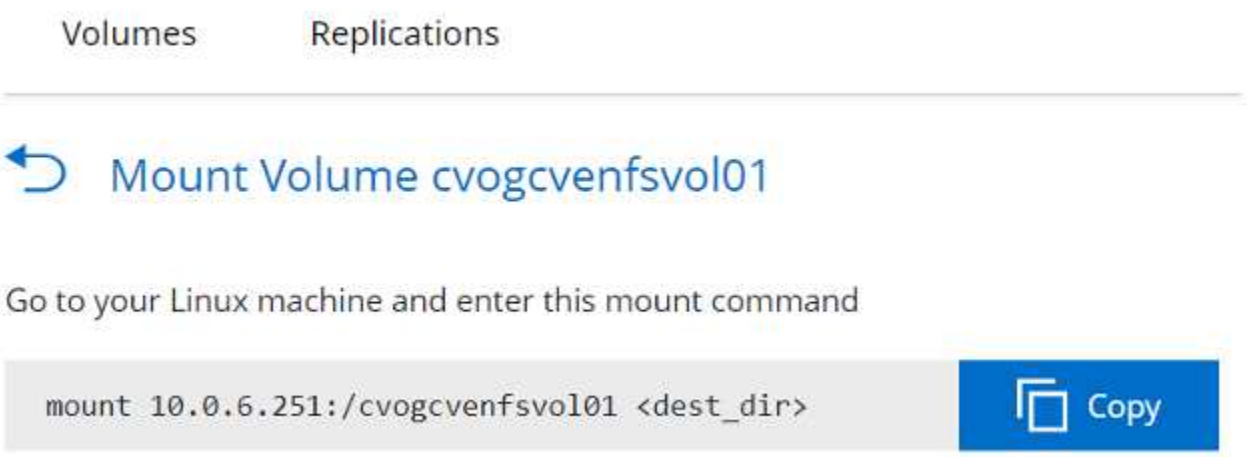
So mounten Sie das Cloud Volumes ONTAP-Dateisystem (DIY) von VMs in der Google Cloud VMware Engine:

Stellen Sie das Volume gemäß den nachstehenden Schritten bereit

1. Klicken Sie auf der Registerkarte Volumes auf Neues Volume erstellen .
2. Wählen Sie auf der Seite Neues Volume erstellen einen Volume-Typ aus:



3. Legen Sie auf der Registerkarte Volumes den Mauszeiger über die Lautstärke, wählen Sie das Menüsymbol (º) und klicken Sie dann auf Mount Command.



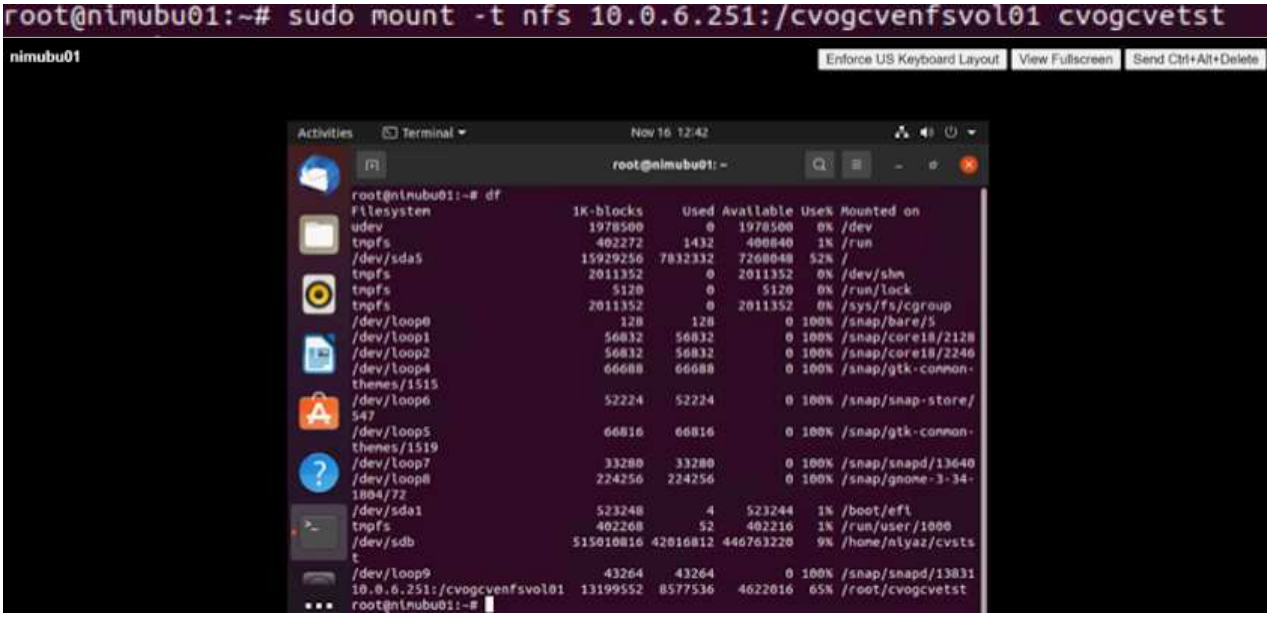
4. Klicken Sie auf Kopieren .
5. Stellen Sie eine Verbindung mit der angegebenen Linux-Instanz her.
6. Öffnen Sie ein Terminal auf der Instanz mithilfe von Secure Shell (SSH), und melden Sie sich mit den entsprechenden Anmeldedaten an.
7. Erstellen Sie mit dem folgenden Befehl ein Verzeichnis für den Mount-Punkt des Volumes.

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. Mounten Sie das Cloud Volumes ONTAP-NFS-Volume in das Verzeichnis, das im vorherigen Schritt erstellt wurde.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



Cloud Volumes Service (CVS)

Cloud Volumes Services (CVS) ist ein umfassendes Portfolio von Datenservices für erweiterte Cloud-Lösungen. Cloud Volumes Services unterstützt diverse Dateizugriffsprotokolle für wichtige Cloud-Provider (NFS- und SMB-Unterstützung).

Weitere Vorteile und Funktionen sind Datensicherung und -Wiederherstellung mit Snapshot, besondere Features für Replizierung, Synchronisierung und Migration von Datenzielen auf On-Premises- oder Cloud-Basis sowie eine konsistent hohe Performance auf dem Niveau eines dedizierten Flash-Storage-Systems.

Cloud Volumes Service (CVS) als Storage mit Gastverbunden

Konfiguration von Cloud Volumes Service mit der VMware Engine

Cloud Volumes Service Shares können von VMs gemountet werden, die in der VMware Engine Umgebung erstellt wurden. Die Volumes können auch auf dem Linux-Client eingebunden und auf dem Windows-Client zugeordnet werden, da Cloud Volumes Service SMB- und NFS-Protokolle unterstützt. Cloud Volumes Service Volumes lassen sich in einfachen Schritten einrichten.

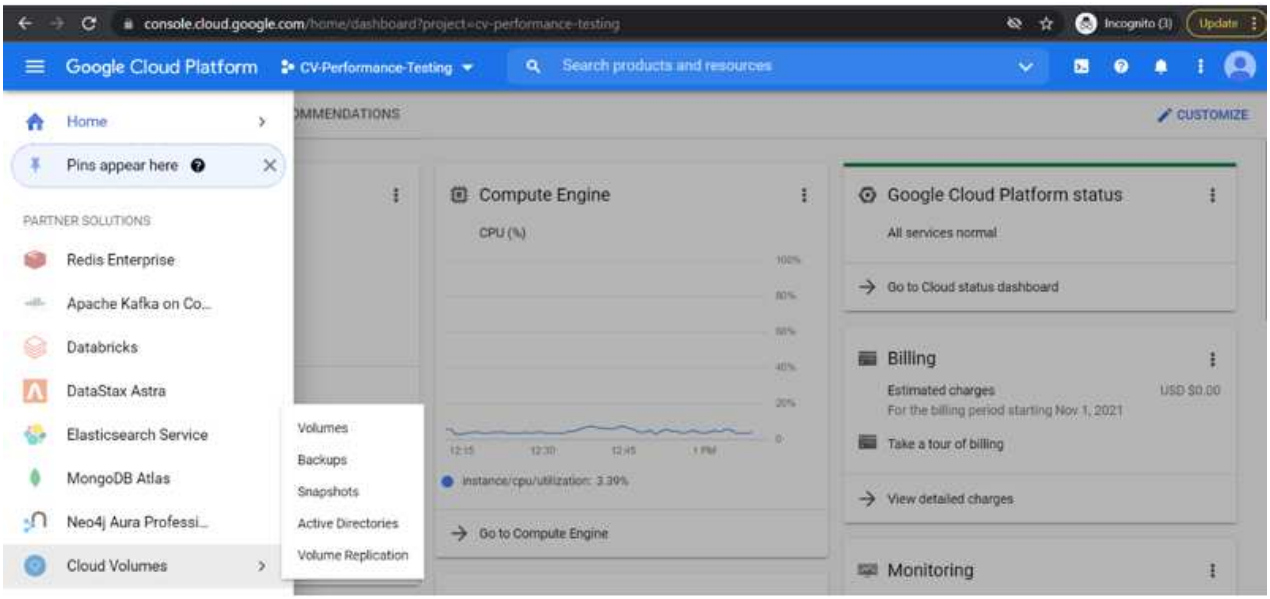
Cloud Volume Service und Google Cloud VMware Engine Private Cloud müssen sich in derselben Region befinden.

Im folgenden Dokument können Sie NetApp Cloud Volumes Service für Google Cloud über den Google Cloud Marketplace erwerben, aktivieren und konfigurieren "Begleiten".

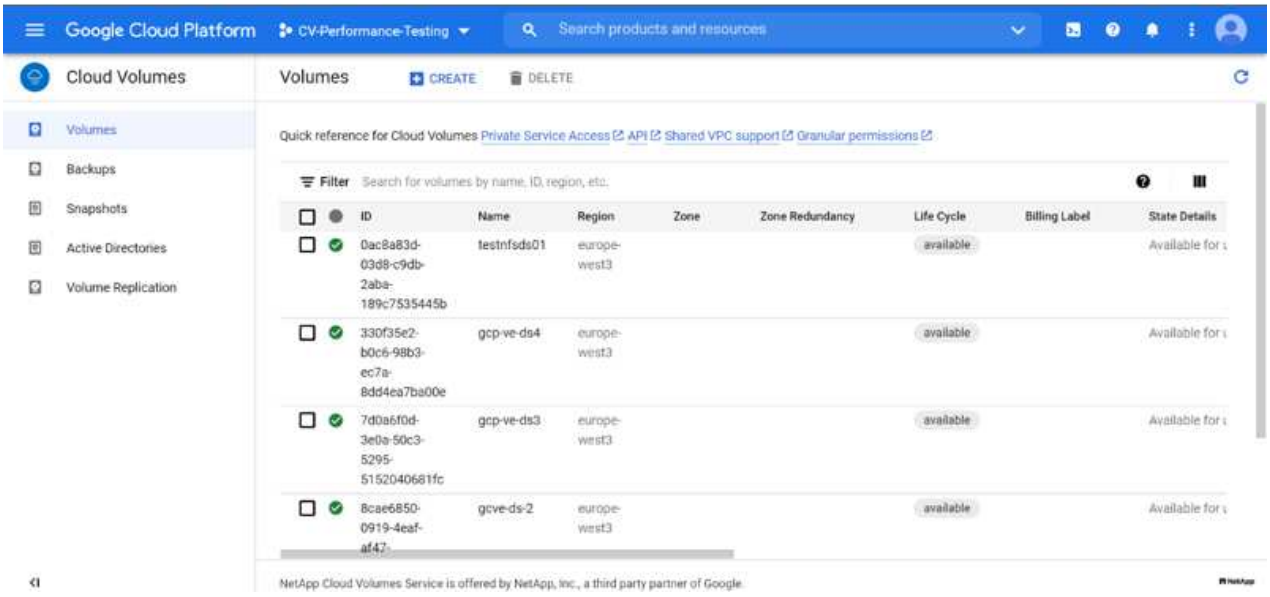
Erstellen eines CVS NFS-Volumes in die GCVE Private Cloud

Führen Sie folgende Schritte aus, um NFS-Volumes zu erstellen und einzubinden:

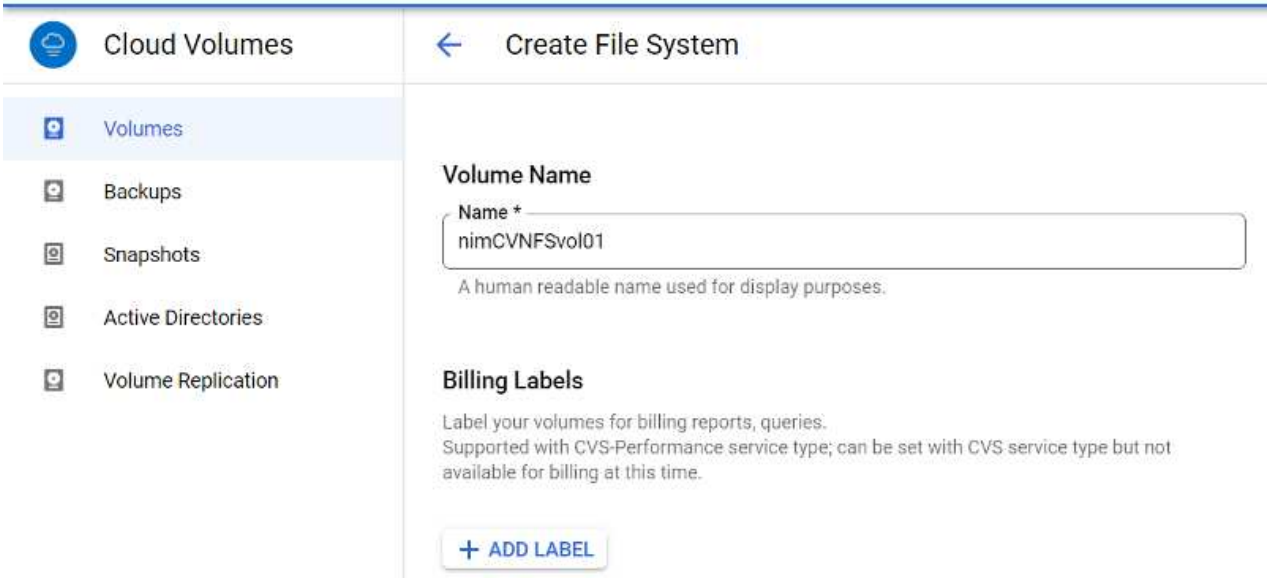
1. Zugriff auf Cloud Volumes über Partnerlösungen finden Sie über die Google Cloud-Konsole.



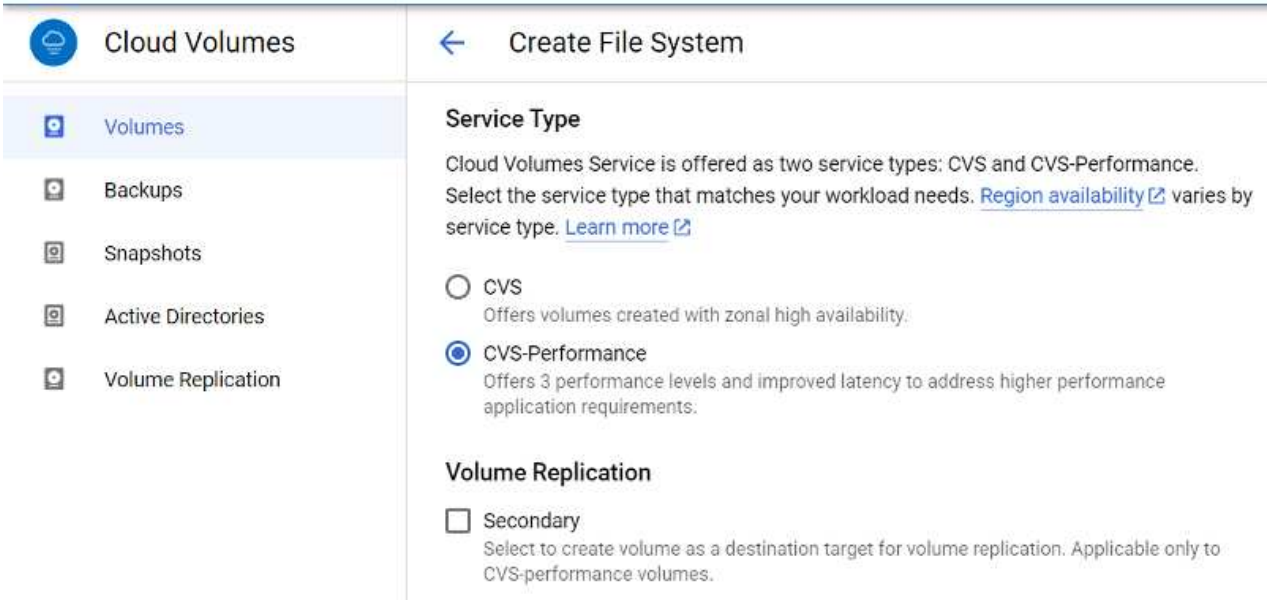
2. Rufen Sie in der Cloud Volumes Console die Seite Volumes auf und klicken Sie auf Erstellen.



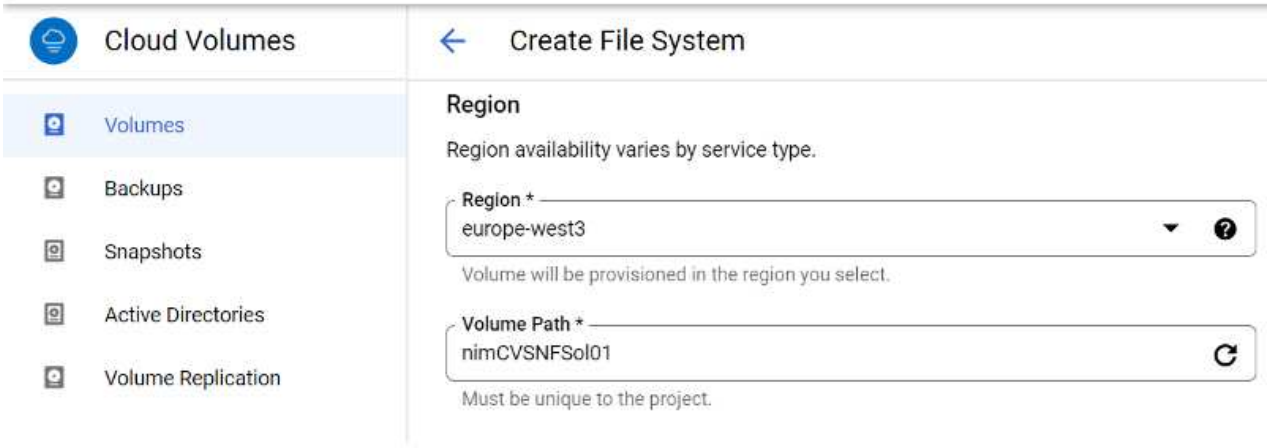
3. Geben Sie auf der Seite Create File System den Namen des Volumes und die Rechnungs-Labels an, die für Chargeback-Mechanismen erforderlich sind.



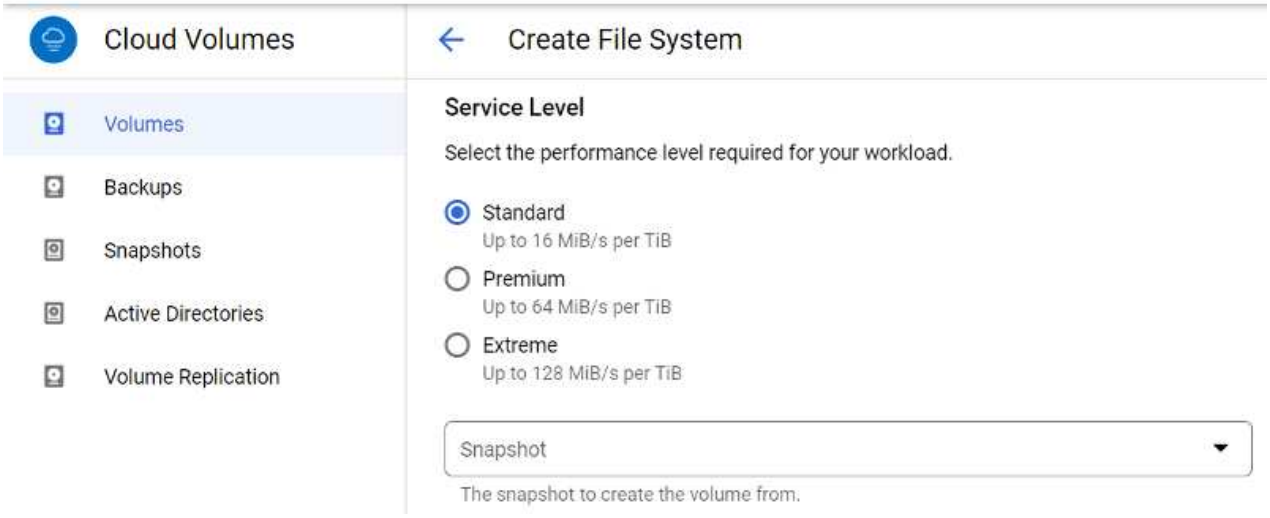
4. Wählen Sie den entsprechenden Service aus. Wählen Sie für GCVE CVS-Performance und das gewünschte Service-Level aus, um basierend auf den Applikations-Workload-Anforderungen die Latenz und eine höhere Performance zu verbessern.



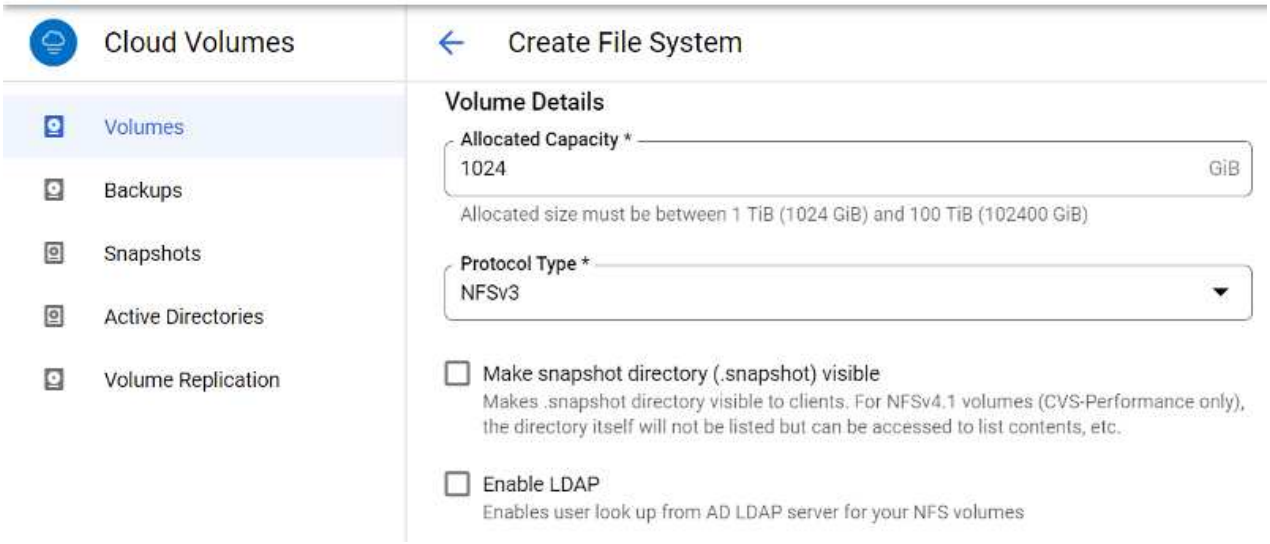
5. Legen Sie die Google Cloud-Region für den Volume- und Volume-Pfad fest (der Volume-Pfad muss für alle Cloud Volumes im Projekt eindeutig sein).



6. Wählen Sie das Performance-Level für das Volume aus.

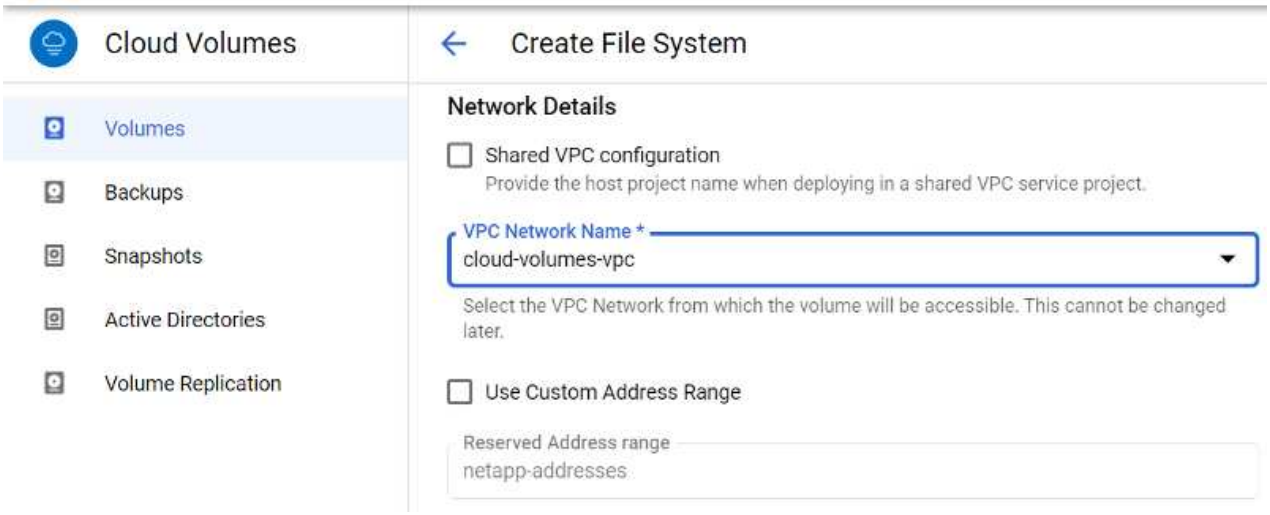


7. Geben Sie die Größe des Volume und den Protokolltyp an. In diesem Test wird NFSv3 verwendet.



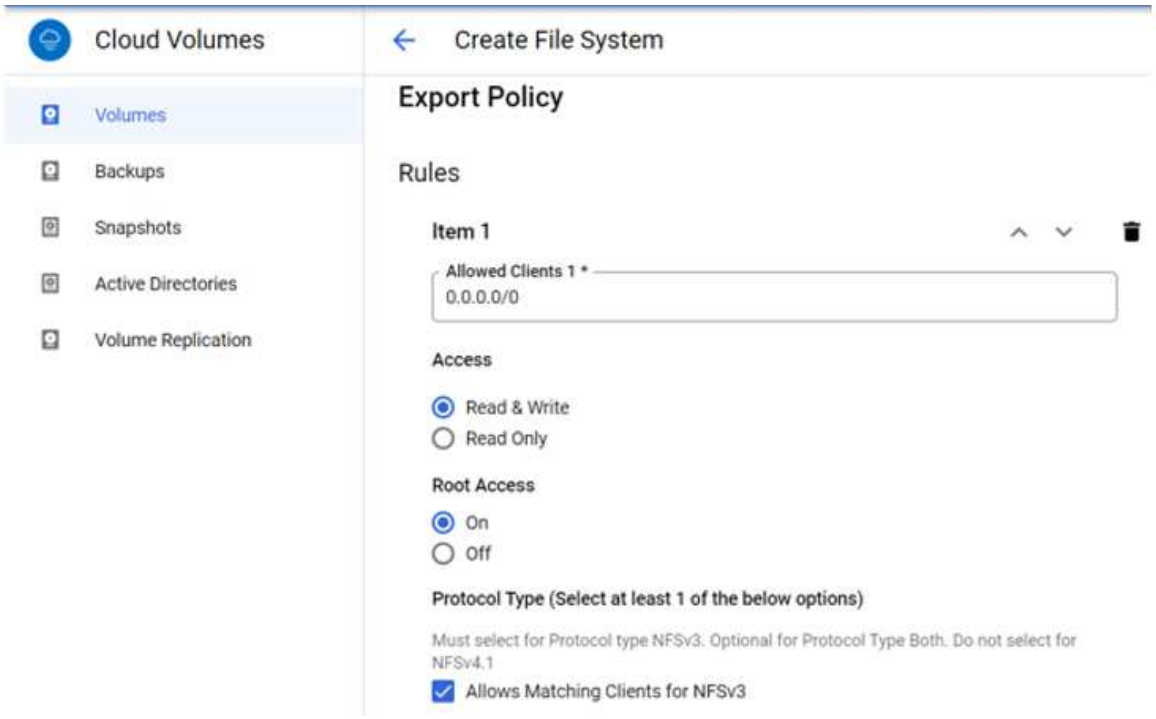
8. In diesem Schritt wählen Sie das VPC-Netzwerk aus, auf das das Volume zugegriffen werden soll. VPC-Peering sicherstellen.

HINWEIS: Falls VPC-Peering nicht durchgeführt wurde, wird ein Pop-up-Button angezeigt, der Sie durch die Peering-Befehle leitet. Öffnen Sie eine Cloud-Shell-Sitzung und führen Sie die entsprechenden Befehle aus, um mit Cloud Volumes Service Producer Ihre VPC zu tauschen. Falls Sie sich dazu entschließen, das VPC-Peering vorab vorzubereiten, lesen Sie diese Anweisungen.



9. Managen Sie die Exportrichtlinien, indem Sie die entsprechenden Regeln hinzufügen, und aktivieren Sie das Kontrollkästchen für die entsprechende NFS-Version.

   Hinweis: Der Zugriff auf NFS-Volumes ist erst möglich, wenn eine Exportrichtlinie hinzugefügt wird.



10. Klicken Sie auf Speichern, um das Volume zu erstellen.

Mounten von NFS-Exporten auf VMs, die auf der VMware Engine ausgeführt werden

Stellen Sie vor dem Bereitstellen des NFS-Volumes sicher, dass der Peering-Status der privaten Verbindung als aktiv aufgeführt ist. Sobald der Status „aktiv“ lautet, verwenden Sie den Befehl „Mount“.

Gehen Sie zum Mounten eines NFS-Volumes wie folgt vor:

1. Wechseln Sie in der Cloud Console zu Cloud Volumes > Volumes.
2. Wechseln Sie zur Seite Volumes
3. Klicken Sie auf das NFS-Volumen, für das Sie NFS-Exporte mounten möchten.
4. Scrollen Sie nach rechts unter Mehr anzeigen auf Mount Instructions.

So führen Sie den Montageprozess innerhalb des Gastbetriebssystems der VMware VM aus:

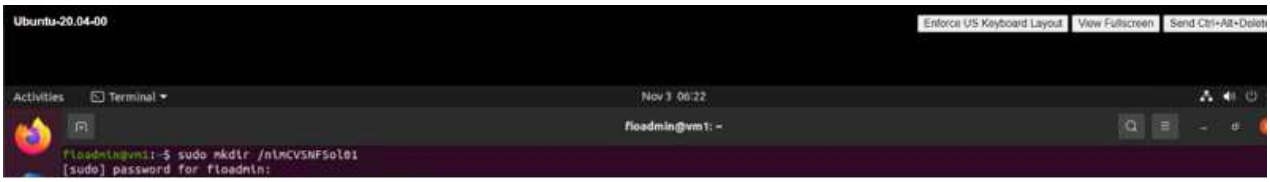
1. Verwenden Sie SSH Client und SSH für die virtuelle Maschine.
2. installieren Sie den nfs-Client auf der Instanz.
   a. Auf Red hat Enterprise Linux oder SUSE Linux-Instanz:

```
 sudo yum install -y nfs-utils
.. Auf einer Ubuntu oder Debian-Instanz:
```

```
sudo apt-get install nfs-common
```

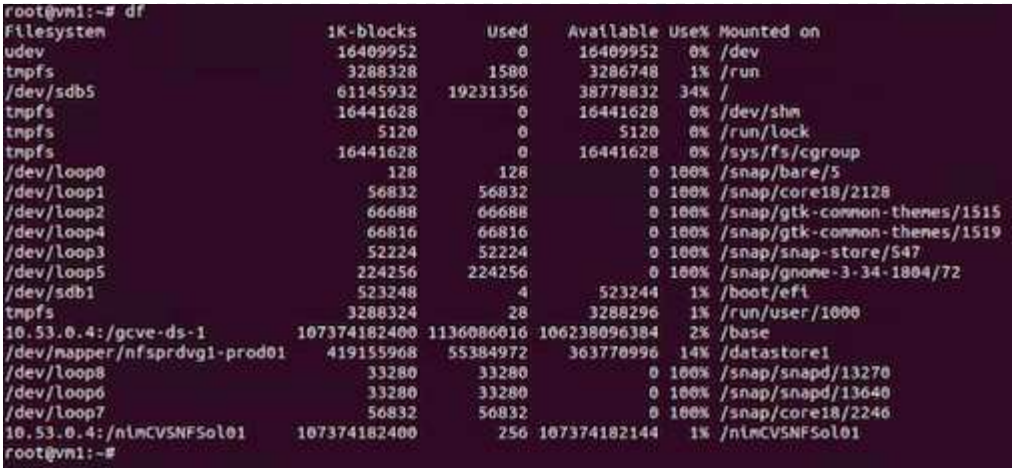
3. Erstellen Sie ein neues Verzeichnis auf der Instanz, z. B. „/nimCVSNFSol01“:

```
sudo mkdir /nimCVSNFSol01
```



4. Mounten Sie den Volume mit dem entsprechenden Befehl. Beispiel-Befehl aus dem Labor ist unten:

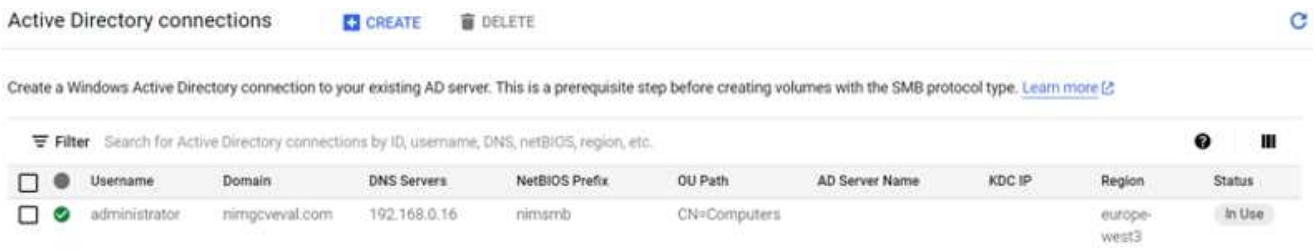
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     38778832  34% /
tmpfs                           16441628           0     16441628   0% /dev/shm
tmpfs                               5120           0         5120   0% /run/lock
tmpfs                           16441628           0     16441628   0% /sys/fs/cgroup
/dev/loop0                            128         128            0 100% /snap/bare/5
/dev/loop1                          56832       56832            0 100% /snap/core18/2128
/dev/loop2                          66688       66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                          66816       66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                          52224       52224            0 100% /snap/snap-store/547
/dev/loop5                         224256      224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                          523248           4       523244   1% /boot/efi
tmpfs                             3288324          28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1          107374182400  1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01    419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nlmCVSNFSol01      107374182400         256 107374182144   1% /nlmCVSNFSol01
root@vm1:~#
```

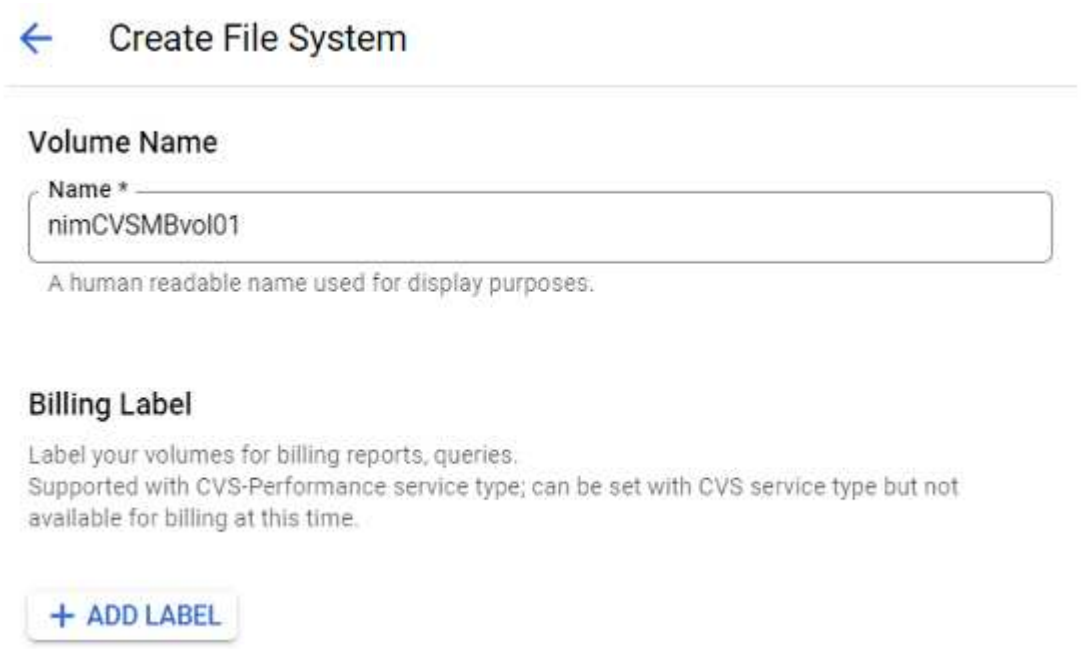
Erstellen und Mounten von SMB-Share an VMs, die auf VMware Engine ausgeführt werden

Vergewissern Sie sich bei SMB-Volumes, dass die Active Directory-Verbindungen vor dem Erstellen des SMB-Volume konfiguriert sind.

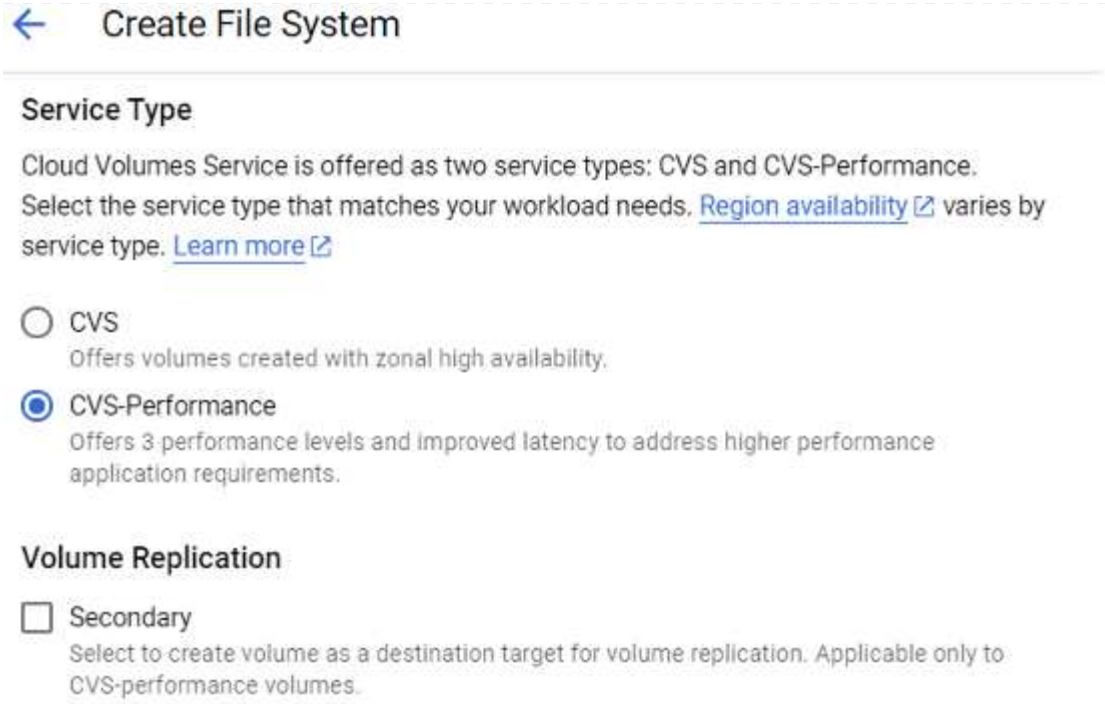


Sobald die AD-Verbindung hergestellt ist, erstellen Sie das Volume mit dem gewünschten Service-Level. Die Schritte sind wie die Erstellung eines NFS-Volume, außer Auswahl des entsprechenden Protokolls.

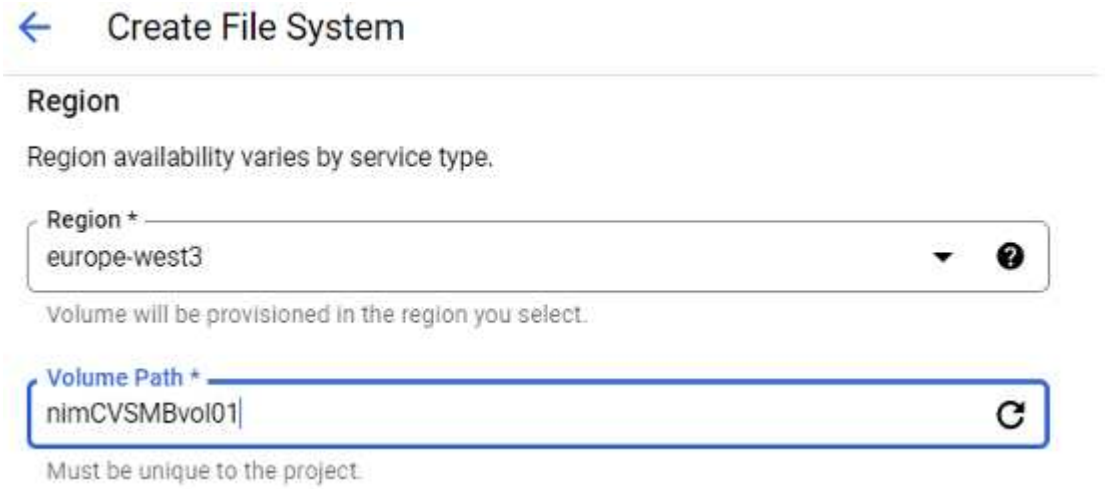
1. Rufen Sie in der Cloud Volumes Console die Seite Volumes auf und klicken Sie auf Erstellen.
2. Geben Sie auf der Seite Create File System den Namen des Volumes und die Rechnungs-Labels an, die für Chargeback-Mechanismen erforderlich sind.



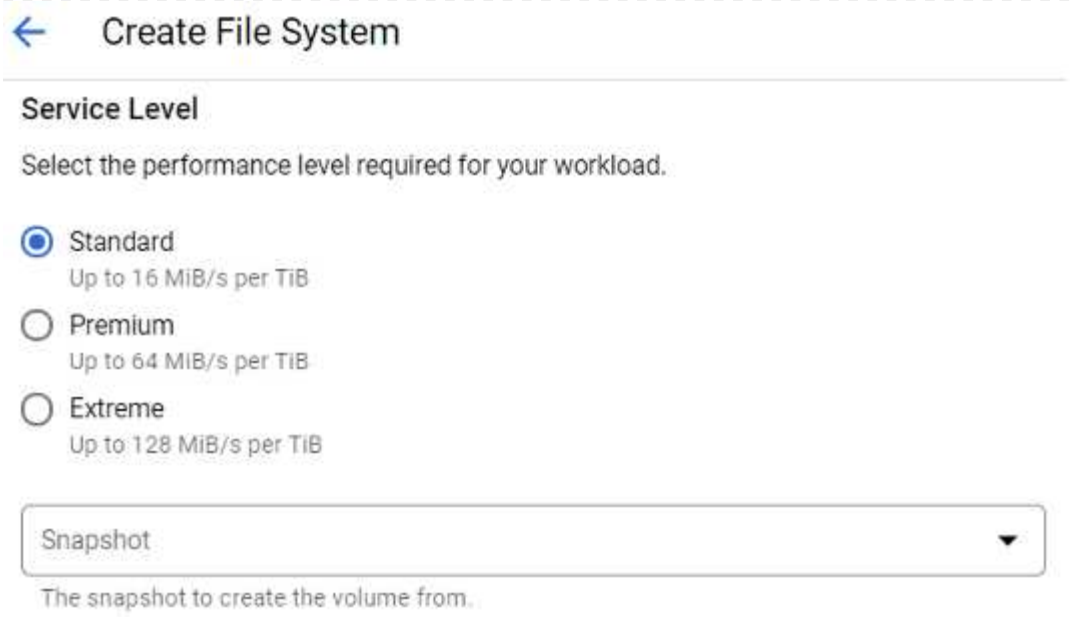
3. Wählen Sie den entsprechenden Service aus. Wählen Sie für GCVE CVS-Performance und den gewünschten Service Level aus, um basierend auf den Workload-Anforderungen die Latenz und eine höhere Performance zu verbessern.



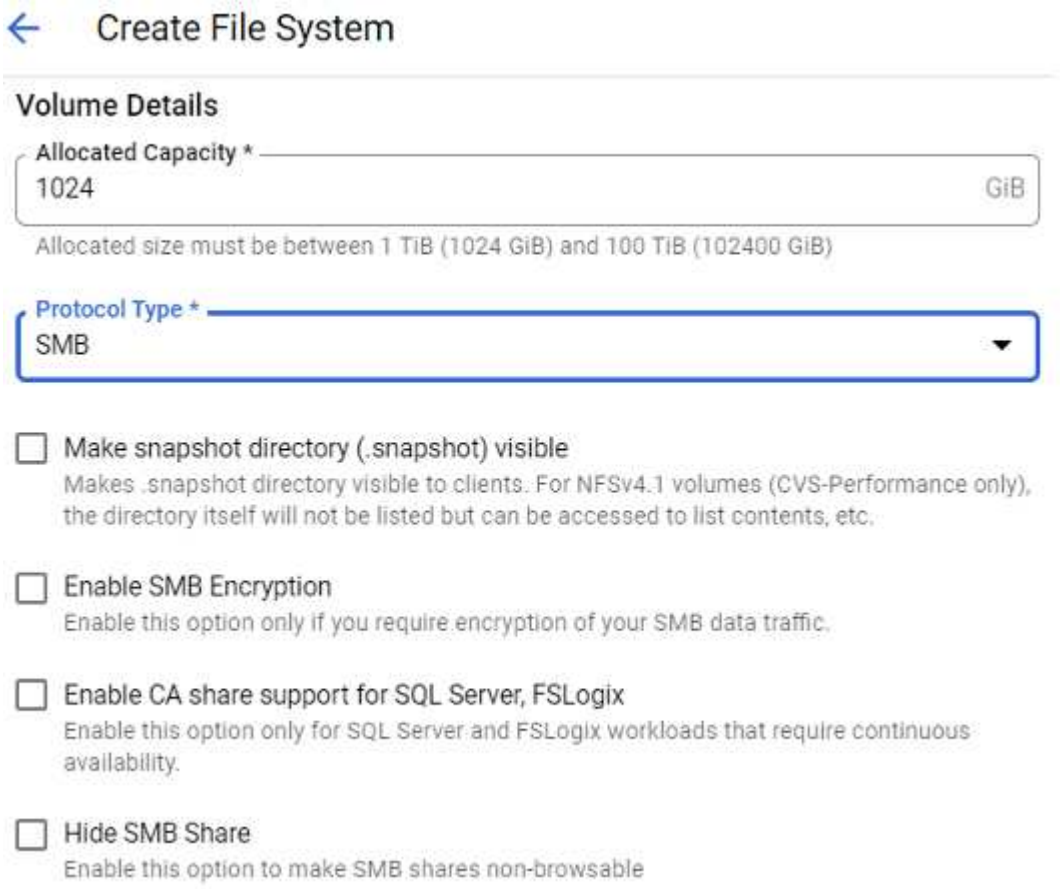
4. Legen Sie die Google Cloud-Region für den Volume- und Volume-Pfad fest (der Volume-Pfad muss für alle Cloud Volumes im Projekt eindeutig sein).



5. Wählen Sie das Performance-Level für das Volume aus.



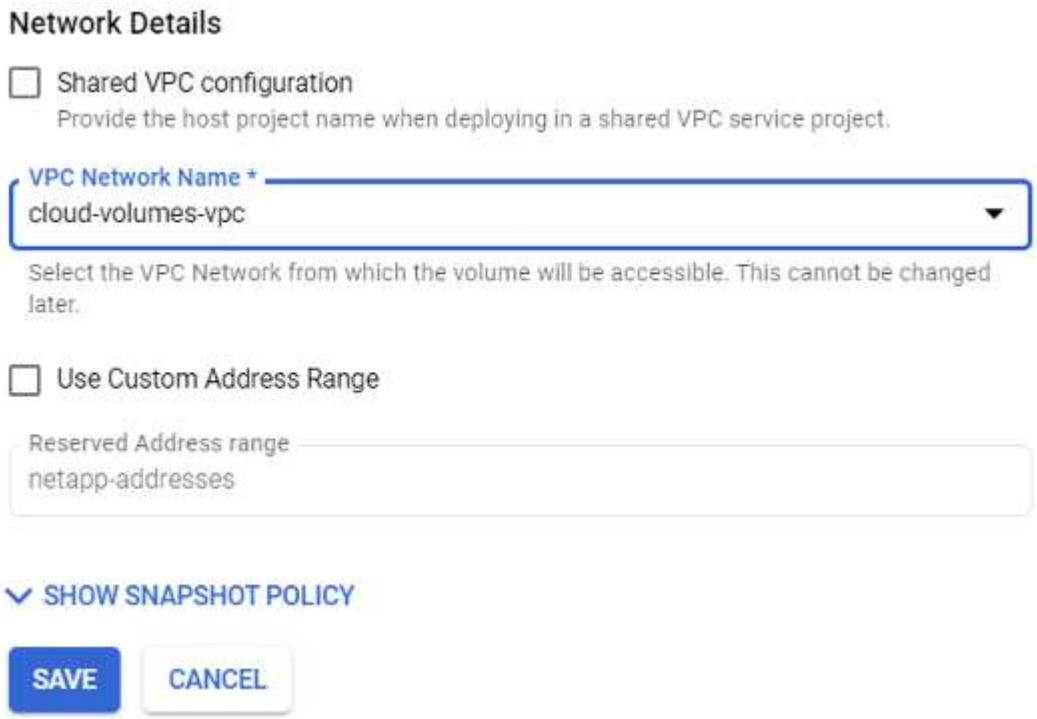
6. Geben Sie die Größe des Volume und den Protokolltyp an. In diesem Test wird SMB verwendet.



7. In diesem Schritt wählen Sie das VPC-Netzwerk aus, auf das das Volume zugegriffen werden soll. VPC-Peering sicherstellen.

   HINWEIS: Falls VPC-Peering nicht durchgeführt wurde, wird ein Pop-up-Button angezeigt, der Sie durch die Peering-Befehle leitet. Öffnen Sie eine Cloud-Shell-Sitzung und führen Sie die entsprechenden Befehle aus, um mit Cloud Volumes Service Producer Ihre VPC zu tauschen. Falls

Sie sich dazu entschließen, VPC Peering vorab vorzubereiten, lesen Sie diese "Anweisungen".



8. Klicken Sie auf Speichern, um das Volume zu erstellen.

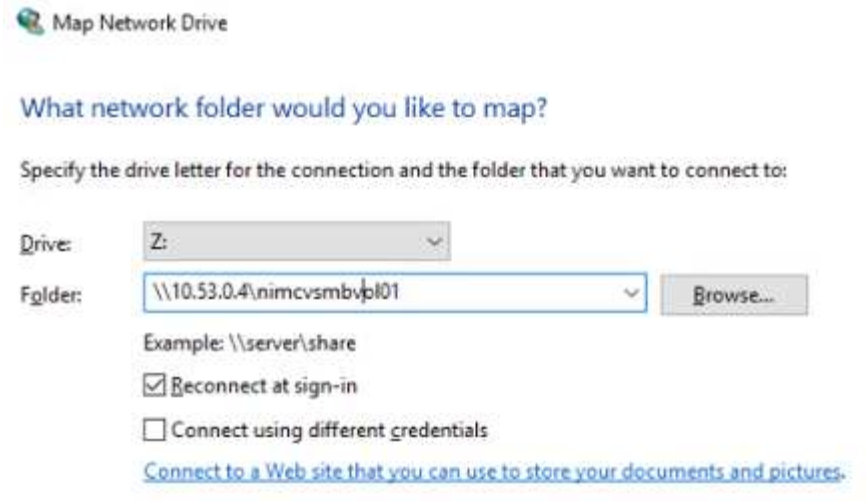
Gehen Sie zum Mounten des SMB-Volumes wie folgt vor:

1. Wechseln Sie in der Cloud Console zu Cloud Volumes > Volumes.
2. Wechseln Sie zur Seite Volumes
3. Klicken Sie auf das SMB-Volume, für das eine SMB-Freigabe zugeordnet werden soll.
4. Scrollen Sie nach rechts unter Mehr anzeigen auf Mount Instructions.

So führen Sie den Einmounten innerhalb des Windows Gastbetriebssystems der VMware VM durch:

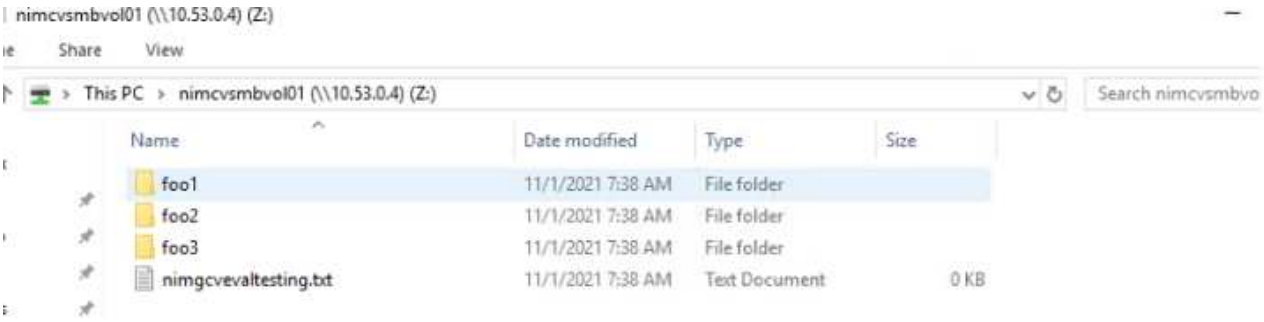
1. Klicken Sie auf die Schaltfläche Start und dann auf Computer.
2. Klicken Sie Auf Netzlaufwerk Zuordnen.
3. Klicken Sie in der Liste Laufwerk auf einen beliebigen verfügbaren Laufwerksbuchstaben.
4. Geben Sie im Feld Ordner Folgendes ein:

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



Aktivieren Sie das Kontrollkästchen bei der Anmeldung erneut verbinden, um jedes Mal eine Verbindung herzustellen.

5. Klicken Sie Auf Fertig Stellen.



Regionale Verfügbarkeit für zusätzliche NFS-Datastores auf AWS, Azure und GCP

Weitere Informationen zur Unterstützung der globalen Region für zusätzliche NFS-Datastores auf AWS, Azure und Google Cloud Platform (GCP).

Verfügbarkeit der AWS Region

Die Verfügbarkeit von zusätzlichen NFS-Datenspeichern auf AWS/VMC wird durch Amazon festgelegt. Zunächst müssen Sie feststellen, ob VMC und FSxN in einer bestimmten Region verfügbar sind. Als Nächstes müssen Sie feststellen, ob der FSxN zusätzliche NFS-Datastore in dieser Region unterstützt wird.

- Überprüfen Sie die Verfügbarkeit von VMC "Hier".
- Der Amazon Preisleitfaden enthält Informationen dazu, wo FSxN (FSX ONTAP) verfügbar ist. Diese Informationen finden Sie hier "Hier".
- Der zusätzlich zu NFS Datastore für VMC verfügbare FSxN wird demnächst verfügbar sein.

Obwohl noch Informationen freigegeben werden, zeigt das folgende Diagramm die aktuelle Unterstützung für VMC, FSxN und FSxN als zusätzliche NFS-Datenspeicher.

Nord- Und Südamerika

AWS Region	VMC Verfügbarkeit	FSX ONTAP Verfügbarkeit	Verfügbarkeit von NFS-Datenspeichern
US East (Northern Virginia)	Ja.	Ja.	Ja.
US-Osten (Ohio)	Ja.	Ja.	Ja.
USA West (Nordkalifornien)	Ja.	Nein	Nein
US West (Oregon)	Ja.	Ja.	Ja.
GovCloud (USA – Westen)	Ja.	Ja.	Ja.
Kanada (Zentral)	Ja.	Ja.	Ja.
Südamerika (Sao Paulo)	Ja.	Ja.	Ja.

Zuletzt aktualisiert am: 2. Juni 2022.

EMEA

AWS Region	VMC Verfügbarkeit	FSX ONTAP Verfügbarkeit	Verfügbarkeit von NFS-Datenspeichern
Europa (Irland)	Ja.	Ja.	Ja.
Europa (London)	Ja.	Ja.	Ja.
Europa (Frankfurt)	Ja.	Ja.	Ja.
Europa (Paris)	Ja.	Ja.	Ja.
Europa (Mailand)	Ja.	Ja.	Ja.
Europa (Stockholm)	Ja.	Ja.	Ja.

Zuletzt aktualisiert am: 2. Juni 2022.

Asien/Pazifik

AWS Region	VMC Verfügbarkeit	FSX ONTAP Verfügbarkeit	Verfügbarkeit von NFS-Datenspeichern
Asien/Pazifik (Sydney)	Ja.	Ja.	Ja.
Asien/Pazifik (Tokio)	Ja.	Ja.	Ja.
Asien/Pazifik (Osaka)	Ja.	Nein	Nein
Asien/Pazifik (Singapur)	Ja.	Ja.	Ja.
Asien/Pazifik (Seoul)	Ja.	Ja.	Ja.
Asien/Pazifik (Mumbai)	Ja.	Ja.	Ja.
Asien/Pazifik (Jakarta)	Nein	Nein	Nein
Asien/Pazifik (Hongkong)	Ja.	Ja.	Ja.

Zuletzt aktualisiert am: 28. September 2022.

Verfügbarkeit Der Azure Region

Die Verfügbarkeit von zusätzlichen NFS-Datenspeichern auf Azure/AVS wird von Microsoft definiert. Zunächst müssen Sie feststellen, ob sowohl AVS als auch ANF in einer bestimmten Region verfügbar sind. Als Nächstes müssen Sie ermitteln, ob der zusätzliche ANF NFS-Datastore in dieser Region unterstützt wird.

- Überprüfen Sie die Verfügbarkeit von AVS und ANF "Hier".
- Prüfen Sie die Verfügbarkeit des zusätzlichen ANF NFS-Datenspeichers "Hier".

Verfügbarkeit der GCP-Region

Wenn GCP in die öffentliche Verfügbarkeit eintritt, wird GCP verfügbar sein.

Zusammenfassung und Schlussfolgerung: Warum NetApp Hybrid Multicloud mit VMware

NetApp Cloud Volumes bietet zusammen mit VMware Lösungen für die wichtigsten Hyperscaler ein großes Potenzial für Unternehmen, die Hybrid Cloud nutzen möchten. Der Rest dieses Abschnitts enthält die Nutzungsfälle, in denen die Integration von NetApp Cloud Volumes echte Hybrid-Multi-Cloud-Funktionen ermöglicht.

Anwendungsfall #1: Storage-Optimierung

Bei einer Größenbemessung mit RVTools-Ausgabe ist es immer offensichtlich, dass die leistungsstarke Skalierung (vCPU/Vmem) parallel zum Storage erfolgt. Viele Unternehmen stellen sich in einer Situation wieder fest, dass durch den Storage-Platzbedarf die Größe des Clusters deutlich größer ist als für jede Leistung nötig.

Durch die Integration von NetApp Cloud Volumes können Unternehmen eine auf vSphere basierende Cloud-Lösung mit einem einfachen Migrationsansatz realisieren, ohne dass eine neue Plattform erforderlich ist oder IP-Änderungen vorgenommen werden müssen. Zudem ermöglicht diese Optimierung eine Skalierung des Storage-Platzbedarfs, während die Host-Anzahl auf die geringste Menge in vSphere beschränkt wird, jedoch keine Änderung der Storage-Hierarchie, der Sicherheit oder der verfügbaren Dateien vorgenommen werden muss. Somit können Sie die Implementierung optimieren und die Gesamtbetriebskosten um 35 bis 45 % senken. Dank dieser Integration ist außerdem die Möglichkeit möglich, in Sekundenschnelle Storage von warmen Storage-Ressourcen auf Produktionsebene zu skalieren.

Anwendungsfall #2: Cloud-Migration

Unternehmen stehen unter dem Druck, Applikationen aus verschiedenen Gründen von lokalen Datacentern in die Public Cloud zu migrieren: Zu einem bevorstehenden Ablauf des Leasing-Vertrags, zu einer Finanzrichtlinie zur Ausgabenübernahme (Investitions-) in Betriebskosten oder einfach zu einem Top-down-Auftrag, um alles in die Cloud zu verschieben.

Wenn Geschwindigkeit entscheidend ist, ist nur ein optimierter Migrationsansatz möglich, da die Rekonfiguration und Refakturierung von Anwendungen zur Anpassung an die spezielle IaaS-Plattform der Cloud langsam und teuer ist und oft Monate in Anspruch nimmt. Durch die Kombination von NetApp Cloud Volumes mit der bandbreiteneffizienten SnapMirror Replizierung für Storage mit Anbindung an den Gast-Storage (einschließlich RDMs in Verbindung mit applikationskonsistenten Snapshot Kopien und HCX, Cloud-spezifische Migration (z. B. Azure Migrate) oder Produkte von Drittanbietern zur Replizierung von VMs) ist dieser Wechsel noch einfacher, als auf zeitaufwändige I/O-Filtermechanismen zurückgreifen zu müssen.

Anwendungsfall #3: Datacenter-Erweiterung

Wenn in einem Datacenter aufgrund von saisonalen Bedarfsspitzen oder einem stabilen organischen Wachstum Kapazitätsgrenzen erreicht werden, ist der Wechsel zu VMware in Cloud-Umgebungen zusammen mit NetApp Cloud Volumes eine einfache Lösung. Der Einsatz von NetApp Cloud Volumes ermöglicht das sehr einfache Erstellen, Replizieren und erweitern von Storage, da über Verfügbarkeitszonen hinweg Hochverfügbarkeit und dynamische Skalierungsfunktionen sichergestellt sind. Mithilfe von NetApp Cloud Volumes minimieren Sie die Host-Cluster-Kapazität, da es dafür keine Stretch-Cluster mehr braucht.

Anwendungsfall #4: Disaster Recovery in der Cloud

Bei einem herkömmlichen Ansatz würden im Falle eines Ausfalls die in die Cloud replizierten VMs vor der Wiederherstellung auf die Cloud eigene Hypervisor-Plattform umgewandelt werden müssen – und das in einer Krise nicht.

Durch den Einsatz von NetApp Cloud Volumes für miteinander verbundenen Storage mit SnapCenter und SnapMirror Replizierung aus lokalen Systemen sowie mit Public-Cloud-Virtualisierungslösungen lässt sich ein besserer Disaster-Recovery-Ansatz entwickeln, der die Wiederherstellung von VM-Replikaten in einer vollständig konsistenten VMware SDDC-Infrastruktur sowie Cloud-spezifischen Recovery-Tools (z. B. Azure Site Recovery) oder vergleichbare Tools anderer Hersteller wie Veeam Dieser Ansatz unterstützt Sie auch bei der schnellen Durchführung von Disaster-Recovery-Prozessen und Recovery von Ransomware. Außerdem lassen sich dank bedarfsorientierter Hosts die gesamte Produktion zu Testzwecken oder bei einem Ausfall skalieren.

Anwendungsfall #5: Applikationsmodernisierung

Sobald Applikationen in der Public Cloud bereitgestellt wurden, möchten Unternehmen die zahlreichen leistungsstarken Cloud-Services nutzen, um sie zu modernisieren und zu erweitern. Mit NetApp Cloud Volumes ist eine Modernisierung ein einfacher Prozess, da die Applikationsdaten nicht in vSAN geschützt sind. Außerdem ermöglicht sie Datenmobilität für zahlreiche Anwendungsfälle, einschließlich Kubernetes.

Schlussfolgerung

Egal, ob Sie eine All-Cloud oder eine Hybrid Cloud abzielen – NetApp Cloud Volumes bietet Ihnen hervorragende Optionen für die Implementierung und das Management von Applikations-Workloads zusammen mit Fileservices und Blockprotokollen. Gleichzeitig reduziert es die TCO, indem die Datenanforderungen nahtlos auf die Applikationsebene übertragen werden.

Welche Anwendungsfälle auch immer sind: Wählen Sie Ihre bevorzugten Cloud/Hyperscaler zusammen mit NetApp Cloud Volumes, um schnell von den Vorteilen der Cloud zu profitieren, konsistente Infrastruktur und Abläufe zwischen On-Premises- und diversen Clouds, bidirektionaler Portabilität von Workloads sowie Kapazität und Performance der Enterprise-Klasse zu profitieren.

Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, mit denen der Speicher verbunden wird. Denken Sie daran, es ist nur die Position der Daten, die sich mit neuen Namen geändert haben. NetApp Cloud Volumes bleiben dieselben Tools und Prozesse, und NetApp Cloud Volumes helfen bei der Optimierung der generellen Implementierung.

Anwendungsfälle für VMware Hybrid Cloud

Anwendungsfälle für NetApp Hybrid-Multi-Cloud mit VMware

Ein Überblick über die Anwendungsfälle, die für DIE IT-Abteilung bei der Planung von Hybrid-Cloud- oder Cloud-First-Implementierungen von Bedeutung sind

Gängige Anwendungsfälle

Anwendungsfälle:

- Disaster Recovery,
- Hosting von Workloads während der Rechenzentrumswartung, * schneller Burst, in dem zusätzliche Ressourcen über die im lokalen Rechenzentrum bereitgestellten Ressourcen erforderlich sind,
- VMware-Site-Erweiterung,
- Schnelle Migration in die Cloud,
- Entwicklung/Test und
- Modernisierung von Applikationen mithilfe von zusätzlichen Cloud-Technologien

In der gesamten Dokumentation werden die Referenzen für Cloud-Workloads anhand der VMware Anwendungsfälle detailliert beschrieben. Anwendungsfälle sind:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Migrieren
- Erweitern

In DER IT-Entwicklung

Die meisten Unternehmen befinden sich auf dem Weg zur Transformation und Modernisierung. Im Rahmen dieses Prozesses versuchen Unternehmen, ihre vorhandenen VMware Investitionen zu nutzen und gleichzeitig von den Vorteilen der Cloud zu profitieren und Möglichkeiten für eine nahtlose Migration zu entdecken. Durch diesen Ansatz würde sich ihre Modernisierungsbemühungen sehr vereinfachen, da sich die Daten bereits in der Cloud befinden.

Die einfachste Antwort auf dieses Szenario sind die Angebote von VMware in jedem Hyperscaler. Wie bei NetApp Cloud Volumes bietet VMware eine Möglichkeit, lokale VMware Umgebungen in jede Cloud zu verschieben oder zu erweitern. So können Sie vorhandene Ressourcen, Fachkenntnisse und Tools weiterhin nutzen, während Sie Workloads nativ in der Cloud ausführen. Das verringert die Risiken, da keine Serviceunterbrechungen oder IP-Änderungen erforderlich sind. Das IT-Team kann so unter Verwendung vorhandener Fachkenntnisse und Tools vor Ort Verfahren. Dies ermöglicht beschleunigte Cloud-Migrationen und einen viel reibungsloseren Übergang zu einer Hybrid Multi Cloud Architektur.

Bedeutung von zusätzlichen NFS-Storage-Optionen

Während VMware in jeder Cloud seinen Kunden einzigartige Hybrid-Funktionen bietet, haben begrenzte zusätzliche NFS-Storage-Optionen den Nutzen für Unternehmen mit Storage-lastigen Workloads eingeschränkt. Da Storage direkt an Hosts gebunden ist, besteht die einzige Möglichkeit zur Skalierung von Storage darin, weitere Hosts hinzuzufügen. Die Kosten können bei Storage-intensiven Workloads um 35 bis 40 % oder mehr gesenkt werden. Diese Workloads erfordern nur zusätzlichen Storage und keine zusätzliche Leistung. Aber das bedeutet, dass zusätzliche Hosts bezahlt werden.

Betrachten wir das folgende Szenario:

Ein Kunde benötigt nur fünf Hosts für CPU und Arbeitsspeicher, hat aber hohe Storage-Anforderungen und benötigt 12 Hosts, um die Storage-Anforderungen zu erfüllen. Diese Anforderung kippt letztlich in Richtung Finanzskalierung, indem sie zusätzliche Leistung kaufen müssen, wenn sie nur den Storage erhöhen müssen.

Wenn Sie Cloud-Einführung und -Migrationen planen, ist es immer wichtig, den besten Ansatz zu bewerten und den einfachsten Weg zu gehen, der die Gesamtinvestitionen reduziert. Der gängigste und einfachste

Ansatz für jede Applikationsmigration besteht in Rehosting (auch bekannt als „Lift and Shift“), in dem keine Virtual Machine (VM) oder Datenkonvertierung vorhanden ist. NetApp Cloud Volumes mit dem softwaredefinierten Datacenter (SDDC) von VMware und ergänzen vSAN und bieten eine einfache „Lift-and-Shift“-Option.

NetApp Lösungen für Amazon VMware Managed Cloud (VMC)

Erfahren Sie mehr über die Lösungen von NetApp für AWS.

VMware definiert Cloud-Workloads in eine von drei Kategorien:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Migrieren
- Erweitern

Durchsuchen Sie die verfügbaren Lösungen in den folgenden Abschnitten.

Sichern

- "Disaster Recovery mit VMC auf AWS (mit Gast verbunden)"
- "Veeam Backup amp; Restore in VMC mit FSX for ONTAP"
- "Disaster Recovery (DRO) mit FSX für ONTAP und VMC"
- "Verwenden von Veeam Replizierung und FSX for ONTAP für die Disaster Recovery in VMware Cloud on AWS"

Migrieren

- "Migrieren Sie Workloads mithilfe von VMware HCX zu FSxN-Datenspeichern"

Erweitern

IN KÜRZE:

NetApp Lösungen für Azure VMware (AVS)

Erfahren Sie mehr über die Lösungen von NetApp für Azure.

VMware definiert Cloud-Workloads in eine von drei Kategorien:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Migrieren
- Erweitern

Durchsuchen Sie die verfügbaren Lösungen in den folgenden Abschnitten.

Sichern

- "Disaster Recovery mit ANF und JetStream (zusätzlicher NFS-Datastore)"
- "Disaster Recovery mit ANF und CVO (über Gast verbundener Storage)"
- "Disaster Recovery (DRO) mit ANF und AVS"
- "Verwenden von Veeam Replizierung und Azure NetApp Files-Datastore für die Disaster Recovery zu Azure VMware-Lösung"

Migrieren

- "Migrieren Sie Workloads mithilfe von VMware HCX zum Azure NetApp Files Datastore"

Erweitern

IN KÜRZE:

NetApp Lösungen für die Google Cloud VMware Engine (GCVE)

Erfahren Sie mehr über die Lösungen von NetApp für GCP.

VMware definiert Cloud-Workloads in eine von drei Kategorien:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Migrieren
- Erweitern

Durchsuchen Sie die verfügbaren Lösungen in den folgenden Abschnitten.

Sichern

- "Disaster Recovery für Applikationen mit SnapCenter, Cloud Volumes ONTAP und Veeam Replication"
- "Applikationskonsistente Disaster Recovery mit NetApp SnapCenter und Veeam Replizierung zu NetApp CVS auf GCVE"

Migrieren

- "Workload-Migration mit VMware HCX zu NetApp Cloud Volume Service NFS Datastore"
- "VM-Replizierung mit Veeam zu einem NetApp Cloud Volume Service NFS-Datastore"

Erweitern

IN KÜRZE:

NetApp Funktionen für AWS VMC

Erfahren Sie mehr über die Funktionen, die NetApp für die AWS VMware Cloud (VMC) zur Verfügung stellt – von NetApp als Storage-Gerät mit Gastverbunden oder als zusätzlicher NFS-Datastore für die Migration von Workflows, Erweiterung/Bursting in die Cloud, Backup/Wiederherstellung und Disaster Recovery.

Springen Sie zum Abschnitt zum gewünschten Inhalt, indem Sie eine der folgenden Optionen auswählen:

- "Konfiguration von VMC in AWS"
- "NetApp Storage-Optionen für VMC"
- "NetApp/VMware Cloud-Lösungen"

Konfiguration von VMC in AWS

Wie bei lokalen Systemen ist die Planung einer Cloud-basierten Virtualisierungsumgebung eine entscheidende Voraussetzung für eine erfolgreiche, sofort einsatzbereite Umgebung zum Erstellen von VMs und Migrationen.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS SDDC einrichten und managen und es in Kombination mit den verfügbaren Optionen zur Verbindung von NetApp Storage nutzen.

Der in-Guest Storage ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit AWS VMC.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Implementieren und Konfigurieren von VMware Cloud für AWS
- Verbinden Sie VMware Cloud mit FSX ONTAP

Details anzeigen "Konfigurationsschritte für VMC".

NetApp Storage-Optionen für VMC

NetApp Storage kann innerhalb der AWS VMC auf verschiedene Arten genutzt werden – entweder als angebundenen oder als zusätzlicher NFS-Datenspeicher.

Besuchen Sie "Unterstützte NetApp Storage-Optionen" Finden Sie weitere Informationen.

AWS unterstützt NetApp Storage in den folgenden Konfigurationen:

- FSX ONTAP als Storage mit Gastverbunden
- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- FSX ONTAP als zusätzlichen NFS-Datastore

Details anzeigen "Storage-Optionen für VMC für Gastverbindung". Details anzeigen "Zusätzliche NFS-Datastore-Optionen für VMC".

Anwendungsfälle Für Lösungen

Mit Cloud-Lösungen von NetApp und VMware sind viele Anwendungsfälle einfach in AWS VMC zu implementieren. Anwendungsfälle sind für jeden der von VMware definierten Cloud-Bereiche definiert:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Erweitern
- Migrieren

"NetApp Lösungen für AWS VMC"

Schutz von Workloads auf AWS/VMC

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

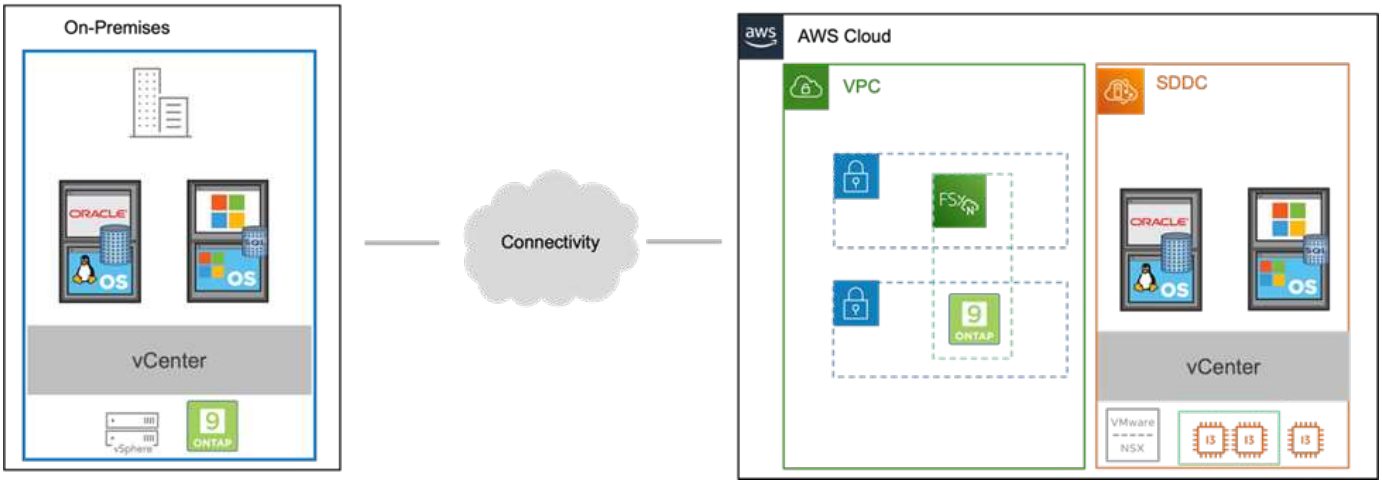
Autoren: Chris Reno, Josh Powell und Suresh ThopPay – NetApp Solutions Engineering

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.

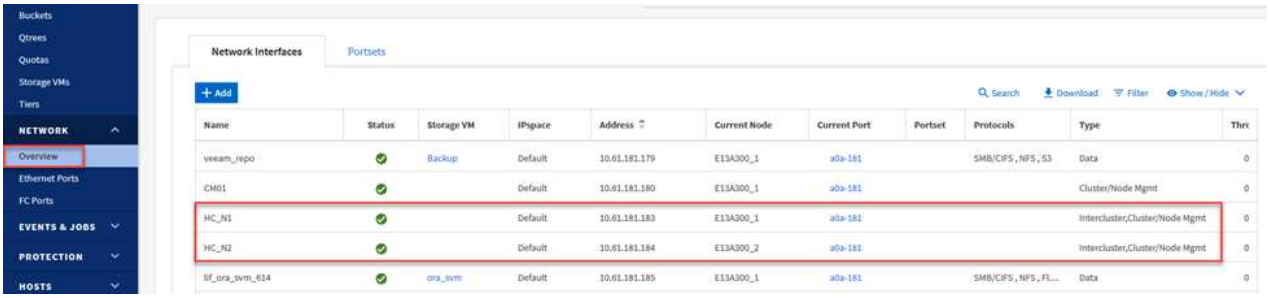
Die folgenden Schritte sind zum Einrichten von SnapMirror Beziehungen zwischen einem lokalen ONTAP System und FSX ONTAP erforderlich:

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.
```

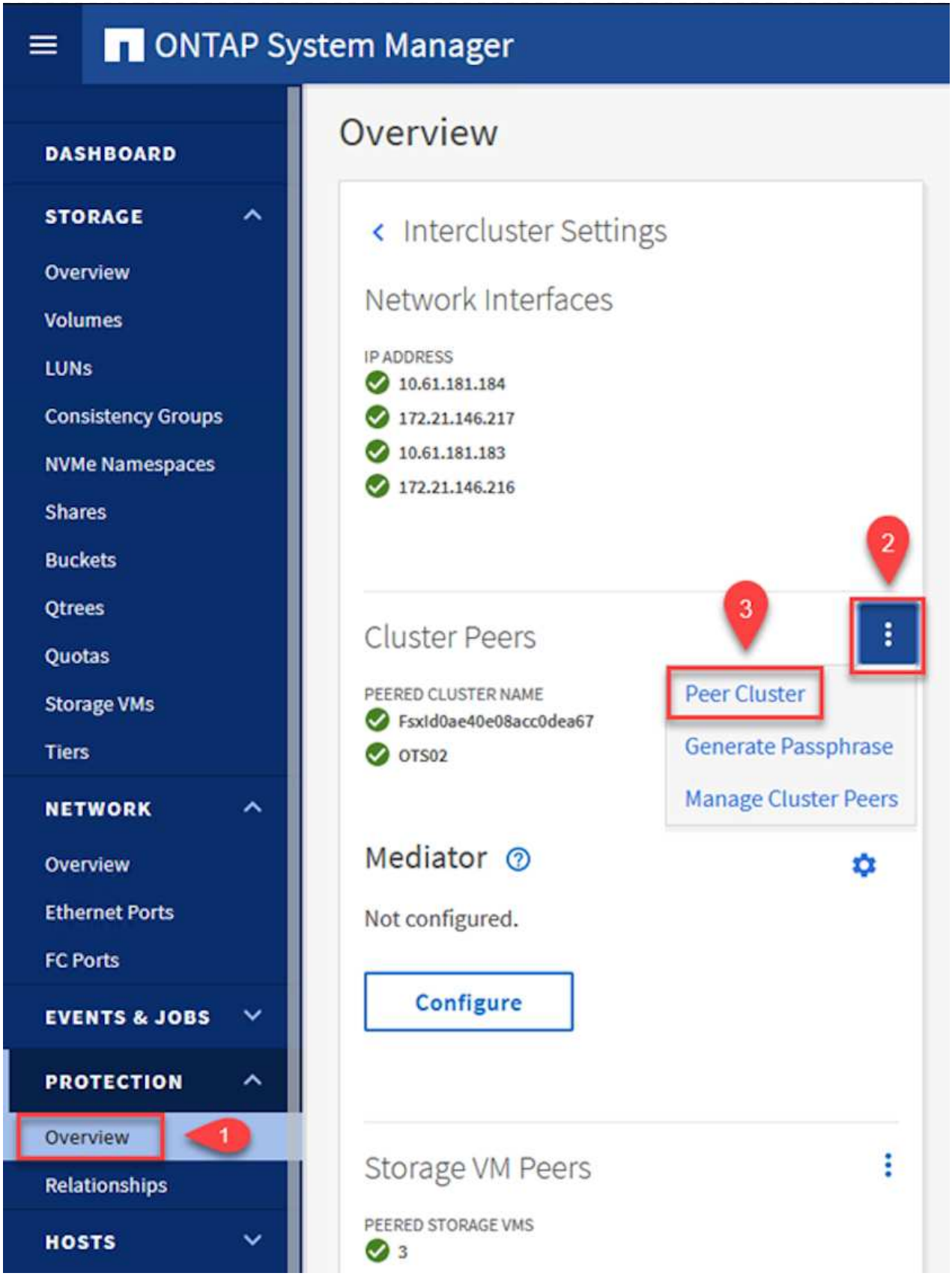
Cluster-Peering zwischen ONTAP und FSX einrichten

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.

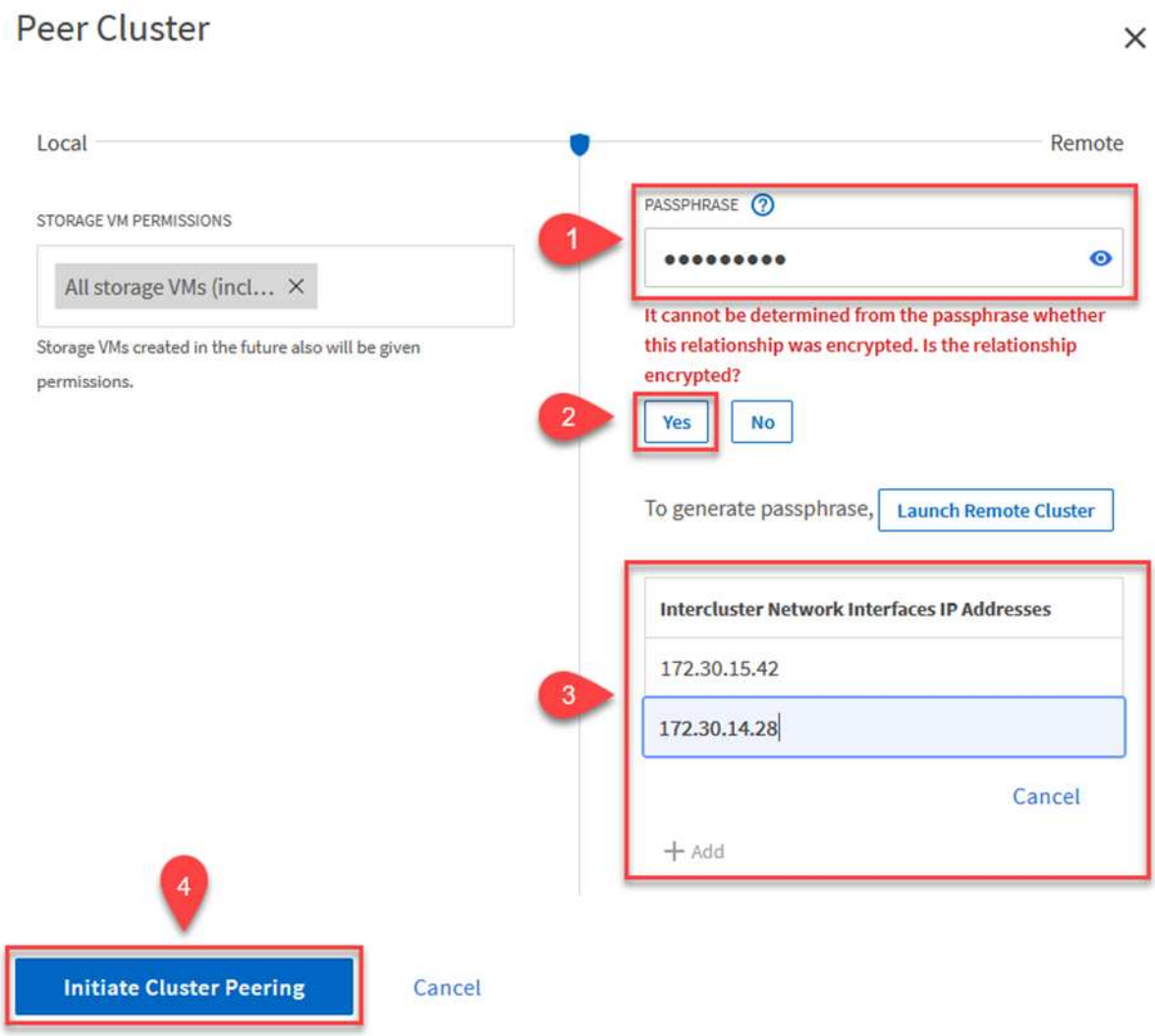


3. Füllen Sie im Dialogfeld Peer Cluster die erforderlichen Informationen aus:
   a. Geben Sie die Passphrase ein, die zum Erstellen der Peer-Cluster-Beziehung auf dem Ziel-FSX-Cluster verwendet wurde.

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
```

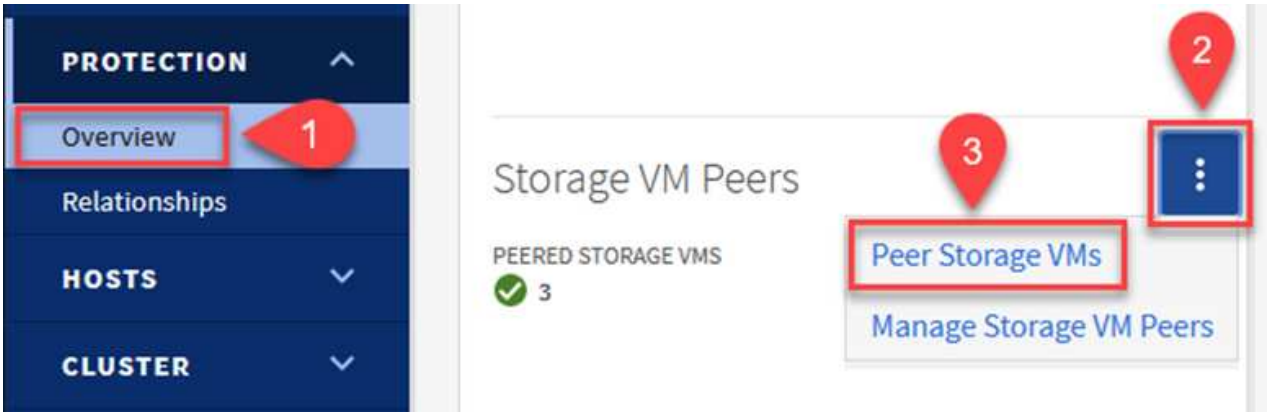
SVM-Peering-Beziehung einrichten

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.

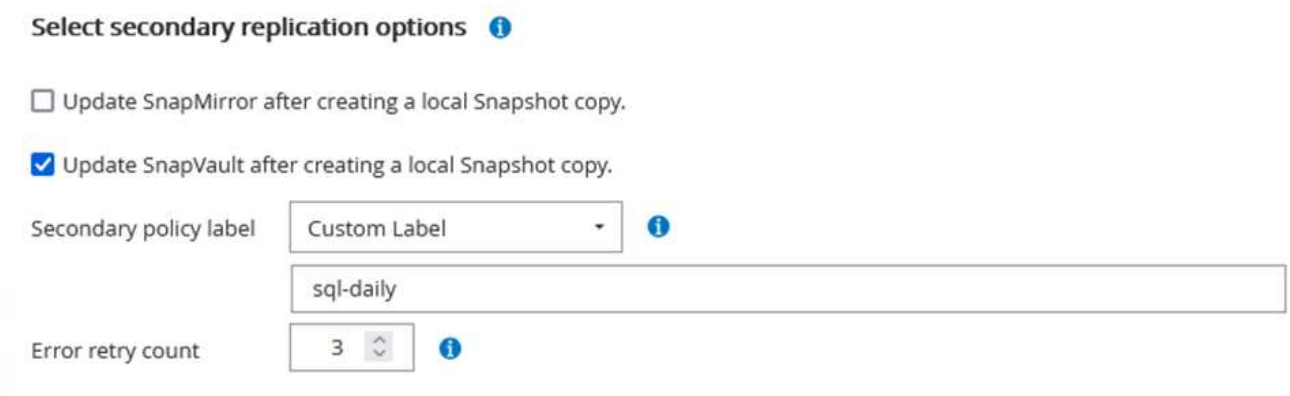
Erstellen einer Snapshot Aufbewahrungsrichtlinie

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".

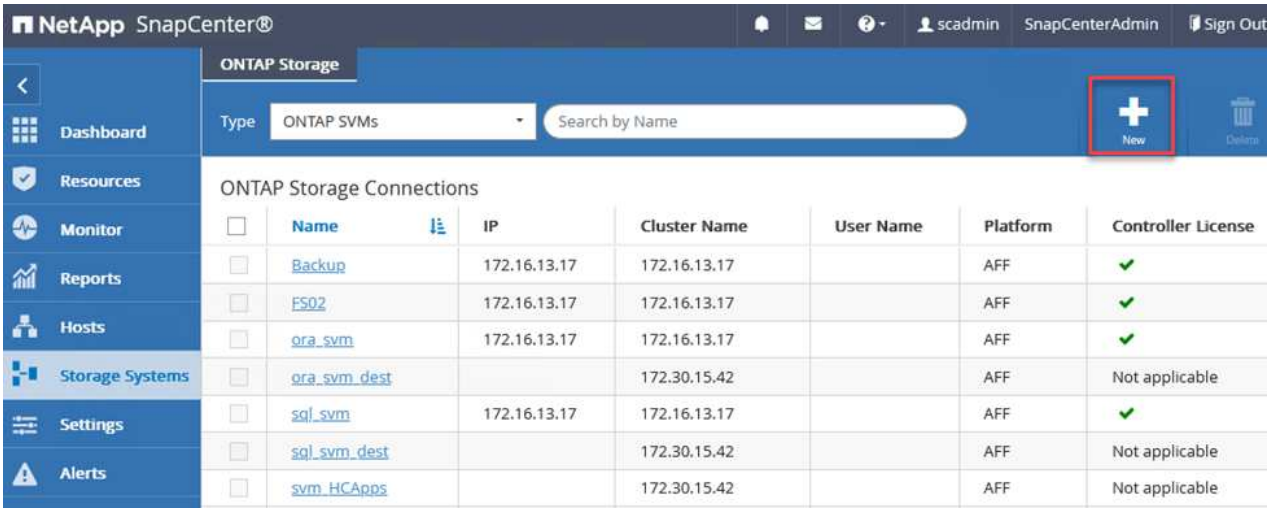
Nach der Installation können Sie über einen Webbrowser mit *https://Virtual_Cluster_IP_or_FQDN:8146* auf die SnapCenter Konsole zugreifen.

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

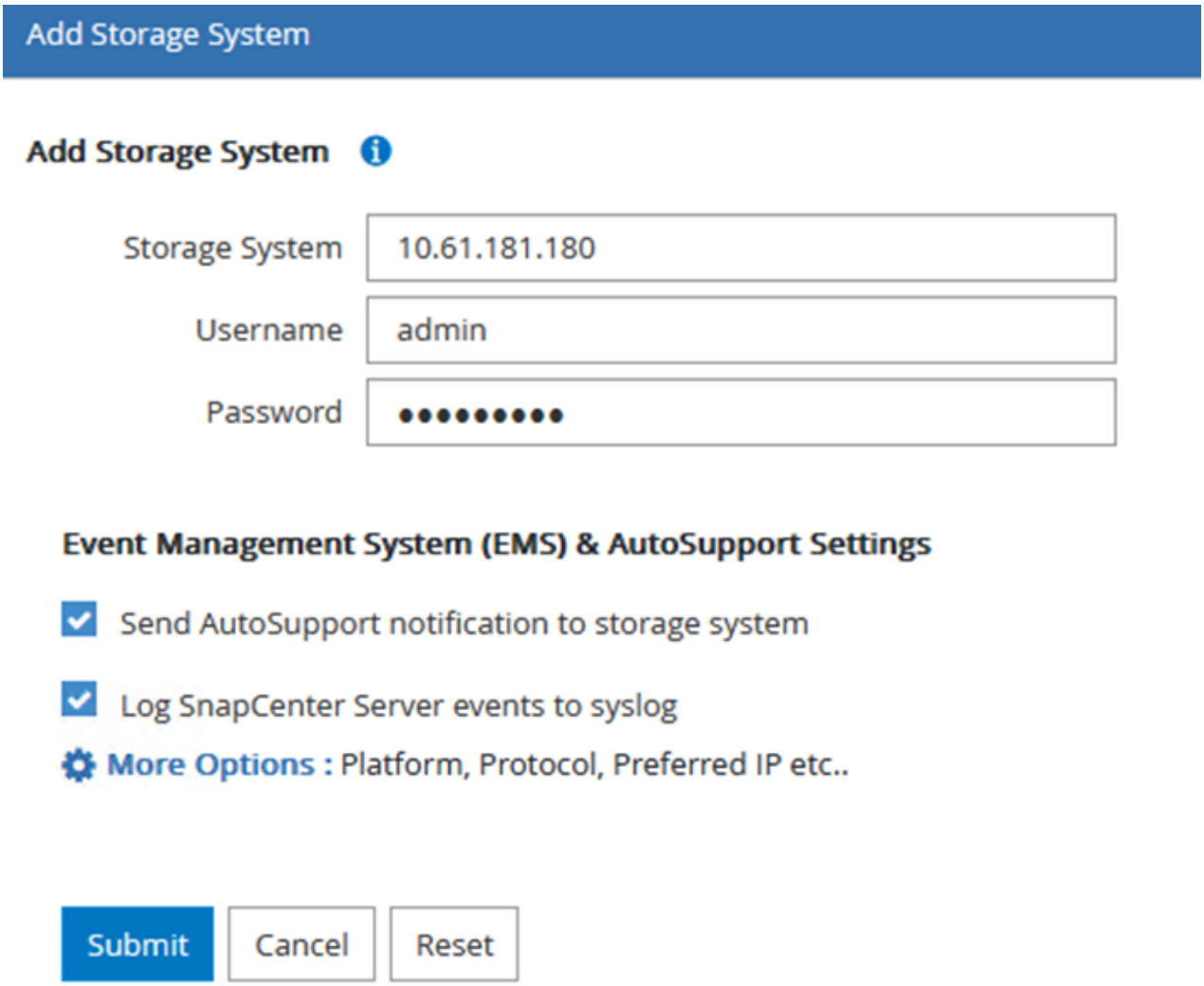
Hinzufügen von Storage-Controllern zu SnapCenter

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

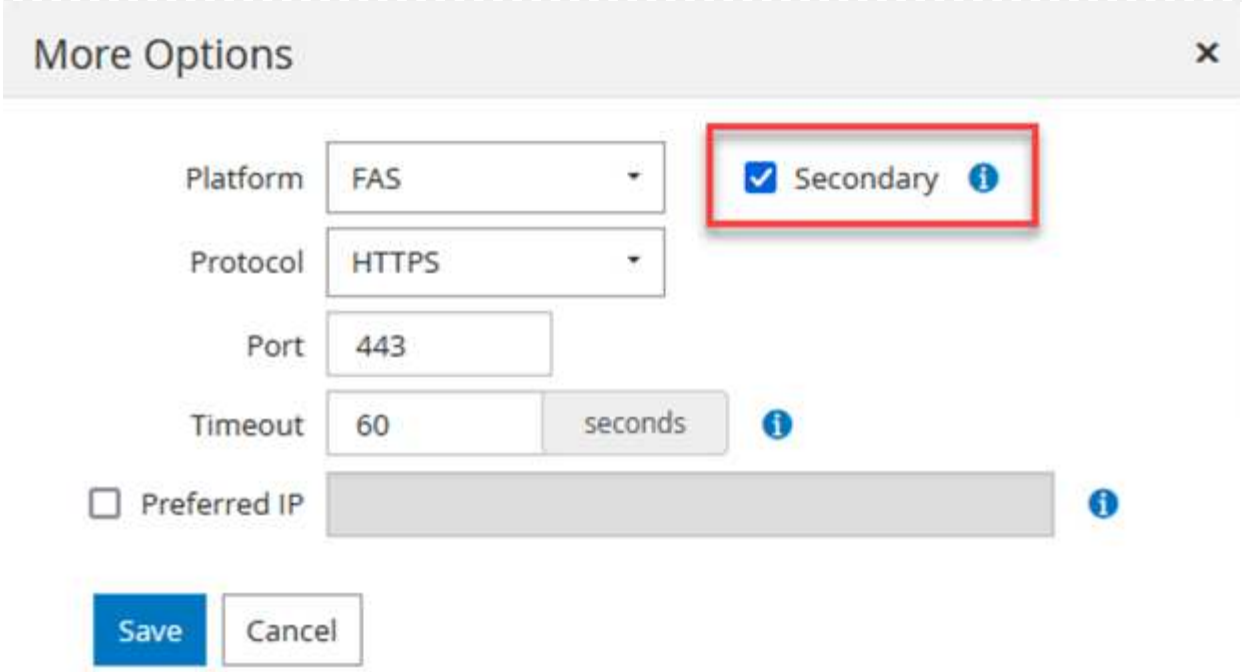
1. Wählen Sie im linken Menü Storage Systems aus und klicken Sie dann auf Neu, um mit dem Hinzufügen Ihrer Storage Controller zu SnapCenter zu beginnen.



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.

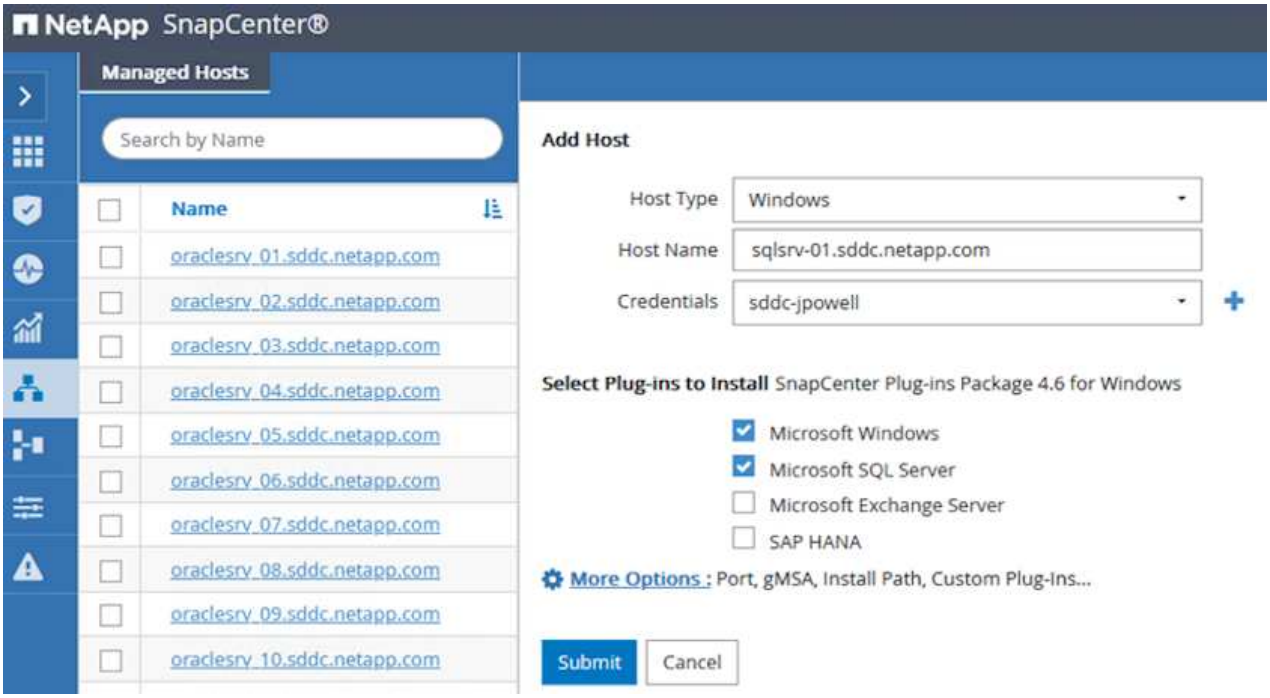


Weitere Informationen zum Hinzufügen von Storage-Systemen zum SnapCenter finden Sie in der Dokumentation unter "Dieser Link".

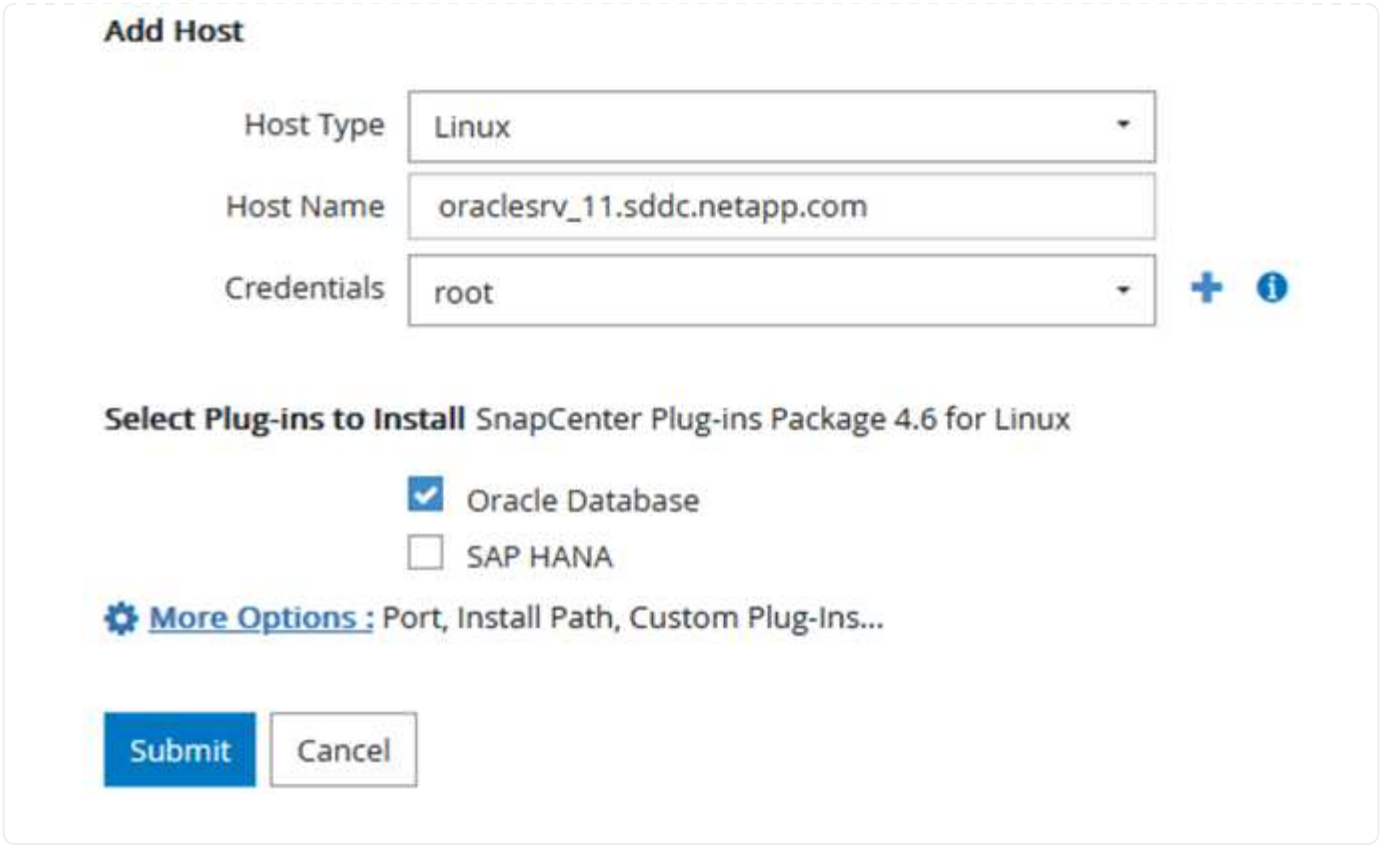
Fügen Sie Hosts zum SnapCenter hinzu

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.



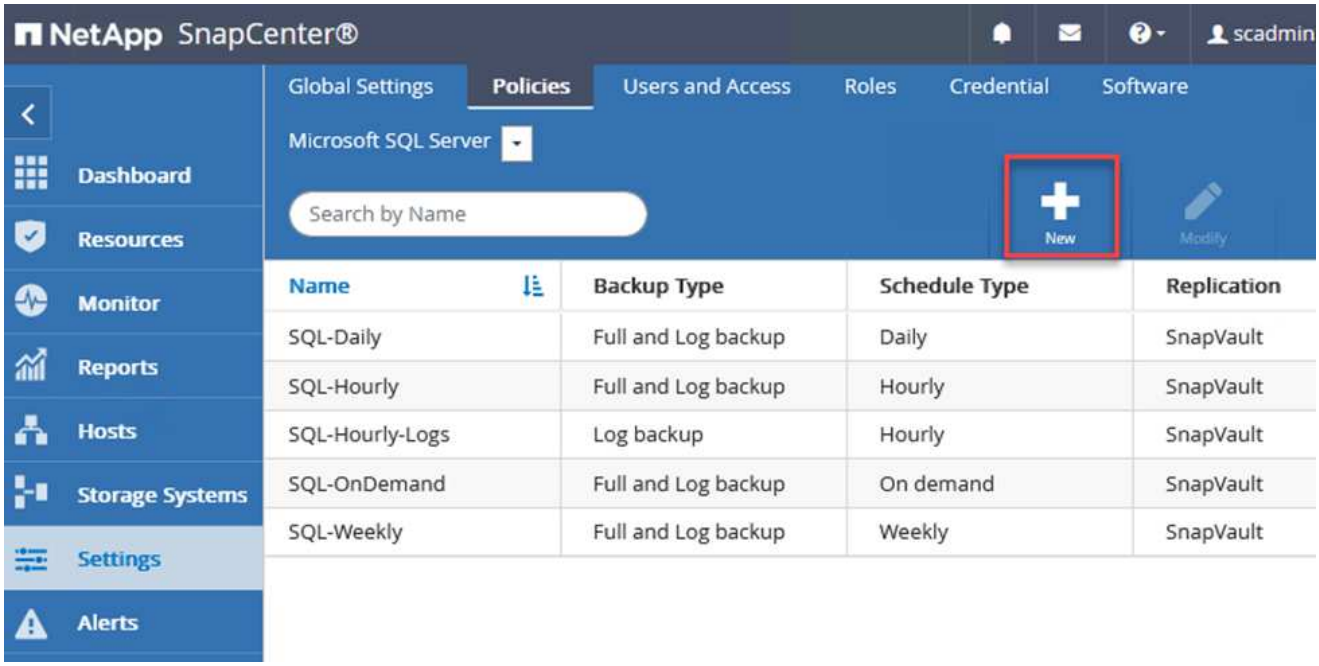
3. Füllen Sie für Oracle die erforderlichen Felder im Dialogfeld „Host hinzufügen“ aus, und aktivieren Sie das Kontrollkästchen für das Oracle Database Plug-in. Klicken Sie dann auf Senden, um den Erkennungsvorgang zu starten und den Host zu SnapCenter hinzuzufügen.


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
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.



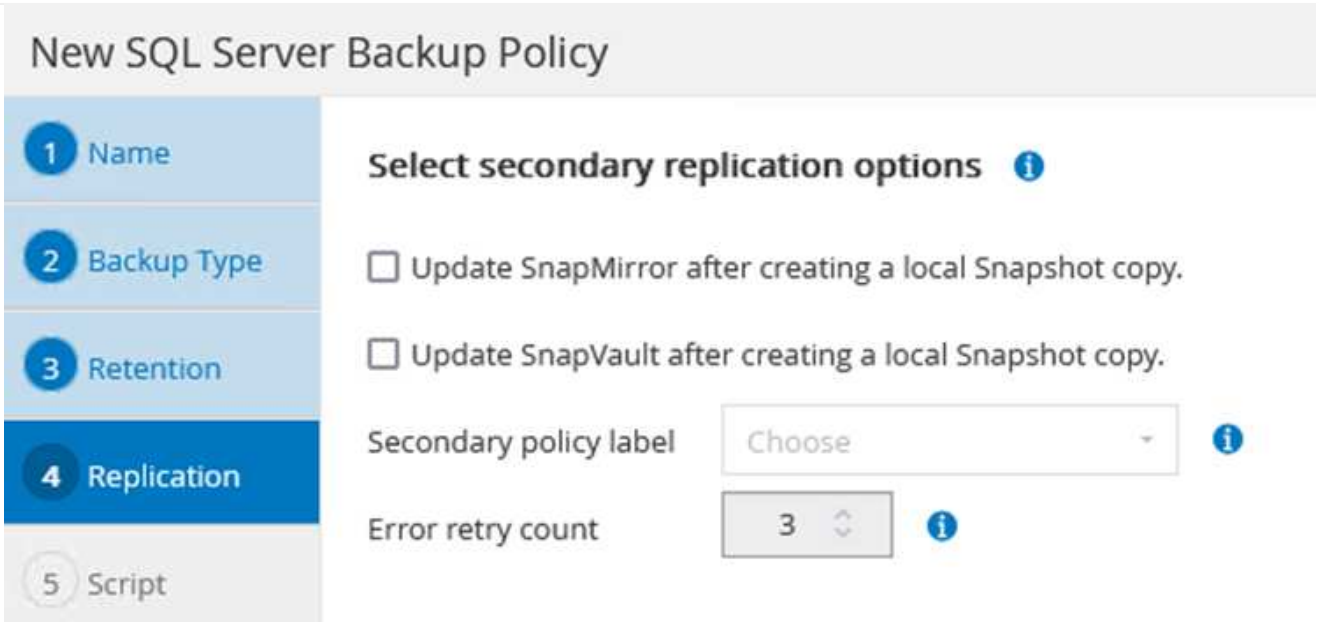
Vollständige Informationen zum Erstellen von Richtlinien für SQL Server-Backups finden Sie im "SnapCenter-Dokumentation".

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.

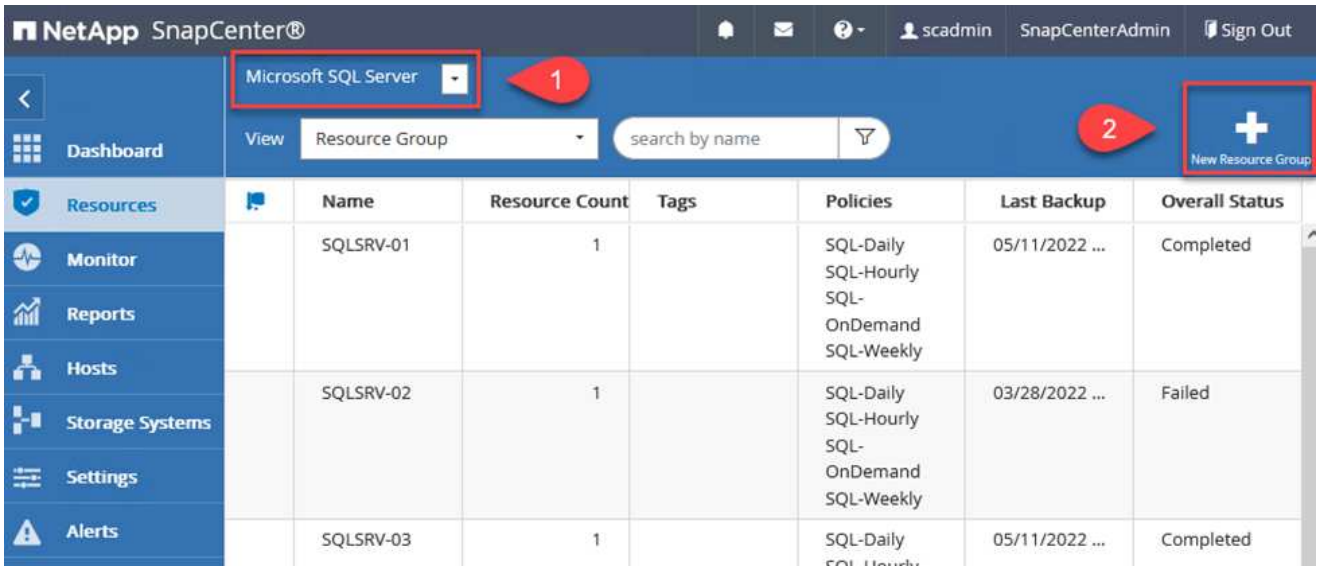
Die folgende Abbildung zeigt die vorhergehenden Optionen und deren Aussehen im Backup Policy Wizard.



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.

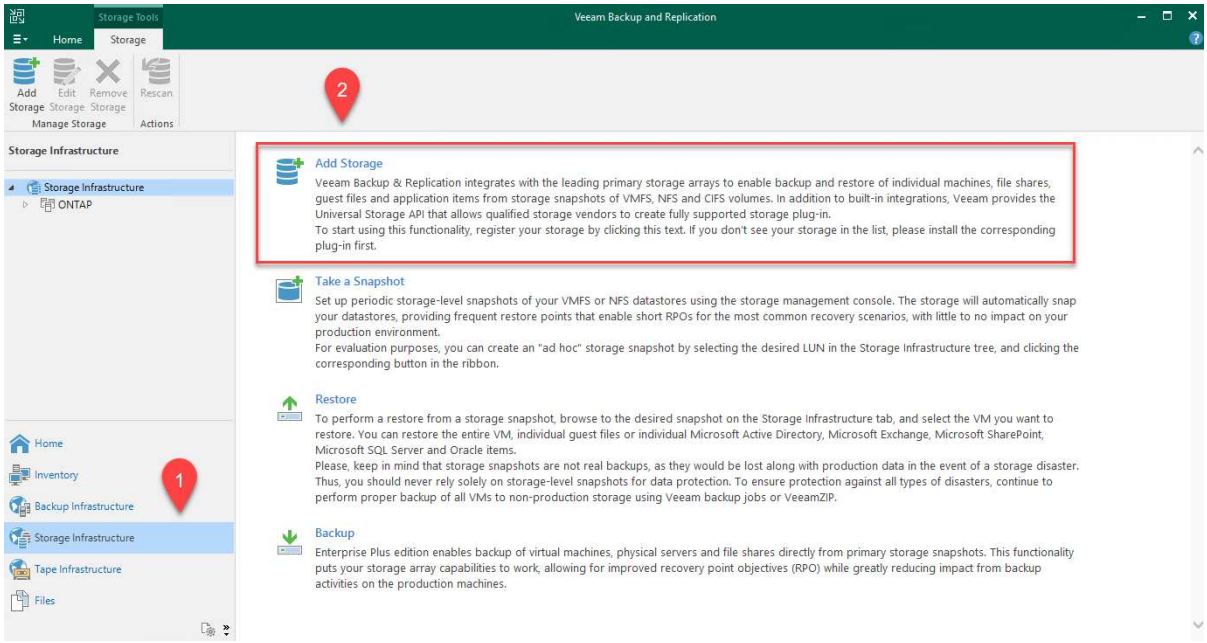
Lesen Sie die folgenden Voraussetzungen, bevor Sie beginnen.

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.

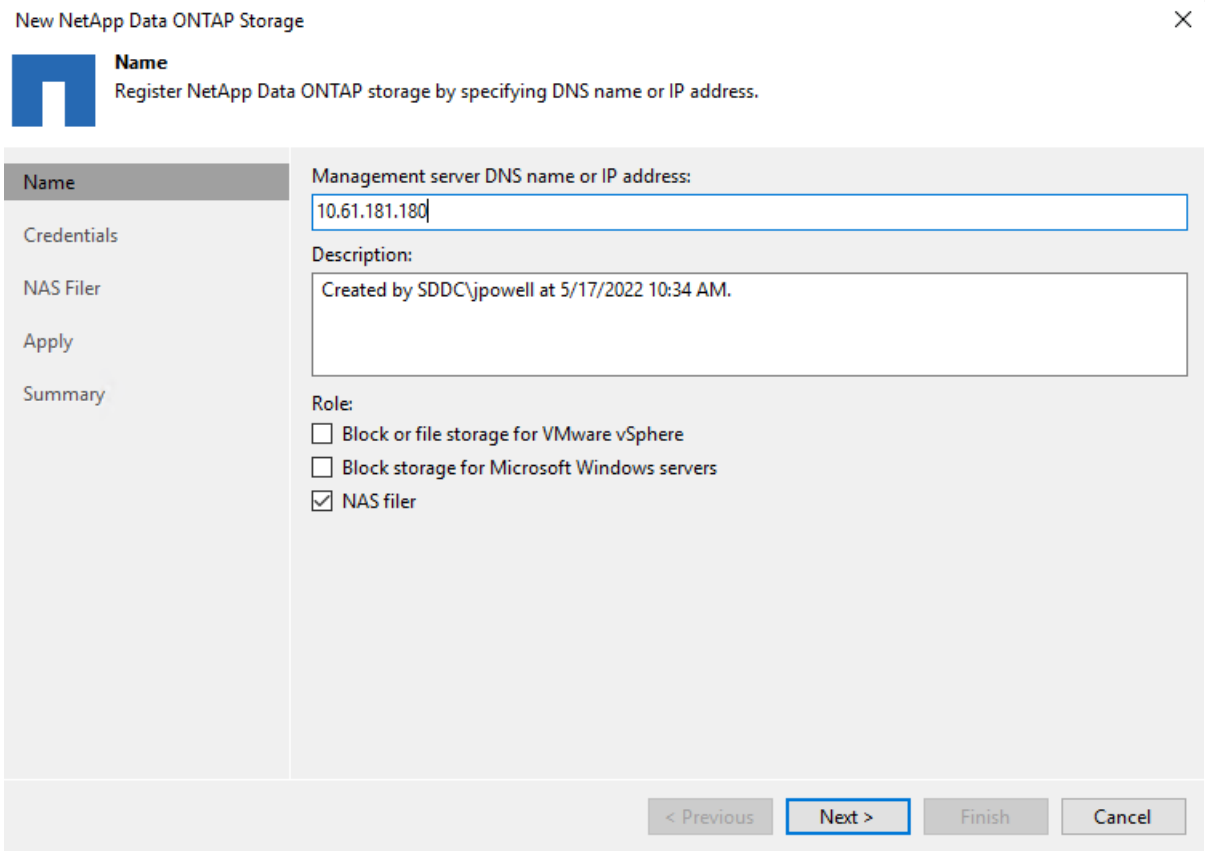
Fügen Sie ONTAP Storage zu Veeam hinzu

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

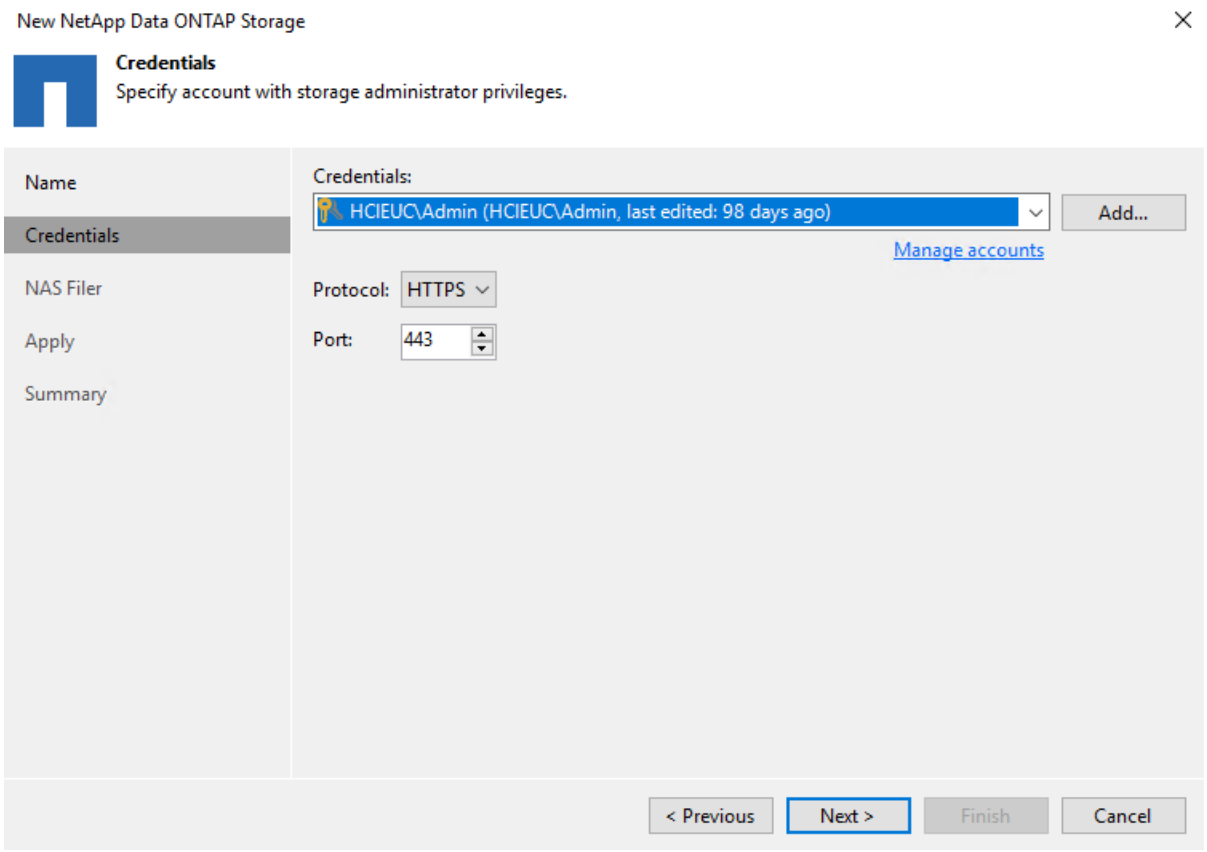
1. Öffnen Sie die Veeam-Konsole, und melden Sie sich an. Navigieren Sie zu Storage Infrastructure, und wählen Sie Add Storage aus.



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.

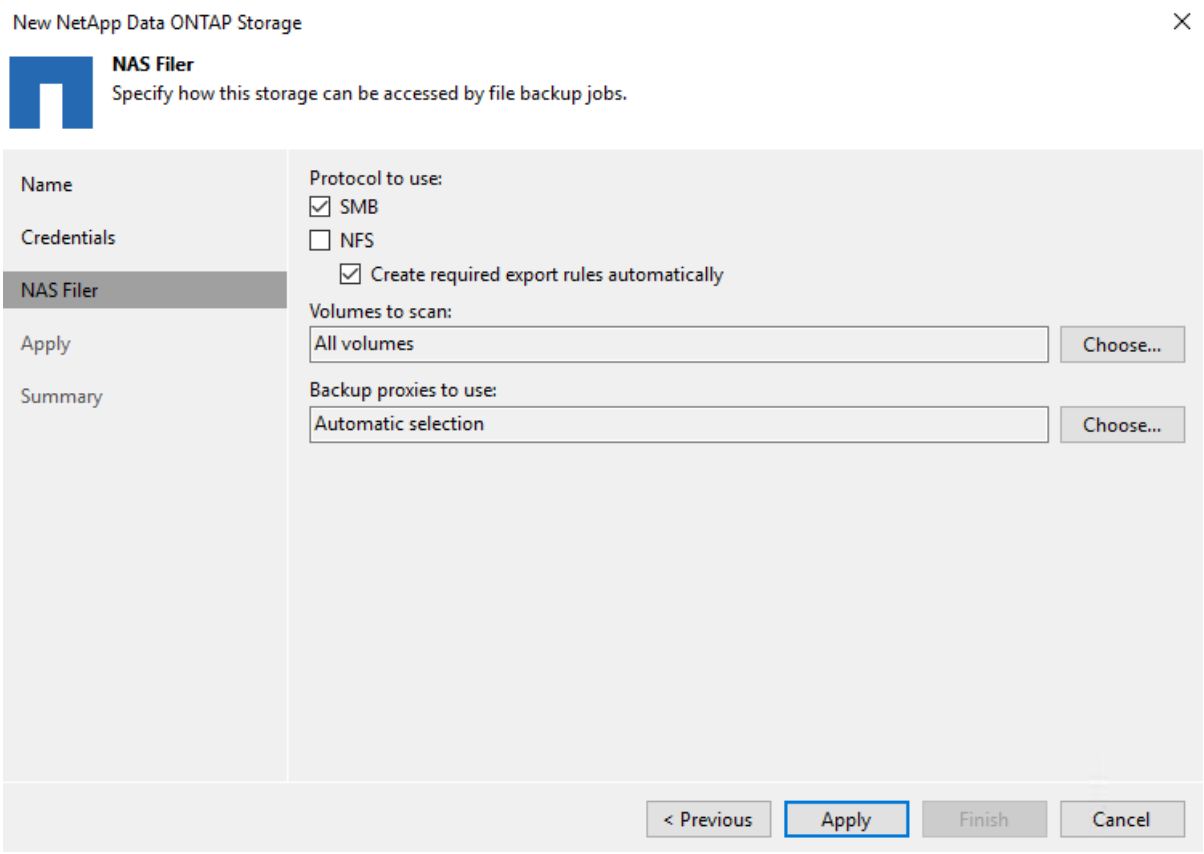


4. Fügen Sie Ihre Zugangsdaten ein, um auf das ONTAP Cluster zuzugreifen.

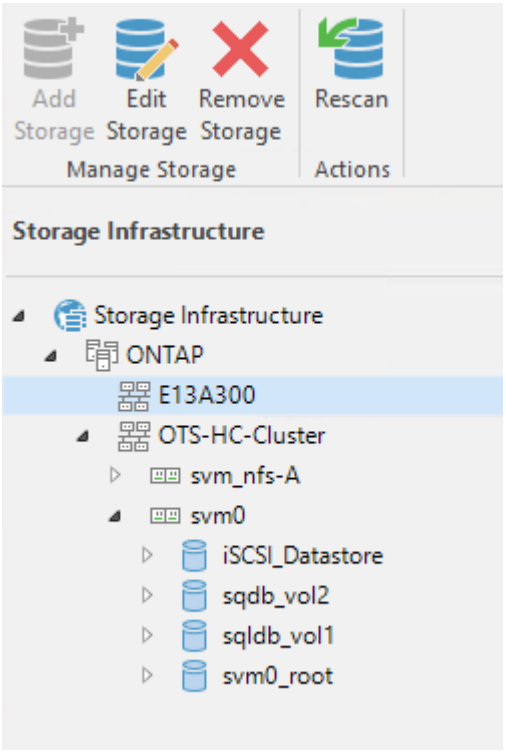


5. Wählen Sie auf der Seite NAS Filer die gewünschten Protokolle zum Scannen aus und wählen

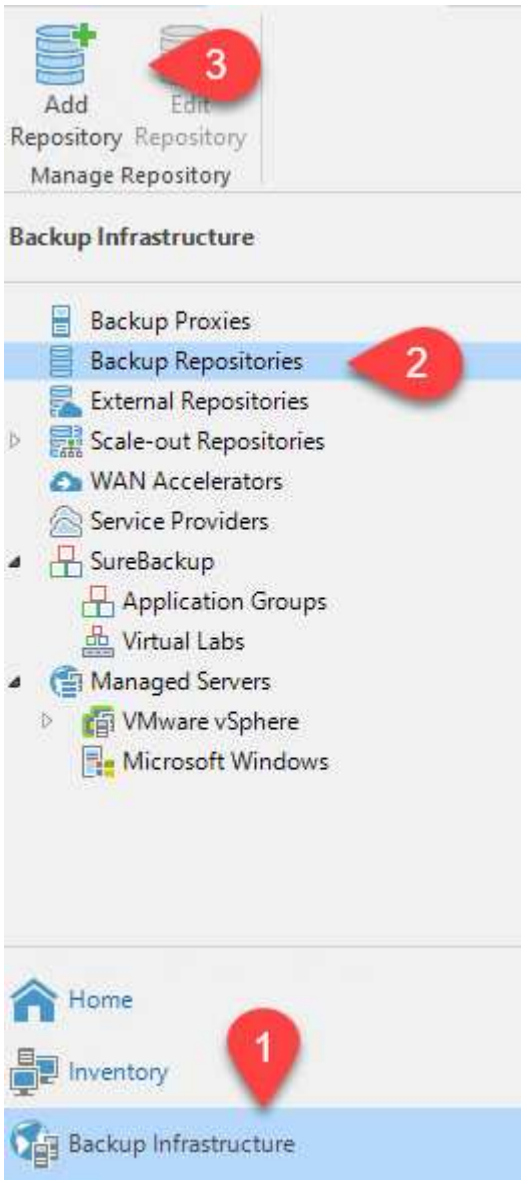
Sie Weiter.



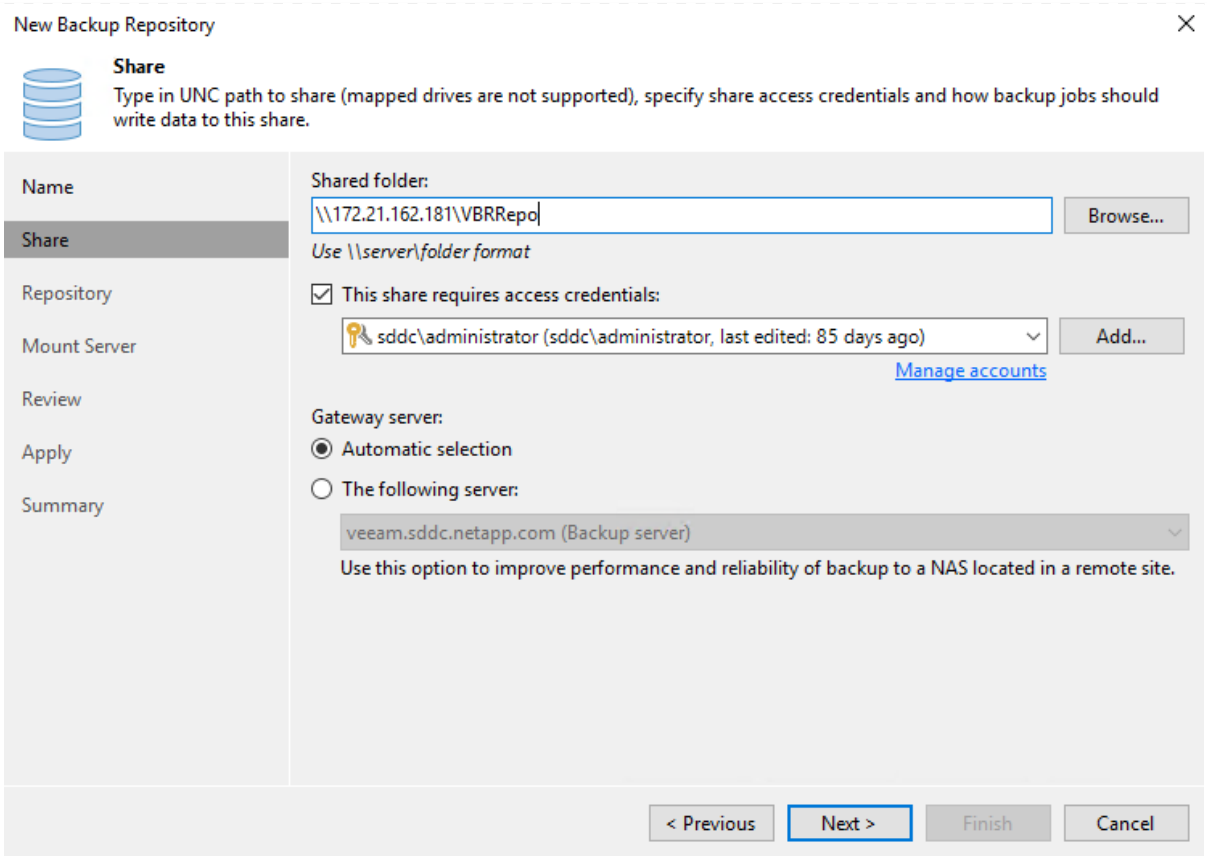
6. Schließen Sie die Seiten „Übernehmen“ und „Zusammenfassung“ des Assistenten ab, und klicken Sie auf „Fertig stellen“, um den Speicherermittlungsprozess zu starten. Nach Abschluss des Scans wird das ONTAP-Cluster zusammen mit den NAS-Filern als verfügbare Ressourcen hinzugefügt.



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.



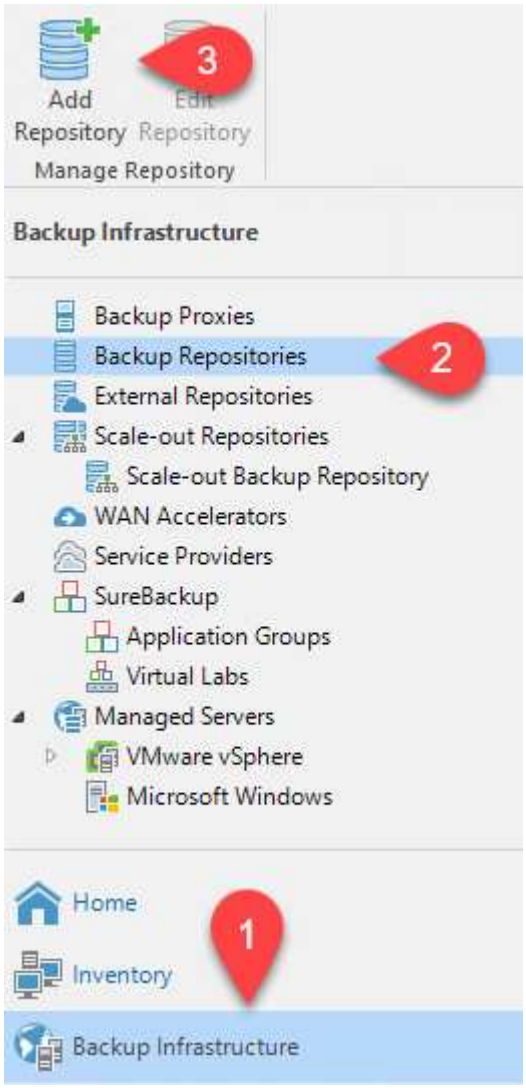
8. Führen Sie alle Schritte im Assistenten für das Neue Backup-Repository aus, um das Repository zu erstellen. Detaillierte Informationen zum Erstellen von Veeam Backup Repositorys finden Sie im "Veeam-Dokumentation".


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

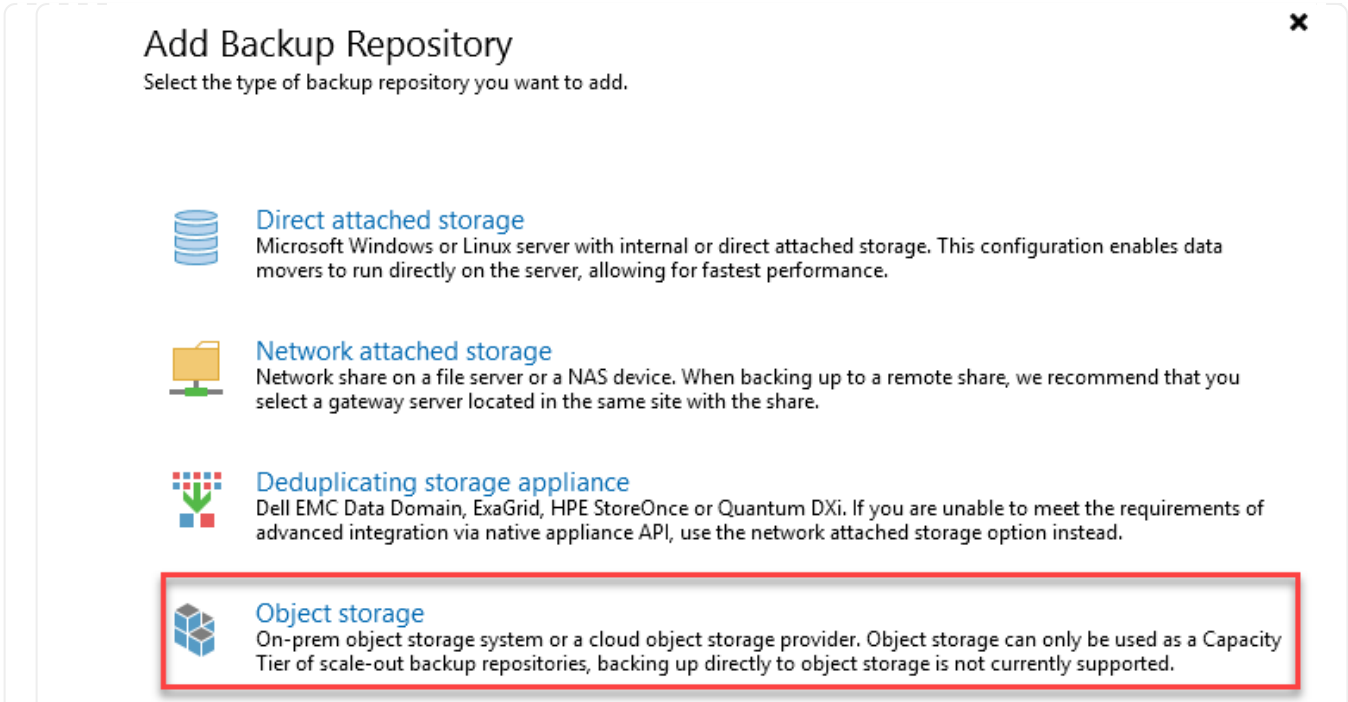
Fügen Sie den Amazon S3-Bucket als Backup-Repository hinzu

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

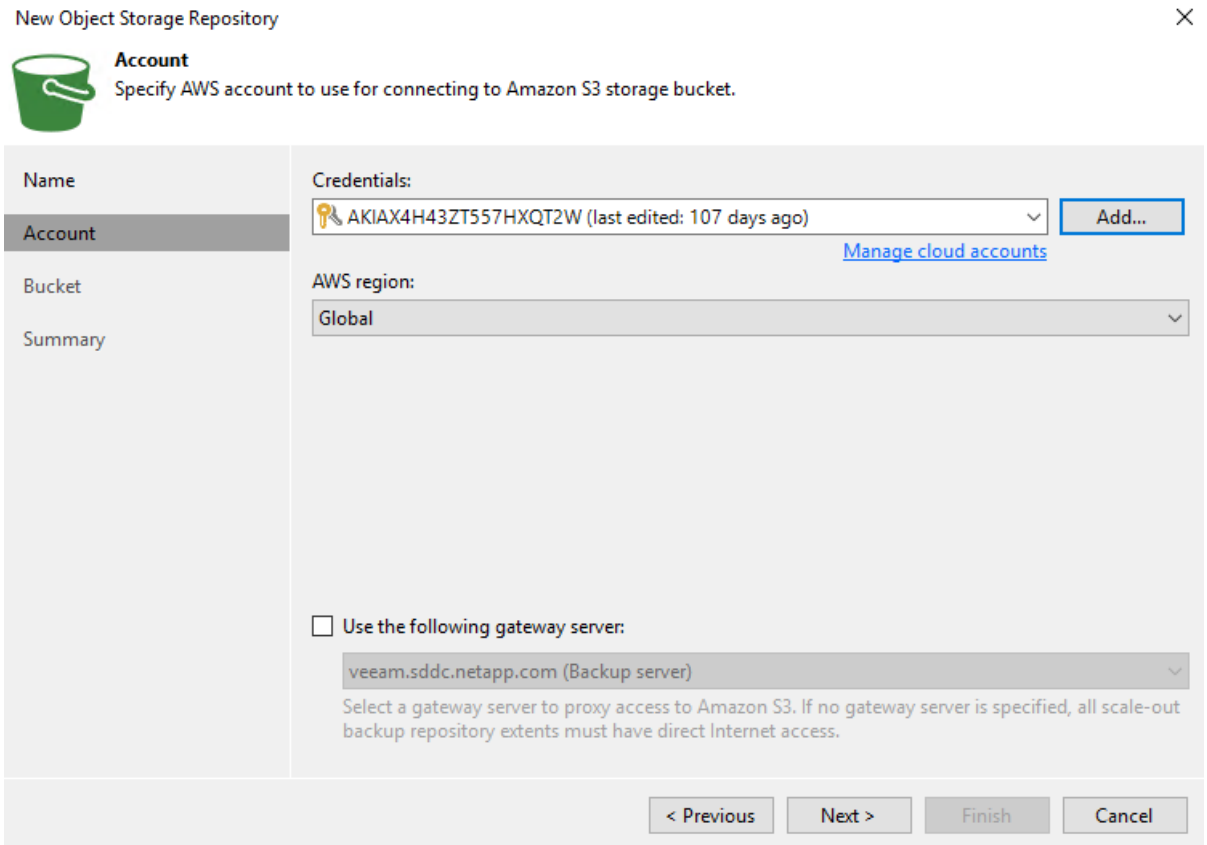
1. Navigieren Sie zu Backup Infrastructure > Backup Repositorys. Klicken Sie Auf Repository Hinzufügen.



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.

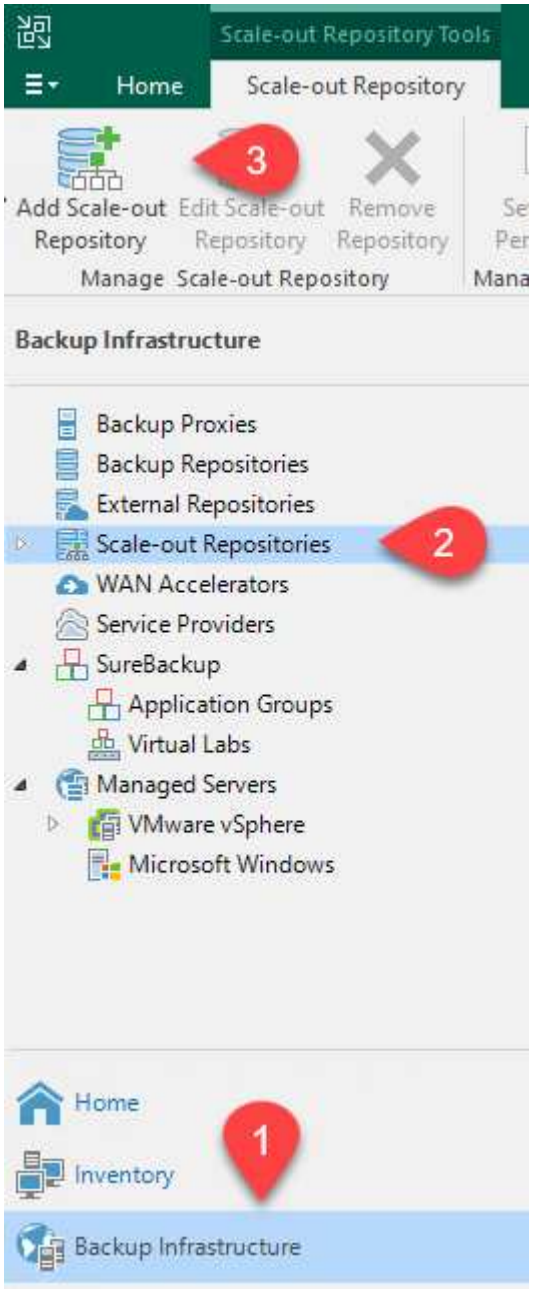


5. Wählen Sie nach dem Laden der Amazon Konfiguration Ihr Datacenter, Ihren Bucket und den Ordner aus und klicken Sie auf Anwenden. Klicken Sie abschließend auf Fertig stellen, um den Assistenten zu schließen.

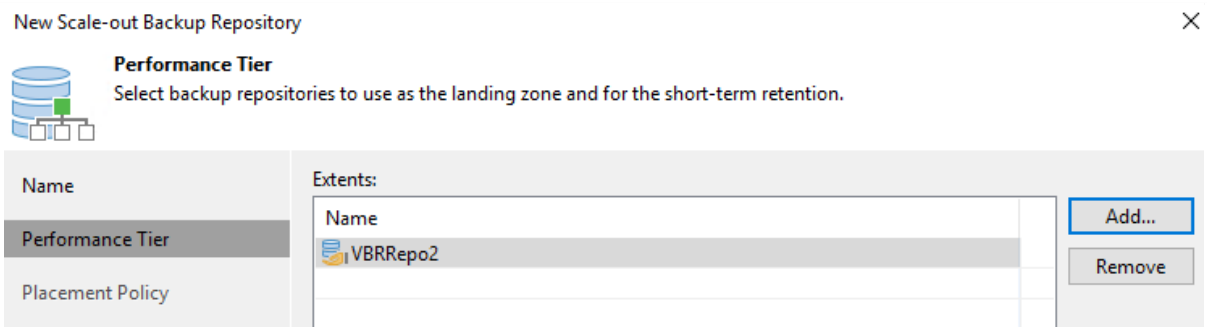
Scale-out-Backup-Repository erstellen

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.

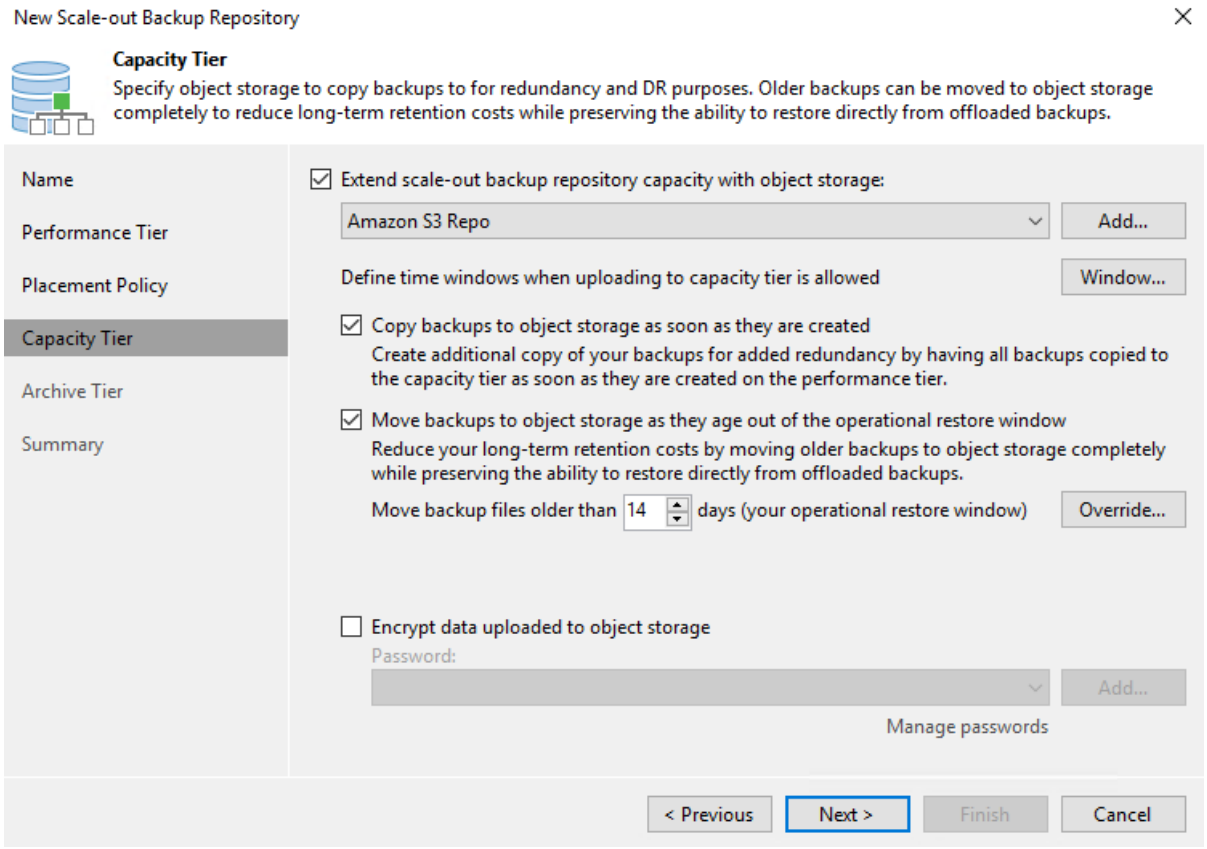
1. Wählen Sie in Backup Infrastructure die Option Scale-Out Repositorys aus, und klicken Sie dann auf das Menüelement Scale-Out Repository hinzufügen.



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.

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.

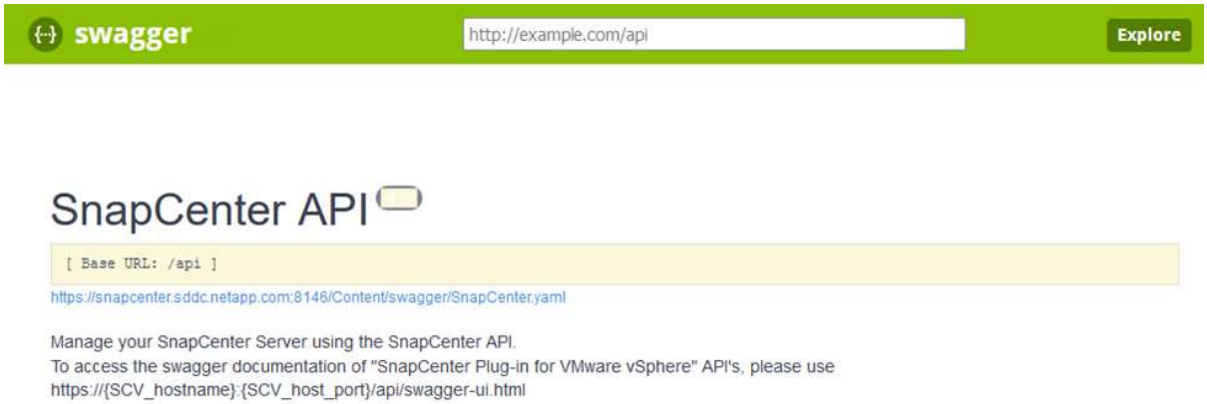
Backup der SnapCenter-Datenbank und -Konfiguration

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".

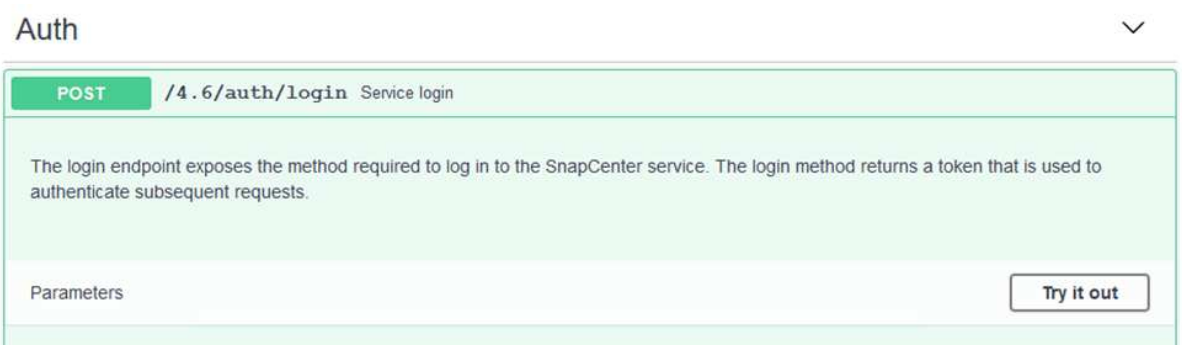
Melden Sie sich bei Swagger an und erhalten Sie ein Autorisierungs-Token

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

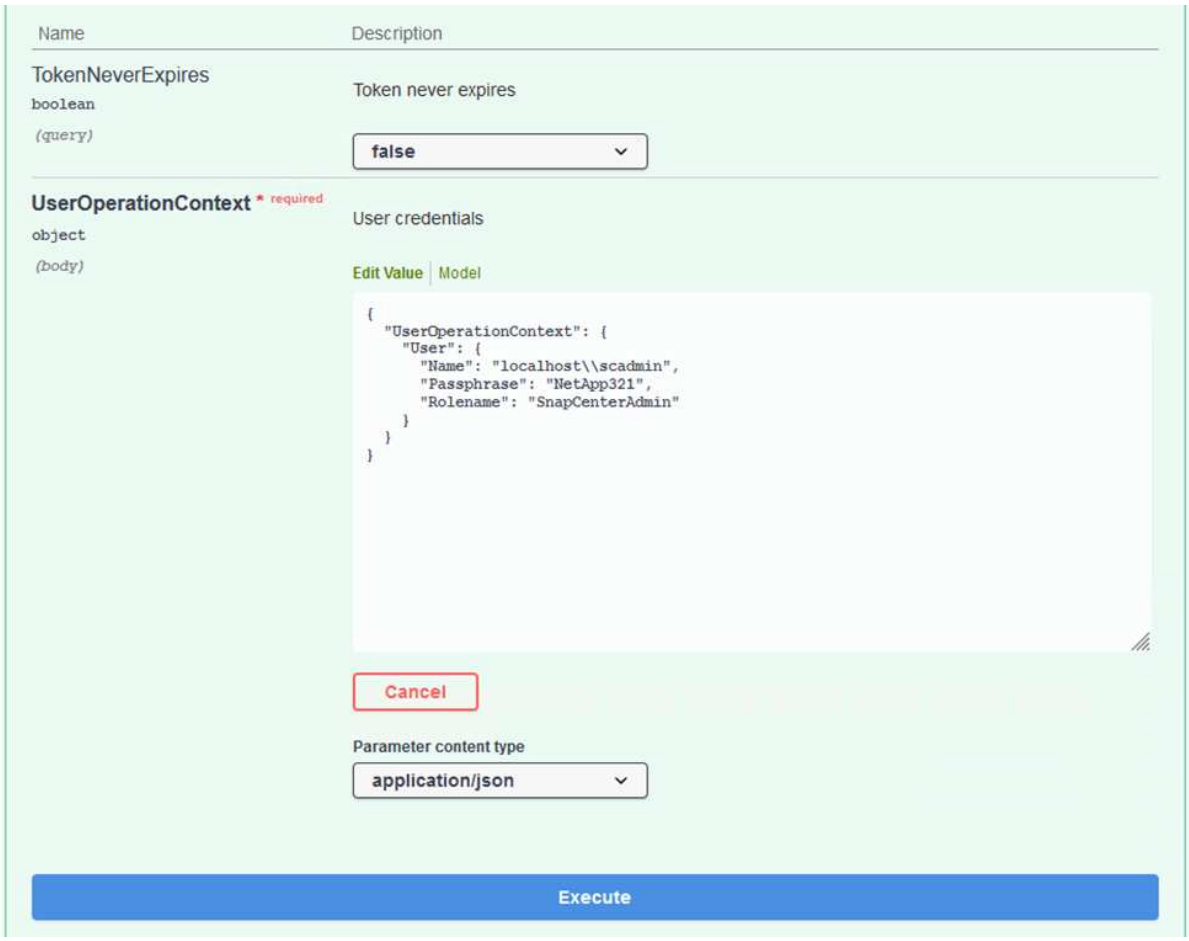
1. Rufen Sie die Webseite der SnapCenter Swagger API auf unter *https://<SnapCenter Server IP>:8146/Swagger/*.



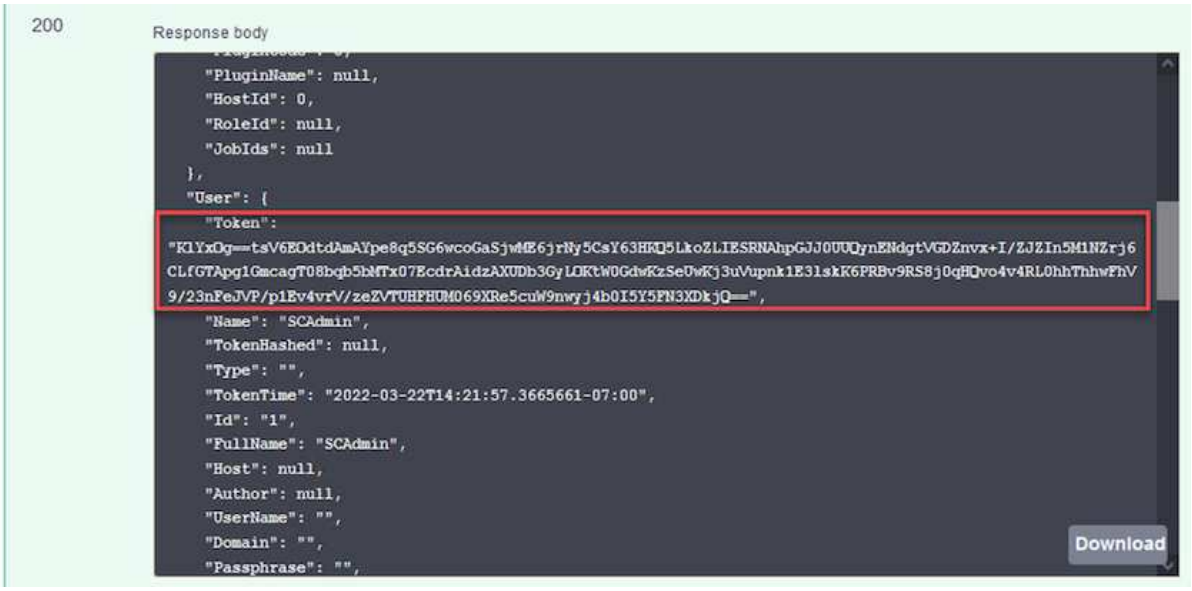
2. Erweitern Sie den Abschnitt „Auth“, und klicken Sie auf „Probieren Sie es aus“.



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



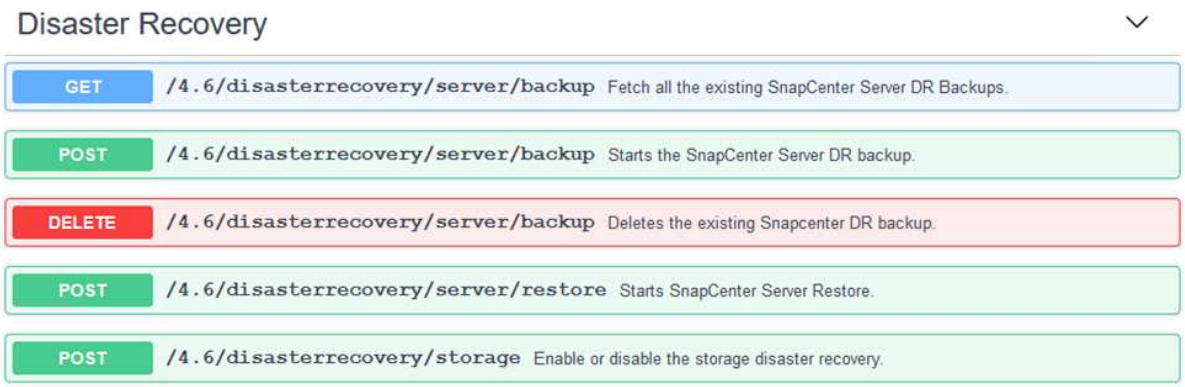
4. Im unten stehenden Antwortkörper können Sie das Token sehen. Kopieren Sie den Token-Text zur Authentifizierung, wenn Sie den Backup-Prozess ausführen.



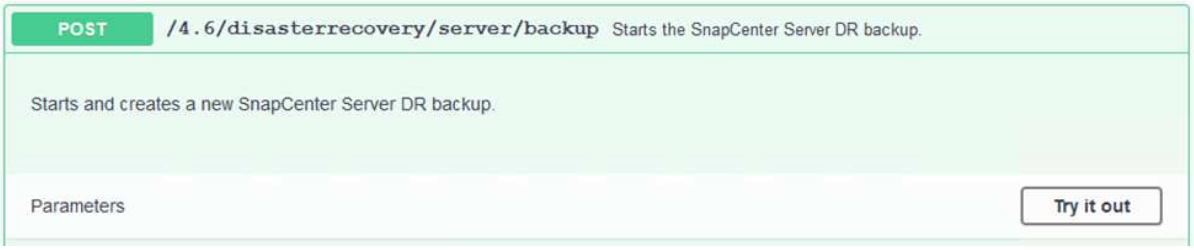
Backup einer SnapCenter-Datenbank durchführen

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.

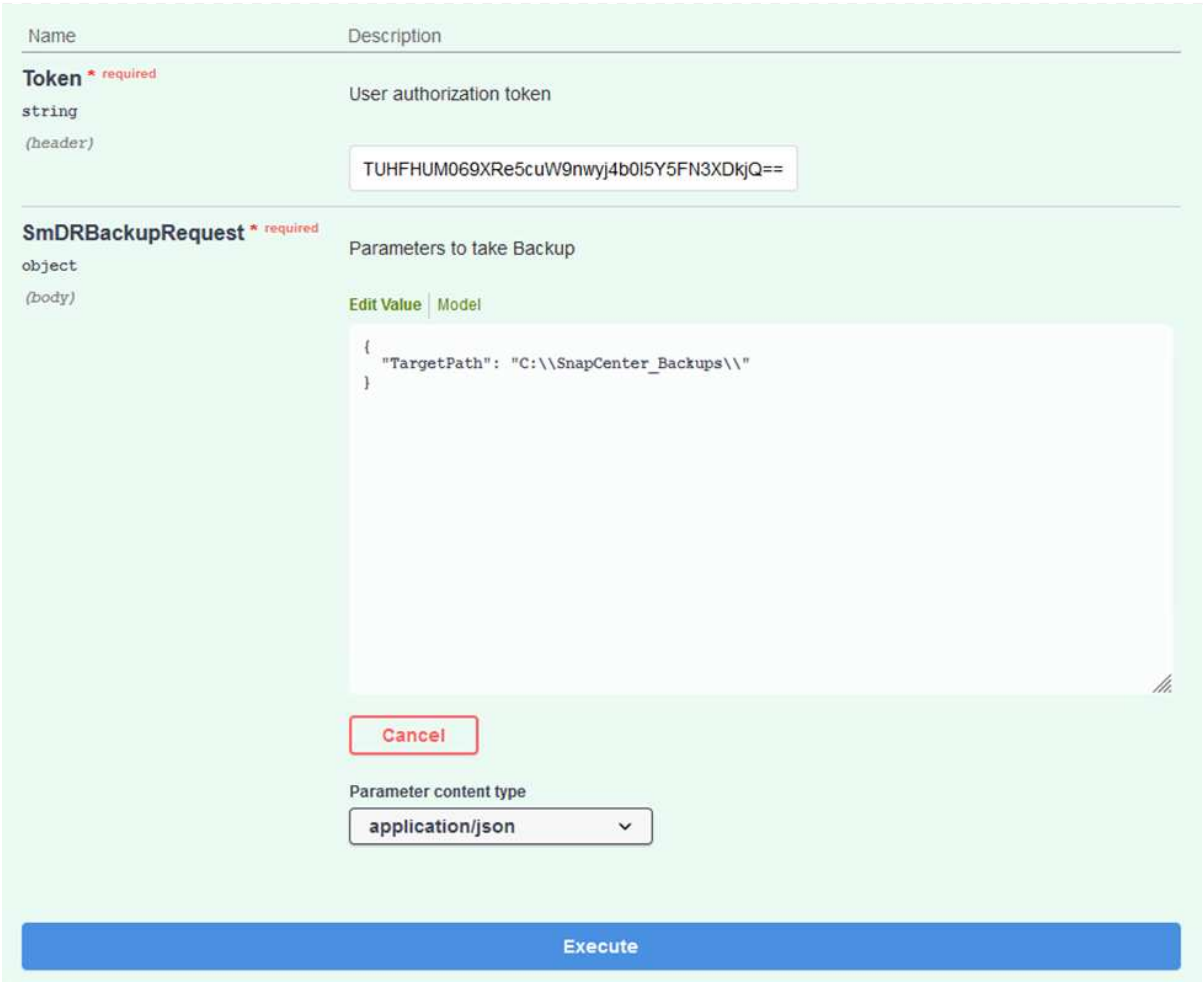


2. Erweitern Sie den `/4.6/disasterrecovery/server/backup` Und klicken Sie auf „Probieren“.



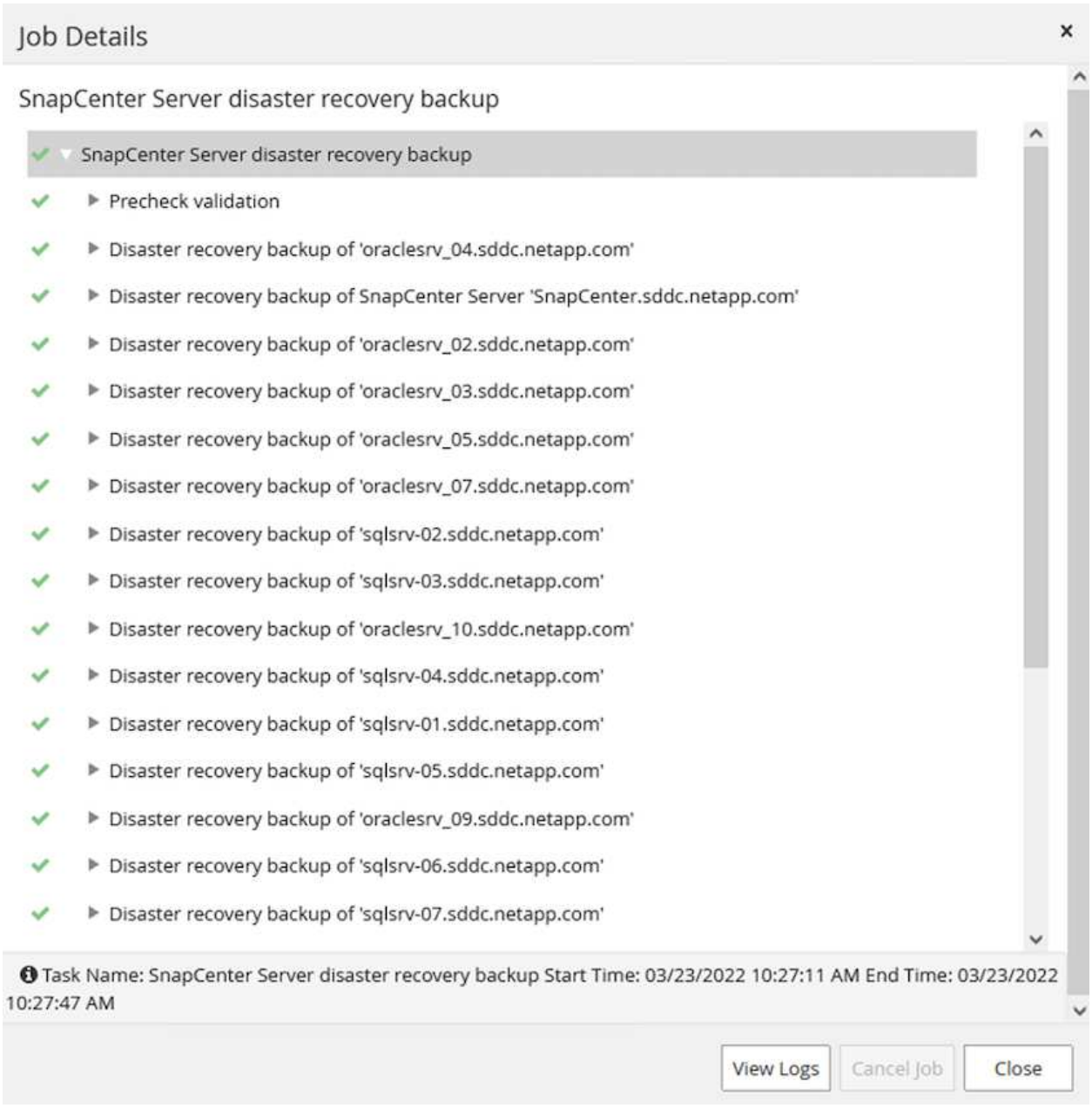
3. Fügen Sie im Abschnitt SmDRBackupRequest den korrekten lokalen Zielpfad hinzu und wählen Sie Ausführen, um das Backup der SnapCenter-Datenbank und -Konfiguration zu starten.

> 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

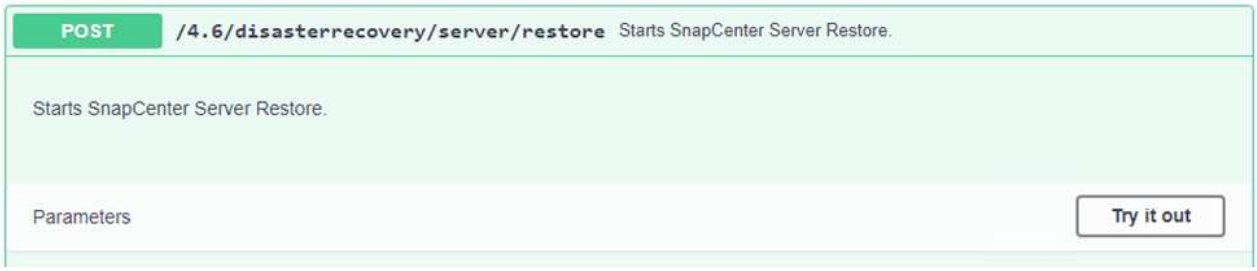
SnapCenter unterstützt Disaster Recovery-Szenarien, da das Backup und Restore seiner MySQL Datenbank und Konfigurationsdateien gestattet werden. So kann ein Administrator regelmäßige Backups der SnapCenter Datenbank im lokalen Datacenter durchführen und diese Datenbank später in einer sekundären SnapCenter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

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

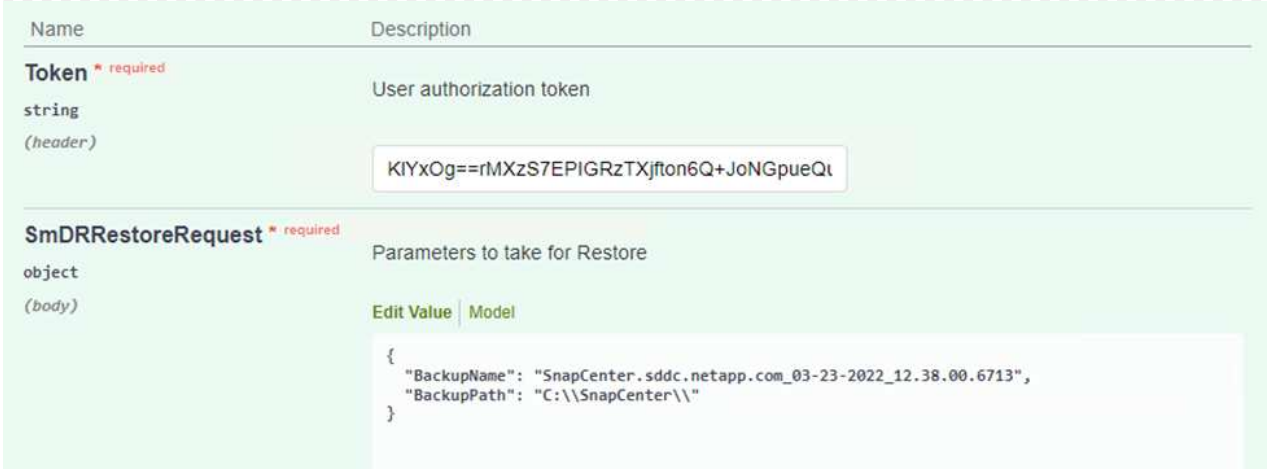
1. SnapMirror Beziehung vom FSX Cluster lösen, wodurch das Volume Lese-/Schreibzugriff ermöglicht.
2. Erstellen Sie (falls erforderlich) einen CIFS-Server und erstellen Sie eine CIFS-Freigabe, die zum Verbindungspfad des geklonten Volume führt.
3. Verwenden Sie xcopy, um die Sicherungsdateien in ein 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:

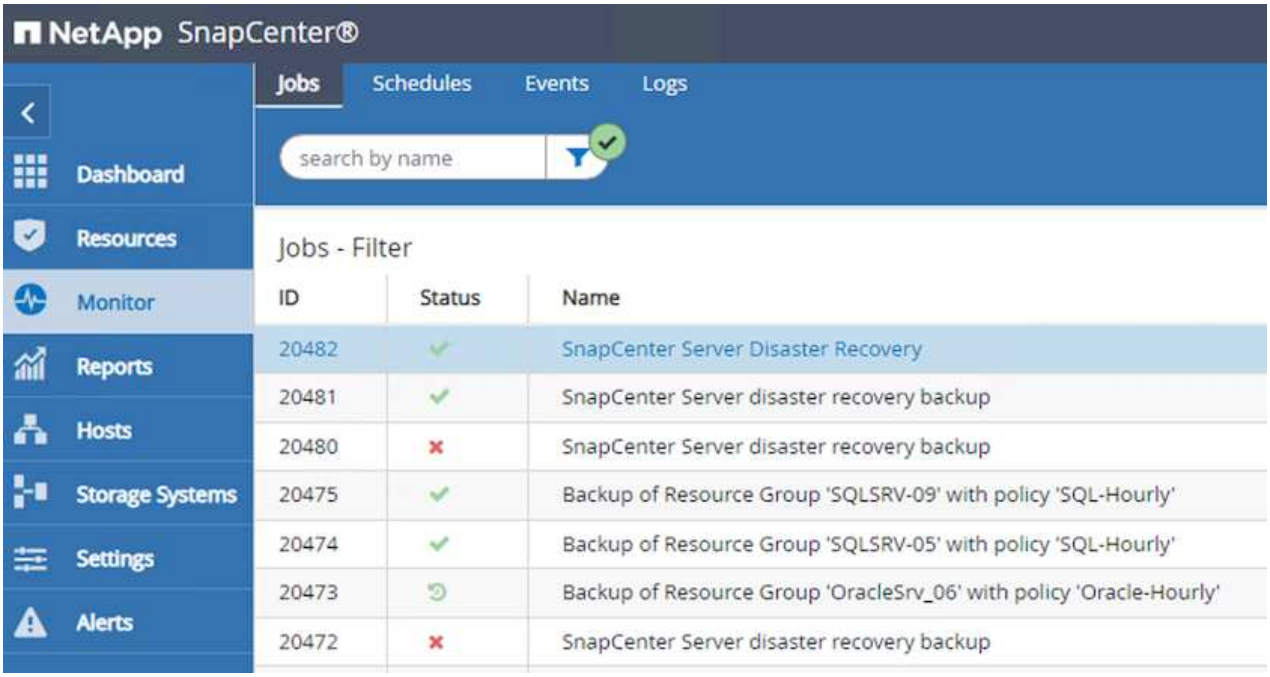
1. Navigieren Sie zur Swagger API-Webseite für den sekundären SnapCenter-Server, und folgen Sie den vorherigen Anweisungen, um ein Autorisierungs-Token zu erhalten.
2. Navigieren Sie auf der Seite Swagger zum Abschnitt Disaster Recovery, und wählen Sie `/4.6/disasterrecovery/server/restore`, Und klicken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

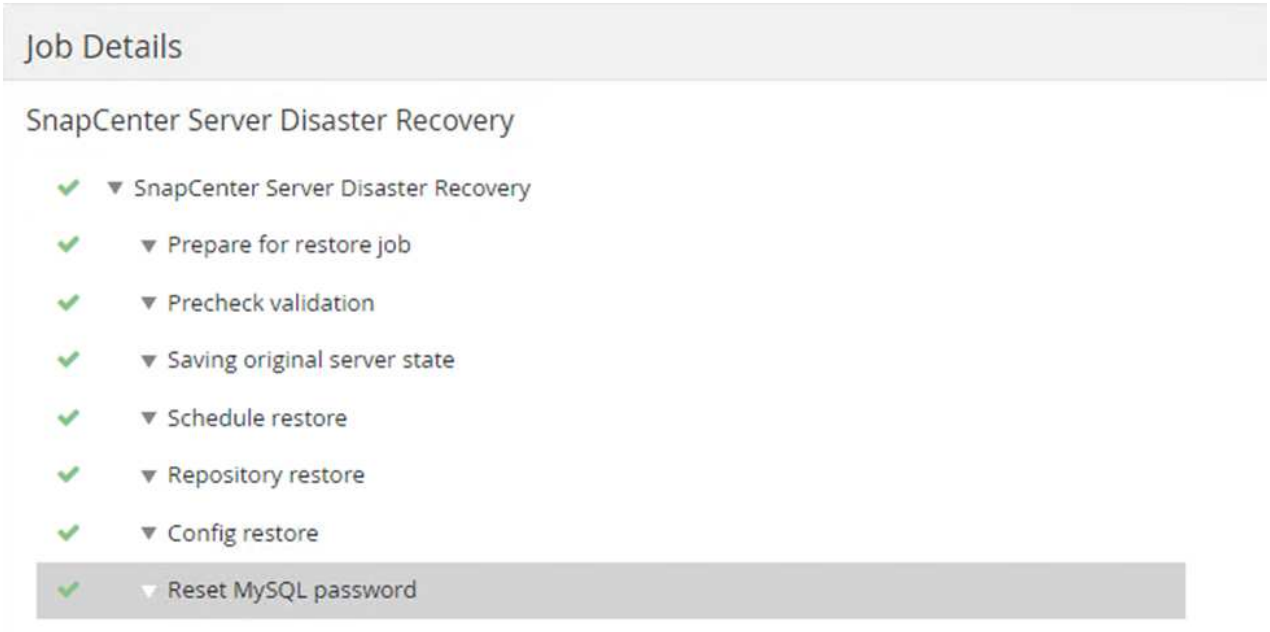


3. Fügen Sie das Autorisierungs-Token ein, und fügen Sie im Abschnitt SmDRResterRequest den Namen des Backups und das lokale Verzeichnis auf dem sekundären SnapCenter-Server ein.



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.





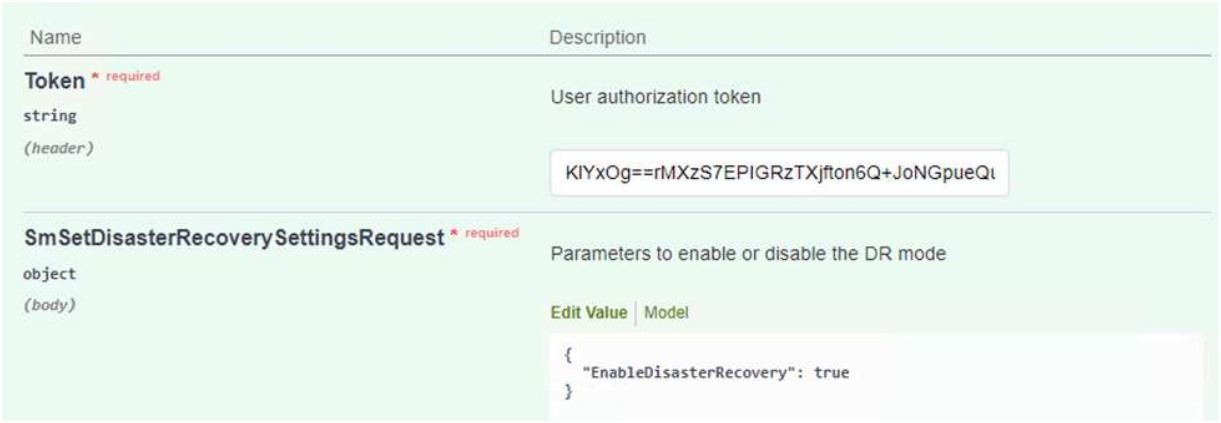
6. Um SQL Server Restores von einem sekundären Storage zu aktivieren, müssen Sie die SnapCenter-Datenbank in den Disaster Recovery-Modus schalten. Dies wird als separate Operation durchgeführt und auf der Swagger API Webseite initiiert.

   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.

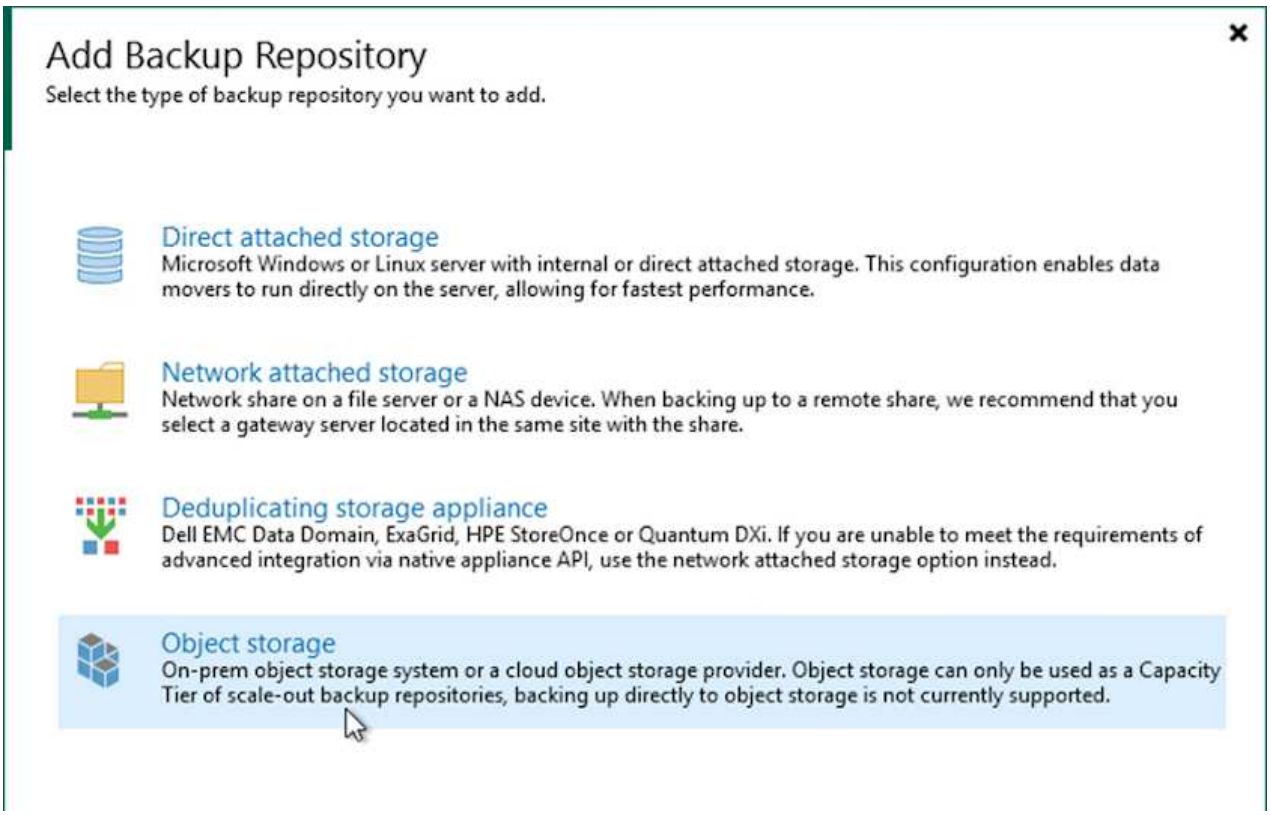
Wiederherstellung von Applikations-VMs mit vollständiger Veeam-Wiederherstellung

Backup-Repository erstellen und Backups aus S3 importieren

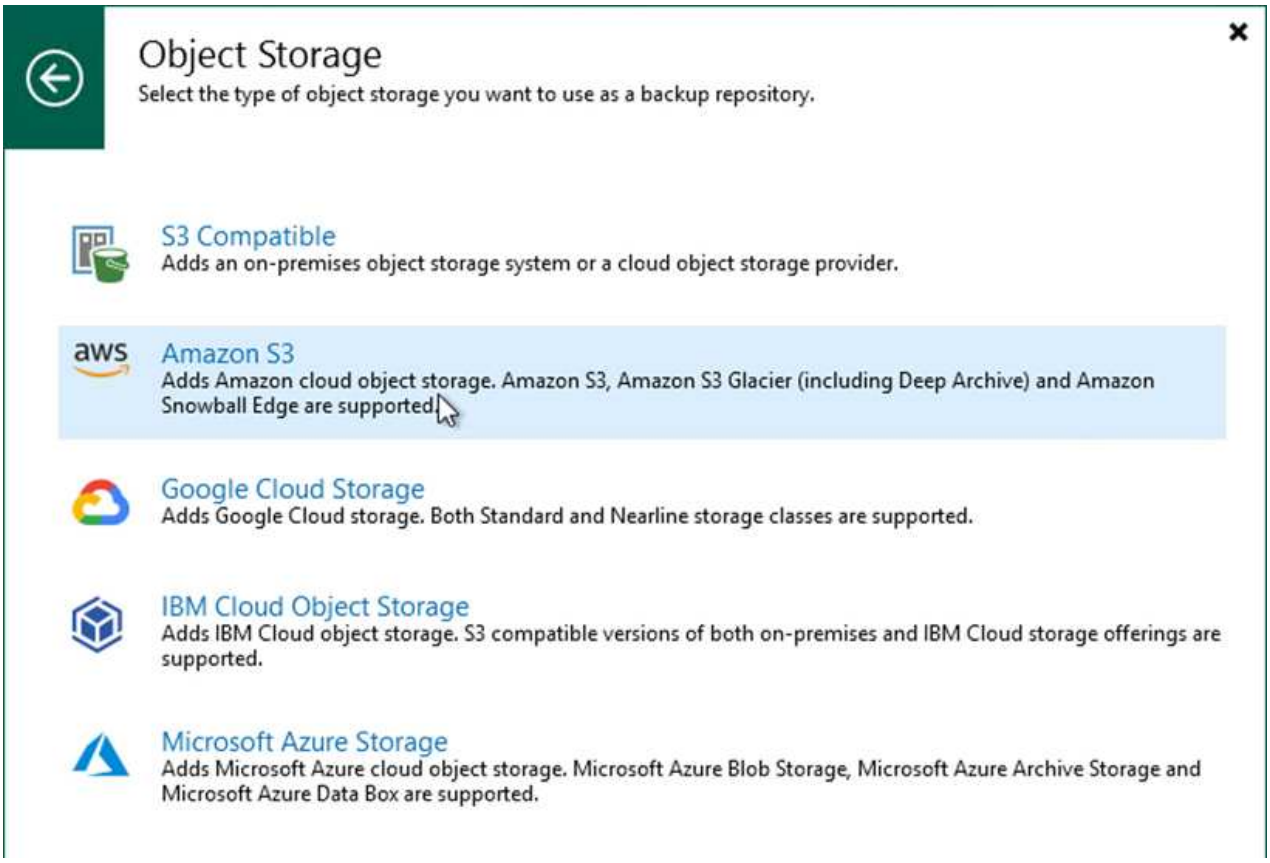
Importieren Sie vom sekundären Veeam-Server die Backups aus S3 Storage und stellen Sie SQL Server und Oracle VMs in Ihr VMware Cloud-Cluster wieder her.

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.

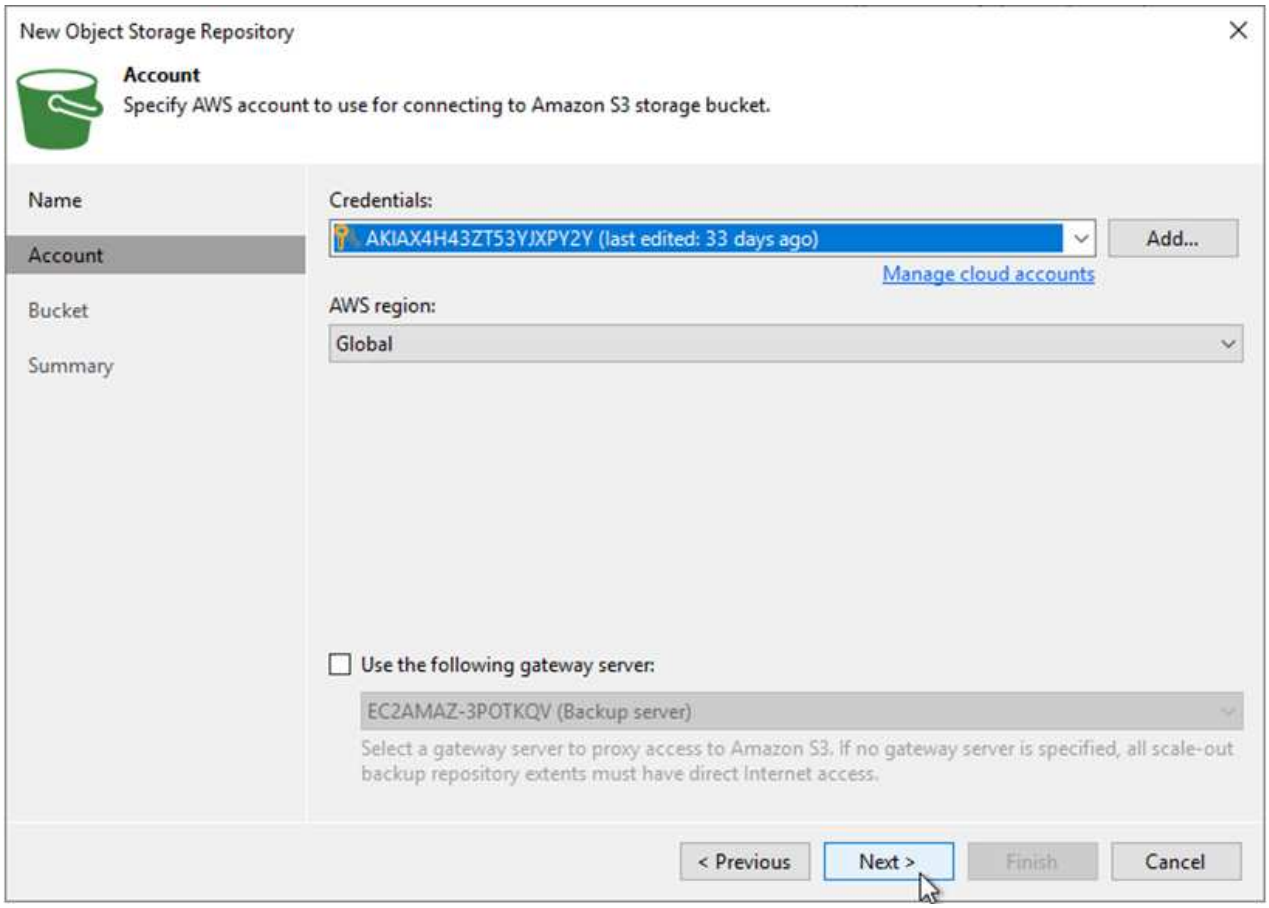


2. Wählen Sie Amazon S3 als Objektspeichertyp aus.

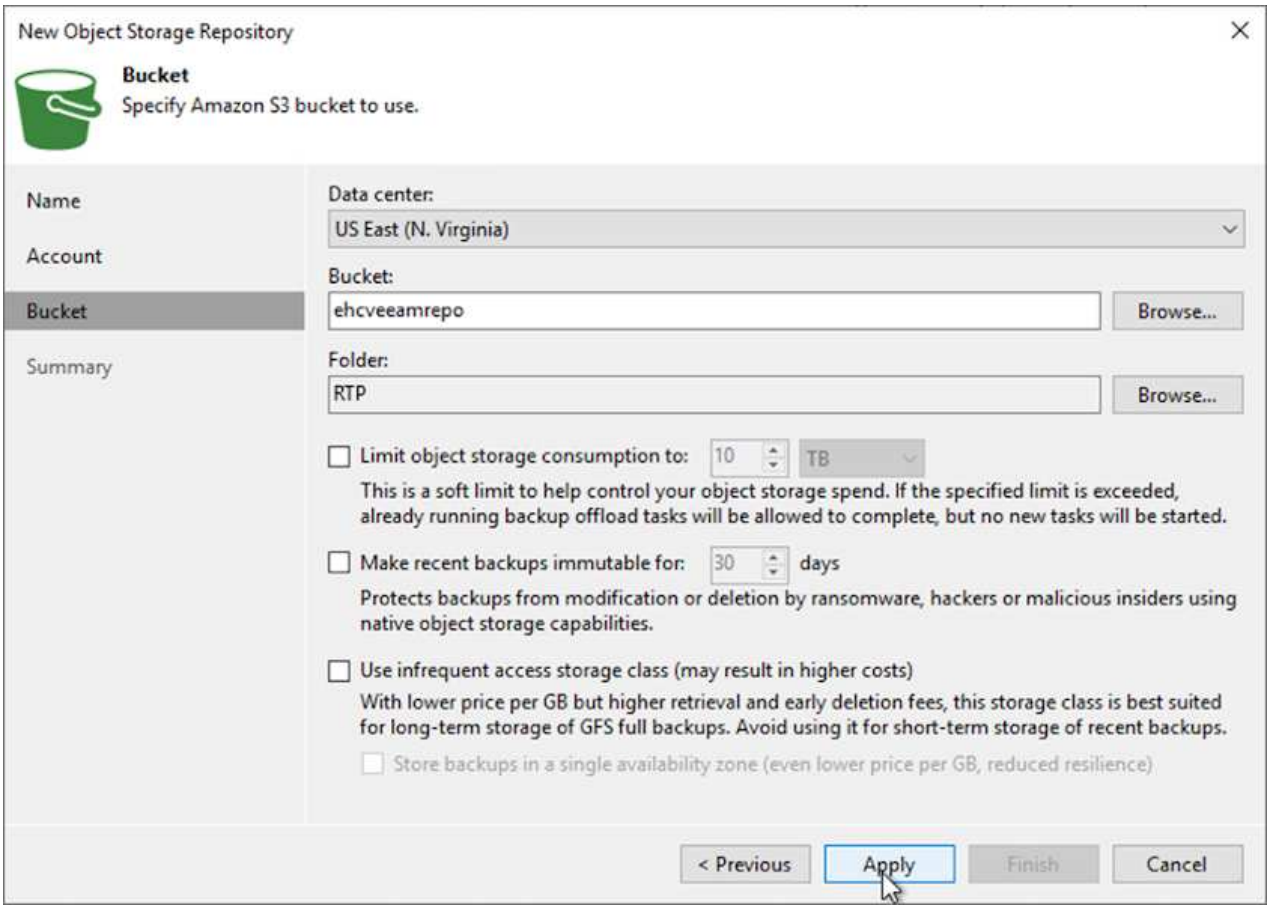


3. Wählen Sie aus der Liste der Amazon Cloud Storage Services Amazon S3 aus.

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.

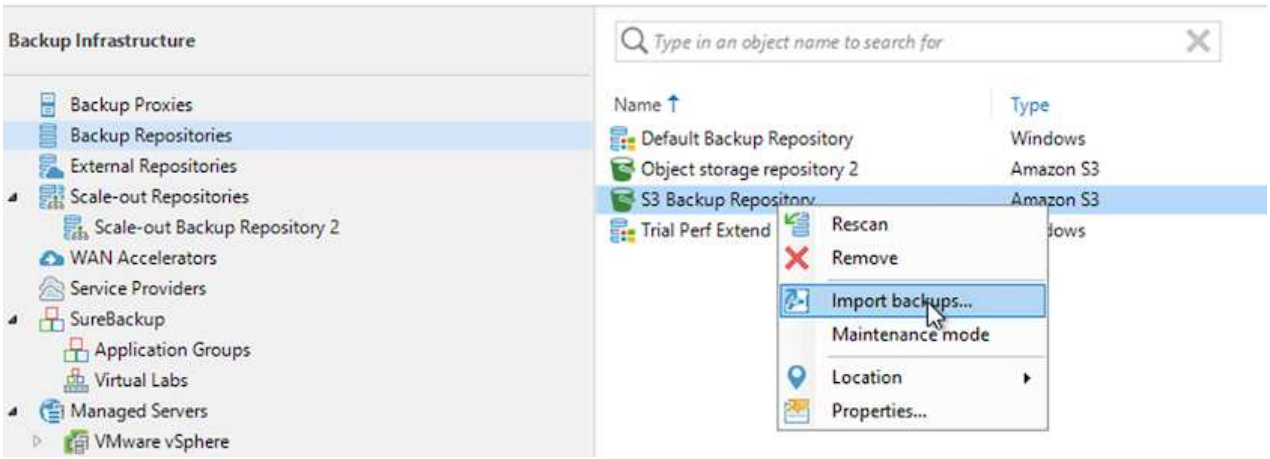


6. Wählen Sie abschließend Fertigstellen aus, um den Prozess abzuschließen und das Repository hinzuzufügen.

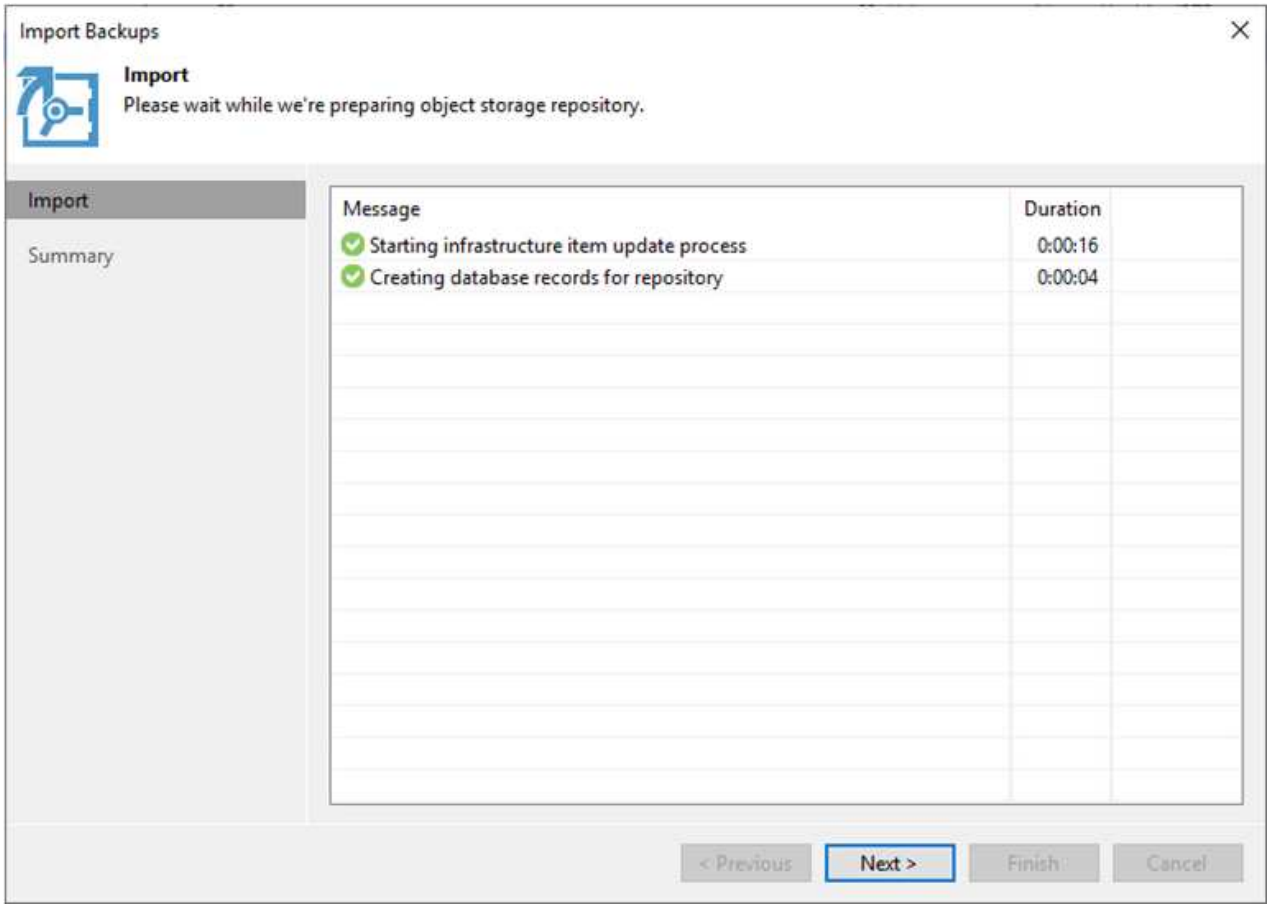
Backups aus S3 Objekt-Storage importieren

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

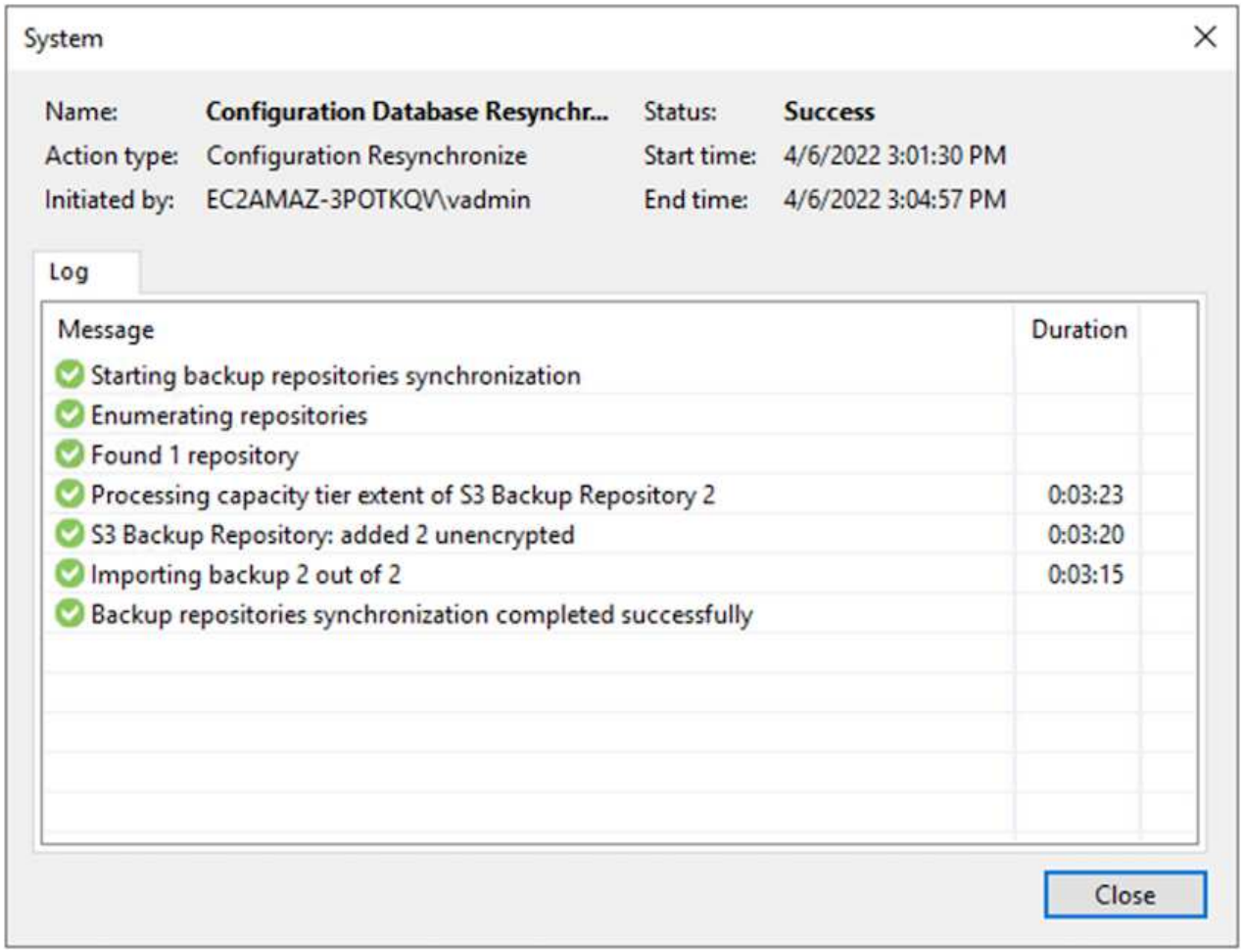
1. Wählen Sie aus dem S3-Backup-Repository die Option Backups importieren aus, um den Assistenten zum Importieren von Backups zu starten.



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



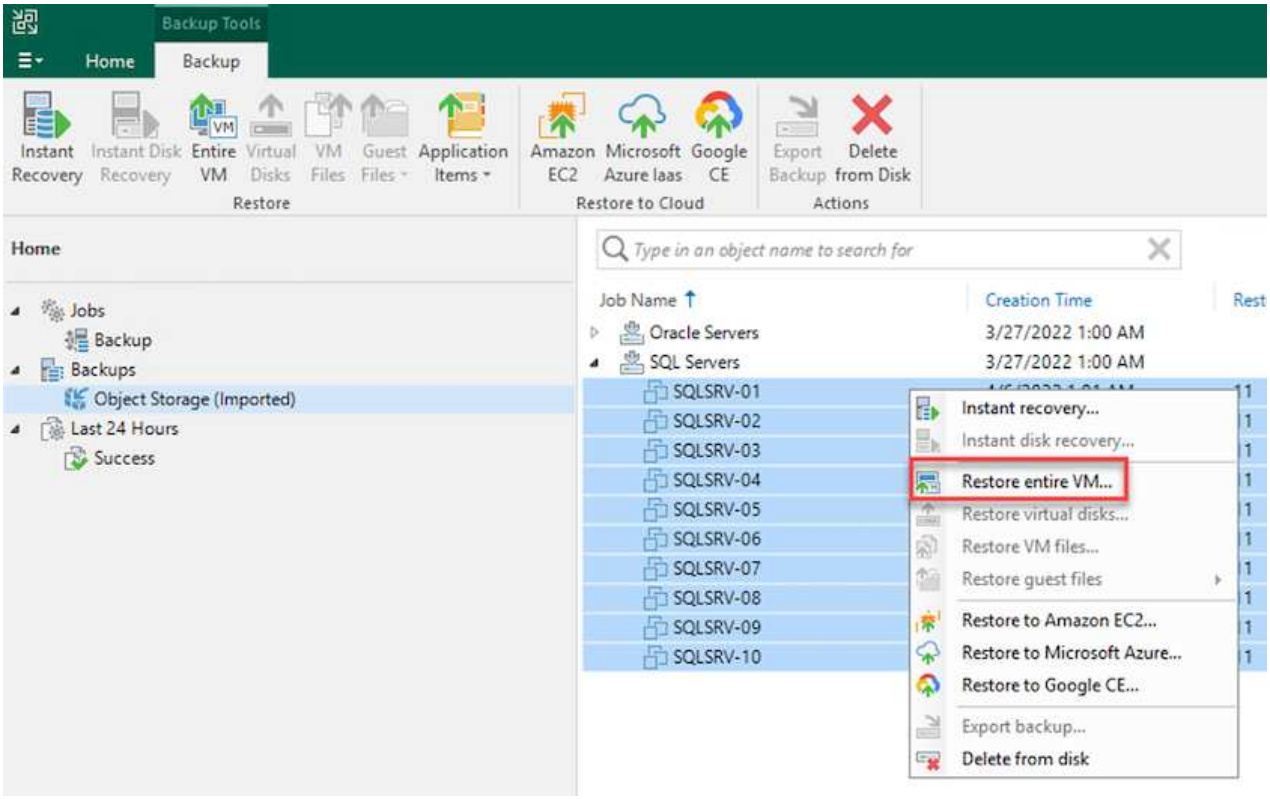
3. Nach Abschluss des Imports können Sie die VMs in das VMware Cloud Cluster wiederherstellen.


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

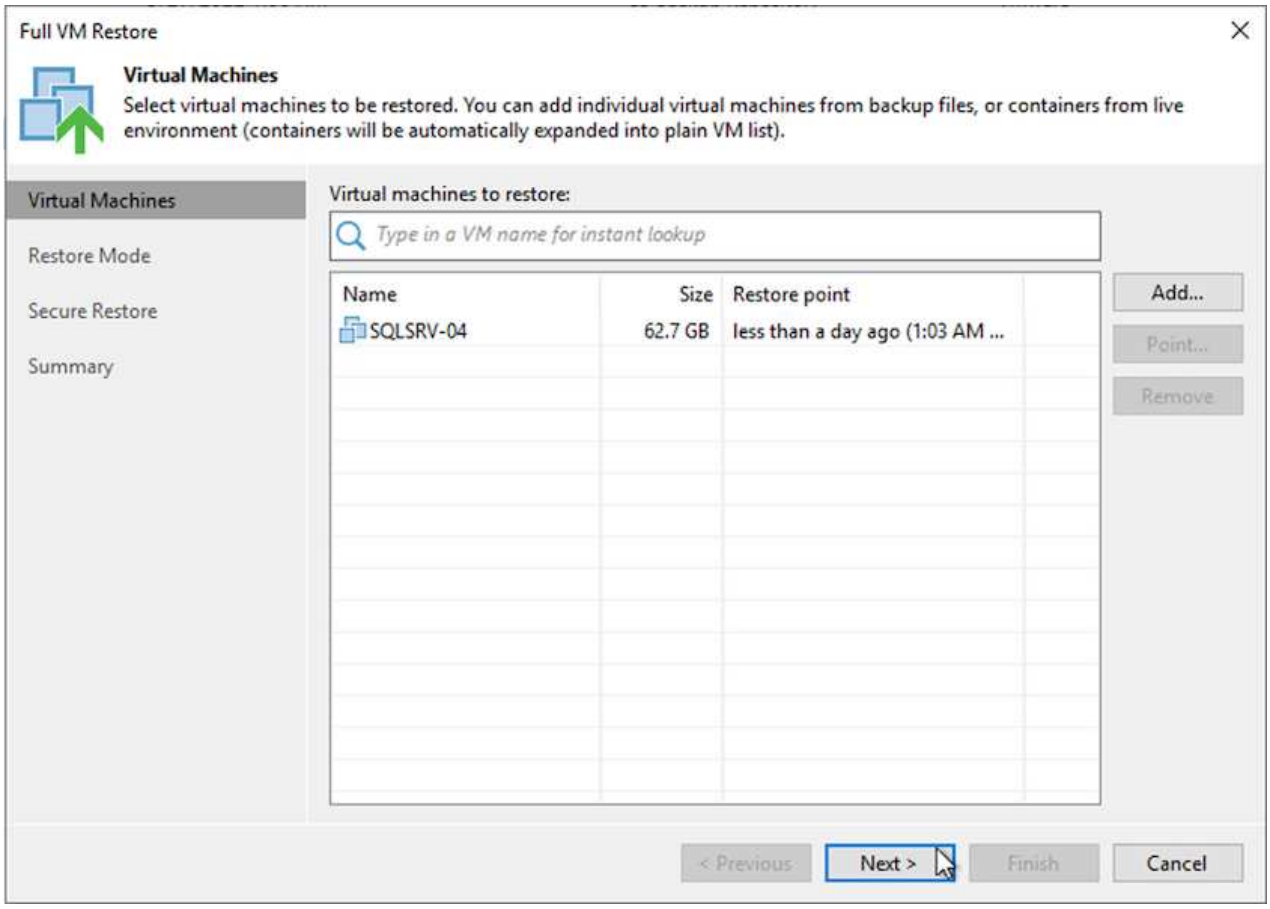
Wiederherstellung von Applikations-VMs mit vollständiger Wiederherstellung durch Veeam in VMware Cloud

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

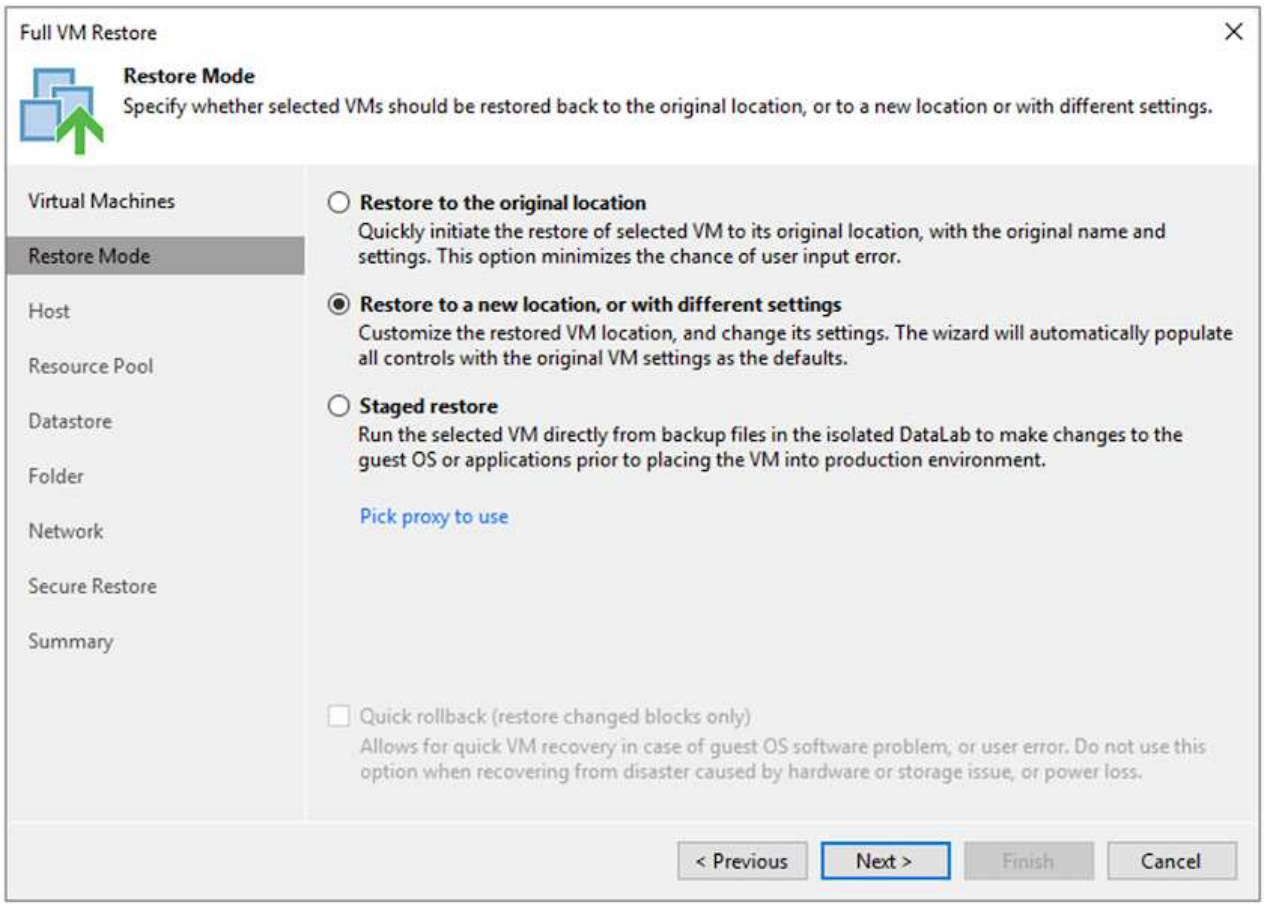
1. Wählen Sie auf der Veeam-Startseite den Objektspeicher aus, der die importierten Backups enthält, wählen Sie die wiederherzustellenden VMs aus, und klicken Sie dann mit der rechten Maustaste, und wählen Sie die Option gesamte VM wiederherstellen aus.



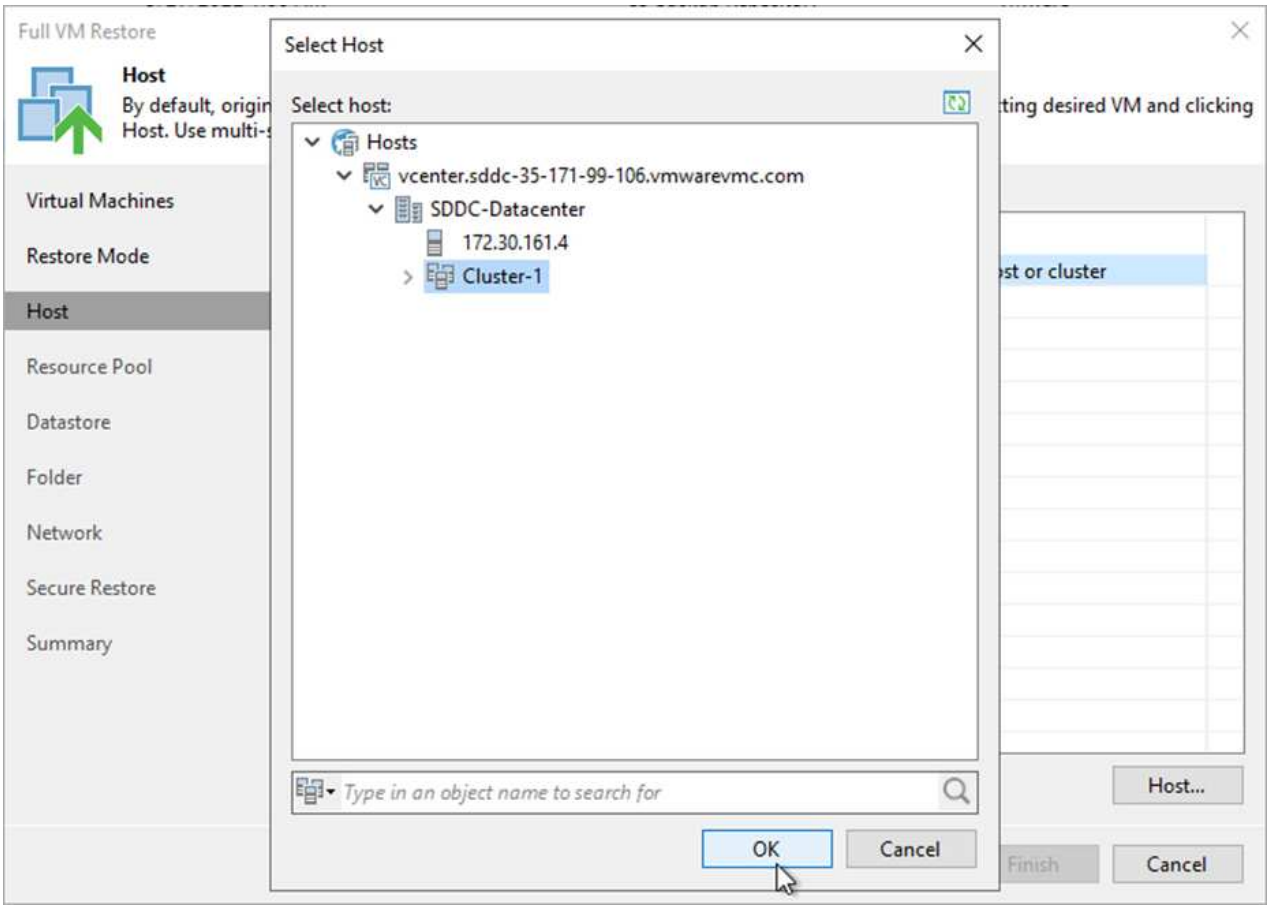
2. Ändern Sie auf der ersten Seite des Assistenten zur vollständigen VM-Wiederherstellung die VMs, die gesichert werden sollen, falls gewünscht, und wählen Sie Weiter.



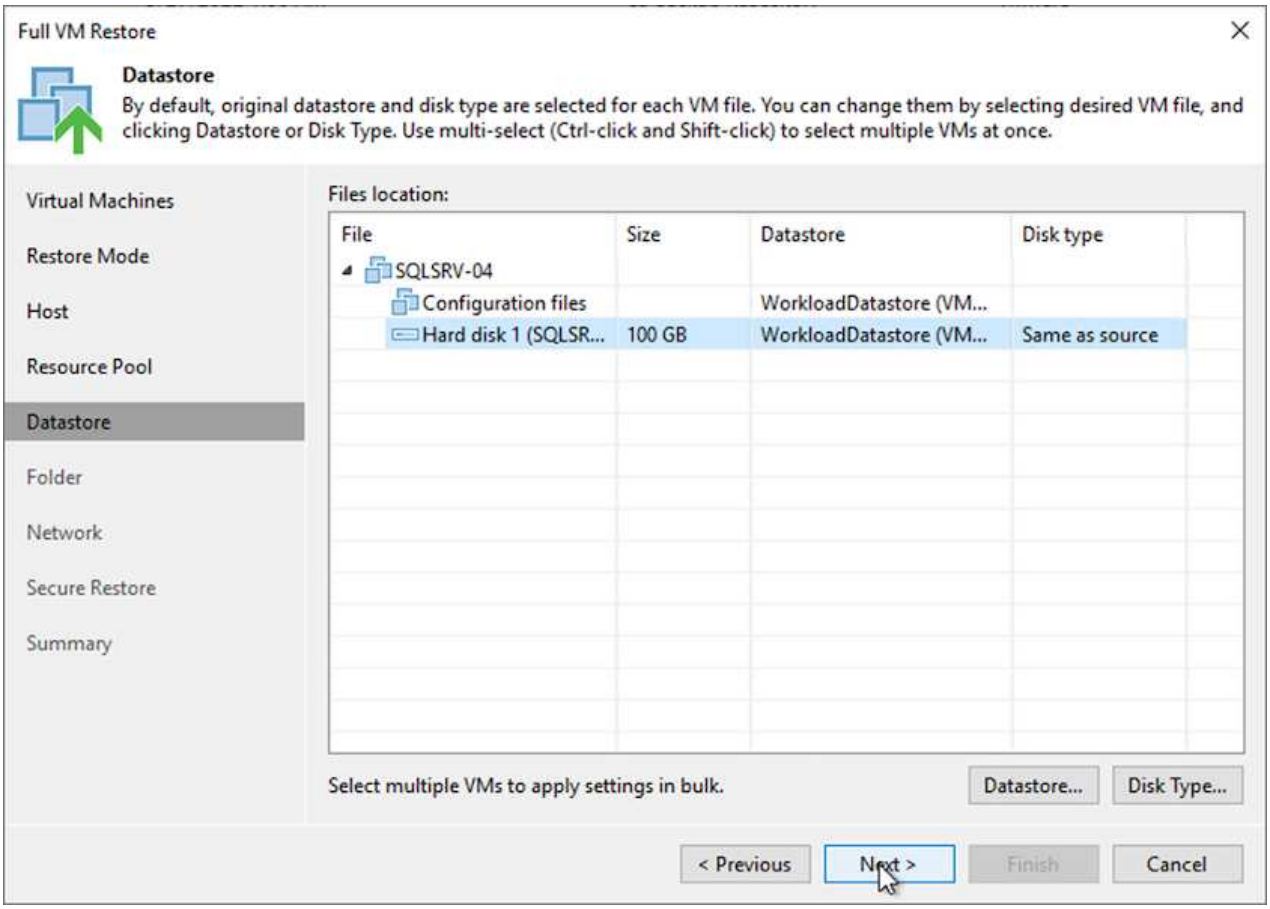
3. Wählen Sie auf der Seite Wiederherstellungsmodus die Option Wiederherstellen an einem neuen Speicherort oder mit anderen Einstellungen.



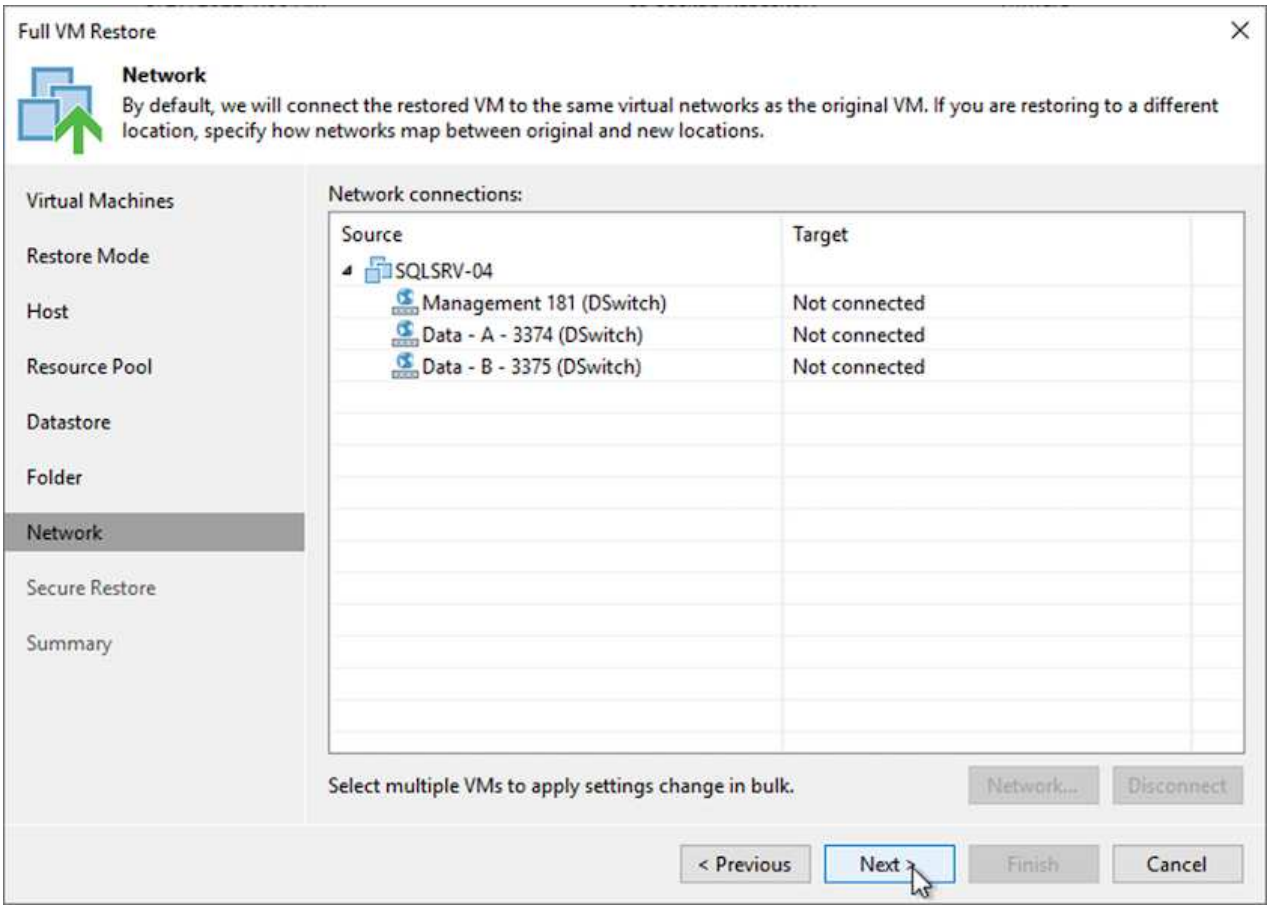
4. Wählen Sie auf der Host-Seite den Ziel-ESXi-Host oder das Ziel-Cluster aus, auf dem die VM wiederhergestellt werden soll.

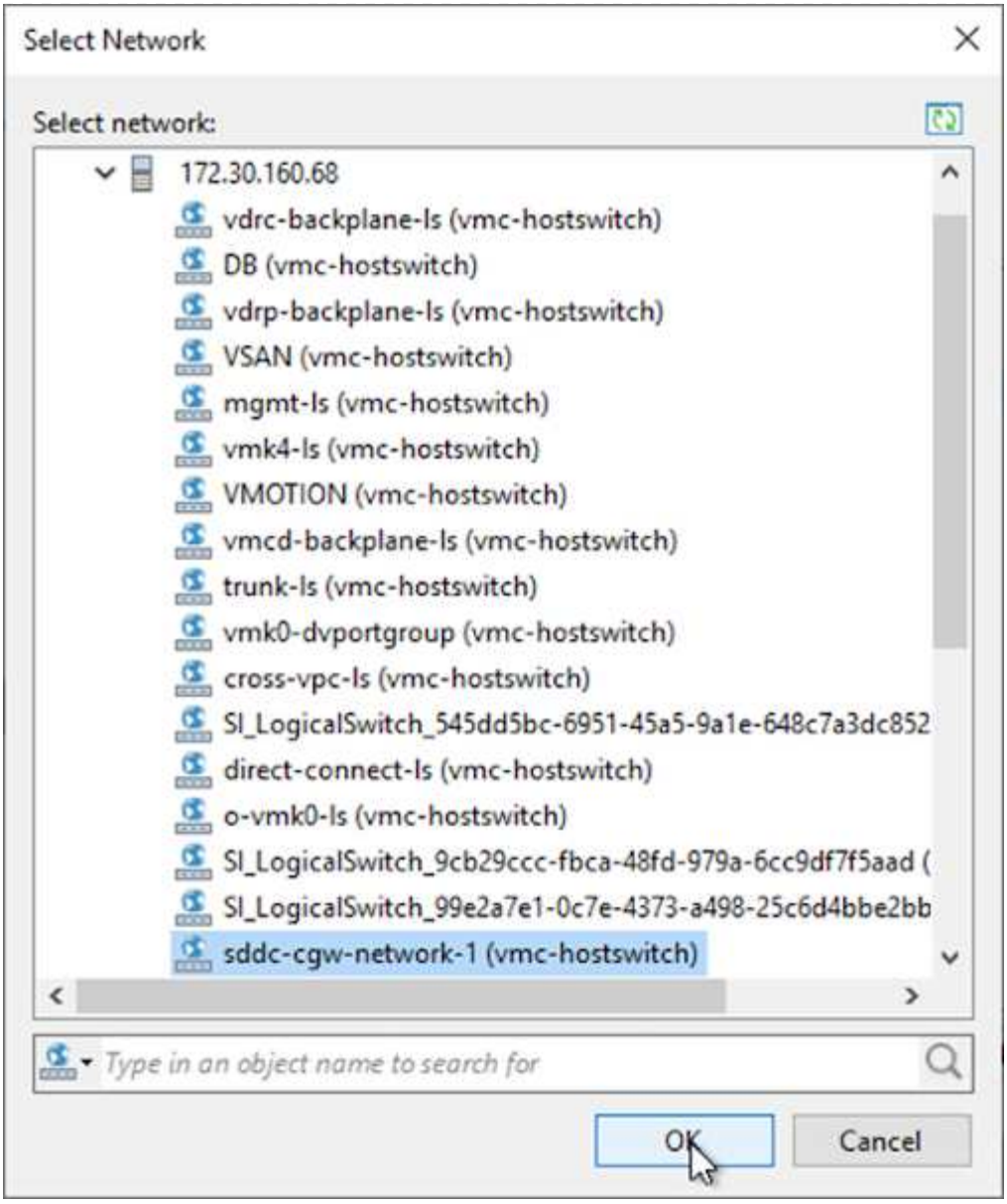


5. Wählen Sie auf der Seite Datastores den Speicherort des Ziel-Datenspeichers für die Konfigurationsdateien und die Festplatte aus.



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
```

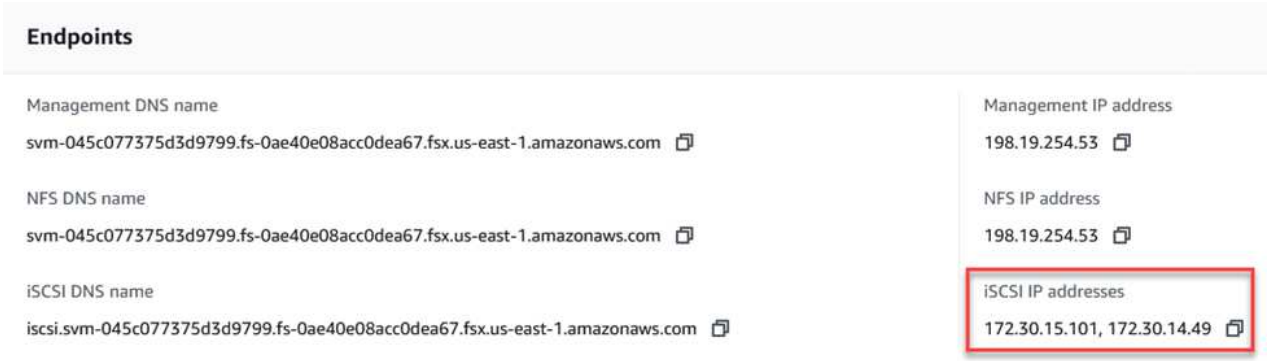
3. Schließlich ordnen Sie die LUNs der Initiatorgruppe zu, die Sie gerade erstellt haben:

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

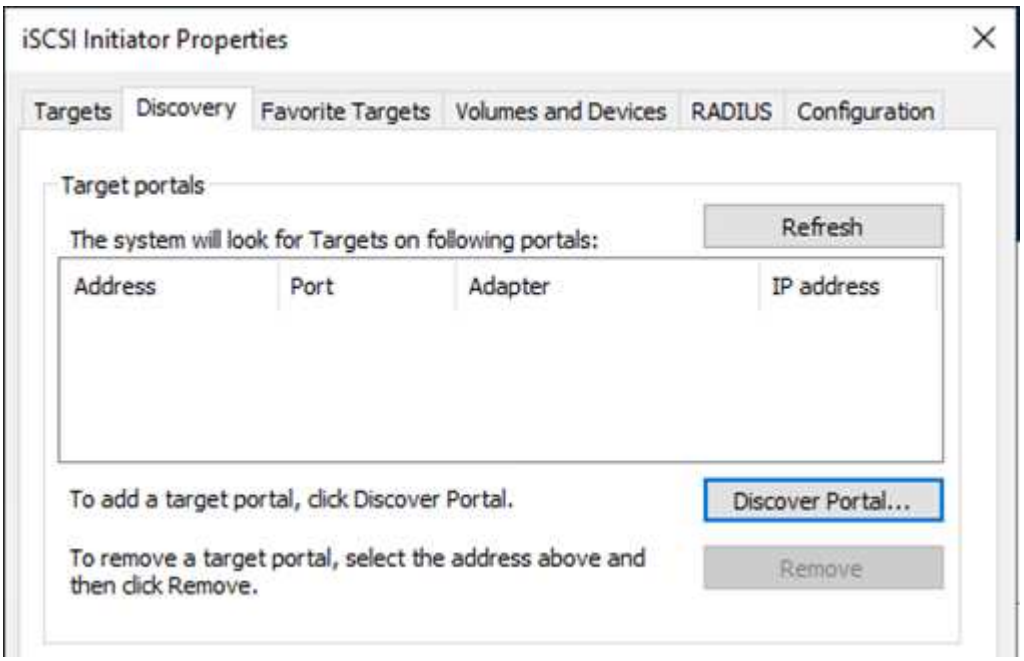
4. Um den Namen des Pfads zu finden, führen Sie den aus `lun show` Befehl.

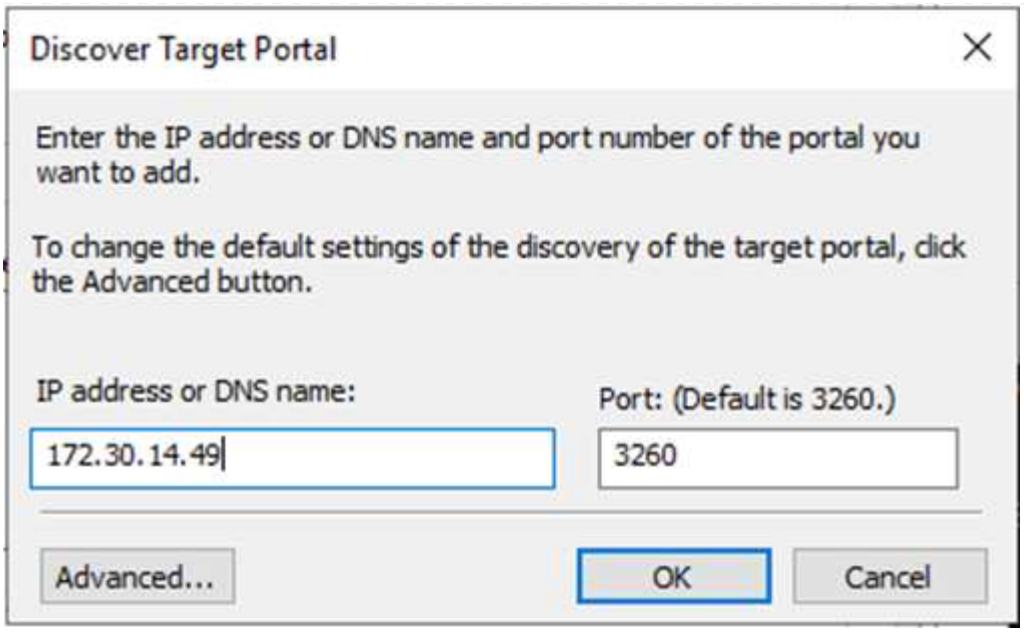
Richten Sie Windows VM für iSCSI-Zugriff ein und ermitteln Sie die Dateisysteme

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.

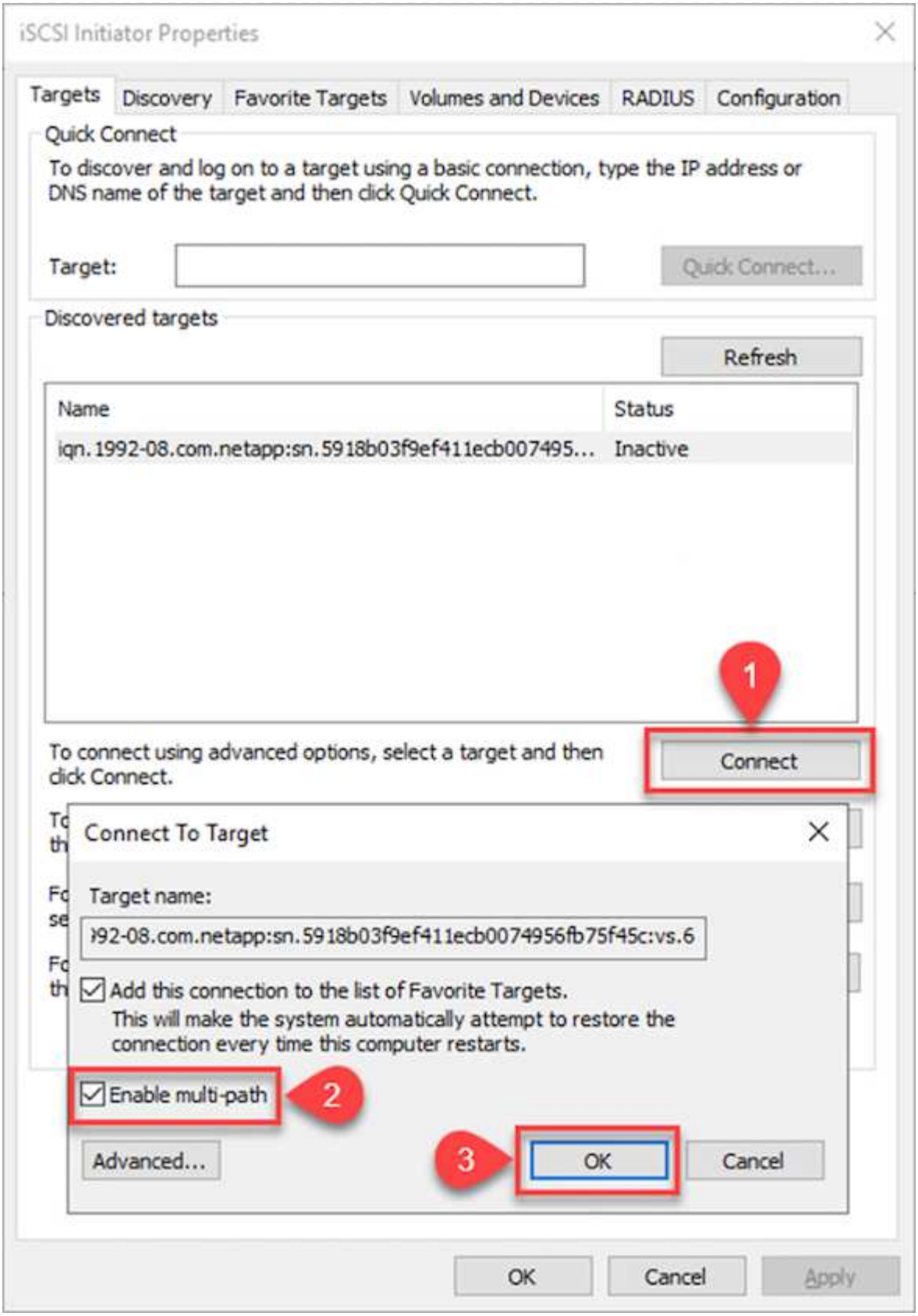


4. Klicken Sie auf der Registerkarte Erkennung auf Portal ermitteln, und geben Sie die IP-Adressen für Ihre FSX-iSCSI-Ziele ein.

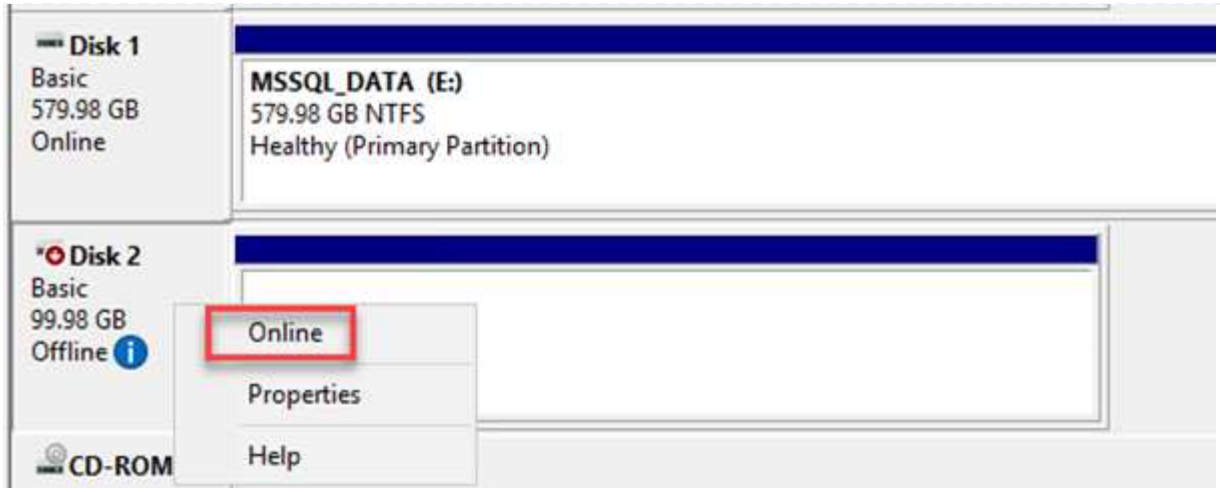




5. Klicken Sie auf der Registerkarte Ziel auf Verbinden, wählen Sie gegebenenfalls Multi-Path aktivieren für Ihre Konfiguration aus, und klicken Sie dann auf OK, um eine Verbindung zum Ziel herzustellen.

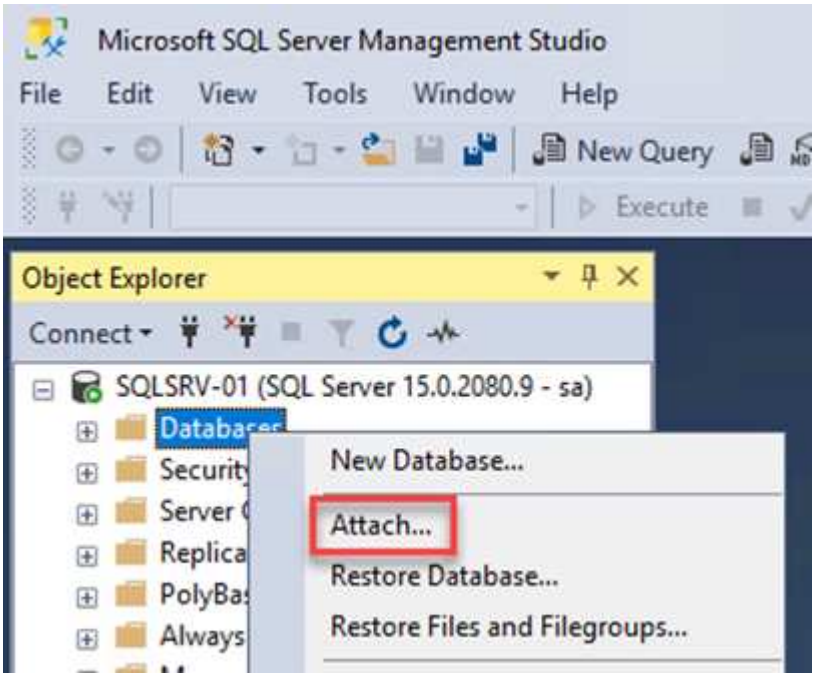


6. Öffnen Sie das Computer Management-Dienstprogramm, und bringen Sie die Laufwerke online. Vergewissern Sie sich, dass sie die gleichen Laufwerksbuchstaben wie zuvor gehalten haben.

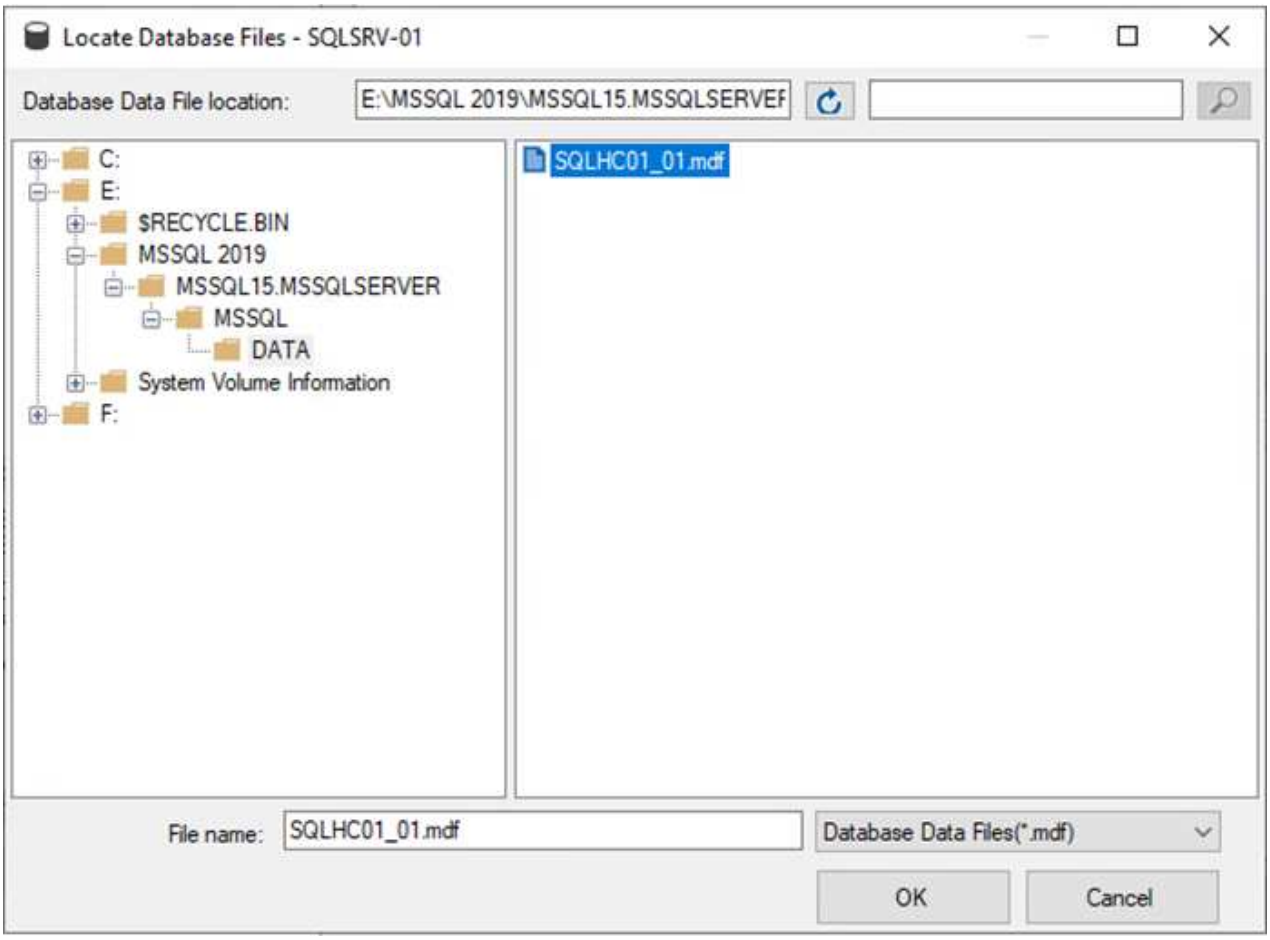

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Verbinden Sie die SQL Server-Datenbanken

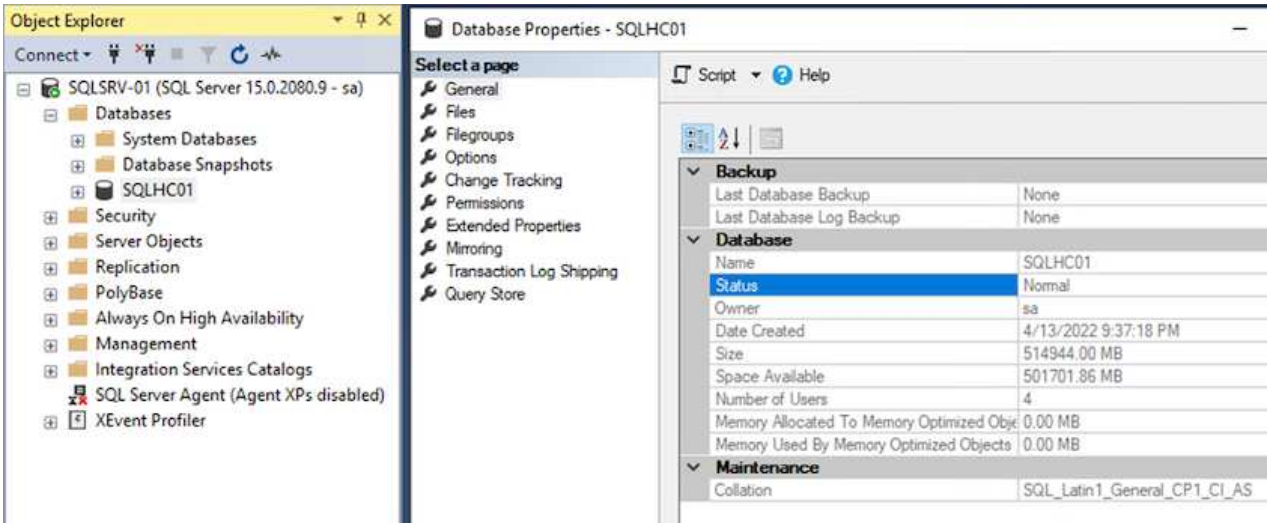
1. Öffnen Sie in der SQL Server VM Microsoft SQL Server Management Studio, und wählen Sie Attach aus, um den Prozess der Verbindung zur Datenbank zu starten.



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.

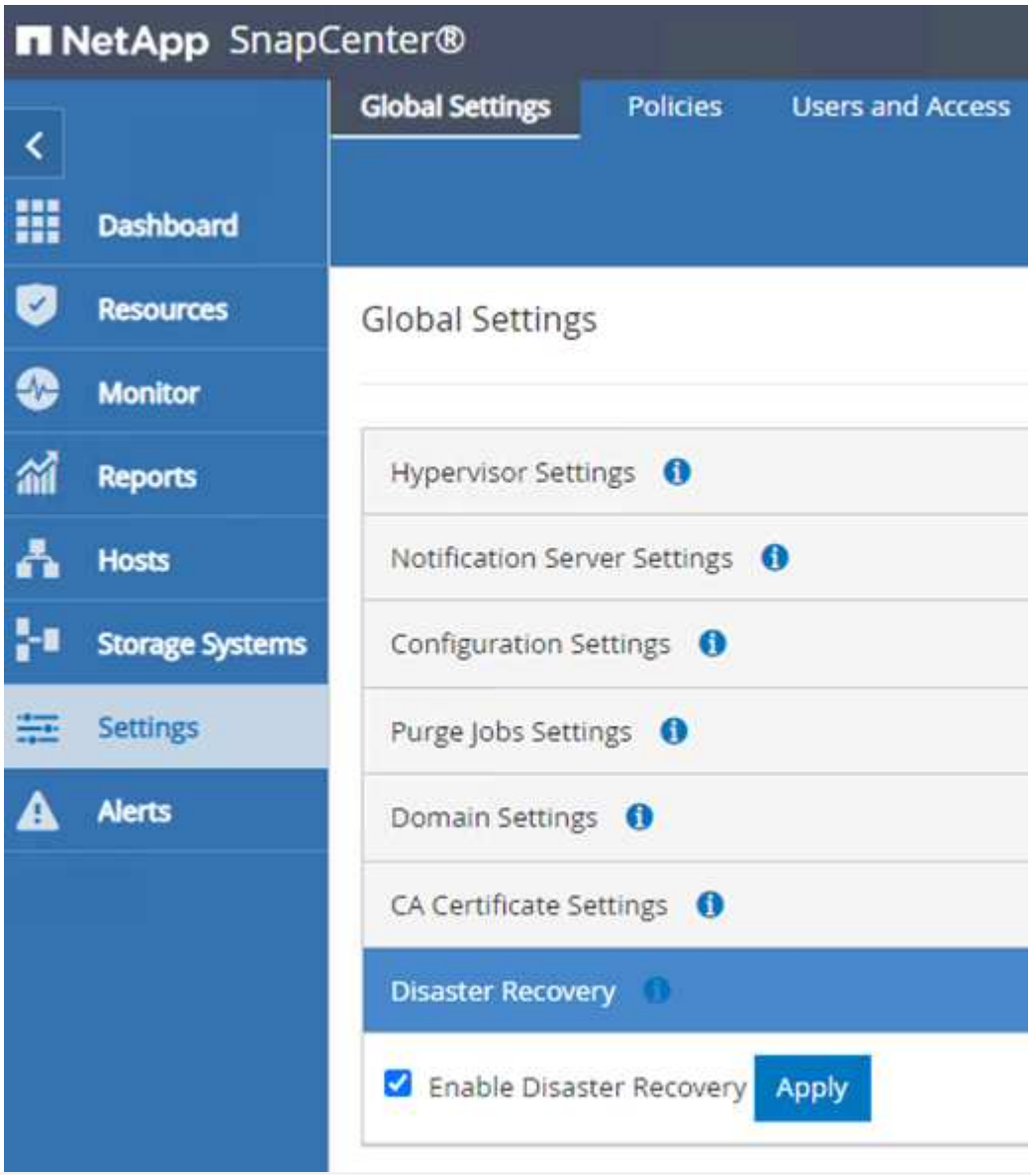


Bestätigen Sie die SnapCenter-Kommunikation mit dem SQL Server-Plug-in

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*
```

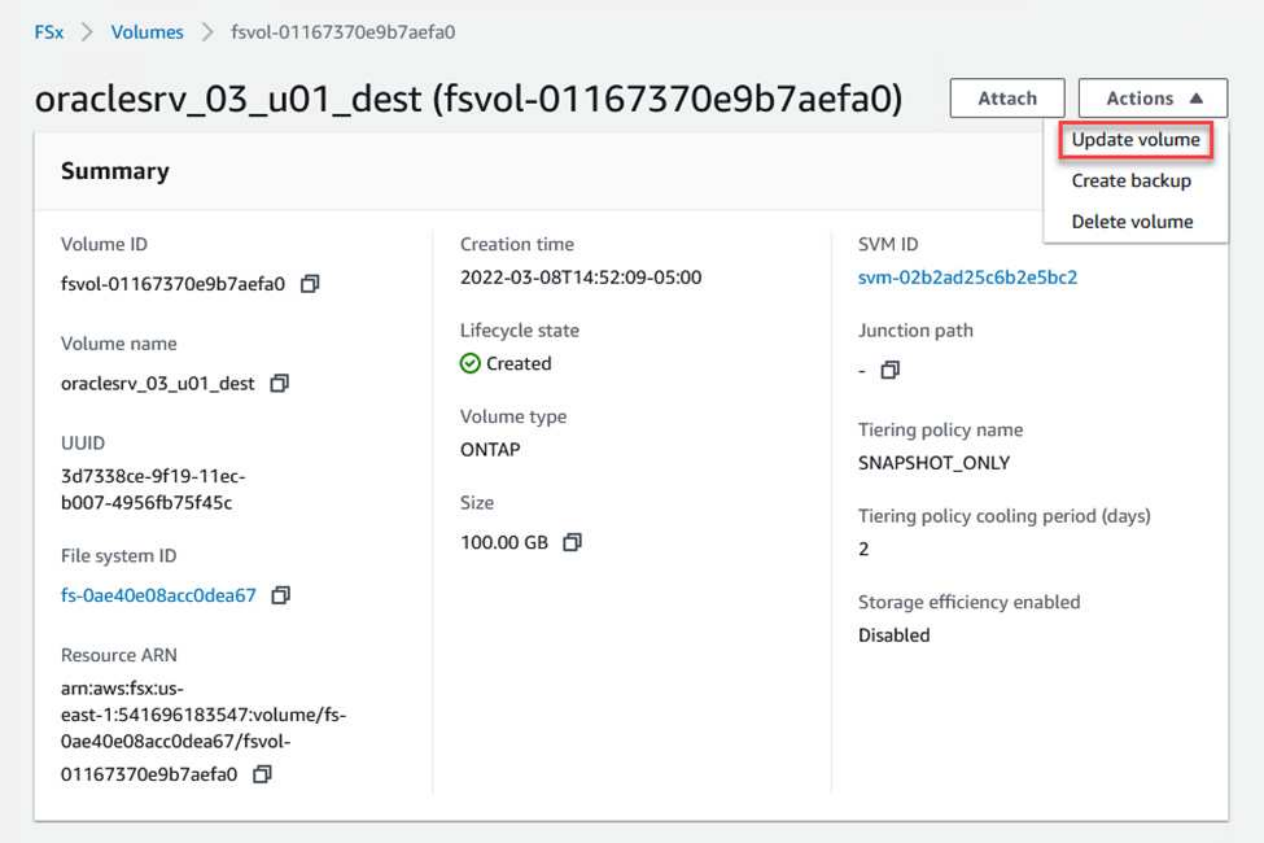
```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        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.

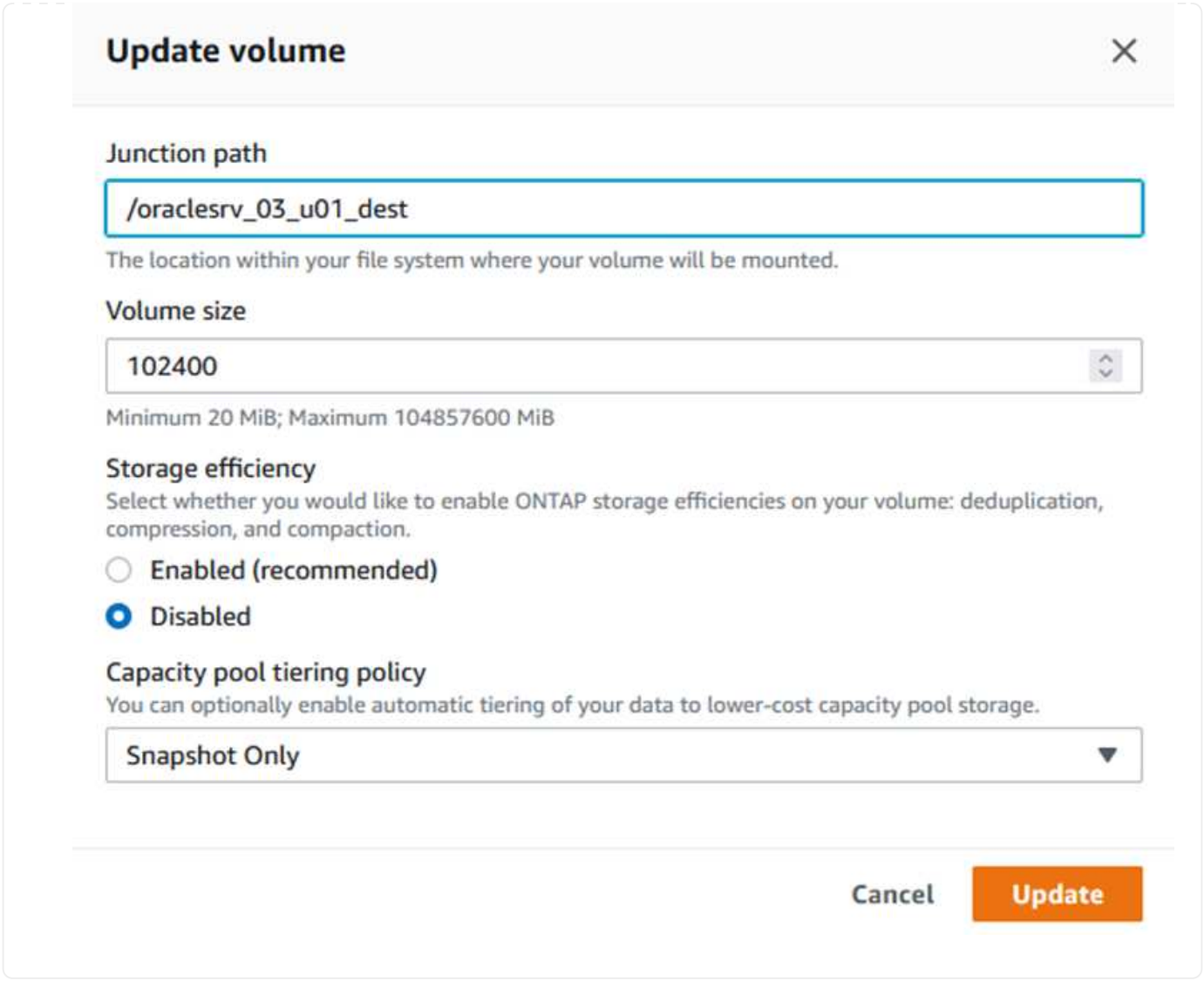
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
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:



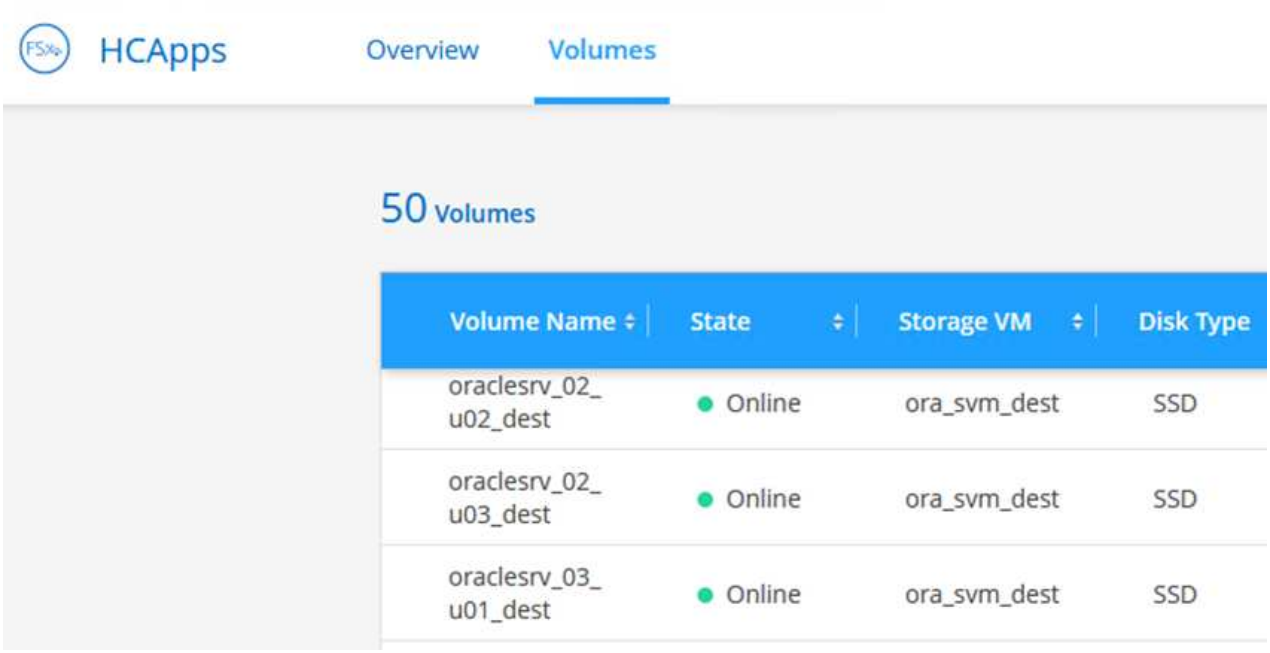
4. Fügen Sie den Namen des Verbindungspfads hinzu, und klicken Sie auf Aktualisieren. Geben Sie diesen Verbindungspfad an, wenn Sie das NFS Volume vom Oracle Server mounten.


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

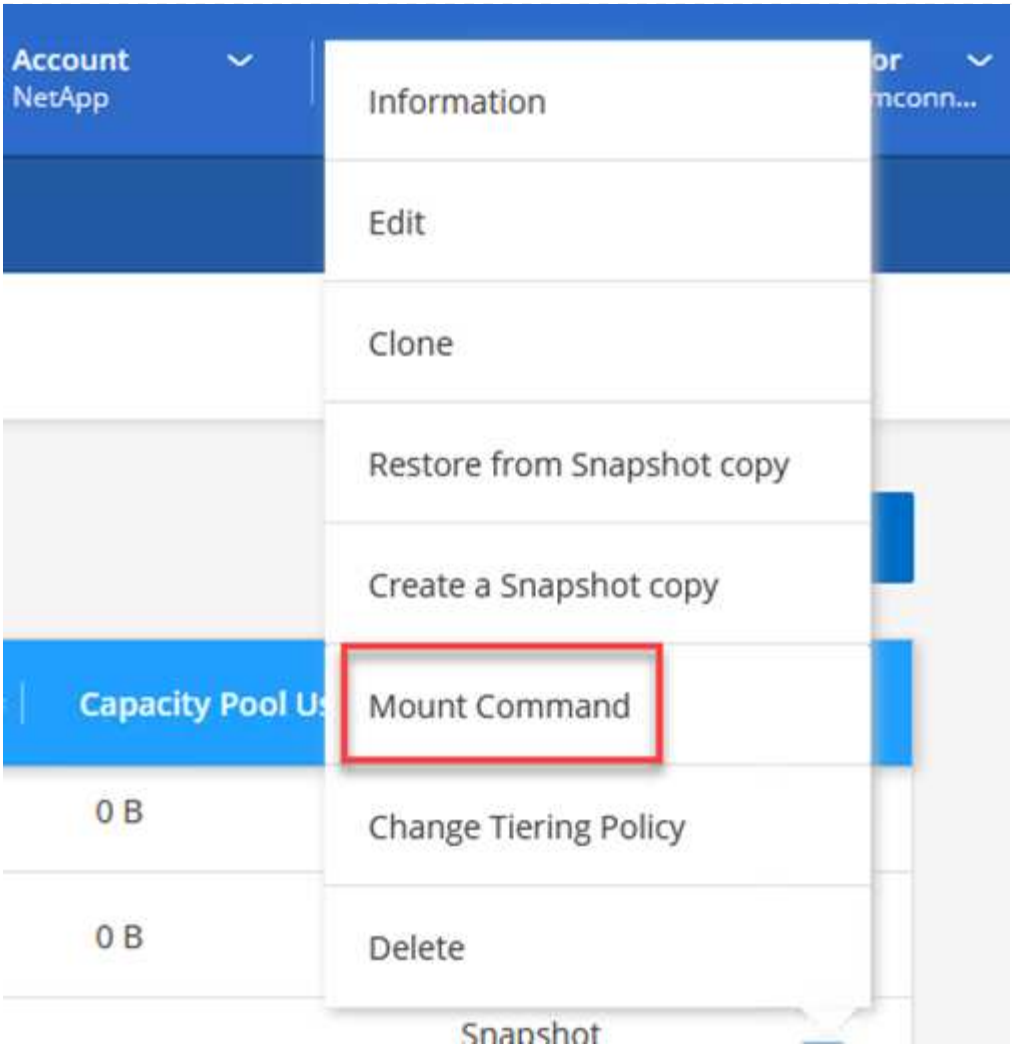
Mounten Sie NFS Volumes auf Oracle Server

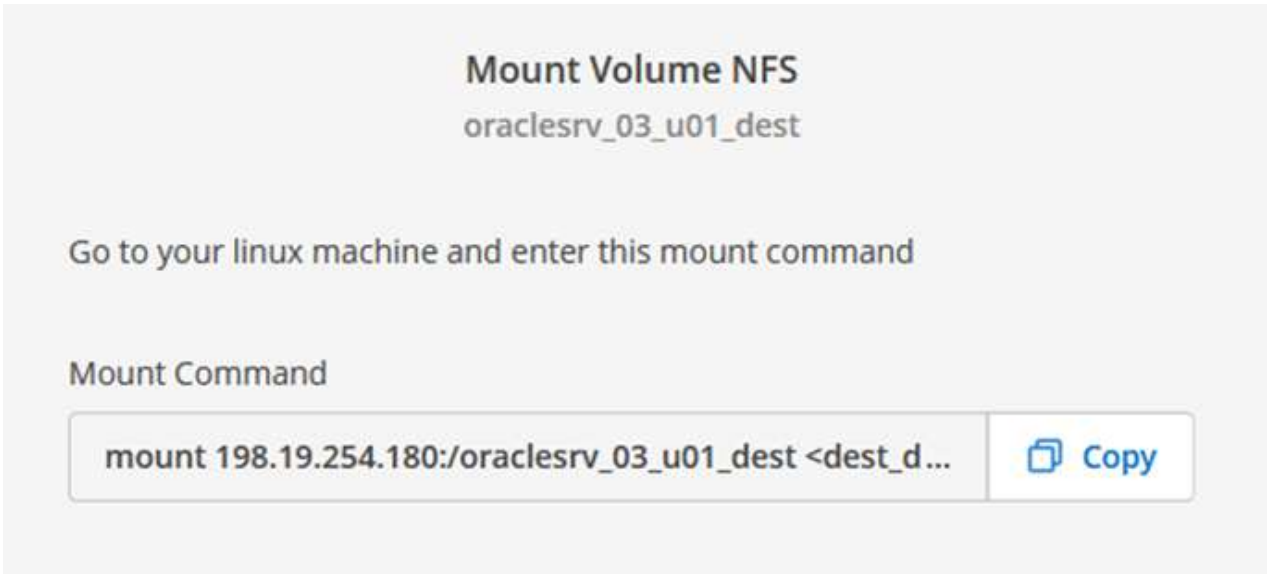
In Cloud Manager erhalten Sie den Mount-Befehl mit der richtigen NFS-LIF-IP-Adresse zum Mounten der NFS-Volumes, die die Oracle-Datenbankdateien und -Protokolle enthalten.

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

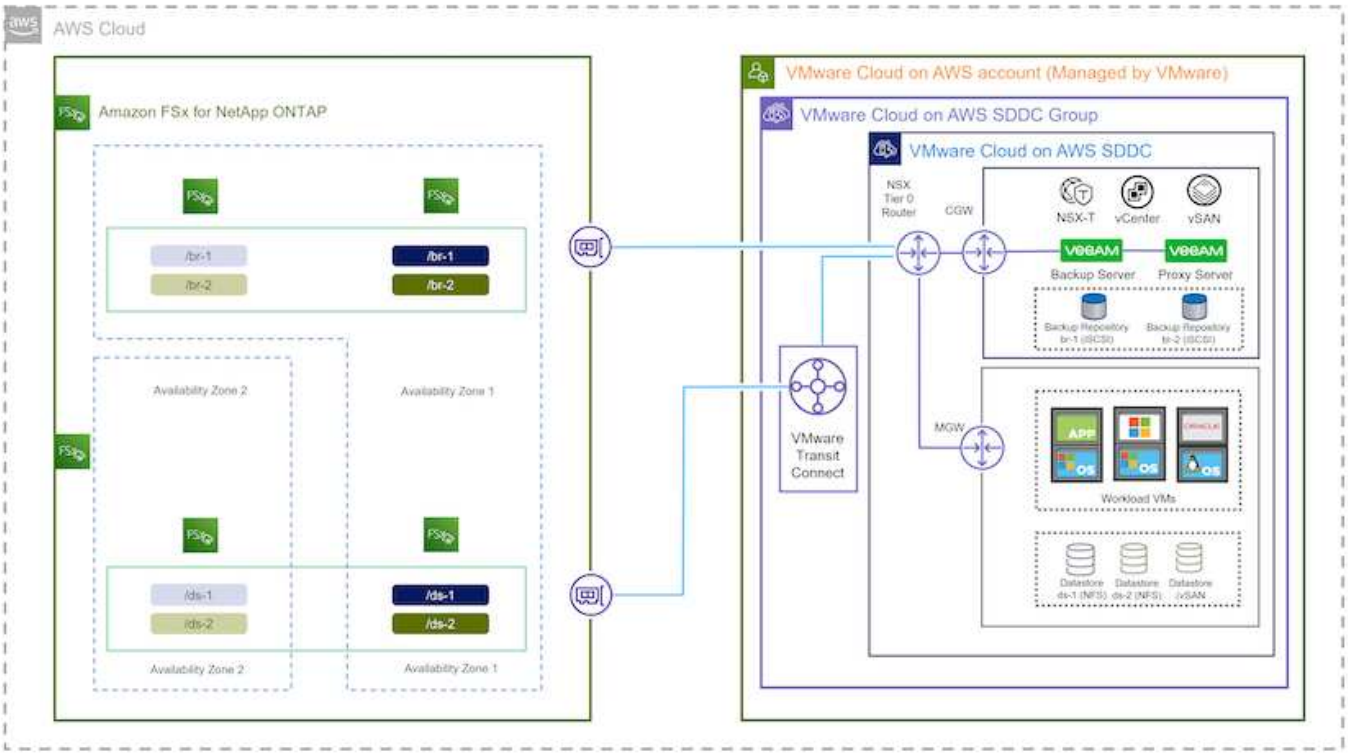
Der Zweck dieser Lösung besteht darin, die Datensicherung von Virtual Machines zu demonstrieren, die in der VMware Cloud ausgeführt werden und sich in NFS-Datenspeichern befinden, die von FSX for NetApp ONTAP gehostet werden. Bei dieser Lösung wird vorausgesetzt, dass die folgenden Komponenten konfiguriert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

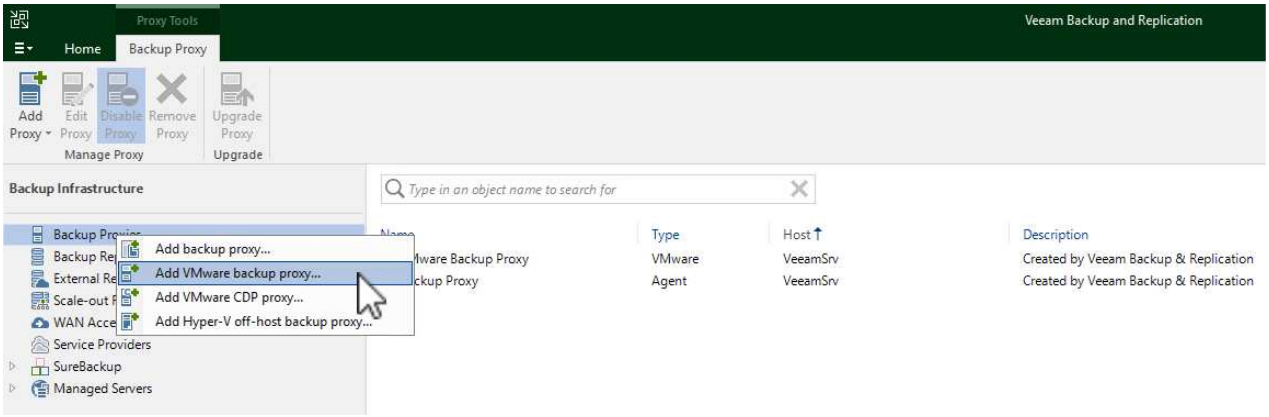
Weitere Informationen zu den Transportmodi finden Sie im "Veeam Backup and Replication User Guide for VMware vSphere".

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

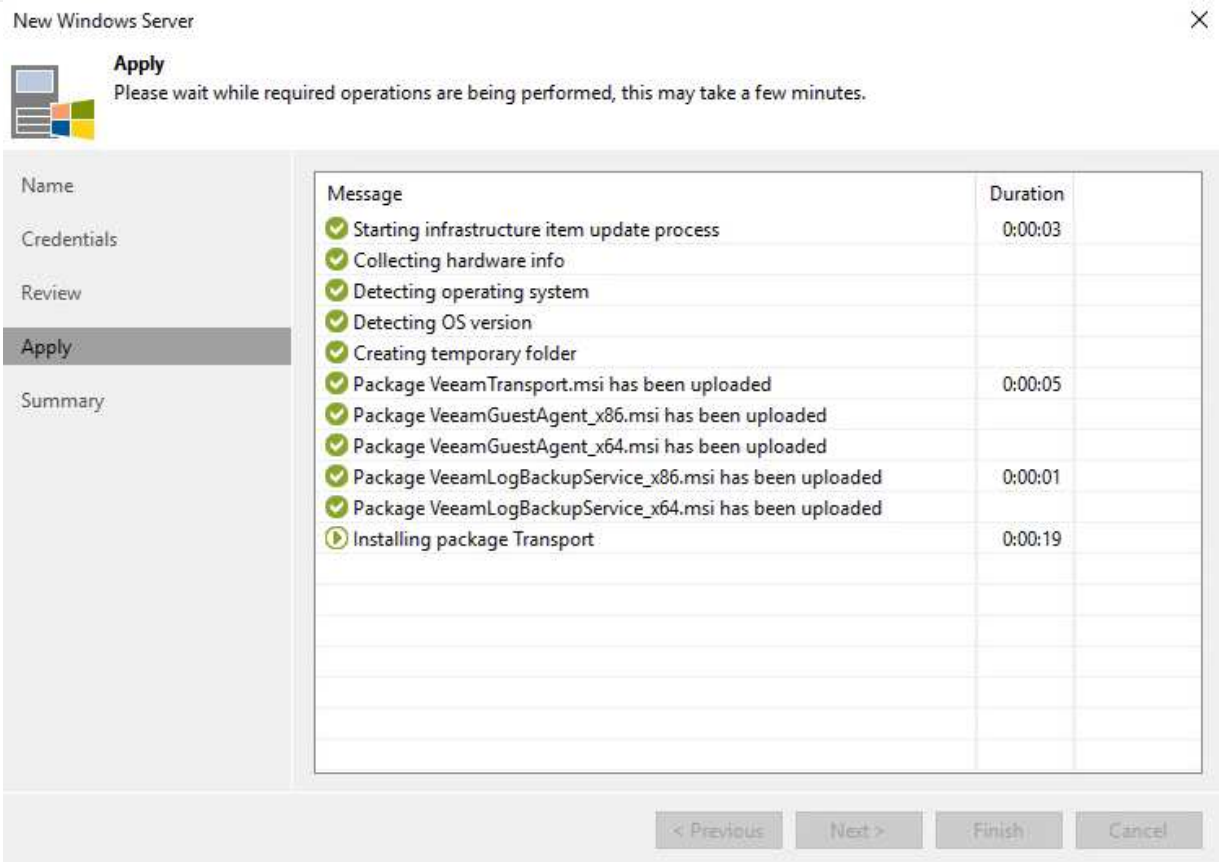
In diesem Schritt wird der Veeam Proxy auf einer vorhandenen Windows-VM bereitgestellt. So können Backup-Jobs zwischen dem primären Veeam Backup-Server und dem Veeam Proxy verteilt werden.

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.

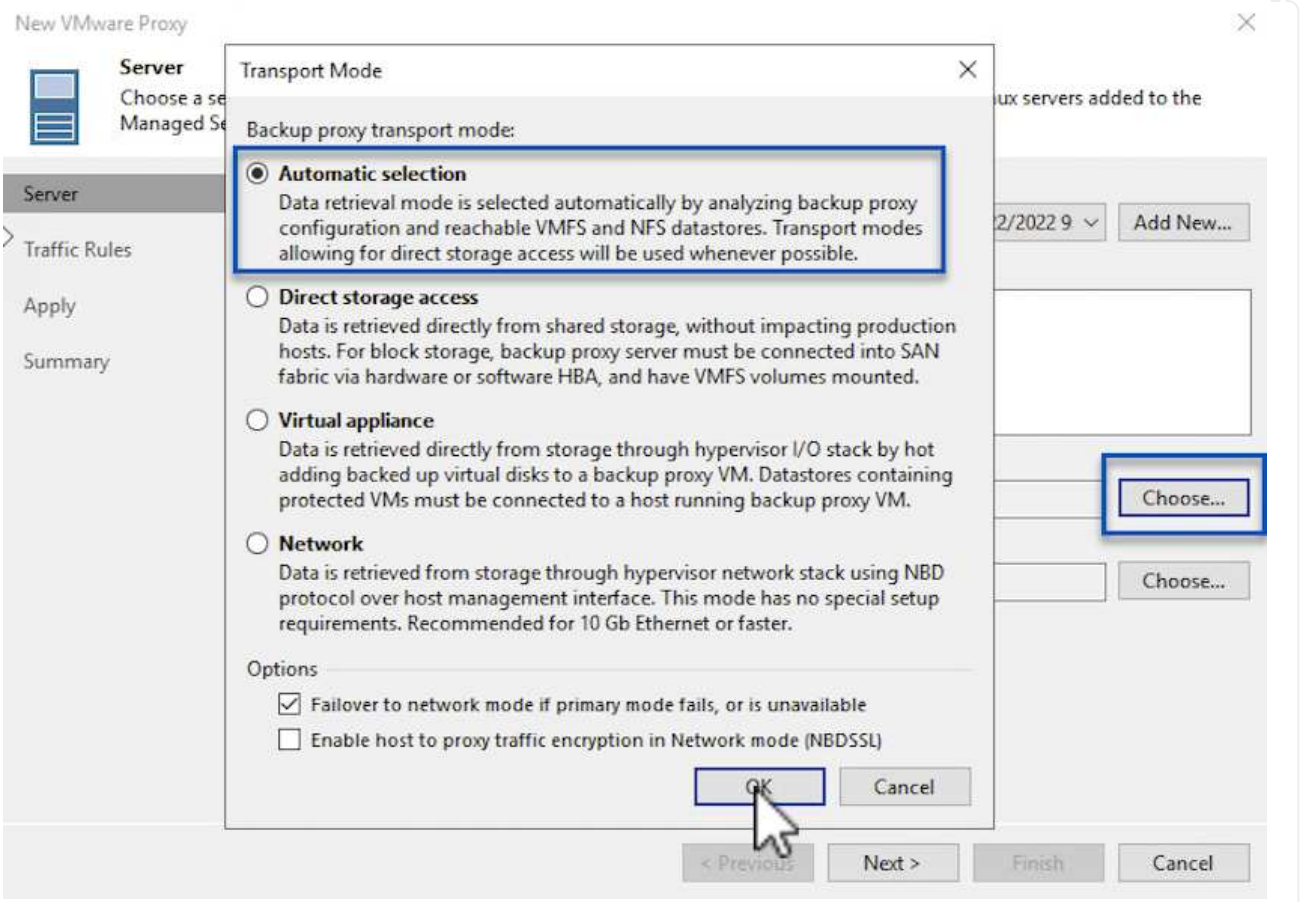


3. Klicken Sie im **Add VMware Proxy** Wizard auf die Schaltfläche **Add New…**, um einen neuen Proxyserver hinzuzufügen.

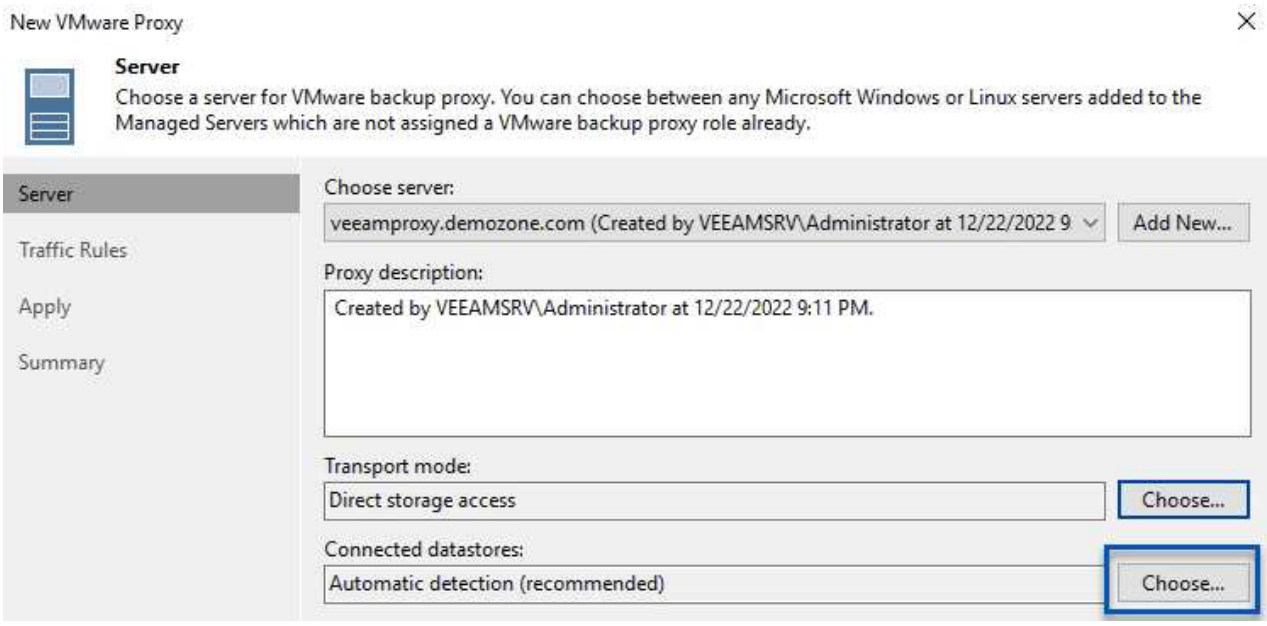
4. Wählen Sie diese Option, um Microsoft Windows hinzuzufügen, und befolgen Sie die Anweisungen zum Hinzufügen des Servers:
   - Geben Sie den DNS-Namen oder die IP-Adresse ein
   - Wählen Sie ein Konto aus, das für Anmeldeinformationen auf dem neuen System verwendet werden soll, oder fügen Sie neue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

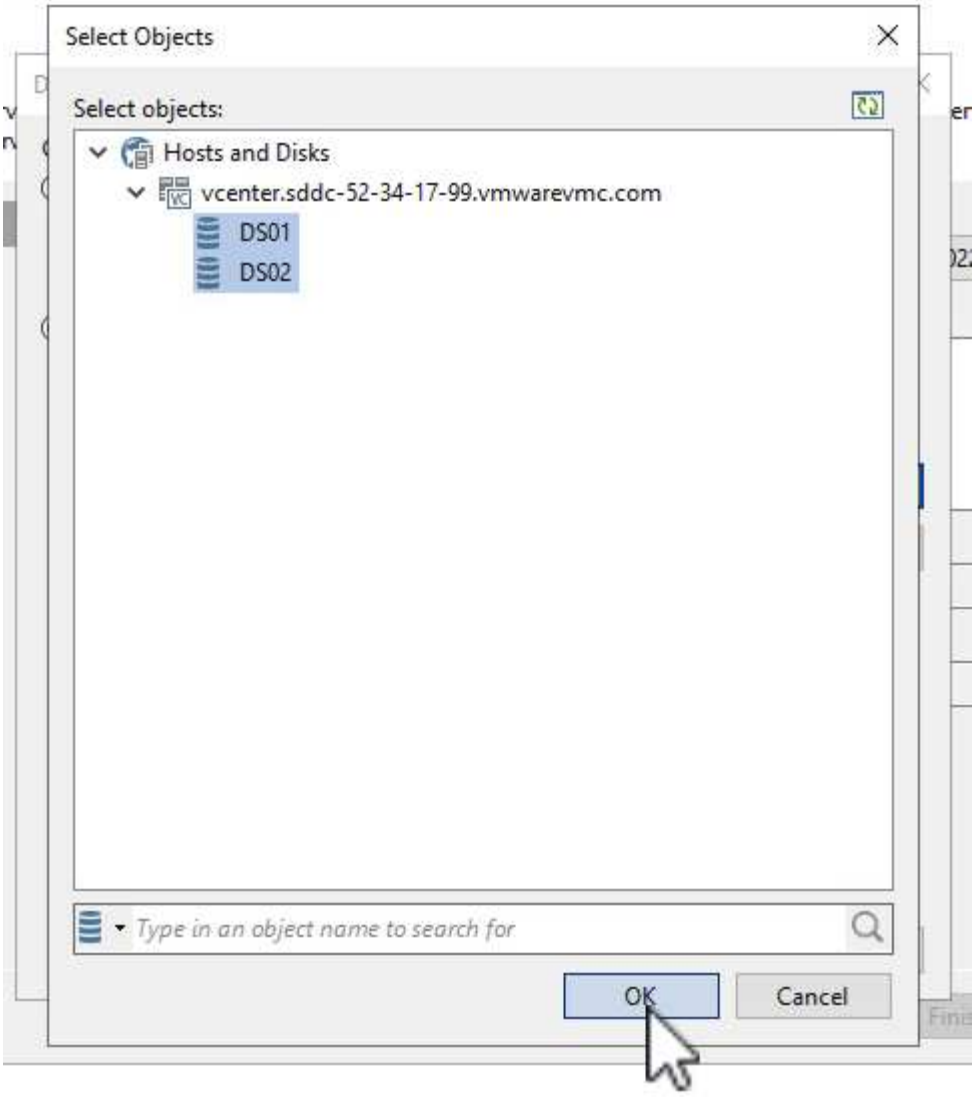


5. Wählen Sie im Assistenten **New VMware Proxy** einen Transportmodus aus. In unserem Fall haben wir uns für **Automatische Auswahl** entschieden.

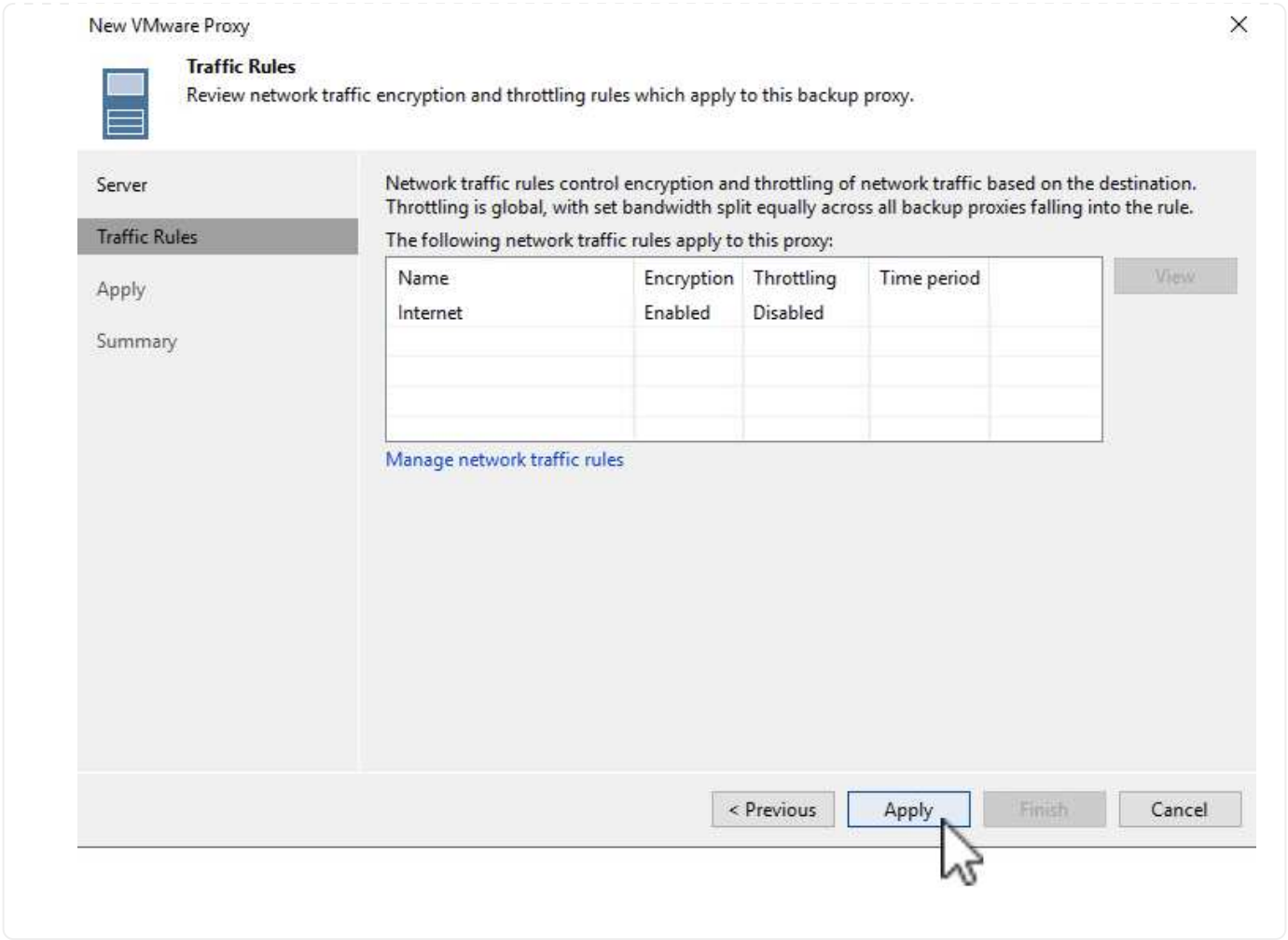


6. Wählen Sie die verbundenen Datastores aus, auf die der VMware Proxy direkten Zugriff haben soll.





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.



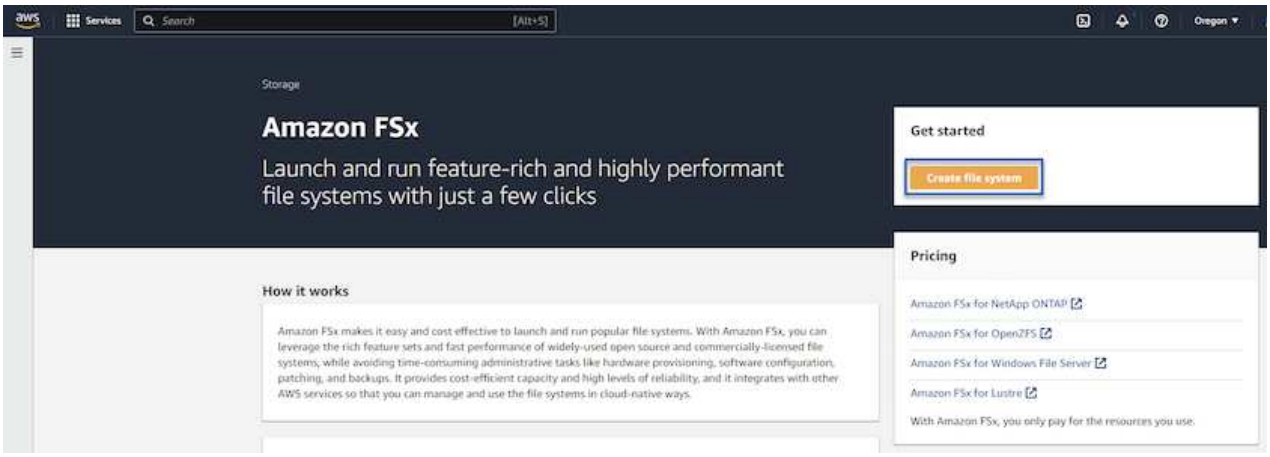
Konfiguration von Storage- und Backup-Repositorys

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

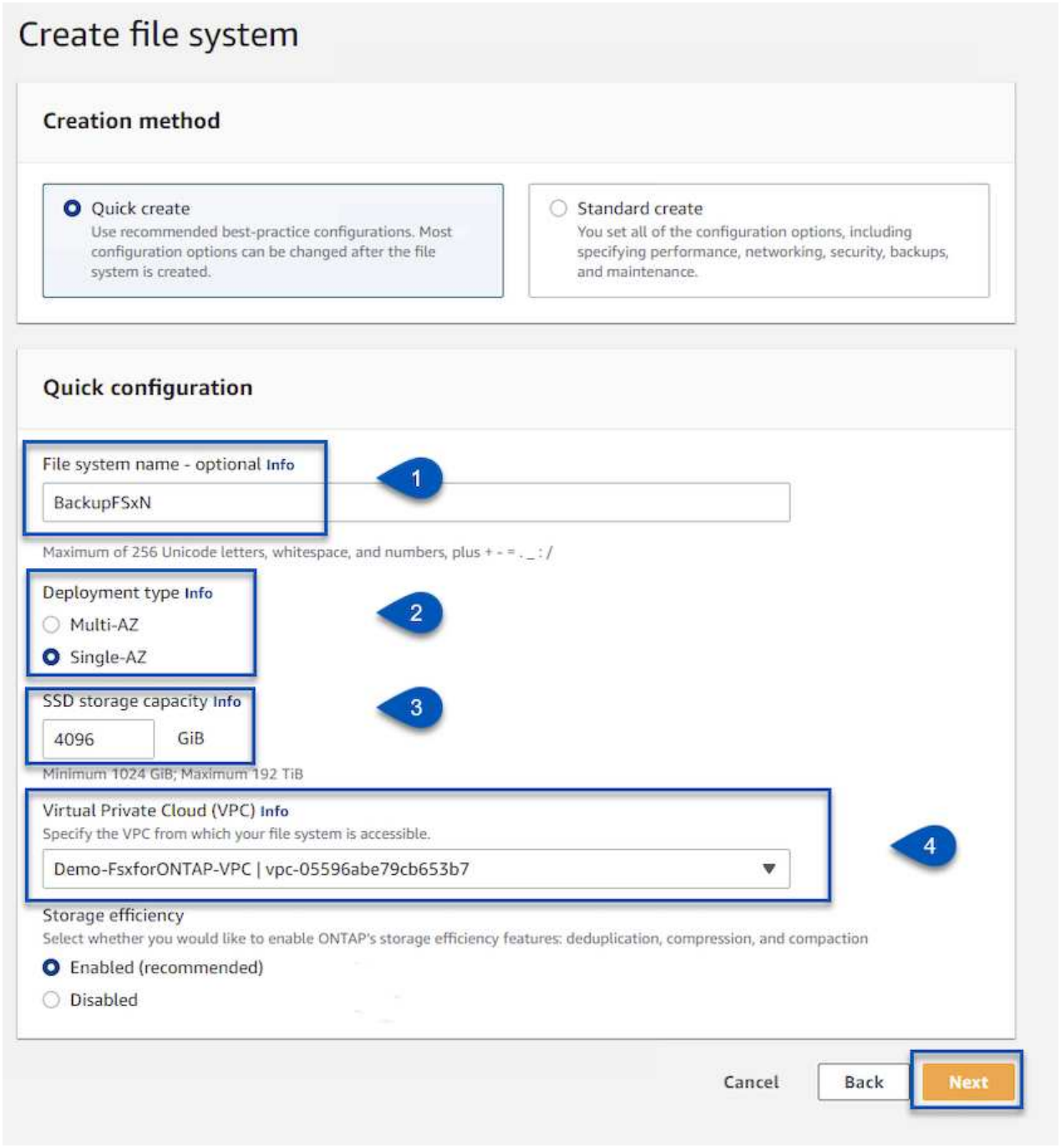
Erstellen Sie ein FSX für ONTAP-Dateisystem, das zum Hosten der iSCSI-Volumes für die Veeam Backup-Repositorys verwendet wird.

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:

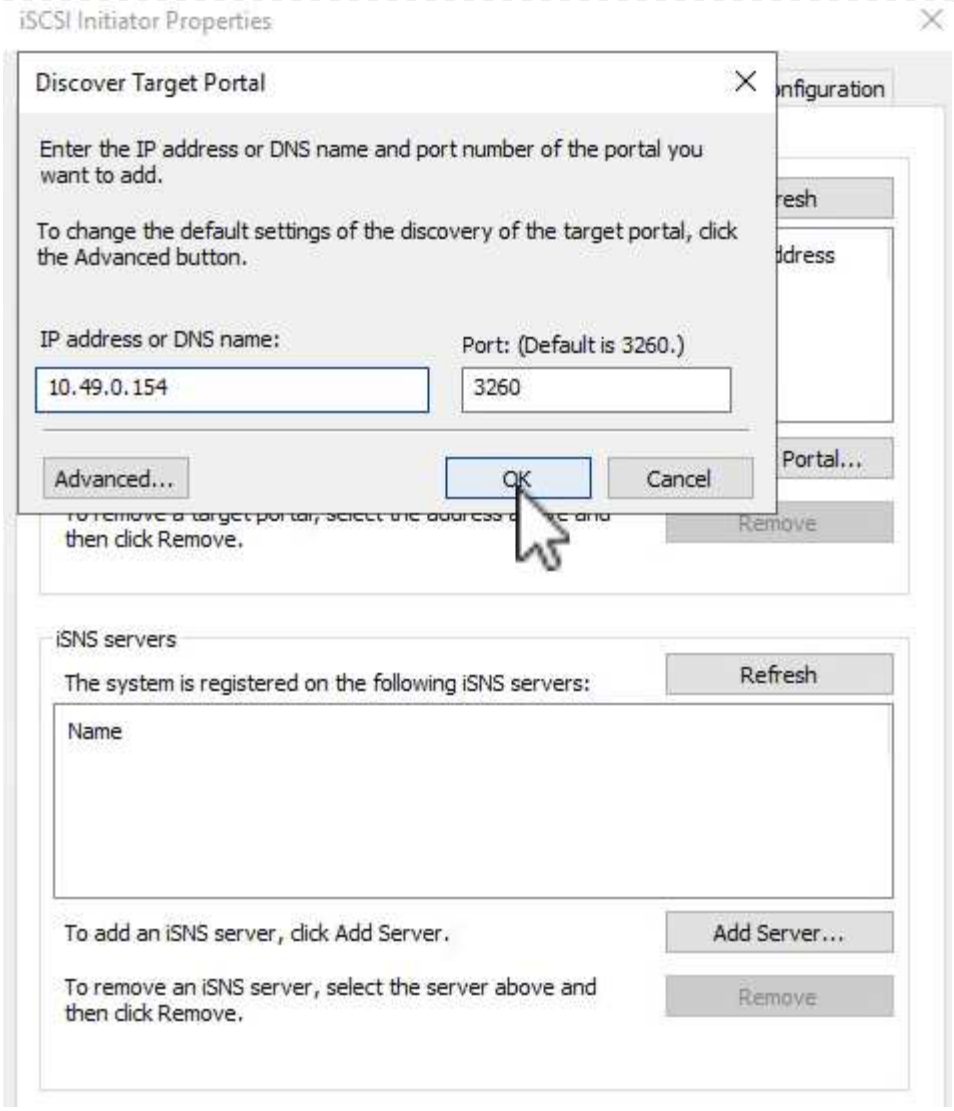
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

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

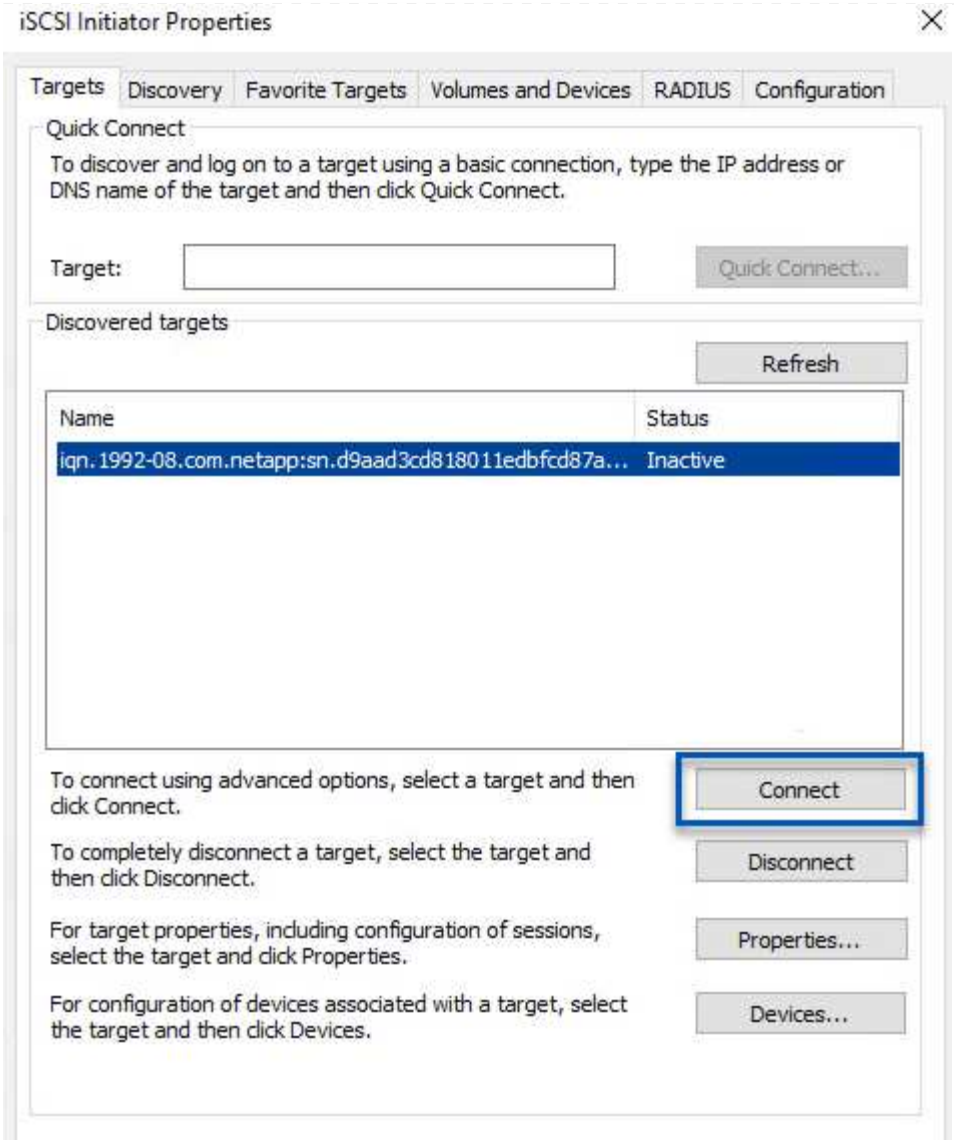
4. Schließlich ordnen Sie die LUNs der Initiatorgruppe zu, die Sie gerade erstellt haben:

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

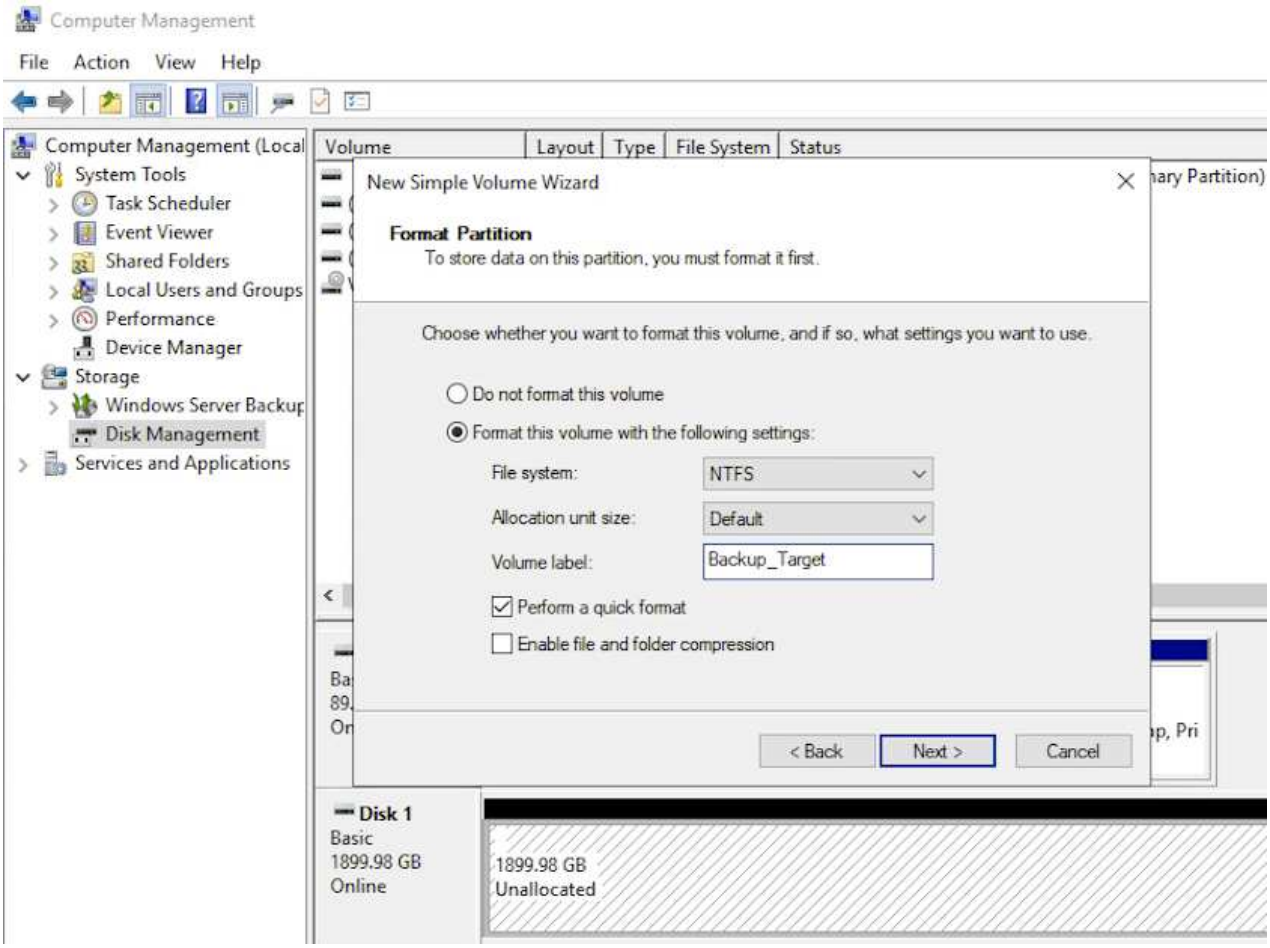
5. Melden Sie sich zum Mounten der iSCSI-LUNs beim Veeam Backup & Replication Server an, und öffnen Sie die iSCSI-Initiatoreigenschaften. Gehen Sie auf die Registerkarte **Discover** und geben Sie die iSCSI-Ziel-IP-Adresse ein.



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.

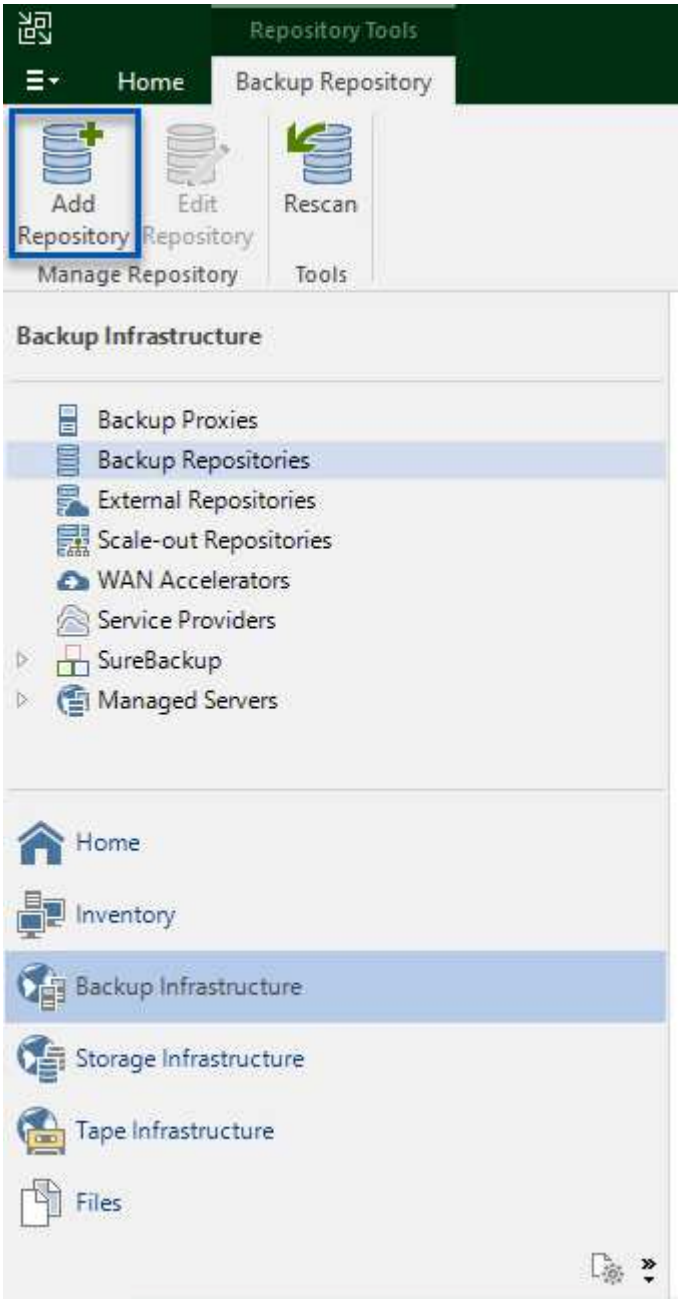


8. Wiederholen Sie diese Schritte, um die iSCSI-Volumes auf den Veeam Proxy-Server zu mounten.

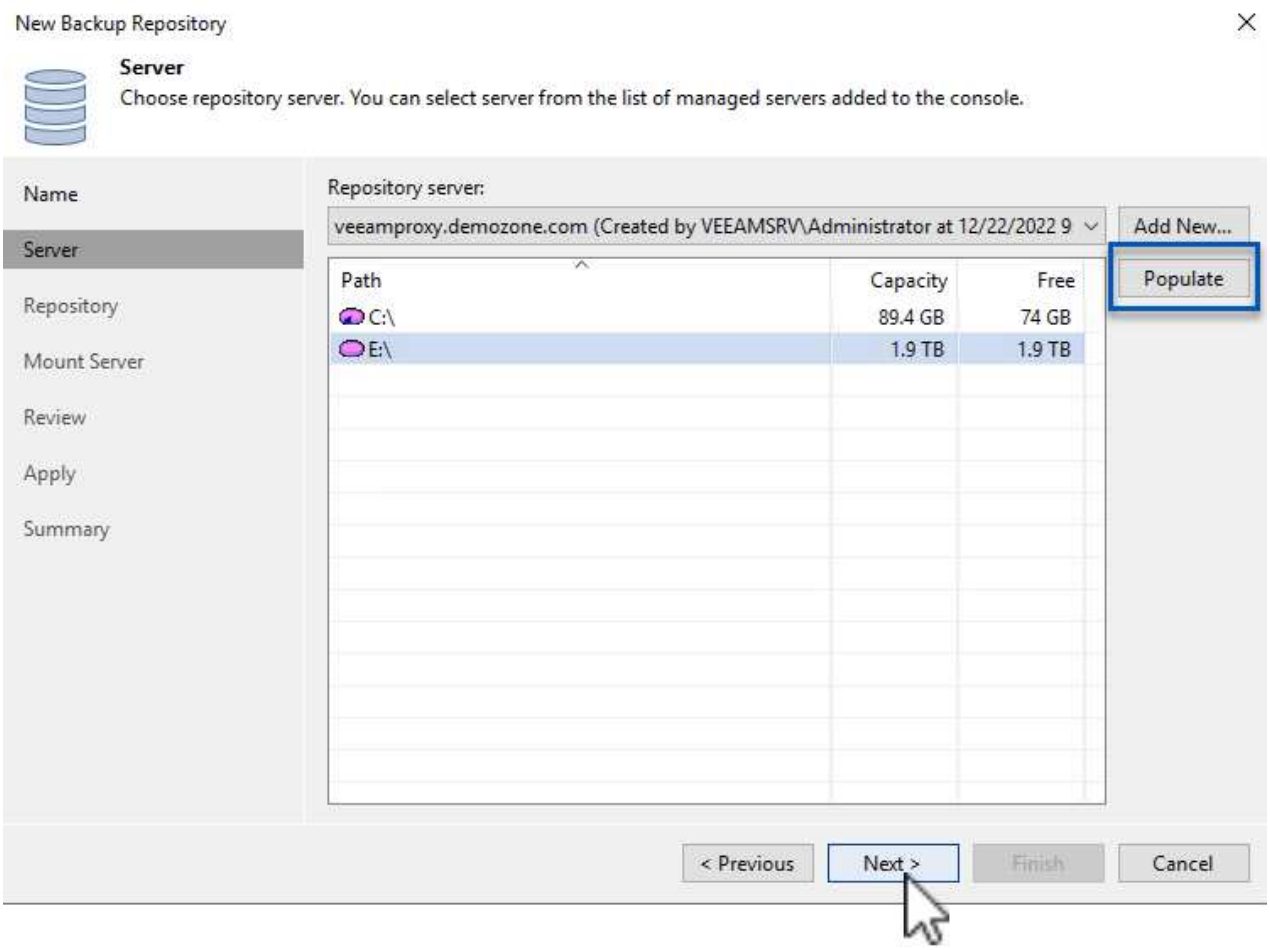
Veeam Backup Repositorys Erstellen

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.

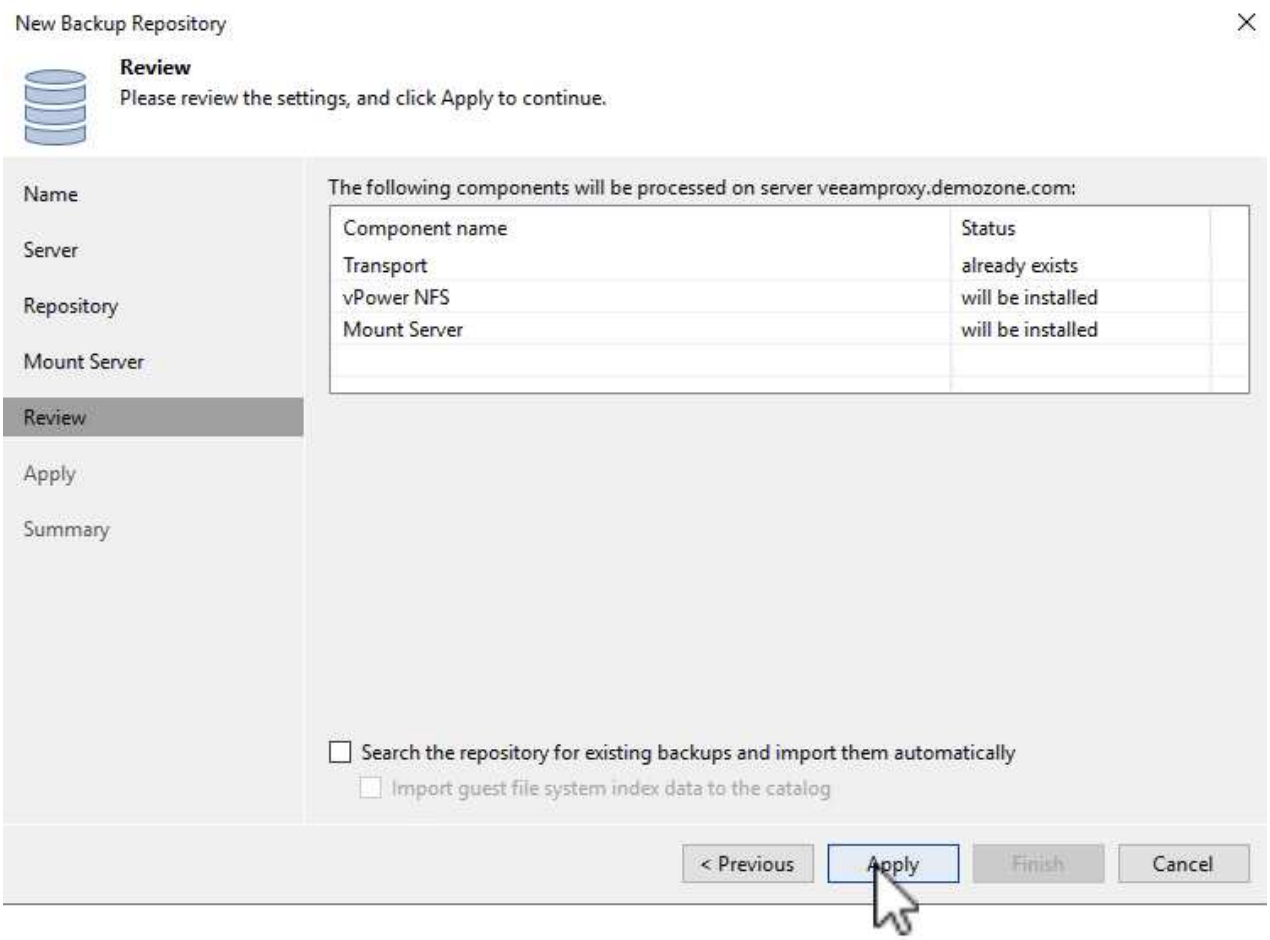
1. Klicken Sie in der Veeam Backup and Replication Konsole unten links auf **Backup Infrastructure** und wählen Sie dann **Add Repository**



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

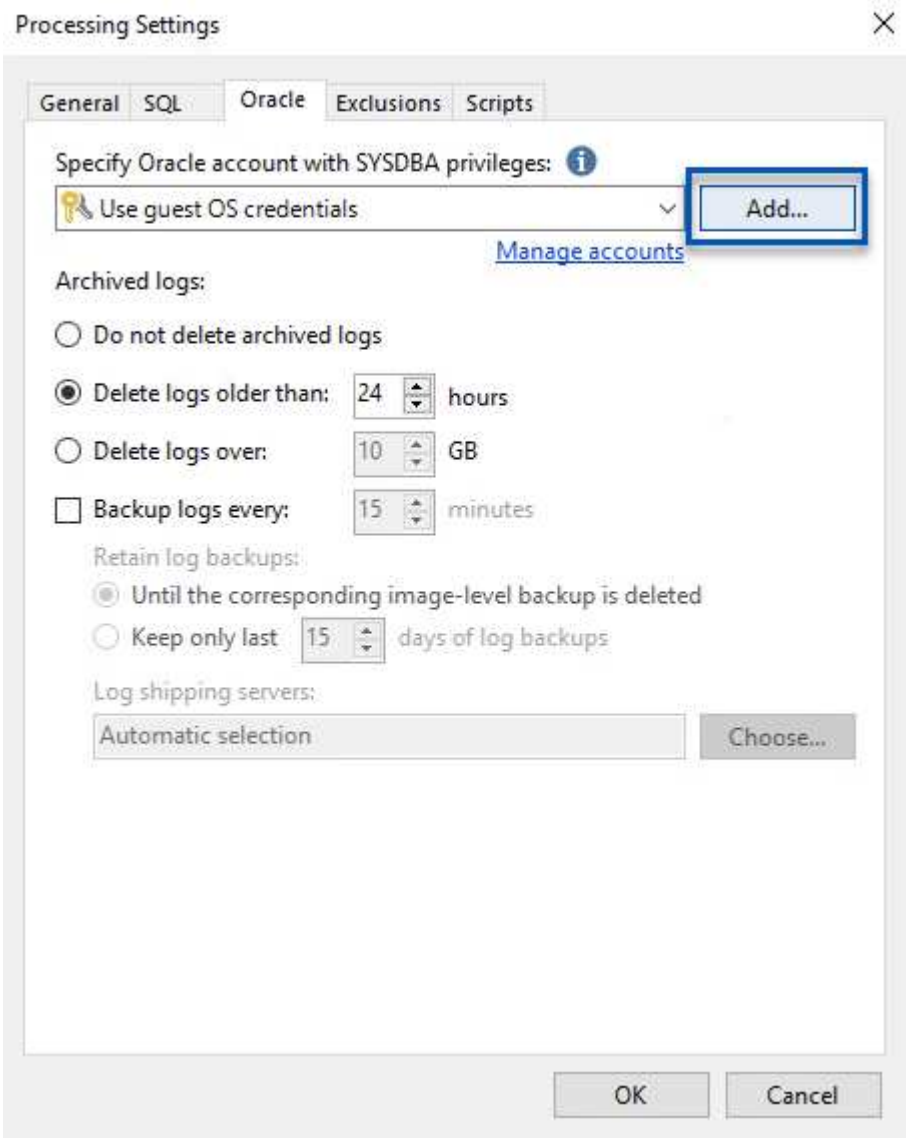
Backup-Jobs sollten mithilfe der Backup-Repositorys im vorherigen Abschnitt erstellt werden. Die Erstellung von Backup-Jobs gehört normalerweise zum Repertoire eines Storage-Administrators und wir werden hier nicht alle Schritte besprechen. Nähere Informationen zum Erstellen von Backup-Jobs in Veeam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

In dieser Lösung wurden separate Backup-Jobs erstellt für:

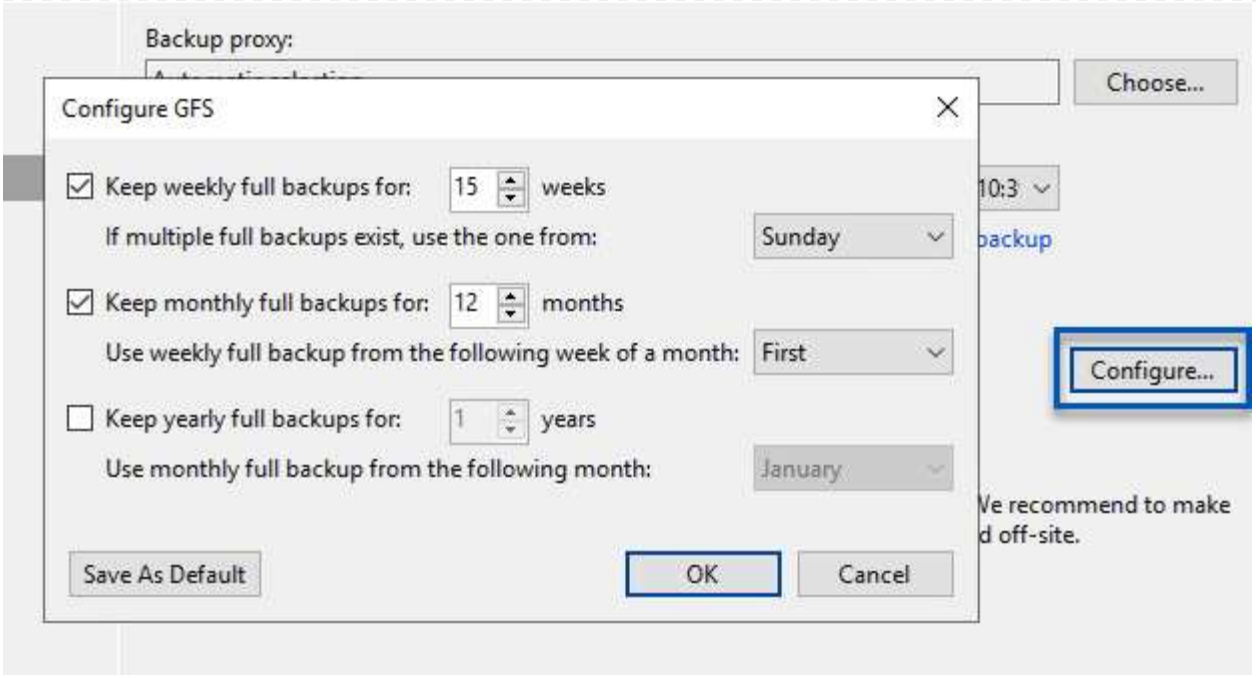
- Microsoft Windows SQL Server
- Oracle Database Server
- Windows File-Server
- Linux-File-Server

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".

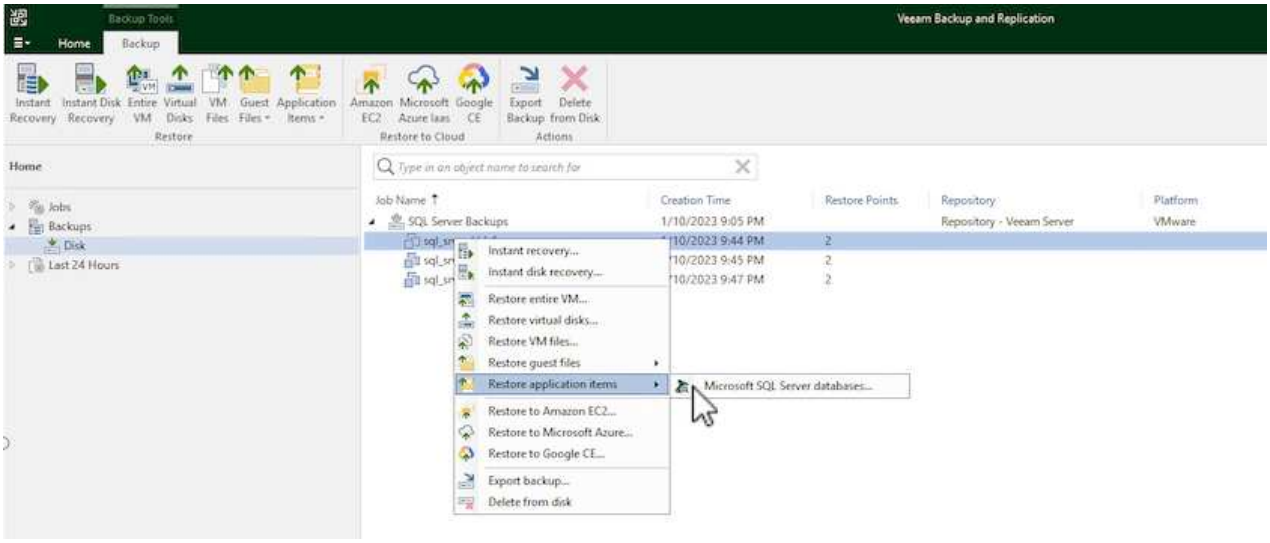
SQL Server-Datenbanken wiederherstellen

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:

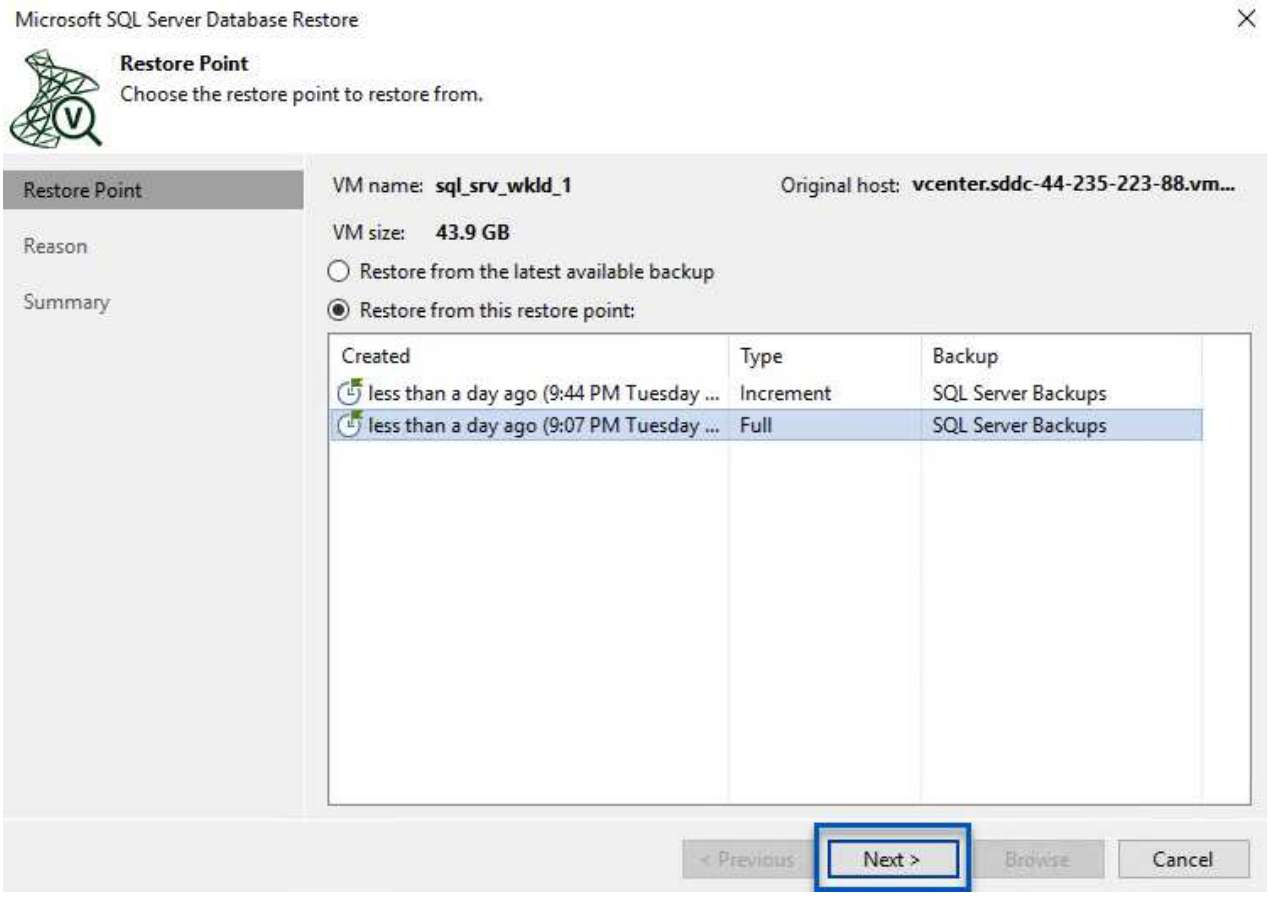
- Veeam Explorer **mountet das Backup** mit der zu wiederherzufüenden SQL Server Datenbank.
- Die Software **veröffentlicht die Datenbank** direkt aus den gemounteten Dateien und macht sie als temporäre Datenbank auf der SQL Server-Zielinstanz zugänglich.
- Während die temporäre Datenbank verwendet wird, 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.



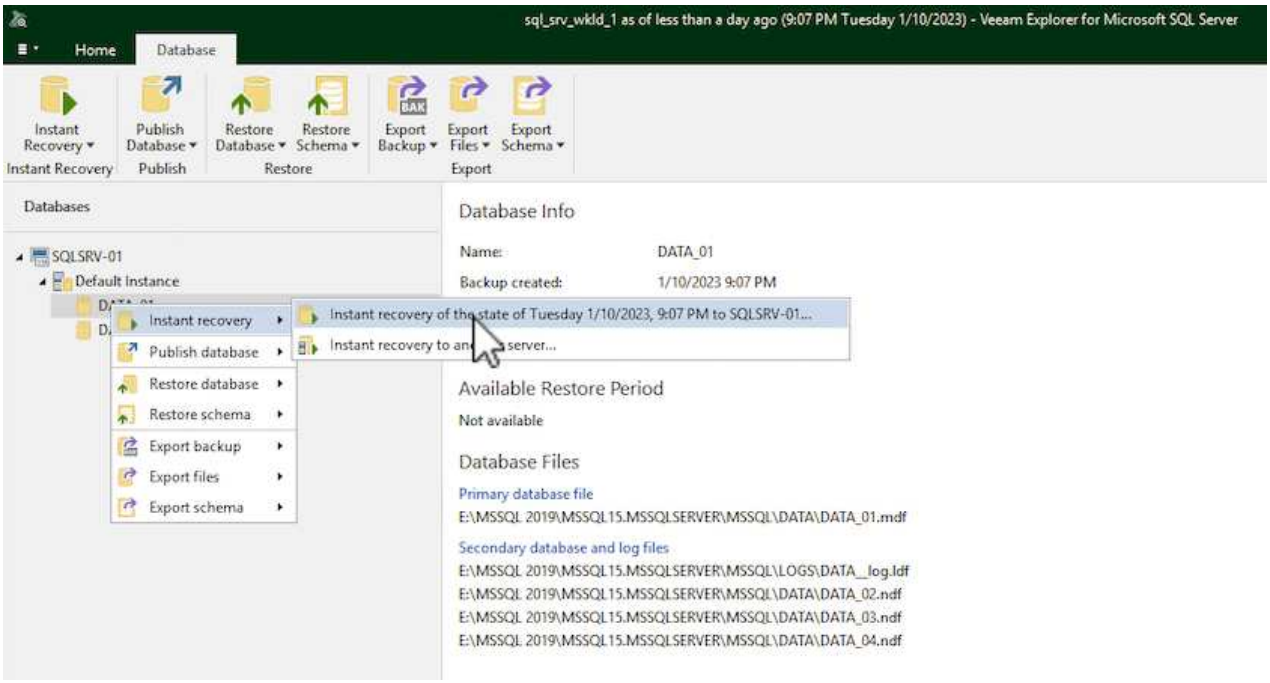
2. Wählen Sie im Microsoft SQL Server Datenbankwiederherstellungsassistenten einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.



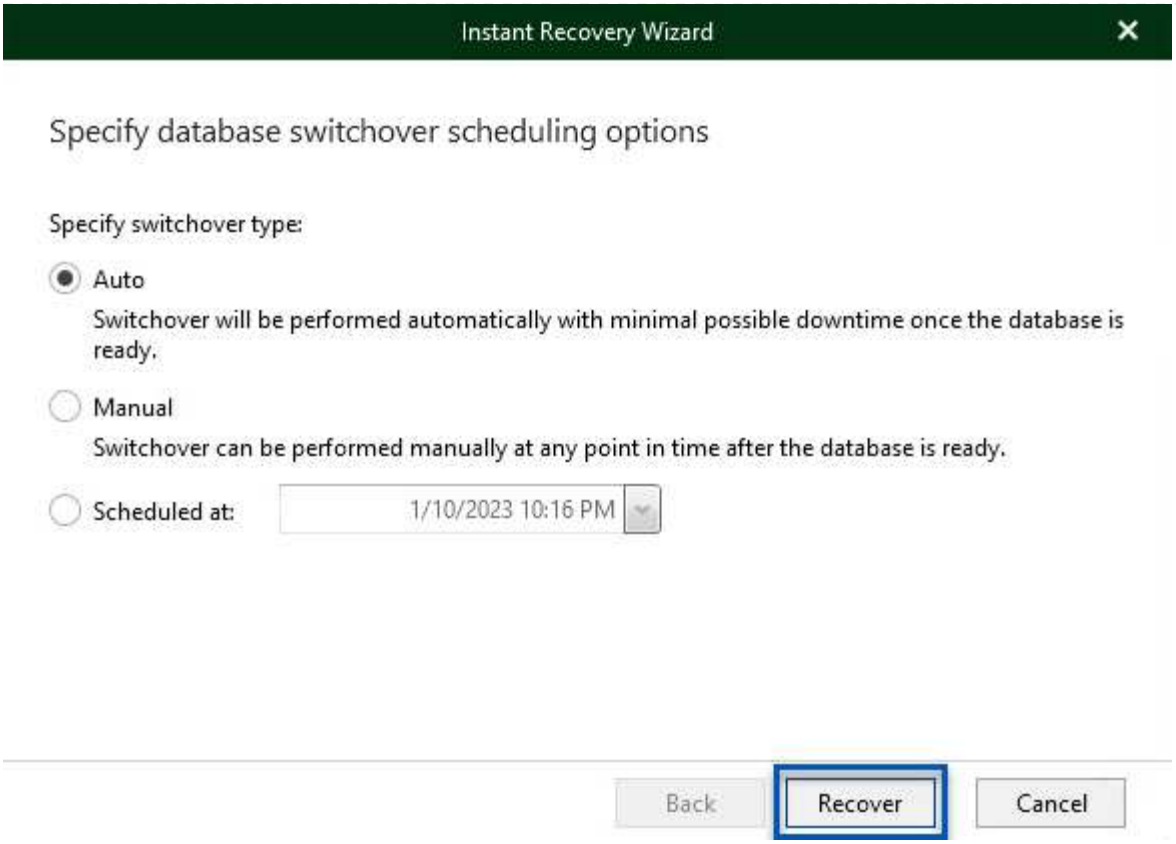
3. Geben Sie bei Bedarf einen * Wiederherstellungsgrund* ein, und klicken Sie dann auf der Übersichtsseite auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Microsoft SQL Server zu

starten.

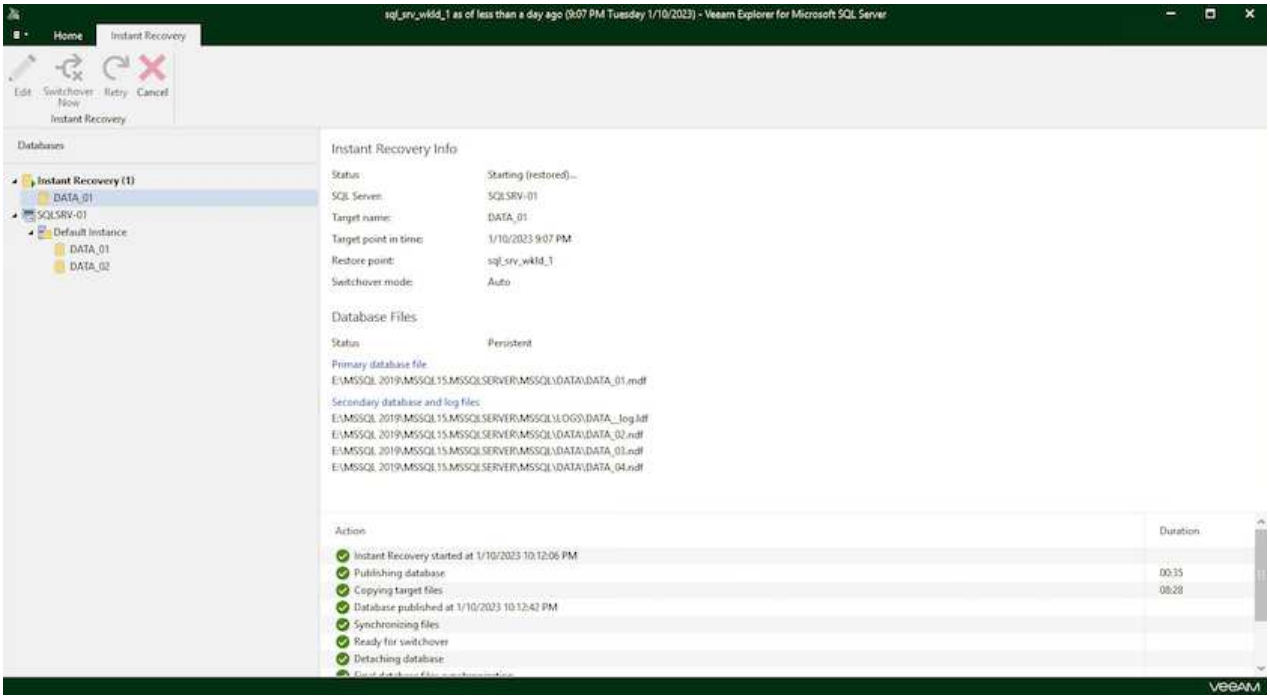
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie mit der rechten Maustaste und wählen Sie * sofortige Wiederherstellung * und dann den spezifischen Wiederherstellungspunkt für die Wiederherstellung.



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

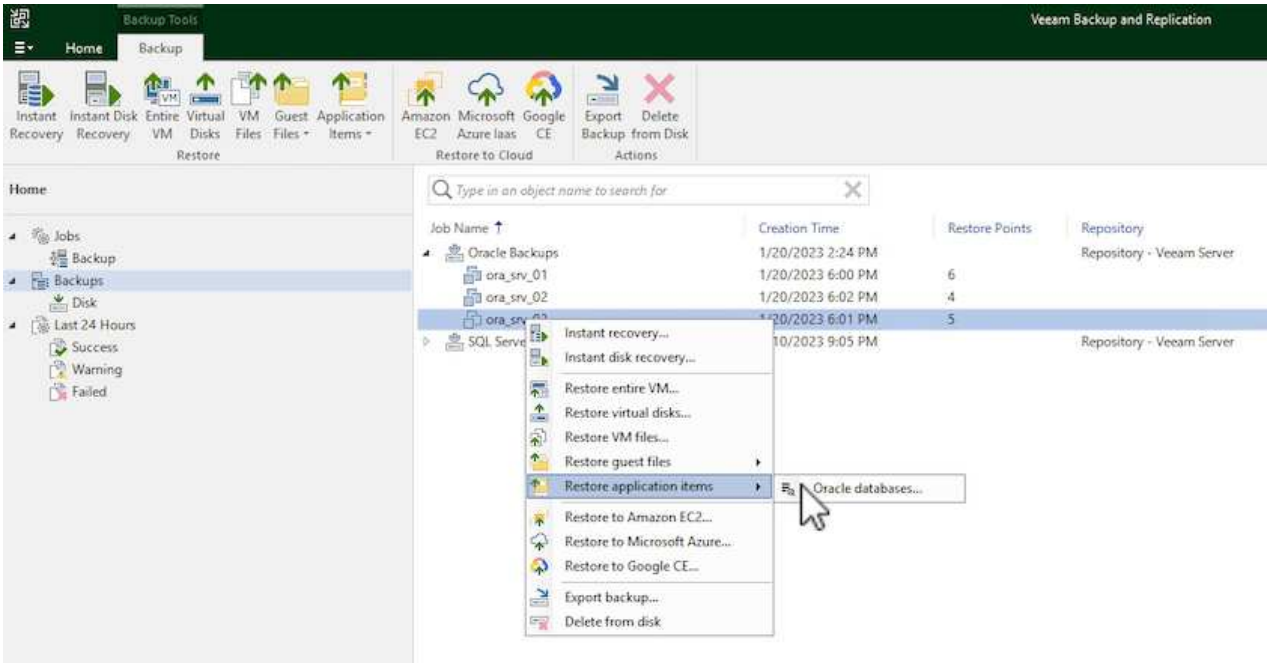
Mit dem Veeam Explorer für Oracle Database können Sie eine standardmäßige Wiederherstellung von Oracle-Datenbanken oder eine unterbrechungsfreie Wiederherstellung mithilfe von Instant Recovery durchführen. Es unterstützt auch die Veröffentlichung von Datenbanken für schnellen Zugriff, Recovery von Data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

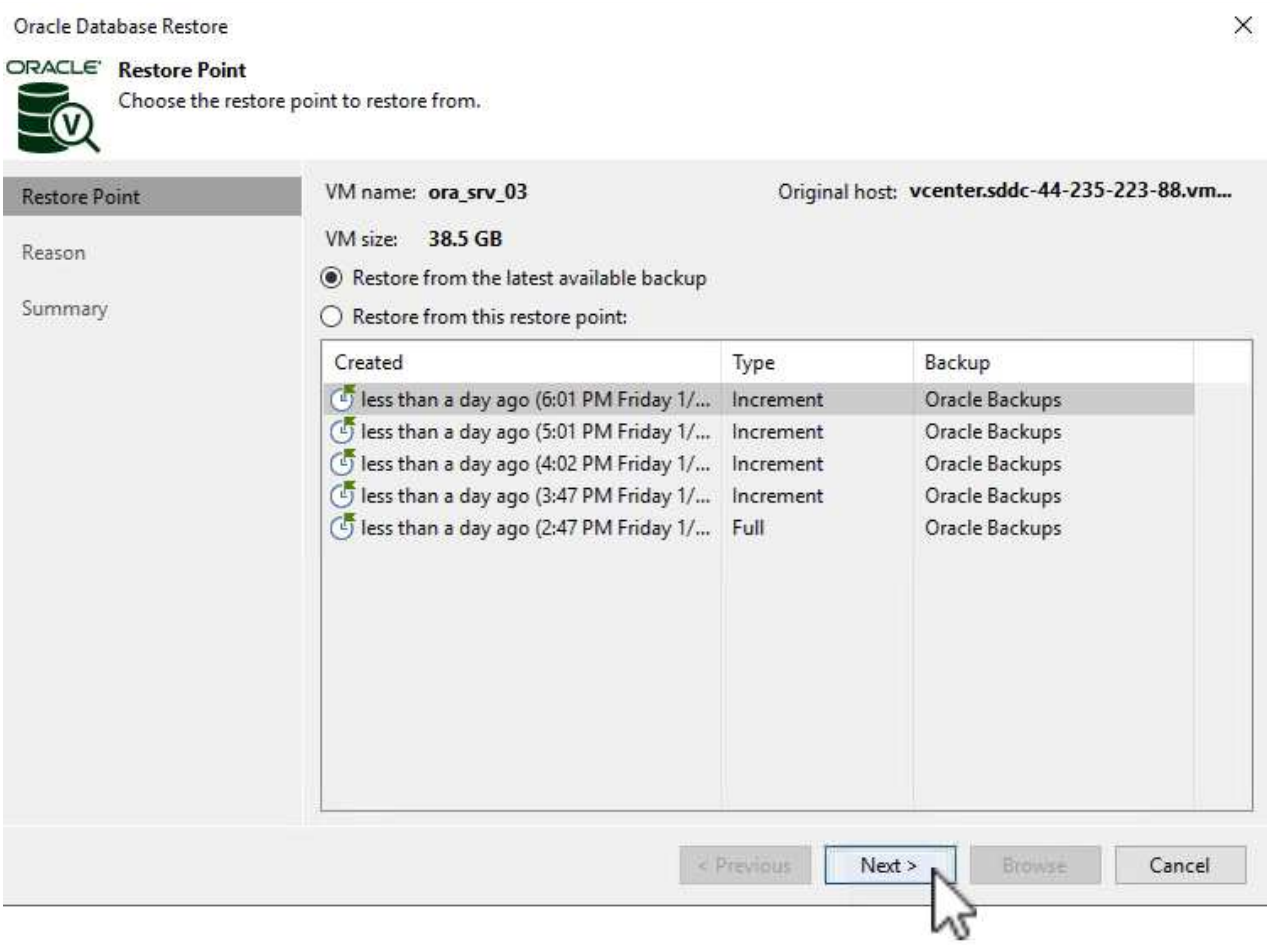
Stellen Sie Oracle Datenbanken mit Veeam Explorer wieder her

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.

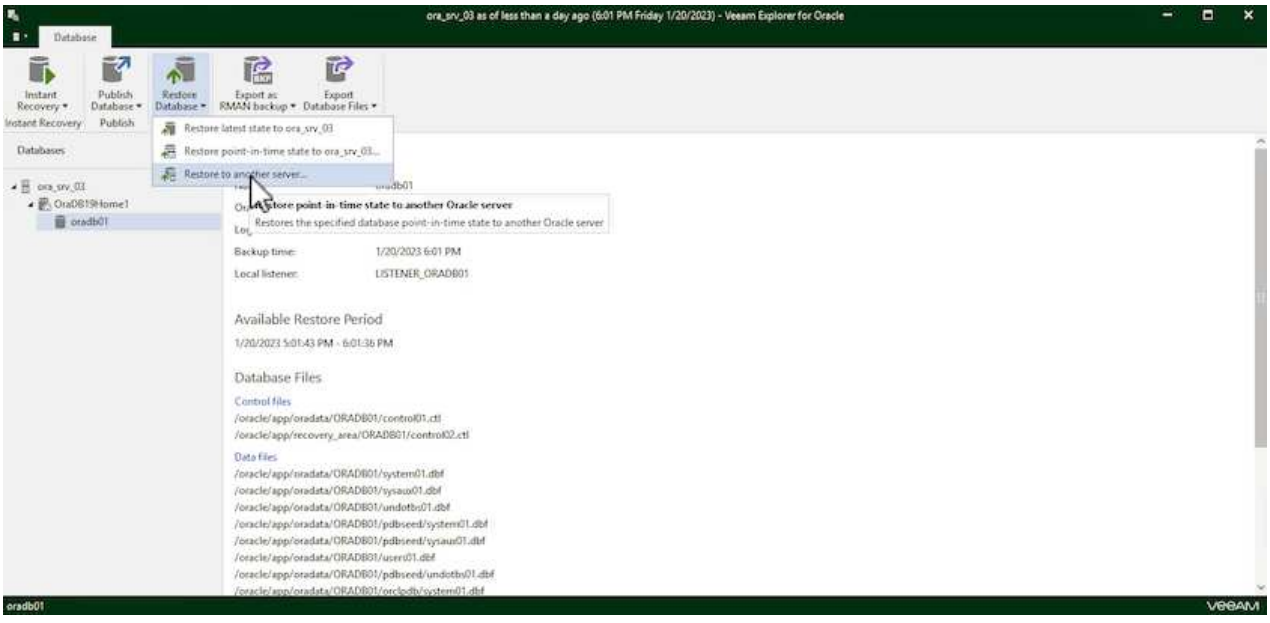


2. Wählen Sie im Oracle Database Restore Wizard einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.

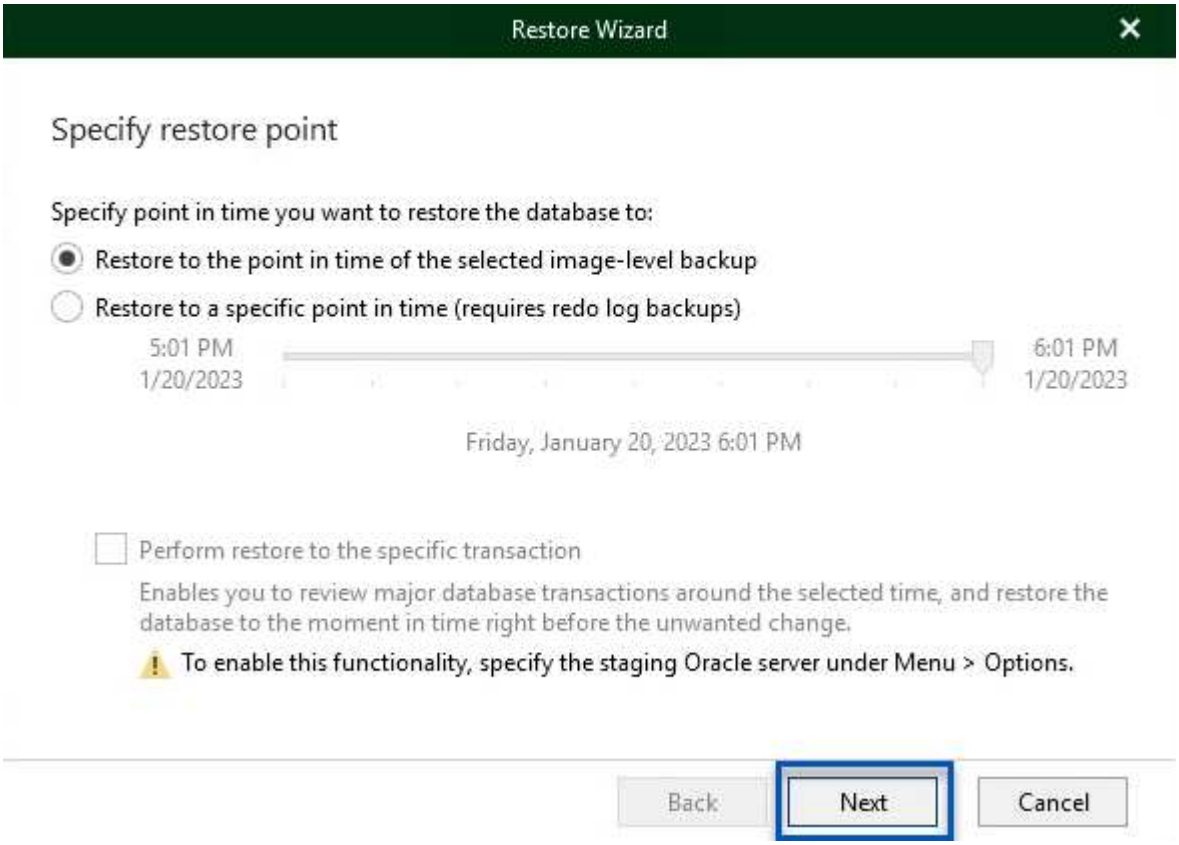


3. Geben Sie bei Bedarf einen * Wiederherstellungsgrund* ein, und klicken Sie dann auf der Übersichtsseite auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Oracle zu starten.

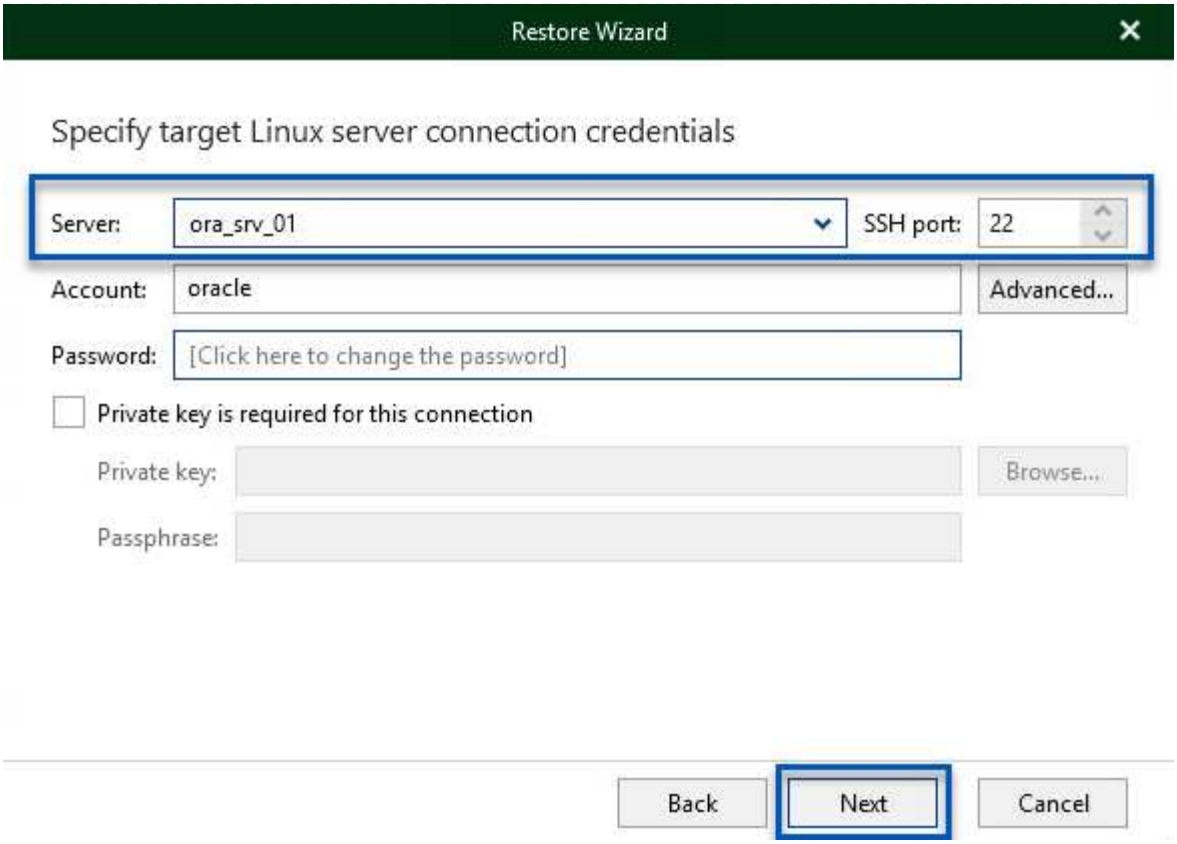
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie auf die Datenbank, die wiederhergestellt werden soll, und wählen Sie dann aus dem Dropdown-Menü **Datenbank wiederherstellen** oben **auf einem anderen Server wiederherstellen…**.



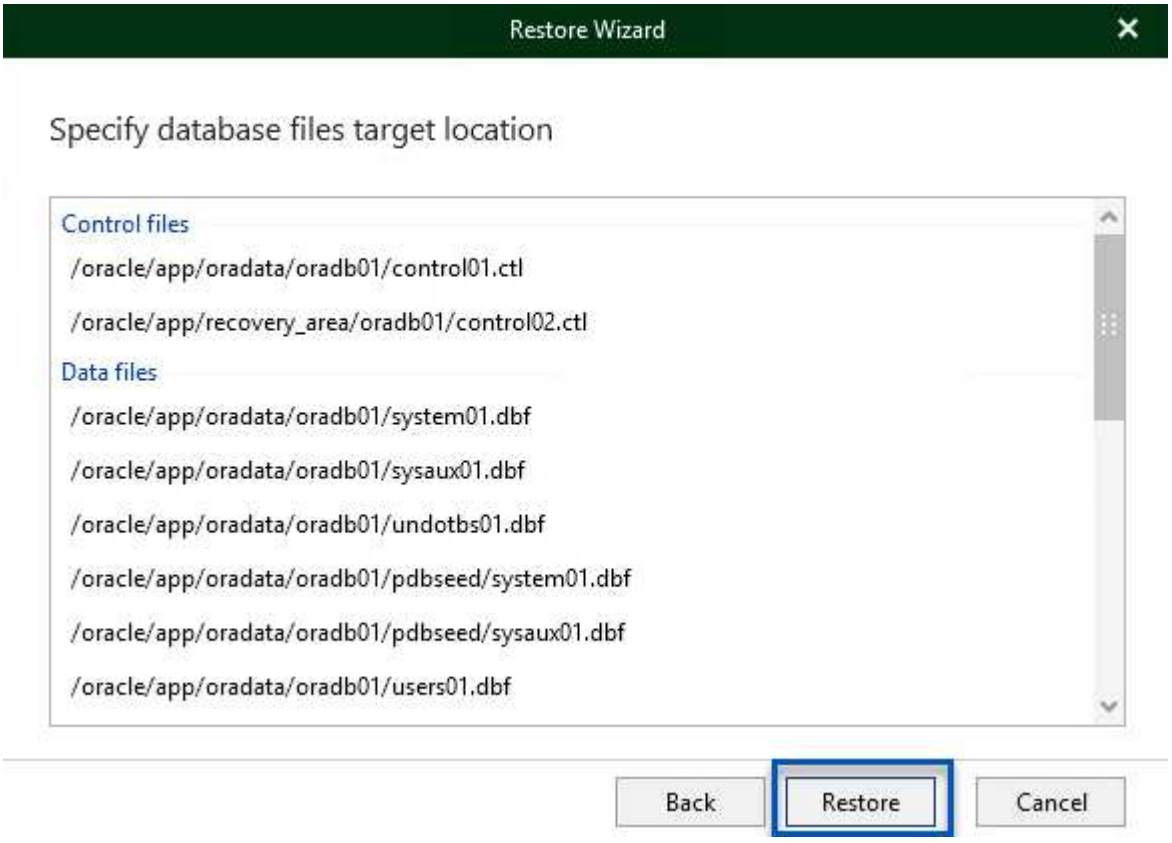
5. Geben Sie im Wiederherstellungsassistenten den Wiederherstellungspunkt an, von dem aus wiederhergestellt werden soll, und klicken Sie auf **Weiter**.



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.



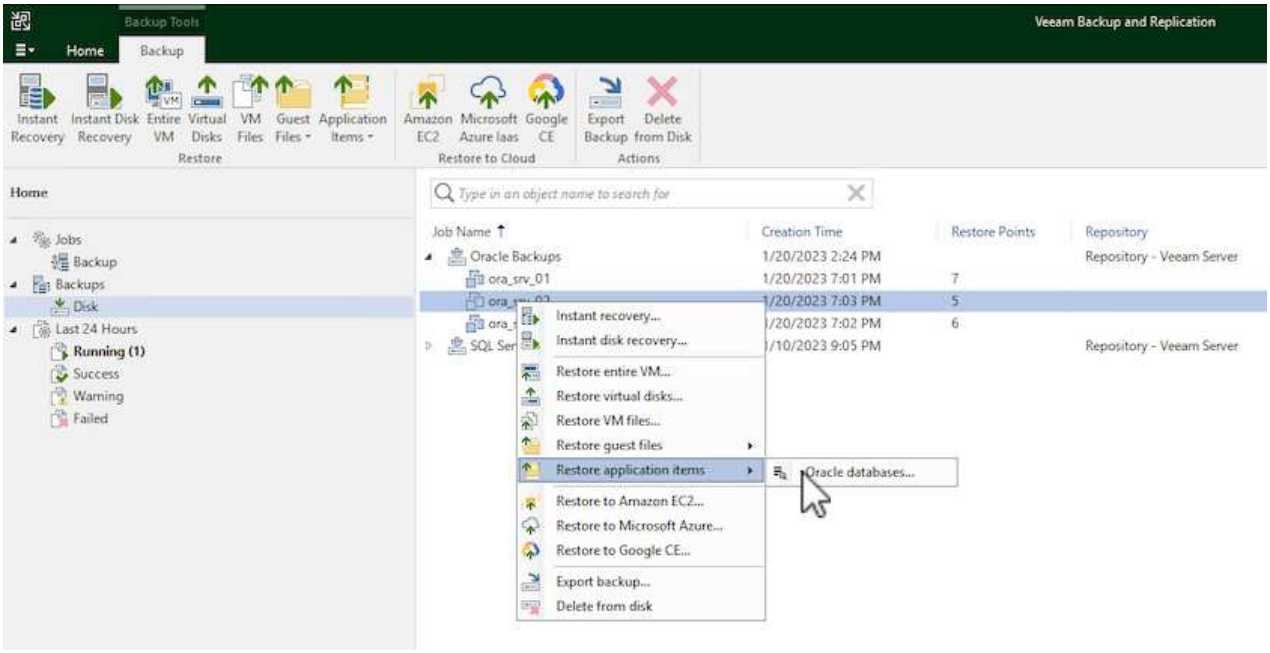
8. Sobald die Wiederherstellung der Datenbank abgeschlossen ist, überprüfen Sie, ob die Oracle-

Datenbank ordnungsgemäß auf dem Server gestartet wird.

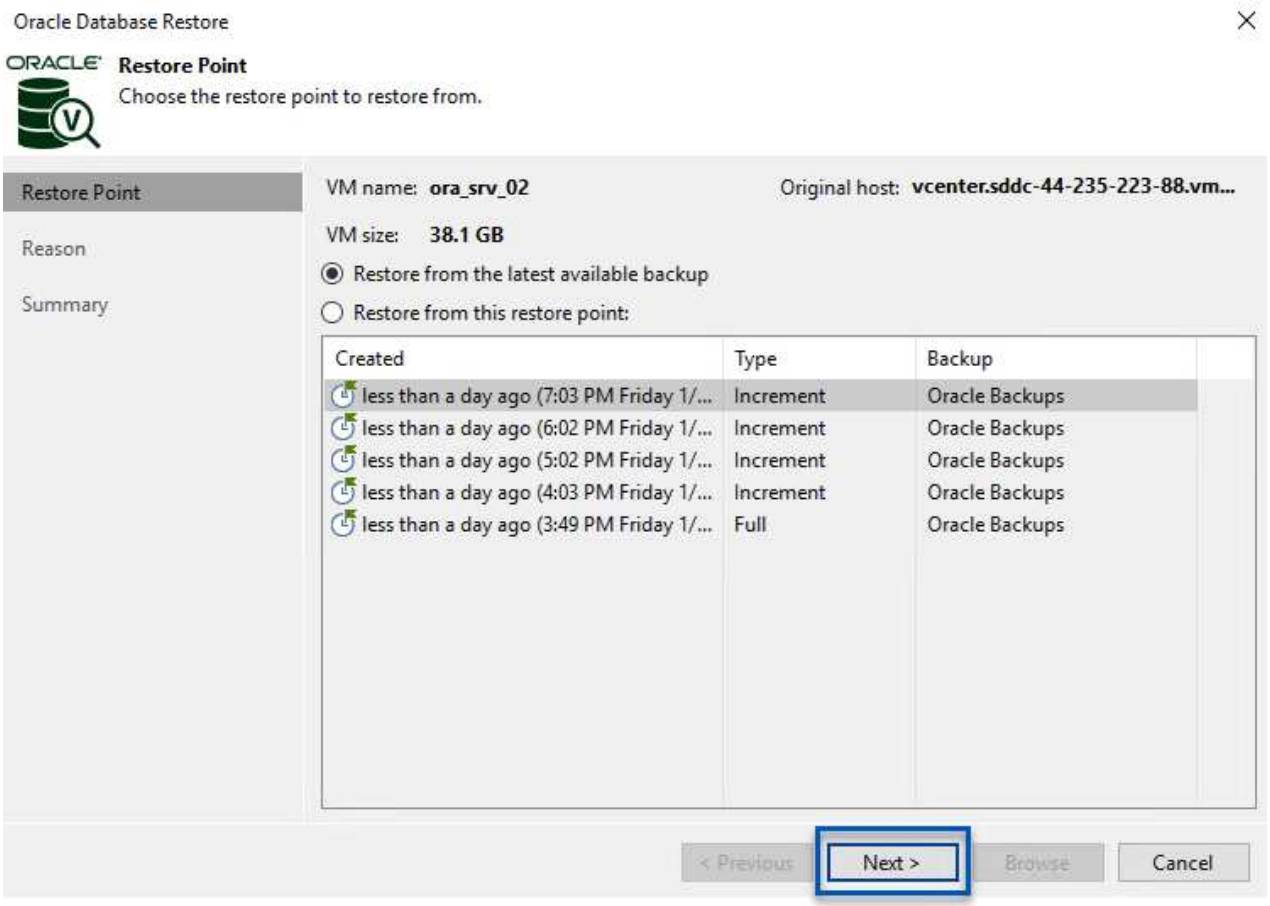
Veröffentlichen der Oracle-Datenbank auf einem alternativen Server

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

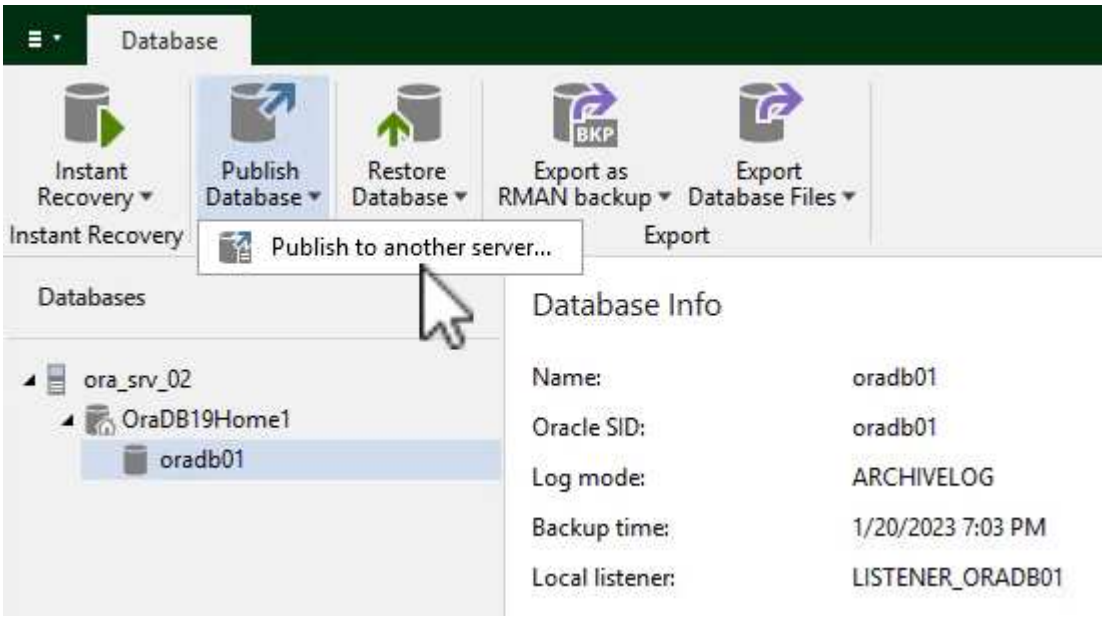
1. Navigieren Sie in der Veeam Backup and Replication-Konsole zur Liste der Oracle-Backups, klicken Sie mit der rechten Maustaste auf einen Server und wählen Sie **Restore Application items** und dann **Oracle Databases…** aus.



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

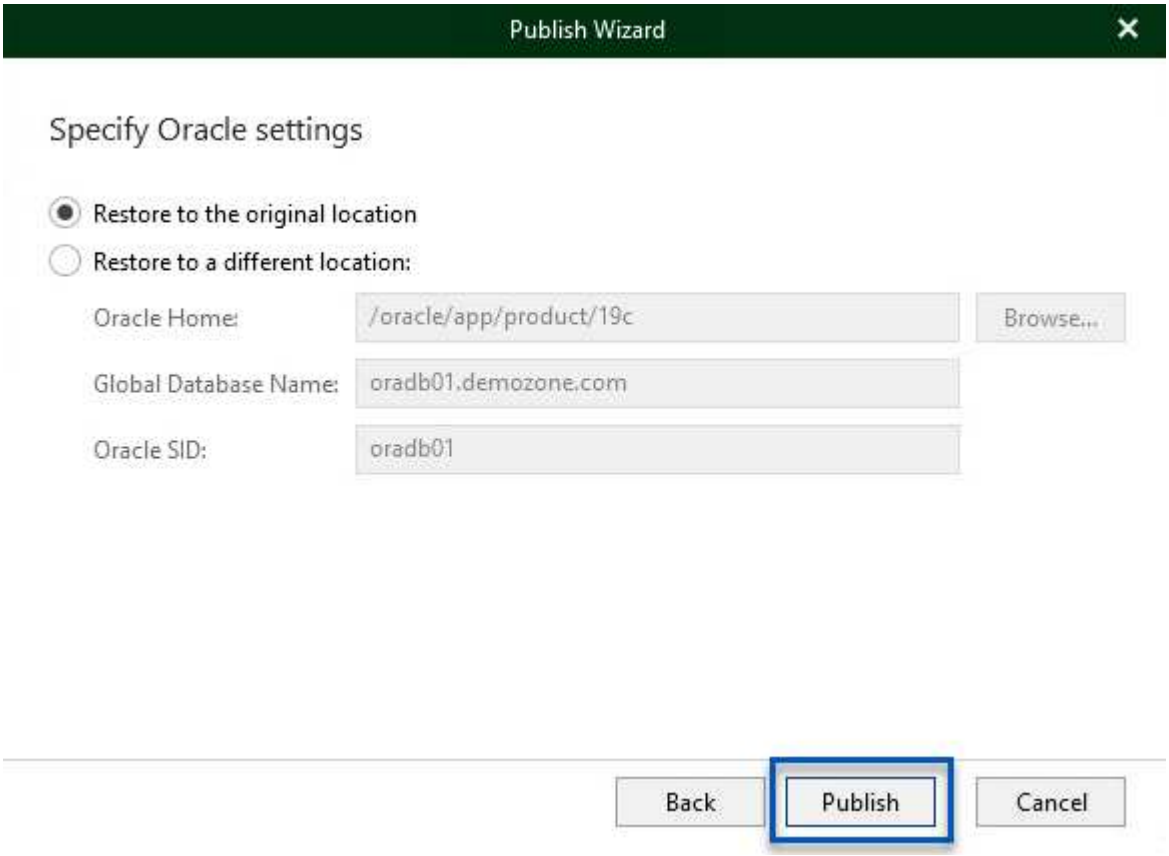


3. Geben Sie bei Bedarf einen * Wiederherstellungsgrund* ein, und klicken Sie dann auf der Übersichtsseite auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Oracle zu starten.
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie auf die Datenbank, die wiederhergestellt 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**.

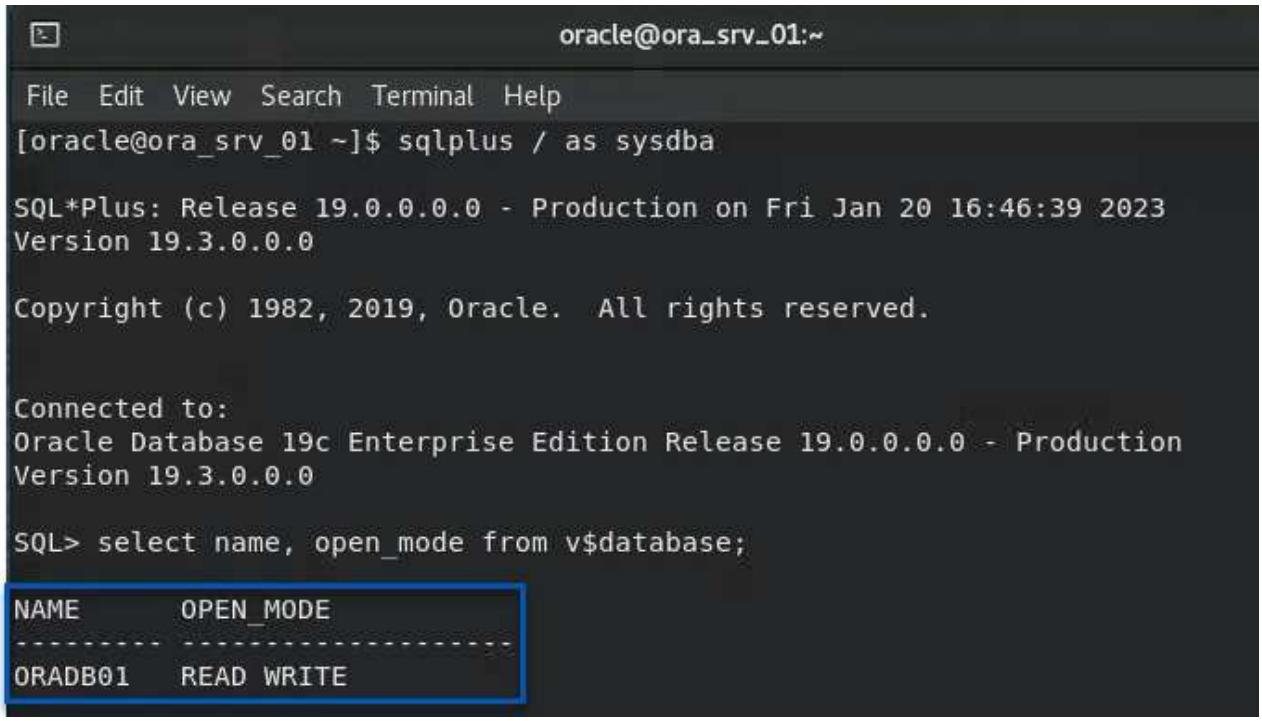
6. Geben Sie schließlich den Speicherort des Linux-Dateisystems an und klicken Sie auf **Veröffentlichen**, um den Wiederherstellungsprozess zu starten.



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;
```



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
```

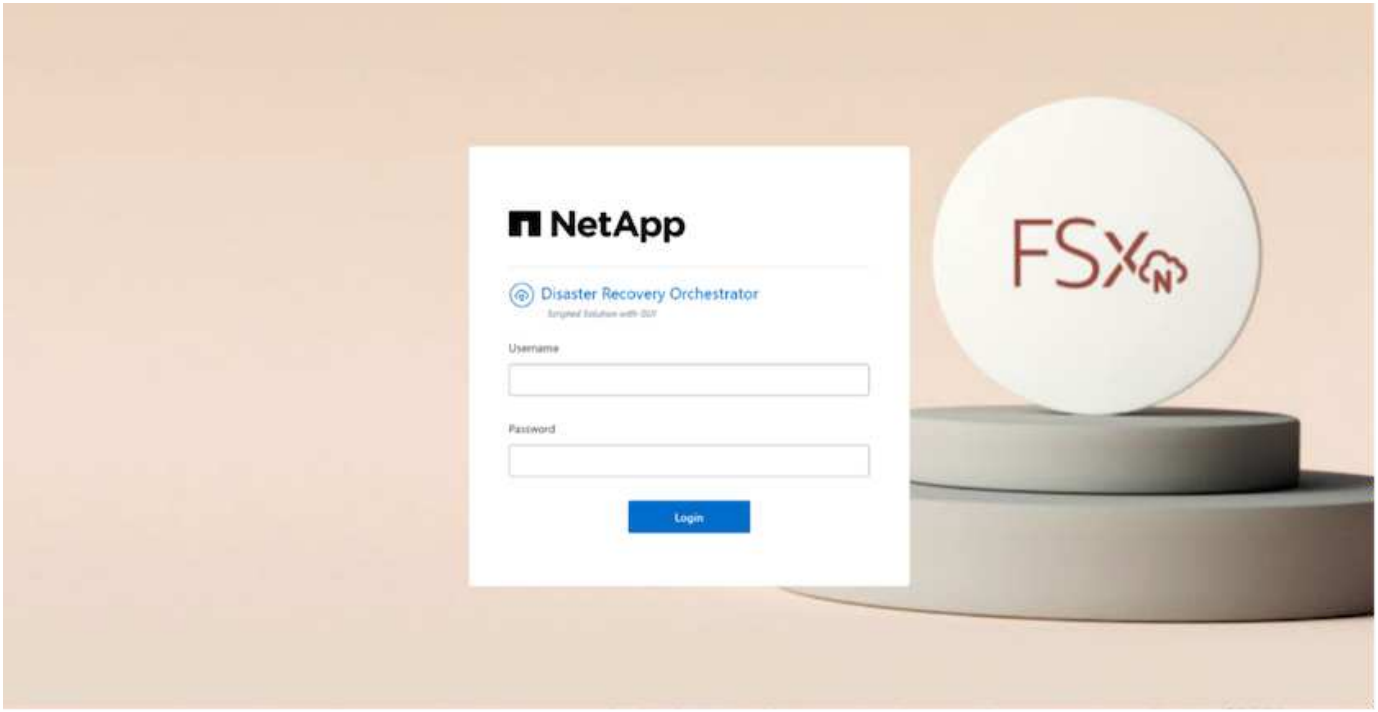
4. Greifen Sie über folgende Funktionen auf die UI zu:

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

   Mit den folgenden Standardanmeldeinformationen:

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

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



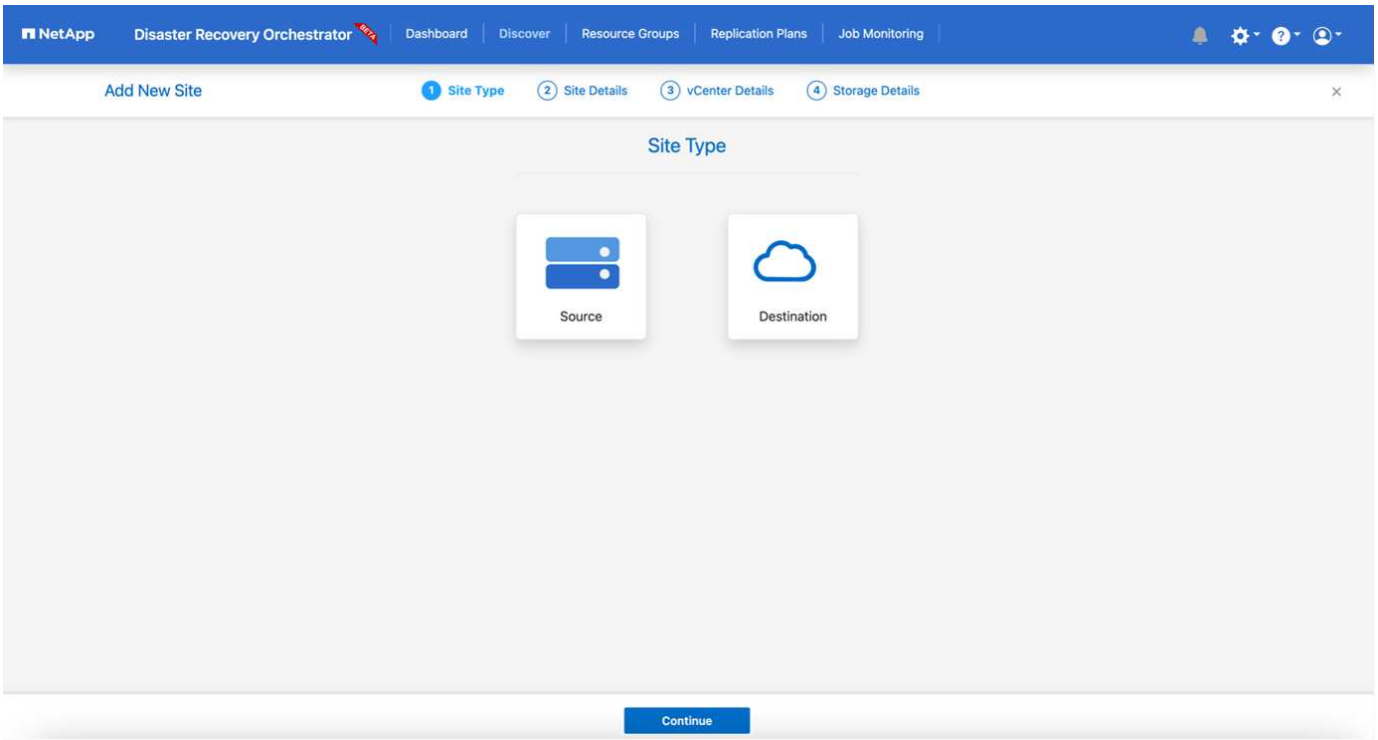
DRO-Konfiguration

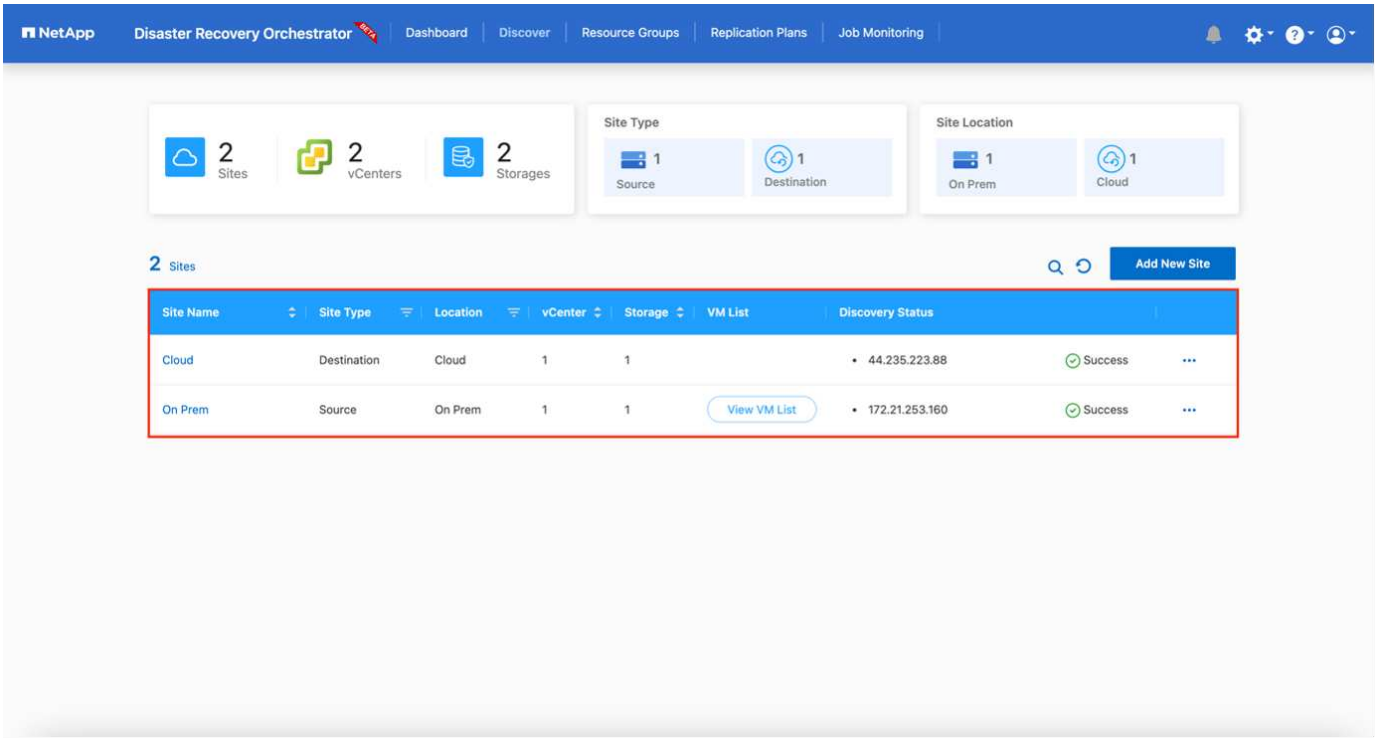
Nachdem FSX für ONTAP und VMC ordnungsgemäß konfiguriert wurden, können Sie DRO konfigurieren, um die Wiederherstellung lokaler Workloads auf VMC zu automatisieren. Dazu werden die schreibgeschützten SnapMirror Kopien auf FSX für ONTAP verwendet.

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.

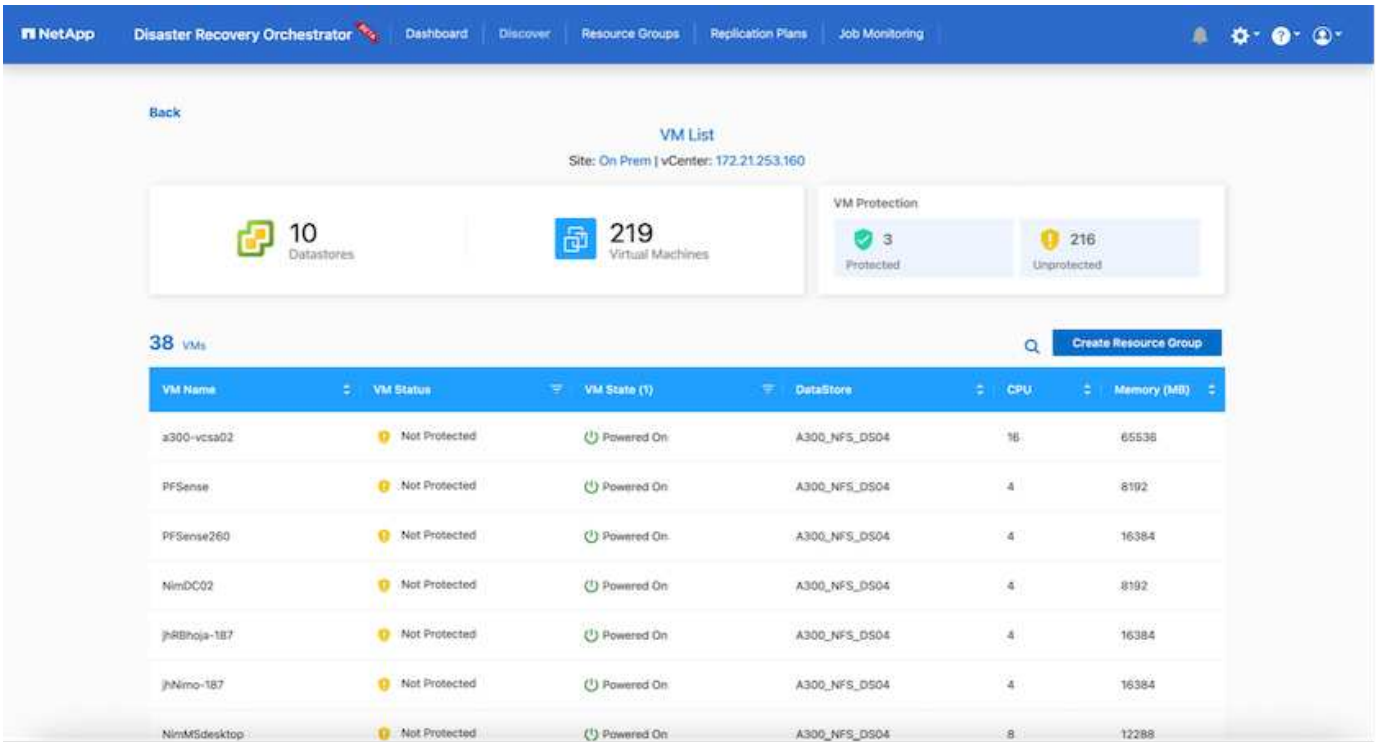
Im ersten Schritt werden lokale und Cloud-Ressourcen (vCenter und Storage) zu DRO hinzugefügt. Öffnen Sie DRO in einem unterstützten Browser, und verwenden Sie den Standardbenutzernamen und das Standardpasswort (admin/admin) und Add Sites. Standorte können auch mithilfe der Option Entdecken hinzugefügt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

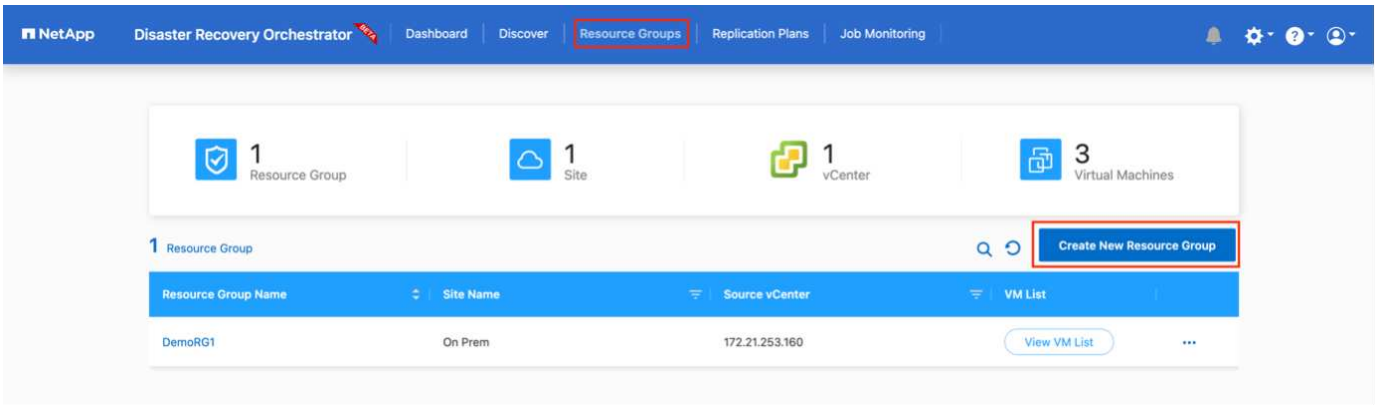
Gehen Sie wie folgt vor, um mit dem Erstellen von Ressourcengruppen zu beginnen:

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**.

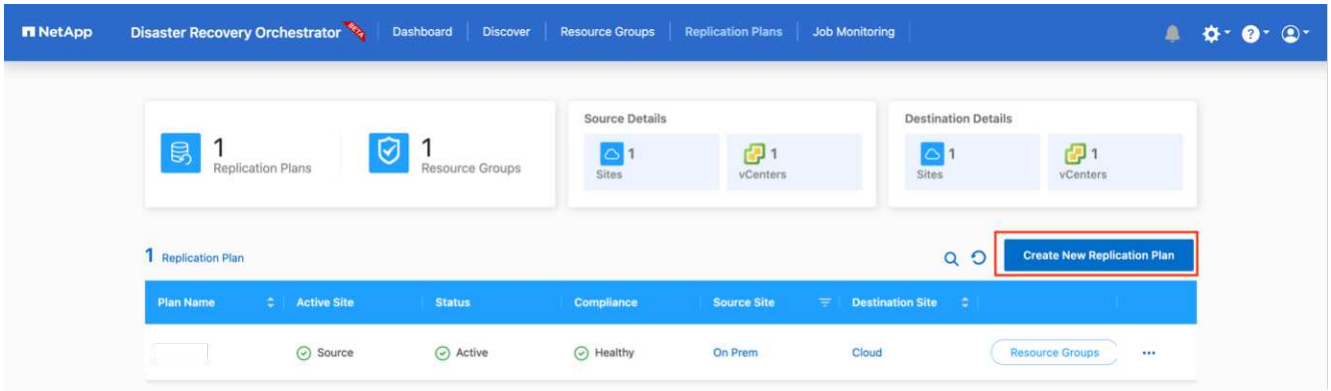


Replizierungspläne

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**.

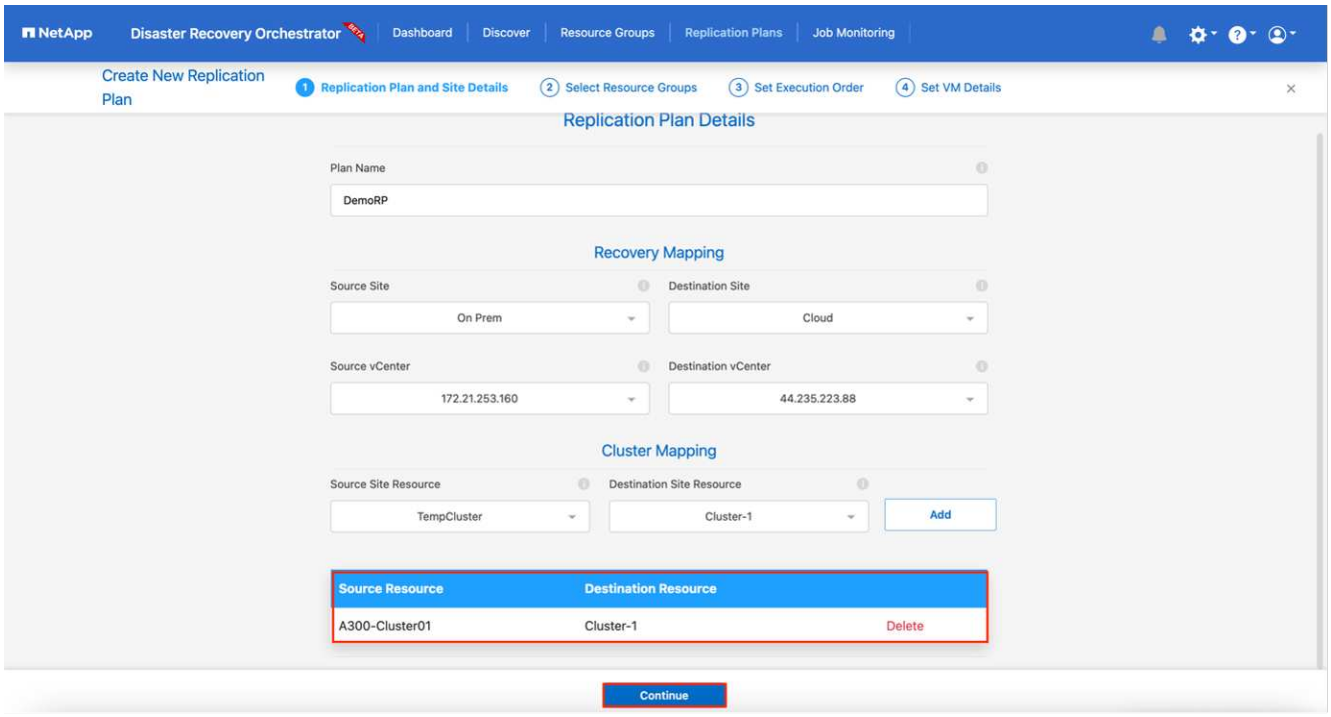
Gehen Sie wie folgt vor, um mit der Erstellung eines Replikationsplans zu beginnen:

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



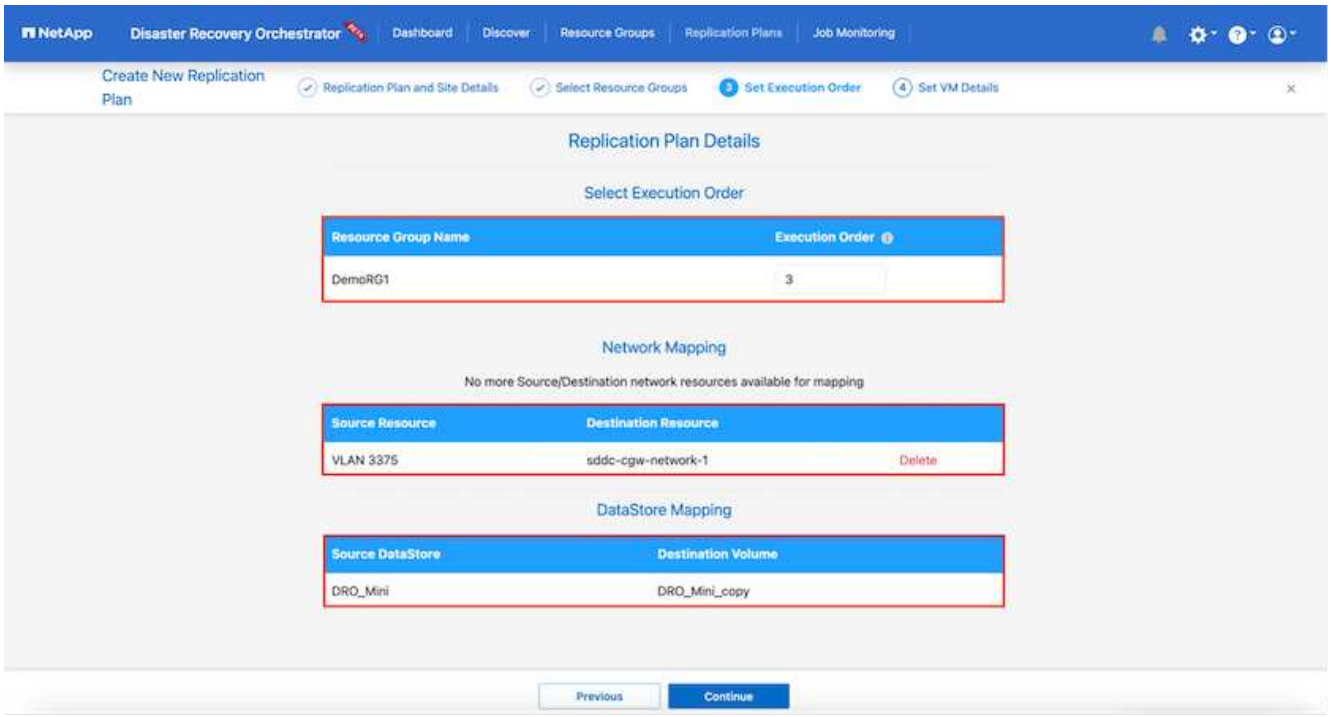
2. Geben Sie unter **New Replication Plan** einen Namen für den Plan ein und fügen Sie Recovery Mappings hinzu, indem Sie den Quellstandort, das zugehörige vCenter, den Zielstandort und das zugehörige vCenter auswählen.

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

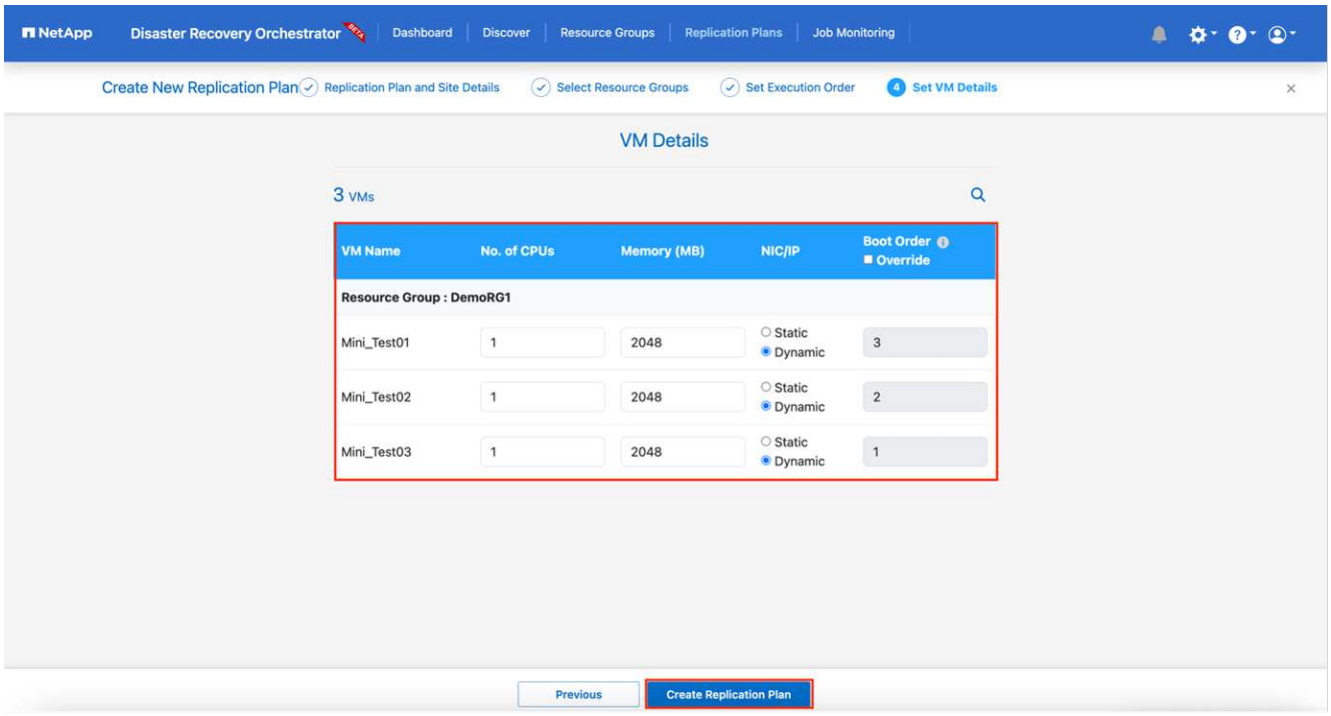


4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
6. Wählen Sie nach dem Beenden die Netzwerkzuordnung 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.

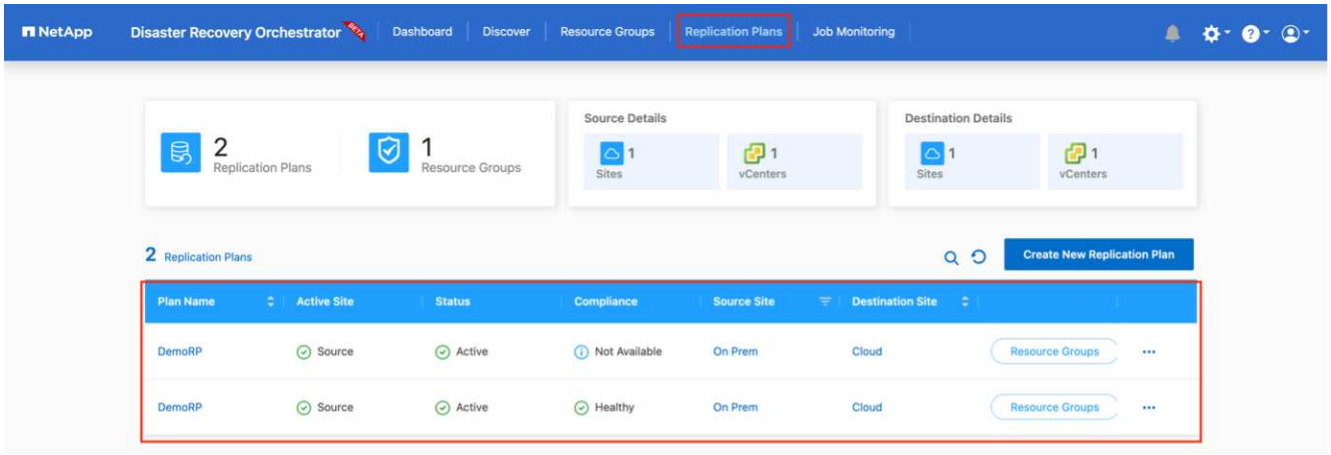
> SnapMirror befindet sich auf Volume-Ebene. Daher werden alle VMs zum Replizierungsziel repliziert. Vergewissern Sie sich, dass alle VMs ausgewählt sind, die Teil des Datastores sind. Sind sie nicht ausgewählt, werden nur die VMs verarbeitet, die Teil des Replikationsplans sind.



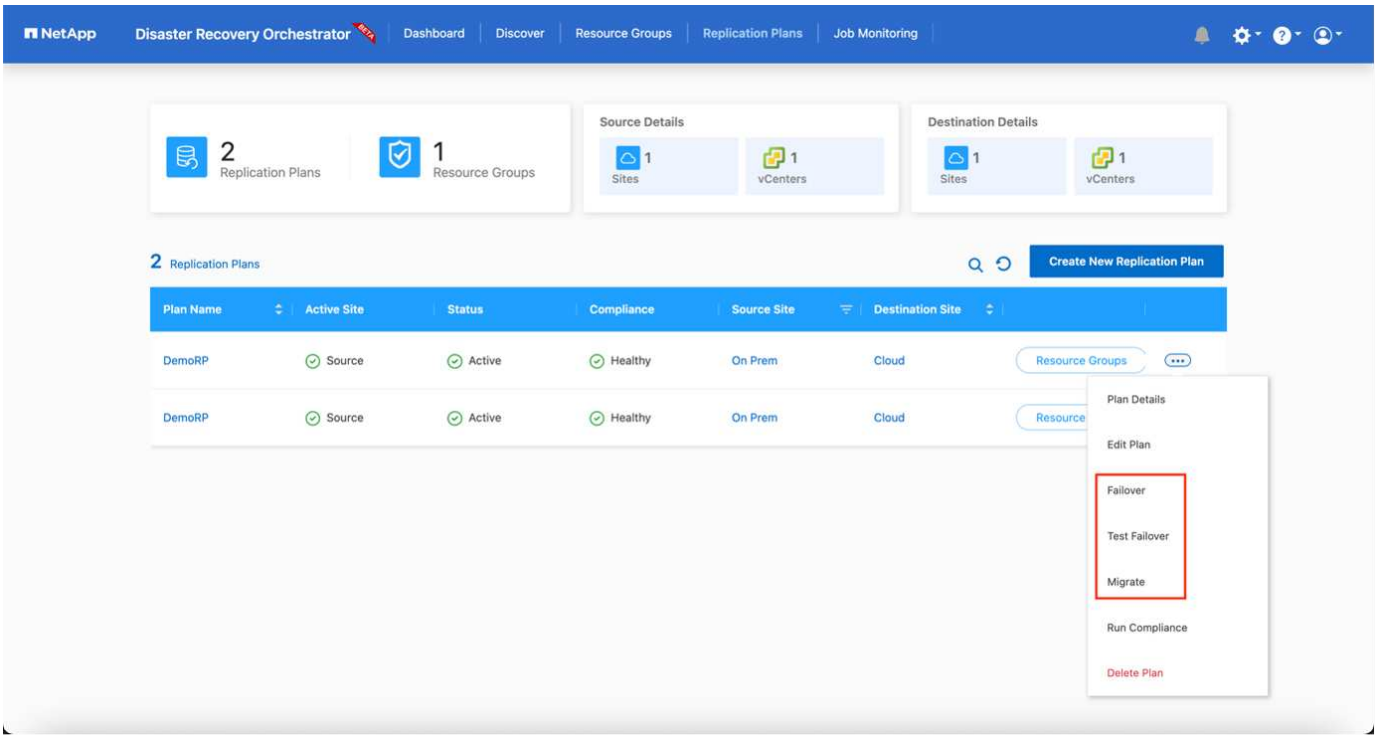
8. Unter den VM-Details können Sie optional die Größe der CPU- und RAM-Parameter der VM ändern. Dies kann sich sehr hilfreich erweisen, wenn Sie große Umgebungen auf kleinere Zielcluster wiederherstellen oder DR-Tests durchführen möchten, ohne eine eineineineineinone physische VMware-Infrastruktur bereitstellen 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.

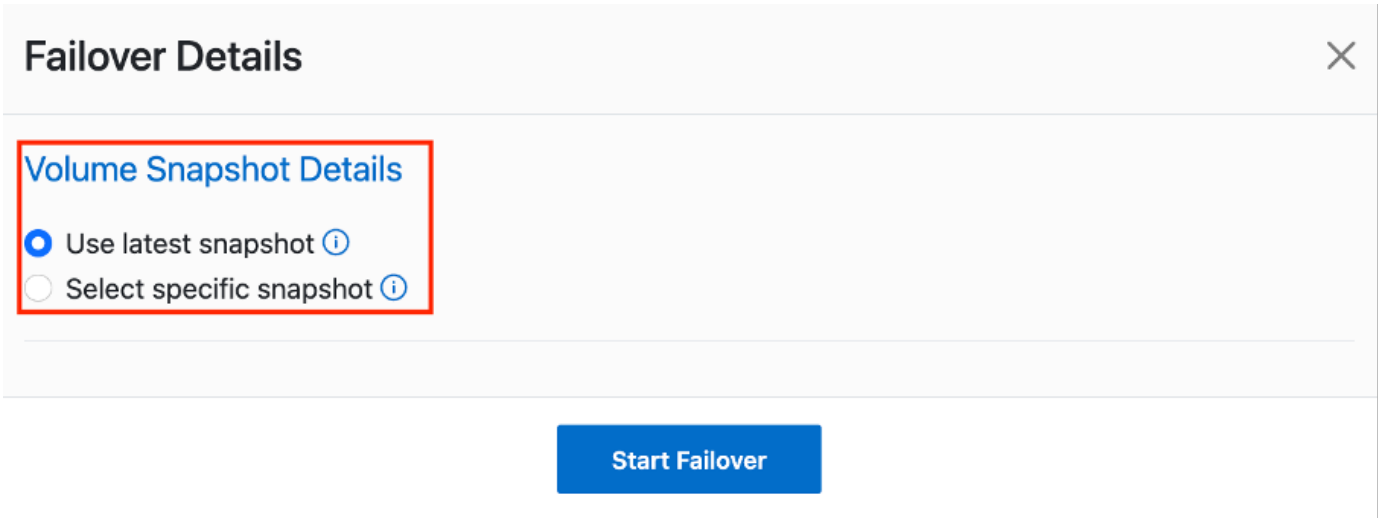


9. Klicken Sie Auf **Replikationsplan Erstellen**.

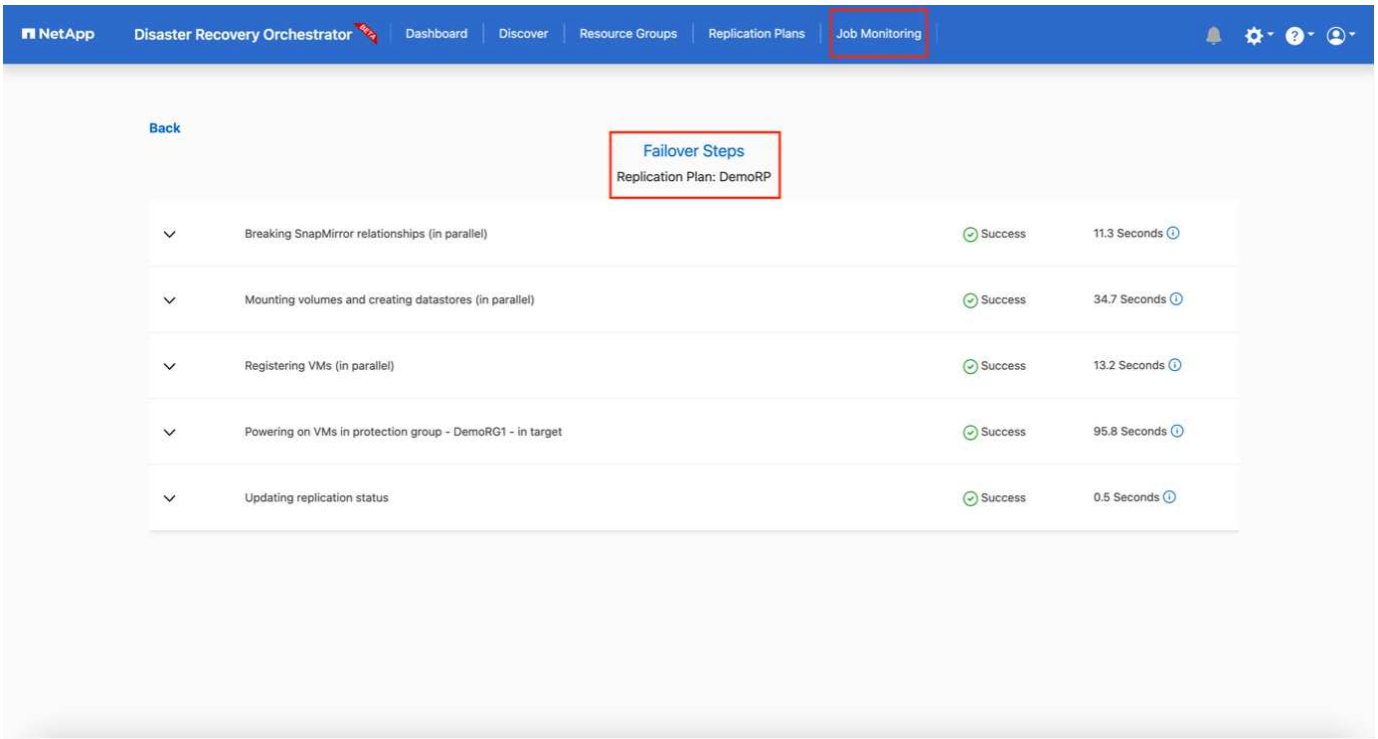


Nach dem Erstellen des Replizierungsplans können je nach Anforderungen die Failover-Option, die Test-Failover-Option oder die Migrationsoption ausgeübt werden. Während der Failover- und Test-Failover-Optionen wird die aktuellste SnapMirror Snapshot Kopie verwendet. Zudem kann aus einer zeitpunktgenauen 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.

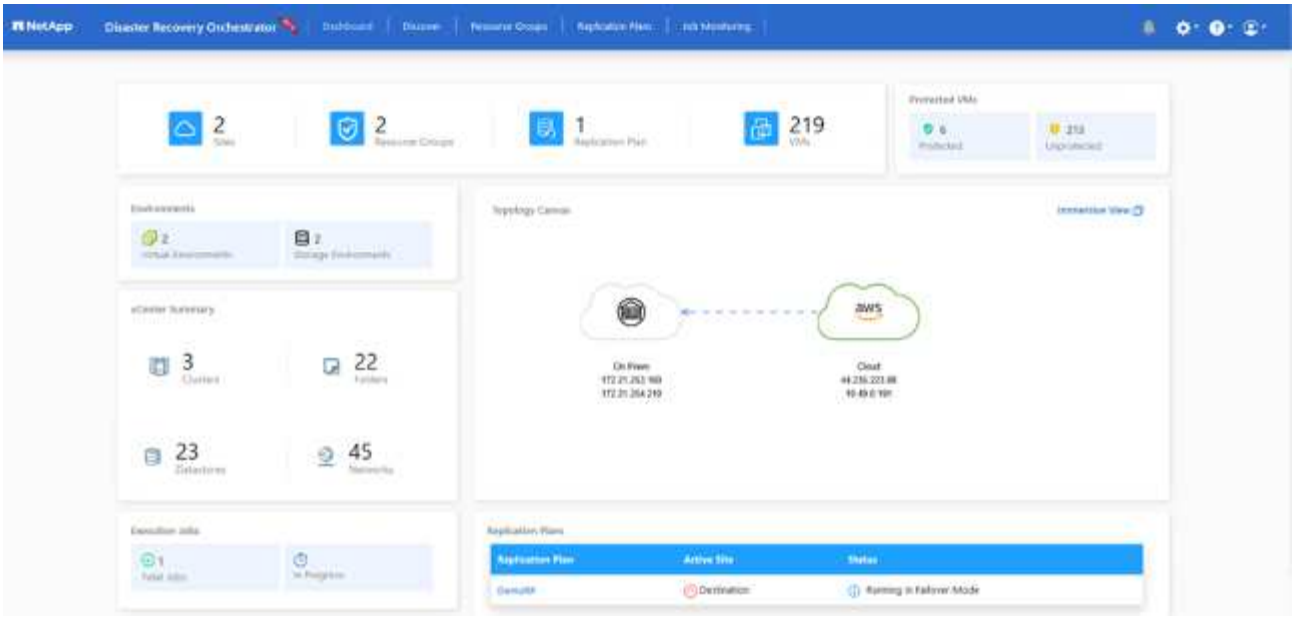




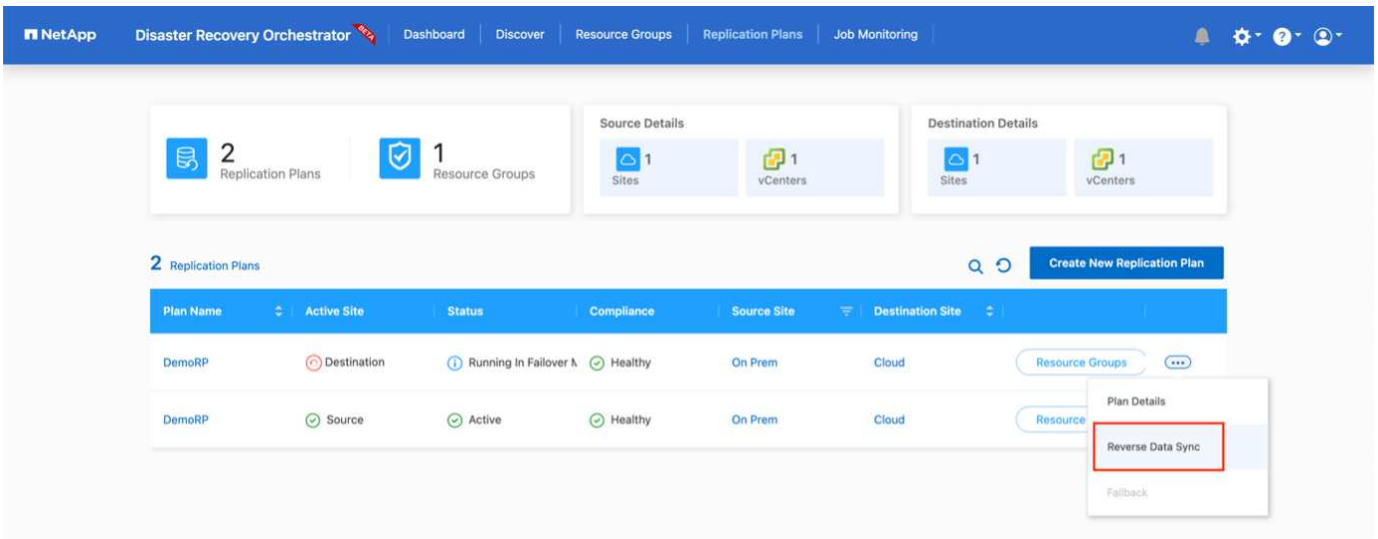
Der Replikationsplan kann im Aufgabenmenü überwacht werden:

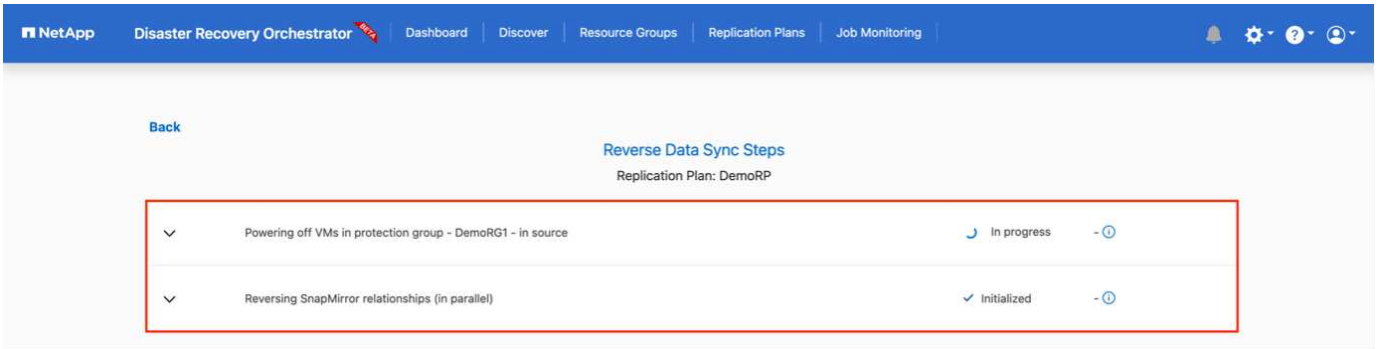


Nach der Auslösung des Failover sind die wiederhergestellten Elemente in VMC vCenter (VMs, Netzwerke, Datastores) ersichtlich. Standardmäßig werden die VMs in den Workload-Ordner wiederhergestellt.

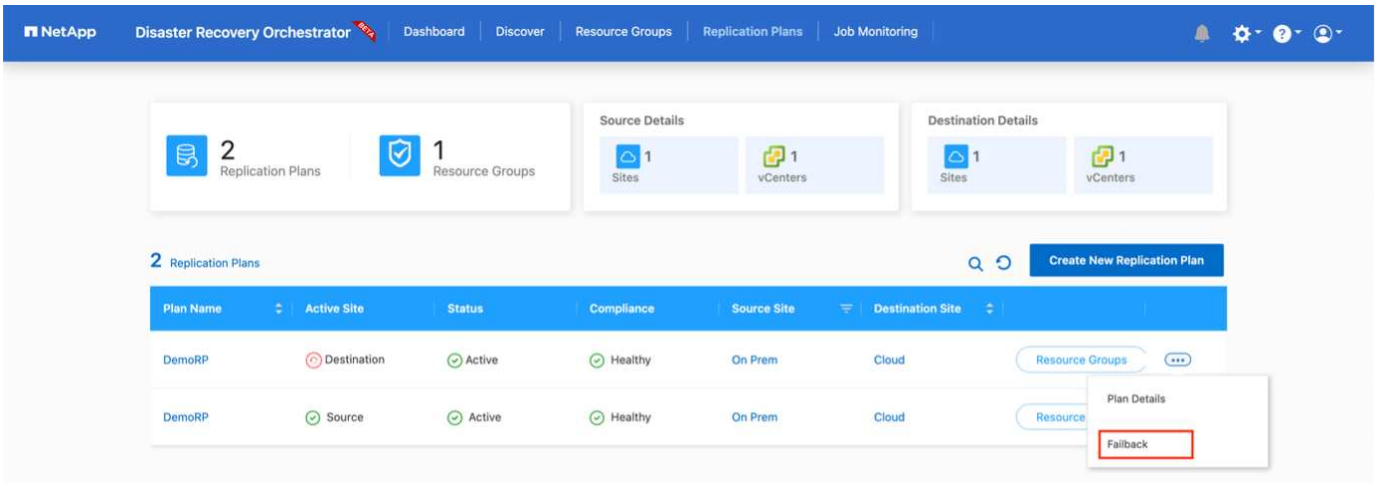


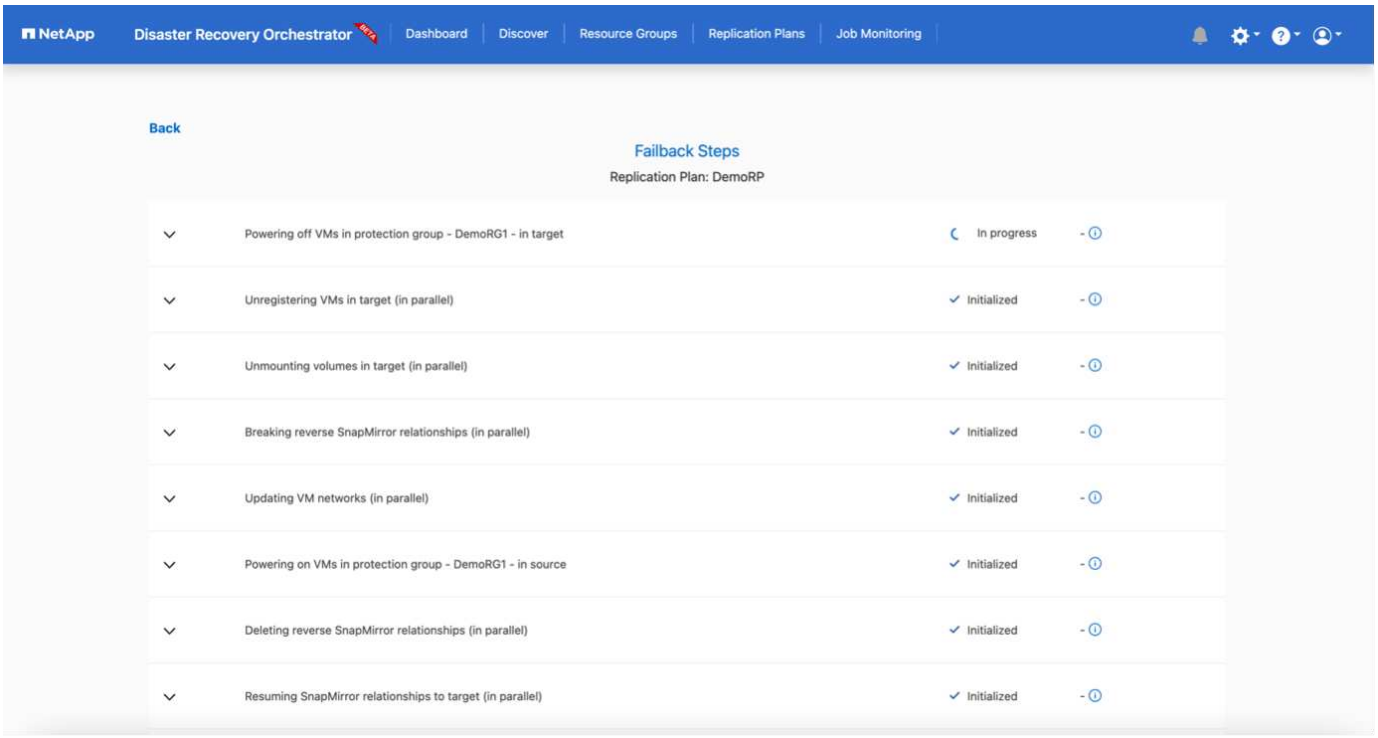
Failback kann auf der Ebene des Replikationsplans ausgelöst werden. Bei einem Test-Failover kann mit der Option „Tear-Down“ ein Rollback der Änderungen durchgeführt und die FlexClone Beziehung entfernt werden. Failback ist in Verbindung mit Failover ein Prozess in zwei Schritten. Wählen Sie den Replikationsplan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



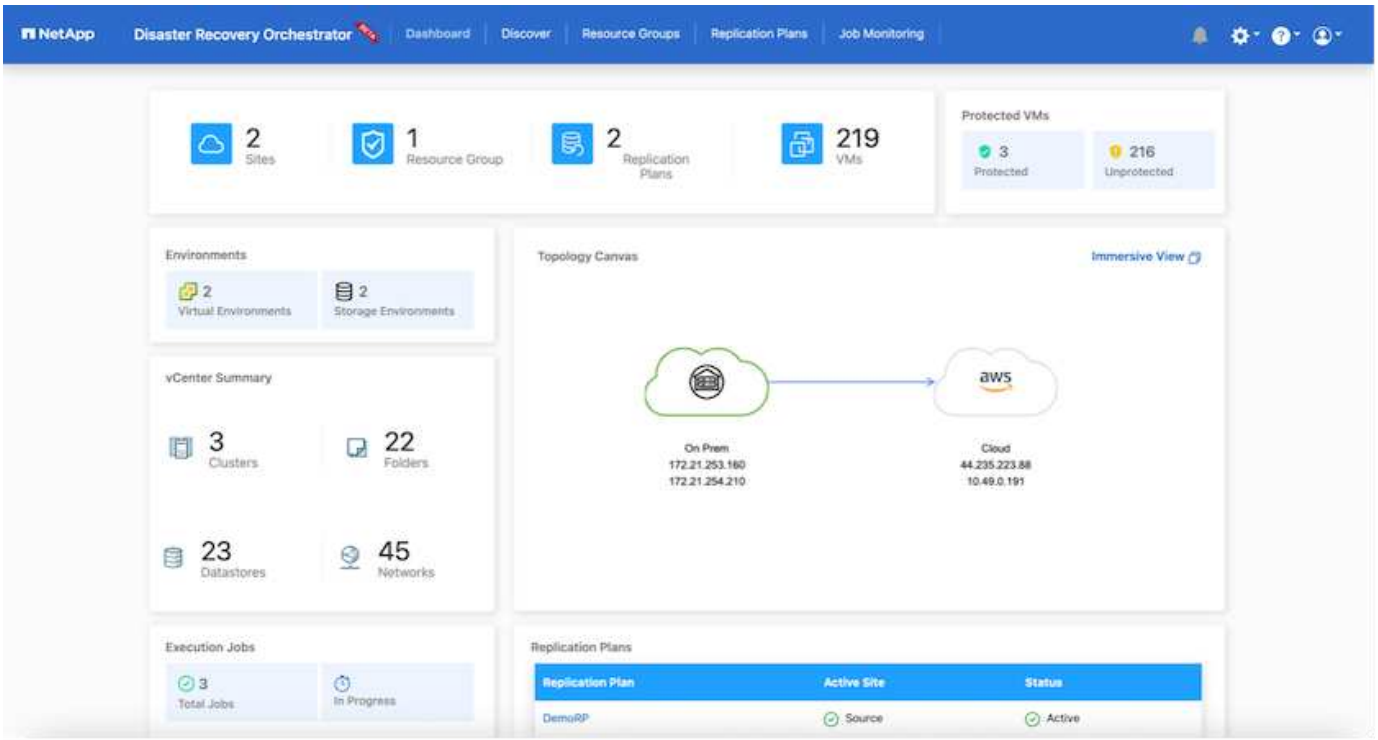


Wenn dieser Vorgang abgeschlossen ist, können Sie ein Failback auslösen und zum ursprünglichen Produktionsstandort zurückkehren.





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.

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

Migration von Workloads auf AWS/VMC

TR 4942: Migration von Workloads auf FSX ONTAP Datastore mithilfe von VMware HCX

Autor(en): NetApp Solutions Engineering

Übersicht: Migration von Virtual Machines mit VMware HCX, FSX ONTAP zusätzlichen Datastores und VMware Cloud

Als typischer Anwendungsfall für VMware Cloud (VMC) auf Amazon Web Services (AWS) mit seinem zusätzlichen NFS-Datastore auf Amazon FSX für NetApp ONTAP ist die Migration von VMware Workloads zu verwenden. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmethoden zum Verschieben von On-Premises-Virtual Machines (VMs) und deren Daten, die auf beliebigen von VMware unterstützten Datastores ausgeführt werden, in VMC-Datastores, darunter zusätzliche NFS-Datastores auf FSX für ONTAP.

VMware HCX ist primär eine Mobilitätsplattform, die speziell zur Cloud-übergreifenden Vereinfachung der Workload-Migration, des Ausgleichs von Workloads und der Business Continuity entwickelt wurde. Es wird im Rahmen von VMware Cloud auf AWS enthalten und bietet viele Möglichkeiten zur Migration von Workloads und kann für Disaster-Recovery-Vorgänge (DR) genutzt werden.

Dieses Dokument bietet eine Schritt-für-Schritt-Anleitung zur Implementierung und Konfiguration von VMware HCX, einschließlich aller Hauptkomponenten – vor Ort und im Cloud-Datacenter –, die verschiedene VM-Migrationsmechanismen unterstützt.

Weitere Informationen finden Sie unter "Einführung in HCX-Implementierungen" Und "Checkliste B – HCX mit einer VMware Cloud auf AWS SDDC Zielumgebung installieren".

Allgemeine Schritte

Diese Liste enthält grundlegende Schritte zur Installation und Konfiguration von VMware HCX:

1. Aktivieren Sie HCX für das softwaredefinierte VMC Datacenter (SDDC) über die VMware Cloud Services Console.
2. Laden Sie das OVA-Installationsprogramm für HCX Connector im lokalen vCenter Server herunter und stellen Sie es bereit.
3. HCX mit einem Lizenzschlüssel aktivieren.
4. Verbinden Sie den VMware HCX Connector vor Ort mit VMC HCX Cloud Manager.
5. Sie konfigurieren das Netzwerkprofil, das Computing-Profil und das Service-Mesh.
6. (Optional) Führen Sie eine Netzwerkerweiterung aus, um das Netzwerk zu erweitern und eine erneute IP-Adresse zu vermeiden.
7. Validieren des Appliance-Status und Sicherstellen der Möglichkeit der Migration
8. Migration der VM-Workloads

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "Vorbereitung der HCX-Installation". Nachdem die Voraussetzungen einschließlich Konnektivität erfüllt sind, konfigurieren und aktivieren Sie HCX, indem Sie einen Lizenzschlüssel aus der VMware HCX-Konsole bei VMC generieren. Nach der Aktivierung von HCX wird das vCenter Plug-in implementiert und kann über die vCenter-Konsole zur Verwaltung aufgerufen werden.

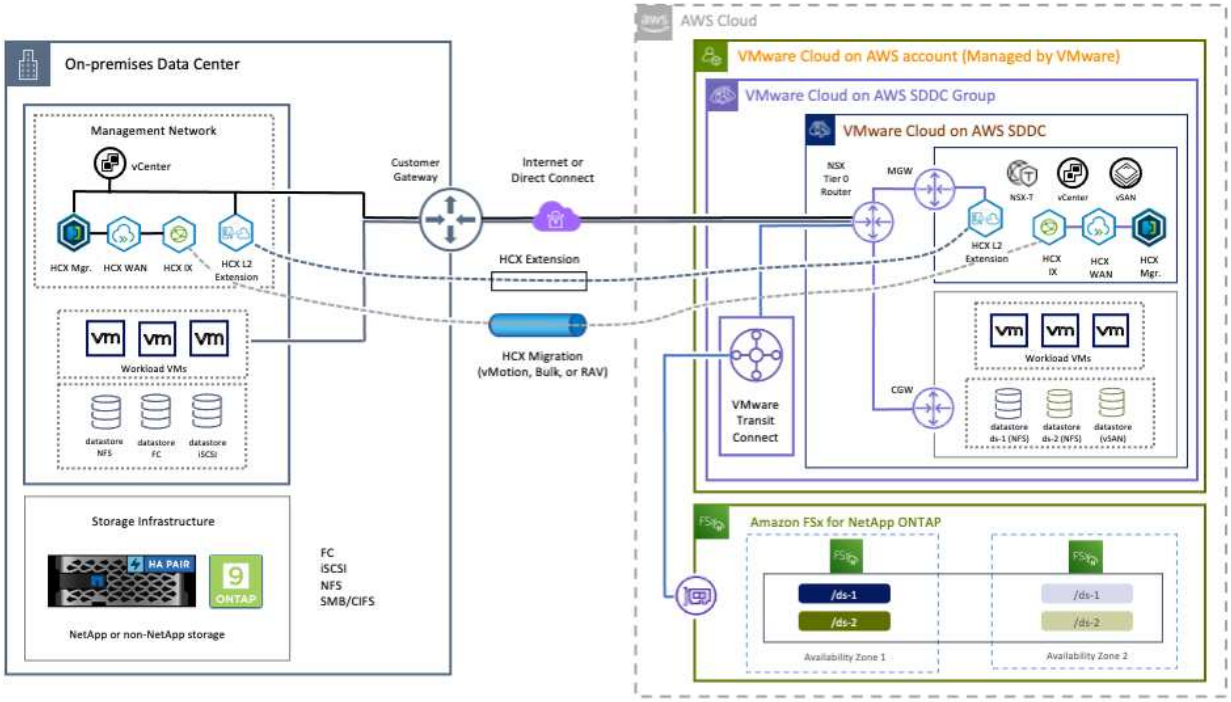
Die folgenden Installationsschritte müssen ausgeführt werden, bevor Sie mit der HCX-Aktivierung und -Bereitstellung fortfahren:

1. Verwenden Sie ein vorhandenes VMC SDDC oder erstellen Sie nach diesem Vorgang ein neues SDDC "Link von NetApp" Oder hier "Link zu VMware".
2. Der Netzwerkpfad von der lokalen vCenter Umgebung zu VMC SDDC muss die Migration von VMs über vMotion unterstützen.
3. Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und -Ports" Sind für vMotion Traffic zwischen dem lokalen vCenter Server und dem SDDC vCenter zulässig.
4. Das FSX für ONTAP-NFS-Volume sollte als zusätzlicher Datastore im VMC SDDC gemountet werden. Befolgen Sie die in diesem Schritt beschriebenen Schritte, um die NFS-Datenspeicher an den entsprechenden Cluster anzuhängen "Link von NetApp" Oder hier "Link zu VMware".

Übergeordnete Architektur

Die für diese Validierung verwendete On-Premises-Lab-Umgebung wurde zu Testzwecken über ein Site-to-Site-VPN mit AWS VPC verbunden. Dies ermöglichte eine On-Premises-Konnektivität mit AWS und dem VMware Cloud SDDC über ein externes Transit Gateway. HCX-Migration und Netzwerkerweiterungsverkehr fließen über das Internet zwischen On-Premises- und VMware-Cloud-Ziel SDDC. Diese Architektur kann auf private virtuelle Direct Connect-Schnittstellen geändert werden.

Das folgende Bild stellt die allgemeine Architektur dar.



Lösungsimplementierung

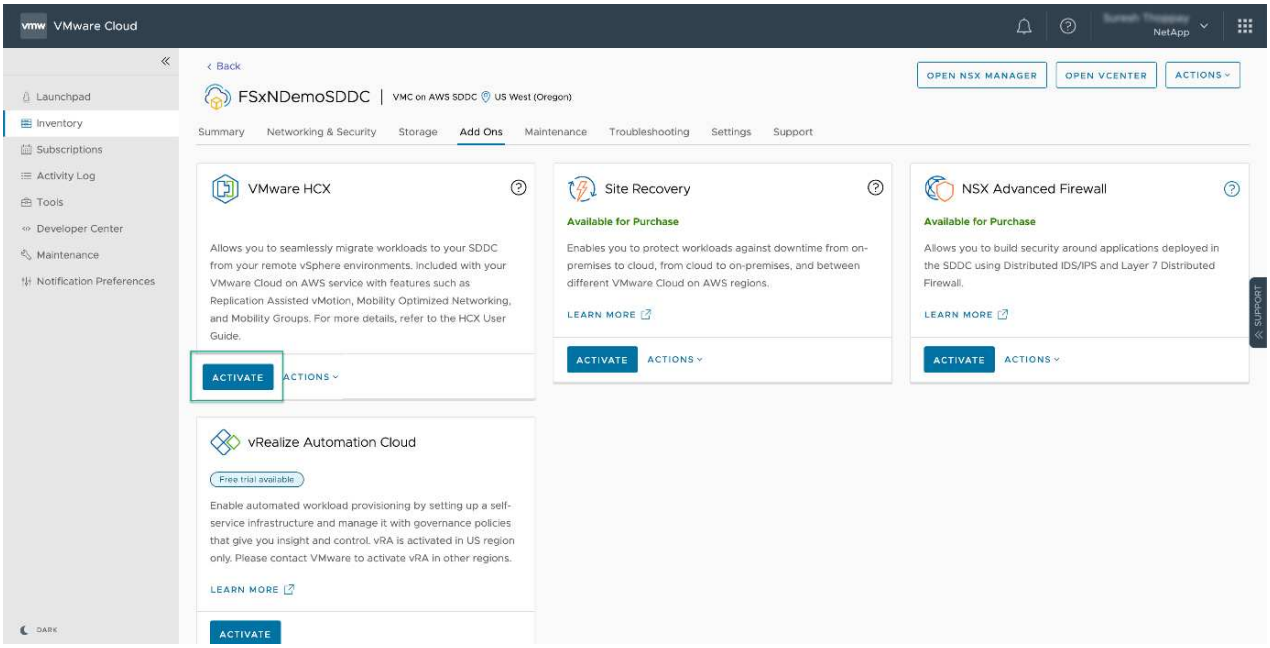
Führen Sie die folgenden Schritte aus, um die Implementierung dieser Lösung abzuschließen:

Schritt 1: HCX über VMC SDDC mit der Option Add-ons aktivieren

Gehen Sie wie folgt vor, um die Installation durchzuführen:

1. Melden Sie sich an der VMC-Konsole unter an "vmc.vmware.com" Und greifen Sie auf das Inventar zu.
2. Um das entsprechende SDDC auszuwählen und auf Add-ons zuzugreifen, klicken Sie auf Details anzeigen im SDDC und wählen Sie die Registerkarte Add-ons aus.
3. Klicken Sie auf Aktivieren für VMware HCX.

   Dieser Schritt dauert bis zu 25 Minuten.

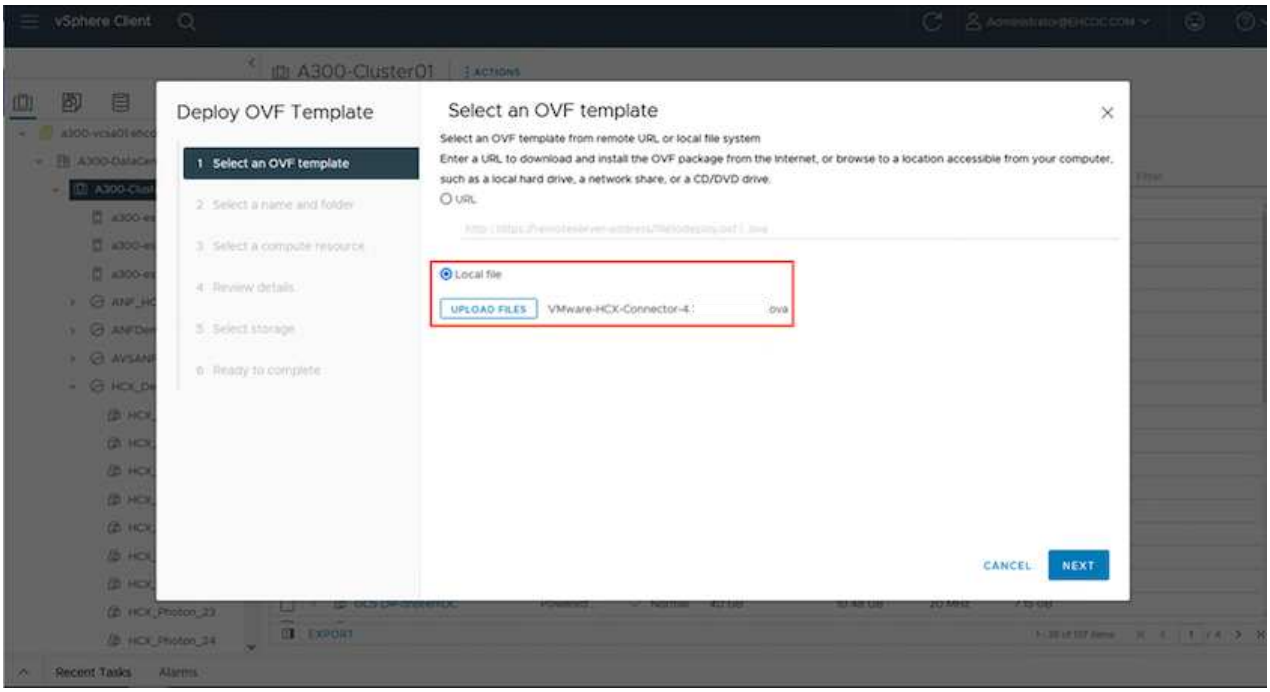


4. Nachdem die Implementierung abgeschlossen ist, validieren Sie die Implementierung, indem Sie bestätigen, dass HCX Manager und die zugehörigen Plug-ins in der vCenter Console verfügbar sind.
5. Erstellen Sie die entsprechenden Management Gateway-Firewalls, um die erforderlichen Ports für den Zugriff auf HCX Cloud Manager zu öffnen.HCX Cloud Manager ist jetzt für HCX-Vorgänge bereit.

Schritt 2: Stellen Sie das Installationsprogramm OVA im lokalen vCenter Server bereit

Damit der On-Premises Connector mit dem HCX Manager in VMC kommunizieren kann, stellen Sie sicher, dass die entsprechenden Firewall-Ports in der On-Premises-Umgebung geöffnet sind.

1. Navigieren Sie von der VMC-Konsole zum HCX Dashboard, gehen Sie zu Administration und wählen Sie die Registerkarte Systemaktualisierung aus. Klicken Sie auf Download-Link für das OVA-Bild des HCX-Connectors anfordern.
2. Stellen Sie die OVA beim Herunterladen des HCX Connectors im lokalen vCenter Server bereit. Klicken Sie mit der rechten Maustaste auf vSphere Cluster und wählen Sie die Option OVF-Vorlage bereitstellen aus.

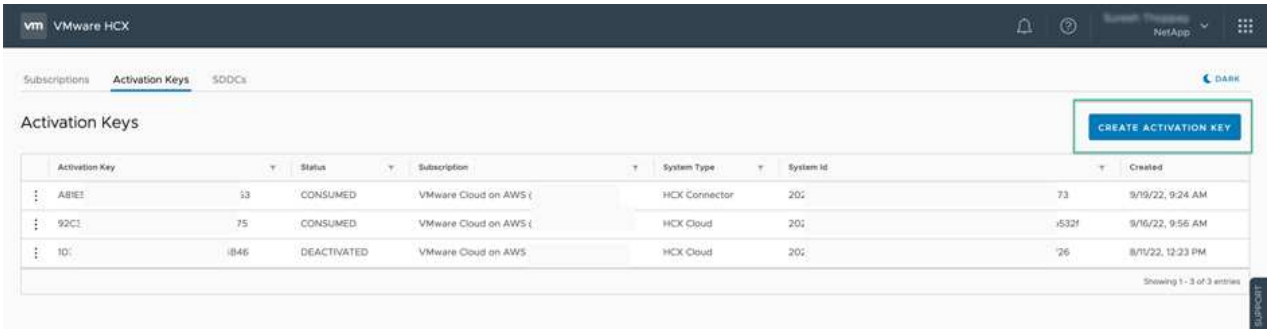


3. Geben Sie die erforderlichen Informationen im Assistenten zur Bereitstellung von OVF-Vorlagen ein, klicken Sie auf Weiter und anschließend auf Fertig stellen, um die OVA des VMware HCX-Connectors bereitzustellen.
4. Schalten Sie das virtuelle Gerät manuell ein.Schritt-für-Schritt-Anleitungen finden Sie unter "VMware HCX-Benutzerhandbuch".

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie den VMware HCX Connector OVA vor Ort bereitgestellt und das Gerät gestartet haben, führen Sie die folgenden Schritte aus, um den HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel von der VMware HCX Console bei VMC und geben Sie die Lizenz während der VMware HCX Connector-Einrichtung ein.

1. Wählen Sie in der VMware Cloud Console „Inventar“, wählen Sie das SDDC und klicken Sie auf „Details anzeigen“. Klicken Sie auf der Registerkarte Add ons in der Kachel VMware HCX auf Open HCX.
2. Klicken Sie auf der Registerkarte Aktivierungsschlüssel auf Aktivierungsschlüssel erstellen. Wählen Sie den Systemtyp als HCX-Anschluss aus, und klicken Sie auf Bestätigen, um den Schlüssel zu generieren. Kopieren Sie den Aktivierungsschlüssel.



> Für jeden HCX Connector, der vor Ort eingesetzt wird, ist ein separater Schlüssel erforderlich.

3. Melden Sie sich beim lokalen VMware HCX Connector unter an "https://hcxconnectorIP:9443" Administratordaten werden verwendet.

> Verwenden Sie das während der OVA-Bereitstellung definierte Passwort.

4. Geben Sie im Abschnitt Lizenzierung den Aktivierungsschlüssel ein, der aus Schritt 2 kopiert wurde, und klicken Sie auf Aktivieren.

> Der HCX-Connector vor Ort muss über einen Internetzugang verfügen, damit die Aktivierung erfolgreich abgeschlossen werden kann.

5. Geben Sie unter Datacenter Location den gewünschten Speicherort für die Installation des VMware HCX Manager vor Ort an. Klicken Sie auf Weiter .
6. Aktualisieren Sie unter Systemname den Namen, und klicken Sie auf Weiter.
7. Wählen Sie Ja, und fahren Sie fort.
8. Geben Sie unter vCenter verbinden die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) und die Anmeldeinformationen für den vCenter-Server ein, und klicken Sie auf Weiter.

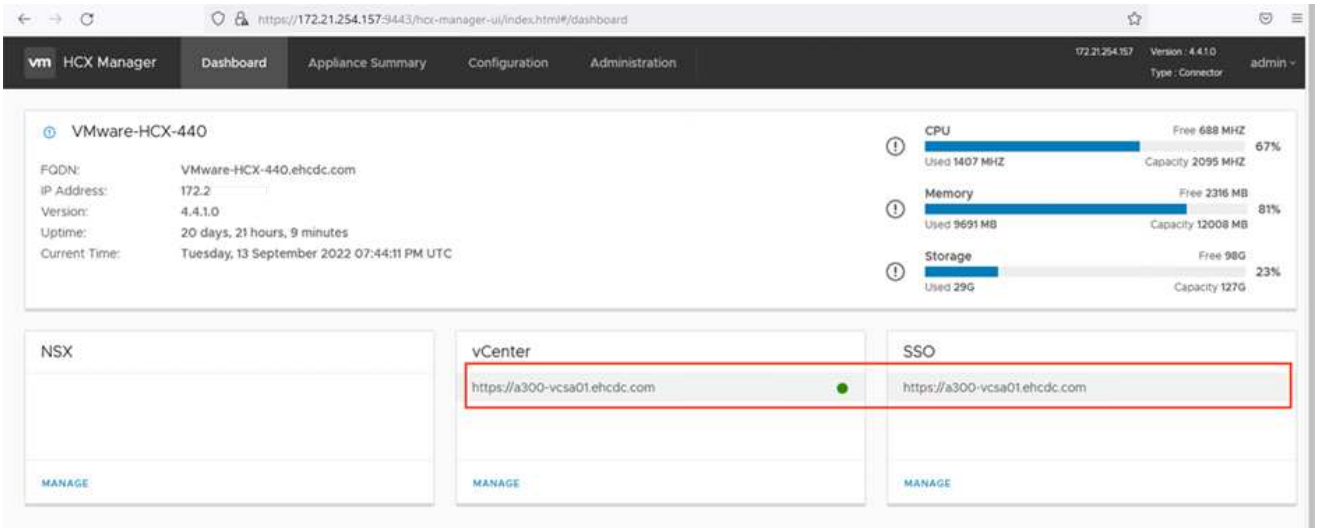
> Verwenden Sie den FQDN, um später Kommunikationsprobleme zu vermeiden.

9. Geben Sie unter SSO/PSC konfigurieren den FQDN oder die IP-Adresse des Plattform-Services-Controllers an, und klicken Sie auf Weiter.

Geben Sie die IP-Adresse oder den FQDN des vCenter-Servers ein.

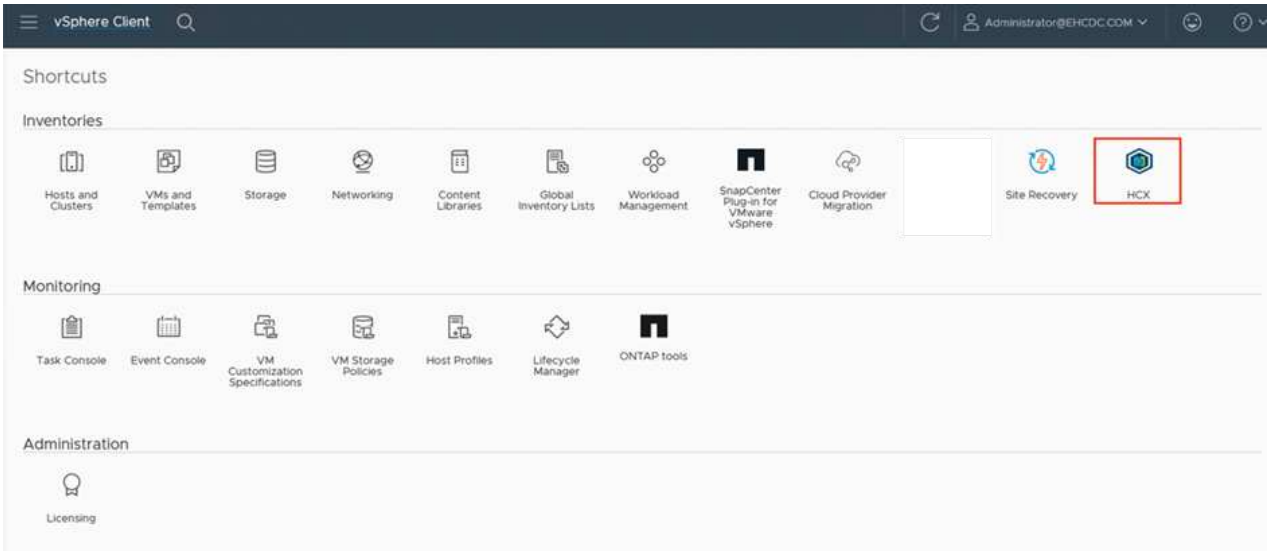
10. Überprüfen Sie, ob die Informationen korrekt eingegeben wurden, und klicken Sie auf Neu starten.
11. Nach Abschluss wird der vCenter-Server grün angezeigt. Sowohl der vCenter-Server als auch das SSO müssen über die richtigen Konfigurationsparameter verfügen, die mit der vorherigen Seite identisch sein sollten.

Dieser Vorgang dauert etwa 10 bis 20 Minuten, und das Plug-in wird dem vCenter Server hinzugefügt.

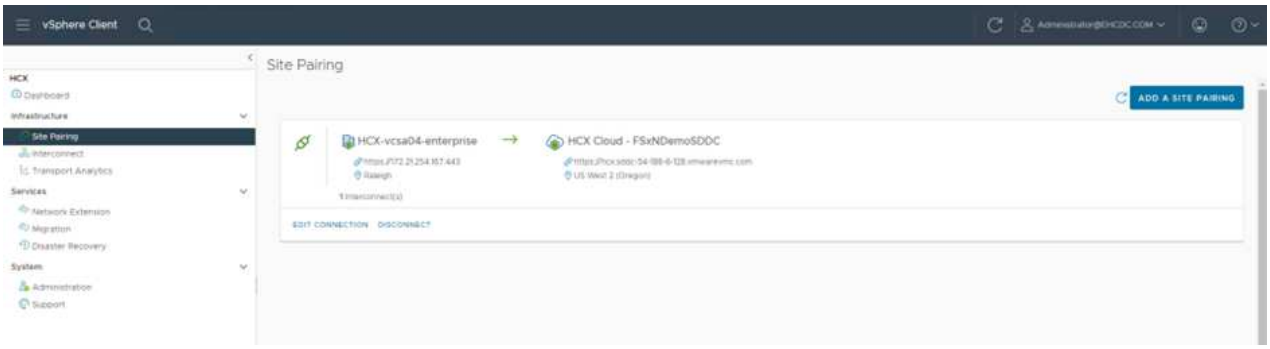


Schritt 4: Koppeln Sie den VMware HCX Connector vor Ort mit VMC HCX Cloud Manager

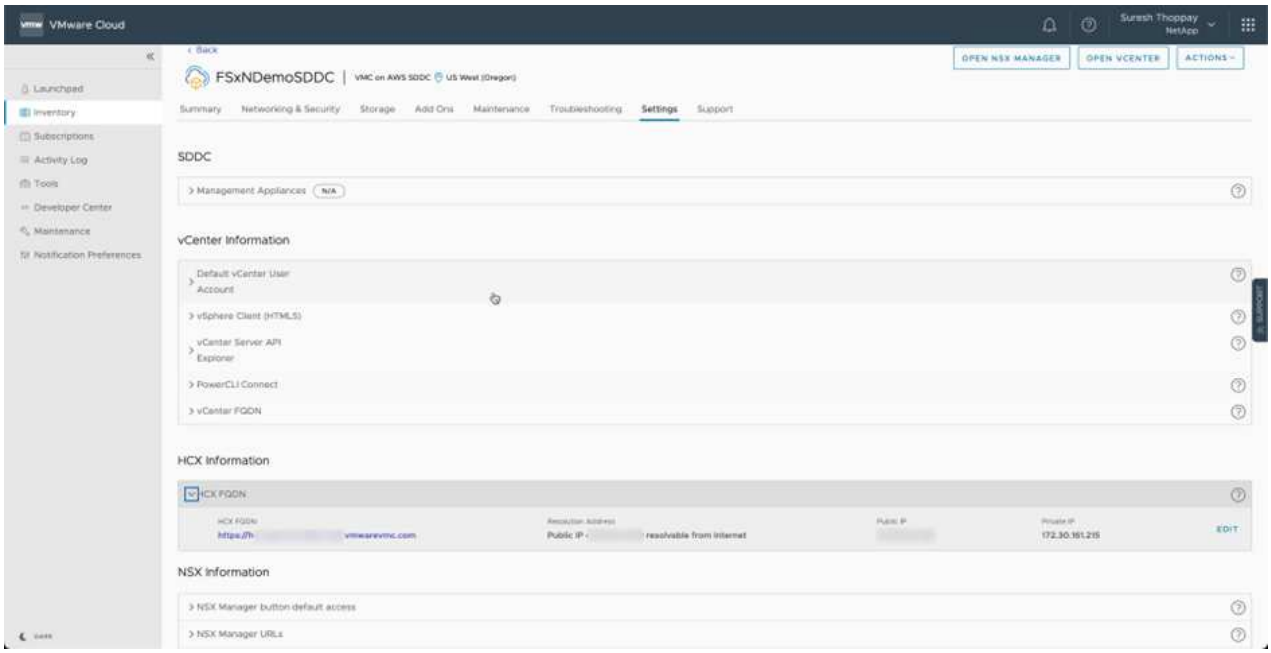
1. Um ein Standortpaar zwischen dem lokalen vCenter Server und dem VMC SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das HCX vSphere Web Client Plug-in zu.

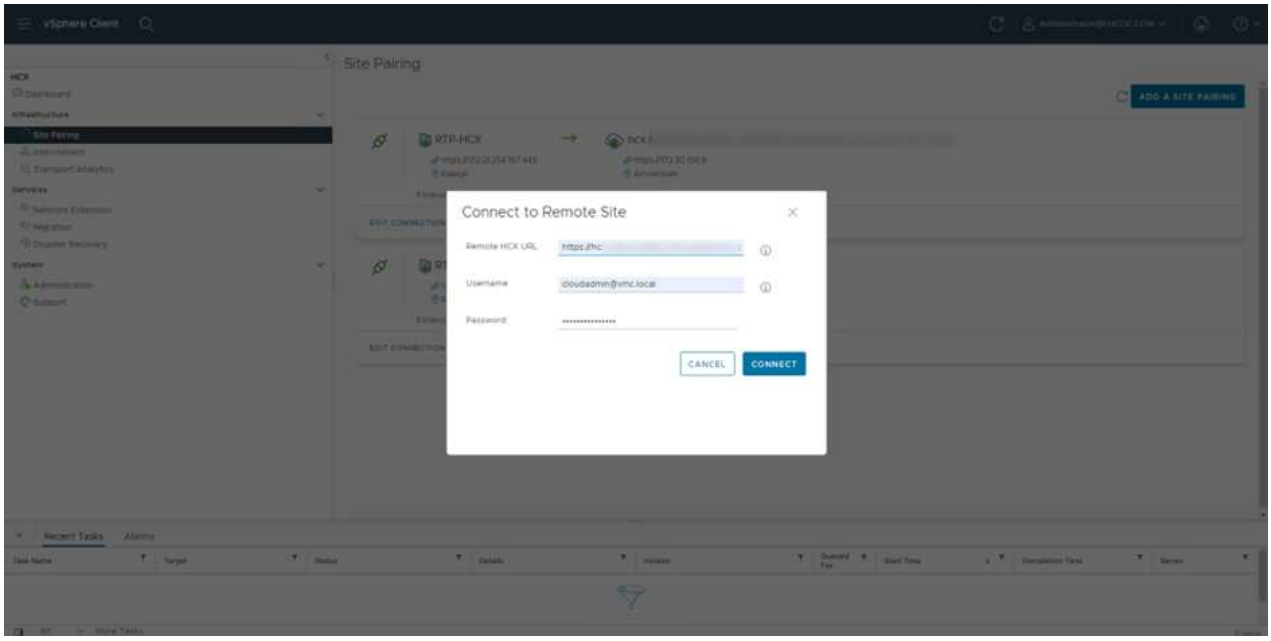


2. Klicken Sie unter Infrastruktur auf Site Pairing hinzufügen. Geben Sie zur Authentifizierung des Remote-Standorts die URL oder IP-Adresse des VMC HCX Cloud Manager und die Anmeldeinformationen für die CloudAdmin-Rolle ein.



HCX-Informationen sind auf der Seite SDDC-Einstellungen abrufbar.





3. Klicken Sie auf Verbinden, um die Standortpaarung zu starten.

> VMware HCX Connector muss in der Lage sein, über Port 443 mit der HCX Cloud Manager IP zu kommunizieren.

4. Nach der Erstellung der Kopplung steht die neu konfigurierte Standortpairing auf dem HCX Dashboard zur Verfügung.

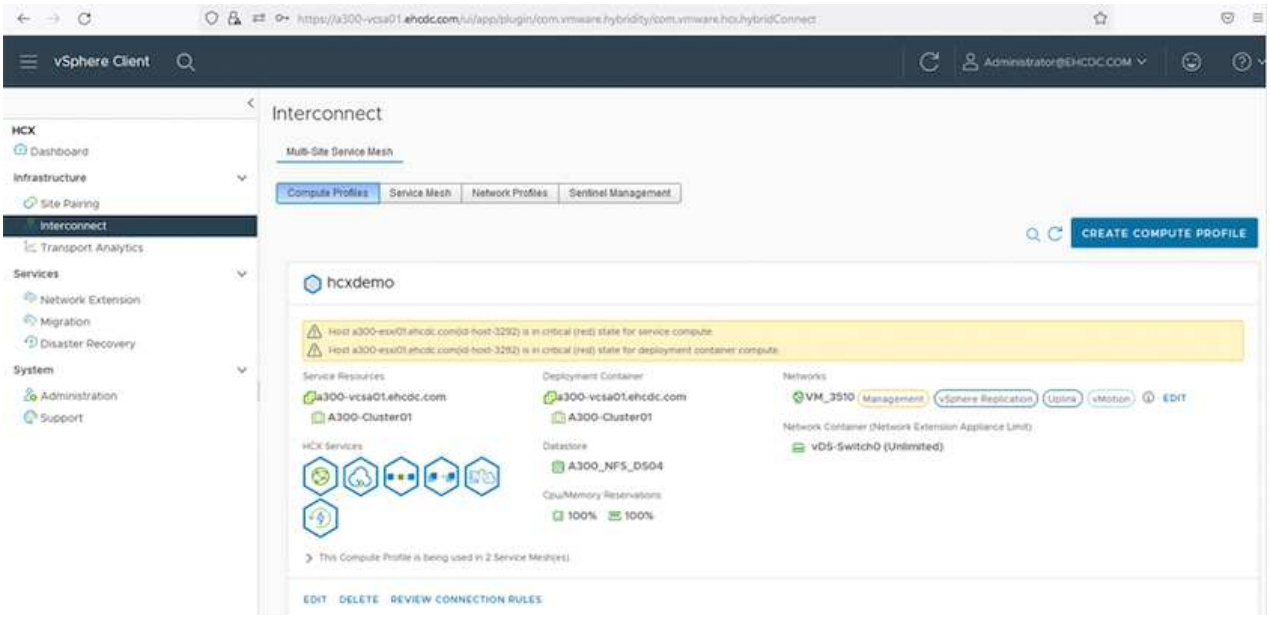
Schritt 5: Netzwerkprofil, Computing-Profil und Service-Mesh konfigurieren

Die VMware HCX Interconnect (HCX-IX) Appliance bietet sichere Tunnelfunktionen über das Internet und private Verbindungen zum Zielstandort, die Replizierung und vMotion-basierte Funktionen ermöglichen. Das Interconnect bietet Verschlüsselung, Traffic Engineering und SD-WAN. Um die HCI-IX Interconnect Appliance zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie unter Infrastruktur die Option Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile.

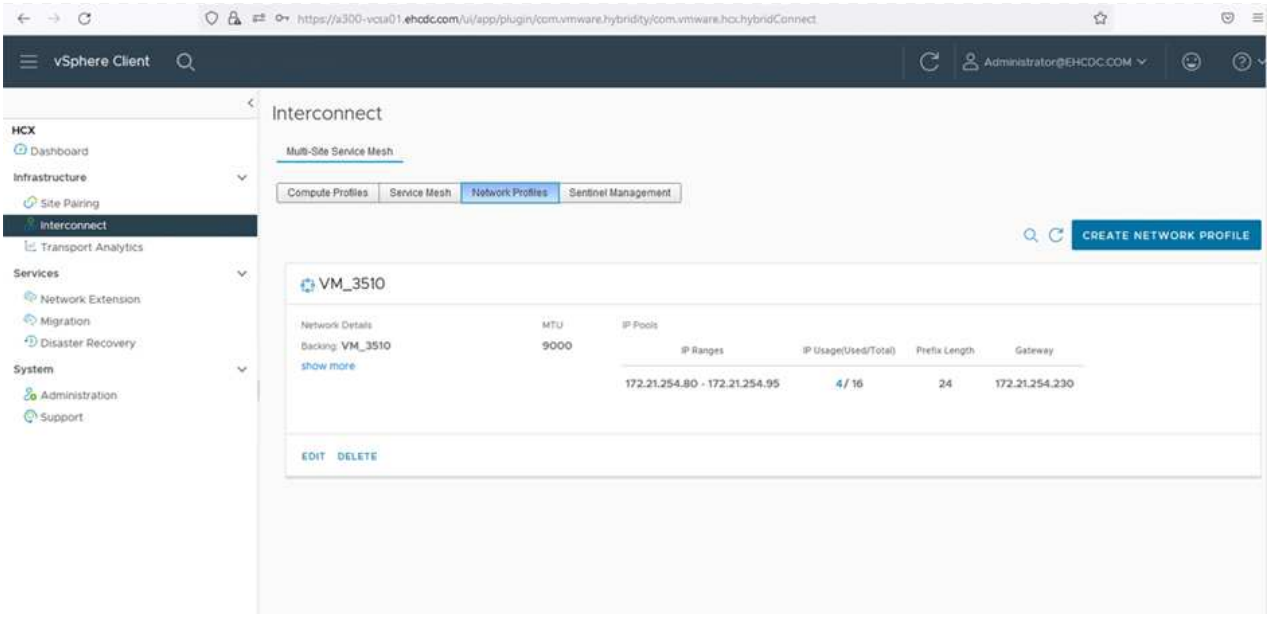
> Computing-Profile beinhalten die Parameter für die Computing-, Storage- und Netzwerkimplementierung, die für die Implementierung einer virtuellen Interconnect Appliance erforderlich sind. Außerdem wird angegeben, welcher Teil des VMware Datacenters für den HCX-Service verfügbar sein soll.

Ausführliche Anweisungen finden Sie unter "Erstellen eines Computing-Profils".



2. Erstellen Sie nach dem Erstellen des Rechenprofils das Netzwerkprofil, indem Sie Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen auswählen.
3. Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

> Dafür benötigen Sie mindestens zwei IP-Adressen. Diese IP-Adressen werden virtuellen Appliances vom Managementnetzwerk zugewiesen.

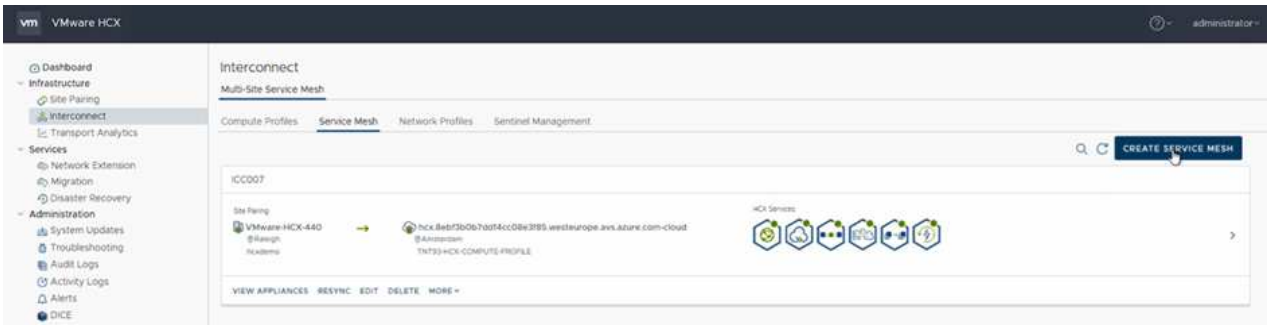


Ausführliche Anweisungen finden Sie unter "Erstellen eines Netzwerkprofils".

Wenn Sie eine Verbindung mit einem SD-WAN über das Internet herstellen, müssen Sie öffentliche IPs im Abschnitt Netzwerk und Sicherheit reservieren.

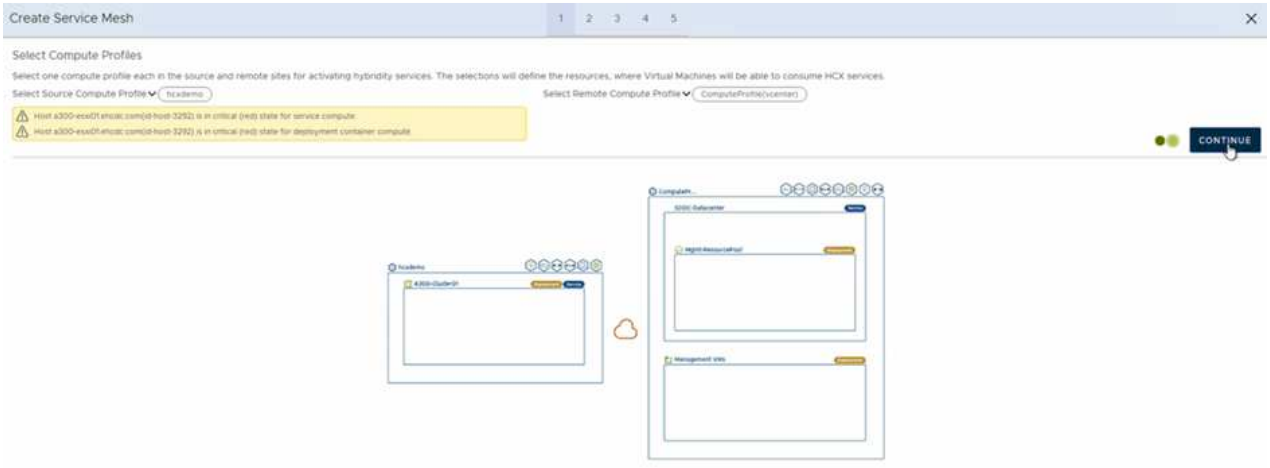
4. Um ein Service-Mesh zu erstellen, wählen Sie in der Option Interconnect die Registerkarte Service Mesh aus, und wählen Sie On-Premises- und VMC SDDC-Standorte aus.

   Das Service-Netz stellt ein lokales und entferntes Compute- und Netzwerkprofil-Paar bereit.

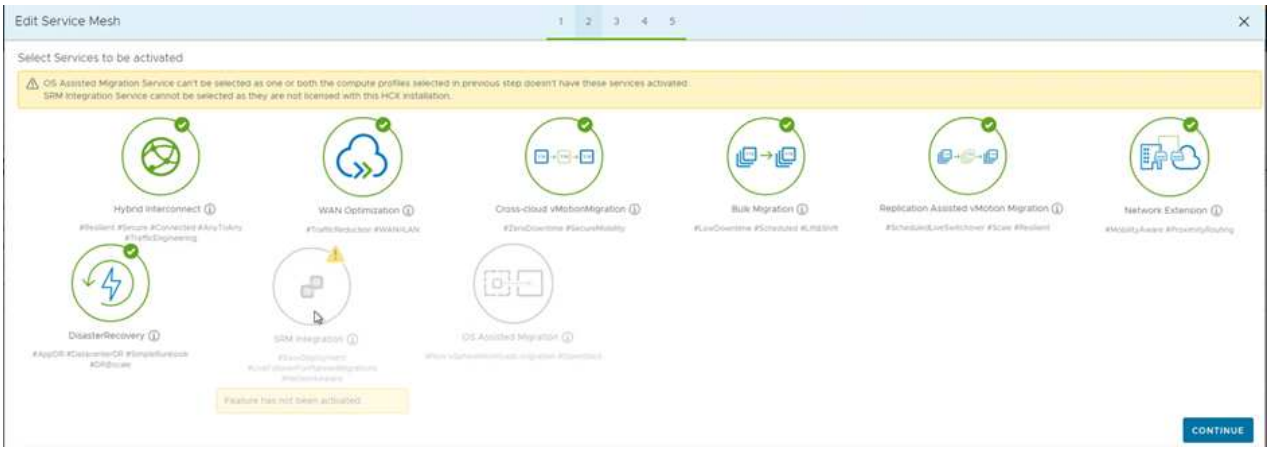


Bei diesem Prozess werden HCX-Appliances bereitgestellt, die automatisch am Quell- und Zielspeicherort konfiguriert werden und so eine sichere Transportstruktur erstellen.

5. Wählen Sie die Quell- und Remote-Computing-Profile aus, und klicken Sie auf Weiter.

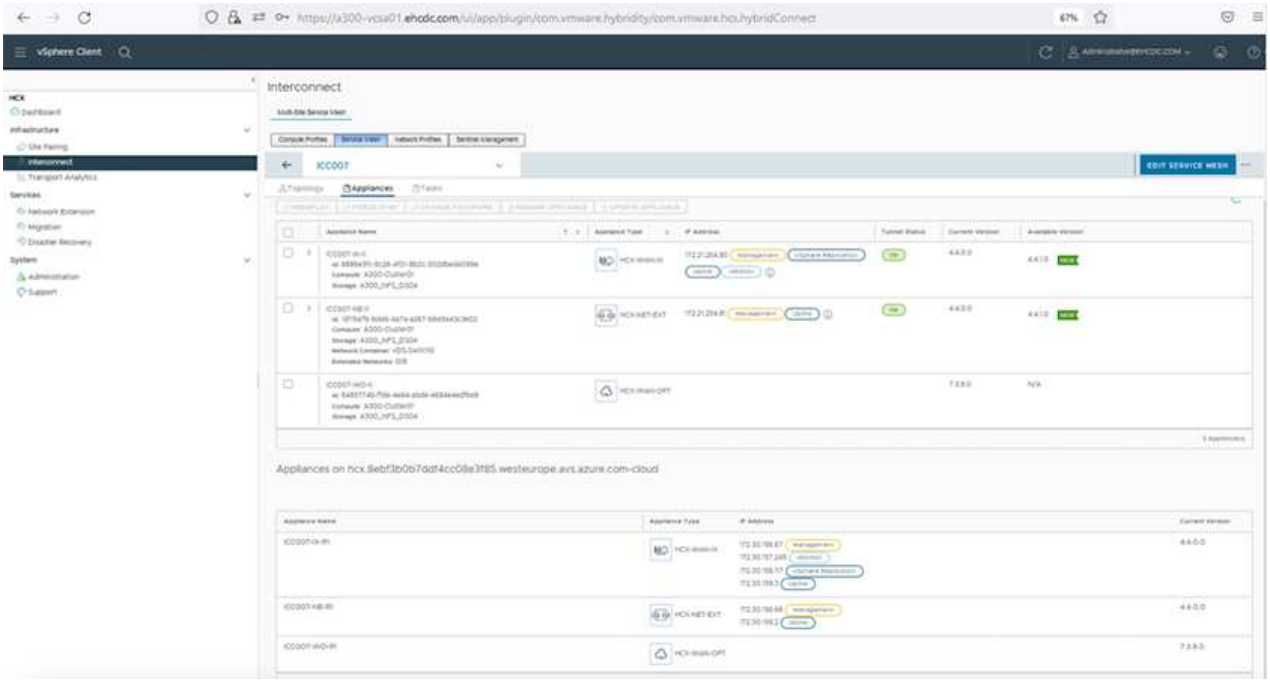


6. Wählen Sie den Dienst aus, der aktiviert werden soll, und klicken Sie auf Weiter.



Für die Replication Assisted vMotion Migration, die SRM-Integration und die BS-gestützte Migration ist eine HCX Enterprise-Lizenz erforderlich.

7. Erstellen Sie einen Namen für das Service-Mesh, und klicken Sie auf Fertig stellen, um den Erstellungsvorgang zu starten. Die Implementierung dauert etwa 30 Minuten. Nach der Konfiguration des Service-Mesh wurden die virtuelle Infrastruktur und die für die Migration der Virtual Machines erforderlichen Netzwerke erstellt.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

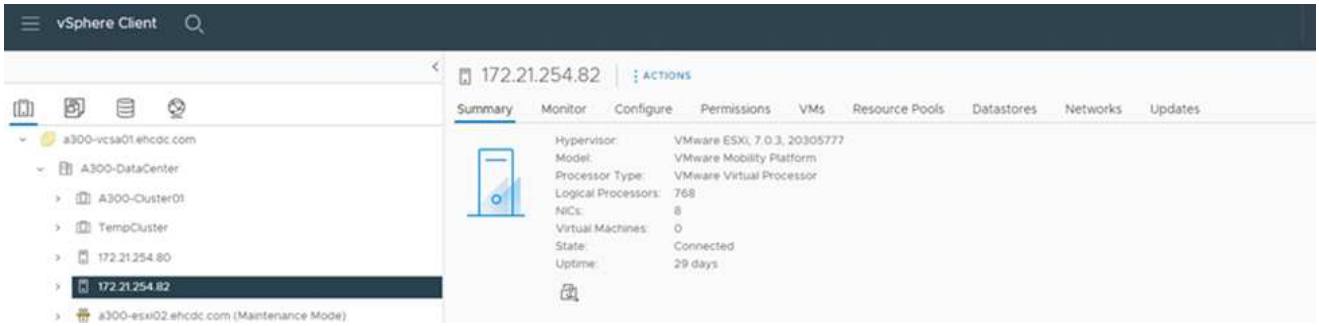
Schritt 6: Migration Von Workloads

HCX bietet bidirektionale Migrationsservices zwischen zwei oder mehr Umgebungen, beispielsweise On-Premises- und VMC SDDCs. Applikations-Workloads können mithilfe verschiedener Migrationstechnologien wie HCX Bulk Migration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (erhältlich mit HCX Enterprise Edition) und HCX OS Assisted Migration (erhältlich mit HCX Enterprise Edition) zu und von aktivierten Standorten migriert werden (mit HCX Enterprise Edition erhältlich).

Weitere Informationen über verfügbare HCX-Migrationstechnologien finden Sie unter "Migrationstypen von VMware HCX"

Die HCX-IX Appliance verwendet den Mobility Agent Service, um vMotion-, Cold- und Replication Assisted vMotion-Migrationen (RAV) durchzuführen.

> Die HCX-IX Appliance fügt den Mobility Agent-Service als Hostobjekt im vCenter Server hinzu. Der auf diesem Objekt angezeigte Prozessor, Arbeitsspeicher, Speicher und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch des physischen Hypervisors dar, der die IX-Appliance hostet.

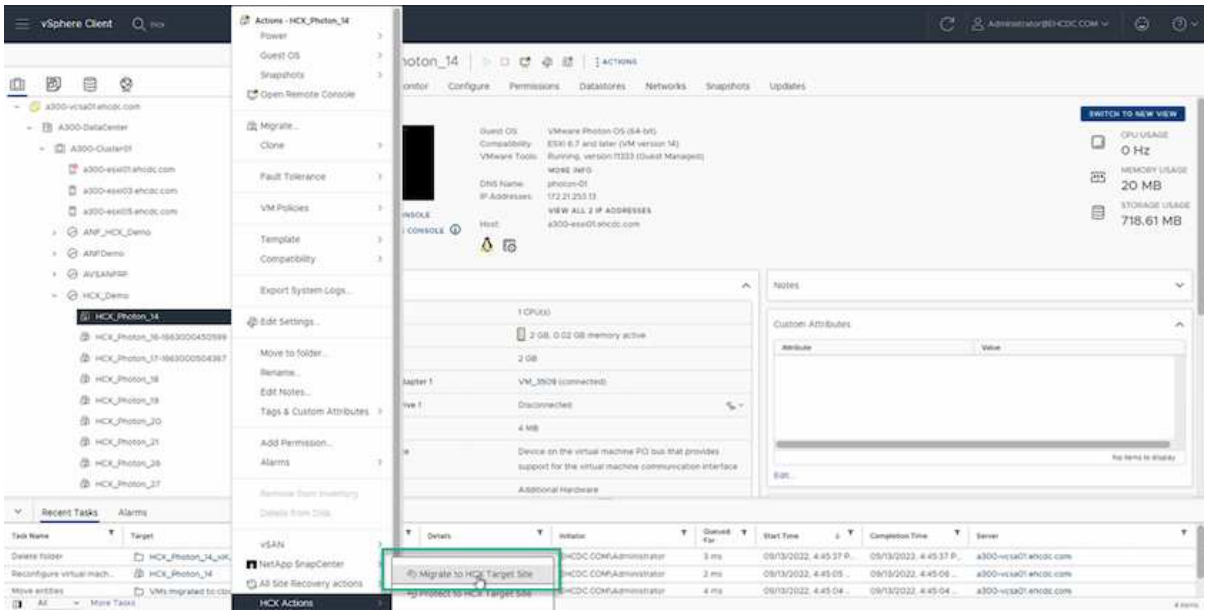


VMware HCX vMotion

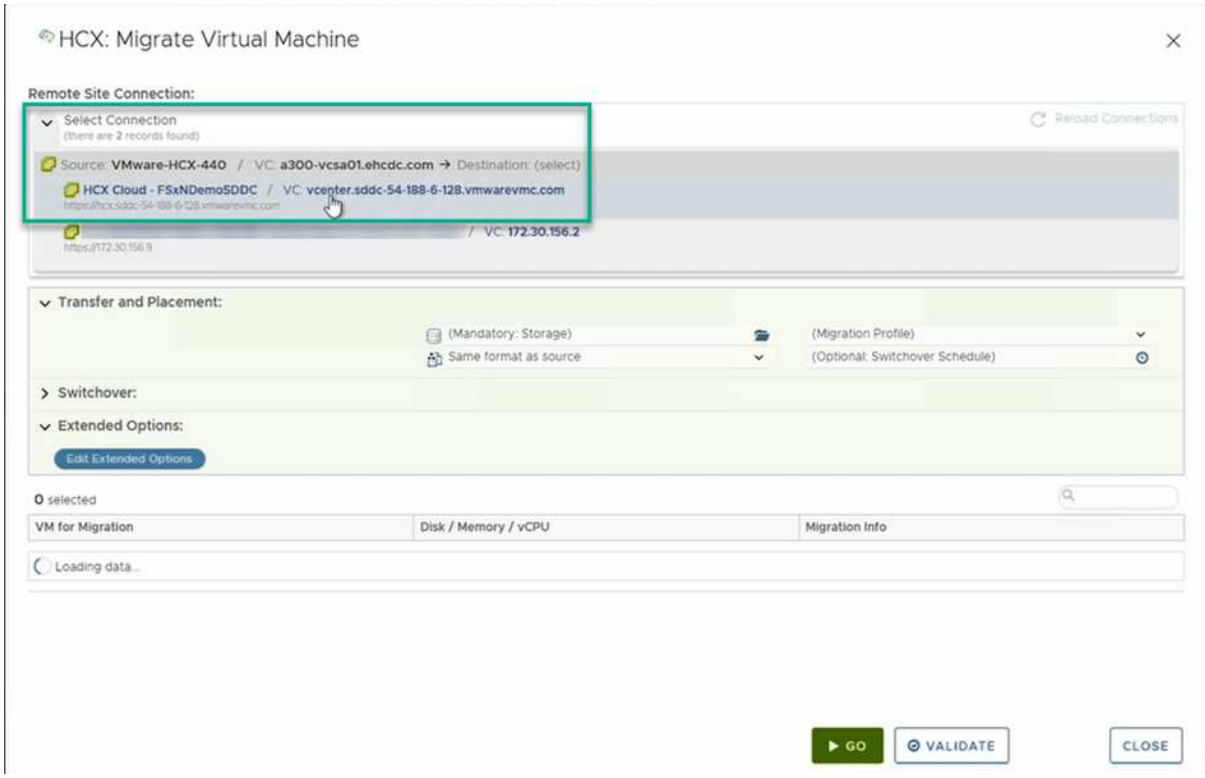
In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie nutzt das VMware vMotion Protokoll für die Migration einer VM zu VMC SDDC. Die vMotion Migrationsoption wird verwendet, um den VM-Status einer einzelnen VM gleichzeitig zu migrieren. Während dieser Migrationsmethode kommt es zu keiner Serviceunterbrechung.

> Eine Netzwerkerweiterung sollte vorhanden sein (für die Portgruppe, an der die VM angeschlossen ist), um die VM zu migrieren, ohne dass eine IP-Adressänderung notwendig ist.

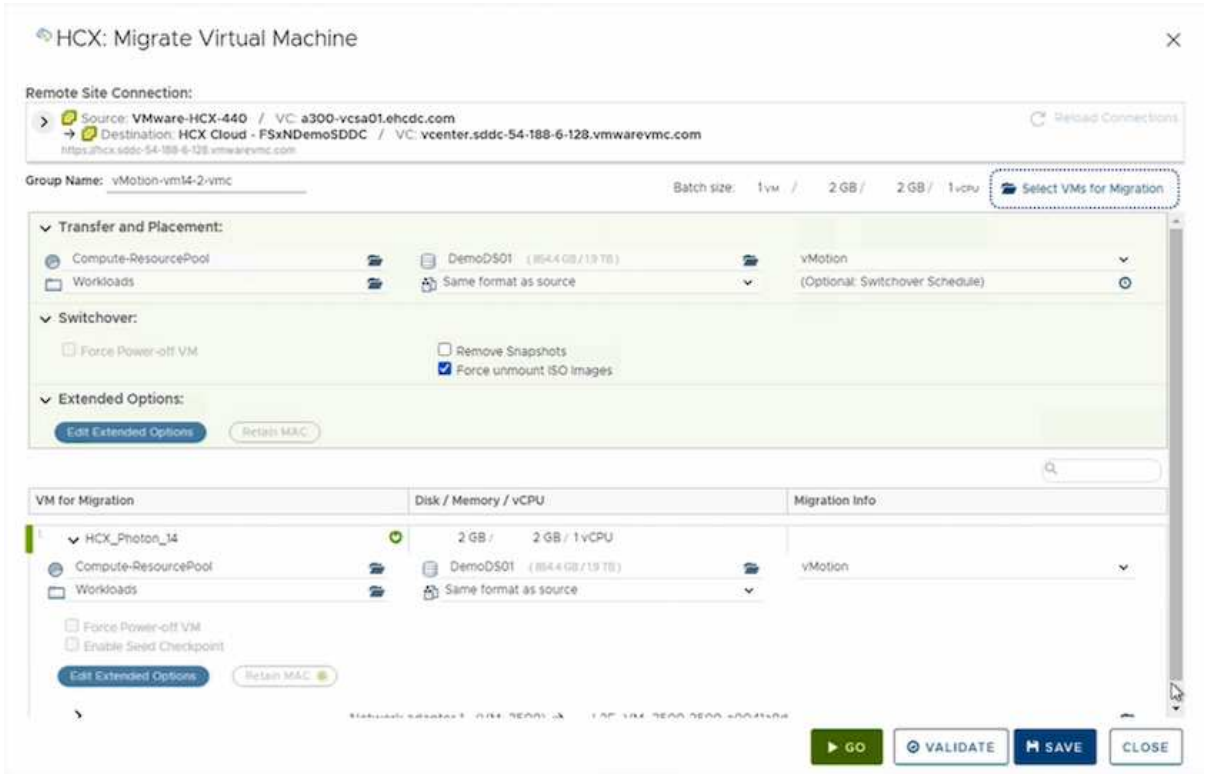
1. Wechseln Sie vom lokalen vSphere-Client zum Inventory, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie HCX Actions > Migrate to HCX Target Site aus.



2. Wählen Sie im Assistenten für die Migration von Virtual Machines die Remote-Standortverbindung (Ziel-VMC SDDC) aus.



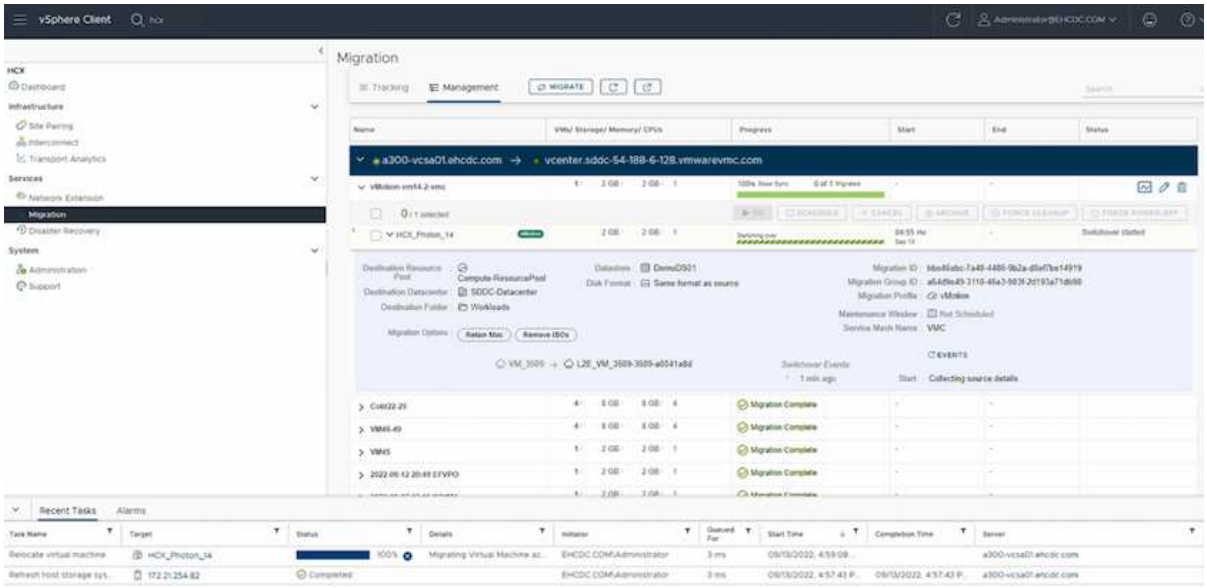
3. Fügen Sie einen Gruppennamen hinzu und aktualisieren Sie unter Übertragen und Platzierung die Pflichtfelder (Cluster, Storage und Zielnetzwerk), und klicken Sie auf Validieren.



4. Klicken Sie nach Abschluss der Validierungsprüfungen auf Los, um die Migration zu starten.

Der vMotion Transfer erfasst den aktiven VM-Speicher, seinen Ausführungszustand, seine IP-Adresse und seine MAC-Adresse. Weitere Informationen zu den Anforderungen und Einschränkungen von HCX vMotion finden Sie unter "VMware HCX vMotion und „Cold Migration“ verstehen".

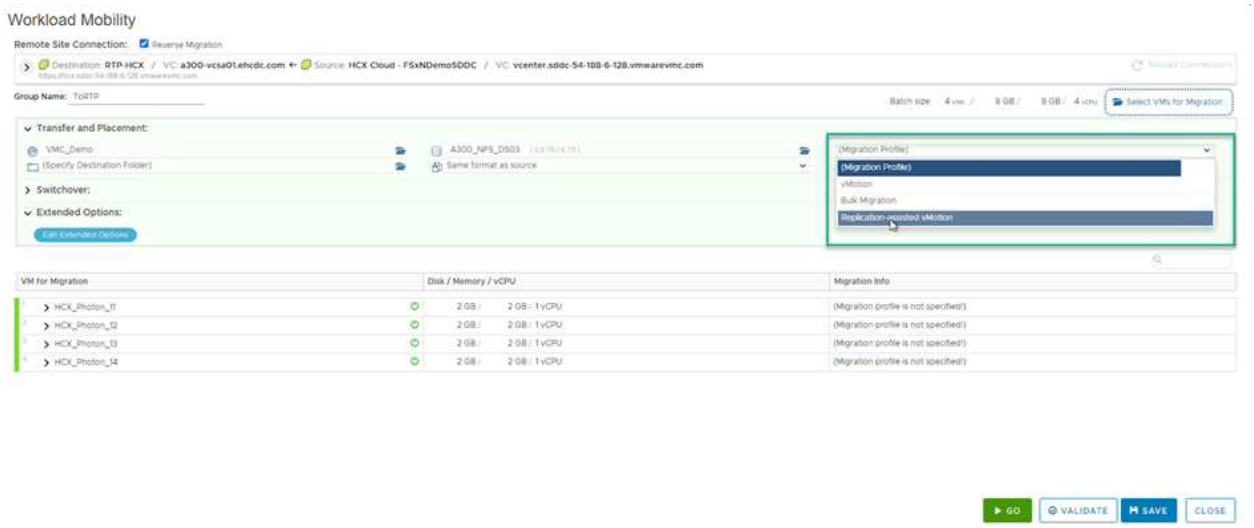
5. Über das Dashboard HCX > Migration können Sie den Fortschritt und den Abschluss von vMotion überwachen.



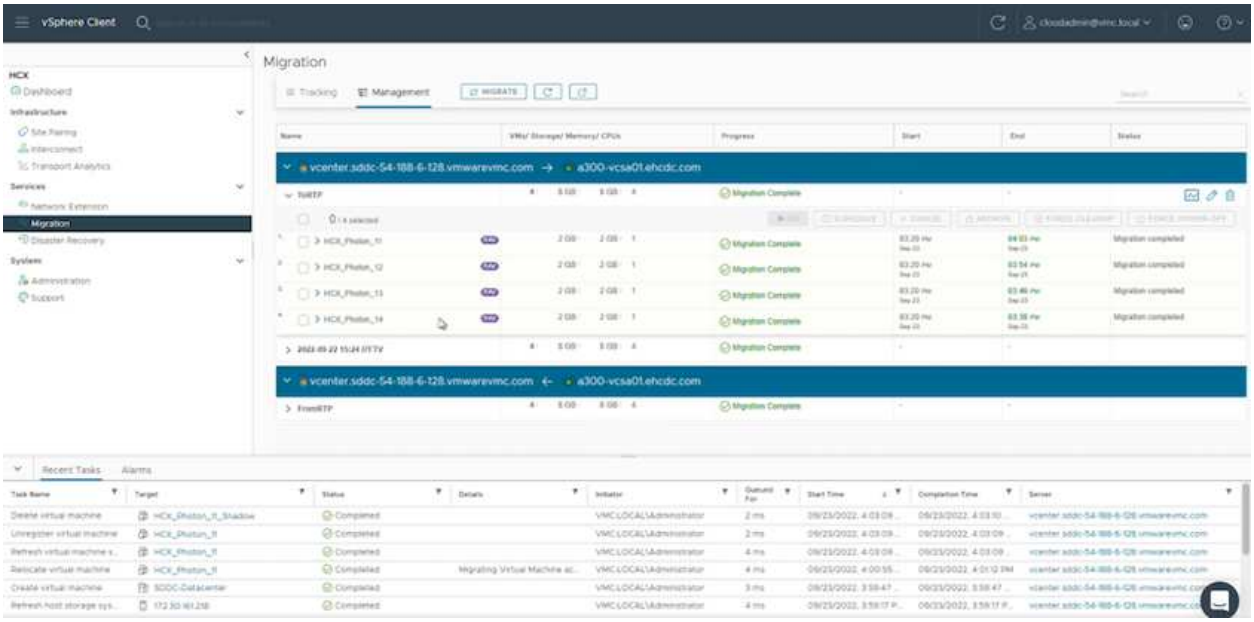
VMotion wird mithilfe von VMware Replizierung unterstützt

Wie Sie in der VMware Dokumentation möglicherweise schon bemerkt haben, vereint VMware HCX Replication Assisted vMotion (RAV) die Vorteile der Massenmigration mit vMotion. Bei der Massenmigration wird mit vSphere Replication mehrere VMs parallel migriert – die VM wird während der Umschaltung neu gestartet. HCX vMotion migriert ohne Ausfallzeiten, wird aber seriell eine VM nacheinander in einer Replizierungsgruppe ausgeführt. RAV repliziert die VM parallel und hält sie bis zum Switchover-Fenster synchron. Während des Switchover migriert sie eine VM nach dem anderen, ohne Ausfallzeiten für die VM.

Im folgenden Screenshot wird das Migrationsprofil als Replication Assisted vMotion angezeigt.



Die Dauer der Replizierung kann gegenüber vMotion einer kleinen Anzahl von VMs länger dauern. Mit RAV synchronisieren Sie nur die Deltas und beinhalten den Speicherinhalt. Nachfolgend sehen Sie einen Screenshot des Migrationsstatus: Hier wird die Startzeit der Migration angegeben, und die Endzeit ist unterschiedlich für jede VM.



Weitere Informationen zu den HCX-Migrationsoptionen und zur Migration von Workloads von On-

Premises zu VMware Cloud on AWS mit HCX finden Sie im "VMware HCX-Benutzerhandbuch".

VMware HCX vMotion erfordert eine Durchsatzfunktion von 100 MB/s oder mehr.

Die FSX für das Ziel-VMC für ONTAP-Datenspeicher muss über ausreichend Speicherplatz für die Migration verfügen.

Schlussfolgerung

Ganz gleich, ob Sie nur auf All-Cloud- oder Hybrid Cloud-Umgebungen abzielen und Daten in On-Premises-Storage eines beliebigen Typs oder Anbieters speichern: Amazon FSX für NetApp ONTAP bietet in Kombination mit HCX hervorragende Optionen für Implementierung und Migration der Workloads, während Sie gleichzeitig die TCO senken, indem die Datenanforderungen nahtlos auf die Applikationsebene reduziert werden. Unabhängig vom Anwendungsfall entscheiden Sie sich für VMC und FSX für ONTAP Datastore, um schnell von den Vorteilen der Cloud zu profitieren. Sie profitieren von konsistenter Infrastruktur und On-Premises- und diversen Clouds, bidirektionaler Portabilität von Workloads sowie Kapazität und Performance der Enterprise-Klasse. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, die zum Verbinden des Storage und zur Migration von VMs mithilfe der VMware vSphere Replizierung, VMware vMotion oder sogar einer NFC-Kopie verwendet werden.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können nun Amazon FSX ONTAP als Datastore mit VMC SDDC nutzen.
- Daten lassen sich problemlos von lokalen Datacentern zu VMC migrieren, die mit FSX für ONTAP Datastores ausgeführt werden
- Erweitern und reduzieren Sie den FSX ONTAP Datastore ganz einfach, um die Kapazitäts- und Performance-Anforderungen während der Migration zu erfüllen.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie unter den folgenden Links:

- Dokumentation zu VMware Cloud

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Dokumentation zu Amazon FSX für NetApp ONTAP

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX-Benutzerhandbuch

- "https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Regionale Verfügbarkeit – ergänzender NFS-Datenspeicher für VMC

Die Verfügbarkeit von zusätzlichen NFS-Datenspeichern auf AWS/VMC wird durch Amazon festgelegt. Zunächst müssen Sie feststellen, ob VMC und FSxN in einer

bestimmten Region verfügbar sind. Als Nächstes müssen Sie feststellen, ob der FSxN zusätzliche NFS-Datastore in dieser Region unterstützt wird.

- Überprüfen Sie die Verfügbarkeit von VMC "Hier".
- Der Amazon Preisleitfaden enthält Informationen dazu, wo FSxN (FSX ONTAP) verfügbar ist. Diese Informationen finden Sie hier "Hier".
- Der zusätzlich zu NFS Datastore für VMC verfügbare FSxN wird demnächst verfügbar sein.

Obwohl noch Informationen freigegeben werden, zeigt das folgende Diagramm die aktuelle Unterstützung für VMC, FSxN und FSxN als zusätzliche NFS-Datenspeicher.

Nord- Und Südamerika

AWS Region	VMC Verfügbarkeit	FSX ONTAP Verfügbarkeit	Verfügbarkeit von NFS-Datenspeichern
US East (Northern Virginia)	Ja.	Ja.	Ja.
US-Osten (Ohio)	Ja.	Ja.	Ja.
USA West (Nordkalifornien)	Ja.	Nein	Nein
US West (Oregon)	Ja.	Ja.	Ja.
GovCloud (USA – Westen)	Ja.	Ja.	Ja.
Kanada (Zentral)	Ja.	Ja.	Ja.
Südamerika (Sao Paulo)	Ja.	Ja.	Ja.

Zuletzt aktualisiert am: 2. Juni 2022.

EMEA

AWS Region	VMC Verfügbarkeit	FSX ONTAP Verfügbarkeit	Verfügbarkeit von NFS-Datenspeichern
Europa (Irland)	Ja.	Ja.	Ja.
Europa (London)	Ja.	Ja.	Ja.
Europa (Frankfurt)	Ja.	Ja.	Ja.
Europa (Paris)	Ja.	Ja.	Ja.
Europa (Mailand)	Ja.	Ja.	Ja.
Europa (Stockholm)	Ja.	Ja.	Ja.

Zuletzt aktualisiert am: 2. Juni 2022.

Asien/Pazifik

AWS Region	VMC Verfügbarkeit	FSX ONTAP Verfügbarkeit	Verfügbarkeit von NFS-Datenspeichern
Asien/Pazifik (Sydney)	Ja.	Ja.	Ja.
Asien/Pazifik (Tokio)	Ja.	Ja.	Ja.
Asien/Pazifik (Osaka)	Ja.	Nein	Nein
Asien/Pazifik (Singapur)	Ja.	Ja.	Ja.
Asien/Pazifik (Seoul)	Ja.	Ja.	Ja.
Asien/Pazifik (Mumbai)	Ja.	Ja.	Ja.
Asien/Pazifik (Jakarta)	Nein	Nein	Nein
Asien/Pazifik (Hongkong)	Ja.	Ja.	Ja.

Zuletzt aktualisiert am: 28. September 2022.

NetApp Funktionen für Azure AVS

Erfahren Sie mehr über die Funktionen, die NetApp in die Azure VMware Lösung (AVS) bietet: Von NetApp als Storage-Gerät mit Anbindung an den Gast oder über einen zusätzlichen NFS Datastore für die Migration von Workflows, über Erweiterung/Bursting in die Cloud, Backup/Wiederherstellung und Disaster Recovery.

Springen Sie zum Abschnitt zum gewünschten Inhalt, indem Sie eine der folgenden Optionen auswählen:

- "AVS wird in Azure konfiguriert"
- "NetApp Storage-Optionen für AVS"
- "NetApp/VMware Cloud-Lösungen"

AVS wird in Azure konfiguriert

Wie bei lokalen Systemen ist die Planung einer Cloud-basierten Virtualisierungsumgebung eine entscheidende Voraussetzung für eine erfolgreiche, sofort einsatzbereite Umgebung zum Erstellen von VMs und Migrationen.

In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Lösung einrichten und managen und in Kombination mit den verfügbaren Optionen für die Verbindung von NetApp Storage verwenden.

Der in-Guest-Speicher ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit Azure VMware-Lösung.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Registrieren Sie den Ressourcenanbieter und erstellen Sie eine Private Cloud
- Stellen Sie eine Verbindung zu einem neuen oder vorhandenen virtuellen ExpressRoute Netzwerk-Gateway her
- Netzwerkverbindung validieren und auf Private Cloud zugreifen

Details anzeigen "Konfigurationsschritte für AVS".

NetApp Storage-Optionen für AVS

NetApp Storage kann innerhalb von Azure AVS auf verschiedene Arten genutzt werden – entweder als angebundenen oder als zusätzlicher NFS-Datenspeicher.

Besuchen Sie "Unterstützte NetApp Storage-Optionen" Finden Sie weitere Informationen.

Azure unterstützt NetApp Storage in den folgenden Konfigurationen:

- Azure NetApp Files (ANF) als Storage mit Gastverbunden
- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- Azure NetApp Files (ANF) als zusätzlicher NFS-Datastore

Details anzeigen "Gastanbindung Speicheroptionen für AVS". Details anzeigen "Zusätzliche NFS-Datastore-Optionen für AVS".

Anwendungsfälle Für Lösungen

Mit Cloud-Lösungen von NetApp und VMware können viele Anwendungsfälle problemlos in Azure AVS implementiert werden. se-Fälle werden für jeden der von VMware definierten Cloud-Bereiche definiert:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Erweitern
- Migrieren

"Die NetApp Lösungen für Azure AVS"

Schutz von Workloads auf Azure/AVS

Disaster Recovery mit ANF und JetStream

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz der Workloads vor Standortausfällen und Datenbeschädigungen (z. B. Ransomware). Mithilfe des VMware VAIO Frameworks können VMware On-Premises-Workloads auf Azure Blob Storage und für die Recovery repliziert werden, was zu minimalen oder fast keinem Datenverlust und nahezu keinem RTO führt.

Jetstream DR kann verwendet werden, um die Workloads, die von On-Premises-Systemen auf AVS repliziert wurden, nahtlos wiederherzustellen. Insbesondere können sie auf Azure NetApp Files übertragen werden. Sie ermöglicht eine kostengünstige Disaster Recovery, da minimale Ressourcen am DR-Standort und kostengünstiger Cloud Storage genutzt werden. Jetstream DR automatisiert die Recovery auf ANF-Datastores über Azure Blob Storage. Jetstream DR stellt unabhängige VMs oder Gruppen zugehöriger VMs in der Infrastruktur des Recovery-Standorts entsprechend der Netzwerkzuordnung wieder her und sorgt für zeitpunktgenaue Recovery zur Sicherung von Ransomware.

Dieses Dokument vermittelt ein Verständnis der JetStream DR-Prinzipien des Betriebs und seiner Hauptkomponenten.

Übersicht über die Lösungsimplementierung

1. Installation der JetStream DR-Software im lokalen Datacenter
   a. Laden Sie das JetStream DR-Software-Bundle aus Azure Marketplace (ZIP) herunter, und implementieren Sie das JetStream DR MSA (OVA) im dafür vorgesehenen Cluster.
   b. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket (JetStream VIB installieren).
   c. Bereitstellen von Azure Blob (Azure Storage-Konto) in derselben Region wie das DR-AVS-Cluster
   d. Implementierung von DRVA-Appliances und Zuweisung von Protokoll-Volumes (VMDK aus vorhandenem Datastore oder gemeinsam genutztem iSCSI-Storage)
   e. Erstellen Sie geschützte Domänen (Gruppen zugehöriger VMs) und weisen Sie DRVAs und Azure Blob Storage/ANF zu.
   f. Schutz starten.
2. Installieren Sie die JetStream DR-Software in der Private Cloud der Azure VMware Lösung.
   a. Verwenden Sie den Befehl Ausführen, um JetStream DR zu installieren und zu konfigurieren.
   b. Fügen Sie denselben Azure Blob-Container hinzu und entdecken Sie Domänen mithilfe der Option „Scan Domains“.
   c. Bereitstellung der erforderlichen DRVA-Appliances
   d. Verwenden von verfügbaren vSAN oder ANF-Datastores für Replizierungsprotokolle erstellen
   e. Importieren Sie geschützte Domänen und konfigurieren Sie RocVA (Recovery VA), um einen ANF-Datenspeicher für VM-Platzierungen zu verwenden.
   f. Wählen Sie die entsprechende Failover-Option aus, und beginnen Sie mit der kontinuierlichen Wiederherstellung nach RTO-Domänen von nahezu null oder VMs.
3. Bei einem Notfall wird ein Failover zu Azure NetApp Files-Datastores am zugewiesenen AVS-DR-Standort ausgelöst.
4. Rufen Sie den geschützten Standort nach der Wiederherstellung des geschützten Standorts auf.bevor Sie beginnen, stellen Sie sicher, dass die Voraussetzungen wie in diesem angegeben erfüllt sind "Verlinken" Führen Sie außerdem das von JetStream Software zur Verfügung gestellte Bandwidth Testing Tool (BWT) aus, um die potenzielle Performance des Azure Blob Storage und dessen Replikationsbandbreite in Verbindung mit der JetStream DR-Software zu bewerten. Nachdem die Voraussetzungen, einschließlich Konnektivität, vorhanden sind, richten Sie JetStream DR für AVS von der ein und abonnieren Sie sie "Azure Marketplace". Nachdem das Software Bundle heruntergeladen wurde, fahren Sie mit dem oben beschriebenen Installationsvorgang fort.

Verwenden Sie beim Planen und Starten des Schutzes für eine große Anzahl von VMs (z. B. 100+) das Capacity Planning Tool (CPT) aus dem JetStream DR Automation Toolkit. Geben Sie eine Liste der VMs an, die zusammen mit ihren RTO- und Recovery-Gruppeneinstellungen geschützt werden sollen, und führen Sie dann das CPT aus.

CPT führt die folgenden Funktionen aus:

- Die Kombination von VMs in Sicherungsdomänen entsprechend ihrer RTO-Vorgaben.
- Die optimale Anzahl von DRVAs und deren Ressourcen festlegen.
- Schätzen der erforderlichen Replikationsbandbreite
- Ermittlung der Merkmale von Replikationsprotokollvolumes (Kapazität, Bandbreite usw.)

- Schätzung der erforderlichen Objekt-Storage-Kapazität und mehr

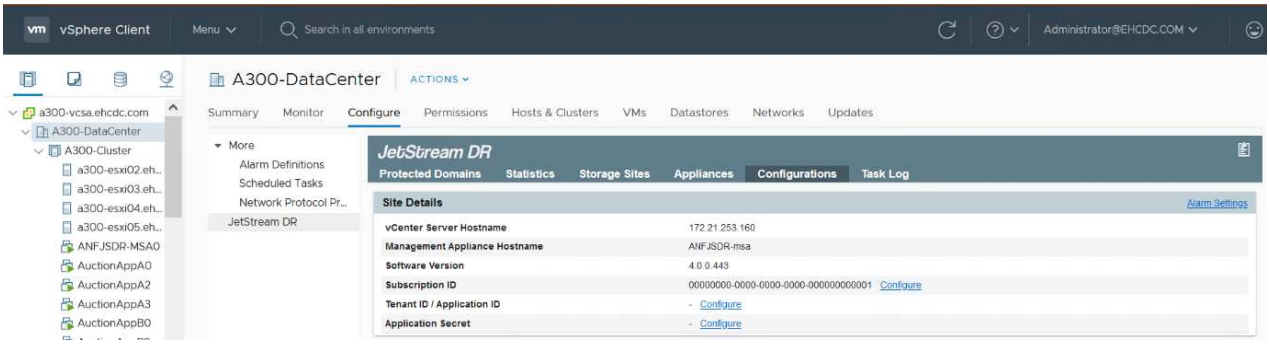
> Die Anzahl und der Inhalt der Domänen hängen von den verschiedenen VM-Merkmalen ab, wie beispielsweise durchschnittlichen IOPS, Gesamtkapazität, Priorität (die Failover-Reihenfolge definiert), RTO und anderen.

Installation der JetStream DR im lokalen Datacenter

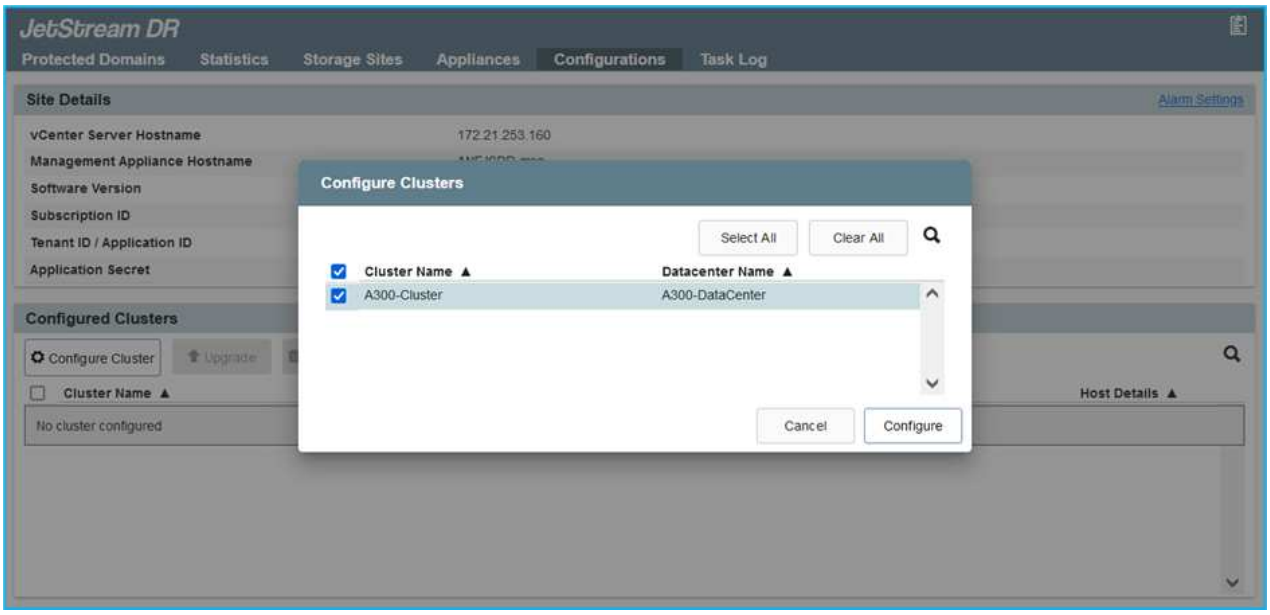
Die Jetstream DR-Software besteht aus drei Hauptkomponenten: Jetstream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) und Host-Komponenten (I/O-Filterpakete). MSA wird verwendet, um Hostkomponenten auf dem Computing-Cluster zu installieren und zu konfigurieren und anschließend JetStream DR-Software zu verwalten. Die folgende Liste enthält eine ausführliche Beschreibung des Installationsprozesses:

Installation von JetStream DR für On-Premises

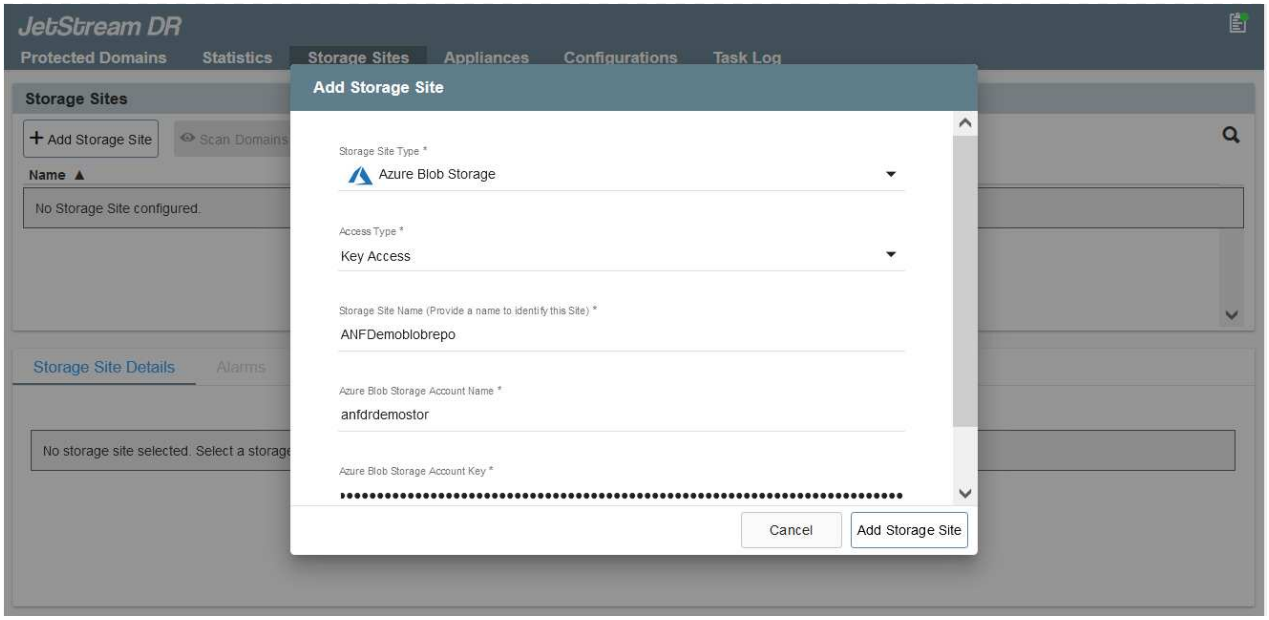
1. Voraussetzungen prüfen.
2. Führen Sie das Capacity Planning Tool für Ressourcen- und Konfigurationsempfehlungen aus (optional, jedoch für Proof-of-Concept-Tests empfohlen).
3. Implementieren Sie JetStream DR MSA auf einem vSphere-Host im zugewiesenen Cluster.
4. Starten Sie das MSA-Produkt mit dem DNS-Namen in einem Browser.
5. Registrieren Sie den vCenter-Server mit dem MSA.um die Installation durchzuführen, führen Sie die folgenden detaillierten Schritte aus:
6. Nachdem JetStream DR MSA implementiert und der vCenter Server registriert wurde, greifen Sie über den vSphere Web Client auf das JetStream DR Plug-in zu. Dazu können Sie im Datacenter > Configure > JetStream DR navigieren.



7. Wählen Sie über die JetStream DR-Schnittstelle den entsprechenden Cluster aus.



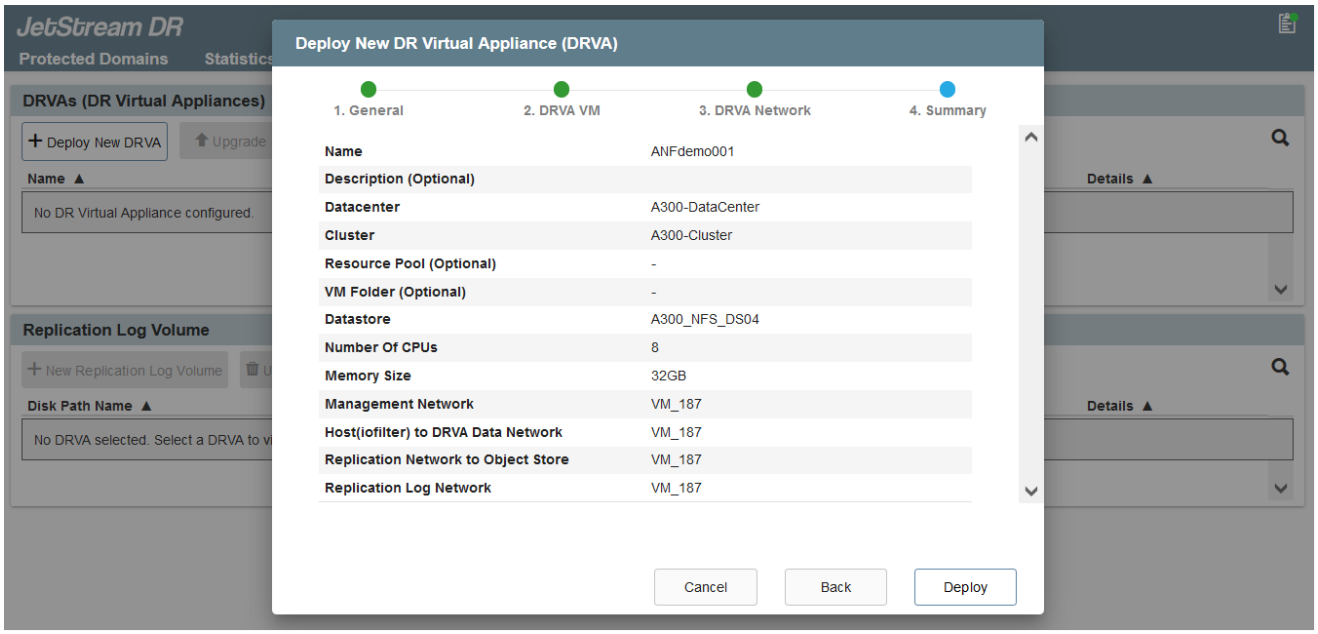
8. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket.



9. Fügen Sie Azure Blob Storage am Recovery-Standort hinzu.
10. Stellen Sie eine DR Virtual Appliance (DRVA) über die Registerkarte Appliances bereit.

> DRVAs können automatisch durch CPT erstellt werden. Für POC-Tests wird jedoch empfohlen, den DR-Zyklus manuell zu konfigurieren und auszuführen (Schutz starten > Failover > Failback).

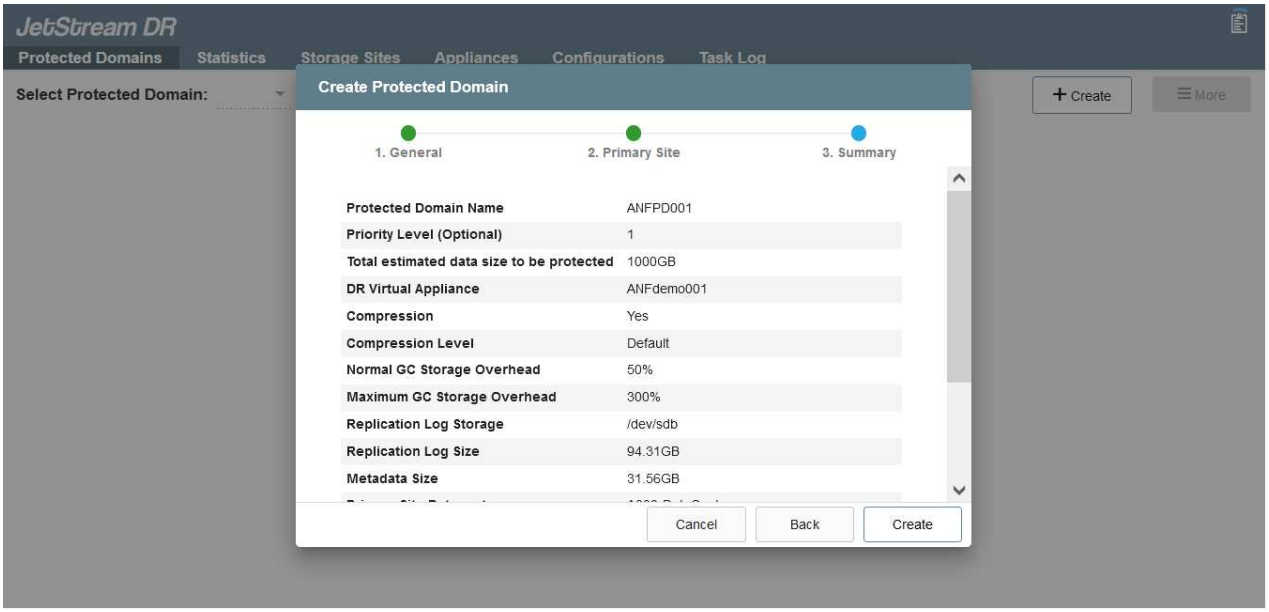
JetStream DRVA ist eine virtuelle Appliance, die wichtige Funktionen bei der Datenreplizierung unterstützt. Ein geschützter Cluster muss mindestens eine DRVA enthalten, und normalerweise ist pro Host ein DRVA konfiguriert. Jeder DRVA kann mehrere geschützte Domänen verwalten.



In diesem Beispiel wurden vier DRVA's für 80 virtuelle Maschinen erstellt.

1. Erstellen Sie Protokoll-Volumes für jedes DRVA unter Verwendung von VMDK aus den verfügbaren Datastores oder unabhängigen, gemeinsam genutzten iSCSI-Speicherpools.

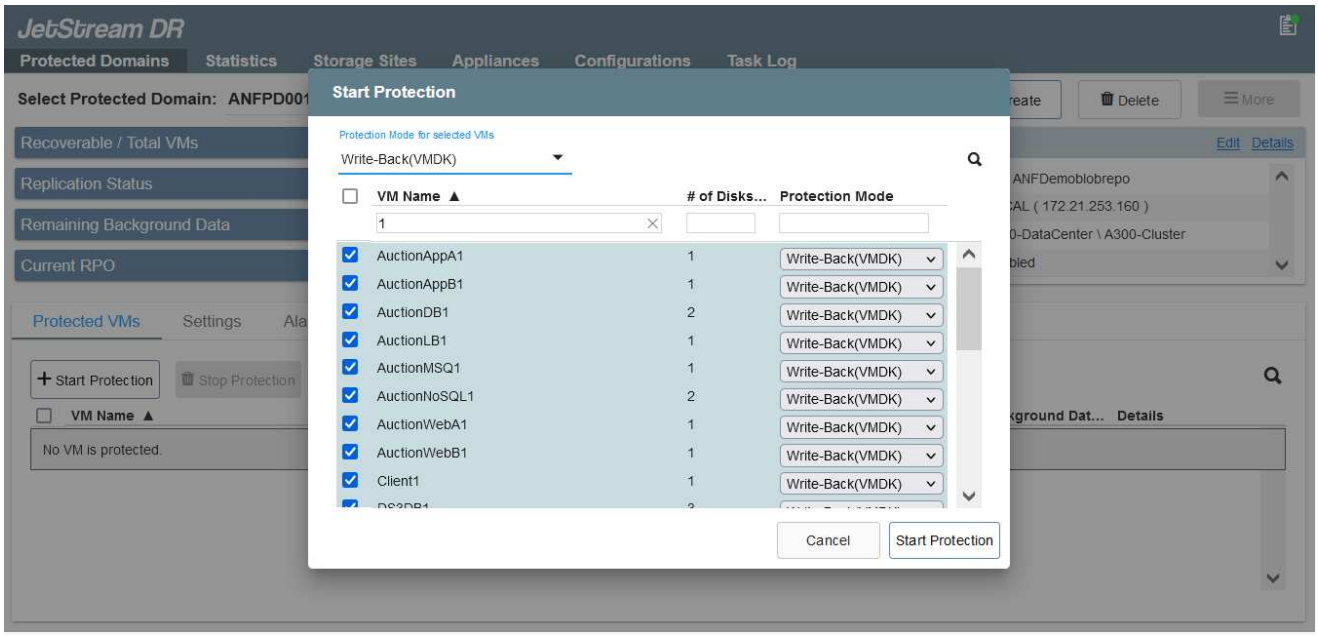
2. Erstellen Sie auf der Registerkarte geschützte Domänen die erforderliche Anzahl geschützter Domänen mithilfe von Informationen über die Azure Blob Storage-Site, die DRVA-Instanz und das Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder einen Satz von VMs innerhalb des Clusters, die gemeinsam geschützt werden, und weist eine Prioritätsreihenfolge für Failover-/Failback-Vorgänge zu.



3. Wählen Sie VMs aus, die Sie sichern möchten, und starten Sie den VM-Schutz der geschützten Domäne. Dies beginnt mit der Datenreplizierung zum zugewiesenen Blob-Store.

Vergewissern Sie sich, dass derselbe Sicherungsmodus für alle VMs in einer geschützten Domäne verwendet wird.

Write Back(VMDK)-Modus kann eine höhere Performance bieten.



Vergewissern Sie sich, dass die Protokoll-Volumes für die Replizierung auf hochperformanten Storage

platziert sind.

Failover Run Books können so konfiguriert werden, dass sie die VMs (namens Recovery Group) gruppieren, die Boot-Reihenfolge festlegen und die CPU-/Speichereinstellungen sowie die IP-Konfigurationen ändern.

Installieren Sie JetStream DR für AVS mit dem Befehl Run in einer Private Cloud der Azure VMware Lösung

Eine Best Practice für einen Recovery-Standort (AVS) ist die Erstellung eines Pilotlichtclusters mit drei Knoten im Voraus. Dadurch kann die Infrastruktur am Recovery-Standort vorkonfiguriert werden, einschließlich der folgenden Elemente:

- Netzwerkzielsegmente, Firewalls, Services wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF Volumes als Datastores und mehrJetStream DR unterstützt RTO-Modus von nahezu null für geschäftskritische Domänen. In diesen Domänen sollte der Ziel-Storage vorinstalliert sein. ANF ist in diesem Fall ein empfohlener Speichertyp.

Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster entsprechend den Anforderungen vor Ort konfiguriert werden.

Je nach SLA- und RTO-Anforderungen kann für einen kontinuierlichen Failover oder einen normalen (Standard-) Failover-Modus verwendet werden. Für eine RTO von nahezu null sollte am Recovery-Standort eine kontinuierliche Rehydrierung gestartet werden.

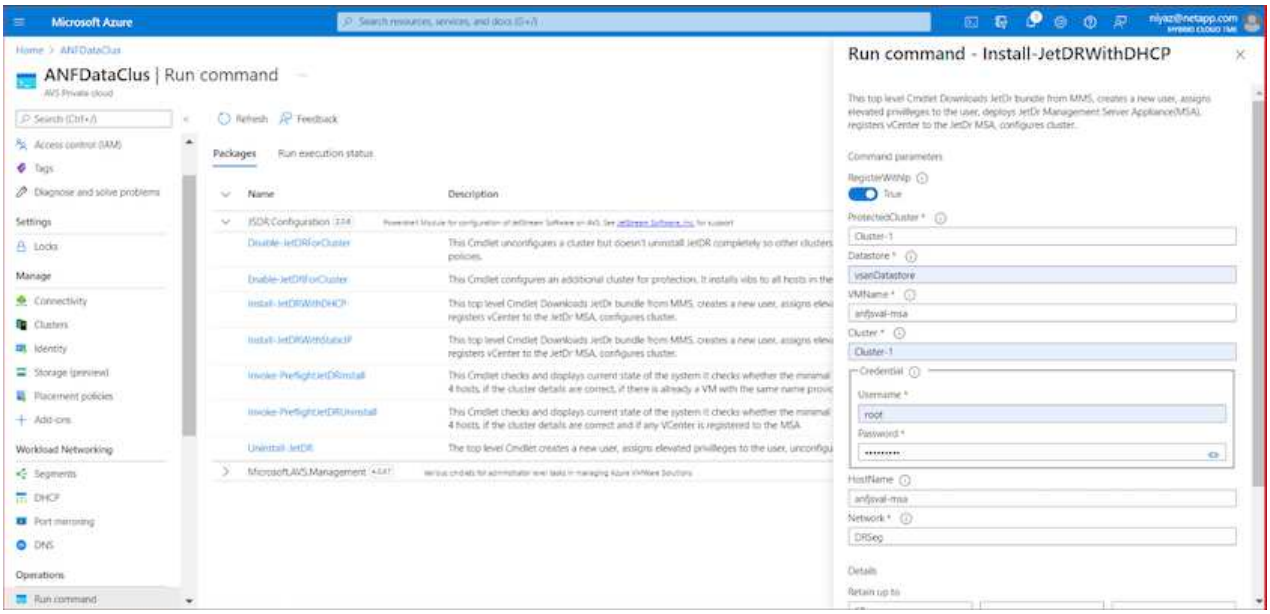
So installieren Sie JetStream DR für AVS in einer Private Cloud

So installieren Sie JetStream DR für AVS auf einer privaten Cloud der Azure VMware-Lösung:

1. Wählen Sie im Azure-Portal die Azure VMware-Lösung aus, wählen Sie die Private Cloud aus und wählen Sie Ausführen Command > Packages > JSDR.Configuration.

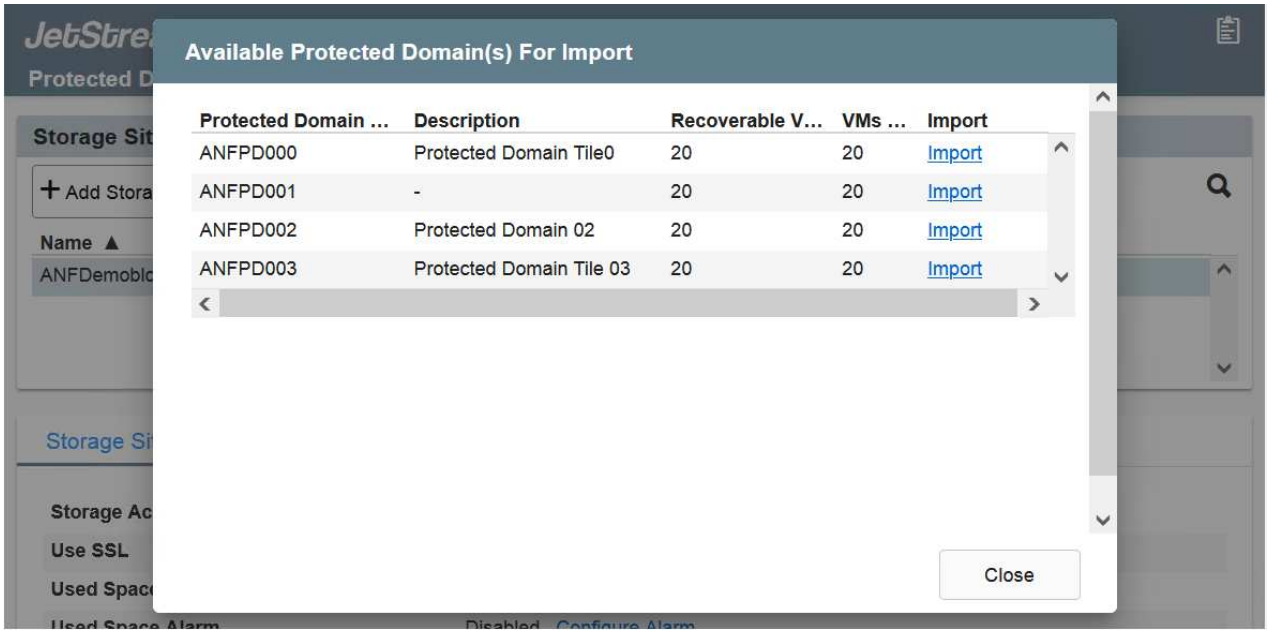
   > Der CloudAdmin-Standardbenutzer in Azure VMware verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Lösung ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Befehls Azure VMware Solution Run für JetStream DR.

   Der folgende Screenshot zeigt die Installation mithilfe einer DHCP-basierten IP-Adresse.



2. Nachdem die JetStream DR für AVS-Installation abgeschlossen ist, aktualisieren Sie den Browser. Um auf die JetStream DR-UI zuzugreifen, wechseln Sie zum SDDC Datacenter > Configure > JetStream DR.

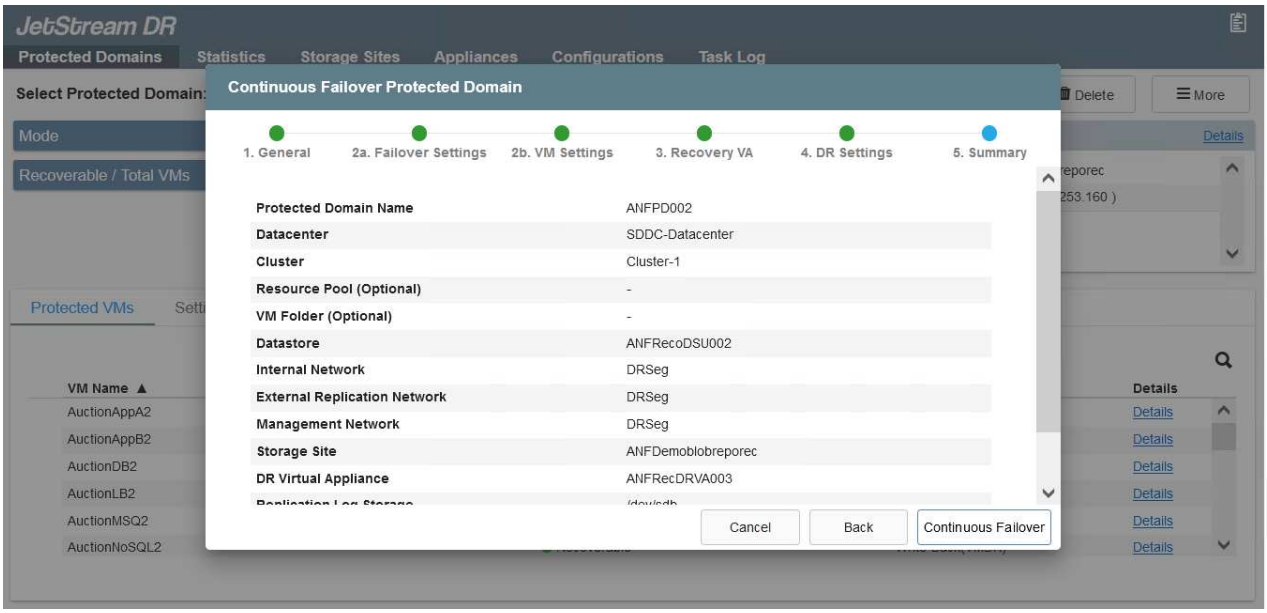
3. Fügen Sie über die JetStream DR-Schnittstelle das Azure Blob Storage-Konto hinzu, das zum Schutz des lokalen Clusters als Storage-Standort verwendet wurde, und führen Sie die Option Scan Domains aus.



4. Nachdem die geschützten Domains importiert wurden, sollten DRVA-Appliances bereitgestellt werden. In diesem Beispiel wird mithilfe der JetStream DR-Benutzeroberfläche eine kontinuierliche Rehydrierung manuell vom Wiederherstellungsstandort gestartet.

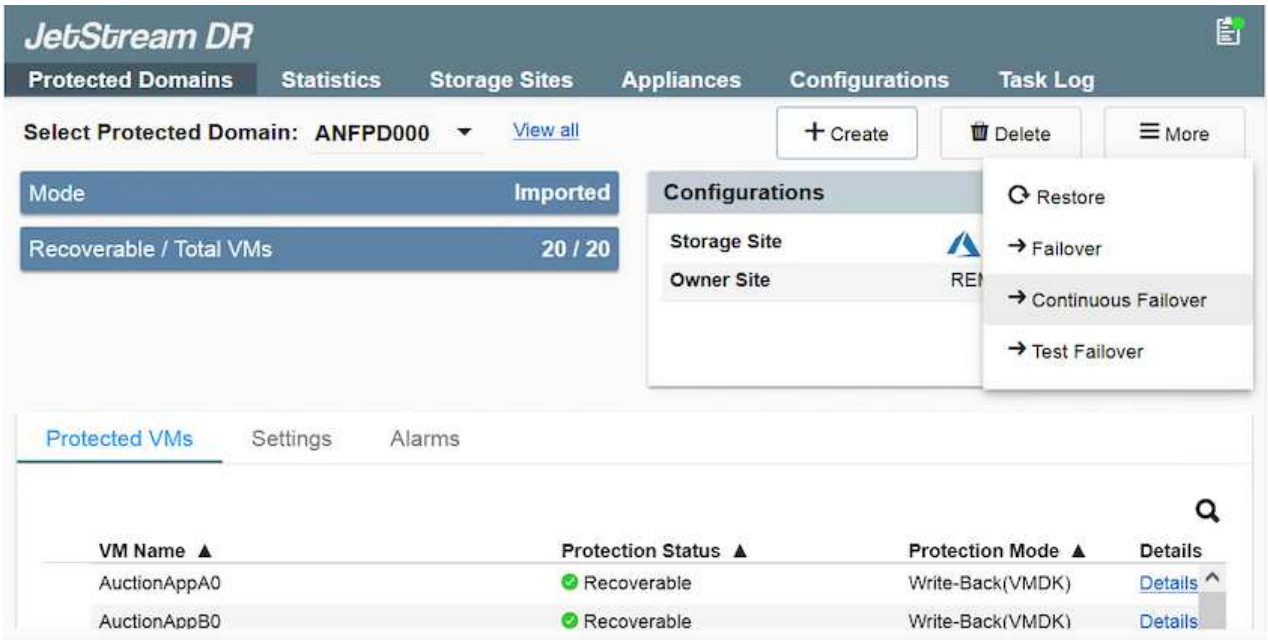
> Diese Schritte können auch mithilfe von CPT erstellten Plänen automatisiert werden.

5. Verwenden von verfügbaren vSAN oder ANF-Datastores für Replizierungsprotokolle erstellen
6. Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery VA, um den ANF-Datenspeicher für VM-Platzierungen zu verwenden.



Stellen Sie sicher, dass DHCP für das ausgewählte Segment aktiviert ist und genügend IP-Adressen verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen sich wiederherstellen. Jede wiederherzuckernde VM (einschließlich kontinuierlicher Rehydrierung) erfordert eine individuelle dynamische IP-Adresse. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

7. Wählen Sie die entsprechende Failover-Option (Continuous Failover oder Failover) aus. In diesem Beispiel wird die kontinuierliche Rehydrierung (kontinuierliches Failover) ausgewählt.



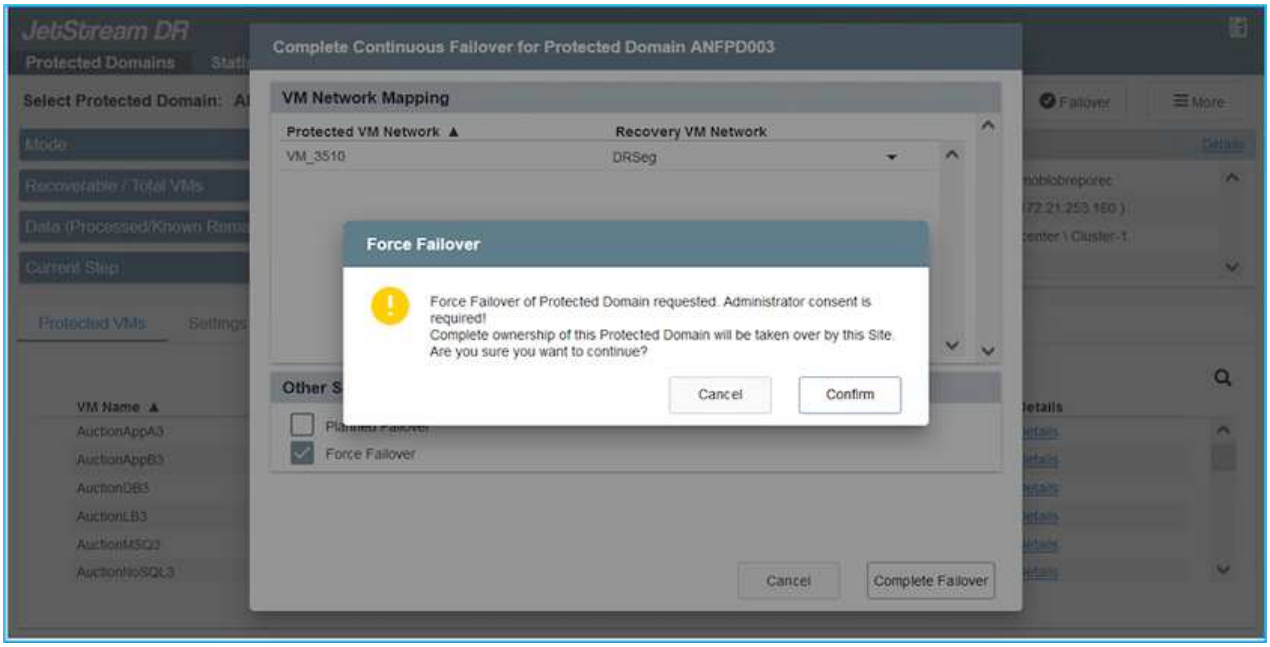
Failover/Failback Wird Durchgeführt

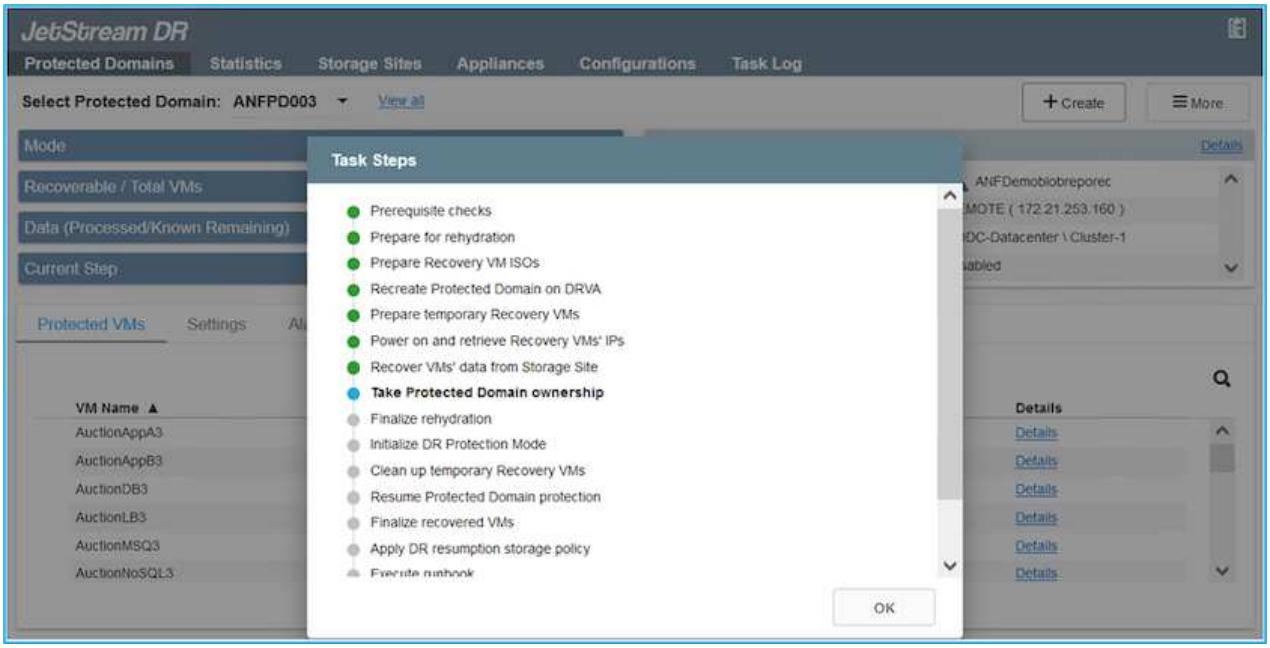
So führen Sie ein Failover/Failback aus

1. Nachdem im geschützten Cluster der lokalen Umgebung ein Ausfall auftritt (ein teilweiser oder vollständiger Ausfall), lösen Sie den Failover aus.

   CPT kann verwendet werden, um den Failover-Plan zur Wiederherstellung der VMs von Azure Blob Storage auf dem AVS Cluster Recovery-Standort auszuführen.

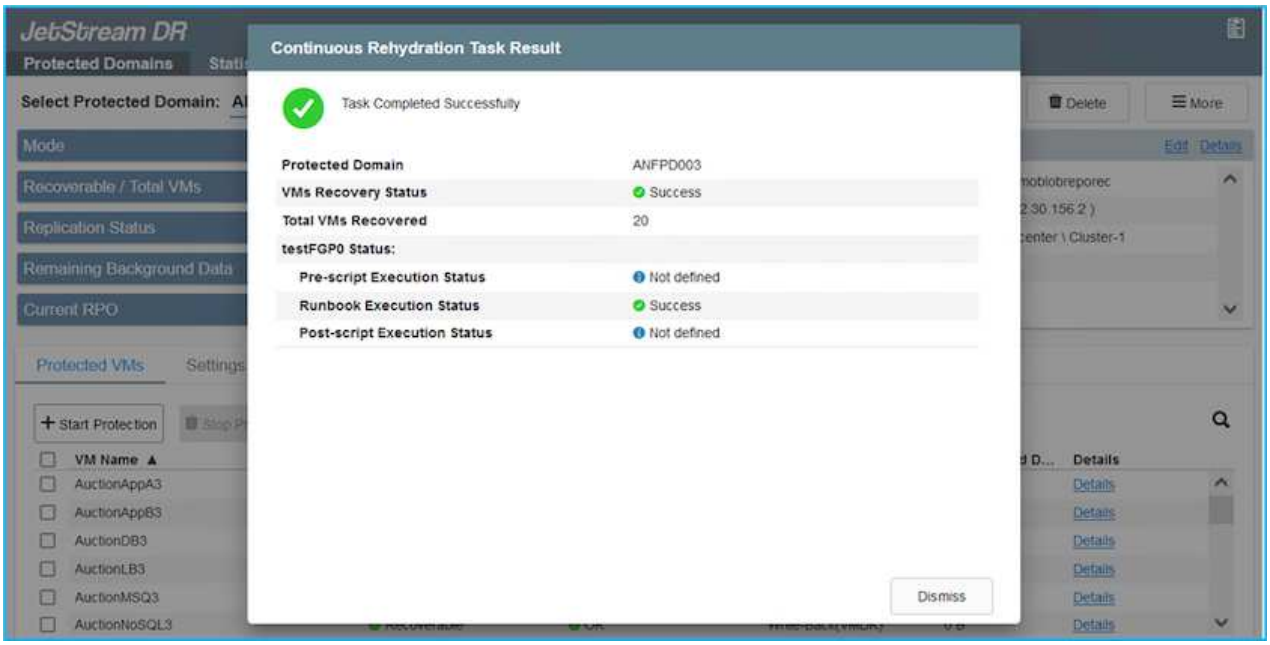
   Nach dem Failover (zur kontinuierlichen oder standardmäßigen Wiederherstellung), wenn die geschützten VMs in AVS gestartet wurden, wird der Schutz automatisch fortgesetzt und JetStream DR repliziert ihre Daten weiterhin in den entsprechenden/Original-Containern im Azure Blob Storage.





   In der Taskleiste wird der Status von Failover-Aktivitäten angezeigt.

2. Nach Abschluss der Aufgabe greifen Sie auf die wiederhergestellten VMs zu, und der Geschäftsbetrieb läuft normal weiter.

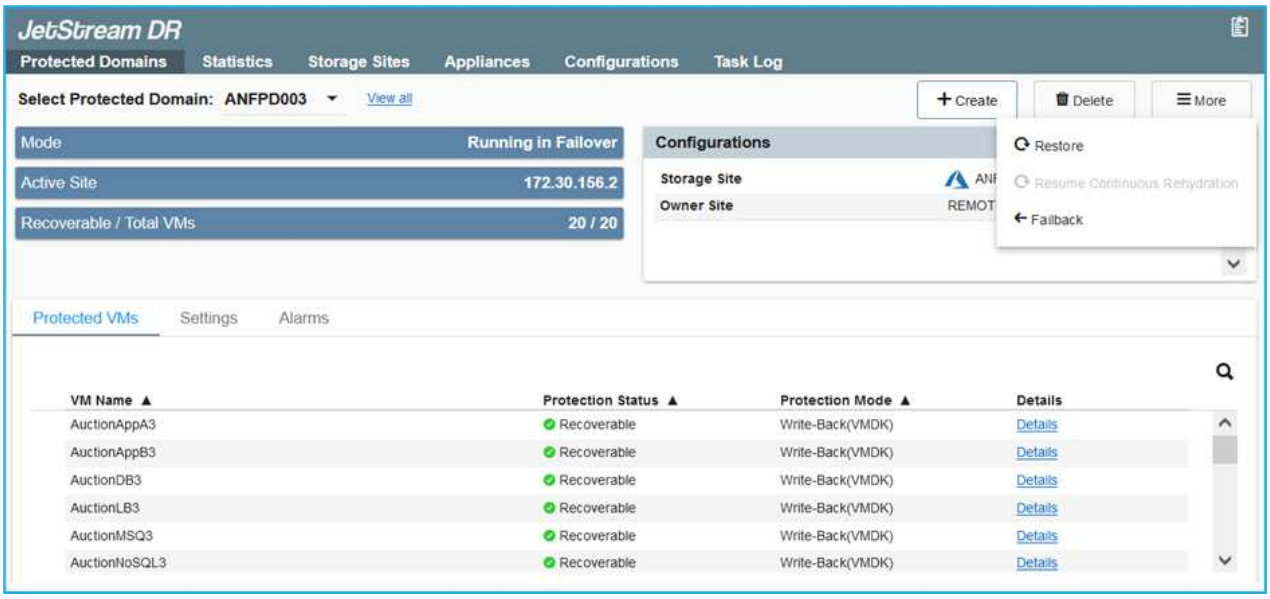


Wenn der primäre Standort wieder in Betrieb ist, kann ein Failback durchgeführt werden. Der VM-Schutz wird wieder aufgenommen und die Datenkonsistenz sollte überprüft werden.

3. Wiederherstellung der lokalen Umgebung Je nach Art des Notfalleinfalls sind möglicherweise die Wiederherstellung und/oder Überprüfung der Konfiguration des geschützten Clusters erforderlich. Falls erforderlich, muss die JetStream DR-Software möglicherweise erneut installiert werden.

> Hinweis: Der `recovery_utility_prepare_failback` Das im Automation Toolkit zur Verfügung gestellte Skript kann verwendet werden, um die ursprüngliche geschützte Site von veralteten VMs, Domäneninformationen usw. zu reinigen.

4. Greifen Sie auf die wiederhergestellte On-Premises-Umgebung zu, rufen Sie die Jetstream DR UI auf und wählen Sie die entsprechende geschützte Domäne aus. Nachdem der geschützte Standort für Failback bereit ist, wählen Sie die Failback-Option in der UI aus.



Mit dem durch CPT generierten Failback-Plan kann außerdem die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher in die ursprüngliche VMware Umgebung initiiert werden.

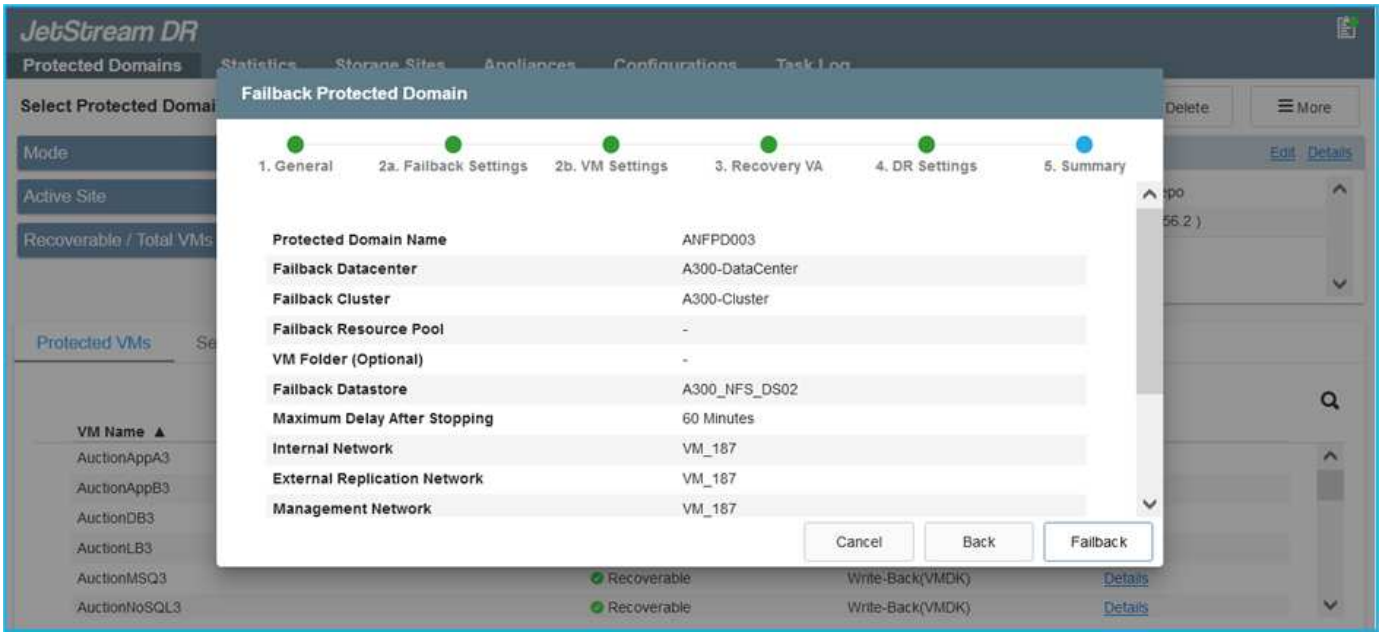
Geben Sie die maximale Verzögerung an, nachdem Sie die VMs am Recovery-Standort angehalten und am geschützten Standort neu gestartet haben. Diese Zeit umfasst das Abschließen der Replizierung nach dem Stoppen von Failover-VMs, die Zeit für die Bereinigung des Recovery-Standorts und die Zeit zur Wiederherstellung von VMs am geschützten Standort. Der von NetApp empfohlene Wert beträgt 10 Minuten.

Schließen Sie den Failback-Prozess ab, und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

Wiederherstellung Von Lösegeld-Waren

Die Wiederherstellung von Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Abteilungen schwierig sein, den sicheren Rückgabepunkt zu ermitteln und einmal festgestellt zu haben, wie sichergestellt werden kann, dass wiederhergestellte Workloads vor den erneuten Angriffen (vom Schlafen von Malware oder durch anfällige Anwendungen) geschützt sind.

Jetstream DR für AVS kann zusammen mit Azure NetApp Files Datastores diese Bedenken lösen, da Unternehmen eine Recovery von verfügbaren Zeitpunkten durchführen können, sodass Workloads bei Bedarf in einem funktionsfähigen, isolierten Netzwerk wiederhergestellt werden können. Durch Recovery können Applikationen funktionieren und miteinander kommunizieren, ohne dass sie dem Nord- Süd-Datenverkehr ausgesetzt werden. So erhalten Sicherheitsteams einen sicheren Ort, um forensische und andere notwendige Korrekturmaßnahmen durchzuführen.



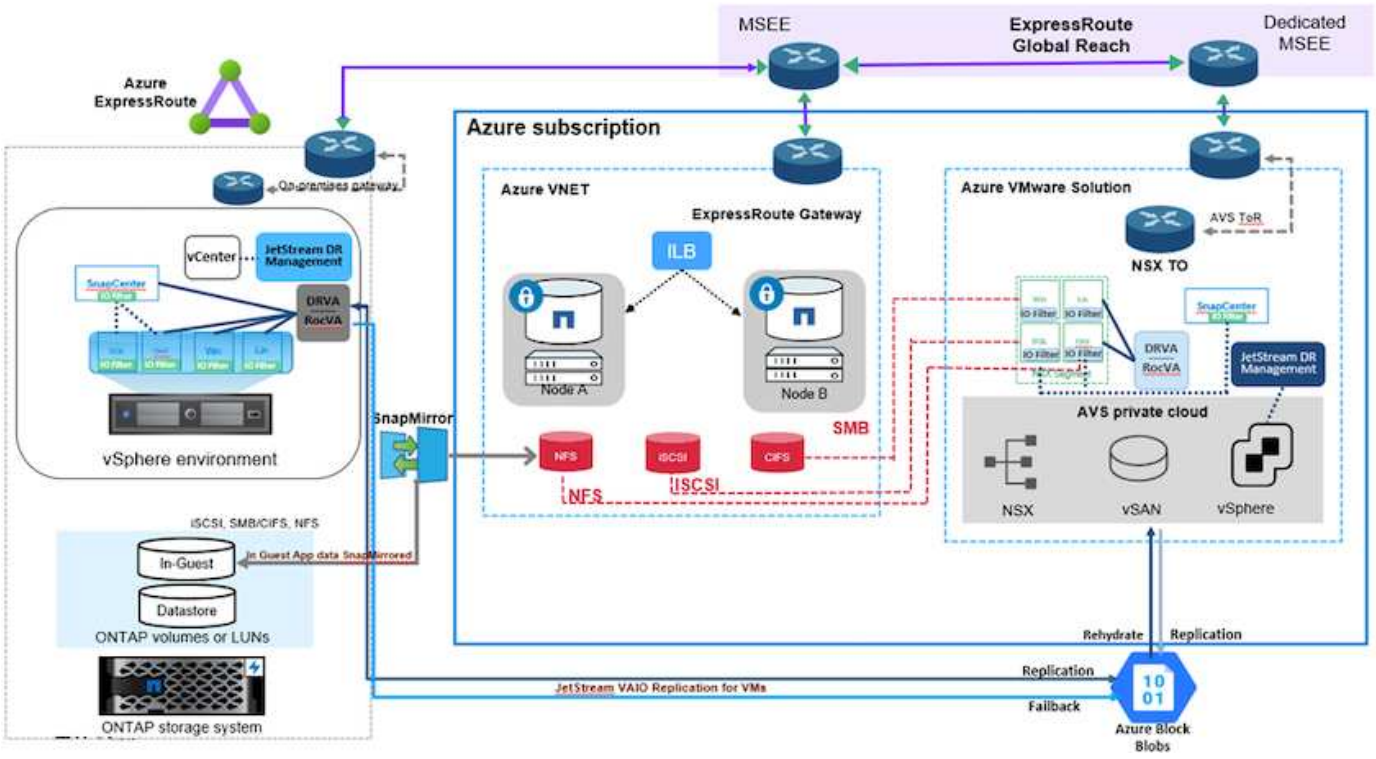
Disaster Recovery mit CVO und AVS (Storage mit Anbindung an den Gast)

Überblick

Autoren: Ravi BCB und Niyaz Mohamed, NetApp

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die einen mit dem Gast verbundenen Storage verwenden, auf NetApp Cloud Volumes ONTAP in Azure repliziert werden. Dies bezieht sich auf Applikationsdaten, doch was ist mit den eigentlichen VMs selbst. Disaster Recovery sollte alle abhängigen Komponenten, einschließlich Virtual Machines, VMDKs, Applikationsdaten und mehr, abdecken. Zu diesem Zweck kann SnapMirror zusammen mit Jetstream verwendet werden, um Workloads, die von On-Premises zu Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen und gleichzeitig vSAN Storage für VM-VMDKs zu verwenden.

Dieses Dokument bietet einen Schritt-für-Schritt-Ansatz zur Einrichtung und Durchführung von Disaster Recovery mit NetApp SnapMirror, JetStream und der Azure VMware Lösung (AVS).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.

> Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Konnektivität zwischen der On-Premises-Umgebung und dem virtuellen Azure-Netzwerk nutzen Sie die globale Express Route oder ein virtuelles WAN mit einem VPN-Gateway. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Azure zu verbinden, sodass wir nicht einen bestimmten Workflow in diesem Dokument beschreiben können. Die entsprechende On-Premises-zu-Azure-Konnektivitätsmethode finden Sie in der Azure-Dokumentation.

Implementieren der DR-Lösung

Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mithilfe von Cloud Manager Cloud Volumes ONTAP mit der richtigen Instanzgröße innerhalb des entsprechenden Abonnements und des virtuellen Netzwerks bereit.
    a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes

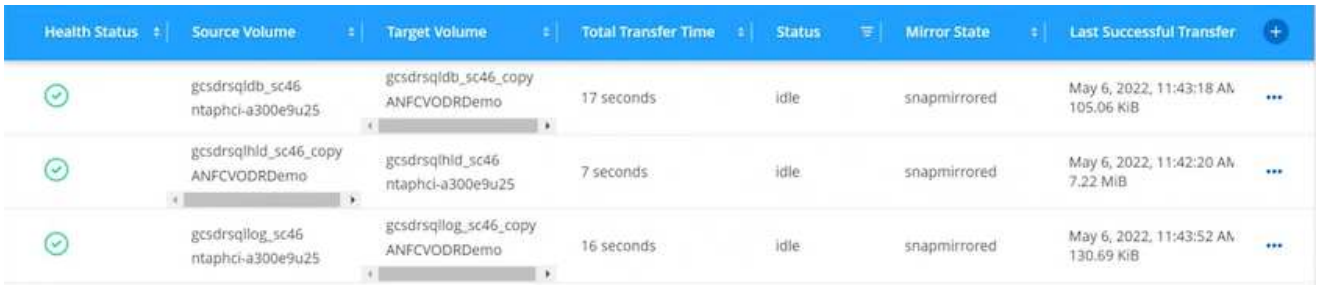
b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.

3. Installieren Sie die JetStream DR-Software im lokalen Datacenter, und beginnen Sie mit dem Schutz für Virtual Machines.
4. Installieren Sie die JetStream DR-Software in der Private Cloud der Azure VMware Lösung.
5. Bei einem Notfall können Sie die SnapMirror Beziehung mithilfe von Cloud Manager unterbrechen und das Failover von Virtual Machines zu Azure NetApp Files oder zu vSAN Datastores im vorgesehenen AVS-DR-Standort auslösen.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
6. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Azure und Replizierung von Volumes zu CVO

Der erste Schritt besteht darin, Cloud Volumes ONTAP auf Azure (zu konfigurieren"Verlinken") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.



Konfigurieren Sie AVS-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der Azure VMware Lösung und die Dauer des SDDC im Service. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Die Entscheidung für die Implementierung eines AVS-Clusters hängt in erster Linie von den RPO/RTO-Anforderungen ab. Mit der Azure VMware Lösung kann das SDDC bereits rechtzeitig zur Verfügung gestellt werden, um entweder für das Testen oder für ein tatsächliches Notfallereignis zu sorgen. Ein durch die Just-in-time-Implementierung implementierter SDDC spart ESXi Hostkosten, wenn Sie keine Katastrophe mehr haben. Diese Form der Implementierung wirkt sich jedoch auf das RTO um einige Stunden aus, während das SDDC bereitgestellt wird.

Am häufigsten implementiert wird die SDDC-Option in einem Pilot-Light-Modus, der immer aktiviert ist. Diese Option bietet einen kleinen Platzbedarf von drei Hosts, die immer verfügbar sind. Außerdem werden Recovery-Vorgänge durch eine Basis für Simulationsaktivitäten und Compliance-Prüfungen beschleunigt, sodass das Risiko einer operativen Abweichungen zwischen dem Produktions- und dem DR-Standort vermieden wird. Der Pilot-Light-Cluster kann bei Bedarf schnell auf das gewünschte Niveau skaliert werden, um tatsächliche DR-Ereignisse zu bewältigen.

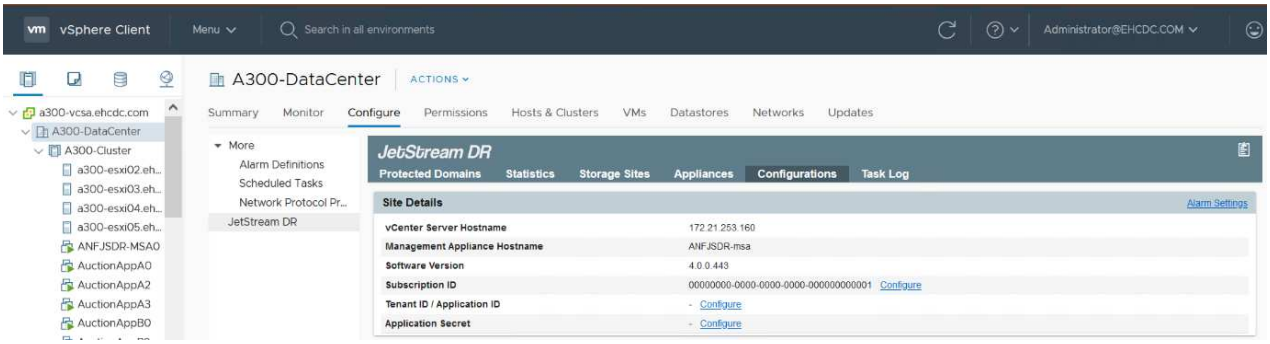
Informationen zur Konfiguration des AVS SDDC (ob On-Demand oder im Pilot-Light-Modus) finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf Azure". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den AVS-Hosts nach dem Einrichten der Konnektivität Daten von Cloud Volumes ONTAP nutzen können.

Nach der ordnungsgemäßen Konfiguration von Cloud Volumes ONTAP und AVS beginnen Sie mit der Konfiguration des Jetstream zur Automatisierung der Wiederherstellung lokaler Workloads auf AVS (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) mithilfe des VAIO Mechanismus und durch Nutzung von SnapMirror für Applikations-Volumes-Kopien auf Cloud Volumes ONTAP.

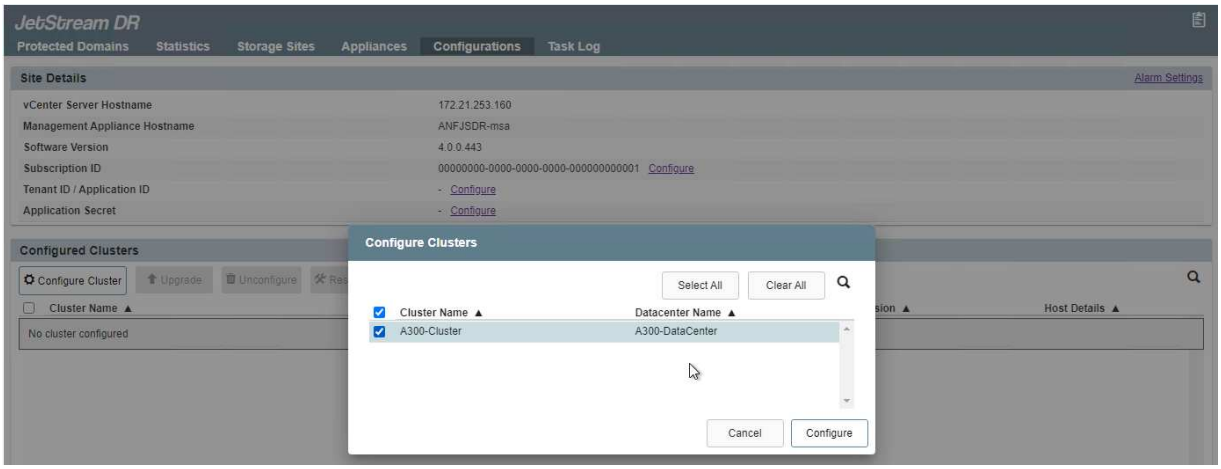
Installieren Sie JetStream DR im lokalen Datacenter

Die Jetstream DR-Software besteht aus drei Hauptkomponenten: Der JetStream DR Management Server Virtual Appliance (MSA), der DR Virtual Appliance (DRVA) und den Host-Komponenten (I/O-Filterpakete). Mit dem MSA-System werden Hostkomponenten auf dem Compute-Cluster installiert und konfiguriert und JetStream DR-Software verwaltet. Die Installation erfolgt wie folgt:

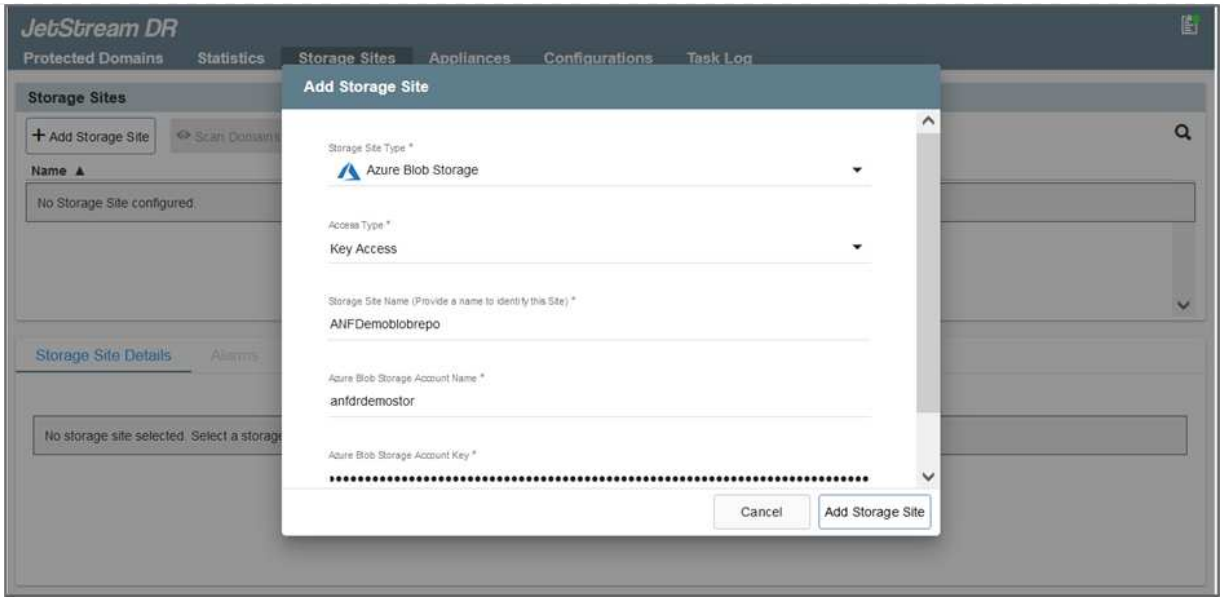
1. Voraussetzungen prüfen.
2. Nutzen Sie das Kapazitätsplanungs-Tool für Ressourcen- und Konfigurationsempfehlungen.
3. Implementieren Sie JetStream DR MSA auf jedem vSphere-Host im zugewiesenen Cluster.
4. Starten Sie das MSA-Produkt mit dem DNS-Namen in einem Browser.
5. Registrieren Sie den vCenter-Server mit dem MSA.
6. Nachdem JetStream DR MSA implementiert und der vCenter Server registriert wurde, navigieren Sie zum JetStream DR Plug-in mit dem vSphere Web Client. Dazu können Sie im Datacenter > Configure > JetStream DR navigieren.



7. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
   a. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket.

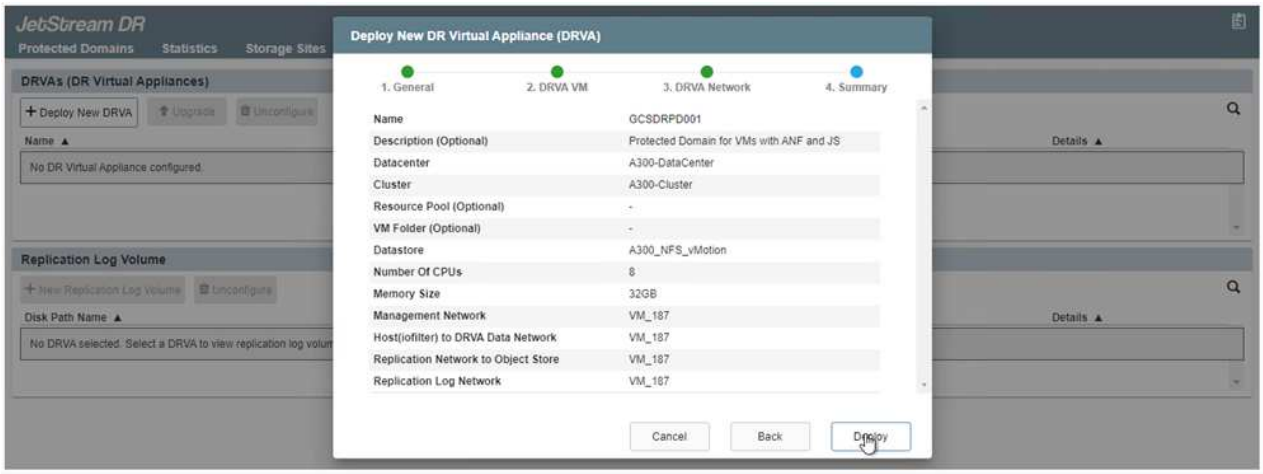


   b. Fügen Sie den Azure Blob-Storage am Recovery-Standort hinzu.

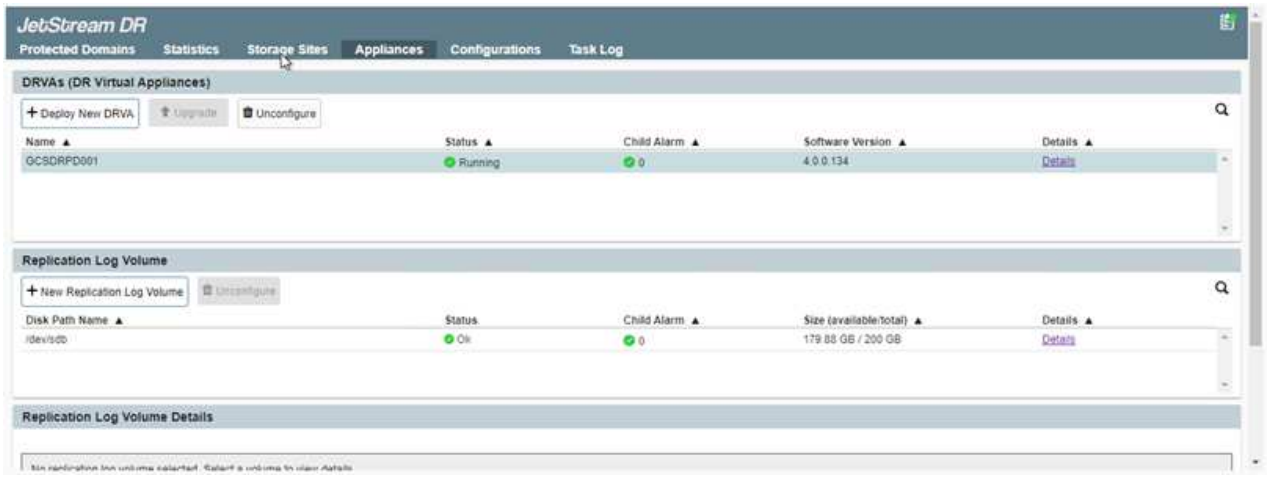


8. Stellen Sie die erforderliche Anzahl an DR Virtual Appliances (DRVAs) über die Registerkarte Appliances bereit.

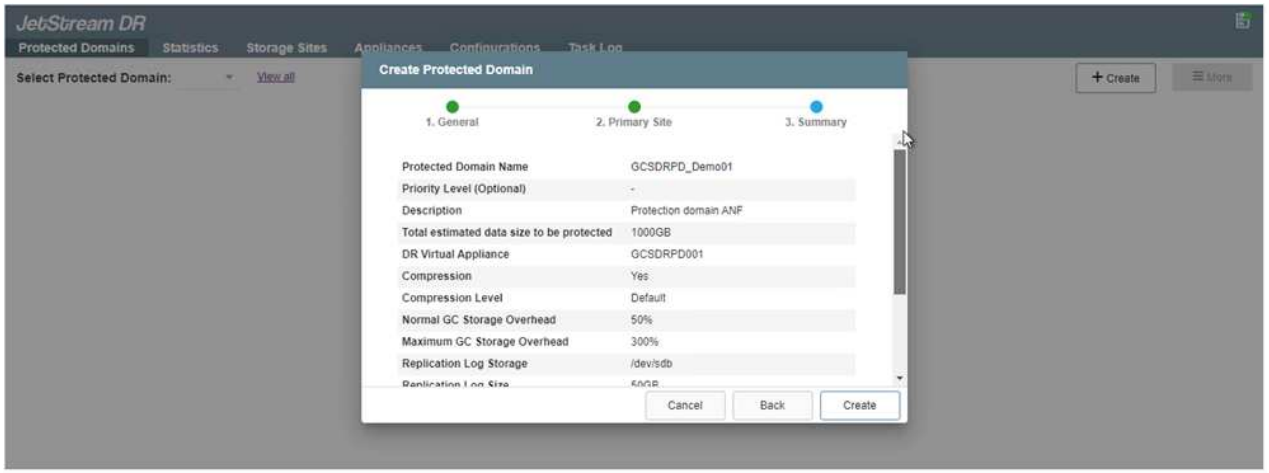
> Verwenden Sie das Kapazitätsplanungs-Tool, um die Anzahl der benötigten DRVAs zu ermitteln.

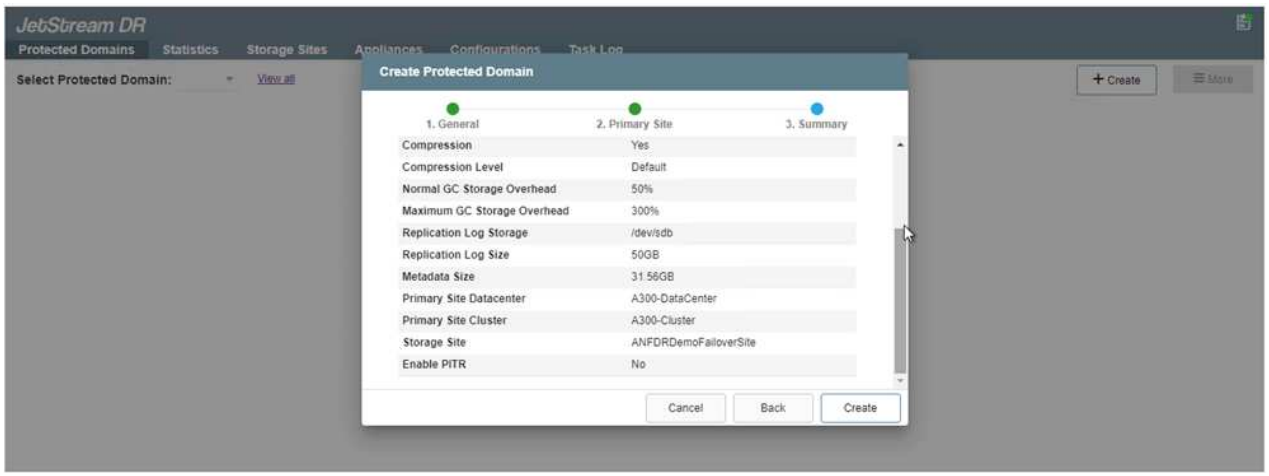


9. Erstellen Sie Protokoll-Volumes für jedes DRVA unter Verwendung der VMDK aus den verfügbaren Datenspeichern oder dem unabhängigen gemeinsamen iSCSI-Speicherpool.



10. Erstellen Sie auf der Registerkarte geschützte Domänen die erforderliche Anzahl geschützter Domänen mithilfe von Informationen über die Azure Blob Storage-Site, die DRVA-Instanz und das Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder einen Satz von Applikations-VMs innerhalb des Clusters, die gemeinsam gesichert werden und einer Prioritätsreihenfolge für Failover-/Failback-Vorgänge zugewiesen ist.

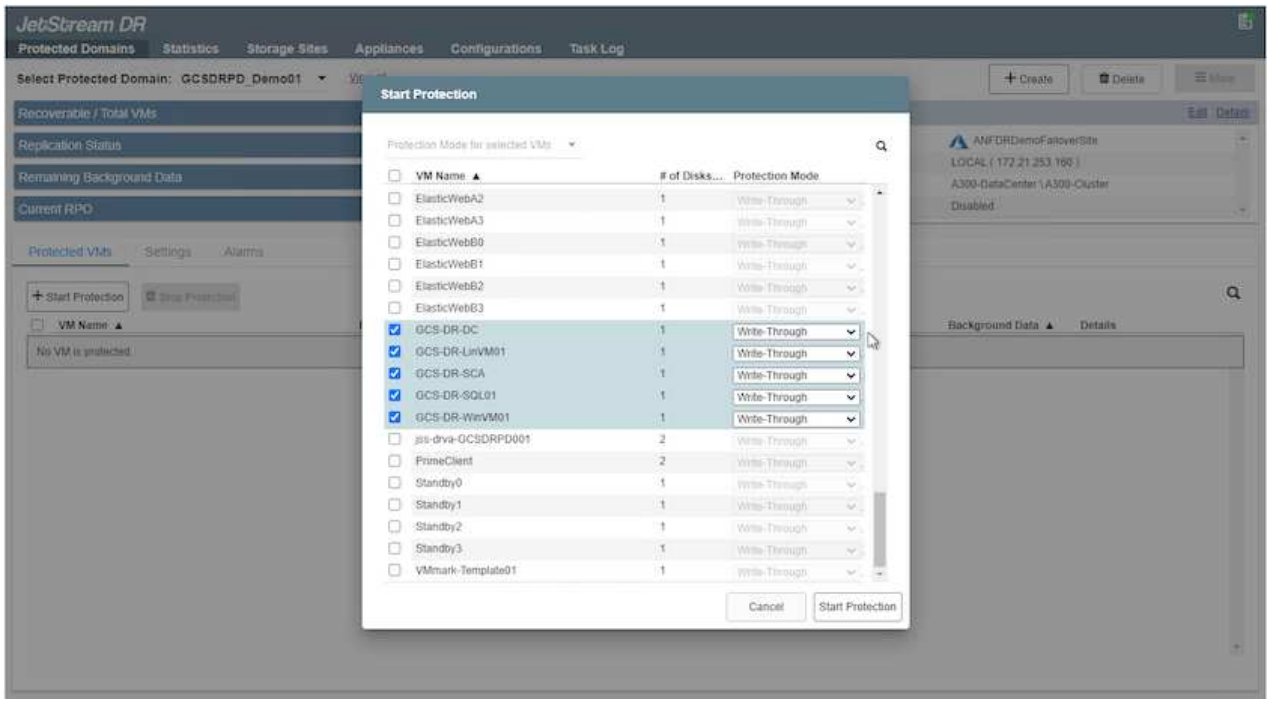




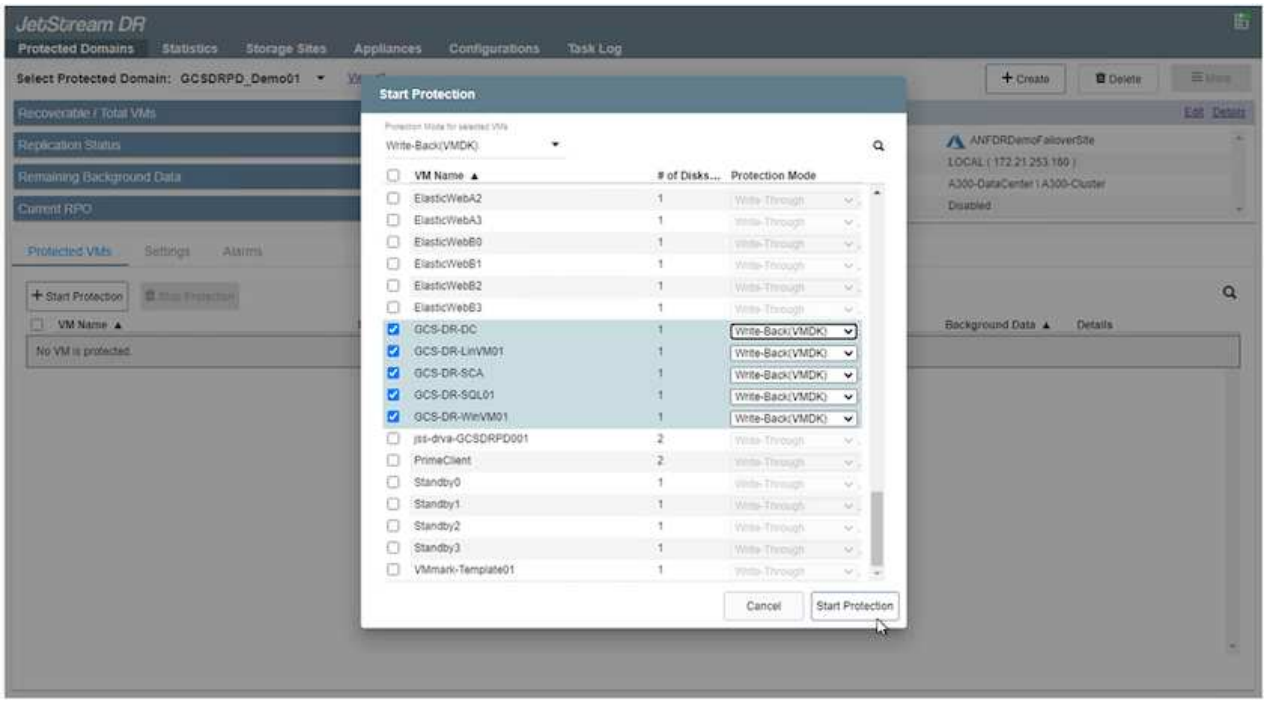
11. Wählen Sie die zu sichernden VMs aus und gruppieren Sie die VMs je nach Abhängigkeit in Applikationsgruppen. Anhand von Applikationsdefinitionen können Gruppen von VMs zu logischen Gruppen gruppiert werden, die ihre Boot-Aufträge, Boot-Verzögerungen und optionale Applikationsvalidierungen enthalten, die nach der Recovery ausgeführt werden können.

Vergewissern Sie sich, dass derselbe Sicherungsmodus für alle VMs in einer geschützten Domäne verwendet wird.

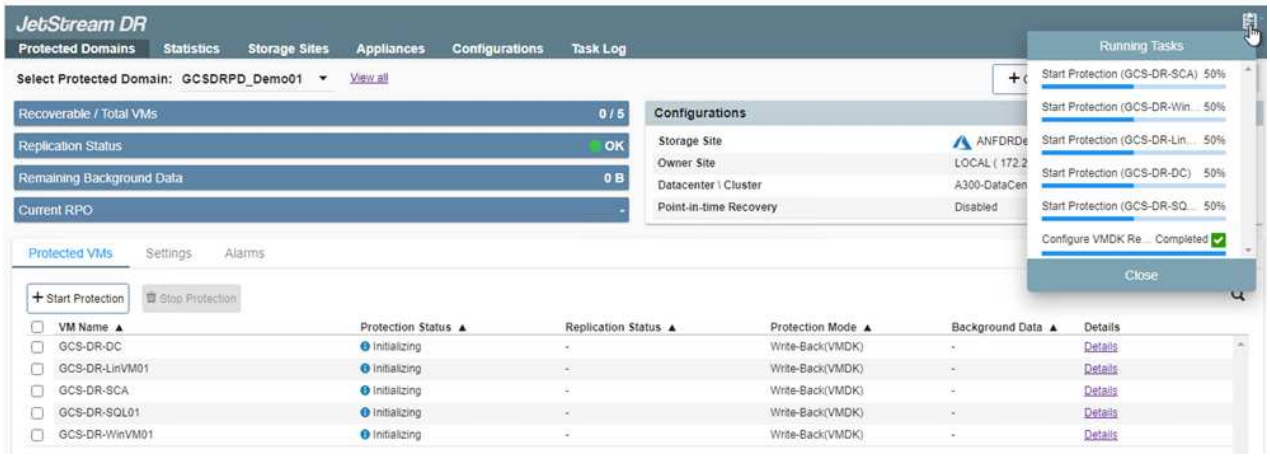
Write Back(VMDK)-Modus bietet eine höhere Performance.



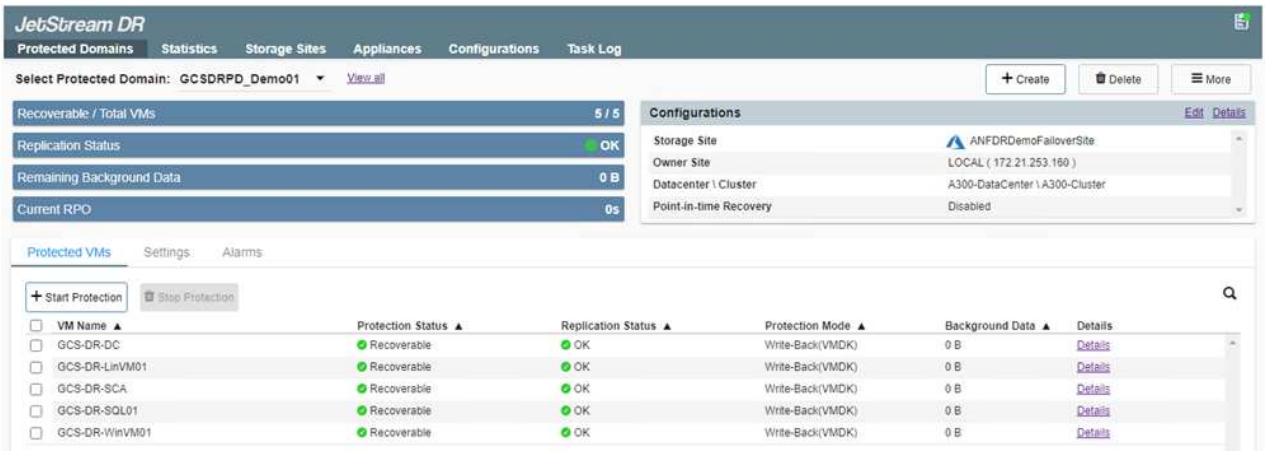
12. Stellen Sie sicher, dass Replizierungs-Protokoll-Volumes auf hochperformanten Storage platziert werden.



13. Klicken Sie nach dem Abschluss auf Schutz für die geschützte Domäne starten. Damit wird die Datenreplizierung für die ausgewählten VMs auf den zugewiesenen Blob-Speicher gestartet.



14. Nach Abschluss der Replizierung wird der Sicherungsstatus der VM als wiederherstellbar markiert.

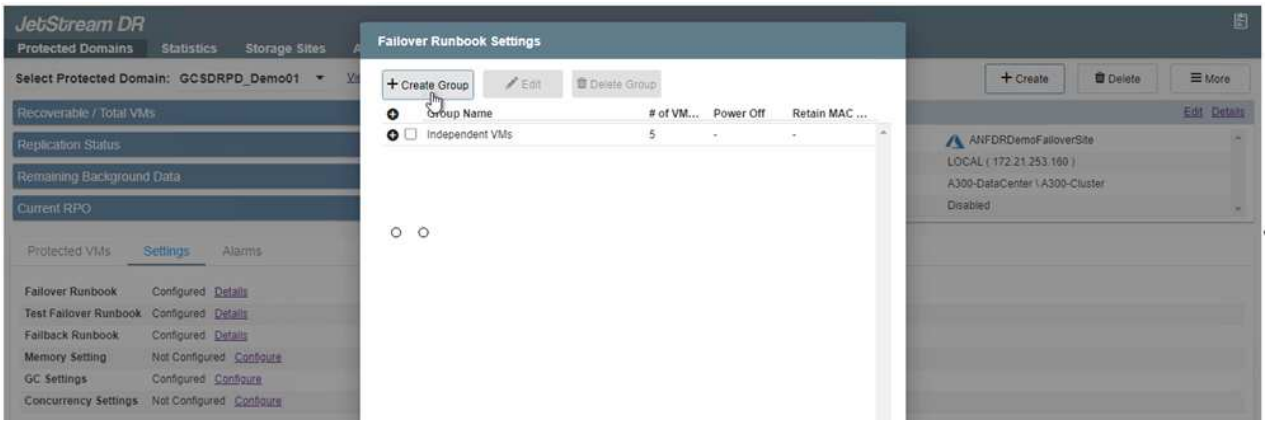


Failover-Runbooks können so konfiguriert werden, dass sie die VMs gruppieren (so genannte Recovery-Gruppe), die Boot-Reihenfolge festlegen und die CPU-/Speichereinstellungen zusammen mit den IP-Konfigurationen ändern.

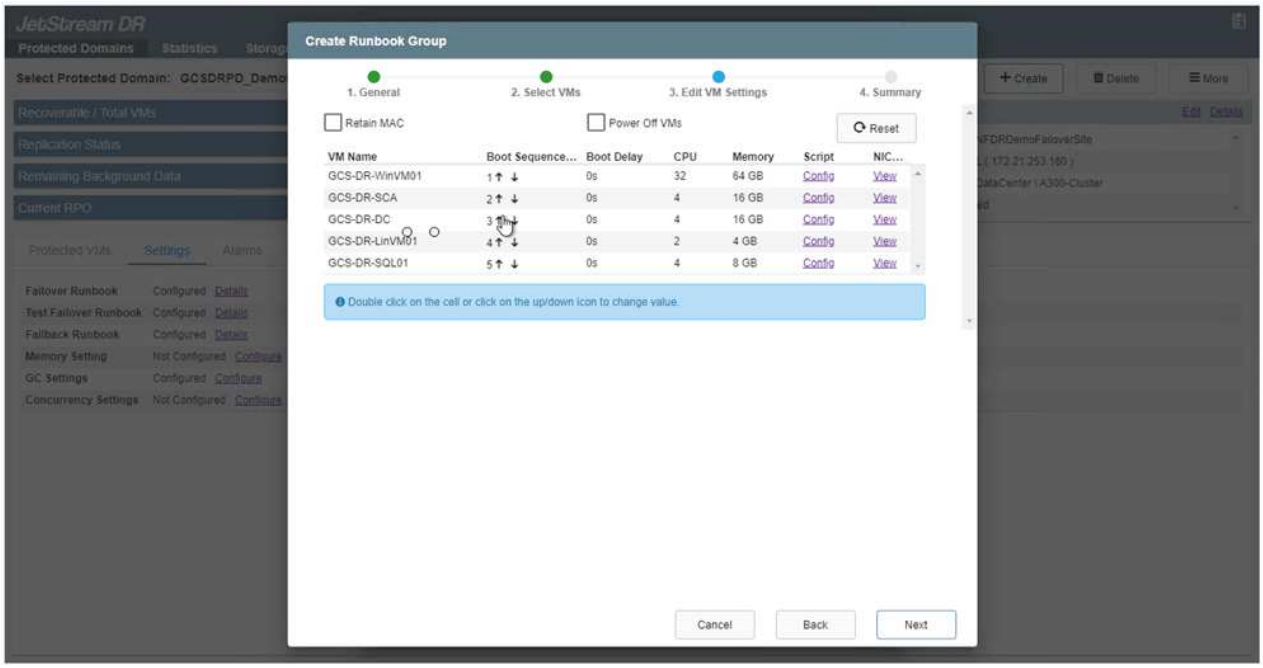
15. Klicken Sie auf Einstellungen und dann auf den Link Runbook Configure, um die Runbook-Gruppe zu konfigurieren.

16. Klicken Sie auf die Schaltfläche Gruppe erstellen, um mit der Erstellung einer neuen Runbook-Gruppe zu beginnen.

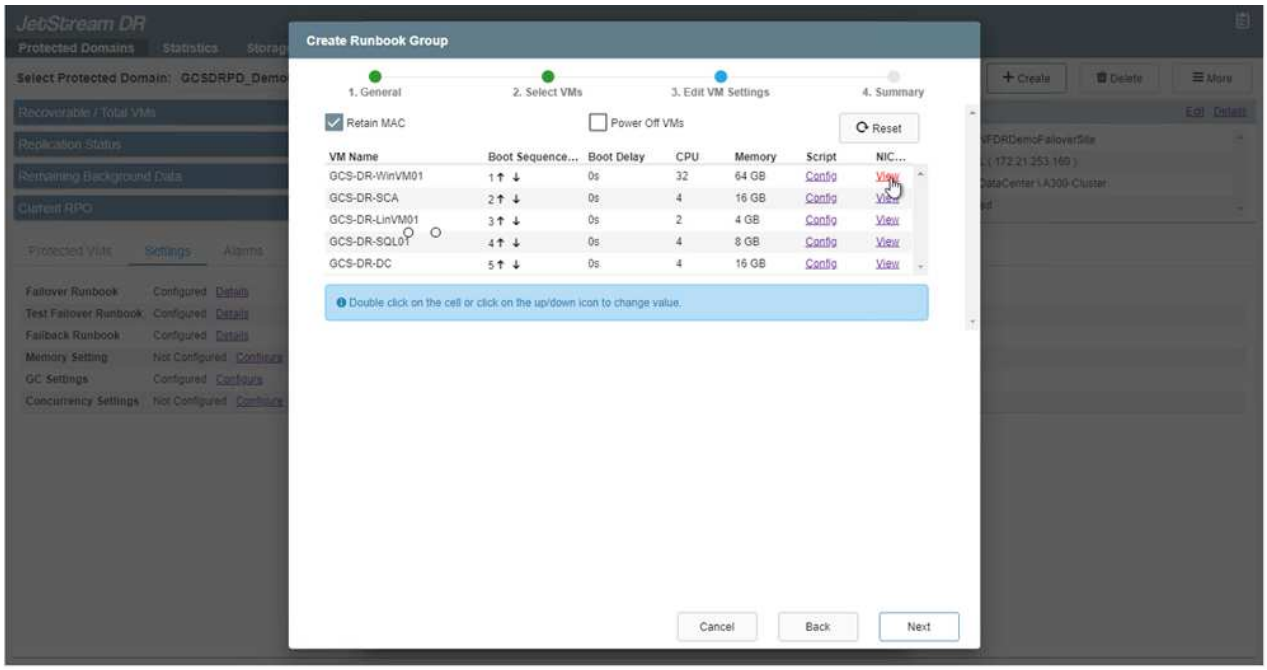
Falls erforderlich, wenden Sie im unteren Teil des Bildschirms benutzerdefinierte Pre-scripts und Post-scripts an, um automatisch vor und nach dem Betrieb der Runbook-Gruppe auszuführen. Stellen Sie sicher, dass die Runbook-Skripte auf dem Management-Server residieren.



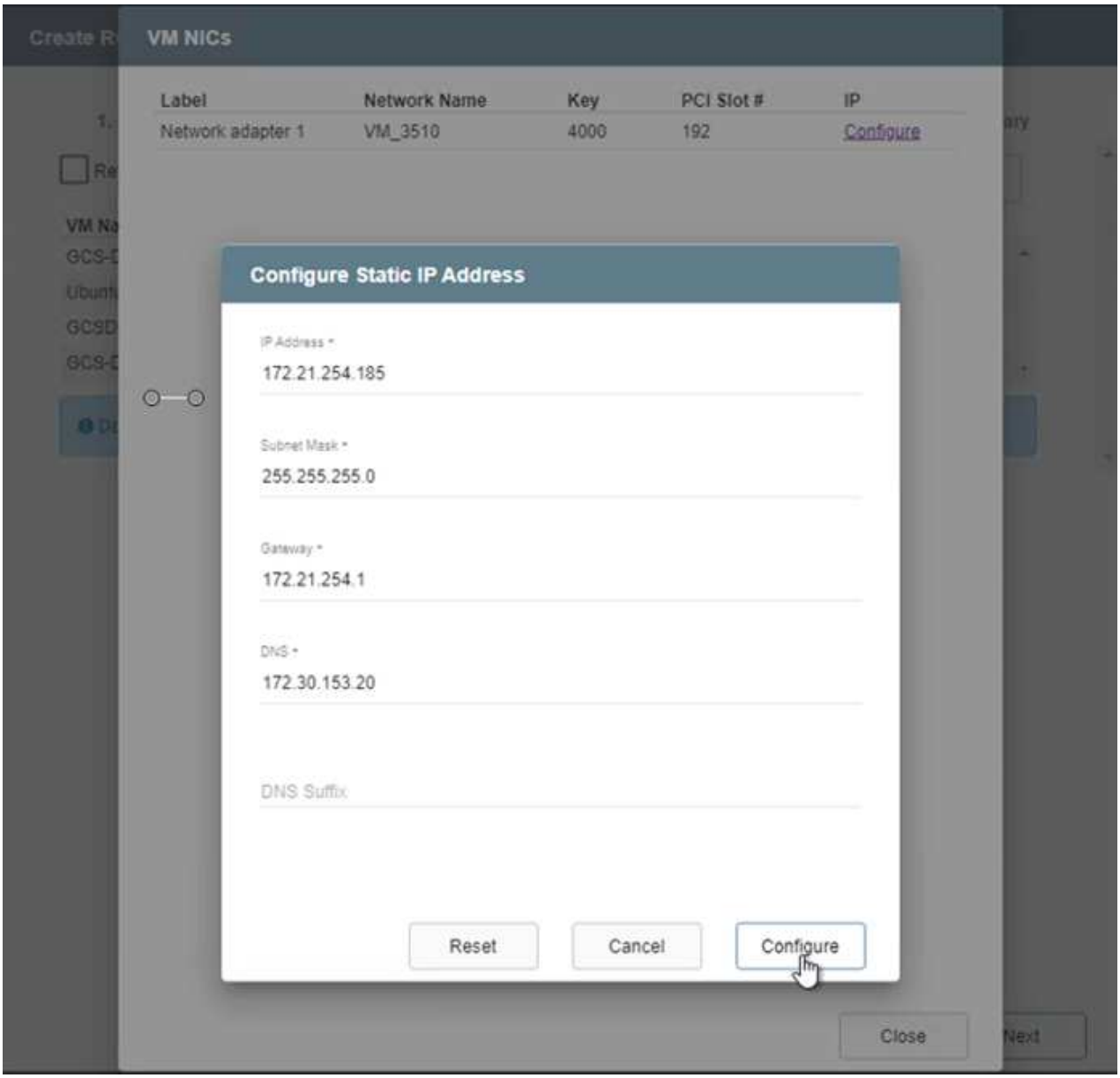
17. Bearbeiten Sie die VM-Einstellungen nach Bedarf. Geben Sie die Parameter für die Wiederherstellung der VMs an, einschließlich der Boot-Sequenz, der Boot-Verzögerung (angegeben in Sekunden), der Anzahl der CPUs und der zuzuzuzuzuzuzuzuzuzuzuzuzuzuweist. Ändern Sie die Boot-Sequenz der VMs, indem Sie auf die Pfeile nach oben oder unten klicken. Zur Aufbewahrung von MAC stehen auch Optionen zur Verfügung.

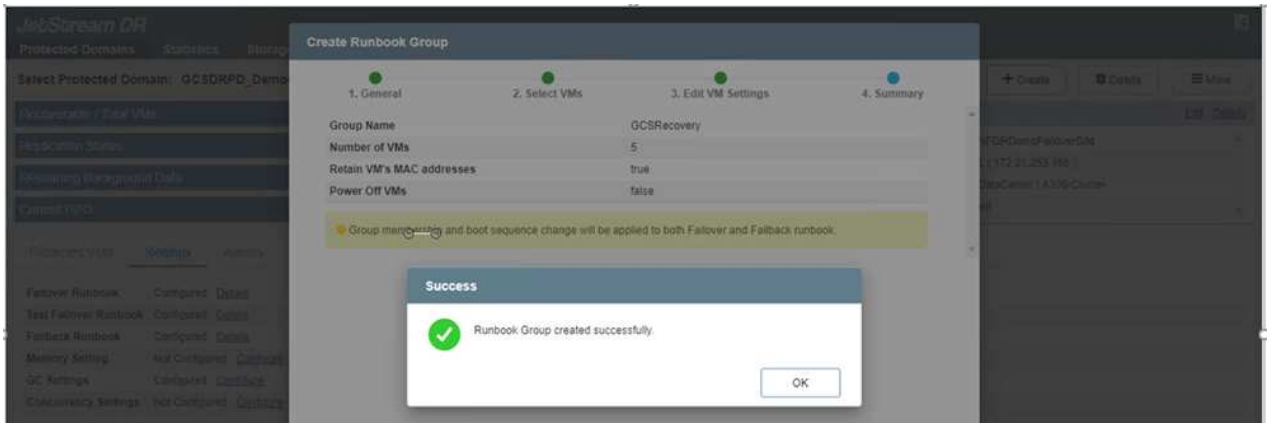


18. Statische IP-Adressen können manuell für die einzelnen VMs der Gruppe konfiguriert werden. Klicken Sie auf den Link „NIC-Ansicht“ einer VM, um die IP-Adresseinstellungen manuell zu konfigurieren.



19. Klicken Sie auf die Schaltfläche Konfigurieren, um die NIC-Einstellungen für die jeweiligen VMs zu speichern.





Der Status der Failover- und Failback-Runbooks wird nun als konfiguriert aufgeführt. Failover- und Failback-Runbook-Gruppen werden paarweise erstellt, wobei dieselbe erste Gruppe von VMs und Einstellungen verwendet wird. Bei Bedarf können die Einstellungen einer Runbook-Gruppe individuell angepasst werden, indem Sie auf den entsprechenden Link Details klicken und Änderungen vornehmen.

Installieren Sie JetStream DR für AVS in der Private Cloud

Eine Best Practice für einen Recovery-Standort (AVS) ist die Erstellung eines Pilotlichtclusters mit drei Knoten im Voraus. Dadurch kann die Infrastruktur am Recovery-Standort vorkonfiguriert werden, einschließlich:

- Netzwerkzielsegmente, Firewalls, Services wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF-Volumes als Datastores und mehr

Jetstream DR unterstützt einen RTO-Modus von nahezu null für geschäftskritische Domänen. In diesen Domänen sollte der Ziel-Storage vorinstalliert sein. ANF ist in diesem Fall ein empfohlener Speichertyp.

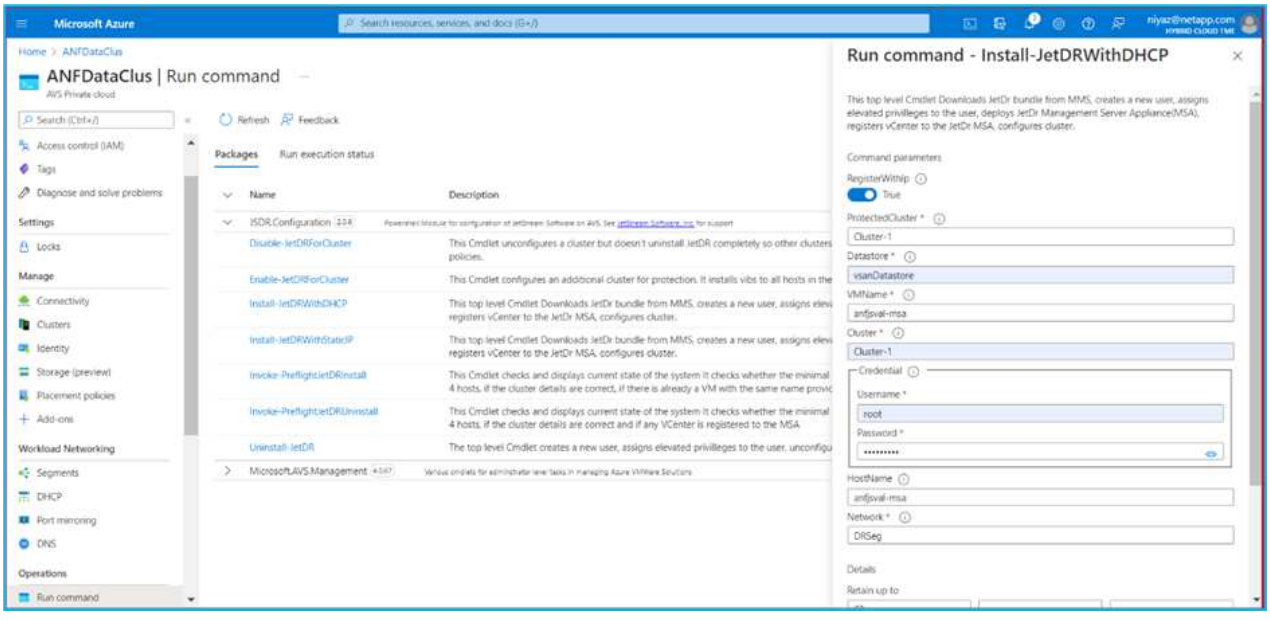
Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster entsprechend den Anforderungen vor Ort konfiguriert werden.

Je nach SLA- und RTO-Anforderungen können Sie einen kontinuierlichen Failover oder einen normalen (Standard-) Failover-Modus verwenden. Bei einer RTO von nahezu null sollten Sie am Recovery-Standort mit der kontinuierlichen Rehydrierung beginnen.

1. Verwenden Sie den Befehl Ausführen, um JetStream DR für AVS auf einer privaten Cloud der Azure VMware-Lösung zu installieren. Wählen Sie im Azure-Portal zur Azure VMware-Lösung die Private Cloud aus und wählen Sie Ausführen Command > Packages > JSDR.Configuration.

   Der CloudAdmin-Standardbenutzer der Azure VMware-Lösung verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Lösung ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Befehls Azure VMware Solution Run für JetStream DR.

   Der folgende Screenshot zeigt die Installation mithilfe einer DHCP-basierten IP-Adresse.

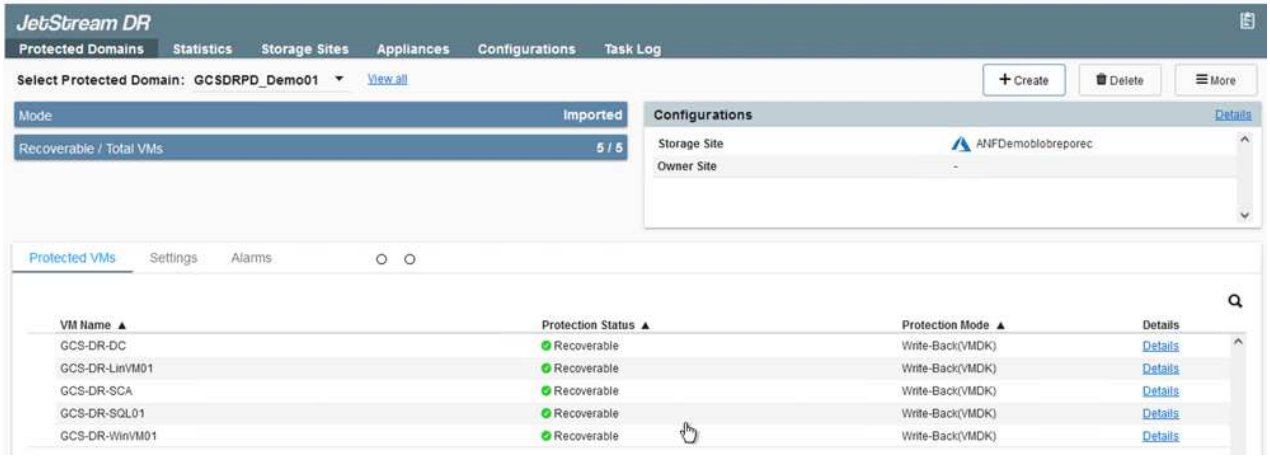


2. Nachdem die JetStream DR für AVS-Installation abgeschlossen ist, aktualisieren Sie den Browser.

Um auf die JetStream DR-UI zuzugreifen, wechseln Sie zum SDDC Datacenter > Configure > JetStream DR.

3. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
   a. Fügen Sie das Azure Blob Storage-Konto hinzu, das zur Sicherung des lokalen Clusters als Storage-Standort verwendet wurde, und starten Sie dann die Option Scan Domains.
   b. Wählen Sie im angezeigten Popup-Dialogfeld die zu importierende geschützte Domäne aus, und klicken Sie anschließend auf den Link Importieren.

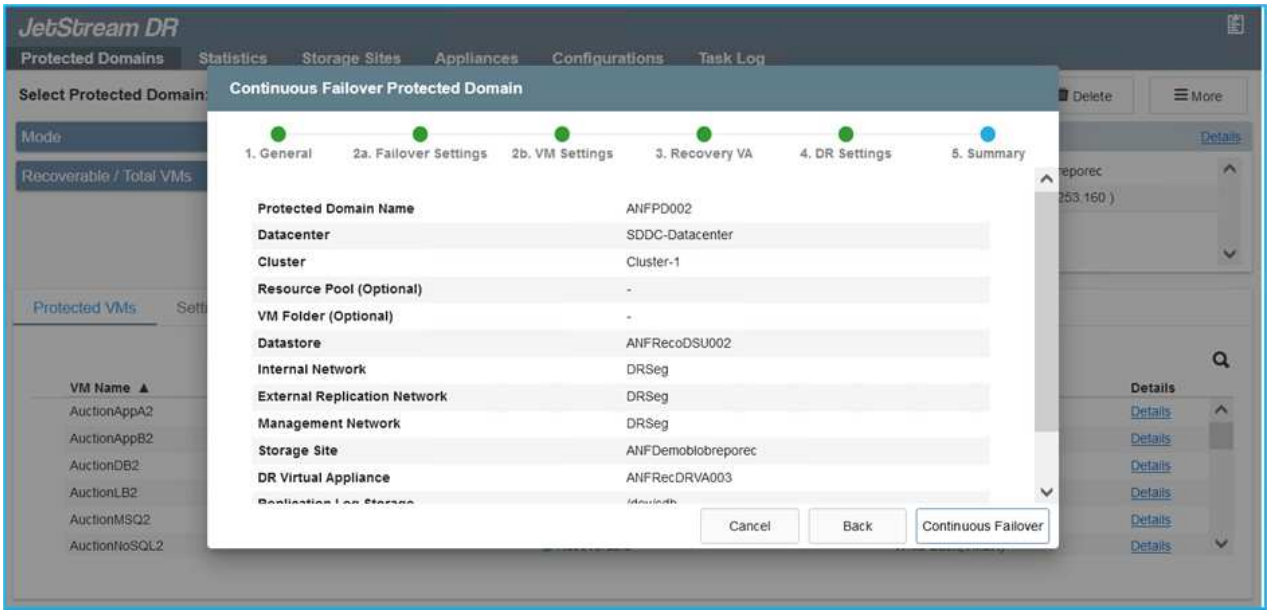
4. Die Domäne wird zur Wiederherstellung importiert. Gehen Sie auf die Registerkarte geschützte Domänen und überprüfen Sie, ob die vorgesehene Domäne ausgewählt wurde, oder wählen Sie die gewünschte aus dem Menü geschützte Domäne auswählen aus. Eine Liste der wiederherstellbaren VMs in der geschützten Domäne wird angezeigt.



5. Nachdem die geschützten Domains importiert wurden, sollten DRVA-Appliances bereitgestellt werden.

> Diese Schritte können auch mithilfe von CPT- erstellten Plänen automatisiert werden.

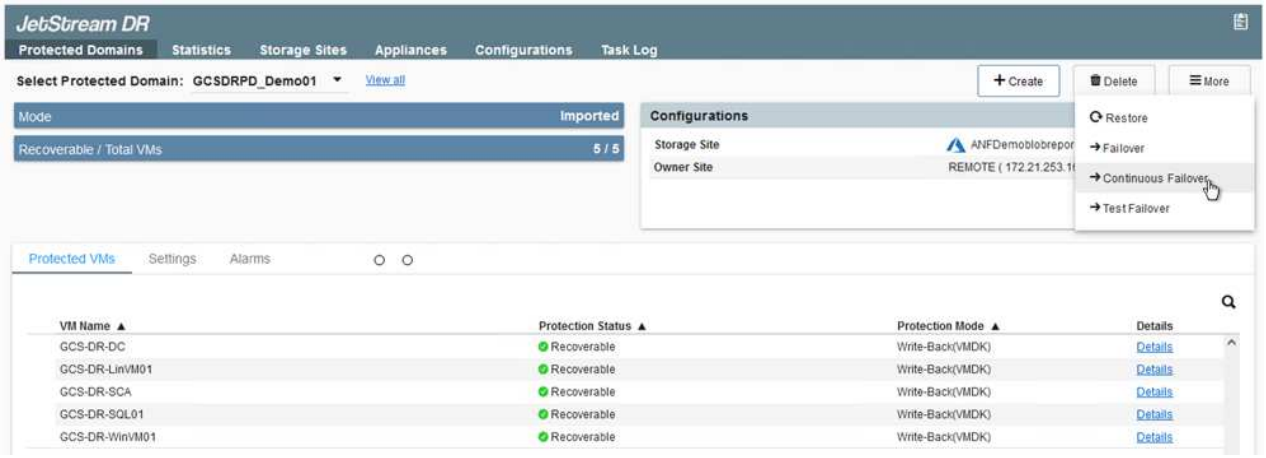
6. Verwenden von verfügbaren vSAN oder ANF-Datastores für Replizierungsprotokolle erstellen
7. Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery-VA, um einen ANF-Datenspeicher für VM-Platzierungen zu verwenden.



> Stellen Sie sicher, dass DHCP für das ausgewählte Segment aktiviert ist und genügend IP-Adressen verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen sich wiederherstellen. Jede wiederherzuckernde VM (einschließlich kontinuierlicher Rehydrierung) erfordert eine individuelle dynamische IP-Adresse. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

8. Wählen Sie die entsprechende Failover-Option (Continuous Failover oder Failover) aus. In diesem Beispiel wird die kontinuierliche Rehydrierung (kontinuierliches Failover) ausgewählt.

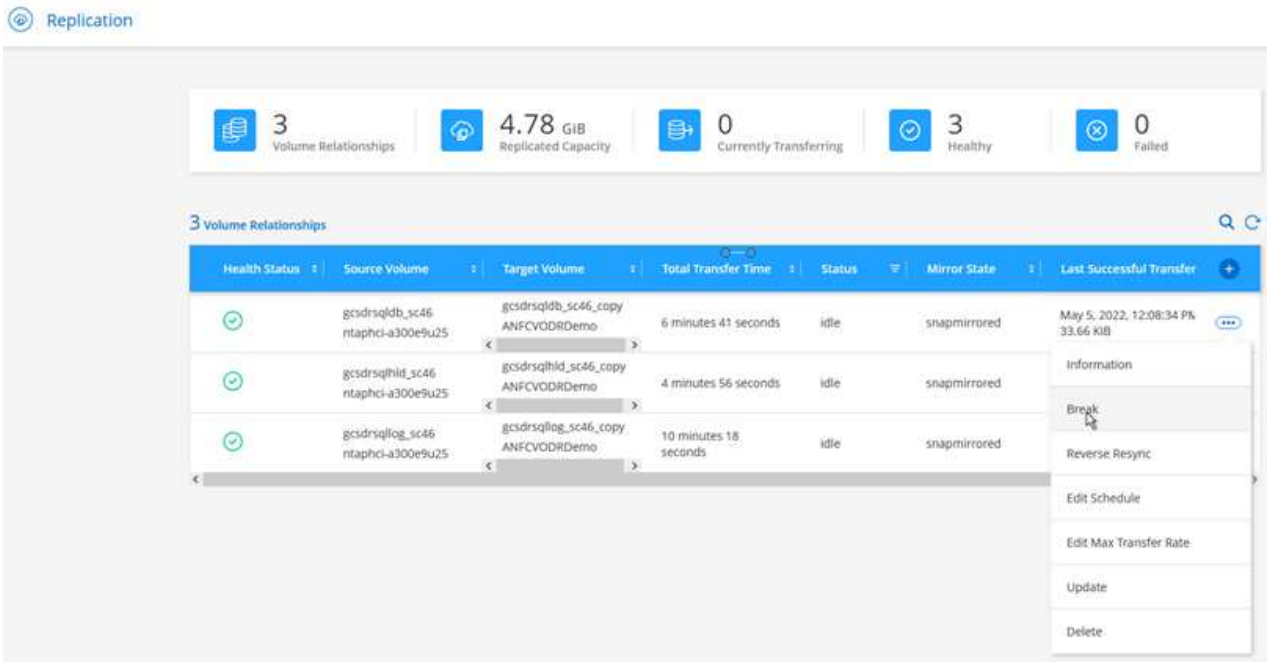
> Obwohl sich der kontinuierliche Failover- und Failover-Modus bei der Konfiguration unterscheiden, werden beide Failover-Modi mit den gleichen Schritten konfiguriert. Failover-Schritte werden als Reaktion auf ein Notfall konfiguriert und durchgeführt. Ein kontinuierlicher Failover kann jederzeit konfiguriert werden und dann im Hintergrund während des normalen Systembetriebs ausgeführt werden. Nach einem Zwischenfall wird der fortlaufende Failover abgeschlossen, sodass die Eigentümerschaft der geschützten VMs direkt auf den Recovery-Standort übertragen wird (RTO von nahezu null).

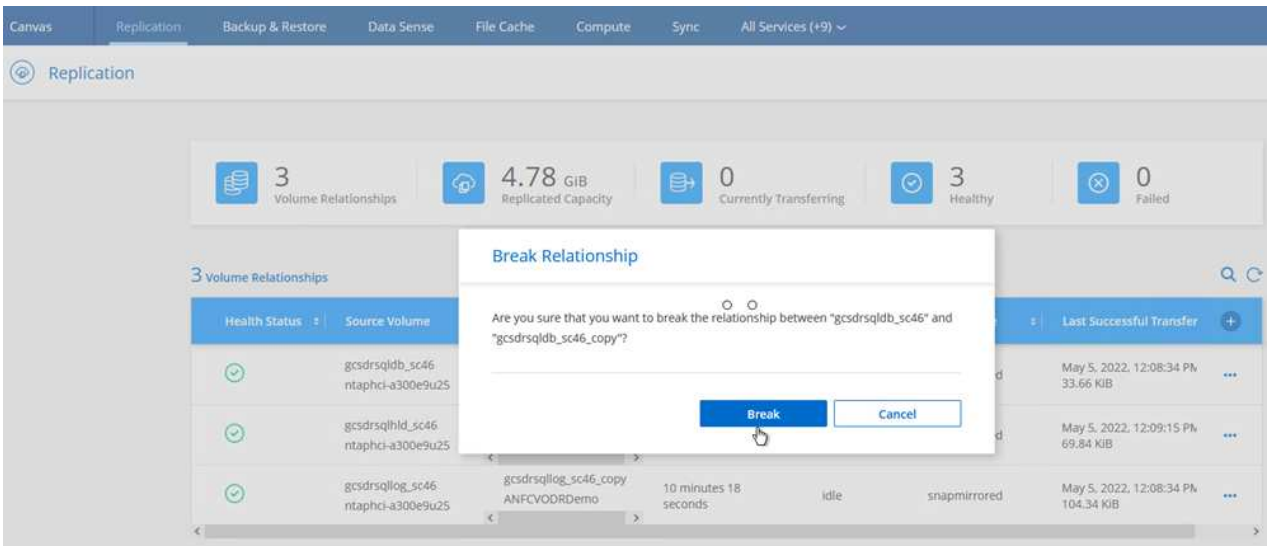


Der kontinuierliche Failover-Prozess beginnt und der Fortschritt kann über die UI überwacht werden. Durch Klicken auf das blaue Symbol im Abschnitt „Aktueller Schritt“ wird ein Popup-Fenster angezeigt, in dem Details zum aktuellen Schritt des Failover-Prozesses angezeigt werden.

Failover und Failback

1. Nach einem Ausfall im geschützten Cluster der lokalen Umgebung (teilweiser oder kompletter Ausfall) können Sie das Failover für VMs auslösen. Dazu verwenden Sie Jetstream, nachdem die SnapMirror Beziehung für die jeweiligen Applikations-Volumes unterbrochen wurde.

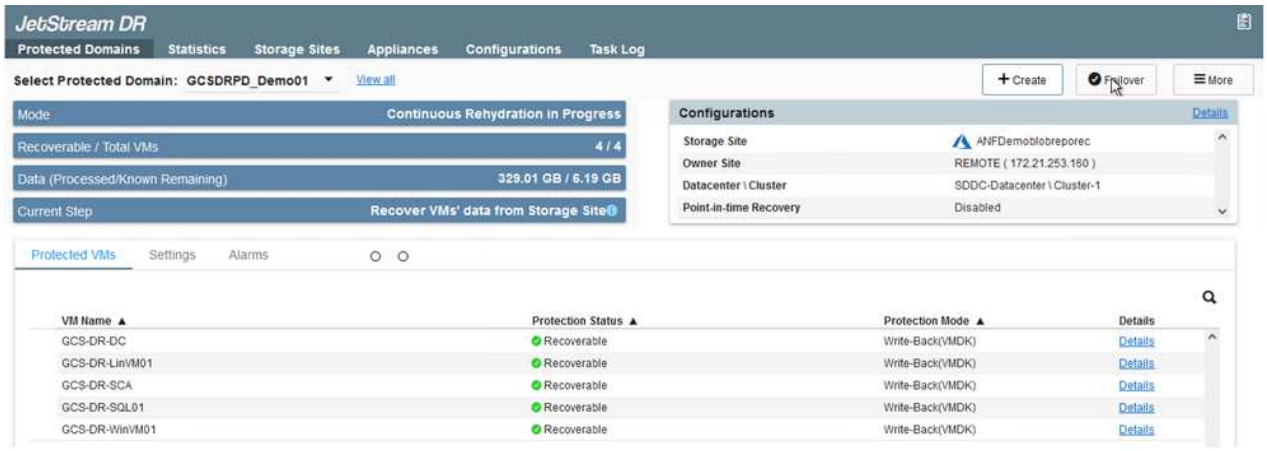


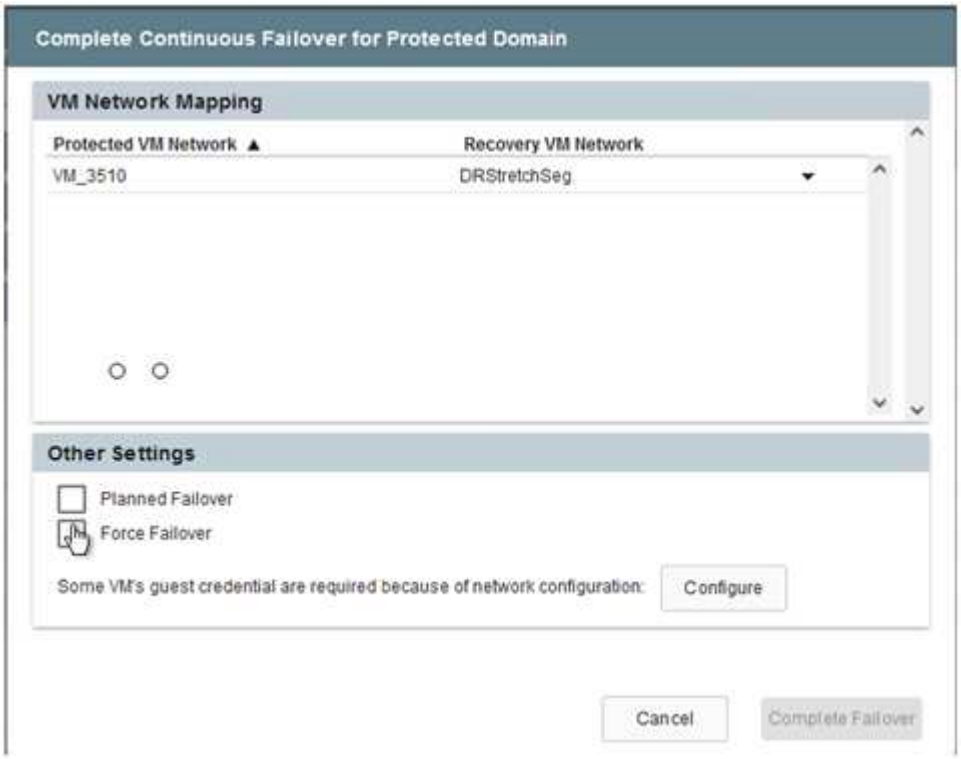


> Dieser Schritt kann zur Erleichterung des Recovery-Prozesses einfach automatisiert werden.

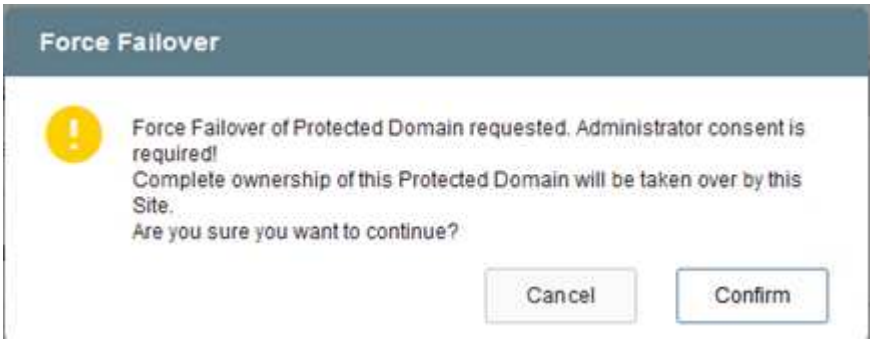
2. Greifen Sie auf die Jetstream UI auf dem AVS SDDC (Zielseite) zu und lösen Sie die Failover-Option aus, um den Failover abzuschließen. Die Taskleiste zeigt den Fortschritt für Failover-Aktivitäten an.

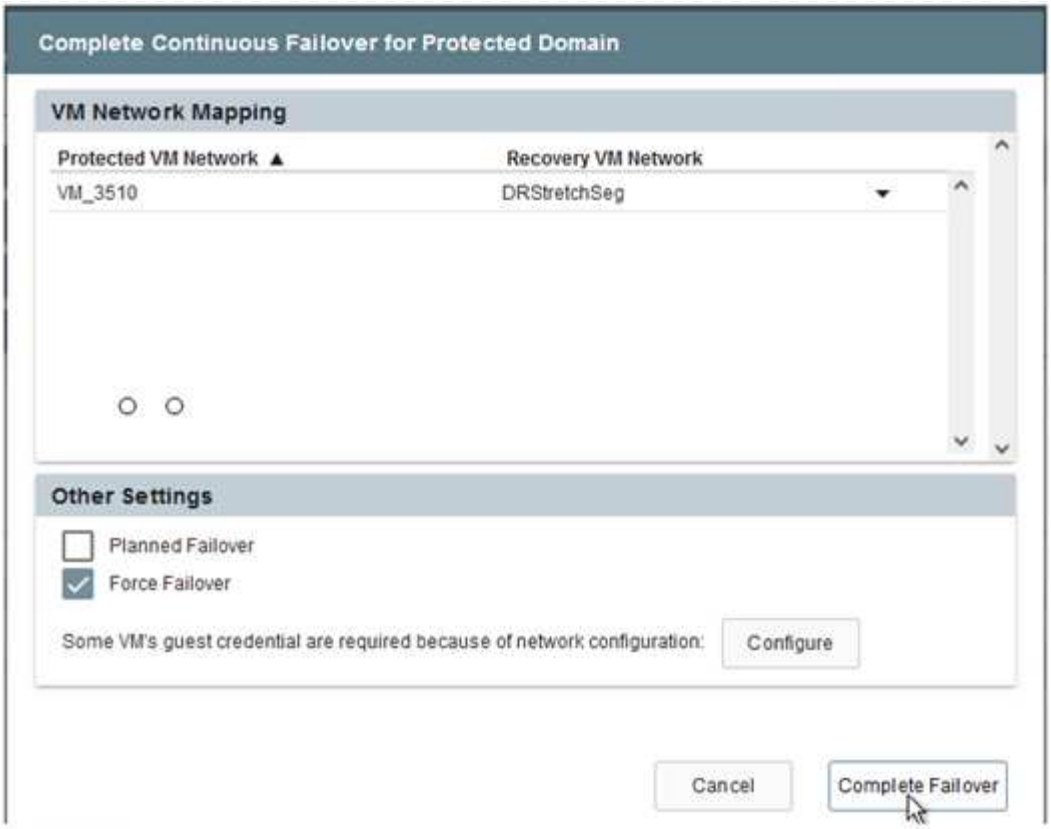
   Im Dialogfeld, das beim Abschluss des Failover angezeigt wird, kann die Failover-Aufgabe als geplant oder als erzwungen angegeben werden.





Erzwungenes Failover geht davon aus, dass auf den primären Standort nicht mehr zugegriffen werden kann und die Eigentümerschaft der geschützten Domäne direkt vom Recovery-Standort übernommen werden muss.



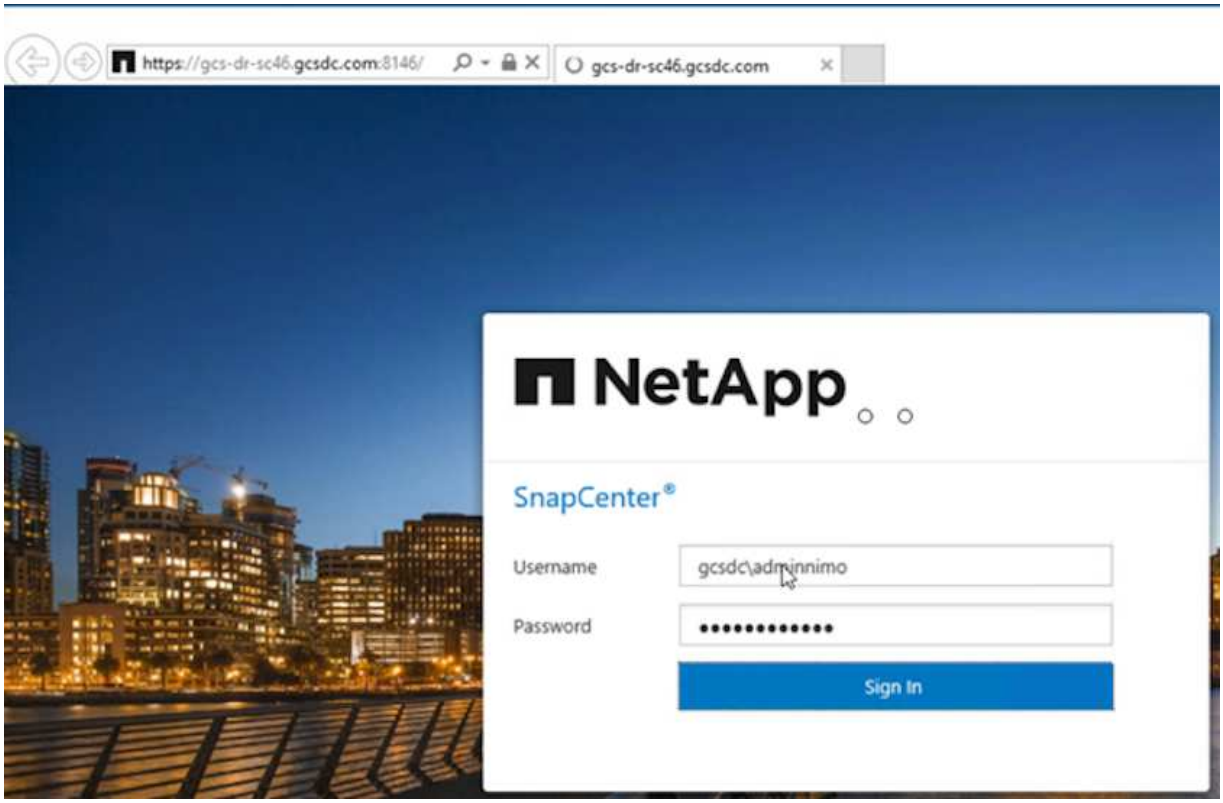


3. Nachdem der kontinuierliche Failover abgeschlossen ist, wird eine Meldung angezeigt, die den Abschluss der Aufgabe bestätigt. Nach Abschluss der Aufgabe greifen Sie auf die wiederhergestellten VMs zu, um ISCSI- oder NFS-Sitzungen zu konfigurieren.

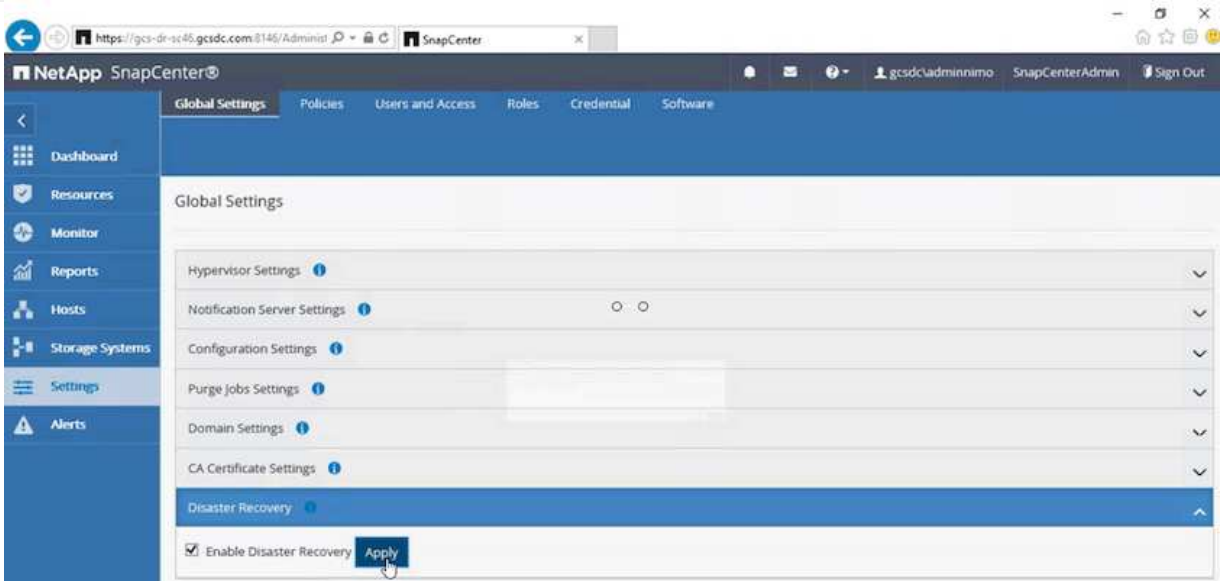
Der Failover-Modus wird in Failover ausgeführt, und der Status der VM ist wiederherstellbar. Alle VMs der geschützten Domäne werden jetzt am Recovery-Standort in dem von den Failover-Runbook-Einstellungen angegebenen Zustand ausgeführt.

Um die Failover-Konfiguration und die Infrastruktur zu überprüfen, kann JetStream DR im Testmodus (Option Test Failover) betrieben werden, um die Wiederherstellung von Virtual Machines und deren Daten vom Objektspeicher in einer Test-Recovery-Umgebung zu beobachten. Wenn ein Failover-Verfahren im Testmodus ausgeführt wird, ähnelt sein Vorgang einem tatsächlichen Failover-Prozess.

4. Sobald die Virtual Machines wiederhergestellt sind, wird Disaster Recovery für Storage auf dem Gast-Storage eingesetzt. Um diesen Prozess zu demonstrieren, wird SQL-Server in diesem Beispiel verwendet.
5. Melden Sie sich bei der wiederhergestellten SnapCenter-VM auf dem AVS SDDC an und aktivieren Sie den DR-Modus.
   a. Greifen Sie über Browsern auf die SnapCenter-Benutzeroberfläche zu.



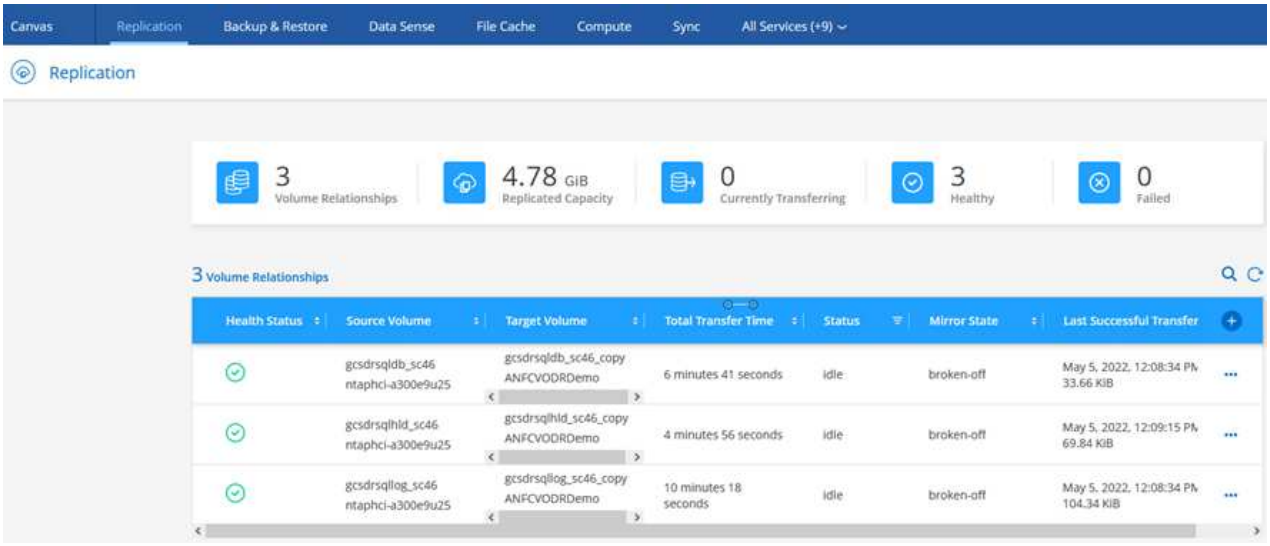
   b. Navigieren Sie auf der Seite Einstellungen zu Einstellungen > Globale Einstellungen > Disaster Recovery.
   c. Wählen Sie Disaster Recovery Aktivieren.
   d. Klicken Sie Auf Anwenden.



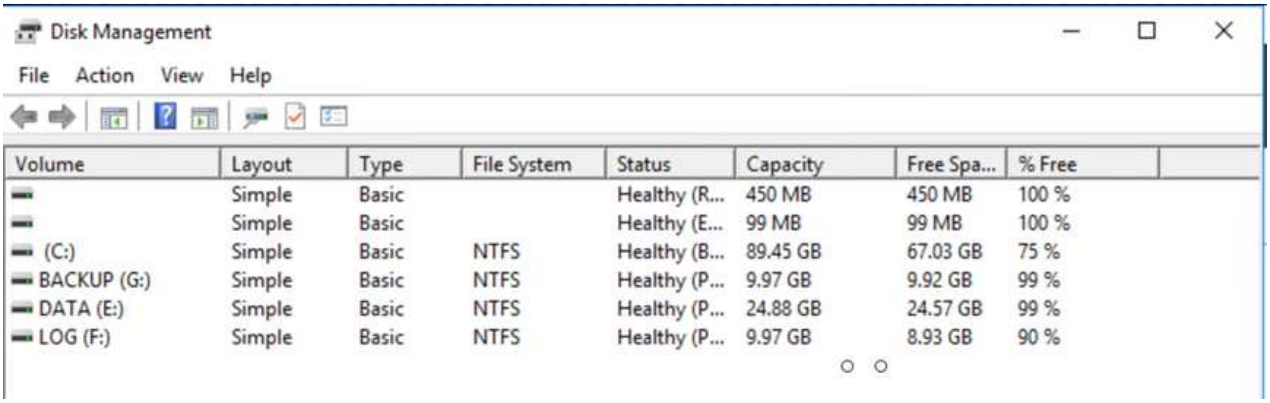
e. Überprüfen Sie, ob der DR-Job aktiviert ist, indem Sie auf Überwachen > Jobs klicken.

> Für das Storage Disaster Recovery sollte NetApp SnapCenter 4.6 oder höher verwendet werden. Frühere Versionen sollten applikationskonsistente Snapshots (replizierte mit SnapMirror) verwenden und ein manuelles Recovery ausführen, falls frühere Backups am Disaster Recovery-Standort wiederhergestellt werden müssen.

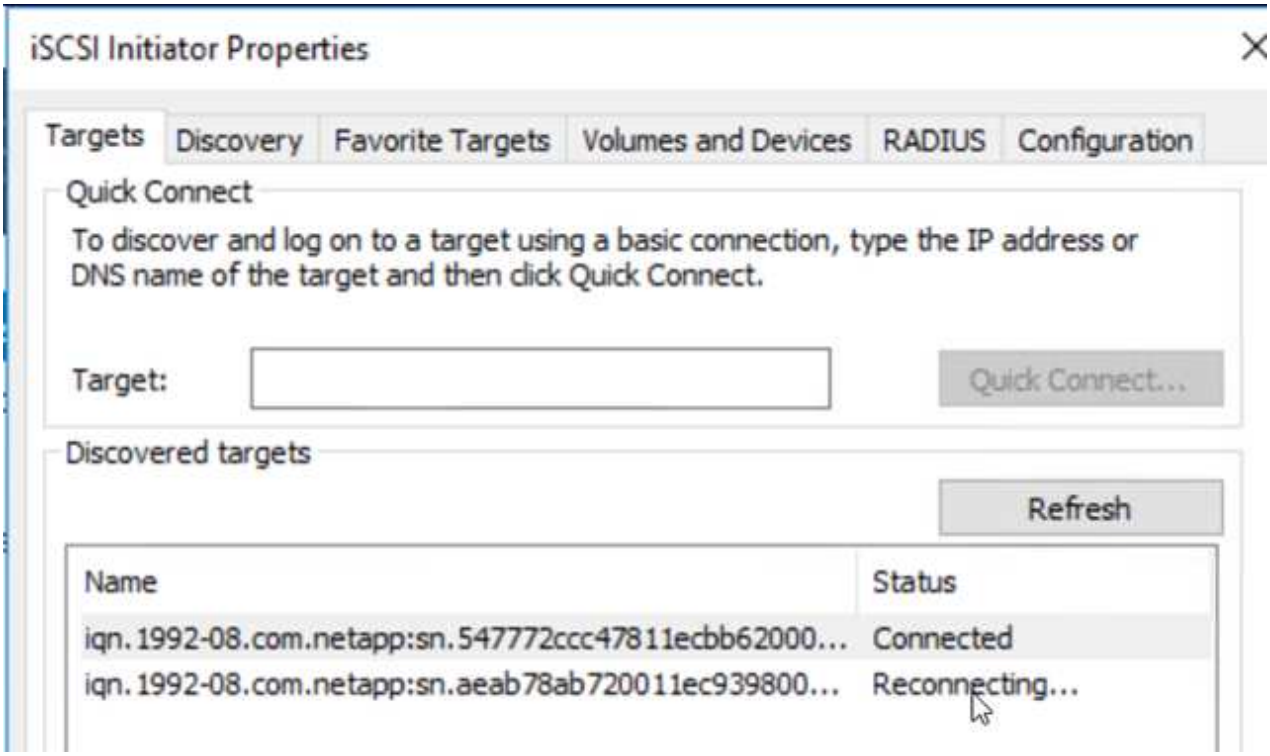
6. Stellen Sie sicher, dass die SnapMirror Beziehung beschädigt ist.



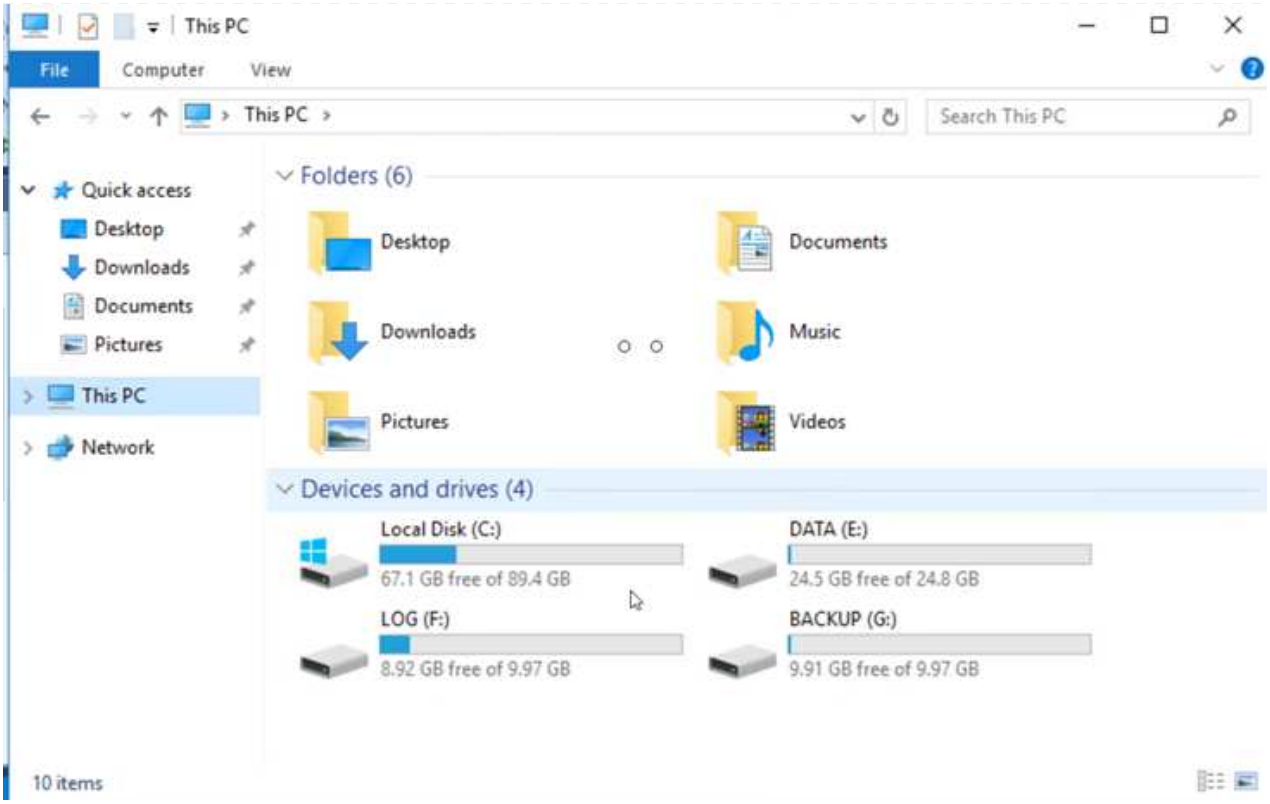
7. Verbinden Sie die LUN aus Cloud Volumes ONTAP mit der wiederhergestellten SQL Gast-VM mit gleichen Laufwerksbuchstaben.



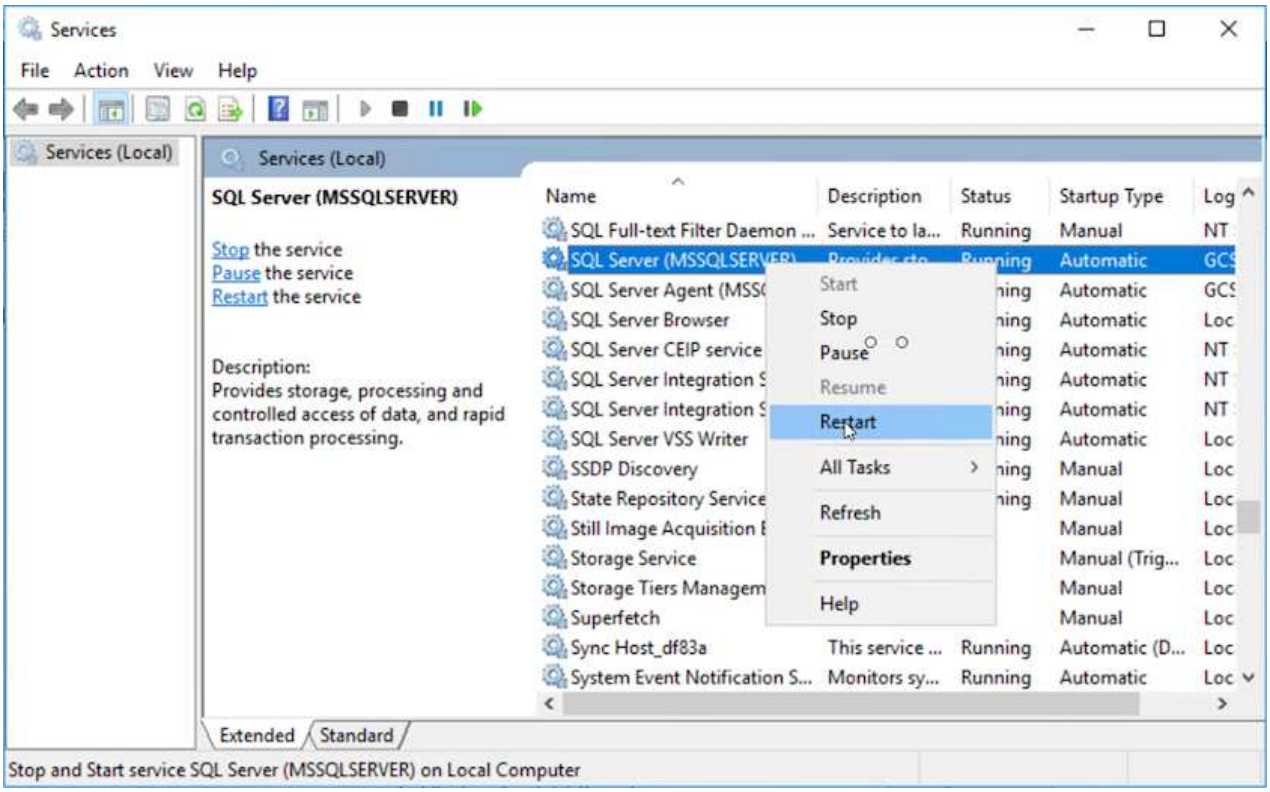
8. Öffnen Sie den iSCSI-Initiator, löschen Sie die vorherige getrennte Sitzung und fügen Sie das neue Ziel zusammen mit Multipath für die replizierten Cloud Volumes ONTAP Volumes hinzu.



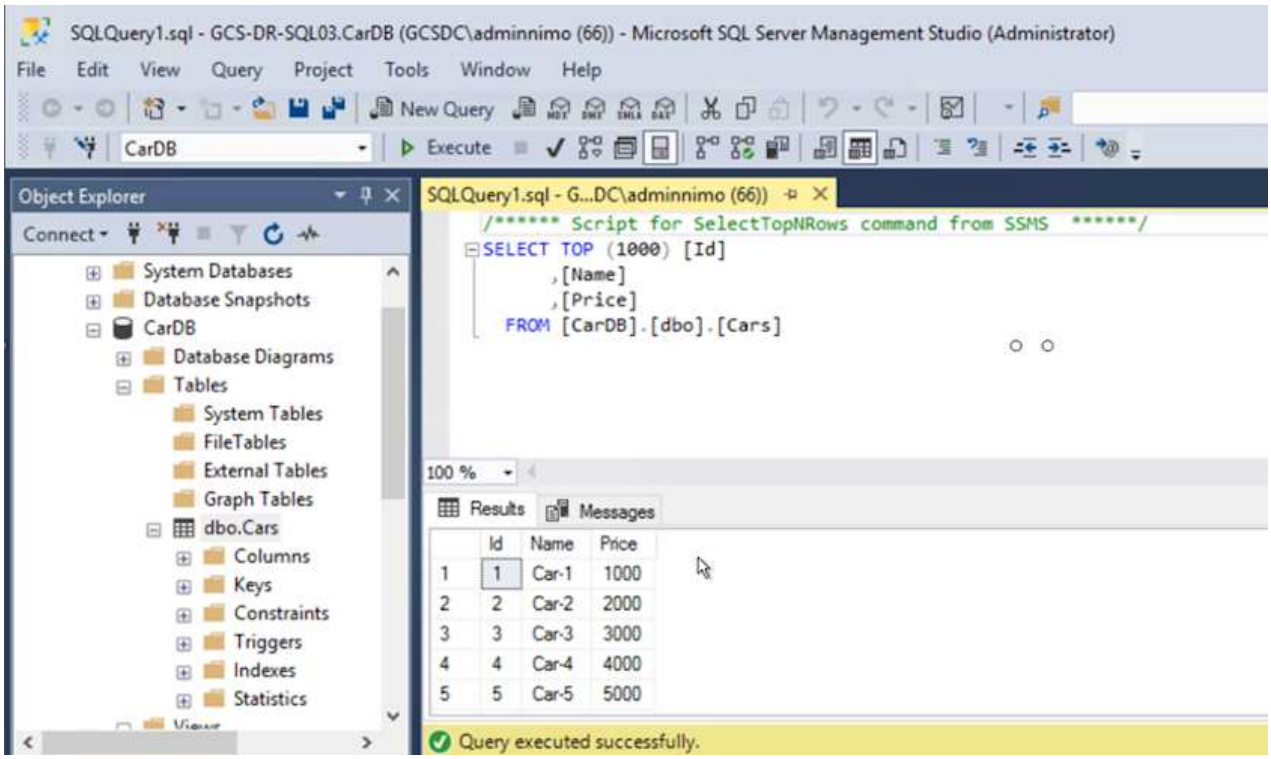
9. Stellen Sie sicher, dass alle Laufwerke mit denselben Laufwerksbuchstaben verbunden sind, die vor DR verwendet wurden.



10. Starten Sie den MSSQL-Serverdienst neu.



11. Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.



Hängen Sie im Fall von NFS die Volumes mit dem Mount-Befehl an, und aktualisieren Sie die `/etc/fstab` Einträge.

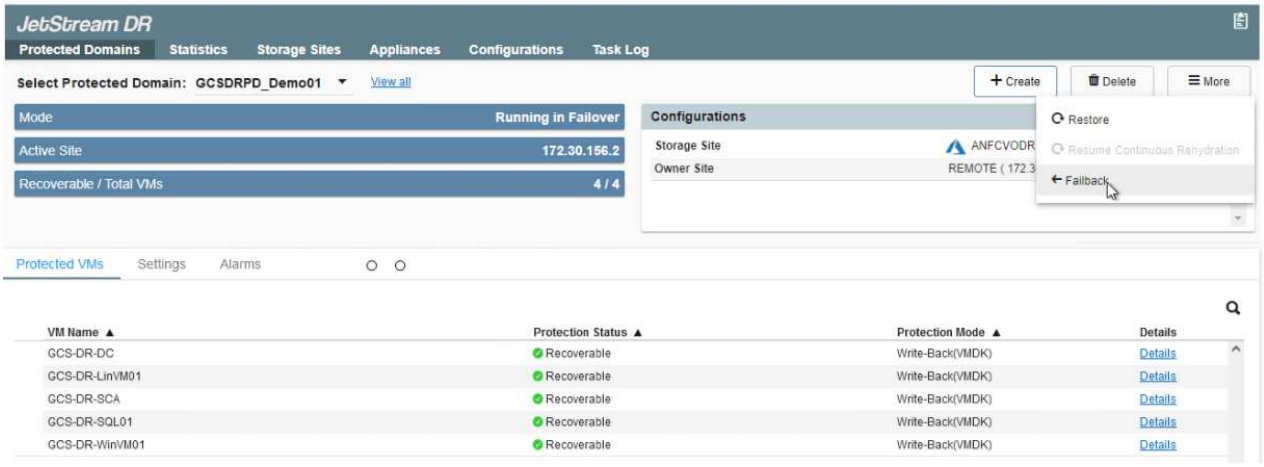
An diesem Punkt können Betriebsabläufe ausgeführt werden und der Geschäftsbetrieb normal weiterläuft.

Am NSX-T-Ende kann ein separates, dediziertes Tier-1 Gateway zur Simulation von Failover-Szenarien erstellt werden. So ist sichergestellt, dass alle Workloads miteinander kommunizieren können, dass jedoch kein Traffic in die bzw. aus der Umgebung geleitet werden kann. So können alle Triage-, Containment- oder Härteaufgaben ohne das Risiko einer Kreuzkontamination durchgeführt werden. Dieser Vorgang ist außerhalb des Anwendungsbereichs dieses Dokuments, kann aber problemlos zur Simulation der Isolation durchgeführt werden.

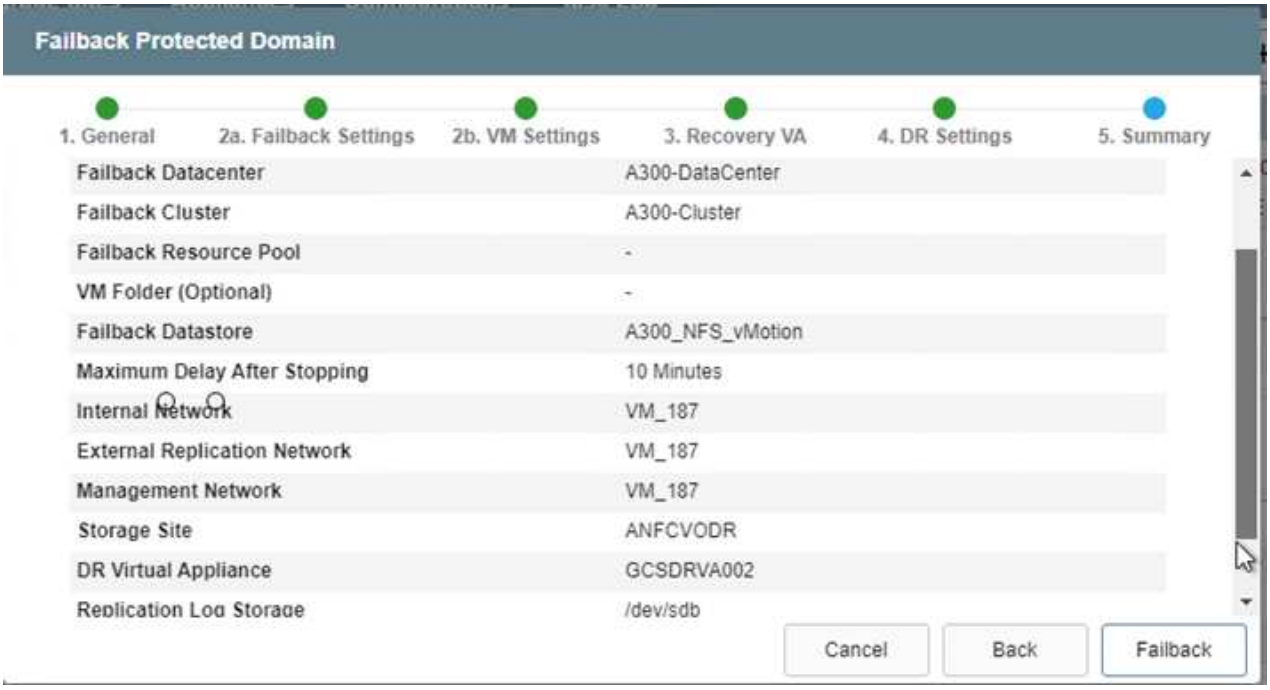
Wenn der primäre Standort wieder in Betrieb ist, können Sie ein Failback durchführen. Die VM-Sicherung wird durch Jetstream fortgesetzt, und die SnapMirror Beziehung muss umgekehrt werden.

1. Wiederherstellung der lokalen Umgebung Je nach Art des Notfalleinfalls sind möglicherweise die Wiederherstellung und/oder Überprüfung der Konfiguration des geschützten Clusters erforderlich. Falls erforderlich, muss die JetStream DR-Software möglicherweise erneut installiert werden.
2. Greifen Sie auf die wiederhergestellte On-Premises-Umgebung zu, rufen Sie die Jetstream DR UI auf und wählen Sie die entsprechende geschützte Domäne aus. Nachdem der geschützte Standort für Failback bereit ist, wählen Sie die Failback-Option in der UI aus.

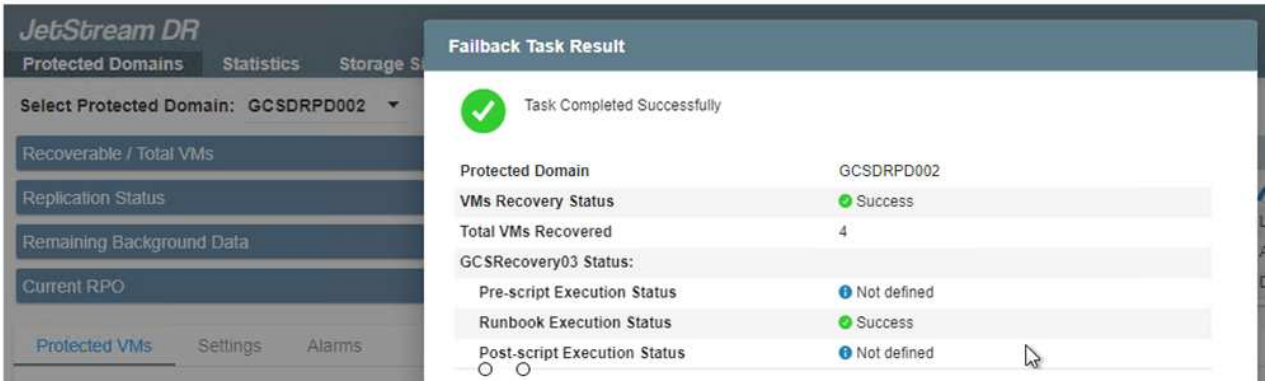
Mit dem CPT-generierten Failback-Plan kann außerdem die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher in die ursprüngliche VMware Umgebung initiiert werden.



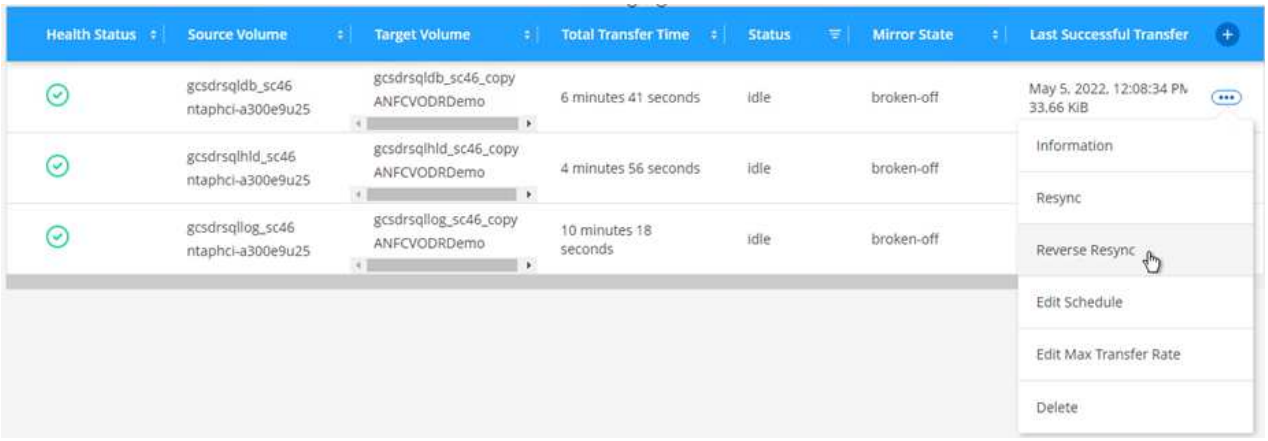
Geben Sie die maximale Verzögerung an, nachdem Sie die VMs am Recovery-Standort angehalten und am geschützten Standort neu gestartet haben. Die zum Abschluss dieses Prozesses erforderliche Zeit umfasst das Abschließen der Replizierung nach dem Stoppen von Failover-VMs, die zum Reinigen des Recovery-Standorts benötigte Zeit und die Zeit zur Wiederherstellung von VMs am geschützten Standort. NetApp empfiehlt 10 Minuten.

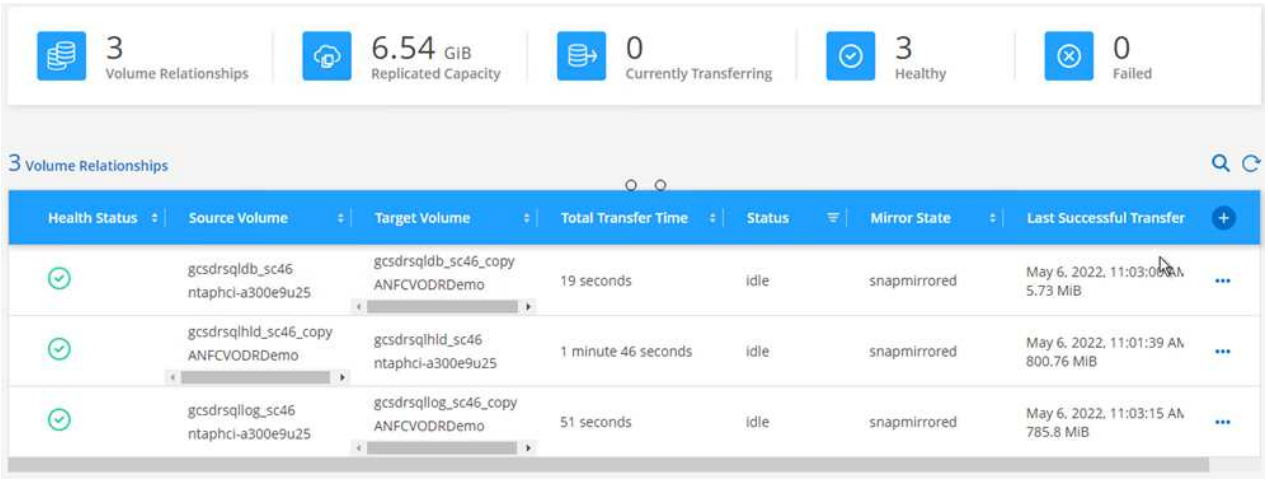


3. Schließen Sie den Failback-Prozess ab, und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

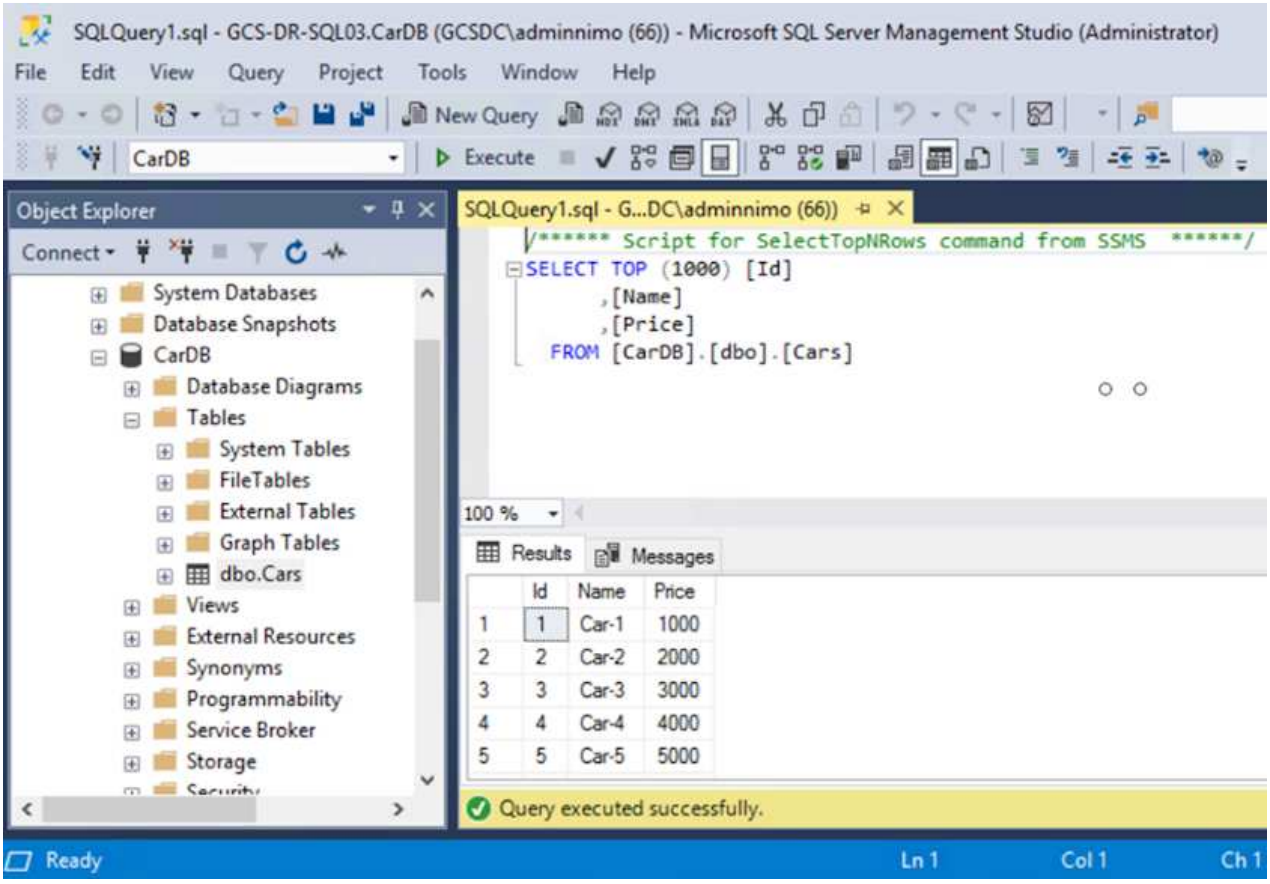


4. Nachdem die VMs wiederhergestellt wurden, trennen Sie den sekundären Storage vom Host und stellen eine Verbindung zum primären Storage her.





5. Starten Sie den MSSQL-Serverdienst neu.
6. Vergewissern Sie sich, dass die SQL-Ressourcen wieder online sind.



Für ein Failback auf den primären Storage sollten Sie sicherstellen, dass die Beziehungsrichtung vor dem Failover unverändert bleibt, indem Sie einen umgekehrten Resynchronisierungsvorgang durchführen.

Um die Rollen des primären und sekundären Storage nach der umgekehrten Resynchronisierung beizubehalten, führen Sie den umgekehrten Resync-Vorgang erneut aus.

Dieser Prozess gilt für andere Applikationen wie Oracle, ähnliche Datenbankumgebungen und andere Applikationen, die mit Gast-vernetztem Storage verwenden.

Testen Sie wie immer die Schritte zur Wiederherstellung der kritischen Workloads, bevor Sie sie in die Produktionsumgebung portieren.

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.

- Keine Replizierungsunterbrechungen während der DR-Test-Workflows
- Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests

- CPU- und RAM-Optimierung können die Cloud-Kosten senken, indem Recovery auf kleinere Computing-Cluster ermöglicht wird.

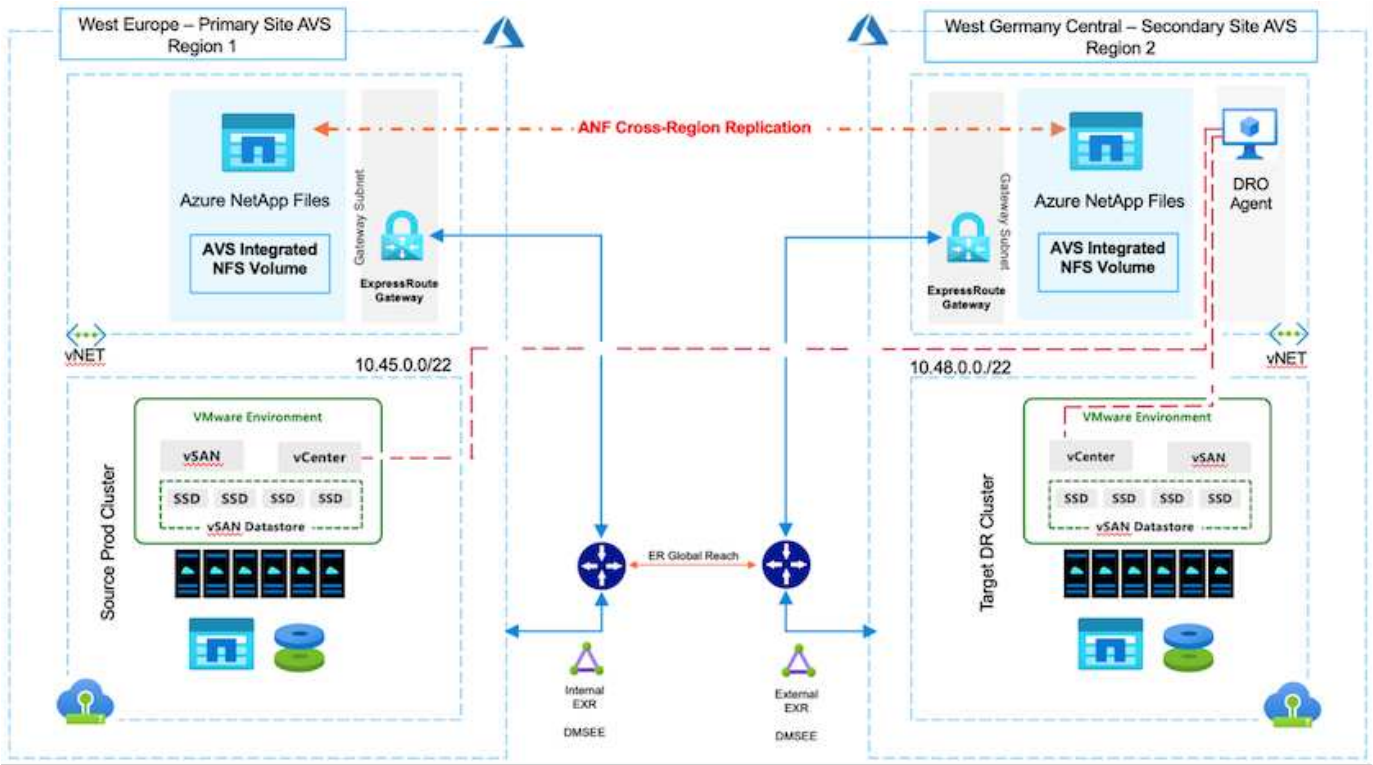
TR-4955: Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware Solution (AVS)

Autor(en): Niyaz Mohamed, NetApp Solutions Engineering

Überblick

Disaster Recovery mit Replizierung auf Blockebene zwischen Regionen in der Cloud ist eine ausfallsichere und kostengünstige Möglichkeit, um Workloads vor Standortausfällen und Datenbeschädigung (z. B. Ransomware) zu schützen. Mit der regionsübergreifenden Volume-Replizierung über Azure NetApp Files (ANF) können VMware-Workloads, die auf einem AVS-Standort (Azure VMware Solution) mit Azure NetApp Files Volumes als NFS-Datastore auf dem primären AVS-Standort ausgeführt werden, auf einen designierten sekundären AVS-Standort in der Zielwiederherstellungsregion repliziert werden.

Disaster Recovery Orchestrator (DRO) (eine skriptbasierte Lösung mit einer Benutzeroberfläche) kann verwendet werden, um Workloads, die von einem AVS-SDDC zum anderen repliziert werden, nahtlos wiederherzustellen. DRO automatisiert die Recovery, indem Replikations-Peering gebrochen und das Ziel-Volume dann als Datastore gemountet wird. Dies geschieht durch VM-Registrierung in AVS, um Netzwerkzuordnungen direkt auf NSX-T (in allen AVS Private Clouds enthalten) zu ermöglichen.



Voraussetzungen und allgemeine Empfehlungen

- Vergewissern Sie sich, dass Sie die regionsübergreifende Replikation aktiviert haben, indem Sie Replikations-Peering erstellen. Siehe "Volume-Replizierung für Azure NetApp Files erstellen".

- Sie müssen ExpressRoute Global Reach zwischen den Private Clouds der Quell- und Ziellösung von Azure VMware konfigurieren.
- Sie müssen über einen Dienstprinzipal verfügen, der auf Ressourcen zugreifen kann.
- Die folgende Topologie wird unterstützt: Primärer AVS-Standort zum sekundären AVS-Standort.
- Konfigurieren Sie die "Replizierung" Planen Sie für jedes Volume entsprechend den Geschäftsanforderungen und der Datenänderungsrate ein.

Kaskadierung und Fan-in- und Fan-out-Topologien werden nicht unterstützt.

Erste Schritte

Implementieren Sie die Azure-VMware-Lösung

Der "Azure VMware Lösung" (AVS) ist ein Hybrid-Cloud-Service mit voll funktionsfähigen VMware SDDCs in einer Microsoft Azure Public Cloud. AVS ist eine Lösung eines Erstanbieters, die vollständig von Microsoft verwaltet und unterstützt wird und von VMware überprüft wurde, die eine Azure-Infrastruktur nutzt. Daher erhalten Kunden VMware ESXi für die Compute-Virtualisierung, vSAN für hyperkonvergenten Storage und NSX für Netzwerk und Sicherheit. Gleichzeitig profitieren sie von der globalen Präsenz und den erstklassigen Datacenter-Einrichtungen von Microsoft Azure sowie der Nähe zum umfassenden Ecosystem nativer Azure-Services und -Lösungen. Eine Kombination aus Azure VMware Solution SDDC und Azure NetApp Files bietet die beste Performance bei minimaler Netzwerklatenz.

Gehen Sie wie folgt vor, um eine AVS Private Cloud auf Azure zu konfigurieren "Verlinken" Zu NetApp-Dokumentation und in diesem "Verlinken" Für Microsoft-Dokumentation. Für DR-Zwecke kann eine Pilotumgebung mit minimaler Konfiguration verwendet werden. Dieses Setup enthält nur Kernkomponenten zur Unterstützung kritischer Applikationen. Es kann horizontal skalierbar sein und weitere Hosts aufbauen, um den Großteil der Auslastung bei einem Failover zu übernehmen.

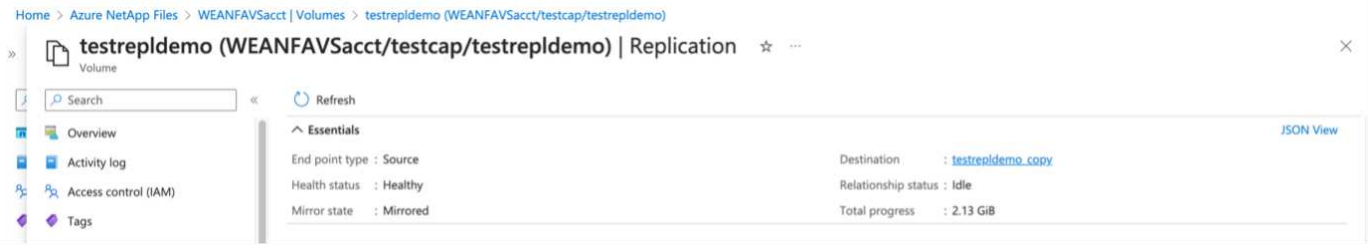
In der ersten Version unterstützt DRO einen vorhandenen AVS SDDC-Cluster. Die Erstellung eines On-Demand SDDC wird in einer kommenden Version verfügbar sein.

Bereitstellung und Konfiguration von Azure NetApp Files

"Azure NetApp Dateien" Der hochperformante gemessene File-Storage-Service der Enterprise-Klasse. Befolgen Sie die hier beschriebenen Schritte "Verlinken" Die Bereitstellung und Konfiguration von Azure NetApp Files als NFS-Datastore zur Optimierung von AVS Private-Cloud-Implementierungen.

Volume-Replizierung für Datastore-Volumes mit Azure NetApp Files erstellen

Der erste Schritt besteht darin, regionsübergreifende Replikation für die gewünschten Datastore Volumes vom primären AVS-Standort zum sekundären AVS-Standort mit den entsprechenden Frequenzen und Aufbewahrungen einzurichten.



Befolgen Sie die hier beschriebenen Schritte "Verlinken" Zur Einrichtung einer regionsübergreifenden Replikation durch Erstellen von Replikations-Peering. Das Service-Level für den Zielkapazitätspool kann mit dem des Quell-Kapazitäts-Pools übereinstimmen. Für diesen speziellen Anwendungsfall können Sie jedoch das Standard-Service-Level und dann auswählen "Ändern Sie den Service-Level" Im Falle einer echten Katastrophe oder DR-Simulationen.

Eine regionsübergreifende Replikationsbeziehung ist Voraussetzung und muss zuvor erstellt werden.

DRO-Installation

Um mit DRO zu beginnen, verwenden Sie das Ubuntu-Betriebssystem auf der zugewiesenen virtuellen Azure-Maschine und stellen Sie sicher, dass Sie die Voraussetzungen erfüllen. Installieren Sie dann das Paket.

Voraussetzungen:

- Dienstprinzipal, das auf Ressourcen zugreifen kann.
- Stellen Sie sicher, dass entsprechende Konnektivität mit den SDDC Quell- und Ziel-Instanzen und den Azure NetApp Files Instanzen besteht.
- DNS-Auflösung sollte vorhanden sein, wenn Sie DNS-Namen verwenden. Verwenden Sie andernfalls die IP-Adressen für vCenter.

OS-Anforderungen:

- Ubuntu Focal 20.04 (LTS)die folgenden Pakete müssen auf der zugewiesenen virtuellen Agent-Maschine installiert werden:
- Docker
- Docker – Komposition
- JqChange `docker.sock` Zu dieser neuen Berechtigung: `sudo chmod 666 /var/run/docker.sock`.

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

Dies sind die Schritte:

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

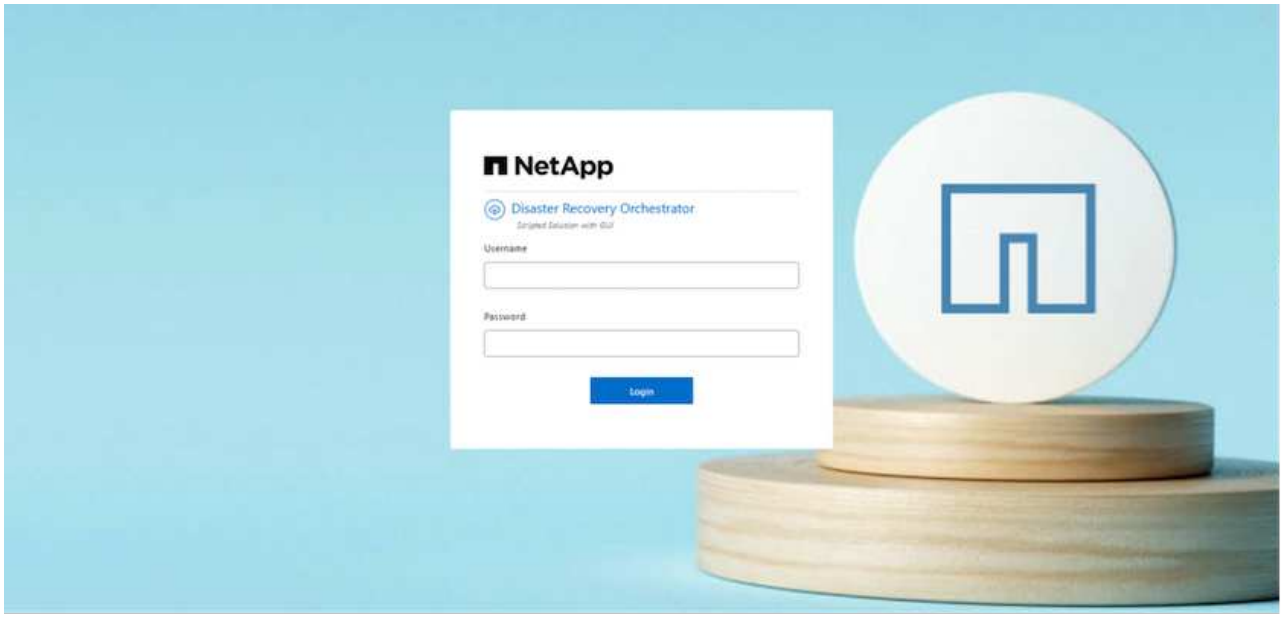
```
git clone https://github.com/NetApp/DRO-Azure.git
```

Der Agent muss in der sekundären AVS-Standortregion oder in der primären AVS-Standortregion in einer separaten AZ als dem SDDC 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 draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Greifen Sie mit den folgenden Anmeldedaten auf die UI zu:
    - Benutzername: `admin`
    - Kennwort: `admin`



DRO-Konfiguration

Nachdem Azure NetApp Files und AVS ordnungsgemäß konfiguriert wurden, können Sie mit der Konfiguration von DRO beginnen, um die Wiederherstellung von Workloads vom primären AVS-Standort zum sekundären AVS-Standort zu automatisieren. NetApp empfiehlt, den DRO-Agent am sekundären AVS-Standort bereitzustellen und die ExpressRoute Gateway-Verbindung zu konfigurieren, damit der DRO-Agent über das Netzwerk mit den entsprechenden AVS- und Azure NetApp Files-Komponenten kommunizieren kann.

Der erste Schritt besteht darin, Anmeldeinformationen hinzuzufügen. FÜR DIE Erkennung von Azure NetApp Files und der Azure VMware-Lösung ist DIE DRO-Berechtigung erforderlich. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie eine Azure Active Directory (AD)-Anwendung erstellen und einrichten und die Azure-Anmeldeinformationen erhalten, die DRO benötigt. Sie müssen den Service-Prinzipal an Ihr Azure-Abonnement binden und ihm eine benutzerdefinierte Rolle zuweisen, die über die entsprechenden erforderlichen Berechtigungen verfügt. Wenn Sie Quell- und Zielumgebungen hinzufügen, werden Sie aufgefordert, die Anmeldeinformationen auszuwählen, die dem Dienstprinzipal zugeordnet sind. Sie müssen diese Anmeldeinformationen zu DRO hinzufügen, bevor Sie auf Neuen Standort hinzufügen klicken können.

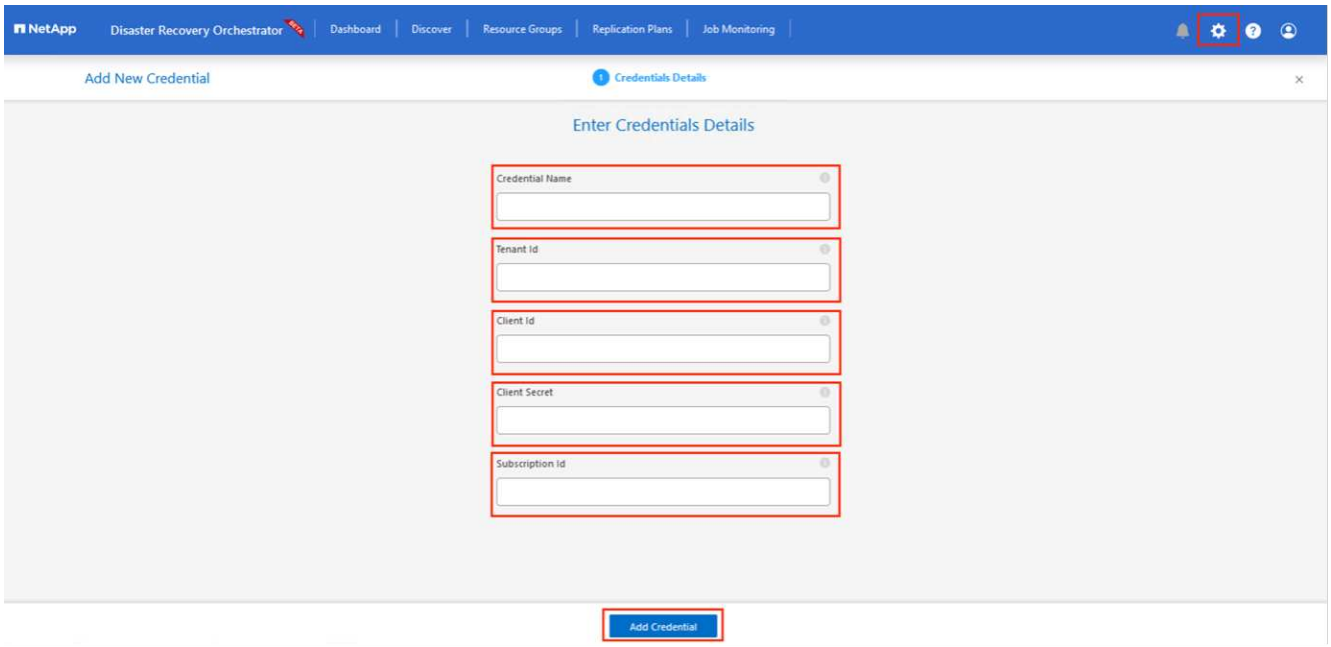
Um diesen Vorgang auszuführen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie DRO in einem unterstützten Browser und verwenden Sie den Standardbenutzernamen und das Standardpasswort (`admin`/`admin`). Das Passwort kann nach der ersten Anmeldung mit der Option Passwort ändern zurückgesetzt werden.
2. Klicken Sie oben rechts auf der DRO-Konsole auf das Symbol **Einstellungen** und wählen Sie **Anmeldeinformationen** aus.
3. Klicken Sie auf Neue Anmeldedaten hinzufügen, und befolgen Sie die Schritte im Assistenten.
4. Geben Sie zum Definieren der Anmeldeinformationen Informationen über den Azure Active Directory-Dienstprinzipal ein, der die erforderlichen Berechtigungen gewährt:

- Name der Anmeldeinformationen
- Mandanten-ID
- Client-ID
- Kundengeheimnis
- Abonnement-ID

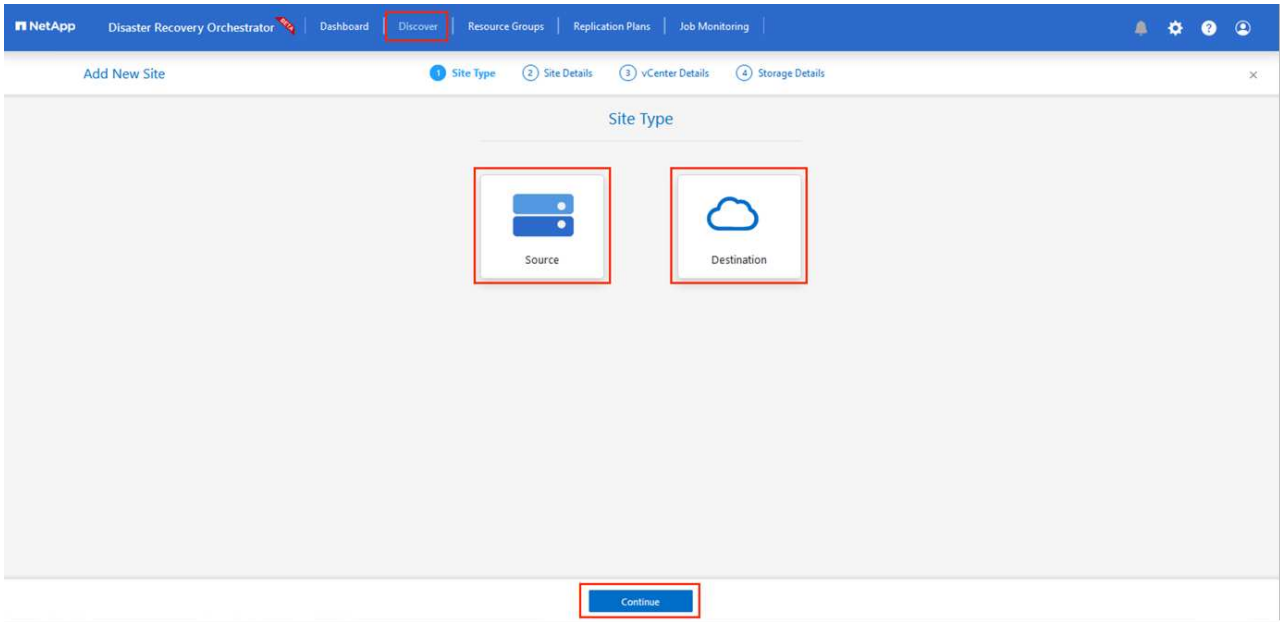
  Sie sollten diese Informationen bei der Erstellung der AD-Anwendung erfasst haben.

5. Bestätigen Sie die Details zu den neuen Anmeldeinformationen, und klicken Sie auf Credential hinzufügen.



Nachdem Sie die Anmeldedaten hinzugefügt haben, wird es Zeit, den primären und sekundären AVS-Standort (sowohl vCenter als auch das Azure NetApp Files-Speicherkonto) zu ermitteln und zu DRO hinzuzufügen. Gehen Sie wie folgt vor, um den Quell- und Zielstandort hinzuzufügen:

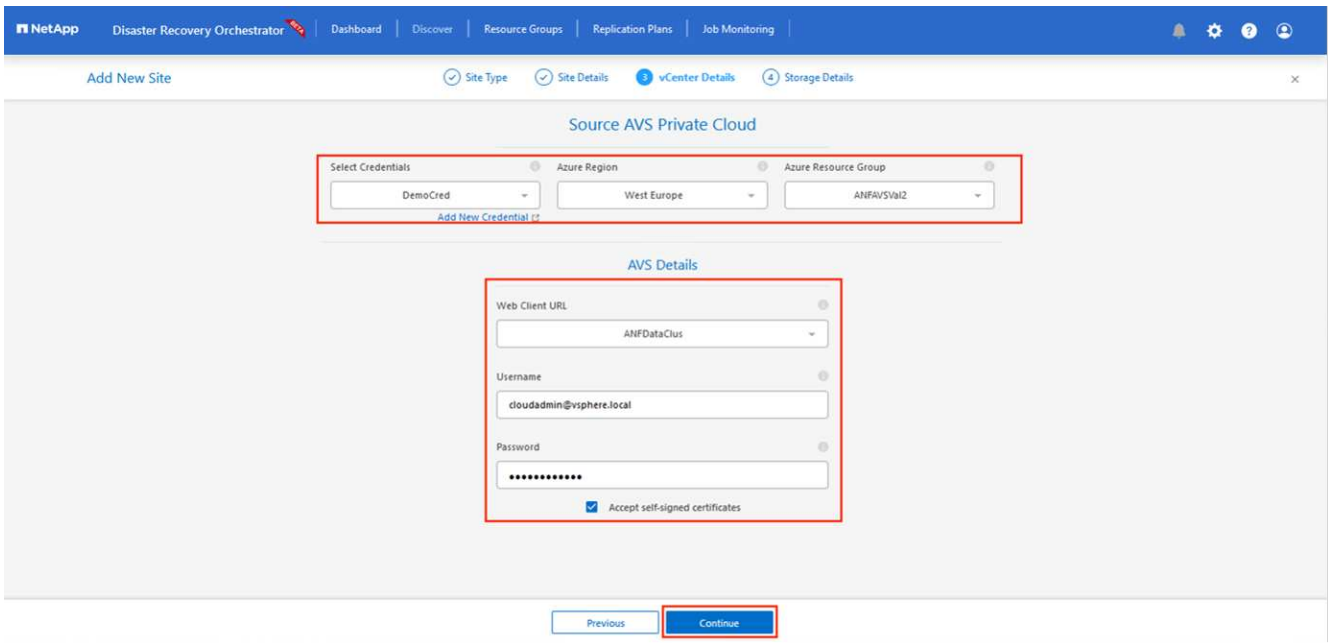
6. Gehen Sie auf die Registerkarte **Entdecken**.
7. Klicken Sie Auf **Neue Site Hinzufügen**.
8. Fügen Sie den folgenden primären AVS-Standort hinzu (in der Konsole als **Quelle** bezeichnet).
   - SDDC vCenter
   - Azure NetApp Files Storage Konto
9. Fügen Sie den folgenden sekundären AVS-Standort hinzu (in der Konsole als **Ziel** bezeichnet).
   - SDDC vCenter
   - Azure NetApp Files Storage Konto



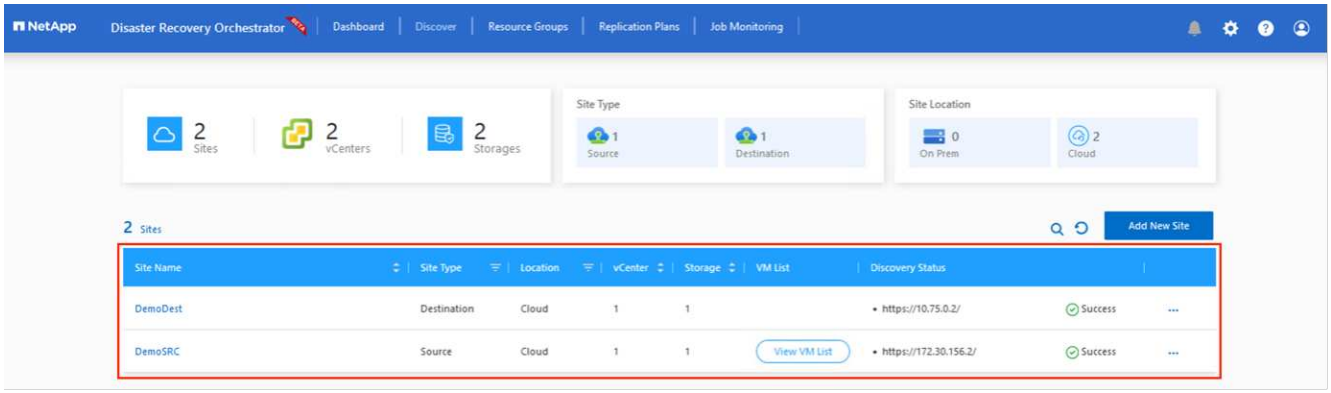
10. Fügen Sie Standortdetails hinzu, indem Sie auf **Quelle** klicken und einen freundlichen Standortnamen eingeben und den Konnektor auswählen. Klicken Sie dann auf **Weiter**.

> Das Hinzufügen einer Quellwebsite wird zu Demonstrationszwecken in diesem Dokument behandelt.

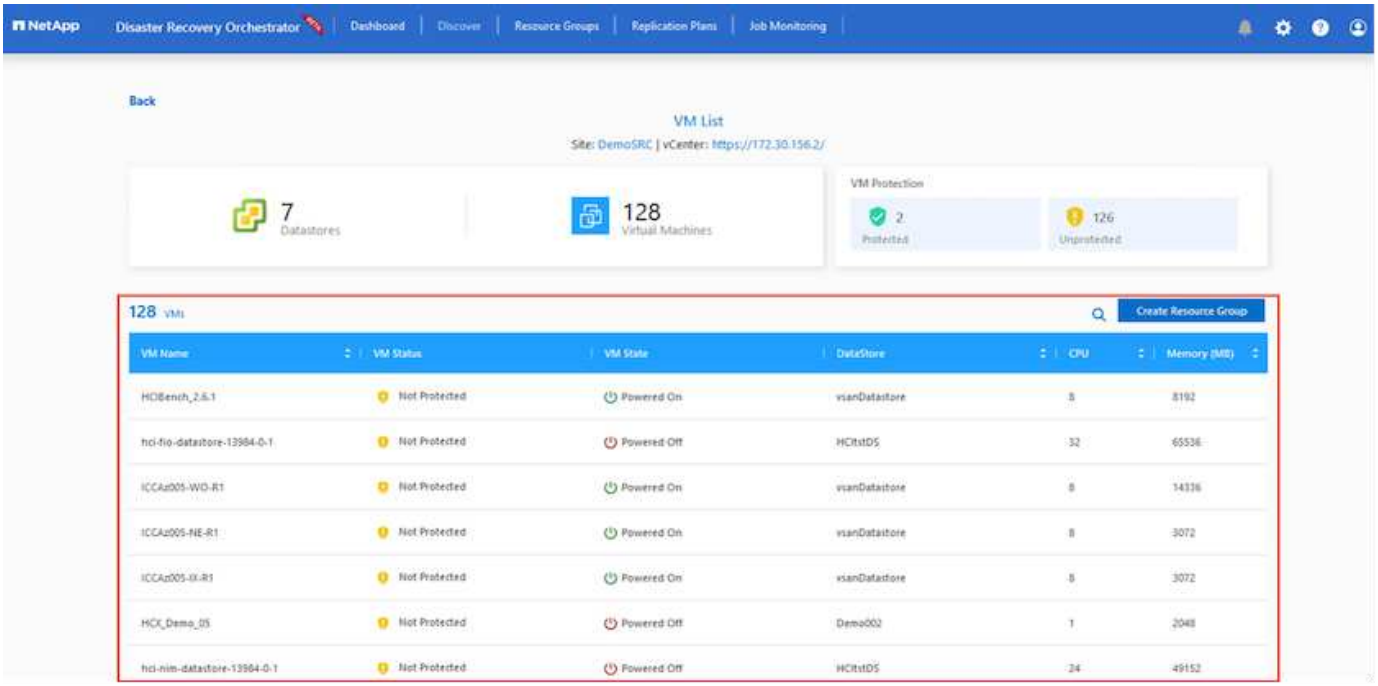
11. Aktualisieren Sie die vCenter-Details. Wählen Sie dazu die Anmeldedaten, die Azure-Region und die Ressourcengruppe aus der Dropdown-Liste für das primäre AVS-SDDC aus.
12. DRO listet alle verfügbaren SDDCs innerhalb der Region auf. Wählen Sie die entsprechende Private-Cloud-URL aus der Dropdown-Liste aus.
13. Geben Sie das ein `cloudadmin@vsphere.local` Benutzeranmeldeinformationen. Auf diese kann über das Azure-Portal zugegriffen werden. Befolgen Sie die hier beschriebenen Schritte "Verlinken". Klicken Sie anschließend auf **Weiter**.



14. Wählen Sie die Details zum Quell-Storge (ANF) aus, indem Sie die Azure Ressourcengruppe und das NetApp Konto auswählen.
15. Klicken Sie Auf **Site Erstellen**.



Nach dem Hinzufügen führt DRO eine automatische Erkennung durch und zeigt die VMs an, die entsprechende regionsübergreifende Replikate vom Quellstandort zum Zielstandort haben. DRO erkennt automatisch die Netzwerke und Segmente, die von den VMs verwendet werden, und füllt diese aus.



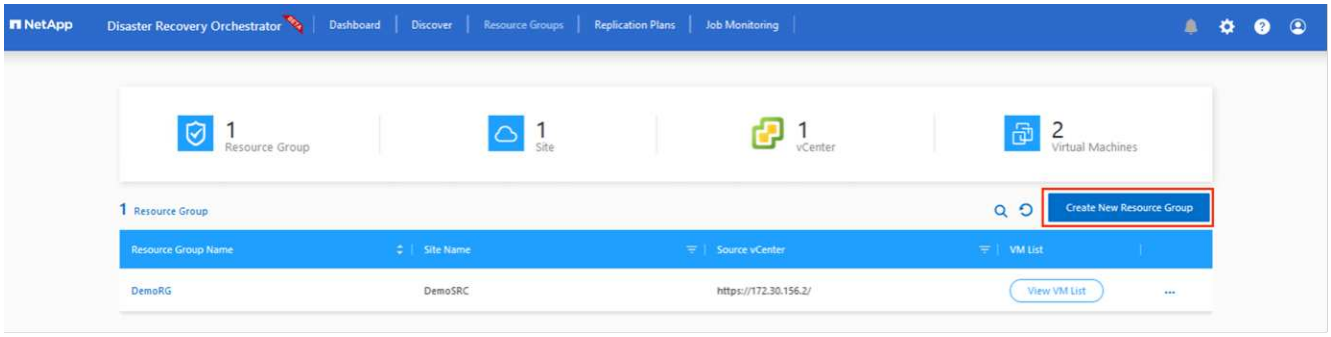
Im nächsten Schritt werden die erforderlichen VMs als Ressourcengruppen in ihre funktionalen Gruppen gruppiert.

Ressourcen-Gruppierungen

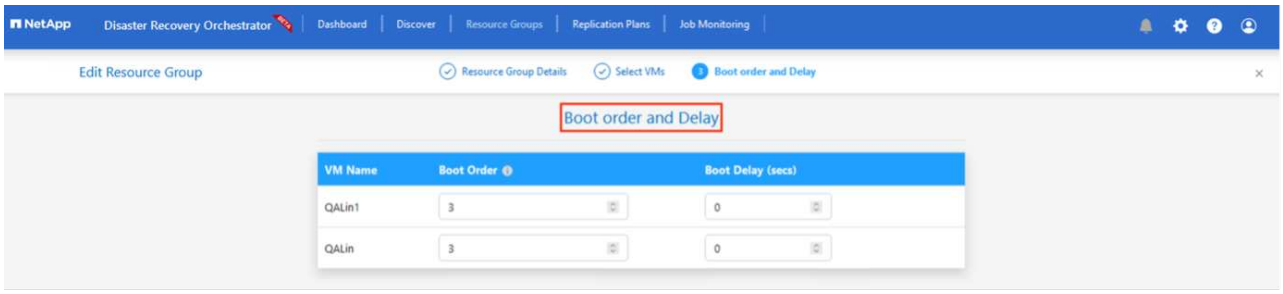
Nachdem die Plattformen hinzugefügt wurden, gruppieren Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen. MIT DRO-Ressourcengruppen können Sie eine Gruppe abhängiger VMs zu logischen Gruppen gruppieren, die ihre Boot-Aufträge, Boot-Verzögerungen und optionale Applikationsvalidierungen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

Um Ressourcengruppen zu erstellen, klicken Sie auf den Menüpunkt **Neue Ressourcengruppe erstellen**.

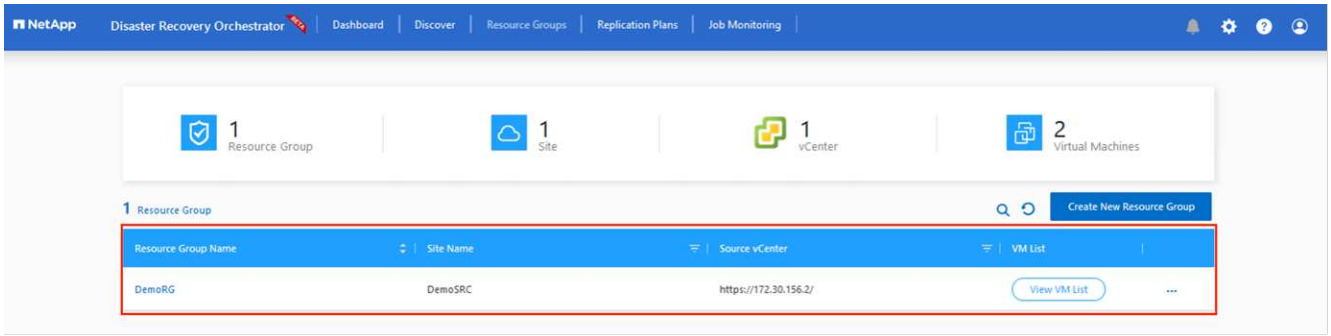
1. Greifen Sie auf **Resource Grou*ps zu und klicken Sie auf *Neue Ressourcengruppe erstellen**.



2. Wählen Sie unter Neue Ressourcengruppe den Quellstandort aus dem Dropdown-Menü aus und klicken Sie auf **Erstellen**.
3. Geben Sie die Details der Ressourcengruppe ein und klicken Sie auf **Weiter**.
4. Wählen Sie über die Suchoption die entsprechenden VMs aus.
5. Wählen Sie für alle ausgewählten VMs die Optionen **Boot Order** und **Boot Delay** (s) aus. Legen Sie die Reihenfolge der Einschaltsequenz fest, indem Sie jede virtuelle Maschine auswählen und die Priorität für sie festlegen. Der Standardwert für alle virtuellen Maschinen ist 3. Folgende Optionen stehen zur Verfügung:
   - Die erste virtuelle Maschine, die eingeschaltet wird
   - Standard
   - Die letzte virtuelle Maschine, die eingeschaltet werden muss



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



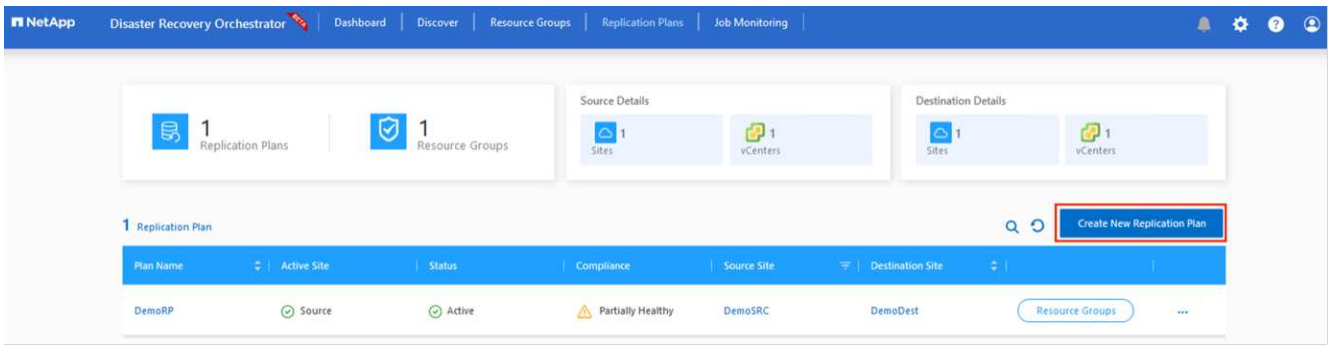
Replizierungspläne

Die Wiederherstellung von Applikationen im K-Fall ist unverzichtbar. Wählen Sie in der Dropdown-Liste die Quell- und Ziel-vCenter-Plattformen aus und wählen Sie die Ressourcengruppen aus, die in diesen Plan

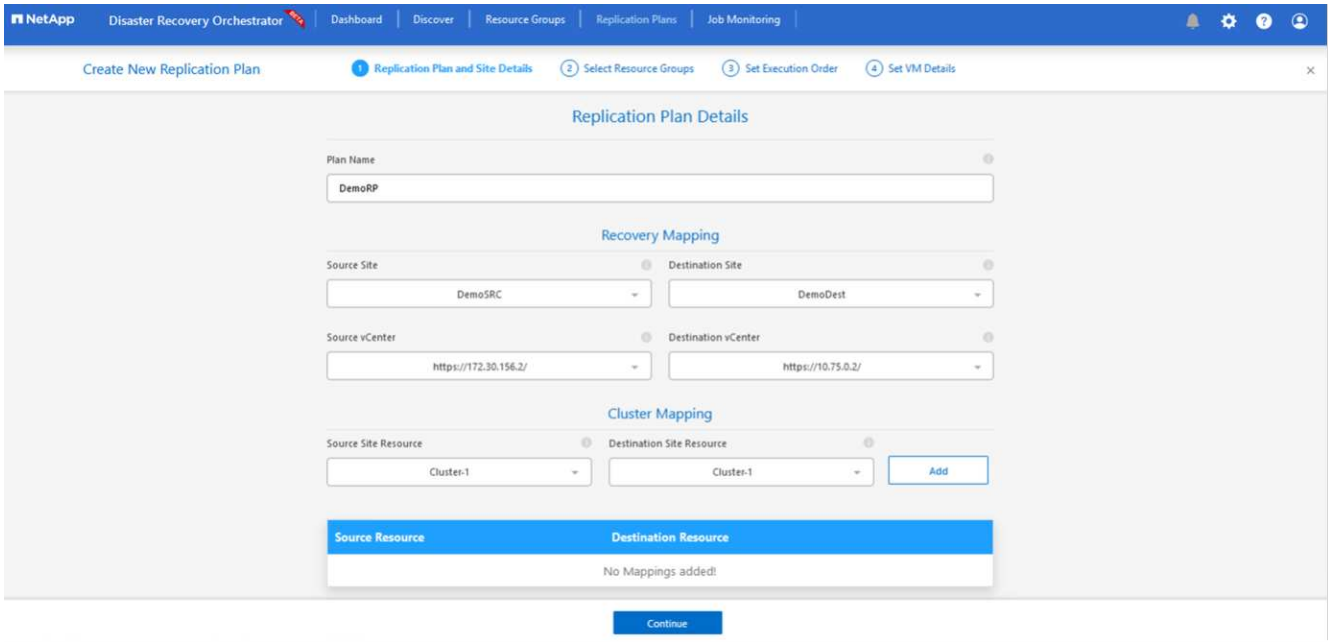
aufgenommen werden sollen. Außerdem berücksichtigen Sie die Gruppierung der wiederherzustellenden und hochzusteuenden Applikationen (z. B. Domain Controller, Tier-1, Tier-2 usw.). Pläne werden oft auch Blaupausen genannt. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte Replikationsplan und klicken Sie auf **Neuer Replikationsplan**.

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

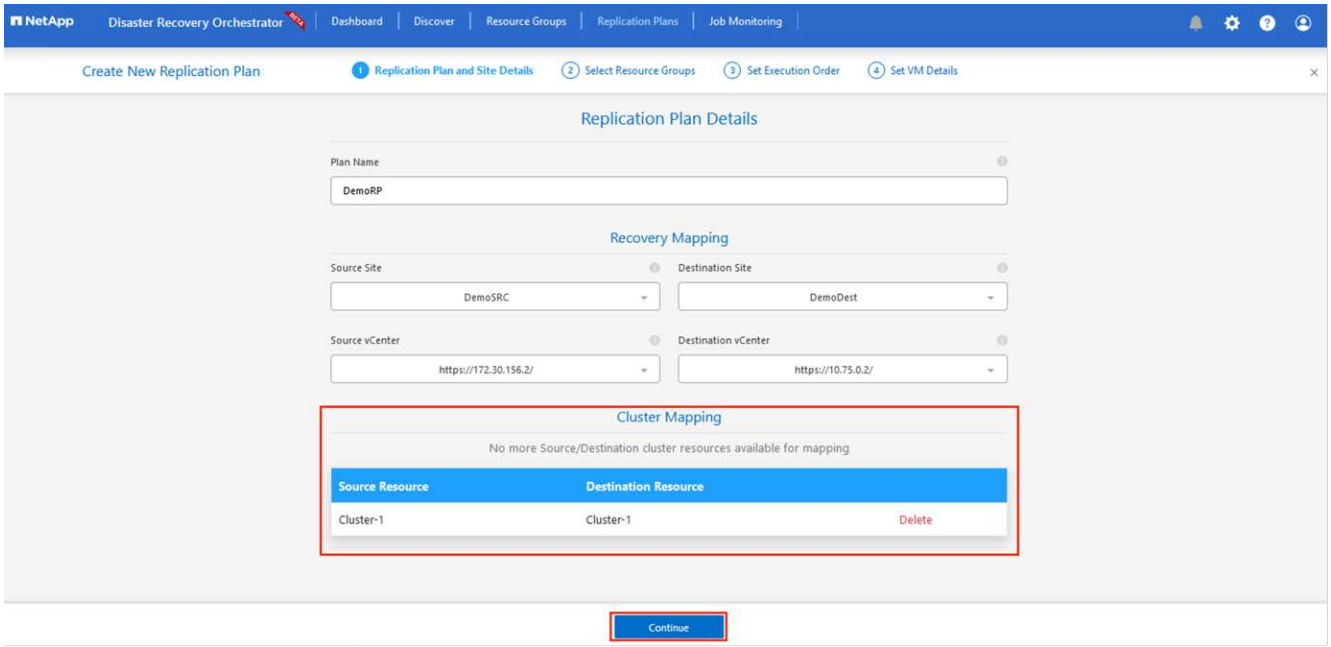
1. Navigieren Sie zu **Replikationspläne** und klicken Sie auf **Neuen Replikationsplan erstellen**.



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

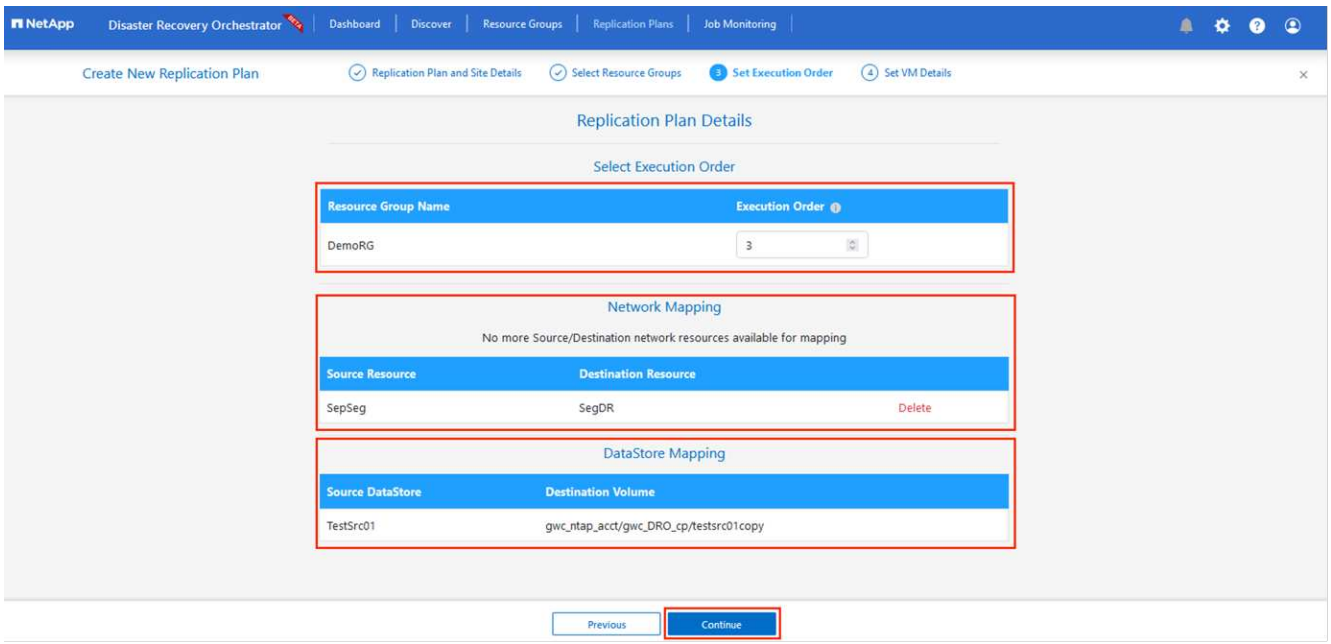


3. Nachdem die Wiederherstellungszuordnung abgeschlossen ist, wählen Sie die Option **Cluster Mapping** aus.

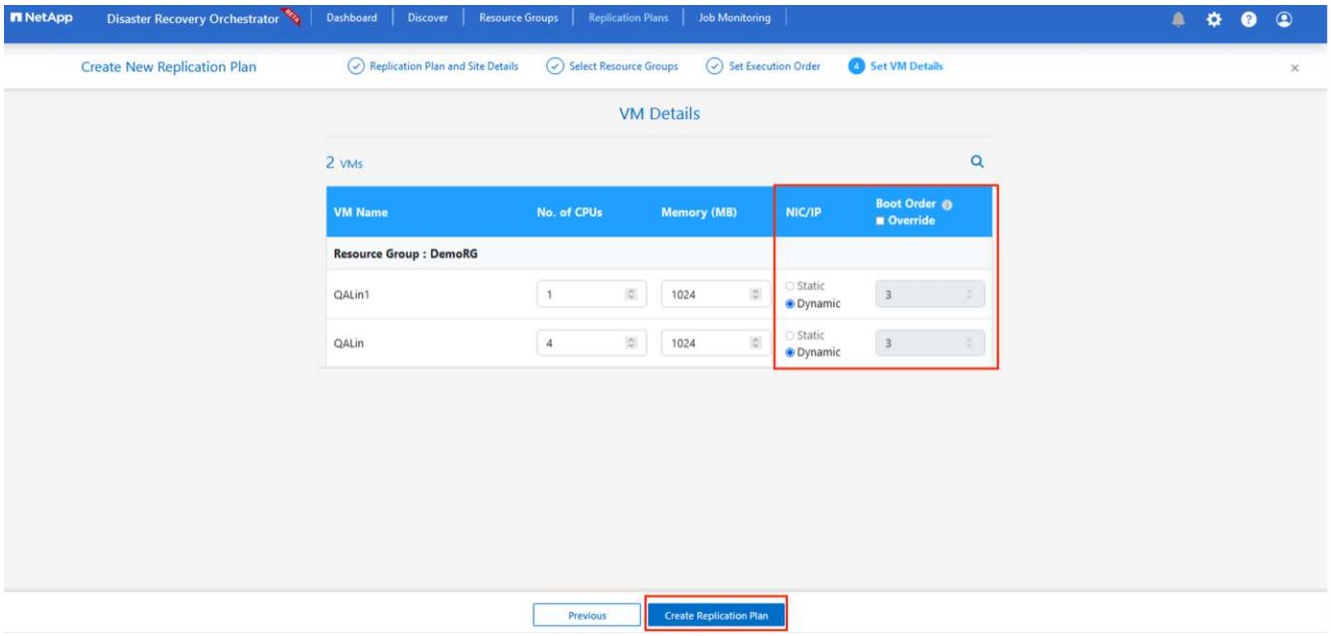


4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
6. Stellen Sie anschließend die Netzwerkzuordnung auf das entsprechende Segment ein. Die Segmente sollten bereits auf dem sekundären AVS-Cluster bereitgestellt werden. Um die VMs diesen zuzuordnen, wählen Sie das entsprechende Segment aus.
7. Aufgrund der Auswahl der VMs werden automatisch Datastore-Zuordnungen ausgewählt.

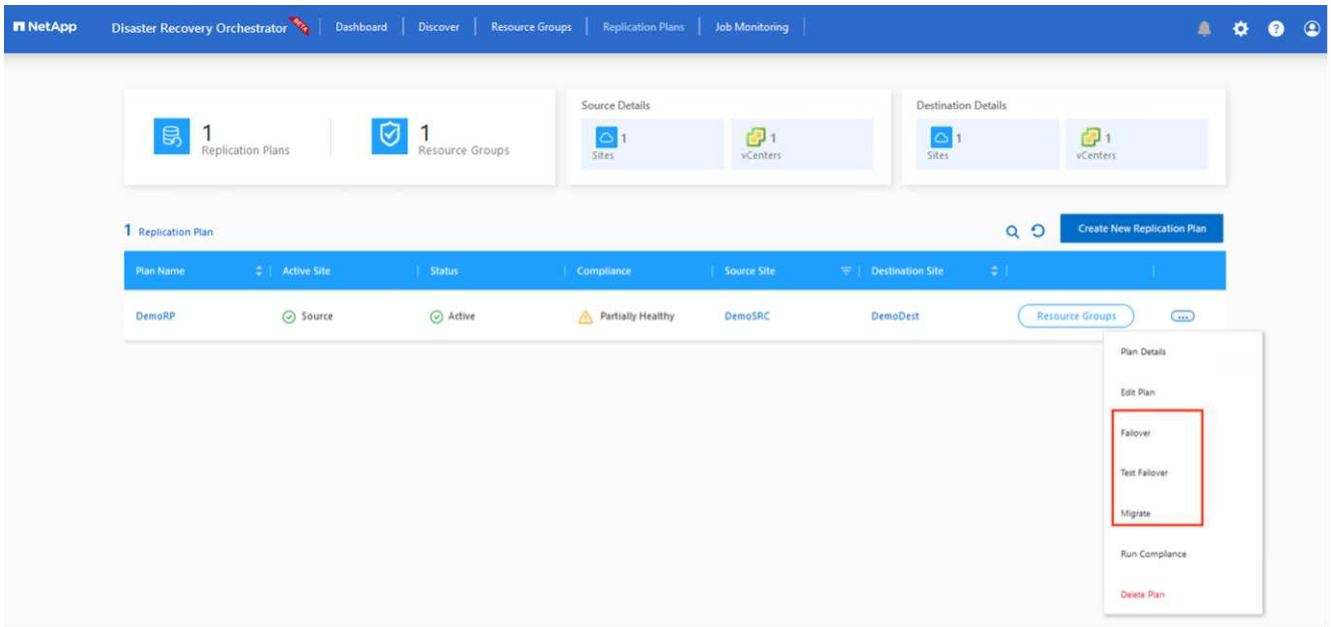
> Die regionsübergreifende Replikation (CRR) befindet sich auf Volume-Ebene. Daher werden alle VMs auf dem jeweiligen Volume auf das CRR-Ziel repliziert. Stellen Sie sicher, dass alle VMs ausgewählt werden, die Teil des Datenspeichers sind, da nur virtuelle Maschinen verarbeitet werden, die Teil des Replikationsplans sind.



8. Unter VM-Details können Sie optional die Größe der CPU- und RAM-Parameter der VMs ändern. Das ist vor allem hilfreich, wenn Sie große Umgebungen auf kleinere Ziel-Cluster wiederherstellen oder DR-Tests durchführen, ohne eine 1:1-physische VMware-Infrastruktur bereitstellen zu müssen. Ändern Sie außerdem die Startreihenfolge und die Startverzögerung (s) für alle ausgewählten VMs in den Ressourcengruppen. Es gibt eine zusätzliche Option, um die Startreihenfolge zu ändern, wenn Änderungen an den Änderungen erforderlich sind, die Sie bei der Auswahl des Ressource- Gruppe-Startauftrags ausgewählt haben. Standardmäßig wird die während der Auswahl der Ressourcengruppe ausgewählte Startreihenfolge verwendet. Änderungen können jedoch in dieser Phase vorgenommen werden.

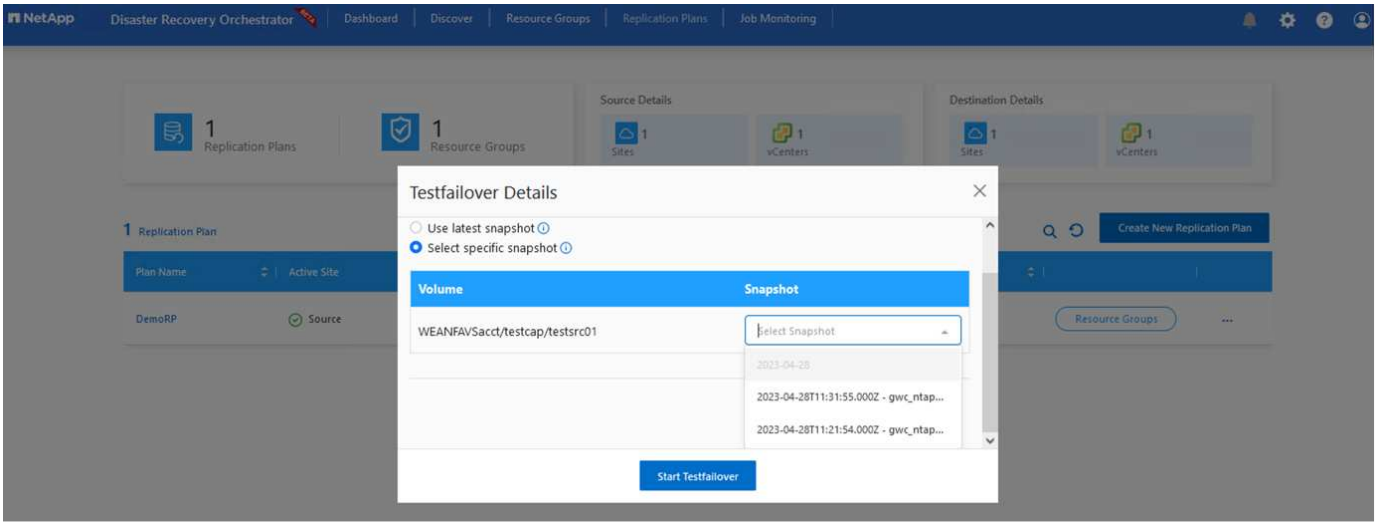


9. Klicken Sie auf **Create Replication Plan**.Nachdem der Replikationsplan erstellt wurde, können Sie die Failover-, Test-Failover- oder Migrationsoptionen je nach Ihren Anforderungen ausführen.

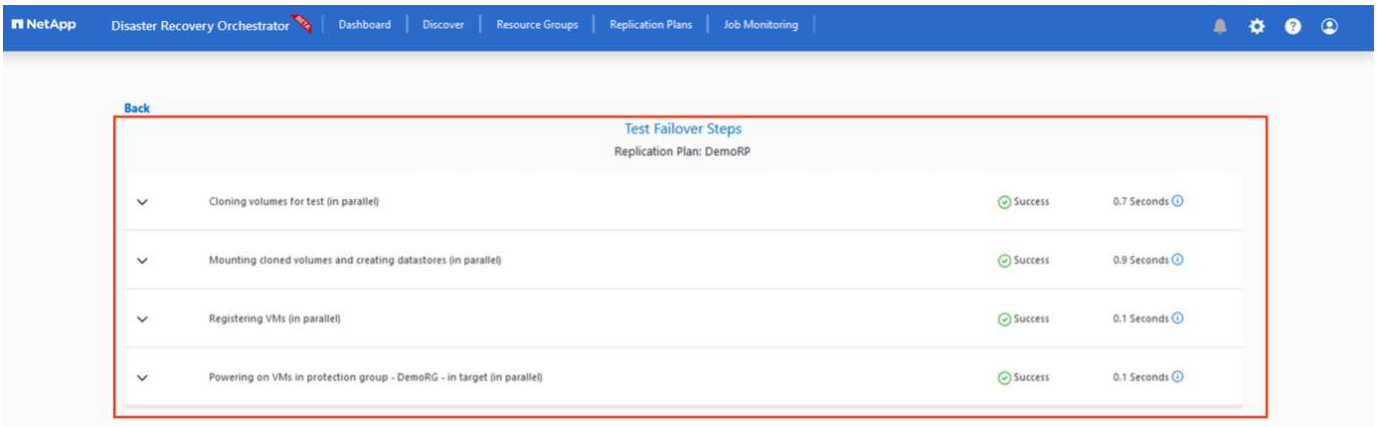


Während der Failover- und Test-Failover-Optionen wird der aktuellste Snapshot verwendet, oder ein bestimmter Snapshot kann aus einem Point-in-Time-Snapshot ausgewählt werden. Die Point-in-Time-Option

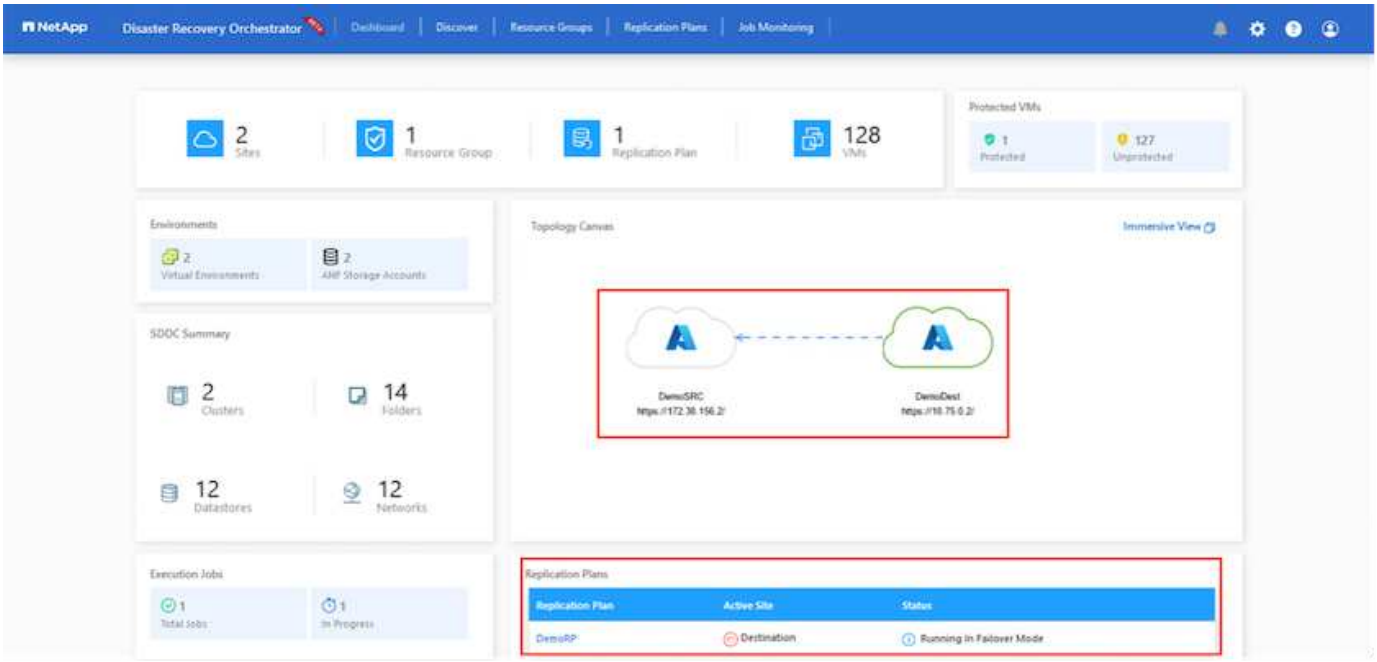
kann sehr vorteilhaft sein, wenn Sie vor einem Korruptionsereignis wie Ransomware stehen, wo die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. DRO zeigt alle verfügbaren Zeitpunkte an.



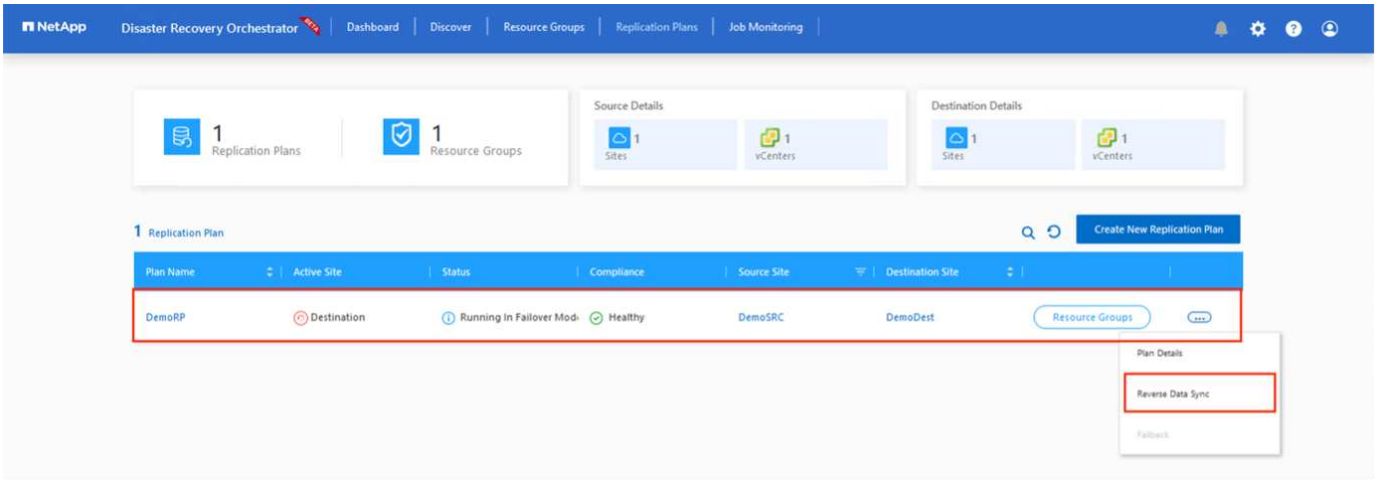
Um Failover oder Test Failover mit der im Replikationsplan angegebenen Konfiguration auszulösen, können Sie auf **Failover** oder **Test Failover** klicken. Sie können den Replikationsplan im Aufgabenmenü überwachen.



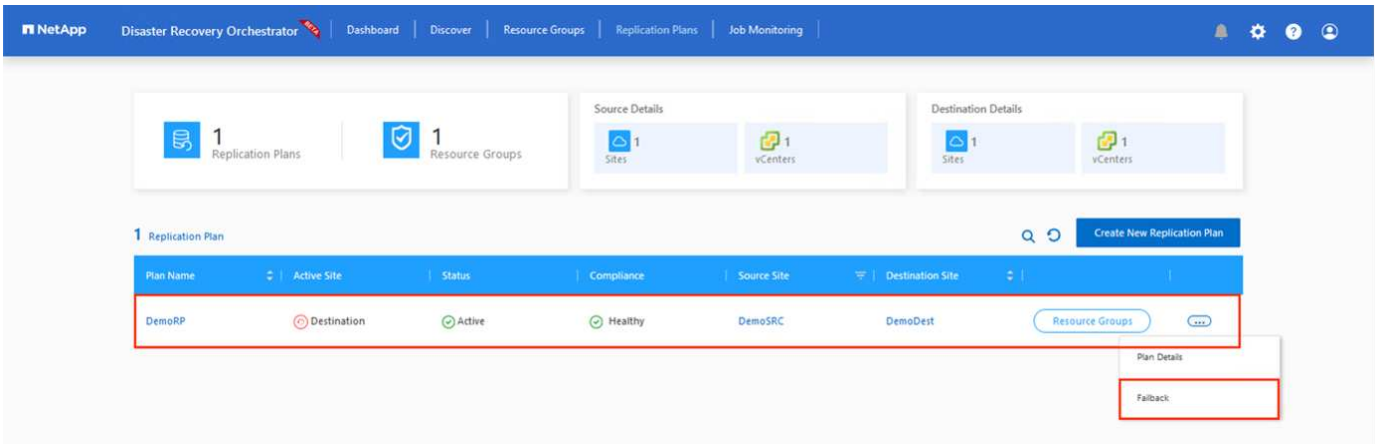
Nachdem der Failover ausgelöst wurde, können die wiederhergestellten Objekte im sekundären Standort AVS SDDC vCenter (VMs, Netzwerke und Datastores) erkannt werden. Standardmäßig werden die VMs im Workload-Ordner wiederhergestellt.

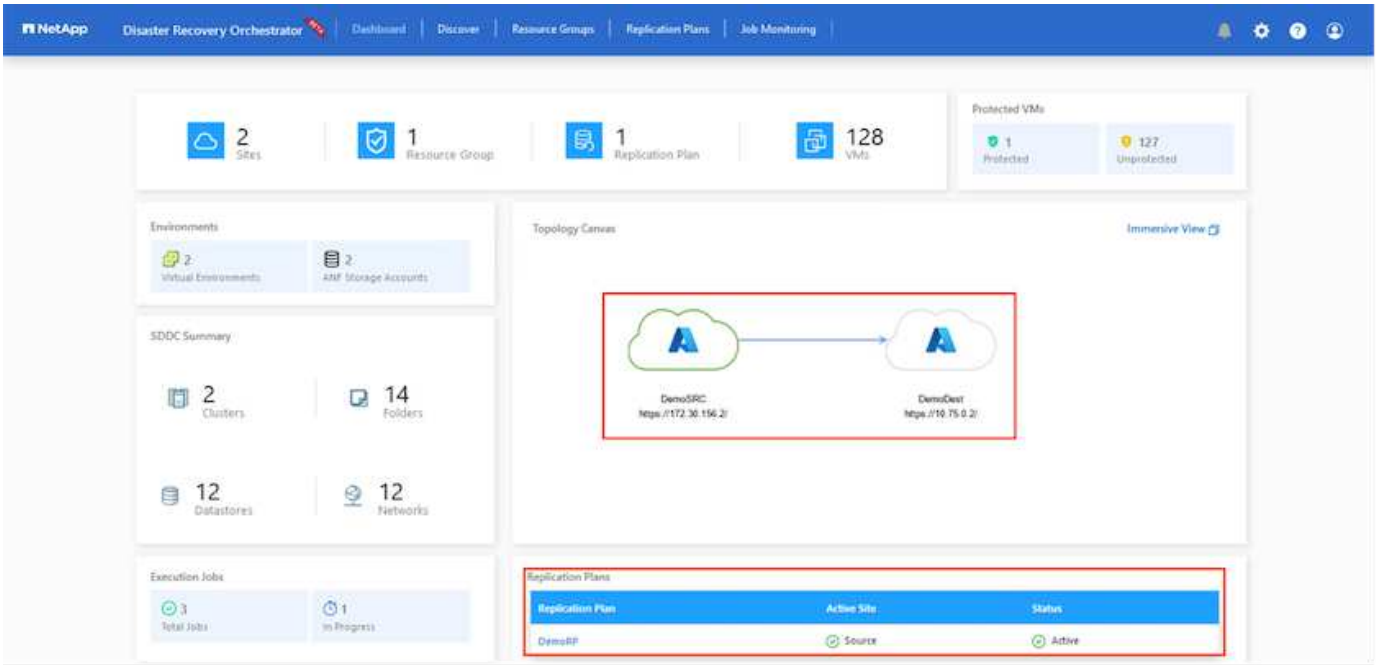


Failback kann auf der Ebene des Replikationsplans ausgelöst werden. Im Falle eines Test-Failovers kann die Option zum Abreißen verwendet werden, um die Änderungen rückgängig zu machen und das neu erstellte Volume zu entfernen. Failbacks im Zusammenhang mit Failover sind ein zweistufiger Prozess. Wählen Sie den Replikationsplan aus und wählen Sie **Reverse Data Sync** aus.



Wenn dieser Schritt abgeschlossen ist, führen Sie ein Failback aus, um zum primären AVS-Standort zurückzukehren.





Über das Azure-Portal können wir sehen, dass der Zustand der Replizierung für die entsprechenden Volumes unterbrochen wurde, die dem AVS SDDC am sekundären Standort als Lese-/Schreib-Volumes zugeordnet wurden. Beim Test-Failover weist DRO nicht das Ziel- oder Replikatvolume zu. Stattdessen wird ein neues Volume des erforderlichen regionsübergreifenden Replikations-Snapshots erstellt und das Volume als Datenspeicher bereitgestellt, wodurch zusätzliche physische Kapazität aus dem Kapazitäts-Pool verbraucht wird und sichergestellt wird, dass das Quell-Volume nicht geändert wird. Bemerkenswert ist, dass Replizierungsjobs während DR-Tests oder Triage Workflows fortgesetzt werden können. Darüber hinaus stellt dieser Prozess sicher, dass die Wiederherstellung bereinigt werden kann, ohne dass das Risiko besteht, dass das Replikat zerstört wird, wenn Fehler auftreten oder beschädigte Daten wiederhergestellt werden.

Recovery durch Ransomware

Die Wiederherstellung von Ransomware kann eine gewaltige Aufgabe sein. Insbesondere KANN es für IT-Abteilungen schwierig sein, den sicheren Rückgabepunkt zu bestimmen und, sobald dies festgelegt ist, zu gewährleisten, dass wiederhergestellte Workloads vor den wiederholten Angriffen geschützt werden (zum Beispiel vor dem Einschlafen von Malware oder durch anfällige Anwendungen).

DRO löst diese Probleme, indem es Unternehmen ermöglicht, Wiederherstellungen von beliebigen Zeitpunkten aus durchzuführen. Die Workloads werden dann in funktionsfähigen, aber isolierten Netzwerken wiederhergestellt, sodass Applikationen zwar funktionieren und miteinander kommunizieren können, aber

keinem Nord-/Süd-Datenverkehr ausgesetzt sind. Dieser Prozess bietet Sicherheitsteams einen sicheren Ort, um forensische Analysen durchzuführen und versteckte oder schlafende Malware zu identifizieren.

Schlussfolgerung

Die Disaster-Recovery-Lösung Azure NetApp Files und Azure VMware bietet folgende Vorteile:

- Effiziente und ausfallsichere regionsübergreifende Azure NetApp Files Replizierung
- Recovery zu einem beliebigen verfügbaren Point-in-Time mit Snapshot-Aufbewahrung.
- Automatisieren Sie alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden VMs aus den Validierungsschritten für Storage, Compute, Netzwerk und Applikationen.
- Workload Recovery nutzt den Prozess „Erstellung neuer Volumes aus den neuesten Snapshots“, der das replizierte Volume nicht manipuliert.
- Vermeiden Sie das Risiko der Datenbeschädigung auf den Volumes oder Snapshots.
- Keine Replizierungsunterbrechungen während DR-Test-Workflows
- Nutzen Sie DR-Daten und Cloud-Computing-Ressourcen für Workflows, die über DR hinausgehen, wie z. B. Entwicklungs-/Test, Sicherheitstests, Patch- und Upgrade-Tests oder Fehlerbehebungstests.
- Die CPU- und RAM-Optimierung kann dazu beitragen, Cloud-Kosten zu senken, indem eine Recovery auf kleinere Compute-Cluster ermöglicht wird.

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:

- Volume-Replizierung für Azure NetApp Files erstellen

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Regionsübergreifende Replizierung von Azure NetApp Files Volumes

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Azure VMware Lösung"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Implementieren und Konfigurieren der Virtualisierungsumgebung auf Azure

  "AVS auf Azure einrichten"

- Implementierung und Konfiguration der Azure-VMware-Lösung

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Verwenden von Veeam Replizierung und Azure NetApp Files-Datastore für die Disaster Recovery zu Azure VMware-Lösung

Autor: Niyaz Mohamed - NetApp Solutions Engineering

Überblick

Azure NetApp Files Datastores (ANF) entkoppeln Storage von Computing und ermöglichen jedem Unternehmen die erforderliche Flexibilität, um Workloads in die Cloud zu verlagern. Sie bietet eine flexible, hochperformante Storage-Infrastruktur, die unabhängig von den Compute-Ressourcen skaliert werden kann. Azure NetApp Files Datastore vereinfacht und optimiert die Implementierung zusammen mit der Azure VMware Lösung (AVS) als Disaster-Recovery-Standort für lokale VMware Umgebungen.

Mit Volume-basierten Azure NetApp Files (ANF) NFS-Datastores können Daten mit jeder validierten Drittanbieterlösung, die VM-Replizierungsfunktionen bietet, aus On-Premises-Systemen repliziert werden. Durch das Hinzufügen von Azure NetApp Files-Datenspeichern kann eine kostenoptimierte Implementierung durchgeführt werden, anstatt eine SDDC-Lösung für Azure VMware mit einer enormen Anzahl an ESXi-Hosts für den Storage einzurichten. Dieser Ansatz wird als „Pilot Light Cluster“ bezeichnet. Ein Pilot-Light-Cluster ist eine minimale AVS-Hostkonfiguration (3 AVS-Knoten) zusammen mit der Kapazität des Azure NetApp Files-Datenspeichers.

Ziel ist es, eine kostengünstige Infrastruktur mit allen Kernkomponenten für ein Failover zu erhalten. Ein Pilot-Light-Cluster kann horizontal skalieren und im Falle eines Failovers weitere AVS-Hosts bereitstellen. Sobald der Failover abgeschlossen und der normale Betrieb wiederhergestellt ist, kann das Pilot Light-Cluster wieder auf den kostengünstigen Betriebsmodus zurückskaliert werden.

Zweck dieses Dokuments

In diesem Artikel wird beschrieben, wie Sie Azure NetApp Files mit Veeam Backup and Replication die Disaster Recovery für lokale VMware-VMs auf (AVS) mithilfe der Veeam VM-Replizierungssoftware einrichten.

Veeam Backup & Replication ist eine Backup- und Replizierungsapplikation für virtuelle Umgebungen. Wenn virtuelle Maschinen repliziert werden, wird Veeam Backup & Replication von auf AVS repliziert, erstellt die Software eine exakte Kopie der VMs im nativen VMware vSphere-Format auf dem Ziel-AVS SDDC-Cluster. Veeam Backup & Replication hält die Kopie mit der ursprünglichen VM synchron. Die Replizierung bietet die beste Recovery Time Objective (RTO), da am DR-Standort eine gemountete Kopie einer VM in einem startfähigen Zustand ist.

Dieser Replizierungsmechanismus sorgt dafür, dass die Workloads bei einem Notfall schnell in einem AVS SDDC gestartet werden können. Die Veeam Backup & Replication Software optimiert darüber hinaus die Datenübertragung zur Replizierung über WAN und für langsame Verbindungen. Außerdem werden doppelte Datenblöcke, keine Datenblöcke, Swap-Dateien und „ausgeschlossene VM Gast-OS-Dateien“ herausgefiltert. Die Software komprimiert auch den Replikatverkehr. Um zu verhindern, dass Replikationsjobs die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Regeln zur Netzwerkdrosselung verwendet 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. Veeam Backup & Replication bietet mehrere Optionen für unterschiedliche Disaster-Recovery-Szenarien.

[]

Lösungsimplementierung

Übergeordnete Schritte

1. Die Veeam Backup & Replication-Software wird in einer On-Premises-Umgebung mit entsprechender Netzwerkverbindung ausgeführt.
2. "Implementieren der Azure-VMware-Lösung (AVS)" Private Cloud und "Verbinden Sie Azure NetApp Files-Datastores" Auf Hosts der Azure-VMware-Lösung.

   Für DR-Zwecke kann eine Pilot-Light-Umgebung 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 den Replikationsjob 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 AVS- und ANF-Datastores

1. Stellen Sie sicher, dass die Backup-VM von Veeam Backup & Replication sowohl mit den Quell- als auch den Ziel-AVS 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. Der Ziel-Azure NetApp Files-Datastore muss über genügend freien Speicherplatz für die VMDKs replizierter VMs verfügen.

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

Einzelheiten Zur Bereitstellung

Schritt: Replizierung von VMs

Veeam Backup & Replication nutzt VMware vSphere Snapshot-Funktionen/während der Replizierung fordert Veeam Backup & Replication VMware vSphere zur Erstellung eines VM-Snapshots an. Der VM-Snapshot ist die Point-in-Time-Kopie einer VM, die virtuelle Laufwerke, den Systemstatus, die Konfiguration und Metadaten 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. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Knoten Jobs, und wählen Sie Replikationsjob > Virtuelle Maschine 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 die Bandbreite zwischen On-Premises und Azure eingeschränkt ist.
     *Aktivieren Sie das Kontrollkästchen Network Remapping (für AVS SDDC-Standorte mit unterschiedlichen Netzwerken), wenn Segmente auf der Azure VMware-Lösung SDDC nicht mit denen auf lokalen Netzwerken übereinstimmen.
   - Wenn sich das IP-Adressierungsschema am Produktionsstandort vor Ort vom Schema am Ziel-AVS-Standort unterscheidet, aktivieren Sie das Kontrollkästchen Replica RE-IP (für DR-Standorte mit unterschiedlichem IP-Adressierungsschema).

     []
4. Wählen Sie im Schritt **Virtuelle** Maschinen* die VMs aus, die auf einen Azure NetApp Files-Datastore repliziert werden sollen, der mit einem Azure VMware-Lösung 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 lassen sich problemlos auf Azure NetApp Files Datenspeichern platzieren, um die VMs wiederherzustellen und das Cluster zu erweitern, um die CPU-/mem-Anforderungen zu erfüllen. 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**.

   []
5. Wählen Sie anschließend das Ziel als Azure VMware Solution SDDC Cluster/Host und den entsprechenden Ressourcen-Pool, VM-Ordner und FSX for ONTAP Datastore für VM-Replikate aus. Klicken Sie anschließend auf **Weiter**.

   []
6. Erstellen Sie im nächsten Schritt die Zuordnung zwischen dem virtuellen Quell- und Zielnetzwerk nach Bedarf.

   []
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**.

   []

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.

    []

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

[]

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**. 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. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Knoten Replikate, und wählen Sie Failover Plans > Failover Plan > VMware vSphere.

   []

2. Geben Sie als nächstes einen Namen und eine Beschreibung für den Plan an. 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.

   []

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

   []

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 die Netzwerksegmentierung vorhanden ist, um IP-Konflikte während des Failovers zu vermeiden.

Um den Failover-Plan zu starten, klicken Sie einfach auf die Registerkarte **Failover Plans** und klicken Sie mit der rechten Maustaste auf Ihren 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.

[]

[]

Der Status des VM-Replikats ändert sich von „bereit“ zu „Failover“, und die VMs werden auf dem Ziel-Cluster/Host des SDDC der Azure VMware-Lösung (AVS) gestartet.

[]

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

[]

> 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 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.

[]

[]

[]

[]

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".

[]

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

[]

Schlussfolgerung

Mit der Datastore-Funktion von Azure NetApp Files können Veeam oder jedes beliebige validierte Drittanbieter-Tool eine kostengünstige DR-Lösung anbieten, indem Pilot-Light-Cluster eingesetzt werden, anstatt nur ein großes Cluster einzurichten, um VM-Replikate aufzunehmen. So wird ein maßgeschneiderter und individuell angepasster Disaster-Recovery-Plan effizient umgesetzt und vorhandene Backup-Produkte intern für DR wiederverwendet. So wird Cloud-basierte Disaster Recovery durch das Beenden von DR-Datacentern vor Ort möglich. Bei einem Ausfall kann ein Failover durch Klicken auf eine Schaltfläche oder bei

einem Ausfall automatisch durchgeführt werden.

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=2855e0d5-97e7-430f-944a-b061015e9278

Migration von Workloads auf Azure/AVS

TR-4940: Migration von Workloads auf Azure NetApp Files Datastore mithilfe von VMware HCX - QuickStart Guide

Autor(en): NetApp Solutions Engineering

Übersicht: Migration von Virtual Machines mit VMware HCX, Azure NetApp Files Datastores und Azure VMware Lösung

Eine der gängigsten Anwendungsfälle für die Azure VMware Lösung und den Azure NetApp Files Datastore ist die Migration von VMware Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmechanismen zum Verschieben von On-Premises-Virtual Machines (VMs) und deren Daten in Azure NetApp Files Datastores.

VMware HCX ist primär eine Migrationsplattform, die entwickelt wurde, um die Migration von Applikationen, die Ausbalancierung von Workloads und sogar Business Continuity Cloud-übergreifend zu vereinfachen. Es ist im Rahmen von Azure VMware Solution Private Cloud enthalten und bietet viele Möglichkeiten zum Migrieren von Workloads und kann für Disaster-Recovery-(DR-)Vorgänge genutzt werden.

Dieses Dokument enthält eine Schritt-für-Schritt-Anleitung zur Bereitstellung von Azure NetApp Files Datastore. Anschließend werden die Komponenten von VMware HCX heruntergeladen, implementiert und konfiguriert, einschließlich aller Hauptkomponenten vor Ort und der Seite der Azure VMware Lösung, einschließlich Interconnect, Netzwerkerweiterung und WAN-Optimierung, um verschiedene VM-Migrationsmechanismen zu ermöglichen.

> VMware HCX arbeitet mit jedem Datenspeichertyp zusammen, da die Migration auf VM-Ebene erfolgt. Dieses Dokument eignet sich daher für bestehende NetApp Kunden sowie für Kunden anderer Anbieter, die eine Implementierung der Azure NetApp Files Lösung mit Azure VMware als kostengünstige VMware Cloud-Implementierung planen.

Allgemeine Schritte

Diese Liste enthält grundlegende Schritte, die für die Installation und Konfiguration von HCX Cloud Manager auf der Azure Cloud-Seite und die Installation von HCX Connector vor Ort erforderlich sind:

1. Installieren Sie HCX über das Azure-Portal.
2. Laden Sie das Installationsprogramm für die HCX Connector Open Virtualization Appliance (OVA) im lokalen VMware vCenter Server herunter und implementieren Sie es.
3. HCX mit dem Lizenzschlüssel aktivieren.
4. Verbinden Sie den lokalen VMware HCX Connector mit der Azure VMware-Lösung HCX Cloud Manager.
5. Sie konfigurieren das Netzwerkprofil, das Computing-Profil und das Service-Mesh.
6. (Optional) Sie können eine Netzwerkerweiterung vornehmen, um bei Migrationen eine erneute IP-Adresse zu vermeiden.
7. Validieren des Appliance-Status und Sicherstellen der Möglichkeit der Migration
8. Migration der VM-Workloads

Voraussetzungen

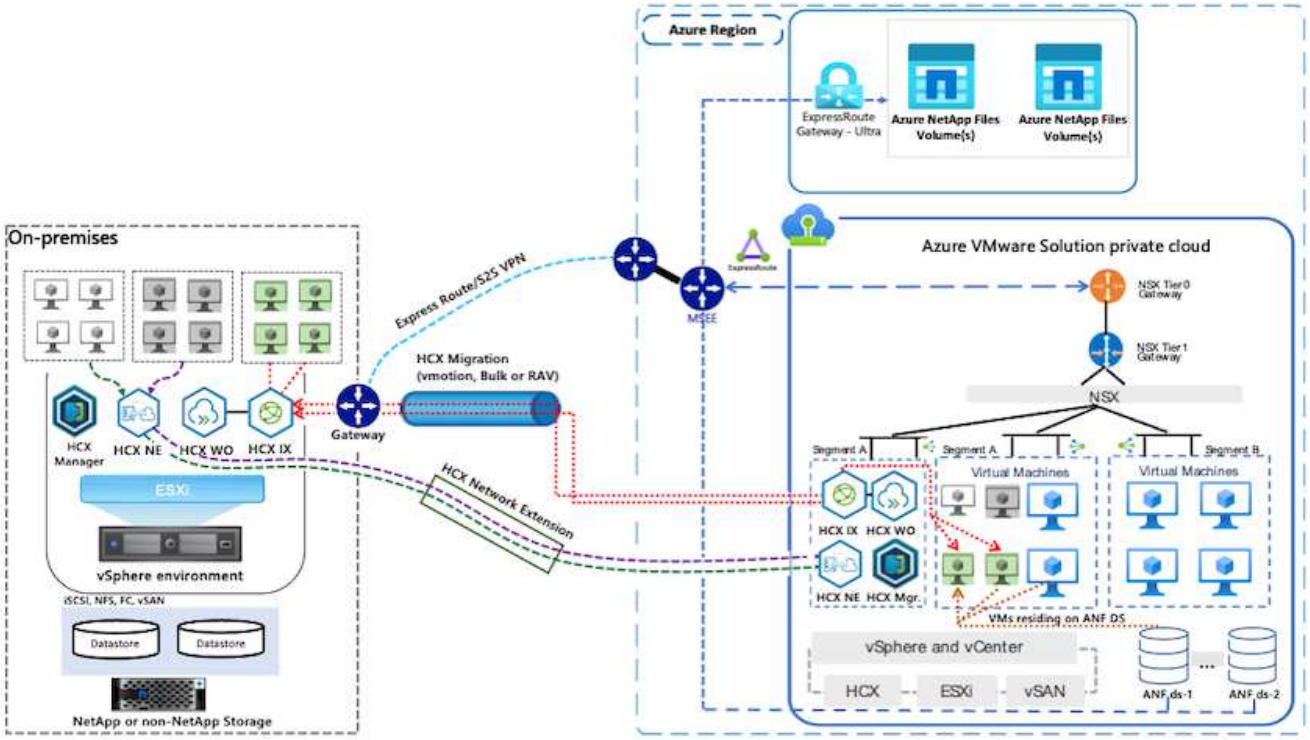
Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "Verlinken". Nachdem die Voraussetzungen, einschließlich der Konnektivität, vorhanden sind, konfigurieren und aktivieren Sie HCX, indem Sie den Lizenzschlüssel aus dem Azure VMware-Lösungsportal generieren. Nach dem Herunterladen des OVA-Installationsprogramms gehen Sie wie unten beschrieben mit der Installation vor.

HCX Advanced ist die Standardoption und die VMware HCX Enterprise Edition ist auch über ein Support-Ticket erhältlich und wird ohne zusätzliche Kosten unterstützt.

- Nutzen Sie ein bereits softwaredefiniertes Datacenter (SDDC) einer Azure VMware Lösung oder erstellen Sie mithilfe dieses Modells eine Private Cloud "Link von NetApp" Oder hier "Microsoft-Link".
- Die Migration von VMs und zugehörigen Daten vom lokalen Datacenter mit VMware vSphere erfordert Netzwerkkonnektivität vom Datacenter zur SDDC-Umgebung. Vor der Migration von Workloads "Richten Sie eine Site-to-Site-VPN- oder Express-Route-globale REACH-Verbindung ein" Zwischen der lokalen Umgebung und der jeweiligen Private Cloud verschieben.
- Der Netzwerkpfad von der lokalen VMware vCenter Server Umgebung zur Private Cloud der Azure VMware Lösung muss die Migration von VMs mithilfe von vMotion unterstützen.
- Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und -Ports" Sind für vMotion Traffic zwischen dem lokalen vCenter Server und SDDC vCenter zulässig. In der Private Cloud ist das Routing im vMotion Netzwerk standardmäßig konfiguriert.
- Das Azure NetApp Files NFS-Volume sollte als Datastore in der Azure VMware-Lösung eingebunden werden. Befolgen Sie die in diesem Schritt beschriebenen Schritte "Verlinken" Um Azure NetApp Files-Datenspeicher an Azure VMware Solutions Hosts anzuschließen.

Übergeordnete Architektur

Die für diese Validierung verwendete Lab-Umgebung wurde zu Testzwecken über ein Site-to-Site-VPN verbunden, das On-Premises-Konnektivität mit der Azure VMware Lösung ermöglicht.



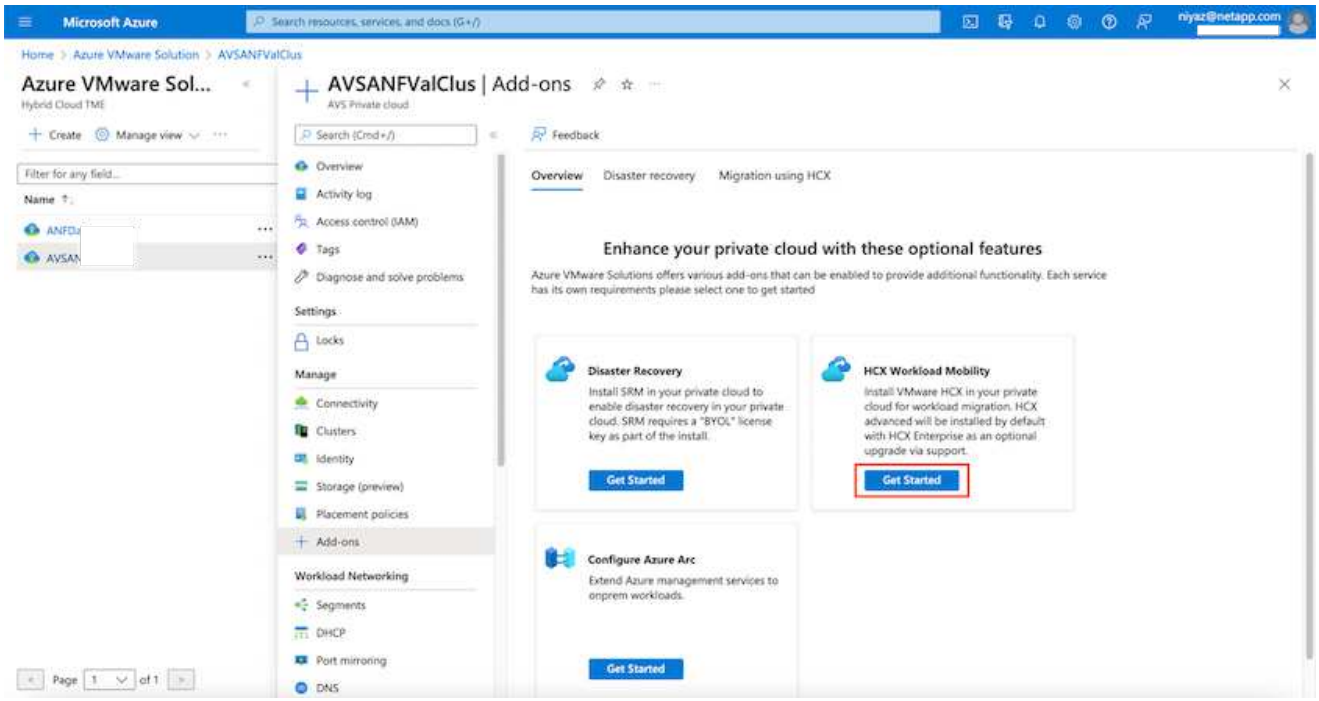
Lösungsimplementierung

Führen Sie die folgenden Schritte aus, um die Implementierung dieser Lösung abzuschließen:

Schritt 1: Installieren Sie HCX über Azure Portal mit der Option Add-ons

Gehen Sie wie folgt vor, um die Installation durchzuführen:

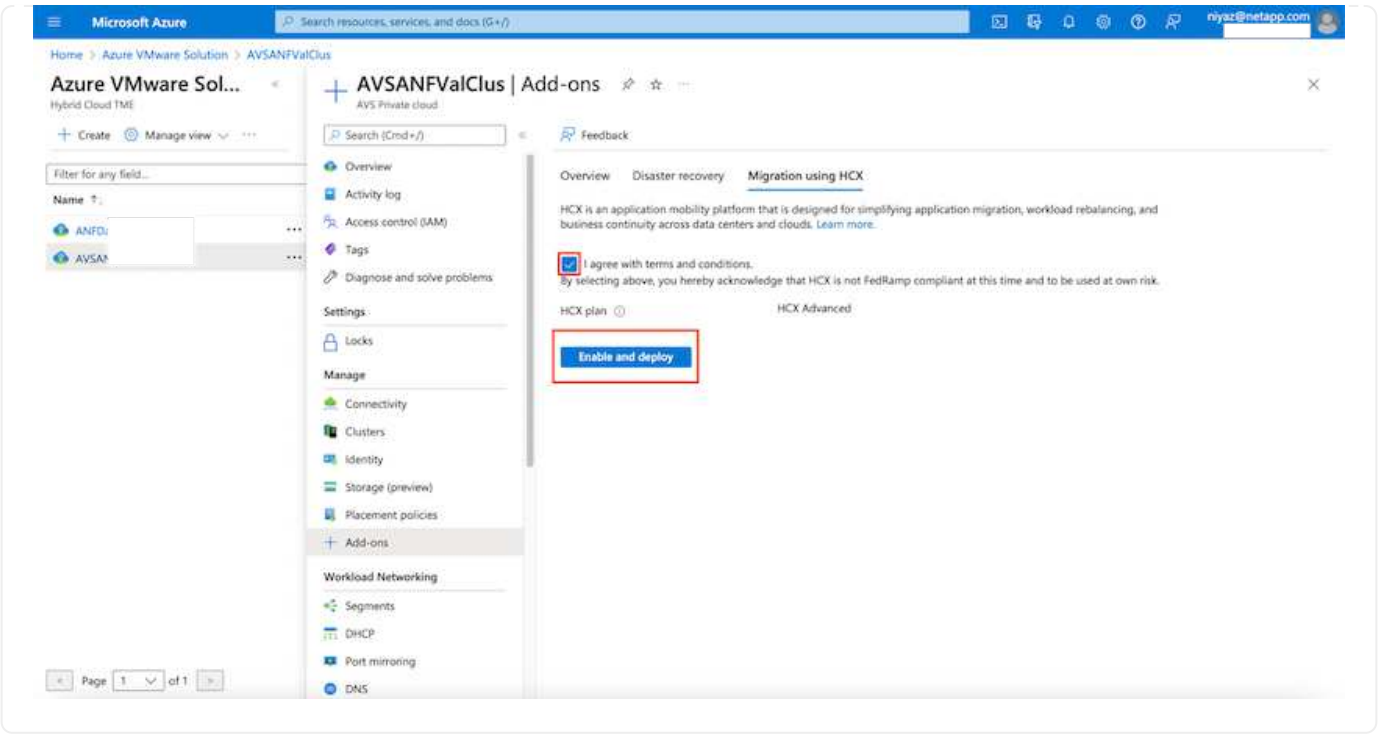
1. Melden Sie sich im Azure-Portal an und greifen Sie auf die Private Cloud der Azure VMware Lösung zu.
2. Wählen Sie die entsprechende private Cloud aus, und greifen Sie auf Add-ons zu. Dazu navigieren Sie zu **Verwalten > Add-ons**.
3. Klicken Sie im Bereich HCX Workload Mobility auf **Get Started**.



1. Wählen Sie die Option **Ich stimme den Allgemeinen Geschäftsbedingungen** zu und klicken Sie auf **Aktivieren und Bereitstellen**.

> Die Standardbereitstellung ist HCX Advanced. Öffnen Sie eine Support-Anfrage, um die Enterprise Edition zu aktivieren.

> Die Implementierung dauert etwa 25 bis 30 Minuten.


Microsoft Azure
Search resources, services, and docs (G+/)
niyaz@netapp.com
Home > Azure VMware Solution > AVSANFValClus
Azure VMware Sol...
Hybrid Cloud TME
Create
Manage view
Filter for any field...
Name
ANFDu
AVSAN
Page 1 of 1
AVSANFValClus | Add-ons
AVS Private cloud
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Clusters
Identity
Storage (preview)
Placement policies
Add-ons
Workload Networking
Segments
DHCP
Port mirroring
DNS
Feedback
Overview
Disaster recovery
Migration using HCX
HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. Learn more.
I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.
HCX plan
HCX Advanced
Enable and deploy

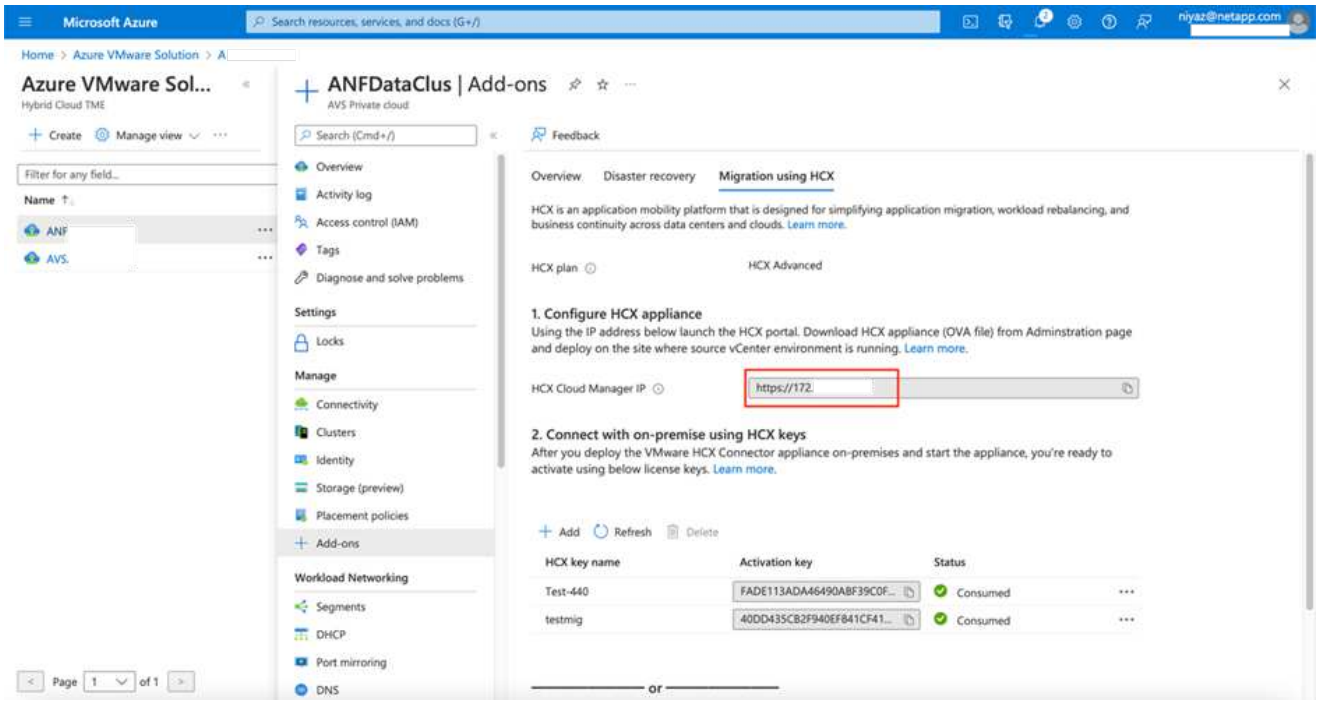
Schritt 2: Stellen Sie das Installationsprogramm OVA im lokalen vCenter Server bereit

Damit der On-Premises Connector eine Verbindung zum HCX Manager in Azure VMware herstellen kann, müssen in der On-Premises-Umgebung die entsprechenden Firewall-Ports geöffnet sein.

So laden Sie den HCX Connector auf dem lokalen vCenter Server herunter und installieren ihn:

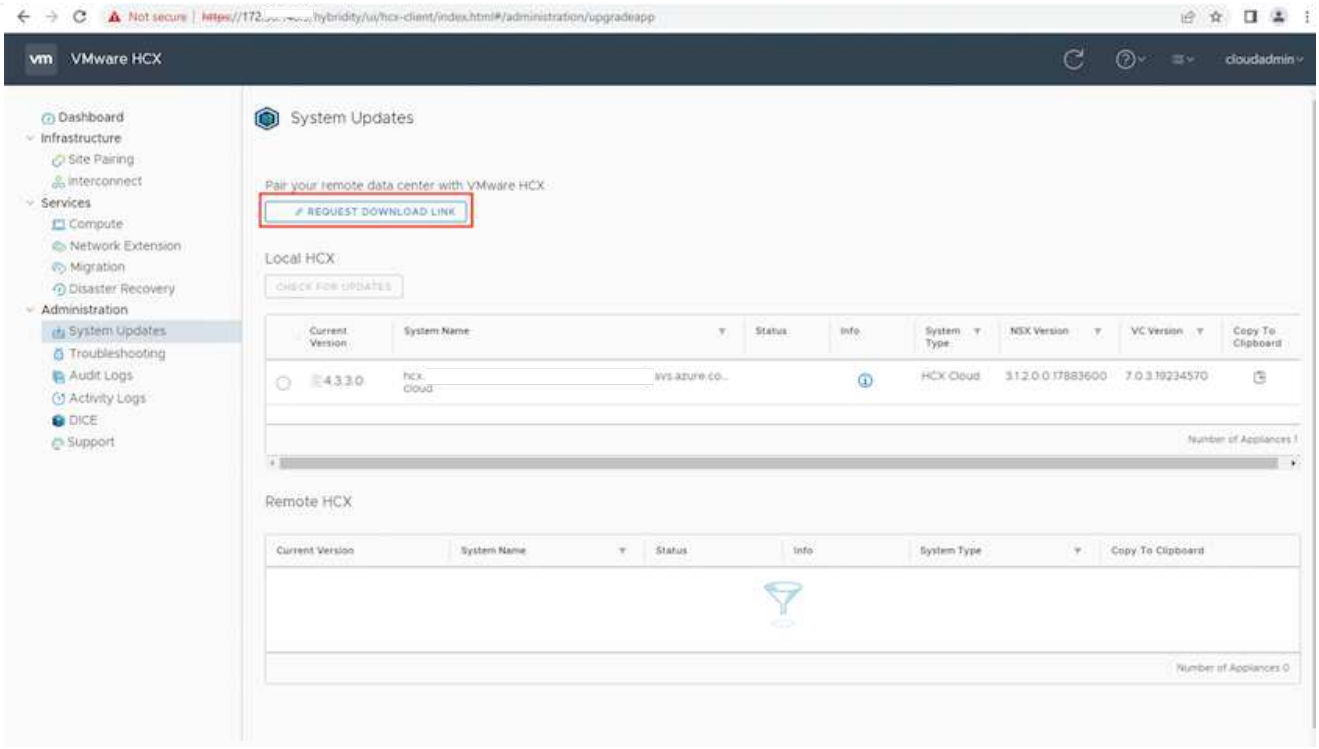
1. Wählen Sie im Azure-Portal die Azure-VMware-Lösung aus, wählen Sie die Private Cloud aus, und wählen Sie **Verwalten > Add-ons > Migration** mit HCX aus. Kopieren Sie das HCX-Cloud-Manager-Portal, um die OVA-Datei herunterzuladen.

Verwenden Sie die standardmäßigen CloudAdmin-Benutzeranmeldeinformationen für den Zugriff auf das HCX-Portal.

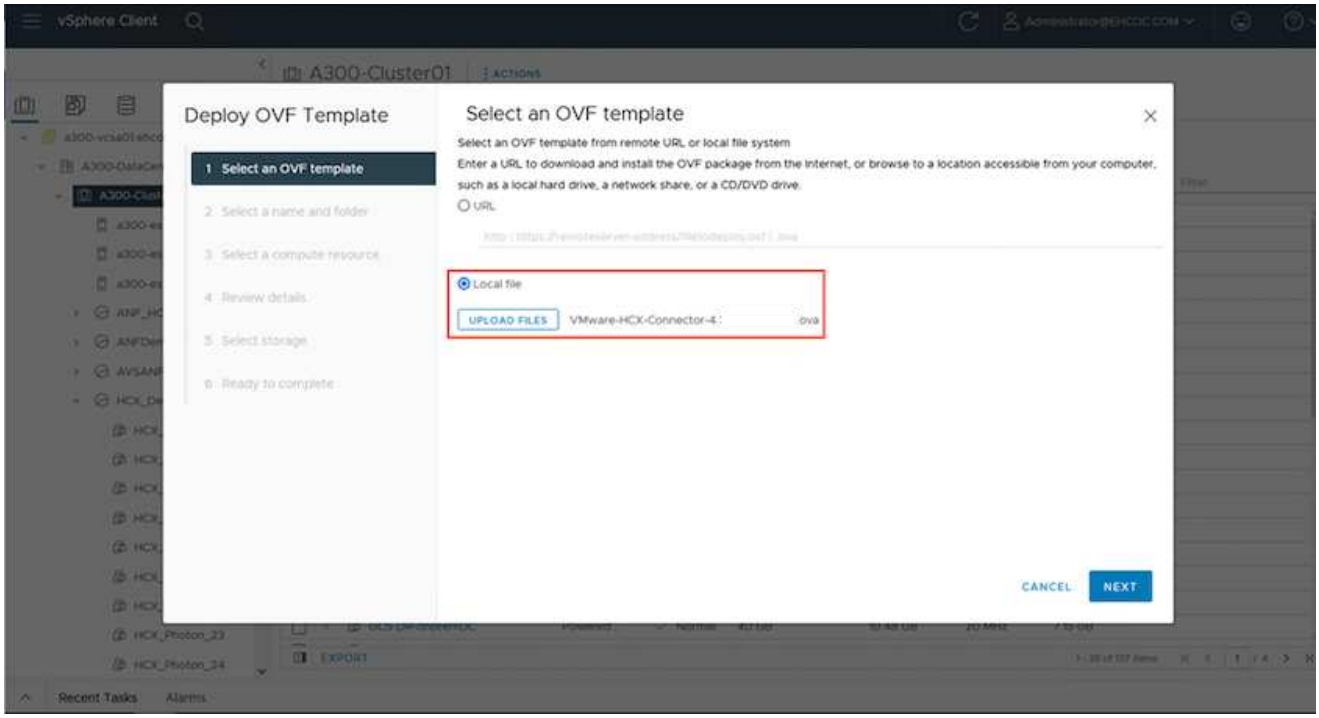


1. Nachdem Sie über den Jumphost auf das HCX-Portal mit cloudadmin@vsphere.local zugegriffen haben, navigieren Sie zu **Administration > Systemaktualisierungen** und klicken Sie auf **Download anfordern Link**.

Laden Sie entweder den Link zur OVA herunter oder kopieren Sie ihn in einen Browser, um den Download-Prozess der OVA-Datei von VMware HCX Connector zu starten, um sie auf dem lokalen vCenter Server bereitzustellen.



1. Nachdem die OVA heruntergeladen wurde, stellen Sie sie in der lokalen VMware vSphere Umgebung mithilfe der Option **Deploy OVF Template** bereit.



1. Geben Sie alle erforderlichen Informationen für die OVA-Bereitstellung ein, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um die OVA des VMware HCX-Connectors bereitzustellen.

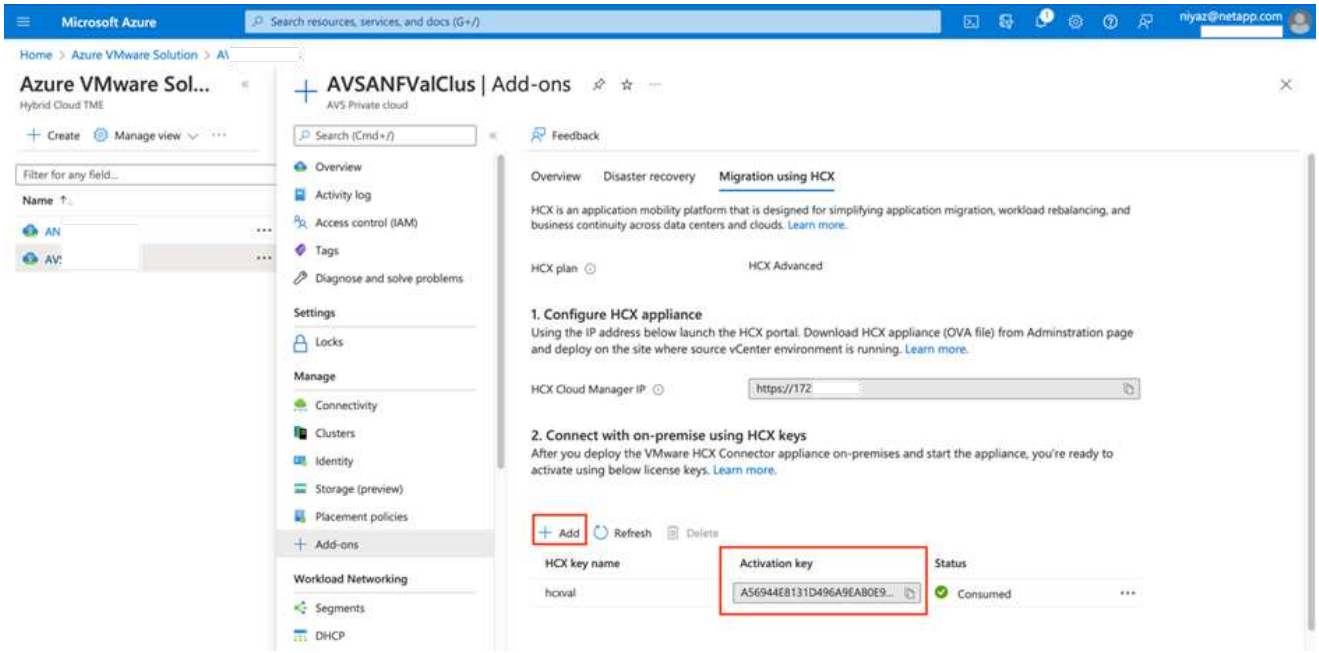
Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "VMware HCX-Benutzerhandbuch".

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie den VMware HCX Connector OVA vor Ort bereitgestellt und das Gerät gestartet haben, führen Sie die folgenden Schritte aus, um den HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel aus dem Azure VMware Lösungs-Portal und aktivieren Sie ihn in VMware HCX Manager.

1. Wählen Sie im Azure-Portal die Azure VMware-Lösung, wählen Sie die Private Cloud aus und wählen Sie **Verwalten > Add-ons > Migration Using HCX** aus.
2. Klicken Sie unter **Verbindung mit On-Premise mit HCX-Tasten** auf **Hinzufügen** und kopieren Sie den Aktivierungsschlüssel.



Für jeden bereitgestellten HCX-Connector vor Ort ist ein separater Schlüssel erforderlich.

1. Melden Sie sich beim lokalen VMware HCX Manager unter an "https://hcxmanagerIP:9443" Administratordaten werden verwendet.

Verwenden Sie das während der OVA-Bereitstellung definierte Passwort.

1. Geben Sie in der Lizenzierung den aus Schritt 3 kopierten Schlüssel ein und klicken Sie auf **Aktivieren**.

Der HCX-Connector sollte über einen Internetzugang verfügen.

1. Geben Sie unter **Datacenter Location** den nächstgelegenen Standort für die Installation des VMware HCX Managers vor Ort an. Klicken Sie Auf **Weiter**.
2. Aktualisieren Sie unter **Systemname** den Namen und klicken Sie auf **Weiter**.
3. Klicken Sie Auf **Ja, Weiter**.
4. Geben Sie unter **Connect Your vCenter** den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des vCenter Servers und die entsprechenden Anmeldeinformationen an und klicken Sie auf **Continue**.

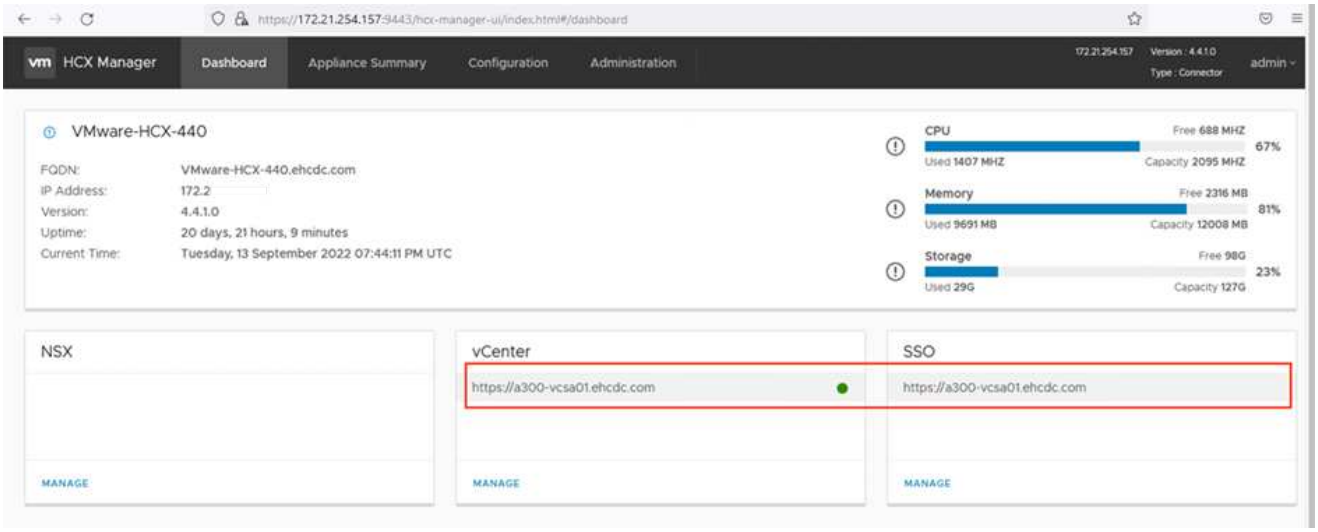
Verwenden Sie den FQDN, um Verbindungsprobleme später zu vermeiden.

1. Geben Sie unter * SSO/PSC konfigurieren* den FQDN oder die IP-Adresse des Plattform-Services-Controllers an und klicken Sie auf **Weiter**.

Geben Sie den VMware vCenter Server FQDN oder die IP-Adresse ein.

1. Überprüfen Sie, ob die eingegebenen Informationen korrekt sind, und klicken Sie auf **Neustart**.
2. Nach dem Neustart der Dienste wird vCenter Server auf der angezeigten Seite grün angezeigt. Sowohl vCenter Server als auch SSO müssen über die entsprechenden Konfigurationsparameter verfügen, die mit der vorherigen Seite übereinstimmen sollten.

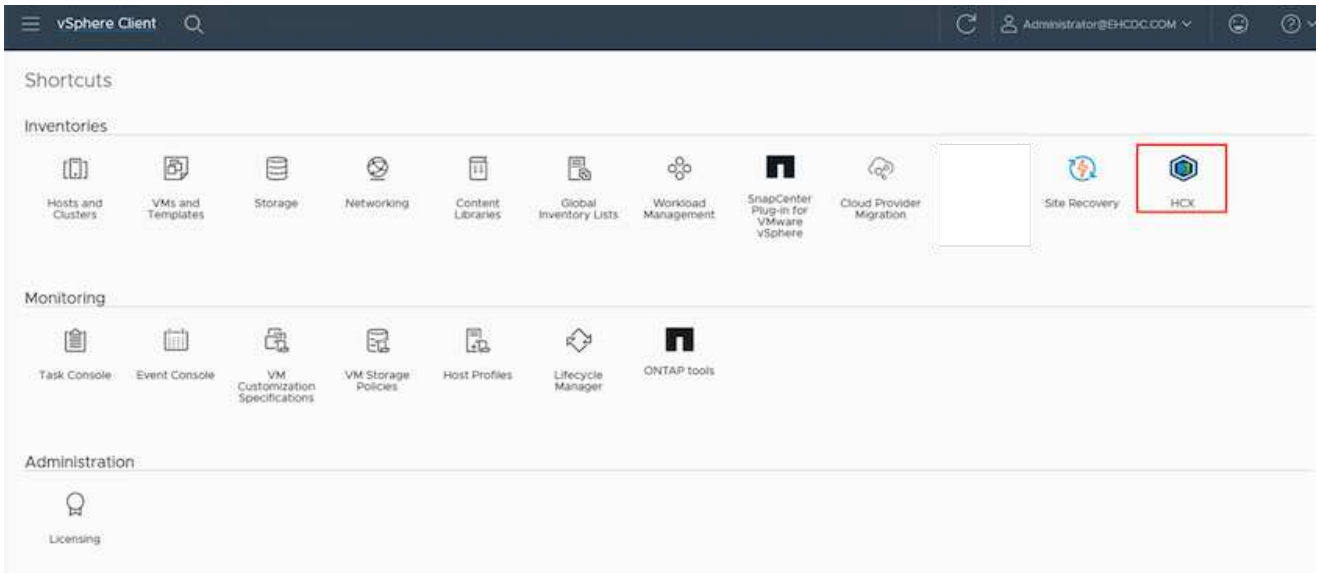
Dieser Vorgang dauert etwa 10 bis 20 Minuten, und das Plug-in wird dem vCenter Server hinzugefügt.



Schritt 4: Verbinden Sie den lokalen VMware HCX Connector mit der Azure VMware-Lösung HCX Cloud Manager

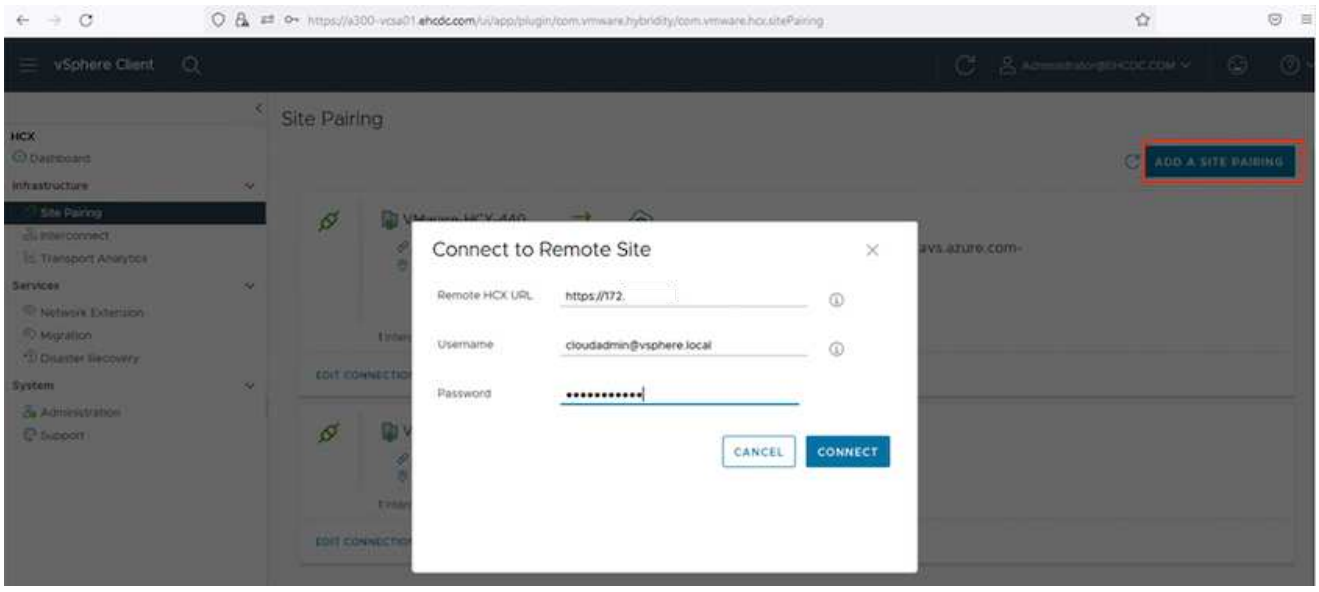
Nachdem HCX Connector sowohl in der lokalen als auch in der Azure VMware-Lösung installiert wurde, konfigurieren Sie die private Cloud der lokalen VMware HCX Connector for Azure VMware-Lösung, indem Sie die Paarung hinzufügen. Gehen Sie wie folgt vor, um die Standortpaarung zu konfigurieren:

1. Um ein Standortpaar zwischen der lokalen vCenter Umgebung und der Azure VMware Solution SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das neue HCX vSphere Web Client Plug-in zu.



1. Klicken Sie unter Infrastruktur auf **Site Pairing hinzufügen**.

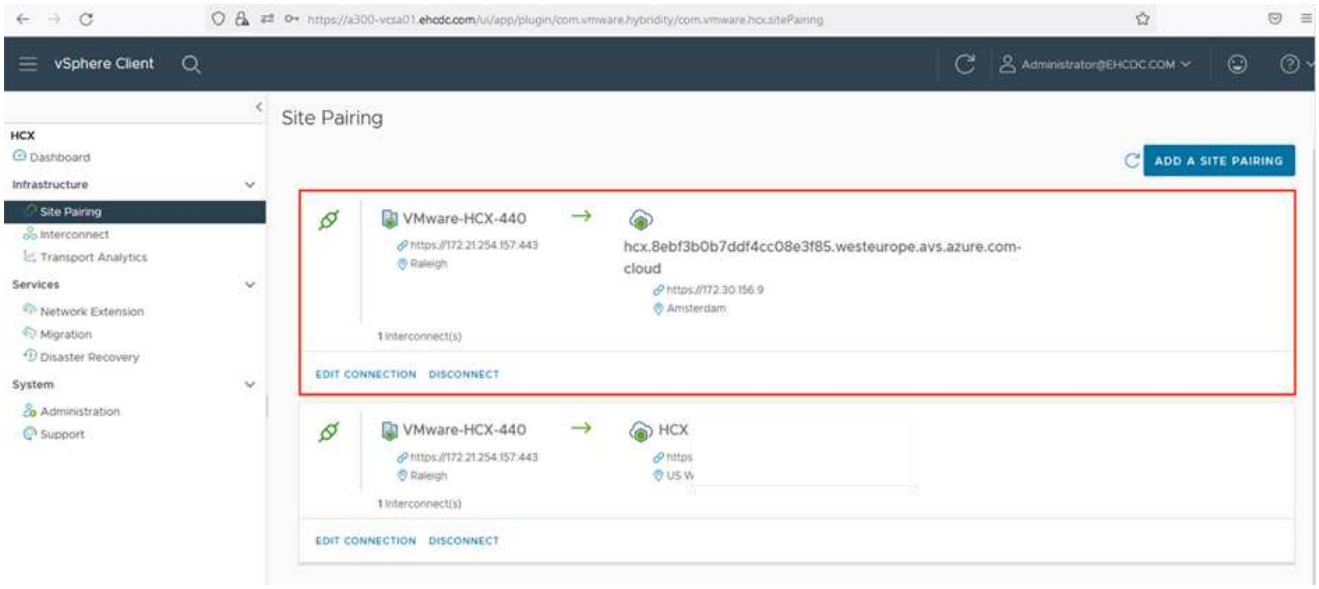
Geben Sie die URL oder IP-Adresse der Azure VMware Solution HCX Cloud Manager und die Anmeldedaten für CloudAdmin-Rolle für den Zugriff auf die private Cloud ein.



1. Klicken Sie Auf **Verbinden**.

VMware HCX Connector muss über Port 443 zu HCX Cloud Manager IP weiterleiten können.

1. Nach der Erstellung der Kopplung steht die neu konfigurierte Standortpairing auf dem HCX Dashboard zur Verfügung.

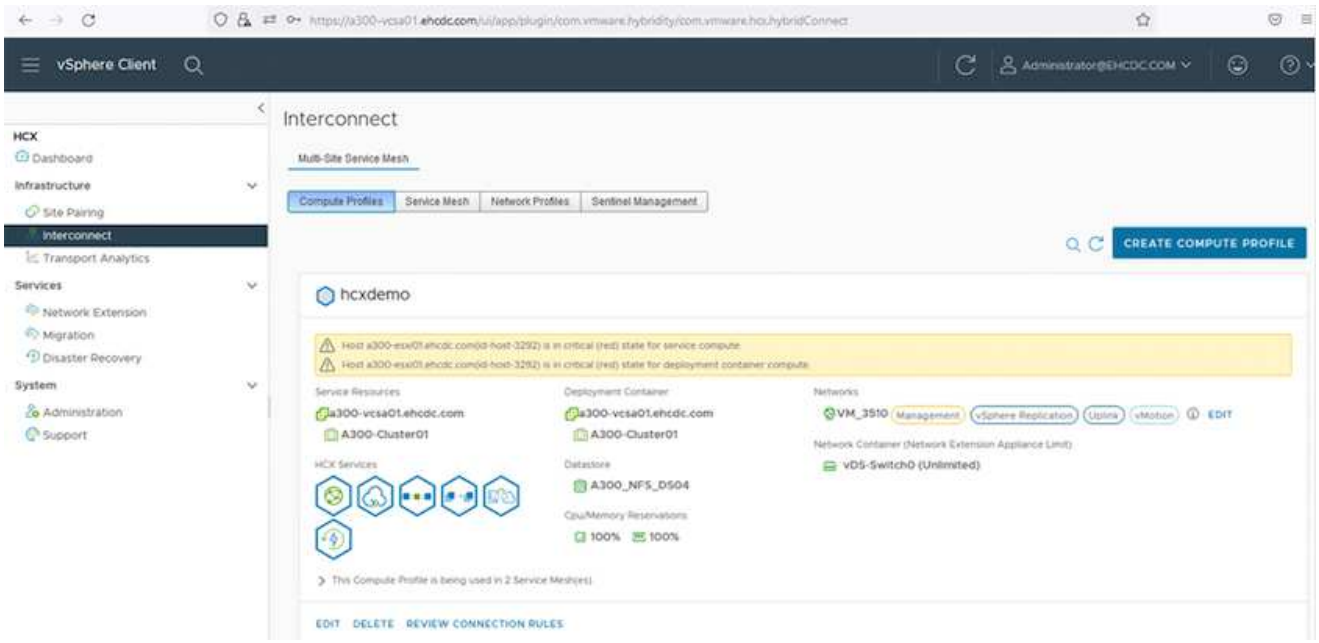


Schritt 5: Netzwerkprofil, Computing-Profil und Service-Mesh konfigurieren

Die VMware HCX Interconnect Service Appliance bietet Replizierungs- und vMotion-basierte Migrationsfunktionen über das Internet und private Verbindungen zum Zielstandort. Das Interconnect bietet Verschlüsselung, Traffic Engineering und VM-Mobilität. Um eine Interconnect Service Appliance zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie unter Infrastruktur die Option **Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile** aus.

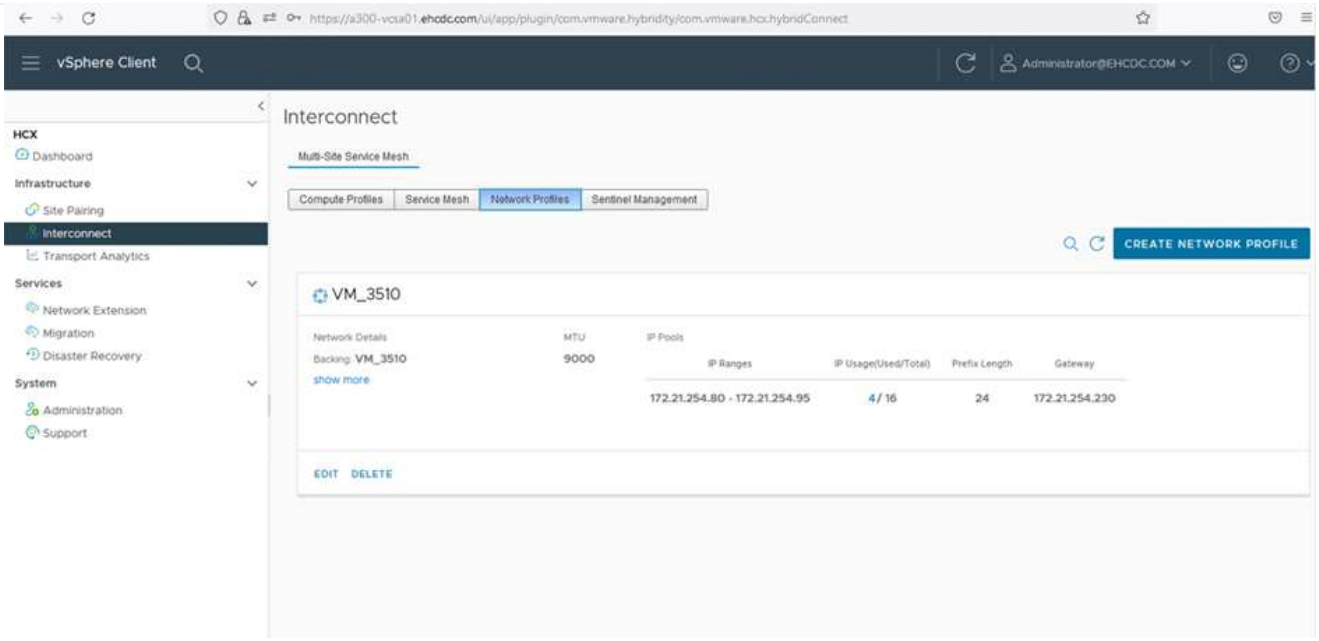
Die Computing-Profile definieren die Implementierungsparameter einschließlich der Appliances, die bereitgestellt werden und welche Teile des VMware Datacenters für den HCX-Service verfügbar sind.



1. Erstellen Sie nach dem Erstellen des Rechenprofils die Netzwerkprofile, indem Sie **Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen** auswählen.

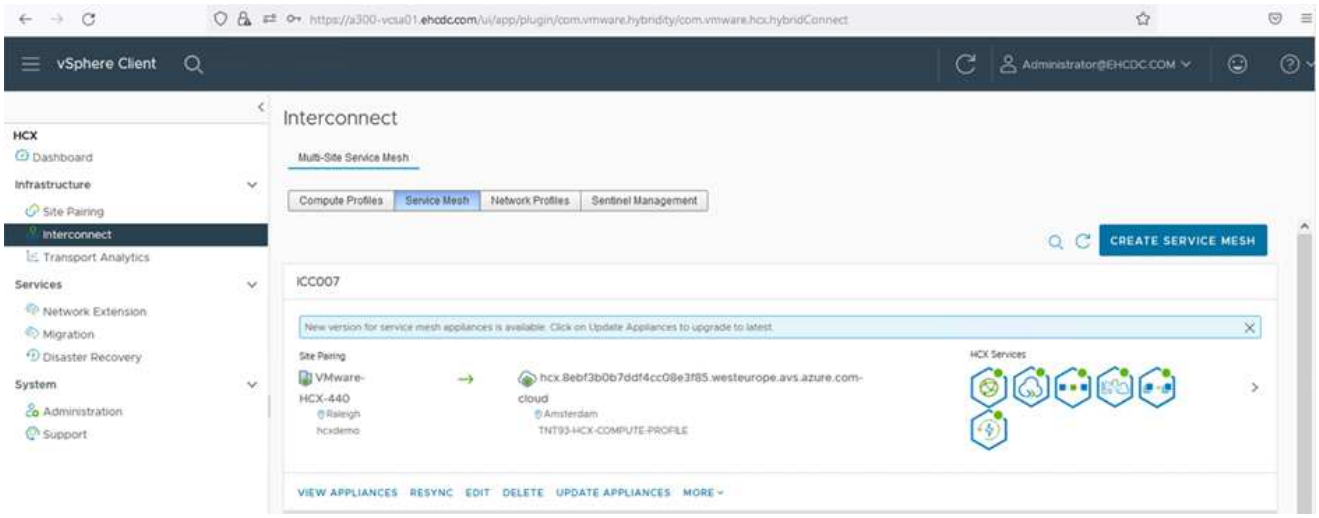
Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

Für diesen Schritt werden mindestens zwei IP-Adressen benötigt. Diese IP-Adressen werden den Interconnect Appliances vom Managementnetzwerk zugewiesen.

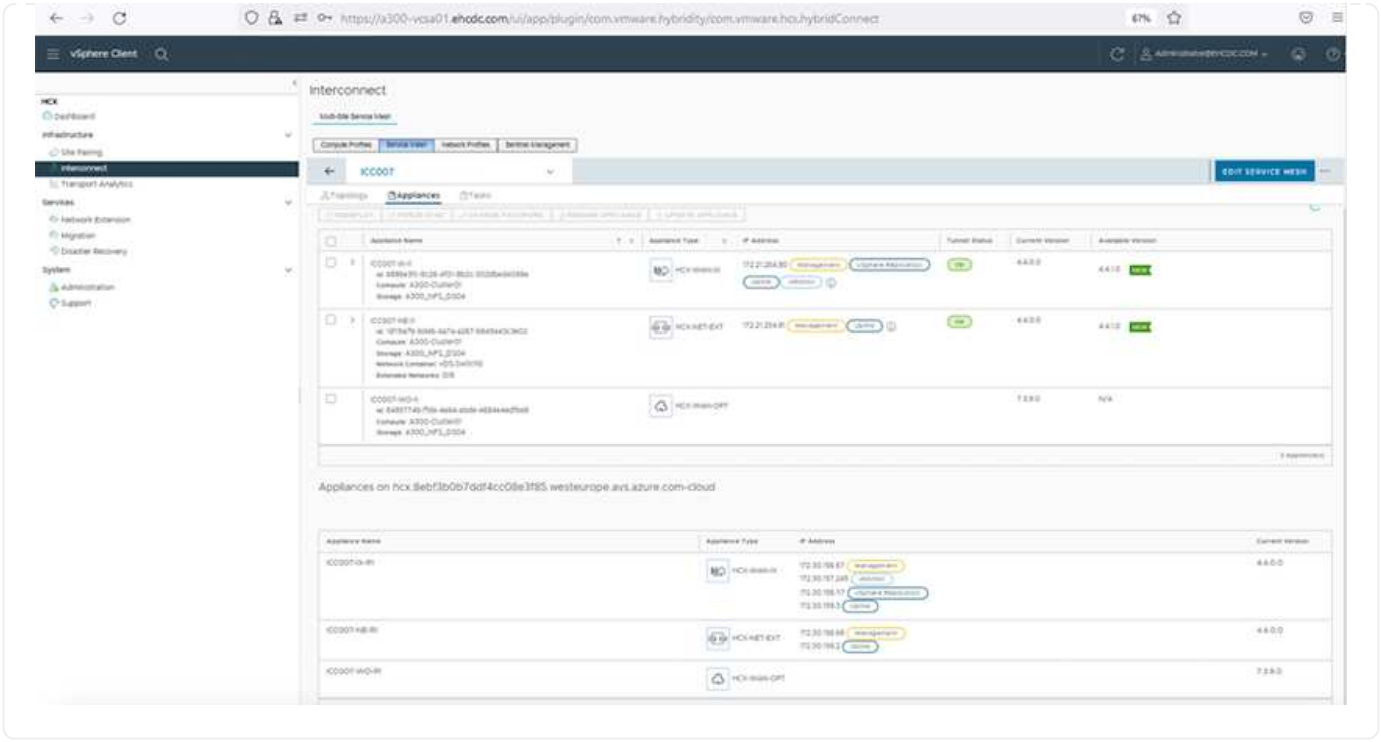


1. Derzeit wurden die Computing- und Netzwerkprofile erfolgreich erstellt.
2. Erstellen Sie das Service Mesh, indem Sie in der Option **Interconnect** die Registerkarte **Service Mesh** auswählen und die On-Premises- und Azure SDDC-Sites auswählen.
3. Das Service Mesh gibt ein lokales und entferntes Compute- und Netzwerkprofilpaar an.

Im Rahmen dieses Prozesses werden die HCX-Appliances sowohl an den Quell- als auch an den Zielstandorten bereitgestellt und automatisch konfiguriert, um eine sichere Transportstruktur zu erstellen.



1. Dies ist der letzte Konfigurationsschritt. Die Implementierung sollte also fast 30 Minuten dauern. Nach der Konfiguration des Service-Mesh ist die Umgebung bereit, wobei die IPsec-Tunnel erfolgreich erstellt wurden, um die Workload-VMs zu migrieren.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

Schritt 6: Migration von Workloads

Workloads können mithilfe verschiedener VMware HCX Migrationstechnologien bidirektional zwischen lokalen und Azure SDDCs migriert werden. VMs können mithilfe von mehreren Migrationstechnologien wie HCX Bulk Migration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (erhältlich mit HCX Enterprise Edition) und HCX OS Assisted Migration (erhältlich mit der HCX Enterprise Edition) in und von VMware HCX Enterprise Edition verschoben werden.

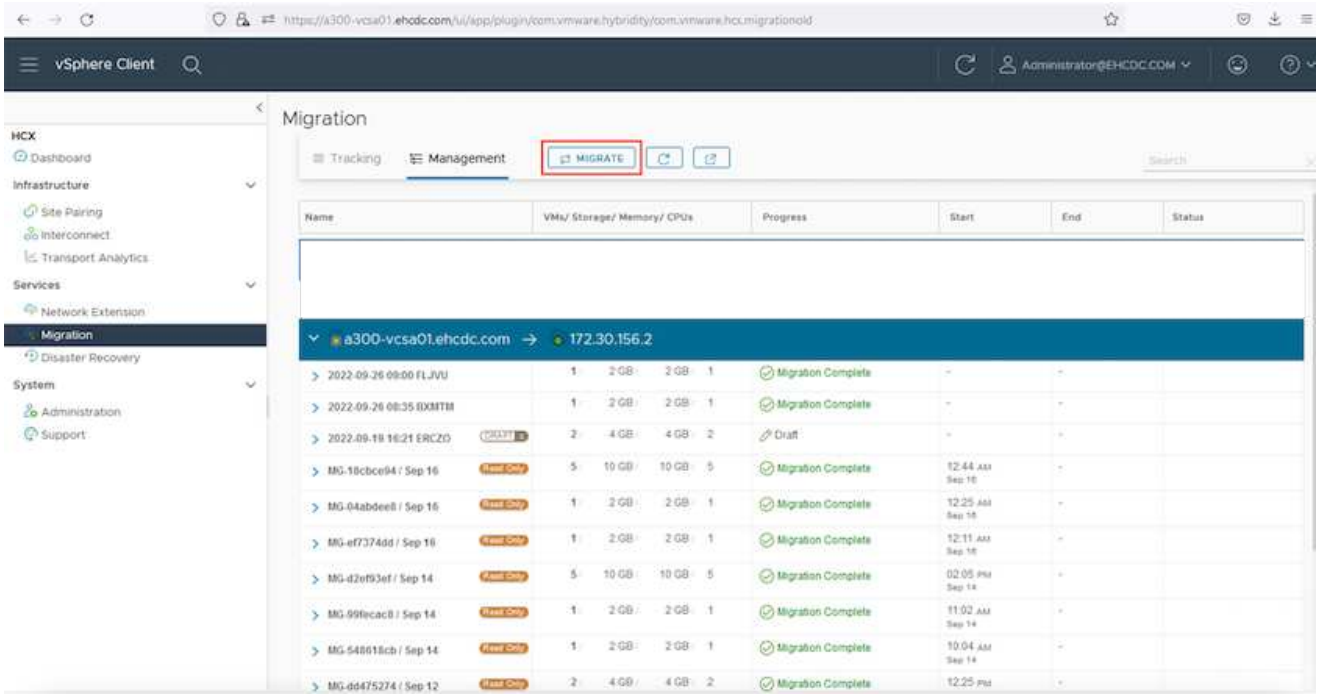
Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter "Migrationstypen von VMware HCX".

Massenmigration

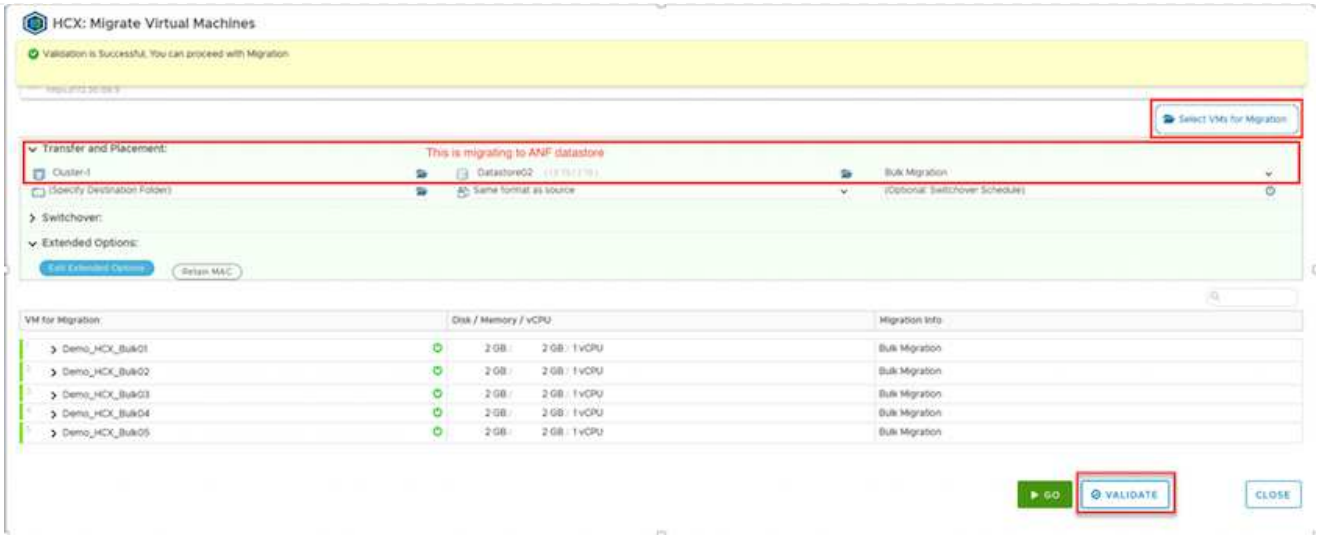
In diesem Abschnitt wird der Migrationsmechanismus für große Datenmengen beschrieben. Während einer Massenmigration nutzt die Funktion zur Massenmigration von HCX vSphere Replication, um Festplattendateien zu migrieren und die VM auf der vSphere HCX-Zielinstanz neu zu erstellen.

Um VM-Massenmigrationen zu initiieren, führen Sie die folgenden Schritte aus:

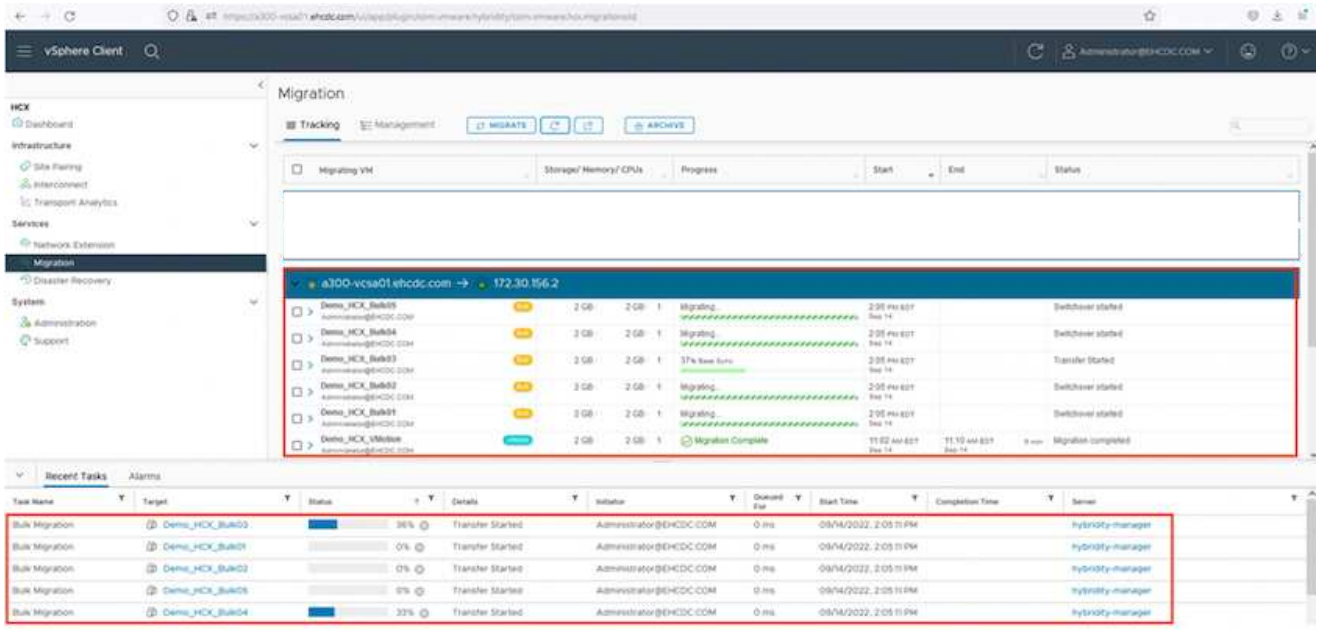
1. Öffnen Sie die Registerkarte * Migrate* unter **Services > Migration**.



1. Wählen Sie unter **Remote-Standortverbindung** die Verbindung mit dem Remote-Standort aus und wählen Sie die Quelle und das Ziel aus. In diesem Beispiel wird als Ziel der SDDC HCX-Endpunkt der Azure VMware-Lösung verwendet.
2. Klicken Sie auf **Select VMs for Migration**. Hier wird eine Liste aller lokalen VMs angezeigt. Wählen Sie die VMs basierend auf dem Ausdruck Match:value aus und klicken Sie auf **Add**.
3. Aktualisieren Sie im Abschnitt **Transfer und Platzierung** die Pflichtfelder (**Cluster**, **Storage**, **Ziel** und **Netzwerk**), einschließlich des Migrationsprofils, und klicken Sie auf **Validieren**.

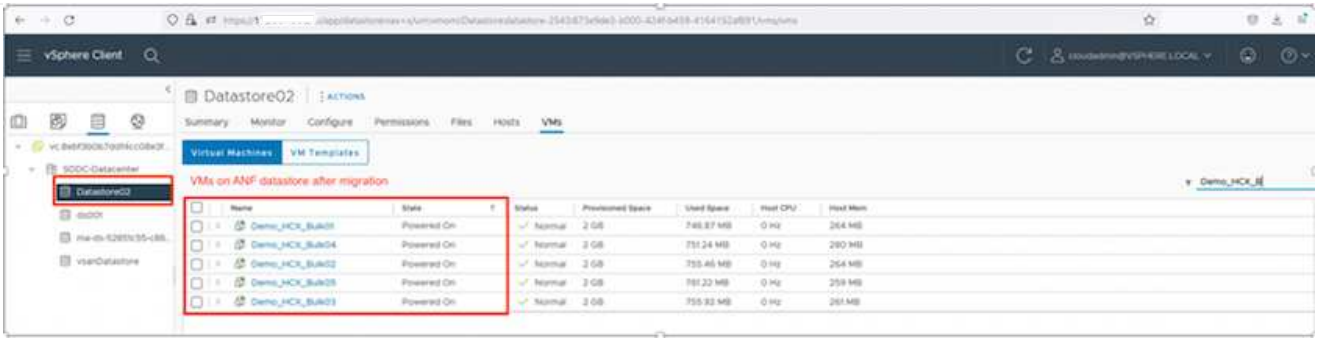


1. Nachdem die Validierungsprüfungen abgeschlossen sind, klicken Sie auf **Go**, um die Migration zu starten.



Während dieser Migration wird auf dem angegebenen Azure NetApp Files Datastore im Ziel-vCenter eine Platzhalterfestplatte erstellt, um die Daten der Quell-VM-Festplatte auf die Platzhalterfestplatten replizieren zu können. HBR wird ausgelöst, um eine vollständige Synchronisierung zum Ziel zu ermöglichen. Nach Abschluss der Baseline wird basierend auf dem RPO-Zyklus (Recovery Point Objective) eine inkrementelle Synchronisierung durchgeführt. Nach Abschluss der vollständigen/inkrementellen Synchronisierung wird die Umschaltung automatisch ausgelöst, es sei denn, ein bestimmter Zeitplan ist festgelegt.

1. Nach Abschluss der Migration können Sie dies durch Zugriff auf das SDDC Ziel-vCenter validieren.

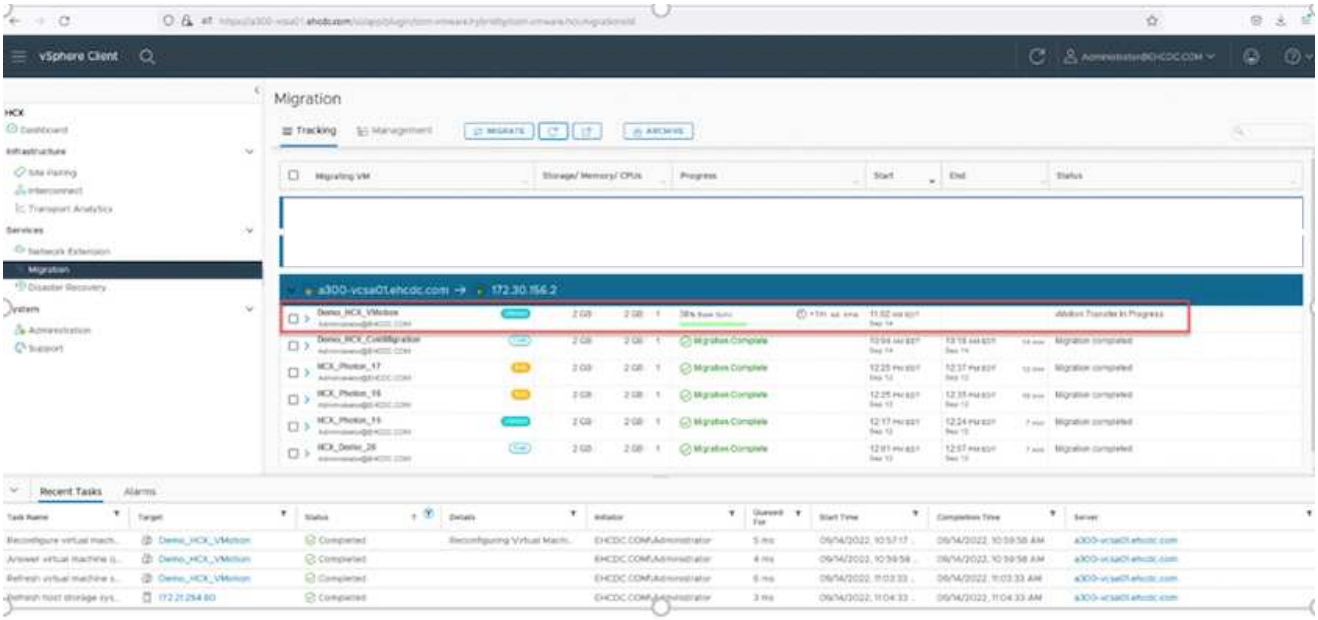


Weitere und detaillierte Informationen zu verschiedenen Migrationsoptionen und zur Migration von Workloads von On-Premises-Systemen zur Azure VMware Lösung mithilfe von HCX finden Sie unter "VMware HCX-Benutzerhandbuch".

Wenn Sie mehr über diesen Prozess erfahren möchten, sehen Sie sich das folgende Video an:

Workload-Migration mithilfe von HCX

Hier sehen Sie einen Screenshot der HCX vMotion Option.



Wenn Sie mehr über diesen Prozess erfahren möchten, sehen Sie sich das folgende Video an:

HCX vMotion

Stellen Sie sicher, dass für die Migration ausreichend Bandbreite zur Verfügung steht.

Der Ziel-ANF-Datastore sollte über genügend Speicherplatz für die Migration verfügen.

Schlussfolgerung

Ganz gleich, ob Sie nur auf All-Cloud- oder Hybrid Cloud-Umgebungen abzielen und Daten in On-Premises-Storage eines beliebigen Typs oder Anbieters speichern – Azure NetApp Files und HCX bieten hervorragende

Optionen für die Implementierung und Migration der Applikations-Workloads und senken gleichzeitig die TCO, da die Datenanforderungen nahtlos auf die Applikationsebene integriert sind. Wie auch immer der Anwendungsfall ist: Wählen Sie Azure VMware Lösung zusammen mit Azure NetApp Files, um schnell von den Vorteilen der Cloud zu profitieren, eine konsistente Infrastruktur und Abläufe vor Ort und in mehreren Clouds, bidirektionale Portabilität von Workloads und Kapazität und Performance der Enterprise-Klasse. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, die zum Verbinden des Storage und zur Migration von VMs mithilfe von VMware vSphere Replication, VMware vMotion oder sogar NFS (Network File Copy) verwendet werden.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können Azure NetApp Files nun als Datastore auf dem Azure VMware Solution SDDC verwenden.
- Daten lassen sich problemlos von lokalen Systemen zu Azure NetApp Files Datastores migrieren.
- Erweitern und verkleinern Sie den Azure NetApp Files-Datastore einfach, um die Kapazitäts- und Performance-Anforderungen während der Migration zu erfüllen.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie unter den folgenden Links:

- Dokumentation der Azure VMware Lösung

"https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Azure NetApp Files-Dokumentation

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- VMware HCX-Benutzerhandbuch

"https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"

Regionale Verfügbarkeit – Ergänzender NFS-Datenspeicher für ANF

Die Verfügbarkeit von zusätzlichen NFS-Datenspeichern auf Azure/AVS wird von Microsoft definiert. Zunächst müssen Sie feststellen, ob sowohl AVS als auch ANF in einer bestimmten Region verfügbar sind. Als Nächstes müssen Sie ermitteln, ob der zusätzliche ANF NFS-Datastore in dieser Region unterstützt wird.

- Überprüfen Sie die Verfügbarkeit von AVS und ANF "Hier".
- Prüfen Sie die Verfügbarkeit des zusätzlichen ANF NFS-Datenspeichers "Hier".

NetApp Funktionen für die Google Cloud Platform GSCVE

Weitere Informationen zu den Funktionen, die NetApp für die Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) bietet – von NetApp als Storage-Gerät mit Gastverbindung oder als ergänzenden NFS-Datastore bis hin zur Migration von Workflows zur Erweiterung/Bursting in die Cloud, Backup/Restore und Disaster Recovery.

Springen Sie zum Abschnitt zum gewünschten Inhalt, indem Sie eine der folgenden Optionen auswählen:

- "GCVE wird in GCP konfiguriert"
- "NetApp Storage-Optionen für GCVE"
- "NetApp/VMware Cloud-Lösungen"

GCVE wird in GCP konfiguriert

Wie bei lokalen Systemen ist die Planung einer Cloud-basierten Virtualisierungsumgebung eine entscheidende Voraussetzung für eine erfolgreiche, sofort einsatzbereite Umgebung zum Erstellen von VMs und Migrationen.

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und managen und in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp Storage verwenden.

Der in-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP und Cloud Volumes Services mit GCVE.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von GCVE
- Aktivieren Sie den privaten Zugriff auf GCVE

Details anzeigen "Konfigurationsschritte für GCVE".

NetApp Storage-Optionen für GCVE

NetApp Storage kann in GCP GCVE auf verschiedene Weise genutzt werden – entweder als „Raten“ verbunden oder als zusätzlicher NFS-Datenspeicher.

Besuchen Sie "Unterstützte NetApp Storage-Optionen" Finden Sie weitere Informationen.

Google Cloud unterstützt NetApp Storage in den folgenden Konfigurationen:

- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- Cloud Volumes Service (CVS) als Storage mit Gastverbunden
- Cloud Volumes Service (CVS) als zusätzlicher NFS Datastore

Details anzeigen "Speicheroptionen für die Gastverbindung für GCVE".

Weitere Informationen "Unterstützung von NetApp Cloud Volumes Service-Datastores für die Google Cloud VMware Engine (NetApp Blog)" Oder "Verwendung von NetApp CVS als Datastores für Google Cloud VMware Engine (Google Blog)"

Anwendungsfälle Für Lösungen

Mit Cloud-Lösungen von NetApp und VMware können viele Anwendungsfälle problemlos in Azure AVS implementiert werden. se-Fälle werden für jeden der von VMware definierten Cloud-Bereiche definiert:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Erweitern
- Migrieren

"Informieren Sie sich über die NetApp Lösungen für Google Cloud GCVE"

Schutz von Workloads in GCP/GCVE

Applikationskonsistente Disaster Recovery mit NetApp SnapCenter und Veeam Replizierung

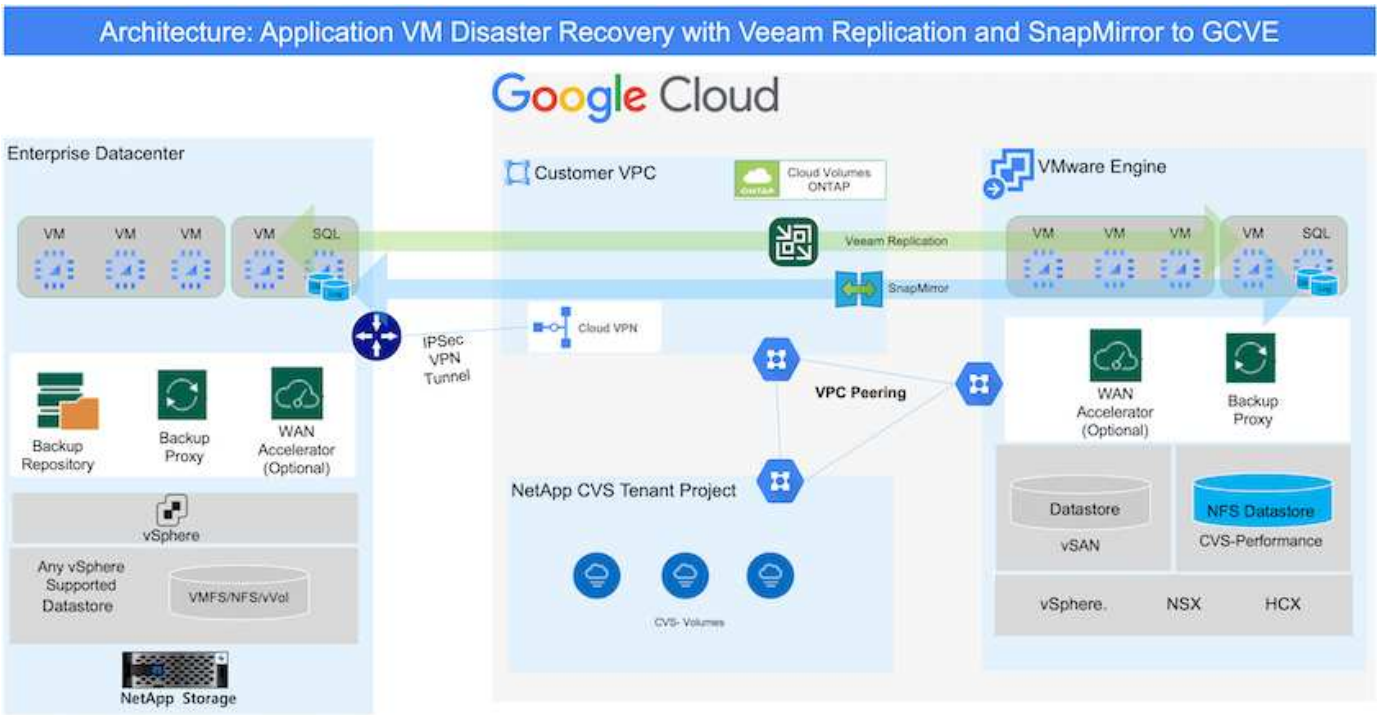
Autoren: Suresh ThopPay, NetApp

Überblick

Viele Kunden suchen nach einer effektiven Disaster Recovery-Lösung für ihre Applikations-VMs, die auf VMware vSphere gehostet werden. Viele von ihnen nutzen ihre bestehende Backup-Lösung, um im Diaster Recovery durchzuführen.
Oft erhöht diese Lösung die RTO und entspricht nicht ihren Erwartungen. Um RPO und RTO zu reduzieren, kann die Veeam VM-Replizierung sogar von On-Premises zu GCVE genutzt werden, sofern Netzwerkverbindungen und Umgebung mit entsprechenden Berechtigungen verfügbar sind.
HINWEIS: Veeam VM Replication schützt keine über VM-Gastsysteme verbundenen Storage-Geräte wie iSCSI- oder NFS-Mounts innerhalb der Gast-VM. Sie müssen sie separat schützen.

Für eine applikationskonsistente Replizierung für SQL VM und zur Reduzierung des RTO wurde SnapCenter zum Orchestrieren von snapmirror Vorgängen von SQL Datenbank- und Protokoll-Volumes eingesetzt.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.

Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

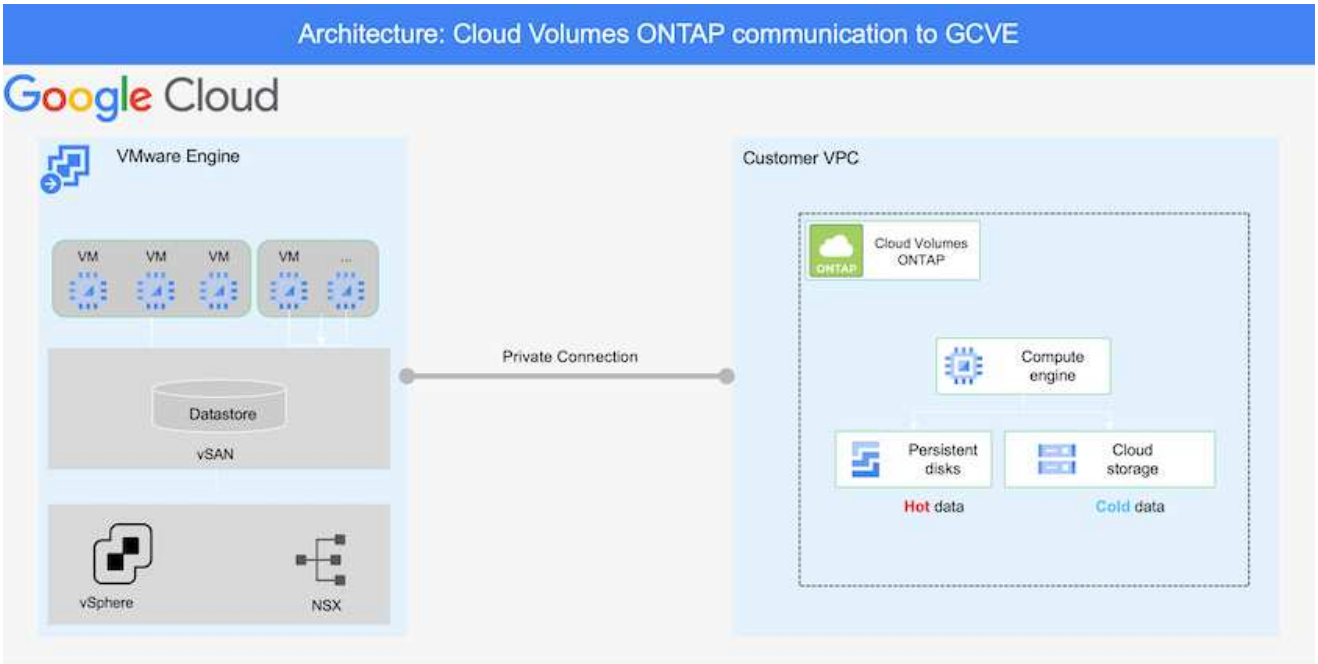
Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mit BlueXP innerhalb des entsprechenden Abonnements und virtuellen Netzwerks Cloud Volumes ONTAP mit der korrekten Instanzgröße bereit.
   a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
   b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Ausfalls die SnapMirror Beziehung mit BlueXP auf und lösen Sie Failover von Virtual Machines mit Veeam aus.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
   b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

Der erste Schritt besteht darin, Cloud Volumes ONTAP auf Google Cloud (zu konfigurieren"cvo") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Überprüfen Sie den SQL VM-Schutz mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer, bis das SDDC den Betrieb aufrecht erhalten hat. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Der NetApp Cloud Volume Service für NFS-Datastore und die Cloud Volumes ONTAP für SQL-Datenbanken und das Protokoll können in jede VPC implementiert werden. GCVE sollte über eine private Verbindung zu dieser VPC verfügen, um den NFS-Datastore zu mounten und die VM mit den iSCSI-LUNs zu verbinden.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.
"Das Installationsverfahren finden Sie in der Veeam-Dokumentation"
Weitere Informationen finden Sie unter "Migration mit Veeam Replication"

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Failover von Microsoft SQL Server VM

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung

- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.

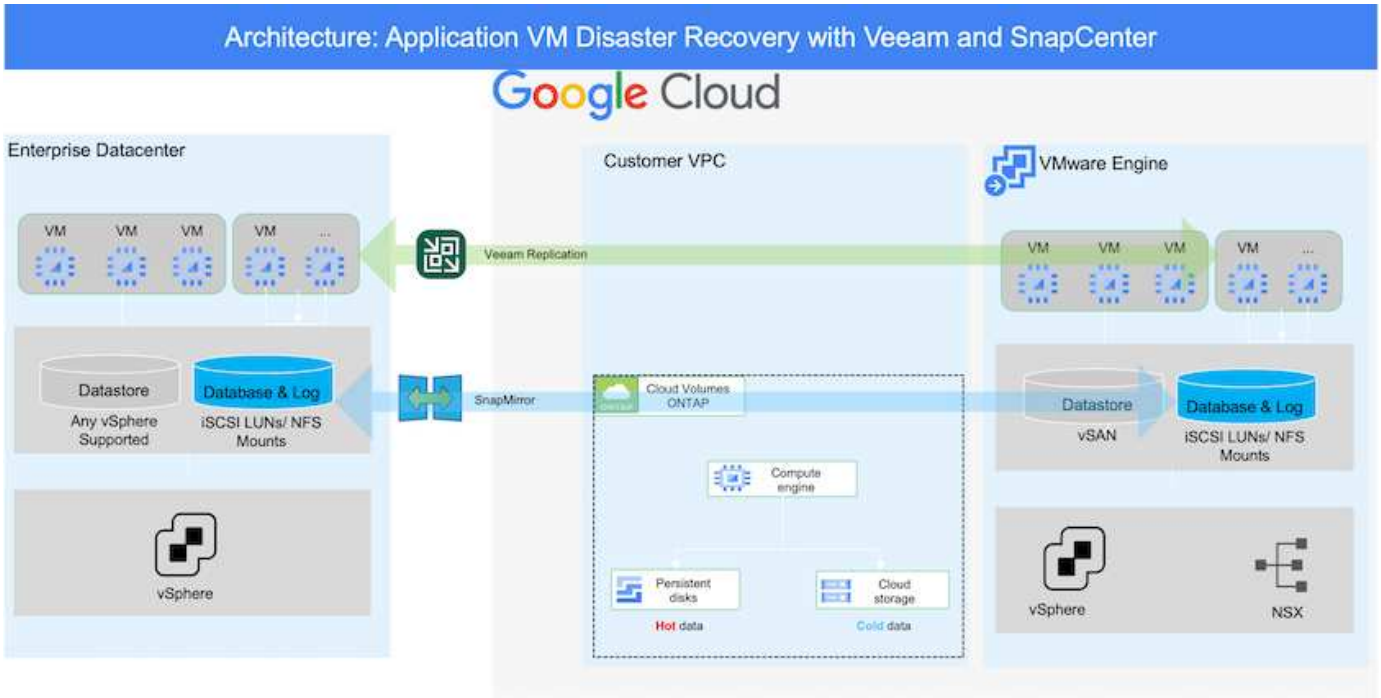
Disaster Recovery für Applikationen mit SnapCenter, Cloud Volumes ONTAP und Veeam Replication

Autoren: Suresh ThopPay, NetApp

Überblick

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die Storage mit Anbindung des Gastspeichers verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, die in Google Cloud ausgeführt werden. Dies bezieht sich auf Applikationsdaten, doch was ist mit den eigentlichen VMs selbst. Disaster Recovery sollte alle abhängigen Komponenten, einschließlich Virtual Machines, VMDKs, Applikationsdaten und mehr, abdecken. Dazu kann SnapMirror zusammen mit Veeam verwendet werden, um Workloads, die von On-Premises zu Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen und gleichzeitig mit vSAN Storage für VM-VMDKs zu verwenden.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.

> Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

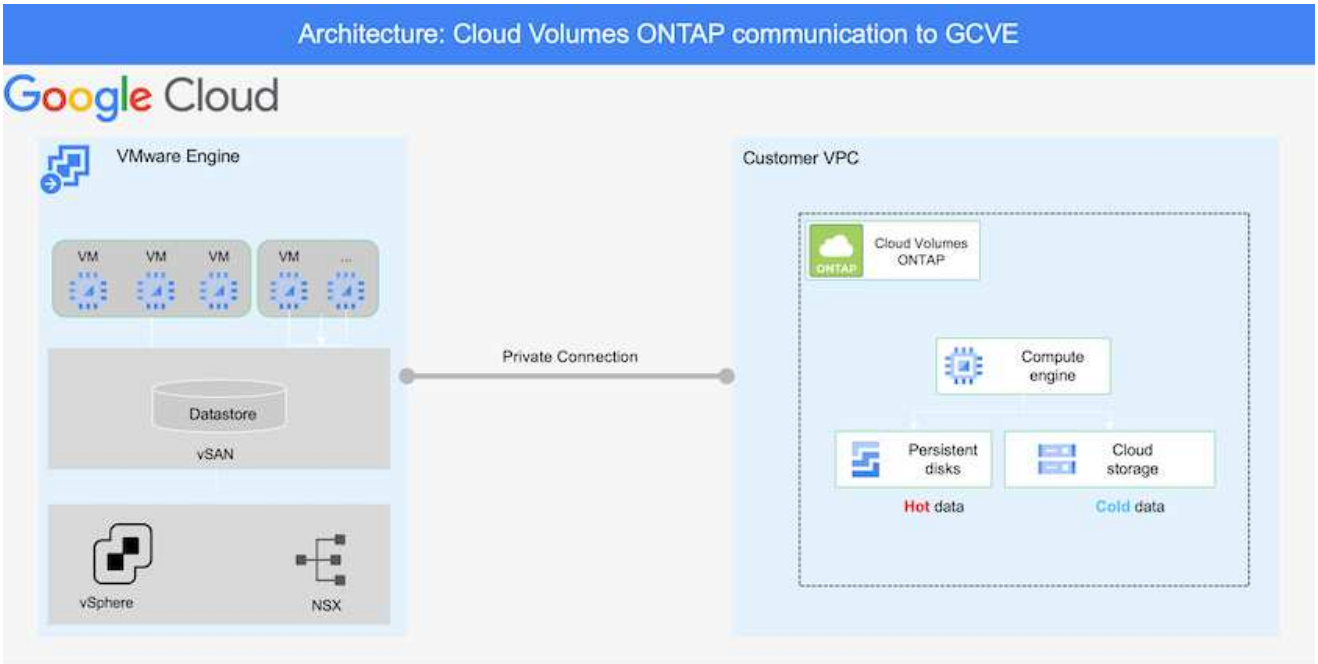
Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mithilfe von Cloud Manager Cloud Volumes ONTAP mit der richtigen Instanzgröße innerhalb des entsprechenden Abonnements und des virtuellen Netzwerks bereit.
    a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
    b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Notfallereignisses die SnapMirror Beziehung mithilfe von Cloud Manager auf und lösen Sie das Failover von Virtual Machines mit Veeam aus.
    a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
    b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

Der erste Schritt besteht darin, Cloud Volumes ONTAP auf Google Cloud (zu konfigurieren"cvo") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Einrichtung der Replikation mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer, bis das SDDC den Betrieb aufrecht erhalten hat. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Cloud Volumes ONTAP kann in jede VPC implementiert werden und GCVE sollte über eine private Verbindung zu dieser VPC verfügen, damit VM-Verbindung mit iSCSI-LUNs hergestellt werden kann.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Das Installationsverfahren finden Sie in der Veeam-Dokumentation"]

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

VSphere VM Replication Job einrichten

Failover von Microsoft SQL Server VM

Failover von Microsoft SQL Server VM

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.

Migration von Workloads auf GCP/GCVE

Workloads mit VMware HCX - QuickStart Guide auf den NetApp Cloud Volume Service Datastore auf der Google Cloud VMware Engine migrieren

Autor(en): NetApp Solutions Engineering

Übersicht: Migration von Virtual Machines mit VMware HCX, NetApp Cloud Volume Service Datastores und Google Cloud VMware Engine (GCVE)

Eine der gängigsten Anwendungsfälle für die Google Cloud VMware Engine und einen Cloud Volume Service-Datastore ist die Migration von VMware Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmechanismen zum Verschieben von On-Premises-Virtual Machines (VMs) und deren Daten in NFS-Datastores des Cloud Volume Service.

VMware HCX ist primär eine Migrationsplattform, die entwickelt wurde, um die Migration von Applikationen, die Ausbalancierung von Workloads und sogar Business Continuity Cloud-übergreifend zu vereinfachen. Dies ist Teil von Google Cloud VMware Engine Private Cloud und bietet zahlreiche Möglichkeiten zur Migration von Workloads und kann für Disaster-Recovery-Vorgänge (DR) genutzt werden.

Dieses Dokument enthält eine Schritt-für-Schritt-Anleitung für die Bereitstellung von Cloud Volume Service Datastore. Anschließend werden alle wichtigen Komponenten von VMware HCX heruntergeladen, implementiert und konfiguriert, einschließlich aller wichtigen Komponenten vor Ort und der Google Cloud VMware Engine Seite mit Interconnect, Netzwerkerweiterung und WAN-Optimierung für die Aktivierung verschiedener VM-Migrationsmechanismen.

VMware HCX arbeitet mit jedem Datenspeichertyp zusammen, da die Migration auf VM-Ebene erfolgt. Daher eignet sich dieses Dokument für bestehende NetApp Kunden und andere Kunden, die den Cloud Volume Service mit der Google Cloud VMware Engine als kostengünstige VMware Cloud-Implementierung planen.

Allgemeine Schritte

Diese Liste enthält die grundlegenden Schritte, die zum Pairing und Migrieren der VMs zu HCX Cloud Manager auf der Google Cloud VMware Engine Seite von HCX Connector vor Ort erforderlich sind:

1. Bereiten Sie HCX über das Google VMware Engine Portal vor.
2. Laden Sie das Installationsprogramm für die HCX Connector Open Virtualization Appliance (OVA) im lokalen VMware vCenter Server herunter und implementieren Sie es.
3. HCX mit dem Lizenzschlüssel aktivieren.
4. Verbinden Sie den lokalen VMware HCX Connector mit der Google Cloud VMware Engine HCX Cloud Manager.
5. Sie konfigurieren das Netzwerkprofil, das Computing-Profil und das Service-Mesh.
6. (Optional) Sie können eine Netzwerkerweiterung vornehmen, um bei Migrationen eine erneute IP-Adresse zu vermeiden.
7. Validieren des Appliance-Status und Sicherstellen der Möglichkeit der Migration
8. Migration der VM-Workloads

Voraussetzungen

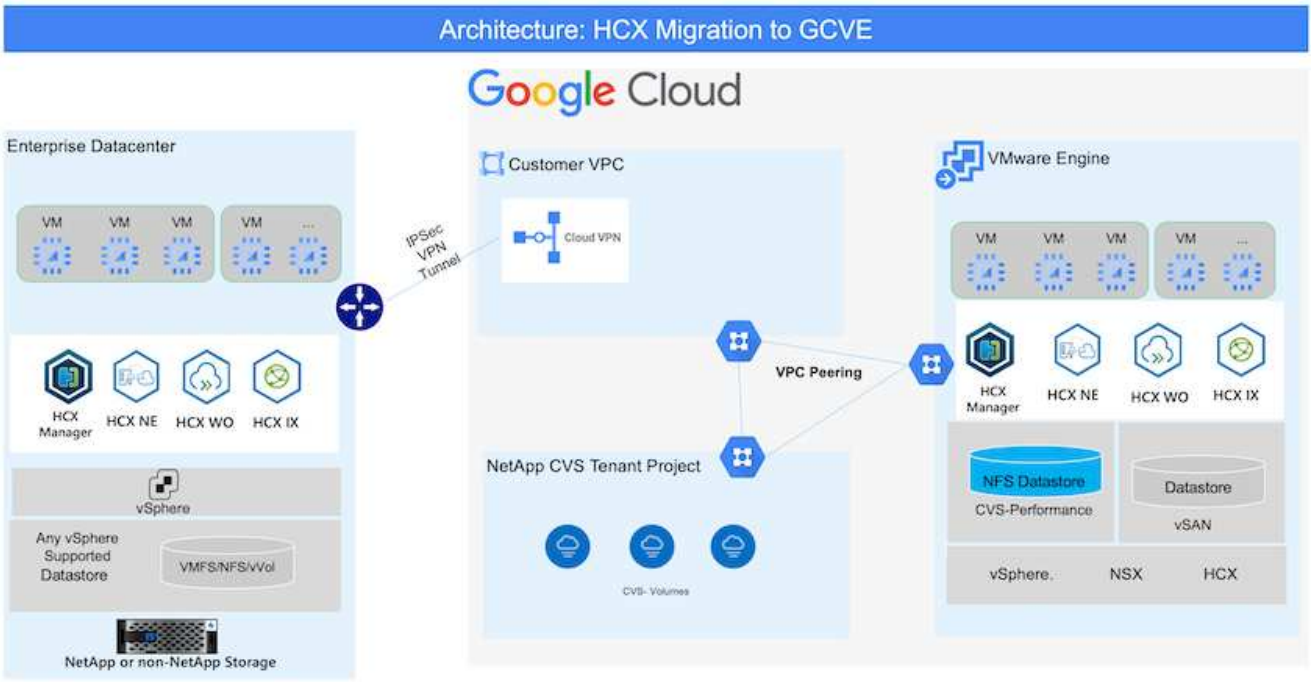
Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "Verlinken". Nachdem die Voraussetzungen, einschließlich Konnektivität, vorhanden sind, laden Sie den HCX-Lizenzschlüssel aus dem Google Cloud VMware Engine-Portal herunter. Nach dem Herunterladen des OVA-Installationsprogramms gehen Sie wie unten beschrieben mit der Installation vor.

> HCX Advanced ist die Standardoption und die VMware HCX Enterprise Edition ist auch über ein Support-Ticket erhältlich und wird ohne zusätzliche Kosten unterstützt. Siehe "Dieser Link"

- Verwenden Sie ein vorhandenes softwaredefiniertes Google Cloud VMware Engine Datacenter (SDDC) oder erstellen Sie mithilfe dieses Modells eine Private Cloud "Link von NetApp" Oder hier "Google-Link".
- Die Migration von VMs und zugehörigen Daten vom lokalen Datacenter mit VMware vSphere erfordert Netzwerkkonnektivität vom Datacenter zur SDDC-Umgebung. Vor der Migration von Workloads "Einrichten eines Cloud-VPN oder einer Cloud Interconnect-Verbindung" Zwischen der lokalen Umgebung und der jeweiligen Private Cloud verschieben.
- Der Netzwerkpfad von der lokalen VMware vCenter Server Umgebung zur privaten Cloud der Google Cloud VMware Engine muss die Migration von VMs mithilfe von vMotion unterstützen.
- Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und -Ports" Sind für vMotion Traffic zwischen dem lokalen vCenter Server und SDDC vCenter zulässig.
- Cloud Volume Service NFS-Volume sollte als Datastore in der Google Cloud VMware Engine gemountet werden. Befolgen Sie die in diesem Schritt beschriebenen Schritte "Verlinken" Cloud Volume Service-Datenspeicher an Google Cloud VMware Engines Hosts anhängen.

Übergeordnete Architektur

Die Lab-Umgebung vor Ort für diese Validierung wurde zu Testzwecken über ein Cloud-VPN verbunden, das On-Premises-Konnektivität mit Google Cloud VPC ermöglicht.



Nähere Informationen zu HCX finden Sie unter "Link zu VMware"

Lösungsimplementierung

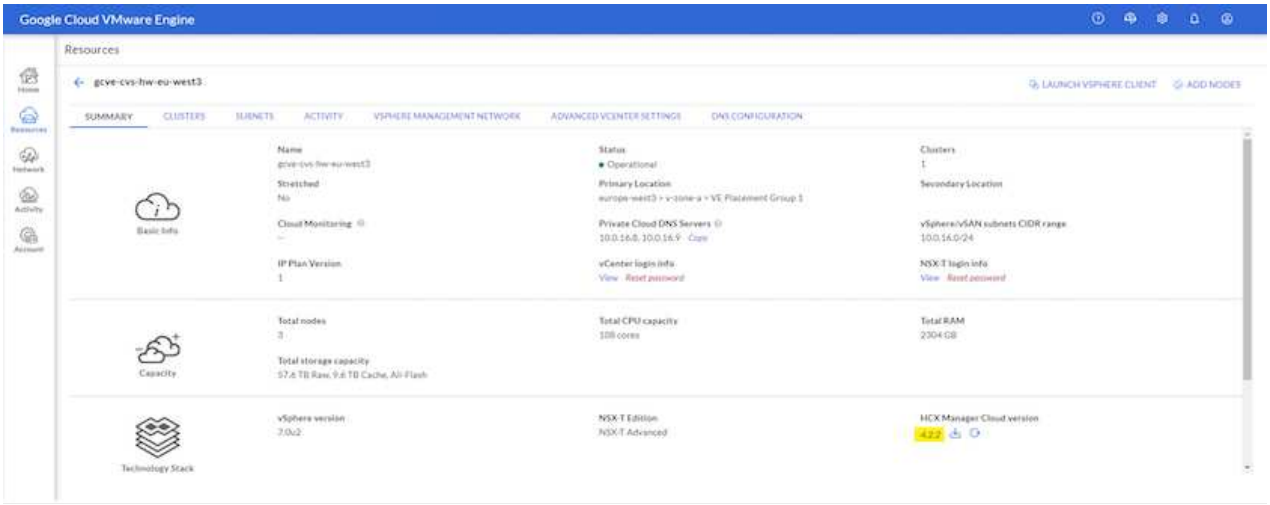
Führen Sie die folgenden Schritte aus, um die Implementierung dieser Lösung abzuschließen:

Schritt 1: HCX über das Google VMware Engine Portal vorbereiten

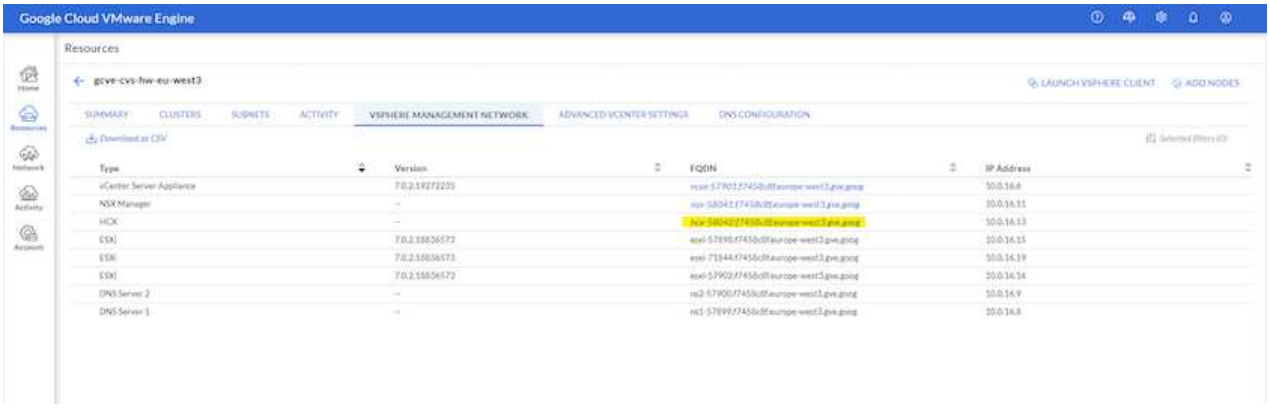
HCX Cloud Manager wird automatisch installiert, wenn Sie eine Private Cloud mit VMware Engine bereitstellen. Gehen Sie wie folgt vor, um die Standortpaarung vorzubereiten:

1. Melden Sie sich beim Google VMware Engine Portal an und melden Sie sich beim HCX Cloud Manager an.

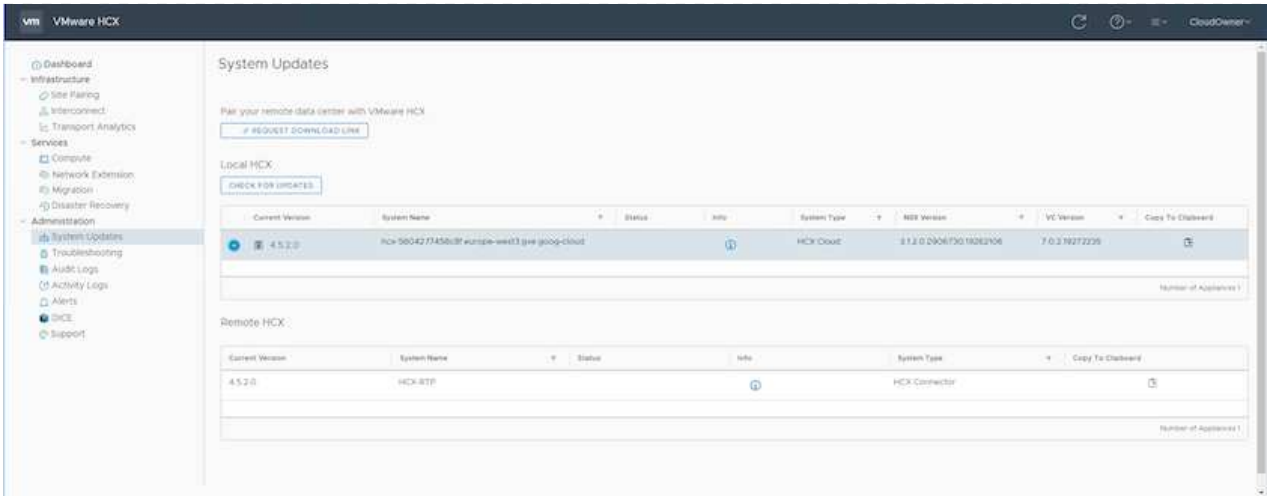
   Sie können sich bei der HCX Console anmelden, indem Sie auf den Link zur HCX-Version klicken



   Oder klicken Sie unter der Registerkarte vSphere Management Network auf HCX FQDN.



2. Gehen Sie in HCX Cloud Manager zu **Administration > System Updates**.
3. Klicken Sie auf **Download-Link anfordern** und laden Sie die OVA-Datei herunter.



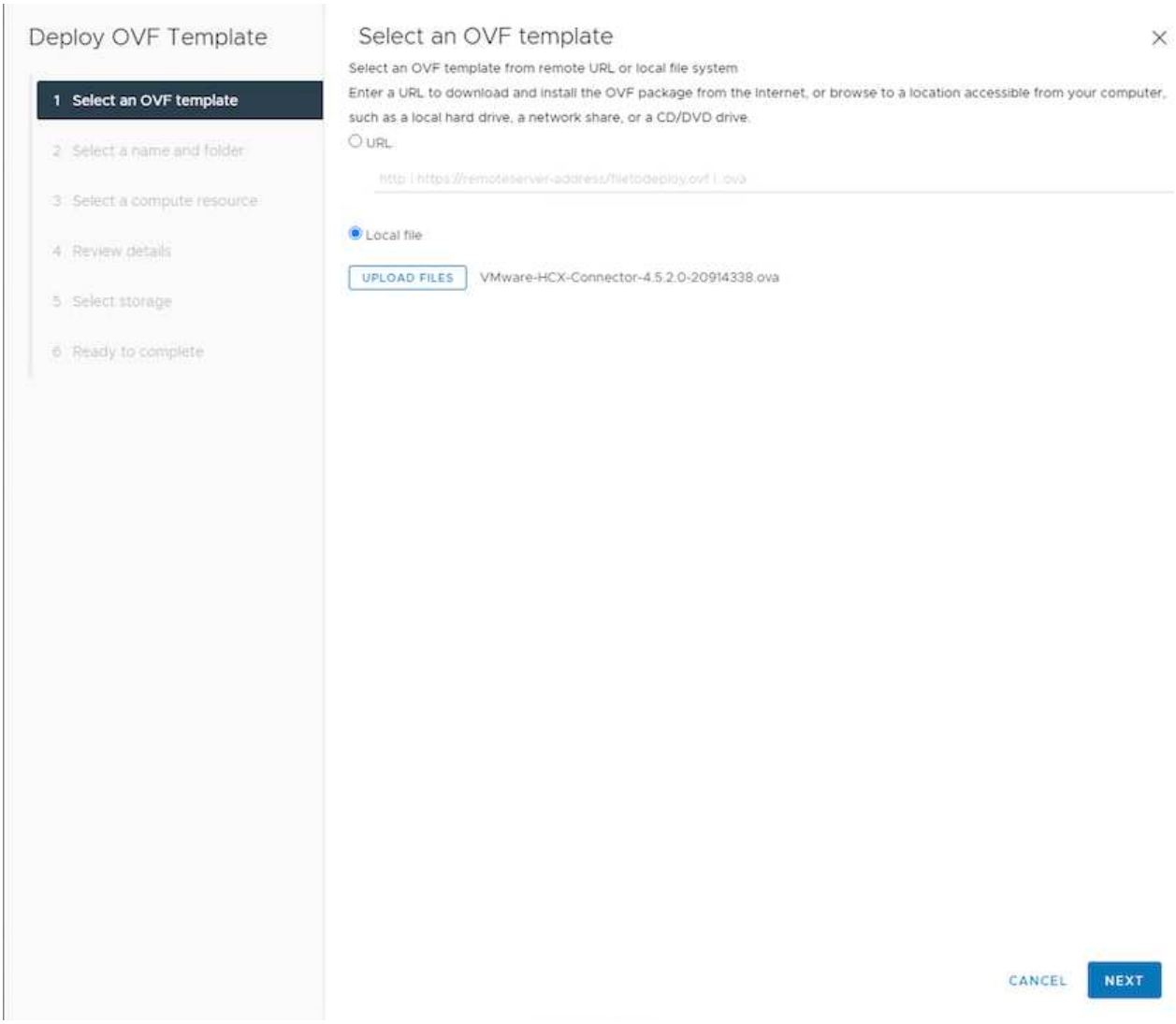
4. Aktualisieren Sie HCX Cloud Manager auf die neueste Version, die über die Benutzeroberfläche von HCX Cloud Manager verfügbar ist.

Schritt 2: Stellen Sie das Installationsprogramm OVA im lokalen vCenter Server bereit

Damit der On-Premises Connector eine Verbindung zum HCX Manager in der Google Cloud VMware Engine herstellen kann, müssen die entsprechenden Firewall-Ports in der On-Premises-Umgebung geöffnet sein.

So laden Sie den HCX Connector auf dem lokalen vCenter Server herunter und installieren ihn:

1. Laden Sie die ova von der HCX-Konsole auf Google Cloud VMware Engine wie im vorherigen Schritt angegeben herunter.
2. Nachdem die OVA heruntergeladen wurde, stellen Sie sie in der lokalen VMware vSphere Umgebung mithilfe der Option **Deploy OVF Template** bereit.



3. Geben Sie alle erforderlichen Informationen für die OVA-Bereitstellung ein, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um die OVA des VMware HCX-Connectors bereitzustellen.

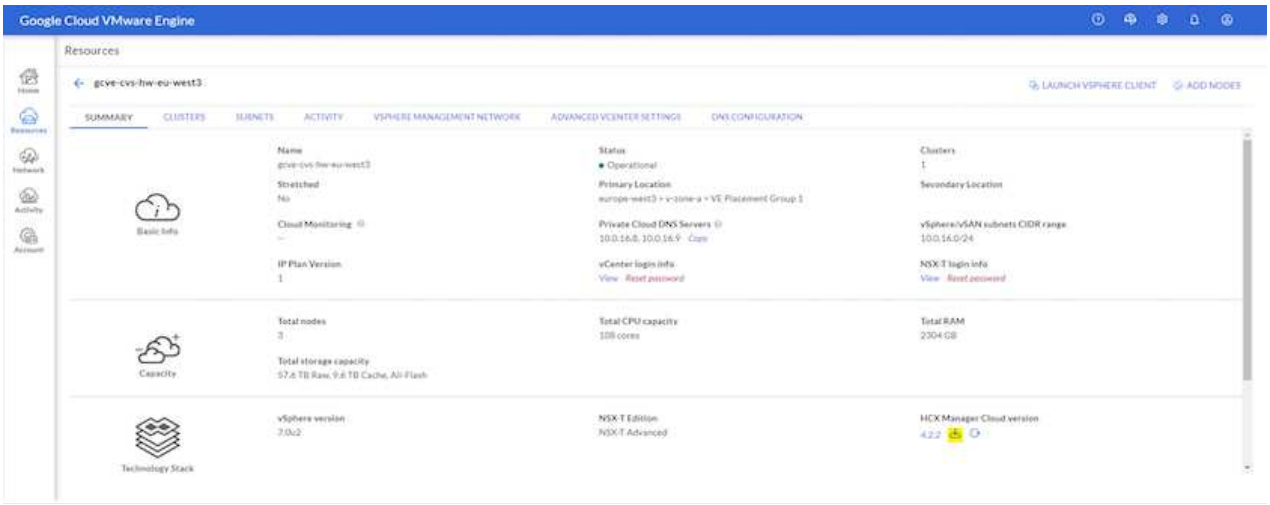
   Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "VMware HCX-Benutzerhandbuch".

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie den VMware HCX Connector OVA vor Ort bereitgestellt und das Gerät gestartet haben, führen Sie die folgenden Schritte aus, um den HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel aus dem Google Cloud VMware Engine Portal und aktivieren Sie ihn im VMware HCX Manager.

1. Klicken Sie im VMware Engine-Portal auf Ressourcen, wählen Sie die Private Cloud und **Klicken Sie auf das Download-Symbol unter HCX Manager Cloud Version**
.



Öffnen Sie die heruntergeladene Datei und kopieren Sie die Zeichenfolge für den Lizenzschlüssel.

2. Melden Sie sich beim lokalen VMware HCX Manager unter an "https://hcxmanagerIP:9443" Administratordaten werden verwendet.

> Verwenden Sie die hcxmanagerIP und das Passwort, das während der OVA-Bereitstellung definiert wurde.

3. Geben Sie in der Lizenzierung den aus Schritt 3 kopierten Schlüssel ein und klicken Sie auf **Aktivieren**.

> Der HCX-Connector sollte über einen Internetzugang verfügen.

4. Geben Sie unter **Datacenter Location** den nächstgelegenen Standort für die Installation des VMware HCX Managers vor Ort an. Klicken Sie Auf **Weiter**.
5. Aktualisieren Sie unter **Systemname** den Namen und klicken Sie auf **Weiter**.
6. Klicken Sie Auf **Ja, Weiter**.
7. Geben Sie unter **Connect Your vCenter** den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des vCenter Servers und die entsprechenden Anmeldeinformationen an und klicken Sie auf **Continue**.

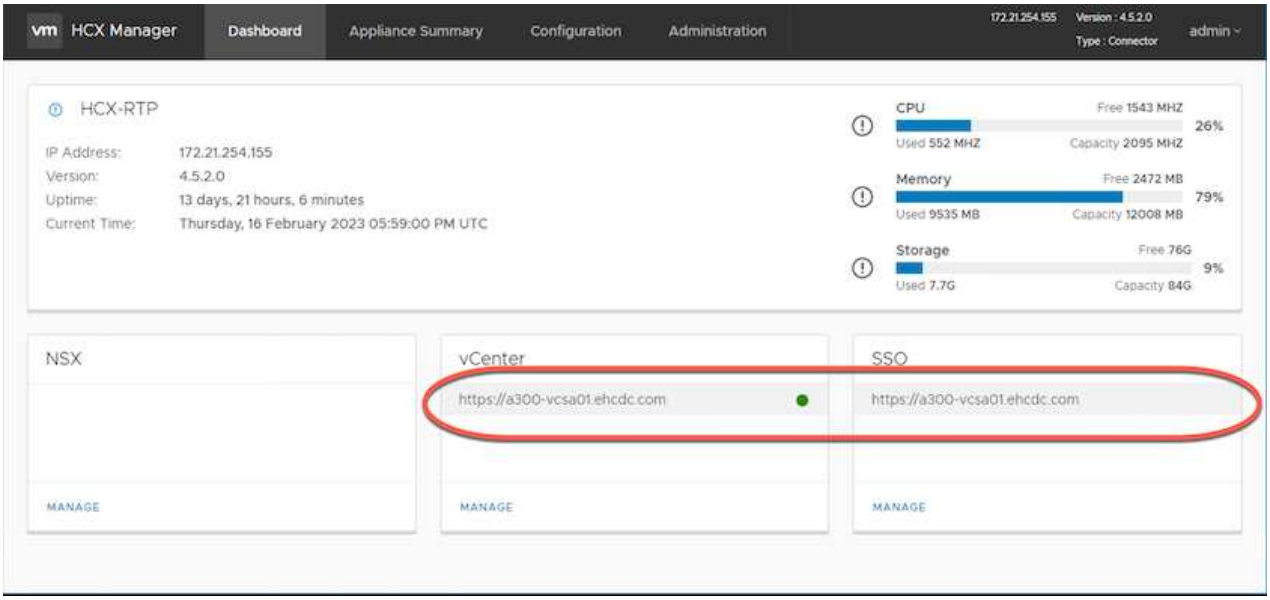
> Verwenden Sie den FQDN, um Verbindungsprobleme später zu vermeiden.

8. Geben Sie unter **SSO/PSC** konfigurieren den (PSC) FQDN oder die IP-Adresse des Plattform-Services-Controllers an und klicken Sie auf **Weiter**.

Geben Sie für Embedded PSC den VMware vCenter Server FQDN oder die IP-Adresse ein.

9. Überprüfen Sie, ob die eingegebenen Informationen korrekt sind, und klicken Sie auf **Neustart**.
10. Nach dem Neustart der Dienste wird vCenter Server auf der angezeigten Seite grün angezeigt. Sowohl vCenter Server als auch SSO müssen über die entsprechenden Konfigurationsparameter verfügen, die mit der vorherigen Seite übereinstimmen sollten.

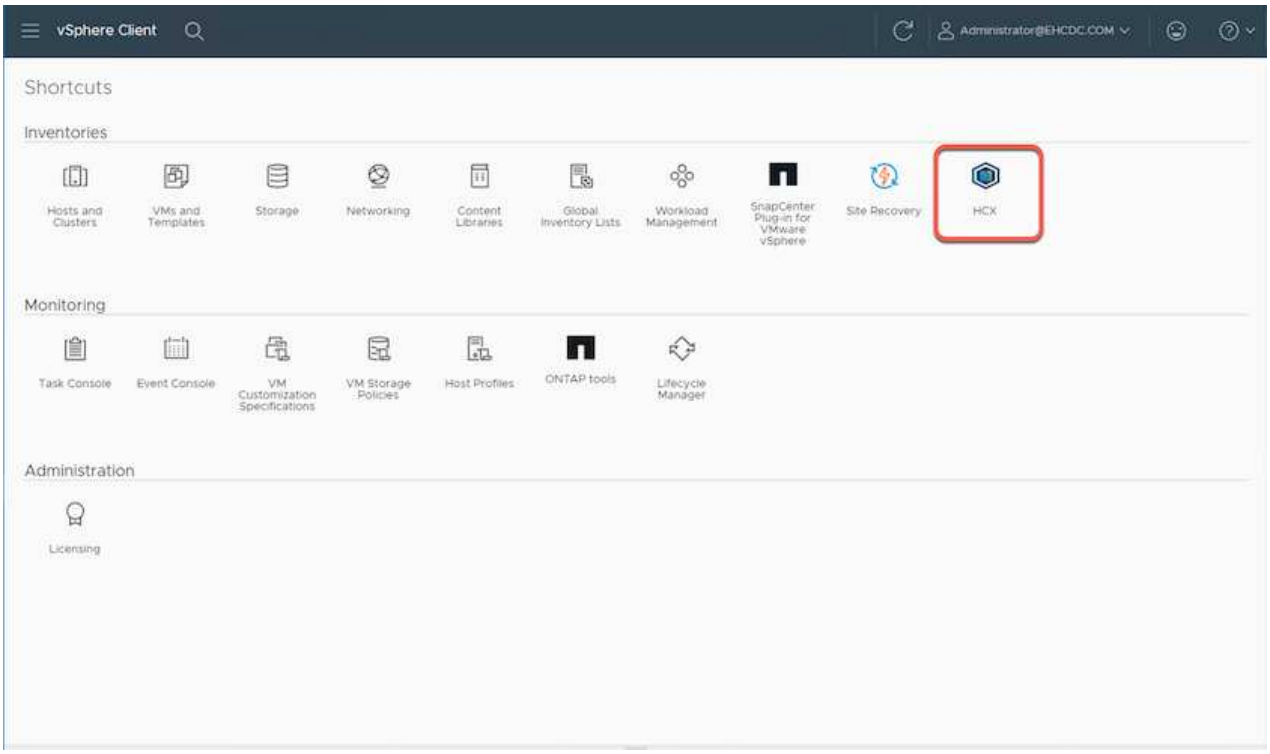
Dieser Vorgang dauert etwa 10 bis 20 Minuten, und das Plug-in wird dem vCenter Server hinzugefügt.



Schritt 4: Verbinden Sie den VMware HCX Connector vor Ort mit der Google Cloud VMware Engine HCX Cloud Manager

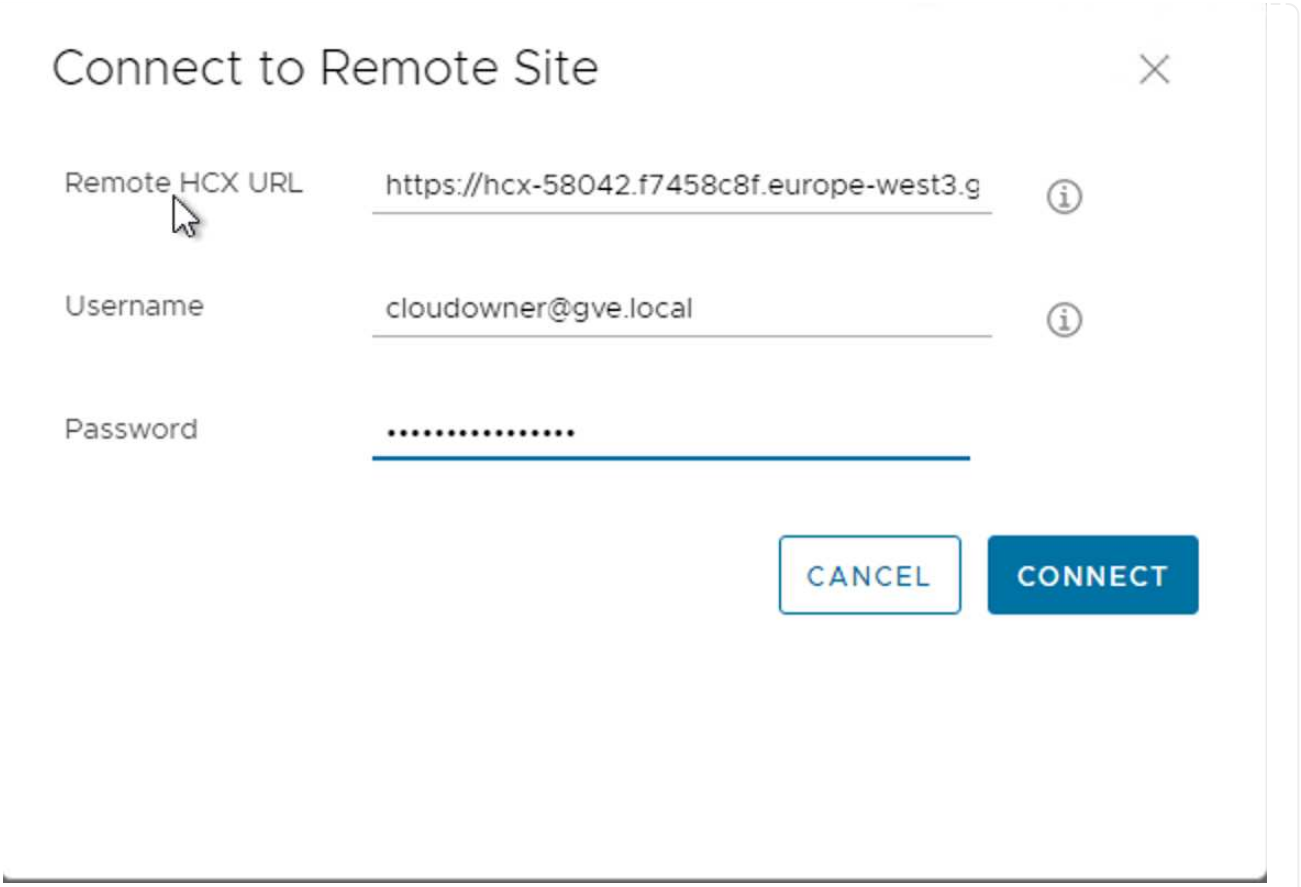
Nachdem HCX Connector im lokalen vCenter bereitgestellt und konfiguriert wurde, stellen Sie eine Verbindung zum Cloud Manager her, indem Sie die Paarung hinzufügen. Gehen Sie wie folgt vor, um die Standortpaarung zu konfigurieren:

1. Um ein Standortpaar zwischen der lokalen vCenter Umgebung und der Google Cloud VMware Engine SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das neue HCX vSphere Web Client Plug-in zu.



2. Klicken Sie unter Infrastruktur auf **Site Pairing hinzufügen**.

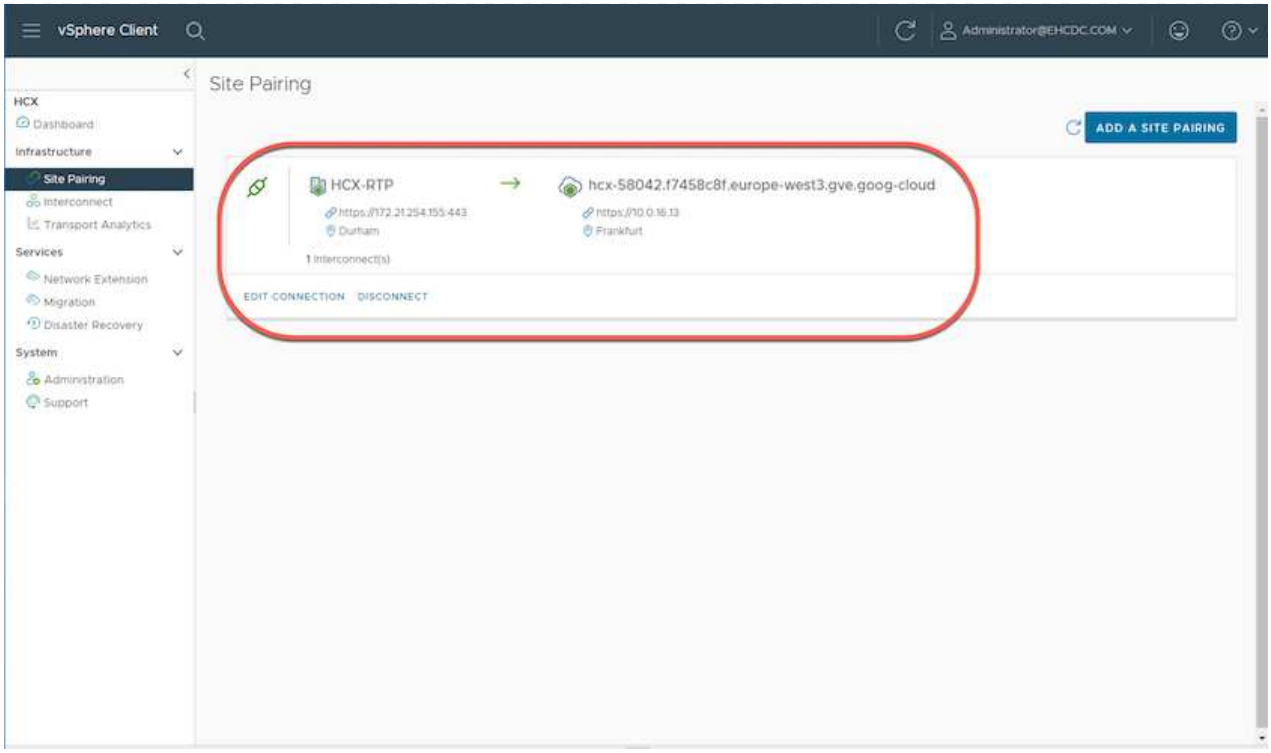
> Geben Sie die URL oder IP-Adresse des Google Cloud VMware Engine HCX Cloud Manager und die Anmeldedaten für Benutzer mit Cloud-Owner-Rollenberechtigungen für den Zugriff auf die private Cloud ein.



3. Klicken Sie Auf **Verbinden**.

   VMware HCX Connector muss über Port 443 zu HCX Cloud Manager IP weiterleiten können.

4. Nach der Erstellung der Kopplung steht die neu konfigurierte Standortpairing auf dem HCX Dashboard zur Verfügung.

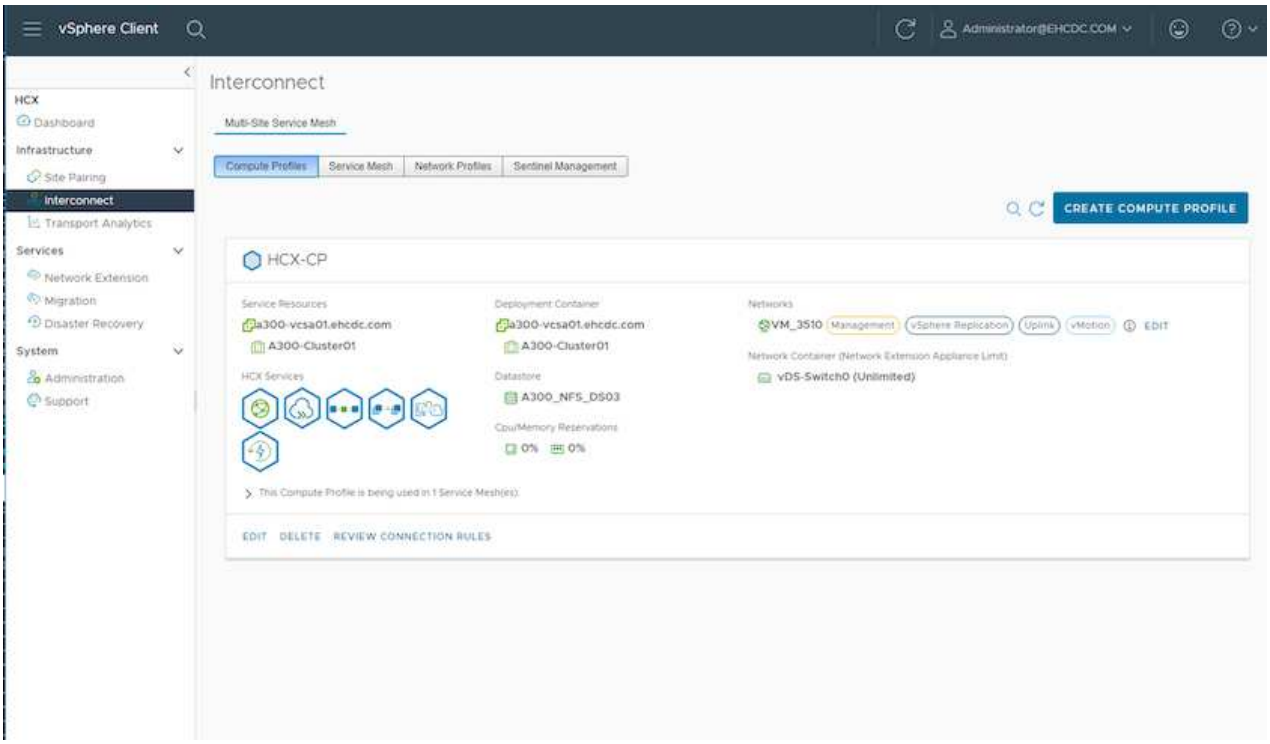

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

Schritt 5: Netzwerkprofil, Computing-Profil und Service-Mesh konfigurieren

Die VMware HCX Interconnect Service Appliance bietet Replizierungs- und vMotion-basierte Migrationsfunktionen über das Internet und private Verbindungen zum Zielstandort. Das Interconnect bietet Verschlüsselung, Traffic Engineering und VM-Mobilität. Um eine Interconnect Service Appliance zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie unter Infrastruktur die Option **Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile** aus.

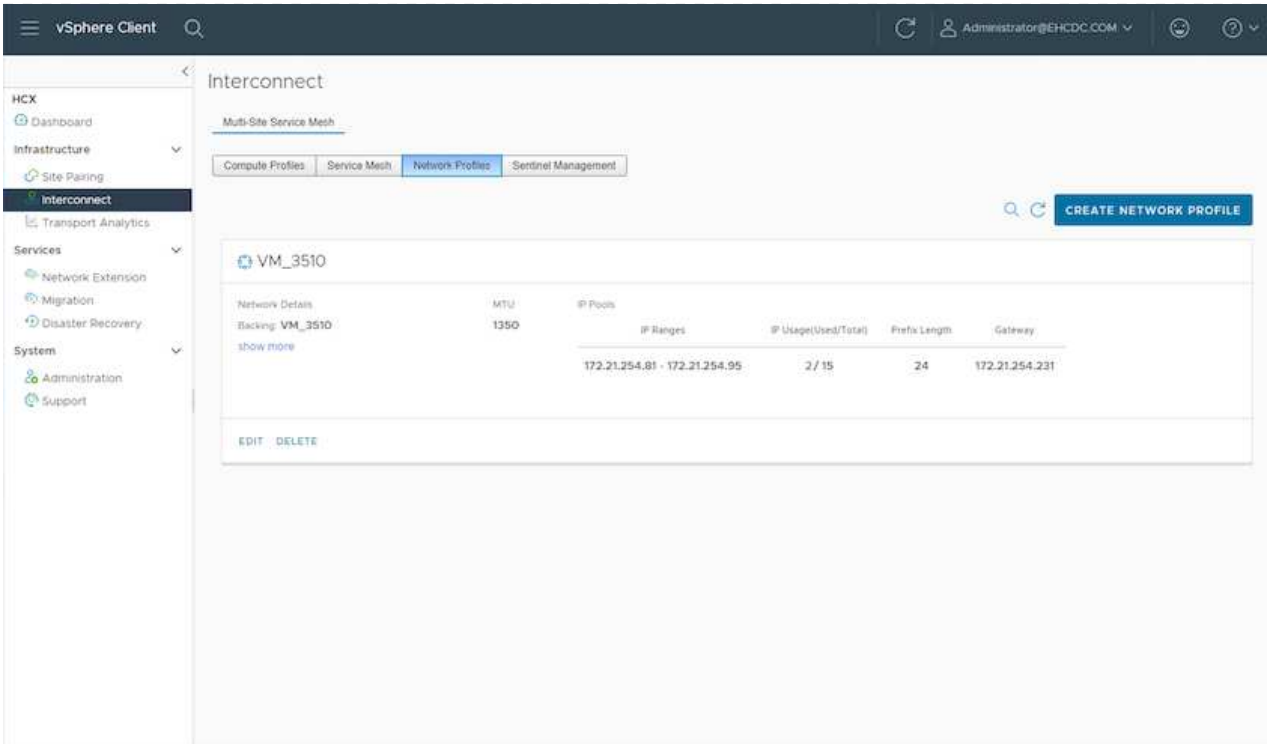
   Die Computing-Profile definieren die Implementierungsparameter einschließlich der Appliances, die bereitgestellt werden und welche Teile des VMware Datacenters für den HCX-Service verfügbar sind.



2. Erstellen Sie nach dem Erstellen des Rechenprofils die Netzwerkprofile, indem Sie **Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen** auswählen.

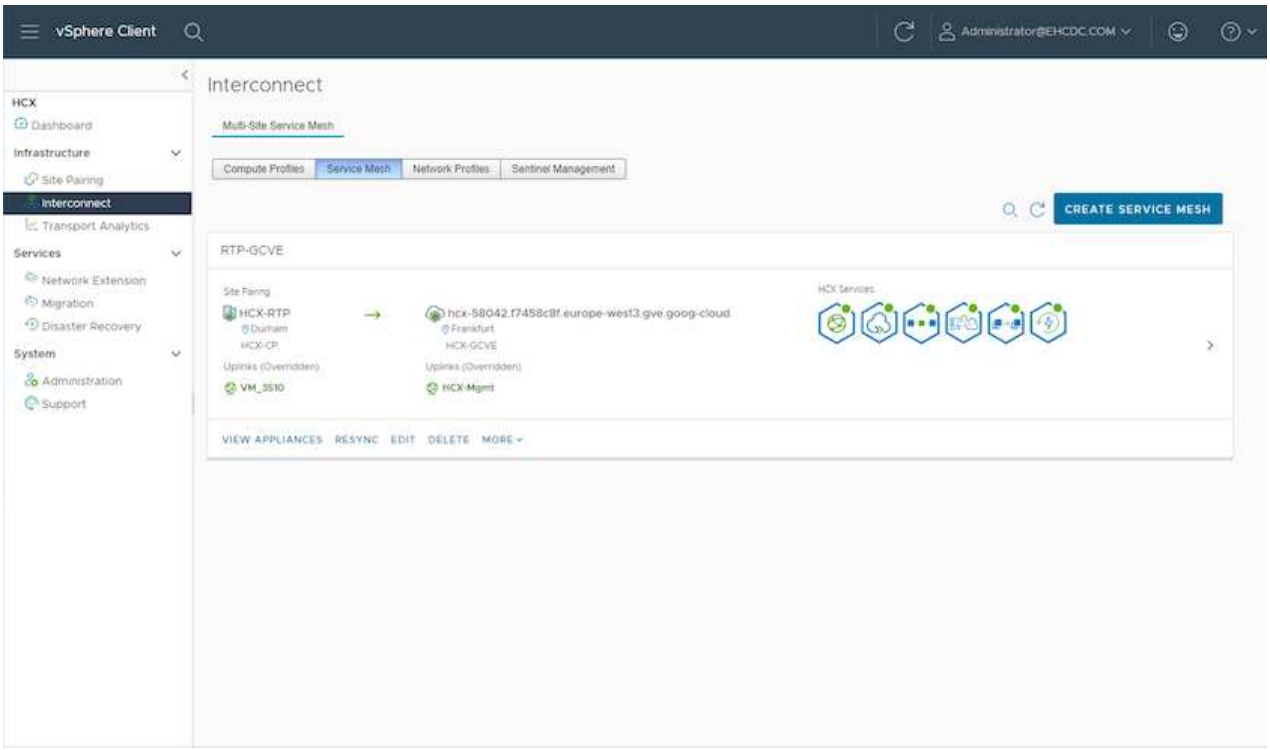
   Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

   Für diesen Schritt werden mindestens zwei IP-Adressen benötigt. Diese IP-Adressen werden den Interconnect Appliances vom Managementnetzwerk zugewiesen.

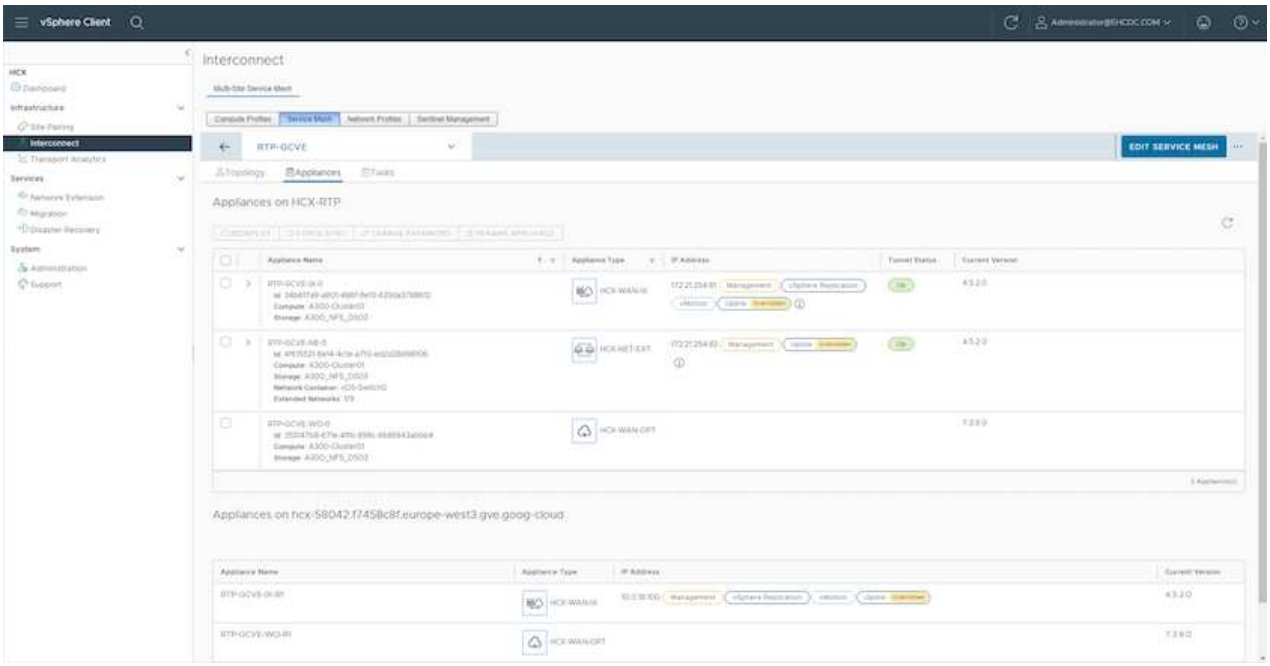


3. Derzeit wurden die Computing- und Netzwerkprofile erfolgreich erstellt.
4. Erstellen Sie das Service Mesh, indem Sie in der Option **Interconnect** die Registerkarte **Service Mesh** auswählen und die On-Premises- und GCVE SDDC-Sites auswählen.
5. Das Service Mesh gibt ein lokales und entferntes Compute- und Netzwerkprofilpaar an.

Im Rahmen dieses Prozesses werden die HCX-Appliances sowohl an den Quell- als auch an den Zielstandorten bereitgestellt und automatisch konfiguriert, um eine sichere Transportstruktur zu erstellen.



6. Dies ist der letzte Konfigurationsschritt. Die Implementierung sollte also fast 30 Minuten dauern. Nach der Konfiguration des Service-Mesh ist die Umgebung bereit, wobei die IPsec-Tunnel erfolgreich erstellt wurden, um die Workload-VMs zu migrieren.



Schritt 6: Migration von Workloads

Workloads können mithilfe verschiedener VMware HCX Migrationstechnologien bidirektional zwischen lokalen und GCVE SDDCs migriert werden. VMs können mithilfe von mehreren Migrationstechnologien wie HCX Bulk Migration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (erhältlich mit HCX Enterprise Edition) und HCX OS Assisted Migration (erhältlich mit der HCX Enterprise Edition) in und von VMware HCX Enterprise Edition verschoben werden.

Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter "Migrationstypen von VMware HCX".

Die HCX-IX Appliance verwendet den Mobility Agent Service, um vMotion-, Cold- und Replication Assisted vMotion-Migrationen (RAV) durchzuführen.

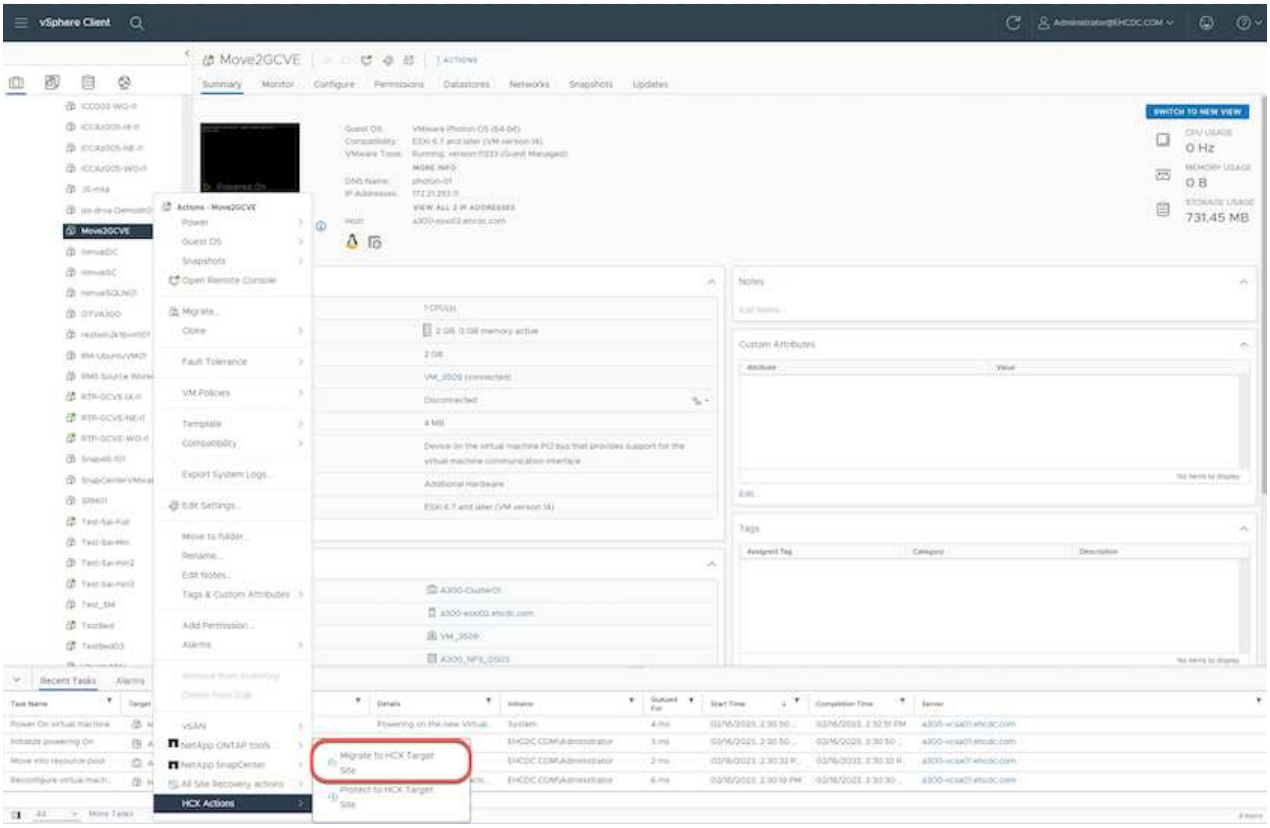
> Die HCX-IX Appliance fügt den Mobility Agent-Service als Hostobjekt im vCenter Server hinzu. Der auf diesem Objekt angezeigte Prozessor, Arbeitsspeicher, Speicher und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch des physischen Hypervisors dar, der die IX-Appliance hostet.

HCX vMotion

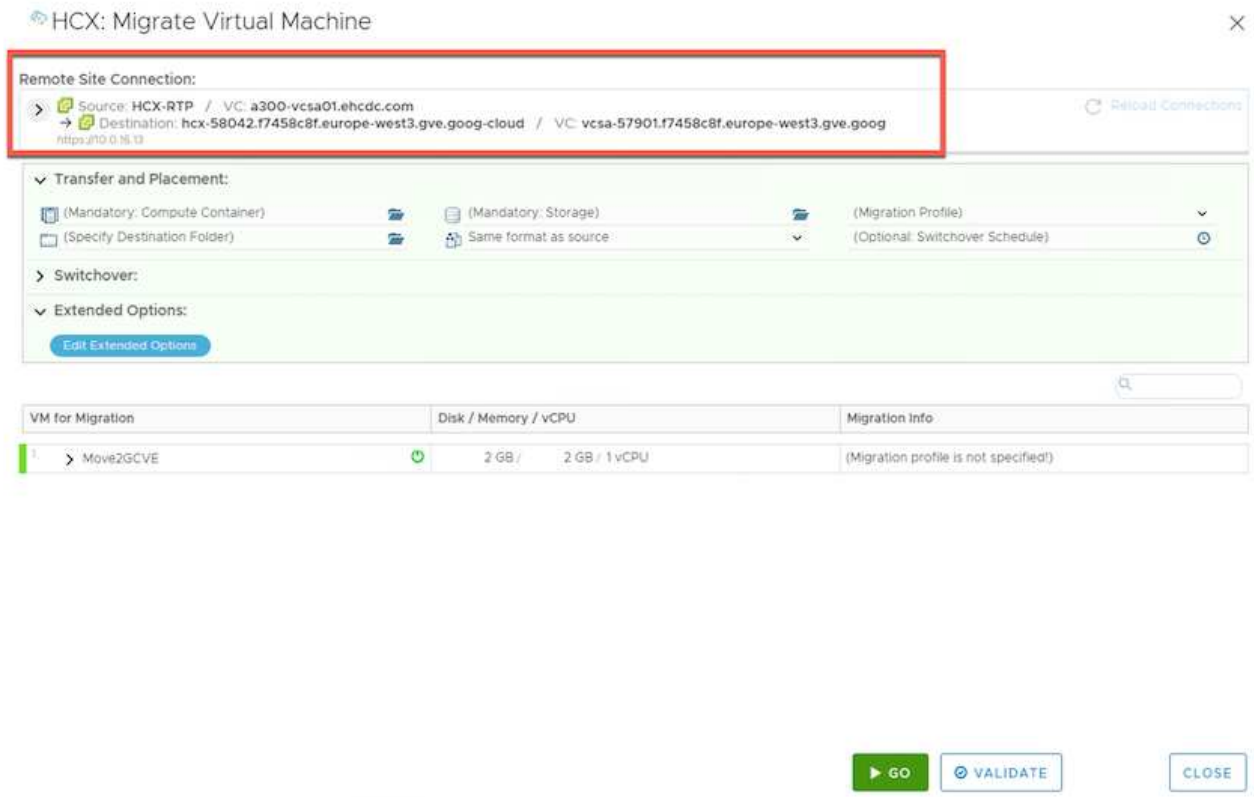
In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie verwendet das VMware vMotion Protokoll für die Migration einer VM zu GCVE. Die vMotion Migrationsoption wird verwendet, um den VM-Status einer einzelnen VM gleichzeitig zu migrieren. Während dieser Migrationsmethode kommt es zu keiner Serviceunterbrechung.

> Eine Netzwerkerweiterung sollte vorhanden sein (für die Portgruppe, an der die VM angeschlossen ist), um die VM zu migrieren, ohne dass eine IP-Adressänderung notwendig ist.

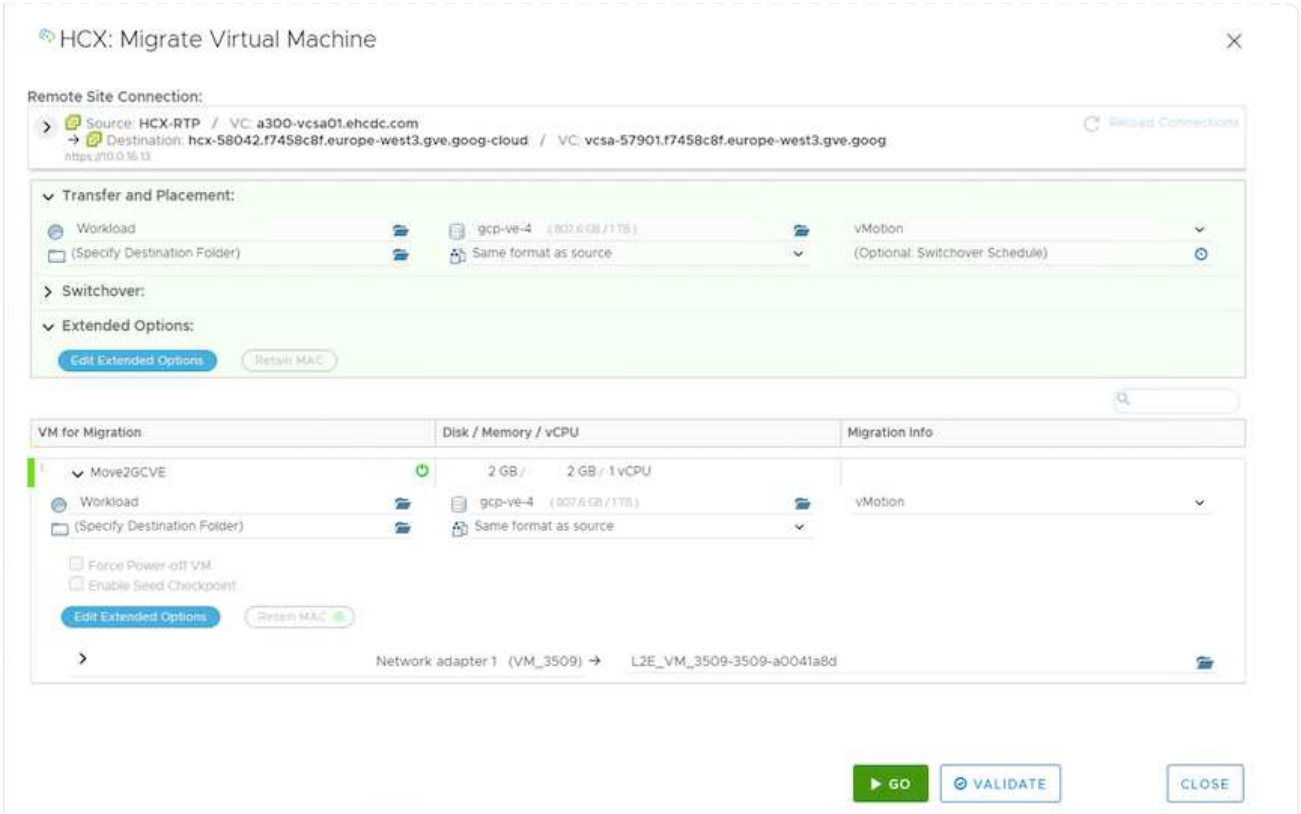
1. Wechseln Sie vom lokalen vSphere-Client zum Inventory, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie HCX Actions > Migrate to HCX Target Site aus.



2. Wählen Sie im Assistenten zum Migrieren von Virtual Machine die Remote-Standortverbindung (Ziel-GCVE) aus.



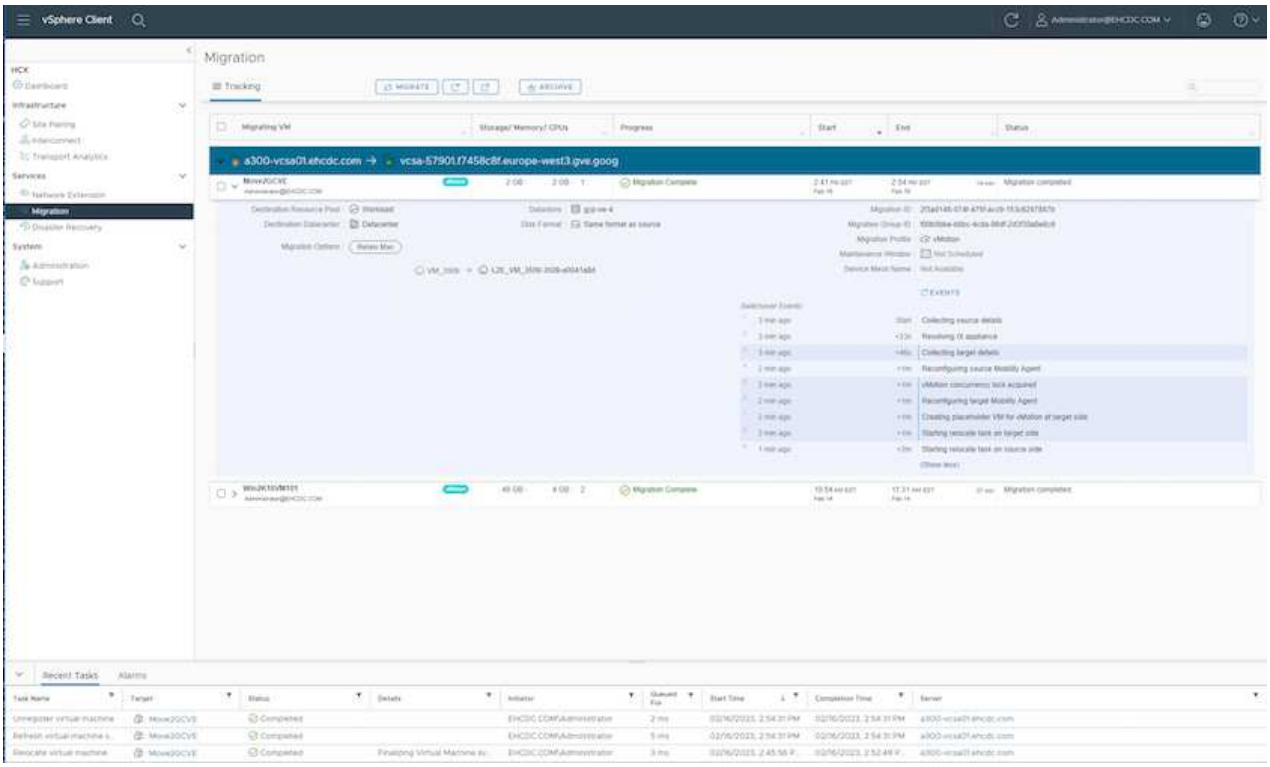
3. Aktualisieren Sie die Pflichtfelder (Cluster, Speicher und Zielnetzwerk), und klicken Sie auf Validieren.



4. Klicken Sie nach Abschluss der Validierungsprüfungen auf Los, um die Migration zu starten.

> Der vMotion Transfer erfasst den aktiven VM-Speicher, seinen Ausführungszustand, seine IP-Adresse und seine MAC-Adresse. Weitere Informationen zu den Anforderungen und Einschränkungen von HCX vMotion finden Sie unter "VMware HCX vMotion und „Cold Migration“ verstehen".

5. Über das Dashboard HCX > Migration können Sie den Fortschritt und den Abschluss von vMotion überwachen.



Der CVS Ziel-NFS-Datastore sollte über ausreichend Speicherplatz für die Migration verfügen.

Schlussfolgerung

Egal, ob Sie auf All-Cloud- oder Hybrid-Cloud-Umgebungen oder Daten auf Storage eines beliebigen Typs oder Anbieters vor Ort abzielen – Cloud Volume Service und HCX bieten hervorragende Optionen für die Implementierung und Migration der Applikations-Workloads und senken gleichzeitig die TCO, indem die Datenanforderungen nahtlos auf die Applikationsebene reduziert werden. Wie auch immer der Anwendungsfall aussieht: Die Google Cloud VMware Engine und Cloud Volume Service sorgen für die schnelle Realisierung der Cloud-Vorteile, eine konsistente Infrastruktur und Abläufe vor Ort und in mehreren Clouds, bidirektionale Workload-Portabilität und Kapazität und Performance der Enterprise-Klasse. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, die zum Verbinden des Storage und zur Migration von VMs mithilfe von VMware vSphere Replication, VMware vMotion oder sogar NFS (Network File Copy) verwendet werden.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können Cloud Volume Service jetzt als Datastore auf dem Google Cloud VMware Engine SDDC nutzen.
- Daten lassen sich problemlos von On-Premises- zu Cloud Volume Service-Datastores migrieren.
- Erweitern und verkleinern Sie den Cloud Volume Service-Datastore einfach, um die Kapazitäts- und Performance-Anforderungen während der Migration zu erfüllen.

Videos von Google und VMware als Referenz

Von Google

- "HCX Connector mit GCVE bereitstellen"
- "Konfigurieren Sie HCX ServiceMesh mit GCVE"
- "VM mit HCX auf GCVE migrieren"

Von VMware

- "HCX Connector-Bereitstellung für GCVE"
- "HCX ServiceMesh-Konfiguration für GCVE"
- "HCX-Workload-Migration zu GCVE"

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie unter den folgenden Links:

- Dokumentation der Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Dokumentation des Cloud Volume Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- VMware HCX-Benutzerhandbuch

  "https://docs.vmware.com/en/VMware-HCX/index.html"

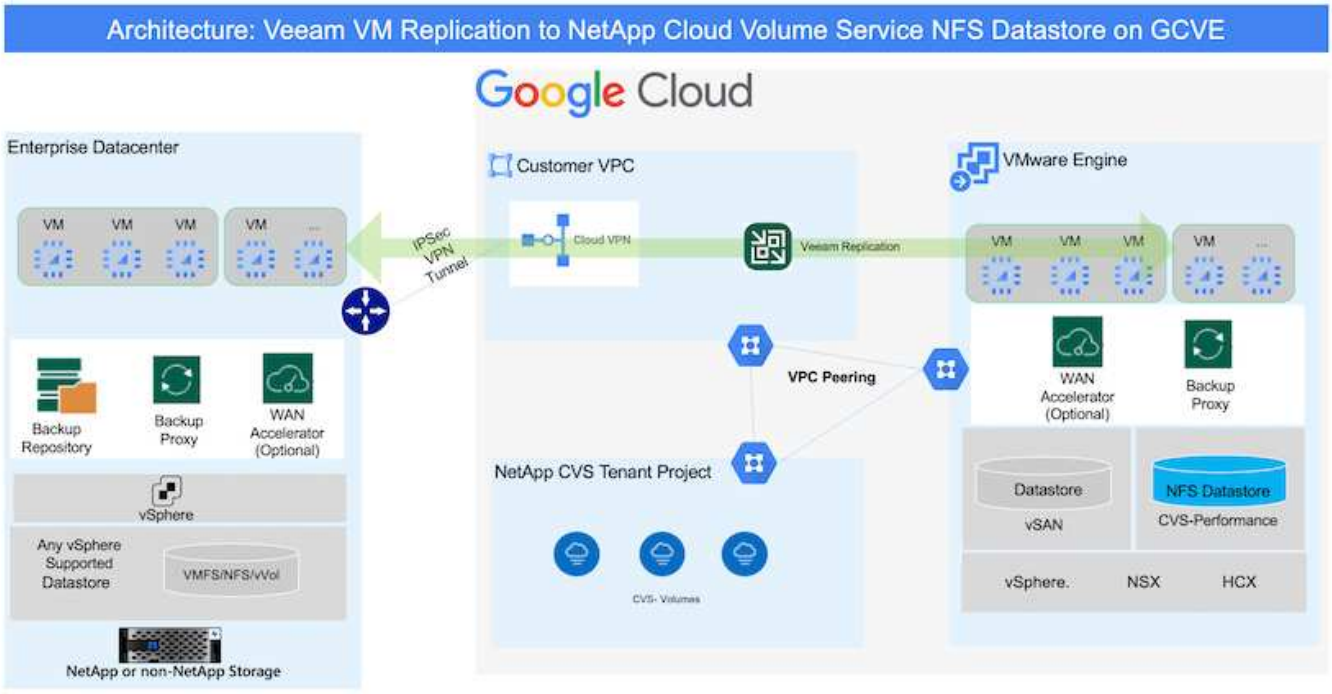
VM-Migration zu NetApp Cloud Volume Service NFS-Datastore auf Google Cloud VMware Engine mithilfe der Veeam Replizierungsfunktion

Überblick

Autoren: Suresh ThopPay, NetApp

VM-Workloads, die auf VMware vSphere ausgeführt werden, können mithilfe der Veeam Replication-Funktion in die Google Cloud VMware Engine (GCVE) migriert werden.

Dieses Dokument bietet einen Schritt-für-Schritt-Ansatz für die Einrichtung und Durchführung der VM-Migration mit NetApp Cloud Volume Service, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

In diesem Dokument wird vorausgesetzt, dass Sie entweder Google Cloud VPN oder Cloud Interconnect oder eine andere Netzwerkoption einsetzen, um die Netzwerkverbindung von bestehenden vSphere Servern zur Google Cloud VMware Engine herzustellen.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Siehe "Google Cloud-Dokumentation" Für die geeignete On-Premises-zu-Google-Verbindungsmethode.

Bereitstellen der Migrationslösung

Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass der NFS-Datastore aus dem NetApp-Cloud-Volume-Service in GCVE vCenter gemountet ist.
2. Sicherstellen, dass Veeam Backup Recovery in vorhandener VMware vSphere-Umgebung implementiert wird
3. Erstellen Sie einen Replikationsjob, um die Replikation virtueller Maschinen auf die Instanz der Google Cloud VMware Engine zu starten.
4. Führen Sie ein Failover des Veeam Replication Job durch.
5. Führen Sie ein Permanent Failover auf Veeam durch.

Einzelheiten Zur Bereitstellung

Stellen Sie sicher, dass der NFS-Datastore aus dem NetApp-Cloud-Volume-Service in GCVE vCenter gemountet ist

Melden Sie sich bei GCVE vCenter an, und stellen Sie sicher, dass ein NFS-Datastore mit ausreichend

Speicherplatz verfügbar ist.
Falls nicht, wenden Sie sich bitte an "Mounten Sie NetApp CVS als NFS-Datastore in GCVE"

Sicherstellen, dass Veeam Backup Recovery in vorhandener VMware vSphere-Umgebung implementiert wird

Weitere Informationen finden Sie unter "Veeam Replizierungskomponenten" Dokumentation zur Installation der erforderlichen Komponenten.

Erstellen Sie einen Replikationsjob, um die Replikation virtueller Maschinen auf die Instanz der Google Cloud VMware Engine zu starten.

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten"
Hier ist ein Video, in dem erklärt wird, wie
"Konfigurieren Sie Den Replikationsjob".

> Die ReplikatVM kann eine andere IP-Adresse als die Quell-VM haben und kann auch mit einer anderen Portgruppe verbunden werden. Weitere Informationen finden Sie im Video oben.

Führen Sie ein Failover des Veeam Replication Job durch

Führen Sie zum Migrieren von VMs aus "Führen Sie Ein Failover Durch"

Führen Sie ein Permanent Failover auf Veeam durch.

Um GCVE als Ihre neue Quellumgebung zu behandeln, führen Sie aus "Permanenter Failover"

Vorteile dieser Lösung

- Die vorhandene Veeam Backup-Infrastruktur kann für die Migration genutzt werden.
- Veeam Replication ermöglicht das Ändern von VM-IP-Adressen am Zielstandort.
- Vorhandene Daten, die außerhalb von Veeam repliziert wurden (wie replizierte Daten von BlueXP), können neu zugeordnet werden.
- Kann unterschiedliche Netzwerk-Portgruppen am Zielstandort angeben.
- Kann die Reihenfolge der VMs angeben, die eingeschaltet werden sollen.
- Verwendet VMware Change Block Tracking, um die Datenmenge zu minimieren, die über WAN gesendet werden soll.
- Möglichkeit zum Ausführen von Pre- und Post-Skripten für die Replizierung.
- Möglichkeit zur Ausführung von Pre-und Post-Skripten für Snapshots.

Regionale Verfügbarkeit – ergänzender NFS-Datastore für Google Cloud Platform (GCP)

Zusätzlicher NFS-Datastore für GCVE wird von NetApp Cloud Volume Service unterstützt.

> Für den GCVE NFS Datastore können nur CVS-Performance Volumes verwendet werden. Informationen zum verfügbaren Speicherort finden Sie unter "Globale Regionalkarte"

Google Cloud VMware Engine ist an folgenden Standorten verfügbar

Um die Latenz zu minimieren, sollten sich NetApp CVS Volume und GCVE, wo Sie das Volume mounten möchten, in derselben Verfügbarkeitszone befinden.
Arbeiten Sie mit Google und NetApp Solution Architects zusammen, um Verfügbarkeit und TCO-Optimierung zu optimieren.

Sicherheitsüberblick – NetApp Cloud Volumes Service (CVS) in Google Cloud

TR-4918: Sicherheitsübersicht - NetApp Cloud Volumes Service in Google Cloud

Oliver Krause, Justin Parisi, NetApp

Dokumentumfang

Die Sicherheit – insbesondere in der Cloud, wo die Infrastruktur außerhalb der Kontrolle der Storage-Administratoren liegt – ist entscheidend, wenn es um die Übergabe der Daten an die von Cloud-Providern angebotenen Service-Angebote geht. Dieses Dokument bietet einen Überblick über die Sicherheitsangebote von NetApp "Cloud Volumes Service bietet in Google Cloud".

Zielgruppe

Die Zielgruppe dieses Dokuments umfasst die folgenden Rollen:

- Cloud Provider
- Storage-Administratoren
- Storage-Architekten
- Feldressourcen
- Geschäftliche Entscheidungsträger

Wenn Sie Fragen zum Inhalt dieses technischen Berichts haben, finden Sie im Abschnitt "„Kontaktieren Sie uns.“"

Abkürzung	Definition
CVS-SW	Cloud Volumes Service, Diensttyp CVS
CVS-Performance	Cloud Volume Service, Servicetyp CVS-Performance
PSA	

Wie Cloud Volumes Service in Google Cloud Ihre Daten sichert

Cloud Volumes Service in Google Cloud bietet zahlreiche Möglichkeiten zur nativen Sicherung Ihrer Daten.

Sichere Architektur und Mandantenmodell

Cloud Volumes Service bietet eine sichere Architektur in Google Cloud, indem das Service-Management (Kontrollebene) und der Datenzugriff (Datenebene) über verschiedene Endpunkte segmentiert werden, sodass keine Auswirkung auf den anderen Endpunkte besteht (siehe Abschnitt "„Cloud Volumes Service Architecture“"). Sie verwendet Googles "Zugang zu privaten Services" (PSA) Framework zur Bereitstellung des Service. In diesem Rahmen wird zwischen dem von NetApp bereitgestellten und betriebenen Service-Produzenten unterschieden. Dabei handelt es sich um eine Virtual Private Cloud (VPC) in einem Kundenprojekt, in dem die Clients gehostet werden, die auf Cloud Volumes Service-Dateifreigaben zugreifen möchten.

In dieser Architektur finden Mandanten (siehe Abschnitt "„Tenancy model“") Sind als Google Cloud-Projekte definiert, die vollständig voneinander getrennt sind, es sei denn, der Benutzer hat ausdrücklich eine Verbindung. Mandanten ermöglichen durch die Cloud Volumes Service Volume-Plattform die vollständige

Isolierung von Daten-Volumes, externen Name Services und anderen wichtigen Lösungselementen von anderen Mandanten. Da die Cloud Volumes Service Plattform über VPC Peering verbunden ist, gilt diese Isolierung auch für die IT. Sie können die Freigabe von Cloud Volumes Service Volumes zwischen mehreren Projekten mithilfe einer gemeinsam genutzten VPC aktivieren (siehe Abschnitt "„Gemeinsame VPCs“"). Zugriffssteuerung kann auf SMB-Freigaben und NFS-Exporte angewendet werden, um zu beschränken, wer bzw. welche Datensätze angezeigt oder geändert werden können.

Starkes Identitätsmanagement für die Kontrollebene

In der Kontrollebene, auf der die Cloud Volumes Service-Konfiguration stattfindet, wird das Identitätsmanagement mit verwaltet "Identitäts-Zugriffsmanagement (Identity Access Management, IAM)". IAM ist ein Standardservice, mit dem die Authentifizierung (Logins) und Autorisierung (Berechtigungen) für Google Cloud-Projektinstanzen gesteuert werden kann. Die gesamte Konfiguration erfolgt über Cloud Volumes Service APIs über einen sicheren HTTPS-Transport mithilfe der TLS 1.2-Verschlüsselung. Die Authentifizierung erfolgt über JWT-Token für zusätzliche Sicherheit. Die Google-Konsole-Benutzeroberfläche für Cloud Volumes Service übersetzt Benutzereingaben in Cloud Volumes Service-API-Aufrufe.

Sicherheitshärtung – Begrenzung von Angriffsflächen

Ein Teil der effektiven Sicherheit ist die Begrenzung der Anzahl der Angriffsflächen, die in einem Service verfügbar sind. Angriffsflächen können eine Vielzahl von Dingen umfassen, beispielsweise Daten im Ruhezustand, Übertragungs- und Logins während der Übertragung und die Datensätze selbst.

Ein Managed Service entfernt einige Angriffsflächen inhärent in seinem Design. Infrastruktur-Management, wie im Abschnitt beschrieben "„Service-Betrieb“," Wird von einem dedizierten Team durchgeführt und verringert automatisch die Anzahl der Male, die ein Mensch tatsächlich bei Konfigurationen berührt, wodurch die Anzahl vorsätzlicher und unbeabsichtigter Fehler reduziert wird. Die Netzwerkumgebung ist abgezäunt, sodass nur erforderliche Services aufeinander zugreifen können. Die Verschlüsselung wird in den Datenspeicher integriert. Cloud Volumes Service Administratoren benötigen lediglich die Datenebene Sicherheitsaspekte. Wenn Sie den Großteil der Verwaltung hinter einer API-Schnittstelle verbergen, wird die Sicherheit durch Begrenzung der Angriffsflächen erreicht.

Zero-Trust-Modell

In der Vergangenheit BESTAND DIE IT-Sicherheitsphilosophie darin, Vertrauen zu geben, zu verifizieren und zu manifestieren, dass sie sich ausschließlich auf externe Mechanismen (wie Firewalls und Intrusion Detection Systems) zur Minderung von Bedrohungen verlassen. Angriffe und Verstöße wurden jedoch entwickelt, um die Verifizierung in Umgebungen durch Phishing, Social Engineering, Bedrohungen von innen und andere Methoden zu umgehen, die die Verifizierung in Netzwerke und Verwüstung ermöglichen.

Zero Trust hat sich zu einer neuen Sicherheitsmethode entwickelt, wobei das aktuelle Mantra „Vertrauen Sie nichts, während Sie noch alles überprüfen“ ist. Daher ist standardmäßig kein Zugriff zulässig. Dieses Mantra wird auf verschiedene Arten durchgesetzt, darunter Standard-Firewalls und Intrusion Detection-Systeme (IDS) sowie folgende Methoden:

- Starke Authentifizierungsmethoden (z. B. AES-verschlüsselte Kerberos- oder JWT-Token)
- Einzelne, starke Identifikationsquellen (z. B. Windows Active Directory, Lightweight Directory Access Protocol (LDAP) und Google IAM)
- Netzwerksegmentierung und sichere Mandantenfähigkeit (standardmäßig sind nur Mandanten Zugriff erlaubt)
- Granulare Zugriffssteuerung mit den geringsten Zugriffsrichtlinien
- Kleine exklusive Listen von engagierten, vertrauenswürdigen Administratoren mit digitalen Audit- und Papiertrails

Cloud Volumes Service läuft in Google Cloud hält sich an das Zero-Trust-Modell durch die Umsetzung der "Vertrauen nichts, alles überprüfen" Haltung.

Verschlüsselung

Verschlüsselung von Daten im Ruhezustand (siehe Abschnitt "„Datenverschlüsselung im Ruhezustand“") Mit XTS-AES-256-Chiffren mit NetApp Volume Encryption (NVE) und im Flight mit "„SMB-Verschlüsselung“" Oder NFS Kerberos 5p-Support. Gut zu wissen, dass regionsübergreifende Replikationstransfers durch TLS 1.2-Verschlüsselung geschützt sind (siehe Abschnitt "„Regionenübergreifende Replikation“"). Darüber hinaus bietet Google Networking auch verschlüsselte Kommunikation (siehe Abschnitt "„Datenverschlüsselung während der Übertragung“") Für eine zusätzliche Schutzschicht gegen Angriffe. Weitere Informationen zur Transportverschlüsselung finden Sie im Abschnitt "„Google Cloud-Netzwerk“".

Datensicherung und Backups

Bei der Sicherheit geht es nicht nur um die Verhinderung von Angriffen. Es geht auch darum, wie wir nach Angriffen eine Wiederherstellung durchführen, wenn sie auftreten. Diese Strategie umfasst Datenschutz und -Backups. Cloud Volumes Service bietet Methoden zur Replizierung in andere Regionen bei Ausfällen (siehe Abschnitt "„Regionenübergreifende Replikation“") Oder wenn ein Datensatz von einem Ransomware-Angriff betroffen ist. Sie kann auch asynchrone Daten-Backups von Standorten außerhalb der Cloud Volumes Service Instanz mithilfe von durchführen "Cloud Volumes Service-Backup". Mit regelmäßigen Backups kann das Abmildern von Sicherheitsereignissen Zeit in Anspruch nehmen, Geld und Aufwand für Administratoren einsparen.

Schnelle Abwehr von Ransomware mit branchenführenden Snapshot Kopien

Zusätzlich zu Datensicherung und Backups unterstützt Cloud Volumes Service auch unveränderliche Snapshot Kopien (siehe Abschnitt "„Unveränderliche Snapshot Kopien“") Von Volumes, die eine Wiederherstellung nach Ransomware-Angriffen ermöglichen (siehe Abschnitt "„Service-Betrieb“"Innerhalb von Sekunden nach der Entdeckung des Problems und mit minimaler Unterbrechung. Die Recovery-Zeit und -Auswirkungen hängen vom Snapshot Zeitplan ab. Allerdings können Snapshot-Kopien erstellt werden, die bei Ransomware-Angriffen nur eine Stunde Deltawerte liefern. Snapshot Kopien haben nahezu unmerkliche Auswirkungen auf die Performance und Kapazitätsauslastung und stellen einen Ansatz mit niedrigem Risiko und hoher Rendite zum Schutz Ihrer Datensätze dar.

Sicherheitsüberlegungen und Angriffsflächen

Der erste Schritt zum Verständnis der Datensicherung besteht darin, die Risiken und potenziellen Angriffsflächen zu identifizieren.

Dazu gehören (aber nicht beschränkt auf) die folgenden:

- Administration und Anmeldung
- Daten im Ruhezustand
- Genutzte Daten
- Netzwerk und Firewalls
- Ransomware, Malware und Viren

Das Verständnis von Angriffsflächen kann Ihnen helfen, Ihre Umgebungen besser zu schützen. Cloud Volumes Service in Google Cloud berücksichtigt bereits viele dieser Themen und implementiert Sicherheitsfunktionen standardmäßig ohne administrative Eingriffe.

Sichere Anmeldungen sicherstellen

Bei der Sicherung Ihrer kritischen Infrastrukturkomponenten ist es von größter Wichtigkeit, sicherzustellen, dass nur genehmigte Benutzer sich einloggen und Ihre Umgebungen managen können. Wenn fehlerhafte Akteure die Anmeldedaten in Ihrem System verletzen, haben sie die Schlüssel zum Schloss und können alles tun, was sie wollen: Konfigurationen ändern, Volumes und Backups löschen, Backdoors erstellen oder Snapshot-Zeitpläne deaktivieren.

Cloud Volumes Service für Google Cloud bietet Schutz vor unautorisierten administrativen Anmeldungen durch den Ausfall von Storage als Service (StaaS). Cloud Volumes Service wird vom Cloud-Provider komplett gewartet, ohne dass eine externe Anmeldung verfügbar ist. Alle Setup- und Konfigurationsvorgänge sind vollautomatisiert, sodass ein Administrator in seltenen Fällen nie mit den Systemen interagieren muss.

Wenn Anmeldung erforderlich ist, sichert Cloud Volumes Service in Google Cloud Anmeldungen, indem eine sehr kurze Liste vertrauenswürdiger Administratoren geführt wird, die Zugriff haben, um sich bei den Systemen anzumelden. Diese Gatekeeping hilft, die Anzahl potenzieller schlechter Akteure mit Zugriff zu reduzieren. Darüber hinaus verbirgt das Google Cloud-Netzwerk die Systeme hinter Schichten der Netzwerksicherheit und legt nur das, was für die Außenwelt benötigt wird, offen. Weitere Informationen zur Google Cloud- und Cloud Volumes Service-Architektur finden Sie im Abschnitt "„Cloud Volumes Service Architecture“."

Cluster-Administration und Upgrades

Zu den zwei Bereichen mit potenziellen Sicherheitsrisiken zählen die Clusterverwaltung (was passiert, wenn ein schlechter Akteur Administratorzugriff hat) und Upgrades (was passiert, wenn ein Software-Image beeinträchtigt wird).

Sicherung der Storage-Administration

Der als Service bereitgestellte Storage beseitigt das zusätzliche Risiko, dass Administratoren diesem Zugriff nicht mehr an Anwender außerhalb des Cloud-Datacenters ausgesetzt sind. Stattdessen gilt die einzige Konfiguration für die Datenzugriffsebene durch Kunden. Jeder Mandant managt seine eigenen Volumes, und ein Mandant kann andere Cloud Volumes Service Instanzen nicht erreichen. Der Service wird durch Automatisierung gemanagt, wobei in einer sehr kleinen Liste vertrauenswürdiger Administratoren über die im Abschnitt behandelten Prozesse Zugriff auf die Systeme gewährt wird "„Service-Betrieb“."

Der Servicetyp CVS-Performance bietet regionenübergreifende Replizierung als Option zur Sicherung von Daten für eine andere Region bei Ausfall. In diesen Fällen kann ein Failover der Cloud Volumes Service in die nicht betroffene Region durchgeführt werden, um den Datenzugriff zu gewährleisten.

Service-Upgrades

Updates helfen, gefährdete Systeme zu schützen. Jedes Update bietet Verbesserungen der Sicherheit und Fehlerbehebungen zur Minimierung von Angriffsflächen. Software-Updates werden aus zentralen Repositorys heruntergeladen und validiert, bevor die Updates überprüft werden, ob offizielle Bilder verwendet werden und dass die Upgrades nicht durch fehlerhafte Akteure beeinträchtigt werden.

Mit Cloud Volumes Service werden Updates von den Cloud-Provider-Teams durchgeführt, die Risiken für Administratoren abschaffen, indem Experten versiert in Konfiguration und Upgrades sind, die den Prozess automatisiert und vollständig getestet haben. Upgrades werden unterbrechungsfrei durchgeführt und Cloud Volumes Service behält die neuesten Updates bei, um optimale Ergebnisse zu erzielen.

Informationen über das Administrator-Team, das diese Service-Upgrades durchführt, finden Sie im Abschnitt "„Service-Betrieb“."

Sicherheit von Daten im Ruhezustand

Die Verschlüsselung ruhender Daten ist wichtig, um sensible Daten bei Diebstahl, Rückgabe oder neuer Verwendung einer Festplatte zu schützen. Daten in Cloud Volumes Service werden mithilfe von softwarebasierter Verschlüsselung im Ruhezustand gesichert.

- Google-generierte Schlüssel werden für CVS-SW verwendet.
- Für die CVS-Performance werden die Schlüssel pro Volume in einem in Cloud Volumes Service integrierten Schlüsselmanager gespeichert, der mit NetApp ONTAP CryptoMod die AES-256-Verschlüsselung generiert. CryptoMod ist in der nach FIPS 140-2 validierten CMVP-Modulliste aufgeführt. Siehe "FIPS 140-2 Zertifikat #4144".

Im November 2021 wurde eine Vorschau auf die Funktionalität Customer-Managed Encryption (CMEK) für CVS-Performance bereitgestellt. Diese Funktionalität ermöglicht Ihnen die Verschlüsselung der Schlüssel pro Volume mit Master-Schlüsseln für einzelne Projekte und Regionen, die im Google Key Management Service (KMS) gehostet werden. KMS ermöglicht es Ihnen, externe Schlüsselmanager anzubinden.

Details zur Konfiguration von KMS für CVS-Performance finden Sie unter "Weitere Informationen finden Sie in der Cloud Volumes Service-Dokumentation".

Weitere Informationen zur Architektur finden Sie im Abschnitt "„Cloud Volumes Service Architecture“."

Sicherheit der aktiven Daten

Sie müssen nicht nur Daten im Ruhezustand sichern, sondern auch bei laufender Übertragung zwischen der Cloud Volumes Service Instanz und einem Client oder Replizierungsziel sichern können. Cloud Volumes Service bietet Verschlüsselung von Daten auf der Übertragungsstrecke über NAS-Protokolle. Dabei kommen Verschlüsselungsmethoden wie SMB-Verschlüsselung mit Kerberos, das Signing/Sealing von Paketen und NFS Kerberos 5p für die End-to-End-Verschlüsselung von Datentransfers zum Einsatz.

Die Replizierung von Cloud Volumes Service Volumes verwendet TLS 1.2, die von AES-GCM-Verschlüsselungsmethoden profitiert.

Die unsicheres in-Flight-Protokolle wie Telnet, NDMP usw. sind standardmäßig deaktiviert. DNS ist jedoch nicht durch Cloud Volumes Service verschlüsselt (keine DNS-sec-Unterstützung) und sollte, wenn möglich, mit externer Netzwerkverschlüsselung verschlüsselt werden. Siehe Abschnitt "„Datenverschlüsselung während der Übertragung“" Finden Sie weitere Informationen über die Sicherung Ihrer aktiven Daten.

Informationen zur Verschlüsselung von NAS-Protokollen finden Sie im Abschnitt "„NAS-Protokolle“."

Benutzer und Gruppen für NAS-Berechtigungen

Bei der Sicherung Ihrer Daten in der Cloud ist eine ordnungsgemäße Benutzer- und Gruppenauthentifizierung erforderlich, wobei die Benutzer, die auf die Daten zugreifen, als echte Benutzer in der Umgebung überprüft werden und die Gruppen gültige Benutzer enthalten. Diese Benutzer und Gruppen bieten ersten Zugriff auf Freigabe und Export sowie Berechtigungsvalidierung für Dateien und Ordner im Speichersystem.

Cloud Volumes Service verwendet die standardmäßige, auf Active Directory basierende Windows-Benutzer- und Gruppenauthentifizierung für SMB-Freigaben und Windows-artige Berechtigungen. Der Service kann auch UNIX Identitätsanbieter wie LDAP für UNIX Benutzer und Gruppen für NFS-Exporte, NFSv4 ID-Validierung, Kerberos-Authentifizierung und NFSv4 ACLs nutzen.

Derzeit wird mit Cloud Volumes Service nur Active Directory LDAP zur LDAP-Funktionalität unterstützt.

Erkennung, Verhinderung und Minimierung von Ransomware, Malware und Viren

Ransomware, Malware und Viren sind für Administratoren eine persistente Bedrohung. Die Erkennung, das Vorbeugen und die Minimierung dieser Bedrohungen steht für Unternehmen immer im Mittelpunkt. Ein einzelnes Ransomware-Ereignis auf einem kritischen Datensatz kann potenziell Millionen US-Dollar kosten. Daher ist es vorteilhaft, alles zu tun, um das Risiko zu minimieren.

Obwohl Cloud Volumes Service derzeit nicht schließt native Detection oder Prävention Maßnahmen, wie Virenschutz oder "Automatische Ransomware-Erkennung", Es gibt Möglichkeiten, nach einem Ransomware-Ereignis schnell wiederherzustellen, indem es regelmäßige Snapshot-Zeitpläne ermöglicht. Snapshot-Kopien sind unveränderliche und schreibgeschützte Verweise auf geänderte Blöcke im Filesystem, werden praktisch sofort erzeugt, haben minimale Auswirkungen auf die Performance und verbrauchen nur Speicherplatz, wenn Daten geändert oder gelöscht werden. Sie können Zeitpläne für Snapshot Kopien einrichten, die auf Ihre gewünschte akzeptable Recovery Point Objective (RPO)/Recovery Time Objective (RTO) abgestimmt sind und bis zu 1,024 Snapshot Kopien pro Volume aufbewahren.

Snapshot Support ist ohne zusätzliche Kosten enthalten (Storage-Kosten für veränderte Blöcke/Daten, die von Snapshot Kopien aufbewahrt Cloud Volumes Service werden) und kann bei einem Ransomware-Angriff genutzt werden, um ein Rollback auf eine Snapshot Kopie vor dem Angriff durchzuführen. Snapshot Wiederherstellungen dauern nur wenige Sekunden und Daten können wieder wie gewohnt bereit sein. Weitere Informationen finden Sie unter "NetApp Lösung gegen Ransomware".

Die Auswirkungen von Ransomware auf Ihr Unternehmen zu verhindern, ist ein mehrschichtiger Ansatz erforderlich, der einen oder mehrere der folgenden Elemente umfasst:

- Endpoint-Schutz
- Schutz vor externen Bedrohungen durch Netzwerk-Firewalls
- Erkennung von Datenanomalien
- Mehrere Backups (vor Ort und extern) kritischer Datensätze
- Regelmäßige Restore-Tests von Backups
- Unveränderliche schreibgeschützte NetApp Snapshot Kopien
- Multi-Faktor-Authentifizierung für kritische Infrastrukturen
- Sicherheitsprüfungen von Systemanmeldungen

Diese Liste ist bei weitem nicht erschöpfend, aber ist eine gute Blaupause, wenn man mit dem Potential der Ransomware-Angriffe zu folgen. Cloud Volumes Service in Google Cloud bietet verschiedene Möglichkeiten zum Schutz vor Ransomware-Ereignissen und zur Reduzierung der Auswirkungen.

Unveränderliche Snapshot Kopien

Cloud Volumes Service bietet native unveränderliche, schreibgeschützte Snapshot Kopien, die in einem anpassbaren Zeitplan erstellt werden, um schnelle zeitpunktgenaue Recovery beim Löschen von Daten zu ermöglichen oder wenn ein gesamtes Volume durch einen Ransomware-Angriff zu Opfer gebracht wurde. Snapshots können zu vorherigen guten Snapshot Kopien schnell wiederhergestellt werden und minimieren Datenverluste aufgrund der Aufbewahrungsdauer Ihrer Snapshot-Zeitpläne und RTO/RPO. Der Performance-Effekt mit der Snapshot Technologie ist zu vernachlässigen.

Da Snapshot Kopien in Cloud Volumes Service schreibgeschützt sind, können diese nicht durch Ransomware infiziert werden, wenn die Ransomware nicht in den Datensatz „unbemerkt“ und Snapshot-Kopien der von Ransomware infizierten Daten erstellt wurde. Deshalb ist es notwendig, auf der Basis von Datenanomalien auch Ransomware-Erkennung in Betracht zu ziehen. Cloud Volumes Service bietet derzeit keine native Erkennung, Sie können jedoch externe Überwachungssoftware verwenden.

Backups und Restores

Cloud Volumes Service bietet standardmäßige NAS-Client-Backup-Funktionen (z. B. Backups über NFS oder SMB).

- CVS-Performance bietet regionenübergreifende Volume-Replizierung zu anderen CVS-Performance Volumes. Weitere Informationen finden Sie unter "Volume-Replizierung" In der Cloud Volumes Service-Dokumentation.
- CVS-SW bietet Service-native Backup-/Restore-Funktionen für Volumes. Weitere Informationen finden Sie unter "Cloud-Backup" In der Cloud Volumes Service-Dokumentation.

Die Volume-Replizierung liefert eine exakte Kopie des Quell-Volumes für schnelles Failover im Falle eines Ausfalls, einschließlich Ransomware-Ereignissen.

Regionsübergreifende Replizierung

CVS-Performance ermöglicht die sichere Replizierung von Volumes über Google Cloud Regionen hinweg zur Datensicherung und Archivierung von Anwendungsfällen. Dazu wird mit TLS1.2 AES 256 GCM-Verschlüsselung auf einem von NetApp gesteuerten Backend-Service-Netzwerk über spezifische Schnittstellen verwendet, die für die Replizierung im Google-Netzwerk verwendet werden. Ein primäres Volume (Quell-Volume) enthält die aktiven Produktionsdaten und repliziert auf ein sekundäres Volume (Ziel-Volume), um ein exaktes Replikat des primären Datensatzes zu erstellen.

Bei der anfänglichen Replizierung werden alle Blöcke übertragen, jedoch werden nur die geänderten Blöcke in einem primären Volume übertragen. Wird beispielsweise eine Datenbank mit 1 TB auf einem primären Volume auf das sekundäre Volume repliziert, so werden bei der ersten Replizierung 1 TB Speicherplatz übertragen. Wenn diese Datenbank einige hundert Zeilen (hypothetisch einige MB) hat, die zwischen der Initialisierung und dem nächsten Update wechseln, werden nur die Blöcke mit den geänderten Zeilen auf das sekundäre (wenige MB) repliziert. So wird sichergestellt, dass die Übertragungszeiten niedrig bleiben und die Replizierungskosten sinken.

Alle Berechtigungen für Dateien und Ordner werden auf das sekundäre Volume repliziert, aber die Zugriffsberechtigungen für die Freigabe (wie Exportrichtlinien und Regeln oder SMB-Freigaben und ACLs für die Freigabe) müssen separat gehandhabt werden. Bei einem Site-Failover sollte der Zielstandort dieselben Namensdienste und Active Directory-Domänenverbindungen nutzen, um eine konsistente Handhabung von Benutzer- und Gruppenidentitäten und -Berechtigungen zu ermöglichen. Sie können ein sekundäres Volume im Notfall als Failover-Ziel verwenden, indem Sie die Replizierungsbeziehung unterbrechen, die das sekundäre Volume in Lese- und Schreibvorgänge konvertiert.

Volume-Replikate sind schreibgeschützt, d. h. eine unveränderliche Kopie der Daten an einem externen Standort zur schnellen Recovery von Daten in Instanzen, in denen ein Virus infizierte Daten hat oder Ransomware den primären Datensatz verschlüsselt hat. Nur-Lese-Daten werden nicht verschlüsselt, aber, wenn das primäre Volume betroffen ist und Replikation auftritt, die infizierten Blöcke replizieren auch. Zur Wiederherstellung können Sie ältere, nicht betroffene Snapshot Kopien verwenden. Je nachdem, wie schnell ein Angriff erkannt wird, fallen jedoch unter Umständen die versprochenen RTO/RPO-Vorgaben aus.

Darüber hinaus können Sie mit dem Management der regionsübergreifenden Replizierung (CRR) in Google Cloud böswillige Administratoraktionen, wie z. B. Volume-Löschungen, Snapshot-Löschungen oder Änderungen bei Snapshot-Planungen, verhindern. Dazu werden benutzerdefinierte Rollen erstellt, die Volume-Administratoren trennen, die Quell-Volumes löschen, aber keine Spiegelungen unterbrechen und daher keine Ziel-Volumes von CRR-Administratoren löschen können, die keine Volume-Vorgänge ausführen können. Siehe "Überlegungen Zur Sicherheit" In der Cloud Volumes Service-Dokumentation finden Sie Berechtigungen, die von den einzelnen Administratorgruppen zulässig sind.

Cloud Volumes Service-Backup

Cloud Volumes Service bietet zwar eine hohe Datenaufbewahrung, externe Ereignisse können jedoch zu Datenverlusten führen. Falls es zu Sicherheitsereignisse wie Viren oder Ransomware kommt, werden Backups und Restores so wichtig, dass der Datenzugriff rechtzeitig wiederaufgenommen werden kann. Ein Administrator kann ein Cloud Volumes Service Volume versehentlich löschen. Oder Benutzer möchten einfach noch viele Monate Backup-Versionen ihrer Daten aufbewahren und den zusätzlichen Speicherplatz für Snapshot-Kopien innerhalb des Volumes zu einer Kostenanforderung machen. Snapshot-Kopien sollten die bevorzugte Methode sein, Backup-Versionen für die letzten Wochen zu behalten, um verlorene Daten von ihnen wiederherzustellen, sie befinden sich jedoch im Volume und gehen verloren, wenn das Volume entfernt wird.

Aus allen diesen Gründen bietet NetApp Cloud Volumes Service Backup-Services über an "Cloud Volumes Service-Backup".

Cloud Volumes Service Backup erzeugt eine Kopie des Volumes auf Google Cloud Storage (GCS). Es sichert nur die tatsächlichen Daten, die innerhalb des Volume gespeichert sind, nicht den freien Speicherplatz. Es funktioniert wie immer inkrementell, d. h., es überträgt den Volume-Inhalt einmal und von dort auf wird nur geänderte Daten gesichert. Im Vergleich zu klassischen Backup-Konzepten mit mehreren vollständigen Backups spart das Unternehmen viel Storage und senkt dadurch die Kosten. Da der monatliche Preis von Backup-Speicherplatz im Vergleich zu einem Volume niedriger ist, ist es der ideale Ort, um Backup-Versionen länger zu halten.

Benutzer können ein Cloud Volumes Service Backup verwenden, um jede Backup-Version auf demselben oder einem anderen Volume innerhalb derselben Region wiederherzustellen. Wenn das Quell-Volume gelöscht wird, werden die Backup-Daten aufbewahrt und müssen unabhängig gemanagt werden (beispielsweise gelöscht).

Cloud Volumes Service Backup ist optional in Cloud Volumes Service integriert. Benutzer legen fest, welche Volumes gesichert werden sollen, indem Cloud Volumes Service Backup für einzelne Volumes aktiviert wird. Siehe "Cloud Volumes Service Backup-Dokumentation" Weitere Informationen zu Backups finden Sie im "Anzahl der maximal unterstützten Backup-Versionen", Planung, und "Preisgestaltung".

Alle Backup-Daten eines Projekts werden innerhalb eines GCS-Buckets gespeichert, der durch den Service gemanagt wird und für den Benutzer nicht sichtbar ist. Jedes Projekt verwendet einen anderen Bucket. Derzeit befinden sich die Buckets im gleichen Bereich wie die Cloud Volumes Service Volumes, es werden jedoch noch weitere Optionen erläutert. In der Dokumentation finden Sie den aktuellen Status.

Der Datentransport von einem Cloud Volumes Service-Bucket zu GCS nutzt Service-interne Google-Netzwerke mit HTTPS und TLS1.2. Die Daten werden im Ruhezustand mit von Google gemanagten Schlüsseln verschlüsselt.

Um Cloud Volumes Service-Backups zu managen (Backups erstellen, löschen und wiederherstellen), muss ein Benutzer über die verfügen "Rollen/netappCloudVolumes.admin" Rolle:

Der Netapp Architektur Sind

Überblick

Als Teil des Vertrauens einer Cloud-Lösung müssen Sie die Architektur und die Art und Weise der Sicherheit kennen. In diesem Abschnitt werden verschiedene Aspekte der Cloud Volumes Service-Architektur in Google erläutert, um mögliche Bedenken hinsichtlich der Datensicherheit zu zerstreuen und Bereiche herauszurufen, in denen zusätzliche Konfigurationsschritte erforderlich sind, um die sichere Implementierung zu erhalten.

Die allgemeine Architektur von Cloud Volumes Service kann in zwei Hauptkomponenten aufgeteilt werden: Die Kontrollebene und die Datenebene.

Kontrollebene

Die Kontrollebene in Cloud Volumes Service ist die von Cloud Volumes Service-Administratoren und der nativen Automatisierungssoftware von NetApp gemanagte Back-End-Infrastruktur. Diese Ebene ist für Endbenutzer vollständig transparent und beinhaltet Netzwerk, Storage-Hardware, Software-Updates usw., um einen Mehrwert für eine Cloud-residente Lösung wie Cloud Volumes Service bereitzustellen.

Datenebene

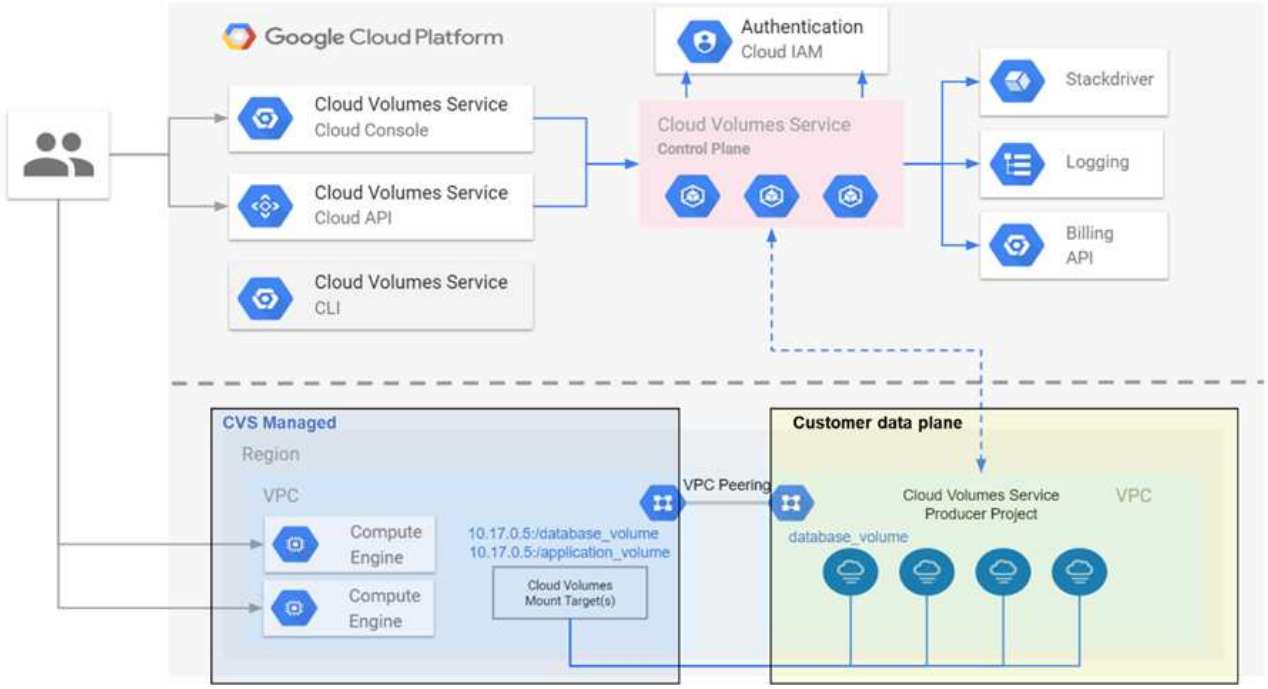
Die Datenebene in Cloud Volumes Service umfasst die tatsächlichen Daten-Volumes und die gesamte Cloud Volumes Service-Konfiguration (wie Zugriffssteuerung, Kerberos Authentifizierung usw.). Die Datenebene unterliegt vollständig der Kontrolle von Endbenutzern und Nutzern der Cloud Volumes Service Plattform.

Es gibt unterschiedliche Arten, wie jede Ebene gesichert und verwaltet wird. In den folgenden Abschnitten werden diese Unterschiede näher beschrieben. Zunächst wird die Cloud Volumes Service Architektur im Überblick angezeigt.

Architektur von Cloud Volumes Service

Cloud Volumes Service verwendet in ähnlicher Weise wie andere Cloud-native Dienste von Google wie CloudSQL, Google Cloud VMware Engine (GCVE) und FileStore "Google PSA" Für die Bereitstellung des Service. In PSA werden Dienste innerhalb eines Service-Producer-Projekts aufgebaut, das verwendet wird "VPC-Netzwerk-Peering" So stellen Sie eine Verbindung zum Serviceverbraucher her. Der Hersteller des Service wird von NetApp bereitgestellt und betrieben. Der Serviceverbraucher ist eine VPC in einem Kundenprojekt und hostet die Clients, die auf Cloud Volumes Service Dateifreigaben zugreifen möchten.

Die folgende Abbildung, auf die im Bezug genommen wird "Abschnitt zur Architektur" In der Cloud Volumes Service-Dokumentation wird eine allgemeine Ansicht angezeigt.



Der Teil über der gepunkteten Linie zeigt die Kontrollebene des Services an, der den Volumenlebenszyklus steuert. Der Teil unterhalb der gepunkteten Linie zeigt die Datenebene. Das linke blaue Feld zeigt die Benutzer-VPC (Service-Verbraucher), das rechte blaue Feld ist der von NetApp bereitgestellte Service-Hersteller. Beide sind über VPC-Peering verbunden.

Tenancy-Modell

In Cloud Volumes Service gelten einzelne Projekte als eigenständige Mandanten. Das bedeutet, dass Manipulationen von Volumes, Snapshot Kopien usw. pro Projekt durchgeführt werden. Das heißt, alle Volumes sind im Besitz des Projekts, in dem sie erstellt wurden. Nur das Projekt kann standardmäßig die darin enthaltenen Daten managen und darauf zugreifen. Dies wird als Ansicht der Kontrollebene des Services betrachtet.

Gemeinsam genutzte VPCs

In der Ansicht „Datenebene“ kann Cloud Volumes Service eine Verbindung zu einer gemeinsamen VPC herstellen. Sie können Volumes im Hosting-Projekt oder in einem der Service-Projekte erstellen, die mit der gemeinsam genutzten VPC verbunden sind. Alle mit dieser gemeinsamen VPC verbundenen Projekte (Host oder Service) sind in der Lage, die Volumes auf der Netzwerkebene (TCP/IP) zu erreichen. Da alle Clients mit Netzwerkkonnektivität auf der gemeinsam genutzten VPC potenziell über NAS-Protokolle auf die Daten zugreifen können, muss die Zugriffssteuerung für das individuelle Volume (z. B. User-/Group-Zugriffssteuerungslisten (ACLs) und Hostnamen/IP-Adressen für NFS-Exporte) verwendet werden, um zu kontrollieren, wer auf die Daten zugreifen kann.

Sie können Cloud Volumes Service mit bis zu fünf VPCs pro Kundenprojekt verbinden. In der Kontrollebene können Sie mit dem Projekt alle erstellten Volumes managen – unabhängig von der VPC, mit der sie verbunden sind. Auf der Datenebene sind VPCs voneinander isoliert, wobei jedes Volume nur mit einer VPC verbunden werden kann.

Der Zugriff auf einzelne Volumes wird über protokollspezifische Zugriffskontrollmechanismen (NFS/SMB) gesteuert.

Das bedeutet, dass auf der Netzwerkebene alle mit der gemeinsam genutzten VPC verbundenen Projekte in der Lage sind, das Volume zu sehen, während auf der Managementseite nur die Kontrollebene es dem Owner-Projekt erlaubt, das Volume zu sehen.

VPC-Service-Kontrollen

VPC-Service-Kontrollen einrichten eine Zugriffskontrollumgebung um Google Cloud Services herum, die mit dem Internet verbunden sind und weltweit zugänglich sind. Diese Dienste bieten Zugriffskontrolle über Benutzeridentitäten, können aber nicht einschränken, aus welchen Netzwerkstandortanforderungen stammen. Die VPC-Service-Kontrollen schließen diese Lücke, indem sie Funktionen zur Einschränkung des Zugriffs auf definierte Netzwerke einführen.

Die Cloud Volumes Service-Datenebene ist nicht mit dem externen Internet verbunden, sondern mit privaten VPCs mit klar definierten Netzwerkgrenzen (Perimeter). Innerhalb dieses Netzwerks verwendet jedes Volume eine protokollspezifische Zugriffssteuerung. Jegliche externe Netzwerkverbindung wird explizit von Google Cloud-Projektadministratoren erstellt. Die Kontrollebene bietet jedoch nicht denselben Schutz wie die Datenebene und kann von jedem beliebigen Ort mit gültigen Zugangsdaten aufgerufen werden ("JWT-Token").

Kurz gesagt, die Cloud Volumes Service Datenebene bietet die Möglichkeit der Netzwerk-Zugriffssteuerung, ohne dass die VPC-Service-Kontrollen unterstützt werden müssen. Außerdem werden nicht explizit VPC-Service-Controls verwendet.

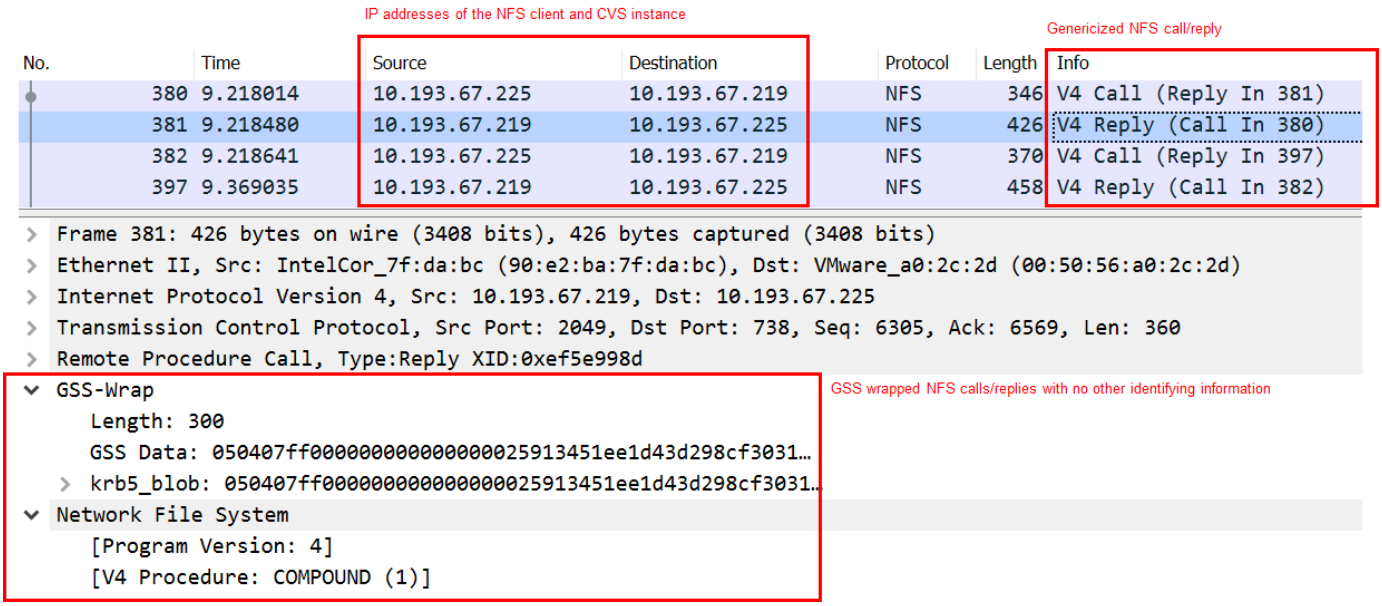
Überlegungen zu Packet Sniffing/Trace

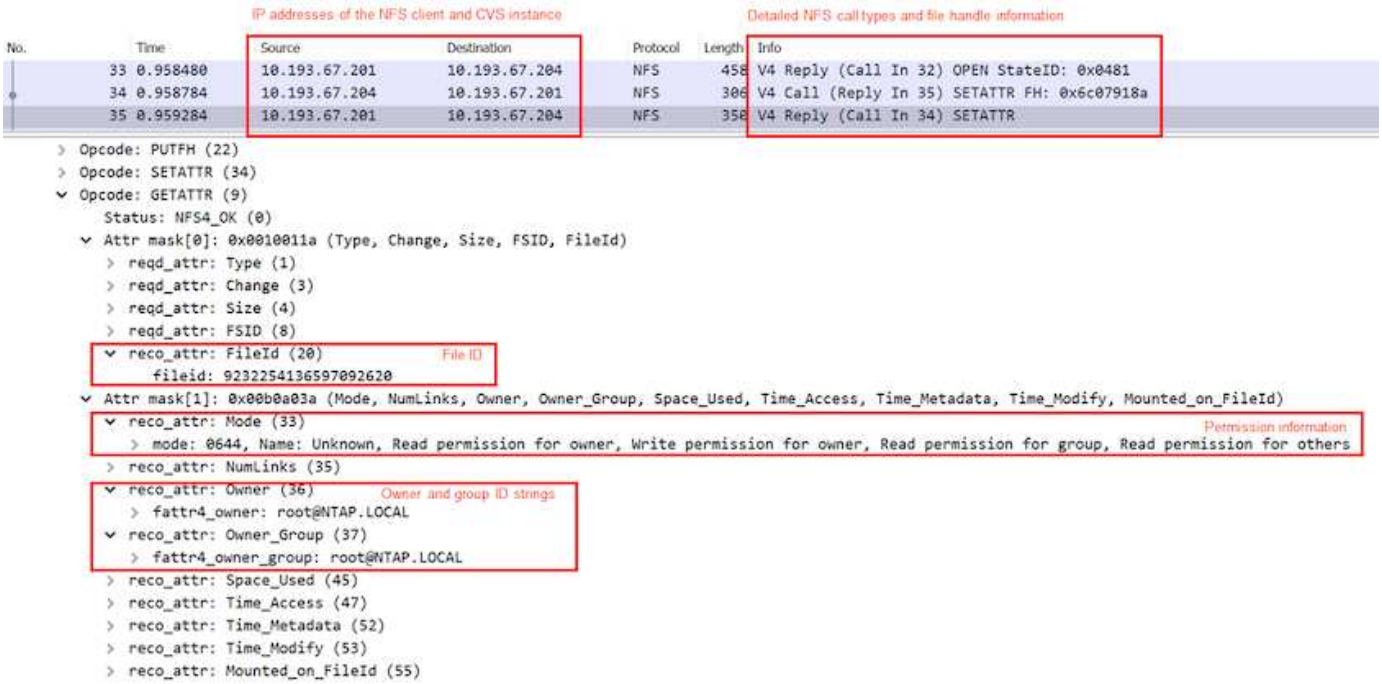
Paketerfassungen können für die Behebung von Netzwerkproblemen oder anderen Problemen (z. B. NAS-Berechtigungen, LDAP-Konnektivität usw.) nützlich sein, können aber auch missverständlich verwendet werden, um Informationen über Netzwerk-IP-Adressen, MAC-Adressen, Benutzer- und Gruppennamen und die Sicherheitsstufe für Endpunkte zu erhalten. Aufgrund der Art und Weise, wie Google Cloud-Netzwerke, VPCs und Firewall-Regeln konfiguriert werden, sollte ein unerwünschter Zugriff auf Netzwerkpakete ohne Benutzeranmeldung oder nur schwer zu erhalten sein "JWT-Token" In Cloud-Instanzen integriert. Paketerfassungen sind nur auf Endpunkten (z. B. Virtual Machines (VMs) möglich und nur in Endpunkten innerhalb der VPC möglich, es sei denn, ein Shared VPC und/oder ein externer Netzwerktunnel/IP-Weiterleitung wird verwendet, um explizit externen Traffic zu Endpunkten zu erlauben. Es gibt keine Möglichkeit, den Verkehr außerhalb der Kunden zu schnuppern.

Bei gemeinsamen VPCs wird die Verschlüsselung auf der Übertragungsstrecke mit NFS Kerberos und/oder genutzt "SMB-Verschlüsselung" Kann einen Großteil der Informationen aus Spuren verbergen. Allerdings wird noch etwas Verkehr in Klartext gesendet, wie "DNS" Und "LDAP-Abfragen". Die folgende Abbildung zeigt eine Paketerfassung aus einer Klartext-LDAP-Abfrage, die aus Cloud Volumes Service stammt, und die potenziellen identifizierenden Informationen, die freigelegt wurden. LDAP-Abfragen in Cloud Volumes Service unterstützen derzeit keine Verschlüsselung oder LDAP über SSL. CVS-Performance unterstützt LDAP-Signatur, falls durch Active Directory angefordert. CVS-SW unterstützt LDAP-Signatur nicht.

UnixUserPassword wird von LDAP abgefragt und nicht im Klartext, sondern in einem gesalzenem Hash gesendet. Standardmäßig füllt Windows LDAP die Felder unixUserPassword nicht aus. Dieses Feld ist nur erforderlich, wenn Sie Windows LDAP für interaktive Anmeldungen über LDAP für Clients verwenden müssen. Cloud Volumes Service unterstützt keine interaktiven LDAP-Anmeldungen bei den Instanzen.

Die folgende Abbildung zeigt eine Paketerfassung aus einem NFS-Kerberos-Gespräch neben einer NFS-Erfassung über AUTH_SYS. Beachten Sie, wie sich die Informationen in einer Kurve zwischen den beiden unterscheiden und wie die Aktivierung der Verschlüsselung während der Übertragung eine größere Gesamtsicherheit für den NAS-Datenverkehr bietet.





VM-Netzwerkschnittstellen

Angreifer können versuchen, eine neue Netzwerkschnittstellenkarte (NIC) zu einer VM in hinzuzufügen "Promiskuous Modus" (Port-Spiegelung) oder aktivieren Sie den Promiskuus-Modus auf einer vorhandenen NIC, um den gesamten Datenverkehr zu entschnüffeln. Beim Hinzufügen einer neuen NIC muss in Google Cloud eine VM vollständig heruntergefahren werden, was zu Warnmeldungen führt. So können Angreifer nicht unbemerkt das tun.

Darüber hinaus können NICs überhaupt nicht auf den promiskuitiven Modus eingestellt werden und erzeugen in Google Cloud Warnmeldungen.

Kontrollebene Architektur

Alle Management-Aktionen an Cloud Volumes Service werden über die API ausgeführt. Das in die GCP Cloud Console integrierte Cloud Volumes Service-Management verwendet auch die Cloud Volumes Service-API.

Identitäts- und Zugriffsmanagement

Identitäts- und Zugriffsmanagement ("IAM") Ist ein Standardservice, mit dem Sie Authentifizierung (Logins) und Berechtigungen (Berechtigungen) für Google Cloud-Projektinstanzen steuern können. Google IAM bietet ein vollständiges Audit-Protokoll über Berechtigungen zum Berechtigungs- und Entfernen. Derzeit bietet Cloud Volumes Service keine Prüfung auf Kontrollebenen.

Autorisierungs-/Berechtigungs-Übersicht

IAM bietet integrierte, granulare Berechtigungen für Cloud Volumes Service. Hier finden Sie ein "Vollständige Liste mit granularen Berechtigungen hier".

IAM bietet außerdem zwei vordefinierte Rollen, die als Namen bezeichnet werden `netappcloudvolumes.admin` Und `netappcloudvolumes.viewer`. Diese Rollen können bestimmten Benutzern oder Servicekonten zugewiesen werden.

Weisen Sie geeignete Rollen und Berechtigungen zu, um IAM-Benutzern das Management von Cloud Volumes Service zu ermöglichen.

Beispiele für die Verwendung granularer Berechtigungen sind:

- Erstellen Sie eine benutzerdefinierte Rolle nur mit Berechtigungen zum Abrufen/Auflisten/Erstellen/Aktualisieren, damit Benutzer Volumes nicht löschen können.
- Verwenden Sie eine benutzerdefinierte Rolle nur mit `snapshot.*` Berechtigungen zum Erstellen eines Servicekontos, das zum Aufbau einer applikationskonsistenten Snapshot Integration verwendet wird.
- Erstellen Sie eine benutzerdefinierte Rolle zum Delegieren `volumereplication.*` An bestimmte Benutzer.

Servicekonten

Um Cloud Volumes Service-API-Aufrufe über Skripte oder durchzuführen "Terraform", Sie müssen ein Dienstkonto mit dem erstellen `roles/netappcloudvolumes.admin` Rolle: Sie können dieses Dienstkonto verwenden, um die JWT-Token zu generieren, die zur Authentifizierung von Cloud Volumes Service-API-Anforderungen erforderlich sind:

- Generieren Sie einen JSON-Schlüssel und verwenden Sie Google APIs, um daraus ein JWT-Token abzuleiten. Dies ist der einfachste Ansatz, aber es beinhaltet manuelle Geheimnisse (den JSON-Schlüssel) Management.
- Nutzung "Imitation von Servicekonten" Mit `roles/iam.serviceAccountTokenCreator`. Der Code (Skript, Terraform usw.) läuft mit "Standardanmeldedaten Für Anwendungen" Und personifiziert das Servicekonto, um seine Berechtigungen zu erhalten. Dieser Ansatz spiegelt die Best Practices für die Sicherheit von Google wider.

Siehe "Erstellen Ihres Servicekontos und privaten Schlüssels" In der Google Cloud Dokumentation finden Sie weitere Informationen.

Cloud Volumes Service API

Die Cloud Volumes Service API verwendet eine REST-basierte API mithilfe von HTTPS (TLSv1.2) als zugrunde liegenden Netzwerktransport. Hier finden Sie die neueste API-Definition "Hier" Und Informationen zur Verwendung der API unter "Cloud Volumes APIs in der Google Cloud-Dokumentation".

Der API-Endpunkt wird durch NetApp mit Standard-HTTPS-Funktionalität (TLSv1.2) betrieben und gesichert.

JWT-Token

Die Authentifizierung an der API erfolgt mit JWT-Inhabertoken ("RFC-7519"). Gültige JWT-Token müssen über die Google Cloud IAM-Authentifizierung abgerufen werden. Dazu muss ein Token vom IAM abgerufen werden, indem ein JSON-Schlüssel für ein Servicekonto bereitgestellt wird.

Audit-Protokollierung

Derzeit sind keine vom Benutzer zugänglichen Prüfprotokolle für Kontrollebenen verfügbar.

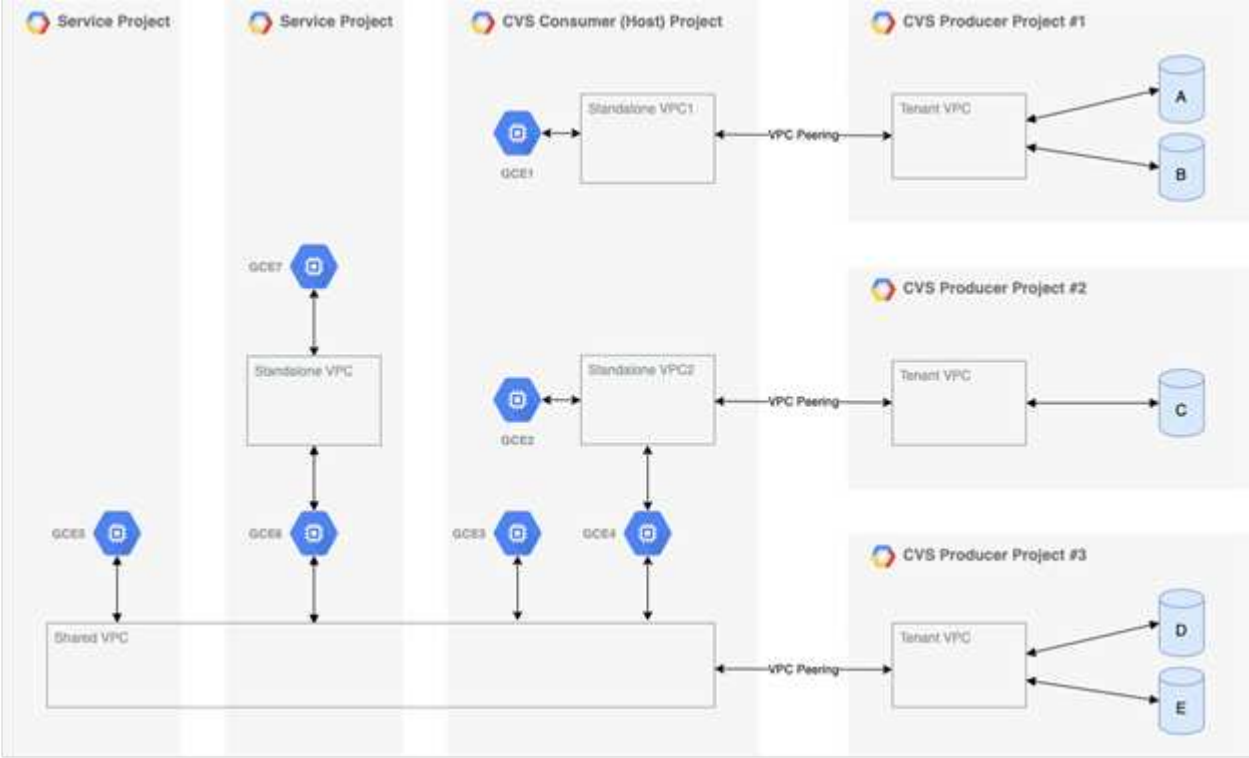
Datenplanarchitektur

Cloud Volumes Service für Google Cloud nutzt die Google Cloud "Zugang zu privaten Services" Framework: In diesem Framework können sich Benutzer mit dem Cloud

Volumes Service verbinden. Dieses Framework verwendet Service Networking und VPC Peering so wie andere Google Cloud-Services, dass die vollständige Isolierung zwischen Mandanten gewährleistet ist.

Eine Übersicht über die Architektur von Cloud Volumes Service für Google Cloud finden Sie unter "Architektur für Cloud Volumes Service".

Benutzer-VPCs (Standalone oder Shared) werden an VPCs innerhalb von Cloud Volumes Service gemanagten Mandantenprojekten weitergegeben, die die Volumes hostet.



Die obige Abbildung zeigt ein Projekt (das CVS Verbraucherprojekt in der Mitte) mit drei VPC-Netzwerken, die mit Cloud Volumes Service verbunden sind, und mehreren Compute Engine VMs (GCE1-7), die Volumes gemeinsam nutzen:

- VPC1 ermöglicht GCE1 auf Volumes A und B. zuzugreifen
- VPC2 ermöglicht GCE2 und GCE4 den Zugriff auf Lautstärke C.
- Das dritte VPC-Netzwerk ist eine gemeinsame VPC, von der zwei Service-Projekte gemeinsam genutzt werden. GCE3, GCE4, GCE5 und GCE6 können auf Volumes D und E. zugreifen Shared VPC-Netzwerke werden nur für Volumes des Servicetyps „CVS-Performance“ unterstützt.

GCE7 kann auf keine Volumes zugreifen.

Die Daten können sowohl bei der Übertragung (mit Kerberos- und/oder SMB-Verschlüsselung) als auch im Ruhezustand in Cloud Volumes Service verschlüsselt werden.

Datenverschlüsselung während der Übertragung

Die übertragenen Daten können auf der NAS-Protokollebene verschlüsselt und das Google Cloud-Netzwerk selbst verschlüsselt werden, wie in den folgenden Abschnitten

beschrieben.

Google Cloud Network

Google Cloud verschlüsselt den Datenverkehr auf Netzwerkebene wie in beschrieben "Verschlüsselung während der Übertragung" In der Google-Dokumentation. Wie im Abschnitt „Cloud Volumes Services Architecture“ erwähnt, wird Cloud Volumes Service aus einem von NetApp gesteuerten PSA Producer-Projekt bereitgestellt.

Im Fall von CVS-SW führt der Producer-Mandant Google VMs aus, um den Service bereitzustellen. Der Datenverkehr zwischen Benutzer-VMs und Cloud Volumes Service-VMs wird automatisch durch Google verschlüsselt.

Obwohl der Datenpfad für CVS-Performance nicht vollständig auf der Netzwerkebene verschlüsselt ist, verwenden NetApp und Google eine Kombination "Der IEEE 802.1AE Verschlüsselung (MACsec)", "Kapselung" (Datenverschlüsselung) und Netzwerke mit physischen Einschränkungen zum Schutz der Daten bei der Übertragung zwischen dem Cloud Volumes Service CVS-Performance Servicetyp und Google Cloud

NAS-Protokolle

Die NAS-Protokolle NFS und SMB bieten optionale Transportverschlüsselung auf Protokollebene.

SMB-Verschlüsselung

"SMB-Verschlüsselung" Bietet End-to-End-Verschlüsselung von SMB-Daten und schützt Daten vor abfallenden Ereignissen in nicht vertrauenswürdigen Netzwerken. Sie können die Verschlüsselung sowohl für die Client-/Server-Datenverbindung (nur für SMB3.x-fähige Clients verfügbar) als auch für die Server/Domain-Controller-Authentifizierung aktivieren.

Wenn die SMB-Verschlüsselung aktiviert ist, können Clients, die keine Verschlüsselung unterstützen, nicht auf die Freigabe zugreifen.

Cloud Volumes Service unterstützt RC4-HMAC, AES-128-CTS-HMAC-SHA1 und AES-256-CTS-HMAC-SHA1-Sicherheitschiffren für SMB-Verschlüsselung. SMB verhandelt den vom Server am häufigsten unterstützten Verschlüsselungstyp.

Kerberos: NFSv4.1

Für NFSv4.1 bietet CVS-Performance Kerberos-Authentifizierung wie in beschrieben "RFC7530". Sie können Kerberos auf Volume-Basis aktivieren.

Der derzeit stärkste verfügbare Verschlüsselungstyp für Kerberos ist AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service unterstützt AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 und DES für NFS. Es unterstützt auch ARCFOUR-HMAC (RC4) für CIFS/SMB-Datenverkehr, jedoch nicht für NFS.

Kerberos bietet drei verschiedene Sicherheitsstufen für NFS-Mounts, die Möglichkeiten bieten, wie stark die Kerberos-Sicherheit sein sollte.

As per RedHat "Allgemeine Mount-Optionen" Dokumentation:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

Je mehr der Kerberos-Sicherheitslevel zu tun hat, desto schlechter ist die Performance, da Client und Server Zeit damit verbringen, NFS-Vorgänge für jedes gesendete Paket zu verschlüsseln und zu entschlüsseln. Viele Clients und NFS Server unterstützen AES-NI-Entlastung der CPUs, um insgesamt eine bessere Benutzererfahrung zu erzielen. Die Auswirkungen von Kerberos 5p (vollständige End-to-End-Verschlüsselung) sind jedoch deutlich höher als die Auswirkungen von Kerberos 5 (Benutzerauthentifizierung).

Die folgende Tabelle zeigt Unterschiede in den einzelnen Ebenen in Bezug auf Sicherheit und Performance.

Sicherheitsstufe	Sicherheit	Leistung
NFSv3 – sys	• Am wenigsten sicher; Klartext mit numerischen Benutzer-IDs/Gruppen-IDs • Kann UID, GID, Client-IP-Adressen, Exportpfade, Dateinamen, Berechtigungen in Paketaufnahmen	• Das Beste für die meisten Fälle
NFSv4.x – sys	• Sicherer als NFSv3 (Client-IDs, Namenszeichenfolge/Domänen zeichenfolge-Übereinstimmung), aber immer noch Klartext • Kann UID, GID, Client-IP-Adressen, Namensstrings, Domänen-IDs, anzeigen Pfade, Dateinamen und Berechtigungen in Paketaufnahmen exportieren	• Gut für sequenzielle Workloads (z. B. VMs, Datenbanken, große Dateien) • Schlecht mit hoher Dateianzahl/hohen Metadaten (30-50% schlechter)

Sicherheitsstufe	Sicherheit	Leistung
NFS – krb5	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – schließt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Benutzer, die Zugriff auf das Mount anfordern, benötigen ein gültiges Kerberos-Ticket (entweder über den Benutzernamen/das Passwort oder den Austausch des manuellen Schlüssels); das Ticket läuft nach einem bestimmten Zeitraum ab und der Benutzer muss sich erneut authentifizieren, um Zugriff zu erhalten • Keine Verschlüsselung für NFS-Vorgänge oder Zusatz-Protokolle wie Mount/Portmapper/nlm (kann Exportpfade, IP-Adressen, Dateihandles, Berechtigungen, Dateinamen, Uhrzeit/Mtime in Paketaufnahmen)	• Am besten in den meisten Fällen für Kerberos; schlechter als AUTH_SYS

Sicherheitsstufe	Sicherheit	Leistung
NFS – krb5i	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – schließt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Benutzer, die Zugriff auf das Mount anfordern, benötigen ein gültiges Kerberos-Ticket (entweder über Benutzernamen/Passwort oder den Austausch des manuellen Schlüssels); das Ticket läuft nach einem bestimmten Zeitraum ab und der Benutzer muss sich erneut authentifizieren, um Zugriff zu erhalten • Keine Verschlüsselung für NFS-Vorgänge oder Zusatz-Protokolle wie Mount/Portmapper/nlm (kann Exportpfade, IP-Adressen, Dateihandles, Berechtigungen, Dateinamen, Uhrzeit/Mtime in Paketaufnahmen) • Kerberos GSS-Prüfsumme wird zu jedem Paket hinzugefügt, damit die Pakete nicht abgefangen werden. Wenn Prüfsummen übereinstimmen, ist das Gespräch zulässig.	• Besser als krb5p, da die NFS-Nutzlast nicht verschlüsselt ist; nur der zusätzliche Overhead im Vergleich zu krb5 ist die Integritäts-Prüfsumme. Die Leistung von krb5i wird nicht viel schlechter sein als krb5, aber wird einige Verschlechterung zu sehen.

Sicherheitsstufe	Sicherheit	Leistung
NFS – krb5p	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – schließt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Benutzer, die Zugriff auf das Mount anfordern, benötigen ein gültiges Kerberos-Ticket (entweder über Benutzernamen/Passwort oder den manuellen Schlüsseltab-Austausch); das Ticket läuft nach einem festgelegten Zeitraum ab und der Benutzer muss sich erneut authentifizieren, um Zugriff zu erhalten • Alle Payloads des NFS-Pakets sind mit dem GSS-Wrapper verschlüsselt (Dateihandles, Berechtigungen, Dateinamen, atime/mtime in Paketaufnahmen können nicht angezeigt werden). • Umfasst die Integritätsprüfung. • Der NFS Operationstyp ist sichtbar (FSINFO, ACCESS, GETATTR usw.). • Zusatzprotokolle (Mount, Portmap, nlm usw.) sind nicht verschlüsselt - (kann Exportpfade, IP-Adressen sehen)	• Schlechteste Leistung der Sicherheitsstufen; krb5p muss mehr verschlüsseln/entschlüsseln. • Bessere Performance als krb5p mit NFSv4.x für Workloads mit hoher Dateianzahl.

In Cloud Volumes Service wird ein konfigurierter Active Directory-Server als Kerberos-Server und LDAP-Server verwendet (um Benutzeridentitäten aus einem RFC2307-kompatiblen Schema zu suchen). Es werden keine anderen Kerberos oder LDAP-Server unterstützt. NetApp empfiehlt besonders, LDAP für das Identitätsmanagement in Cloud Volumes Service zu verwenden. Informationen darüber, wie NFS Kerberos in Paketaufnahmen angezeigt wird, finden Sie im Abschnitt "„Packet Sniffing/Trace Betrachtungen.“"

Verschlüsselung von Daten im Ruhezustand

Alle Volumes in Cloud Volumes Service werden im Ruhezustand mit AES-256-Verschlüsselung verschlüsselt, d. h. alle auf das Medium geschriebenen Benutzerdaten werden verschlüsselt und können nur mit einem Schlüssel pro Volume entschlüsselt werden.

- Für CVS-SW werden von Google generierte Schlüssel verwendet.

- Die Schlüssel für CVS-Performance werden in einem im Cloud Volumes Service integrierten Schlüsselmanager gespeichert, der die Schlüssel pro Volume enthält.

Ab November 2021 wurde eine Vorschau auf die Funktionalität der vom Kunden gemanagten Verschlüsselungsschlüssel (CMEK) bereitgestellt. So können Sie die Schlüssel pro Volume mit einem in einzelnen Projekten und Regionen gehosteten Master-Schlüssel verschlüsseln "Google Key Management Service (KMS):" KMS ermöglicht es Ihnen, externe Schlüsselmanager anzubinden.

Informationen zur Konfiguration von KMS für CVS-Performance finden Sie unter "Einrichten von vom Kunden gemanagten Verschlüsselungsschlüsseln".

Firewall

Cloud Volumes Service legt mehrere TCP Ports für NFS- und SMB-Freigaben bereit:

- "Für NFS-Zugriff erforderliche Ports"
- "Für SMB-Zugriff erforderliche Ports"

Außerdem erfordern SMB, NFS mit LDAP, einschließlich Kerberos und Dual-Protokoll-Konfigurationen den Zugriff auf eine Windows Active Directory Domain. Active Directory-Verbindungen müssen sein "Konfiguriert" Pro Region. Active Directory-Domänencontroller (DC) werden mithilfe identifiziert "DNS-basierte DC-Erkennung" Verwenden der angegebenen DNS-Server. Alle zurückgegebenen Datacenter werden genutzt. Die Liste der geeigneten DCs kann durch Angabe einer Active Directory-Site beschränkt werden.

Cloud Volumes Service erreicht mit IP-Adressen aus dem CIDR-Bereich, der dem zugewiesen ist `gcloud compute address` Befehl während "On-Boarding the Cloud Volumes Service". Sie können dieses CIDR als Quelladressen verwenden, um eingehende Firewalls für Ihre Active Directory-Domänencontroller zu konfigurieren.

Active Directory-Domänencontroller müssen "Legen Sie wie hier erwähnt Ports den Cloud Volumes Service-CIDRs offen".

NAS-Protokolle

Übersicht über NAS-Protokolle

Die NAS-Protokolle umfassen NFS (v3 und v4.1) und SMB/CIFS (2.x und 3.x). Mit diesen Protokollen ermöglicht CVS gemeinsamen Zugriff auf Daten über mehrere NAS Clients hinweg. Darüber hinaus ermöglicht Cloud Volumes Service den gleichzeitigen Zugriff auf NFS- und SMB/CIFS-Clients (Dual-Protokoll), während sämtliche Identitäts- und Berechtigungseinstellungen auf Dateien und Ordnern in den NAS-Freigaben berücksichtigt werden. Cloud Volumes Service unterstützt die Protokollverschlüsselung im laufenden Betrieb mit SMB-Verschlüsselung und NFS Kerberos 5p, um die höchstmögliche Sicherheit bei Datentransfers zu gewährleisten.

Das Dual-Protokoll ist nur mit CVS-Performance verfügbar.

Grundlagen der NAS-Protokolle

NAS-Protokolle sind Möglichkeiten für mehrere Clients im Netzwerk, um auf dieselben Daten in einem Storage-System zuzugreifen, beispielsweise auf Cloud Volumes Service

in GCP. NFS und SMB sind die definierten NAS-Protokolle und werden auf Client-/Server-Basis ausgeführt, wobei Cloud Volumes Service als Server fungiert. Clients senden Zugriffs-, Lese- und Schreibanfragen an den Server, und der Server ist für die Koordinierung der Sperrmechanismen für Dateien, die Speicherung von Berechtigungen und die Bearbeitung von Identitäts- und Authentifizierungsanforderungen zuständig.

Der folgende allgemeine Prozess wird beispielsweise verfolgt, wenn ein NAS-Client eine neue Datei in einem Ordner erstellen möchte.

1. Der Client fragt den Server nach Informationen zum Verzeichnis (Berechtigungen, Eigentümer, Gruppe, Datei-ID, verfügbarer Speicherplatz, Und so weiter); der Server antwortet mit den Informationen, wenn der anfragende Client und der Benutzer die erforderlichen Berechtigungen für den übergeordneten Ordner haben.
2. Wenn die Berechtigungen im Verzeichnis den Zugriff zulassen, fragt der Client den Server, ob der erstellte Dateiname bereits im Dateisystem vorhanden ist. Wenn der Dateiname bereits verwendet wird, schlägt die Erstellung fehl. Wenn der Dateiname nicht vorhanden ist, lässt der Server dem Client wissen, dass er fortgesetzt werden kann.
3. Der Client ruft den Server aus, um die Datei mit dem Verzeichnis-Handle und dem Dateinamen zu erstellen, und legt die Zugriffszeiten und die geänderten Zeiten fest. Der Server gibt eine eindeutige Datei-ID für die Datei aus, um sicherzustellen, dass keine anderen Dateien mit derselben Datei-ID erstellt werden.
4. Der Client sendet einen Anruf, um Dateiattribute vor DEM SCHREIBVORGANG zu überprüfen. Falls dies durch Berechtigungen möglich ist, schreibt der Client die neue Datei. Falls das Protokoll oder die Applikation gesperrt wird, fordert der Client den Server zur Sperrung auf, um zu verhindern, dass andere Clients auf die Datei zugreifen können, während diese gesperrt ist, um Datenbeschädigungen zu verhindern.

NFS

NFS ist ein Distributed File System-Protokoll. Es handelt sich um einen offenen IETF-Standard, der in Request for Comments (RFC) definiert ist und unter dem jeder dieses Protokoll implementieren kann.

Volumes in Cloud Volumes Service werden für NFS-Clients freigegeben, indem ein Pfad exportiert wird, der für einen Client oder eine Gruppe von Clients zugänglich ist. Die Berechtigungen zum Mounten dieser Exporte werden durch Richtlinien und Regeln für den Export definiert, die von Cloud Volumes Service-Administratoren konfiguriert werden können.

Die NetApp NFS-Implementierung gilt als Gold-Standard für das Protokoll und wird in unzähligen Enterprise-NAS-Umgebungen eingesetzt. In den folgenden Abschnitten werden NFS, spezifische Sicherheitsfunktionen in Cloud Volumes Service sowie deren Implementierung behandelt.

Lokale UNIX-Standardbenutzer und -Gruppen

Cloud Volumes Service enthält mehrere UNIX Standard-Benutzer und -Gruppen für verschiedene grundlegende Funktionen. Diese Benutzer und Gruppen können derzeit nicht geändert oder gelöscht werden. Neue lokale Benutzer und Gruppen können derzeit nicht zu Cloud Volumes Service hinzugefügt werden. UNIX-Benutzer und -Gruppen außerhalb der Standardbenutzer und -Gruppen müssen von einem externen LDAP-Namensdienst bereitgestellt werden.

Die folgende Tabelle zeigt die Standardbenutzer und -Gruppen sowie die zugehörigen numerischen IDs. NetApp empfiehlt, keine neuen Benutzer oder Gruppen in LDAP oder auf den lokalen Clients zu erstellen, die

diese numerischen IDs erneut verwenden.

Standardbenutzer: Numerische IDs	Standardgruppen: Numerische IDs
• Stammverzeichnis:0 • Pcuser:65534 • Niemand:65535	• Stammverzeichnis:0 • Daemon: 1 • Pcuser:65534 • Niemand:65535

Bei der Verwendung von NFSv4.1 wird der Root-Benutzer möglicherweise als niemand angezeigt, wenn er Verzeichnislisting-Befehle auf NFS-Clients ausführt. Dies liegt an der Konfiguration der ID-Domänenzuordnung des Clients. Siehe Abschnitt genannt NFSv4.1 und der niemand-Benutzer/Gruppe Finden Sie weitere Informationen zu diesem Problem und wie Sie es lösen können.

Der Root-Benutzer

In Linux hat das Root-Konto Zugriff auf alle Befehle, Dateien und Ordner in einem Linux-basierten Dateisystem. Aufgrund der Leistungsfähigkeit dieses Kontos müssen Benutzer häufig aufgrund von Best Practices für die Sicherheit deaktiviert oder auf irgendeine Weise eingeschränkt werden. Bei NFS-Exporten kann die Leistung, die ein Root-Benutzer über die Dateien und Ordner hat, im Cloud Volumes Service über Exportrichtlinien und -Regeln gesteuert werden. Auch das Konzept wird als Root Squash bezeichnet.

Root-Squashing sorgt dafür, dass der Root-Benutzer, der auf eine NFS-Bereitstellung zugreift, auf den anonymen numerischen Benutzer 65534 (siehe Abschnitt „Der anonyme Benutzer“) und ist derzeit nur verfügbar, wenn CVS-Performance verwendet wird, indem Sie bei der Erstellung von Regeln für Exportrichtlinien aus für Root-Zugriff auswählen. Wenn der Root-Benutzer auf den anonymen Benutzer zerquetscht wird, hat er keinen Zugriff mehr auf das Ausführen von Chown oder "Setuid/setgid-Befehle (das klebrige Bit)" In Dateien oder Ordnern im NFS-Mount und Dateien oder Ordnern, die vom Root-Benutzer erstellt wurden, zeigen die Anon-UID als Eigentümer/Gruppe an. Darüber hinaus können NFSv4 ACLs nicht vom Root-Benutzer geändert werden. Der Root-Benutzer hat jedoch weiterhin Zugriff auf chmod und gelöschte Dateien, für die er keine expliziten Berechtigungen besitzt. Wenn Sie den Zugriff auf die Datei- und Ordnerberechtigungen eines Root-Benutzers beschränken möchten, ziehen Sie in Betracht, ein Volume mit NTFS ACLs zu verwenden und einen Windows-Benutzer mit dem Namen zu erstellen `root`, Und die gewünschten Berechtigungen auf die Dateien oder Ordner anwenden.

Der anonyme Benutzer

Die anonyme (anon) Benutzer-ID gibt eine UNIX-Benutzer-ID oder einen UNIX-Benutzernamen an, der Client-Anforderungen ohne gültige NFS-Anmeldeinformationen zugeordnet ist. Dies kann den Root-Benutzer einschließen, wenn Root-Squashing verwendet wird. Der anon-Benutzer in Cloud Volumes Service ist 65534.

Diese UID ist normalerweise dem Benutzernamen zugeordnet `nobody` Oder `nfsnobody` In Linux Umgebungen zu managen. Cloud Volumes Service verwendet auch 65534 als den lokalen UNIX-Benutzer` pcuser` (siehe Abschnitt “Lokale UNIX-Standardbenutzer und -Gruppen“), der auch der Standard-Fallback-Benutzer für Windows auf UNIX-Namenszuordnungen ist, wenn kein gültiger übereinstimmender UNIX-Benutzer in LDAP gefunden werden kann.

Aufgrund der Unterschiede bei Benutzernamen in Linux und Cloud Volumes Service für UID 65534, konnte die Namenszeichenfolge für Benutzer, die 65534 zugeordnet sind, bei der Verwendung von NFSv4.1 nicht übereinstimmen. Dies könnte zu sehen sein `nobody` Als Benutzer auf einigen Dateien und Ordnern. Siehe Abschnitt „NFSv4.1 und der niemand-Benutzer/Gruppe“ Für Informationen zu diesem Problem und zur Lösung

dieses Problems.

Zugriffssteuerung/Exporte

Der erste Export-/Freigabzugriff für NFS-Mounts wird über hostbasierte Exportrichtlinien gesteuert, die in einer Exportrichtlinie enthalten sind. Eine Host-IP, ein Hostname, ein Subnetz, eine Netzwerkgruppe oder eine Domäne sind definiert, um den Zugriff auf die Bereitstellung der NFS-Freigabe und die Zugriffsebene zu ermöglichen, die dem Host erlaubt ist. Die Konfigurationsoptionen für die Exportrichtlinie hängen von der Cloud Volumes Service-Ebene ab.

Für CVS-SW stehen die folgenden Optionen für die Konfiguration von Exportrichtlinien zur Verfügung:

- **Client-Match.** kommagetrennte Liste von IP-Adressen, kommagetrennte Liste von Hostnamen, Subnetzen, Netzgruppen, Domain-Namen.
- **RO/RW-Zugriffsregeln.** Wählen Sie Lese-/Schreibschutz oder Schreibschutz, um den Zugriff auf den Export zu steuern.CVS-Performance bietet die folgenden Optionen:
- **Client-Match.** kommagetrennte Liste von IP-Adressen, kommagetrennte Liste von Hostnamen, Subnetzen, Netzgruppen, Domain-Namen.
- **RO/RW-Zugriffsregeln.** Wählen Sie Lese-/Schreibschutz oder Schreibschutz, um den Zugriff auf den Export zu steuern.
- **Root-Zugriff (ein/aus).** konfiguriert Root Squash (siehe Abschnitt „Der Root-Benutzer„ Weitere Informationen).
- **Protokolltyp.** Dies beschränkt den Zugriff auf die NFS-Bereitstellung auf eine bestimmte Protokollversion. Wenn Sie sowohl NFSv3 als auch NFSv4.1 für das Volume angeben, lassen Sie entweder beide Felder leer oder aktivieren Sie beide Kontrollkästchen.
- **Kerberos-Sicherheitsstufe (wenn Kerberos aktivieren ausgewählt ist).** bietet die Optionen von krb5, krb5i und/oder krb5p für schreibgeschützten oder schreibgeschützten Zugriff.

Eigentümerschaft (chown) und Change Group (chgrp) ändern

NFS auf Cloud Volumes Service ermöglicht es dem Root-Benutzer nur chown/chgrp auf Dateien und Ordnern auszuführen. Andere Benutzer sehen ein `Operation not permitted` Fehler – auch bei den eigenen Dateien. Wenn Sie Root Squash verwenden (wie im Abschnitt “ beschriebenDer Root-Benutzer“), wird die Root zu einem nicht-Root-Benutzer gequetscht und darf keinen Zugriff auf Chown und chgrp haben. Derzeit gibt es in Cloud Volumes Service keine Problemumgehungen, um chown und chgrp für nicht-Root-Benutzer zu ermöglichen. Wenn Eigentumsänderungen erforderlich sind, ziehen Sie die Verwendung von doppelten Protokoll-Volumes in Erwägung und legen Sie den Sicherheitsstil auf NTFS fest, um die Berechtigungen von Windows-Seite aus zu steuern.

Berechtigungsmanagement

Cloud Volumes Service unterstützt beide Mode-Bits (z. B. 644, 777 usw. für rwx) und NFSv4.1 ACLs, um die Berechtigungen auf NFS-Clients für Volumes zu steuern, die den UNIX-Sicherheitsstil nutzen. Hierfür wird das standardmäßige Berechtigungsmanagement verwendet (z. B. chmod, chown oder nfs4_setfacl) und arbeitet mit jedem Linux-Client zusammen, der diese unterstützt.

Wenn Sie außerdem Dual-Protokoll-Volumes auf NTFS setzen, können NFS-Clients die Cloud Volumes Service-Namenszuweisung für Windows-Benutzer nutzen, die dann zur Behebung der NTFS-Berechtigungen verwendet werden. Dazu ist eine LDAP-Verbindung zu Cloud Volumes Service erforderlich, um numerische ID-zu-Benutzernamen-Übersetzungen bereitzustellen, da Cloud Volumes Service einen gültigen UNIX-Benutzernamen benötigt, um einen Windows-Benutzernamen korrekt zuzuordnen.

Bereitstellung granularer ACLs für NFSv3

Mode-Bit-Berechtigungen decken nur Besitzer, Gruppe und alle anderen in der Semantik ab. Dies bedeutet, dass für Basic NFSv3 keine granularen Benutzerzugriffskontrollen vorhanden sind. Cloud Volumes Service unterstützt weder POSIX ACLs noch erweiterte Attribute (wie z. B. Chattr), sodass granulare ACLs nur in den folgenden Szenarien mit NFSv3 möglich sind:

- NTFS Security Style Volumes (CIFS Server erforderlich) mit gültigen Zuordnungen von UNIX zu Windows-Benutzern.
- NFSv4.1 ACLs werden mithilfe eines Administrator-Clients unter Verwendung von NFSv4.1 angewendet.

Beide Methoden erfordern eine LDAP-Verbindung für das UNIX-Identitätsmanagement und eine gültige UNIX-Benutzer- und Gruppeninformationen (siehe Abschnitt "„LDAP“") Und sind nur mit CVS-Performance Instanzen verfügbar. Um Volumes im NTFS-Sicherheitsstil mit NFS zu verwenden, müssen Sie Dual-Protokoll (SMB und NFSv3) oder Dual-Protokoll (SMB und NFSv4.1) verwenden, auch wenn keine SMB-Verbindungen hergestellt werden. Um NFSv4.1 ACLs für NFSv3-Mounts zu verwenden, müssen Sie auswählen `Both (NFSv3/NFSv4.1)` Als Protokolltyp.

Normale UNIX Modus Bits bieten nicht die gleiche Granularitätsebene in Berechtigungen, die NTFS oder NFSv4.x ACLs bieten. In der folgenden Tabelle wird die Berechtigungsgranularität zwischen NFSv3-Modus-Bits und NFSv4.1 ACLs verglichen. Informationen zu NFSv4.1 ACLs finden Sie unter "nfs4_acl – NFSv4 Access Control-Listen".

Bits im NFSv3 Modus	NFSv4.1 ACLs
• Legen Sie bei der Ausführung die Benutzer-ID fest • Legen Sie bei der Ausführung die Gruppen-ID fest • Getauschtes Text speichern (nicht in POSIX definiert) • Leseberechtigung für Eigentümer • Schreibberechtigung für Eigentümer • Berechtigung für Eigentümer einer Datei ausführen oder die Berechtigung für Eigentümer im Verzeichnis suchen (suchen) • Berechtigung für Gruppe lesen • Schreibberechtigung für Gruppe • Berechtigung für eine Gruppe in einer Datei ausführen oder die Berechtigung für die Gruppe im Verzeichnis suchen (suchen) • Lesen Sie die Erlaubnis für andere • Schreibberechtigung für andere • Berechtigung für andere in einer Datei ausführen oder die Berechtigung für andere Personen im Verzeichnis suchen (suchen)	ACE-Typen (Access Control Entry) (allow/Deny/Audit) * Vererbung-Flags * Verzeichnis-Erben * Datei-Erben * No-propate-Erben * Erben-only Berechtigungen * Read-Data (Files) / list-Directory (Verzeichnisse) * Write-Data (Files) / create-file (Directories) * append-Data (files) / create-Unterverzeichnis (Directories) * execute (files) / change-Directory (Directories) * delete * delete-child * read-attributes * write-named-aCLL * write-awned-attributes * read-ACL Synchronize-awner

Schließlich ist die NFS-Gruppenmitgliedschaft (sowohl in NFSv3 als AUCH NFSV4.x) auf ein Standardlimit von 16 für AUTH_SYS begrenzt, gemäß den RPC-Paketlimits. NFS Kerberos bietet bis zu 32 Gruppen und NFSv4

ACLs entfernen die Beschränkung durch granulare Benutzer- und Gruppen-ACLs (bis zu 1024 Einträge pro ACE).

Darüber hinaus bietet Cloud Volumes Service erweiterte Gruppen-Support, um die maximal unterstützten Gruppen auf 32 zu erweitern. Dazu ist eine LDAP-Verbindung zu einem LDAP-Server erforderlich, der gültige UNIX-Benutzer- und Gruppenidentitäten enthält. Weitere Informationen zur Konfiguration finden Sie unter "Erstellen und Managen von NFS-Volumes" In der Google-Dokumentation.

NFSv3-Benutzer- und Gruppen-IDs

NFSv3-Benutzer- und Gruppen-IDs kommen über das Netzwerk als numerische IDs und nicht als Namen. Cloud Volumes Service bietet keine Nutzername-Auflösung für diese numerischen IDs mit NFSv3, mit UNIX-Sicherheitsstil-Volumes mit Just-Mode-Bits. Wenn NFSv4.1 ACLs vorhanden sind, ist eine numerische ID-Suche und/oder Suche nach Namespace erforderlich, um die ACL ordnungsgemäß zu lösen – sogar bei Verwendung von NFSv3. Bei NTFS-Volumes im Sicherheitsstil muss Cloud Volumes Service eine numerische ID einem gültigen UNIX-Benutzer auflösen und dann einem gültigen Windows-Benutzer zuordnen, um Zugriffsrechte auszuhandeln.

Sicherheitseinschränkungen von NFSv3 Benutzer- und Gruppen-IDs

Bei NFSv3 müssen Client und Server niemals bestätigen, dass der Benutzer, der einen Lese- oder Schreibversuch mit einer numerischen ID versucht, ein gültiger Benutzer ist; er ist einfach implizit vertrauenswürdig. Das öffnet das Dateisystem bis zu potenziellen Verstößen, indem es einfach eine numerische ID vortäuscht. Um Sicherheitslücken wie diese zu verhindern, gibt es einige Optionen für Cloud Volumes Service.

- Die Implementierung von Kerberos für NFS zwingt Benutzer, sich mit einem Benutzernamen und einem Kennwort oder einer Keytab-Datei zu authentifizieren, um ein Kerberos-Ticket für den Zugriff in einem Mount zu erhalten. Kerberos ist mit CVS-Performance-Instanzen und nur mit NFSv4.1 verfügbar.
- Die Einschränkung der Liste der Hosts in Ihren Exportrichtlinien beschränkt die Grenzen, die NFSv3-Clients auf das Cloud Volumes Service-Volume zugreifen können.
- Durch die Verwendung von Dual-Protokoll-Volumes und die Anwendung von NTFS-ACLs auf das Volume sind NFSv3-Clients gezwungen, numerische IDs auf gültige UNIX-Benutzernamen zu lösen, um sich für den ordnungsgemäßen Zugriff auf Mounts zu authentifizieren. Dazu muss LDAP aktiviert und UNIX-Benutzer- und Gruppenidentitäten konfiguriert werden.
- Das Squashing des Root-Benutzers begrenzt den Schaden, den ein Root-Benutzer auf einen NFS-Mount tun kann, aber das Risiko wird nicht vollständig beseitigt. Weitere Informationen finden Sie im Abschnitt „Der Root-Benutzer.“

Letztendlich ist die NFS-Sicherheit auf das beschränkt, was die Protokollversion verwendet, die Sie Angebote verwenden. NFSv3, obwohl mehr Performance im Allgemeinen als NFSv4.1, nicht dasselbe Maß an Sicherheit bietet.

NFSv4.1

NFSv4.1 bietet im Vergleich zu NFSv3 eine höhere Sicherheit und Zuverlässigkeit. Dies hat folgende Gründe:

- Integrierte Sperrung über einen Leasingbasierten Mechanismus
- Statusorientierte Sessions
- Alle NFS-Funktionen über einen einzelnen Port (2049)
- Nur TCP

- ID-Domain-Zuordnung
- Kerberos Integration (NFSv3 kann Kerberos verwenden, aber nur für NFS, nicht für zusätzliche Protokolle wie NLM)

NFSv4.1-Abhängigkeiten

Aufgrund der zusätzlichen Sicherheitsfunktionen in NFSv4.1 sind einige externe Abhängigkeiten beteiligt, die nicht für die Verwendung von NFSv3 benötigt wurden (ähnlich wie SMB Abhängigkeiten wie Active Directory erfordert).

NFSv4.1 ACLs

Cloud Volumes Service bietet Unterstützung für NFSv4.x ACLs, die bestimmte Vorteile gegenüber normalen POSIX-Berechtigungen bieten, wie z. B.:

- Granulare Steuerung des Benutzerzugriffs auf Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Bessere Interoperabilität mit CIFS/SMB
- Entfernung der NFS-Beschränkung von 16 Gruppen pro Benutzer mit AUTH_SYS-Sicherheit
- ACLs umgehen die Notwendigkeit einer Gruppen-ID-Lösung (GID), die effektiv das GID limitNFSv4.1 ACLs werden von NFS-Clients gesteuert, nicht von Cloud Volumes Service. Um NFSv4.1 ACLs zu verwenden, stellen Sie sicher, dass die Softwareversion Ihres Clients sie unterstützt und die richtigen NFS-Dienstprogramme installiert sind.

Kompatibilität zwischen NFSv4.1 ACLs und SMB-Clients

NFSv4 ACLs unterscheiden sich von Windows ACLs auf Dateiebene (NTFS ACLs), haben aber ähnliche Funktionen. In NAS-Umgebungen mit mehreren Protokollen, wenn NFSv4.1 ACLs vorhanden sind und Sie Dual-Protokoll-Zugriff verwenden (NFS und SMB auf den gleichen Datensätzen), werden Clients mit SMB2.0 und später nicht in der Lage sein, ACLs von Windows-Sicherheitregisterkarten anzuzeigen oder zu verwalten.

Funktionsweise von NFSv4.1 ACLs

Als Referenz sind folgende Begriffe definiert:

- **Access control list (ACL).** eine Liste der Berechtigungs Einträge.
- **Zugangskontrolleintrag (ACE).** Ein Berechtigungseintrag in der Liste.

Wenn ein Client während einer SETATTR-Operation eine NFSv4.1-ACL für eine Datei setzt, setzt Cloud Volumes Service diese ACL für das Objekt und ersetzt eine vorhandene ACL. Wenn es keine ACL für eine Datei gibt, werden die Modus-Berechtigungen für die Datei von EIGENTÜMER@, GROUP@ und EVERYONE@ berechnet. Wenn SUID/SGID/STICKY Bits in der Datei vorhanden sind, sind diese nicht betroffen.

Wenn ein Client während einer GETATTR Operation eine NFSv4.1 ACL für eine Datei erhält, liest Cloud Volumes Service die mit dem Objekt verknüpfte NFSv4.1 ACL, erstellt eine Liste von Aces und gibt die Liste an den Client zurück. Wenn die Datei über eine NT ACL oder Mode Bits verfügt, wird eine ACL aus Modus-Bits erstellt und an den Client zurückgegeben.

Der Zugriff wird verweigert, wenn in der ACL ein ACE VERWEIGERN vorhanden ist; der Zugriff wird gewährt, wenn ACE ZULASSEN vorhanden ist. Der Zugang wird jedoch auch verweigert, wenn keines der Asse in der ACL vorhanden ist.

Ein Sicherheitsdeskriptor besteht aus einer Sicherheits-ACL (SACL) und einer Ermessensdatei (Discretionary ACL, DACL). Bei der Ausführung von NFSv4.1 mit CIFS/SMB ist die DACL 1-to-One-Zuordnung mit NFSv4 und CIFS. Die DACL besteht aus DEM ERLAUBEN und DEN LEUGNEN Assen.

Wenn ein einfaches `chmod` Wird auf einer Datei oder einem Ordner mit NFSv4.1 ACLs gesetzt ausgeführt, bestehende Benutzer- und Gruppen-ACLs bleiben erhalten, aber der STANDARDEIGENTÜMER@, GROUP@, EVERYONE@ ACLs werden geändert.

Ein Client, der NFSv4.1 ACLs verwendet, kann ACLs für Dateien und Verzeichnisse auf dem System festlegen und anzeigen. Wenn eine neue Datei oder ein Unterverzeichnis in einem Verzeichnis erstellt wird, das über eine ACL verfügt, erbt dieses Objekt alle Asse in der ACL, die mit dem entsprechenden gekennzeichnet wurden "Ervererbungsflaggen".

Wenn eine Datei oder ein Verzeichnis über eine NFSv4.1-ACL verfügt, wird diese ACL verwendet, um den Zugriff zu steuern, unabhängig davon, welches Protokoll für den Zugriff auf die Datei oder das Verzeichnis verwendet wird.

Dateien und Verzeichnisse erben Asse von NFSv4 ACLs auf übergeordneten Verzeichnissen (möglicherweise mit entsprechenden Änderungen), solange die Asse mit den korrekten Vererbung-Flags markiert wurden.

Wenn eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anforderung erstellt wird, hängt die ACL für die resultierende Datei oder das Verzeichnis davon ab, ob die Dateierstellungsanforderung eine ACL oder nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält. Die ACL hängt auch davon ab, ob das übergeordnete Verzeichnis über eine ACL verfügt.

- Wenn die Anforderung eine ACL enthält, wird diese ACL verwendet.
- Wenn die Anforderung nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis keine ACL besitzt, wird der Client-Dateimodus verwendet, um standardmäßige UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anforderung nur Standardberechtigungen für den Zugriff auf UNIX-Dateien enthält und das übergeordnete Verzeichnis über eine nicht vererbbare ACL verfügt, wird eine Standard-ACL auf Basis der Mode-Bits, die an die Anforderung übergeben wurden, auf dem neuen Objekt festgelegt.
- Wenn die Anforderung nur Standardzugriffsberechtigungen für UNIX-Dateien enthält, aber das übergeordnete Verzeichnis über eine ACL verfügt, werden die Asse in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis geerbt, solange die Aces mit den entsprechenden Vererbung-Flags gekennzeichnet wurden.

ACE-Berechtigungen

Die Berechtigungen für NFSv4.1 ACLs verwenden eine Reihe von Groß- und Kleinbuchstaben (z. B. `rxtncy`) Um den Zugriff zu steuern. Weitere Informationen zu diesen Buchstabenwerten finden Sie unter "WIE: Verwenden Sie NFSv4 ACL".

NFSv4.1 ACL-Verhalten mit Umask und ACL-Vererbung

"NFSv4 ACLs bieten die Möglichkeit, eine ACL-Vererbung anzubieten". ACL-Vererbung bedeutet, dass Dateien oder Ordner, die unter Objekten mit NFSv4.1 ACLs-Satz erstellt wurden, die ACLs basierend auf der Konfiguration des erben können "ACL-Vererbungskennzeichnung".

"Umfragen" Wird verwendet, um die Berechtigungsstufe zu steuern, auf der Dateien und Ordner in einem Verzeichnis ohne Administratorinteraktion erstellt werden. Standardmäßig können mit Cloud Volumes Service übernommene ACLs überschrieben werden. Dies ist ein erwartetes Verhalten wie per "RFC 5661".

ACL-Formatierung

NFSv4.1 ACLs haben bestimmte Formatierung. Das folgende Beispiel ist ein ACE-Satz für eine Datei:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

Das vorangegangene Beispiel folgt den Richtlinien im ACL-Format von:

```
type:flags:principal:permissions
```

Einen Typ von `A` Bedeutet „Zulassen“. Die Erben-Flags werden in diesem Fall nicht festgelegt, da der Principal keine Gruppe ist und keine Vererbung beinhaltet. Da es sich bei ACE nicht um EINEN AUDIT-Eintrag handelt, müssen die Audit-Flags nicht festgelegt werden. Weitere Informationen zu NFSv4.1 ACLs finden Sie unter "http://linux.die.net/man/5/nfs4_acl".

Wenn die NFSv4.1 ACL nicht richtig eingestellt ist (oder eine Namenszeichenfolge nicht vom Client und Server aufgelöst werden kann), verhält sich die ACL möglicherweise nicht wie erwartet. Andernfalls kann die ACL-Änderung nicht angewendet werden und einen Fehler verursacht.

Beispielfehler sind:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

Explizites ABLEHNEN

Die Berechtigungen in NFSv4.1 können explizite DENY-Attribute für EIGENTÜMER, GRUPPE und ALLE enthalten. Das liegt daran, dass NFSv4.1 ACLs Standard-Deny sind. Dies bedeutet, dass, wenn eine ACL nicht ausdrücklich von einem ACE gewährt wird, sie verweigert wird. Explizite DENY-Attribute überschreiben alle ZUGRIFFSOPTIONEN, explizit oder nicht.

DENY Aces werden mit einem Attribut-Tag von festgelegt `D`.

Im folgenden Beispiel ist DER GRUPPE@ alle Lese- und Ausführungsberechtigungen erlaubt, aber der gesamte Schreibzugriff wird verweigert.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENY Aces sollten möglichst vermieden werden, da sie verwirrend und kompliziert sein können; ACLS, die

nicht explizit definiert sind, WERDEN implizit verweigert. Wenn Asse VERWEIGERN festgelegt sind, wird Benutzern möglicherweise der Zugriff verweigert, wenn sie erwarten, dass ihnen Zugriff gewährt wird.

Der vorhergehende Satz von Assen entspricht 755 im Modus Bits, was bedeutet:

- Der Eigentümer hat volle Rechte.
- Gruppen haben schreibgeschützt.
- Andere haben nur gelesen.

Selbst wenn die Berechtigungen auf das Äquivalent von 775 angepasst werden, kann der Zugriff aufgrund der expliziten DENY-Einstellung für ALLE verweigert werden.

Abhängigkeiten für die Zuordnung der NFSv4.1 ID-Domäne

NFSv4.1 nutzt die ID-Domain-Mapping-Logik als Sicherheitsschicht, um zu überprüfen, ob ein Benutzer, der auf einen NFSv4.1-Mount zugreifen möchte, tatsächlich derjenige ist, der behauptet. In diesen Fällen hängt der vom NFSv4.1-Client stammende Benutzername und Gruppenname eine Namenszeichenfolge an und sendet sie an die Cloud Volumes Service-Instanz. Wenn diese Kombination aus Benutzername/Gruppenname und ID-Zeichenfolge nicht übereinstimmt, dann wird der Benutzer und/oder die Gruppe auf den Standard-niemand-Benutzer gesetzt, der im angegeben wurde `/etc/idmapd.conf` Datei auf dem Client.

Diese ID-Zeichenfolge ist eine Voraussetzung für die ordnungsgemäße Einhaltung von Berechtigungen, insbesondere wenn NFSv4.1 ACLs und/oder Kerberos verwendet werden. Daher sind Serverabhängigkeiten des Nameservice wie LDAP-Server erforderlich, um die Konsistenz zwischen Clients und Cloud Volumes Service für eine ordnungsgemäße Identitätsauflösung von Benutzer und Gruppennamen zu gewährleisten.

Cloud Volumes Service verwendet einen statischen Standard-ID-Domänennamen von `defaultv4iddomain.com`. NFS-Clients verwenden standardmäßig den DNS-Domain-Namen für seine ID-Domain-Namen-Einstellungen. Sie können den ID-Domain-Namen in jedoch manuell anpassen `/etc/idmapd.conf`.

Wenn LDAP in Cloud Volumes Service aktiviert ist, dann Cloud Volumes Service automatisiert die NFS ID Domain zu ändern, was für die Suche Domain in DNS konfiguriert ist und Clients nicht geändert werden müssen, es sei denn sie verwenden unterschiedliche DNS Domain Suchnamen.

Wenn Cloud Volumes Service einen Benutzernamen oder Gruppennamen in lokalen Dateien oder LDAP auflösen kann, wird die Domänenzeichenfolge verwendet und nicht übereinstimmende Domänen-IDs Squash an niemand. Wenn Cloud Volumes Service einen Benutzernamen oder Gruppennamen nicht in lokalen Dateien oder LDAP finden kann, wird der numerische ID-Wert verwendet, und der NFS-Client löst den Namen richtig aus (dies entspricht dem NFSv3-Verhalten).

Ohne die NFSv4.1 ID-Domäne des Clients zu ändern, um mit dem zu übereinstimmen, was der Cloud Volumes Service-Datenträger verwendet, sehen Sie folgendes Verhalten:

- UNIX-Benutzer und -Gruppen mit lokalen Einträgen in Cloud Volumes Service (wie root, wie in lokalen UNIX-Benutzern und -Gruppen definiert) werden auf den nobody-Wert gequetscht.
- UNIX-Benutzer und -Gruppen mit Einträgen in LDAP (wenn Cloud Volumes Service so konfiguriert ist, dass sie LDAP verwenden), nehmen keine Wimpern auf, wenn sich DNS-Domänen zwischen NFS-Clients und Cloud Volumes Service unterscheiden.
- UNIX-Benutzer und -Gruppen ohne lokale Einträge oder LDAP-Einträge verwenden den numerischen ID-Wert und lösen den auf dem NFS-Client angegebenen Namen. Wenn auf dem Client kein Name vorhanden ist, wird nur die numerische ID angezeigt.

Die Ergebnisse des vorhergehenden Szenarios:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Wenn die Client- und Server-ID-Domänen übereinstimmen, wird die gleiche Dateiliste angezeigt:

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Weitere Informationen zu diesem Thema und wie man es löst, finden Sie im Abschnitt „NFSv4.1 und der niemand-Benutzer/Gruppe.“

Kerberos Abhängigkeiten

Wenn Sie Kerberos mit NFS verwenden möchten, müssen Sie für Cloud Volumes Service Folgendes haben:

- Active Directory-Domäne für Kerberos-Verteilzentrum-Dienste (KDC)
- Active Directory-Domäne mit Benutzer- und Gruppenattributen, die mit UNIX-Informationen für LDAP-Funktionalität gefüllt sind (NFS-Kerberos im Cloud Volumes Service benötigt für die ordnungsgemäße Funktion einen Benutzer-SPN für UNIX-Benutzerzuordnung).
- LDAP auf der Cloud Volumes Service-Instanz aktiviert
- Active Directory-Domäne für DNS-Services

NFSv4.1 und der niemand-Benutzer/Gruppe

Eines der häufigsten Probleme bei einer NFSv4.1-Konfiguration ist, wenn eine Datei oder ein Ordner in einer Auflistung mit angezeigt wird `ls` Als im Besitz des `user:group` Kombination von `nobody:nobody`.

Beispiel:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

Und die numerische ID lautet `99`.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

In manchen Fällen wird die Datei möglicherweise den korrekten Eigentümer, aber angezeigt `nobody` Als Gruppe.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

Wer ist niemand?

Der `nobody` Benutzer in NFSv4.1 unterscheidet sich von dem `nfsnobody` Benutzer: Sie können anzeigen, wie ein NFS Client jeden Benutzer sieht, indem Sie die ausführen `id` Befehl:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Mit NFSv4.1, das `nobody` Der von definierte Standardbenutzer ist der Benutzer `idmapd.conf` Datei und kann als jeder Benutzer definiert werden, den Sie verwenden möchten.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Warum passiert das?

Da Sicherheit durch Namenszeichenzuordnung ein Schlüsseltenet von NFSv4.1-Operationen ist, ist das Standardverhalten, wenn eine Namenszeichenfolge nicht richtig übereinstimmt, dass der Benutzer zu einem Squash, der normalerweise keinen Zugriff auf Dateien und Ordner hat, die Benutzer und Gruppen gehören.

Wenn Sie sehen `nobody` Für den Benutzer und/oder die Gruppe in Dateilisten bedeutet dies im Allgemeinen, dass etwas in NFSv4.1 falsch konfiguriert ist. Hier kann die Empfindlichkeit des Falles ins Spiel kommen.

Wenn z. B. user1@CVSDEMO.LOCAL (uid 1234, gid 1234) auf einen Export zugreift, muss Cloud Volumes Service user1@CVSDEMO.LOCAL (uid 1234, gid 1234) finden können. Wenn der Benutzer in Cloud Volumes Service ist USER1@CVSDEMO.LOCAL, dann wird es nicht übereinstimmen (GROSSUSER1 vs. Kleinbuchstaben user1). In vielen Fällen können Sie Folgendes in der Meldungsdatei auf dem Client sehen:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

Der Client und Server müssen beide zustimmen, dass ein Benutzer tatsächlich der Meinung ist, dass er sein soll. Sie müssen daher Folgendes überprüfen, um sicherzustellen, dass der Benutzer, der den Client sieht, dieselben Informationen hat wie der Benutzer, den Cloud Volumes Service sieht.

- **NFSv4.x ID Domain.** Client: `idmapd.conf` Datei; Cloud Volumes Service verwendet `defaultv4iddomain.com` Und kann nicht manuell geändert werden. Bei Verwendung von LDAP mit NFSv4.1 ändert Cloud Volumes Service die ID-Domäne in das, was die DNS-Suchdomäne verwendet, was mit der AD-Domäne identisch ist.
- **Benutzername und numerische IDs.** Dies legt fest, wo der Client nach Benutzernamen sucht und die Namensdienstschalter-Konfiguration nutzt – Client: `nsswitch.conf` Und/oder lokale Passwd- und Gruppendateien; Cloud Volumes Service erlaubt keine Änderungen, sondern fügt der Konfiguration automatisch LDAP hinzu, wenn sie aktiviert ist.
- **Gruppenname und numerische IDs.** Dies legt fest, wo der Client nach Gruppennamen sucht und nutzt die Namensdienst-Switch-Konfiguration – Client: `nsswitch.conf` Und/oder lokale Passwd- und Gruppendateien; Cloud Volumes Service erlaubt keine Änderungen, sondern fügt der Konfiguration automatisch LDAP hinzu, wenn sie aktiviert ist.

In fast allen Fällen, wenn Sie sehen `nobody` Bei Benutzer- und Gruppenlisten von Clients handelt es sich um das Problem der Übersetzung von Benutzer- oder Gruppennamen-Domänen-ID zwischen Cloud Volumes Service und dem NFS-Client. Um dieses Szenario zu vermeiden, verwenden Sie LDAP, um Benutzer- und Gruppeninformationen zwischen Clients und Cloud Volumes Service aufzulösen.

Anzeigen von Name-ID-Strings für NFSv4.1 auf Clients

Wenn Sie NFSv4.1 verwenden, gibt es ein Name-String-Mapping, das während NFS-Vorgängen stattfindet, wie zuvor beschrieben.

Zusätzlich zu verwenden `/var/log/messages` Um ein Problem mit NFSv4-IDs zu finden, können Sie das verwenden "Nfsidmap -l" Befehl auf dem NFS Client, um anzuzeigen, welche Benutzernamen der NFSv4-Domäne ordnungsgemäß zugeordnet haben.

Dies wird beispielsweise nach einem Benutzer ausgegeben, der vom Client gefunden werden kann und Cloud Volumes Service auf einen NFSv4.x Mount zugreift:

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Wenn ein Benutzer, der der NFSv4.1 ID-Domäne nicht ordnungsgemäß zugeordnet ist (in diesem Fall `netapp-user`) Versucht, auf denselben Mount zuzugreifen und berührt eine Datei, sie sind zugewiesen

`nobody:nobody`, Wie erwartet.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

Der `nfsidmap -l` Ausgabe zeigt den Benutzer an `pcuser` Im Display, aber nicht `netapp-user`; Dies ist der anonyme Benutzer in unserer Export-Policy Regel (`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

SMB

"SMB" Das von Microsoft entwickelte Netzwerk-File-Sharing-Protokoll bietet zentralisierte Benutzer-/Gruppenauthentifizierung, Berechtigungen, Sperren und Dateifreigabe für mehrere SMB-Clients über ein Ethernet-Netzwerk. Dateien und Ordner werden Clients über Freigaben angezeigt, die mit einer Vielzahl von Freigabeeigenschaften konfiguriert werden können und die Zugriffskontrolle über Berechtigungen auf Share-Ebene bietet. SMB kann jedem Client angezeigt werden, der Protokolle unterstützt, einschließlich Windows-, Apple- und Linux-Clients.

Cloud Volumes Service unterstützt die Protokollversionen SMB 2.1 und 3.x.

Zugriffssteuerung/SMB-Freigaben

- Wenn ein Windows-Benutzername Zugriff auf das Cloud Volumes Service-Volume anfordert, sucht Cloud Volumes Service nach einem UNIX-Benutzernamen mit den von Cloud Volumes Service-Administratoren konfigurierten Methoden.

- Wenn ein externer UNIX Identity Provider (LDAP) konfiguriert ist und Windows/UNIX Nutzernamen identisch sind, werden Windows-Benutzernamen ohne zusätzliche Konfiguration 1:1 zu UNIX Benutzernamen mappen. Wenn LDAP aktiviert ist, wird Active Directory verwendet, um die UNIX-Attribute für Benutzer- und Gruppenobjekte zu hosten.
- Wenn Windows-Namen und UNIX-Namen nicht identisch sind, muss LDAP konfiguriert werden, damit Cloud Volumes Service die LDAP-Namenszuordnungskonfiguration verwenden kann (siehe Abschnitt "„LDAP für asymmetrisches Namenszuordnungen verwenden“").
- Wenn LDAP nicht verwendet wird, werden Windows SMB-Benutzer einem lokalen UNIX-Standardbenutzer zugeordnet `pcuser` Im Cloud Volumes Service. Das bedeutet Dateien, die von Benutzern in Windows geschrieben wurden, die dem zugeordnet sind `pcuser` Zeigen Sie die UNIX-Eigentümerschaft als `pcuser` In NAS-Umgebungen mit mehreren Protokollen. `pcuser` Hier ist effektiv das `nobody` Benutzer in Linux-Umgebungen (UID 65534).

Bei Implementierungen nur mit SMB gilt das `pcuser` Mapping tritt immer noch auf, aber es wird keine Rolle spielen, weil Windows-Benutzer und Gruppen-Eigentum korrekt angezeigt wird und NFS-Zugriff auf das SMB-only Volumen ist nicht erlaubt. Außerdem unterstützen SMB-only Volumes nach der Erstellung keine Konvertierung in NFS- oder Dual-Protokoll-Volumes.

Windows nutzt Kerberos für die Benutzerauthentifizierung mit den Active Directory-Domänencontrollern, die einen Austausch von Benutzername/Passwort mit den AD-DCs erfordern, die sich außerhalb der Cloud Volumes Service-Instanz befinden. Kerberos-Authentifizierung wird verwendet, wenn das verwendet wird `\\SERVERNAME` UNC-Pfad wird von den SMB-Clients verwendet, und folgende lautet „true“:

- DNS A/AAAA-Eintrag für SERVERNAME vorhanden
- Für SERVERNAME ist ein gültiger SPN für SMB/CIFS-Zugriff vorhanden

Wenn ein Cloud Volumes Service SMB Volume erstellt wird, wird der Name des Maschinenkontos wie in Abschnitt definiert erstellt "„Wie Cloud Volumes Service in Active Directory erscheint.“" Der Name des Computerkontos wird auch zum SMB-Freigabepfad, da Cloud Volumes Service dynamische DNS (DDNS) verwendet, um die erforderlichen A/AAAA- und PTR-Einträge im DNS und die erforderlichen SPN-Einträge auf dem Computerkonto-Principal zu erstellen.

Damit PTR-Einträge erstellt werden können, muss auf dem DNS-Server die Reverse-Lookup-Zone für die IP-Adresse der Cloud Volumes Service-Instanz vorhanden sein.

Beispielsweise verwendet dieses Cloud Volumes Service Volume den folgenden UNC-Freigabepfad: `\\cvs-east- 433d.cvsdemo.local`.

Im Active Directory sind dies die von Cloud Volumes Service generierten SPN-Einträge:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Dies ist das Ergebnis des DNS-Vorwärts-/Reverse-Lookups:

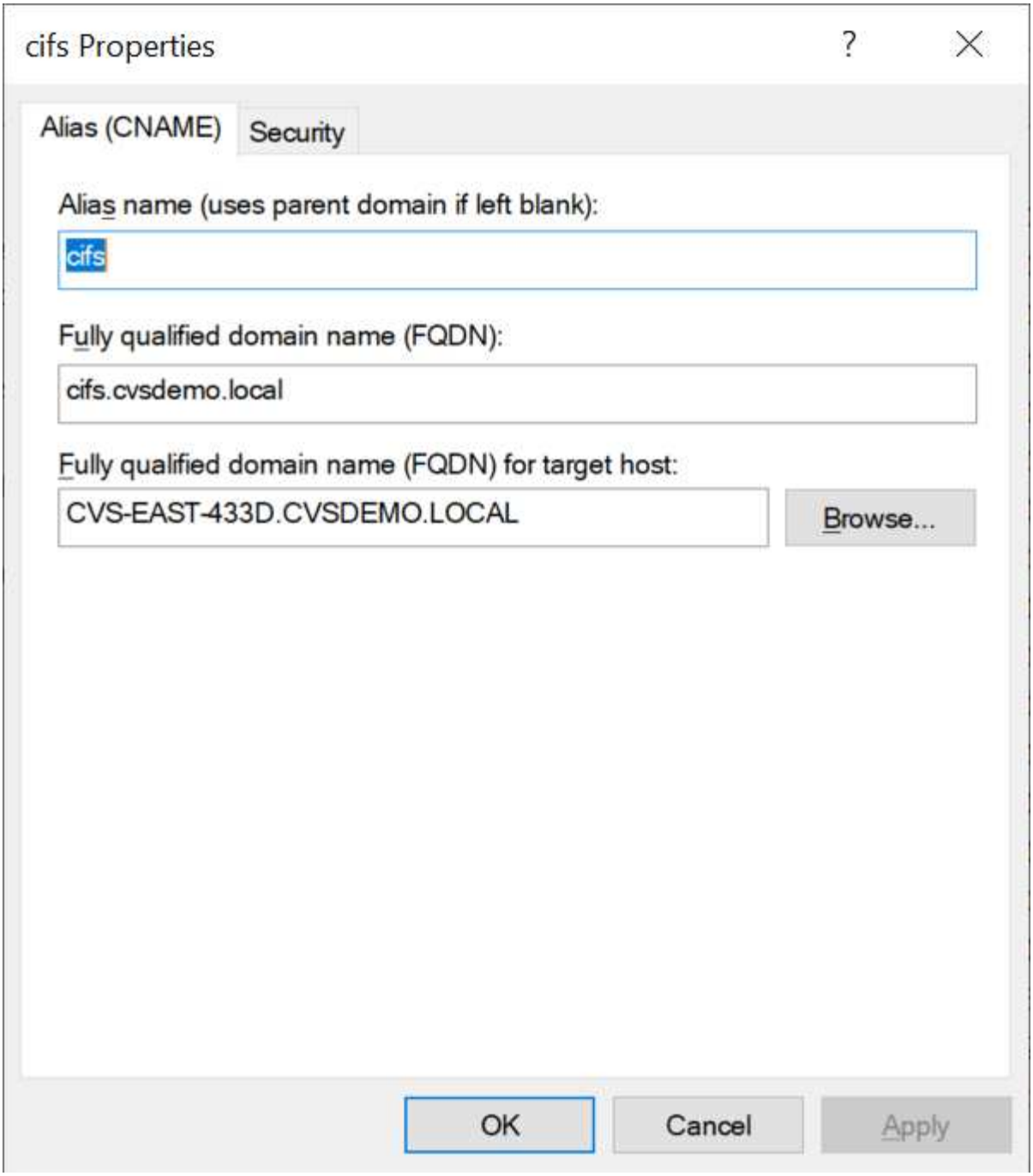
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Optional kann eine bessere Zugriffssteuerung durch Aktivieren/Aktivieren der SMB-Verschlüsselung für SMB-Freigaben in Cloud Volumes Service angewendet werden. Wenn die SMB-Verschlüsselung von einem der Endpunkte nicht unterstützt wird, ist der Zugriff nicht zulässig.

Verwenden von SMB-Namenaliasen

In einigen Fällen kann es ein Sicherheitsbedenken für Endbenutzer sein, den Namen des für Cloud Volumes Service verwendeten Computerkontos zu kennen. In anderen Fällen möchten Sie Ihren Endbenutzern möglicherweise lediglich einen einfacheren Zugriffspfad bieten. In diesen Fällen können Sie SMB-Aliase erstellen.

Wenn Sie Aliase für den SMB-Freigabepfad erstellen möchten, können Sie den Namen CNAME-Datensatz in DNS verwenden. Beispiel: Wenn Sie den Namen verwenden möchten `\\CIFS` Auf Freigaben statt auf `\\cvs-east- 433d.cvsdemo.local`, Aber Sie möchten immer noch Kerberos-Authentifizierung verwenden, ein CNAME in DNS, der auf den vorhandenen A/AAAA-Datensatz verweist, und ein zusätzlicher SPN, der dem bestehenden Computerkonto hinzugefügt wurde, bietet Kerberos-Zugriff.



Dies ist das resultierende DNS-Weitersuchergebnis nach dem Hinzufügen eines CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Dies ist die resultierende SPN-Abfrage nach dem Hinzufügen neuer SPNs:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

In einer Paketerfassung können wir die Session-Setup-Anforderung mit dem SPN sehen, der an den CNAME gebunden ist.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

SMB-Authentifizierungsdialekte

Cloud Volumes Service unterstützt Folgendes "Dialekte" Für SMB-Authentifizierung:

- LM
- NTLM
- NTLMv2
- Kerberos

Kerberos-Authentifizierung für SMB-Freigabe-Zugriff ist die sicherste Authentifizierungsstufe, die Sie verwenden können. Mit AES- und SMB-Verschlüsselung wird die Sicherheit weiter erhöht.

Cloud Volumes Service unterstützt außerdem die Rückwärtskompatibilität für die LM- und NTLM-Authentifizierung. Wenn Kerberos falsch konfiguriert ist (z. B. beim Erstellen von SMB-Aliasen), geht der Zugriff auf Shares auf schwächere Authentifizierungsmethoden zurück (z. B. NTLMv2). Da diese Mechanismen weniger sicher sind, sind sie in einigen Active Directory-Umgebungen deaktiviert. Wenn schwächere Authentifizierungsmethoden deaktiviert sind und Kerberos nicht richtig konfiguriert ist, schlägt der Zugriff auf die Freigabe fehl, da keine gültige Authentifizierungsmethode vorhanden ist, auf die Sie zurückgreifen können.

Informationen zum Konfigurieren/Anzeigen der unterstützten Authentifizierungsstufen in Active Directory finden Sie unter "Netzwerksicherheit: Authentifizierungsebene des LAN Managers".

Berechtigungsmodelle

NTFS/Dateiberechtigungen

NTFS-Berechtigungen sind die Berechtigungen, die auf Dateien und Ordner in Dateisystemen angewendet werden, die der NTFS-Logik entsprechen. Sie können NTFS-Berechtigungen in anwenden `Basic` Oder `Advanced` Und kann auf festgelegt werden `Allow` Oder `Deny` Für die Zugriffssteuerung.

Grundlegende Berechtigungen beinhalten Folgendes:

- Volle Kontrolle
- Ändern
- Lesen Und Ausführen
- Lesen
- Schreiben

Wenn Sie Berechtigungen für einen Benutzer oder eine Gruppe festlegen, die als ACE bezeichnet wird, befindet sie sich in einer ACL. NTFS-Berechtigungen verwenden die gleichen Grundlagen zum Lesen/Schreiben/Ausführen wie UNIX-Mode-Bits, können aber auch auf granularere und erweiterte Zugriffskontrollen (auch bekannt als Spezialberechtigungen), wie zum Beispiel Besitzrechte übernehmen, Ordner erstellen/Daten anhängen, Attribute schreiben usw. erweitern.

Bits des Standard-UNIX-Modus bieten nicht dieselbe Granularität wie NTFS-Berechtigungen (beispielsweise die Möglichkeit, Berechtigungen für einzelne Benutzer und Gruppenobjekte in einer ACL festzulegen oder erweiterte Attribute festzulegen). NFSv4.1 ACLs bieten jedoch dieselben Funktionen wie NTFS ACLs.

NTFS-Berechtigungen sind spezifischer als Freigabeberechtigungen und können in Verbindung mit Freigabeberechtigungen verwendet werden. Bei NTFS-Berechtigungsstrukturen gilt die restriktivere Vorgehensweise. Als solche überschreibt explizite Denals für einen Benutzer oder eine Gruppe sogar die volle Kontrolle, wenn die Zugriffsrechte definiert werden.

NTFS-Berechtigungen werden von Windows SMB Clients gesteuert.

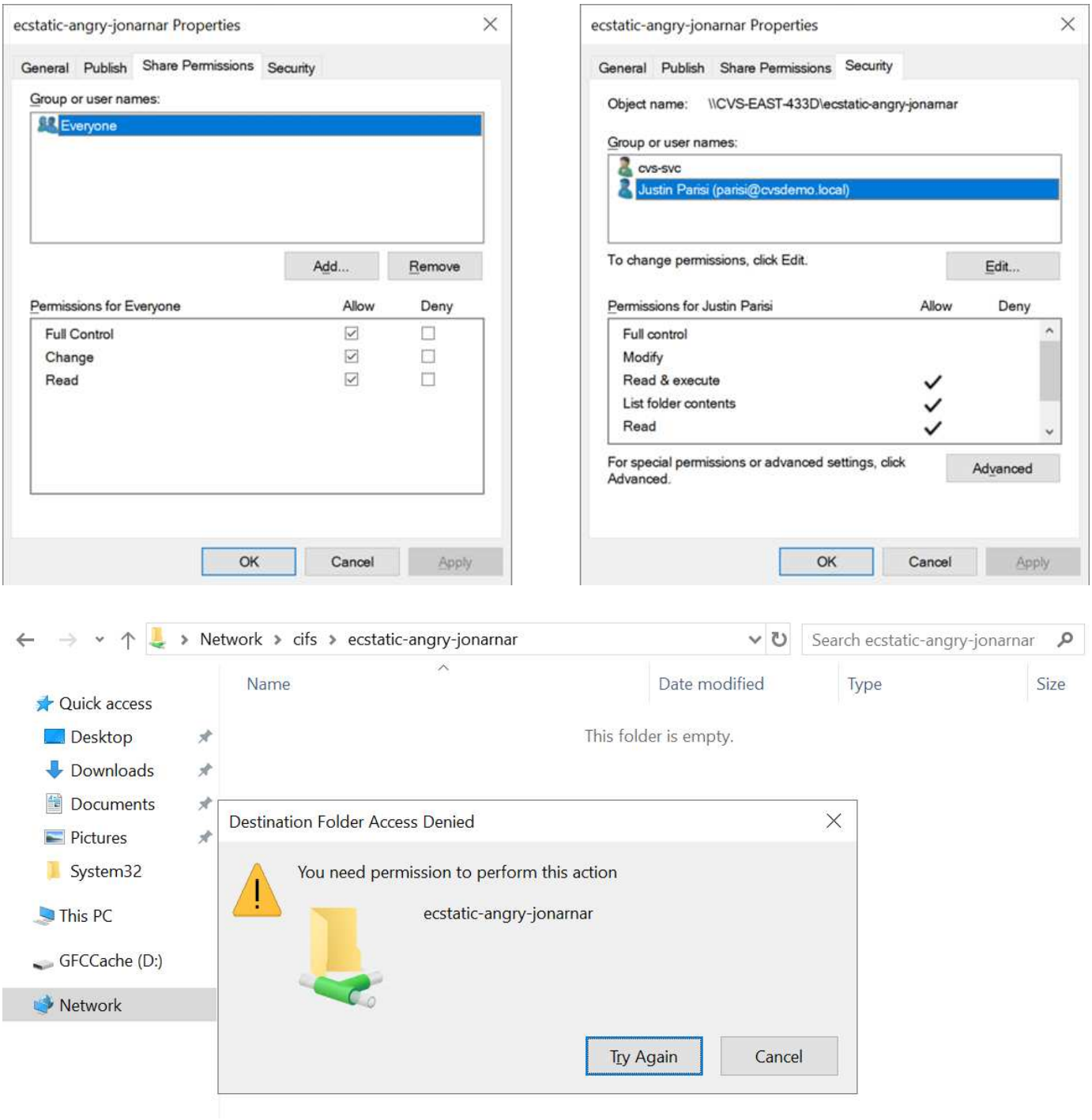
Freigabeberechtigungen

Freigabeberechtigungen sind allgemeiner als NTFS-Berechtigungen (nur Lesen/Ändern/Vollzugriff) und steuern den anfänglichen Eintrag in eine SMB-Freigabe – ähnlich wie die NFS-Exportrichtlinien funktionieren.

Obwohl die NFS-Exportrichtlinien den Zugriff über hostbasierte Informationen wie IP-Adressen oder Hostnamen steuern, können SMB-Freigabe-Berechtigungen den Zugriff über Benutzer- und Gruppennamen in einer Share-ACL steuern. Sie können die Share ACLs entweder über den Windows Client oder über die Cloud Volumes Service Management UI festlegen.

Standardmäßig enthalten alle ACLs und Initial Volume ACLs mit vollständiger Kontrolle. Die Datei ACLs sollten geändert werden, aber Freigabeberechtigungen werden durch die Dateiberechtigungen für Objekte in der Freigabe überbeherrscht.

Wenn ein Benutzer beispielsweise nur Lesezugriff auf die Cloud Volumes Service Volume-Datei-ACL hat, wird ihm der Zugriff auf die Erstellung von Dateien und Ordnern verweigert, obwohl die share ACL für alle mit Full Control eingestellt ist, wie in der folgenden Abbildung dargestellt.



Gehen Sie wie folgt vor, um die besten Sicherheitsergebnisse zu erzielen:

- Entfernen Sie alle aus den Freigabe- und Datei-ACLs und legen Sie stattdessen den Freigaberzugriff für Benutzer oder Gruppen fest.
- Verwenden Sie Gruppen zur Zugriffssteuerung anstelle einzelner Benutzer, um das Management zu vereinfachen und das Entfernen bzw. Hinzufügen von Benutzern zu beschleunigen, um ACLs über das Gruppenmanagement zu teilen.
- Weniger restriktiver, allgemeiner Zugriff auf die Asse auf den Freigabeberechtigungen und Sperrung des Zugriffs auf Benutzer und Gruppen mit Dateiberechtigungen für eine granularere Zugriffskontrolle.
- Die allgemeine Verwendung von expliziten Ablehnen von ACLs vermeiden, da sie ACLs außer Kraft setzen. Beschränken Sie die Verwendung expliziter Ablehnen von ACLs für Benutzer oder Gruppen, die

schnell vom Zugriff auf ein Dateisystem eingeschränkt werden müssen.

- Achten Sie darauf, dass Sie auf die achten "ACL-Vererbung" Einstellungen beim Ändern von Berechtigungen; das Festlegen des Vererbungsfahs auf der obersten Ebene eines Verzeichnisses oder Volumes mit hoher Dateianzahl bedeutet, dass jede Datei unter diesem Verzeichnis oder Volume über geerbte Berechtigungen verfügt, die ihr hinzugefügt wurden. Dies kann unerwünschte Verhaltensweisen wie unbeabsichtigten Zugriff/Denial-of-DoS und lange Abgänge von Berechtigungsänderungen verursachen, wenn jede Datei angepasst wird.

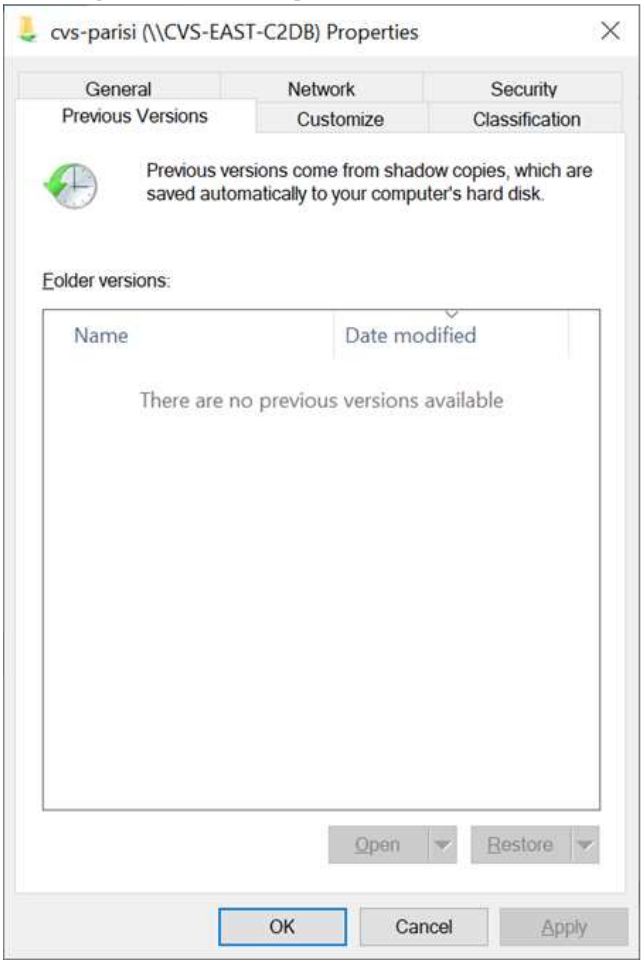
Sicherheitsfunktionen für die SMB-Freigabe

Wenn Sie zum ersten Mal ein Volume mit SMB-Zugriff in Cloud Volumes Service erstellen, erhalten Sie eine Reihe von Optionen zum Sichern des Volumes.

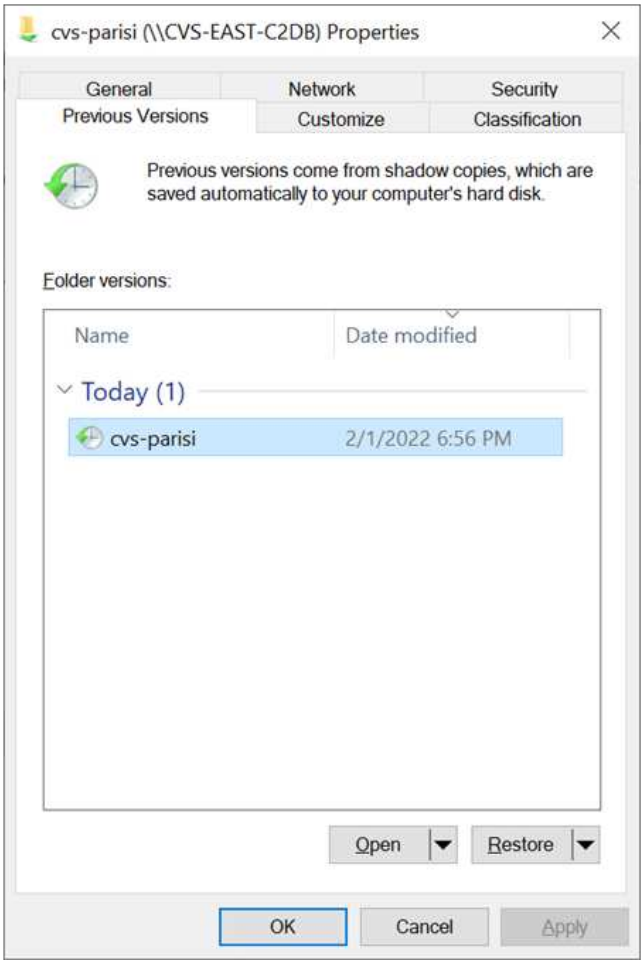
Einige dieser Optionen hängen von der Cloud Volumes Service-Ebene (Leistung oder Software) ab und stehen zur Auswahl:

- **Snapshot-Verzeichnis sichtbar machen (sowohl für CVS-Performance als auch für CVS-SW verfügbar).** mit dieser Option lässt sich kontrollieren, ob SMB-Clients in einem SMB-Share auf das Snapshot-Verzeichnis zugreifen können (`\\server\share\~snapshot` Und/oder Registerkarte frühere Versionen). Die Standardeinstellung ist nicht aktiviert, was bedeutet, dass das Volume standardmäßig den Zugriff auf das ausgeblendet und deaktiviert `~snapshot` Verzeichnis, und es werden keine Snapshot-Kopien auf der Registerkarte Vorherige Versionen des Volumes angezeigt.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Das Ausblenden von Snapshot Kopien vor Endbenutzern kann aus Sicherheitsgründen oder aus Performance-

Gründen (Ausblenden dieser Ordner vor AV-Scans) oder unter Voreinstellung gewünscht werden. Cloud Volumes Service Snapshots sind schreibgeschützt, d. h. selbst wenn diese Snapshots sichtbar sind, können Endanwender Dateien im Snapshot Verzeichnis nicht löschen oder ändern. Dateiberechtigungen auf die Dateien oder Ordner beim Erstellen der Snapshot Kopie. Wenn sich die Berechtigungen einer Datei oder eines Ordners zwischen Snapshot Kopien ändern, gelten die Änderungen auch für die Dateien oder Ordner im Snapshot Verzeichnis. Benutzer und Gruppen können auf Basis von Berechtigungen auf diese Dateien oder Ordner zugreifen. Das Löschen oder Modifizierungen von Dateien im Snapshot Verzeichnis ist zwar nicht möglich, aber es ist möglich, Dateien oder Ordner aus dem Snapshot Verzeichnis zu kopieren.

- **SMB-Verschlüsselung aktivieren (sowohl für CVS-Performance als auch für CVS-SW verfügbar).** SMB-Verschlüsselung ist auf der SMB-Freigabe standardmäßig deaktiviert (deaktiviert). Wenn Sie das Kontrollkästchen aktiviert SMB-Verschlüsselung aktivieren, bedeutet dies, dass der Datenverkehr zwischen dem SMB-Client und dem -Server im laufenden Vorgang verschlüsselt wird, wobei die am höchsten unterstützten Verschlüsselungsstufen ausgehandelt werden. Cloud Volumes Service unterstützt bis zu AES-256-Verschlüsselung für SMB. Durch die Aktivierung der SMB-Verschlüsselung kommen Performance-Einbußen mit sich, die für Ihre SMB-Clients möglicherweise nicht spürbar sind – in etwa im Bereich von 10 bis 20 %. NetApp empfiehlt Tests nachdrücklich, um zu prüfen, ob diese Performance-Einbußen akzeptabel sind.
- **SMB-Share ausblenden (verfügbar sowohl für CVS-Performance als auch CVS-SW).** durch diese Option wird der SMB-Share-Pfad vom normalen Browsing ausgeblendet. Das bedeutet, dass Clients, die den Freigabepfad nicht kennen, die Freigaben beim Zugriff auf den Standard-UNC-Pfad nicht sehen können (z. B. `\\CVS-SMB`). Wenn das Kontrollkästchen aktiviert ist, können nur Clients darauf zugreifen, die den SMB-Freigabepfad explizit kennen oder über den von einem Gruppenrichtlinienobjekt definierten Freigabepfad verfügen (Sicherheit durch Obfuscation).
- **Access-Based Enumeration (ABE) aktivieren (nur CVS-SW).** Dies ähnelt dem Ausblenden der SMB-Freigabe, außer die Freigaben oder Dateien sind nur Benutzern oder Gruppen verborgen, die keine Berechtigung zum Zugriff auf die Objekte haben. Beispiel: Wenn Windows-Benutzer `joe` Ist mindestens nicht erlaubt Lese-Zugriff durch die Berechtigungen, dann der Windows-Benutzer `joe` SMB-Freigabe oder Dateien können überhaupt nicht angezeigt werden. Dies ist standardmäßig deaktiviert und Sie können sie durch Aktivieren des Kästchens aktivieren. Weitere Informationen zu ABE finden Sie im NetApp Knowledge Base-Artikel "Wie funktioniert Access Based Enumeration (ABE)?"
- **Kontinuierliche verfügbare (CA) Freigabesupport aktivieren (nur CVS-Performance).** "Kontinuierlich verfügbare SMB-Freigaben" Bietet eine Möglichkeit, Applikationsunterbrechungen bei Failover-Ereignissen zu minimieren, indem Sperrstatus über Nodes im Cloud Volumes Service-Back-End-System hinweg repliziert werden. Dies ist keine Sicherheitsfunktion, bietet aber insgesamt eine höhere Ausfallsicherheit. Derzeit werden nur SQL Server- und FSLogix-Anwendungen unterstützt.

Ausgeblendete Standardfreigaben

Wenn in Cloud Volumes Service ein SMB Server erstellt wird, gibt es diese "Versteckte administrative Freigaben" (Unter Verwendung der Namenskonvention für USD), die zusätzlich zum SMB-Share des Daten-Volumes erstellt werden. Dazu gehören C€ (Namespace Access) und IPC€ (gemeinsame Nutzung von benannten Rohren für die Kommunikation zwischen Programmen, wie z. B. die Remote Procedure Calls (RPC), die für den Zugriff auf die Microsoft Management Console (MMC) verwendet werden).

Die IPC-USD-Freigabe enthält keine Share-ACLs und kann nicht geändert werden – sie wird streng für RPC-Aufrufe und verwendet "Windows deaktiviert standardmäßig den anonymen Zugriff auf diese Freigaben".

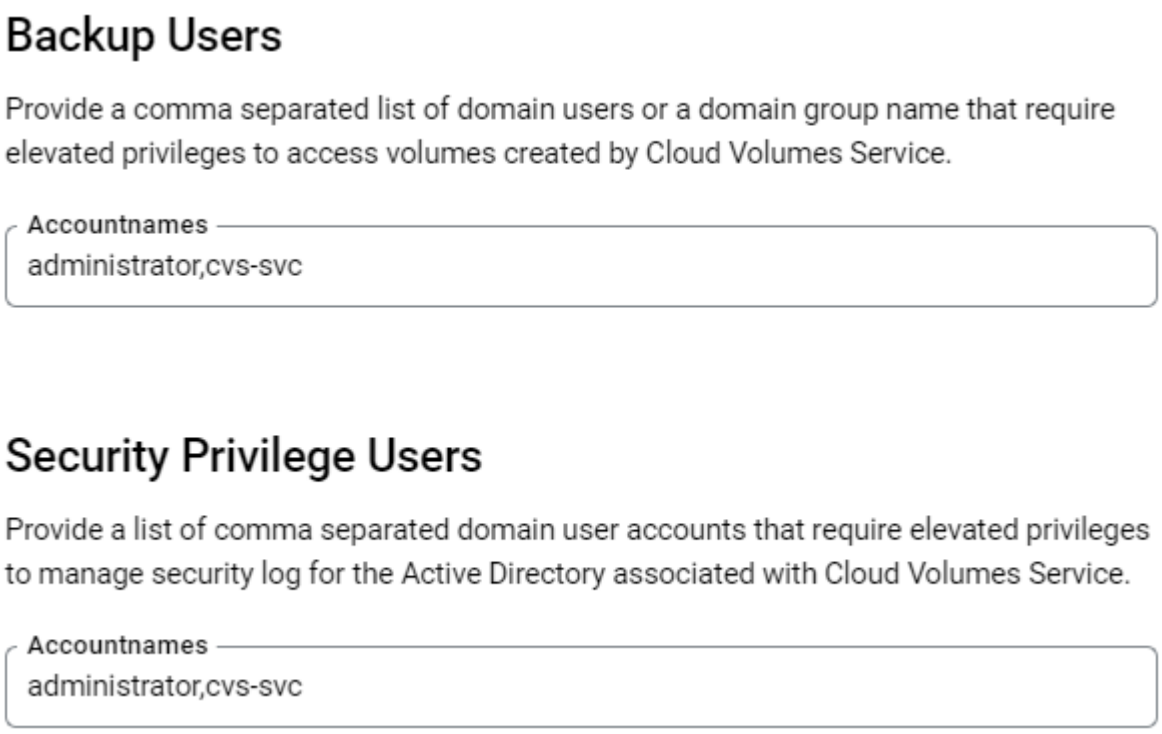
Der Wert-Anteil ermöglicht standardmäßig den Zugriff von BUILTIN/Administratoren, aber die Cloud Volumes Service-Automatisierung entfernt das Share-ACL und erlaubt keinen Zugriff auf jemanden, da der Zugriff auf die C€-Aktie eine Übersicht über alle gemounteten Volumes in den Cloud Volumes Service-Dateisystemen ermöglicht. Daher wird versucht, zu navigieren `\\SERVER\C$` Fehler.

Konten mit lokalen/BUILTIN-Administrator/Backup-Rechten

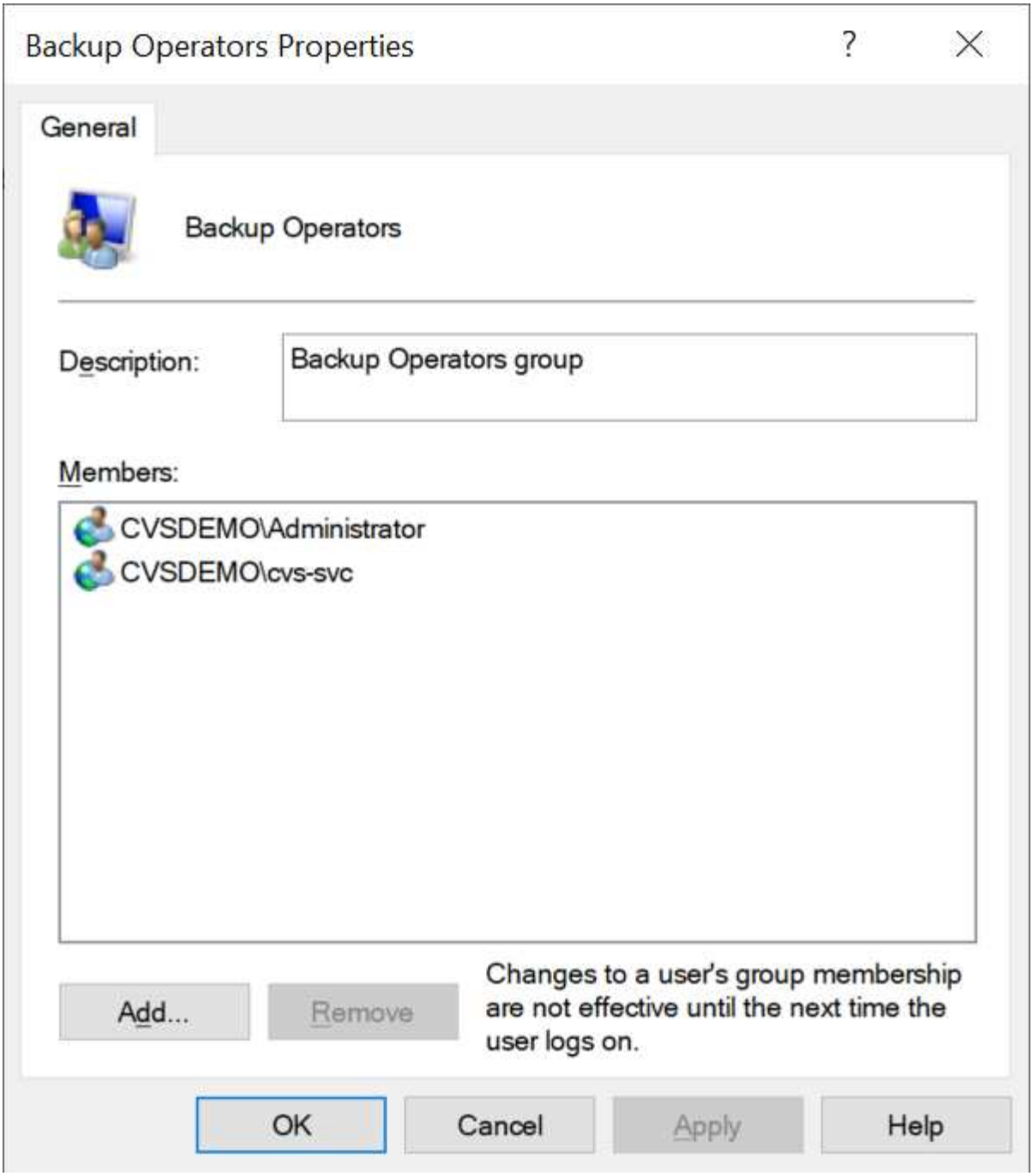
Cloud Volumes Service SMB-Server verfügen über ähnliche Funktionen wie normale Windows SMB-Server, da lokale Gruppen (z. B. BUILTIN\-Administratoren) Zugriffsrechte für ausgewählte Domänenbenutzer und -Gruppen anwenden.

Wenn Sie einen Benutzer angeben, der zu Backup-Benutzern hinzugefügt werden soll, wird der Benutzer der Gruppe BUILTIN\Backup Operators in der Cloud Volumes Service-Instanz hinzugefügt, die diese Active Directory-Verbindung verwendet, die dann den ruft "SeBackupPrivilege und SeRestorePrivilege".

Wenn Sie Benutzern von Sicherheitsberechtigungen einen Benutzer hinzufügen, erhält der Benutzer die SeSecurityPrivilege, die in einigen Anwendungsanwendungsfällen, wie z. B., nützlich ist "SQL Server auf SMB-Freigaben".



Sie können die Mitgliedschaften der lokalen Cloud Volumes Service-Gruppen über das MMC mit den entsprechenden Berechtigungen anzeigen. Die folgende Abbildung zeigt Benutzer, die mit der Cloud Volumes Service Konsole hinzugefügt wurden.

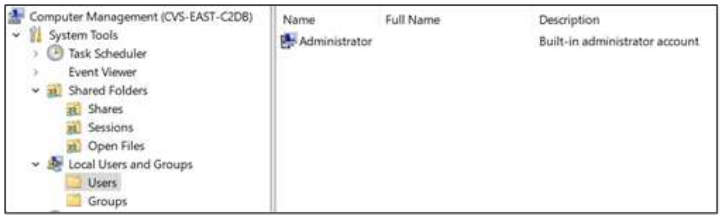


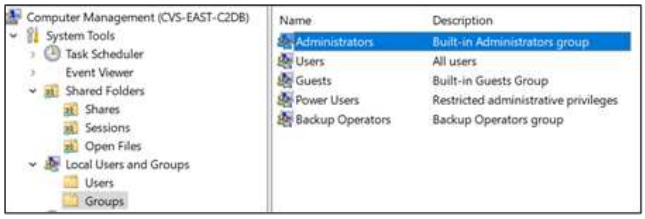
Die folgende Tabelle zeigt die Liste der Standard-BUILTIN-Gruppen und welche Benutzer/Gruppen standardmäßig hinzugefügt werden.

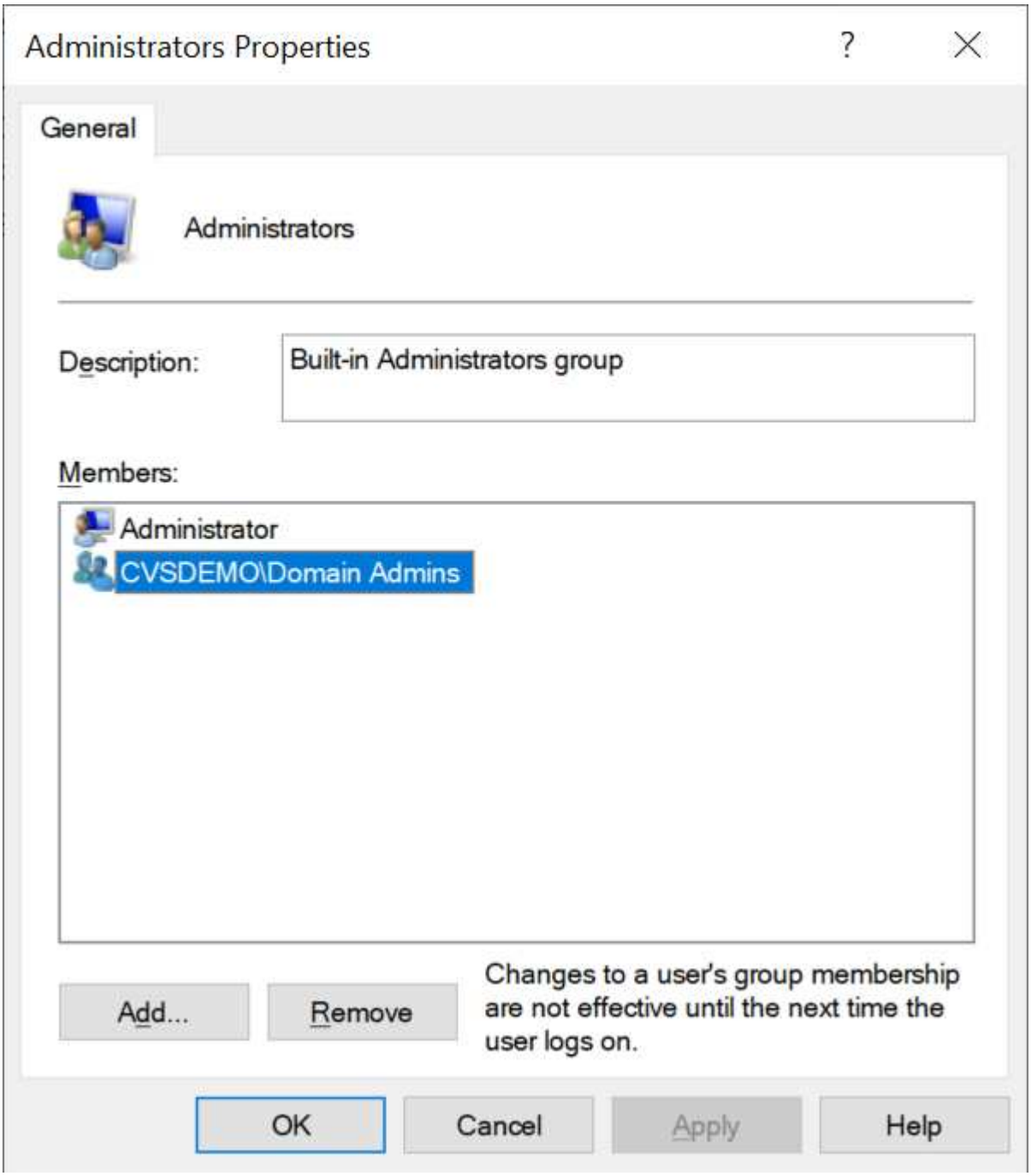
Lokale/BUILTIN-Gruppe	Standardmitglieder
BUILTIN\Administratoren*	DOMAIN\Domänen-Administratoren
BUILTIN\Backup Operators*	Keine
BAUEN Sie\Gäste	DOMAIN\Domain-Gäste
BUILTIN\Power-User	Keine
BUILTIN\Domain-Benutzer	DOMAIN\Domain-Benutzer

*Gruppenmitgliedschaft in Cloud Volumes Service Active Directory Verbindungskonfiguration gesteuert.

Sie können lokale Benutzer und Gruppen (und Gruppenmitglieder) im MMC-Fenster anzeigen, aber Sie können keine Objekte hinzufügen oder löschen oder Gruppenmitgliedschaften von dieser Konsole aus ändern. Standardmäßig werden nur die Gruppe Domänenadministratoren und der Administrator der BUILTIN\Administrators in Cloud Volumes Service hinzugefügt. Derzeit können Sie dies nicht ändern.







MMC-/Computermanagement-Zugriff

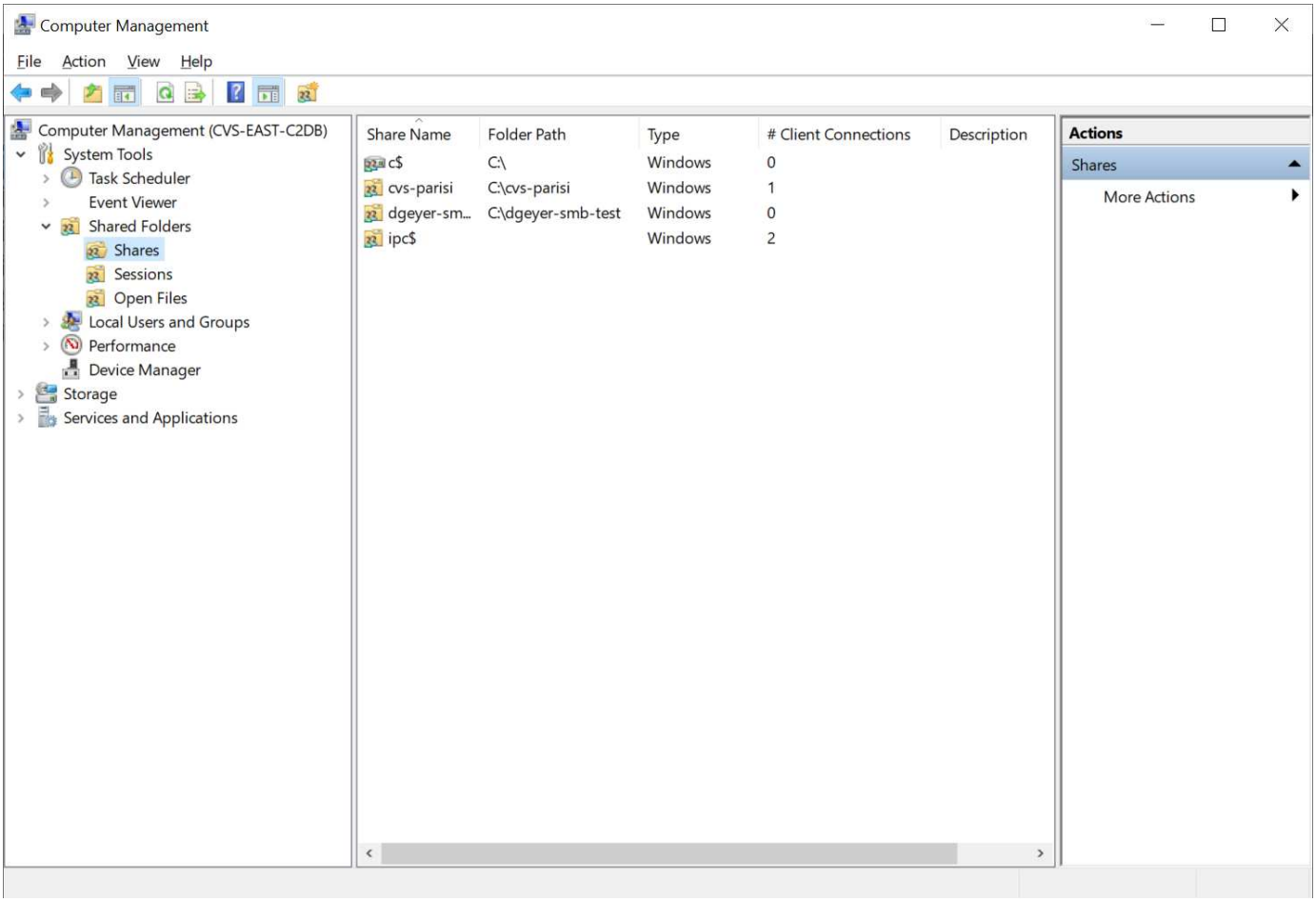
SMB-Zugriff in Cloud Volumes Service bietet Konnektivität zum Computer Management MMC, mit dem Sie Freigaben anzeigen, ACLs gemeinsam nutzen, SMB-Sessions anzeigen/managen und Dateien öffnen können.

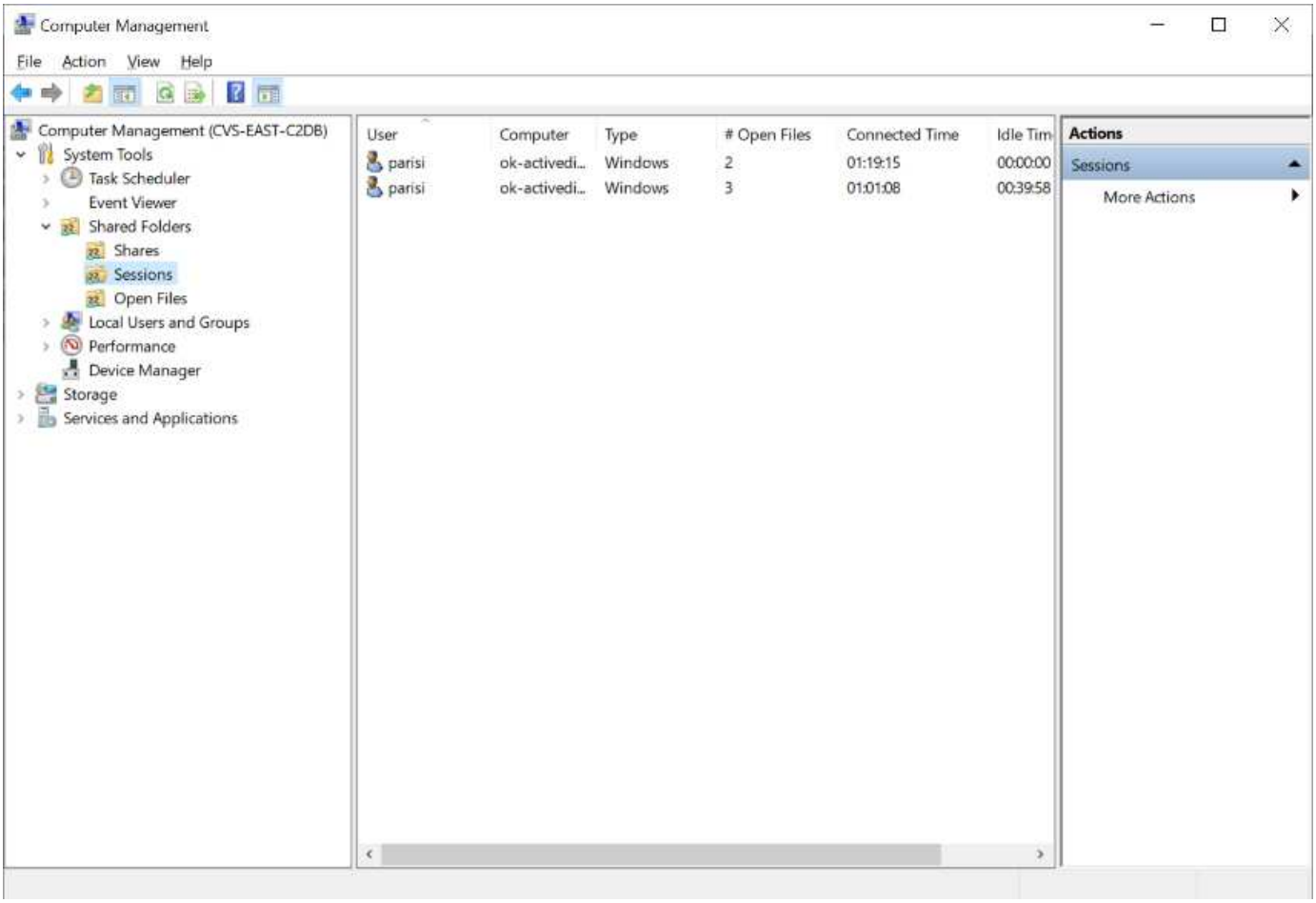
Damit Sie die MMC verwenden können, um SMB-Freigaben und -Sitzungen in Cloud Volumes Service anzuzeigen, muss der aktuell angemeldete Benutzer ein Domänenadministrator sein. Andere Benutzer haben Zugriff auf das Anzeigen oder Verwalten des SMB-Servers von MMC aus und erhalten ein Dialogfeld ohne Berechtigungen, wenn Sie versuchen, Freigaben oder Sitzungen in der Cloud Volumes Service SMB-Instanz anzuzeigen.

Um eine Verbindung zum SMB-Server herzustellen, öffnen Sie Computerverwaltung, klicken Sie mit der rechten Maustaste auf Computerverwaltung, und wählen Sie dann Verbindung zu einem anderen Computer herstellen. Daraufhin wird das Dialogfeld „Computer auswählen“ geöffnet, in dem Sie den SMB-Servernamen eingeben können (zu finden in den Cloud Volumes Service-Volume-Informationen).

Wenn Sie SMB-Freigaben mit den entsprechenden Berechtigungen anzeigen, sehen Sie alle verfügbaren Freigaben in der Cloud Volumes Service-Instanz, die die Active Directory-Verbindung nutzen. Um dieses Verhalten zu steuern, legen Sie die Option SMB-Freigaben ausblenden auf der Cloud Volumes Service-Volume-Instanz fest.

Denken Sie daran, dass pro Region nur eine Active Directory-Verbindung zulässig ist.





Die folgende Tabelle zeigt eine Liste der unterstützten/nicht unterstützten Funktionen für MMC.

Unterstützte Funktionen	Nicht unterstützte Funktionen
• Freigaben anzeigen • Anzeigen von aktiven SMB-Sitzungen • Öffnen Sie Dateien anzeigen • Zeigen Sie lokale Benutzer und Gruppen an • Zeigen Sie lokale Gruppenmitgliedschaften an • Listen Sie die Liste der Sitzungen, Dateien und Baumverbindungen im System auf • Schließen Sie offene Dateien im System • Offene Sitzungen schließen • Freigaben erstellen/managen	• Erstellen neuer lokaler Benutzer/Gruppen • Verwalten/Anzeigen vorhandener lokaler Benutzer/Gruppen • Zeigt Ereignisse oder Performance-Protokolle an • Storage-Management • Management von Services und Applikationen

Sicherheitsinformationen für SMB-Server

Der SMB-Server in Cloud Volumes Service verwendet eine Reihe von Optionen, die Sicherheitsrichtlinien für SMB-Verbindungen definieren, einschließlich Kerberos-Clock-Skew, Ticketalter, Verschlüsselung und mehr.

Die folgende Tabelle enthält eine Liste dieser Optionen, was sie tun, der Standardkonfigurationen und, ob sie mit Cloud Volumes Service geändert werden können. Einige Optionen gelten nicht für Cloud Volumes Service.

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Maximale Kerberos-Uhr-Skew (Minuten)	Maximale Zeitabweichung zwischen Cloud Volumes Service und Domain Controllern Wenn die Zeitskew 5 Minuten überschreitet, schlägt die Kerberos-Authentifizierung fehl. Dieser Wert ist auf den Standardwert von Active Directory gesetzt.	5	Nein
Lebensdauer von Kerberos-Tickets (Stunden)	Maximale Zeit, bis ein Kerberos-Ticket gültig bleibt, bevor eine Erneuerung erforderlich ist. Wenn keine Verlängerung vor 10 Stunden erfolgt, müssen Sie ein neues Ticket einholen. Cloud Volumes Service führt diese Verlängerungen automatisch durch. 10 Stunden ist der Standardwert von Active Directory.	10	Nein
Maximale Kerberos-Ticketverlängerung (Tage)	Maximale Anzahl der Tage, an denen ein Kerberos-Ticket erneuert werden kann, bevor eine neue Autorisierungsanforderung erforderlich ist. Cloud Volumes Service verlängert automatisch die Tickets für SMB-Verbindungen. Sieben Tage ist der Standardwert von Active Directory.	7	Nein
Kerberos KDC-Verbindungszeitlimit (Sek.)	Die Anzahl der Sekunden, bevor eine KDC-Verbindung ausgeht.	3	Nein

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Für eingehenden SMB-Datenverkehr müssen signiert werden	Für SMB-Datenverkehr muss eine Signatur erforderlich sein. Wenn auf „true“ gesetzt ist, unterstützen Clients, die keine Verbindung zum Signieren von Fehlschlagen unterstützen.	Falsch	
Komplexität des Kennworts für lokale Benutzerkonten erforderlich	Wird für Passwörter für lokale SMB-Benutzer verwendet. Cloud Volumes Service unterstützt die Erstellung lokaler Benutzer nicht, daher gilt diese Option nicht für Cloud Volumes Service.	Richtig	Nein
Verwenden Sie Start_tls für Active Directory-LDAP-Verbindungen	Wird zum Starten von TLS-Verbindungen für Active Directory LDAP verwendet. Cloud Volumes Service unterstützt derzeit die Aktivierung dieses Systems nicht.	Falsch	Nein
AES-128- und AES-256-Verschlüsselung für Kerberos aktiviert	Dies steuert, ob AES-Verschlüsselung für Active Directory-Verbindungen verwendet wird und wird über die Option AES-Verschlüsselung für Active Directory-Authentifizierung aktivieren bei der Erstellung/Änderung der Active Directory-Verbindung gesteuert.	Falsch	Ja.
LM-Kompatibilitätsstufe	Ebene der unterstützten Authentifizierungsdialekte für Active Directory-Verbindungen. Siehe Abschnitt „SMB-Authentifizierungsdialekte„ Weitere Informationen.	ntlmv2-krb	Nein

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
SMB-Verschlüsselung für eingehenden CIFS-Datenverkehr erforderlich	SMB-Verschlüsselung für alle Freigaben erforderlich Dies wird nicht von Cloud Volumes Service verwendet; stattdessen setzen Sie Verschlüsselung auf Volume-Basis (siehe Abschnitt „Sicherheitsfunktionen für die SMB-Freigabe„).	Falsch	Nein
Sicherheit Der Client-Sitzung	Legt das Signing und/oder Sealing für die LDAP-Kommunikation fest. Dies ist derzeit nicht in Cloud Volumes Service eingestellt, kann aber in zukünftigen Versionen zur Adresse benötigt werden. Die Behebung von Problemen mit der LDAP-Authentifizierung aufgrund des Windows-Patches wird im Abschnitt behandelt "„LDAP-Kanalbindung.“".	Keine	Nein
SMB2 aktivieren für Gleichstromverbindungen	Verwendet SMB2 für DC-Verbindungen. Standardmäßig aktiviert.	Systemstandard	Nein
LDAP Referral Chasing	Bei der Verwendung mehrerer LDAP-Server ermöglicht die Verweisungsjagd dem Client, auf andere LDAP-Server in der Liste zu verweisen, wenn ein Eintrag nicht im ersten Server gefunden wird. Dies wird derzeit nicht von Cloud Volumes Service unterstützt.	Falsch	Nein
Verwenden Sie LDAPS für sichere Active Directory-Verbindungen	Aktiviert die Verwendung von LDAP über SSL. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein

Sicherheitsoption	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Für DC-Verbindung ist eine Verschlüsselung erforderlich	Verschlüsselung für erfolgreiche DC-Verbindungen erforderlich. In Cloud Volumes Service standardmäßig deaktiviert.	Falsch	Nein

Dual-Protokoll/Multiprotokoll

Cloud Volumes Service bietet die Möglichkeit, dieselben Datensätze sowohl für SMB- als auch für NFS-Clients zu nutzen, ohne dass die Zugriffsberechtigungen dafür unterbrochen werden ("Dual-Protokoll"). Dies geschieht durch die Koordinierung der Identitätszuordnung zwischen Protokollen und die Verwendung eines zentralen Backend-LDAP-Servers zur Bereitstellung der UNIX-Identitäten an Cloud Volumes Service. Sie können Windows Active Directory verwenden, um sowohl Windows- als auch UNIX-Benutzer zur Benutzerfreundlichkeit bereitzustellen.

Zugriffssteuerung

- **Zugriffskontrollen freigeben.** Bestimmen Sie, welche Clients und/oder Benutzer und Gruppen auf eine NAS-Freigabe zugreifen können. Für NFS kontrollieren Exportrichtlinien und Regeln den Client-Zugriff auf Exporte. NFS-Exporte werden von der Cloud Volumes Service Instanz gemanagt. SMB nutzt CIFS/SMB-Freigaben und ACLs für die Freigabe von ACLs und ermöglicht eine granularere Kontrolle auf Benutzer- und Gruppenebene. Sie können ACLs auf Share-Ebene nur über SMB-Clients konfigurieren "MMC/Computer-Management" Mit einem Konto, das über Administratorrechte auf der Cloud Volumes Service-Instanz verfügt (siehe Abschnitt "„Konten mit lokalen/BUILTIN-Administrator/Backup-Rechten.“").
- **Dateizugriffssteuerung.** Kontrollieren Sie Berechtigungen auf Datei- oder Ordnerebene und werden immer vom NAS-Client verwaltet. NFS Clients können die traditionellen Modus-Bits (rwx) oder NFSv4 ACLs nutzen. SMB-Clients nutzen NTFS-Berechtigungen.

Die Zugriffssteuerung für Volumes, die Daten sowohl für NFS als auch für SMB bereitstellen, hängt vom verwendeten Protokoll ab. Informationen zu Berechtigungen mit Dual-Protokoll finden Sie im Abschnitt „Berechtigungsmodell.“

Benutzerzuordnung

Wenn ein Client auf ein Volume zugreift, versucht Cloud Volumes Service, den eingehenden Benutzer in die entgegengesetzte Richtung einem gültigen Benutzer zuzuordnen. Dies ist notwendig, damit ein ordnungsgemäßer Zugriff über verschiedene Protokolle hinweg festgestellt werden kann und sicherzustellen ist, dass der Benutzer, der Zugriff beantragt, tatsächlich derjenige ist, der von ihm behauptet wird.

Beispiel: Wenn ein Windows-Benutzer mit dem Namen `joe` Versucht über SMB den Zugriff auf ein Volume mit UNIX-Berechtigungen, dann führt Cloud Volumes Service eine Suche durch, um einen entsprechenden UNIX-Benutzer zu finden `joe`. Ist eine vorhanden, so werden Dateien, die als Windows Benutzer in eine SMB-Freigabe geschrieben werden `joe` Wird als UNIX-Benutzer angezeigt `joe` Von NFS-Clients.

Alternativ können Sie auch festlegen, ob ein UNIX-Benutzer den Namen hat `joe` Versucht, auf ein Cloud Volumes Service-Volume mit Windows-Berechtigungen zuzugreifen, dann muss der UNIX-Benutzer in der Lage sein, einem gültigen Windows-Benutzer zuzuordnen. Andernfalls wird der Zugriff auf das Volume

verweigert.

Derzeit wird nur Active Directory für das externe UNIX-Identitätsmanagement mit LDAP unterstützt. Weitere Informationen zum Konfigurieren des Zugriffs auf diesen Dienst finden Sie unter "Erstellen einer AD-Verbindung".

Berechtigungsmodell

Bei der Verwendung von Dual-Protokoll-Setups verwendet Cloud Volumes Service Sicherheitsformate für Volumes, um den Typ der ACL zu bestimmen. Diese Sicherheitsstile werden basierend auf bestimmten NAS-Protokollen oder bei einem dualen Protokoll festgelegt. Sie sollten zur Zeit der Cloud Volumes Service Volume-Erstellung gewählt werden.

- Wenn Sie nur NFS verwenden, verwenden Cloud Volumes Service-Volumes UNIX-Berechtigungen.
- Wenn Sie nur SMB verwenden, verwenden Cloud Volumes Service Volumes NTFS-Berechtigungen.

Wenn Sie ein Dual-Protokoll-Volume erstellen, können Sie bei der Volume-Erstellung den ACL-Stil wählen. Diese Entscheidung sollte auf der Grundlage der gewünschten Berechtigungsverwaltung getroffen werden. Wenn Ihre Benutzer Berechtigungen von Windows-/SMB-Clients verwalten, wählen Sie NTFS. Wenn Ihre Benutzer NFS-Clients und chmod/chown verwenden möchten, verwenden Sie UNIX-Sicherheitsmethoden.

Überlegungen zum Erstellen von Active Directory-Verbindungen

Cloud Volumes Service bietet die Möglichkeit, Ihre Cloud Volumes Service Instanz mit einem externen Active Directory Server zu verbinden, um Identitäts-Management für SMB- und UNIX-Benutzer zu ermöglichen. Für die Verwendung von SMB in Cloud Volumes Service ist das Erstellen einer Active Directory-Verbindung erforderlich.

Bei der Konfiguration hierfür stehen verschiedene Optionen zur Verfügung, bei denen die Sicherheit berücksichtigt werden muss. Der externe Active Directory Server kann eine lokale oder Cloud-native Instanz sein. Wenn Sie einen lokalen Active Directory-Server verwenden, setzen Sie die Domäne nicht dem externen Netzwerk (z. B. mit einer DMZ oder einer externen IP-Adresse) aus. Verwenden Sie stattdessen sichere private Tunnel oder VPNs, One-Way-Forest-Trusts oder dedizierte Netzwerkverbindungen zu den On-Premises-Netzwerken mit "Privater Zugriff Auf Google". In der Google Cloud-Dokumentation finden Sie weitere Informationen zu "Best Practices Using Active Directory in Google Cloud".

> CVS-SW erfordert, dass sich Active Directory-Server in derselben Region befinden. Wenn eine DC-Verbindung in CVS-SW zu einer anderen Region versucht wird, schlägt der Versuch fehl. Wenn Sie CVS-SW verwenden, erstellen Sie Active Directory-Sites, die die Active Directory-Datacenter enthalten, und geben Sie dann Standorte in Cloud Volumes Service an, um regionale DC-Verbindungsversuche zu vermeiden.

Active Directory-Anmeldeinformationen

Wenn SMB oder LDAP für NFS aktiviert ist, interagiert Cloud Volumes Service mit den Active Directory Controllern, um ein Computerkonto-Objekt zu erstellen, das für die Authentifizierung verwendet werden soll. Dies unterscheidet sich nicht von der Verbindung eines Windows SMB-Clients zu einer Domäne und erfordert dieselben Zugriffsrechte für Organisationseinheiten (OUs) in Active Directory.

In vielen Fällen ist die Verwendung eines Windows-Administratorkontos auf externen Servern wie Cloud Volumes Service nicht gestattet. In einigen Fällen ist der Windows Administrator-Benutzer vollständig als bewährte Sicherheitsübung deaktiviert.

Zum Erstellen von SMB-Computerkonten erforderliche Berechtigungen

Um einem Active Directory Cloud Volumes Service-Maschinenobjekte hinzuzufügen, ein Konto, das entweder über Administratorrechte für die Domäne verfügt oder über "Delegierte Berechtigungen zum Erstellen und Ändern von Computerkontontobjekten" Für eine angegebene Organisationseinheit ist erforderlich. Dazu können Sie den Assistenten zur Delegierung von Computerobjekten in Active Directory verwenden, indem Sie eine benutzerdefinierte Aufgabe erstellen, die einem Benutzer den Zugriff auf das Erstellen/Löschen von Computerobjekten mit den folgenden Zugriffsberechtigungen bietet:

- Lese-/Schreibzugriff
- Alle Untergeordneten Objekte Erstellen/Löschen
- Lesen/Schreiben Aller Eigenschaften
- Passwort Ändern/Zurücksetzen

Dadurch wird der OU in Active Directory automatisch eine Sicherheits-ACL für den definierten Benutzer hinzugefügt und der Zugriff auf die Active Directory-Umgebung wird minimiert. Nachdem ein Benutzer delegiert wurde, können dieser Benutzername und dieses Passwort in diesem Fenster als Active Directory-Anmeldeinformationen angegeben werden.

Der Benutzername und das Passwort, das an die Active Directory-Domäne übergeben wird, nutzen die Kerberos-Verschlüsselung während der Abfrage des Computerkontos und der Erstellung für zusätzliche Sicherheit.

Details zur Active Directory-Verbindung

Der "Active Directory-Verbindungsdetails" Bereitstellen von Feldern für Administratoren, um bestimmte Active Directory-Schemainformationen für die Platzierung von Computerkonten bereitzustellen, z. B.:

- **Active Directory-Verbindungstyp.** zur Angabe, ob die Active Directory-Verbindung in einer Region für Volumes von entweder Cloud Volumes Service oder CVS-Performance-Diensttypen verwendet wird. Wenn diese Funktion bei einer vorhandenen Verbindung falsch eingestellt ist, funktioniert sie möglicherweise nicht richtig, wenn sie verwendet oder bearbeitet wird.
- **Domain.** der Active Directory-Domänenname.
- **Site.** beschränkt Active Directory-Server auf einen bestimmten Standort für Sicherheit und Leistung "Überlegungen". Dies ist erforderlich, wenn mehrere Active Directory-Server Regionen umfassen, da Cloud Volumes Service derzeit keine Unterstützung bietet, um Active Directory-Authentifizierungsanforderungen an Active Directory-Server in einer anderen Region als der Cloud Volumes Service-Instanz zu erlauben. (Beispielsweise ist der Active Directory Domain Controller in einer Region, die nur CVS-Performance unterstützt, aber einen SMB-Share in einer CVS-SW-Instanz wünschen.)
- **DNS-Server.** DNS-Server zur Verwendung bei der Namensaufsuchen.
- **NetBIOS-Name (optional).** auf Wunsch der NetBIOS-Name für den Server. Dies wird verwendet, wenn neue Computerkonten mithilfe der Active Directory-Verbindung erstellt werden. Wenn beispielsweise der NetBIOS-Name auf CVS-EAST gesetzt ist, dann sind die Namen des Computerkontos CVS-EAST-{1234}. Siehe Abschnitt "Wie Cloud Volumes Service in Active Directory angezeigt wird" Finden Sie weitere Informationen.
- **Organisationseinheit (Organisationseinheit).** die spezifische Organisationseinheit, die das Computerkonto erstellt. Dies ist nützlich, wenn Sie die Kontrolle an einen Benutzer für Maschinenkonten an eine bestimmte OU delegieren.
- **AES-Verschlüsselung.** Sie können auch das Kontrollkästchen AES-Verschlüsselung für AD-Authentifizierung aktivieren oder deaktivieren. Das Aktivieren der AES-Verschlüsselung für die Active

Directory-Authentifizierung bietet zusätzliche Sicherheit für die Kommunikation zwischen Cloud Volumes Service und Active Directory bei Benutzer- und Gruppensuchen. Bevor Sie diese Option aktivieren, fragen Sie Ihren Domänenadministrator, ob die Active Directory-Domänencontroller die AES-Authentifizierung unterstützen.

> Standardmäßig deaktivieren die meisten Windows-Server schwächere Chiffren (wie DES oder RC4-HMAC) nicht, aber wenn Sie schwächere Chiffren deaktivieren möchten, bestätigen Sie, dass die Cloud Volumes Service Active Directory-Verbindung für die Aktivierung von AES konfiguriert wurde. Andernfalls treten Authentifizierungsfehler auf. Die Aktivierung der AES-Verschlüsselung deaktiviert nicht schwächere Chiffren, sondern fügt dem Cloud Volumes Service SMB-Maschinenkonto Unterstützung für AES-Chiffren hinzu.

Kerberos-Bereich – Details

Diese Option gilt nicht für SMB-Server. Es wird vielmehr verwendet, wenn NFS Kerberos für das Cloud Volumes Service System konfiguriert wird. Wenn diese Details ausgefüllt werden, wird der NFS-Kerberos-Bereich konfiguriert (ähnlich einer krb5.conf-Datei unter Linux) und wird verwendet, wenn NFS-Kerberos bei der Erstellung des Cloud Volumes Service-Volumes angegeben wird, da die Active Directory-Verbindung als NFS Kerberos-Verteilzentrum (KDC) fungiert.

> Nicht-Windows-Rechenzentren werden derzeit nicht für die Verwendung mit Cloud Volumes Service unterstützt.

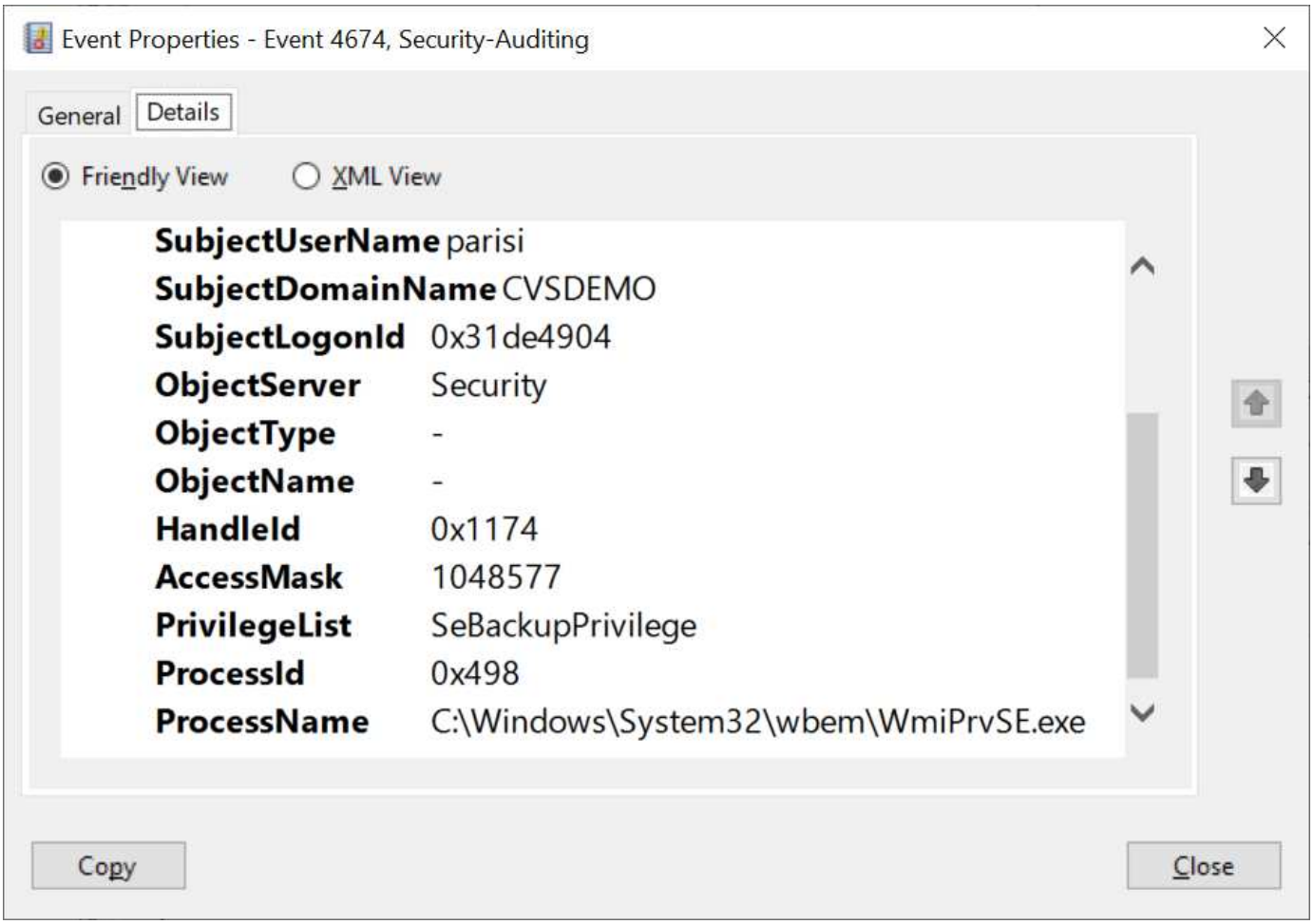
Region

In einer Region können Sie den Speicherort der Active Directory-Verbindung angeben. Diese Region muss dieselbe Region wie das Cloud Volumes Service-Volumen aufweisen.

- **Lokale NFS-Benutzer mit LDAP.** in diesem Abschnitt gibt es auch eine Option, lokale NFS-Benutzer mit LDAP zu erlauben. Diese Option muss nicht ausgewählt werden, wenn Sie Ihre UNIX-Benutzergruppenmitgliedschaft über die 16-Gruppen-Beschränkung von NFS hinaus erweitern möchten (erweiterte Gruppen). Die Verwendung erweiterter Gruppen erfordert jedoch einen konfigurierten LDAP-Server für UNIX-Identitäten. Wenn Sie keinen LDAP-Server haben, lassen Sie diese Option nicht ausgewählt. Wenn Sie über einen LDAP-Server verfügen und auch lokale UNIX-Benutzer verwenden möchten (z. B. Root), wählen Sie diese Option aus.

Backup-Benutzer

Mit dieser Option können Sie Windows-Benutzer angeben, die Sicherungsberechtigungen auf dem Cloud Volumes Service-Volume besitzen. Backup-Berechtigungen (SeBackupPrivilege) sind für einige Anwendungen erforderlich, um Daten in NAS-Volumes ordnungsgemäß zu sichern und wiederherzustellen. Dieser Benutzer hat einen hohen Zugriff auf die Daten des Volumes, daher sollten Sie es in Betracht ziehen "Aktivieren der Prüfung dieses Benutzerzugriffs". Nach Aktivierung werden Audit-Ereignisse in der Ereignisanzeige > Windows-Protokolle > Sicherheit angezeigt.



Benutzer mit Sicherheitsberechtigungen

Mit dieser Option können Sie Windows-Benutzer angeben, die über Sicherheitsberechtigungen für das Cloud Volumes Service-Volume verfügen. Für einige Anwendungen sind Sicherheitsberechtigungen (SeSecurityPrivilege) erforderlich ("Z. B. SQL Server") Die Berechtigungen während der Installation richtig einstellen. Diese Berechtigung ist zur Verwaltung des Sicherheitsprotokolls erforderlich. Obwohl dieses Privileg nicht so mächtig ist wie SeBackupPrivilege, empfiehlt NetApp Folgendes "Prüfung des Benutzerzugriffs von Benutzern" Bei Bedarf mit dieser Berechtigungsebene verfügbar.

Weitere Informationen finden Sie unter "Neue Anmeldung zugewiesene Sonderberechtigungen".

Wie Cloud Volumes Service in Active Directory angezeigt wird

Cloud Volumes Service wird in Active Directory als normales Konto-Objekt angezeigt. Die Namenskonventionen lauten wie folgt.

- CIFS/SMB und NFS Kerberos erstellen separate Computerkontoobjekte.
- NFS mit aktiviertem LDAP erstellt ein Maschinenkonto in Active Directory für Kerberos LDAP bindet.
- Duale Protokoll-Volumes mit LDAP nutzen das CIFS/SMB-Maschinenkonto für LDAP und SMB.
- CIFS/SMB-Maschinenkonten verwenden eine Namensgebungskonvention von NAME-1234 (zufällige vierstellige ID mit Bindestrich angefügt an <10 Zeichen Name) für das Maschinenkonto. SIE können DEN NAMEN durch die Einstellung des NetBIOS-Namens auf der Active Directory-Verbindung definieren (siehe Abschnitt „Details zur Active Directory-Verbindung„).

- NFS Kerberos verwendet NFS-NAME-1234 als Namenskonvention (bis zu 15 Zeichen). Wenn mehr als 15 Zeichen verwendet werden, lautet der Name NFS-CAM-NAME-1234.
- Nur NFS CVS-Performance-Instanzen mit aktiviertem LDAP erstellen ein SMB-Maschinenkonto, um es an den LDAP-Server zu binden, und zwar mit derselben Namenskonvention wie CIFS/SMB-Instanzen.
- Wenn ein SMB-Computerkonto erstellt wird, werden standardmäßig ausgeblendete Admin-Freigaben verwendet (siehe Abschnitt "„Standard versteckte Freigaben“") Werden auch erstellt (c€, Admin-Dollar, ipc-Dollar), aber diese Aktien haben keine ACLs zugewiesen und sind unzugänglich.
- Die Rechnungsobjekte werden standardmäßig in CN=Computer platziert, aber eine können Sie bei Bedarf eine andere OU festlegen. Siehe Abschnitt „Zum Erstellen von SMB-Computerkonten erforderliche Berechtigungen“ Informationen darüber, welche Zugriffsrechte zum Hinzufügen/Entfernen von Gerätekontonobjekten für Cloud Volumes Service erforderlich sind.

Wenn Cloud Volumes Service das SMB-Maschinenkonto zu Active Directory hinzufügt, werden die folgenden Felder ausgefüllt:

- cn (mit dem angegebenen SMB-Servernamen)
- DNSHostName (mit SMBserver.domain.com)
- MSDS-SupportedVerschlüsselungTypes (allows DES_CBC_MD5, RC4_HMAC_MD5, wenn die AES-Verschlüsselung nicht aktiviert ist; WENN die AES-Verschlüsselung aktiviert ist, SIND DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 für den Kerberos-Account zugelassen)
- Name (mit SMB-Servername)
- SAMAccountName (mit SMBserver-Kosten)
- ServicePrincipalName (mit Host/smbserver.domain.com und Host/smbserver-SPNs für Kerberos)

Wenn Sie schwächere Kerberos-Verschlüsselungstypen (Enctype) auf dem Maschinenkonto deaktivieren möchten, können Sie den Wert MSDS-SupportedVerschlüsselungTypes auf dem Maschinenkonto auf einen der Werte in der folgenden Tabelle ändern, um nur AES zu ermöglichen.

MSDS-SupportVerschlüsselungTypes Wert	Zuctype aktiviert
2	DES_CBC_MD5
4	RC4_HMAC
8	NUR AES128_CTS_HMAC_SHA1_96
16	NUR AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 UND AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 UND AES256_CTS_HMAC_SHA1_96

Um die AES-Verschlüsselung für SMB-Computerkonten zu aktivieren, klicken Sie beim Erstellen der Active Directory-Verbindung auf AES-Verschlüsselung für AD-Authentifizierung aktivieren.

Um die AES-Verschlüsselung für NFS-Kerberos zu aktivieren, "Weitere Informationen finden Sie in der Cloud Volumes Service-Dokumentation".

Andere NAS-Infrastruktur-Serviceabhängigkeiten (KDC, LDAP und DNS)

Bei der Verwendung von Cloud Volumes Service für NAS-Freigaben sind möglicherweise externe Abhängigkeiten erforderlich, um ordnungsgemäße Funktion sicherzustellen. Diese Abhängigkeiten spielen unter bestimmten Umständen eine Rolle. Die folgende Tabelle zeigt verschiedene Konfigurationsoptionen und ggf. erforderliche Abhängigkeiten.

Konfiguration	Erforderliche Abhängigkeiten
Nur NFSv3	Keine
Nur NFSv3 Kerberos	Windows Active Directory: * KDC * DNS * LDAP
Nur NFSv4.1	Konfiguration der Client-ID-Zuordnung (/etc/idmap.conf)
Nur Kerberos	• Konfiguration der Client-ID-Zuordnung (/etc/idmap.conf) • Windows Active Directory: KDC-DNS-LDAP
Nur SMB	Active Directory: * KDC * DNS
Multi-Protokoll-NAS (NFS und SMB)	• Konfiguration der Client-ID-Zuordnung (nur NFSv4.1; /etc/idmap.conf) • Windows Active Directory: KDC-DNS-LDAP

Kerberos Keytab-Rotation/Passwort-Reset für Computerkontoobjekte

Bei SMB-Computerkonten plant Cloud Volumes Service regelmäßige Passwortrücksetzungen für das SMB-Maschinenkonto. Diese Kennwortrücksetzung erfolgt mit Kerberos-Verschlüsselung und wird nach einem Zeitplan jeden vierten Sonntag zu einer zufälligen Zeit zwischen 23:00 und 1:00 UHR ausgeführt. Mit diesem Kennwort werden die Kerberos-Schlüsselversionen geändert, die Keytabs, die auf dem Cloud Volumes Service-System gespeichert sind, gedreht und die Sicherheit von SMB-Servern, die in Cloud Volumes Service ausgeführt werden, erhöht. Passwörter für Computerkonten sind randomisiert und Administratoren nicht bekannt.

Bei NFS-Kerberos-Computerkonten erfolgt ein Zurücksetzen des Passworts nur dann, wenn ein neuer Keytab mit dem KDC erstellt/ausgetauscht wird. Derzeit ist dies in Cloud Volumes Service nicht möglich.

Netzwerkports zur Verwendung mit LDAP und Kerberos

Wenn Sie LDAP und Kerberos verwenden, sollten Sie die von diesen Diensten verwendeten Netzwerkports ermitteln. Eine vollständige Liste der von Cloud Volumes Service verwendeten Ports finden Sie im "Cloud Volumes Service Dokumentation zu Sicherheitsüberlegungen".

LDAP

Cloud Volumes Service fungiert als LDAP-Client und verwendet Standard-LDAP-Suchanfragen für Benutzer- und Gruppensuchen nach UNIX-Identitäten. LDAP ist erforderlich, wenn Sie Benutzer und Gruppen außerhalb der von Cloud Volumes Service bereitgestellten Standardbenutzer verwenden möchten. LDAP ist auch erforderlich, wenn Sie die Verwendung von NFS Kerberos mit Benutzerprinzipals (z. B. user1@domain.com) planen. Derzeit wird nur LDAP unterstützt, die Microsoft Active Directory verwenden.

Wenn Sie Active Directory als UNIX LDAP-Server verwenden möchten, müssen Sie die erforderlichen UNIX-Attribute für Benutzer und Gruppen ausfüllen, die Sie für UNIX-Identitäten verwenden möchten. Cloud Volumes Service verwendet eine Standard-LDAP-Schemavorlage, die Attribute basierend auf abfragt "RFC-2307-bis". Die folgende Tabelle zeigt die für Benutzer und Gruppen erforderlichen Mindestattribute für Active Directory und deren Verwendung für die einzelnen Attribute.

Weitere Informationen zum Festlegen von LDAP-Attributen in Active Directory finden Sie unter "Management des Dual-Protokoll-Zugriffs:"

Attribut	Das macht es
uid*	Gibt den UNIX-Benutzernamen an
UidNummer*	Gibt die numerische ID des UNIX-Benutzers an
GidNumber*	Gibt die numerische ID der primären Gruppe des UNIX-Benutzers an
ObjectClass*	Gibt an, welcher Objekttyp verwendet wird; Cloud Volumes Service erfordert, dass „Benutzer“ in die Liste der Objektklassen aufgenommen werden muss (ist standardmäßig in den meisten Active Directory-Bereitstellungen enthalten).
Name	Allgemeine Informationen zum Konto (echter Name, Telefonnummer usw.)
UnixUserpasswort	Kein Grund zur Festlegung; nicht in UNIX-Identitätssuchten für die NAS-Authentifizierung verwendet. Durch diese Einstellung wird der konfigurierte Wert unixUserPassword in Klartext gesetzt.
UnixHomeDirectory	Definiert den Pfad zu UNIX-Home-Verzeichnissen, wenn ein Benutzer sich von einem Linux-Client aus mit LDAP authentifiziert. Legen Sie diesen Wert fest, wenn Sie die Home-Directory-Funktion LDAP für UNIX verwenden möchten.
LoginShell	Definiert den Pfad zur Bash/Profile Shell für Linux-Clients, wenn ein Benutzer sich mit LDAP authentifiziert.

*Bezeichnet das Attribut, das für die ordnungsgemäße Funktion mit Cloud Volumes Service erforderlich ist. Die übrigen Attribute gelten nur für die Client-seitige Verwendung.

Attribut	Das macht es
kn*	Gibt den Namen der UNIX-Gruppe an. Bei der Verwendung von Active Directory für LDAP wird dieser Wert bei der ersten Erstellung des Objekts festgelegt, kann aber später geändert werden. Dieser Name darf nicht mit anderen Objekten identisch sein. Zum Beispiel, wenn Ihr UNIX-Benutzer namens user1 gehört zu einer Gruppe namens user1 auf Ihrem Linux-Client, Windows erlaubt nicht zwei Objekte mit dem gleichen cn-Attribut. Um dies zu umgehen, benennen Sie den Windows-Benutzer in einen eindeutigen Namen um (z. B. user1-UNIX); LDAP in Cloud Volumes Service verwendet das Attribut uid für UNIX-Benutzernamen.
GidNumber*	Gibt die numerische ID der UNIX-Gruppe an.
ObjectClass*	Gibt an, welcher Objekttyp verwendet wird; Cloud Volumes Service erfordert eine Gruppe, die in die Liste der Objektklassen aufgenommen werden soll (dieses Attribut ist standardmäßig in den meisten Active Directory-Bereitstellungen enthalten).
MitgliedschaftenUid	Gibt an, welche UNIX-Benutzer Mitglieder der UNIX-Gruppe sind. Bei Active Directory LDAP in Cloud Volumes Service ist dieses Feld nicht erforderlich. Das Cloud Volumes Service-LDAP-Schema verwendet das Mitgliedfeld für Gruppenmitgliedschaften.
Mitglied*	Erforderlich für Gruppenmitgliedschaften/sekundäre UNIX-Gruppen Dieses Feld wird ausgefüllt, indem Windows-Benutzer zu Windows-Gruppen hinzugefügt werden. Allerdings, wenn die Windows-Gruppen nicht über UNIX-Attribute gefüllt haben, sind sie nicht in der UNIX-Benutzer-Gruppenmitgliedliste enthalten. Alle Gruppen, die in NFS verfügbar sein müssen, müssen die in dieser Tabelle aufgeführten erforderlichen UNIX-Gruppenattribute ausfüllen.

*Bezeichnet das Attribut, das für die ordnungsgemäße Funktion mit Cloud Volumes Service erforderlich ist. Die übrigen Attribute gelten nur für die Client-seitige Verwendung.

LDAP-Bindeinformationen

Um Benutzer in LDAP abfragen zu können, muss Cloud Volumes Service den LDAP-Dienst binden (anmelden). Diese Anmeldung hat schreibgeschützte Berechtigungen und wird verwendet, um LDAP-UNIX-Attribute für Verzeichnissuchen abzufragen. Derzeit ist LDAP-Bindungen nur über die Verwendung eines SMB-Maschinenkontos möglich.

LDAP kann nur für aktiviert werden `CVS-Performance` Instanzen können für NFSv3, NFSv4.1 oder Dual-Protocol Volumes verwendet werden. Für die erfolgreiche Bereitstellung des LDAP-fähigen Volumes muss eine Active Directory-Verbindung in derselben Region wie das Cloud Volumes Service-Volume hergestellt werden.

Wenn LDAP aktiviert ist, tritt in bestimmten Szenarien Folgendes auf.

- Wenn nur NFSv3 oder NFSv4.1 für das Cloud Volumes Service-Projekt verwendet wird, wird im Active Directory-Domänencontroller ein neues Maschinenkonto erstellt, und der LDAP-Client in Cloud Volumes Service bindet sich mithilfe der Anmeldeinformationen für das Computerkonto an Active Directory. Für das NFS Volume und die verborgenen administrativen Standardfreigaben werden keine SMB-Freigaben erstellt (siehe Abschnitt "„Standard versteckte Freigaben“") Haben Freigabe-ACLs entfernt.
- Wenn Dual-Protokoll-Volumes für das Cloud Volumes Service-Projekt genutzt werden, wird nur das für SMB-Zugriff erstellte Maschinenkonto verwendet, um den LDAP-Client in Cloud Volumes Service an Active Directory zu binden. Es werden keine weiteren Computerkonten erstellt.
- Wenn dedizierte SMB-Volumes separat erstellt werden (entweder vor oder nach Aktivierung von NFS-Volumes mit LDAP), wird das Computerkonto für LDAP-Bindungen mit dem SMB-Computerkonto gemeinsam genutzt.
- Wenn NFS Kerberos ebenfalls aktiviert ist, werden zwei Computerkonten erstellt: Eins für SMB-Freigaben und/oder LDAP bindet und eins für die NFS-Kerberos-Authentifizierung.

LDAP-Abfragen

Obwohl LDAP-Bindungen verschlüsselt sind, werden LDAP-Abfragen über das Netzwerk im Klartext über den gemeinsamen LDAP-Port 389 übergeben. Dieser bekannte Port kann derzeit nicht in Cloud Volumes Service geändert werden. Infolgedessen kann ein Benutzer- und Gruppennamen, numerische IDs und Gruppenmitgliedschaften mit Zugriff auf Packet Sniffing im Netzwerk angezeigt werden.

Allerdings können Google Cloud VMs nicht schnuppern andere VM Unicast-Verkehr. Nur VMs, die aktiv am LDAP-Datenverkehr beteiligt sind (das heißt, binden zu können), können Datenverkehr vom LDAP-Server sehen. Weitere Informationen zum Packet Sniffing in Cloud Volumes Service finden Sie im Abschnitt "„Packet Sniffing/Trace Betrachtungen.“"

Standard für die LDAP-Client-Konfiguration

Wenn LDAP in einer Cloud Volumes Service-Instanz aktiviert ist, wird standardmäßig eine LDAP-Client-Konfiguration mit spezifischen Konfigurationsdetails erstellt. In einigen Fällen gelten Optionen entweder nicht für Cloud Volumes Service (nicht unterstützt) oder können nicht konfiguriert werden.

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
LDAP-Serverliste	Legt LDAP-Servernamen oder IP-Adressen für Abfragen fest. Dies wird für Cloud Volumes Service nicht verwendet. Stattdessen wird Active Directory Domain zum Definieren von LDAP-Servern verwendet.	Nicht festgelegt	Nein
Active Directory-Domäne	Legt die Active Directory-Domäne für LDAP-Abfragen fest. Cloud Volumes Service nutzt SRV-Datensätze für LDAP in DNS, um LDAP-Server in der Domäne zu finden.	Legen Sie die Active Directory-Domäne fest, die in der Active Directory-Verbindung angegeben ist.	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Bevorzugte Active Directory-Server	Legt die bevorzugten Active Directory-Server fest, die für LDAP verwendet werden sollen. Nicht unterstützt durch Cloud Volumes Service. Verwenden Sie stattdessen Active Directory-Sites, um die LDAP-Serverauswahl zu steuern.	Nicht festgelegt.	Nein
Binden mit SMB Server Credentials	Bindet an LDAP über das SMB-Maschinenkonto. Derzeit ist die einzige unterstützte LDAP-Bindemethode in Cloud Volumes Service.	Richtig	Nein
Schemavorlage	Die Schemavorlage, die für LDAP-Abfragen verwendet wird.	MS-AD-BIS	Nein
LDAP-Serverport	Die für LDAP-Abfragen verwendete Portnummer. Cloud Volumes Service verwendet derzeit nur den Standard-LDAP-Port 389. LDAPS/Port 636 wird derzeit nicht unterstützt.	389	Nein
Ist LDAPS aktiviert	Steuert, ob LDAP over Secure Sockets Layer (SSL) für Abfragen und Bindungen verwendet wird. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein
Zeitüberschreitung bei Abfrage (Sek.)	Timeout für Abfragen. Wenn Abfragen länger als der angegebene Wert dauern, schlagen Abfragen fehl.	3	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Minimale Stufe Der Bind-Authentifizierung	Die minimal unterstützte Bindestufe. Da Cloud Volumes Service Computerkonten für LDAP-Bindungen verwendet und Active Directory standardmäßig keine anonymen Bindungen unterstützt, kommt diese Option aus Sicherheitsgründen nicht zum Spiel.	Anonym	Nein
DN binden	Der für Bindungen verwendete Benutzer/Distinguished Name (DN) wird verwendet, wenn einfache Bindung verwendet wird. Cloud Volumes Service verwendet Computerkonten für LDAP-Verbindungen und unterstützt derzeit keine einfache Bindeauthentifizierung.	Nicht festgelegt	Nein
Basis-DN	Der Basis-DN, der für LDAP-Suchen verwendet wird.	Die Windows-Domäne, die für die Active Directory-Verbindung im DN-Format verwendet wird (d. h. DC=Domain, DC=local).	Nein
Umfang der Basissuche	Der Suchbereich für Basis-DN-Suchvorgänge. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt nur Unterbaumsuchen.	Unterbaum	Nein
Benutzer-DN	Definiert den DN, in dem der Benutzer nach LDAP-Abfragen startet. Derzeit wird Cloud Volumes Service nicht unterstützt, sodass alle Benutzersuchen am Basis-DN beginnen.	Nicht festgelegt	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Umfang der Benutzersuche	Der Suchbereich für Benutzer-DN sucht. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt das Festlegen des Anwendungsbereichs für die Benutzersuche nicht.	Unterbaum	Nein
Gruppen-DN	Definiert den DN, in dem die Gruppensuche nach LDAP-Abfragen beginnen soll. Derzeit wird Cloud Volumes Service nicht unterstützt, daher beginnen alle Gruppensuchen am Basis-DN.	Nicht festgelegt	Nein
Bereich der Gruppensuche	Der Suchbereich für Gruppen-DN sucht. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt das Festlegen des Umfangs der Gruppensuche nicht.	Unterbaum	Nein
Netzgruppe DN	Definiert den DN, in dem Netzgruppe nach LDAP-Abfragen startet. Derzeit wird Cloud Volumes Service nicht unterstützt, daher beginnen alle Netzgruppensuchvorgänge am Basis-DN.	Nicht festgelegt	Nein
Suchumfang für Netzgruppe	Der Suchbereich für Netzgruppe DN sucht. Werte können Basis, Onelevel oder Unterbaum umfassen. Cloud Volumes Service unterstützt nicht das Festlegen des Suchbereichs für Netzgruppen.	Unterbaum	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
Verwenden Sie Start_tls über LDAP	Nutzt Start TLS für zertifikatbasierte LDAP-Verbindungen über Port 389. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein
Aktivieren Sie die Suche in netgroup-by-Host	Ermöglicht die Suche in einer Netzwerkgruppe nach Hostnamen und nicht die Erweiterung von Netgroups, um alle Mitglieder aufzulisten. Derzeit nicht unterstützt von Cloud Volumes Service.	Falsch	Nein
Netgroup-by-Host DN	Definiert den DN, in dem netgroup-by-Host nach LDAP-Abfragen startet. Netgroup-by-Host wird derzeit für Cloud Volumes Service nicht unterstützt.	Nicht festgelegt	Nein
Suchumfang für Netzgruppe nach Host	Der Suchbereich für netgroup-by-Host DN sucht. Werte können Basis, Onelevel oder Unterbaum enthalten. Netgroup-by-Host wird derzeit für Cloud Volumes Service nicht unterstützt.	Unterbaum	Nein
Sicherheit der Client-Session	Definiert, in welchem Maß die Sitzungssicherheit von LDAP verwendet wird (Zeichen, Siegel oder keine). Das LDAP-Signieren wird von CVS-Performance unterstützt, sofern dies von Active Directory angefordert wird. CVS-SW unterstützt LDAP-Signatur nicht. Für beide Servicetypen wird die Dichtung derzeit nicht unterstützt.	Keine	Nein

LDAP-Client-Option	Das macht es	Standardwert	Können Sie Veränderungen vornehmen?
LDAP-Verweisungsjagd	Bei der Verwendung mehrerer LDAP-Server ermöglicht die Verweisungsjagd dem Client, auf andere LDAP-Server in der Liste zu verweisen, wenn ein Eintrag nicht im ersten Server gefunden wird. Dies wird derzeit nicht von Cloud Volumes Service unterstützt.	Falsch	Nein
Filter für Gruppenmitgliedschaft	Bietet einen benutzerdefinierten LDAP-Suchfilter, der verwendet werden kann, wenn eine Gruppenmitgliedschaft von einem LDAP-Server aus gesucht wird. Derzeit nicht unterstützt mit Cloud Volumes Service.	Nicht festgelegt	Nein

LDAP für asymmetrische Namenszuweisung verwenden

Cloud Volumes Service ordnet Windows-Benutzern und UNIX-Benutzern standardmäßig ohne spezielle Konfiguration bidirektional identische Benutzernamen zu. Solange Cloud Volumes Service einen gültigen UNIX-Benutzer (mit LDAP) finden kann, erfolgt die 1:1-Namenszuweisung. Beispiel: Wenn Windows-Benutzer `johnsmith` Wird verwendet, dann, wenn Cloud Volumes Service einen UNIX-Benutzer namens finden kann `johnsmith` In LDAP ist die Namenszuordnung für diesen Benutzer erfolgreich, alle Dateien/Ordner, die von erstellt wurden `johnsmith` Zeigen Sie den korrekten Benutzerbesitz und alle ACLs an, die davon betroffen sind `johnsmith` Unabhängig vom verwendeten NAS-Protokoll honoriert werden. Dies wird als symmetrisches Namenszuordnungen bezeichnet.

Asymmetrisches Namenszuordnungen ist, wenn die Windows-Benutzer- und UNIX-Benutzeridentität nicht übereinstimmt. Beispiel: Wenn Windows-Benutzer `johnsmith` Hat eine UNIX-Identität von `jsmith`, Cloud Volumes Service braucht einen Weg, um über die Variation zu erzählen. Da Cloud Volumes Service derzeit nicht die Erstellung von statischen Name Mapping Regeln unterstützt, muss LDAP verwendet werden, um die Identität der Benutzer für Windows und UNIX Identitäten zu suchen, um die ordnungsgemäße Eigentum von Dateien und Ordnern und erwarteten Berechtigungen zu gewährleisten.

Standardmäßig enthält Cloud Volumes Service Folgendes `LDAP` Im ns-Switch der Instanz für die Name-Map-Datenbank, sodass Sie die Namenszuordnungsfunktion durch die Verwendung von LDAP für asymmetrische Namen bereitstellen können, müssen Sie nur einige der Benutzer-/Gruppenattribute ändern, um das zu reflektieren, was Cloud Volumes Service sucht.

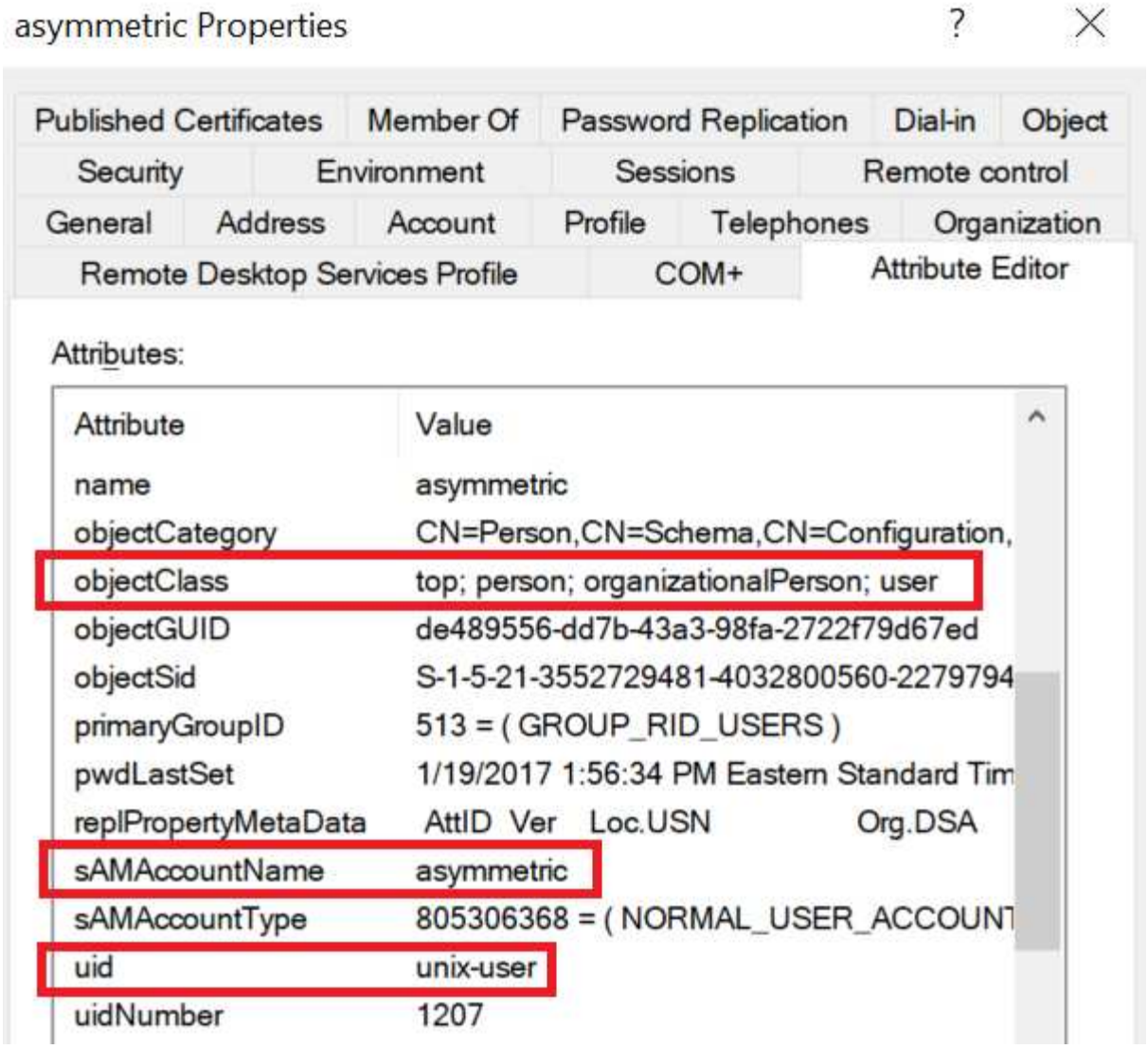
In der folgenden Tabelle wird gezeigt, welche Attribute für die asymmetrische Namenszuordnungsfunktion in LDAP ausgefüllt werden müssen. In den meisten Fällen ist Active Directory bereits dafür konfiguriert.

Cloud Volumes Service Attribut	Das macht es	Von Cloud Volumes Service für die Namenszuweisung verwendeter Wert
Windows auf UNIX objectClass	Gibt den Typ des verwendeten Objekts an. (D. h. Benutzer, Gruppe, PosixAccount usw.)	Muss Benutzer enthalten (kann mehrere andere Werte enthalten, falls gewünscht.)
Attribut Windows zu UNIX	Dies definiert den Windows-Benutzernamen bei der Erstellung. Cloud Volumes Service verwendet dies für Windows-to-UNIX-Lookups.	Hier ist keine Änderung erforderlich; sAMAccountName ist der gleiche wie der Windows-Anmeldename.
UID	Definiert den UNIX-Benutzernamen.	Gewünschter UNIX-Benutzername.

Cloud Volumes Service verwendet derzeit keine Domänenpräfixe in LDAP-Lookups, so dass mehrere Domänen-LDAP-Umgebungen nicht richtig funktionieren mit LDAP-Namemap-Lookups.

Im folgenden Beispiel wird ein Benutzer mit dem Windows-Namen angezeigt `asymmetric`, Der UNIX-Name `unix-user`, Und das Verhalten folgt es beim Schreiben von Dateien sowohl aus SMB und NFS.

Die folgende Abbildung zeigt, wie LDAP-Attribute vom Windows-Server aussehen.



Von einem NFS-Client aus können Sie den UNIX-Namen, nicht jedoch den Windows-Namen abfragen:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Wenn eine Datei aus NFS als geschrieben wird `unix-user`, Das folgende Ergebnis ist von dem NFS Client:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Von einem Windows-Client aus sehen Sie, dass der Eigentümer der Datei auf den richtigen Windows-Benutzer eingestellt ist:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Umgekehrt werden Dateien vom Windows-Benutzer erstellt `asymmetric` Von einem SMB-Client wird der richtige UNIX-Eigentümer angezeigt, wie im folgenden Text dargestellt.

SMB:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

LDAP-Kanalbindung

Aufgrund einer Schwachstelle bei Windows Active Directory-Domänencontrollern "Microsoft Security Advisory ADV190023" Ändert die Art und Weise, wie DCs LDAP-Bindungen zulassen.

Die Auswirkungen von Cloud Volumes Service sind dieselben wie für alle LDAP-Clients. Cloud Volumes Service unterstützt derzeit keine Channel-Bindung. Da Cloud Volumes Service standardmäßig LDAP-Signatur durch Aushandlung unterstützt, sollte die LDAP-Channel-Bindung kein Problem darstellen. Wenn Sie Probleme mit der Bindung an LDAP bei aktivierter Kanalbindung haben, befolgen Sie die Schritte zur Problembehebung in ADV190023, damit LDAP-Bindungen von Cloud Volumes Service erfolgreich durchgeführt werden können.

DNS

Active Directory und Kerberos haben beide Abhängigkeiten von DNS für den Hostnamen zu IP/IP bis zur Auflösung des Hostnamens. DNS erfordert, dass Port 53 offen ist. Cloud Volumes Service nimmt keine Änderungen an DNS-Einträgen vor und unterstützt derzeit nicht die Verwendung von "Dynamisches DNS" An Netzwerkschnittstellen.

Sie können Active Directory DNS so konfigurieren, dass Sie festlegen können, welche Server DNS-Einträge aktualisieren können. Weitere Informationen finden Sie unter "Sicheres Windows DNS".

Beachten Sie, dass Ressourcen innerhalb eines Google-Projekts standardmäßig mit Google Cloud DNS, die nicht mit Active Directory DNS verbunden ist. Clients, die Cloud DNS verwenden, können keine UNC-Pfade auflösen, die von Cloud Volumes Service zurückgegeben werden. Windows-Clients, die mit der Active

Directory-Domäne verbunden sind, sind für die Verwendung von Active Directory DNS konfiguriert und können solche UNC-Pfade auflösen.

Um einem Client zu Active Directory beizutreten, müssen Sie seine DNS-Konfiguration so konfigurieren, dass Active Directory DNS verwendet wird. Optional können Sie Cloud DNS konfigurieren, um Anfragen an Active Directory DNS weiterzuleiten. Siehe "Warum kann mein Client den SMB NetBIOS-Namen nicht lösen?"Finden Sie weitere Informationen.

> Cloud Volumes Service unterstützt derzeit keine DNSSEC- und DNS-Abfragen werden im Klartext ausgeführt.

Prüfung von Dateizugriffen

Derzeit nicht unterstützt für Cloud Volumes Service.

Virenschutz

Sie müssen in Cloud Volumes Service am Client auf eine NAS-Freigabe Antivirenprüfungen durchführen. Derzeit ist keine native Virenschutz-Integration in Cloud Volumes Service möglich.

Service-Betrieb

Das Cloud Volumes Service-Team verwaltet die Backend-Services in Google Cloud und nutzt verschiedene Strategien, um die Plattform zu sichern und unerwünschte Zugriffe zu vermeiden.

Jeder Kunde erhält sein eigenes Subnetz, mit dem standardmäßig Zugriff von anderen Kunden isoliert ist. Jeder Mandant in Cloud Volumes Service erhält seinen eigenen Namespace und VLAN für eine vollständige Datenisolierung. Nachdem ein Benutzer authentifiziert wurde, kann die Service Delivery Engine (SDE) nur noch Konfigurationsdaten für diesen Mandanten lesen.

Physische Sicherheit

Mit entsprechender Vorabgenehmigung haben nur Techniker vor Ort und NetApp Außendiensttechniker (Field Support Engineers, FSEs) Zugriff auf den Käfig und die Racks für physische Arbeiten. Storage- und Netzwerk-Management ist nicht zulässig. Nur diese Ressourcen vor Ort sind in der Lage, Hardware-Wartungsarbeiten durchzuführen.

Für Techniker vor Ort wird ein Ticket für die Leistungsbeschreibung (Statement of Work, SOW) angehoben, das die Rack-ID und den Standort des Geräts (RU) enthält. Alle weiteren Details sind im Ticket enthalten. Bei NetApp FSEs muss ein Besuchsticket vor Ort mit COLO GELEGT werden, und das Ticket enthält die Daten, das Datum und die Zeit der Besucher zu Audit-Zwecken. Das SOW für den FSE wird intern an NetApp kommuniziert.

Operations Team

Das Betriebsteam für Cloud Volumes Service setzt sich aus Produktionstechnik und einem Site Reliability Engineer (SRE) für Cloud Volume Services sowie NetApp Field Support Engineers und Hardware-Partnern zusammen. Alle Mitglieder des Betriebsteams sind für die Arbeit in Google Cloud akkreditiert und für jedes angehobene Ticket werden detaillierte Arbeitsunterlagen aufbewahrt. Darüber hinaus gibt es einen strengen Änderungskontroll- und Genehmigungsprozess, um sicherzustellen, dass jede Entscheidung angemessen überprüft wird.

Das SRE-Team verwaltet die Kontrollebene und wie die Daten von UI-Anfragen an Back-End-Hardware und

-Software in Cloud Volumes Service weitergeleitet werden. Das SRE-Team verwaltet außerdem Systemressourcen, wie z. B. die maximale Anzahl von Volumes und Inode. SRES dürfen nicht mit Kundendaten interagieren oder Zugriff haben. Darüber hinaus koordiniert SRES mit Return Material Authorizations (RMAs), wie z. B. neue Festplatten- oder Speicherersatzanfragen für die Backend-Hardware.

Mitwirkungspflichten des Kunden

Kunden von Cloud Volumes Service verwalten das Active Directory und die Benutzerrollenverwaltung sowie die Menge und die Datenvorgänge ihrer Organisation. Kunden können über Administratorrollen verfügen und Berechtigungen an andere Endbenutzer innerhalb desselben Google Cloud-Projekts delegieren. Dabei werden die beiden vordefinierten Rollen verwendet, die NetApp und Google Cloud (Administrator und Viewer) bereitstellen.

Der Administrator kann eine beliebige VPC im Kundenprojekt an Cloud Volumes Service Peer, die der Kunde für angemessen entscheidet. Der Kunde ist selbst dafür verantwortlich, den Zugriff auf sein Google Cloud Marketplace Abonnement zu managen und die VPCs zu managen, die Zugriff auf die Datenebene haben.

Bösartiger SRE-Schutz

Ein Problem, das entstehen könnte, ist, wie schützt Cloud Volumes Service vor Szenarien, in denen es einen bösartigen SRE gibt oder wenn die SRE-Anmeldeinformationen kompromittiert wurden?

Der Zugang zur Produktionsumgebung ist nur mit einer begrenzten Anzahl von SRE-Einzelpersonen möglich. Darüber hinaus sind Administratorrechte auf eine Handvoll erfahrener Administratoren beschränkt. Alle Aktionen, die von jedem Mitarbeiter der Cloud Volumes Service Produktionsumgebung ausgeführt werden, werden protokolliert. Anomalien an der Basis- oder verdächtigen Aktivitäten werden durch unsere SIEM-Plattform (Security Information and Event Management) Threat Intelligence (Threat Intelligence Platform) erkannt. Dadurch können böswillige Aktionen nachverfolgt und abgemildert werden, bevor das Cloud Volumes Service-Backend zu einem zu großen Schaden angerichtet wird.

Volumenlebenszyklus

Cloud Volumes Service managt nur die Objekte innerhalb des Service, nicht die Daten innerhalb der Volumes. Nur Clients, die auf die Volumes zugreifen, können die Daten, ACLs, Dateieigentümer usw. managen. Die Daten in diesen Volumes sind im Ruhezustand verschlüsselt und der Zugriff ist auf Mandanten der Cloud Volumes Service Instanz beschränkt.

Der Lebenszyklus eines Volumes für Cloud Volumes Service ist create-Update-delete. Volumes behalten Snapshot Kopien von Volumes, bis die Volumes gelöscht werden. Nur validierte Cloud Volumes Service Administratoren können Volumes in Cloud Volumes Service löschen. Wenn ein Administrator eine Volume-Löschung angefordert hat, muss ein zusätzlicher Schritt zur Eingabe des Volume-Namens erforderlich sein, um die Löschung zu überprüfen. Nachdem ein Volume gelöscht wurde, ist das Volume verschwunden und kann nicht wiederhergestellt werden.

Falls ein Cloud Volumes Service-Vertrag beendet wird, kennzeichnet NetApp Volumes nach einem bestimmten Zeitraum zum Löschen. Bevor dieser Zeitraum abläuft, können Sie Volumes auf Kundenwunsch wiederherstellen.

Zertifizierungen

Cloud Volumes Services für Google Cloud sind derzeit nach den Standards ISO/IEC 27001:2013 und ISO/IEC 27018:2019 zertifiziert. Der Service erhielt kürzlich auch seinen SOC2 Type I Attestation Report. Weitere Informationen über die Verpflichtung von NetApp zur Datensicherheit und zum Datenschutz finden Sie unter "Compliance: Datensicherheit und Datenschutz".

DSGVO

Unsere Verpflichtung zu Datenschutz und Einhaltung der DSGVO steht in mehreren unserer zahlreichen verfügbar "Kundenverträge", Wie unsere "Ergänzung Zur Kundendatenverarbeitung", Das beinhaltet die "Standardvertragsklauseln" Von der Europäischen Kommission bereitgestellt. Diese Verpflichtungen stellen wir auch in unserer Datenschutzrichtlinie ein, die durch die zentralen Werte unseres Unternehmenskodex eingehalten wird.

Weitere Informationen und Kontaktdaten

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

- Google Cloud-Dokumentation für Cloud Volumes Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes/"

- Google Private Service-Zugriff

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp Produktdokumentation

  "https://www.netapp.com/support-and-training/documentation/"

- Kryptografisches Validierungsmodul-Programm – NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- NetApp Lösung gegen Ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: NFS Kerberos im ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Kontaktieren Sie uns

Lassen Sie uns wissen, wie wir diesen technischen Bericht verbessern können.

Kontaktieren Sie uns unter doccomments@netapp.com. Nehmen SIE den TECHNISCHEN BERICHT 4918 in die Betreffzeile auf.

BlueXP Backup und Recovery

BlueXP Backup und Recovery für VMs

3-2-1 Datensicherung für VMware mit SnapCenter Plug-in und BlueXP Backup und Recovery für VMs

Autor: Josh Powell – NetApp Solutions Engineering

Überblick

Die 3-2-1-1-Backup-Strategie ist eine in der Branche anerkannte Datenschutzmethode, die einen umfassenden Ansatz für den Schutz wertvoller Daten bietet. Diese Strategie ist zuverlässig und stellt sicher, dass auch bei unerwarteten Notfällen weiterhin eine Kopie der Daten verfügbar ist.

Die Strategie setzt sich aus drei Grundregeln zusammen:

1. Bewahren Sie mindestens drei Kopien Ihrer Daten auf. Dadurch wird sichergestellt, dass selbst wenn eine Kopie verloren geht oder beschädigt ist, noch mindestens zwei Kopien vorhanden sind, auf die Sie zurückfallen können.
2. Speichern Sie zwei Sicherungskopien auf verschiedenen Speichermedien oder Geräten. Durch die Diversifizierung von Storage-Medien werden Geräte- oder medienspezifische Ausfälle geschützt. Wenn ein Gerät beschädigt wird oder ein Medientyp ausfällt, bleibt die andere Sicherungskopie davon unberührt.
3. Außerdem muss mindestens eine Backup-Kopie extern aufbewahrt werden. Externer Storage dient als ausfallsicher bei lokalen Katastrophen wie Bränden oder Überschwemmungen, bei denen Kopien vor Ort nicht mehr verwendet werden können.

Dieses Lösungsdokument umfasst eine 3-2-1-1-Backup-Lösung mit dem SnapCenter Plug-in für VMware vSphere (SCV) zur Erstellung primärer und sekundärer Backups unserer lokalen Virtual Machines sowie BlueXP Backup und Recovery für Virtual Machines, um eine Kopie unserer Daten im Cloud Storage oder StorageGRID zu sichern.

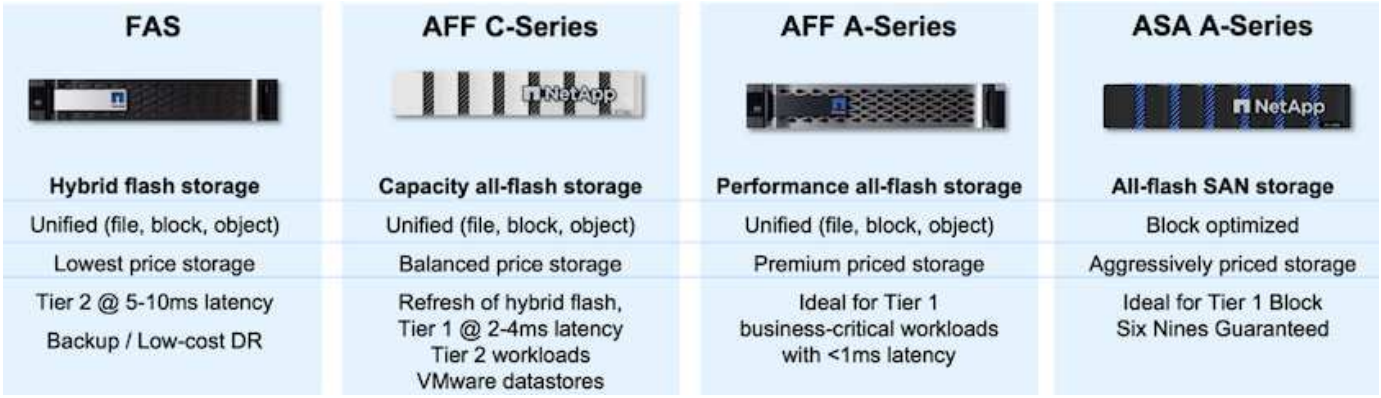
Anwendungsfälle

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Backup und Restore von lokalen Virtual Machines und Datastores mit dem SnapCenter Plug-in für VMware vSphere
- Backup und Restore von lokalen Virtual Machines und Datastores, die auf ONTAP Clustern gehostet und mit BlueXP Backup und Recovery für Virtual Machines in Objekt-Storage gesichert werden.

NetApp ONTAP Datenspeicher

ONTAP ist die branchenführende Storage-Lösung von NetApp mit Unified Storage, auch wenn der Zugriff über SAN- oder NAS-Protokolle erfolgt. Die 3-2-1-1-Backup-Strategie stellt sicher, dass lokale Daten auf mehr als einem Medientyp geschützt sind. NetApp bietet Plattformen von Hochgeschwindigkeits-Flash bis hin zu kostengünstigeren Medien.



Weitere Informationen zu allen Hardware-Plattformen von NetApp finden Sie im Checkout "NetApp Datenspeicher".

SnapCenter Plug-in für VMware vSphere

Das SnapCenter Plug-in für VMware vSphere ist ein Datensicherangebot, das eng in VMware vSphere integriert ist und das ein einfaches Management von Backup und Restore für Virtual Machines ermöglicht. Als Teil dieser Lösung bietet SnapMirror eine schnelle und zuverlässige Methode zur Erstellung einer zweiten unveränderlichen Backup-Kopie der Daten von Virtual Machines auf einem sekundären ONTAP Storage Cluster. Dank dieser Architektur können Wiederherstellungen für Virtual Machines problemlos von primären oder sekundären Backup-Standorten aus initiiert werden.

SCV wird als virtuelle linux-Appliance mit einer OVA-Datei bereitgestellt. Das Plug-in verwendet jetzt ein Remote-Plug-in
Der NetApp Architektur sind. Das Remote-Plug-in läuft außerhalb des vCenter-Servers und wird auf der virtuellen SCV-Appliance gehostet.

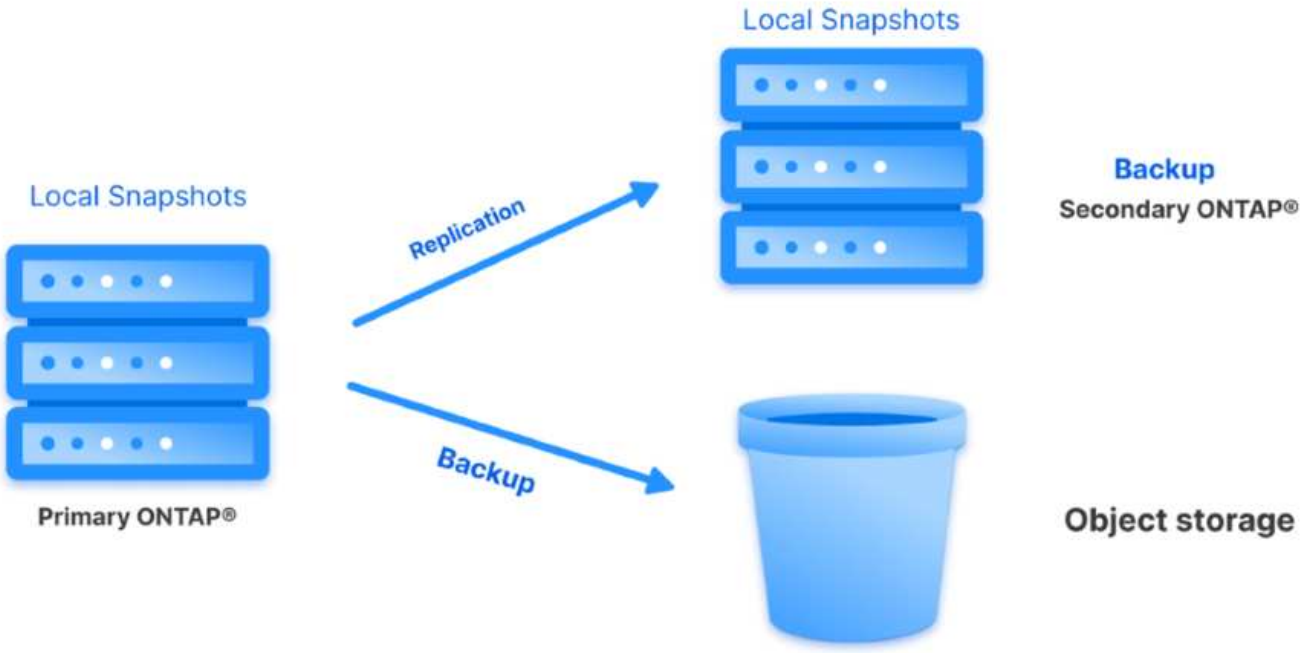
Ausführliche Informationen zu SCV finden Sie unter "Dokumentation zum SnapCenter Plug-in für VMware vSphere".

BlueXP Backup und Recovery für Virtual Machines

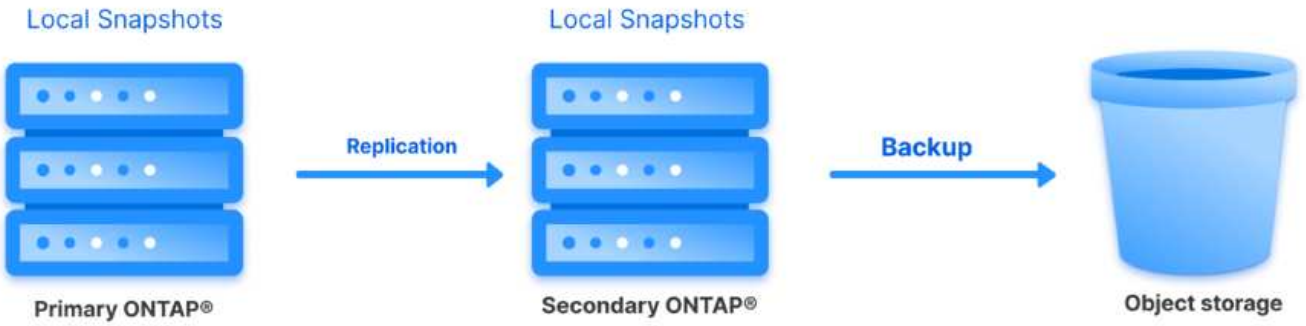
BlueXP Backup und Recovery ist ein Cloud-basiertes Tool für das Datenmanagement. Es bietet eine zentrale Managementoberfläche für eine Vielzahl von Backup- und Recovery-Vorgängen sowohl in On-Premises- als auch in Cloud-Umgebungen. Ein Bestandteil der NetApp BlueXP Backup und Recovery Suite ist eine Funktion, die in das SnapCenter Plug-in für VMware vSphere (lokal) integriert werden kann, um eine Kopie der Daten auf den Objekt-Storage in der Cloud zu erweitern. Auf diese Weise wird eine dritte Kopie der Daten an einem externen Standort erstellt, die aus den primären oder sekundären Storage-Backups stammt. Mit BlueXP Backup und Recovery lassen sich Storage-Richtlinien zur Übertragung von Datenkopien von beiden lokalen Standorten ganz einfach festlegen.

Wenn Sie sich für die primären und sekundären Backups als Quelle in BlueXP Backup und Recovery entscheiden, werden Sie eines von zwei Topologien implementieren:

Fan-out-Topologie – Wenn ein Backup vom SnapCenter-Plugin für VMware vSphere initiiert wird, wird sofort ein lokaler Snapshot erstellt. SCV initiiert dann einen SnapMirror-Vorgang, der den letzten Snapshot auf den sekundären ONTAP-Cluster repliziert. In BlueXP Backup und Recovery gibt eine Richtlinie das primäre ONTAP-Cluster als Quelle für eine Snapshot Kopie der Daten an einen Objektspeicher Ihres gewünschten Cloud-Providers an.



Kaskadierung der Topologie – die Erstellung der primären und sekundären Datenkopien mittels SCV ist identisch mit der oben genannten Fan-out-Topologie. Diesmal wird jedoch in BlueXP Backup und Recovery eine Richtlinie erstellt, die angibt, dass das Backup in Objektspeicher vom sekundären ONTAP-Cluster stammen soll.



Mit BlueXP Backup und Recovery können Backup-Kopien von lokalen ONTAP Snapshots in AWS Glacier, Azure Blob und GCP Archiv-Storage erstellt werden.

AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

Außerdem kann NetApp StorageGRID als Objekt-Storage-Backup-Ziel verwendet werden. Weitere Informationen zu StorageGRID finden Sie im "StorageGRID Landing Page".

Übersicht Zur Lösungsimplementierung

Diese Liste enthält die allgemeinen Schritte, die erforderlich sind, um diese Lösung zu konfigurieren und Backup- und Restore-Vorgänge von SCV und BlueXP Backup- und Recovery-Vorgängen auszuführen:

1. Konfiguration der SnapMirror Beziehung zwischen den ONTAP Clustern, die für primäre und sekundäre Datenkopien verwendet werden soll
2. Konfigurieren Sie das SnapCenter-Plug-in für VMware vSphere.
    a. Fügen Sie Storage-Systeme Hinzu
    b. Backup-Richtlinien erstellen
    c. Erstellen von Ressourcengruppen
    d. Führen Sie die ersten Backup-Jobs aus
3. Konfigurieren Sie BlueXP Backup und Recovery für Virtual Machines
    a. Arbeitsumgebung hinzufügen
    b. Erkennen von SCV- und vCenter-Appliances
    c. Backup-Richtlinien erstellen
    d. Aktivieren Sie Backups
4. Stellen Sie virtuelle Maschinen aus dem primären und sekundären Speicher mithilfe von SCV wieder her.
5. Wiederherstellung von Virtual Machines aus Objekt-Storage mithilfe von BlueXP Backup und Restore

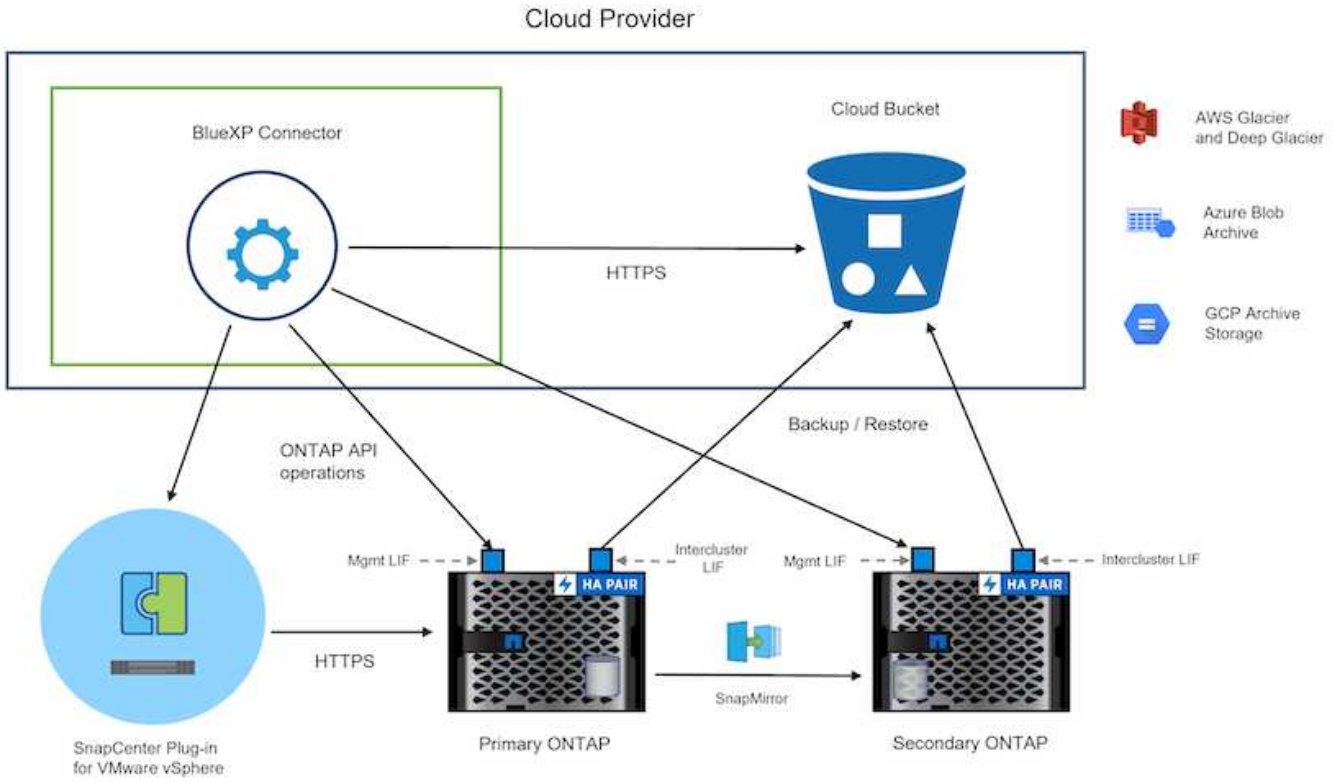
Voraussetzungen

Mit dieser Lösung soll die Datensicherung von Virtual Machines demonstriert werden, die in VMware vSphere ausgeführt werden und sich in NFS-Datenspeichern befinden, die von NetApp ONTAP gehostet werden. Bei dieser Lösung wird vorausgesetzt, dass die folgenden Komponenten konfiguriert und einsatzbereit sind:

1. ONTAP Storage-Cluster mit NFS- oder VMFS-Datenspeichern, die mit VMware vSphere verbunden sind. Sowohl NFS- als auch VMFS-Datastores werden unterstützt. Für diese Lösung wurden NFS-Datenspeicher verwendet.
2. Sekundärer ONTAP Storage-Cluster mit SnapMirror Beziehungen, die für Volumes erstellt werden, die für NFS-Datastores verwendet werden.
3. Für Objekt-Storage-Backups installierter BlueXP Connector beim Cloud-Provider
4. Zu sichernde Virtual Machines befinden sich in NFS-Datenspeichern auf dem primären ONTAP-Storage-Cluster.
5. Netzwerkkonnektivität zwischen dem BlueXP Connector und den lokalen ONTAP Storage-Cluster-Managementschnittstellen
6. Netzwerkverbindung zwischen dem BlueXP Connector und der lokalen SCV Appliance VM und zwischen dem BlueXP Konnektor und vCenter.
7. Netzwerkverbindung zwischen den lokalen ONTAP Intercluster LIFs und dem Objekt-Storage-Service
8. Für Management-SVM auf primären und sekundären ONTAP Storage-Clustern konfigurierter DNS Weitere Informationen finden Sie unter "Konfigurieren Sie DNS für die Auflösung des Host-Namens".

Übergeordnete Architektur

Die Test-/Validierung dieser Lösung wurde in einem Labor durchgeführt, das in der endgültigen Implementierungsumgebung eventuell nicht übereinstimmt.



Lösungsimplementierung

In dieser Lösung stellen wir detaillierte Anweisungen für die Implementierung und Validierung einer Lösung bereit, die das SnapCenter Plug-in für VMware vSphere zusammen mit Backup und Recovery von BlueXP nutzt. Damit können Backup und Recovery von Windows und Linux Virtual Machines innerhalb eines VMware vSphere Clusters in einem lokalen Datacenter durchgeführt werden. Die Virtual Machines in diesem Setup werden auf NFS-Datenspeichern gespeichert, die von einem ONTAP A300 Storage-Cluster gehostet werden. Darüber hinaus dient ein separates ONTAP A300 Storage-Cluster als sekundäres Ziel für mit SnapMirror replizierte Volumes. Darüber hinaus wurde Objekt-Storage, der auf Amazon Web Services und Azure Blob gehostet wird, als Ziele für eine dritte Kopie der Daten genutzt.

Wir werden über die Erstellung von SnapMirror Beziehungen für sekundäre Kopien unserer durch SCV gemanagten Backups und die Konfiguration von Backup-Jobs in SCV und BlueXP Backup und Recovery hinweggehen.

Detaillierte Informationen zum SnapCenter-Plug-in für VMware vSphere finden Sie im "Dokumentation zum SnapCenter Plug-in für VMware vSphere".

Detaillierte Informationen zu Backup und Recovery von BlueXP finden Sie im "BlueXP Backup- und Recovery-Dokumentation".

Einrichten von SnapMirror Beziehungen zwischen ONTAP Clustern

Das SnapCenter Plug-in für VMware vSphere nutzt ONTAP SnapMirror Technologie zum Management des Transports von sekundären SnapMirror bzw. SnapVault Kopien zu einem sekundären ONTAP Cluster.

SCV Backup-Richtlinien haben die Möglichkeit, SnapMirror oder SnapVault Beziehungen zu verwenden. Der Hauptunterschied liegt darin, dass der für Backups in der Richtlinie konfigurierte Aufbewahrungszeitplan am primären und sekundären Standort identisch ist. SnapVault wurde für die Archivierung entwickelt. Bei Verwendung dieser Option kann mit der SnapMirror Beziehung ein separater Aufbewahrungszeitplan für die

Snapshot-Kopien auf dem sekundären ONTAP Storage-Cluster aufgestellt werden.

Sie können SnapMirror Beziehungen in BlueXP einrichten, wo viele der Schritte automatisiert sind oder dies mit System Manager und der ONTAP CLI möglich ist. Alle diese Methoden werden im Folgenden erläutert.

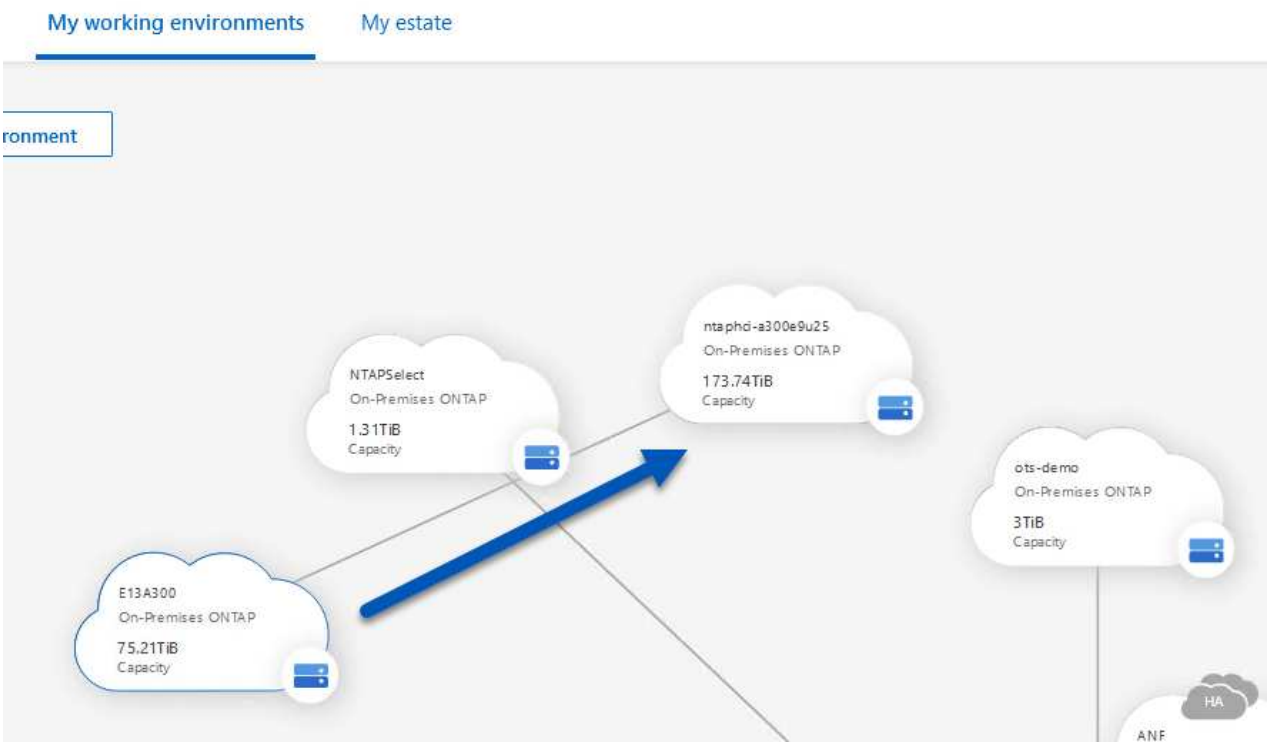
SnapMirror Beziehungen mit BlueXP aufbauen

Folgende Schritte müssen über die BlueXP Webkonsole durchgeführt werden:

Einrichtung der Replizierung für primäre und sekundäre ONTAP Storage-Systeme

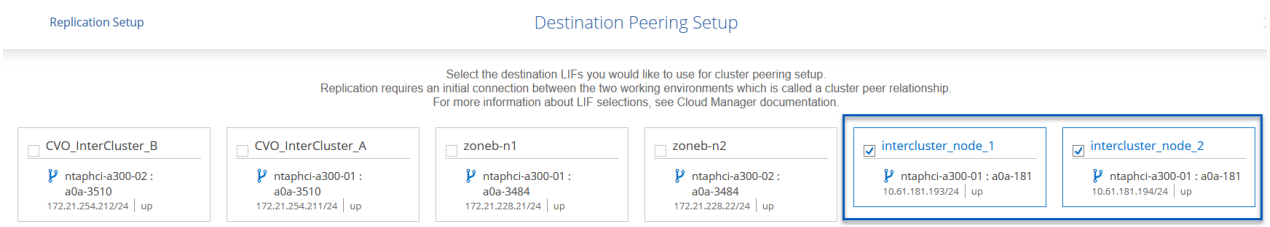
Melden Sie sich zunächst bei der BlueXP Webkonsole an und navigieren Sie zu den Leinwand.

1. Ziehen Sie das (primäre) ONTAP Quell-Storage-System per Drag & Drop auf das (sekundäre) ONTAP Ziel-Storage-System.

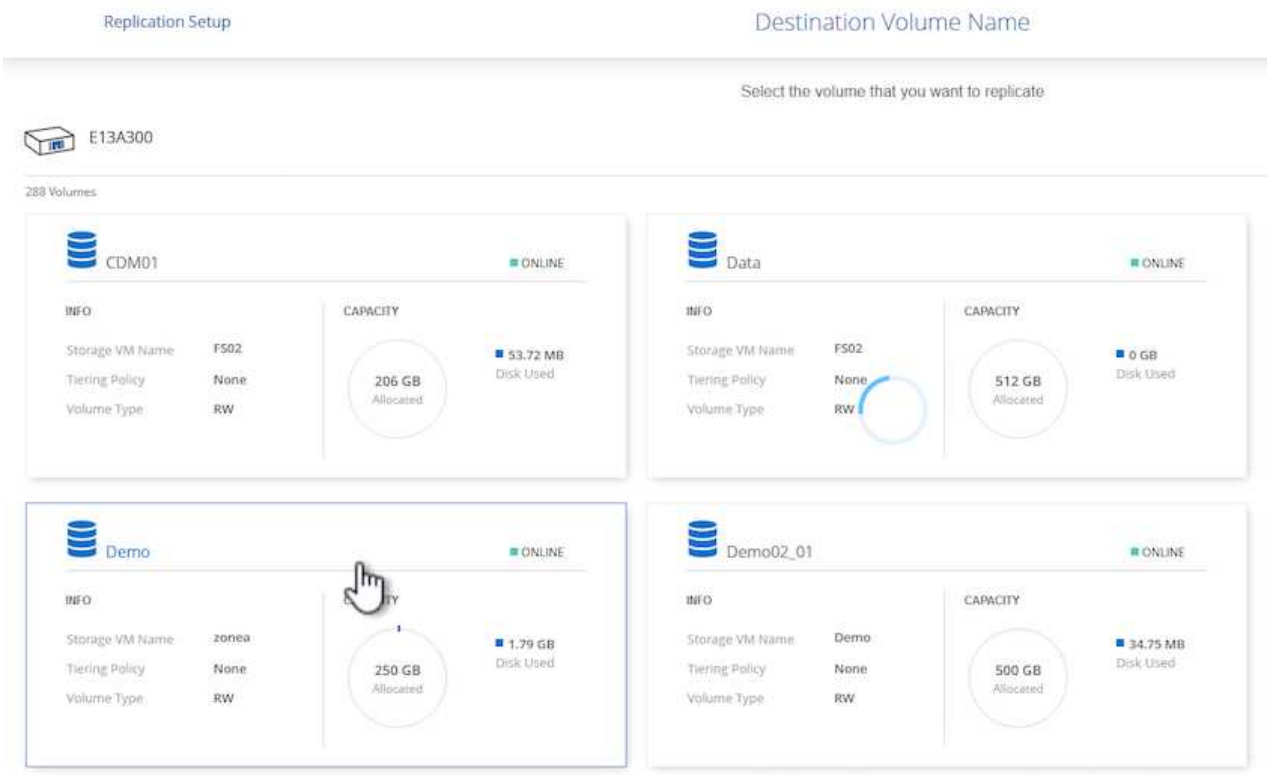


2. Wählen Sie aus dem angezeigten Menü **Replikation**.

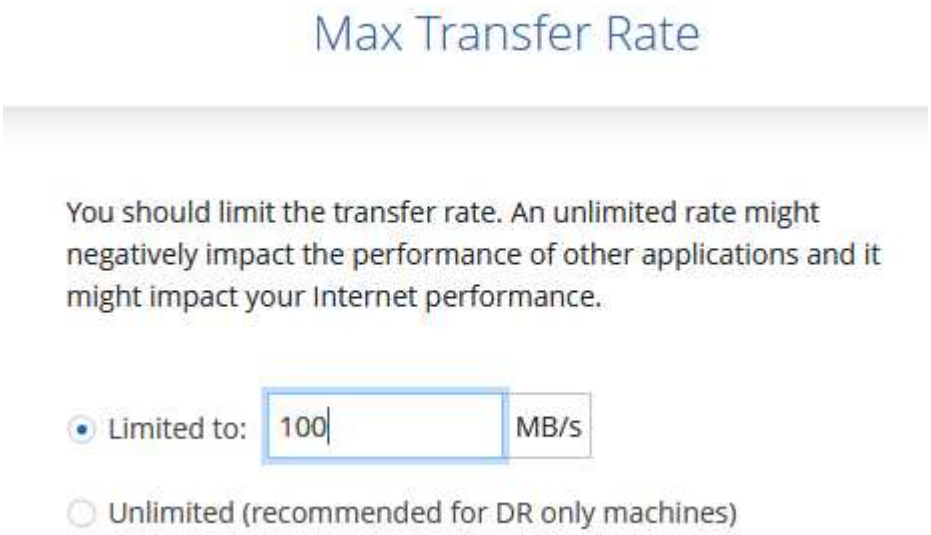
3. Wählen Sie auf der Seite **Destination Peering Setup** die Ziel-Intercluster-LIFs aus, die für die Verbindung zwischen Speichersystemen verwendet werden sollen.



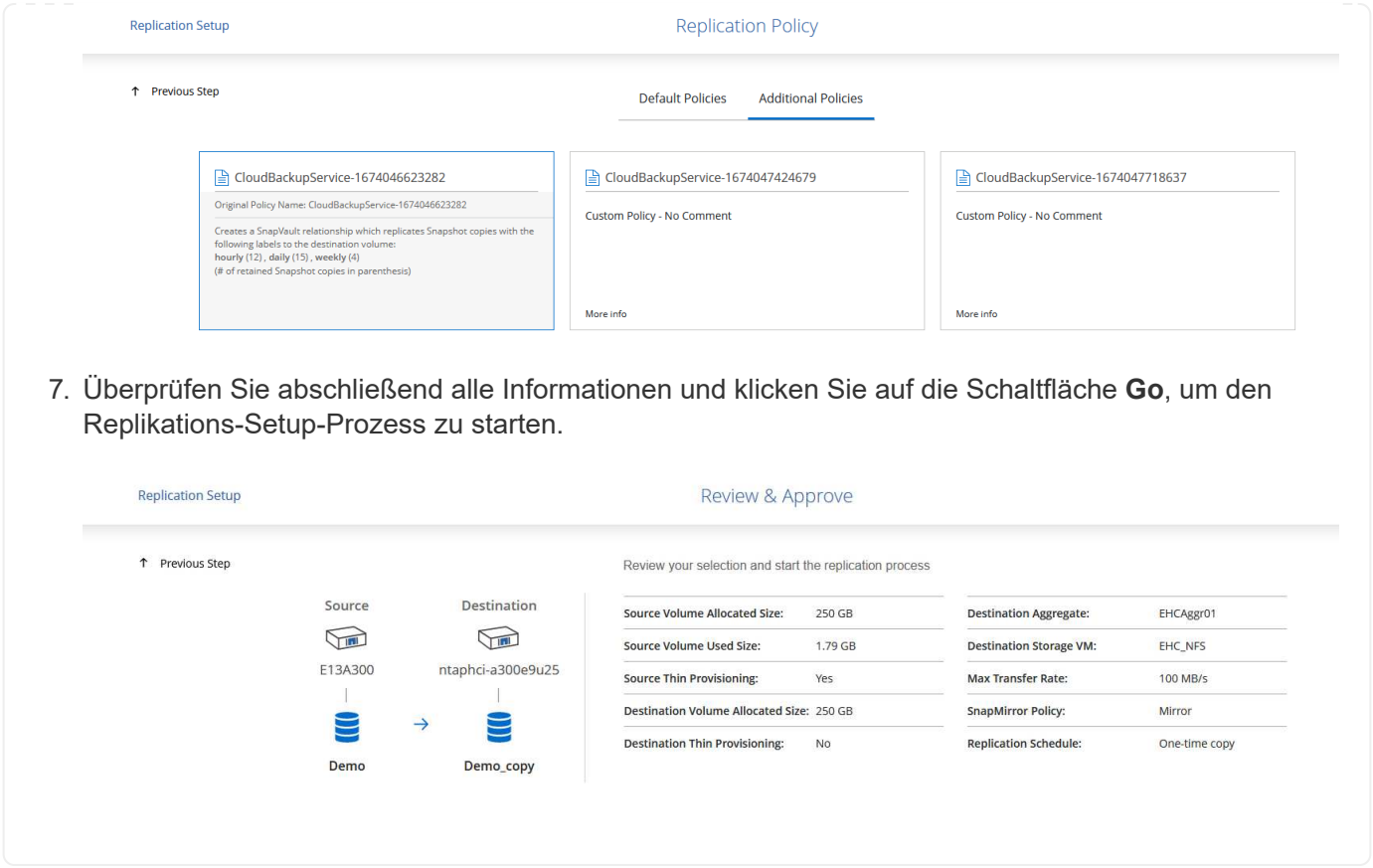
4. Wählen Sie auf der Seite **Destination Volume Name** zunächst das Quell-Volume aus, füllen Sie dann den Namen des Ziel-Volumes aus und wählen Sie die Ziel-SVM und das Aggregat aus. Klicken Sie auf **Weiter**, um fortzufahren.



5. Wählen Sie die maximale Übertragungsrate für die Replikation aus.



6. Wählen Sie die Richtlinie aus, die den Aufbewahrungsplan für sekundäre Backups bestimmt. Diese Policy kann im Vorfeld erstellt werden (siehe den manuellen Prozess unten im Schritt **Create a Snapshot Retention Policy**) oder nach Bedarf geändert werden.



7. Überprüfen Sie abschließend alle Informationen und klicken Sie auf die Schaltfläche **Go**, um den Replikations-Setup-Prozess zu starten.

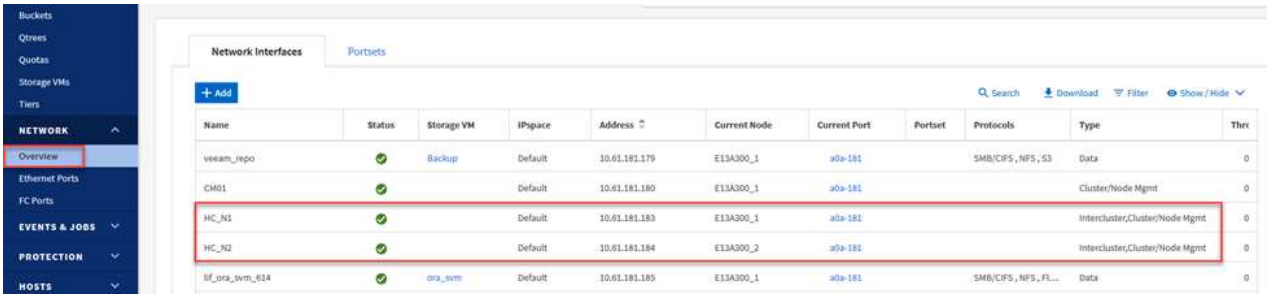
Einrichten von SnapMirror Beziehungen mit System Manager und ONTAP CLI

Alle erforderlichen Schritte zum Aufbau von SnapMirror Beziehungen können mit System Manager oder der ONTAP CLI durchgeführt werden. Im folgenden Abschnitt finden Sie detaillierte Informationen zu beiden Methoden:

Zeichnen Sie die logischen Schnittstellen von Intercluster und Ziel auf

Sie können die logischen Inter-Cluster-Informationen für die ONTAP Quell- und Ziel-Cluster aus System Manager oder aus der 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 über die CLI abzurufen, führen Sie den folgenden Befehl aus:

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

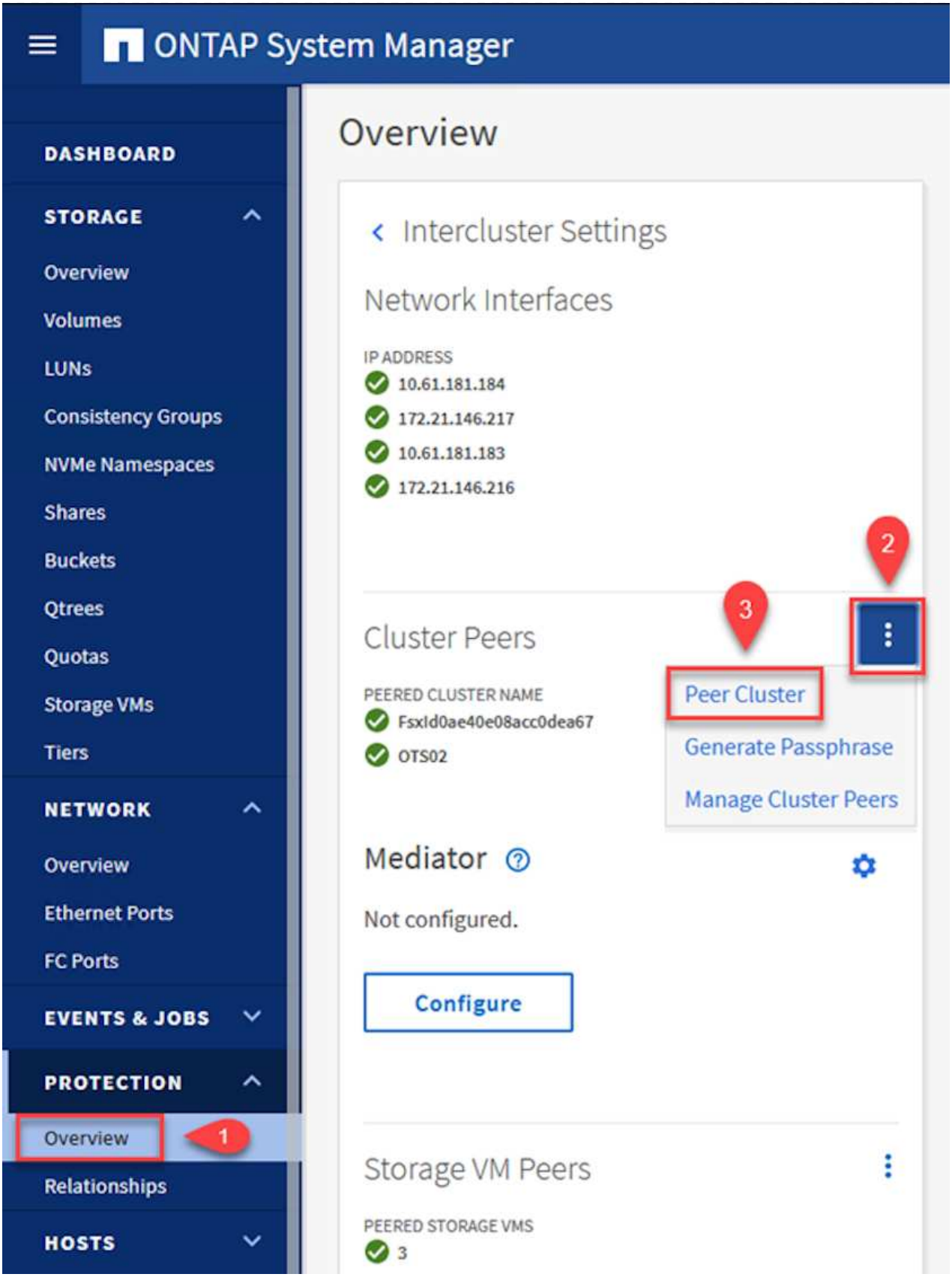
Cluster-Peering zwischen ONTAP Clustern einrichten

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 Peering auf dem Ziel-ONTAP-Cluster mit 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.

```
ONTAP-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.

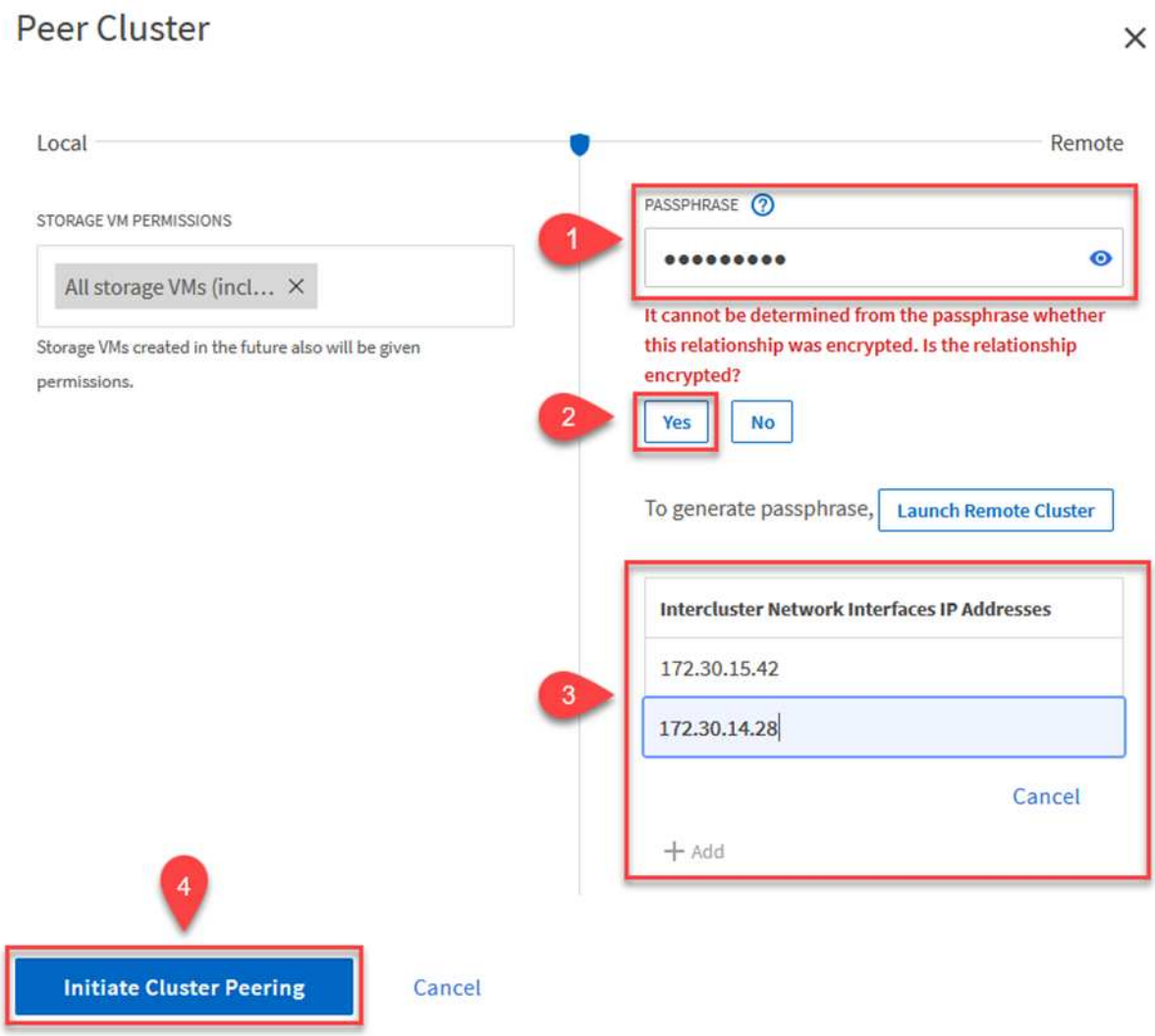


3. Füllen Sie im Dialogfeld Peer Cluster die erforderlichen Informationen aus:
   a. Geben Sie die Passphrase ein, um die Peer-Cluster-Beziehung auf dem Ziel-ONTAP-Cluster herzustellen.

b. Wählen Sie `Yes` Um eine verschlüsselte Beziehung aufzubauen.

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

d. Klicken Sie auf Cluster Peering initiieren, um den Prozess abzuschließen.



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

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

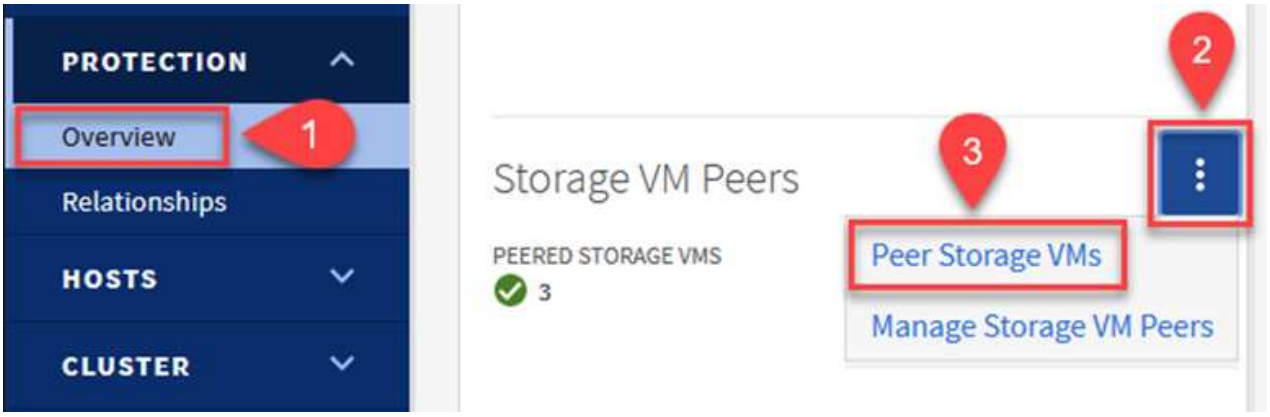
SVM-Peering-Beziehung einrichten

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.

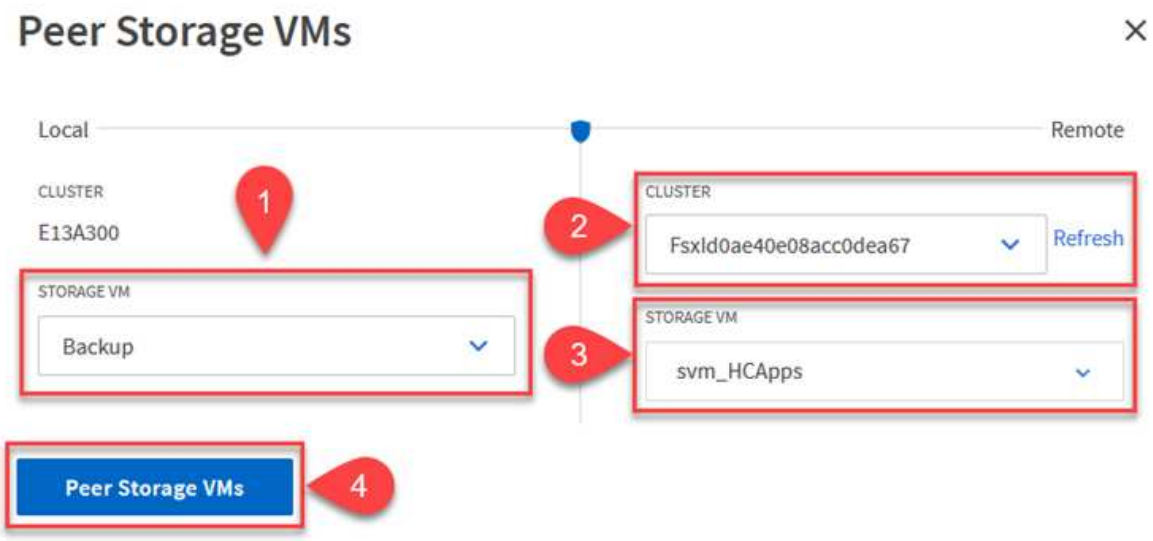
1. Verwenden Sie aus dem ONTAP-Zielcluster den folgenden Befehl in der CLI, um die SVM-Peer-Beziehung zu erstellen:

```
ONTAP-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.

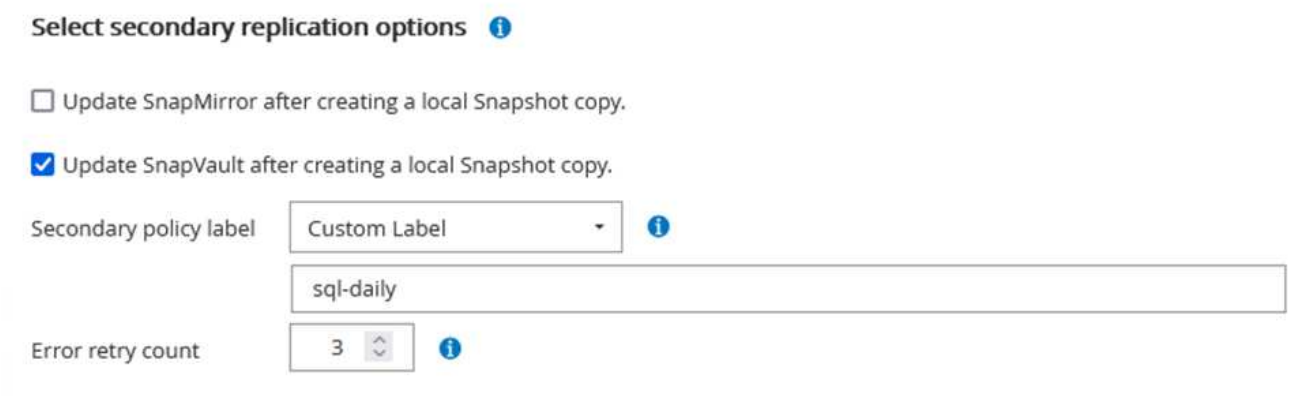
Erstellen einer Snapshot Aufbewahrungsrichtlinie

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.

```
ONTAP-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.

```
ONTAP-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:

```
ONTAP-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

Um ein Ziel-Volume auf ONTAP zu erstellen, das der Empfänger von Snapshot-Kopien aus unseren Quell-Volumes sein wird, führen Sie den folgenden Befehl auf dem Ziel-ONTAP-Cluster aus:

```
ONTAP-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 dem Ziel-ONTAP-Cluster aus, um eine SnapMirror Beziehung zwischen einem Quell- und Ziel-Volume zu erstellen:

```
ONTAP-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.

Führen Sie zum Erstellen eines Volumes den folgenden Befehl auf dem ONTAP-Zielcluster aus:

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

Konfigurieren Sie das SnapCenter-Plug-in für VMware vSphere

Nach der Installation kann das SnapCenter-Plug-in für VMware vSphere über die vCenter Server Appliance Management-Schnittstelle aufgerufen werden. SCV verwaltet Backups für die NFS-Datastores, die auf den ESXi-Hosts gemountet sind und die die Windows- und Linux-VMs enthalten.

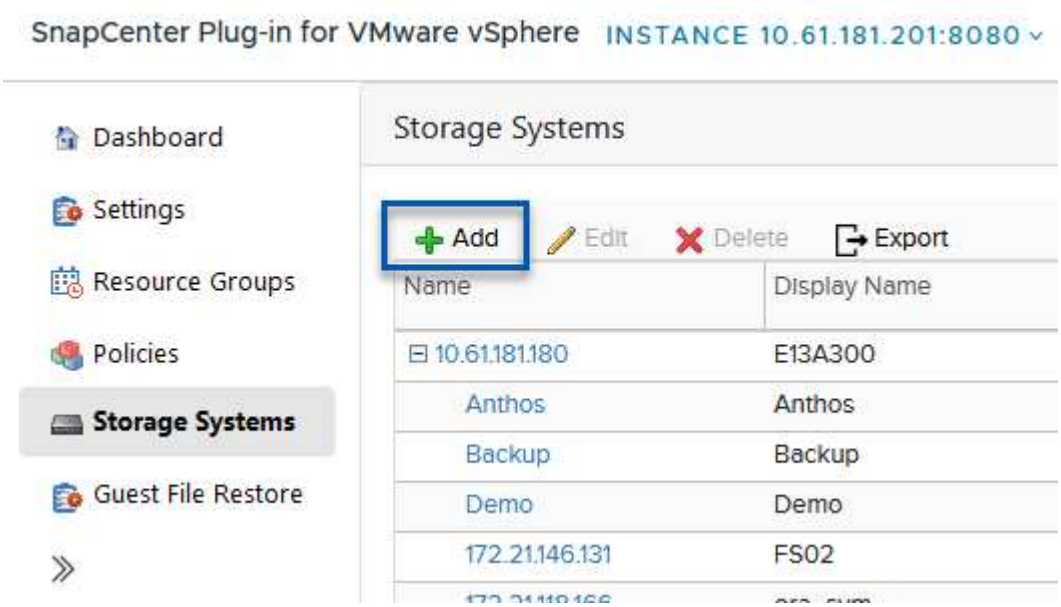
Überprüfen Sie die "Datensicherungs-Workflow" Abschnitt der SCV-Dokumentation enthält weitere Informationen zu den Schritten, die bei der Konfiguration von Backups erforderlich sind.

Um Backups Ihrer virtuellen Maschinen und Datenspeicher zu konfigurieren, müssen die folgenden Schritte über die Plug-in-Schnittstelle durchgeführt werden.

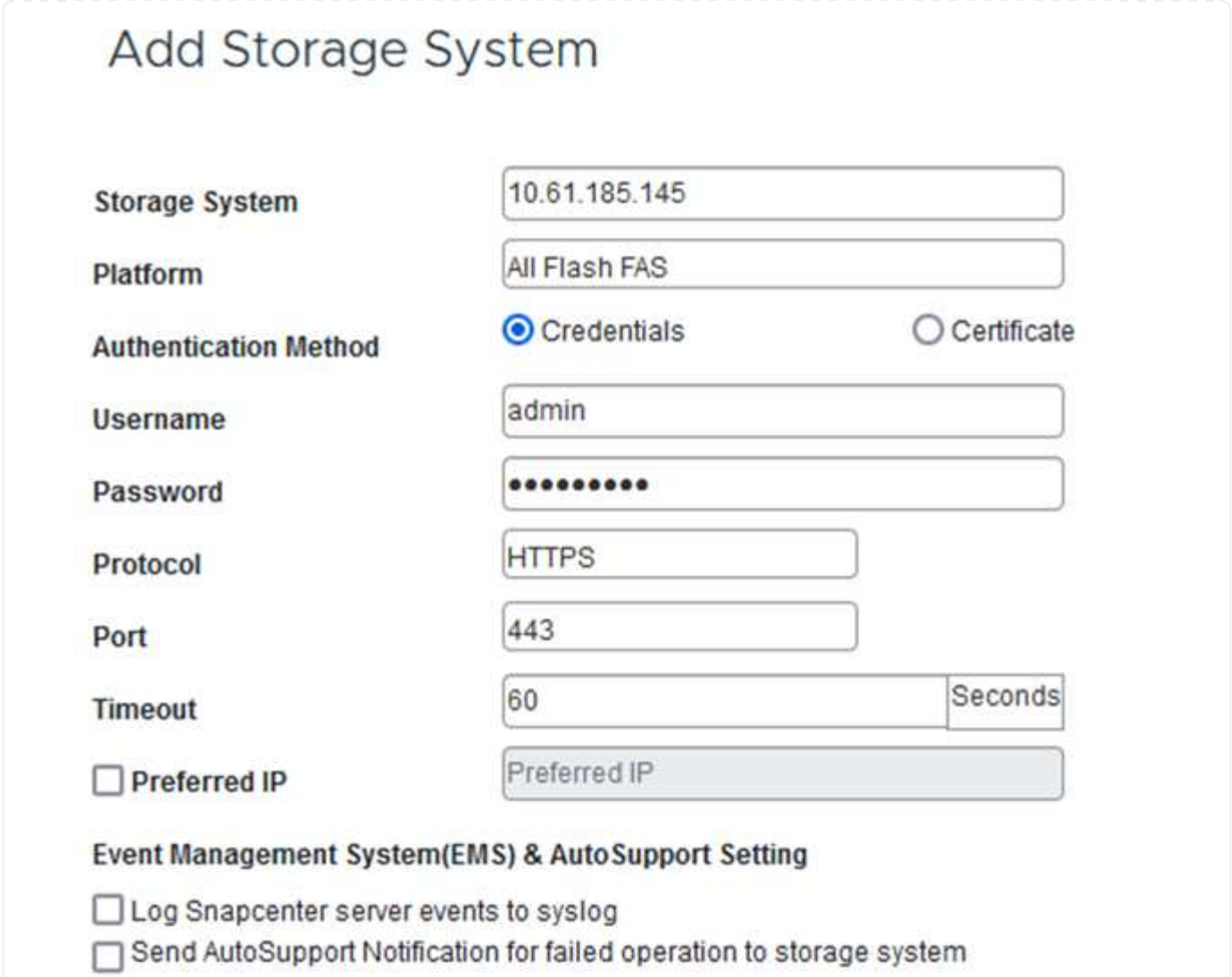
ONTAP Storage-Systeme ermitteln

Die ONTAP Storage-Cluster ermitteln, die für primäre und sekundäre Backups verwendet werden können.

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Speichersysteme** und klicken Sie auf die Schaltfläche **Hinzufügen**.



2. Geben Sie die Zugangsdaten und den Plattformtyp für das primäre ONTAP-Speichersystem ein und klicken Sie auf **Hinzufügen**.



3. Wiederholen Sie diesen Vorgang für das sekundäre ONTAP-Speichersystem.

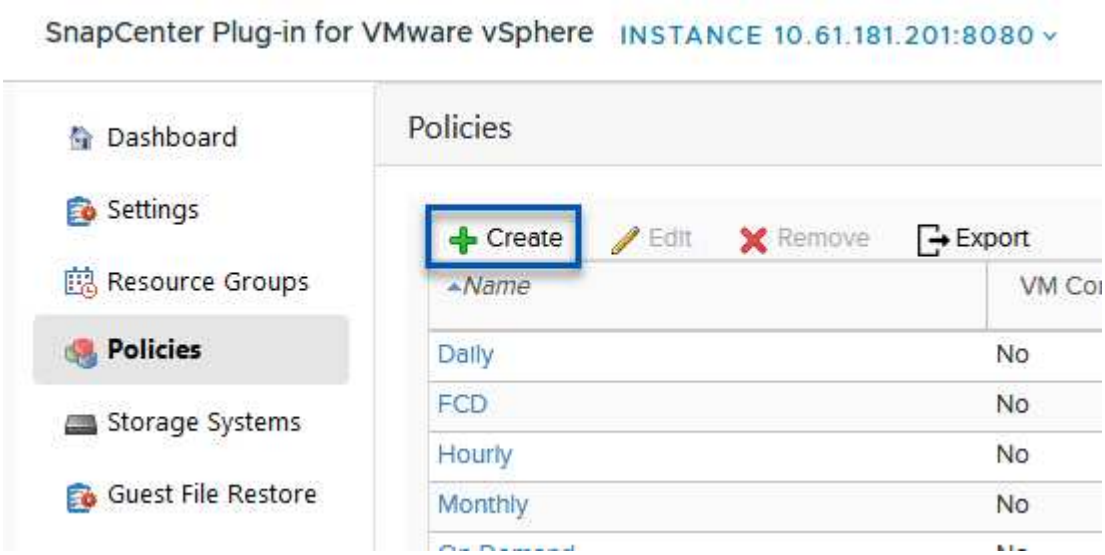
Erstellen Sie SCV-Backup-Richtlinien

Richtlinien legen den Aufbewahrungszeitraum, die Häufigkeit und die Replikationsoptionen für die von SCV verwalteten Backups fest.

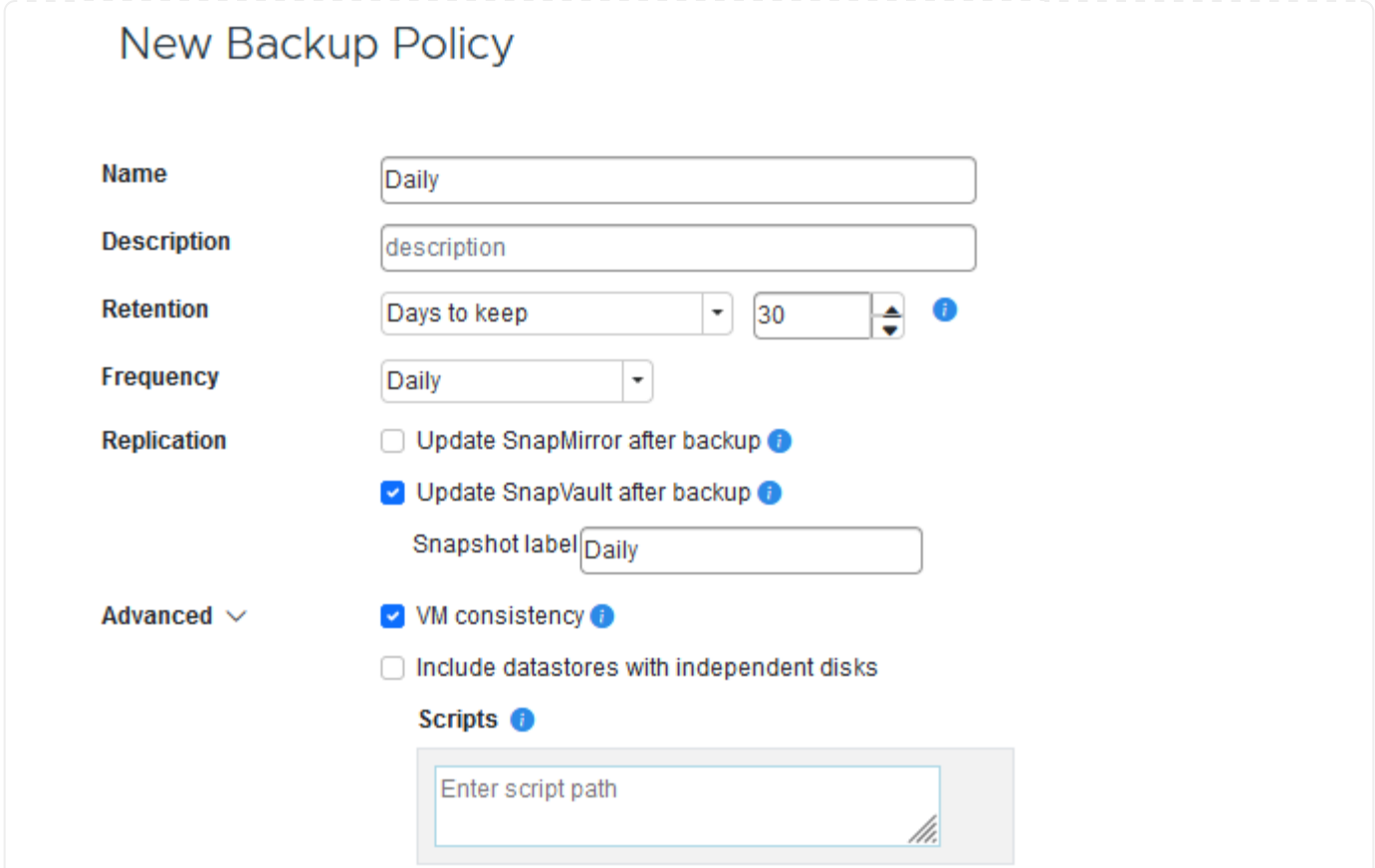
Überprüfen Sie die "Erstellen von Backup-Richtlinien für VMs und Datastores" Weitere Informationen finden Sie in der Dokumentation.

Führen Sie die folgenden Schritte aus, um Backup-Richtlinien zu erstellen:

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Richtlinien** und klicken Sie auf die Schaltfläche **Erstellen**.



2. Geben Sie einen Namen für die Richtlinie, den Aufbewahrungszeitraum, die Häufigkeit und die Replikationsoptionen sowie die Snapshot-Bezeichnung an.



Beim Erstellen einer Richtlinie im SnapCenter-Plug-in werden Optionen für SnapMirror und SnapVault angezeigt. Wenn Sie SnapMirror wählen, ist der in der Richtlinie angegebene Zeitplan für die Aufbewahrung sowohl für die primären als auch für die sekundären Snapshots identisch. Wenn Sie SnapVault wählen, wird der Aufbewahrungszeitplan für den sekundären Snapshot auf einem separaten Zeitplan basieren, der mit der SnapMirror Beziehung implementiert wurde. Dies ist nützlich, wenn Sie längere Aufbewahrungsfristen für sekundäre Backups wünschen.

Snapshot-Labels sind nützlich, da sie verwendet werden können, um Richtlinien mit einem bestimmten Aufbewahrungszeitraum für die SnapVault Kopien, die auf das sekundäre ONTAP Cluster repliziert werden, durchzuführen. Wenn SCV in Verbindung mit BlueXP Backup und Restore verwendet wird, muss das Feld „Snapshot“ entweder leer sein oder match das in der BlueXP Backup-Richtlinie angegebene Label aufweisen.

3. Wiederholen Sie das Verfahren für jede Richtlinie. Zum Beispiel separate Richtlinien für tägliche, wöchentliche und monatliche Backups.

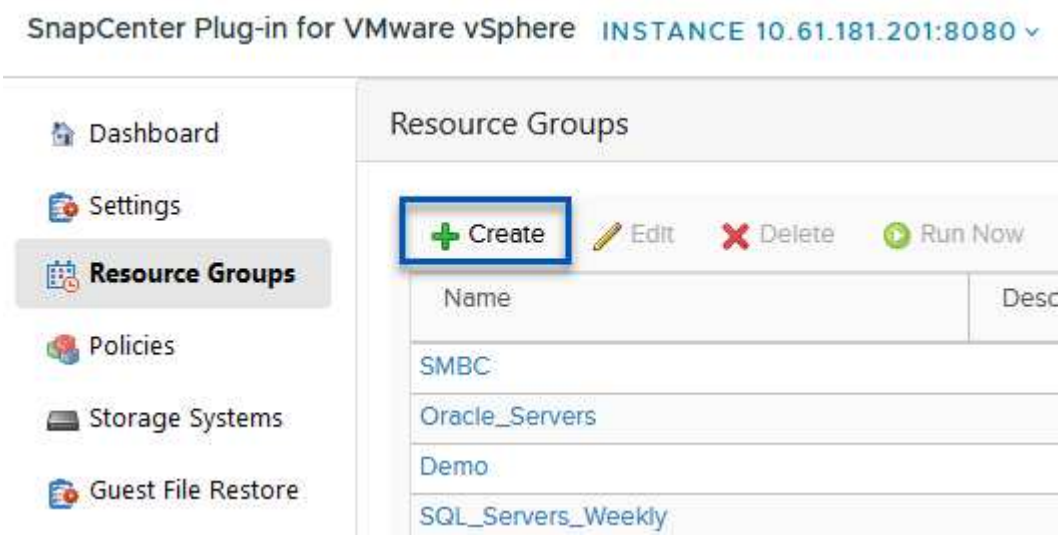
Erstellen von Ressourcengruppen

Ressourcengruppen enthalten die Datastores und virtuellen Maschinen, die in einen Backup-Job aufgenommen werden sollen, sowie die zugehörige Richtlinie und den Backup-Zeitplan.

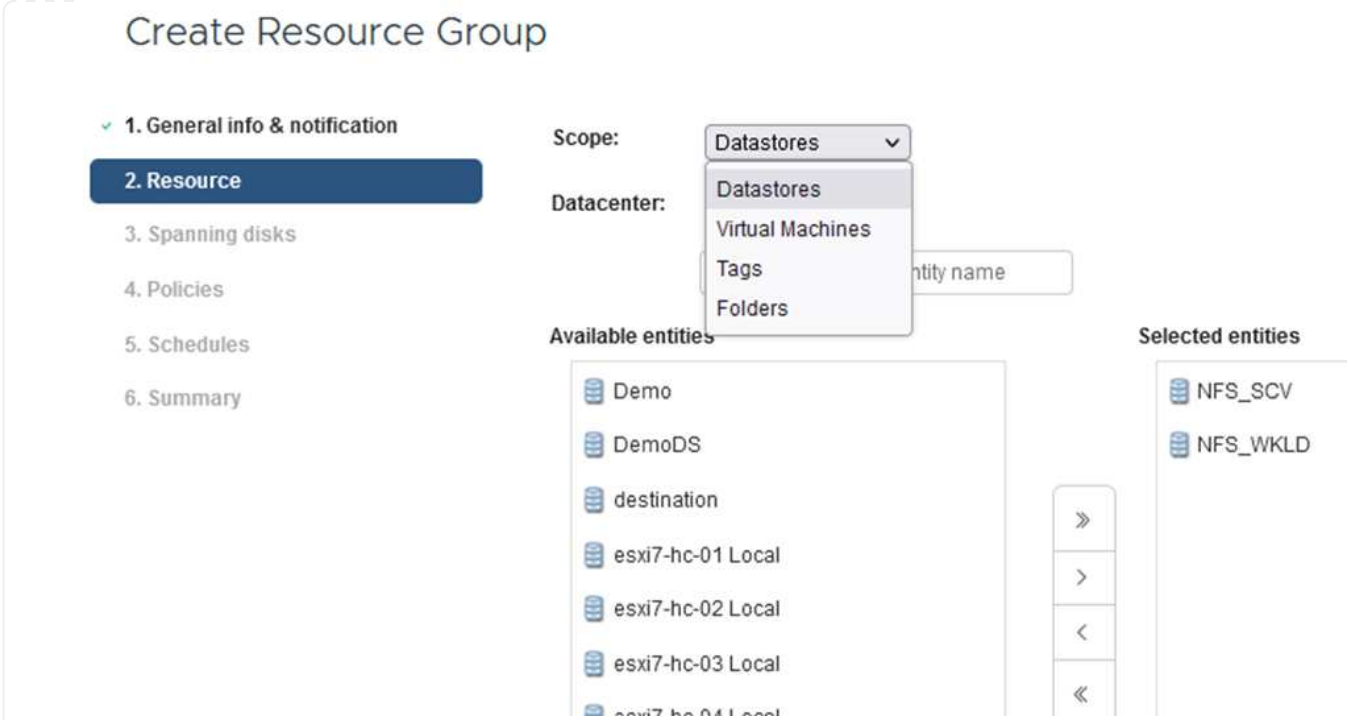
Überprüfen Sie die "Erstellen von Ressourcengruppen" Weitere Informationen finden Sie in der Dokumentation.

Führen Sie die folgenden Schritte aus, um Ressourcengruppen zu erstellen.

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Ressourcengruppen** und klicken Sie auf die Schaltfläche **Erstellen**.

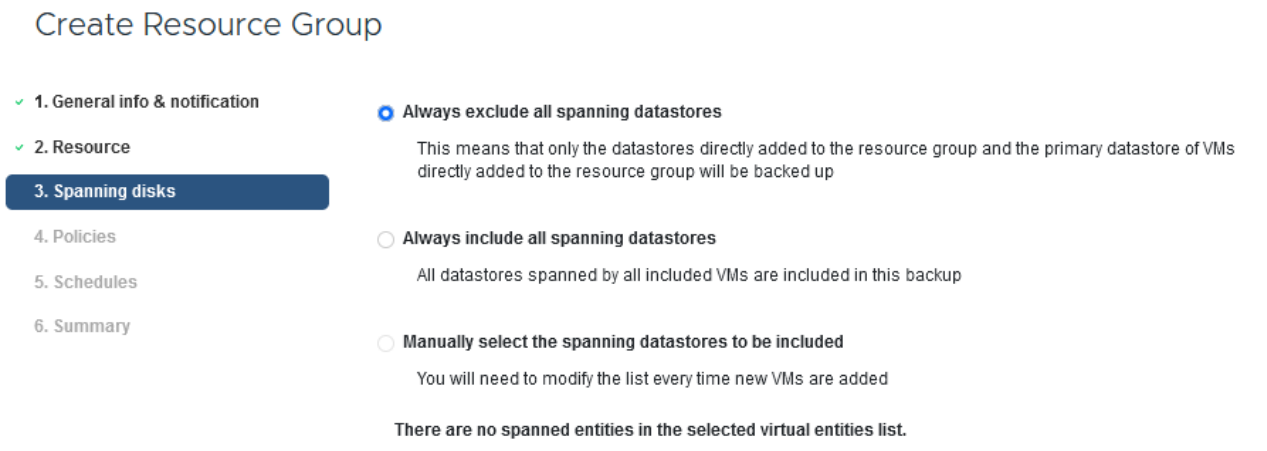


2. Geben Sie im Assistenten Ressourcengruppe erstellen einen Namen und eine Beschreibung für die Gruppe sowie Informationen ein, die für den Empfang von Benachrichtigungen erforderlich sind. Klicken Sie auf **Weiter**
3. Wählen Sie auf der nächsten Seite die Datastores und virtuellen Maschinen aus, die in den Backup-Job aufgenommen werden sollen, und klicken Sie dann auf **Weiter**.



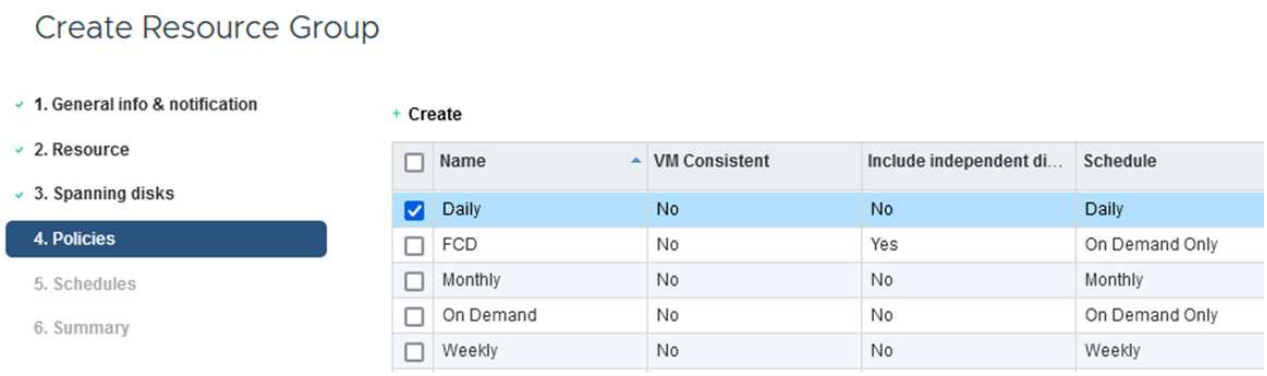
Es besteht die Möglichkeit, spezifische VMs oder vollständige Datastores auszuwählen. Unabhängig davon, welchen Sie wählen, wird das gesamte Volume (und Datastore) gesichert, da der Backup das Ergebnis der Erstellung eines Snapshots des zugrunde liegenden Volumes ist. In den meisten Fällen ist es am einfachsten, den gesamten Datastore auszuwählen. Wenn Sie jedoch beim Wiederherstellen die Liste der verfügbaren VMs begrenzen möchten, können Sie nur eine Teilmenge der VMs für das Backup auswählen.

4. Wählen Sie Optionen für das Spanning von Datastores für VMs mit VMDKs, die sich auf mehreren Datastores befinden, und klicken Sie dann auf **Weiter**.



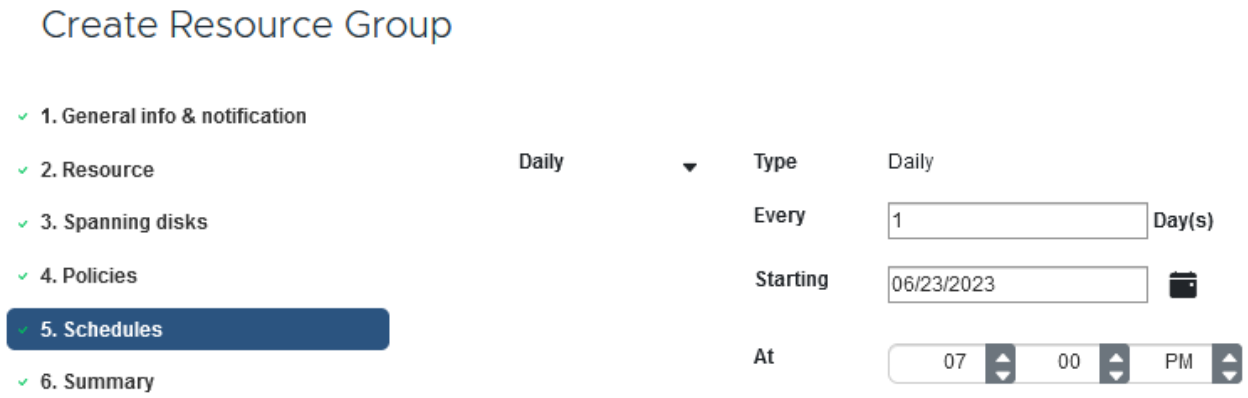
BlueXP Backup und Recovery unterstützt derzeit nicht die Sicherung von VMs mit VMDKs, die mehrere Datastores umfassen.

5. Wählen Sie auf der nächsten Seite die Richtlinien aus, die der Ressourcengruppe zugeordnet werden sollen, und klicken Sie auf **Weiter**.



Beim Backup von über SCV gemanagten Snapshots in Objektspeicher mithilfe von BlueXP Backup und Recovery kann jede Ressourcengruppe nur einer einzigen Richtlinie zugeordnet werden.

6. Wählen Sie einen Zeitplan aus, der bestimmt, zu welchem Zeitpunkt die Backups ausgeführt werden. Klicken Sie auf **Weiter**.

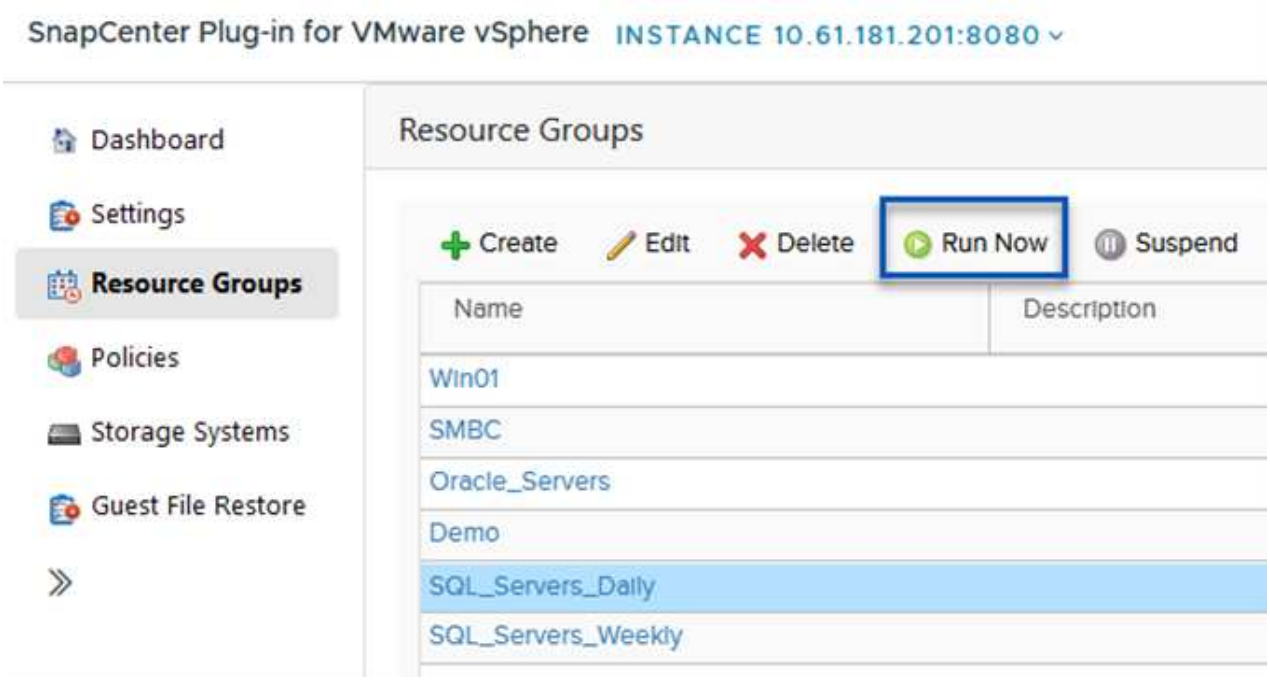


7. Überprüfen Sie abschließend die Übersichtsseite und dann auf **Finish**, um die Erstellung der Ressourcengruppe abzuschließen.

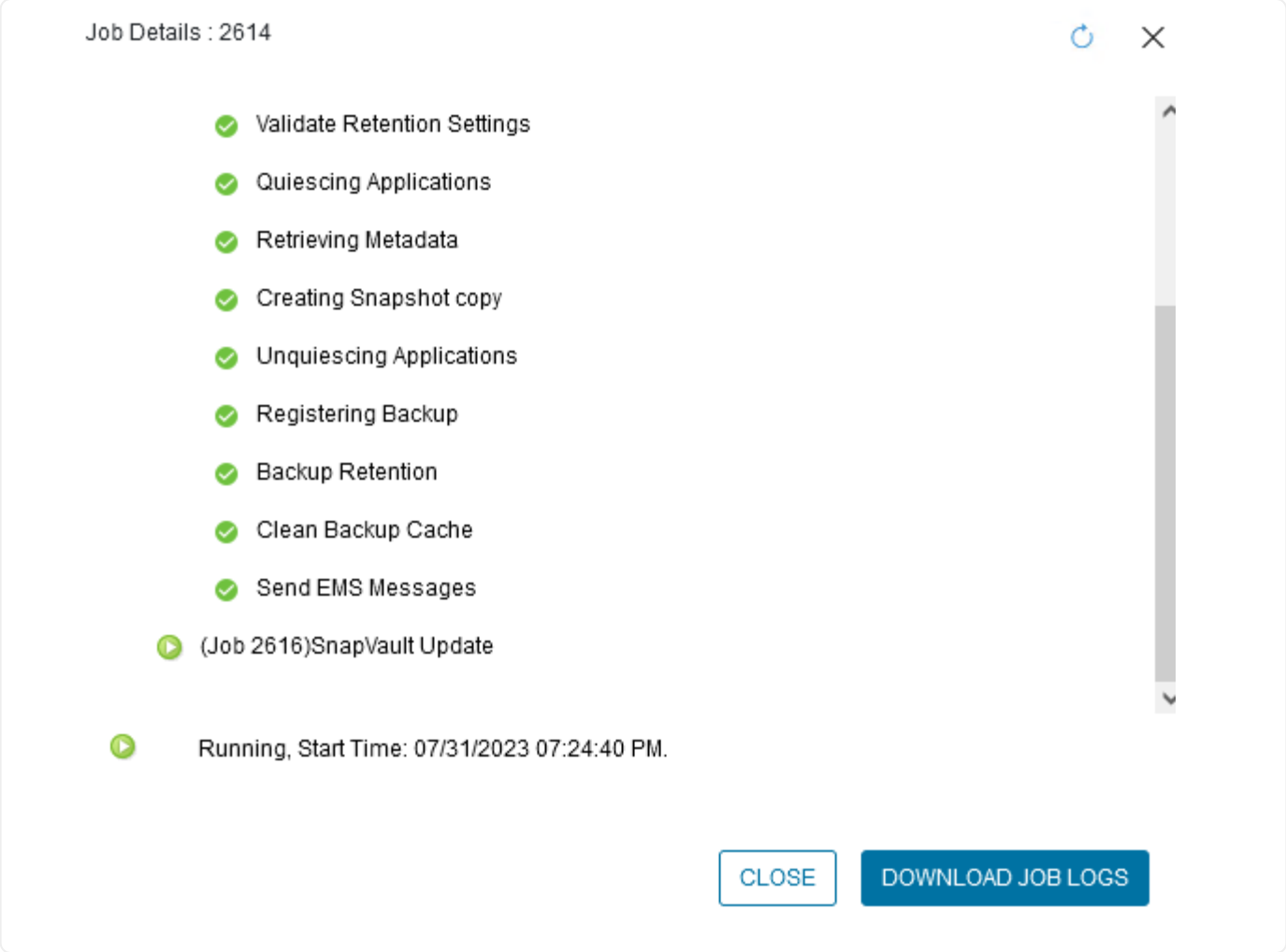
Führen Sie einen Backupjob aus

Führen Sie in diesem letzten Schritt einen Backupjob aus und überwachen Sie dessen Fortschritt. Mindestens ein Backup-Job muss in SCV erfolgreich abgeschlossen werden, bevor Ressourcen von BlueXP Backup und Recovery erkannt werden können.

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Ressourcengruppen**.
2. Um einen Backup-Job zu starten, wählen Sie die gewünschte Ressourcengruppe aus und klicken Sie auf die Schaltfläche **Jetzt ausführen**.



3. Um den Sicherungsauftrag zu überwachen, navigieren Sie im linken Menü zu **Dashboard**. Klicken Sie unter **Recent Job Activities** auf die Job-ID-Nummer, um den Job-Fortschritt zu überwachen.



Konfigurieren Sie Backups auf Objekt-Storage in BlueXP Backup und Recovery

Damit BlueXP die Dateninfrastruktur effektiv managen kann, ist die vorherige Installation eines Connectors erforderlich. Der Connector führt die Aktionen aus, die für die Erkennung von Ressourcen und das Management von Datenvorgängen erforderlich sind.

Weitere Informationen zu BlueXP Connector finden Sie unter "Erfahren Sie mehr über Steckverbinder" In der BlueXP Dokumentation.

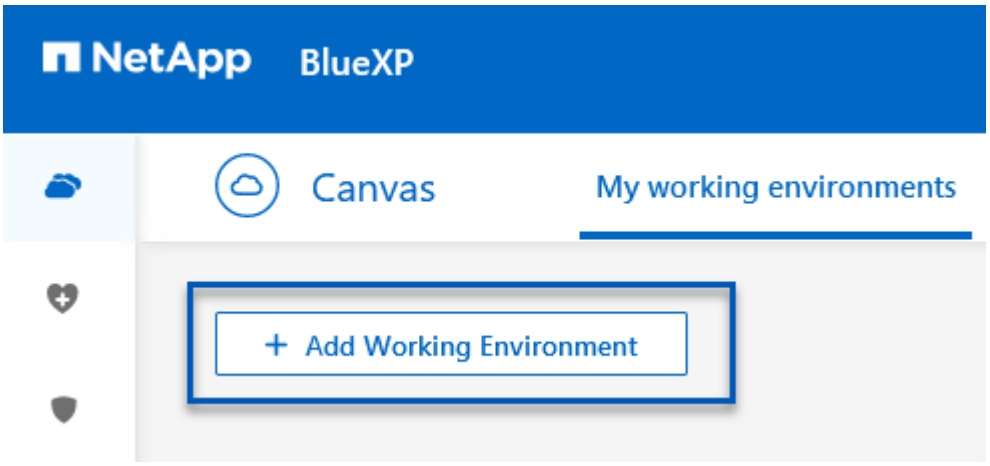
Sobald der Connector für den verwendeten Cloud-Provider installiert ist, wird eine grafische Darstellung des Objektspeichers im Bildschirm angezeigt.

Gehen Sie wie folgt vor, um BlueXP Backup und Recovery für Backup-Daten zu konfigurieren, die durch SCV On-Premises gemanagt werden:

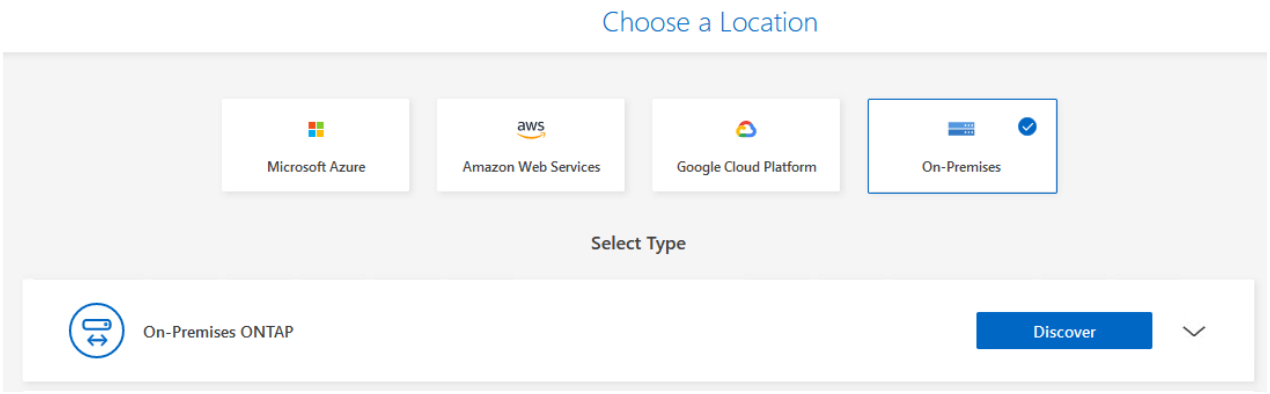
Arbeitsumgebungen zum Bildschirm hinzufügen

In einem ersten Schritt fügen Sie die lokalen ONTAP Storage-Systeme zu BlueXP hinzu

1. Wählen Sie auf dem Bildschirm **Arbeitsumgebung hinzufügen**, um zu beginnen.



2. Wählen Sie **On-Premises** aus der Wahl der Standorte und klicken Sie dann auf die Schaltfläche **Discover**.



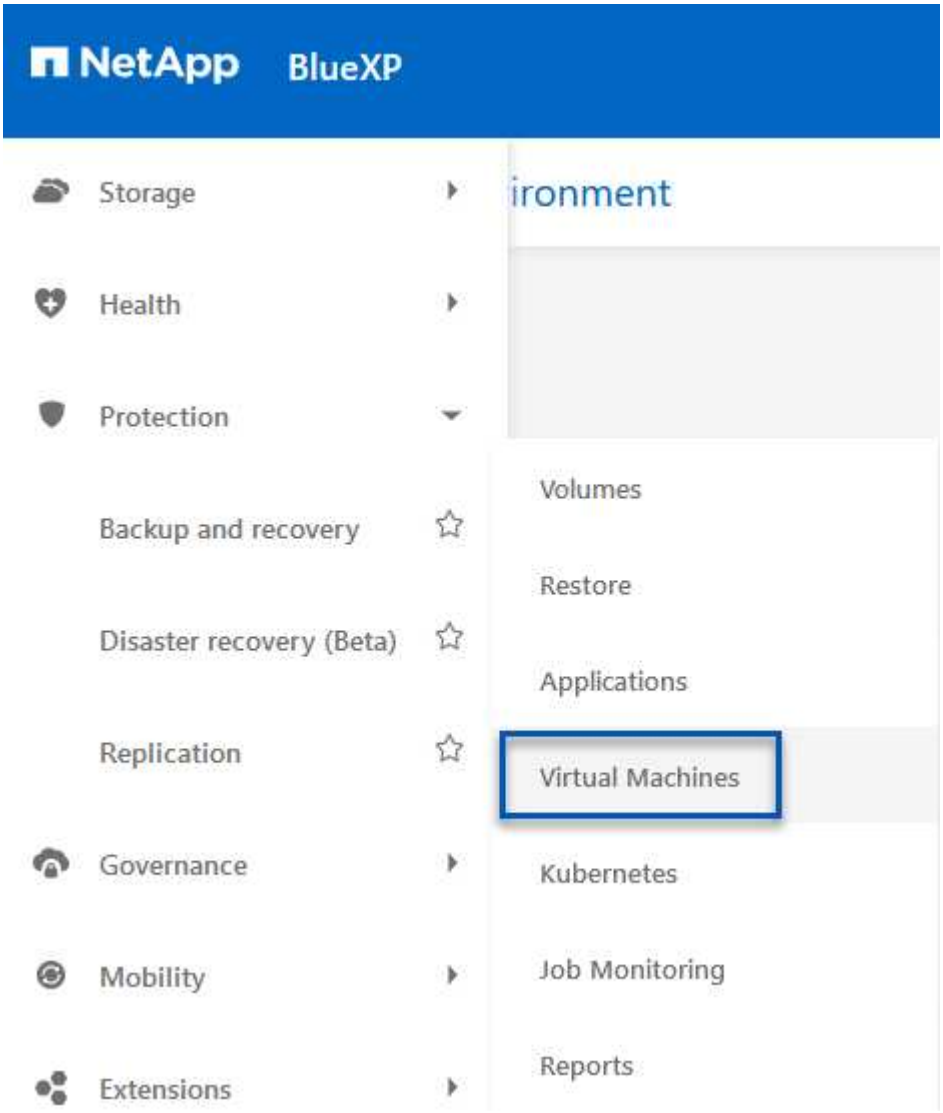
3. Geben Sie die Anmeldeinformationen für das ONTAP-Speichersystem ein, und klicken Sie auf die Schaltfläche **Entdecken**, um die Arbeitsumgebung hinzuzufügen.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

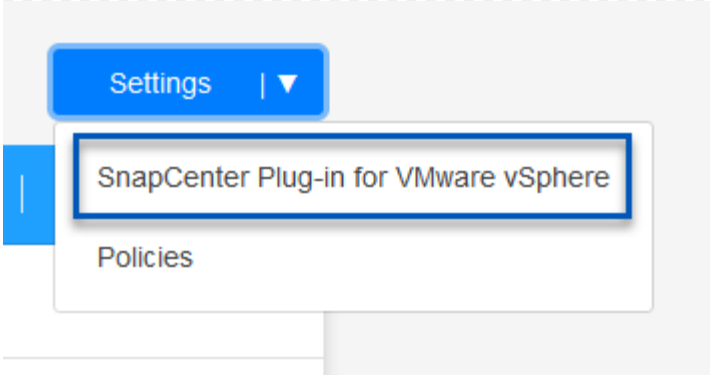
Erkennen Sie lokale SCV-Appliance und vCenter

Um den lokalen Datastore und die Ressourcen der virtuellen Maschine zu ermitteln, fügen Sie Informationen für den SCV-Daten-Broker und Anmeldeinformationen für die vCenter Management-Appliance hinzu.

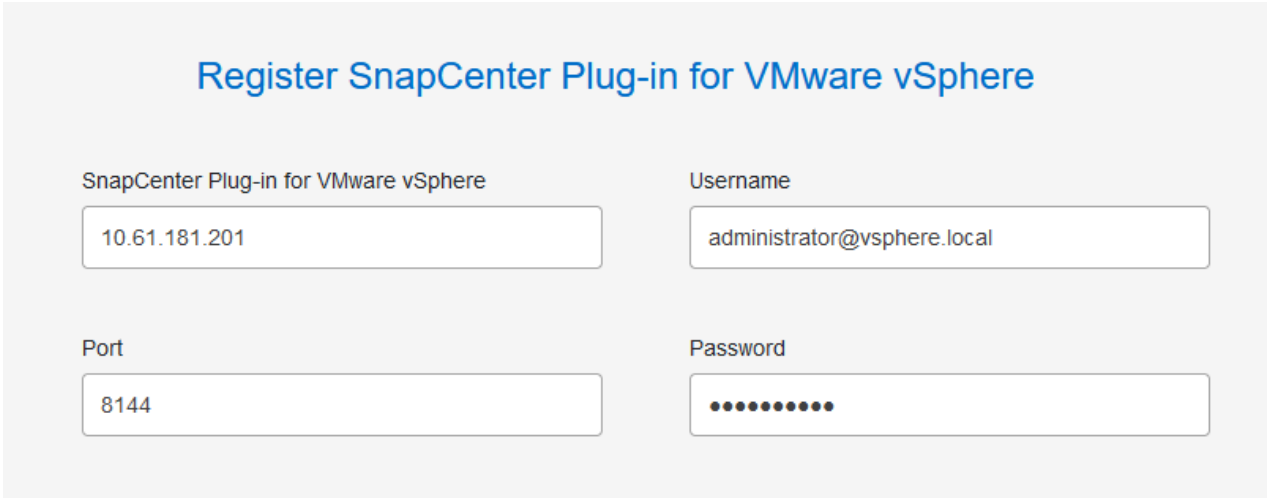
1. Wählen Sie im linken Menü von BlueXP die Option **Schutz > Backup und Recovery > Virtual Machines**



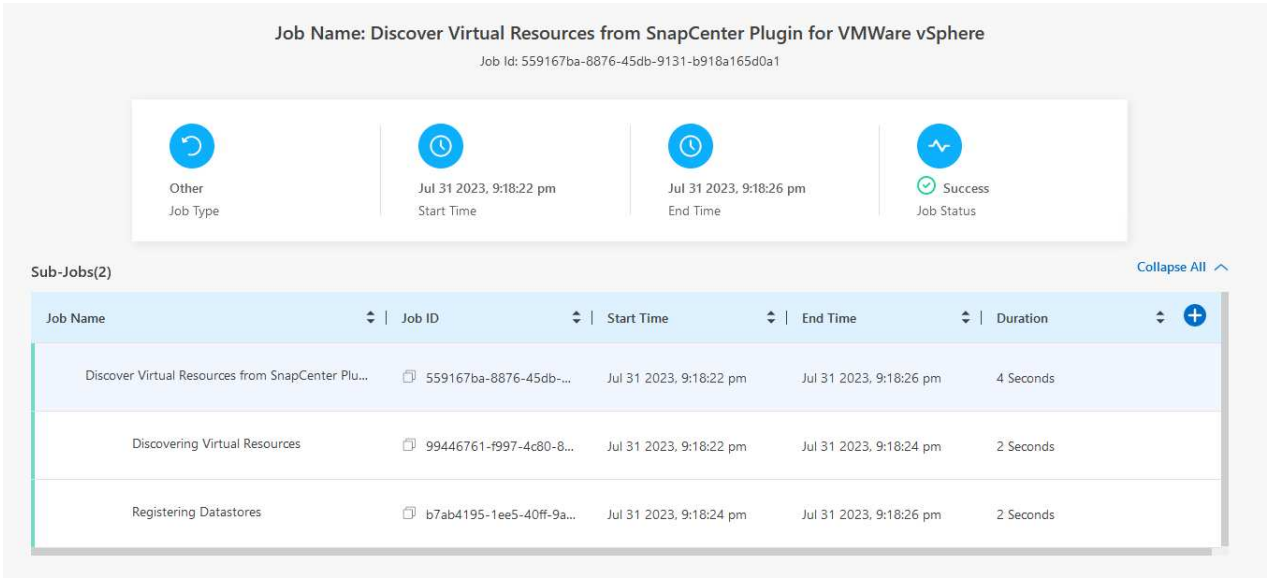
2. Rufen Sie im Hauptbildschirm der virtuellen Maschinen das Dropdown-Menü **Einstellungen** auf und wählen Sie **SnapCenter Plug-in für VMware vSphere**.



3. Klicken Sie auf die Schaltfläche **Registrieren** und geben Sie dann die IP-Adresse und die Portnummer für die SnapCenter-Plug-in-Appliance sowie den Benutzernamen und das Passwort für die vCenter-Management-Appliance ein. Klicken Sie auf die Schaltfläche **Registrieren**, um den Ermittlungsvorgang zu starten.



4. Der Fortschritt von Jobs kann über die Registerkarte Jobüberwachung überwacht werden.



5. Sobald die Erkennung abgeschlossen ist, können Sie die Datenspeicher und virtuellen Maschinen in allen erkannten SCV-Appliances anzeigen.

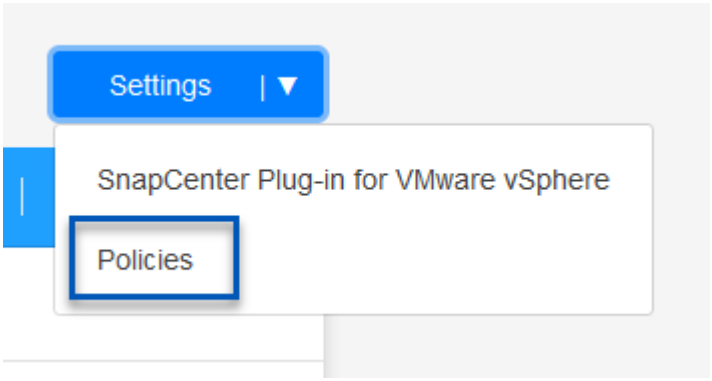
Bild::bxp-scv-Hybrid-23.png[Verfügbare Ressourcen anzeigen]

BlueXP Backup-Richtlinien erstellen

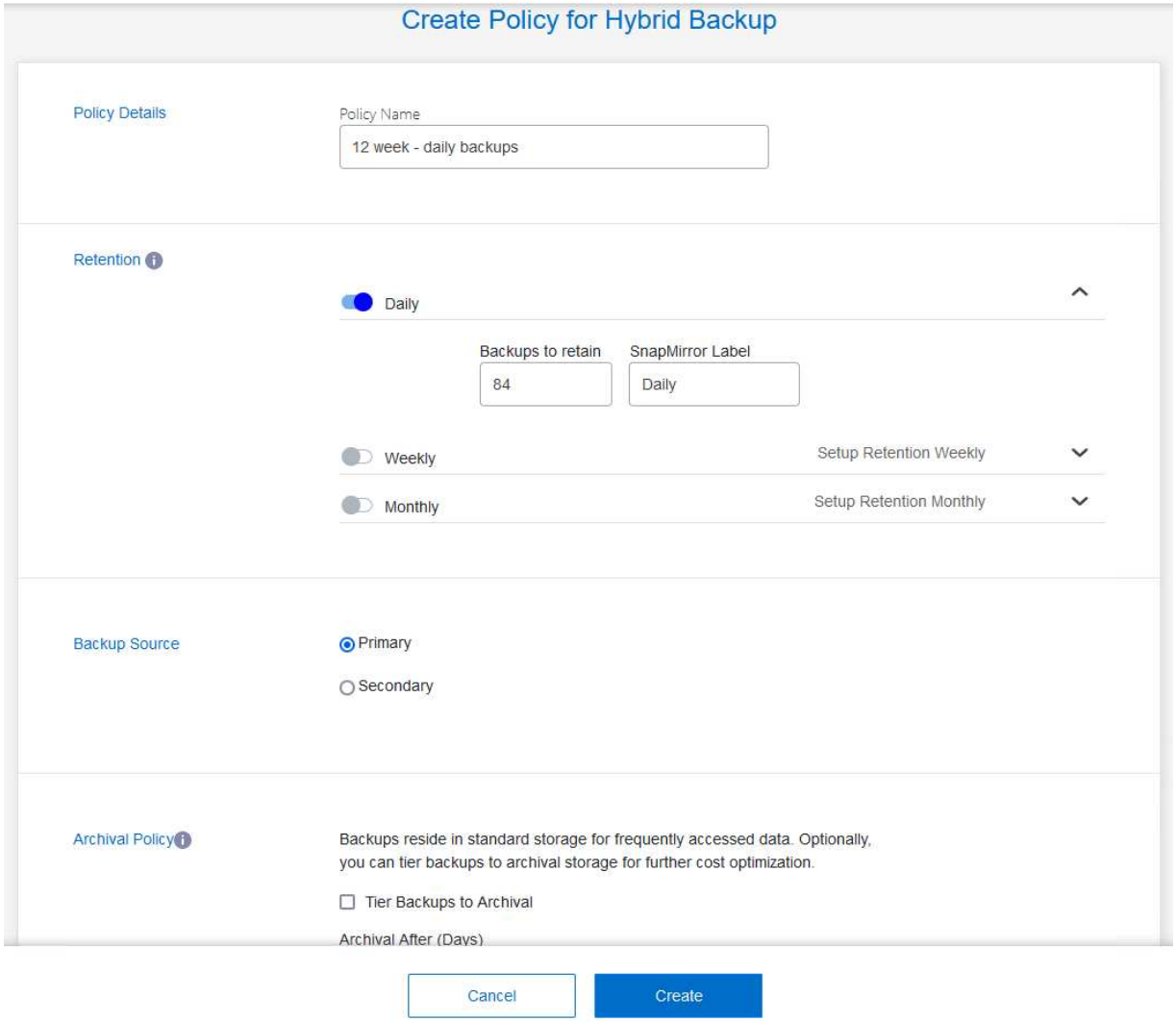
Erstellen Sie in BlueXP Backup und Recovery für Virtual Machines Richtlinien zur Angabe des Aufbewahrungszeitraums, der Backup-Quelle und der Archivierungsrichtlinie.

Weitere Informationen zum Erstellen von Richtlinien finden Sie unter "Erstellen Sie eine Richtlinie zum Backup von Datastores".

1. Rufen Sie auf der Hauptseite von BlueXP Backup und Recovery für virtuelle Maschinen das Dropdown-Menü **Einstellungen** auf und wählen Sie **Richtlinien** aus.



2. Klicken Sie auf **Create Policy**, um auf das Fenster **Create Policy for Hybrid Backup** zuzugreifen.
   a. Fügen Sie einen Namen für die Richtlinie hinzu
   b. Wählen Sie die gewünschte Aufbewahrungsfrist aus
   c. Legen Sie fest, ob Backups vom primären oder sekundären lokalen ONTAP Storage-System bezogen werden
   d. Geben Sie optional an, nach welcher Zeitspanne Backups auf Archiv-Storage verschoben werden sollen, um zusätzliche Kosteneinsparungen zu erzielen.



Das hier eingegebene SnapMirror-Label wird verwendet, um zu ermitteln, welche Backups die Richtlinie auch anwenden sollen. Der Name der Beschriftung muss mit dem Namen der Beschriftung in der entsprechenden On-Premises-SCV-Richtlinie übereinstimmen.

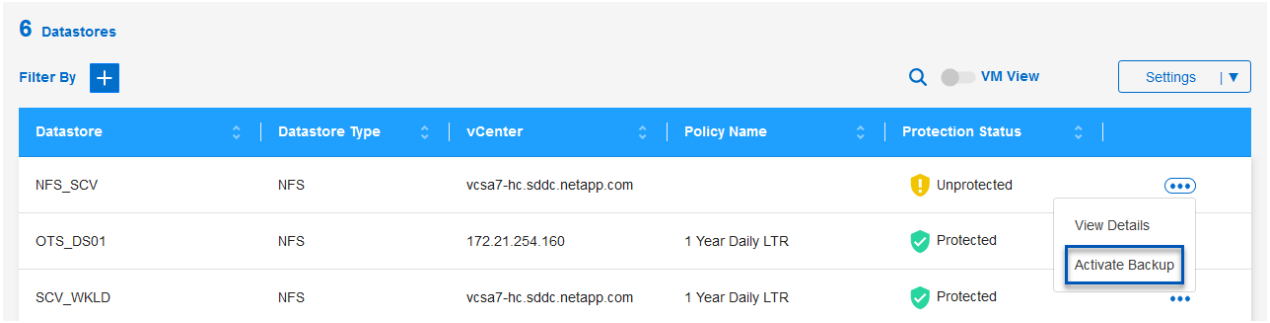
3. Klicken Sie auf **Create**, um die Erstellung der Richtlinie abzuschließen.

Backup von Datastores auf Amazon Web Services

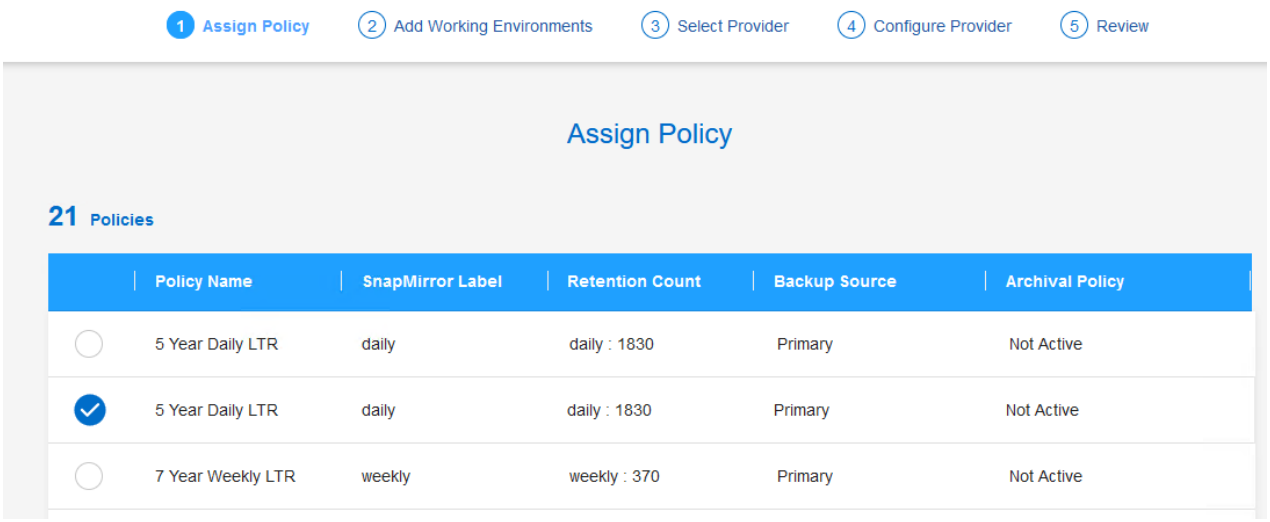
Im letzten Schritt aktivieren Sie die Datensicherung für einzelne Datenspeicher und Virtual Machines. Im folgenden Schritt wird die Aktivierung von Backups auf AWS beschrieben.

Weitere Informationen finden Sie unter "Erstellen Sie Backups von Datastores in Amazon Web Services".

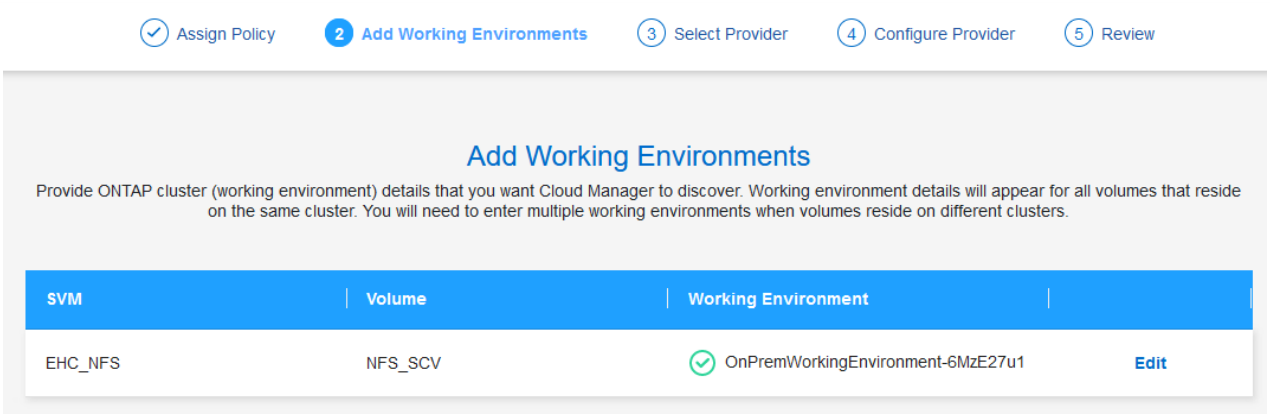
1. Rufen Sie auf der Hauptseite von BlueXP Backup und Recovery für Virtual Machines das Dropdown-Menü Einstellungen für den zu sichernden Datastore auf und wählen Sie **Backup aktivieren** aus.



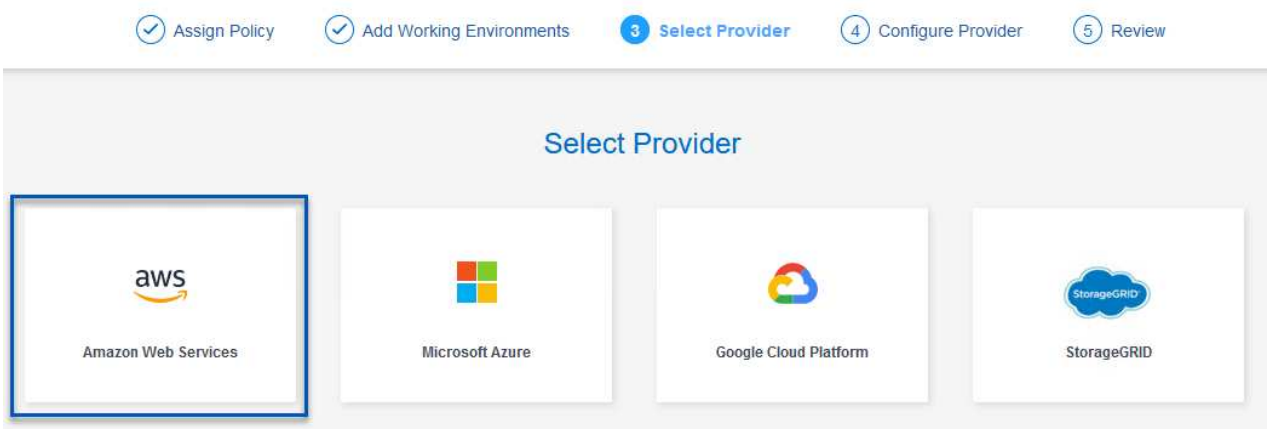
2. Weisen Sie die für den Datenschutzvorgang zu verwendende Richtlinie zu und klicken Sie auf **Weiter**.



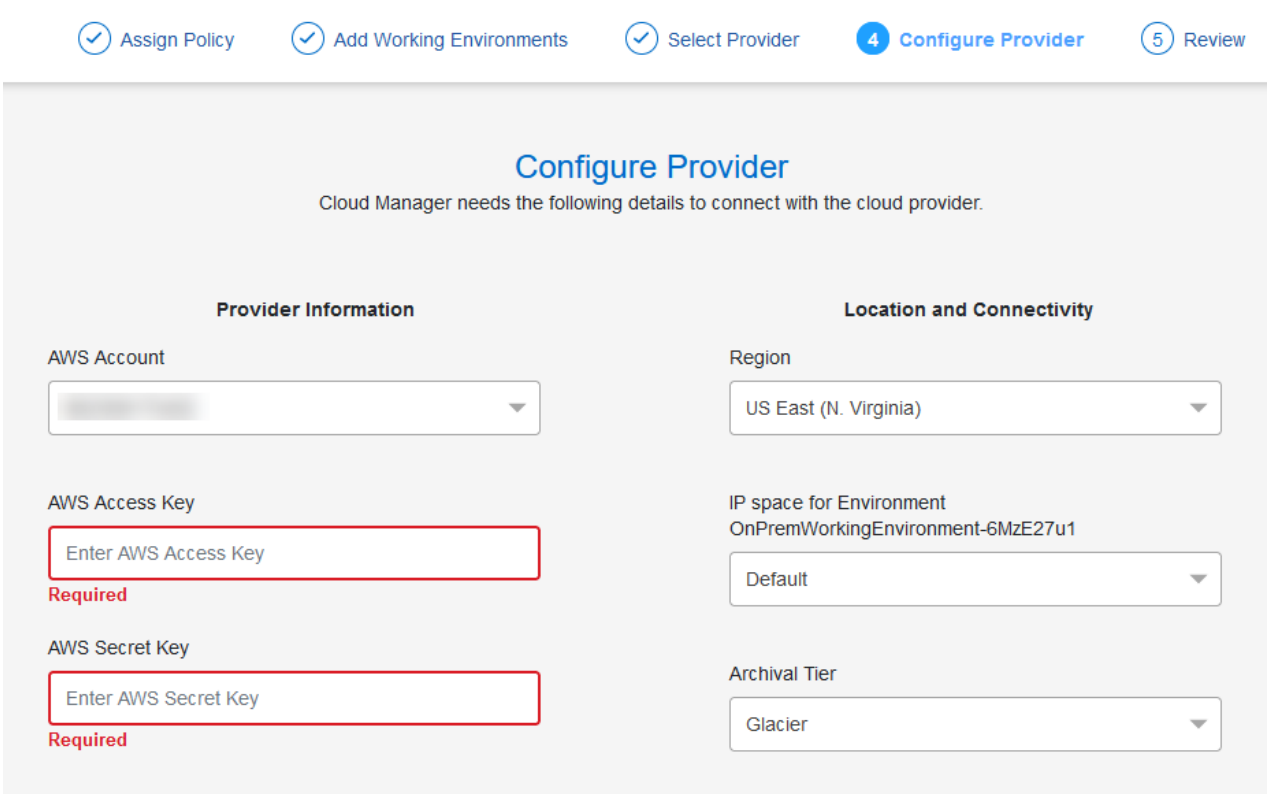
3. Auf der Seite **Add working Environments** sollten der Datastore und die Arbeitsumgebung mit einem Häkchen angezeigt werden, wenn die Arbeitsumgebung zuvor erkannt wurde. Wenn die Arbeitsumgebung noch nicht erkannt wurde, können Sie sie hier hinzufügen. Klicken Sie auf **Weiter**, um fortzufahren.



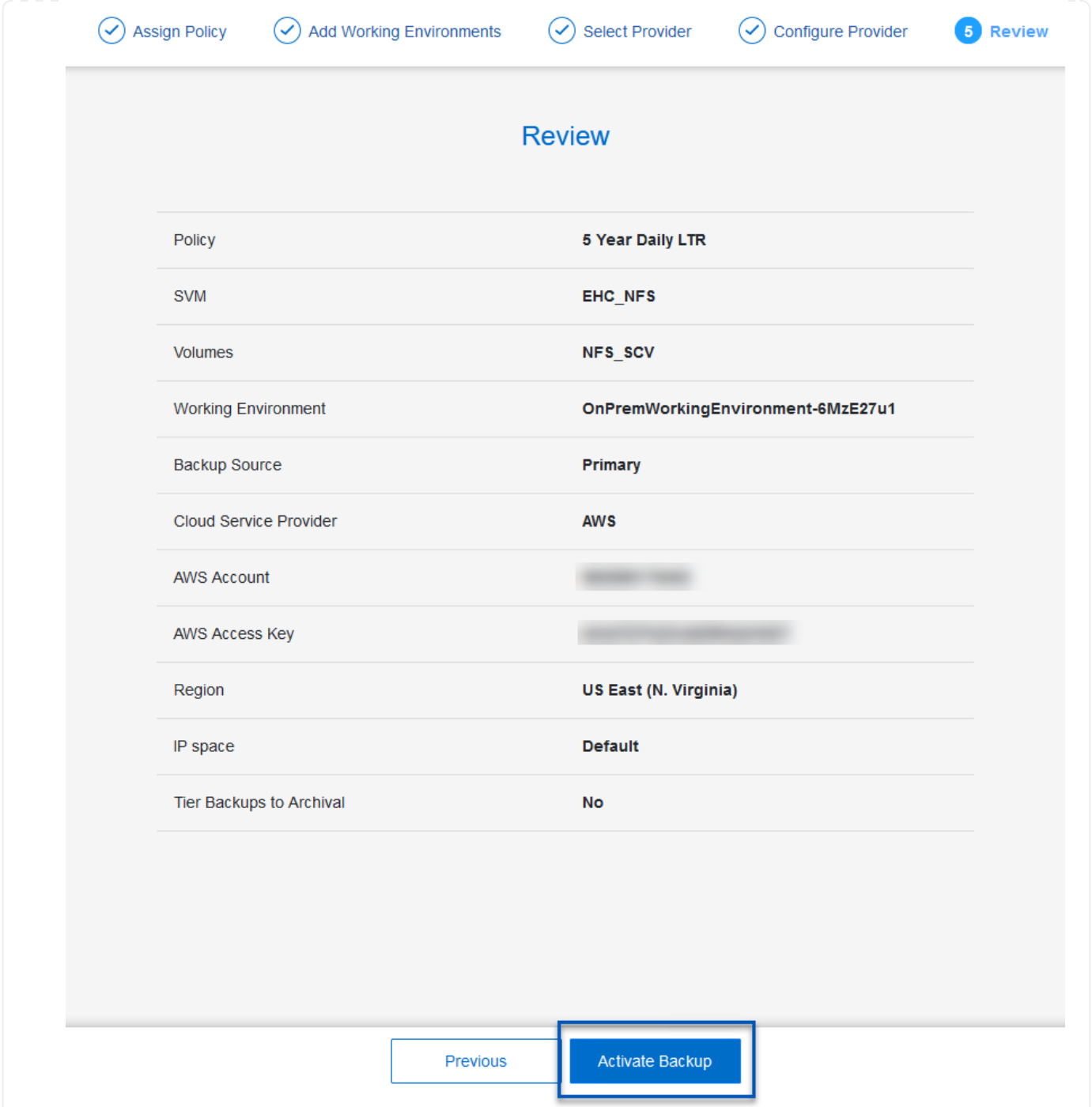
4. Klicken Sie auf der Seite **Select Provider** auf AWS und klicken Sie dann auf die Schaltfläche **Next**, um fortzufahren.



5. Geben Sie die Provider-spezifischen Anmeldeinformationen für AWS an, einschließlich des zu verwendenden AWS Zugriffsschlüssels und des geheimen Schlüssels, der Region und der Archiv-Tier. Wählen Sie außerdem den ONTAP IP-Speicherplatz für das lokale ONTAP Storage-System aus. Klicken Sie auf **Weiter**.



6. Überprüfen Sie abschließend die Details des Backup-Jobs und klicken Sie auf die Schaltfläche **Backup aktivieren**, um den Datenschutz des Datastore zu initiieren.



An diesem Punkt kann die Datenübertragung nicht sofort beginnen. Bei BlueXP Backup und Recovery werden stündlich nach herausragenden Snapshots durchsucht und diese anschließend an den Objekt-Storage übertragen.

Wiederherstellung von Virtual Machines bei Datenverlust

Der Schutz Ihrer Daten zu gewährleisten, ist nur ein Aspekt umfassenden Datenschutzes. Ebenso wichtig ist die Fähigkeit, Daten bei Datenverlust oder Ransomware-Angriffen von jedem Standort aus umgehend wiederherzustellen. Diese Funktion ist von entscheidender Bedeutung für die Aufrechterhaltung eines nahtlosen Geschäftsbetriebs und die Einhaltung von Recovery-Zeitpunkten.

NetApp bietet eine äußerst anpassungsfähige 3-2-1-1-Strategie und bietet individuelle Kontrolle über Aufbewahrungszeitpläne am primären, sekundären und Objekt-Storage. Diese Strategie bietet die Flexibilität, Datensicherungsansätze an spezifische Anforderungen anzupassen.

Dieser Abschnitt bietet einen Überblick über den Datenwiederherstellungsprozess sowohl über das SnapCenter Plug-in für VMware vSphere als auch über das BlueXP Backup und Recovery für Virtual Machines.

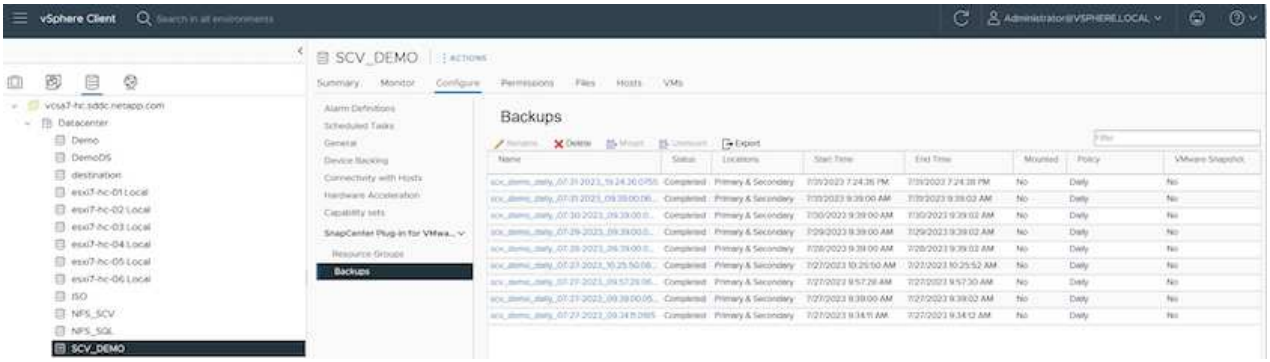
Wiederherstellen virtueller Maschinen aus dem SnapCenter Plug-in für VMware vSphere

Für diese Lösung wurden virtuelle Maschinen an ursprünglichen und alternativen Standorten wiederhergestellt. In dieser Lösung werden nicht alle Aspekte der Datenwiederherstellungsfunktionen von SCV behandelt. Ausführliche Informationen zu allen Angeboten von SCV finden Sie im "Wiederherstellung von VMs aus Backups" In der Produktdokumentation.

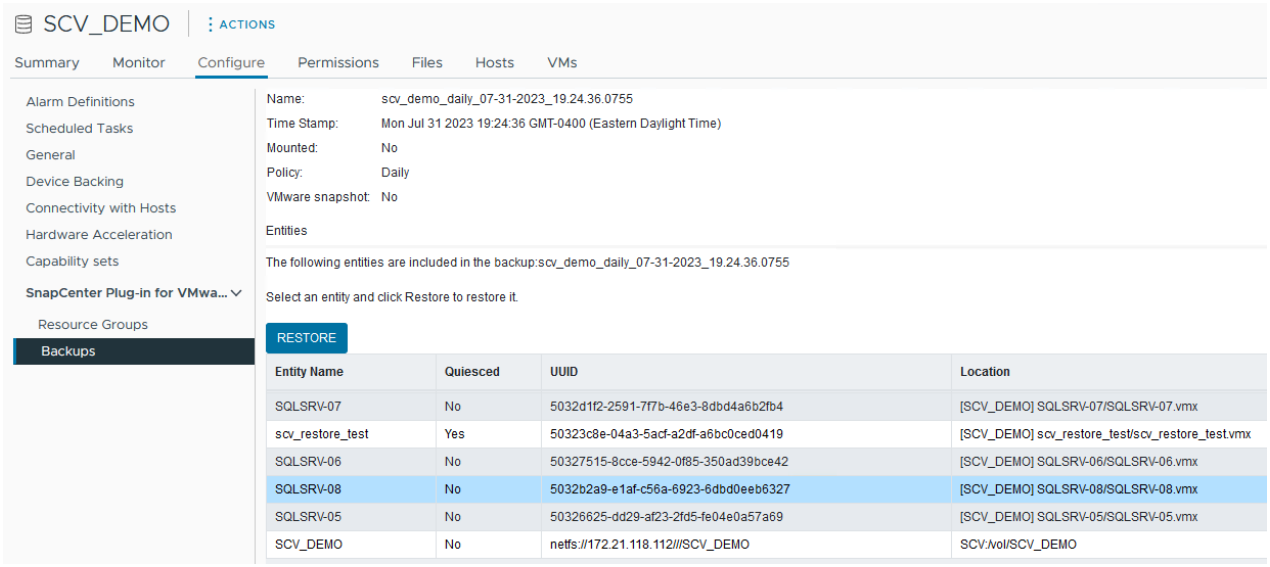
Stellen Sie virtuelle Maschinen über SCV wieder her

Führen Sie die folgenden Schritte aus, um eine VM-Wiederherstellung aus dem primären oder sekundären Speicher wiederherzustellen.

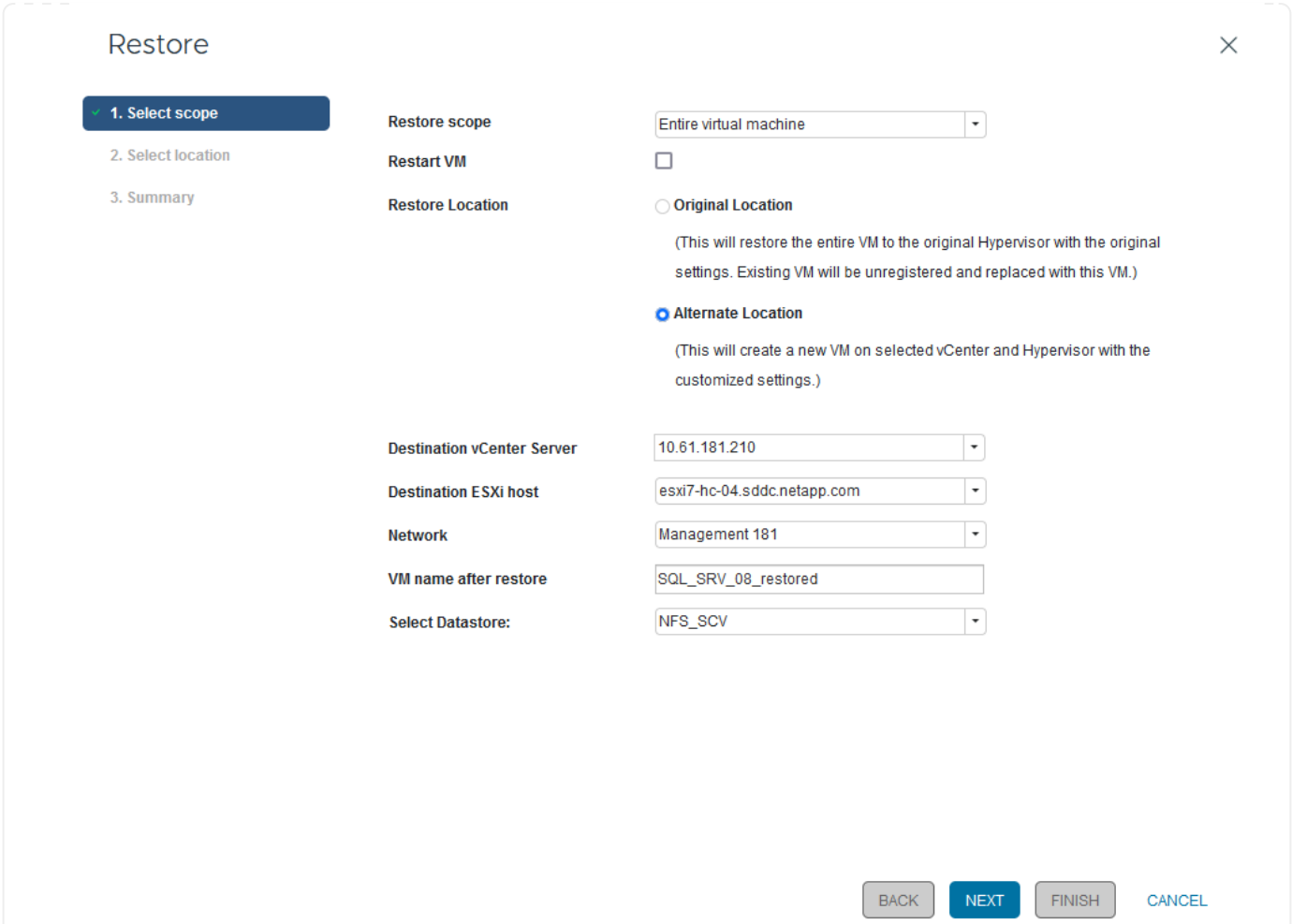
1. Navigieren Sie im vCenter-Client zu **Inventar > Speicher** und klicken Sie auf den Datenspeicher, der die virtuellen Maschinen enthält, die Sie wiederherstellen möchten.
2. Klicken Sie auf der Registerkarte **Configure** auf **Backups**, um die Liste der verfügbaren Backups aufzurufen.



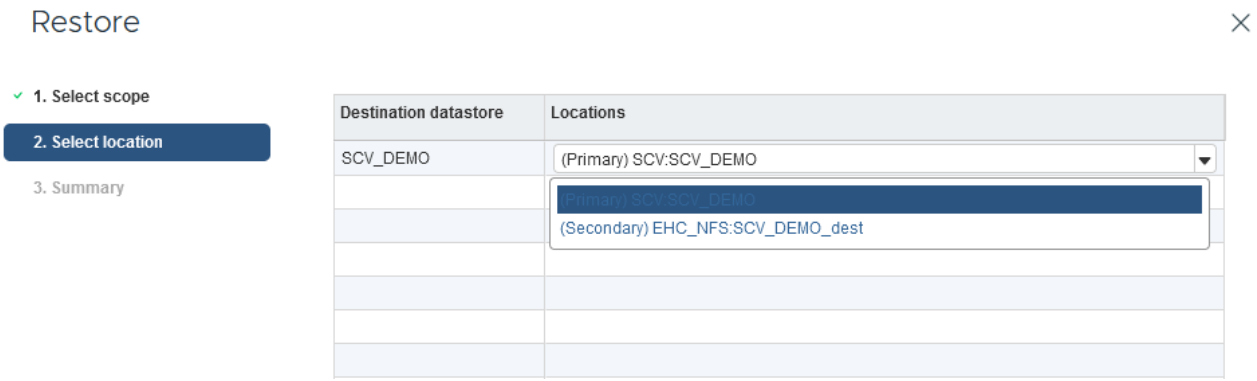
3. Klicken Sie auf ein Backup, um auf die Liste der VMs zuzugreifen, und wählen Sie dann eine wiederherzustellende VM aus. Klicken Sie auf **Wiederherstellen**.



4. Wählen Sie im Wiederherstellungsassistenten aus, um die gesamte virtuelle Maschine oder eine bestimmte VMDK wiederherzustellen. Wählen Sie diese Option aus, um sie am ursprünglichen Speicherort oder an einem alternativen Speicherort zu installieren, geben Sie nach der Wiederherstellung den VM-Namen und den Zieldatenspeicher an. Klicken Sie Auf **Weiter**.



5. Wählen Sie die Option zum Backup vom primären oder sekundären Speicherort aus.



6. Überprüfen Sie abschließend eine Zusammenfassung des Backupjobs, und klicken Sie auf Fertig stellen, um den Wiederherstellungsprozess zu starten.

Wiederherstellung von Virtual Machines aus BlueXP Backup und Recovery für Virtual Machines

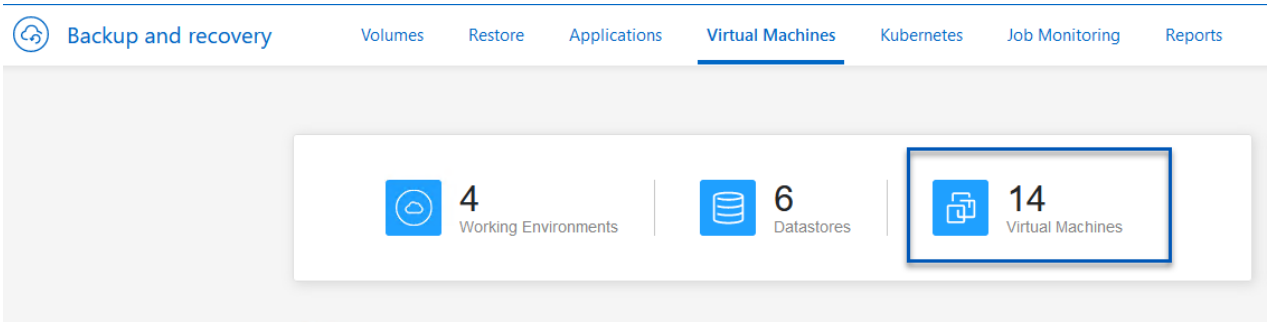
Mit BlueXP Backup und Recovery für Virtual Machines können Virtual Machines an ihrem ursprünglichen Speicherort wiederhergestellt werden. Der Zugriff auf Restore-Funktionen erfolgt über die Web-Konsole von BlueXP.

Weitere Informationen finden Sie unter "Wiederherstellung der Daten von Virtual Machines aus der Cloud".

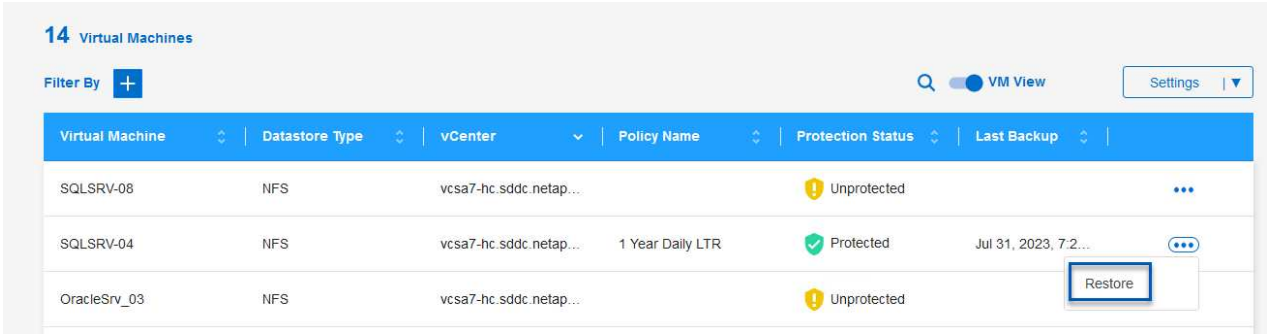
Wiederherstellung von Virtual Machines aus BlueXP Backup und Recovery

Führen Sie die folgenden Schritte aus, um eine Virtual Machine aus dem Backup- und Recovery-Verfahren von BlueXP wiederherzustellen.

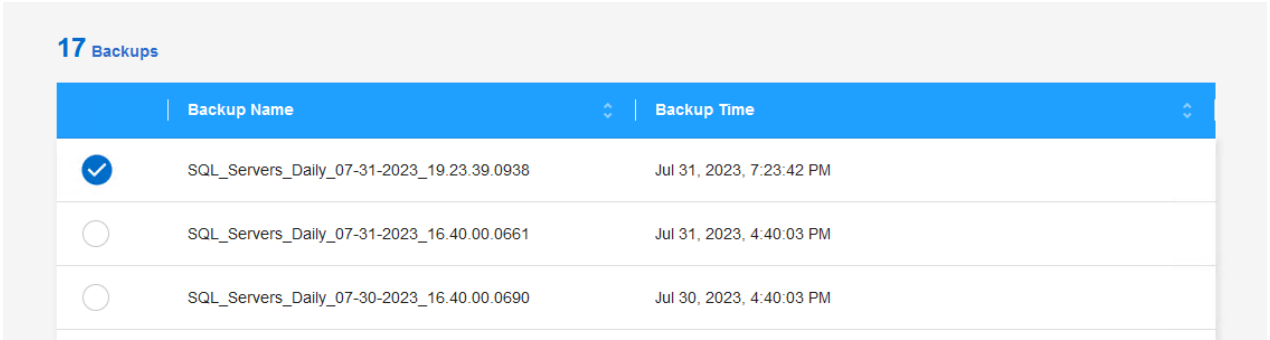
1. Navigieren Sie zu **Schutz > Sicherung und Wiederherstellung > Virtuelle Maschinen** und klicken Sie auf Virtuelle Maschinen, um die Liste der virtuellen Maschinen anzuzeigen, die wiederhergestellt werden können.



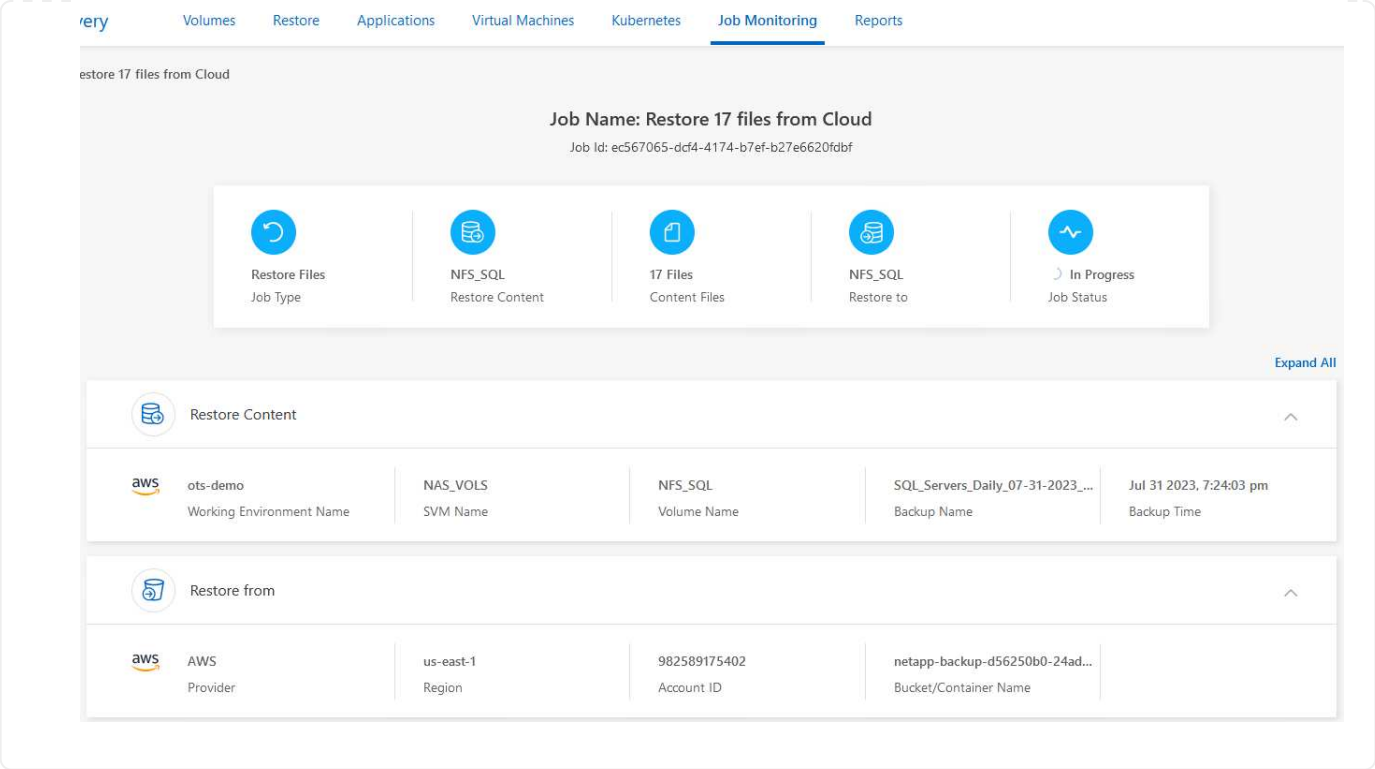
2. Öffnen Sie das Dropdown-Menü Einstellungen für die wiederherzustellende VM, und wählen Sie aus



3. Wählen Sie das zu wiederherstellende Backup aus und klicken Sie auf **Weiter**.



4. Überprüfen Sie eine Zusammenfassung des Backup-Jobs und klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.
5. Überwachen Sie den Fortschritt des Wiederherstellungsjobs über die Registerkarte **Job Monitoring**.



Schlussfolgerung

Die 3-2-1-1-Backup-Strategie nach Implementierung mit dem SnapCenter Plug-in für VMware vSphere und BlueXP Backup- und Recovery-Lösungen für Virtual Machines stellt eine robuste, zuverlässige und kostengünstige Lösung für die Datensicherung dar. Diese Strategie gewährleistet nicht nur Datenredundanz und -Verfügbarkeit, sondern bietet auch die Flexibilität, Daten von jedem Standort aus wiederherzustellen – sowohl aus On-Premises-ONTAP-Storage-Systemen als auch aus Cloud-basiertem Objektspeicher.

Der in dieser Dokumentation präsentierte Anwendungsfall konzentriert sich auf bewährte Datensicherungstechnologien, die die Integration von NetApp, VMware und den führenden Cloud-Providern hervorheben. Das SnapCenter Plug-in für VMware vSphere ermöglicht die nahtlose Integration in VMware vSphere und ermöglicht so ein effizientes und zentralisiertes Management von Datensicherungsvorgängen. Diese Integration optimiert die Backup- und Recovery-Prozesse für Virtual Machines und ermöglicht so einfache Planung, Überwachung und flexible Restore-Vorgänge innerhalb des VMware Ökosystems. BlueXP Backup und Recovery für Virtual Machines bietet das eine (1) in 3-2-1 durch sichere Backups der Daten von Virtual Machines mit Air-Gap-Separierung in Cloud-basiertem Objekt-Storage. Die intuitive Benutzeroberfläche und der logische Workflow bilden eine sichere Plattform für die langfristige Archivierung geschäftskritischer Daten.

Weitere Informationen

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

- "Dokumentation zum SnapCenter Plug-in für VMware vSphere"
- "BlueXP-Dokumentation"

VMware Sovereign Cloud

VMware-Ressourcen für Souveräne Cloud

NetApp und VMware Sovereign Cloud

Überblick über VMware Sovereign Cloud

Das Konzept der Souveränität wird für viele Unternehmen, die hochsensible Daten verarbeiten und pflegen, als notwendige Komponente des Cloud-Computing entwickelt, wie z. B. nationale und staatliche Behörden sowie stark regulierte Branchen wie Finanzen und Gesundheitswesen. Nationale Regierungen wollen außerdem die digitale Wirtschaft erweitern und die Abhängigkeit von multinationalen Unternehmen bei ihren Cloud-Services verringern.

VMware Sovereign Cloud Initiative

VMware definiert eine souveräne Cloud als eine, die:

- Schutz und Freischaltung von wichtigen Daten (z. B. nationale, Unternehmensdaten und personenbezogene Daten) für private und öffentliche Einrichtungen
- Bereitstellung einer nationalen Leistungsfähigkeit für die digitale Wirtschaft
- Sicherung von Daten durch geprüfte Sicherheitskontrollen
- Gewährleistet die Einhaltung von Datenschutzgesetzen
- Verbessert die Kontrolle über die Daten durch die Bereitstellung von Daten-Residency und Datenhoheit mit vollständiger Kontrolle durch die Gerichtsbarkeit

Zusammenarbeit mit einem zuverlässigen VMware Sovereign Cloud Service Provider

Um den Erfolg sicherzustellen, müssen Unternehmen mit Partnern zusammenarbeiten, denen sie vertrauen und die in der Lage sind, authentische und autonome souveräne Cloud-Plattformen zu hosten. VMware Cloud-Provider, die im Rahmen der VMware Sovereign Cloud-Initiative anerkannt sind, verpflichten sich, Cloud-Lösungen auf der Grundlage moderner, softwaredefinierter Architekturen zu entwerfen und zu betreiben, die die wichtigsten Prinzipien und Best Practices des VMware Sovereign Cloud-Frameworks verkörpern.

- **Datensouveränität und Rechtsprechungskontrolle** – Alle Daten sind wohnhaft und unterliegen der ausschließlichen Kontrolle und Autorität des Nationalstaats, in dem diese Daten erfasst wurden. Der Betrieb wird vollständig innerhalb der Gerichtsbarkeit verwaltet
- **Datenzugriff und -Integrität** – die Cloud-Infrastruktur ist ausfallsicher und an mindestens zwei Standorten innerhalb der Gerichtsbarkeit mit sicheren und privaten Verbindungsoptionen verfügbar.
- **Datensicherheit und Compliance** – die Kontrolle der Informationssicherheitsmanagementsysteme ist nach einem branchenweit anerkannten globalen (oder regionalen) Standard zertifiziert und regelmäßig geprüft.
- **Datenunabhängigkeit und -Mobilität** – Unterstützung moderner Anwendungsarchitekturen, um eine Anbieterbindung zu verhindern und Anwendungsportabilität und -Unabhängigkeit zu ermöglichen

Weitere Informationen von VMware finden Sie unter:

- "VMware Sovereign Cloud Overview"
- "Was ist VMware Sovereign Cloud?"
- "Die neue VMware Sovereign Cloud Initiative"

- "VMware Sovereign Cloud: Technisches Whitepaper"

NetApp mit VMware Sovereign Cloud: Anwendungsfälle

NetApp unterstützt VMware Sovereign Cloud-Konzepte durch die Integration mehrerer NetApp-Technologien.

Über die folgenden Links können Sie mehr über die Integration von NetApp-Technologien in VMware Sovereign Cloud erfahren:

- "NetApp StorageGRID als Objektspeicher-Erweiterung"

NetApp StorageGRID als Objektspeicher-Erweiterung

NetApp hat zusammen mit VMware NetApp StorageGRID in VMware Cloud Director integriert, um Unterstützung für den VMware Sovereign Cloud zu erhalten. Mit diesem Plug-in für VMware Cloud Director können Service-Provider StorageGRID als Objekt-Storage-Angebot nutzen (unabhängig vom Anwendungsfall) und StorageGRID Management über dieselbe mandantenfähige VMware Lösung (VMware Cloud Director) nutzen, die von Service-Providern verwendet wird, um andere Teile des Angebotskatalogs zu managen.

Partner, die VMware Sovereign Clouds bereitstellen, können sich für NetApp StorageGRID entscheiden, um sie beim Management und bei der Wartung von Cloud-Umgebungen mit unstrukturierten Daten zu unterstützen. Die universelle Kompatibilität mit nativem Support für Standard-APIs wie Amazon S3 API gewährleistet eine reibungslose Interoperabilität in verschiedenen Cloud-Umgebungen. Einzigartige Innovationen wie automatisiertes Lifecycle Management sorgen für einen kosteneffizienteren Schutz, Storage und langfristige Aufbewahrung unstrukturierter Kundendaten.

Die Sovereign Cloud-Integration von NetApp mit Cloud Director Anbieterlösungen überzeugen durch:

- Gewissheit, dass sensible Daten, einschließlich Metadaten, souverän kontrolliert werden und gleichzeitig den Zugriff ausländischer Behörden verhindern, die Datenschutzgesetze verletzen könnten.
- Höhere Sicherheit und Compliance, die Applikationen und Daten vor sich schnell entwickelnden Angriffsvektoren schützt und gleichzeitig die kontinuierliche Compliance mit einem vertrauenswürdigen lokalen Standort gewährleistet. Infrastruktur, integrierte Frameworks und lokale Experten.
- Zukunftssichere Infrastruktur, um schnell auf veränderte Datenschutzvorschriften, Sicherheitsbedrohungen und Geopolitik reagieren zu können
- Möglichkeit, mit sicherer Datenfreigabe und Analyse den Mehrwert von Daten freizusetzen, um Innovationen voranzutreiben, ohne gegen Datenschutzgesetze zu verstoßen. Die Datenintegrität ist so geschützt, dass genaue Einblicke gewährleistet sind.

Weitere Informationen zur Integration von StorageGRID finden Sie hier:

- "NetApp-Ankündigung"

NetApp Hybrid-Multi-Cloud mit Container-Workloads Red hat OpenShift

NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

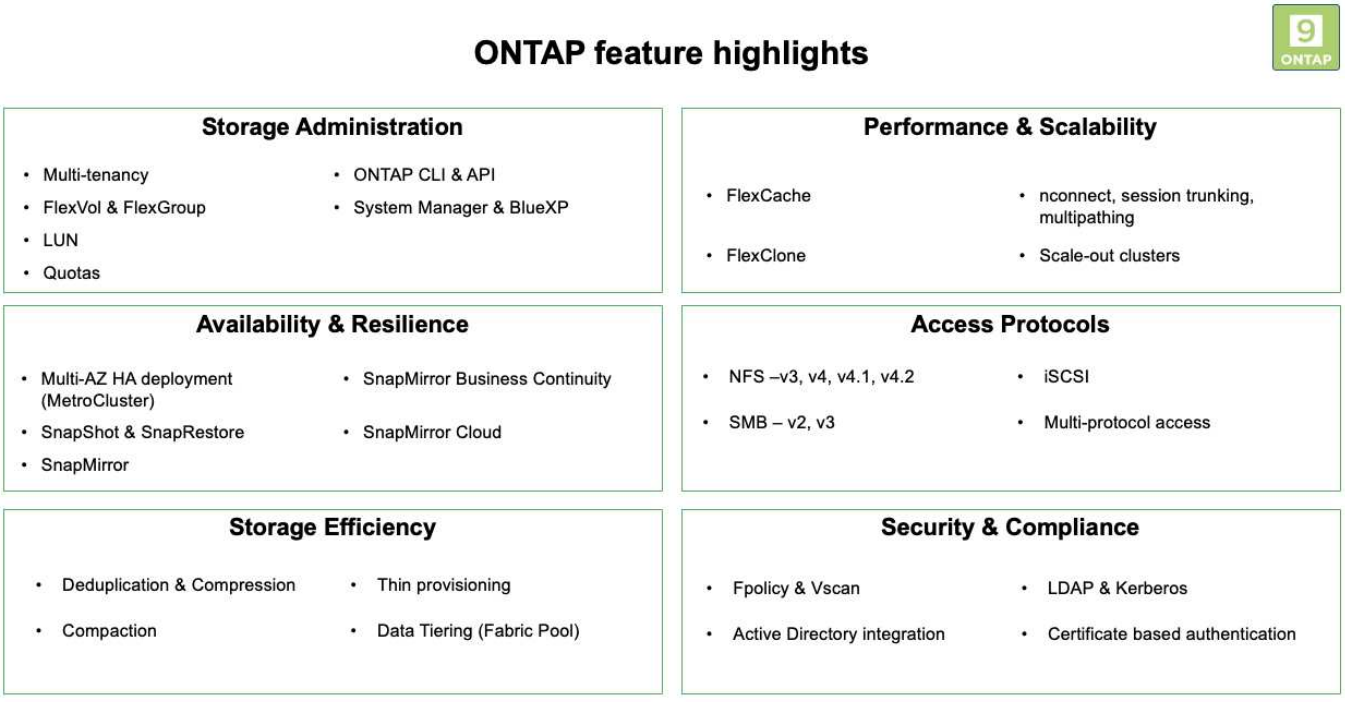
Überblick

Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Implementierungen.

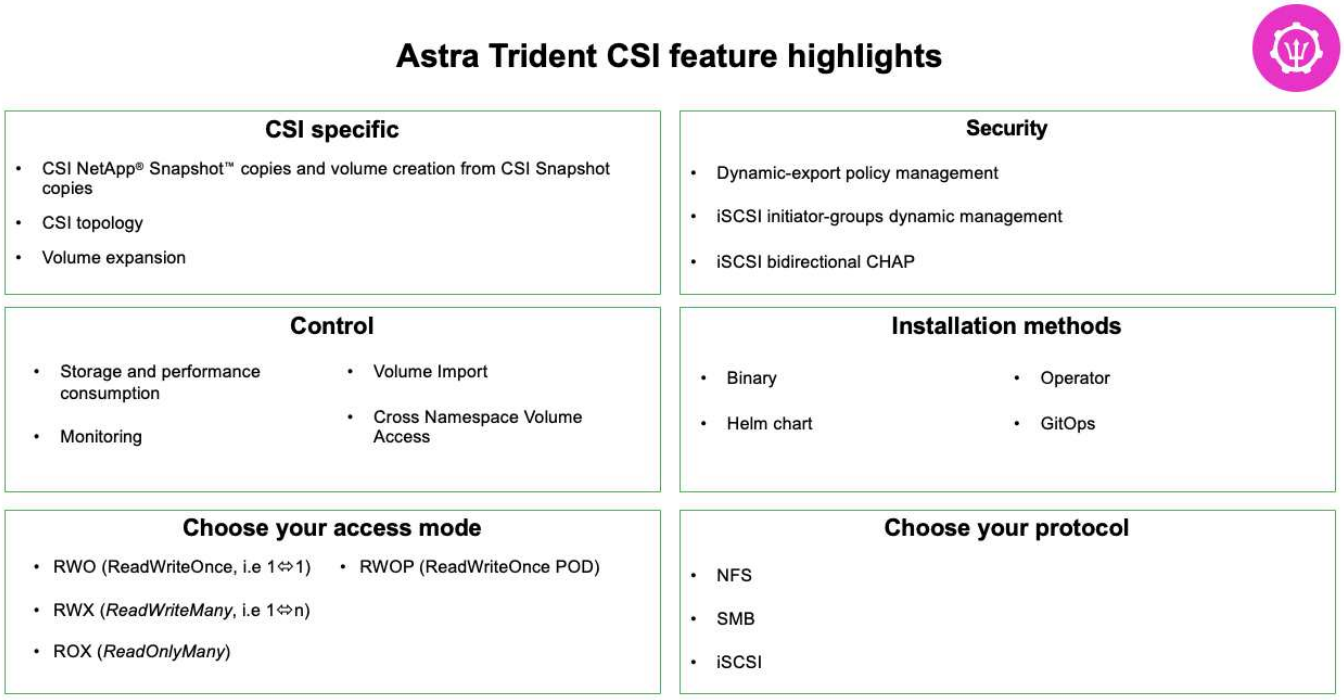
- Automatisierter, lokaler Storage:
  - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
  - NetApp Keystone stellt Storage-als-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
  - NetApp Cloud Volumes ONTAP(CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
  - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern



NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.



Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.

Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "Astra-Dokumentation" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

Wertversprechen von NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Die meisten Kunden beginnen nicht nur mit der Entwicklung von Kubernetes-basierten Umgebungen ohne die vorhandene Infrastruktur. Möglicherweise handelt es sich bei ihnen um eine herkömmliche IT-Abteilung, die die meisten ihrer Enterprise-Applikationen auf Virtual Machines ausführt (z. B. in großen VMware-Umgebungen). Dann beginnen sie, kleine containerbasierte Umgebungen zu erstellen, die die Anforderungen ihrer modernen Applikationsentwicklungsteams erfüllen. Diese Initiativen beginnen in der Regel klein und werden immer mehr verbreitet, wenn die Teams diese neuen Technologien und Fähigkeiten erlernen und beginnen, die vielen Vorteile der Einführung zu erkennen. Die gute Nachricht für Kunden ist, dass NetApp die Anforderungen beider Umgebungen erfüllen kann. Mit diesen Lösungen für Hybrid-Multi-Clouds mit Red hat OpenShift können NetApp Kunden moderne Cloud-Technologien und -Services einführen, ohne die gesamte Infrastruktur und das gesamte Unternehmen überarbeiten zu müssen. Ganz gleich, ob Applikationen und Daten der Kunden lokal, in der Cloud, auf Virtual Machines oder in Containern gehostet werden – NetApp bietet konsistentes Datenmanagement, Sicherung, Sicherheit und Portabilität. Mit diesen neuen Lösungen wird derselbe Wert, den NetApp seit Jahrzehnten in On-Premises-Datacenter-Umgebungen bietet, für das gesamte Datenhorizont des Unternehmens verfügbar sein, ohne dass erhebliche Investitionen in die Tools, die Anschaffung neuer Fähigkeiten oder die Entwicklung neuer Teams erforderlich sind. NetApp unterstützt Kunden dabei, diese geschäftlichen Herausforderungen zu bewältigen – unabhängig von der aktuellen Phase des Cloud-Übergangs.

NetApp Hybrid-Multi-Cloud mit Red hat OpenShift:

- Die Lösung bietet Kunden validierte Designs und Verfahren, die zeigen, wie Kunden ihre Daten und Applikationen am besten managen, schützen, sichern und migrieren können, wenn sie Red hat OpenShift mit NetApp Storage-Lösungen einsetzen.
- Präsentieren von Best Practices für Kunden, die Red hat OpenShift mit NetApp Storage in VMware Umgebungen, Bare Metal-Infrastruktur oder einer Kombination aus beidem ausführen
- Strategien und Optionen sowohl für On-Premises- und Cloud-Umgebungen als auch für Hybrid-Umgebungen aufzeigen, in denen beide eingesetzt werden

Unterstützte Lösungen für die NetApp Hybrid-Multi-Cloud-Umgebung für Container-Workloads mit Red hat OpenShift

Die Lösung testet und validiert Migration und zentralisierte Datensicherung mit OpenShift Container-Plattform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp BlueXP und NetApp Astra Control Center (ACC).

Folgende Szenarien werden von NetApp getestet und validiert. Die Lösung ist in mehrere Szenarien aufgeteilt, die auf folgenden Merkmalen basieren:

- On-Premises
- Cloud

- Selbst gemanagte OpenShift-Cluster und selbstverwalteter NetApp Storage
- Von Providern gemanagte OpenShift-Cluster und NetApp Storage, der vom Provider gemanagt wird

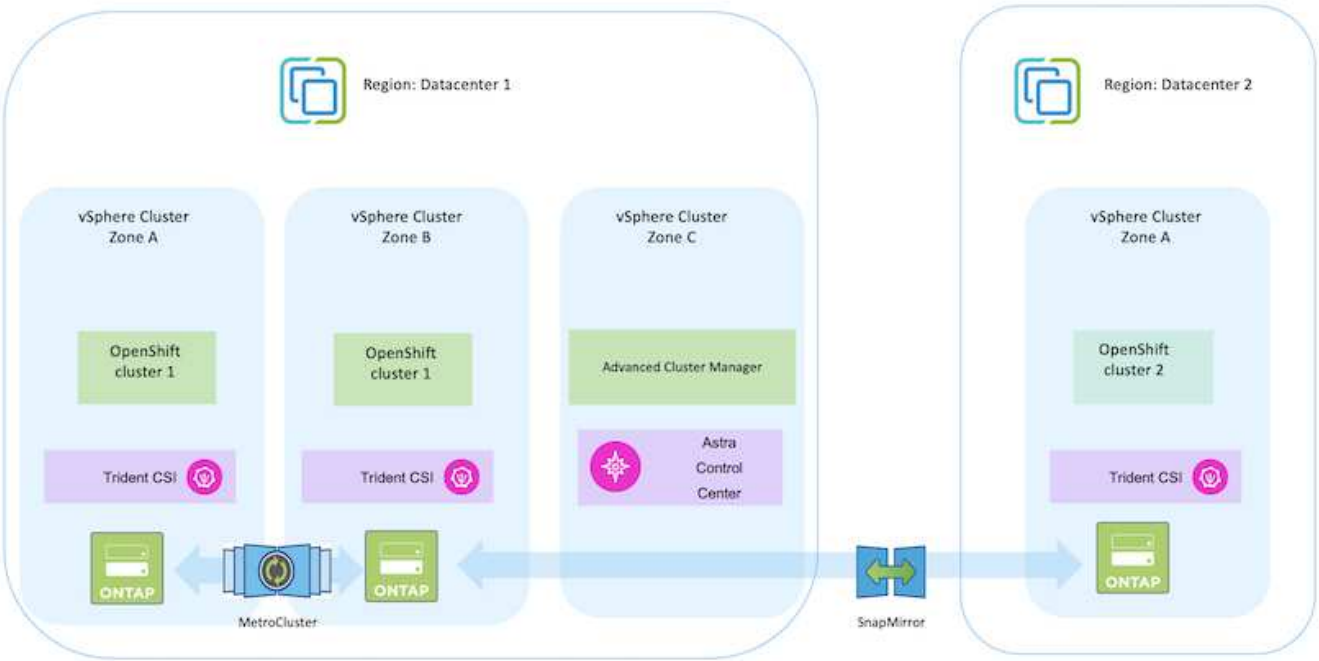
Wir werden in Zukunft weitere Lösungen und Anwendungsfälle entwickeln.

Szenario 1: Datenschutz und Migration innerhalb der On-Premise-Umgebung mittels ACC

Lokal: Selbst gemanagte OpenShift-Cluster und automatisierter NetApp Storage

- Erstellen Sie mithilfe von ACC Snapshot Kopien, Backups und Wiederherstellungen für den Datenschutz.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen durch.

Szenario 1

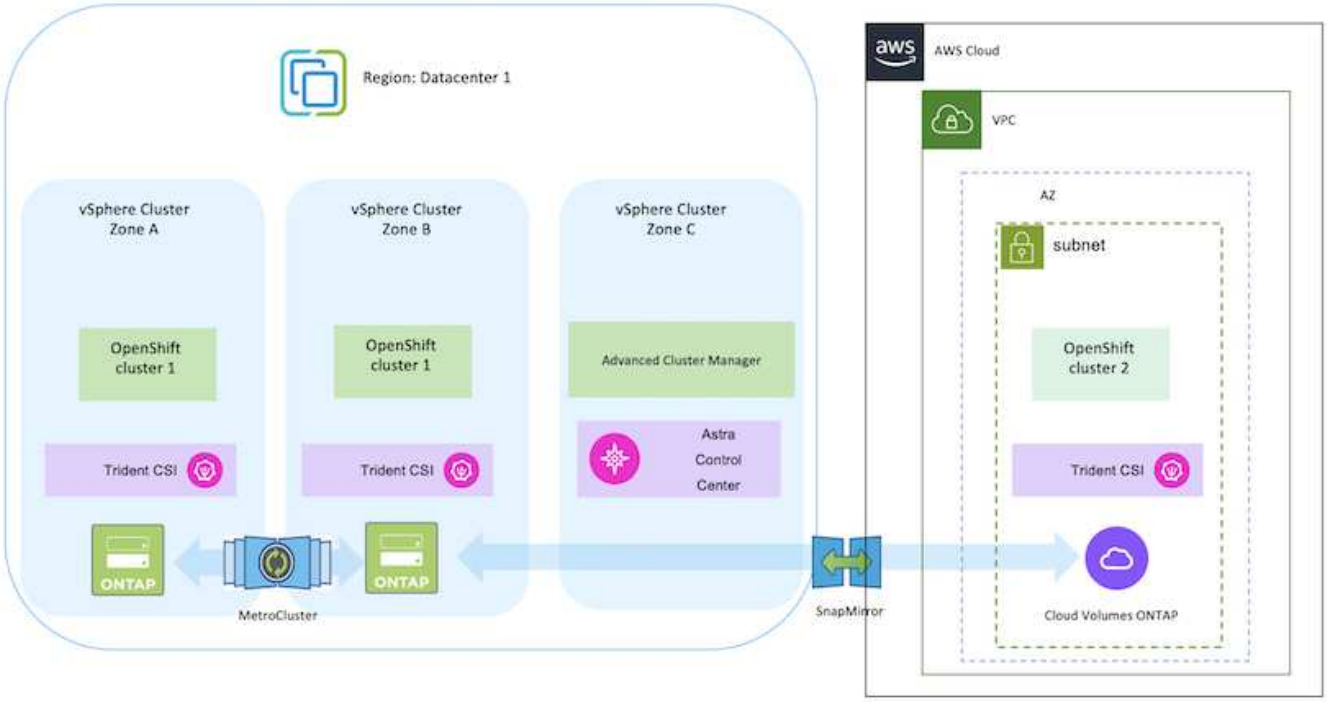


Szenario 2: Datensicherung und Migration von der On-Premises-Umgebung in die AWS-Umgebung mittels ACC

On-Premises: Selbst verwalteter OpenShift-Cluster und selbstverwalteter Storage AWS Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage

- Führen Sie mithilfe von ACC Backups und Wiederherstellungen für den Datenschutz durch.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen durch.

Szenario 2

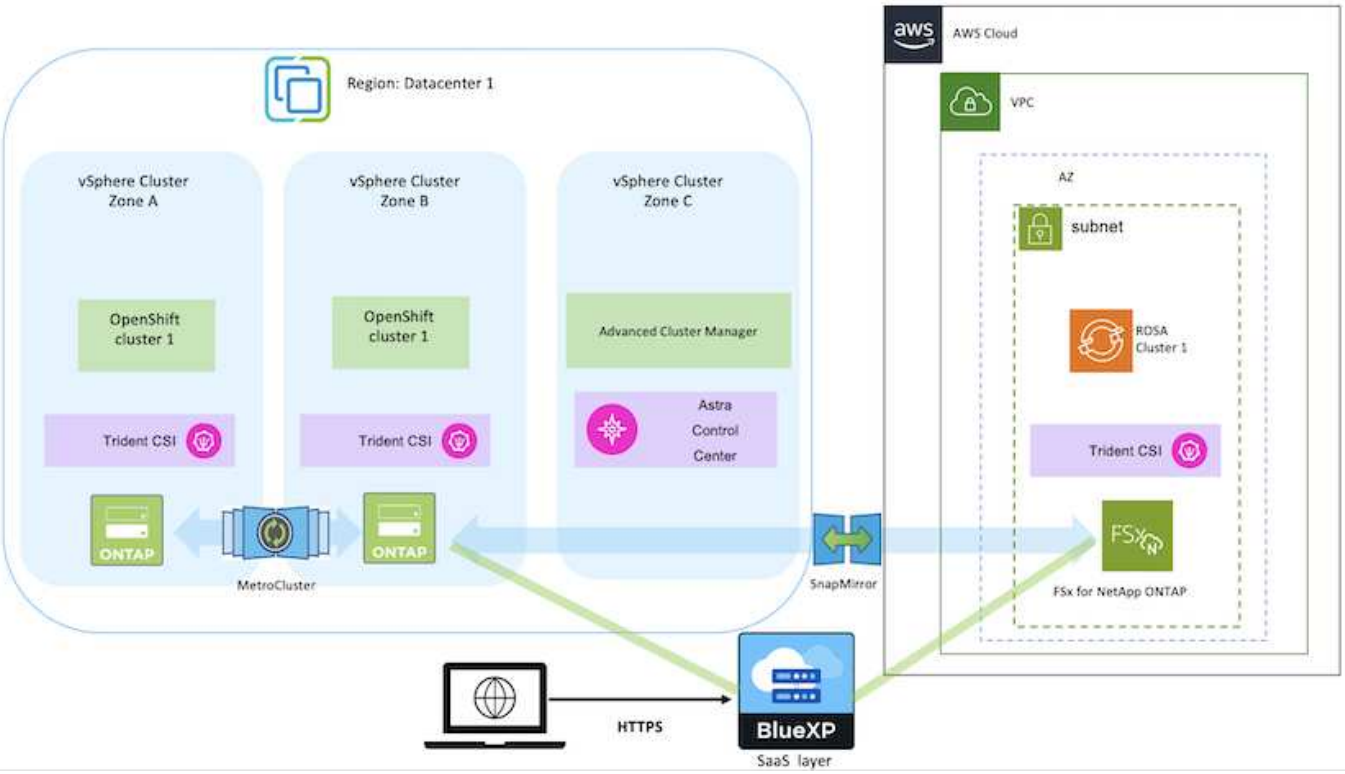


Szenario 3: Datensicherung und Migration von der On-Premises-Umgebung in die AWS-Umgebung

On-Premises: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage AWS Cloud: Vom Provider verwaltetes OpenShift-Cluster (ROSA) und Provider-Managed Storage (FSxN)

- Führen Sie mit BlueXP die Replizierung persistenter Volumes (FSxN) durch.
- Erstellen Sie mithilfe von OpenShift GitOps Anwendungsmetadaten neu.

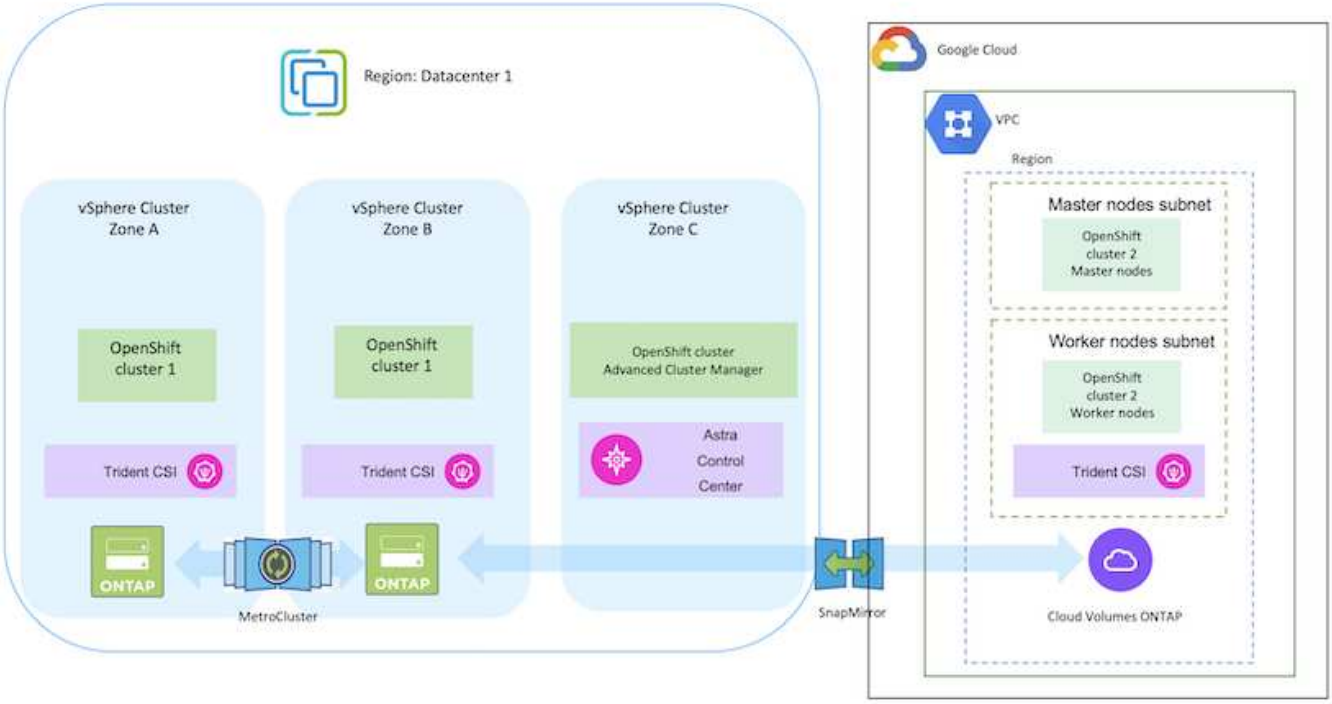
Szenario 3



Szenario 4: Datenschutz und Migration von der On-Premise-Umgebung in die GCP-Umgebung mittels ACC

On-Premises: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage
Google Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage

- Führen Sie mithilfe von ACC Backups und Wiederherstellungen für den Datenschutz durch.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen durch.

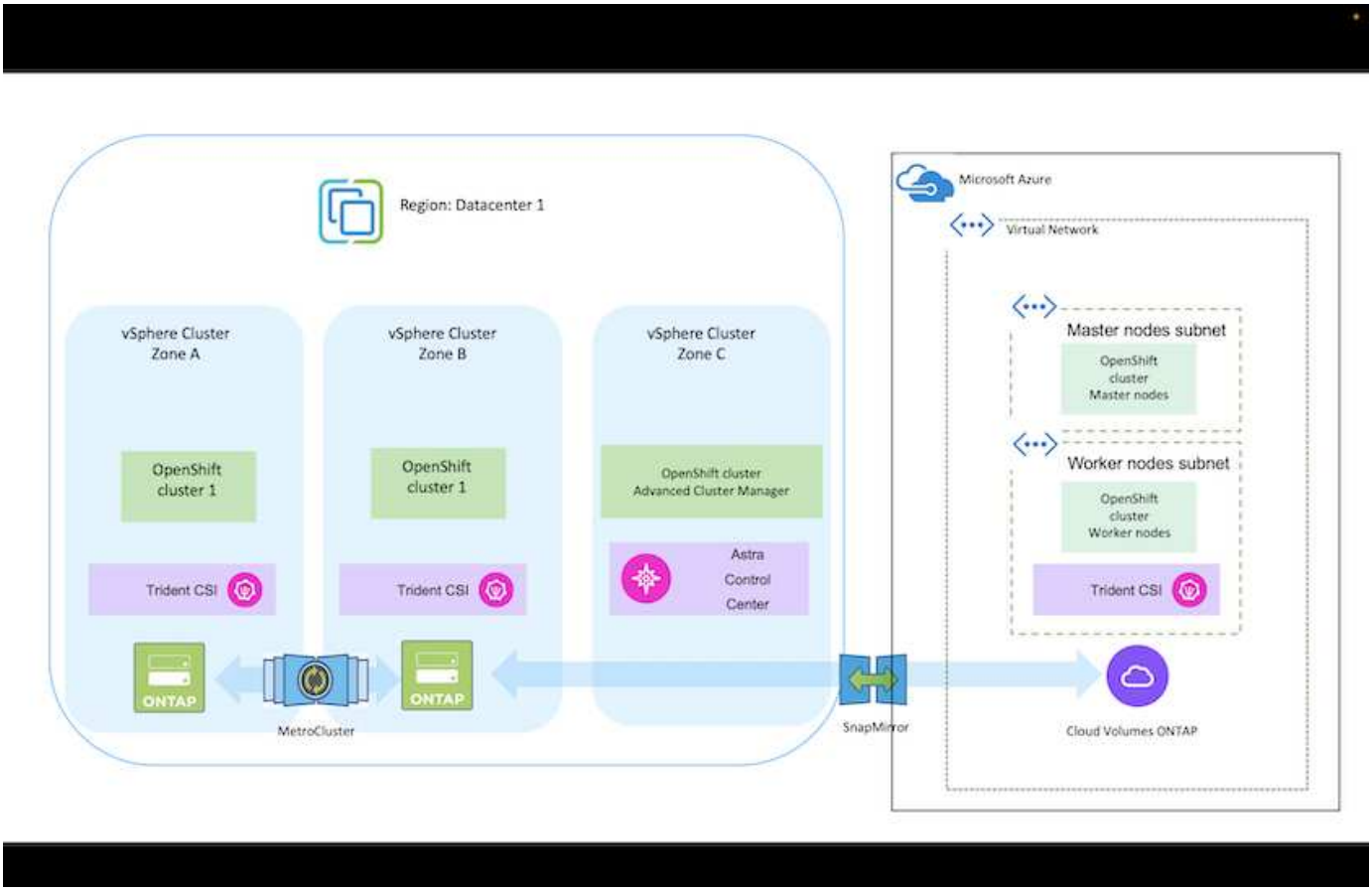


Hinweise zur Verwendung von ONTAP in einer MetroCluster-Konfiguration finden Sie unter "Hier".

Szenario 5: Datenschutz und Migration von der On-Premises-Umgebung in die Azure-Umgebung mittels ACC

On-Premises: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Storage
Azure Cloud: Automatisiertes OpenShift-Cluster und automatisierter Storage

- Führen Sie mithilfe von ACC Backups und Wiederherstellungen für den Datenschutz durch.
- Führen Sie mithilfe von ACC eine SnapMirror Replizierung der Container-Applikationen durch.



Hinweise zur Verwendung von ONTAP in einer MetroCluster-Konfiguration finden Sie unter "Hier".

Versionen verschiedener Komponenten, die bei der Lösungsvalidierung verwendet werden

Die Lösung testet und validiert die Migration und zentralisierte Datensicherung mit der OpenShift Container-Plattform, OpenShift Advanced Cluster Manager, NetApp ONTAP und NetApp Astra Control Center.

Die Szenarien 1, 2 und 3 der Lösung wurden mit den Versionen validiert, wie in der folgenden Tabelle dargestellt:

* Komponente*	**Version**
VMware	VSphere Client Version 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Hub-Cluster	OpenShift 4.11.34
Quell- und Zielcluster	OpenShift 4.12.9 On-Premises und in AWS
NetApp Astra Trident	Trident Server und Client 23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1
AWS FSX for NetApp ONTAP	Single AZ

Szenario 4 der Lösung wurde mit den Versionen validiert, wie in der folgenden Tabelle dargestellt:

* Komponente*	**Version**
VMware	VSphere Client Version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Hub-Cluster	OpenShift 4.13.13
Quell- und Zielcluster	OpenShift 4.13.12 On-Premises und in Google Cloud
NetApp Astra Trident	Trident Server und Client 23.07.0
NetApp Astra Control Center	ACC 23.07.0-25
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Single AZ, Single Node, 9.14.0

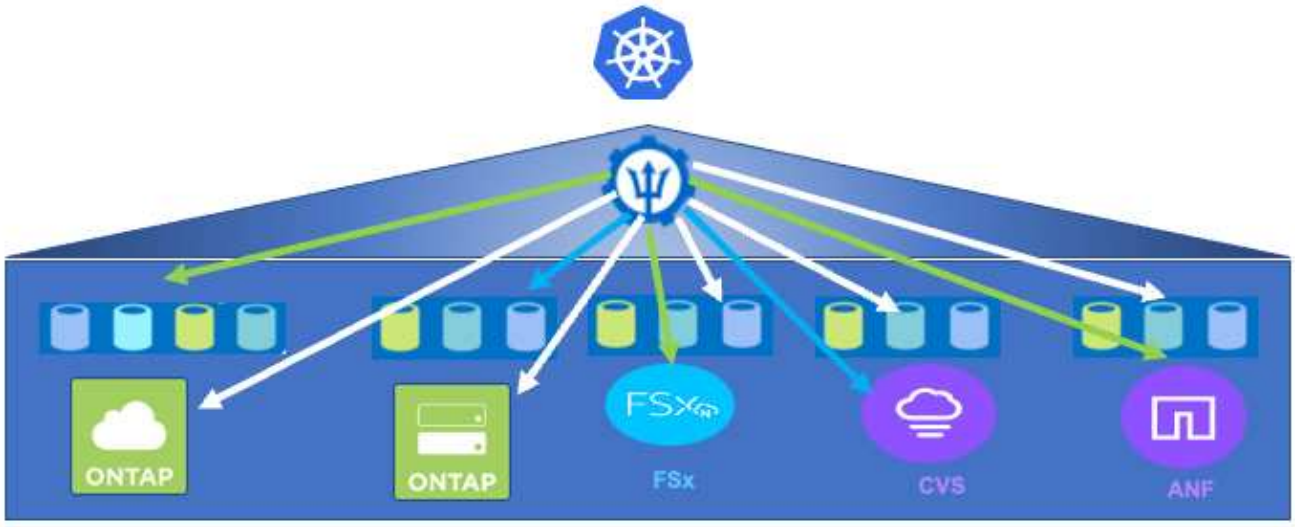
Szenario 5 der Lösung wurde mit den Versionen validiert, wie in der folgenden Tabelle dargestellt:

* Komponente*	**Version**
VMware	VSphere Client Version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Quell- und Zielcluster	OpenShift 4.13.25 On-Premises und in Azure
NetApp Astra Trident	Trident Server, Client und Astra Control Provisioner 23.10.0
NetApp Astra Control Center	ACC 23.10
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Single AZ, Single Node, 9.14.0

Unterstützte NetApp Storage-Integrationen in Red hat Open Shift Container

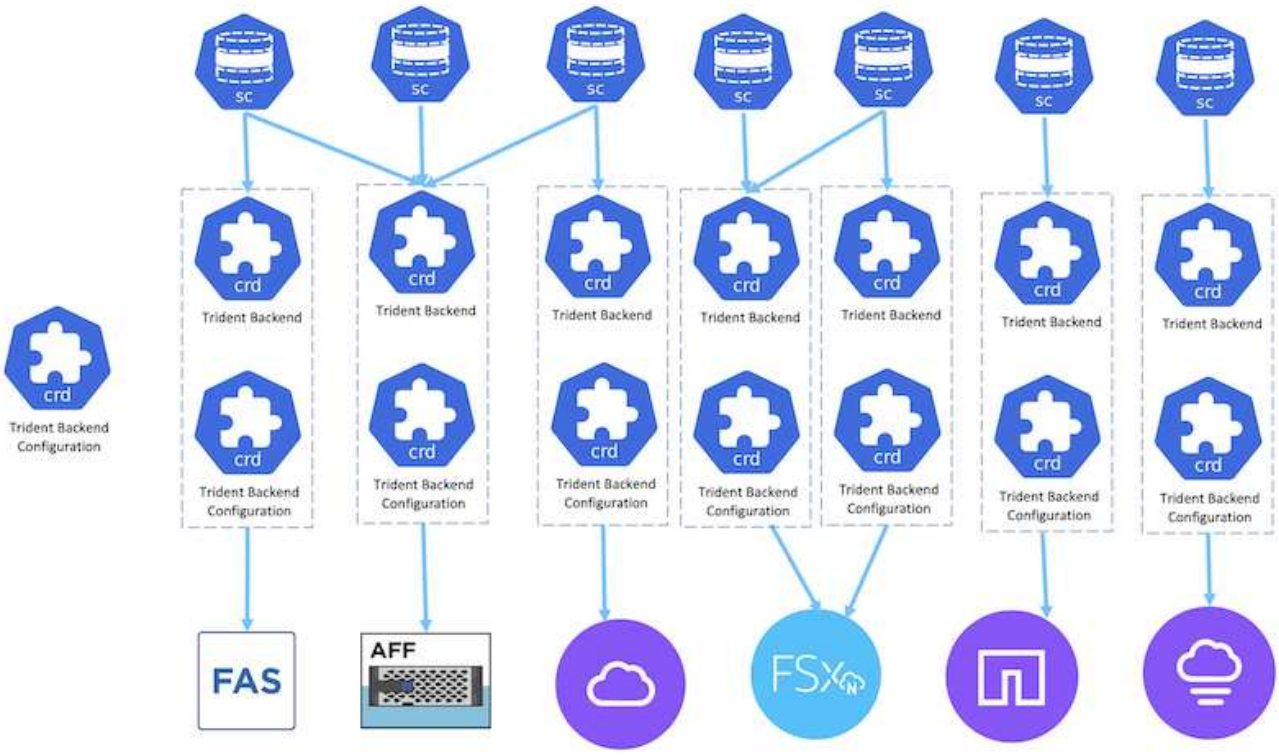
Ganz gleich, ob die Red hat Open Shift Container auf VMware oder in den Hyperscalern ausgeführt werden, NetApp Astra Trident kann als CSI-bereitstellung für die verschiedenen von ihm unterstützten Back-End-Storage-Typen von NetApp verwendet werden.

In der folgenden Abbildung sind die verschiedenen NetApp Back-End-Storage-Systeme dargestellt, die mithilfe von NetApp Astra Trident in OpenShift-Cluster integriert werden können.

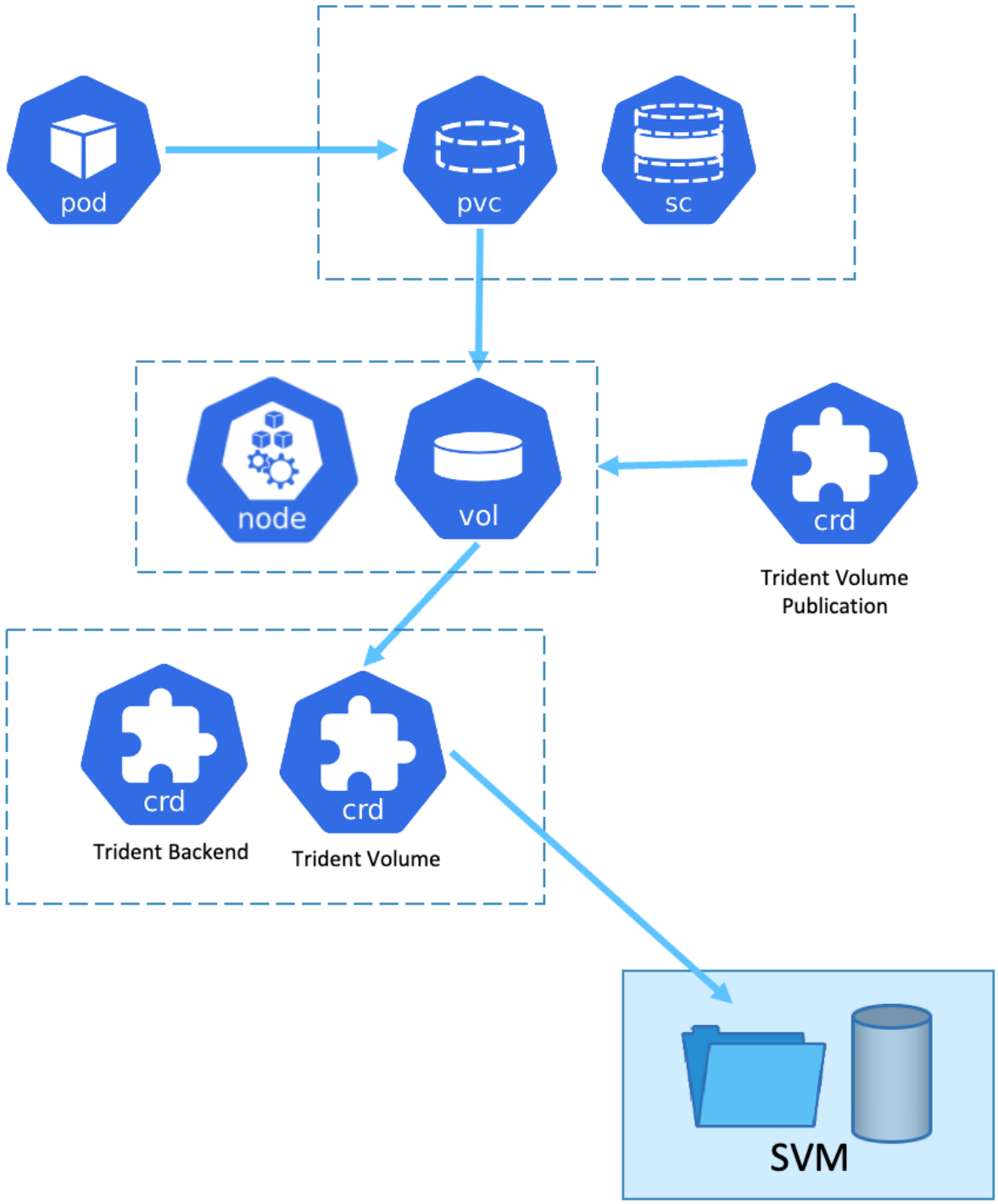


Die ONTAP Storage Virtual Machine (SVM) bietet sichere Mandantenfähigkeit. Ein einziger OpenShift-Cluster kann eine Verbindung zu einer einzelnen SVM oder mehreren SVMs oder sogar zu mehreren ONTAP-Clustern herstellen. Die Storage-Klasse filtert den Back-End-Speicher nach Parametern oder Etiketten. Storage-Administratoren definieren die Parameter für die Verbindung zum Storage-System über eine dreigearbeitete Backend-Konfiguration. Bei erfolgreichem Verbindungsaufbau erstellt es das dreilagige Backend und füllt die Informationen aus, die von der Speicherklasse gefiltert werden können.

Die Beziehung zwischen Storageclass und Backend ist unten dargestellt.



Applikationseigentümer fordert persistentes Volume mithilfe von Storage-Klassen an. Die Storage-Klasse filtert den Back-End Storage. Die Beziehung zwischen dem Pod und dem Back-End Storage wird unten dargestellt.



CSI-Optionen (Container Storage Interface)

In vSphere Umgebungen können Kunden zur Integration mit ONTAP VMware CSI-Treiber und/oder Astra Trident CSI wählen. Mit VMware CSI werden die persistenten Volumes als lokale SCSI-Festplatten verwendet, mit Trident dagegen über ein Netzwerk. Da VMware CSI keine RWX-Zugriffsmodi mit ONTAP unterstützt, müssen Applikationen Trident CSI verwenden, wenn der RWX-Modus erforderlich ist. FC-basierte Implementierungen bevorzugen VMware CSI und SnapMirror Business Continuity (SMBC) bietet Hochverfügbarkeit auf Zonenebene.

VMware CSI unterstützt

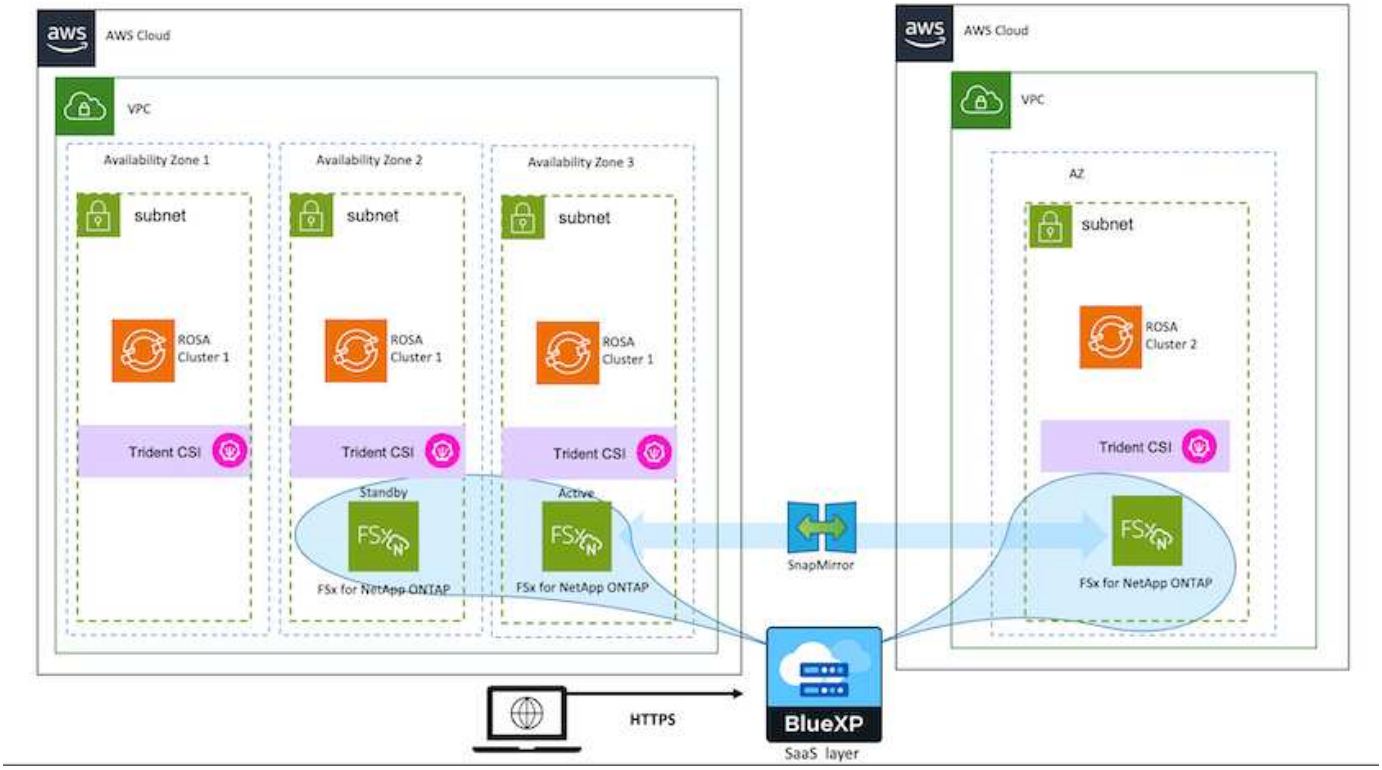
- Core-Block-basierte Datastores (FC, FCoE, iSCSI, NVMeoF)
- Dateibasierte Core-Datastores (NFS v3, v4)
- VVol Datastores (Block und Datei)

Trident verfügt über folgende Treiber zur Unterstützung von ONTAP

- ontap-san (dediziertes Volume)
- ontap-san-Economy (gemeinsam genutztes Volume)
- ontap-nas (dediziertes Volume)
- ontap-nas-Economy (gemeinsam genutztes Volume)
- ontap-nas-Flexgroup (dediziertes, großes Volume)

Sowohl für VMware CSI als auch für Astra Trident CSI unterstützt ONTAP nconnect, Session-Trunking, kerberos usw. für NFS- und Multipathing, chap-Authentifizierung usw. für Blockprotokolle.

In AWS kann FSX für NetApp ONTAP (FSxN) in einer einzelnen Verfügbarkeitszone (AZ) oder in Multi AZ implementiert werden. Für Produktions-Workloads, die Hochverfügbarkeit erfordern, bietet eine Multi-AZ-Fehlertoleranz auf zonaler Ebene und einen besseren NVMe-Lese-Cache als eine einzelne AZ. Weitere Informationen finden Sie unter "AWS Performance-Richtlinien".
Um Kosten für den Disaster Recovery-Standort zu sparen, kann ein einzelner AZ FSX ONTAP genutzt werden.



Weitere Informationen zur Anzahl der von FSX ONTAP unterstützten SVMs finden Sie unter "Management der FSX ONTAP-Storage-Virtual Machine"

NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

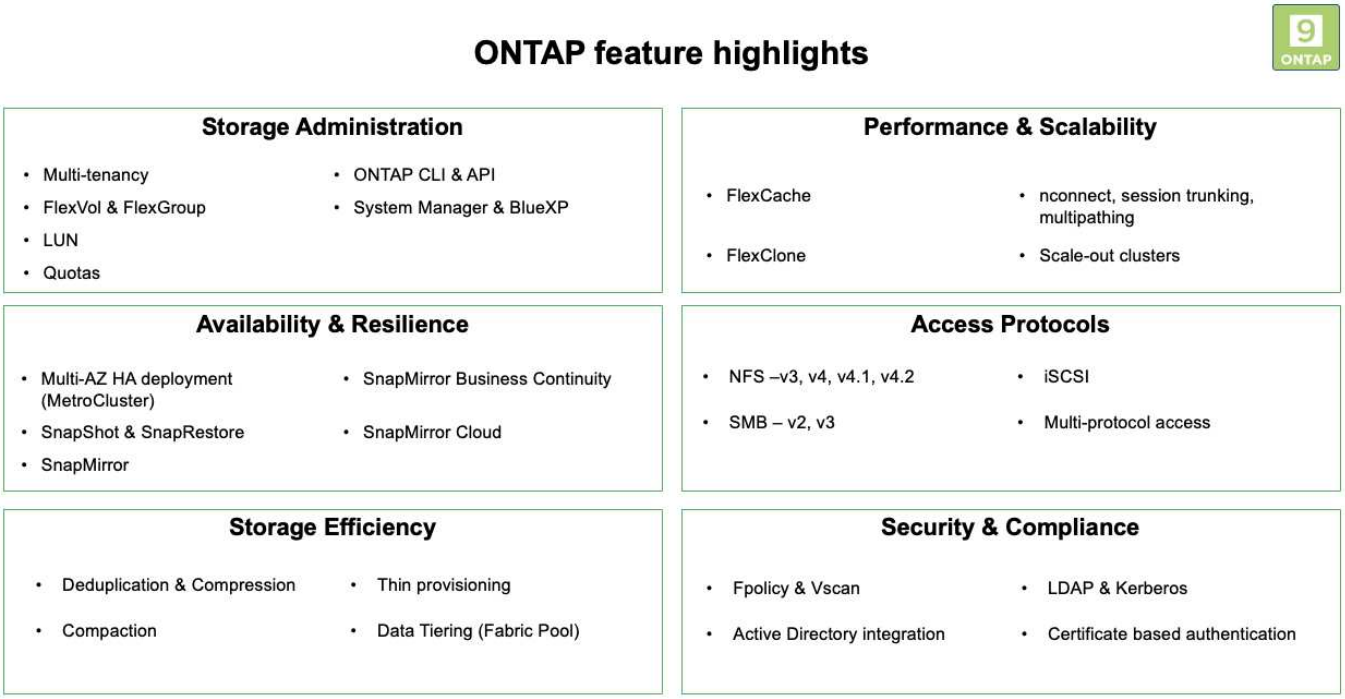
Überblick

Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Implementierungen.

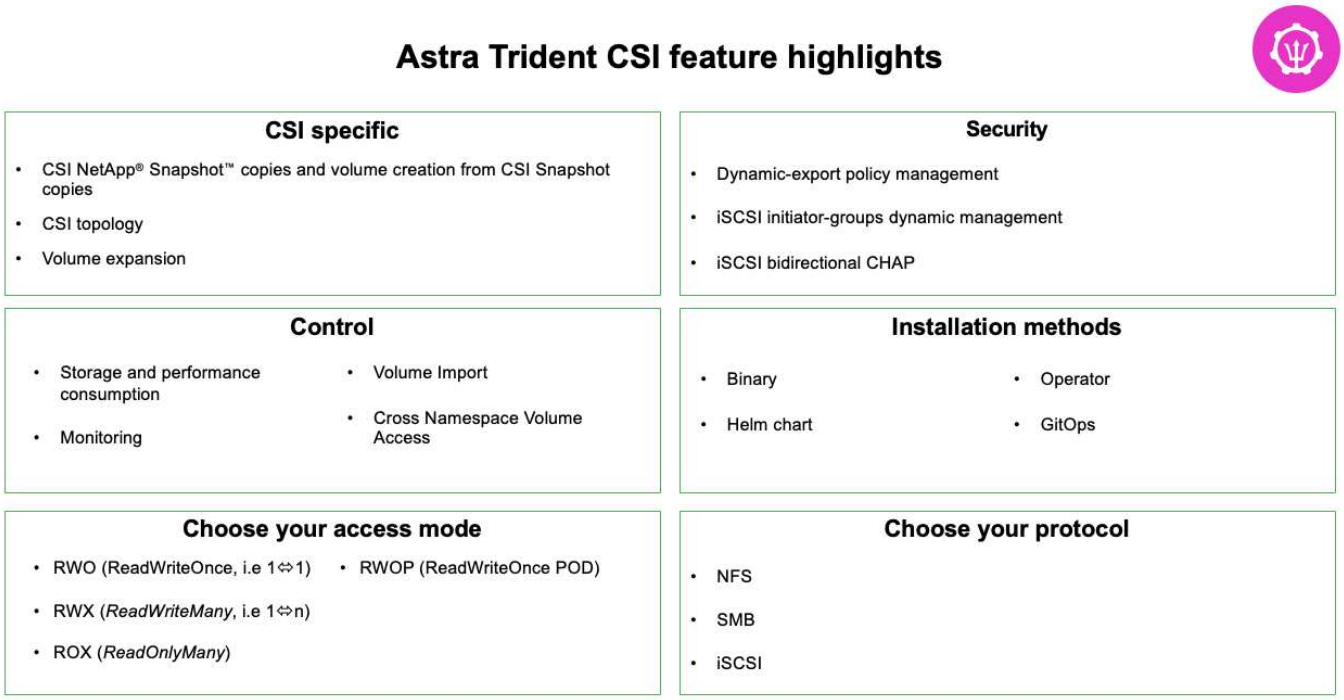
- Automatisierter, lokaler Storage:
  - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
  - NetApp Keystone stellt Storage-als-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
  - NetApp Cloud Volumes ONTAP(CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
  - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern



NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.



Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.

Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "Astra-Dokumentation" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus

von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

NetApp Lösung mit Container-Plattform-Workloads von Red hat OpenShift auf VMware

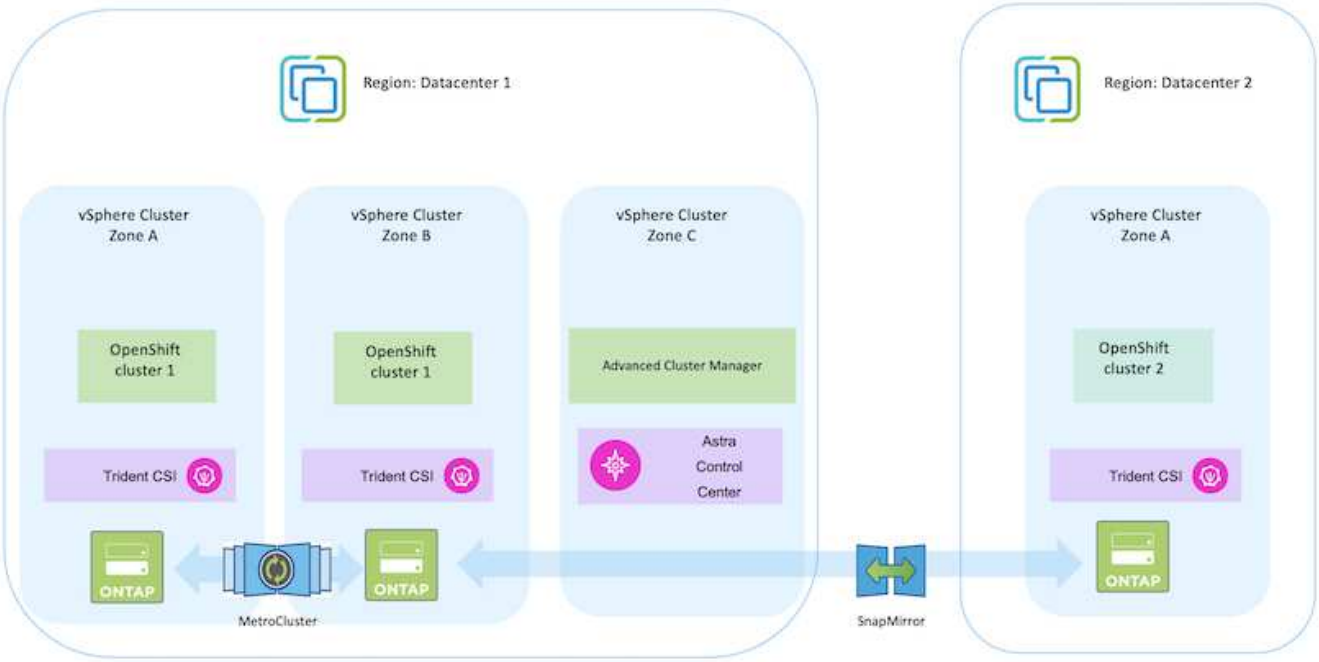
Falls Kunden ihre modernen Container-Applikationen in ihren privaten Datacentern auf einer Infrastruktur ausführen müssen, ist dies möglich. Sie sollten die Container-Plattform Red hat OpenShift (OCP) planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für die Bereitstellung ihrer Container-Workloads zu schaffen. Die OCP Cluster können auf VMware oder Bare Metal bereitgestellt werden.

NetApp ONTAP Storage bietet Datensicherung, Zuverlässigkeit und Flexibilität für Container-Implementierungen. Astra Trident dient als dynamische Storage-bereitstellung zur Nutzung von persistentem ONTAP Storage für statusorientierte Applikationen von Kunden. Astra Control Center kann zur Orchestrierung der vielen Datenmanagementanforderungen zustandsbehafteter Applikationen eingesetzt werden, wie zum Beispiel Datensicherung, Migration und Business Continuity.

Mit VMware vSphere bietet NetApp ONTAP Tools ein vCenter Plug-in, das zur Bereitstellung von Datenspeichern verwendet werden kann. Wenden Sie Tags an und verwenden Sie es mit OpenShift zum Speichern der Node-Konfiguration und -Daten. NVMe-basierter Storage bietet eine niedrigere Latenz und hohe Performance.

Diese Lösung bietet Details zur Datensicherung und Migration von Container-Workloads mithilfe von Astra Control Center. Für diese Lösung werden die Container-Workloads auf Red hat OpenShift-Clustern auf vSphere innerhalb der On-Premises-Umgebung bereitgestellt. HINWEIS: Wir werden in Zukunft eine Lösung für Container-Workloads auf OpenShift-Clustern auf Bare-Metal bereitstellen.

Datensicherungs- und Migrationslösung für Container-Workloads mit OpenShift mithilfe von Astra Control Center

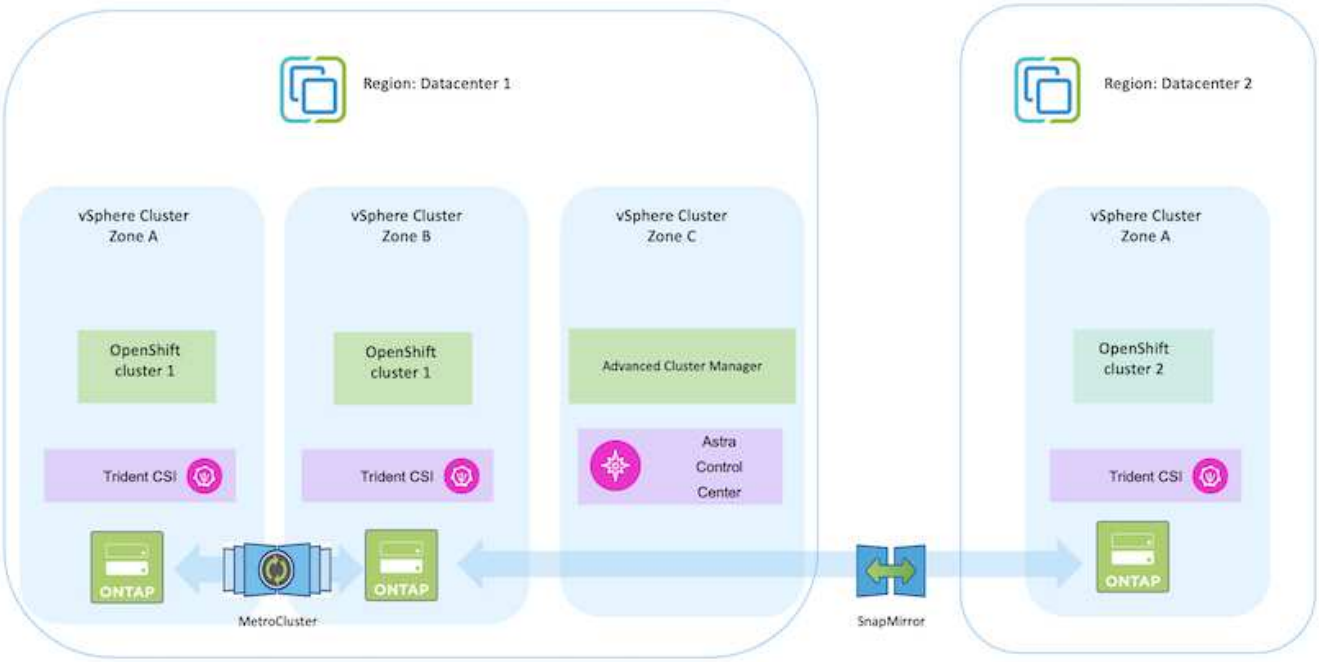


Bereitstellung und Konfiguration der Container-Plattform Red hat OpenShift unter VMware

Dieser Abschnitt beschreibt einen allgemeinen Workflow, in dem erläutert wird, wie OpenShift-Cluster eingerichtet und gemanagt und zustandsbehaftete Anwendungen auf ihnen verwaltet werden. Es zeigt die Nutzung von NetApp ONTAP Storage-Arrays mit Hilfe von Astra Trident zur Bereitstellung persistenter Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.

Es gibt verschiedene Möglichkeiten, Red hat OpenShift Container Platform Cluster bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "Ressourcen".

Im folgenden Diagramm sind die in einem Datacenter unter VMware implementierten Cluster dargestellt.



Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Bereitstellung und Konfiguration einer CentOS VM

- Sie wird in der VMware vSphere Umgebung implementiert.
- Mit dieser VM werden einige Komponenten wie NetApp Astra Trident und das NetApp Astra Control Center für die Lösung implementiert.
- Auf dieser VM wird während der Installation ein Root-Benutzer konfiguriert.

OpenShift-Container-Plattform-Cluster auf VMware vSphere (Hub-Cluster) implementieren und konfigurieren

Beachten Sie die Anweisungen zum "Unterstützte Bereitstellung" Methode zum Bereitstellen eines OCP-Clusters.

Denken Sie daran: - Erstellen Sie ssh öffentlichen und privaten Schlüssel für den Installer zur Verfügung zu stellen. Mit diesen Schlüsseln können Sie sich bei Bedarf bei den Master- und Worker-Knoten anmelden. - Laden Sie das Installationsprogramm vom unterstützten Installer herunter. Dieses Programm wird zum Booten der VMs verwendet, die Sie in der VMware vSphere-Umgebung für die Master- und Worker-Knoten erstellen. - VMs sollten die Mindestanforderung an CPU, Arbeitsspeicher und Festplatte haben. (Siehe vm Create-Befehle auf "Das" Seite für den Master- und den Worker-Knoten, die diese Informationen bereitstellen) - die diskUUID sollte auf allen VMs aktiviert sein. - Erstellen Sie mindestens 3 Knoten für Master und 3 Knoten für worker. - Sobald sie vom Installer entdeckt werden, aktivieren Sie die VMware vSphere Integration Toggle-Taste.

Installieren Sie Advanced Cluster Management auf dem Hub-Cluster

Diese wird mit dem Advanced Cluster Management Operator auf dem Hub-Cluster installiert. Beachten Sie die Anweisungen "Hier".

Installieren Sie eine interne Red hat Quay-Registrierung auf dem Hub-Cluster.

- Zum Push des Astra-Images ist eine interne Registrierung erforderlich. Eine interne Quay-Registrierung wird über den Operator im Hub-Cluster installiert.
- Beachten Sie die Anweisungen "Hier"

Zwei zusätzliche OCP-Cluster installieren (Quelle und Ziel)

- Die zusätzlichen Cluster können über die ACM auf dem Hub-Cluster bereitgestellt werden.
- Beachten Sie die Anweisungen "Hier".

Konfigurieren Sie den NetApp ONTAP Storage

- Installation eines ONTAP-Clusters mit Verbindung zu den OCP-VMs in der VMware-Umgebung
- Erstellen Sie eine SVM.
- Konfigurieren Sie NAS-Daten-LIF für den Zugriff auf den Storage in der SVM.

Installation von NetApp Trident auf den OCP-Clustern

- NetApp Trident lässt sich in allen drei Clustern installieren: Hub-, Quell- und Ziel-Cluster
- Beachten Sie die Anweisungen "Hier".
- Erstellen Sie ein Storage-Backend für ontap-nas.
- Erstellen einer Storage-Klasse für ontap-nas
- Siehe Anweisungen "Hier".

Installation von NetApp Astra Control Center

- NetApp Astra Control Center wird über den Astra Operator auf dem Hub-Cluster installiert.
- Beachten Sie die Anweisungen "Hier".

Wichtige Fakten: * Laden Sie das NetApp Astra Control Center Image von der Support-Website herunter. * Drücken Sie das Bild auf eine interne Registrierung. * Siehe Anweisungen hier.

Stellen Sie eine Anwendung auf dem Quellcluster bereit

Verwenden Sie OpenShift GitOps, um eine Anwendung zu implementieren. (Z. B. Postgres, Ghost)

Fügen Sie die Quell- und Ziel-Cluster zu Astra Control Center hinzu.

Nachdem Sie dem Astra Control-Management einen Cluster hinzugefügt haben, können Sie Apps auf dem Cluster (außerhalb von Astra Control) installieren und anschließend in Astra Control auf der Seite Applications die Apps und ihre Ressourcen definieren. Siehe "Beginnen Sie mit dem Management von Apps im Bereich Astra Control Center".

Der nächste Schritt besteht darin, das Astra Control Center für Datensicherung und Datenmigration von der Quell- zum Ziel-Cluster zu nutzen.

Datensicherung mit Astra

Auf dieser Seite werden die Datenschutzoptionen für Container-basierte Red hat OpenShift-Anwendungen angezeigt, die unter VMware vSphere mit Astra Control Center (ACC) ausgeführt werden.

Wenn Benutzer ihre Anwendungen mit Red hat OpenShift modernisieren, sollte eine Datenschutzstrategie eingerichtet werden, um sie vor versehentlichem Löschen oder anderen menschlichen Fehlern zu schützen. Häufig ist auch eine Sicherungsstrategie für gesetzliche Vorschriften oder Compliance-Zwecke erforderlich, um ihre Daten vor einem Diaster zu schützen.

Die Anforderungen an die Datensicherung reichen von dem Zurücksetzen auf eine zeitpunktgenaue Kopie bis hin zum automatischen Failover auf eine andere Fehlerdomäne ohne menschliches Eingreifen. Viele Kunden entscheiden sich für ONTAP als bevorzugte Storage-Plattform für ihre Kubernetes-Applikationen, da sie umfassende Funktionen wie Mandantenfähigkeit, Multiprotokoll, hohe Performance und Kapazität, Replizierung und Caching für Standorte an mehreren Standorten sowie Sicherheit und Flexibilität bieten.

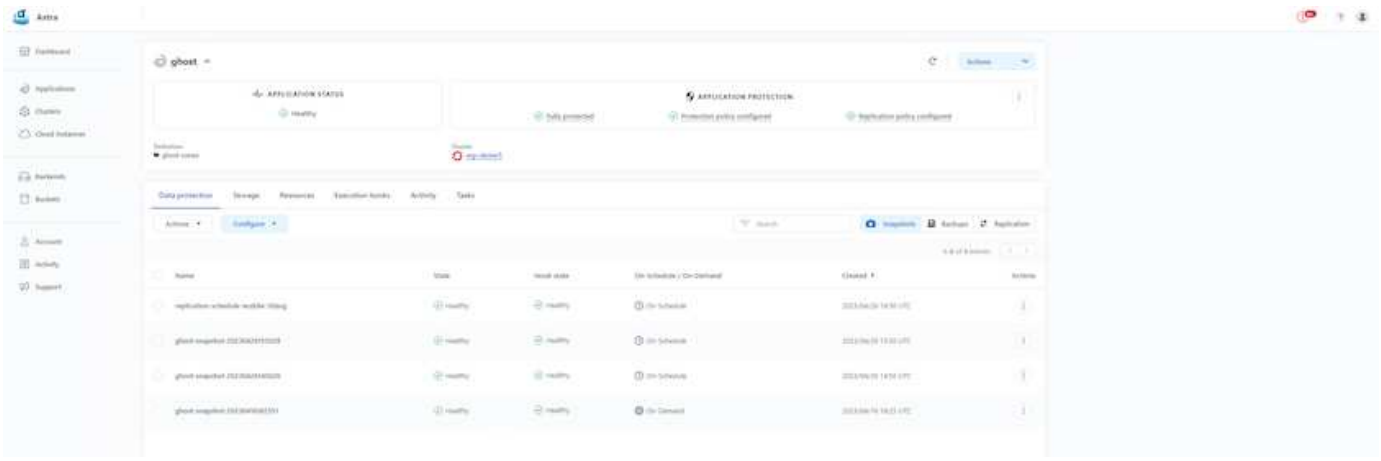
Die Datensicherung in ONTAP kann über Ad-hoc oder richtliniengesteuert erfolgen - **Snapshot** - **Backup und Restore**

Sowohl Snapshot-Kopien als auch Backups schützen die folgenden Datentypen: - **Die Anwendungsmetadaten, die den Status der Applikation darstellen** - **alle mit der Applikation verknüpften persistenten Datenvolumes** - **alle Ressourcenartefakte der Applikation**

Momentaufnahme mit ACC

Mithilfe von Snapshot mit ACC kann eine Point-in-Time-Kopie der Daten erfasst werden. Sicherungsrichtlinie definiert die Anzahl der zu bewahrenden Snapshot Kopien. Die minimale verfügbare Terminplanoption ist stündlich. Manuelle On-Demand Snapshot Kopien können jederzeit und in kürzeren Intervallen als geplante Snapshot Kopien erstellt werden. Snapshot-Kopien werden auf demselben bereitgestellten Volume wie die Applikation gespeichert.

Snapshot mit ACC konfigurieren

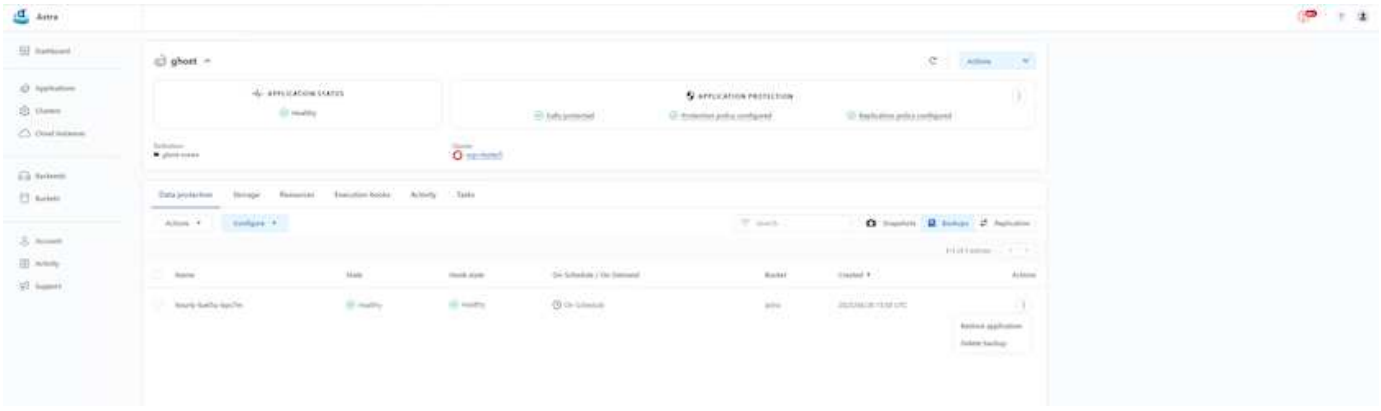


Sichern und Wiederherstellen mit ACC

Ein Backup basiert auf einem Snapshot. ACC kann Snapshot Kopien mithilfe von CSI erstellen und Backups mithilfe der zeitpunktgenauen Snapshot Kopie durchführen. Das Backup wird in einem externen Objektspeicher abgelegt (alle s3-kompatibel einschließlich ONTAP S3 an einem anderen Standort). Die Schutzrichtlinie kann für geplante Backups und die Anzahl der zu bewahrenden Backup-Versionen konfiguriert werden. Der minimale RPO beträgt eine Stunde.

Wiederherstellen einer Anwendung aus einer Sicherung mit ACC

ACC stellt die Applikation aus dem S3-Bucket wieder her, in dem die Backups gespeichert werden.



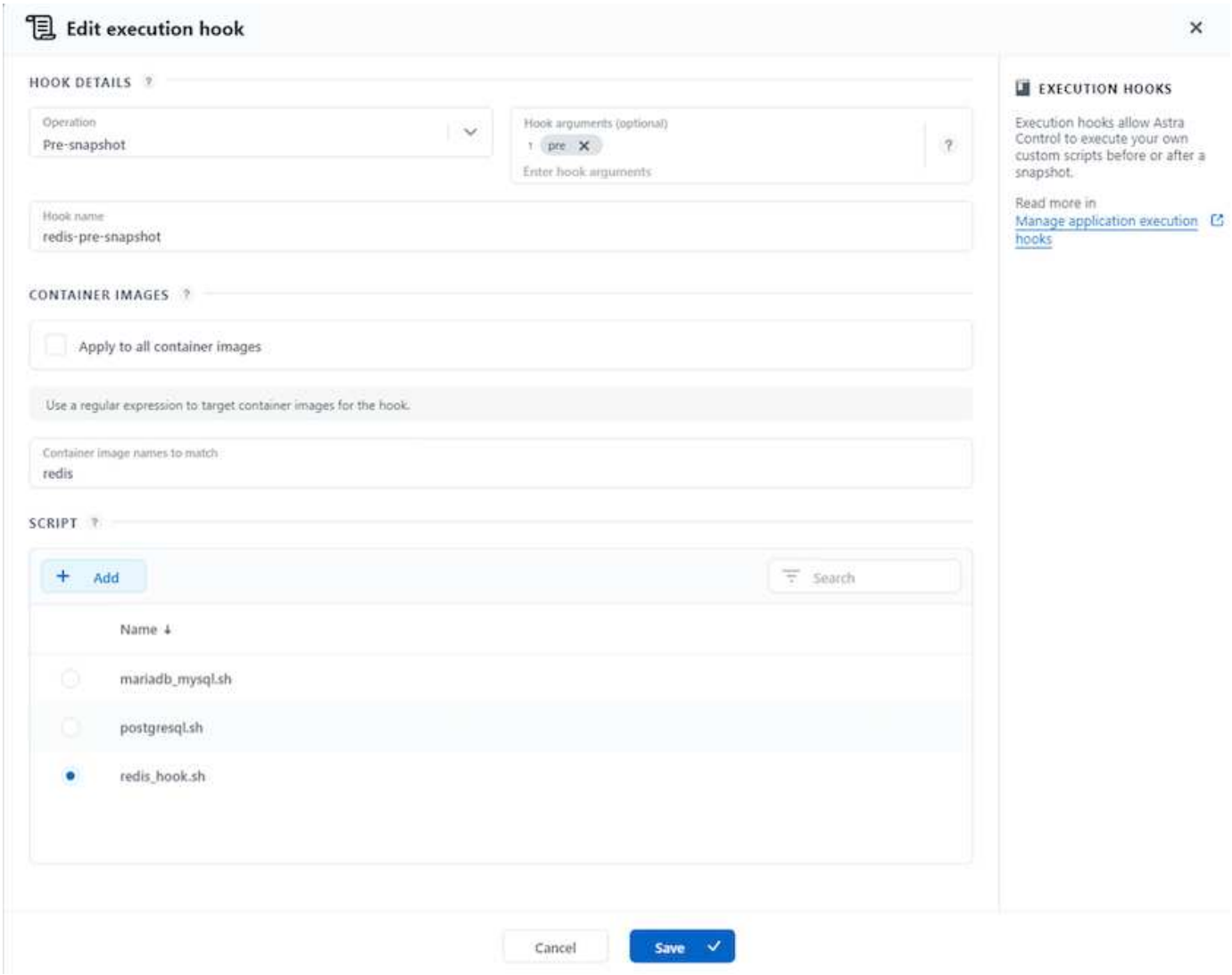
Anwendungsspezifische Ausführungshaken

Darüber hinaus können Ausführungshaken so konfiguriert werden, dass sie in Verbindung mit einer Datenschutzoperation einer verwalteten App ausgeführt werden. Obwohl die Datensicherungsfunktionen auf Storage-Array-Ebene verfügbar sind, sind für Backups und Restores häufig zusätzliche Schritte erforderlich, um die Konsistenz der Applikationen zu erhöhen. Die App-spezifischen zusätzlichen Schritte können sein: - Vor oder nach dem Erstellen einer Snapshot-Kopie. - Vor oder nach der Erstellung einer Sicherung. - Nach der Wiederherstellung aus einer Snapshot-Kopie oder Backup.

Astra Control kann diese applikationsspezifischen Schritte ausführen, die als benutzerdefinierte Skripte, sogenannte Execution Hooks, codiert werden.

"NetApp Verda GitHub Projekt" Diese Lösung bietet Ausführungshaken für gängige Cloud-native Applikationen und ermöglicht so einen einfachen, robusten und einfach zu orchestrierten Schutz von Applikationen. Sie können sich gerne an diesem Projekt beteiligen, wenn Sie genügend Informationen für eine Anwendung haben, die sich nicht im Repository befindet.

Beispiel-Ausführungshaken für Pre-Snapshot einer redis-Anwendung.



Replikation mit ACC

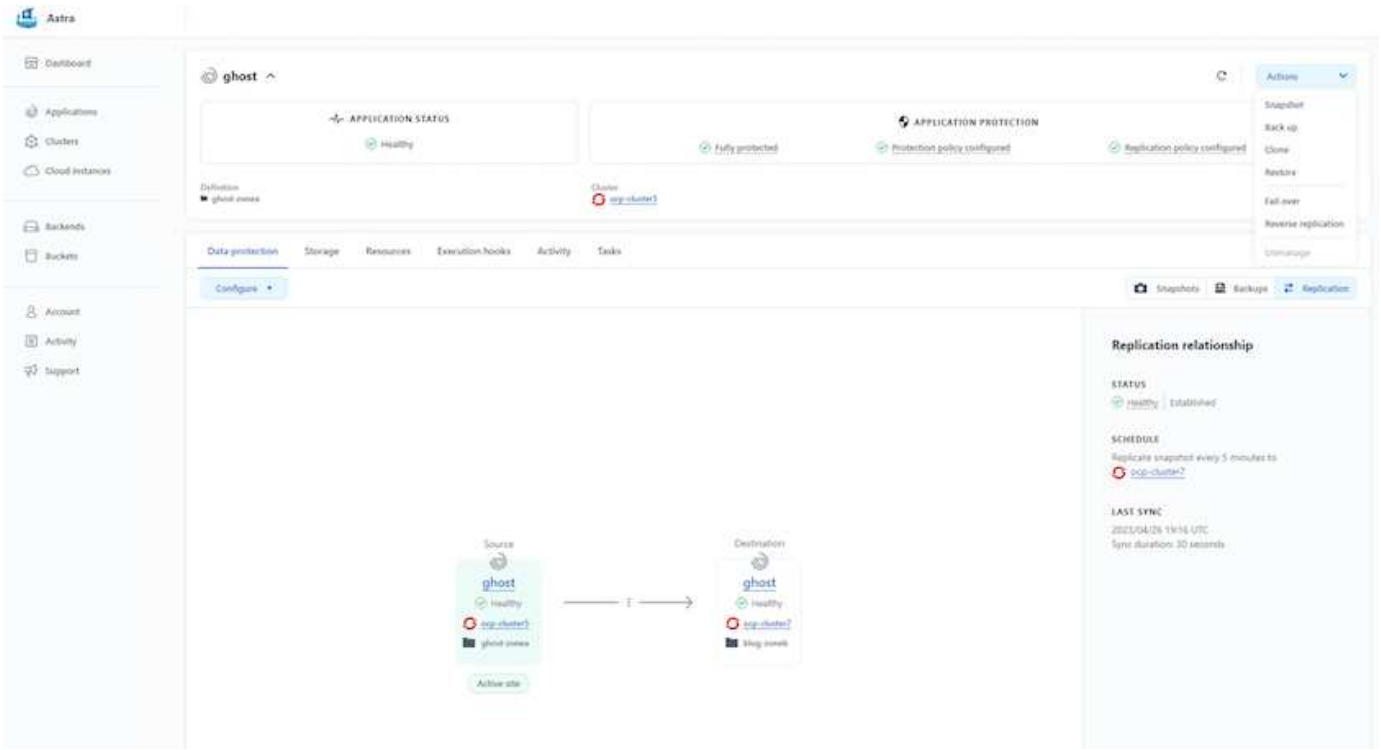
Für regionalen Schutz oder für eine Lösung mit niedriger RPO und RTO, kann eine Applikation auf eine andere Kubernetes-Instanz repliziert werden, die an einem anderen Standort, vorzugsweise in einer anderen Region,

ausgeführt wird. ACC verwendet ONTAP Async SnapMirror mit einem Recovery Point Objective von nur 5 Minuten. Die Replizierung wird durch eine Replizierung zu ONTAP durchgeführt. Bei einem Failover werden die Kubernetes-Ressourcen im Ziel-Cluster erstellt.

Beachten Sie, dass sich die Replizierung von den Backup- und Restore-Prozessen unterscheidet, bei denen das Backup auf S3 erfolgt und die Wiederherstellung von S3 durchgeführt wird. Weitere Details zu den Unterschieden zwischen den beiden Arten der Datensicherung finden Sie unter folgendem Link: here.

Siehe "Hier" Anweisungen zur Einrichtung von SnapMirror finden Sie.

SnapMirror mit ACC



speichertreiber für san-Economy und nas-Economy unterstützen keine Replikationsfunktion. Siehe "Hier" Entnehmen.

Demovideo:

"Demo-Video über Disaster Recovery mit Astra Control Center"

Datensicherung mit Astra Control Center

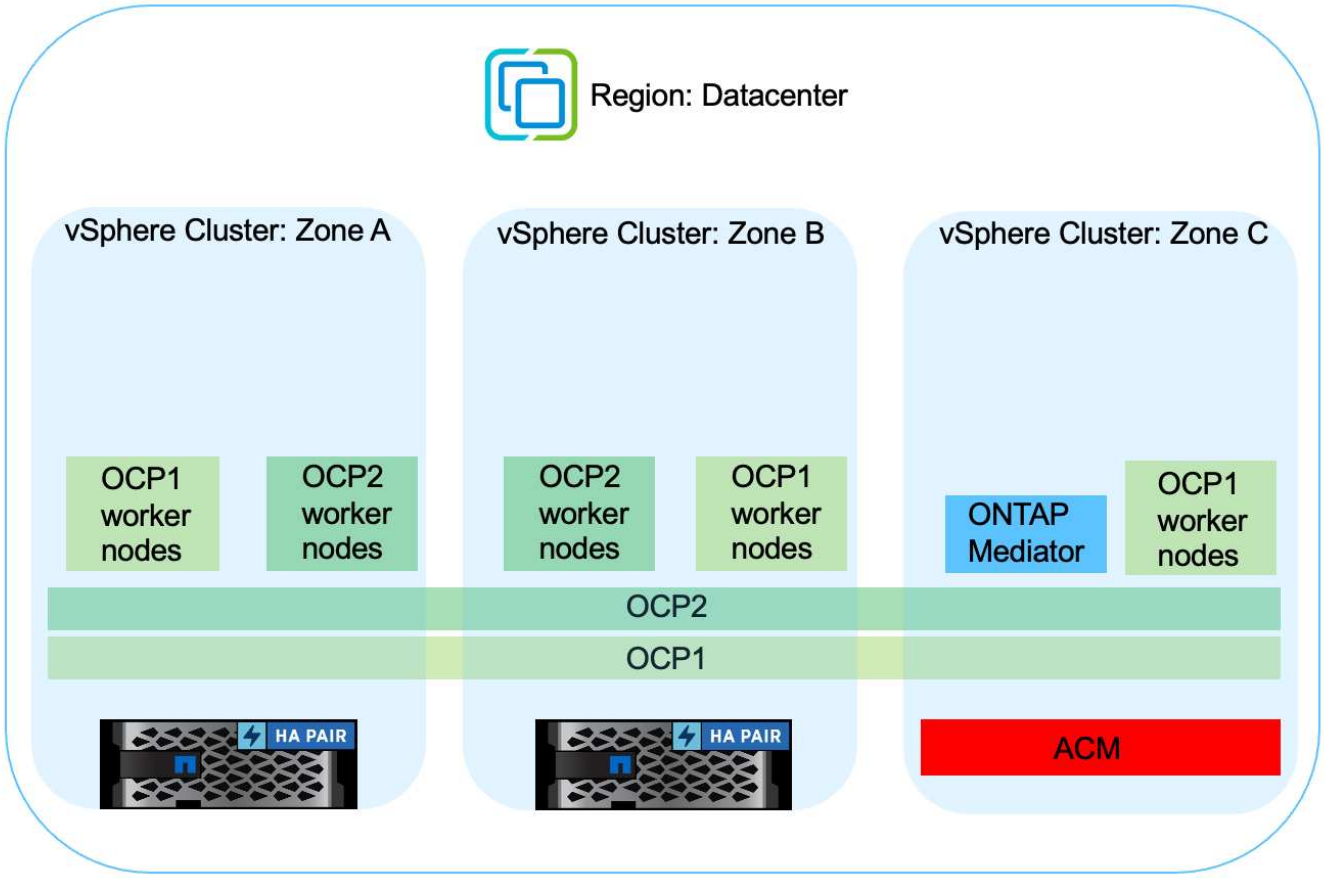
Business Continuity mit MetroCluster

Die meisten unserer Hardware-Plattform für ONTAP verfügt über Hochverfügbarkeitsfunktionen zum Schutz vor Geräteausfällen, um ein diasteres Recovery zu vermeiden. Um jedoch vor Feuer oder anderen Zwischenfällen zu schützen und das Geschäft mit RPO von null und RTO von geringem Wert fortzuführen, kommt oft eine MetroCluster Lösung zum Einsatz.

Kunden, die derzeit über ein ONTAP System verfügen, können sich auf MetroCluster erweitern, indem sie unterstützte ONTAP Systeme innerhalb der genannten Entfernungseinschränkungen hinzufügen, um Disaster

Recovery auf Zonenebene durchzuführen. Astra Trident unterstützt das CSI (Container Storage Interface) NetApp ONTAP, einschließlich der MetroCluster-Konfiguration sowie weitere Optionen wie Cloud Volumes ONTAP, Azure NetApp Files, AWS FSX für NetApp ONTAP usw. Astra Trident bietet fünf Storage-Treiberoptionen für ONTAP und alle werden für die MetroCluster Konfiguration unterstützt. Siehe "Hier" Weitere Informationen zu von Astra Trident unterstützten ONTAP Storage-Treibern.

Für die MetroCluster-Lösung ist eine Layer-2-Netzwerkerweiterung oder -Fähigkeit erforderlich, um von beiden Fehlerdomänen aus auf dieselbe Netzwerkadresse zuzugreifen. Sobald die MetroCluster-Konfiguration eingerichtet ist, ist die Lösung für Applikationseigentümer transparent, da alle Volumes in der MetroCluster svm gesichert sind und die Vorteile von SyncMirror (RPO Null) nutzen.



Geben Sie für die Trident Back-End-Konfiguration (TBC) bei Verwendung der MetroCluster-Konfiguration keine Daten-LIF und SVM an. Geben Sie die SVM-Management-IP für die Management-LIF an und verwenden Sie die vsadmin-Rollen-Anmeldedaten.

Einzelheiten zu den Datensicherungsfunktionen von Astra Control Center sind erhältlich "Hier"

Datenmigration über Astra Control Center

Auf dieser Seite werden die Optionen für die Datenmigration von Container-Workloads auf Red hat OpenShift-Clustern mit Astra Control Center (ACC) angezeigt.

Kubernetes-Applikationen müssen häufig von einer Umgebung in eine andere verschoben werden. Um eine Applikation zusammen mit ihren persistenten Daten zu migrieren, kann NetApp ACC genutzt werden.

Datenmigration zwischen verschiedenen Kubernetes-Umgebungen

ACC unterstützt verschiedene Kubernetes-Varianten, darunter Google Anthos, Red hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Upstream Kubernetes, Usw. Weitere Details finden Sie unter "Hier".

Um die Anwendung von einem Cluster zu einem anderen zu migrieren, können Sie eine der folgenden Funktionen von ACC verwenden:

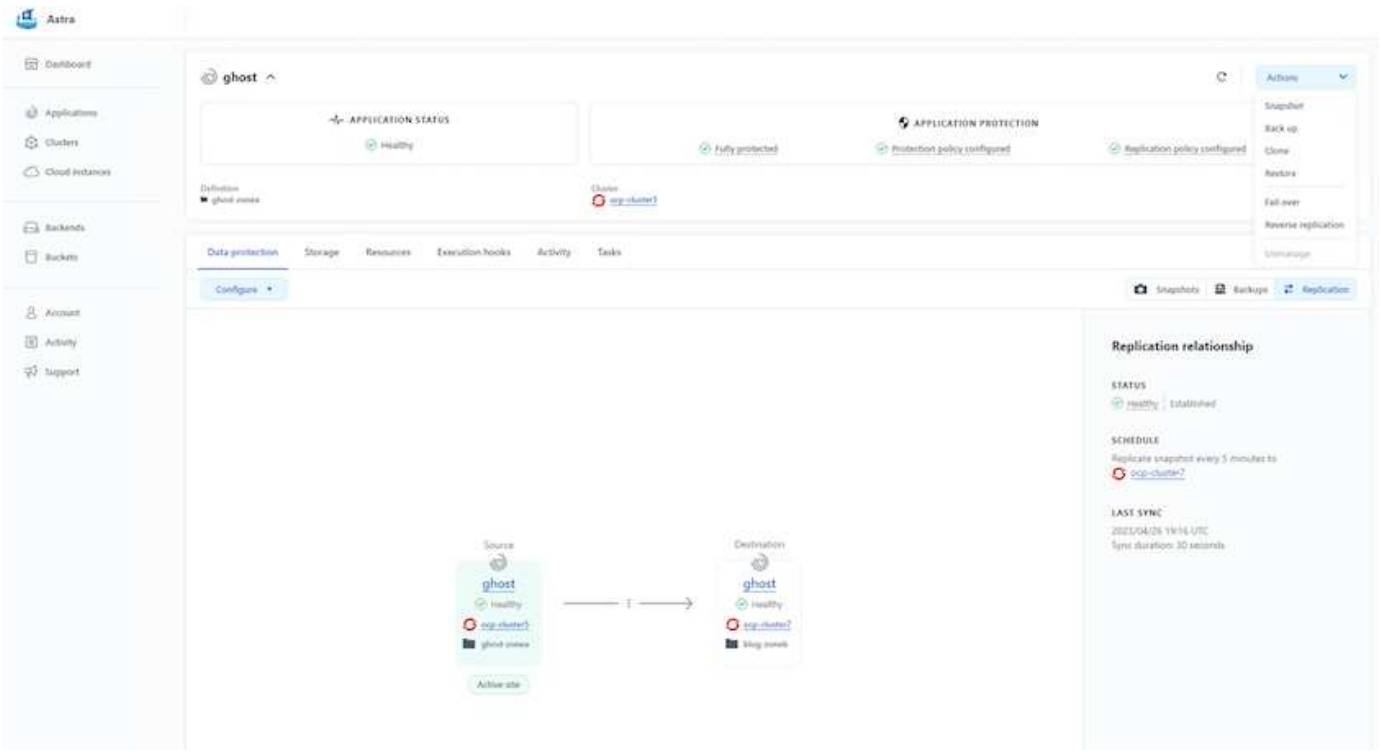
- **Replikation**
- **Sicherung und Wiederherstellung**
- **Klon**

Siehe "Abschnitt zur Datensicherung" Für die Optionen **Replikation und Backup und Restore**.

Siehe "Hier" Für weitere Details über **Klonen**.

> Die Astra Replizierungsfunktion wird nur mit der Trident Container Storage Interface (CSI) unterstützt. Die Replikation wird jedoch nicht von nas-Economy- und san-Economy-Treibern unterstützt.

Durchführen der Datenreplikation mit ACC



NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Überblick

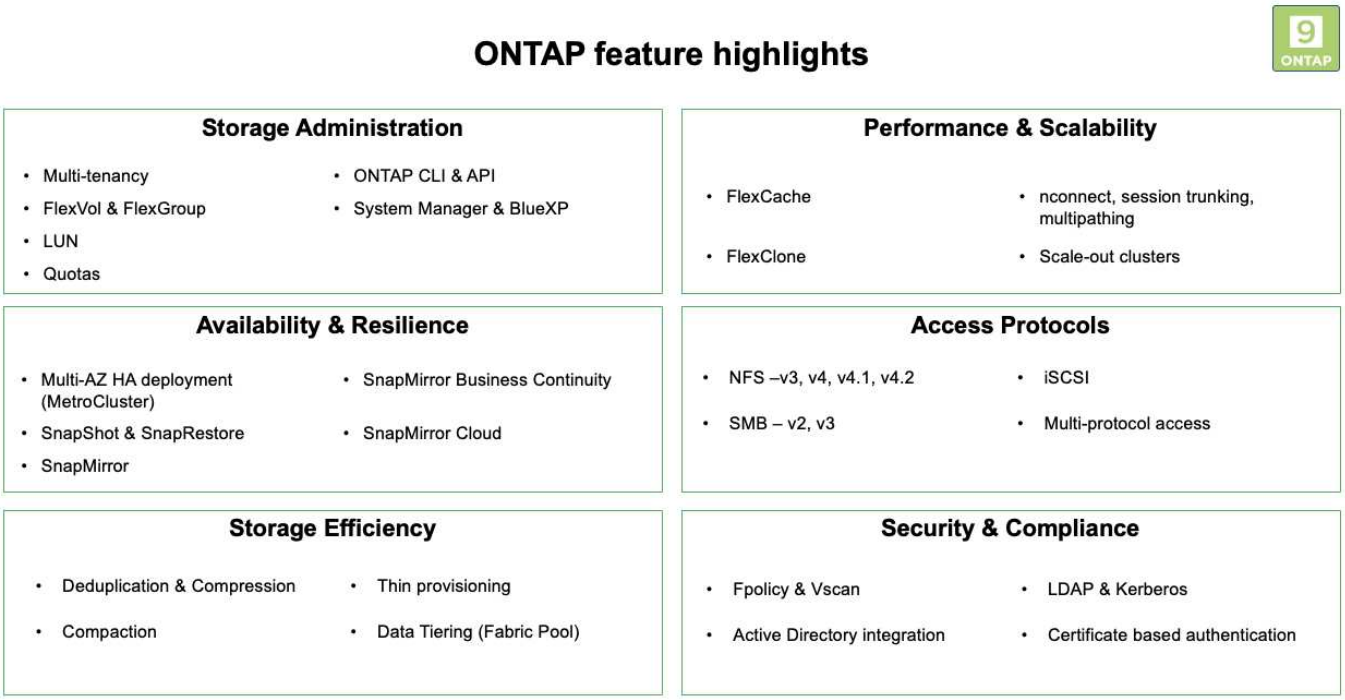
Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von

Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Implementierungen.

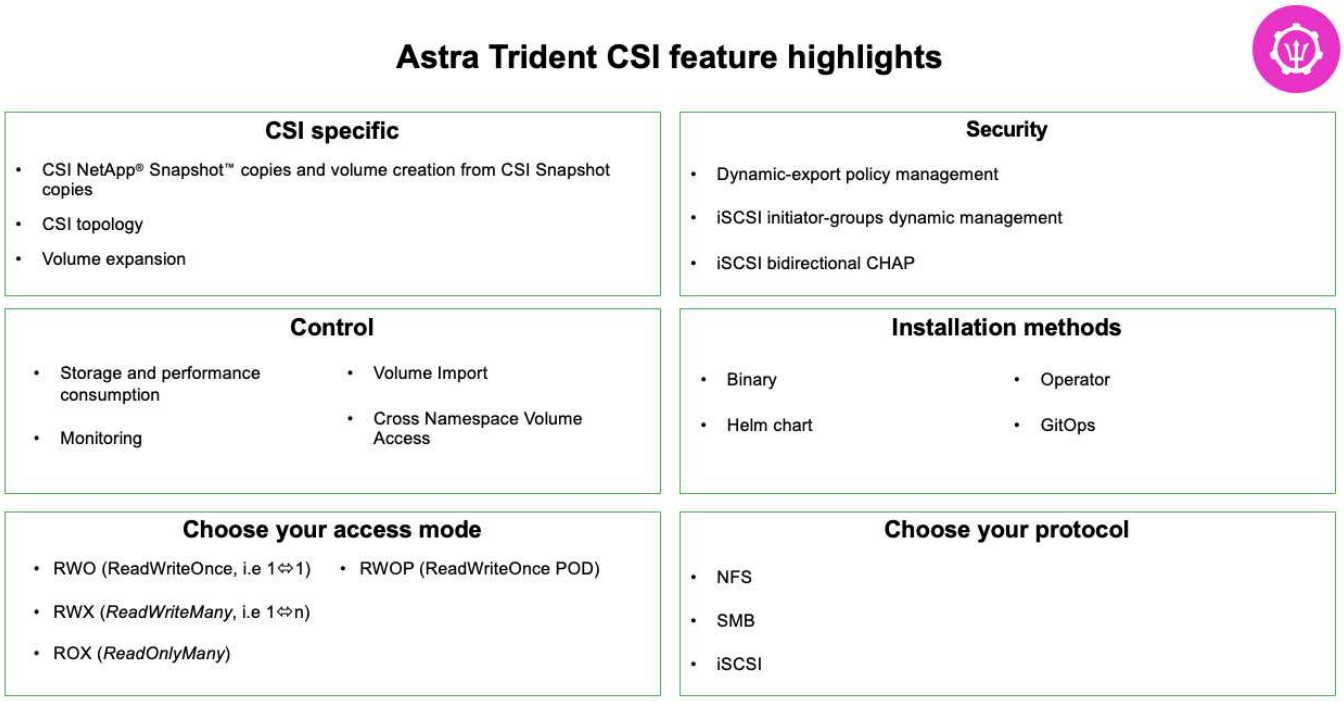
- Automatisierter, lokaler Storage:
  - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
  - NetApp Keystone stellt Storage-als-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
  - NetApp Cloud Volumes ONTAP(CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
  - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern



NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.



Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.

Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "Astra-Dokumentation" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

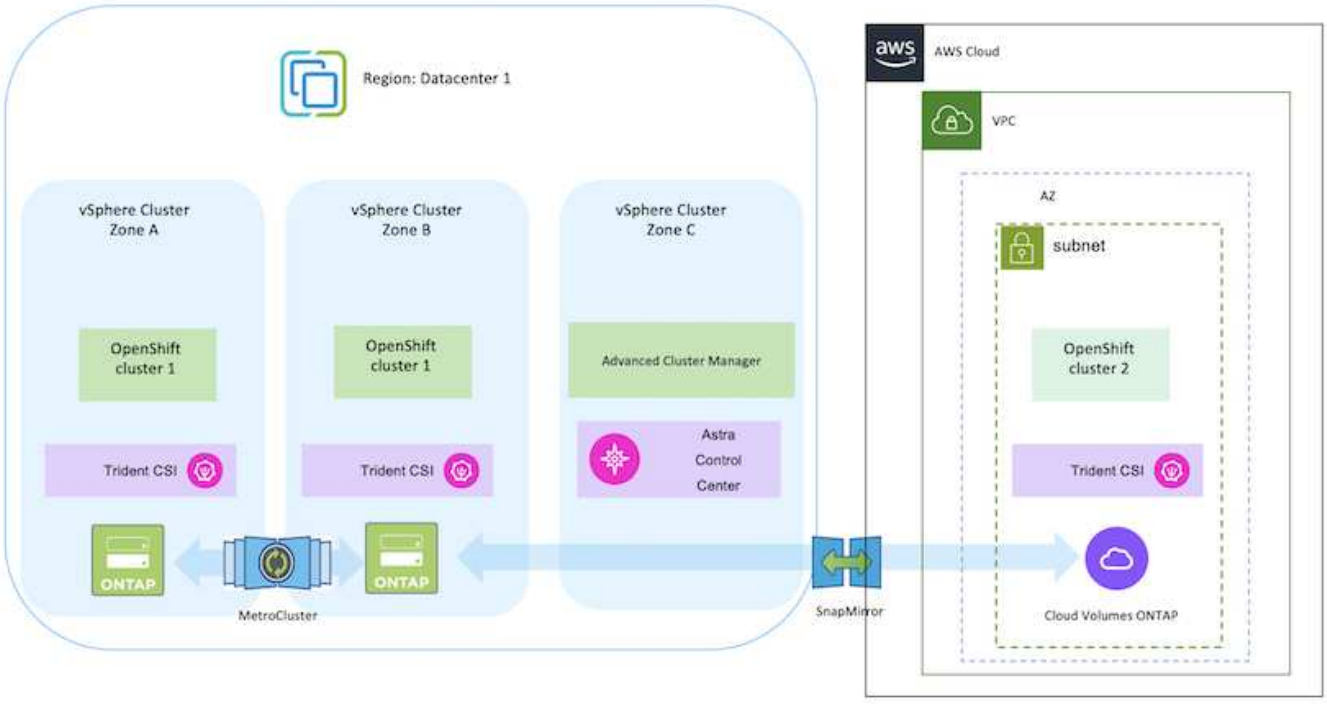
NetApp Lösung mit Container-Plattform-Workloads von Red hat OpenShift in der Hybrid Cloud

Kunden sind möglicherweise an einem Punkt ihrer Modernisierungsstrategie, wenn sie einige ausgewählte Workloads oder alle Workloads aus ihren Datacentern in die Cloud verschieben möchten. Sie können aus verschiedenen Gründen dafür entscheiden, selbst gemanagte OpenShift-Container und selbst gemanagten NetApp Storage in der Cloud zu verwenden. Sie sollten die Container-Plattform Red hat OpenShift (OCP) in der Cloud planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für die Migration ihrer Container-Workloads aus ihren Rechenzentren zu schaffen. Die OCP-Cluster können in ihren Datacentern auf VMware oder Bare Metal bereitgestellt werden und in AWS, Azure oder Google Cloud in der Cloud-Umgebung.

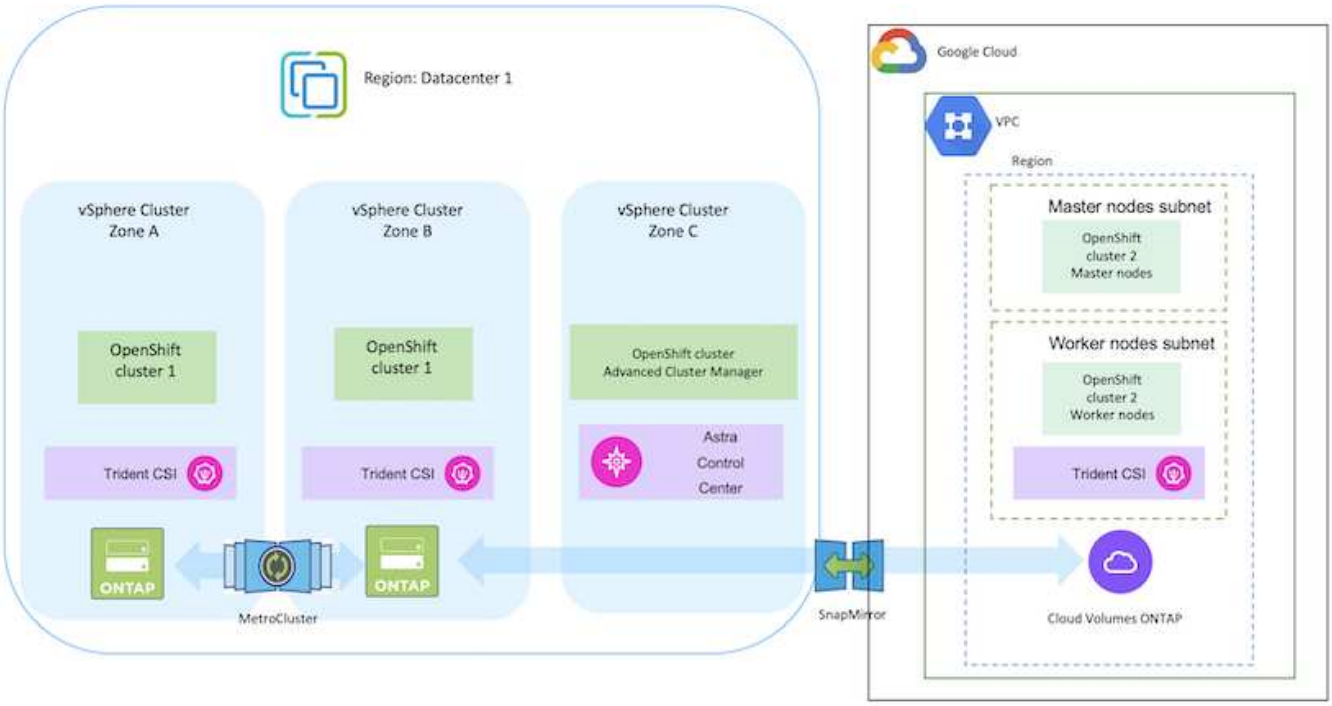
NetApp Cloud Volumes ONTAP Storage bietet Datensicherung, Zuverlässigkeit und Flexibilität für Container-Implementierungen in AWS, Azure und Google Cloud. Astra Trident dient als dynamische Storage-bereitstellung zur Nutzung des persistenten Cloud Volumes ONTAP Storage für zustandsbehaftete Applikationen von Kunden. Astra Control Center kann zur Orchestrierung der vielen Datenmanagementanforderungen zustandsbehafteter Applikationen eingesetzt werden, wie zum Beispiel Datensicherung, Migration und Business Continuity.

Datensicherungslösung und Migrationslösung für OpenShift-Container-Workloads in einer Hybrid Cloud mithilfe von Astra Control Center

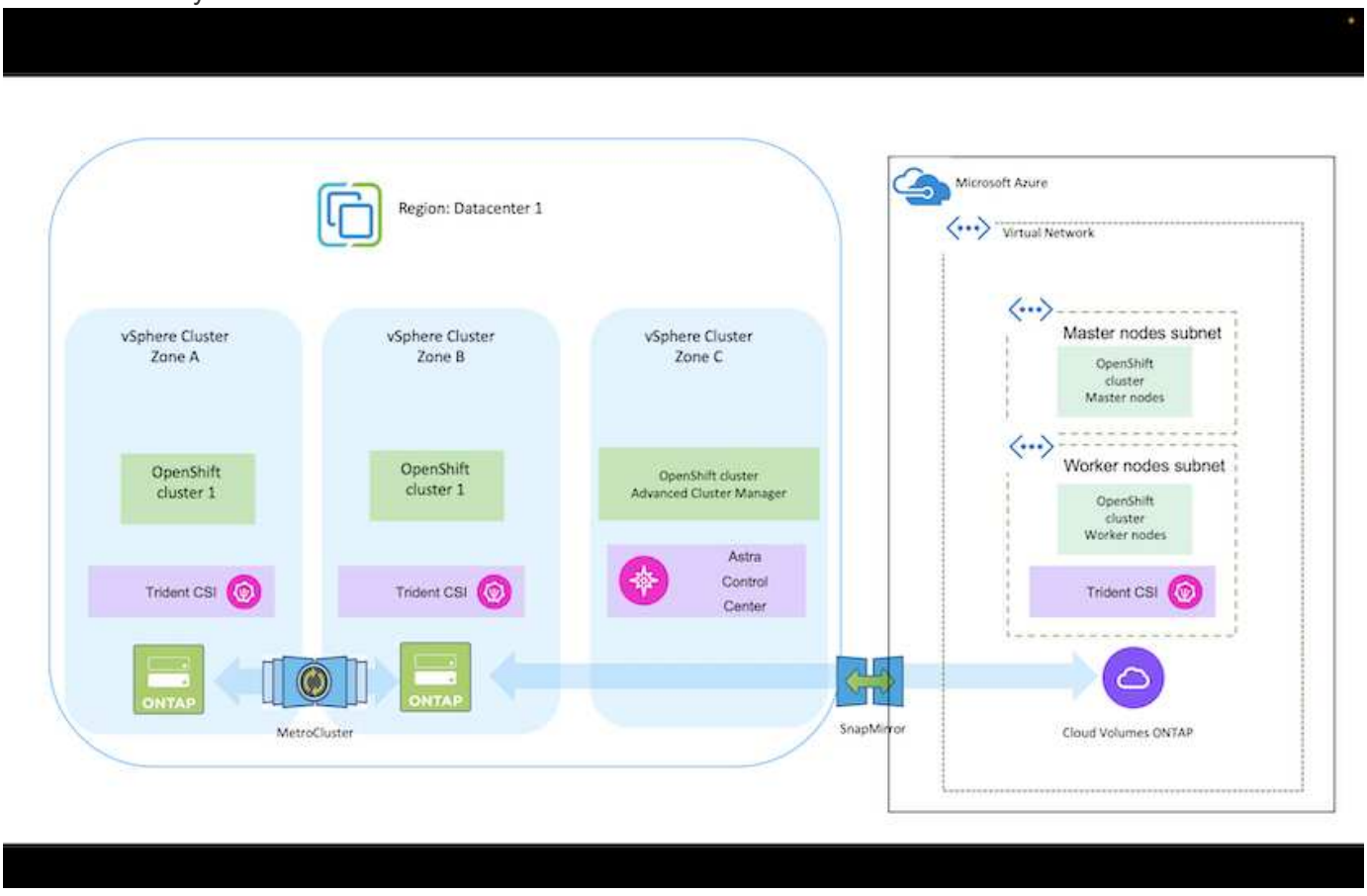
On-Premises- und AWS



On-Premises und Google Cloud



On-Premises-Systeme und Azure Cloud



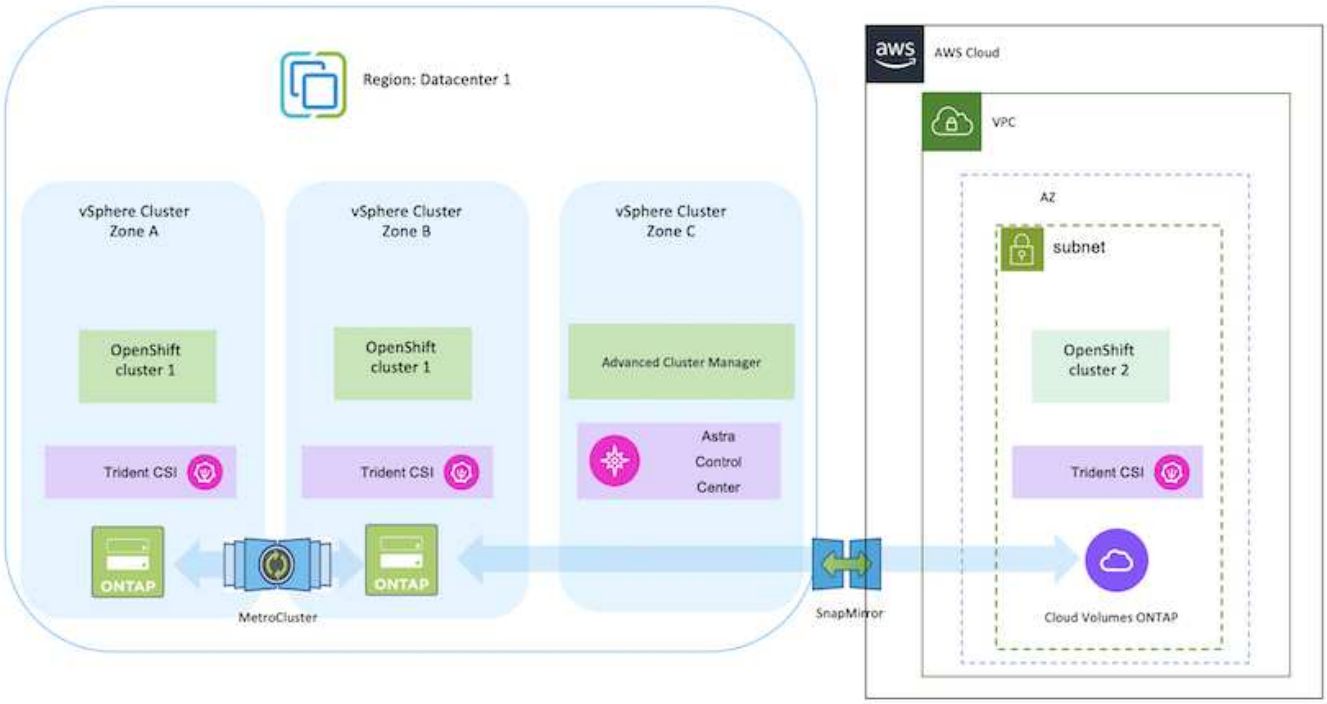
Implementierung und Konfiguration der Container-Plattform Red hat OpenShift auf AWS

In diesem Abschnitt wird ein High-Level-Workflow beschrieben, in dem Sie OpenShift-

Cluster in AWS einrichten und managen und zustandsbehaftete Anwendungen darauf implementieren. Es zeigt die Nutzung von NetApp Cloud Volumes ONTAP Storage mit Hilfe von Astra Trident zur Bereitstellung persistenter Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.

Es gibt verschiedene Möglichkeiten zur Implementierung von Red hat OpenShift Container-Plattform-Clustern auf AWS. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "Ressourcen".

Das folgende Diagramm zeigt die Cluster, die auf AWS implementiert und über ein VPN mit dem Datacenter verbunden sind.



Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Installieren Sie über Advanced Cluster Management einen OCP-Cluster in AWS.

- Erstellen Sie eine VPC mit einer Site-to-Site-VPN-Verbindung (mit pfsense), um eine Verbindung zum On-Premises-Netzwerk herzustellen.
- Das Netzwerk vor Ort verfügt über eine Internetverbindung.
- 3 private Subnetze in 3 verschiedenen AZS erstellen.
- Erstellen Sie eine Route 53 private gehostete Zone und einen DNS-Resolver für die VPC.

Erstellen Sie mithilfe des ACM-Assistenten (Advanced Cluster Management) OpenShift-Cluster auf AWS. Siehe Anweisungen "Hier".

Sie können das Cluster auch in AWS über die OpenShift Hybrid Cloud-Konsole erstellen. Siehe "Hier" Weitere Anweisungen.

Wenn Sie den Cluster mit ACM erstellen, können Sie die Installation anpassen, indem Sie die yaml-Datei nach dem Ausfüllen der Details in der Formularansicht bearbeiten. Nach dem Erstellen des Clusters können Sie sich über ssh bei den Nodes des Clusters zur Fehlerbehebung oder zur manuellen Konfiguration anmelden. Verwenden Sie den SSH-Schlüssel, den Sie während der Installation angegeben haben, und den Benutzernamen-Kern, um sich anzumelden.

Implementieren Sie Cloud Volumes ONTAP in AWS mit BlueXP.

- Installieren Sie den Connector in einer lokalen VMware-Umgebung. Siehe Anweisungen "Hier".
- Stellen Sie über den Connector eine CVO-Instanz in AWS bereit. Siehe Anweisungen "Hier".

Der Connector kann auch in der Cloud-Umgebung installiert werden. Siehe "Hier" Finden Sie weitere Informationen.

Installation von Astra Trident im OCP Cluster

- Implementieren Sie Trident Operator mit Helm. Siehe Anweisungen "Hier"
- Back-End und Storage-Klasse erstellen Siehe Anweisungen "Hier".

Fügen Sie das OCP-Cluster in AWS zum Astra Control Center hinzu.

Fügen Sie das OCP-Cluster in AWS zum Astra Control Center hinzu.

Verwendung der CSI-Topology-Funktion von Trident für Multi-Zone-Architekturen

Heute können Cloud-Provider Kubernetes/OpenShift-Cluster-Administratoren Nodes der zonbasierten Cluster erstellen. Die Nodes können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über verschiedene Regionen hinweg befinden. Astra Trident verwendet CSI Topology, um die Provisionierung von Volumes für Workloads in einer Multi-Zone-Architektur zu vereinfachen. Mithilfe der CSI Topology-Funktion kann der Zugriff auf Volumes auf einen Teil von Nodes basierend auf Regionen und Verfügbarkeitszonen begrenzt werden. Siehe "Hier" Entnehmen.

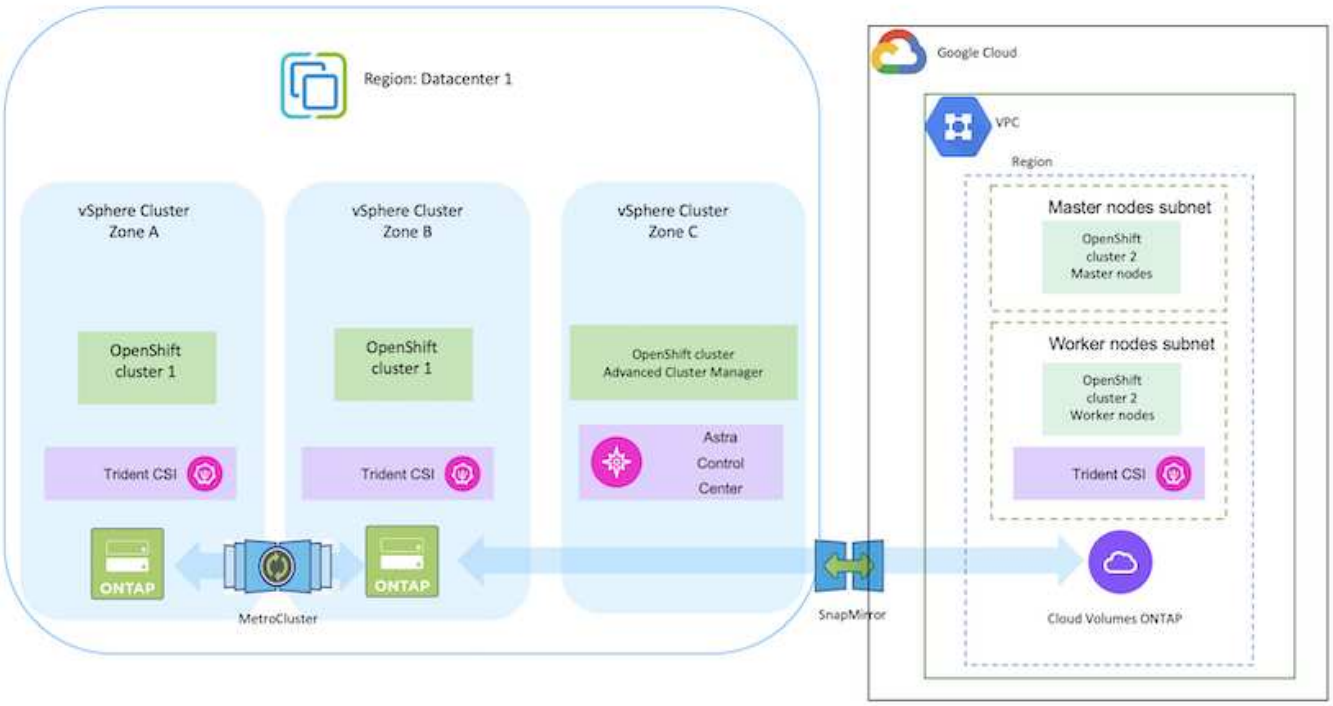
Kubernetes unterstützt zwei Volume-Bindungsmodi: - Wenn ***VolumeBindingMode* auf *Immediate*** (Standard) eingestellt ist, erstellt Astra Trident das Volume ohne Topologieorientierung. Persistente Volumes werden erstellt, ohne dass sie von den Planungsanforderungen des anfragenden Pods abhängig sind. - Wenn ***VolumeBindingMode* auf *WaitForFirstConsumer*** gesetzt wird, wird die Erstellung und Bindung eines Persistent Volume für eine PVC verzögert, bis ein Pod, der die PVC verwendet, geplant und erstellt wird. Auf diese Weise werden Volumes erstellt, um Planungseinschränkungen zu erfüllen, die durch Topologieanforderungen durchgesetzt werden. Astra Trident Storage-Back-Ends können für die selektive Bereitstellung von Volumes basierend auf Verfügbarkeitszonen entwickelt werden (Topologieorientiertes Back-End). Bei StorageClasses, die ein solches Backend nutzen, wird ein Volume nur erstellt, wenn es von einer Applikation angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologieorientierte StorageClass) "Hier" Entnehmen.

Bereitstellung und Konfiguration der Container-Plattform Red hat OpenShift auf GCP

Bereitstellung und Konfiguration der Container-Plattform Red hat OpenShift auf GCP

Dieser Abschnitt beschreibt einen allgemeinen Workflow zur Einrichtung und Verwaltung von OpenShift-Clustern in GCP und zur Bereitstellung zustandsbehafteter Anwendungen. Es zeigt die Nutzung von NetApp Cloud Volumes ONTAP Storage mit Hilfe von Astra Trident zur Bereitstellung persistenter Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.

Das folgende Diagramm zeigt die auf GCP bereitgestellten und über ein VPN mit dem Datacenter verbundenen Cluster.



Es gibt verschiedene Möglichkeiten, Red hat OpenShift Container Platform Cluster in GCP bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "Ressourcen".

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Installieren Sie einen OCP-Cluster auf GCP über die CLI.

- Stellen Sie sicher, dass Sie alle angegebenen Voraussetzungen erfüllt haben "Hier".
- Für die VPN-Verbindung zwischen On-Premises und GCP wurde eine pfsense VM erstellt und konfiguriert. Anweisungen hierzu finden Sie unter "Hier".
  - Die Remote-Gateway-Adresse in pfsense kann erst konfiguriert werden, nachdem Sie ein VPN-Gateway in der Google Cloud Platform erstellt haben.
  - Die Remote-Netzwerk-IP-Adressen für die Phase 2 können erst konfiguriert werden, nachdem das OpenShift-Cluster-Installationsprogramm ausgeführt und die Infrastrukturkomponenten für den Cluster erstellt hat.
  - Das VPN in Google Cloud kann erst konfiguriert werden, nachdem durch das Installationsprogramm die Infrastrukturkomponenten für den Cluster erstellt wurden.
- Jetzt den OpenShift-Cluster auf GCP installieren.
  - Rufen Sie das Installationsprogramm und das Pull-Geheimnis ab, und implementieren Sie den Cluster wie in der Dokumentation beschrieben "Hier".
  - Bei der Installation wird ein VPC-Netzwerk in der Google Cloud Platform erstellt. Außerdem wird eine private Zone in Cloud DNS erstellt und Datensätze hinzugefügt.
    - Verwenden Sie die CIDR-Blockadresse des VPC-Netzwerks, um pfsense zu konfigurieren und die VPN-Verbindung aufzubauen. Stellen Sie sicher, dass Firewalls korrekt eingerichtet sind.
    - Fügen Sie im DNS der lokalen Umgebung mithilfe der IP-Adresse in den A-Datensätzen des Google Cloud DNS Einen Eintrag hinzu.
  - Die Installation des Clusters ist abgeschlossen und stellt eine kubeconfig-Datei sowie einen Benutzernamen und ein Passwort für die Anmeldung bei der Konsole des Clusters bereit.

Implementieren Sie Cloud Volumes ONTAP in GCP mit BlueXP.

- Installieren Sie einen Connector in Google Cloud. Siehe Anweisungen "Hier".
- Stellen Sie über den Connector eine CVO-Instanz in Google Cloud bereit. Anweisungen finden Sie hier. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Astra Trident im OCP-Cluster in GCP installieren

- Wie in der Abbildung dargestellt, gibt es viele Methoden für die Implementierung von Astra Trident "Hier".
- Für dieses Projekt wurde Astra Trident mithilfe der Anweisungen manuell implementiert, indem der Astra Trident Operator installiert wurde "Hier".
- Back-End- und Storage-Klassen erstellen Siehe Anweisungen "Hier".

Fügen Sie den OCP-Cluster in GCP zum Astra Control Center hinzu.

- Erstellen Sie eine separate KubeConfig-Datei mit einer Cluster-Rolle, die die erforderlichen Mindestberechtigungen für das Management eines Clusters durch Astra Control enthält. Die Anweisungen sind zu finden "Hier".
- Fügen Sie das Cluster gemäß den Anweisungen zu Astra Control Center hinzu "Hier"

Verwendung der CSI-Topology-Funktion von Trident für Multi-Zone-Architekturen

Heute können Cloud-Provider Kubernetes/OpenShift-Cluster-Administratoren Nodes der zonbasierten Cluster erstellen. Die Nodes können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über verschiedene Regionen hinweg befinden. Astra Trident verwendet CSI Topology, um die Provisionierung von Volumes für Workloads in einer Multi-Zone-Architektur zu vereinfachen. Mithilfe der CSI Topology-Funktion kann der Zugriff auf Volumes auf einen Teil von Nodes basierend auf Regionen und Verfügbarkeitszonen begrenzt werden. Siehe "Hier" Entnehmen.

> Kubernetes unterstützt zwei Volume-Bindungsmodi: - Wenn ***VolumeBindingMode*** **auf** ***Immediate*** (Standard) eingestellt ist, erstellt Astra Trident das Volume ohne Topologieorientierung. Persistente Volumes werden erstellt, ohne dass sie von den Planungsanforderungen des anfragenden Pods abhängig sind. - Wenn ***VolumeBindingMode*** **auf** ***WaitForFirstConsumer*** gesetzt wird, wird die Erstellung und Bindung eines Persistent Volume für eine PVC verzögert, bis ein Pod, der die PVC verwendet, geplant und erstellt wird. Auf diese Weise werden Volumes erstellt, um Planungseinschränkungen zu erfüllen, die durch Topologieanforderungen durchgesetzt werden. Astra Trident Storage-Back-Ends können für die selektive Bereitstellung von Volumes basierend auf Verfügbarkeitszonen entwickelt werden (Topologieorientiertes Back-End). Bei StorageClasses, die ein solches Backend nutzen, wird ein Volume nur erstellt, wenn es von einer Applikation angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologieorientierte StorageClass) "Hier" Entnehmen.

Demonstrationsvideo

OpenShift Cluster-Installation auf der Google Cloud Platform

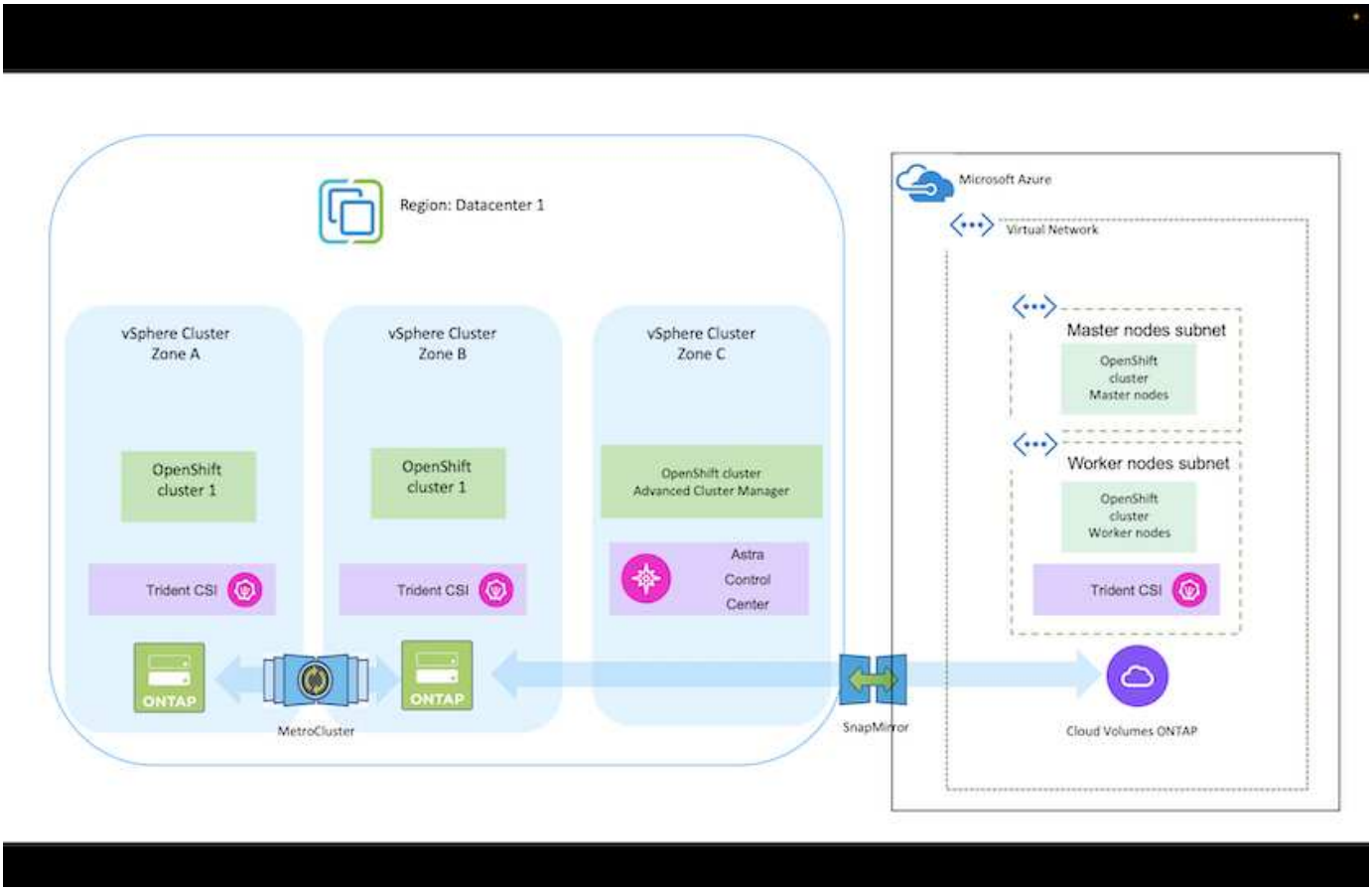
Importieren von OpenShift-Clustern in Astra Control Center

Implementierung und Konfiguration der Container-Plattform Red hat OpenShift auf Azure

Implementierung und Konfiguration der Container-Plattform Red hat OpenShift auf Azure

In diesem Abschnitt wird ein High-Level-Workflow beschrieben, in dem erläutert wird, wie OpenShift-Cluster in Azure eingerichtet und gemanagt und zustandsbehaftete Anwendungen darauf bereitgestellt werden. Er zeigt die Nutzung von NetApp Cloud Volumes ONTAP Storage mit Unterstützung von Astra Trident/Astra Control Provisioner für persistente Volumes. Einzelheiten zur Nutzung von Astra Control Center für die Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen werden bereitgestellt.

Das folgende Diagramm zeigt die auf Azure implementierten Cluster, die über ein VPN mit dem Datacenter verbunden sind.



Es gibt verschiedene Möglichkeiten zur Implementierung von Red hat OpenShift Container-Plattform-Clustern in Azure. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "Ressourcen".

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Installieren Sie einen OCP-Cluster in Azure über die CLI.

- Stellen Sie sicher, dass Sie alle angegebenen Voraussetzungen erfüllt haben "Hier".
- Erstellen Sie ein VPN, Subnetze und Netzwerksicherheitsgruppen sowie eine private DNS-Zone. Erstellen Sie ein VPN-Gateway und eine Site-to-Site-VPN-Verbindung.
- Für die VPN-Verbindung zwischen On-Premises und Azure wurde eine pfsense VM erstellt und konfiguriert. Anweisungen hierzu finden Sie unter "Hier".
- Rufen Sie das Installationsprogramm und das Pull-Geheimnis ab, und implementieren Sie den Cluster wie in der Dokumentation beschrieben "Hier".
- Die Installation des Clusters ist abgeschlossen und stellt eine kubeconfig-Datei sowie einen Benutzernamen und ein Passwort für die Anmeldung bei der Konsole des Clusters bereit.

Im Folgenden finden Sie eine Beispieldatei install-config.yaml.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
```

```
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

Implementieren Sie Cloud Volumes ONTAP in Azure mit BlueXP.

- Installieren Sie einen Connector in Azure. Siehe Anweisungen "Hier".
- Stellen Sie über den Connector eine CVO-Instanz in Azure bereit. Anweisungen finden Sie unter dem Link:https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [hier.]

Installation von Astra Control Provisioner im OCP Cluster in Azure

- Bei diesem Projekt wurde Astra Control Provisioner (ACP) auf allen Clustern installiert (On-Premises-Cluster, On-Premises-Cluster, in dem Astra Control Center implementiert ist, und der Cluster in Azure). Weitere Informationen zur Astra Control Provisionierung "Hier".
- Back-End- und Storage-Klassen erstellen Siehe Anweisungen "Hier".

Fügen Sie das OCP-Cluster in Azure dem Astra Control Center hinzu.

- Erstellen Sie eine separate KubeConfig-Datei mit einer Cluster-Rolle, die die erforderlichen Mindestberechtigungen für das Management eines Clusters durch Astra Control enthält. Die Anweisungen sind zu finden "Hier".
- Fügen Sie das Cluster gemäß den Anweisungen zu Astra Control Center hinzu "Hier"

Verwendung der CSI-Topology-Funktion von Trident für Multi-Zone-Architekturen

Heute können Cloud-Provider Kubernetes/OpenShift-Cluster-Administratoren Nodes der zonbasierten Cluster erstellen. Die Nodes können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über verschiedene Regionen hinweg befinden. Astra Trident verwendet CSI Topology, um die Provisionierung von Volumes für Workloads in einer Multi-Zone-Architektur zu vereinfachen. Mithilfe der CSI Topology-Funktion kann der Zugriff auf Volumes auf einen Teil von Nodes basierend auf Regionen und Verfügbarkeitszonen begrenzt werden. Siehe "Hier" Entnehmen.

> Kubernetes unterstützt zwei Volume-Bindungsmodi: - Wenn ***VolumeBindingMode*** **auf** ***Immediate*** (Standard) eingestellt ist, erstellt Astra Trident das Volume ohne Topologieorientierung. Persistente Volumes werden erstellt, ohne dass sie von den Planungsanforderungen des anfragenden Pods abhängig sind. - Wenn ***VolumeBindingMode*** **auf** ***WaitForFirstConsumer*** gesetzt wird, wird die Erstellung und Bindung eines Persistent Volume für eine PVC verzögert, bis ein Pod, der die PVC verwendet, geplant und erstellt wird. Auf diese Weise werden Volumes erstellt, um Planungseinschränkungen zu erfüllen, die durch Topologieanforderungen durchgesetzt werden. Astra Trident Storage-Back-Ends können für die selektive Bereitstellung von Volumes basierend auf Verfügbarkeitszonen entwickelt werden (Topologieorientiertes Back-End). Bei StorageClasses, die ein solches Backend nutzen, wird ein Volume nur erstellt, wenn es von einer Applikation angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologieorientierte StorageClass) "Hier" Entnehmen.

Demonstrationsvideo

Verwendung von Astra Control für Failover und Failback von Applikationen

Datensicherung über Astra Control Center

Auf dieser Seite werden die Datenschutzoptionen für Container-basierte Red hat OpenShift-Anwendungen angezeigt, die auf VMware vSphere oder in der Cloud mit Astra Control Center (ACC) ausgeführt werden.

Wenn Benutzer ihre Anwendungen mit Red hat OpenShift modernisieren, sollte eine Datenschutzstrategie eingerichtet werden, um sie vor versehentlichem Löschen oder anderen menschlichen Fehlern zu schützen. Häufig ist auch eine Sicherungsstrategie für gesetzliche Vorschriften oder Compliance-Zwecke erforderlich, um ihre Daten vor einem Diaster zu schützen.

Die Anforderungen an die Datensicherung reichen von dem Zurücksetzen auf eine zeitpunktgenaue Kopie bis hin zum automatischen Failover auf eine andere Fehlerdomäne ohne menschliches Eingreifen. Viele Kunden entscheiden sich für ONTAP als bevorzugte Storage-Plattform für ihre Kubernetes-Applikationen, da sie umfassende Funktionen wie Mandantenfähigkeit, Multiprotokoll, hohe Performance und Kapazität, Replizierung und Caching für Standorte an mehreren Standorten sowie Sicherheit und Flexibilität bieten.

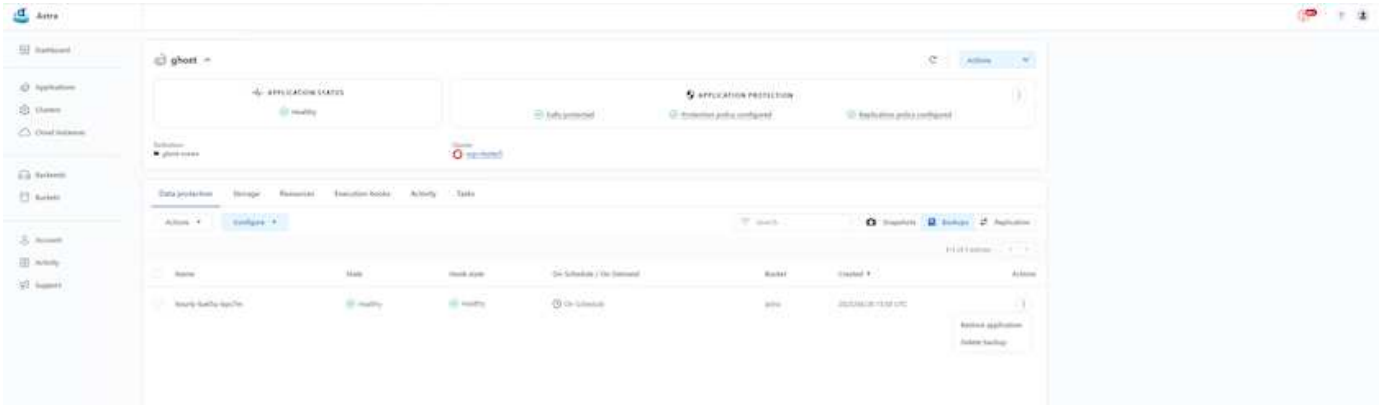
Möglicherweise haben Kunden als Erweiterung ihres Datacenters eine Cloud-Umgebung eingerichtet, um von

den Vorteilen der Cloud zu profitieren und gut vorbereitet zu sein, um ihre Workloads zu einem späteren Zeitpunkt zu verschieben. Für solche Kunden ist das Sichern ihrer OpenShift-Anwendungen und ihrer Daten in der Cloud-Umgebung unausweichlich. Anschließend können sie die Anwendungen und die zugehörigen Daten entweder in einem OpenShift-Cluster in der Cloud oder in ihrem Rechenzentrum wiederherstellen.

Sichern und Wiederherstellen mit ACC

Anwendungseigentümer können die von ACC erkannten Anwendungen überprüfen und aktualisieren. ACC kann Snapshot Kopien mithilfe von CSI erstellen und Backups mithilfe der zeitpunktgenauen Snapshot Kopie durchführen. Das Backup-Ziel kann ein Objektspeicher in der Cloud-Umgebung sein. Die Schutzrichtlinie kann für geplante Backups und die Anzahl der zu bewahrenden Backup-Versionen konfiguriert werden. Der minimale RPO beträgt eine Stunde.

Wiederherstellen einer Anwendung aus einer Sicherung mit ACC

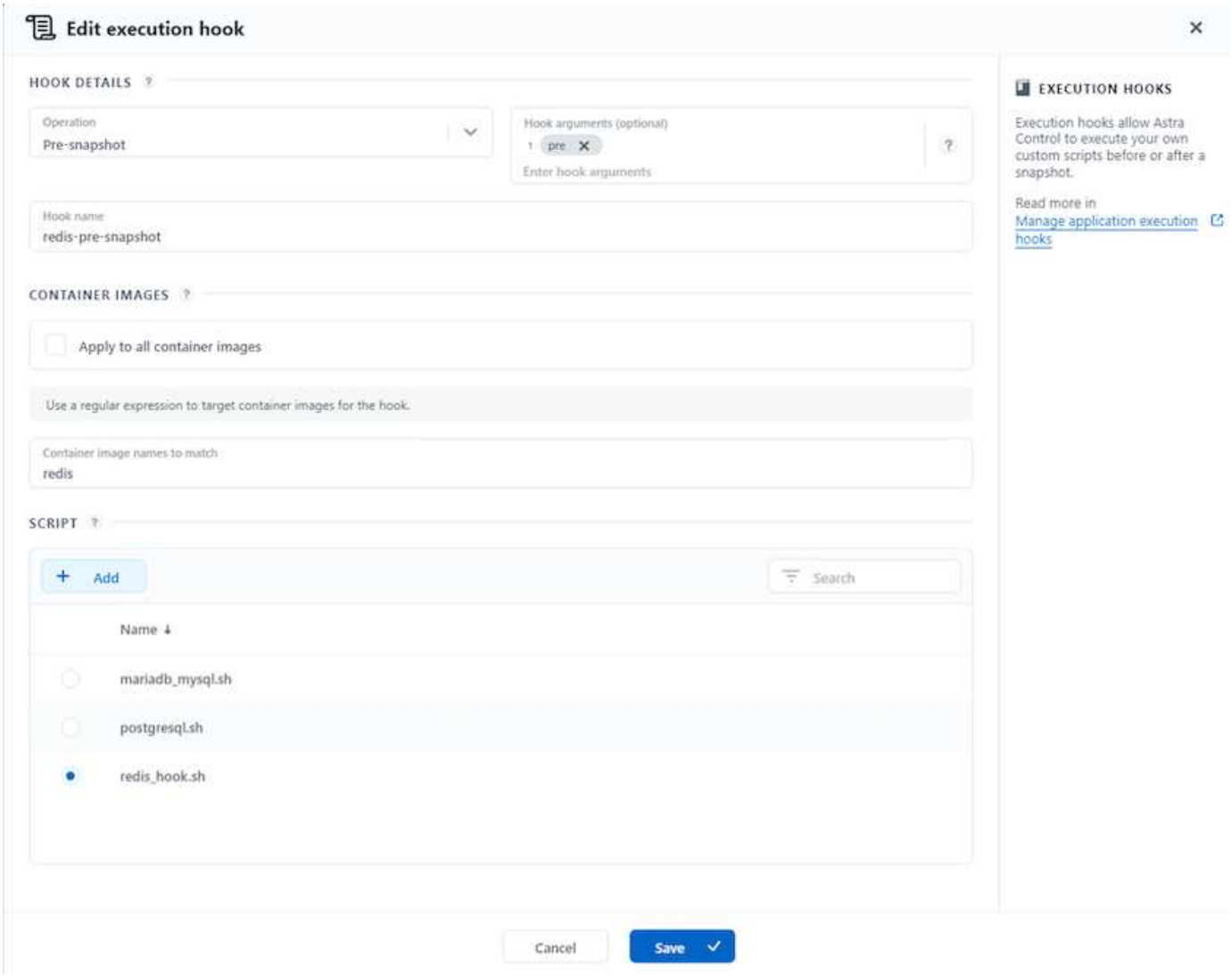


Anwendungsspezifische Ausführungshaken

Obwohl die Datensicherungsfunktionen auf Storage-Array-Ebene verfügbar sind, sind häufig zusätzliche Schritte erforderlich, um Backup- und Restore-Vorgänge applikationskonsistent zu gestalten. Die App-spezifischen zusätzlichen Schritte können sein: - Vor oder nach dem Erstellen einer Snapshot-Kopie. - Vor oder nach der Erstellung einer Sicherung. - Nach der Wiederherstellung aus einer Snapshot-Kopie oder Backup. Astra Control kann diese applikationsspezifischen Schritte ausführen, die als benutzerdefinierte Skripte, sogenannte Execution Hooks, codiert werden.

NetApp "Open-Source-Projekt Verda" Diese Lösung bietet Ausführungshaken für gängige Cloud-native Applikationen und ermöglicht so einen einfachen, robusten und einfach zu orchestrierten Schutz von Applikationen. Sie können sich gerne an diesem Projekt beteiligen, wenn Sie genügend Informationen für eine Anwendung haben, die sich nicht im Repository befindet.

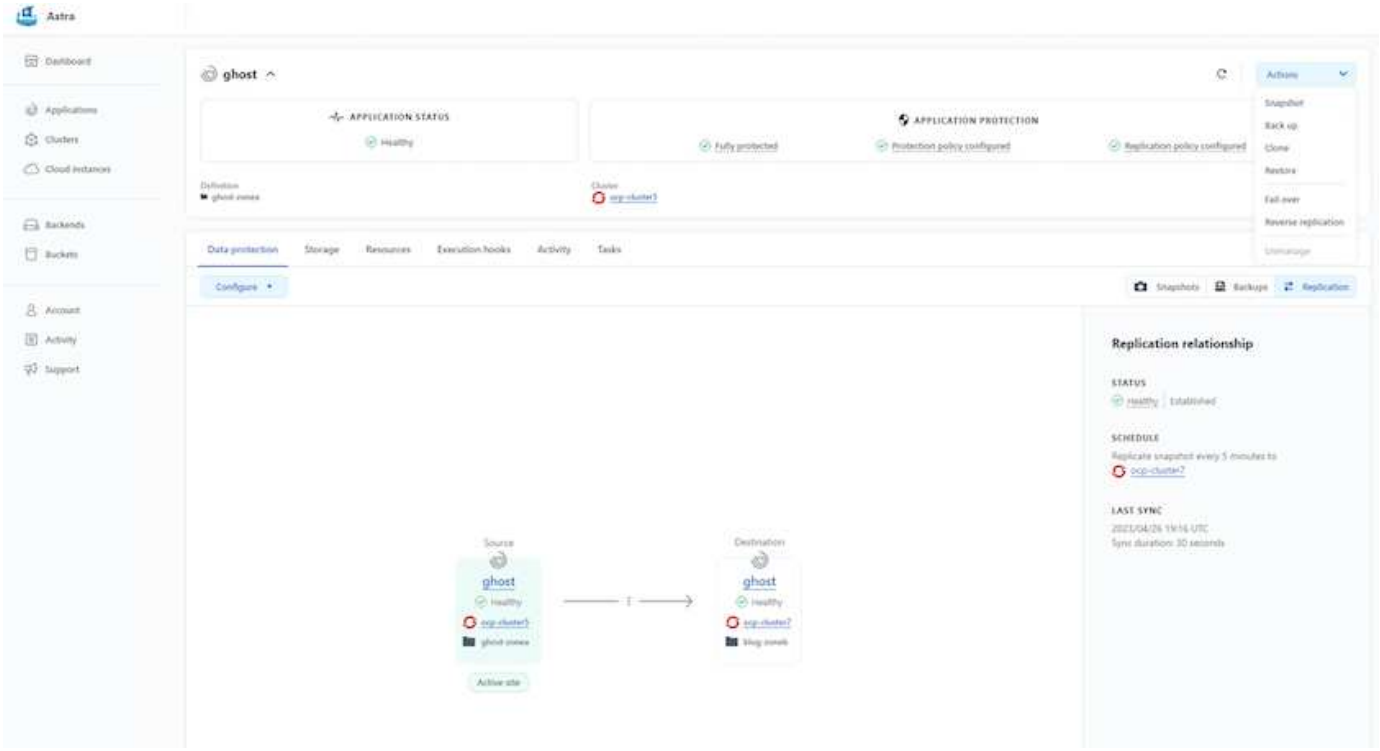
Beispiel-Ausführungshaken für Pre-Snapshot einer redis-Anwendung.



Replikation mit ACC

Für regionalen Schutz oder für eine Lösung mit niedriger RPO und RTO, kann eine Applikation auf eine andere Kubernetes-Instanz repliziert werden, die an einem anderen Standort, vorzugsweise in einer anderen Region, ausgeführt wird. ACC verwendet ONTAP Async SnapMirror mit einem Recovery Point Objective von nur 5 Minuten. Siehe "Hier" Anweisungen zur Einrichtung von SnapMirror finden Sie.

SnapMirror mit ACC



speichertreiber für san-Economy und nas-Economy unterstützen keine Replikationsfunktion. Siehe "Hier" Entnehmen.

Demovideo:

"Demo-Video über Disaster Recovery mit Astra Control Center"

Datensicherung mit Astra Control Center

Einzelheiten zu den Datensicherungsfunktionen von Astra Control Center sind erhältlich "Hier"

Disaster Recovery (Failover und Failback mit Replikation) mit ACC

Verwendung von Astra Control für Failover und Failback von Applikationen

Datenmigration über Astra Control Center

Auf dieser Seite werden die Optionen für die Datenmigration von Container-Workloads auf Red hat OpenShift-Clustern mit Astra Control Center (ACC) angezeigt. Insbesondere können Kunden ACC nutzen, um: Einige ausgewählte Workloads oder alle Workloads aus ihren On-Premises-Datacentern in die Cloud zu verschieben – ihre Apps zu Testzwecken oder zum Verschieben aus dem Datacenter in die Cloud in die Cloud zu klonen

Datenmigration

Um eine Anwendung von einer Umgebung in eine andere zu migrieren, können Sie eine der folgenden Funktionen von ACC verwenden:

- **Replikation**

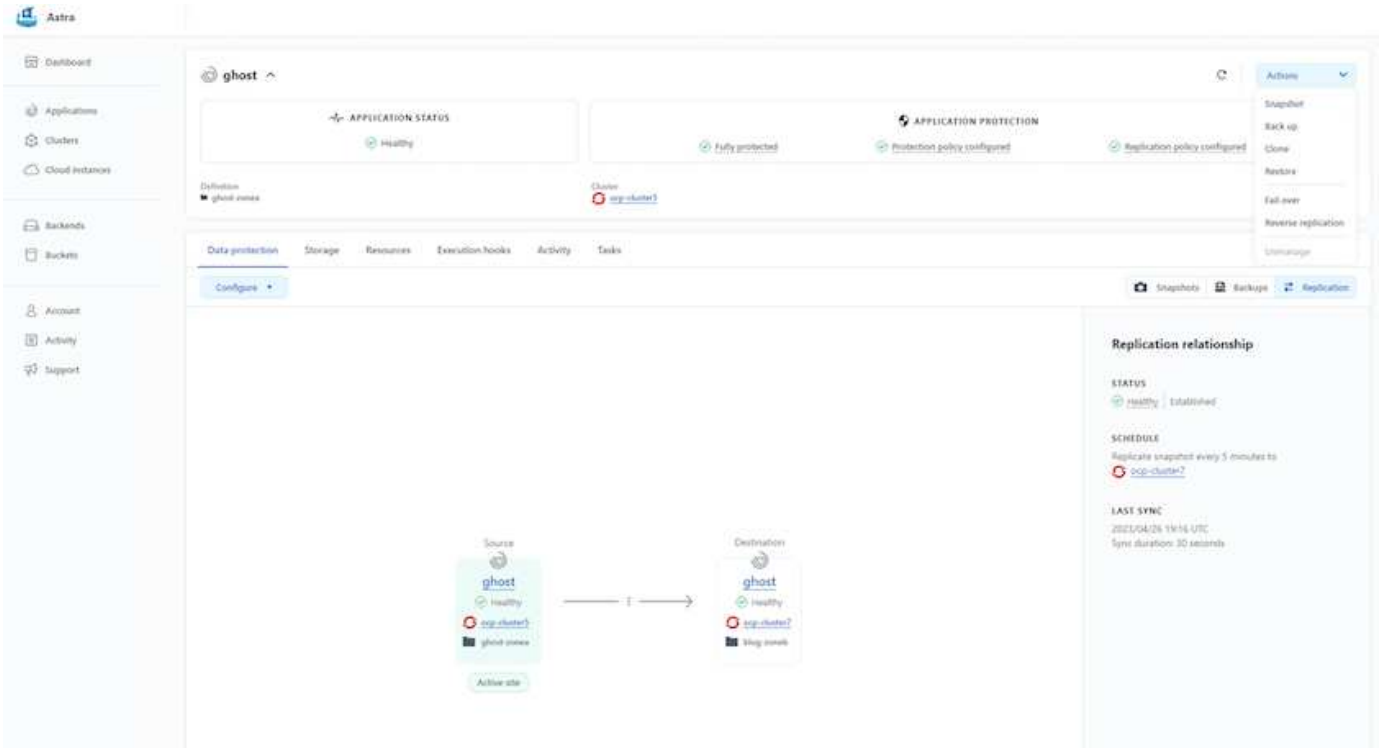
- **Sicherung und Wiederherstellung**
- **Klon**

Siehe "Abschnitt zur Datensicherung" Für die Optionen **Replikation und Backup und Restore**.

Siehe "Hier" Für weitere Details über **Klonen**.

> Die Astra Replizierungsfunktion wird nur mit der Trident Container Storage Interface (CSI) unterstützt. Die Replikation wird jedoch nicht von nas-Economy- und san-Economy-Treibern unterstützt.

Durchführen der Datenreplikation mit ACC



NetApp Hybrid-Multi-Cloud-Lösungen für Container-Workloads mit Red hat OpenShift

Überblick

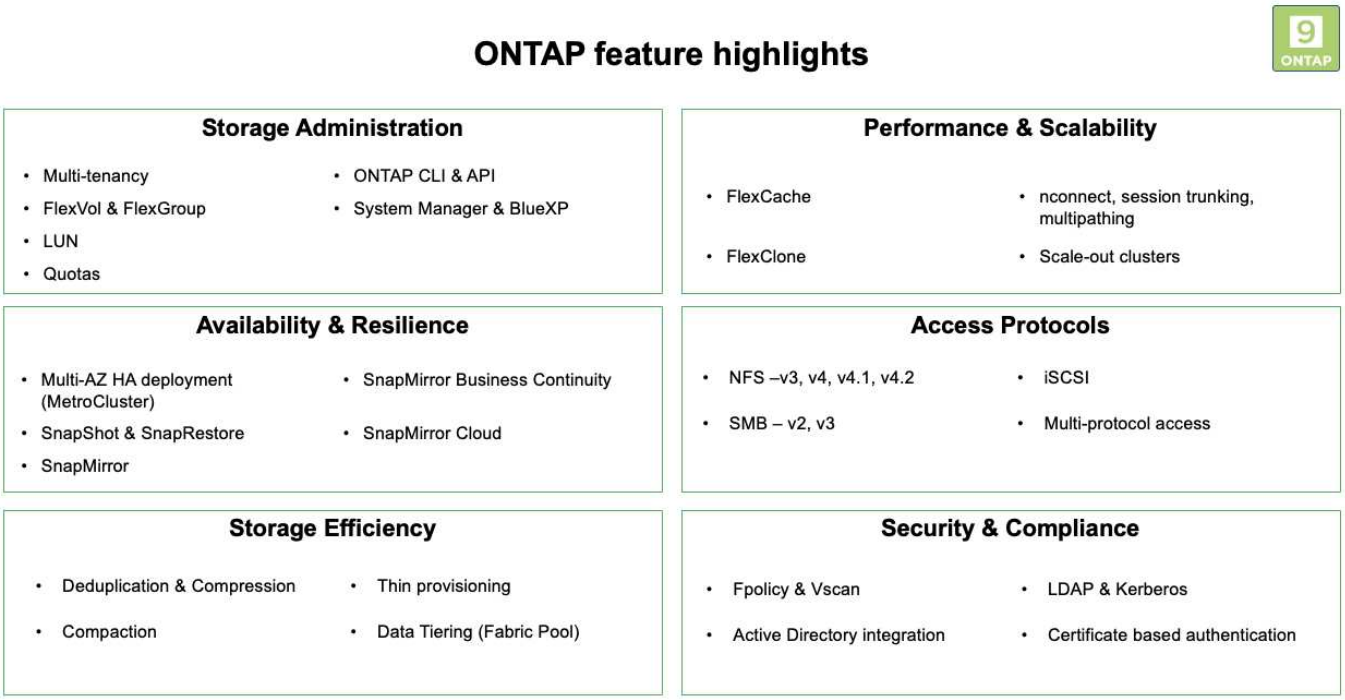
Bei NetApp beobachten wir eine deutliche Zunahme bei Kunden, die ihre älteren Enterprise-Applikationen modernisieren und neue Applikationen mithilfe von Containern und Orchestrierungsplattformen auf Basis von Kubernetes erstellen. Die Red hat OpenShift Container Platform ist ein Beispiel, das wir von vielen unserer Kunden angenommen sehen.

Immer mehr Kunden beginnen mit der Einführung von Containern in ihrem Unternehmen. NetApp ist perfekt aufgestellt, um die persistenten Storage-Anforderungen ihrer zustandsbehafteten Applikationen und klassischen Datenmanagementanforderungen zu erfüllen, beispielsweise Datensicherung, Datensicherheit und Datenmigration. Diese Bedürfnisse werden jedoch mit verschiedenen Strategien, Werkzeugen und Methoden erfüllt.

NetApp ONTAP basierte Storage-Optionen, die unten aufgeführt sind, bieten Sicherheit, Datensicherung,

Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Implementierungen.

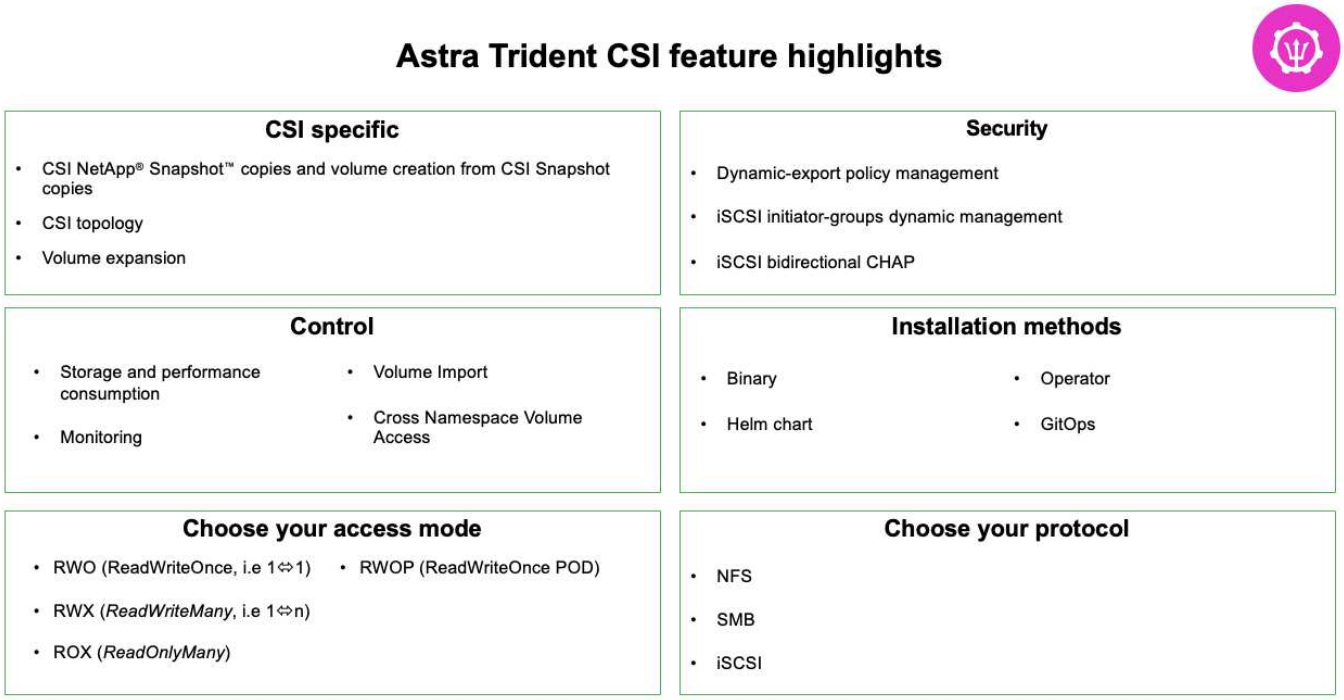
- Automatisierter, lokaler Storage:
  - NetApp Fabric Attached Storage (FAS), NetApp All-Flash-FAS-Arrays (AFF), NetApp All-SAN-Arrays (ASA) und ONTAP Select
- Von Providern gemanagter Storage in On-Premises:
  - NetApp Keystone stellt Storage-als-Service (STaaS) bereit
- Automatisierter Storage in der Cloud:
  - NetApp Cloud Volumes ONTAP(CVO) bieten Self-Managed-Storage in den Hyperscalern
- Von Providern gemanagter Storage in der Cloud:
  - Cloud Volumes Service für Google Cloud (CVS), Azure NetApp Files (ANF) und Amazon FSX für NetApp ONTAP bieten vollständig gemanagten Storage in den Hyperscalern



NetApp BlueXP ermöglicht Ihnen das Management Ihrer gesamten Storage- und Datenbestände über eine einzige Managementoberfläche.

Mit BlueXP können Sie Cloud-Storage erstellen und verwalten (z. B. Cloud Volumes ONTAP und Azure NetApp Files), Daten verschieben, schützen und analysieren sowie zahlreiche lokale und Edge-Storage-Geräte kontrollieren.

NetApp Astra Trident ist ein CSI-konformer Storage Orchestrator, der eine schnelle und einfache Nutzung von persistentem Storage ermöglicht und von einer Vielzahl der oben genannten NetApp Storage-Optionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gewartet und unterstützt wird.



Geschäftskritische Container-Workloads benötigen mehr als nur persistente Volumes. Ihre Datenmanagement-Anforderungen erfordern auch den Schutz und die Migration der Kubernetes-Objekte für die Applikation.

> Neben Benutzerdaten umfassen Applikationsdaten kubernetes-Objekte. Folgende Beispiele sind vorhanden: - kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Implementierungen, Services – benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und -Geheimnisse – persistente Daten wie Snapshot-Kopien, Backups, Klone – benutzerdefinierte Ressourcen wie CRS und CRDs

NetApp Astra Control ist sowohl als vollständig gemanagte als auch als selbst gemanagte Software erhältlich und bietet Orchestrierung für solides Applikations-Datenmanagement. Siehe "Astra-Dokumentation" Weitere Informationen zur Astra Produktfamilie.

Diese Referenzdokumentation unterstützt die Validierung der Migration und des Schutzes von Container-basierten Applikationen, die auf der RedHat OpenShift Container-Plattform über das NetApp Astra Control Center implementiert werden. Darüber hinaus bietet die Lösung allgemeine Details zur Bereitstellung und zur Verwendung von Red hat Advanced Cluster Management (ACM) für die Verwaltung der Container-Plattformen. In diesem Dokument werden auch Einzelheiten zur Integration von NetApp Storage in Container-Plattformen mit Red hat OpenShift mithilfe der Astra Trident CSI-bereitstellung erläutert. Astra Control Center wird auf dem Hub-Cluster bereitgestellt und wird für das Management der Container-Applikationen und ihres Lebenszyklus von persistentem Storage verwendet. Schließlich bietet es eine Lösung für Replizierung, Failover und Failback für Container-Workloads auf gemanagten Red hat OpenShift-Clustern in AWS (ROSA), die Amazon FSX für NetApp ONTAP (FSxN) als persistenten Storage verwenden.

Die NetApp Lösung mit gemanagten Container-Plattform-Workloads aus Red hat OpenShift auf AWS

Die NetApp Lösung mit gemanagten Container-Plattform-Workloads aus Red hat OpenShift auf AWS

Möglicherweise sind Kunden „aus der Cloud hervorgegangen“ oder bereits an einem Punkt der Modernisierung angelangt, wenn sie bereit sind, einige ausgewählte Workloads oder alle Workloads aus ihrem Datacenter in die Cloud zu verschieben. Sie können dafür

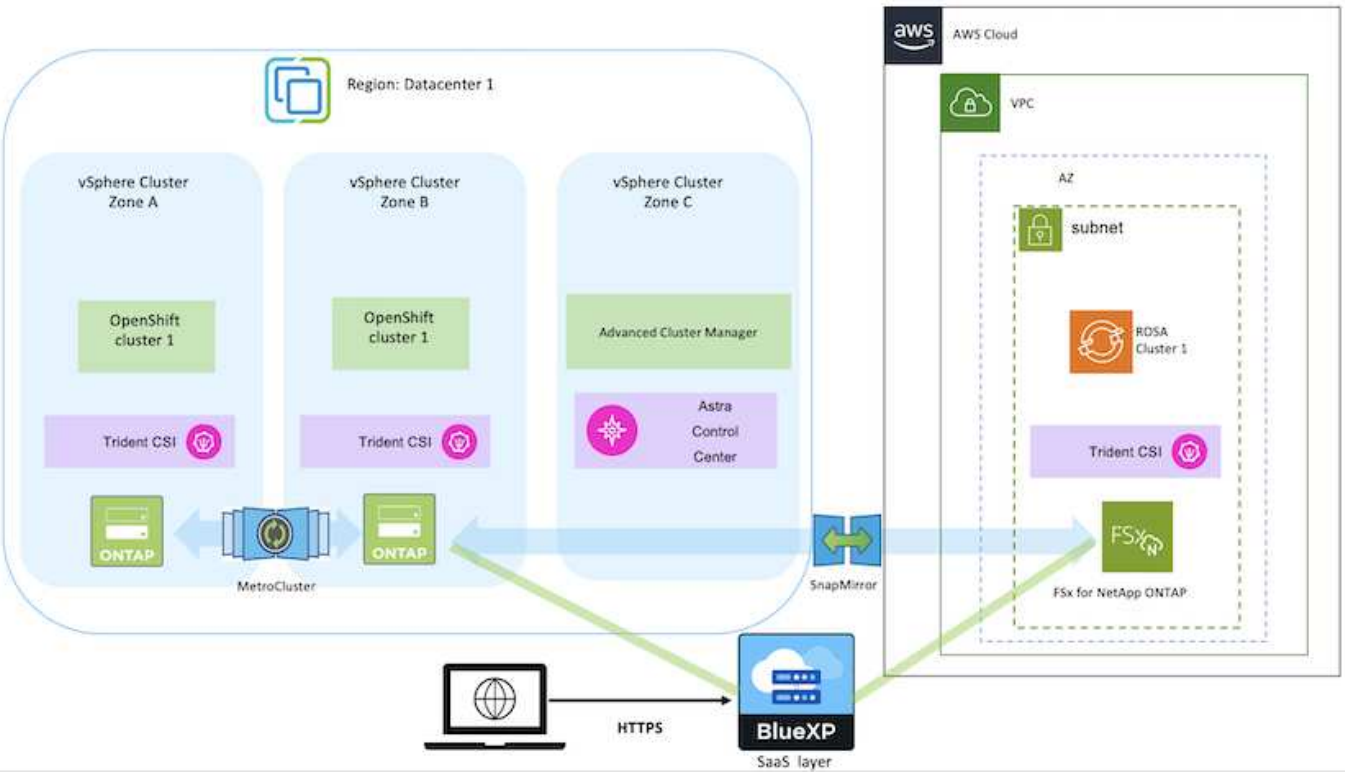
wählen, von Providern gemanagte OpenShift-Container und von Providern gemanagten NetApp Storage in der Cloud zu verwenden, um ihre Workloads auszuführen. Sie sollten die verwalteten Container-Cluster (ROSA) von Red hat OpenShift in der Cloud planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für ihre Container-Workloads zu schaffen. In der AWS-Cloud können sie auch FSX für NetApp ONTAP für die Storage-Anforderungen implementieren.

FSX for NetApp ONTAP bietet Datensicherung, Zuverlässigkeit und Flexibilität für Container-Implementierungen in AWS. Astra Trident dient als dynamische Storage-bereitstellung zur Nutzung des persistenten FSxN Storage für zustandsbehaftete Applikationen von Kunden.

DA ROSA im HA-Modus mit Knoten der Kontrollebene über mehrere Verfügbarkeitszonen hinweg implementiert werden kann, kann FSX ONTAP auch mit Multi-AZ-Option bereitgestellt werden, die hohe Verfügbarkeit bietet und AZ-Ausfälle schützt.

Beim Zugriff auf ein Amazon FSX Filesystem aus der bevorzugten Verfügbarkeitszone (AZ) des Filesystems fallen keine Datenübertragungsgebühren an. Weitere Informationen zur Preisgestaltung finden Sie unter "Hier".

Datensicherungs- und Migrationslösung für OpenShift-Container-Workloads

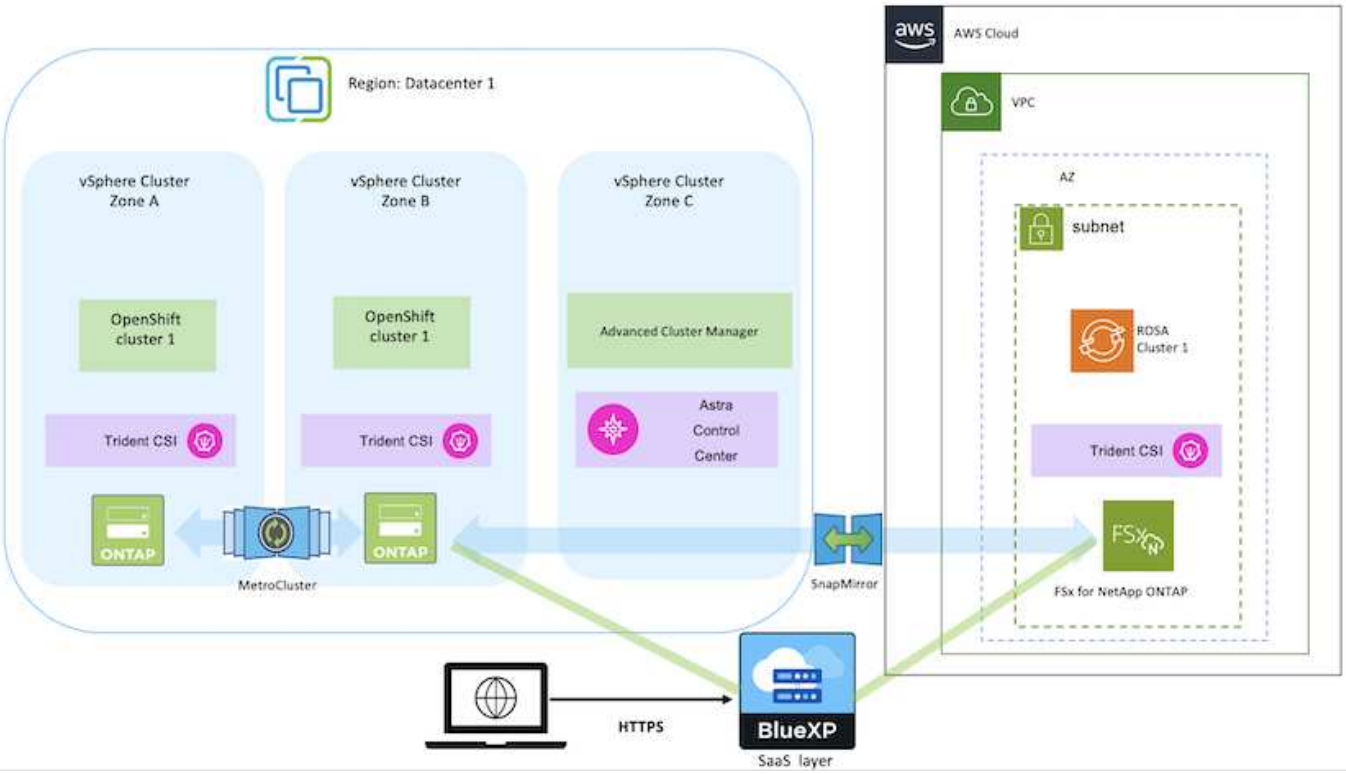


Implementierung und Konfiguration der gemanagten Container-Plattform Red hat OpenShift auf AWS

In diesem Abschnitt wird ein High-Level-Workflow zur Einrichtung der verwalteten Red hat OpenShift-Cluster auf AWS(ROSA) beschrieben. Es zeigt die Nutzung von Managed FSX for NetApp ONTAP (FSxN) als Storage-Backend von Astra Trident zur Bereitstellung persistenter Volumes. Es werden Details zur Implementierung von FSxN auf AWS mithilfe von BlueXP bereitgestellt. Außerdem werden Einzelheiten zur Verwendung von BlueXP

und OpenShift GitOps (Argo CD) bereitgestellt, um Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Applikationen auf ROSA Clustern durchzuführen.

Das folgende Diagramm zeigt die AUF AWS implementierten ROSA-Cluster, die FSxN als Back-End-Storage verwenden.



Diese Lösung wurde mit zwei ROSA-Clustern in zwei VPCs in AWS verifiziert. Jeder ROSA Cluster wurde mithilfe von Astra Trident in FSxN integriert. ES gibt mehrere Möglichkeiten, ROSA-Cluster und FSxN in AWS bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentations-Links für die spezifische verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im "Ressourcen".

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

INSTALLIEREN SIE ROSA Cluster

- Erstellung von zwei VPCs und Einrichtung der VPC-Peering-Konnektivität zwischen den VPCs.
- Siehe "Hier" Für Anweisungen zur Installation VON ROSA Clustern.

Installieren Sie FSxN

- Installieren Sie FSxN auf den VPCs von BlueXP. Siehe "Hier" Für die Erstellung von BlueXP Konten und weitere Schritte. Siehe "Hier" Zur Installation von FSxN. Siehe "Hier" Zum Erstellen eines Connectors in AWS zum Verwalten des FSxN.
- Implementieren Sie FSxN mithilfe von AWS. Siehe "Hier" Für die Implementierung über die AWS-Konsole.

Trident auf ROSA Clustern installieren (mit Helm-Diagramm)

- Verwenden Sie Helm-Diagramm, um Trident auf ROSA Clustern zu installieren. url für das Helm-Diagramm: https://netapp.github.io/trident-helm-chart

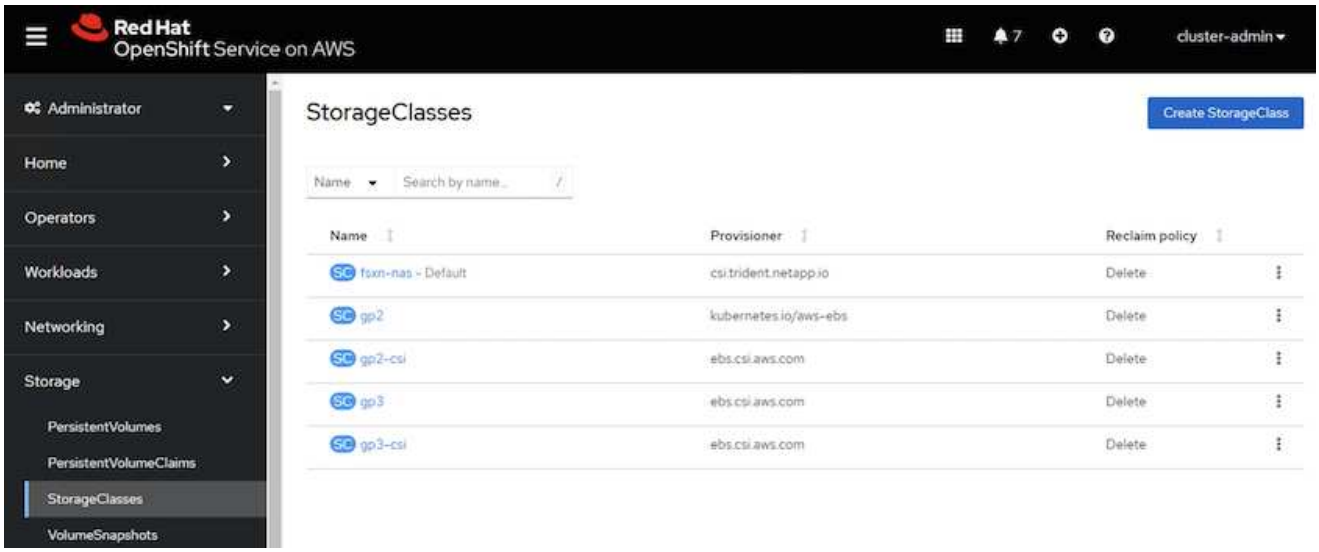
Integration von FSxN mit Astra Trident für ROSA Cluster

OpenShift GitOps kann zur Implementierung von Astra Trident CSI für alle gemanagten Cluster verwendet werden, wenn sie über ApplicationSet auf ArgoCD registriert werden.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```

Back-End- und Storage-Klassen mit Trident (für FSxN) erstellen

- Siehe "Hier" Für Details zum Erstellen von Back-End und Storage-Klasse.
- Erstellen Sie die für FsxN erstellte Storage-Klasse mit Trident CSI standardmäßig aus der OpenShift-Konsole. Siehe Abbildung unten:



Anwendung mit OpenShift GitOps (Argo CD) bereitstellen

- Installieren Sie den OpenShift GitOps Operator auf dem Cluster. Siehe Anweisungen "Hier".
- Richten Sie eine neue Argo-CD-Instanz für den Cluster ein. Siehe Anweisungen "Hier".

Öffnen Sie die Konsole von Argo CD und stellen Sie eine App bereit. Als Beispiel können Sie eine Jenkins-App mithilfe einer Argo-CD mit einem Helm-Diagramm bereitstellen. Beim Erstellen der Anwendung wurden folgende Details angegeben: Projekt: Standardcluster: https://kubernetes.default.svcNamensraum: Jenkins die url für das Helm-Diagramm: https://charts.bitnami.com/bitnami

Helm-Parameter: Global.storageClass: Fsxn-nas

Datensicherung

Auf dieser Seite werden die Datensicherungsoptionen für gemanagte Red hat OpenShift auf AWS (ROSA) Clustern unter Verwendung des Astra Control Service angezeigt. Astra Control Service (ACS) bietet eine intuitive grafische Benutzeroberfläche, mit der Sie Cluster hinzufügen, darauf laufende Applikationen definieren und applikationsorientierte Datenmanagement-Aktivitäten durchführen können. ACS-Funktionen können auch über eine API aufgerufen werden, die die Automatisierung von Workflows ermöglicht.

Astra Control (ACS oder ACC) wird von NetApp Astra Trident angetrieben. Astra Trident integriert mehrere Arten von Kubernetes Clustern wie Red hat OpenShift, EKS, AKS, SUSE Rancher, Anthos usw. mit verschiedenen Ausführungen von NetApp ONTAP-Storage wie FAS/All Flash FAS, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files und Amazon FSX for NetApp ONTAP.

Dieser Abschnitt enthält Details zu den folgenden Datenschutzoptionen, die ACS verwenden:

- Ein Video, das Backup und Restore einer ROSA-Anwendung zeigt, die in einer Region ausgeführt wird und in einer anderen Region wiederhergestellt wird.
- Ein Video, das Snapshot und Wiederherstellung einer ROSA-Anwendung zeigt.
- Schritt-für-Schritt-Details zur Installation eines ROSA-Clusters, Amazon FSX for NetApp ONTAP, Verwendung von NetApp Astra Trident zur Integration mit Storage-Backend, Installation einer postgresql-Anwendung auf ROSA-Cluster, Verwendung von ACS zur Erstellung eines Snapshot der Anwendung und Wiederherstellung der Anwendung von ihm.
- Ein Blog, der Schritt-für-Schritt-Details des Erstellens und Wiederherstellen aus einem Snapshot für eine mysql-Anwendung auf einem ROSA-Cluster mit FSX für ONTAP unter Verwendung von ACS zeigt.

Backup/Wiederherstellung aus Backup

Das folgende Video zeigt die Sicherung einer ROSA-Anwendung, die in einer Region ausgeführt wird und in einer anderen Region wiederhergestellt wird.

FSX NetApp ONTAP für Red hat OpenShift Service auf AWS

Snapshot/Wiederherstellung aus Snapshot

Das folgende Video zeigt, wie Sie einen Snapshot einer ROSA-Anwendung erstellen und danach aus dem Snapshot wiederherstellen.

Snapshot/Wiederherstellung für Anwendungen auf Red hat OpenShift-Service auf AWS (ROSA)-Clustern mit Amazon FSX für NetApp ONTAP-Speicher

Blog

- "Nutzung von Astra Control Service zum Datenmanagement von Applikationen auf ROSA Clustern mit Amazon FSX Storage"

Schritt-für-Schritt-Details zum Erstellen von Snapshot und Wiederherstellen von ihm

Vorbereitende Einrichtung

- "AWS Konto"
- "Red hat OpenShift -Konto"
- IAM-Benutzer mit "Entsprechende Berechtigungen" Um ROSA Cluster zu erstellen und darauf zuzugreifen
- "AWS CLI"
- "ROSA CLI"
- "OpenShift-CLI"(oc)
- VPC mit Subnetzen und entsprechenden Gateways und Routen
- "ROSA Cluster installiert" In die VPC
- "Amazon FSX für NetApp ONTAP" Erstellt in derselben VPC
- Zugriff auf den ROSA-Cluster von "OpenShift Hybrid Cloud Console"

Nächste Schritte

1. Erstellen Sie einen Admin-Benutzer und melden Sie sich beim Cluster an.
2. Erstellen Sie eine kubeconfig-Datei für den Cluster.
3. Installieren Sie Astra Trident auf dem Cluster.
4. Mit der CSI-provisionierung von Trident können Sie eine Back-End-, Storage-Klasse- und Snapshot-Klassenkonfiguration erstellen.
5. Implementieren Sie eine postgresql-Anwendung auf dem Cluster.
6. Erstellen Sie eine Datenbank und fügen Sie einen Datensatz hinzu.
7. Fügen Sie den Cluster zu ACS hinzu.
8. Definieren Sie die Anwendung in ACS.
9. Erstellen Sie einen Snapshot mit ACS.
10. Löschen Sie die Datenbank in der postgresql-Anwendung.
11. Wiederherstellen von einem Snapshot mit ACS.
12. Überprüfen Sie, ob Ihre App aus dem Snapshot wiederhergestellt wurde.

1. Erstellen Sie einen Admin-Benutzer und melden Sie sich beim Cluster an

Greifen Sie auf den ROSA-Cluster zu, indem Sie einen Admin-Benutzer mit dem folgenden Befehl erstellen: (Sie müssen einen Admin-Benutzer nur erstellen, wenn Sie zum Zeitpunkt der Installation keinen Administrator erstellt haben)

```
rosa create admin --cluster=<cluster-name>
```

Der Befehl liefert eine Ausgabe, die wie folgt aussieht. Melden Sie sich mit dem beim Cluster an `oc login` In der Ausgabe bereitgestellter Befehl.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

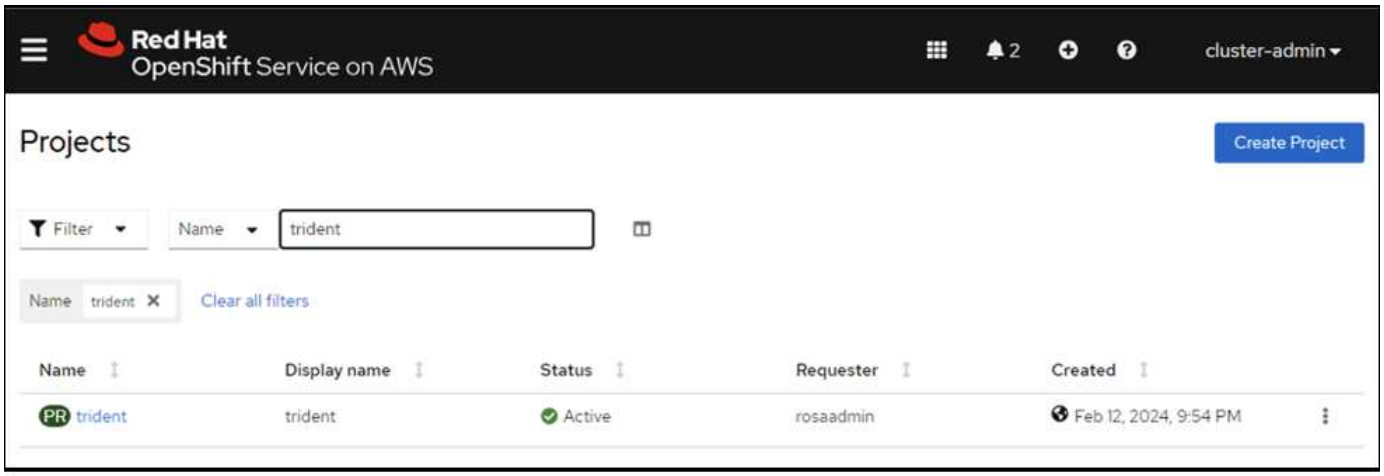
Sie können sich auch mit einem Token beim Cluster anmelden. Wenn Sie zum Zeitpunkt der Cluster-Erstellung bereits einen Admin-Benutzer erstellt haben, können Sie sich über die Red hat OpenShift Hybrid Cloud-Konsole mit den Anmeldedaten des Admin-Benutzers beim Cluster anmelden. Klicken Sie dann auf die obere rechte Ecke, wo der Name des angemeldeten Benutzers angezeigt wird, um den zu erhalten `oc login` Befehl (Token Login) für die Befehlszeile.

2. Erstellen Sie eine kubeconfig-Datei für den Cluster

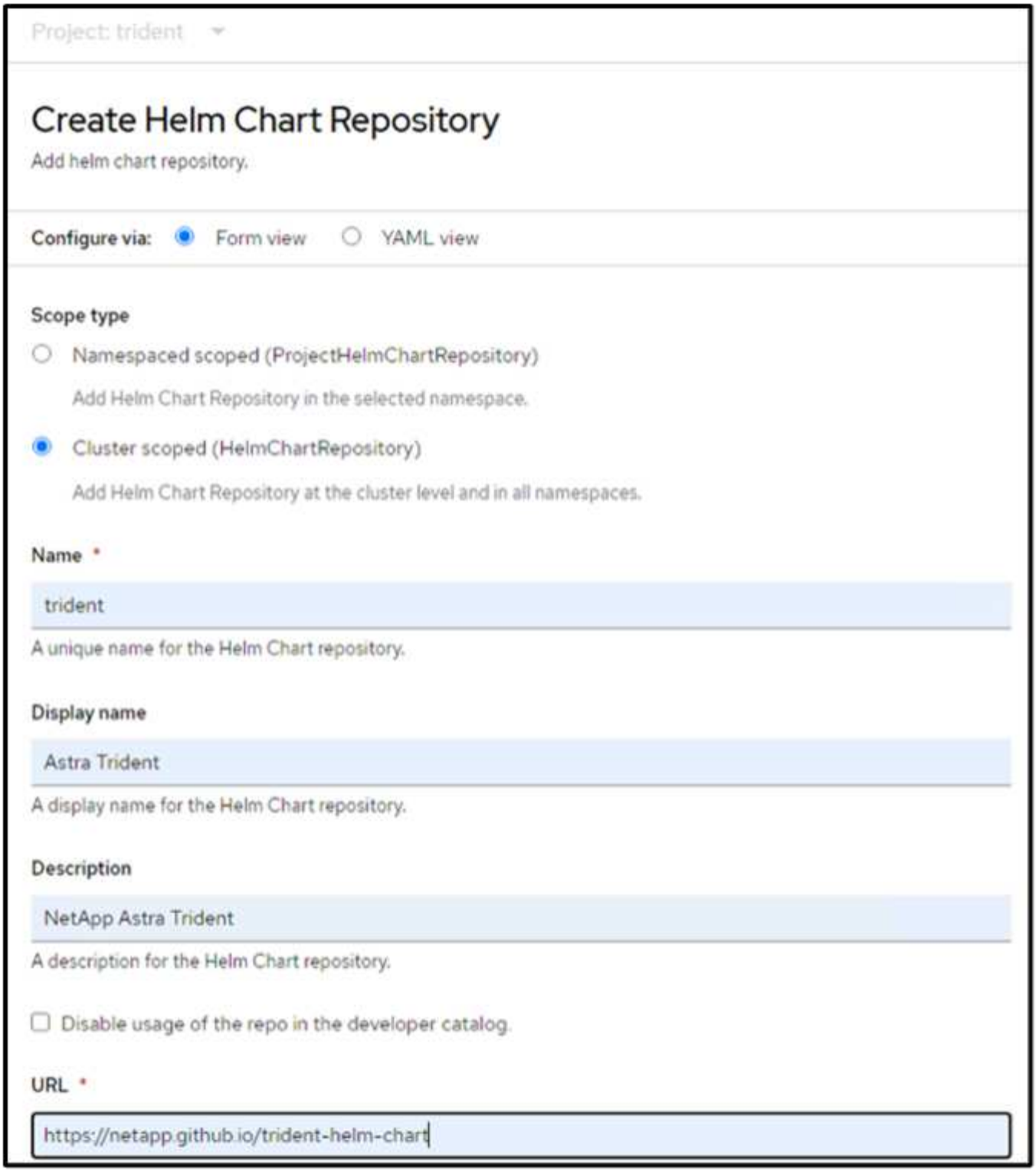
Befolgen Sie die Anweisungen "Hier" Um eine Kubeconfig-Datei für den ROSA-Cluster zu erstellen. Diese kubeconfig-Datei wird später verwendet, wenn Sie den Cluster zu ACS hinzufügen.

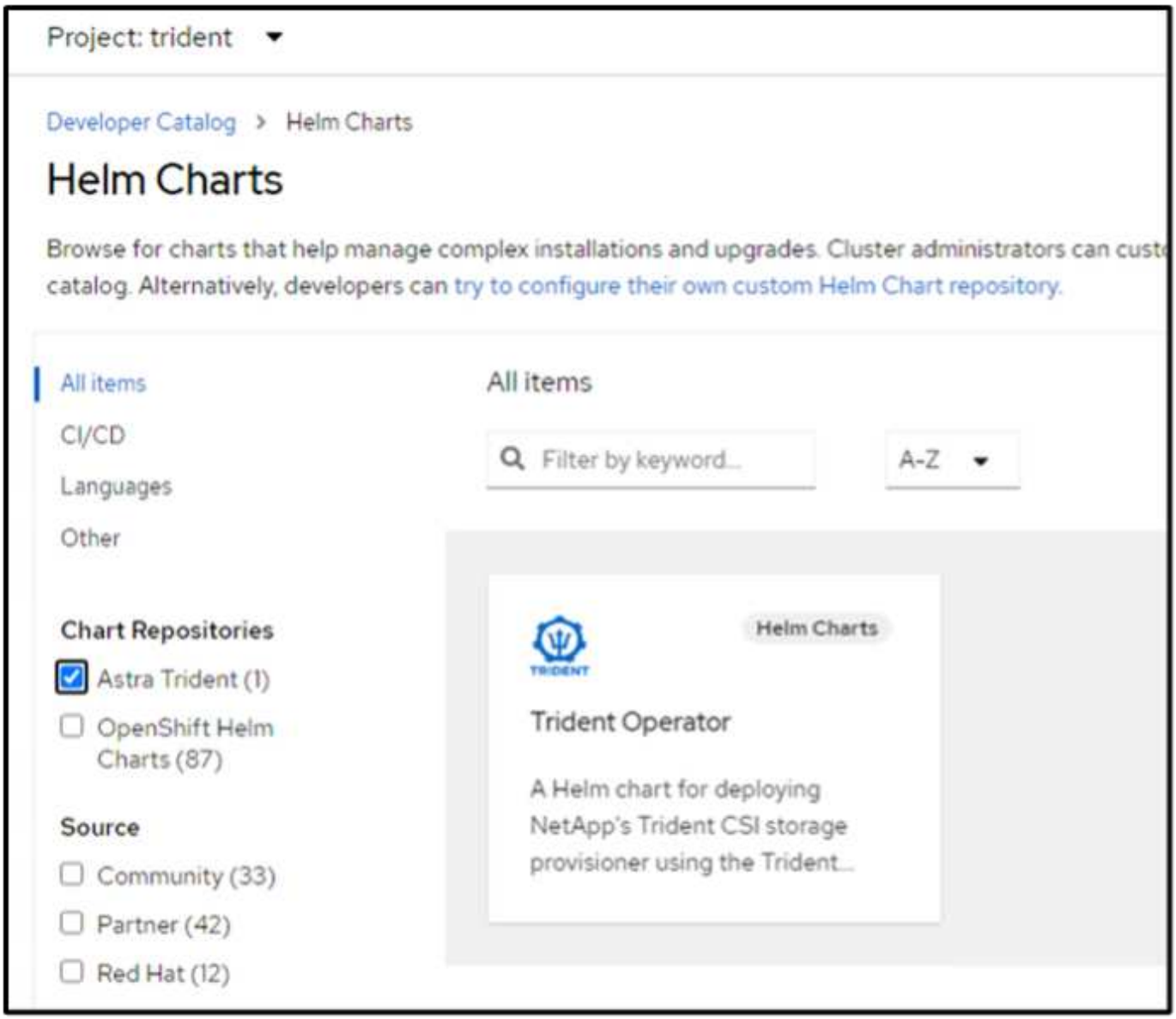
3. Installieren Sie Astra Trident auf dem Cluster

Installieren Sie Astra Trident (neueste Version) im ROSA Cluster. Um dies zu tun, können Sie eine der angegebenen Verfahren befolgen "Hier". Um Trident über das Helm von der Cluster-Konsole zu installieren, erstellen Sie zuerst ein Projekt mit dem Namen Trident.

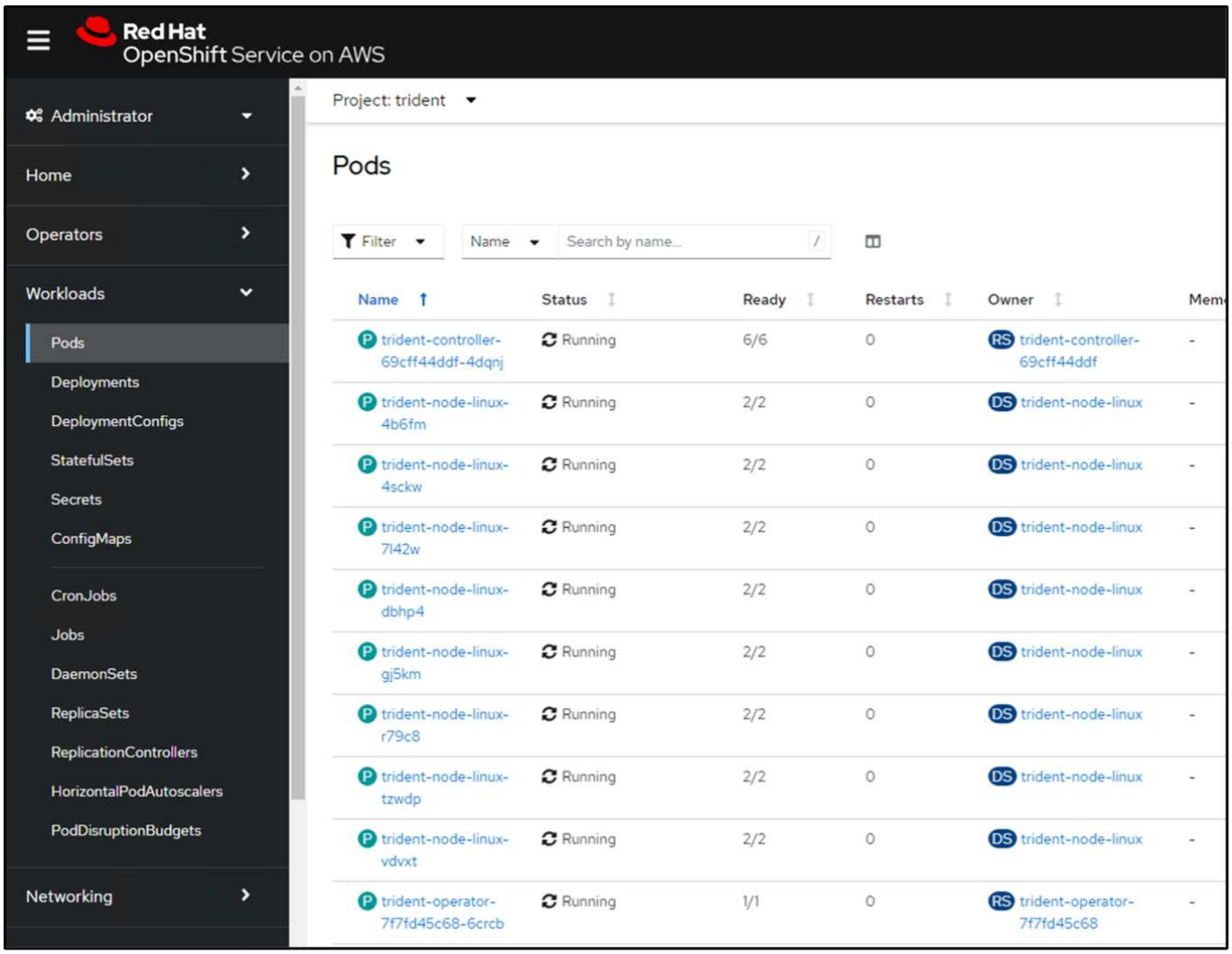


Erstellen Sie dann in der Entwickleransicht ein Helmdiagramm-Repository. Verwenden Sie für das URL-Feld `'https://netapp.github.io/trident-helm-chart'`. Erstellen Sie dann ein Helm Release für den Trident Operator.


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



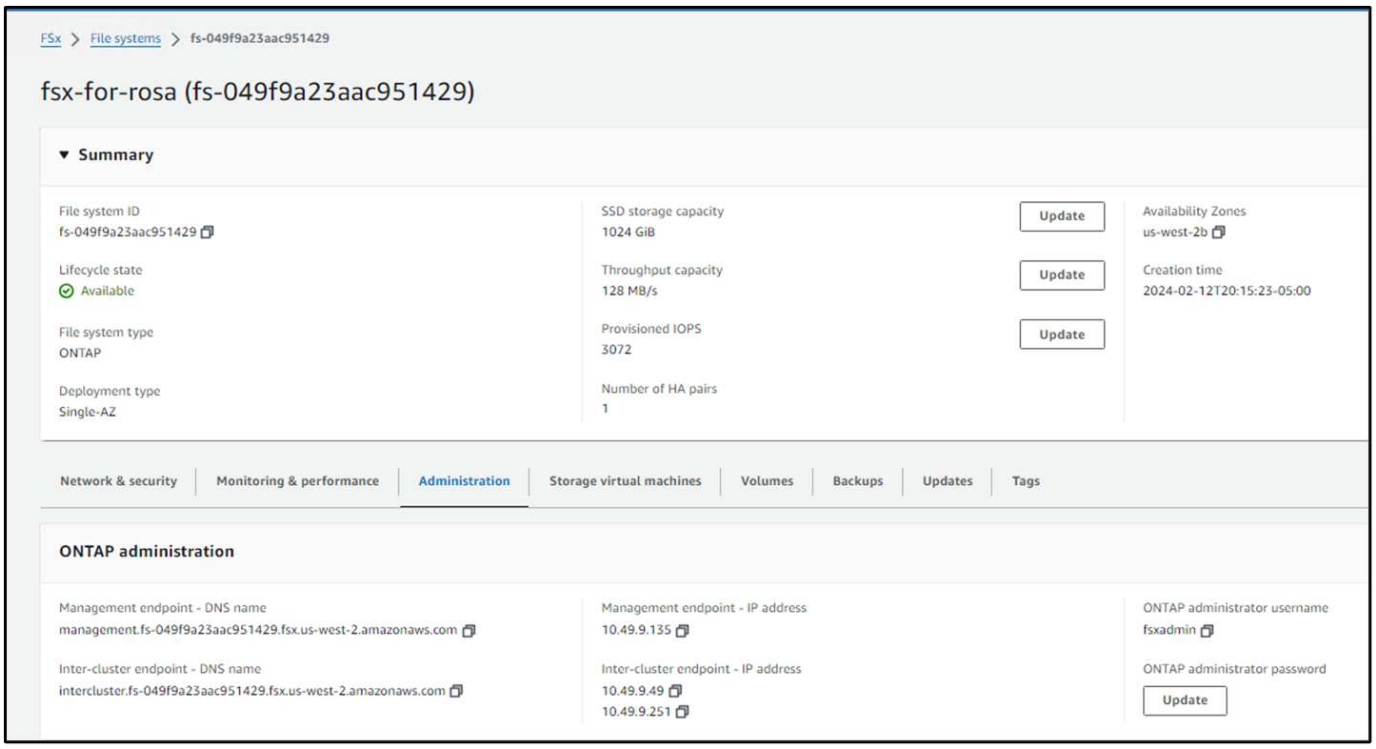
Überprüfen Sie, ob alle Stativpods ausgeführt werden, indem Sie zur Administratoransicht auf der Konsole zurückkehren und Pods im Dreizack-Projekt auswählen.



4. Erstellen Sie mit der Trident CSI-provisionierung eine Back-End-, Storage-Klasse- und Snapshot-Klassenkonfiguration

Verwenden Sie die unten abgebildeten yaml-Dateien, um ein dreigespanntes Backend-Objekt, ein Storage-Klasse-Objekt und das Volumesnapshot-Objekt zu erstellen. Stellen Sie sicher, dass Sie die Anmeldeinformationen für Ihr von Ihnen erstelltes Amazon FSX for NetApp ONTAP-Dateisystem, die Verwaltungs-LIF und den vserver-Namen Ihres Dateisystems in der Konfiguration yaml für das Backend angeben. Um diese Details anzuzeigen, wählen Sie in der AWS-Konsole für Amazon FSX das Dateisystem aus, und wechseln Sie zur Registerkarte Administration. Klicken Sie außerdem auf Aktualisieren, um das Kennwort für das festzulegen `fsxadmin` Benutzer:

Sie können die Objekte über die Befehlszeile erstellen oder mit den yaml-Dateien von der Hybrid Cloud-Konsole aus erstellen.



Trident Back-End-Konfiguration

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

Storage-Klasse

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

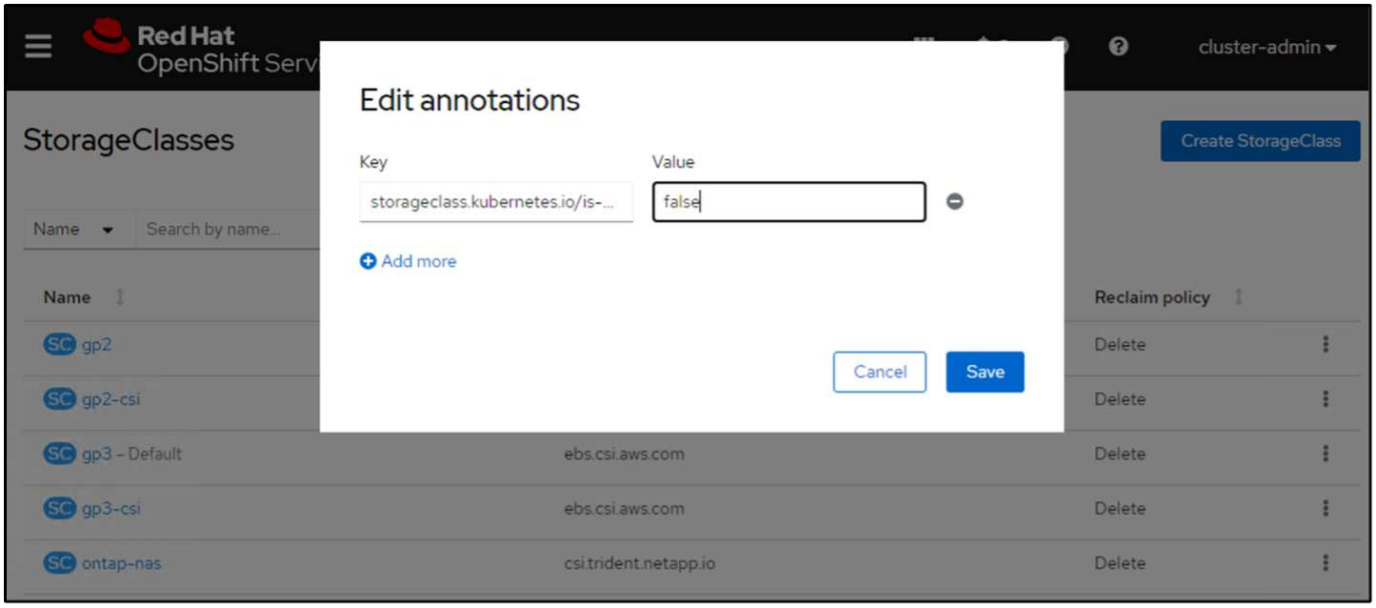
Snapshot-Klasse

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Stellen Sie sicher, dass die Objekte von Backend, Storage-Klasse und Trident-snapshotclass mit den unten gezeigten Befehlen erstellt werden.

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

Zu diesem Zeitpunkt ist eine wichtige Änderung erforderlich, ontap-nas statt gp3 als Standard-Storage-Klasse einzustellen, damit die später zu implementierende postgresql-Applikation die Standard-Storage-Klasse verwenden kann. Wählen Sie in der OpenShift-Konsole Ihres Clusters unter Storage StorageClasses aus. Bearbeiten Sie die Annotation der aktuellen Standardklasse mit „false“ und fügen Sie die Annotation storageclass.kubernetes.io/is-default-class für die ontap-nas Storage-Klasse auf „true“ ein.



5. Implementieren Sie eine postgresql-Anwendung auf dem Cluster

Sie können die Anwendung über die Befehlszeile wie folgt bereitstellen:

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

Wenn die Anwendungspads nicht ausgeführt werden, kann es aufgrund von Einschränkungen im Sicherheitskontext zu einem Fehler kommen.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                     TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/postgresql       ClusterIP   172.30.245.50   <none>        5432/TCP   12m
service/postgresql-hl    ClusterIP   None            <none>        5432/TCP   12m

NAME                             READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer   persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate       statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate           statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

Beheben Sie den Fehler, indem Sie den bearbeiten `runAsUser` Und `fsGroup` Felder in `statefuleset.apps/postgresql` Objekt mit der UID, die sich in der Ausgabe des befindet `oc get project` Wie unten gezeigt.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

die postgresql-App sollte ausgeführt werden und persistente Volumes verwenden, die von Amazon FSX für NetApp ONTAP-Storage unterstützt werden.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

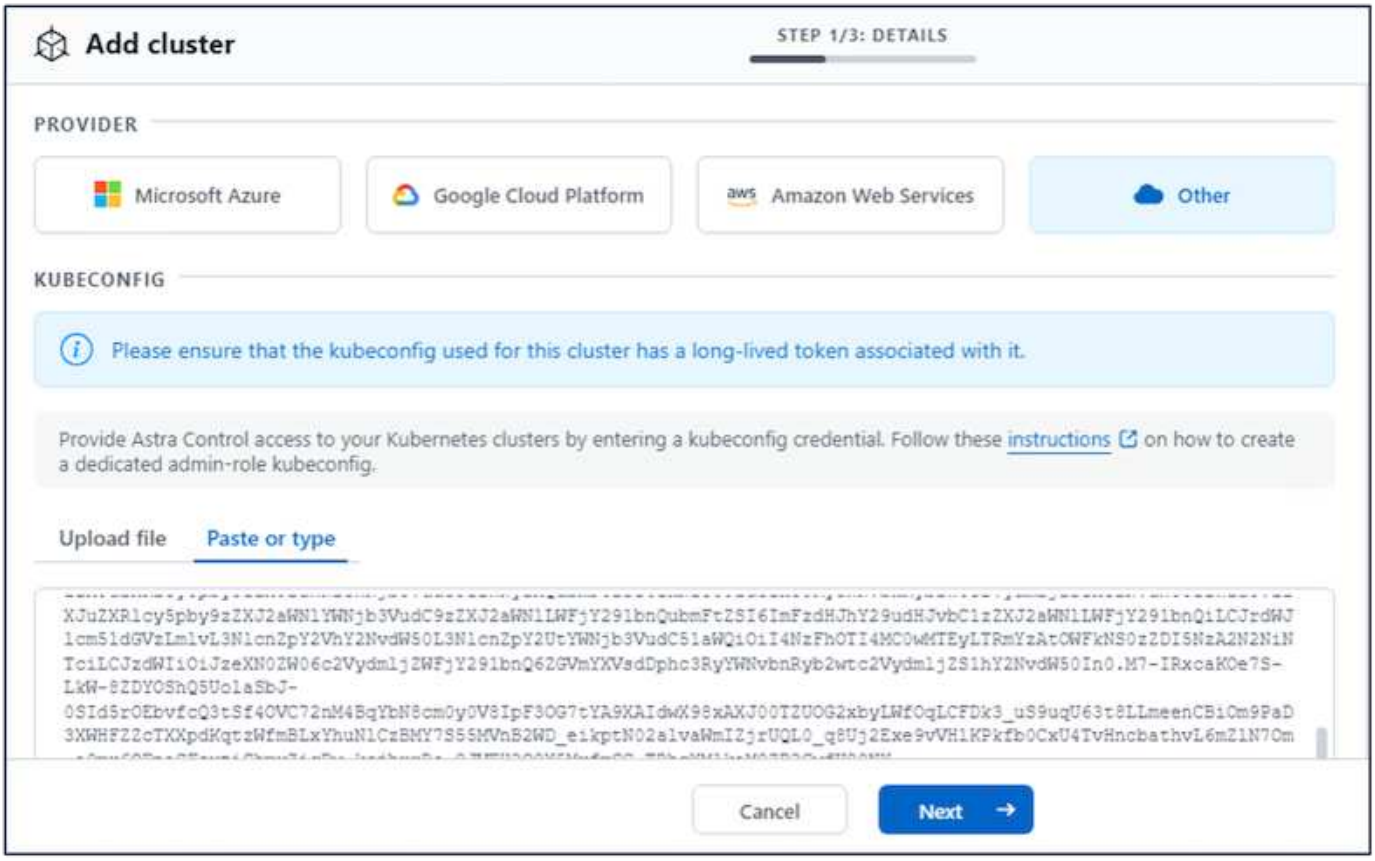
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME               STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0  Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6. Erstellen Sie eine Datenbank und fügen Sie einen Datensatz hinzu

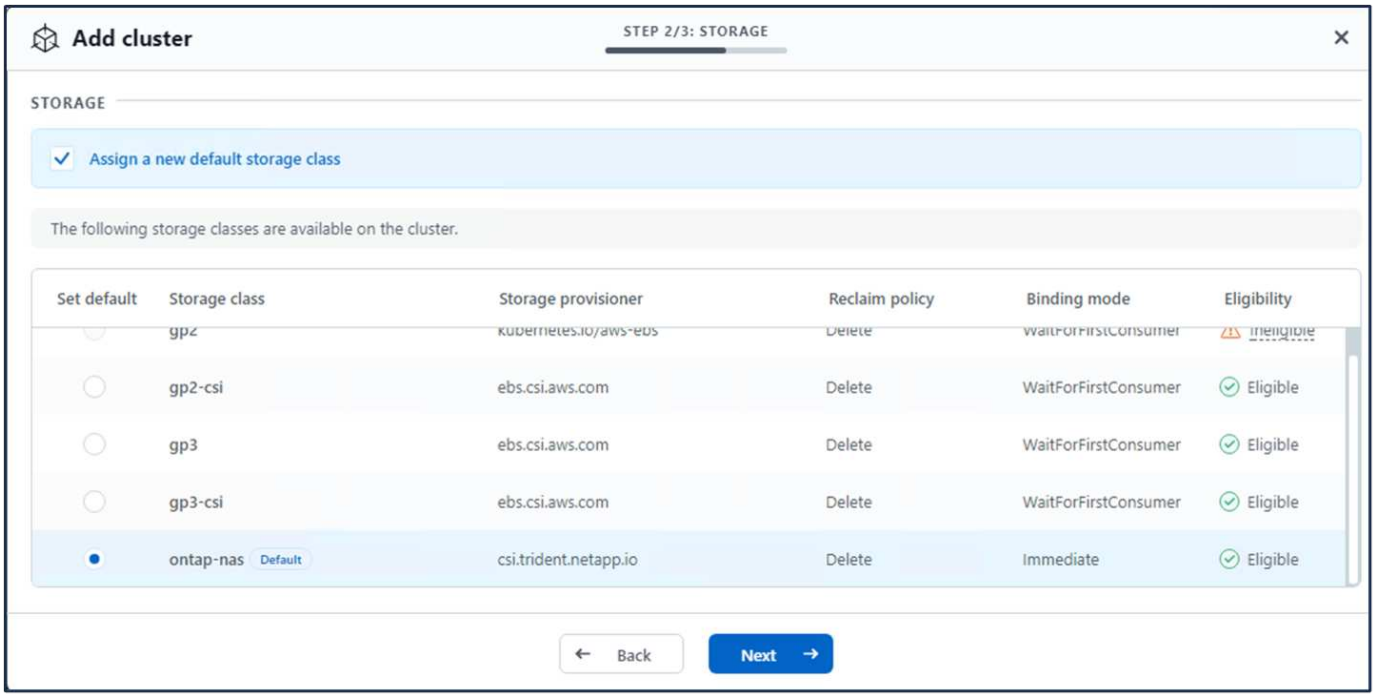
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7. Fügen Sie den Cluster zu ACS hinzu

Melden Sie sich bei ACS an. Wählen Sie Cluster aus, und klicken Sie auf Hinzufügen. Wählen Sie andere aus, und laden Sie die Datei kubeconfig hoch oder fügen Sie sie ein.



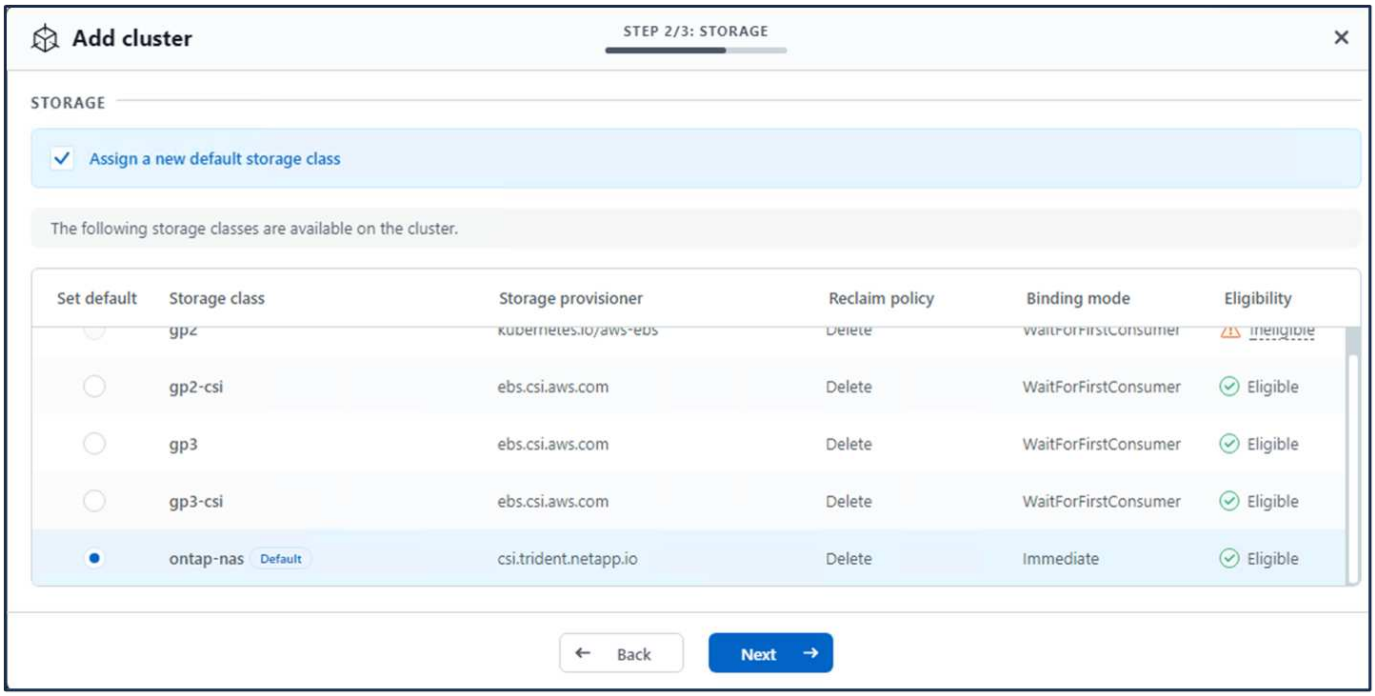
Klicken Sie auf **Weiter** und wählen Sie ontap-nas als Standard-Storage-Klasse für ACS aus. Klicken Sie auf **Weiter**, überprüfen Sie die Details und **Hinzufügen** den Cluster.



8. Definieren Sie die Anwendung in ACS

Definieren Sie die postgresql-Anwendung in ACS. Wählen Sie auf der Landing Page **Applications**, **define** aus und geben Sie die entsprechenden Details ein. Klicken Sie ein paar Mal auf **Weiter**, überprüfen Sie die Details

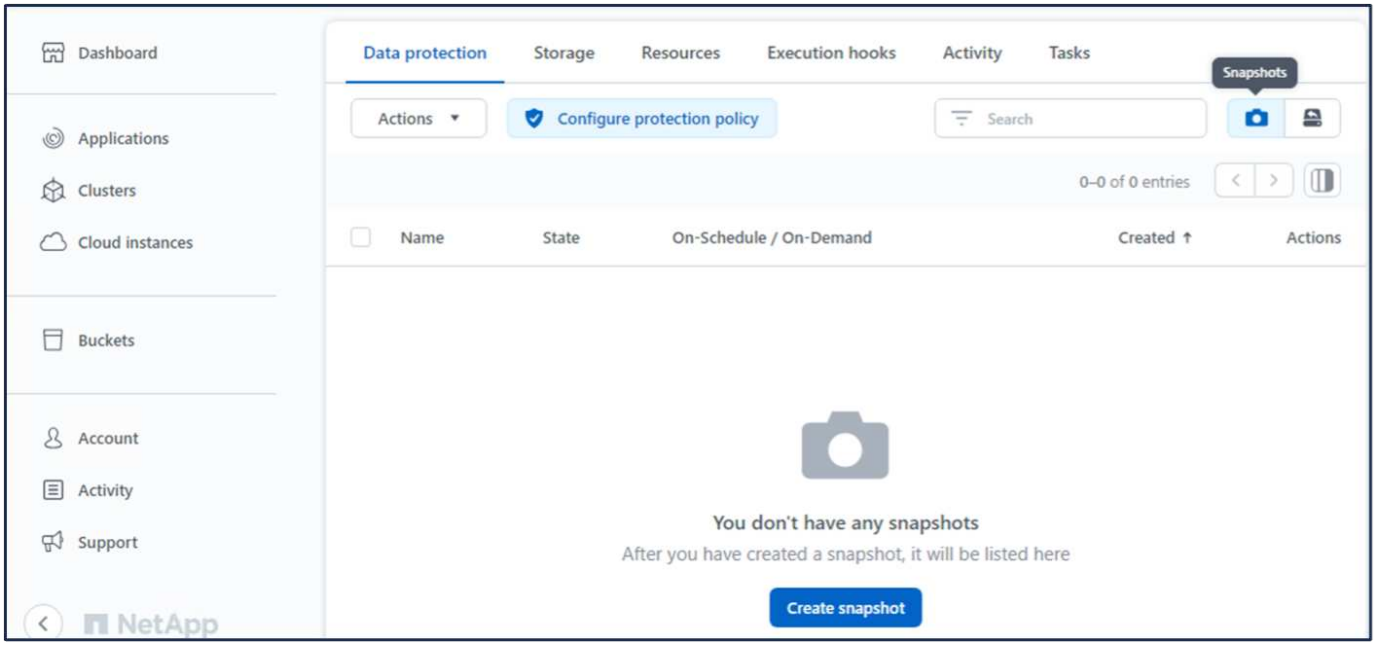
und klicken Sie auf **Definieren**. Die Anwendung wird zu ACS hinzugefügt.

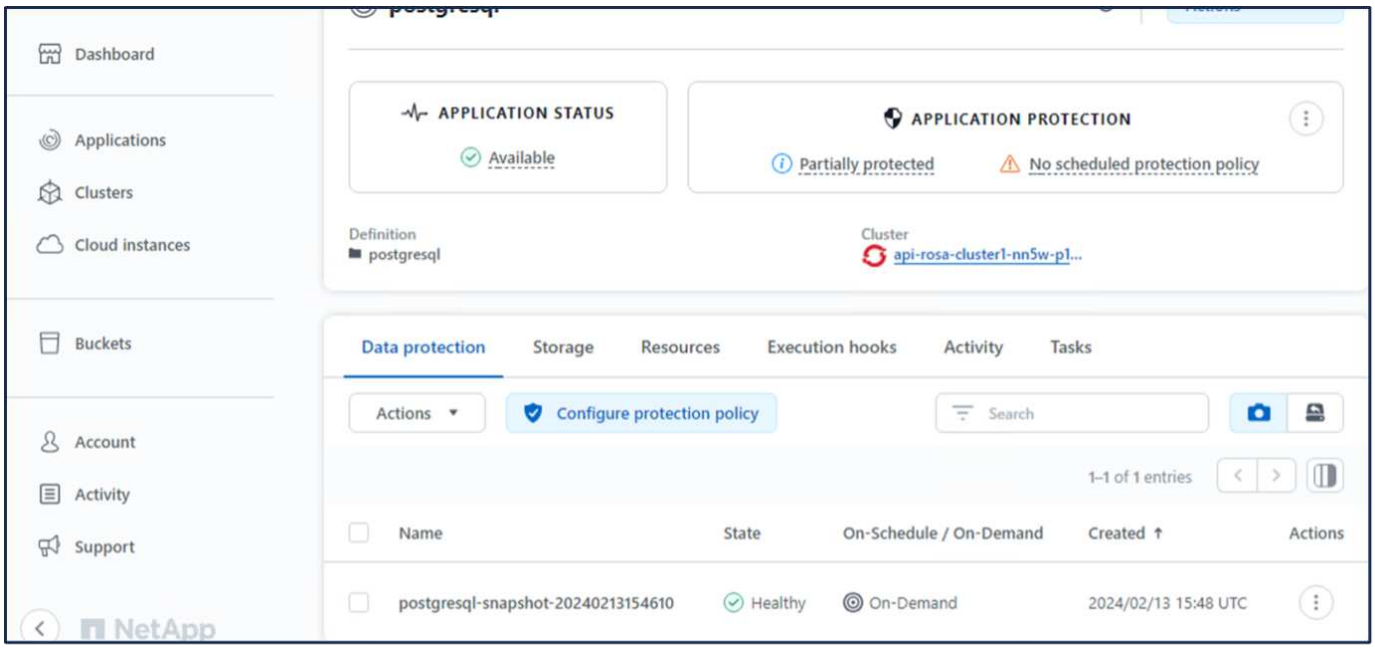


9. Erstellen Sie einen Snapshot mit ACS

Es gibt viele Möglichkeiten, einen Snapshot in ACS zu erstellen. Sie können die Anwendung auswählen und einen Snapshot auf der Seite erstellen, auf der die Details der Anwendung angezeigt werden. Sie können auf Snapshot erstellen klicken, um einen On-Demand-Snapshot zu erstellen oder eine Schutzrichtlinie zu konfigurieren.

Erstellen Sie einen On-Demand-Snapshot, indem Sie einfach auf **Create Snapshot** klicken, einen Namen angeben, die Details überprüfen und auf **Snapshot** klicken. Nach Abschluss des Vorgangs ändert sich der Snapshot-Status in „funktionstüchtiger Zustand“.





10. Löschen Sie die Datenbank in der postgresql-Anwendung

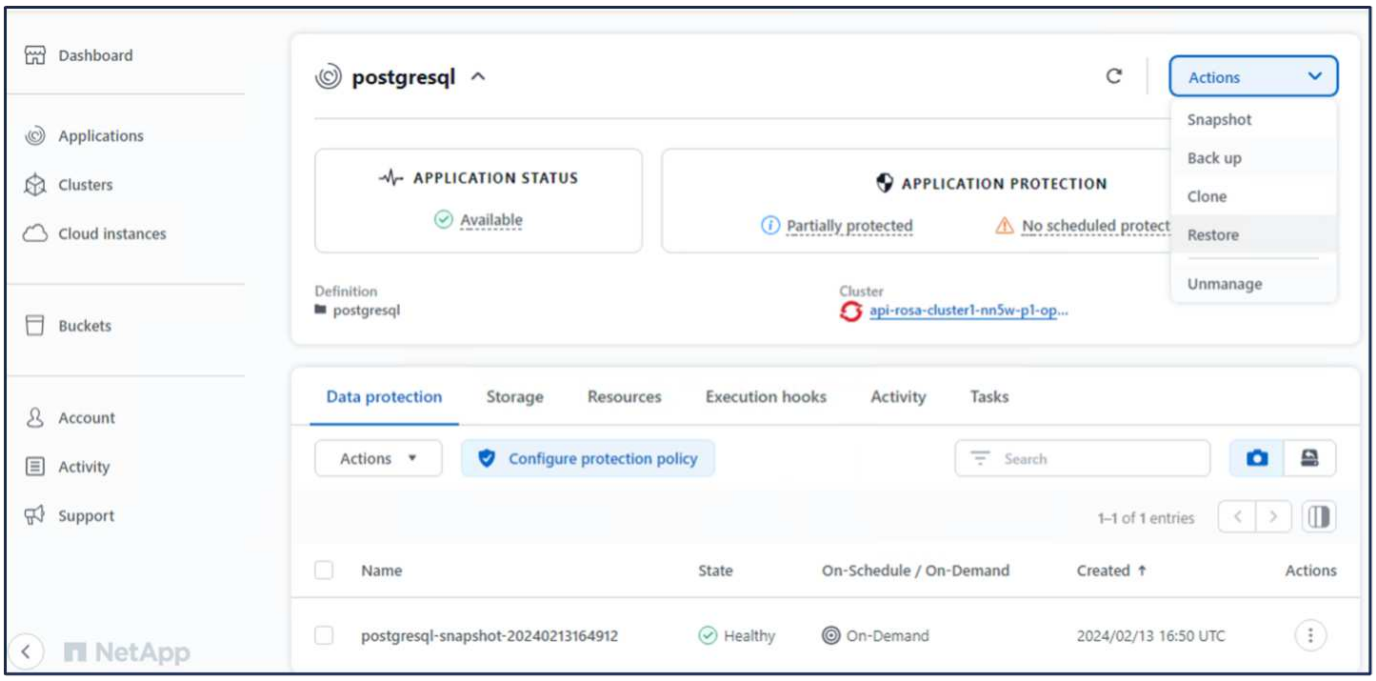
Melden Sie sich wieder bei postgresql an, Listen Sie die verfügbaren Datenbanken auf, löschen Sie die zuvor erstellte Datenbank und führen Sie sie erneut auf, um sicherzustellen, dass die Datenbank gelöscht wurde.

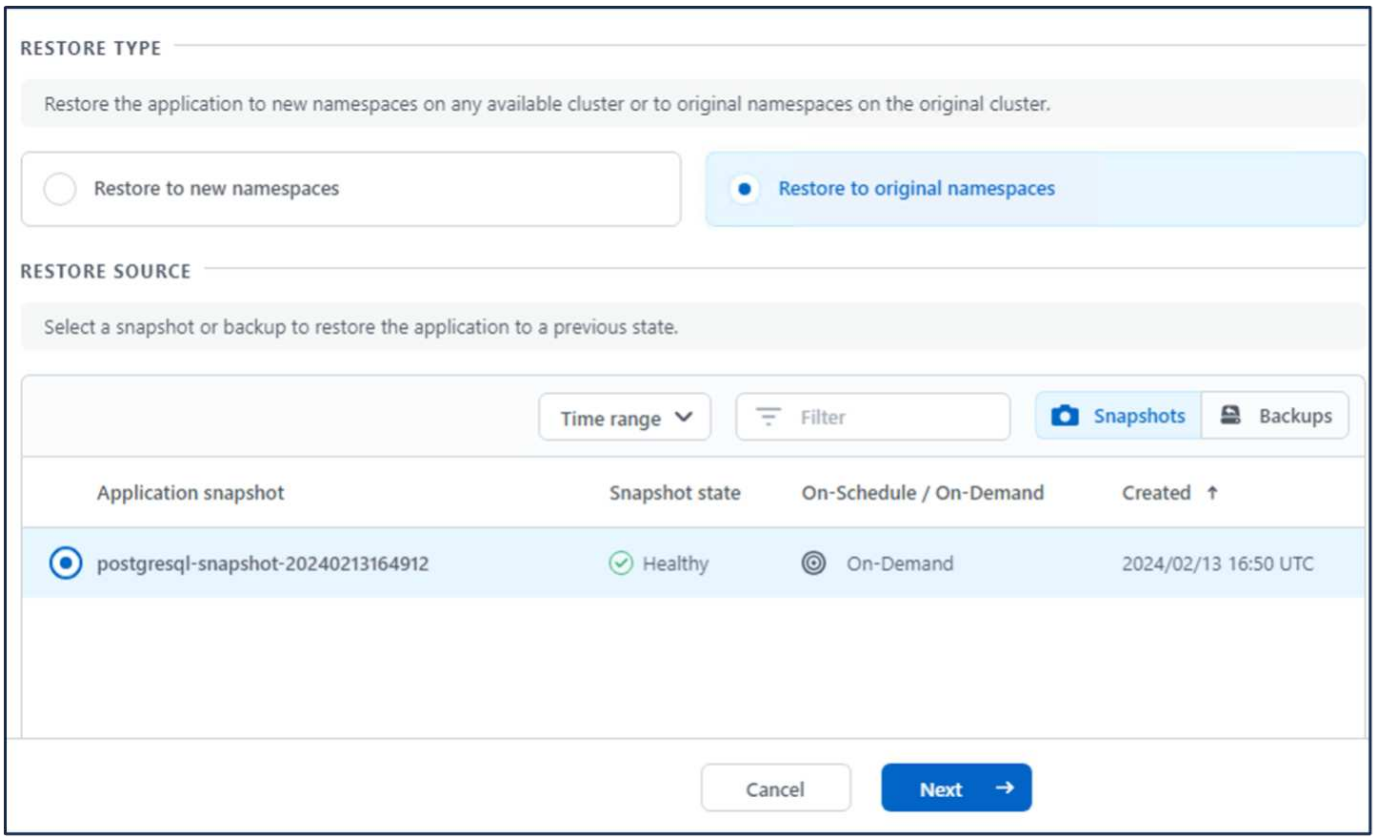
```
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

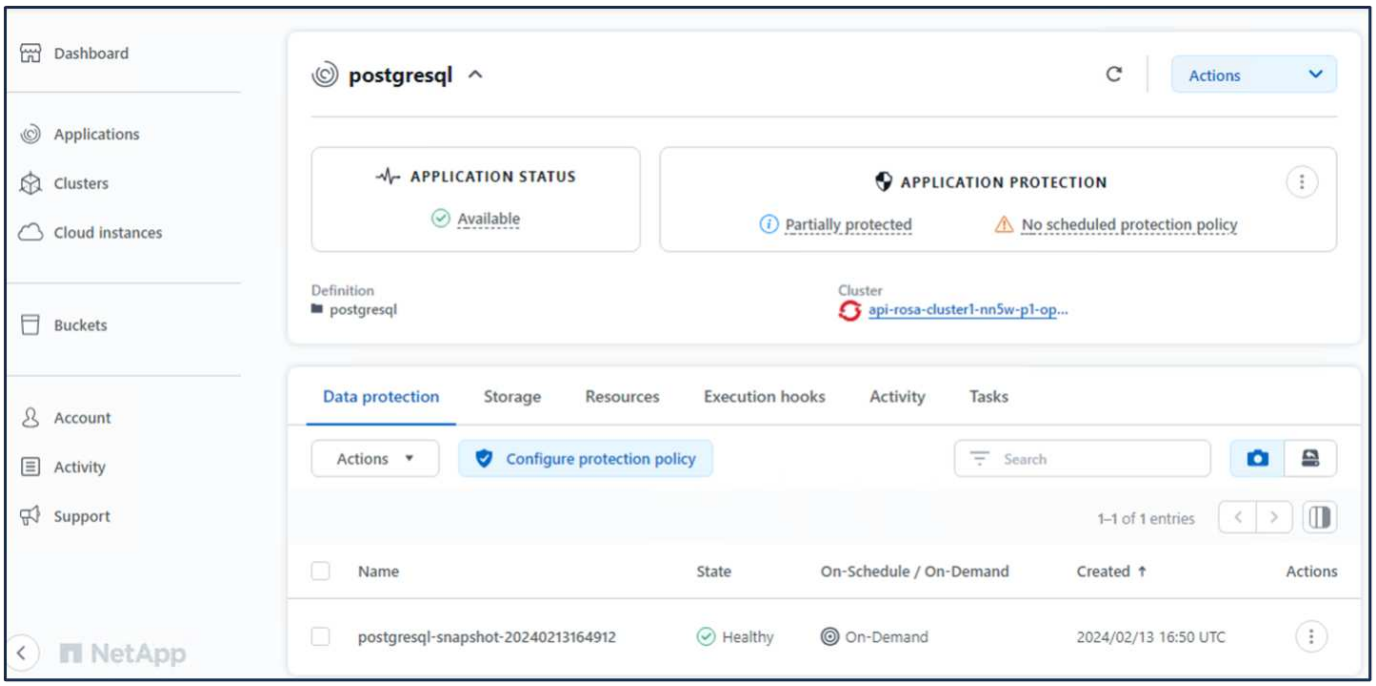
11. Wiederherstellen von einem Snapshot mit ACS

Um die Anwendung von einem Snapshot wiederherzustellen, gehen Sie zur ACS-UI-Landing Page, wählen Sie

die Anwendung aus und wählen Sie Wiederherstellen. Sie müssen einen Snapshot oder ein Backup auswählen, von dem aus wiederhergestellt werden soll. (In der Regel würden auf Basis einer von Ihnen konfigurierten Richtlinie mehrere erstellt werden.) Treffen Sie in den nächsten Bildschirmanzeigen die richtige Auswahl und klicken Sie dann auf **Wiederherstellen**. Der Anwendungsstatus wechselt von Wiederherstellen zu verfügbar, nachdem er aus dem Snapshot wiederhergestellt wurde.







12. Überprüfen Sie, ob Ihre App aus der Momentaufnahme wiederhergestellt wurde

Melden Sie sich beim postgresql-Client an und Sie sollten nun die Tabelle und den Datensatz in der Tabelle sehen, die Sie zuvor hatten. Das ist alles. Durch Klicken auf eine Schaltfläche wurde Ihre Anwendung in einen früheren Zustand zurückgesetzt. So einfach machen wir es unseren Kunden mit Astra Control.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
        List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```


Datenmigration

Auf dieser Seite werden die Datenmigrationsoptionen für Container-Workloads auf verwalteten Red hat OpenShift-Clustern unter Verwendung von FSX for NetApp ONTAP für persistenten Storage angezeigt.

Datenmigration

Red hat OpenShift-Service auf AWS sowie FSX for NetApp ONTAP (FSxN) sind Teil ihres Service-Portfolios von AWS. FSxN ist mit Single AZ- oder Multi-AZ-Optionen verfügbar. Die Multi-Az-Option bietet Datenschutz bei Ausfall einer Verfügbarkeitszone. FSxN kann in Astra Trident integriert werden, um persistenten Storage für Applikationen auf ROSA Clustern bereitzustellen.

Integration von FSxN mit Trident mit Helm Chart

ROSA Cluster Integration mit Amazon FSX for ONTAP

Die Migration von Container-Applikationen umfasst Folgendes:

- Persistente Volumes: Dies ist mit BlueXP möglich. Eine weitere Option ist der Einsatz von Astra Control Center für die Migration von Container-Applikationen von On-Premises- in die Cloud-Umgebung. Automatisierung kann für den gleichen Zweck eingesetzt werden.
- Applikations-Metadaten: Dies kann mithilfe von OpenShift GitOps (Argo CD) erreicht werden.

Failover und Failback von Anwendungen auf ROSA-Cluster mit FSxN für persistenten Speicher

Das folgende Video zeigt eine Demonstration von Failover- und Failback-Szenarien mit BlueXP und der Argo CD.

Failover und Failback von Anwendungen auf ROSA Cluster

Datensicherungs- und Migrationslösung für OpenShift-Container-Workloads