NetApp Public- und Hybrid-Cloud-Lösungen

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

Inhalt

NetApp Public- und Hybrid-Cloud-Lösungen . . . 1
Neuigkeiten zu NetApp Public- und Hybrid-Cloud-Lösungen . . . 2
NetApp Hybrid Multicloud mit VMware-Lösungen . . . 3
VMware für die Public Cloud . . . 3
Übersicht über NetApp Hybrid Multicloud mit VMware . . . 3
NetApp -Lösungen für VMware in Hyperscalern . . . 7
Unterstützte Konfigurationen für NetApp Hybrid Multicloud mit VMware . . . 10
VMware in der Hyperscaler-Konfiguration . . . 10
NetApp Storage in Public Clouds . . . 35
Zusammenfassung und Fazit: Warum NetApp Hybrid Multicloud mit VMware . . . 137
Anwendungsfälle für VMware Hybrid Cloud . . . 139
Anwendungsfälle für NetApp Hybrid Multicloud mit VMware . . . 139
NetApp -Lösungen für VMware in Hyperscalern . . . 140
NetApp -Lösungen für Amazon VMware Managed Cloud (VMC) . . . 141
NetApp -Lösungen für Azure VMware Solution (AVS) . . . 141
NetApp -Lösungen für Google Cloud VMware Engine (GCVE) . . . 142
NetApp für AWS/VMC . . . 142
NetApp -Funktionen für AWS VMC . . . 142
Schützen Sie Workloads auf AWS/VMC . . . 144
Migrieren Sie Workloads auf AWS/VMC . . . 261
NetApp für AWS / EVS . . . 276
Mounten Sie FSx ONTAP als externen Datenspeicher für EVS . . . 276
FSx ONTAP Datenspeicher für EVS schützen . . . 300
NetApp für Azure / AVS . . . 333
NetApp -Funktionen für Azure AVS . . . 334
Schützen Sie Workloads auf Azure/AVS . . . 335
Migrieren von Workloads auf Azure/AVS . . . 404
NetApp für GCP/GCVE . . . 419
NetApp -Funktionen für die Google Cloud Platform GCVE . . . 419
Schützen Sie Workloads auf GCP/GCVE . . . 420
Migrieren Sie Workloads auf GCP/GCVE . . . 452
Sichern Sie Daten mit Google Cloud NetApp Volumes in Google Cloud . . . 469
NetApp Disaster Recovery . . . 541
3-2-1-Datenschutz für VMware mit SnapCenter Plug-in sowie NetApp Backup und Recovery zum Schutz von VMware-Workloads . . . 541
NetApp Disaster Recovery . . . 576
NetApp Hybrid Multicloud mit Red Hat OpenShift Container-Workloads . . . 618
Erste Schritte . . . 618
NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads . . . 618
Wertversprechen der NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads . . . 620
Unterstützte Lösungen von NetApp Hybrid Multicloud für Red Hat OpenShift Container-Workloads . . . 621
Versionen verschiedener Komponenten, die bei der Lösungsvalidierung verwendet werden . . . 625

Unterstützte NetApp Storage-Integrationen mit Red Hat OpenShift Containers . . . 626
Zusätzliche Dokumentation . . . 630
Openshift für lokale Anwendungen . . . 630
NetApp -Lösung mit Red Hat OpenShift Container-Plattform-Workloads auf VMware . . . 630
Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf VMware . . . 631
Datenschutz mit Trident Protect . . . 633
Hybrid Cloud mit selbstverwalteten Komponenten . . . 634
NetApp -Lösung mit Red Hat OpenShift Container-Plattform-Workloads in der Hybrid Cloud . . . 634
Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf AWS . . . 636
Bereitstellen und Konfigurieren der Red Hat OpenShift Container Platform in Google Cloud . . . 638
Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf Azure . . . 640
Datenschutz mit Trident Protect . . . 643
Hybrid Cloud mit vom Anbieter verwalteten Komponenten . . . 644
NetApp -Lösung mit verwalteten Red Hat OpenShift Container-Plattform-Workloads . . . 644
Bereitstellen und Konfigurieren der Managed Red Hat OpenShift Container-Plattform auf AWS . . . 644
Bereitstellen und Konfigurieren von OpenShift Dedicated auf Google Cloud mit Google Cloud NetApp Volumes . . . 647
Datenschutz . . . 649
Zusätzliche NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift-Workloads . . . 650
Schützen Sie Daten mit Trident Protect . . . 650
Datenschutz für Container-Apps in OpenShift Container Platform mit Trident Protect . . . 650
Schützen Sie VMs in Red Hat OpenShift Virtualization mit Trident Protect . . . 662
Schützen Sie Container-Apps mit Tools von Drittanbietern . . . 682
Datenschutz für Container-Apps in der OpenShift Container Platform mithilfe der OpenShift API for Data Protection (OADP) . . . 682
Installation des OpenShift API for Data Protection (OADP)-Operators . . . 684
Erstellen eines On-Demand-Backups für Apps in OpenShift Container Platform . . . 693
Migrieren einer App von einem Cluster zu einem anderen . . . 696
Wiederherstellen einer App aus einem Backup . . . 700
Löschen von Backups und Wiederherstellungen mit Velero . . . 707
Sehen Sie sich Videos und Demos zu Hybrid-Multicloud-Lösungen mit NetApp an . . . 709
Sehen Sie sich Videos zu Hybrid-Multicloud-Lösungen für Amazon Web Services mit NetApp an . . . 709
Mit dem Gast verbundener Speicher . . . 709
Gesamtbetriebskosten und zusätzliche Datenspeicher . . . 709
Migrations-Workflows (HCX) . . . 709
Sehen Sie sich Videos zu Hybrid-Multicloud-Lösungen für Azure VMware Cloud mit NetApp an . . . 709
Ergänzende Datenspeicher . . . 709
Notfallwiederherstellung . . . 709
Migrations-Workflows (HCX) . . . 710
Sehen Sie sich Videos zu Hybrid-Multicloud-Lösungen für Red Hat OpenShift mit NetApp an . . . 710
Snapshots und Wiederherstellung . . . 710
Speicherintegration . . . 710
Failover und Failback . . . 710
Lösungsautomatisierung . . . 710
Lesen Sie die Blogs zu Cloud-Lösungen von NetApp Experten . . . 711

VMware-Integration mit AWS und Amazon FSx für ONTAP . . . 711
Azure VMware-Lösung . . . 711
Google Cloud VMware Engine . . . 711
Datenschutz und -verwaltung . . . 711
NetApp für OpenShift-Container-Workloads . . . 711
VMware Sovereign Cloud . . . 711
Rechtliche Hinweise . . . 712
Copyright . . . 712
Marken . . . 712
Patente . . . 712
Datenschutzrichtlinie . . . 712

NetApp Public- und Hybrid-Cloud-Lösungen

Neuigkeiten zu NetApp Public- und Hybrid-Cloud-Lösungen

Informieren Sie sich über Neuigkeiten zu öffentlichen und hybriden Cloud-Lösungen.

[[18-august-2025]]
== 18. August 2025

Die NetApp Solutions-Site ist jetzt die"NetApp Lösungsfamilie" , das die folgenden Websites umfasst:

- "NetApp Lösungen für künstliche Intelligenz"
- "NetApp Container-Lösungen"
- "NetApp Datenmanagementlösungen"
- "NetApp Datenbanklösungen"
- NetApp Public- und Hybrid-Cloud-Lösungen
- "NetApp Lösungen für SAP"
- "NetApp Virtualisierungslösungen"

NetApp Hybrid Multicloud mit VMware-Lösungen

VMware für die Public Cloud

Übersicht über NetApp Hybrid Multicloud mit VMware

Die meisten IT-Organisationen verfolgen den Hybrid-Cloud-First-Ansatz. Diese Organisationen befinden sich in einer Transformationsphase und die Kunden bewerten ihre aktuelle IT-Landschaft und migrieren dann ihre Workloads auf der Grundlage der Bewertungs- und Ermittlungsübung in die Cloud.

Zu den Faktoren, die Kunden dazu bewegen, in die Cloud zu migrieren, können Elastizität und Burst, der Ausstieg aus Rechenzentren, die Konsolidierung von Rechenzentren, End-of-Life-Szenarien, Fusionen, Übernahmen usw. gehören. Der Grund für diese Migration kann je nach Organisation und ihren jeweiligen Geschäftsprioritäten unterschiedlich sein. Beim Wechsel zur Hybrid Cloud ist die Auswahl des richtigen Speichers in der Cloud sehr wichtig, um die Leistungsfähigkeit und Elastizität der Cloud-Bereitstellung voll auszuschöpfen.

VMware Cloud-Optionen in der Public Cloud

In diesem Abschnitt wird beschrieben, wie jeder der Cloud-Anbieter einen VMware Software Defined Data Center (SDDC)- und/oder VMware Cloud Foundation (VCF)-Stack innerhalb seiner jeweiligen öffentlichen Cloud-Angebote unterstützt.

Azure VMware-Lösung

Azure VMware Solution ist ein Hybrid-Cloud-Dienst, der voll funktionsfähige VMware SDDCs innerhalb der öffentlichen Microsoft Azure-Cloud ermöglicht. Azure VMware Solution ist eine Erstanbieterlösung, die vollständig von Microsoft verwaltet und unterstützt wird und von VMware unter Nutzung der Azure-Infrastruktur verifiziert wurde. Dies bedeutet, dass Kunden bei der Bereitstellung der Azure VMware Solution VMware ESXi für die Computervirtualisierung, vSAN für hyperkonvergenten Speicher und NSX für Netzwerk und Sicherheit erhalten und gleichzeitig von der globalen Präsenz von Microsoft Azure, den erstklassigen Rechenzentrumseinrichtungen und der Nähe zum umfangreichen Ökosystem nativer Azure-Dienste und -Lösungen profitieren.

VMware Cloud auf AWS

VMware Cloud auf AWS bringt die SDDC-Software der Enterprise-Klasse von VMware in die AWS Cloud mit optimiertem Zugriff auf native AWS-Dienste. VMware Cloud on AWS basiert auf VMware Cloud Foundation und integriert die Computing-, Speicher- und Netzwerkvirtualisierungsprodukte von VMware (VMware vSphere, VMware vSAN und VMware NSX) zusammen mit der VMware vCenter Server-Verwaltung, die für die Ausführung auf einer dedizierten, elastischen Bare-Metal-AWS-Infrastruktur optimiert ist.

Google Cloud VMware Engine

Google Cloud VMware Engine ist ein Infrastructure-as-a-Service (IaaS)-Angebot, das auf der leistungsstarken, skalierbaren Infrastruktur und dem VMware Cloud Foundation Stack von Google Cloud basiert – VMware vSphere, vCenter, vSAN und NSX-T. Dieser Dienst ermöglicht einen schnellen Weg in die Cloud und ermöglicht die nahtlose Migration oder Erweiterung bestehender VMware-Workloads von lokalen Umgebungen zur Google Cloud Platform, ohne die Kosten, den Aufwand oder das Risiko einer Neustrukturierung von Anwendungen oder Umrüstungen. Es handelt sich um einen von Google verkauften und unterstützten Dienst in enger Zusammenarbeit mit VMware.

SDDC Private Cloud und NetApp Cloud Volumes Colocation bieten beste Leistung bei minimaler Netzwerklatenz.

Wussten Sie?

Unabhängig von der verwendeten Cloud umfasst der anfängliche Cluster bei der Bereitstellung eines VMware SDDC die folgenden Produkte:

- VMware ESXi-Hosts für die Computervirtualisierung mit einer vCenter Server-Appliance für die Verwaltung
- VMware vSAN hyperkonvergenter Speicher, der die physischen Speicherressourcen jedes ESXi-Hosts integriert
- VMware NSX für virtuelle Netzwerke und Sicherheit mit einem NSX Manager-Cluster für die Verwaltung

Storage-Konfiguration

Für Kunden, die speicherintensive Workloads hosten und auf einer in der Cloud gehosteten VMware-Lösung skalieren möchten, schreibt die standardmäßige hyperkonvergente Infrastruktur vor, dass die Erweiterung sowohl auf den Rechen- als auch auf den Speicherressourcen erfolgen sollte.

Durch die Integration mit NetApp Cloud Volumes, wie Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (verfügbar in allen drei großen Hyperscalern) und Google Cloud NetApp Volumes für Google Cloud, haben Kunden jetzt die Möglichkeit, ihren Speicher unabhängig voneinander zu skalieren und dem SDDC-Cluster nur bei Bedarf Rechenknoten hinzuzufügen.

Hinweise:

- VMware empfiehlt keine unausgeglichenen Clusterkonfigurationen. Daher bedeutet die Erweiterung des Speichers das Hinzufügen weiterer Hosts, was wiederum höhere Gesamtbetriebskosten bedeutet.
- Es ist nur eine vSAN-Umgebung möglich. Daher steht der gesamte Speicherverkehr in direkter Konkurrenz zu den Produktionsarbeitslasten.
- Es besteht keine Möglichkeit, mehrere Leistungsstufen bereitzustellen, um Anwendungsanforderungen, Leistung und Kosten aufeinander abzustimmen.
- Es ist sehr leicht, die Grenzen der Speicherkapazität von vSAN zu erreichen, das auf den Cluster-Hosts aufgebaut ist. Verwenden Sie NetApp Cloud Volumes, um den Speicher zu skalieren und entweder aktive Datensätze zu hosten oder kältere Daten in einen persistenten Speicher zu verschieben.

Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (verfügbar in allen drei großen Hyperscalern) und Google Cloud NetApp Volumes für Google Cloud können in Verbindung mit Gast-VMs verwendet werden. Diese hybride Speicherarchitektur besteht aus einem vSAN-Datenspeicher, der das Gastbetriebssystem und die Binärdaten der Anwendung enthält. Die Anwendungsdaten werden über einen gastbasierten iSCSI-Initiator oder die NFS/SMB-Mounts an die VM angehängt, die direkt mit Amazon FSx ONTAP, Cloud Volume ONTAP, Azure NetApp Files und Google Cloud NetApp Volumes für Google Cloud kommunizieren. Mit dieser Konfiguration können Sie Probleme mit der Speicherkapazität problemlos bewältigen, da bei vSAN der verfügbare freie Speicherplatz vom verwendeten Slack-Speicherplatz und den Speicherrichtlinien abhängt.

Betrachten wir einen SDDC-Cluster mit drei Knoten auf VMware Cloud on AWS:

- Die gesamte Rohkapazität für ein SDDC mit drei Knoten beträgt 31,1 TB (ungefähr 10 TB für jeden Knoten).
- Der vor dem Hinzufügen zusätzlicher Hosts zu wartende Slack-Speicherplatz beträgt 25 % = (0,25 x 31,1

TB) = 7,7 TB.

- Die nutzbare Rohkapazität nach Abzug des Schlupfspeichers beträgt 23,4 TB
- Der tatsächlich verfügbare freie Speicherplatz hängt von der angewendeten Speicherrichtlinie ab.

  Beispiel:

  - RAID 0 = effektiver freier Speicherplatz = 23,4 TB (nutzbare Rohkapazität/1)
  - RAID 1 = effektiver freier Speicherplatz = 11,7 TB (nutzbare Rohkapazität/2)
  - RAID 5 = effektiver freier Speicherplatz = 17,5 TB (nutzbare Rohkapazität/1,33)

Die Verwendung von NetApp Cloud Volumes als Gastspeicher würde daher dazu beitragen, den Speicher zu erweitern und die Gesamtbetriebskosten zu optimieren, während gleichzeitig die Leistungs- und Datenschutzanforderungen erfüllt werden.

Zum Zeitpunkt der Erstellung dieses Dokuments war die In-Guest-Speicherung die einzige verfügbare Option.

Wichtige Punkte

- Platzieren Sie in hybriden Speichermodellen Arbeitslasten der Stufe 1 oder mit hoher Priorität auf dem vSAN-Datenspeicher, um alle spezifischen Latenzanforderungen zu erfüllen, da sie Teil des Hosts selbst und in der Nähe sind. Verwenden Sie In-Guest-Mechanismen für alle Workload-VMs, für die Transaktionslatenzen akzeptabel sind.
- Mit der NetApp SnapMirror Technologie lassen sich die Workload-Daten vom lokalen ONTAP-System zu Cloud Volumes ONTAP oder Amazon FSx ONTAP replizieren, um die Migration mithilfe von Mechanismen auf Blockebene zu vereinfachen. Dies gilt nicht für Azure NetApp Files und Google Cloud NetApp Volumes. Für die Migration von Daten zu Azure NetApp Files oder Google Cloud NetApp Volumes können je nach verwendetem Dateiprotokoll NetApp XCP, NetApp Copy and Sync, rysnc oder robocopy verwendet werden.
- Tests zeigen eine zusätzliche Latenz von 2–4 ms beim Zugriff auf den Speicher von den jeweiligen SDDCs. Berücksichtigen Sie diese zusätzliche Latenz bei der Speicherzuordnung in den Anwendungsanforderungen.
- Stellen Sie zum Mounten von mit dem Gast verbundenem Speicher während des Test-Failovers und des tatsächlichen Failovers sicher, dass die iSCSI-Initiatoren neu konfiguriert sind, DNS für SMB-Freigaben aktualisiert ist und NFS-Mount-Punkte in fstab aktualisiert sind.
- Stellen Sie sicher, dass die Registrierungseinstellungen für Microsoft Multipath I/O (MPIO) im Gastbetriebssystem, die Firewall und das Datenträger-Timeout in der VM richtig konfiguriert sind.

Dies gilt nur für mit dem Gast verbundenen Speicher.

Vorteile von NetApp Cloud Storage

NetApp Cloud Storage bietet die folgenden Vorteile:

- Verbessert die Rechen-zu-Speicher-Dichte durch Skalierung des Speichers unabhängig von der Rechenleistung.
- Ermöglicht Ihnen, die Anzahl der Hosts zu reduzieren und so die Gesamtbetriebskosten zu senken.
- Der Ausfall eines Rechenknotens beeinträchtigt die Speicherleistung nicht.

- Die Volume-Umgestaltung und die dynamischen Service-Level-Funktionen von Azure NetApp Files ermöglichen Ihnen eine Kostenoptimierung durch die Dimensionierung für stationäre Workloads und verhindern so eine Überbereitstellung.
- Die Speichereffizienz, das Cloud-Tiering und die Möglichkeiten zur Änderung des Instanztyps von Cloud Volumes ONTAP ermöglichen optimale Möglichkeiten zum Hinzufügen und Skalieren von Speicher.
- Verhindert eine Überbereitstellung, da Speicherressourcen nur bei Bedarf hinzugefügt werden.
- Effiziente Snapshot-Kopien und -Klone ermöglichen Ihnen das schnelle Erstellen von Kopien ohne Leistungseinbußen.
- Hilft bei der Abwehr von Ransomware-Angriffen durch schnelle Wiederherstellung aus Snapshot-Kopien.
- Bietet eine effiziente, auf inkrementellen Blockübertragungen basierende regionale Notfallwiederherstellung und eine integrierte Blocksicherung über Regionen hinweg, die bessere RPO und RTOs bietet.

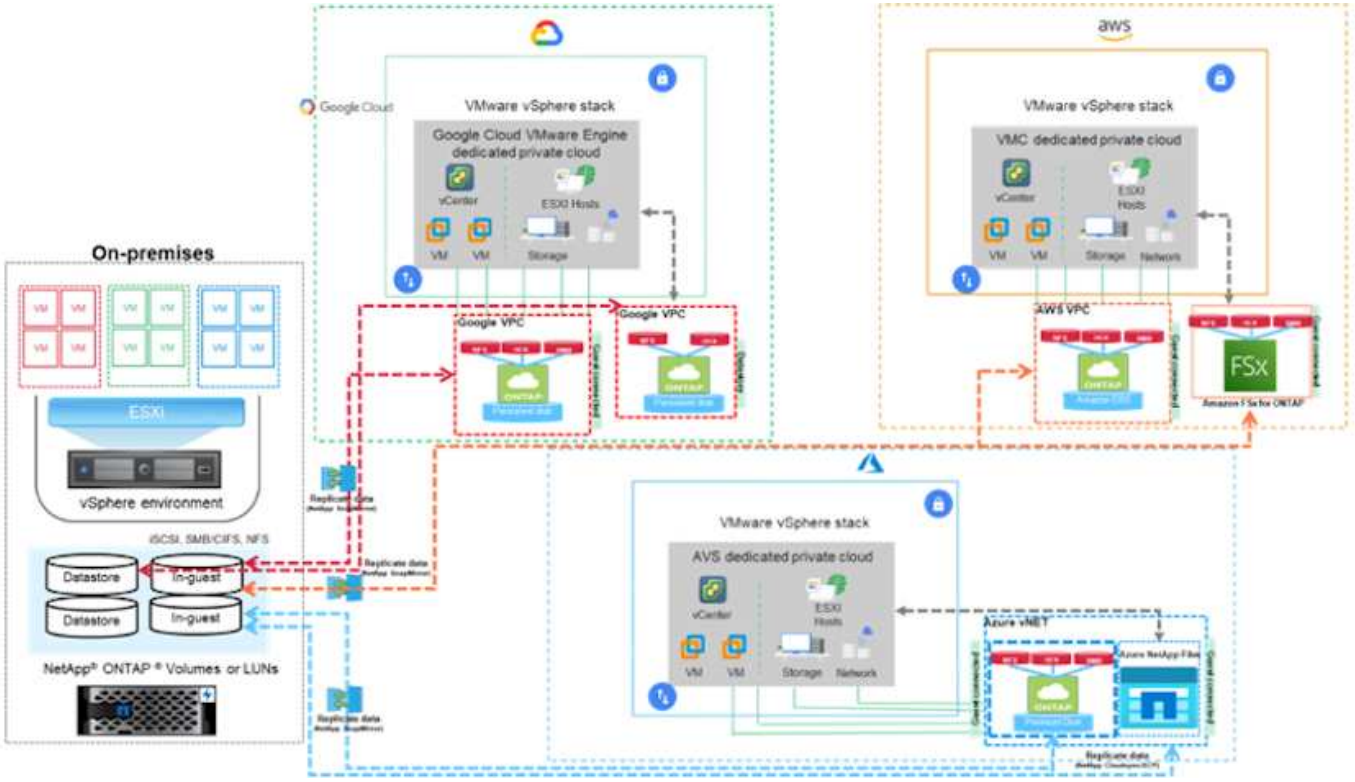
Annahmen

- SnapMirror -Technologie oder andere relevante Datenmigrationsmechanismen sind aktiviert. Es gibt viele Konnektivitätsoptionen, von vor Ort bis zu jeder Hyperscaler-Cloud. Nutzen Sie den passenden Weg und arbeiten Sie mit den entsprechenden Netzwerkteams zusammen.
- Zum Zeitpunkt der Erstellung dieses Dokuments war die In-Guest-Speicherung die einzige verfügbare Option.

> Beauftragen Sie NetApp -Lösungsarchitekten und entsprechende Hyperscaler-Cloud-Architekten mit der Planung und Dimensionierung des Speichers und der erforderlichen Anzahl von Hosts. NetApp empfiehlt, die Speicherleistungsanforderungen zu ermitteln, bevor Sie den Cloud Volumes ONTAP Sizer verwenden, um den Speicherinstanztyp oder das entsprechende Servicelevel mit dem richtigen Durchsatz festzulegen.

Detaillierte Architektur

Aus einer übergeordneten Perspektive zeigt diese Architektur (siehe Abbildung unten), wie hybride Multicloud-Konnektivität und App-Portabilität über mehrere Cloud-Anbieter hinweg erreicht werden kann, indem NetApp Cloud Volumes ONTAP, Google Cloud NetApp Volumes für Google Cloud und Azure NetApp Files als zusätzliche In-Guest-Speicheroption verwendet werden.



NetApp -Lösungen für VMware in Hyperscalern

Erfahren Sie mehr über die Funktionen, die NetApp den drei (3) wichtigsten Hyperscalern bietet – von NetApp als Speichergerät mit Gastanschluss oder als zusätzlicher NFS-Datenspeicher bis hin zur Migration von Workflows, Erweiterung/Bursting in die Cloud, Sicherung/Wiederherstellung und Notfallwiederherstellung.

Wählen Sie Ihre Cloud und überlassen Sie NetApp den Rest!



Um die Funktionen eines bestimmten Hyperscalers anzuzeigen, klicken Sie auf die

entsprechende Registerkarte für diesen Hyperscaler.

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

- "VMware in der Hyperscaler-Konfiguration"
- "NetApp Storage-Optionen"
- "NetApp / VMware Cloud-Lösungen"

VMware in der Hyperscaler-Konfiguration

Wie bei der lokalen Umgebung ist die Planung einer Cloud-basierten Virtualisierungsumgebung entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen und Migrieren von VMs.

AWS / VMC

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud on AWS SDDC einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp -Speicher verwenden.

In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP mit AWS VMC.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von VMware Cloud für AWS
- Verbinden Sie VMware Cloud mit FSx ONTAP

Sehen Sie sich die detaillierte"Konfigurationsschritte für VMC" .

Azure / AVS

In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Solution einrichten und verwalten und in Kombination mit den verfügbaren Optionen zum Anbinden von NetApp -Speicher verwenden.

In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP mit Azure VMware Solution.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Registrieren des Ressourcenanbieters und Erstellen einer privaten Cloud
- Herstellen einer Verbindung mit einem neuen oder vorhandenen virtuellen ExpressRoute-Netzwerkgateway
- Überprüfen Sie die Netzwerkkonnektivität und greifen Sie auf die private Cloud zu

Sehen Sie sich die detaillierte"Konfigurationsschritte für AVS" .

GCP / GCVE

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Anschließen von NetApp -Speicher verwenden.

In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP und Google Cloud NetApp Volumes mit GCVE.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von GCVE
- Privaten Zugriff auf GCVE aktivieren

Sehen Sie sich die detaillierte"Konfigurationsschritte für GCVE" .

NetApp Storage-Optionen

NetApp Speicher kann innerhalb jedes der drei großen Hyperscaler auf verschiedene Weise genutzt werden – entweder als Gastverbindung oder als zusätzlicher NFS-Datenspeicher.

Bitte besuchen Sie"Unterstützte NetApp -Speicheroptionen" für weitere Informationen.

AWS / VMC

AWS unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- FSx ONTAP als Gastspeicher
- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- FSx ONTAP als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungs-Speicheroptionen für VMC" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für VMC" .

Azure / AVS

Azure unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- Azure NetApp Files (ANF) als mit dem Gast verbundener Speicher
- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- Azure NetApp Files (ANF) als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungs-Speicheroptionen für AVS" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für AVS" .

GCP / GCVE

Google Cloud unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- Google Cloud NetApp Volumes (NetApp Volumes) als mit dem Gast verbundener Speicher
- Google Cloud NetApp Volumes (NetApp Volumes) als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungsspeicheroptionen für GCVE" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für GCVE" .

Lesen Sie mehr über"Google Cloud NetApp Volumes Datenspeicherunterstützung für Google Cloud VMware Engine (NetApp -Blog)" oder"So verwenden Sie Google Cloud NetApp Volumes als Datenspeicher für Google Cloud VMware Engine (Google-Blog)"

NetApp / VMware Cloud-Lösungen

Mit den Cloud-Lösungen von NetApp und VMware lassen sich viele Anwendungsfälle ganz einfach in Ihrem bevorzugten Hyperscaler implementieren. VMware definiert die wichtigsten Anwendungsfälle für Cloud-Workloads wie folgt:

- Schützen (beinhaltet sowohl Disaster Recovery als auch Backup/Wiederherstellung)
- Wandern
- Verlängern

AWS / VMC

"Durchsuchen Sie die NetApp -Lösungen für AWS/VMC"

Azure / AVS

"Durchsuchen Sie die NetApp -Lösungen für Azure/AVS"

GCP / GCVE

"Durchsuchen Sie die NetApp -Lösungen für Google Cloud Platform (GCP) / GCVE"

Unterstützte Konfigurationen für NetApp Hybrid Multicloud mit VMware

Verstehen der Kombinationen für NetApp -Speicherunterstützung bei den großen Hyperscalern.

	Gast verbunden	Zusätzlicher NFS-Datenspeicher
AWS	CVO FSx ONTAP"Details"	FSx ONTAP"Details"
Azurblau	CVO ANF"Details"	ANF"Details"
GCP	CVO NetApp Volumes"Details"	NetApp Volumes"Details"

VMware in der Hyperscaler-Konfiguration

Konfigurieren der Virtualisierungsumgebung beim Cloud-Anbieter

Details zur Konfiguration der Virtualisierungsumgebung in jedem der unterstützten Hyperscaler werden hier behandelt.

AWS / VMC

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud on AWS SDDC einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp -Speicher verwenden.

In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP mit AWS VMC.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von VMware Cloud für AWS

- Verbinden Sie VMware Cloud mit FSx ONTAP

Sehen Sie sich die detaillierte"Konfigurationsschritte für VMC" .

Azure / AVS

In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Solution einrichten und verwalten und in Kombination mit den verfügbaren Optionen zum Anbinden von NetApp -Speicher verwenden.

In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP mit Azure VMware Solution.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Registrieren des Ressourcenanbieters und Erstellen einer privaten Cloud
- Herstellen einer Verbindung mit einem neuen oder vorhandenen virtuellen ExpressRoute-Netzwerkgateway
- Überprüfen Sie die Netzwerkkonnektivität und greifen Sie auf die private Cloud zu

Sehen Sie sich die detaillierte"Konfigurationsschritte für AVS" .

GCP / GCVE

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Anschließen von NetApp -Speicher verwenden.

In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP und Google Cloud NetApp Volumes mit GCVE.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von GCVE
- Privaten Zugriff auf GCVE aktivieren

Sehen Sie sich die detaillierte"Konfigurationsschritte für GCVE" .

Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf AWS

Wie bei lokalen Umgebungen ist die Planung von VMware Cloud auf AWS entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen von VMs und zur Migration.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud on AWS SDDC einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp -Speicher verwenden.

In-Guest-Speicher ist derzeit die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP (CVO) mit AWS VMC.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

▼ **Bereitstellen und Konfigurieren von VMware Cloud für AWS**

"VMware Cloud auf AWS"bietet eine Cloud-native Erfahrung für VMware-basierte Workloads im AWS-

Ökosystem. Jedes VMware Software-Defined Data Center (SDDC) läuft in einer Amazon Virtual Private Cloud (VPC) und bietet einen vollständigen VMware-Stack (einschließlich vCenter Server), NSX-T Software-Defined Networking, vSAN Software-Defined Storage und einen oder mehrere ESXi-Hosts, die Ihren Workloads Rechen- und Speicherressourcen bereitstellen.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS einrichten und verwalten und es in Kombination mit Amazon FSx ONTAP und/oder Cloud Volumes ONTAP auf AWS mit In-Guest-Speicher verwenden.

In-Guest-Speicher ist derzeit die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP (CVO) mit AWS VMC.

Der Einrichtungsprozess kann in drei Teile unterteilt werden:

▼ **Registrieren Sie sich für ein AWS-Konto**

Registrieren Sie sich für eine"Amazon Web Services-Konto" .

Sie benötigen zum Einstieg ein AWS-Konto, sofern noch keins erstellt wurde. Ob neu oder bereits vorhanden, für viele Schritte dieses Verfahrens benötigen Sie Administratorrechte im Konto. Sehen Sie dies"Link" für weitere Informationen zu AWS-Anmeldeinformationen.

▼ **Registrieren Sie sich für ein My VMware-Konto**

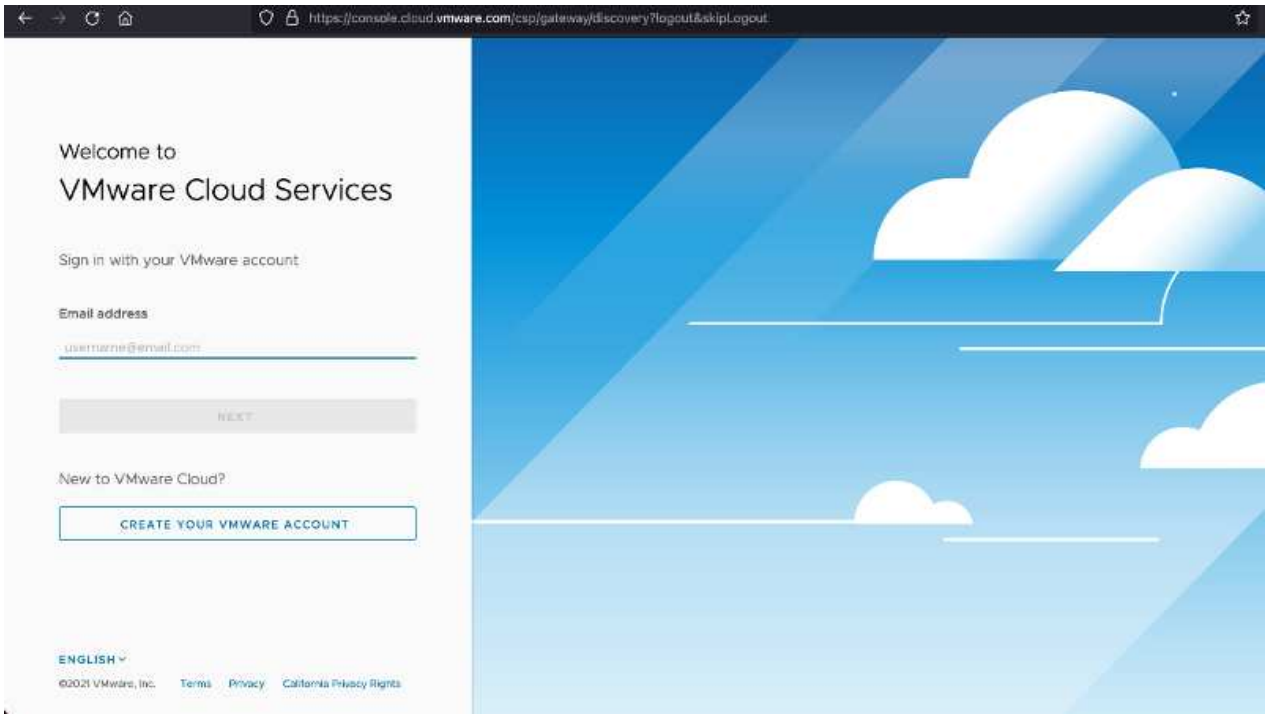
Registrieren Sie sich für eine"Meine VMware" Konto.

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

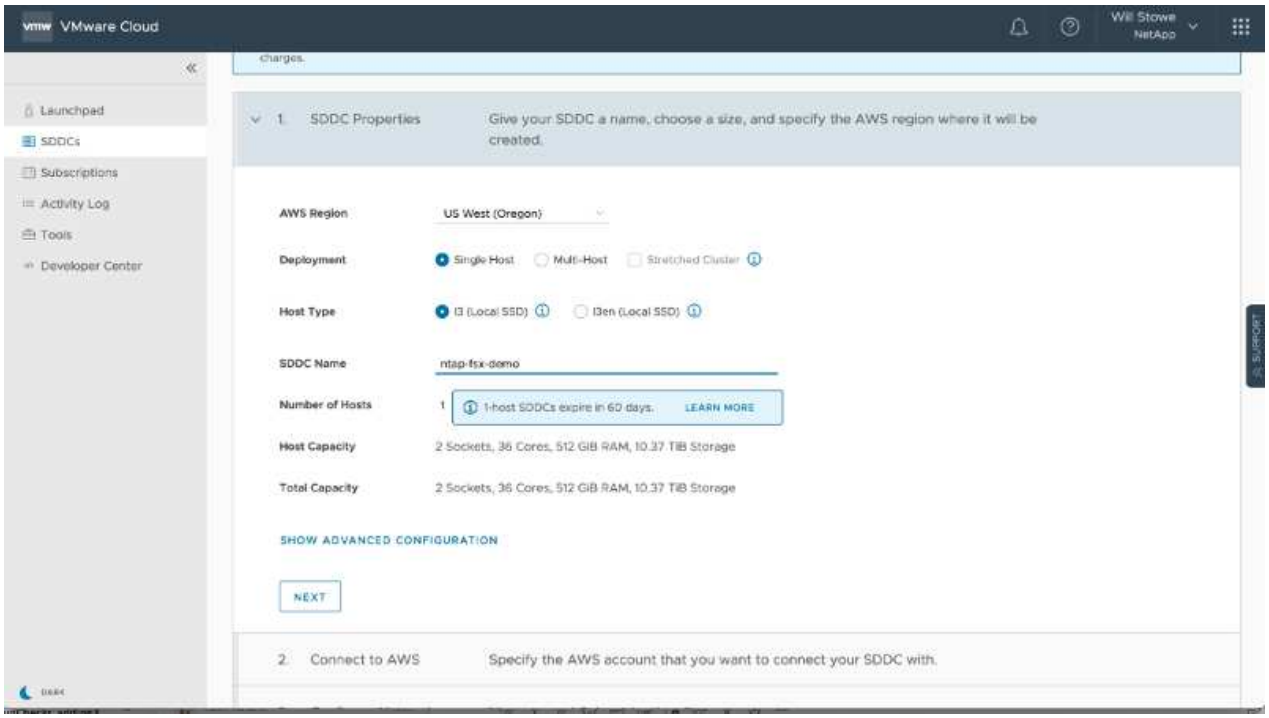
▼ **Bereitstellen von SDDC in VMware Cloud**

Nachdem das VMware-Konto konfiguriert und die richtige Dimensionierung vorgenommen wurde, ist die Bereitstellung eines Software-Defined Data Centers der naheliegende nächste Schritt zur Verwendung des VMware Cloud on AWS-Dienstes. Um ein SDDC zu erstellen, wählen Sie eine AWS-Region als Host aus, geben Sie dem SDDC einen Namen und geben Sie an, wie viele ESXi-Hosts das SDDC enthalten soll. Wenn Sie noch kein AWS-Konto haben, können Sie trotzdem ein SDDC mit Starterkonfiguration erstellen, das einen einzelnen ESXi-Host enthält.

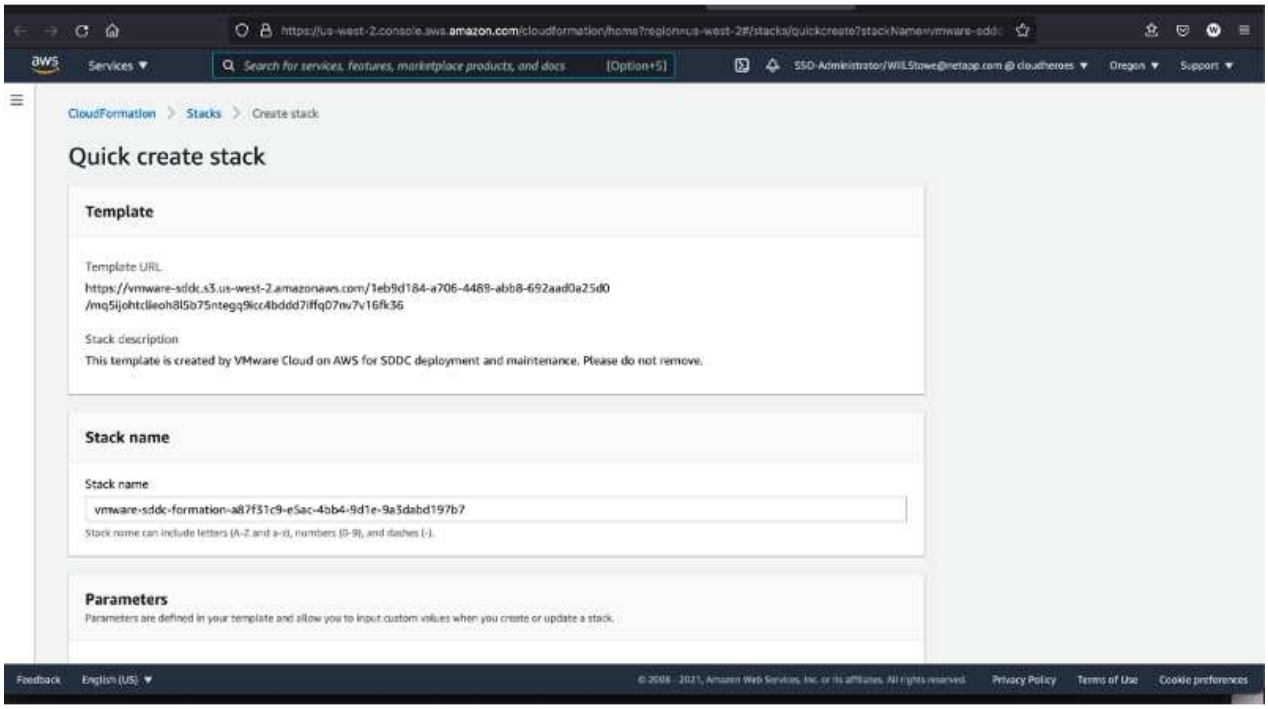
1. Melden Sie sich mit Ihren vorhandenen oder neu erstellten VMware-Anmeldeinformationen bei der VMware Cloud Console an.

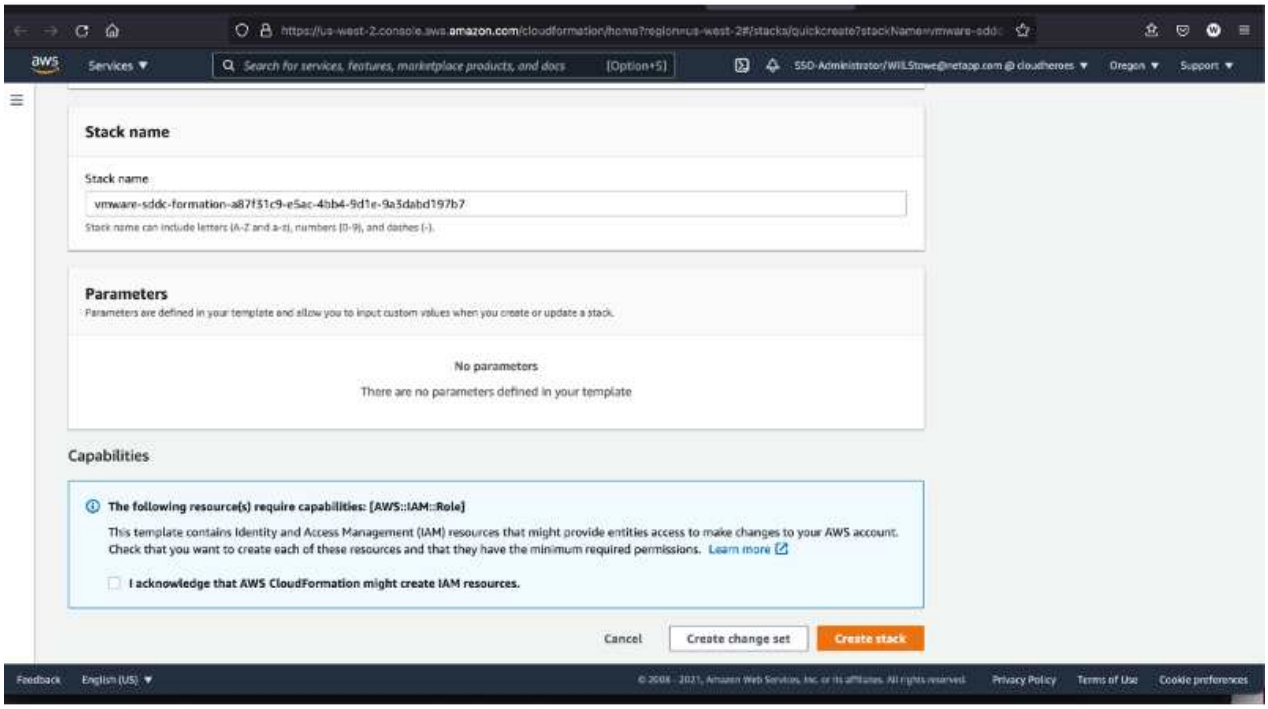


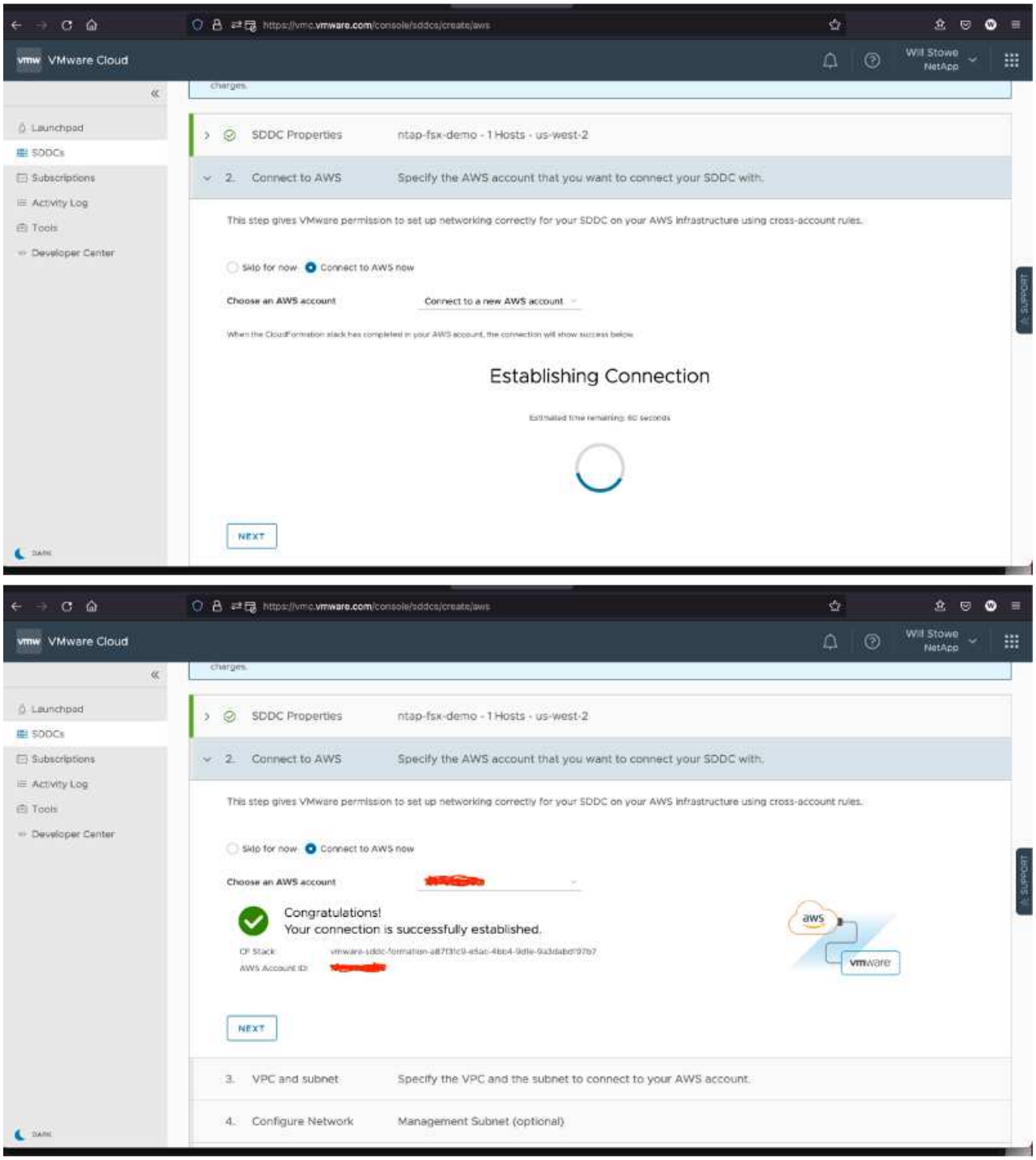
2. Konfigurieren Sie die AWS-Region, die Bereitstellung, den Hosttyp und den SDDC-Namen:



3. Stellen Sie eine Verbindung zum gewünschten AWS-Konto her und führen Sie den AWS Cloud Formation-Stack aus.

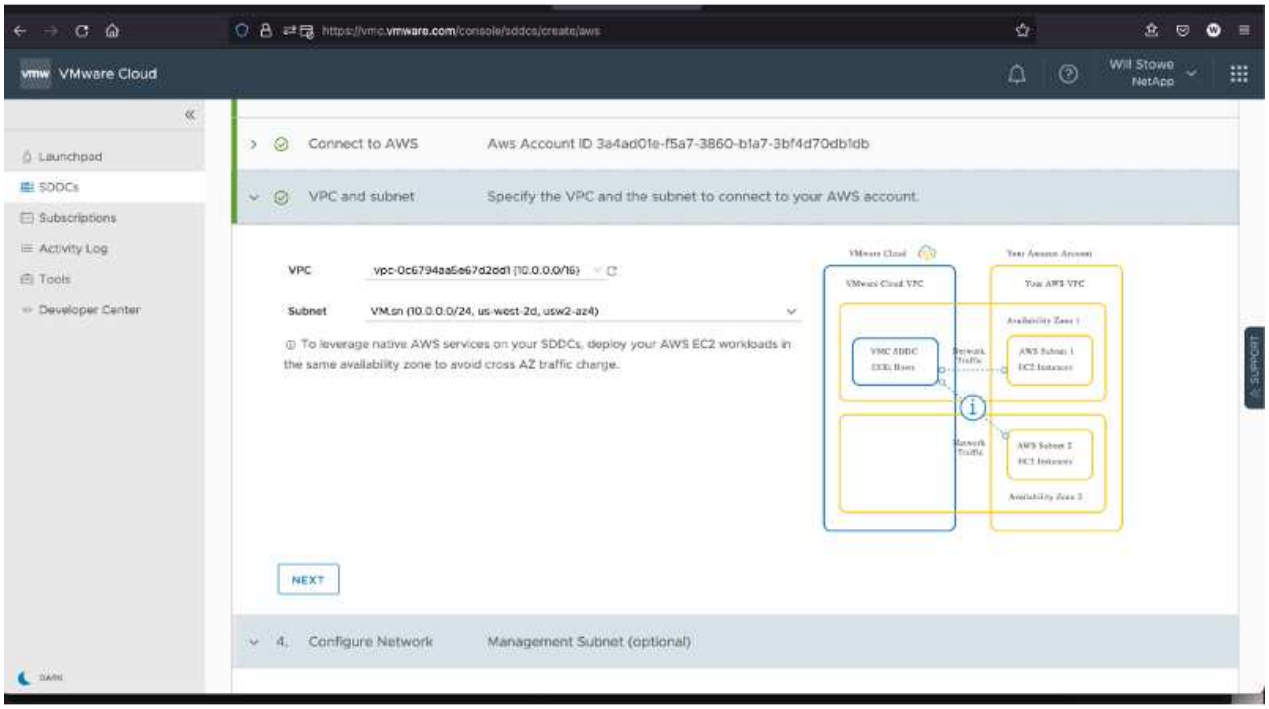

CloudFormation > Stacks > Create stack
Quick create stack
Template
Template URL
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ljohtclieoh8l5b75ntegq9icc4bddd7iffq07nv7v16fk36
Stack description
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.
Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.


Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
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

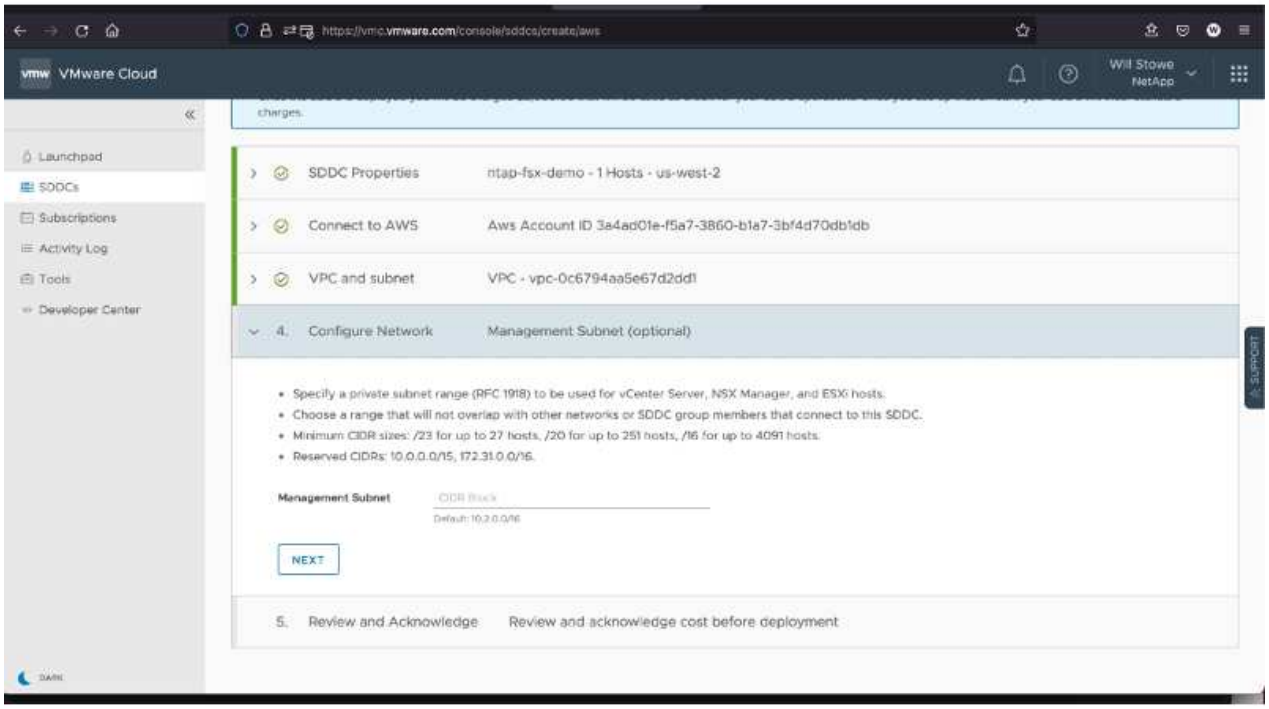


Bei dieser Validierung wird eine Single-Host-Konfiguration verwendet.

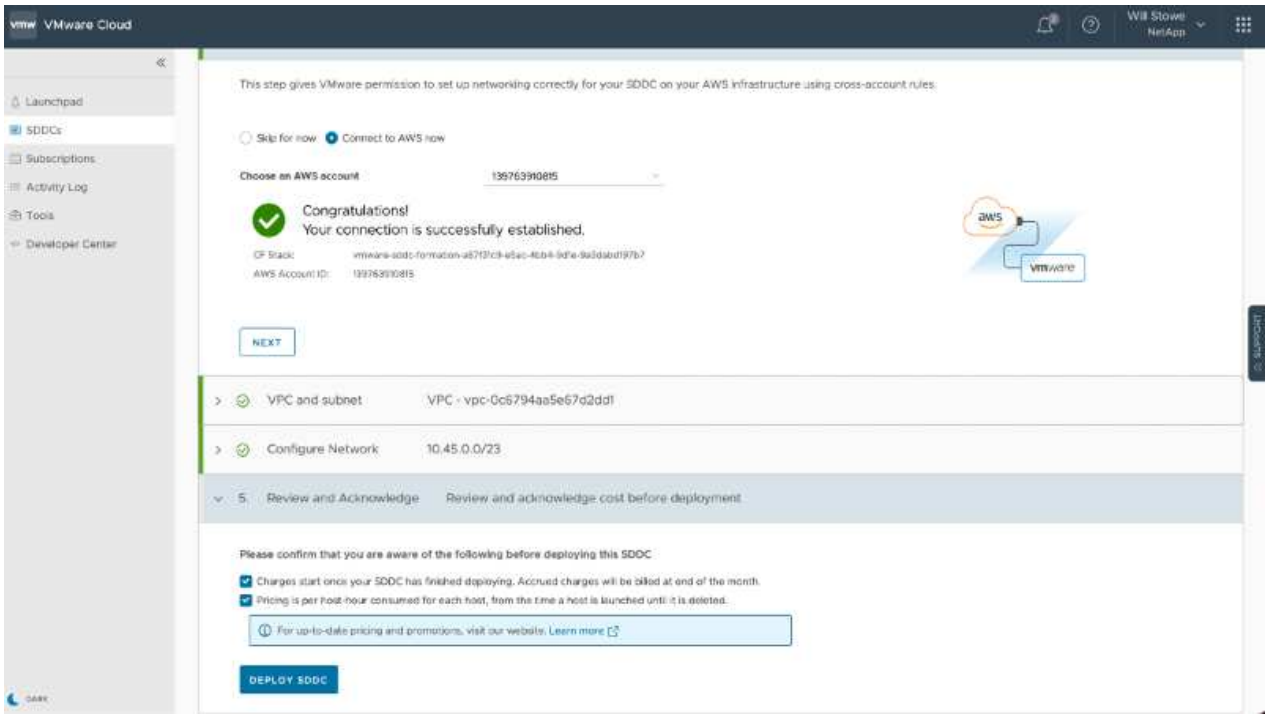
4. Wählen Sie das gewünschte AWS VPC aus, mit dem Sie die VMC-Umgebung verbinden möchten.



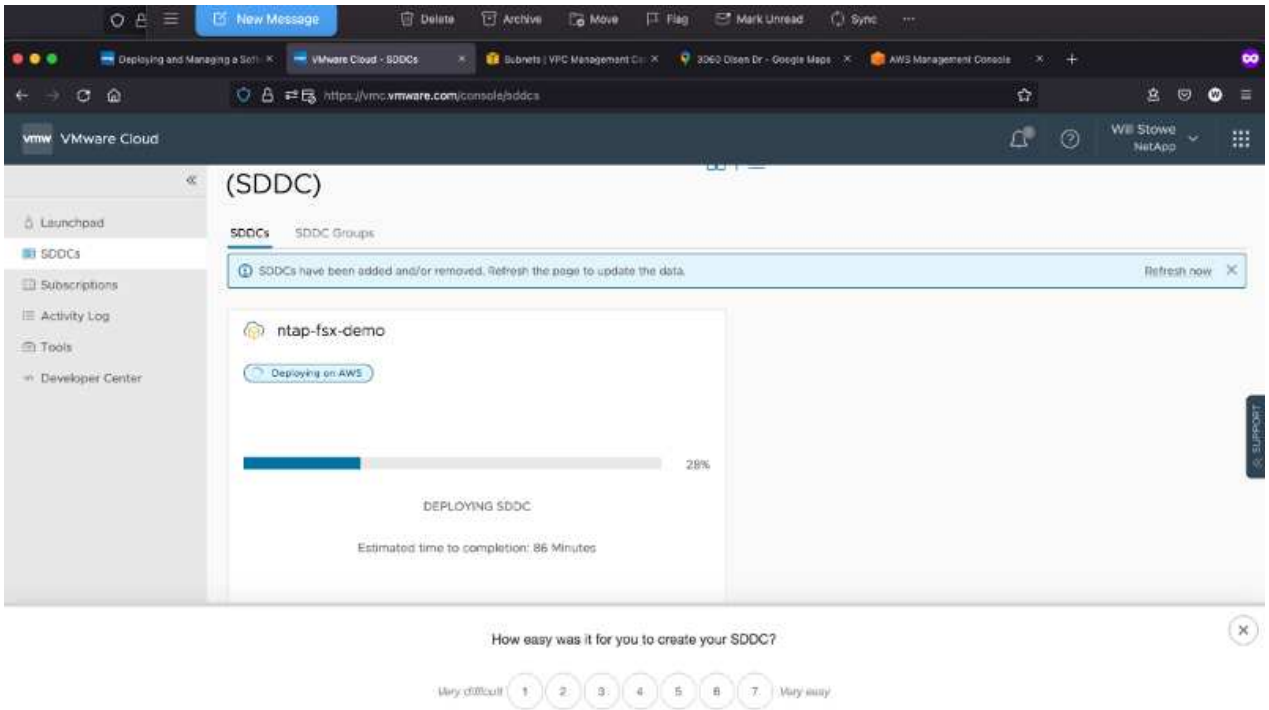
5. Konfigurieren Sie das VMC-Verwaltungssubnetz. Dieses Subnetz enthält von VMC verwaltete Dienste wie vCenter, NSX usw. Wählen Sie keinen Adressraum, der sich mit anderen Netzwerken überschneidet, die eine Verbindung zur SDDC-Umgebung benötigen. Befolgen Sie abschließend die unten aufgeführten Empfehlungen zur CIDR-Größe.



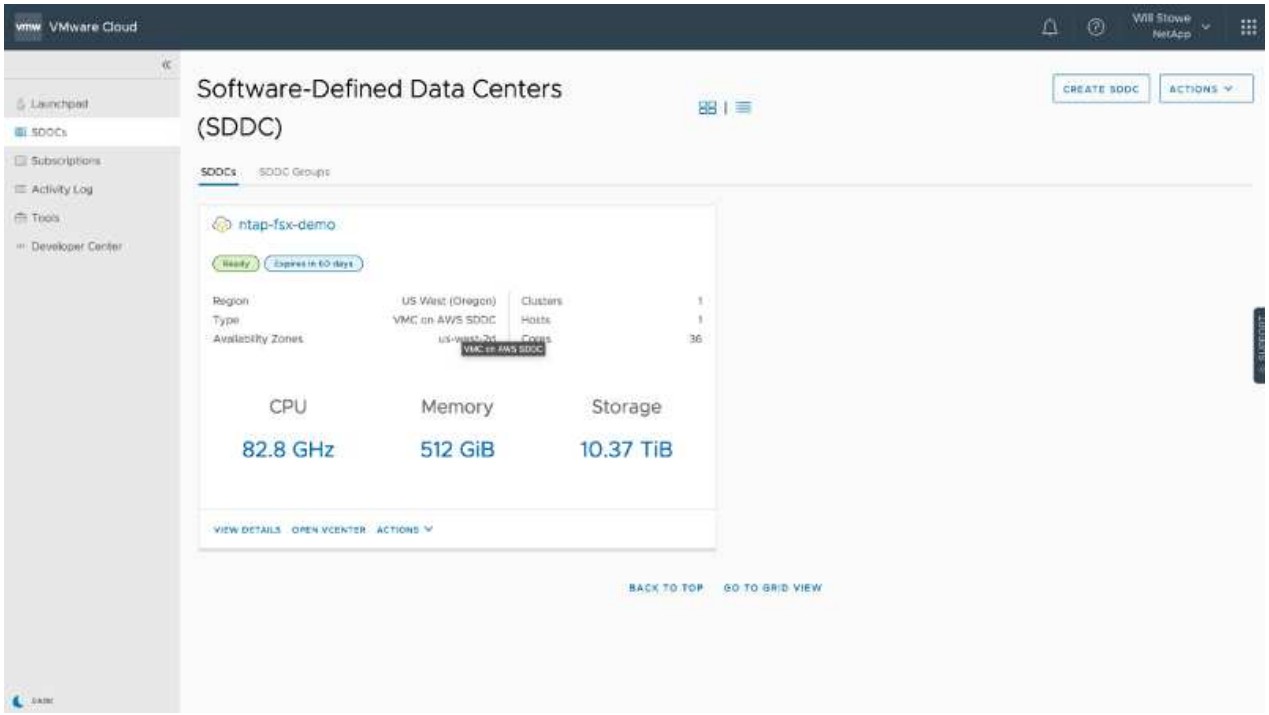
6. Überprüfen und bestätigen Sie die SDDC-Konfiguration und klicken Sie dann auf „SDDC bereitstellen“.



Der Bereitstellungsprozess dauert in der Regel etwa zwei Stunden.



7. Nach Abschluss ist das SDDC einsatzbereit.

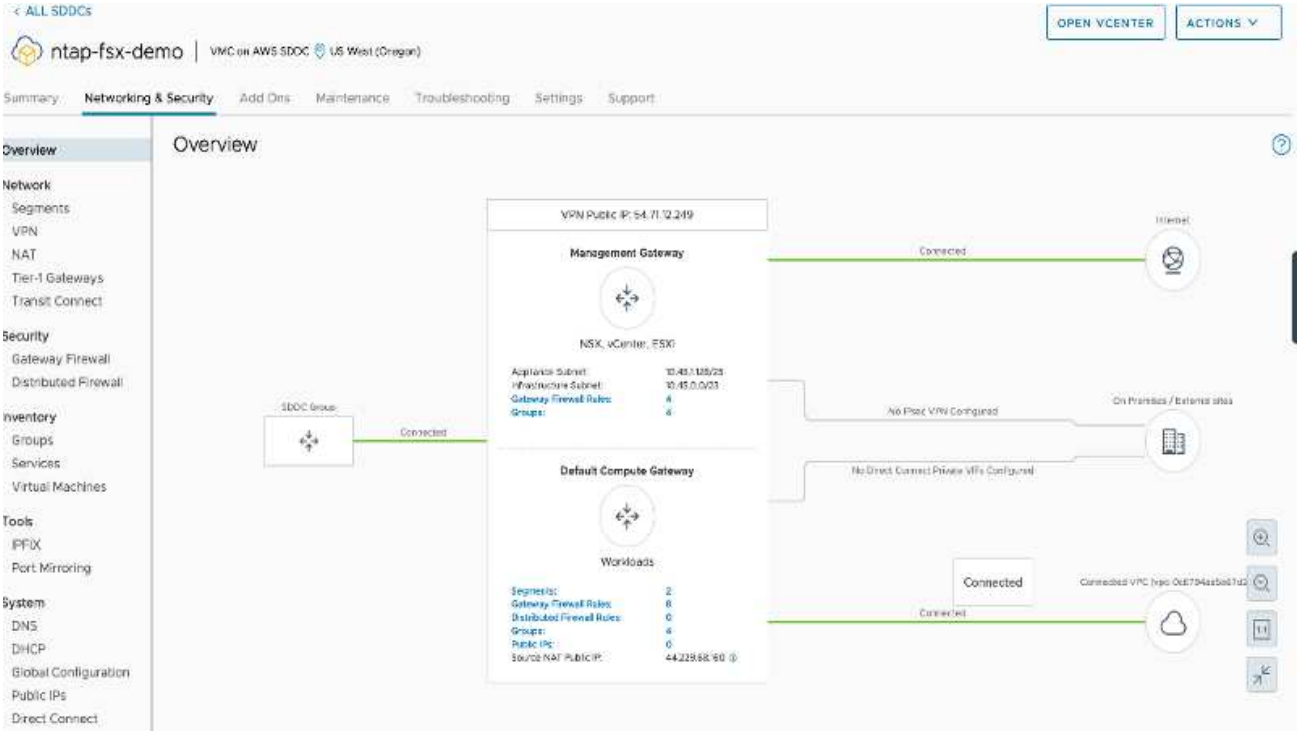


Eine Schritt-für-Schritt-Anleitung zur SDDC-Bereitstellung finden Sie unter"Bereitstellen eines SDDC über die VMC-Konsole" .

▼ **Verbinden Sie VMware Cloud mit FSx ONTAP**

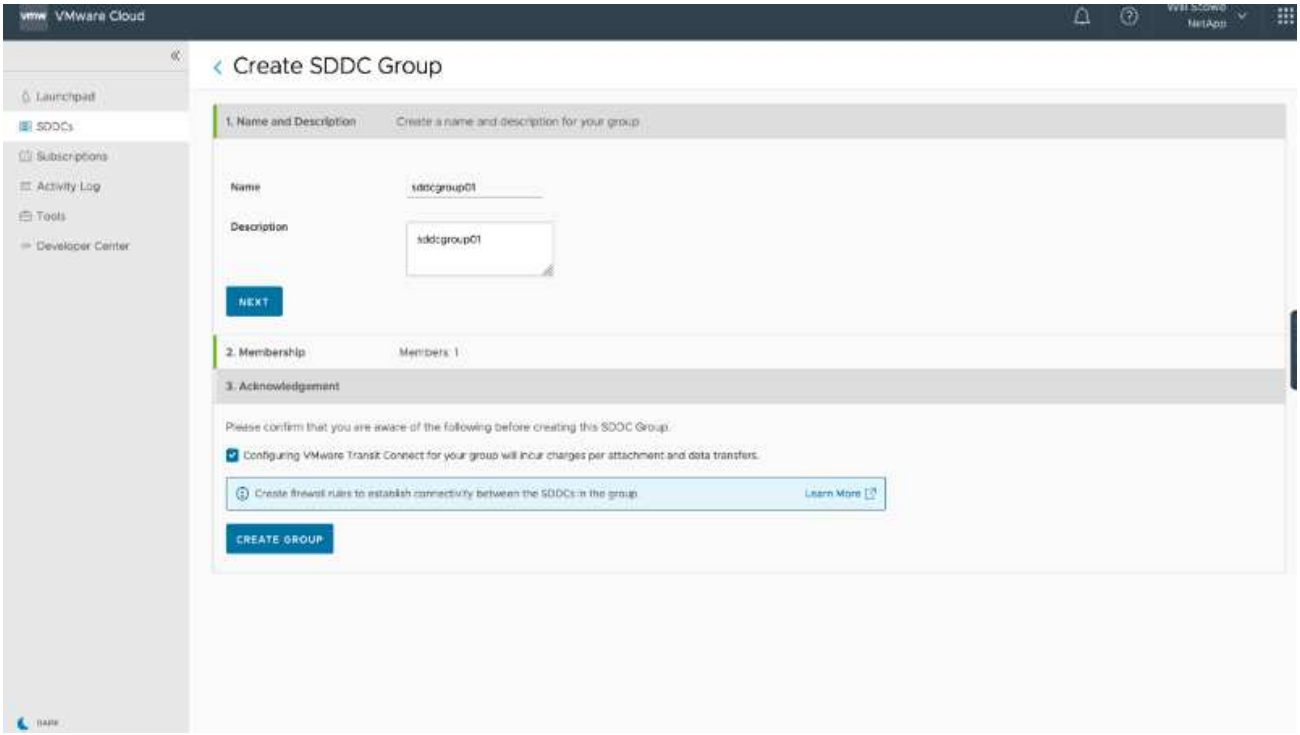
Führen Sie die folgenden Schritte aus, um VMware Cloud mit FSx ONTAP zu verbinden:

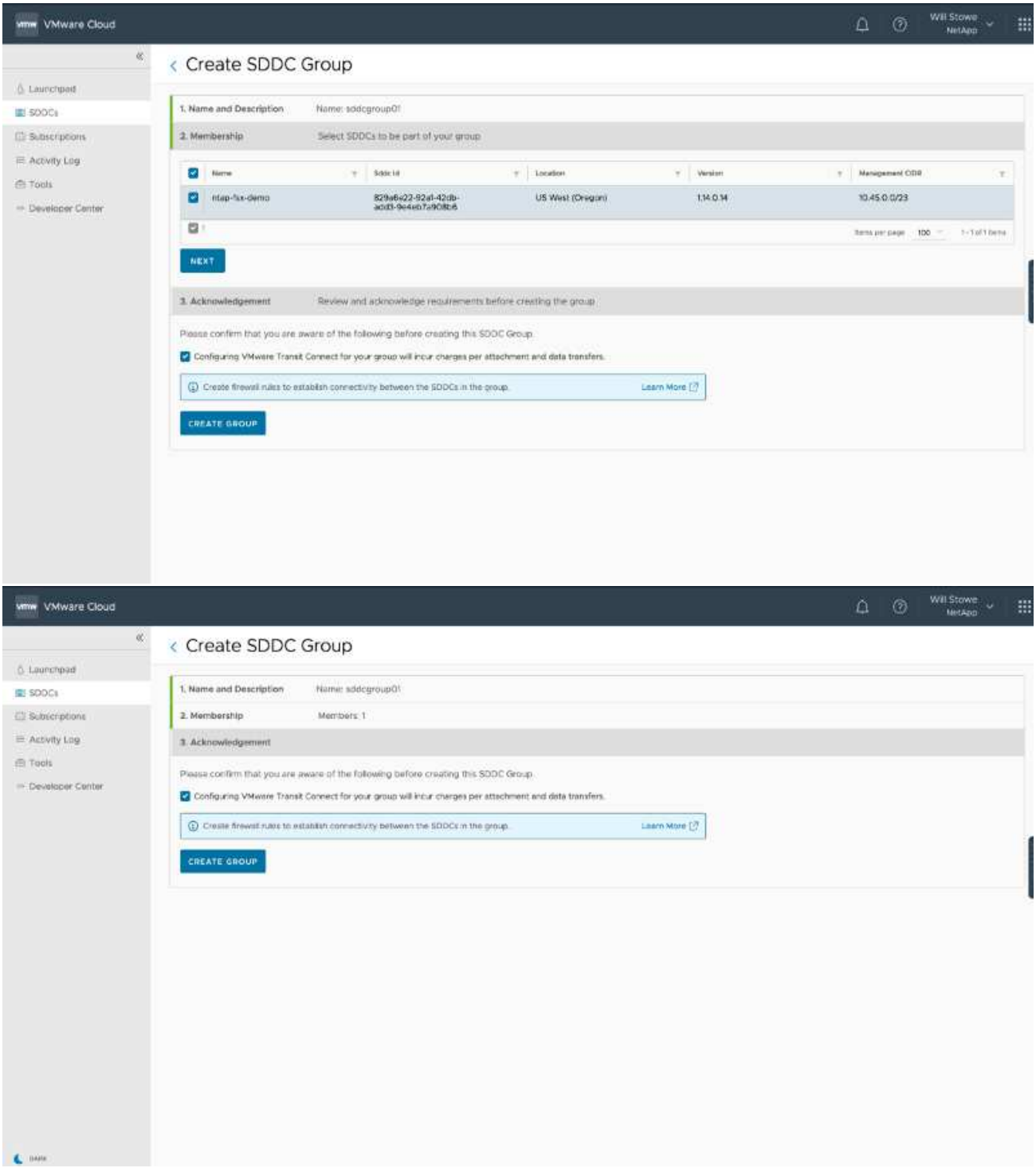
1. Wenn die VMware Cloud-Bereitstellung abgeschlossen und mit AWS VPC verbunden ist, müssen Sie Amazon FSx ONTAP in einer neuen VPC und nicht in der ursprünglich verbundenen VPC bereitstellen (siehe Screenshot unten). Auf FSx (NFS- und SMB-Floating-IPs) kann nicht zugegriffen werden, wenn es im verbundenen VPC bereitgestellt wird. Bedenken Sie, dass ISCSI-Endpunkte wie Cloud Volumes ONTAP vom verbundenen VPC aus einwandfrei funktionieren.



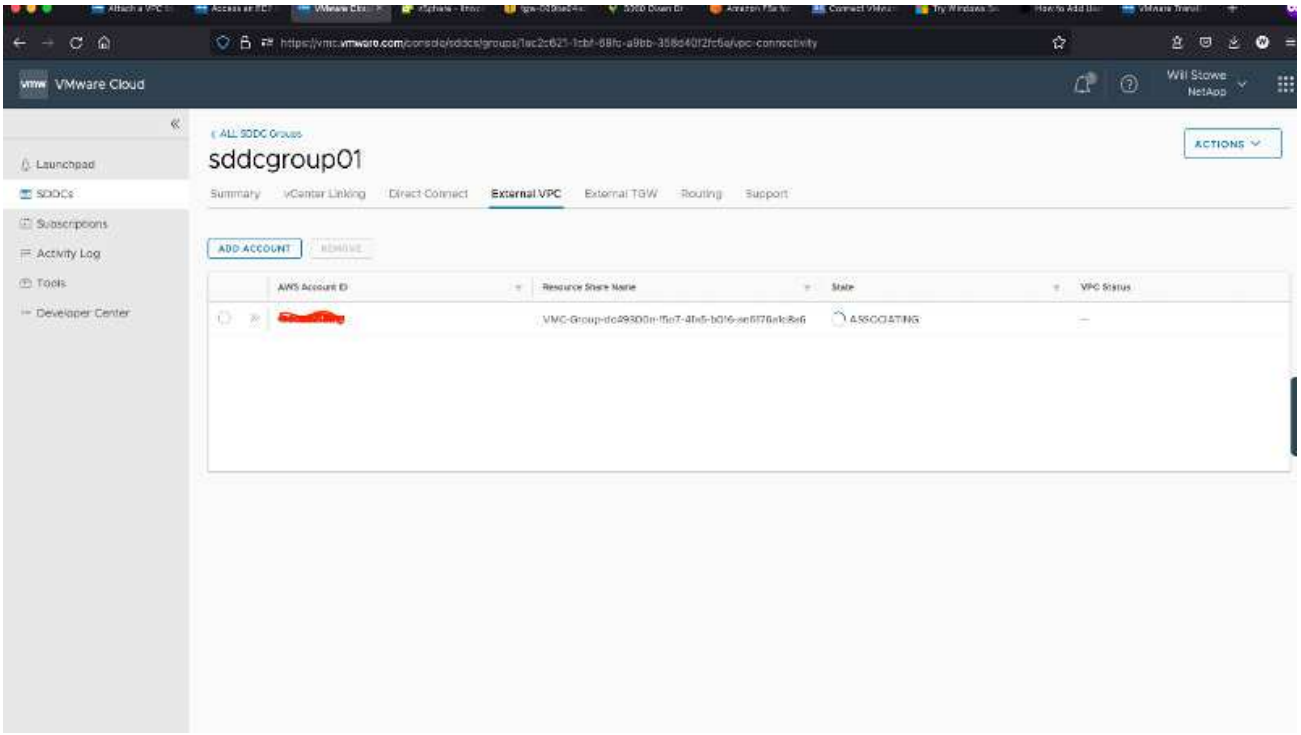
2. Stellen Sie eine zusätzliche VPC in derselben Region bereit und stellen Sie dann Amazon FSx ONTAP in der neuen VPC bereit.

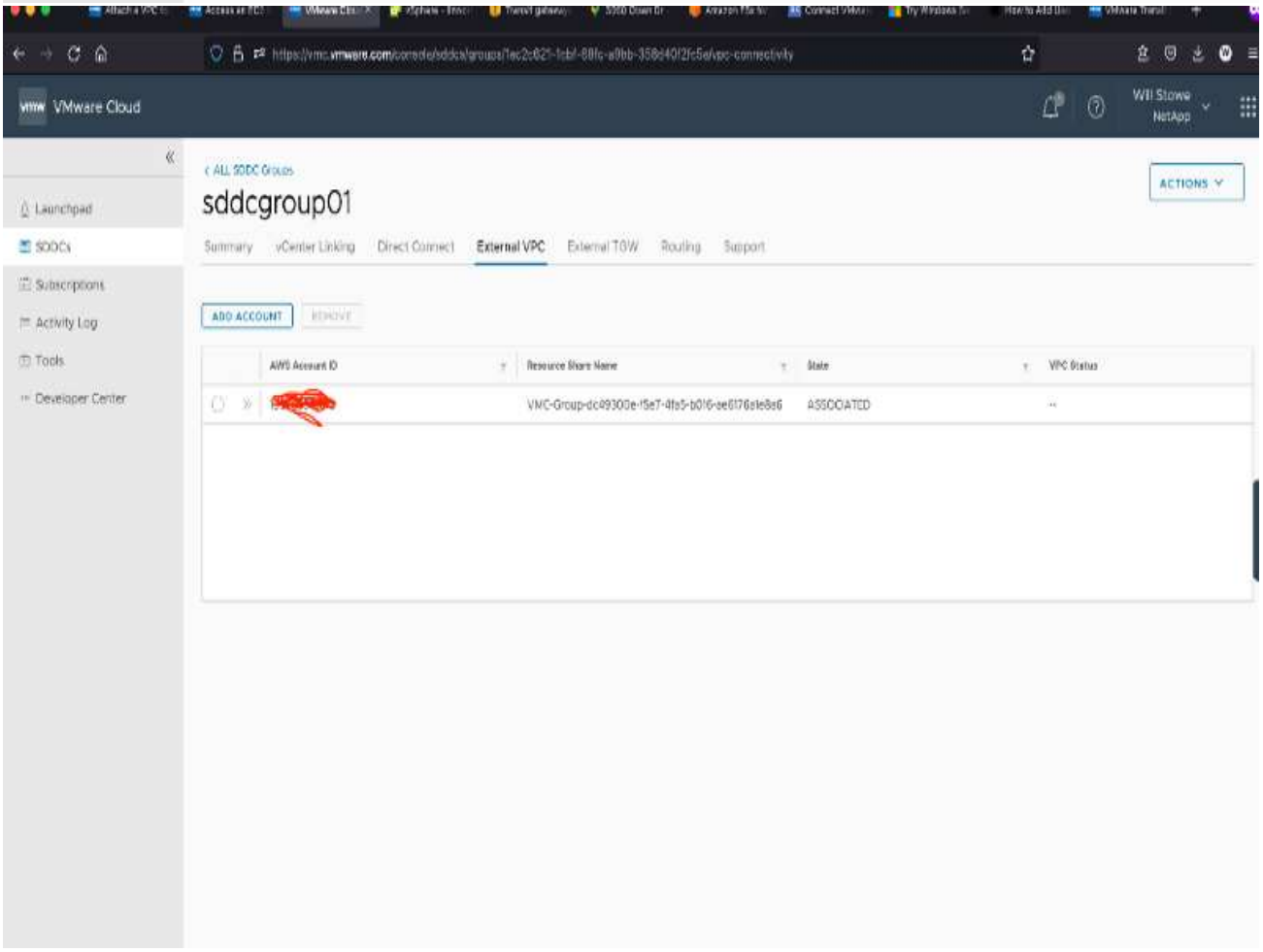
   Durch die Konfiguration einer SDDC-Gruppe in der VMware Cloud-Konsole werden die Netzwerkkonfigurationsoptionen aktiviert, die für die Verbindung mit der neuen VPC erforderlich sind, in der FSx bereitgestellt wird. Überprüfen Sie in Schritt 3, ob „Beim Konfigurieren von VMware Transit Connect für Ihre Gruppe fallen Gebühren pro Anhang und Datenübertragung an“ aktiviert ist, und wählen Sie dann „Gruppe erstellen“ aus. Der Vorgang kann einige Minuten dauern.



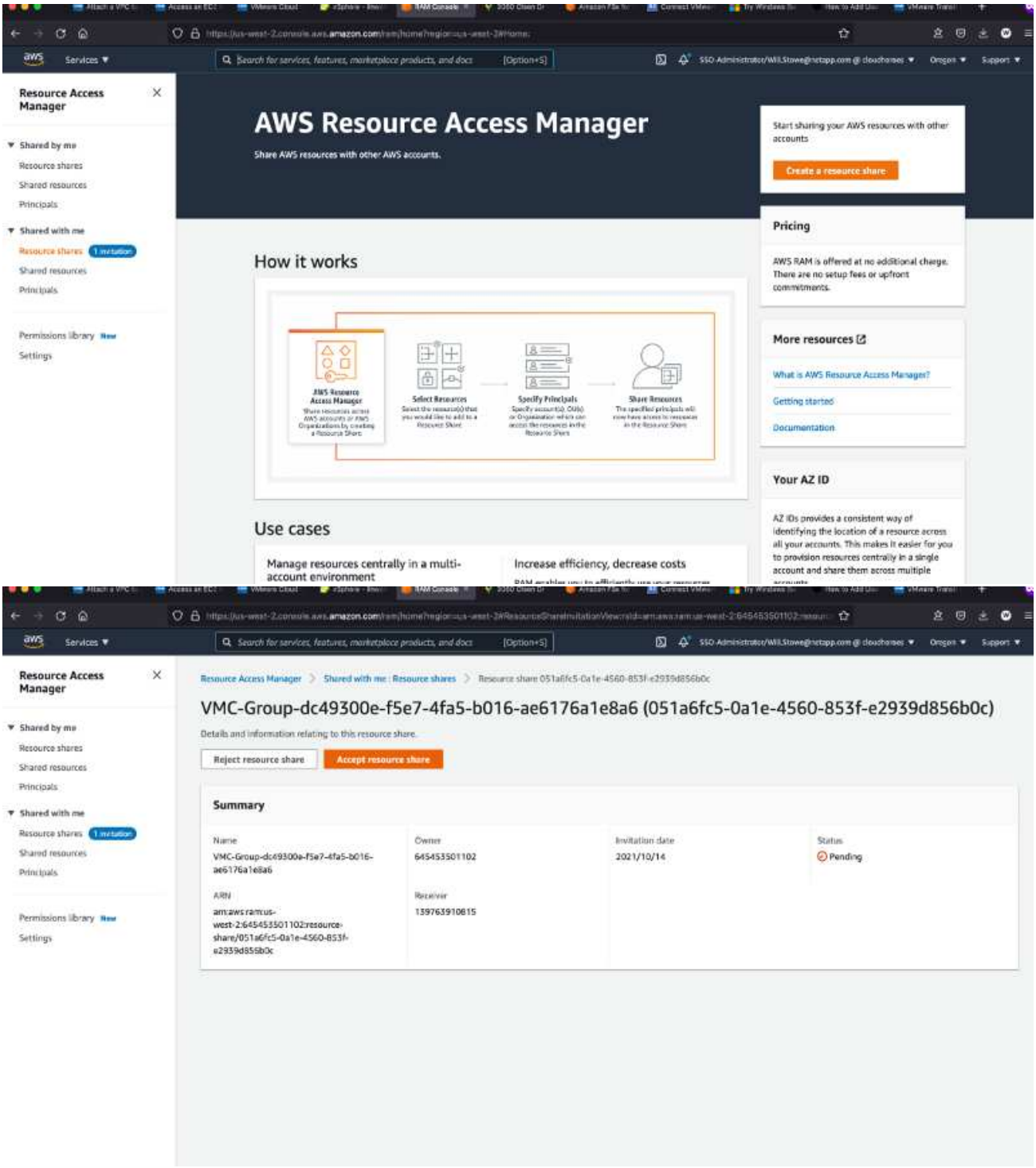


3. Fügen Sie die neu erstellte VPC der gerade erstellten SDDC-Gruppe hinzu. Wählen Sie die Registerkarte „Externe VPC“ und folgen Sie den"Anweisungen zum Anschließen einer externen VPC" zur Gruppe. Dieser Vorgang kann 10 bis 15 Minuten dauern.

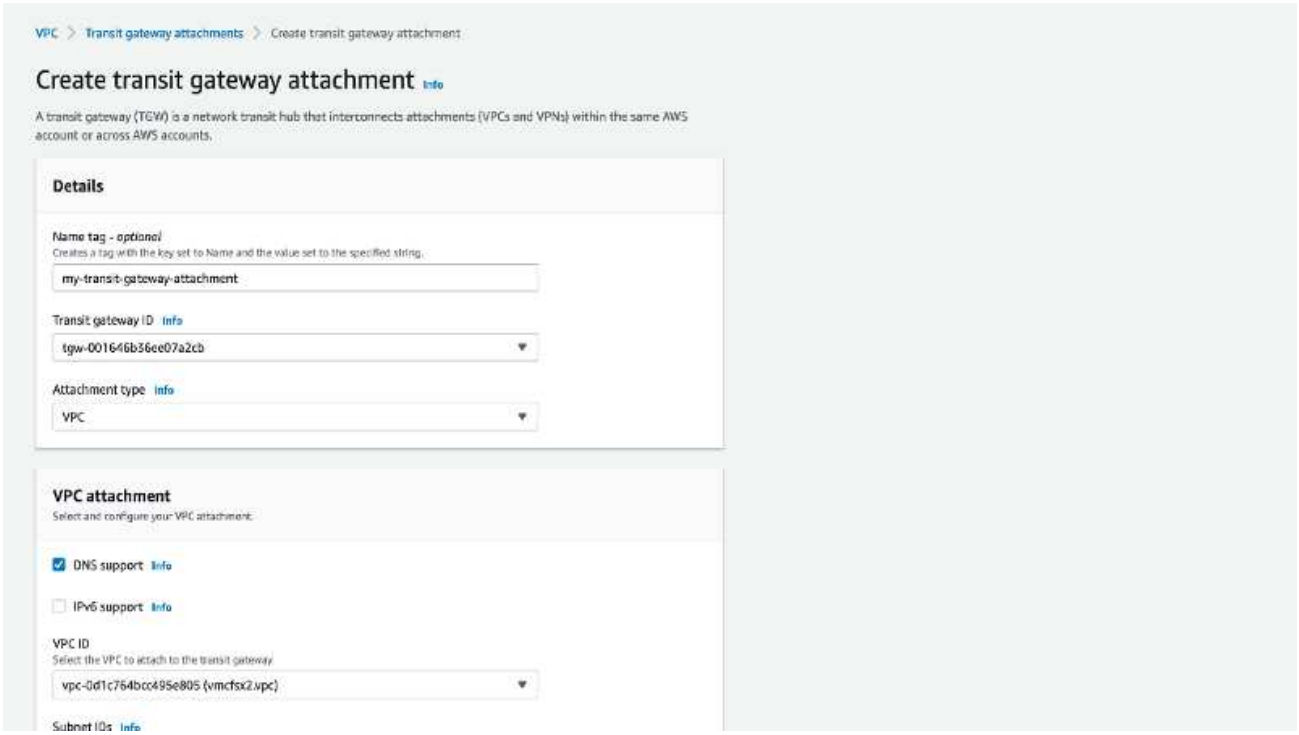




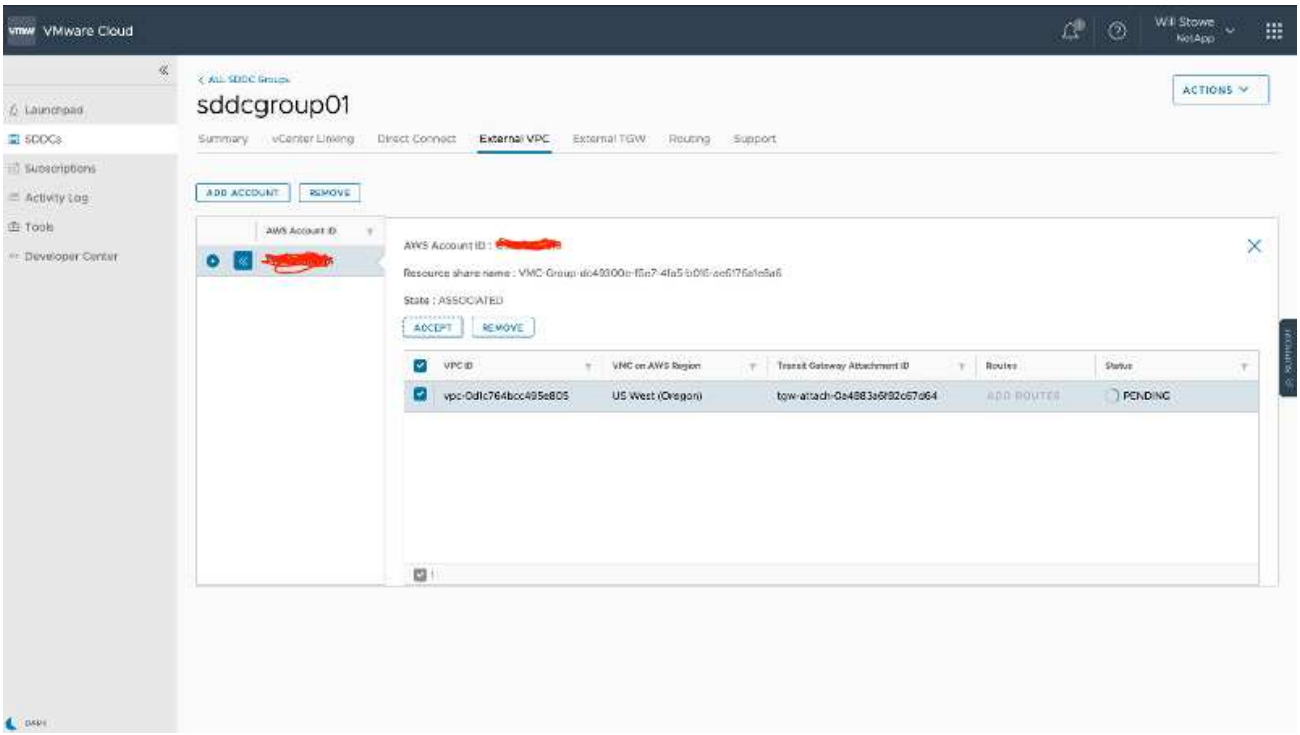
4. Im Rahmen des externen VPC-Prozesses werden Sie über die AWS-Konsole zu einer neuen freigegebenen Ressource über den Resource Access Manager aufgefordert. Die gemeinsam genutzte Ressource ist die"AWS Transit Gateway" verwaltet von VMware Transit Connect.



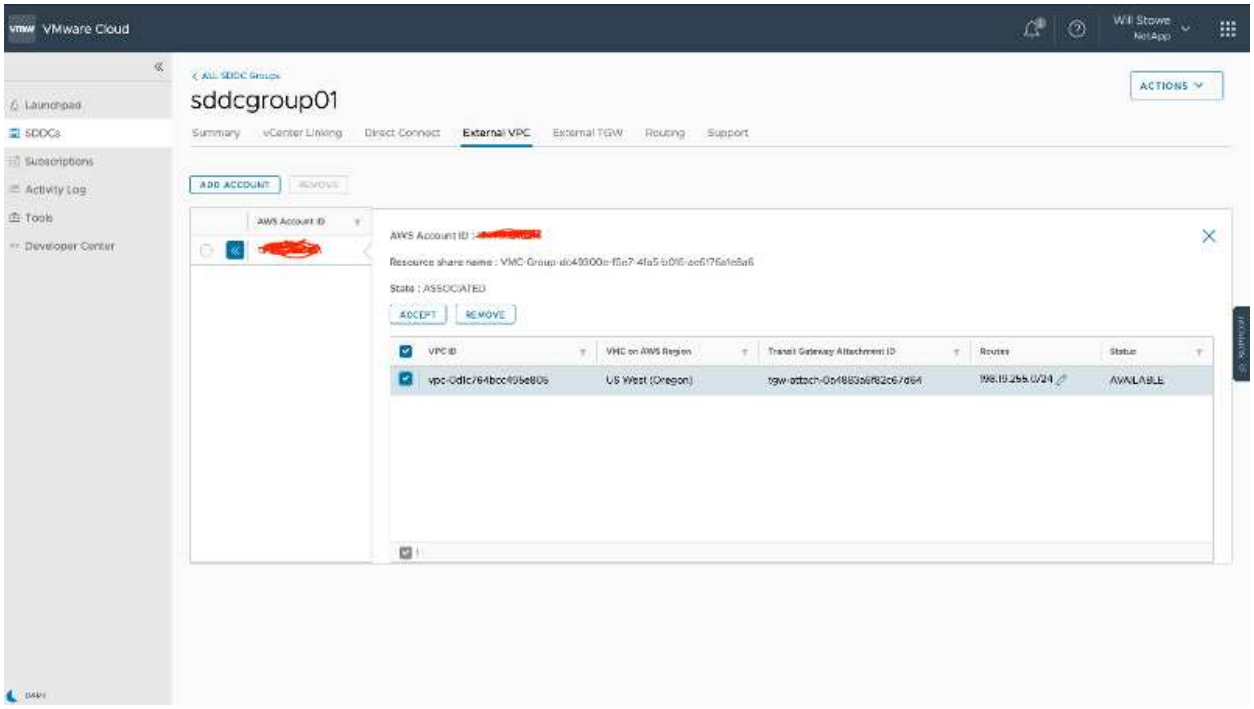
5. Erstellen Sie den Transit Gateway-Anhang.



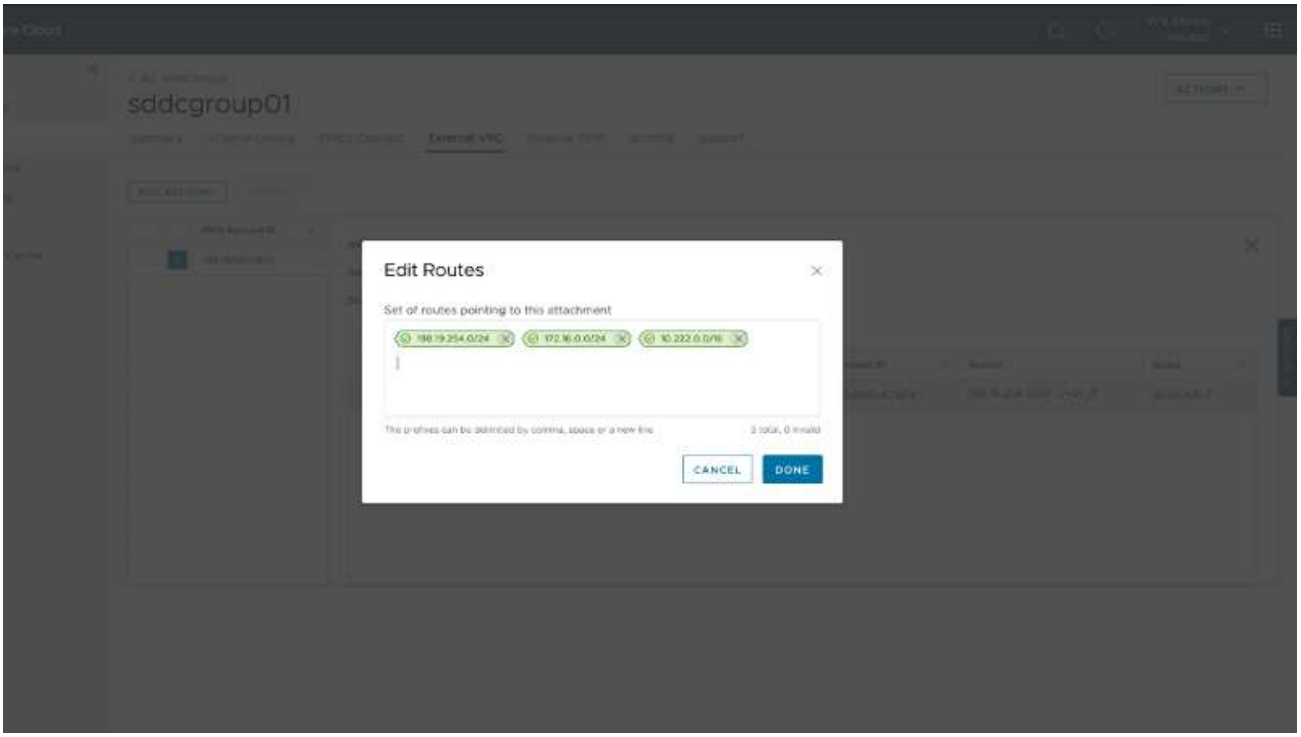
6. Zurück in der VMC-Konsole: Akzeptieren Sie den VPC-Anhang. Dieser Vorgang kann ungefähr 10 Minuten dauern.



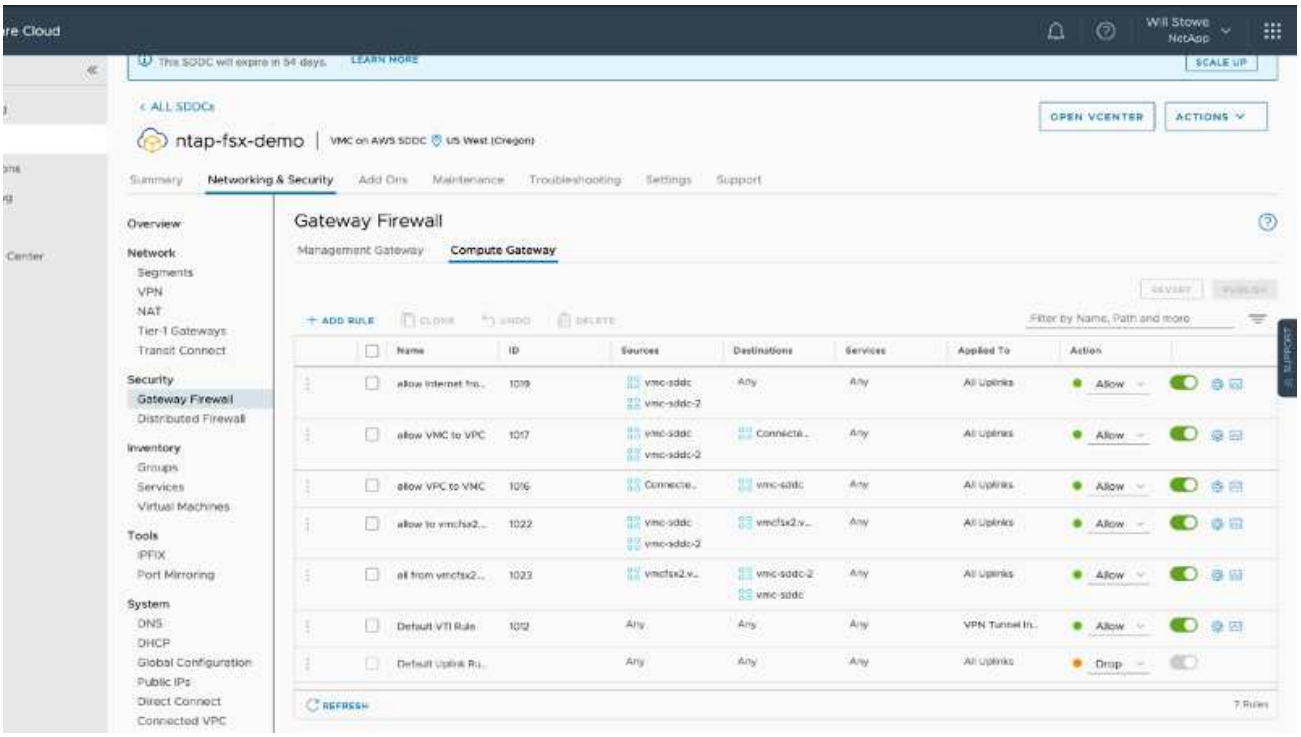
7. Klicken Sie auf der Registerkarte „Externe VPC“ auf das Bearbeitungssymbol in der Spalte „Routen“ und fügen Sie die folgenden erforderlichen Routen hinzu:
   - Eine Route für den Floating-IP-Bereich für Amazon FSx ONTAP"Floating IPs" .
   - Eine Route für den Floating-IP-Bereich für Cloud Volumes ONTAP (falls zutreffend).
   - Eine Route für den neu erstellten externen VPC-Adressraum.



8. Erlauben Sie schließlich bidirektionalen Verkehr"Firewall-Regeln" für den Zugriff auf FSx/CVO. Folgen Sie diesen"detaillierte Schritte" für Compute-Gateway-Firewallregeln für die SDDC-Workload-Konnektivität.



9. Nachdem die Firewall-Gruppen sowohl für das Management- als auch das Compute-Gateway konfiguriert wurden, kann auf das vCenter wie folgt zugegriffen werden:



Im nächsten Schritt überprüfen Sie, ob Amazon FSx ONTAP oder Cloud Volumes ONTAP Ihren Anforderungen entsprechend konfiguriert ist und ob die Volumes so bereitgestellt werden, dass Speicherkomponenten von vSAN ausgelagert werden, um die Bereitstellung zu optimieren.

Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf Azure

Wie bei lokalen Lösungen ist die Planung der Azure VMware-Lösung entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen und Migrieren von VMs.

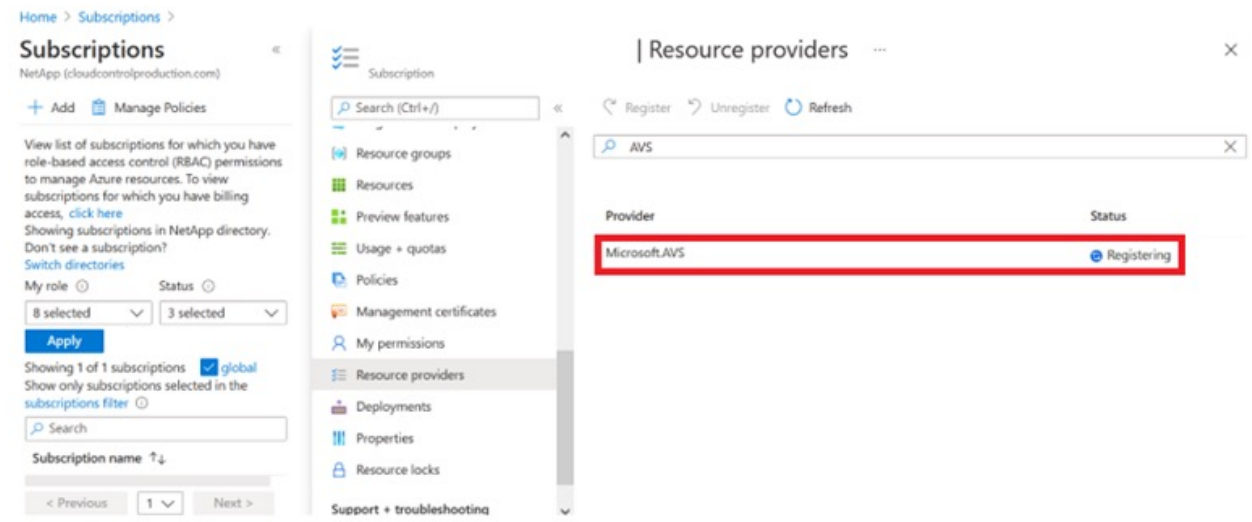
In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Solution einrichten und verwalten und in Kombination mit den verfügbaren Optionen zum Anbinden von NetApp -Speicher verwenden.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

▼ **Registrieren des Ressourcenanbieters und Erstellen einer privaten Cloud**

Um Azure VMware Solution zu verwenden, registrieren Sie zunächst den Ressourcenanbieter innerhalb des angegebenen Abonnements:

1. Sign in .
2. Wählen Sie im Menü des Azure-Portals „Alle Dienste“ aus.
3. Geben Sie im Dialogfeld „Alle Dienste“ das Abonnement ein und wählen Sie dann „Abonnements“ aus.
4. Wählen Sie zum Anzeigen das Abonnement aus der Abonnementliste aus.
5. Wählen Sie „Ressourcenanbieter“ und geben Sie „Microsoft.AVS“ in die Suche ein.
6. Wenn der Ressourcenanbieter nicht registriert ist, wählen Sie Registrieren aus.



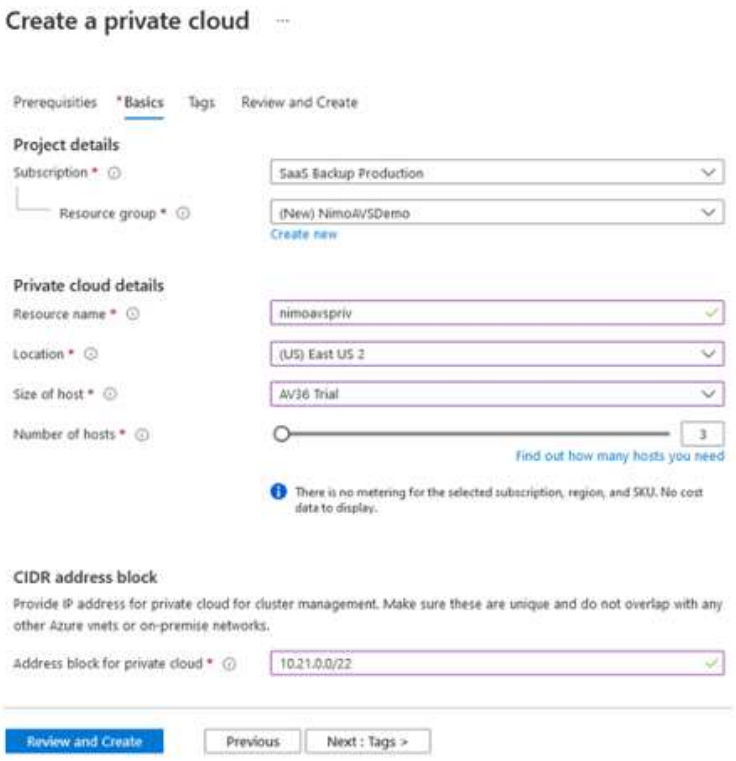


7. Nachdem der Ressourcenanbieter registriert wurde, erstellen Sie mithilfe des Azure-Portals eine private Azure VMware Solution-Cloud.
8. Sign in .
9. Wählen Sie „Neue Ressource erstellen“ aus.
10. Geben Sie im Textfeld „Marketplace durchsuchen“ „Azure VMware Solution“ ein und wählen Sie es aus den Ergebnissen aus.
11. Wählen Sie auf der Seite „Azure VMware Solution“ die Option „Erstellen“ aus.

12. Geben Sie auf der Registerkarte „Grundlagen“ die Werte in die Felder ein und wählen Sie „Überprüfen + Erstellen“ aus.

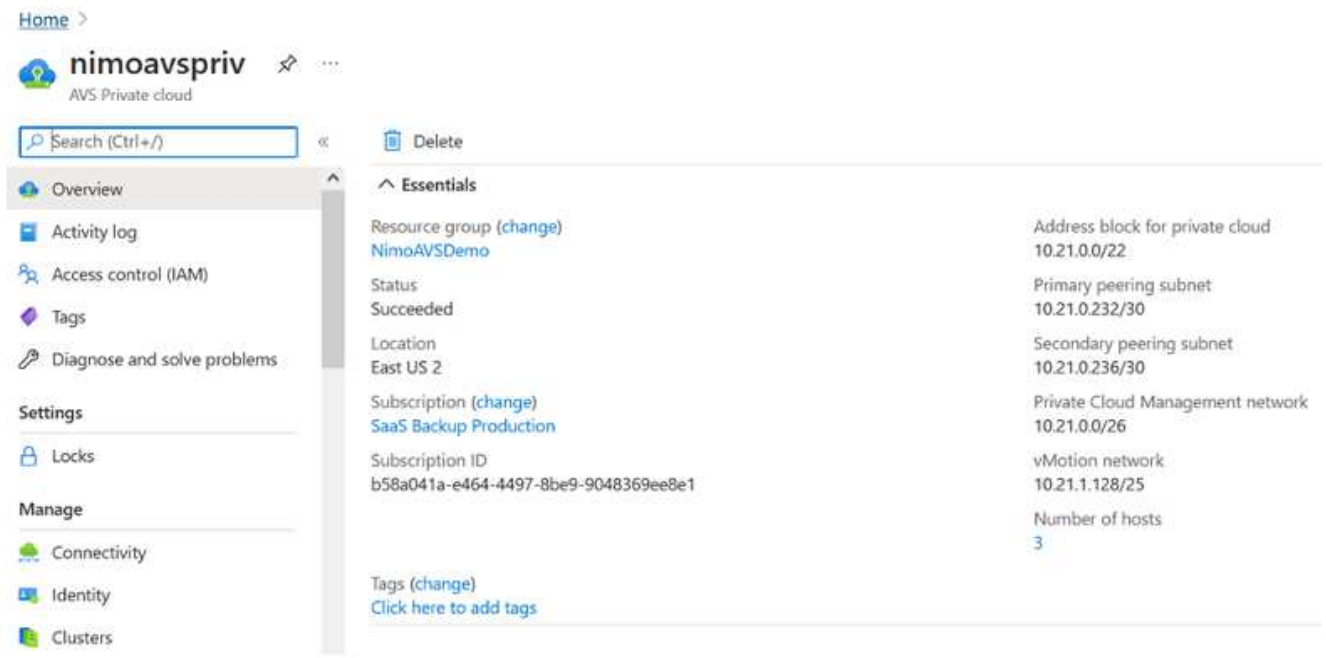
Hinweise:

- Für einen schnellen Start sammeln Sie die erforderlichen Informationen bereits in der Planungsphase.
- 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 bereitgestellt und verwaltet werden.
- Stellen Sie sicher, dass die CIDR-Adresse eindeutig ist und sich nicht mit anderen Azure Virtual Networks oder lokalen Netzwerken überschneidet. Das CIDR stellt das private Cloud-Verwaltungsnetzwerk dar und wird für die Clusterverwaltungsdienste wie vCenter Server und NSX-T Manager verwendet. NetApp empfiehlt die Verwendung eines /22-Adressraums. In diesem Beispiel wird 10.21.0.0/22 verwendet.



Der Bereitstellungsprozess dauert ungefähr 4–5 Stunden. Überprüfen Sie nach Abschluss des Vorgangs, ob die Bereitstellung erfolgreich war, indem Sie über das Azure-Portal auf die private Cloud zugreifen. Wenn die Bereitstellung abgeschlossen ist, wird der Status „Erfolgreich“ angezeigt.

Für eine private Azure VMware Solution-Cloud ist ein Azure Virtual Network erforderlich. Da Azure VMware Solution kein lokales vCenter unterstützt, sind für die Integration in eine vorhandene lokale Umgebung zusätzliche Schritte erforderlich. Außerdem ist die Einrichtung einer ExpressRoute-Verbindung und eines virtuellen Netzwerkgateways erforderlich. Während Sie auf den Abschluss der Clusterbereitstellung warten, erstellen Sie ein neues virtuelles Netzwerk oder verwenden Sie ein vorhandenes, um eine Verbindung mit Azure VMware Solution herzustellen.



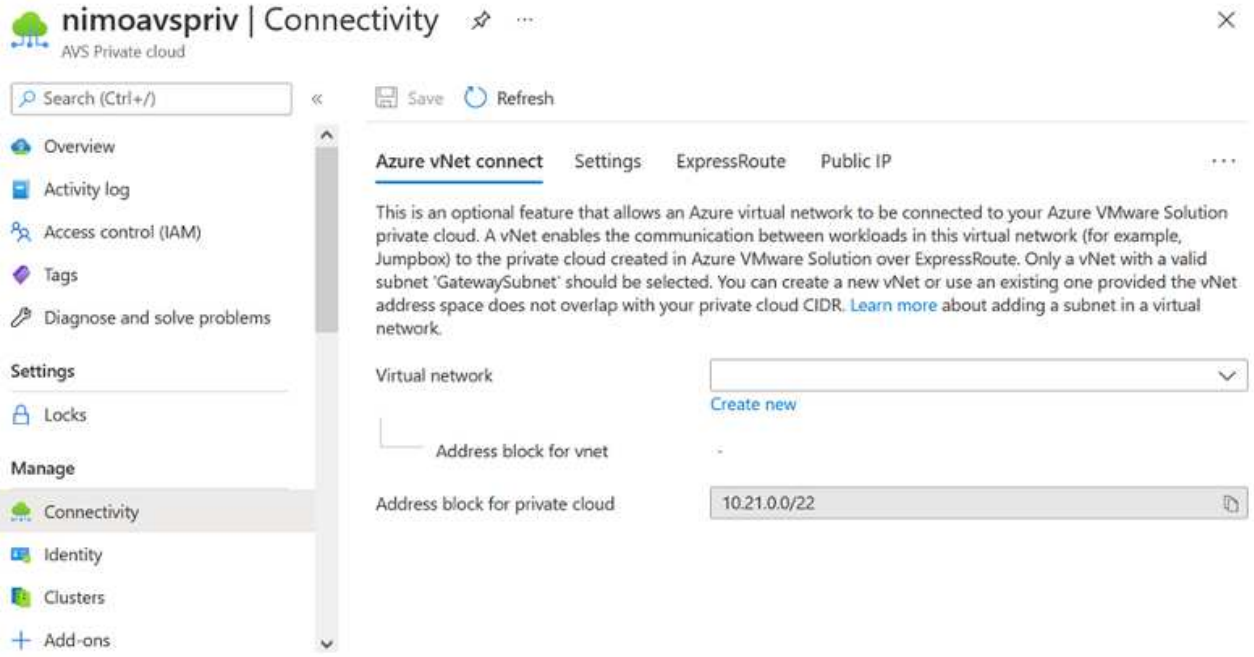
▼ Herstellen einer Verbindung mit einem neuen oder vorhandenen virtuellen ExpressRoute-Netzwerkgateway

Um ein neues Azure Virtual Network (VNet) zu erstellen, wählen Sie die Registerkarte Azure VNet Connect aus. Alternativ können Sie mithilfe des Assistenten „Virtuelles Netzwerk erstellen“ manuell eins über das Azure-Portal erstellen:

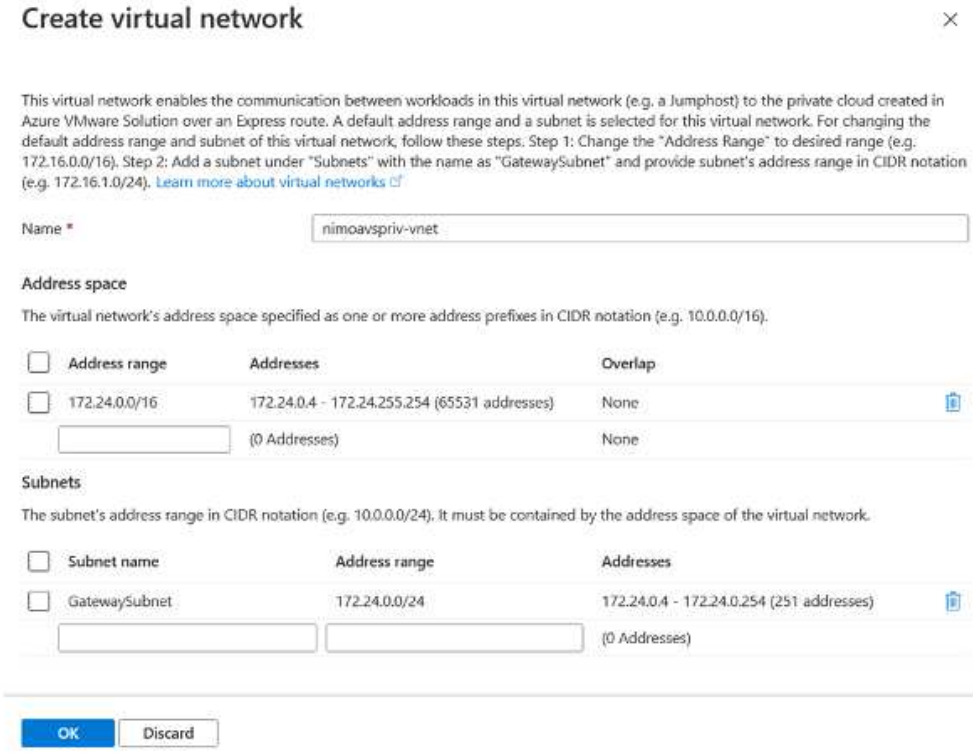
1. Gehen Sie zur privaten Cloud der Azure VMware Solution und greifen Sie unter der Option „Verwalten“ auf „Konnektivität“ zu.
2. Wählen Sie Azure VNet Connect aus.
3. Um ein neues VNet zu erstellen, wählen Sie die Option „Neu erstellen“ aus.

   Mit dieser Funktion kann ein VNet mit der privaten Cloud der Azure VMware Solution verbunden werden. Das VNet ermöglicht die Kommunikation zwischen Workloads in diesem virtuellen Netzwerk, indem es automatisch erforderliche Komponenten (z. B. Jumpbox, gemeinsam genutzte Dienste wie Azure NetApp Files und Cloud Volume ONTAP) für die in Azure VMware Solution erstellte private Cloud über ExpressRoute erstellt.

   Hinweis: Der VNet-Adressraum sollte sich nicht mit dem CIDR der privaten Cloud überschneiden.



4. Geben Sie die Informationen für das neue VNet ein oder aktualisieren Sie sie, und wählen Sie „OK“ aus.



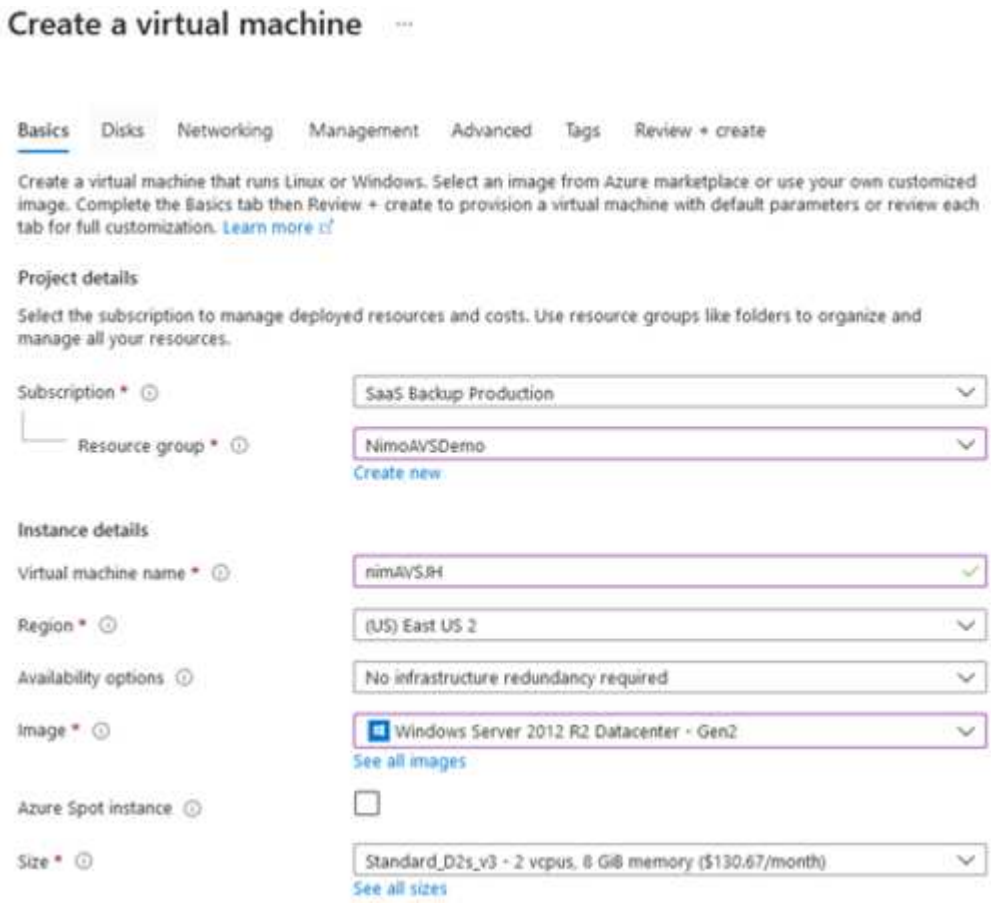
Das VNet mit dem angegebenen Adressbereich und Gateway-Subnetz wird im angegebenen Abonnement und in der angegebenen Ressourcengruppe erstellt.

Wenn Sie ein VNet manuell erstellen, erstellen Sie ein virtuelles Netzwerkgateway mit der entsprechenden SKU und ExpressRoute als Gatewaytyp. Stellen Sie nach Abschluss der Bereitstellung mithilfe des Autorisierungsschlüssels eine Verbindung zwischen der ExpressRoute-Verbindung und dem virtuellen Netzwerkgateway her, das die private Cloud

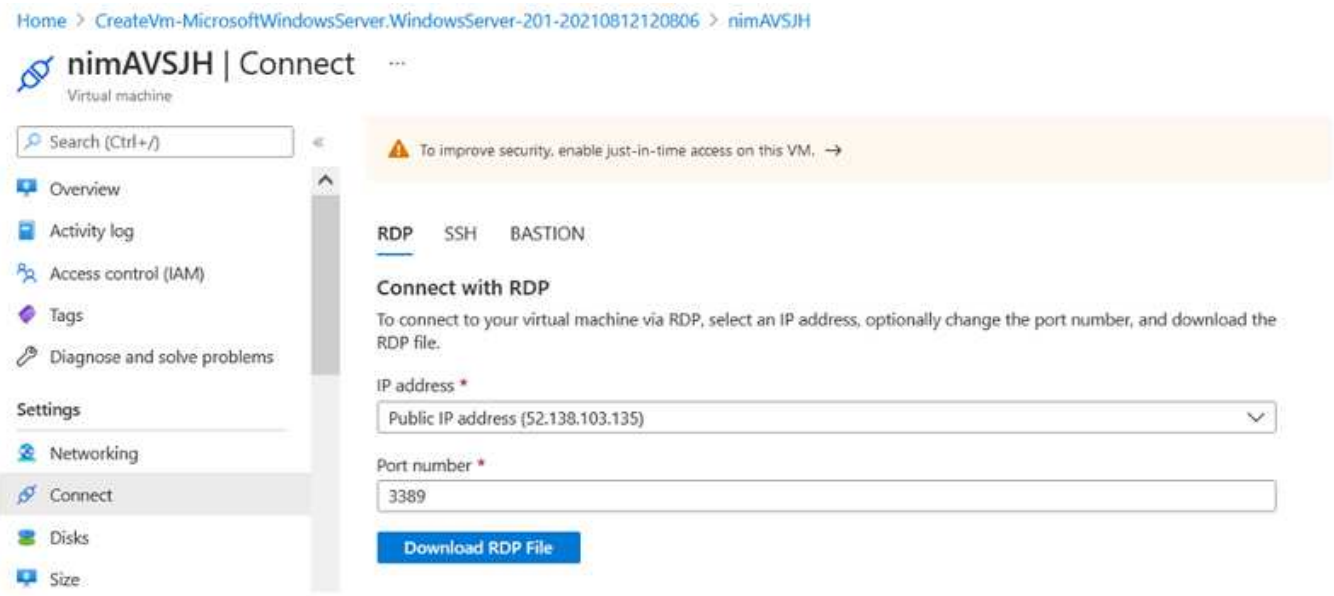
der Azure VMware Solution enthält. Weitere Informationen finden Sie unter "Konfigurieren des Netzwerks für Ihre private VMware-Cloud in Azure" .

▼ **Überprüfen der Netzwerkverbindung und des Zugriffs auf die private Azure VMware Solution-Cloud**

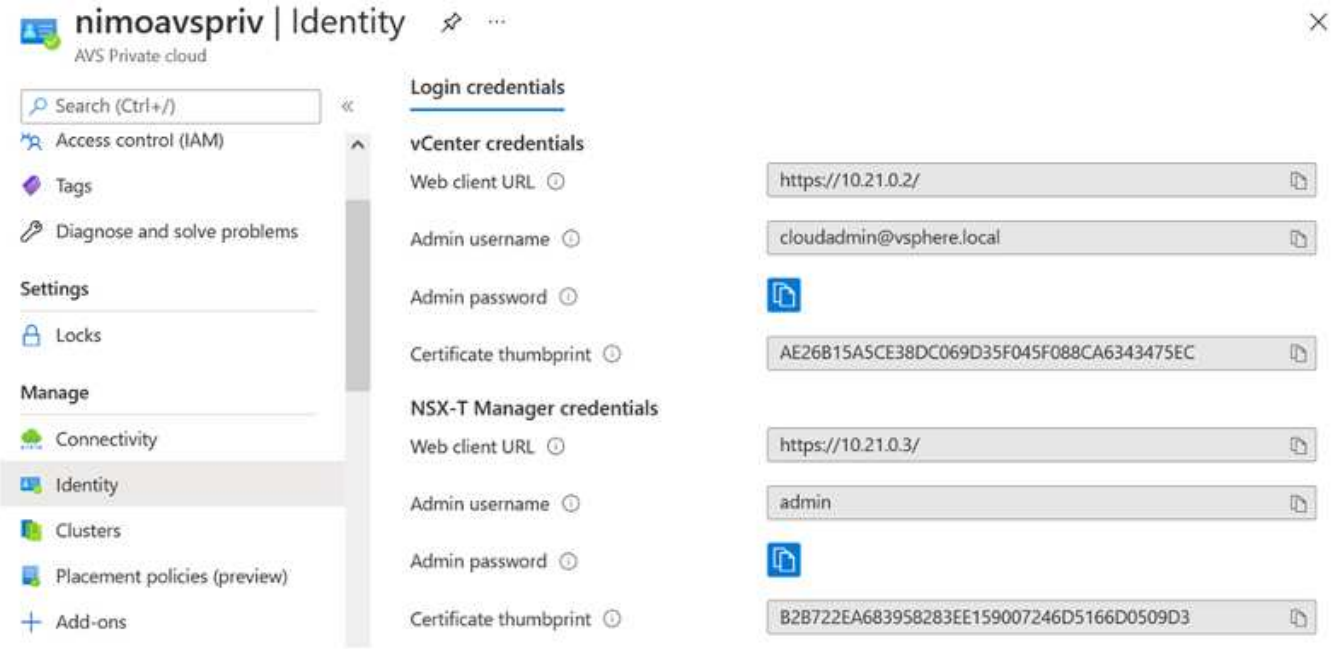
Mit Azure VMware Solution können Sie keine private Cloud mit lokalem VMware vCenter verwalten. Stattdessen ist ein Jump-Host erforderlich, um eine Verbindung mit der Azure VMware Solution vCenter-Instanz herzustellen. Erstellen Sie einen Jump-Host in der angegebenen Ressourcengruppe und melden Sie sich beim Azure VMware Solution vCenter an. Dieser Jump-Host sollte eine Windows-VM im selben virtuellen Netzwerk sein, das für die Konnektivität erstellt wurde, und sollte Zugriff sowohl auf vCenter als auch auf den NSX Manager bieten.



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



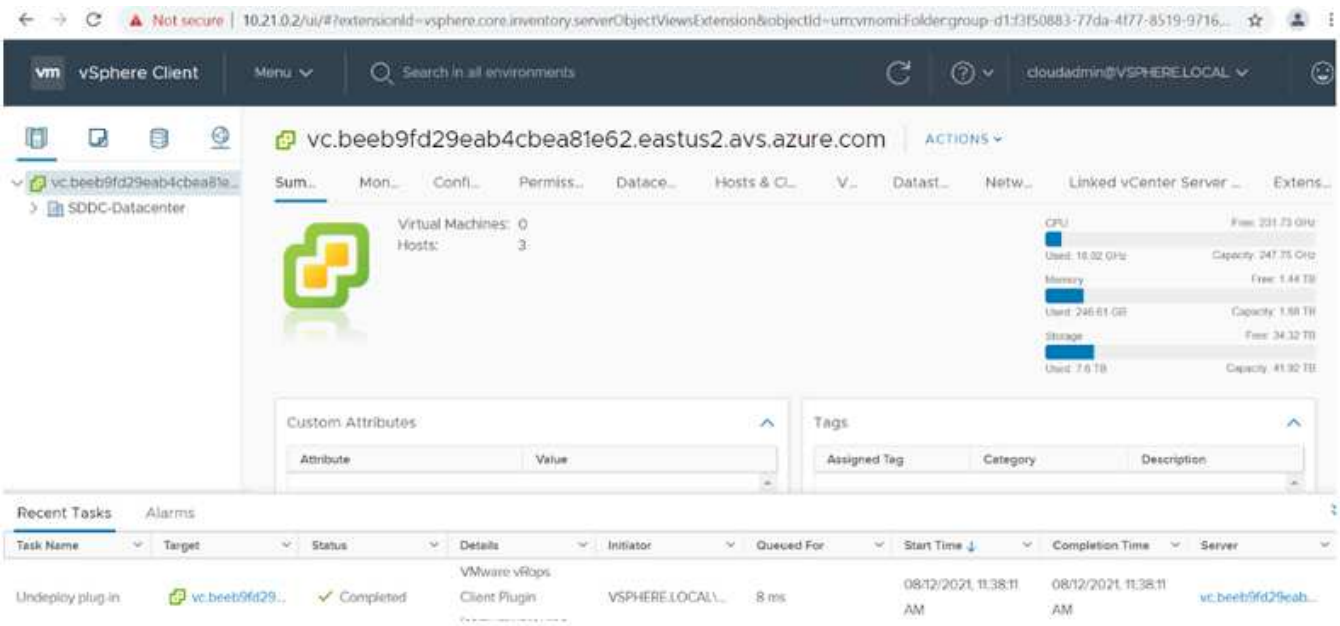
Sign in . Um auf die Anmeldeinformationen zuzugreifen, gehen Sie zum Azure-Portal und navigieren Sie zu „Identität“ (unter der Option „Verwalten“ in der privaten Cloud). Die URLs und Benutzeranmeldeinformationen für das private Cloud-vCenter und den NSX-T-Manager können von hier kopiert werden.



Öffnen Sie in der virtuellen Windows-Maschine einen Browser und navigieren Sie zur URL des vCenter-Webclients.(`"https://10.21.0.2/"`) und verwenden Sie den Administratorbenutzernamen als **cloudadmin@vsphere.local** und fügen Sie das kopierte Kennwort ein. Ebenso kann auf den NSX-T-Manager auch über die Webclient-URL zugegriffen werden(`"https://10.21.0.3/"`) und verwenden Sie den Administratorbenutzernamen und fügen Sie das kopierte Kennwort ein, um neue Segmente zu erstellen oder die vorhandenen Tier-Gateways zu ändern.

Die Webclient-URLs sind für jedes bereitgestellte SDDC unterschiedlich.





Das Azure VMware Solution SDDC ist jetzt bereitgestellt und konfiguriert. Nutzen Sie ExpressRoute Global Reach, um die lokale Umgebung mit der privaten Cloud von Azure VMware Solution zu verbinden. Weitere Informationen finden Sie unter "Peering lokaler Umgebungen mit Azure VMware Solution" .

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

Wie bei lokalen Umgebungen ist die Planung von Google Cloud VMware Engine (GCVE) entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen von VMs und zur Migration.

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Anschließen von NetApp -Speicher verwenden.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

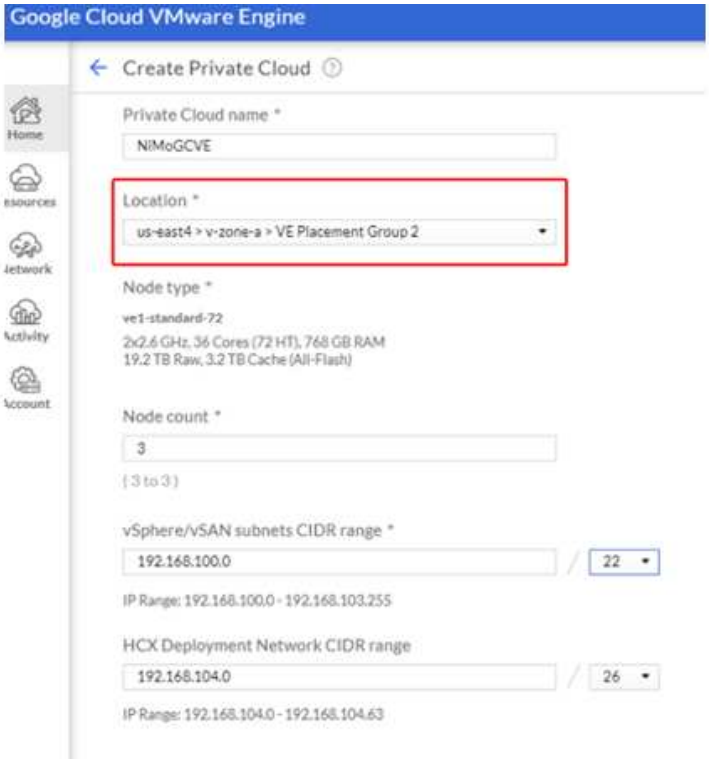
▼ **Bereitstellen und Konfigurieren von GCVE**

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. Stellen Sie unter „Standort“ sicher, dass die private Cloud in derselben Region/Zone bereitgestellt wird, in der NetApp Volumes/CVO bereitgestellt wird, um die beste Leistung und die geringste Latenz sicherzustellen.

Voraussetzungen:

- Einrichten der IAM-Rolle „VMware Engine Service Admin“
- "Aktivieren Sie den VMWare Engine-API-Zugriff und das Knotenkontingent"
- Stellen Sie sicher, dass sich der CIDR-Bereich nicht mit einem Ihrer lokalen oder Cloud-Subnetze überschneidet. Der CIDR-Bereich muss /27 oder höher sein.



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

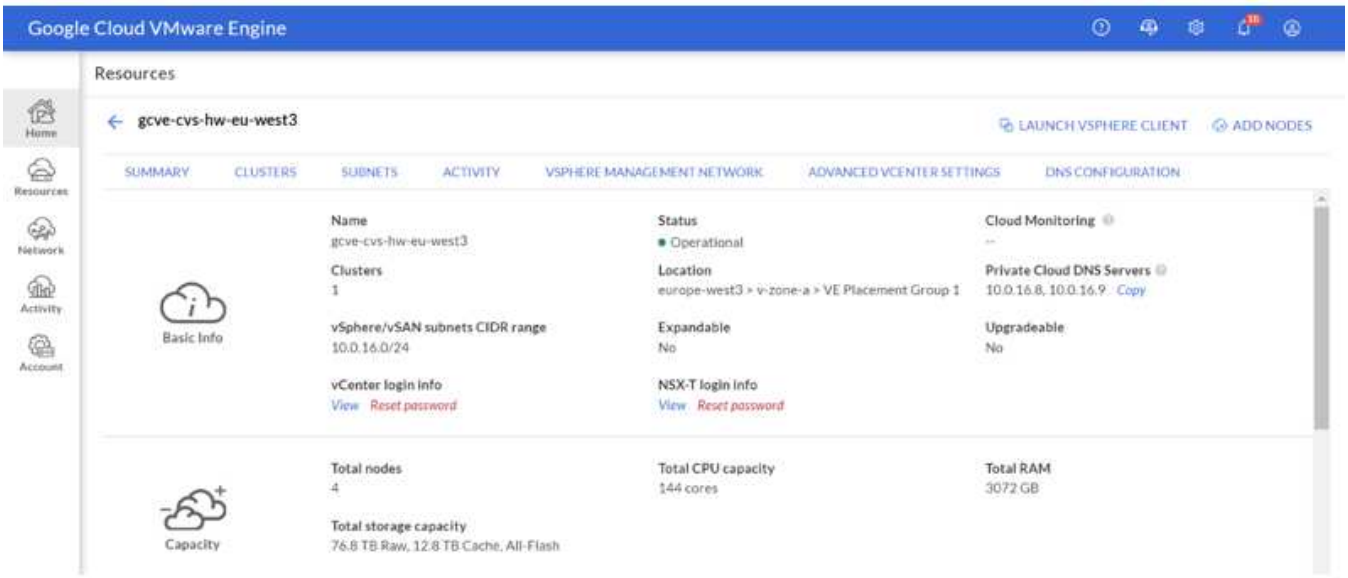
▼ **Privaten Zugriff auf GCVE aktivieren**

Sobald die Private Cloud bereitgestellt ist, konfigurieren Sie den privaten Zugriff auf die Private Cloud für eine Datenpfadverbindung mit hohem Durchsatz und geringer Latenz.

Dadurch wird sichergestellt, dass das VPC-Netzwerk, in dem Cloud Volumes ONTAP Instanzen ausgeführt werden, mit der GCVE Private Cloud kommunizieren kann. Dazu ist der "GCP-Dokumentation" zu befolgen. Für den Cloud Volume Service ist eine Verbindung zwischen VMware Engine und Google Cloud NetApp Volumes herzustellen, indem ein einmaliges Peering zwischen den Tenant-Hostprojekten durchgeführt wird. Detaillierte Schritte sind in diesem "Link" enthalten.

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

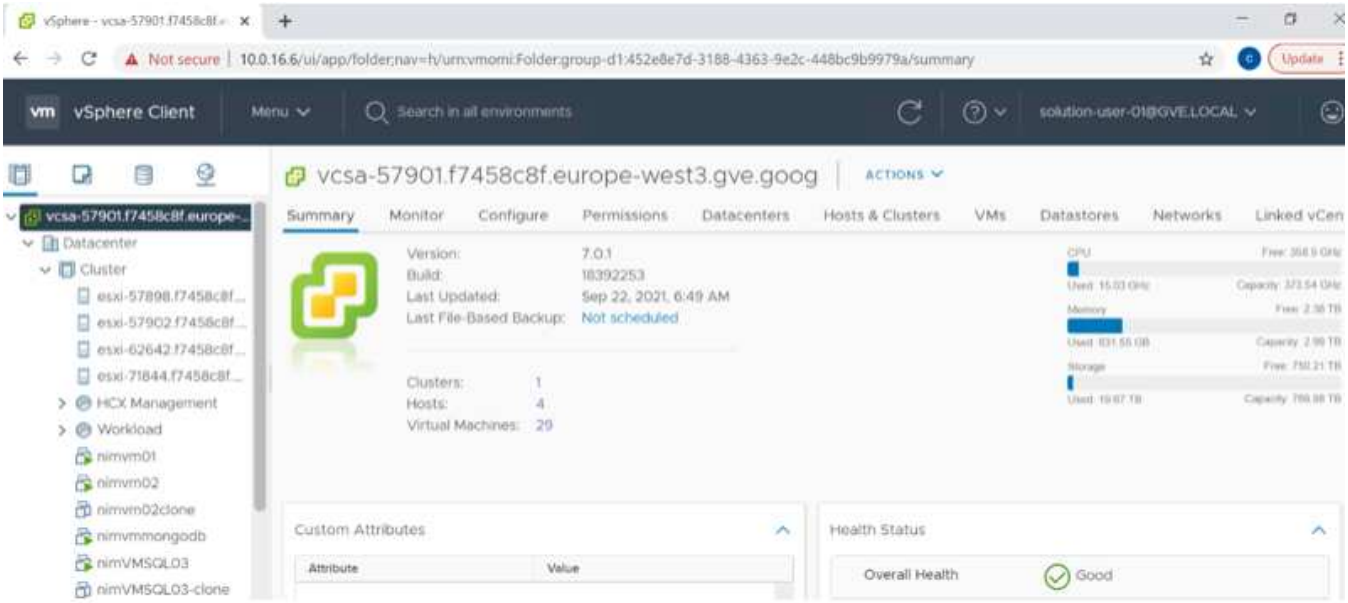
Sign in mit dem Benutzer CloudOwner@gve.local bei vCenter an. Um auf die Anmeldeinformationen zuzugreifen, gehen Sie zum VMware Engine-Portal, gehen Sie zu Ressourcen und wählen Sie die entsprechende private Cloud aus. Klicken Sie im Abschnitt „Grundlegende Informationen“ auf den Link „Anzeigen“, um entweder die vCenter-Anmeldeinformationen (vCenter Server, HCX Manager) oder die NSX-T-Anmeldeinformationen (NSX Manager) anzuzeigen.



Öffnen Sie in einer virtuellen Windows-Maschine einen Browser und navigieren Sie zur URL des vCenter-Webclients.(`"https://10.0.16.6/"`) und verwenden Sie den Administratorbenutzernamen als CloudOwner@gve.local und fügen Sie das kopierte Passwort ein. Ebenso kann auf den NSX-T-Manager auch über die Webclient-URL zugegriffen werden(`"https://10.0.16.11/"`) und verwenden Sie den Administratorbenutzernamen und fügen Sie das kopierte Kennwort ein, um neue Segmente zu erstellen oder die vorhandenen Tier-Gateways zu ändern.

Um eine Verbindung von einem lokalen Netzwerk zur privaten Cloud von VMware Engine herzustellen, nutzen Sie Cloud-VPN oder Cloud Interconnect für die entsprechende Konnektivität und stellen Sie sicher, dass die erforderlichen Ports geöffnet sind. Für detaillierte Schritte folgen Sie diesem"Link" .





▼ **Stellen Sie den zusätzlichen Datenspeicher von Google Cloud NetApp Volumes für GCVE bereit**

Verweisen"Verfahren zum Bereitstellen eines zusätzlichen NFS-Datenspeichers mit NetApp Volumes für GCVE"

NetApp Storage in Public Clouds

NetApp Storage-Optionen für Public Cloud-Anbieter

Entdecken Sie die Optionen für NetApp als Speicher bei den drei großen Hyperscalern.

AWS / VMC

AWS unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- FSx ONTAP als Gastspeicher

- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- FSx ONTAP als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungs-Speicheroptionen für VMC" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für VMC" .

Azure / AVS

Azure unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- Azure NetApp Files (ANF) als mit dem Gast verbundener Speicher
- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- Azure NetApp Files (ANF) als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungs-Speicheroptionen für AVS" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für AVS" .

GCP / GCVE

Google Cloud unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- Google Cloud NetApp Volumes (NetApp Volumes) als mit dem Gast verbundener Speicher
- Google Cloud NetApp Volumes (NetApp Volumes) als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungsspeicheroptionen für GCVE" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für GCVE" .

Lesen Sie mehr über"Google Cloud NetApp Volumes Datenspeicherunterstützung für Google Cloud VMware Engine (NetApp -Blog)" oder"So verwenden Sie Google Cloud NetApp Volumes als Datenspeicher für Google Cloud VMware Engine (Google-Blog)"

Amazon Web Services: Möglichkeiten zur Nutzung von NetApp Storage

NetApp -Speicher kann entweder als Gastspeicher oder als Zusatzspeicher an die Amazon Web Services angeschlossen werden.

Amazon FSx for NetApp ONTAP (FSx ONTAP) als ergänzender NFS-Datenspeicher

Amazon FSx ONTAP bietet hervorragende Optionen zum Bereitstellen und Verwalten von Anwendungs-Workloads zusammen mit Dateidiensten und reduziert gleichzeitig die Gesamtbetriebskosten, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden. Wählen Sie für jeden Anwendungsfall VMware Cloud on AWS zusammen mit Amazon FSx ONTAP , um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und Betriebsabläufe von On-Premises zu AWS zu gewährleisten, Workloads bidirektional zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen. Es handelt sich um denselben bekannten Prozess und dieselben bekannten Verfahren, die zum Verbinden von Speichern verwendet werden.

Weitere Informationen finden Sie unter:

- "FSx ONTAP als ergänzender NFS-Datenspeicher: Übersicht"
- "Amazon FSx für ONTAP als ergänzender Datenspeicher"

Amazon FSx for NetApp ONTAP als mit dem Gast verbundener Speicher

Amazon FSx ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher bietet, der auf dem beliebten ONTAP Dateisystem von NetApp basiert. FSx ONTAP kombiniert die vertrauten Funktionen, Leistung, Fähigkeiten und API-Operationen von NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten AWS-Dienstes.

FSx ONTAP bietet funktionsreichen, schnellen und flexiblen gemeinsamen Dateispeicher, der von Linux-, Windows- und macOS-Recheninstanzen, die in AWS oder vor Ort ausgeführt werden, umfassend zugänglich ist. FSx ONTAP bietet leistungsstarken Solid-State-Drive-Speicher (SSD) mit Latenzen von unter einer Millisekunde. Mit FSx ONTAP können Sie für Ihre Arbeitslast eine SSD-Leistung erzielen und gleichzeitig nur für einen kleinen Teil Ihrer Daten SSD-Speicher bezahlen.

Die Verwaltung Ihrer Daten mit FSx ONTAP ist einfacher, da Sie Ihre Dateien per Mausklick als Snapshot erstellen, klonen und replizieren können. Darüber hinaus verteilt FSx ONTAP Ihre Daten automatisch auf kostengünstigeren, elastischen Speicher, sodass Sie weniger Kapazität bereitstellen oder verwalten müssen.

FSx ONTAP bietet außerdem hochverfügbaren und langlebigen Speicher mit vollständig verwalteten Backups und Unterstützung für regionsübergreifende Notfallwiederherstellung. Um den Schutz und die Sicherung Ihrer Daten zu vereinfachen, unterstützt FSx ONTAP gängige Datensicherheits- und Antivirenanwendungen.

Weitere Informationen finden Sie unter"FSx ONTAP als Gastverbundener Speicher"

Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenverwaltungslösung, die auf der ONTAP -Speichersoftware von NetApp basiert und nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar ist.

Es handelt sich um eine softwaredefinierte Version von ONTAP , die Cloud-nativen Speicher nutzt. Dadurch können Sie in der Cloud und vor Ort dieselbe Speichersoftware verwenden und müssen Ihr IT-Personal nicht mehr in völlig neuen Methoden zur Verwaltung Ihrer Daten schulen.

CVO bietet Kunden die Möglichkeit, Daten nahtlos vom Edge zum Rechenzentrum, in die Cloud und zurück zu verschieben und so Ihre Hybrid Cloud zusammenzuführen – alles verwaltet über eine zentrale Verwaltungskonsole, den NetApp Cloud Manager.

CVO bietet von Haus aus extreme Leistung und erweiterte Datenverwaltungsfunktionen, um selbst Ihre anspruchsvollsten Anwendungen in der Cloud zu erfüllen.

Weitere Informationen finden Sie unter"CVO als Gastverbundener Speicher" .

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

In diesem Dokument wird beschrieben, wie Sie Amazon FSx ONTAP als NFS-Datenspeicher mit VMware Cloud auf AWS mounten.

Einführung

Jede erfolgreiche Organisation befindet sich auf dem Weg der Transformation und Modernisierung. Im Rahmen dieses Prozesses nutzen Unternehmen in der Regel ihre vorhandenen VMware-Investitionen, um die Vorteile der Cloud zu nutzen und zu erkunden, wie sie Prozesse möglichst nahtlos migrieren, erweitern und für die Notfallwiederherstellung bereitstellen können. Kunden, die in die Cloud migrieren, müssen die Anwendungsfälle hinsichtlich Elastizität und Burst, Rechenzentrumsausstieg, Rechenzentrumskonsolidierung,

End-of-Life-Szenarien, Fusionen, Übernahmen usw. bewerten.

Obwohl VMware Cloud auf AWS für die Mehrheit der Kunden die bevorzugte Option ist, da es dem Kunden einzigartige Hybridfunktionen bietet, ist die Nützlichkeit für Unternehmen mit speicherintensiven Workloads aufgrund der begrenzten nativen Speicheroptionen eingeschränkt. Da der Speicher direkt an Hosts gebunden ist, besteht die einzige Möglichkeit zur Skalierung des Speichers darin, weitere Hosts hinzuzufügen, was bei speicherintensiven Workloads zu einer Kostensteigerung von 35–40 % oder mehr führen kann. Diese Workloads erfordern zusätzlichen Speicher und getrennte Leistung, nicht zusätzliche Leistung, aber das bedeutet, dass für zusätzliche Hosts bezahlt werden muss. Hier ist der "jüngste Integration" von FSx ONTAP ist praktisch für speicher- und leistungsintensive Workloads mit VMware Cloud auf AWS.

Betrachten wir das folgende Szenario: Ein Kunde benötigt acht Hosts für die Leistung (vCPU/vMem), hat aber auch einen erheblichen Speicherbedarf. Ihrer Einschätzung nach sind 16 Hosts erforderlich, um die Speicheranforderungen zu erfüllen. Dies erhöht die Gesamtbetriebskosten, da sie die ganze zusätzliche Leistung kaufen müssen, obwohl sie eigentlich nur mehr Speicherplatz benötigen. Dies gilt für alle Anwendungsfälle, einschließlich Migration, Notfallwiederherstellung, Bursting, Entwicklung/Test usw.

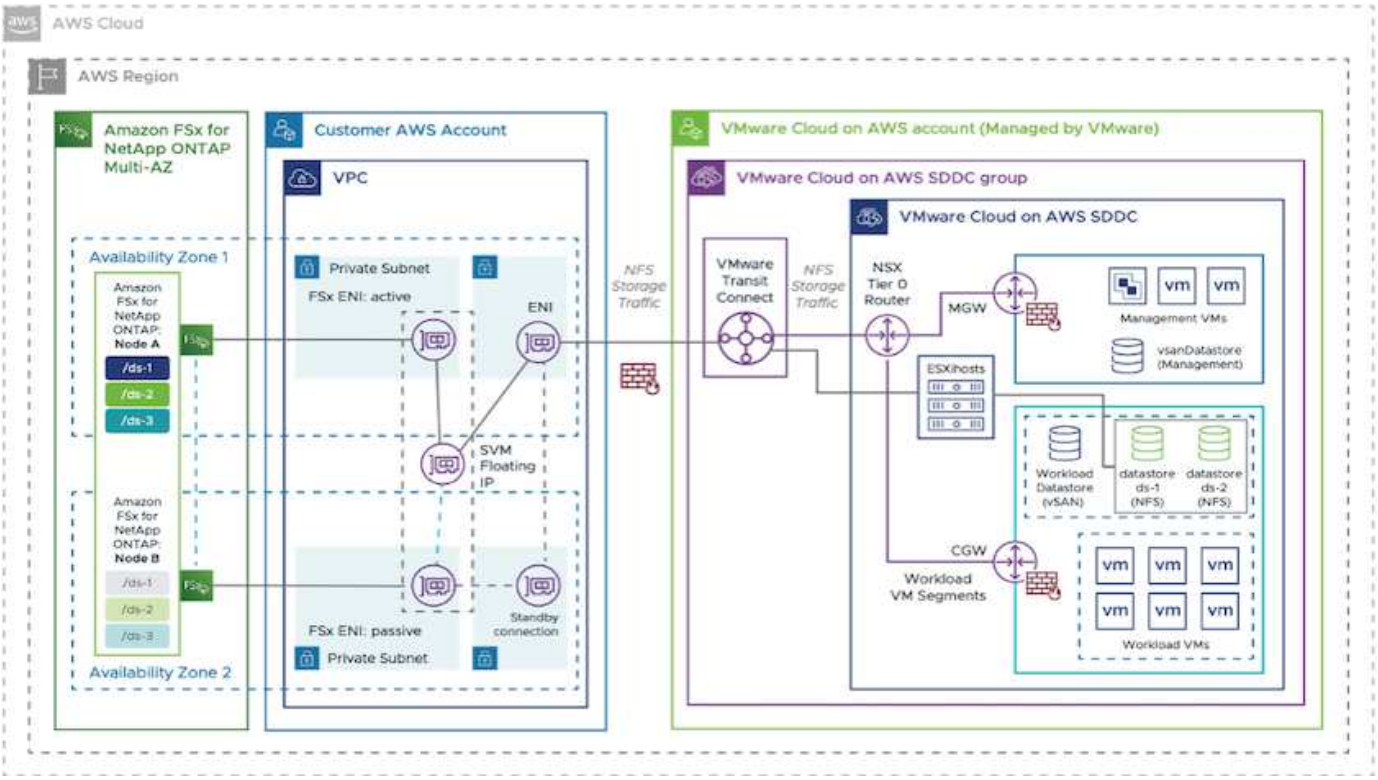
Dieses Dokument führt Sie durch die erforderlichen Schritte zum Bereitstellen und Anschließen von FSx ONTAP als NFS-Datenspeicher für VMware Cloud auf AWS.

Diese Lösung ist auch von VMware erhältlich. Bitte besuchen Sie die"VMware Cloud on AWS-Dokumentation" für weitere Informationen.

Konnektivitätsoptionen

VMware Cloud on AWS unterstützt sowohl Multi-AZ- als auch Single-AZ-Bereitstellungen von FSx ONTAP.

In diesem Abschnitt wird die Konnektivitätsarchitektur auf hoher Ebene sowie die erforderlichen Schritte zum Implementieren der Lösung beschrieben, um den Speicher in einem SDDC-Cluster zu erweitern, ohne dass zusätzliche Hosts hinzugefügt werden müssen.



Die Bereitstellungsschritte auf hoher Ebene sind wie folgt:

1. Erstellen Sie Amazon FSx ONTAP in einer neuen designierten VPC.
2. Erstellen Sie eine SDDC-Gruppe.
3. Erstellen Sie VMware Transit Connect und einen TGW-Anhang.
4. Konfigurieren Sie Routing (AWS VPC und SDDC) und Sicherheitsgruppen.
5. Hängen Sie ein NFS-Volume als Datenspeicher an den SDDC-Cluster an.

Bevor Sie FSx ONTAP als NFS-Datenspeicher bereitstellen und anhängen, müssen Sie zunächst eine VMware on Cloud SDDC-Umgebung einrichten oder ein vorhandenes SDDC auf v1.20 oder höher aktualisieren. Weitere Informationen finden Sie im "Erste Schritte mit VMware Cloud auf AWS" .

FSx ONTAP wird derzeit nicht mit Stretched Clustern unterstützt.

Abschluss

Dieses Dokument behandelt die notwendigen Schritte zur Konfiguration von Amazon FSx ONTAP mit VMware Cloud auf AWS. Amazon FSx ONTAP bietet hervorragende Optionen zum Bereitstellen und Verwalten von Anwendungs-Workloads zusammen mit Dateidiensten und reduziert gleichzeitig die Gesamtbetriebskosten, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden. Wählen Sie für jeden Anwendungsfall VMware Cloud on AWS zusammen mit Amazon FSx ONTAP , um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und Betriebsabläufe von On-Premises zu AWS zu gewährleisten, Workloads bidirektional zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen. Es handelt sich um denselben bekannten Prozess und dieselben bekannten Verfahren, die zum Verbinden von Speichern verwendet werden. Denken Sie daran, dass sich neben den neuen Namen nur die Position der Daten geändert hat. Die Tools und Prozesse bleiben alle gleich und Amazon FSx ONTAP trägt zur Optimierung der gesamten Bereitstellung bei.

Um mehr über diesen Vorgang zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video

ansehen.

Amazon FSx ONTAP VMware Cloud

Erstellen eines zusätzlichen NFS-Datenspeichers in AWS

Nachdem VMware Cloud bereit und mit AWS VPC verbunden ist, müssen Sie Amazon FSx ONTAP in einem neu zugewiesenen VPC und nicht im ursprünglich verbundenen oder vorhandenen Standard-VPC bereitstellen.

Stellen Sie zunächst eine zusätzliche VPC in derselben Region und Verfügbarkeitszone bereit, in der sich SDDC befindet, und stellen Sie dann Amazon FSx ONTAP in der neuen VPC bereit. "Konfiguration einer SDDC-Gruppe in der VMware Cloud" Die Konsole aktiviert die Netzwerkkonfigurationsoptionen, die für die Verbindung mit der neu festgelegten VPC erforderlich sind, in der FSx ONTAP bereitgestellt wird.

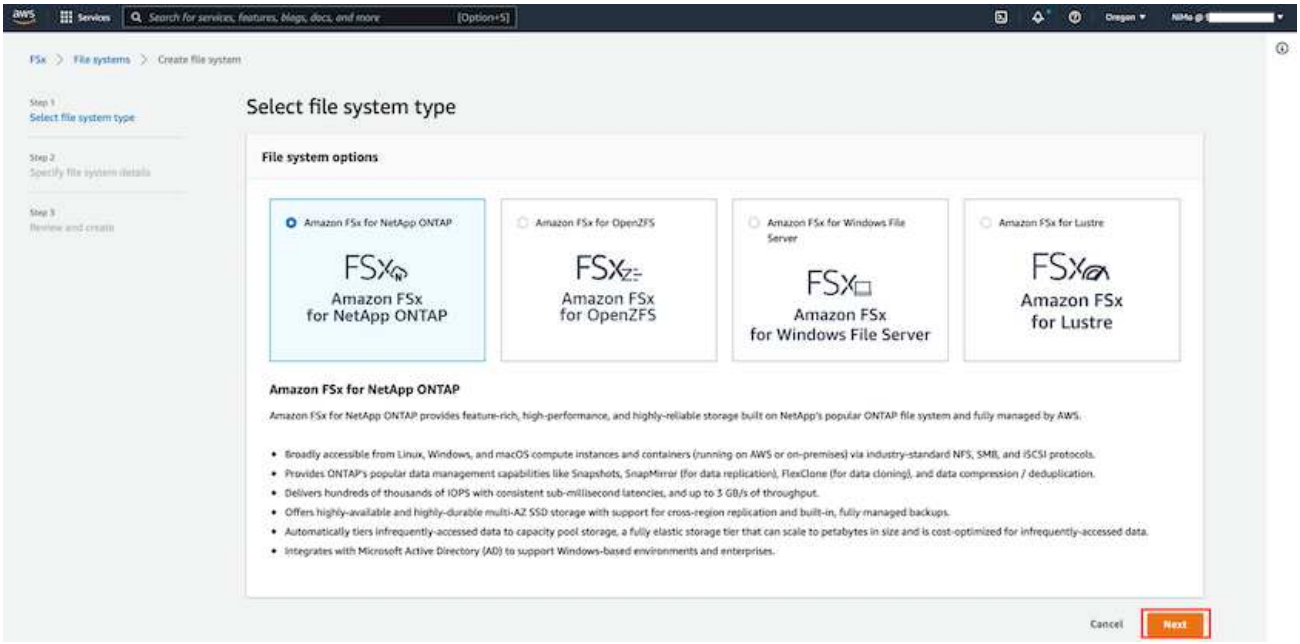
Stellen Sie FSx ONTAP in derselben Availability Zone wie VMware Cloud on AWS SDDC bereit.

Sie können FSx ONTAP nicht im Connected VPC bereitstellen. Stattdessen müssen Sie es in einem neuen, dafür vorgesehenen VPC bereitstellen und das VPC dann über SDDC-Gruppen mit einem VMware Managed Transit Gateway (vTGW) verbinden.

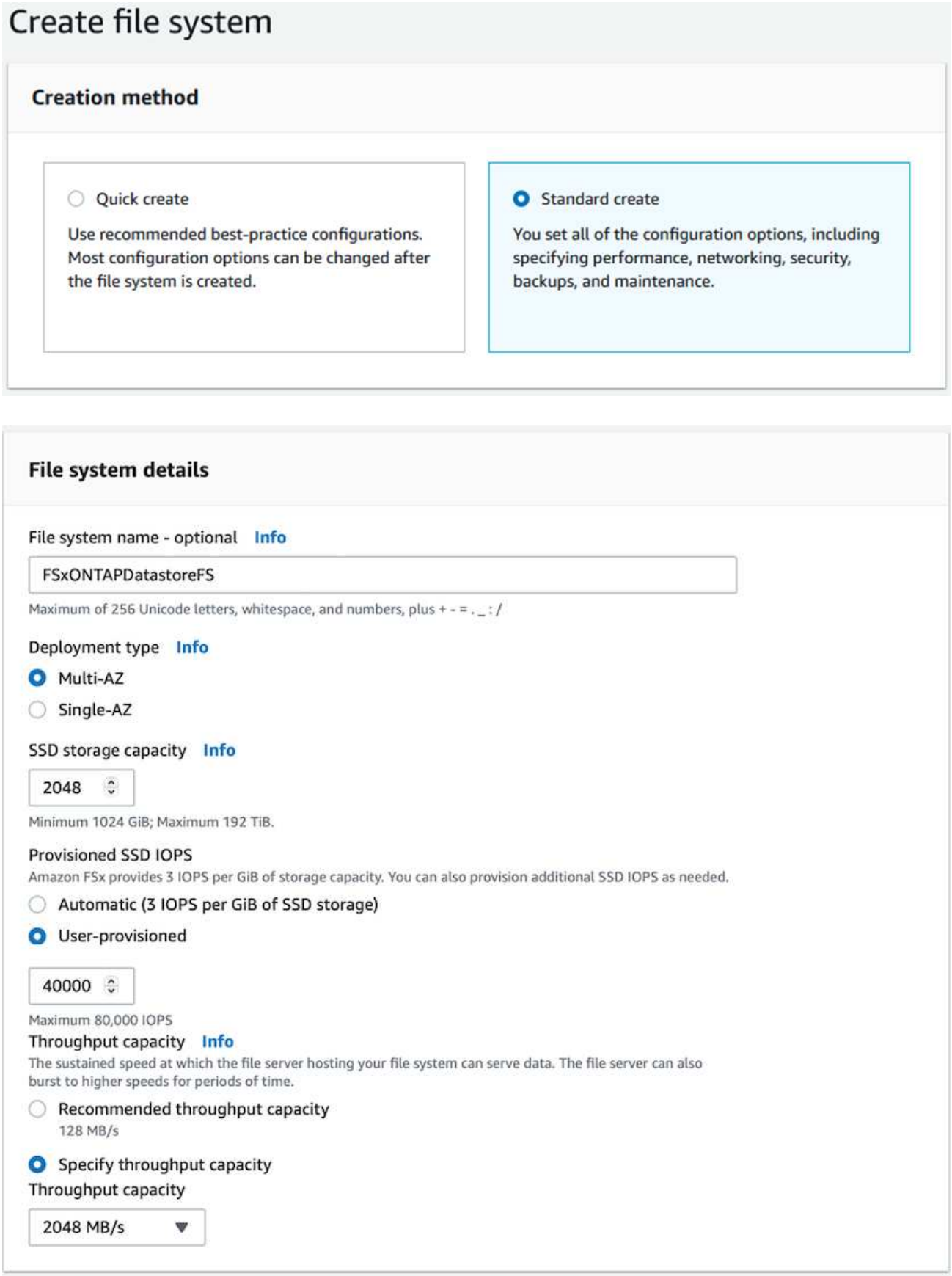
▼ **Schritt 1: Erstellen Sie Amazon FSx ONTAP in einer neuen, designierten VPC**

Führen Sie die folgenden Schritte aus, um das Amazon FSx ONTAP Dateisystem zu erstellen und bereitzustellen:

1. Öffnen Sie die Amazon FSx Konsole unter `https://console.aws.amazon.com/fsx/` und wählen Sie **Dateisystem erstellen**, um den Assistenten **Dateisystem erstellen** zu starten.
2. Wählen Sie auf der Seite „Dateisystemtyp auswählen“ * Amazon FSx ONTAP* aus und klicken Sie dann auf **Weiter**. Die Seite **Dateisystem erstellen** wird angezeigt.



3. Wählen Sie als Erstellungsmethode **Standarderstellung**.



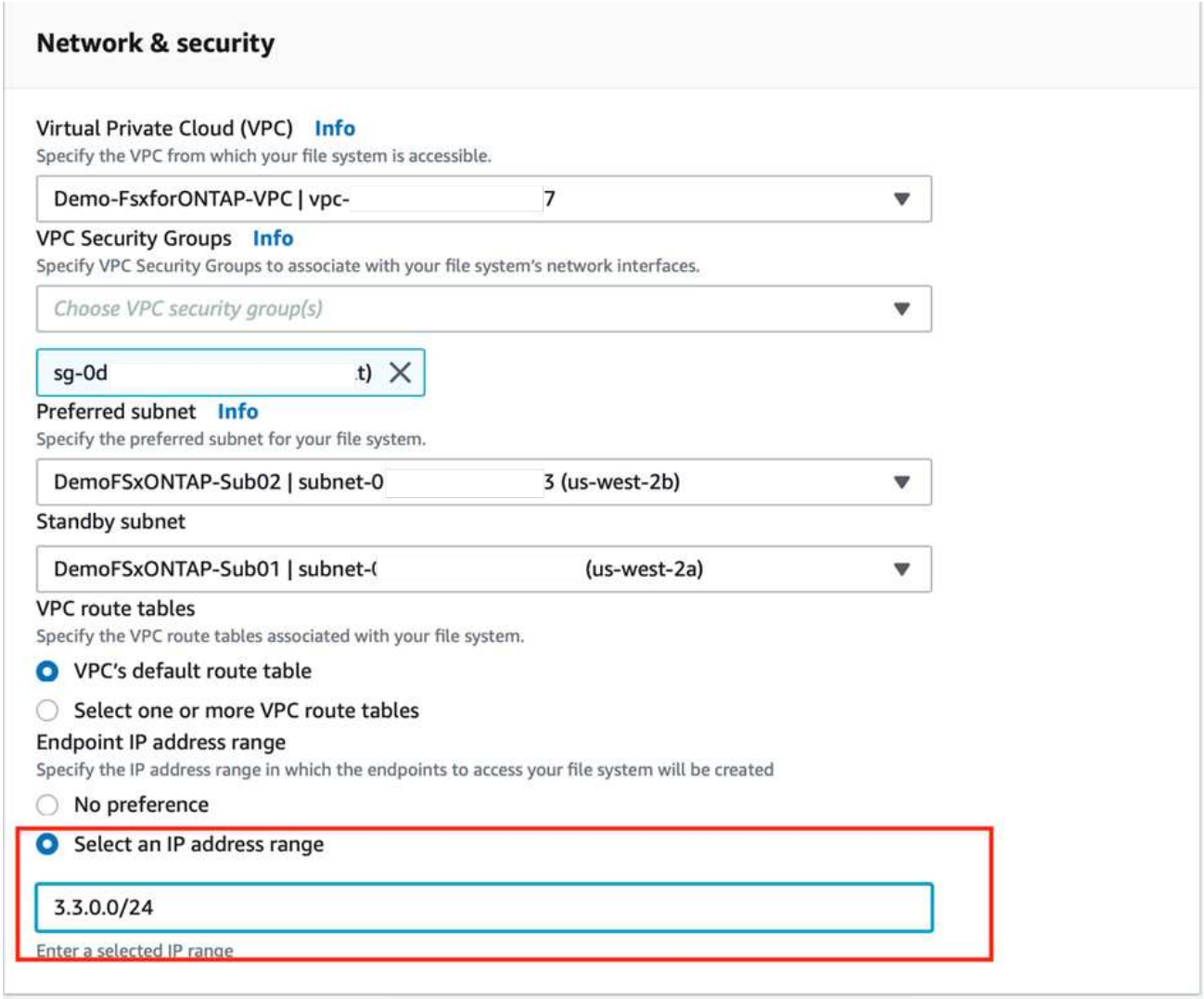
Die Datenspeichergrößen variieren von Kunde zu Kunde erheblich. Obwohl die empfohlene Anzahl virtueller Maschinen pro NFS-Datenspeicher subjektiv ist, wird die

optimale Anzahl VMs, die auf jedem Datenspeicher platziert werden können, von vielen Faktoren bestimmt. Obwohl die meisten Administratoren nur die Kapazität berücksichtigen, ist die Menge der gleichzeitig an die VMDKs gesendeten E/A-Vorgänge einer der wichtigsten Faktoren für die Gesamtleistung. Verwenden Sie Leistungsstatistiken vor Ort, um die Datenspeichervolumes entsprechend zu dimensionieren.

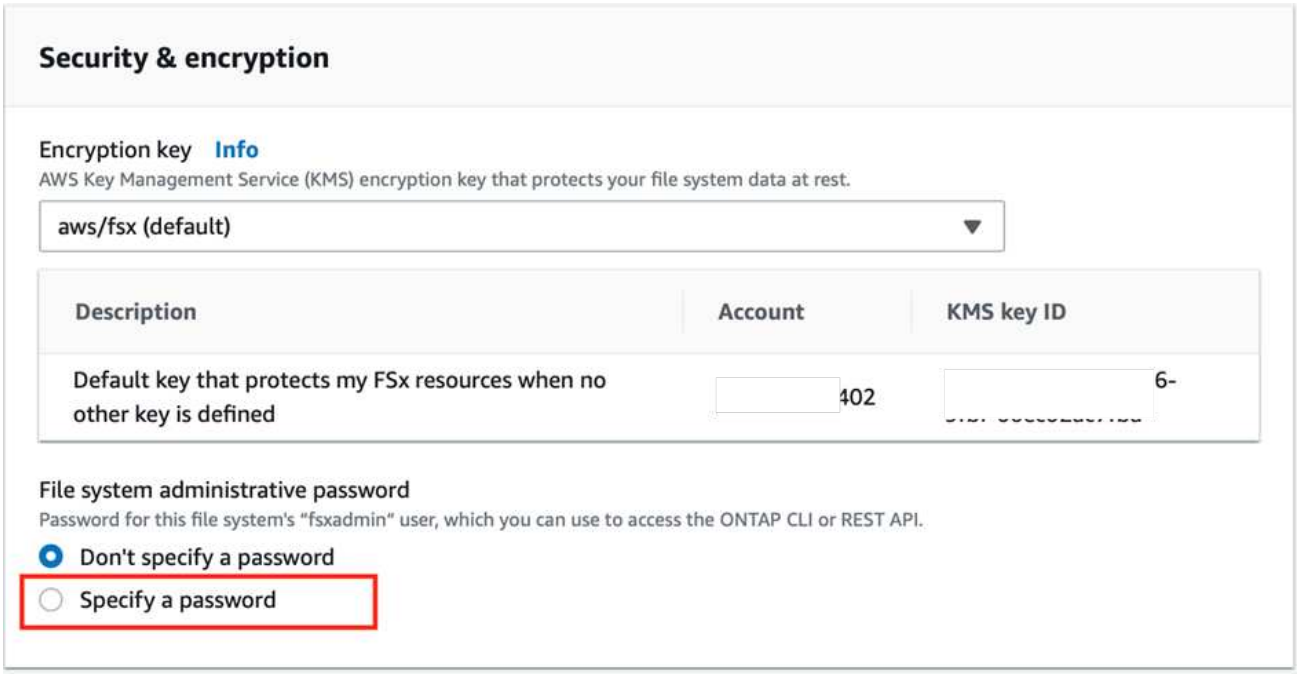
4. Wählen Sie im Abschnitt **Netzwerk** für Virtual Private Cloud (VPC) die entsprechende VPC und die bevorzugten Subnetze zusammen mit der Routentabelle aus. In diesem Fall wird Demo-FSxforONTAP-VPC aus dem Dropdown-Menü ausgewählt.

Stellen Sie sicher, dass es sich um eine neue, designierte VPC und nicht um die verbundene VPC handelt.

Standardmäßig verwendet FSx ONTAP 198.19.0.0/16 als Standard-Endpunkt-IP-Adressbereich für das Dateisystem. Stellen Sie sicher, dass der IP-Adressbereich des Endpunkts nicht mit dem VMC auf dem AWS SDDC, den zugehörigen VPC-Subnetzen und der lokalen Infrastruktur in Konflikt steht. Wenn Sie unsicher sind, verwenden Sie einen nicht überlappenden Bereich ohne Konflikte.

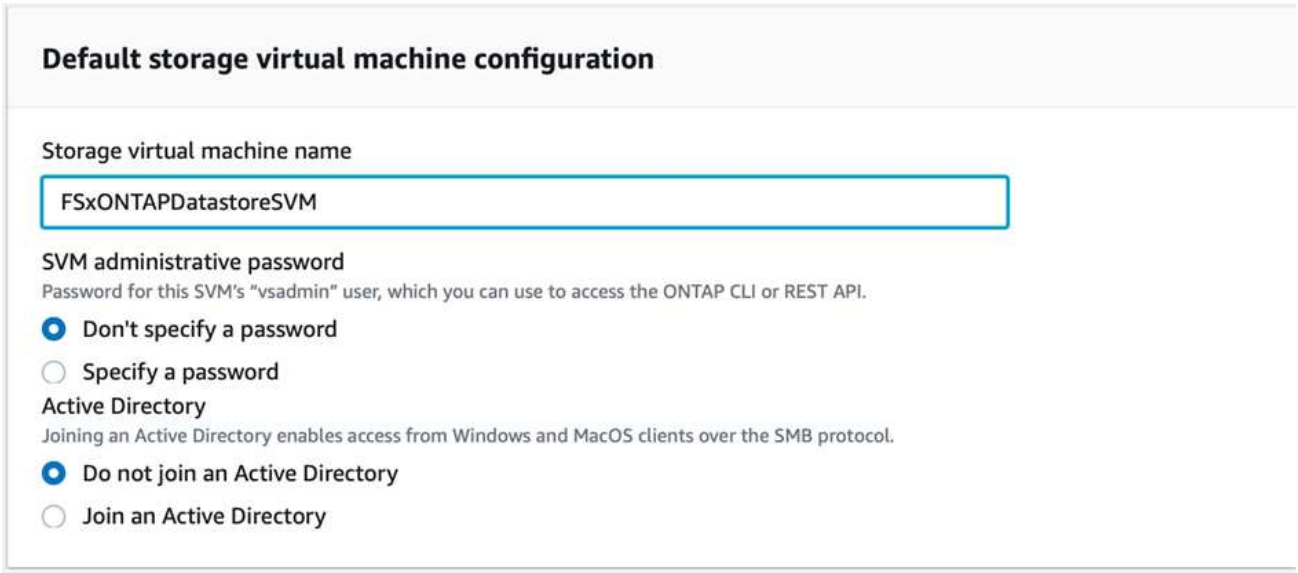


5. Wählen Sie im Abschnitt **Sicherheit und Verschlüsselung** für den Verschlüsselungsschlüssel den Verschlüsselungsschlüssel des AWS Key Management Service (AWS KMS) aus, der die ruhenden Daten des Dateisystems schützt. Geben Sie für das **Dateisystem-Administratorkennwort** ein sicheres Kennwort für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



6. Geben Sie im Abschnitt **Standardkonfiguration der virtuellen Speichermaschine** den Namen der SVM an.

Ab GA werden vier NFS-Datenspeicher unterstützt.



7. Geben Sie im Abschnitt **Standardvolumekonfiguration** den für den Datenspeicher erforderlichen Volumenamen und die Größe an und klicken Sie auf **Weiter**. Dies sollte ein NFSv3-Volume sein. Wählen Sie für **Speichereffizienz Aktiviert**, um die ONTAP Speichereffizienzfunktionen (Komprimierung, Deduplizierung und Kompaktierung) zu aktivieren. Verwenden Sie nach der Erstellung die Shell, um die Volume-Parameter mit ***volume modify*** wie folgt zu ändern:

Einstellung	Konfiguration
Volumengarantie (Space Guarantee Style)	Keine (Thin Provisioning) – standardmäßig eingestellt
fractional_reserve (Teilreserve)	0 % – standardmäßig eingestellt
snap_reserve (Prozent-Snapshot-Speicherplatz)	0 %
Automatische Größe (Autosize-Modus)	wachsen_schrumpfen
Speichereffizienz	Aktiviert – standardmäßig eingestellt
Automatisches Löschen	Volumen / älteste_zuerst
Volume-Tiering-Richtlinie	Nur Snapshot – standardmäßig eingestellt
Versuchen Sie es zuerst	Automatisches Wachstum
Snapshot-Richtlinie	Keine

Verwenden Sie den folgenden SSH-Befehl, um Volumes zu erstellen und zu ändern:

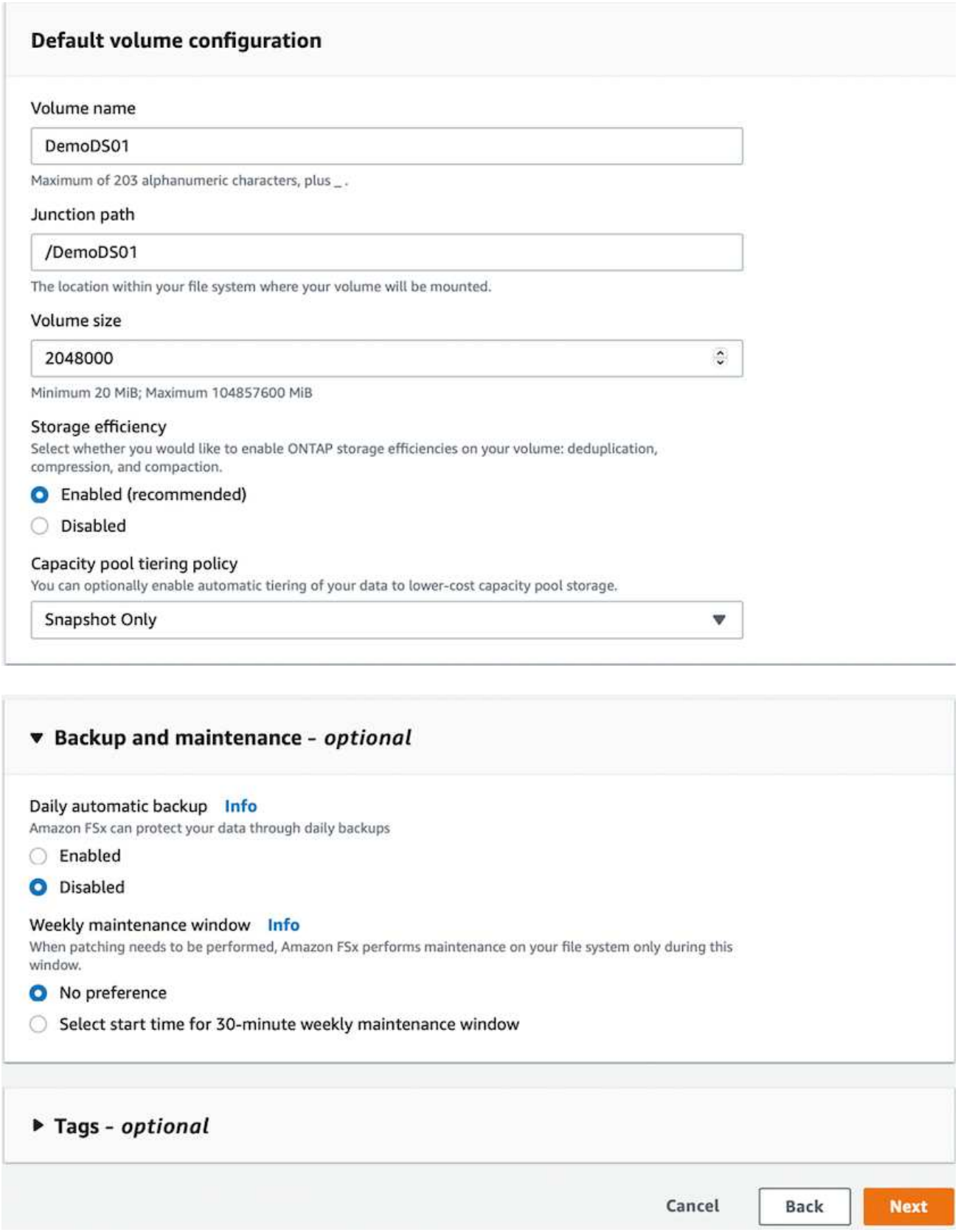
Befehl zum Erstellen eines neuen Datenspeichervolumes von der Shell aus:

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy snapshot-
only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy
none -junction-path /DemoDS002
```

Hinweis: Es dauert einige Minuten, bis die über die Shell erstellten Volumes in der AWS-Konsole angezeigt werden.

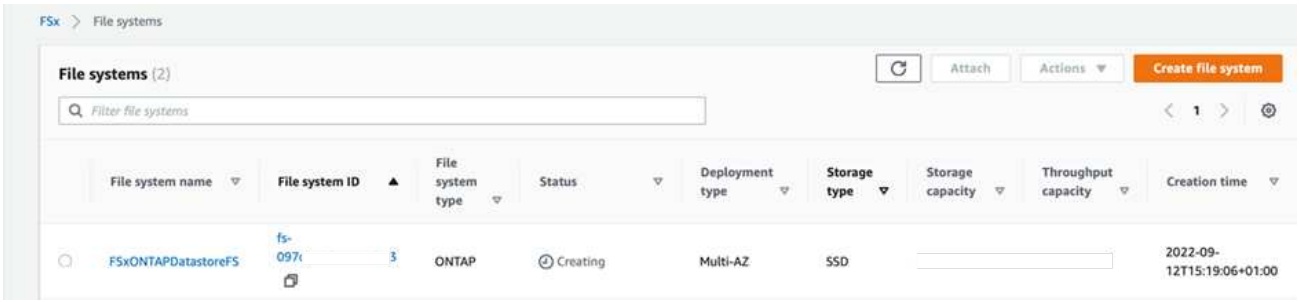
Befehl zum Ändern von Lautstärkeparametern, die nicht standardmäßig festgelegt sind:

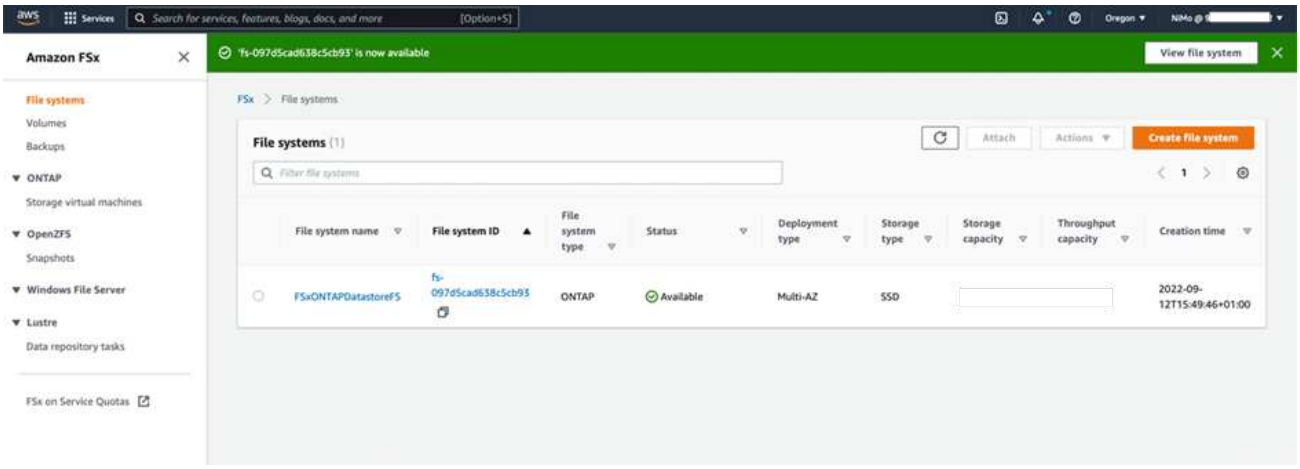
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```



Während des ersten Migrationsszenarios kann die standardmäßige Snapshot-Richtlinie zu Problemen mit der vollen Datenspeicherkapazität führen. Um dies zu umgehen, ändern Sie die Snapshot-Richtlinie entsprechend den Anforderungen.

8. Überprüfen Sie die Dateisystemkonfiguration, die auf der Seite **Dateisystem erstellen** angezeigt wird.
9. Klicken Sie auf **Dateisystem erstellen**.





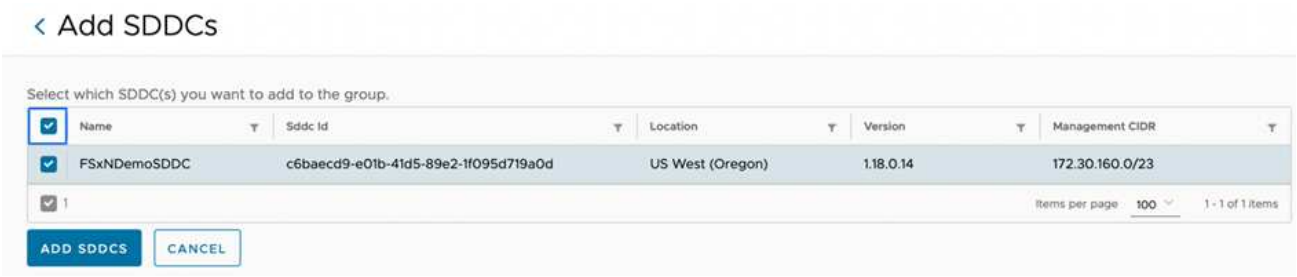
Wiederholen Sie die vorherigen Schritte, um je nach Kapazitäts- und Leistungsanforderungen weitere virtuelle Speichermaschinen oder Dateisysteme und Datenspeichervolumes zu erstellen.

Weitere Informationen zur Leistung von Amazon FSx ONTAP finden Sie unter "Amazon FSx ONTAP -Leistung" .

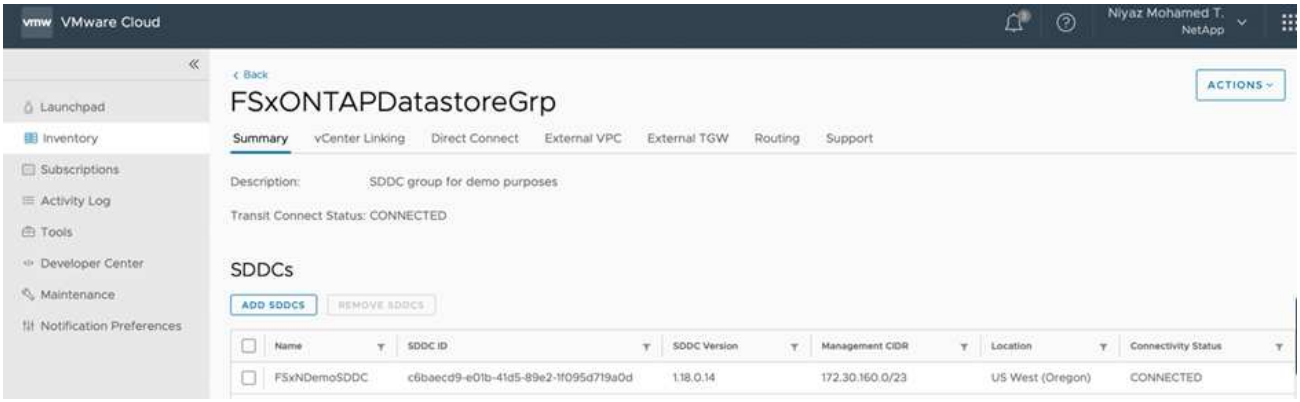
▼ Schritt 2: SDDC-Gruppe erstellen

Nachdem die Dateisysteme und SVMs erstellt wurden, verwenden Sie die VMware-Konsole, um eine SDDC-Gruppe zu erstellen und VMware Transit Connect zu konfigurieren. Führen Sie dazu die folgenden Schritte aus und denken Sie daran, dass Sie zwischen der VMware Cloud Console und der AWS Console navigieren müssen.

1. Melden Sie sich bei der VMC-Konsole an unter `https://vmc.vmware.com` .
2. Klicken Sie auf der Seite **Inventar** auf **SDDC-Gruppen**.
3. Klicken Sie auf der Registerkarte **SDDC-Gruppen** auf **AKTIONEN** und wählen Sie **SDDC-Gruppe erstellen**. Zu Demonstrationszwecken heißt die SDDC-Gruppe `FSxONTAPDatastoreGrp` .
4. Wählen Sie im Raster „Mitgliedschaft“ die SDDCs aus, die als Gruppenmitglieder aufgenommen werden sollen.

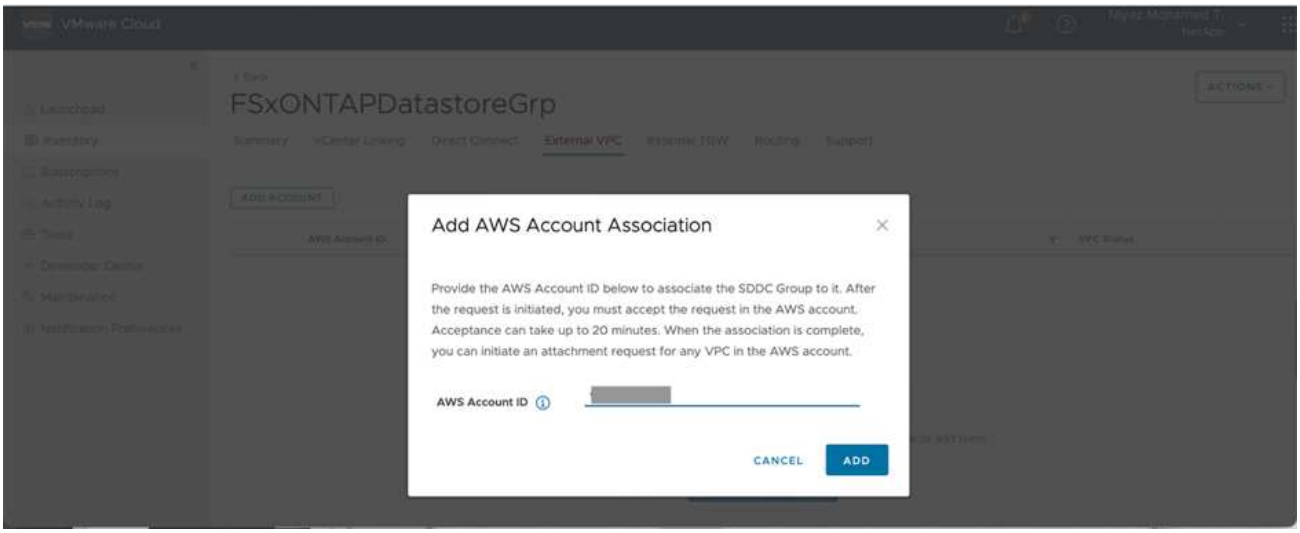


5. Stellen Sie sicher, dass die Option „Beim Konfigurieren von VMware Transit Connect für Ihre Gruppe fallen Gebühren pro Anhang und Datenübertragung an“ aktiviert ist, und wählen Sie dann „Gruppe erstellen“ aus. Der Vorgang kann einige Minuten dauern.



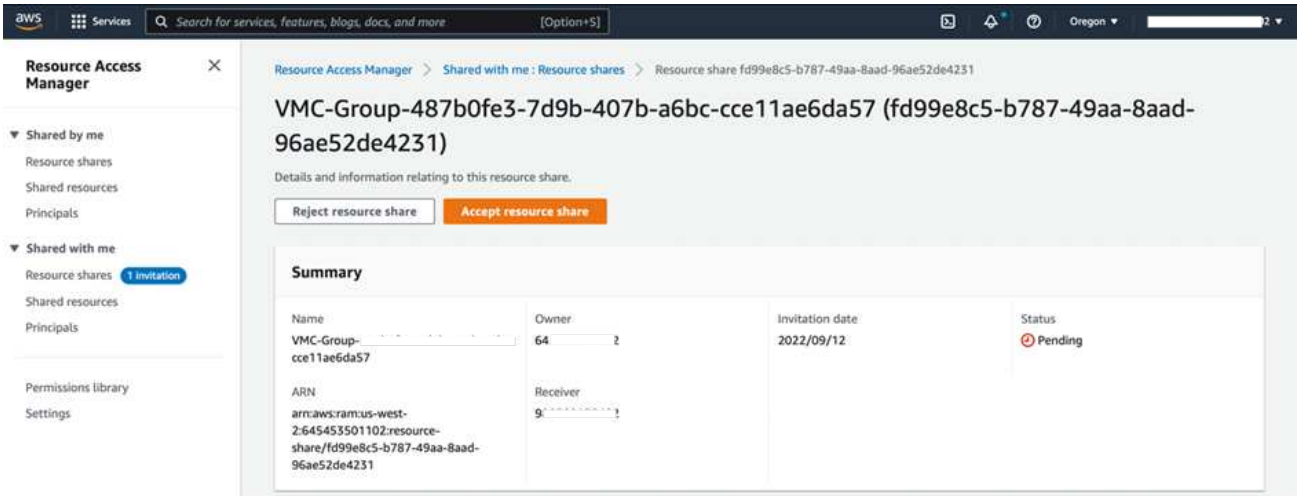
▼ Schritt 3: Konfigurieren Sie VMware Transit Connect

1. Fügen Sie die neu erstellte designierte VPC der SDDC-Gruppe hinzu. Wählen Sie die Registerkarte **Externe VPC** und folgen Sie den "Anweisungen zum Anhängen einer externen VPC an die Gruppe" . Dieser Vorgang kann 10–15 Minuten dauern.



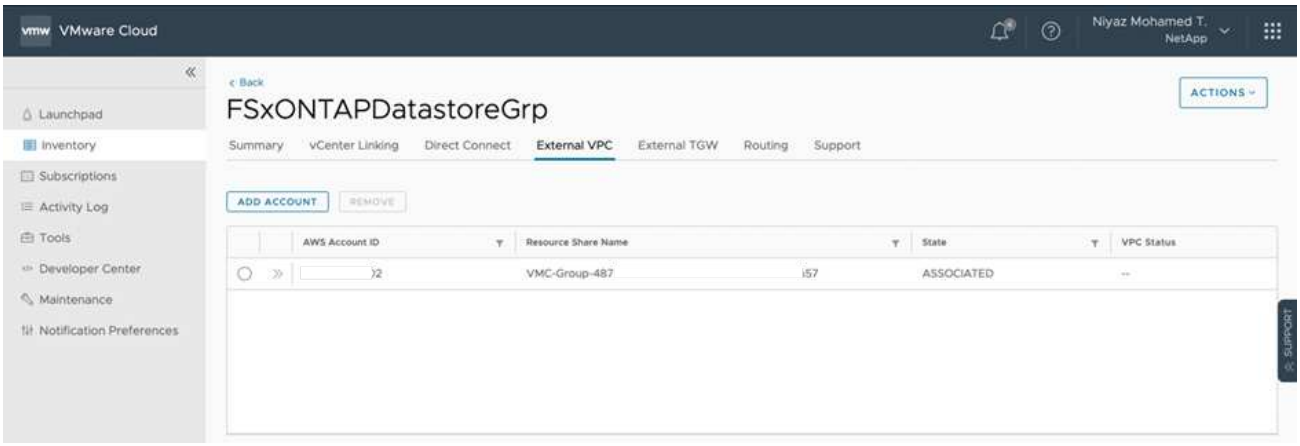
2. Klicken Sie auf **Konto hinzufügen**.
   a. Geben Sie das AWS-Konto an, das zum Bereitstellen des FSx ONTAP Dateisystems verwendet wurde.
   b. Klicken Sie auf **Hinzufügen**.
3. Melden Sie sich in der AWS-Konsole wieder beim selben AWS-Konto an und navigieren Sie zur Serviceseite **Resource Access Manager**. Es gibt eine Schaltfläche, mit der Sie die Ressourcenfreigabe

akzeptieren können.



Im Rahmen des externen VPC-Prozesses werden Sie über die AWS-Konsole zu einer neuen freigegebenen Ressource über den Resource Access Manager aufgefordert. Die gemeinsam genutzte Ressource ist das von VMware Transit Connect verwaltete AWS Transit Gateway.

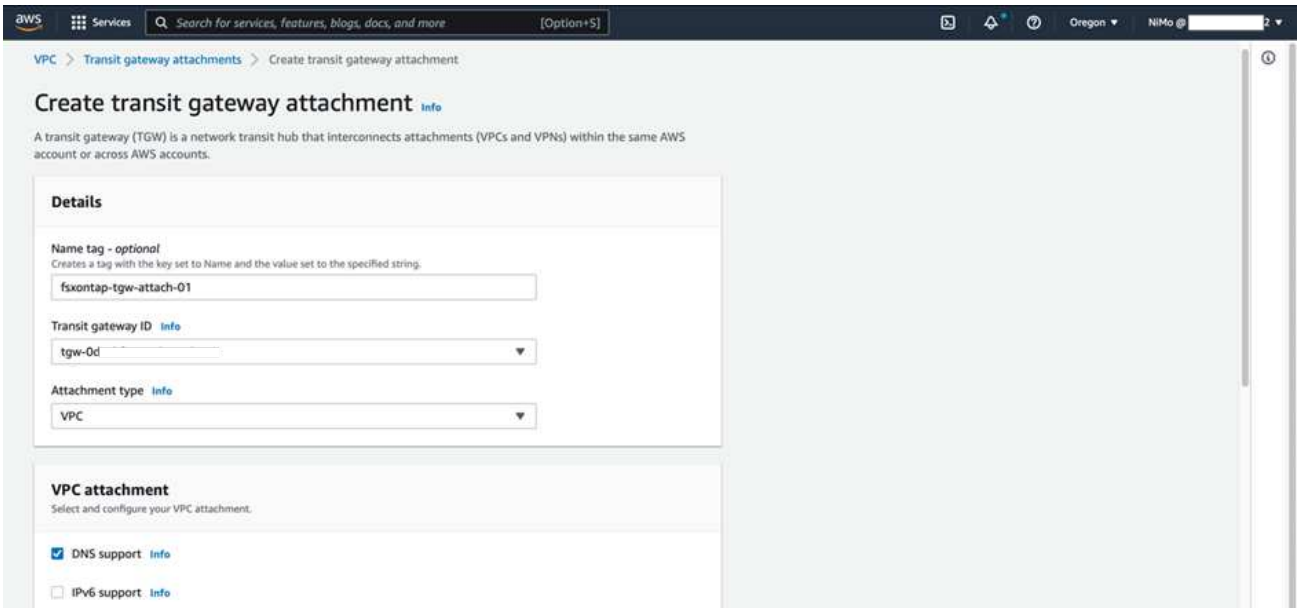
4. Klicken Sie auf **Ressourcenfreigabe akzeptieren**.



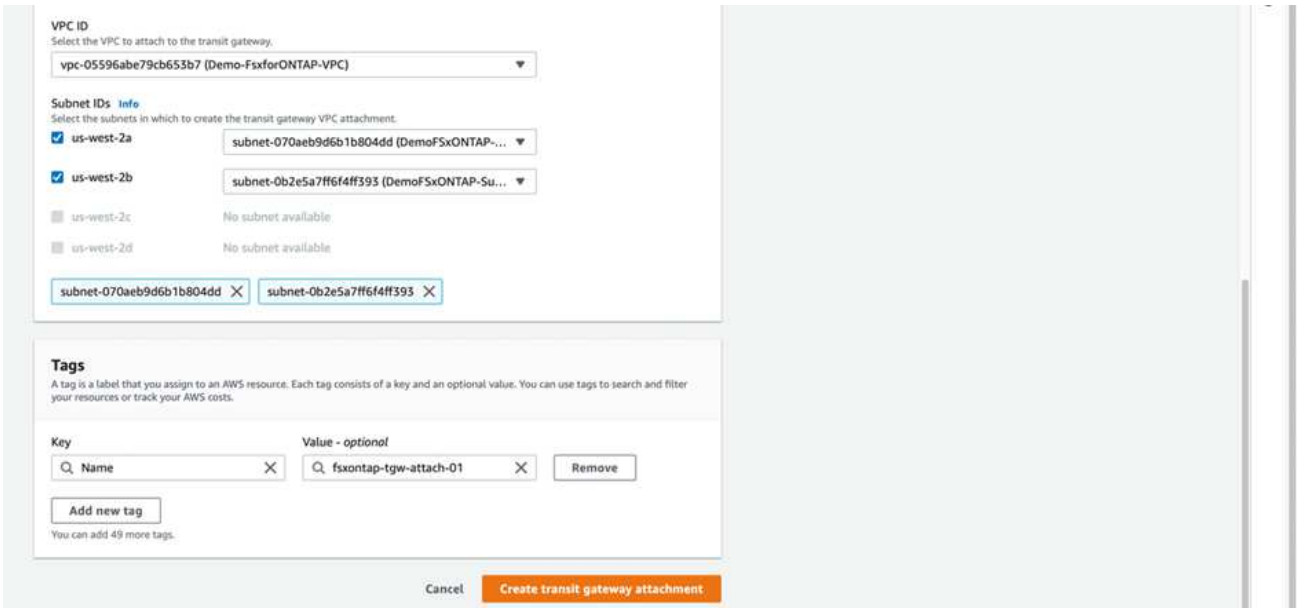
5. Zurück in der VMC-Konsole sehen Sie nun, dass sich die externe VPC in einem zugehörigen Status befindet. Es kann mehrere Minuten dauern, bis dies angezeigt wird.

▼ Schritt 4: Transit-Gateway-Anhang erstellen

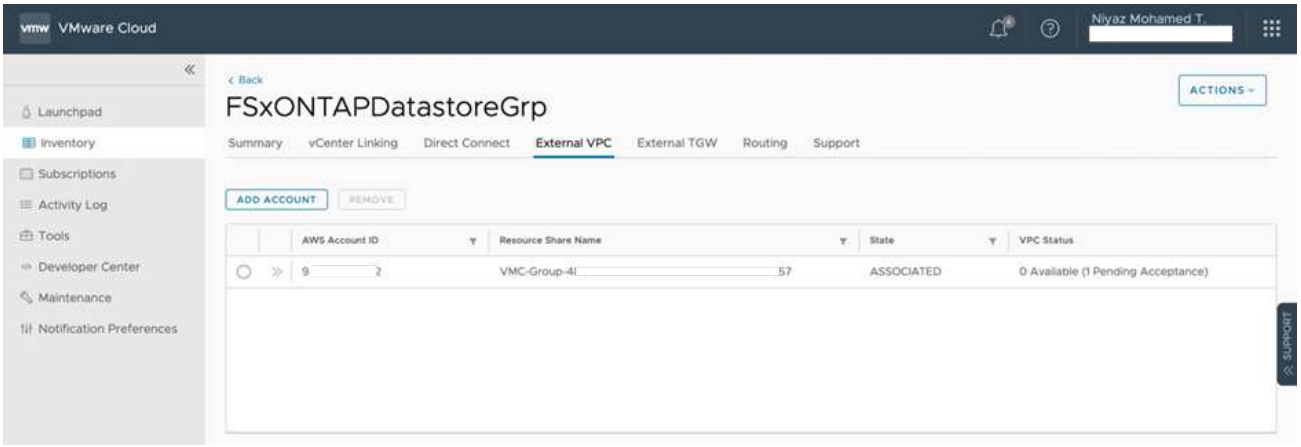
1. Gehen Sie in der AWS-Konsole zur VPC-Serviceseite und navigieren Sie zu der VPC, die für die Bereitstellung des FSx-Dateisystems verwendet wurde. Hier erstellen Sie einen Transit-Gateway-Anhang, indem Sie im Navigationsbereich rechts auf **Transit-Gateway-Anhang** klicken.
2. Stellen Sie unter **VPC-Anhang** sicher, dass DNS-Support aktiviert ist, und wählen Sie die VPC aus, in der FSx ONTAP bereitgestellt wurde.

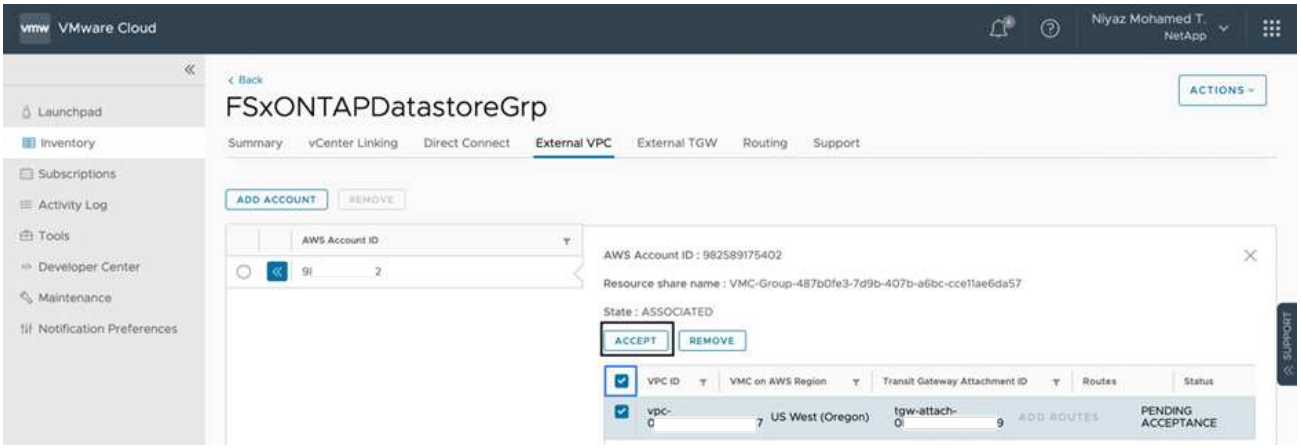


3. Klicken Sie auf **Transit-Gateway-Anhang erstellen**.



4. Navigieren Sie in der VMware Cloud Console zurück zur Registerkarte „SDDC-Gruppe > Externe VPC“. Wählen Sie die für FSx verwendete AWS-Konto-ID aus, klicken Sie auf die VPC und dann auf **Akzeptieren**.

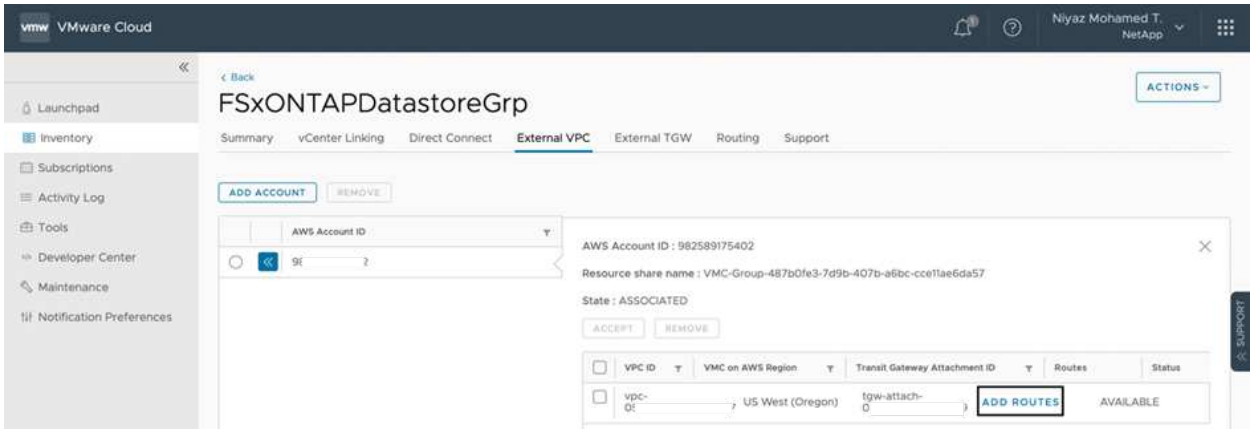


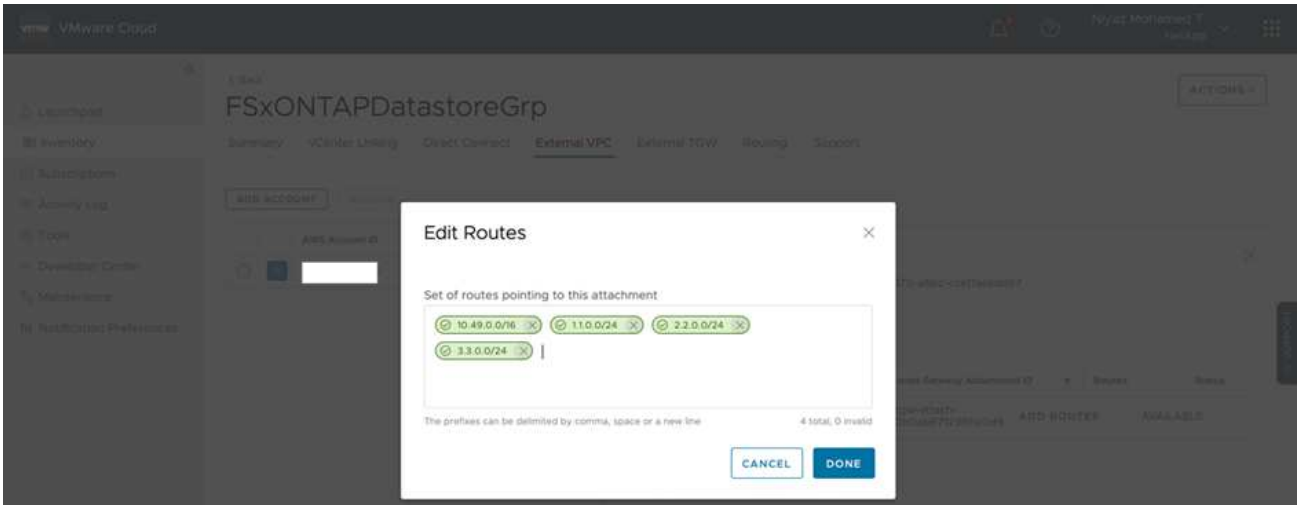


Es kann einige Minuten dauern, bis diese Option angezeigt wird.

5. Klicken Sie dann auf der Registerkarte **Externe VPC** in der Spalte **Routen** auf die Option **Routen hinzufügen** und fügen Sie die erforderlichen Routen hinzu:

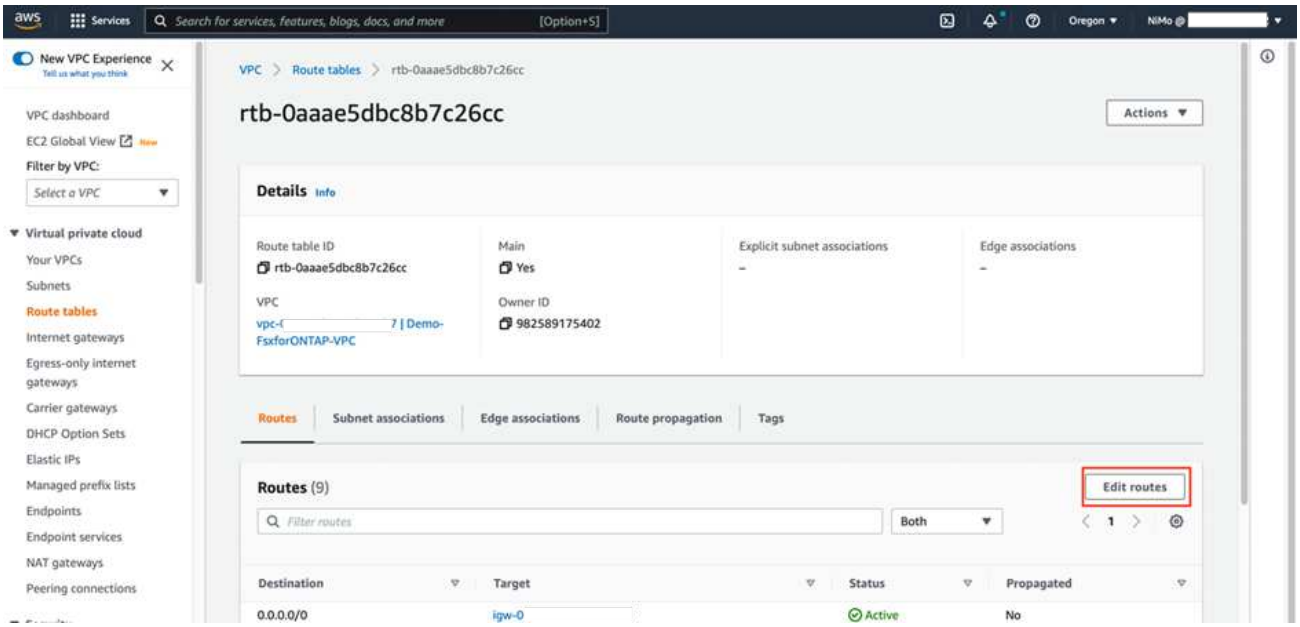
   - Eine Route für den Floating-IP-Bereich für Amazon FSx ONTAP Floating-IPs.
   - Eine Route für den neu erstellten externen VPC-Adressraum.



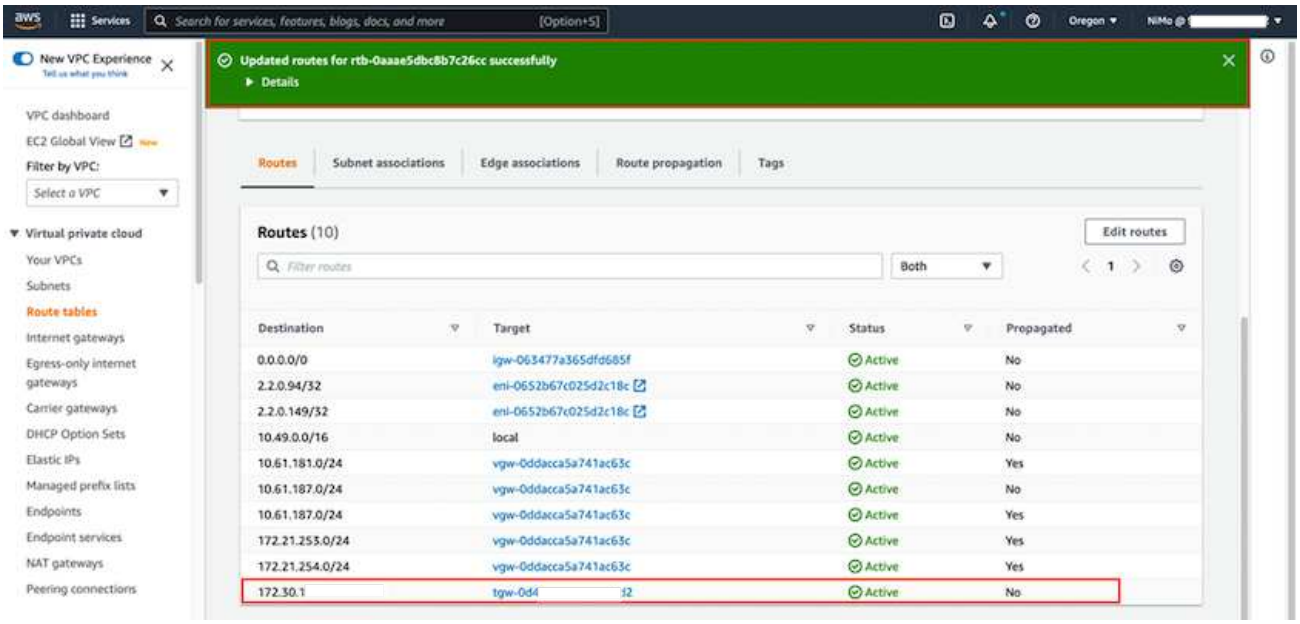


▼ **Schritt 5: Routing (AWS VPC und SDDC) und Sicherheitsgruppen konfigurieren**

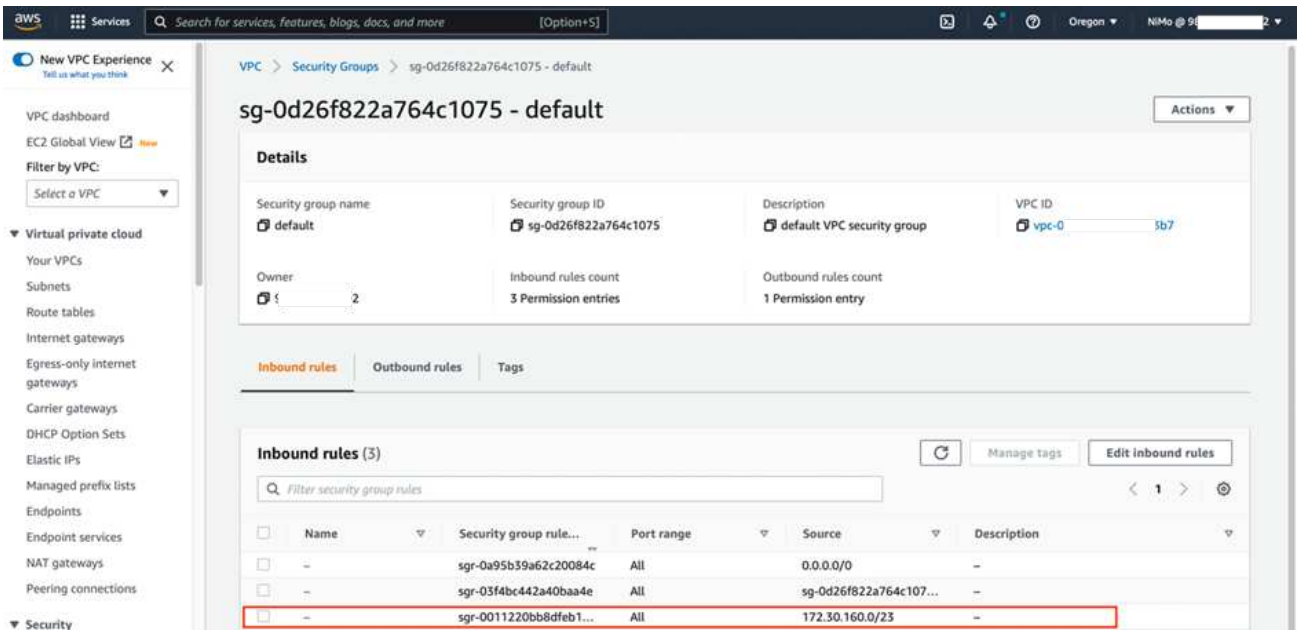
1. Erstellen Sie in der AWS-Konsole die Route zurück zum SDDC, indem Sie die VPC auf der VPC-Serviceseite suchen und die **Haupt**-Routentabelle für die VPC auswählen.
2. Navigieren Sie zur Routentabelle im unteren Bereich und klicken Sie auf **Routen bearbeiten**.



3. Klicken Sie im Bereich **Routen bearbeiten** auf **Route hinzufügen** und geben Sie den CIDR für die SDDC-Infrastruktur ein, indem Sie **Transit Gateway** und die zugehörige TGW-ID auswählen. Klicken Sie auf **Änderungen speichern**.



4. Der nächste Schritt besteht darin, zu überprüfen, ob die Sicherheitsgruppe im zugehörigen VPC mit den richtigen eingehenden Regeln für das SDDC-Gruppen-CIDR aktualisiert ist.
5. Aktualisieren Sie die eingehende Regel mit dem CIDR-Block der SDDC-Infrastruktur.



Stellen Sie sicher, dass die Routentabelle der VPC (wo sich FSx ONTAP befindet) aktualisiert ist, um Verbindungsprobleme zu vermeiden.

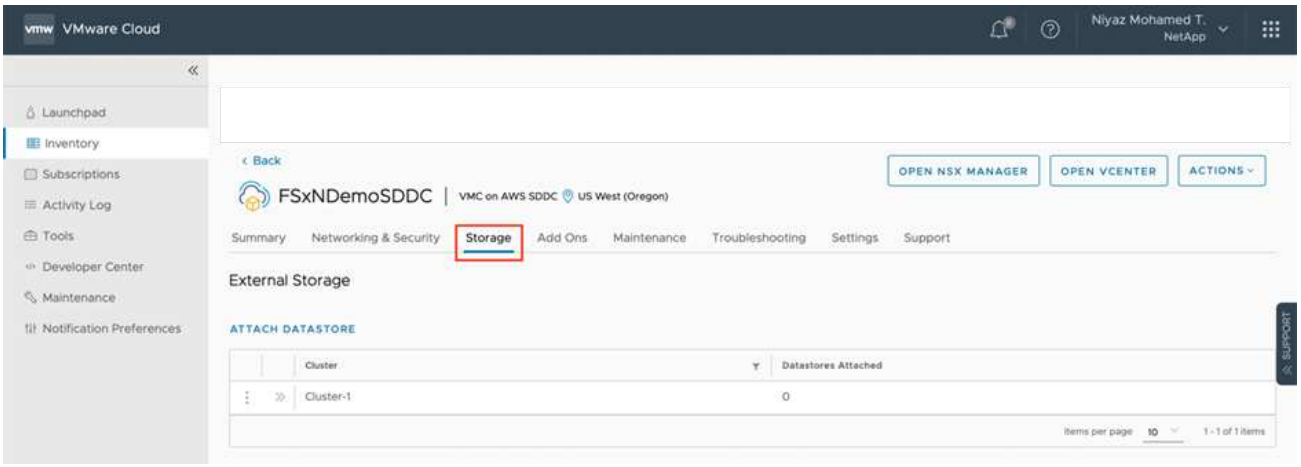
Aktualisieren Sie die Sicherheitsgruppe, um NFS-Verkehr zu akzeptieren.

Dies ist der letzte Schritt bei der Vorbereitung der Konnektivität zum entsprechenden SDDC. Nachdem das Dateisystem konfiguriert, Routen hinzugefügt und Sicherheitsgruppen aktualisiert wurden, ist es an der Zeit, den/die Datenspeicher zu mounten.

▼ Schritt 6: NFS-Volume als Datenspeicher an SDDC-Cluster anhängen

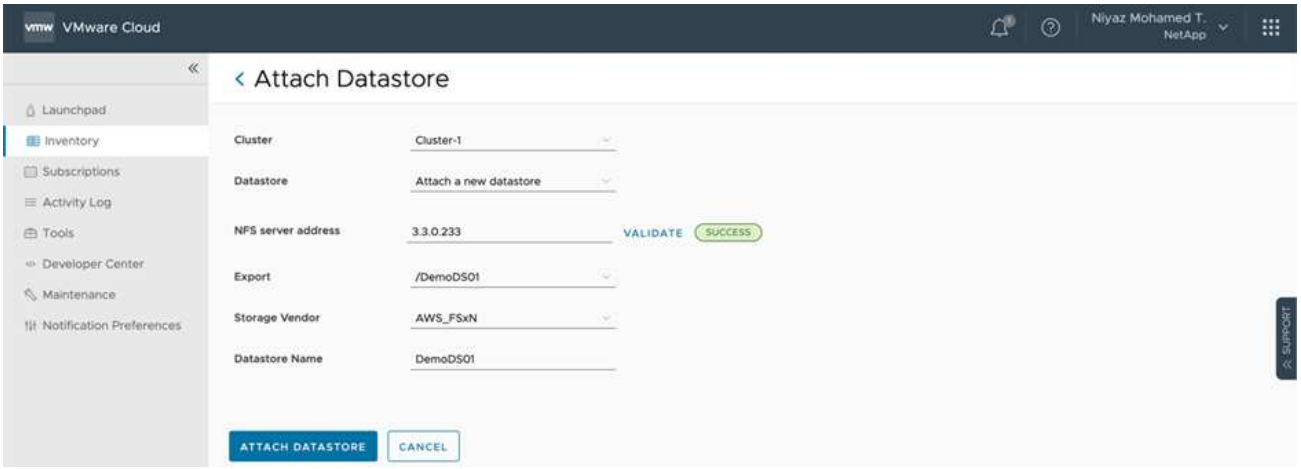
Nachdem das Dateisystem bereitgestellt und die Konnektivität hergestellt wurde, greifen Sie auf die VMware Cloud Console zu, um den NFS-Datenspeicher zu mounten.

1. Öffnen Sie in der VMC-Konsole die Registerkarte **Speicher** des SDDC.

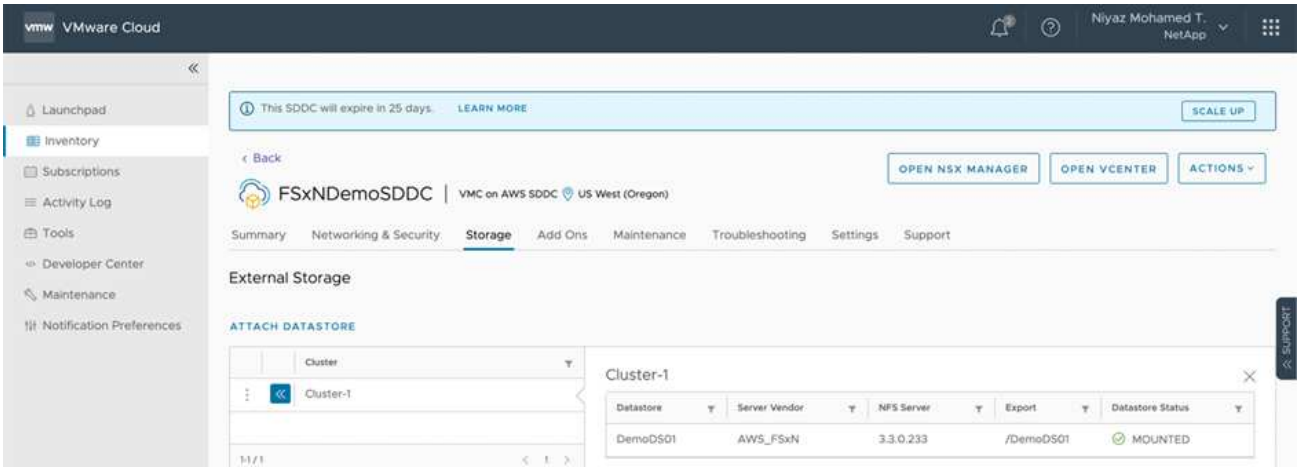


2. Klicken Sie auf **DATENSPEICHER ANHÄNGEN** und geben Sie die erforderlichen Werte ein.

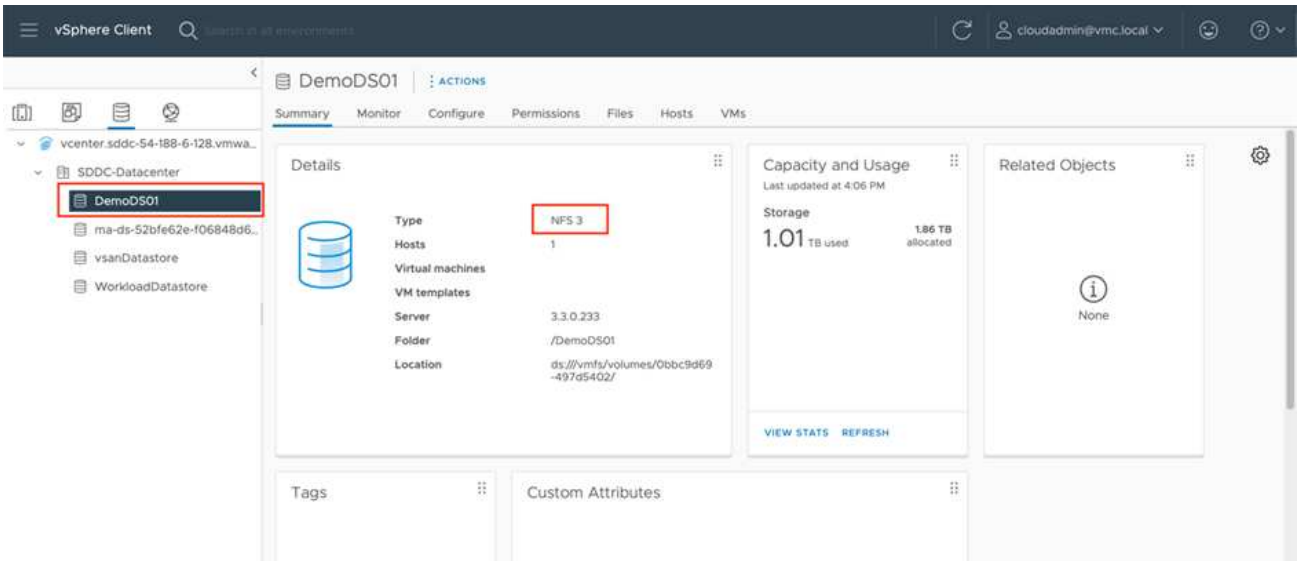
Die NFS-Serveradresse ist die NFS-IP-Adresse, die in der AWS-Konsole unter FSx > Registerkarte „Virtuelle Speichermaschinen“ > „Endpunkte“ zu finden ist.



3. Klicken Sie auf **DATENSPEICHER ANHÄNGEN**, um den Datenspeicher an den Cluster anzuhängen.



4. Validieren Sie den NFS-Datenspeicher, indem Sie wie unten gezeigt auf vCenter zugreifen:



NetApp Guest Connected Storage-Optionen für AWS

AWS unterstützt über Gäste verbundene NetApp -Speicher mit dem nativen FSx-Dienst (FSx ONTAP) oder mit Cloud Volumes ONTAP (CVO).

FSx ONTAP

Amazon FSx ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher bietet, der auf dem beliebten ONTAP Dateisystem von NetApp basiert. FSx ONTAP kombiniert die vertrauten Funktionen, Leistung, Fähigkeiten und API-Operationen von NetApp Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig verwalteten AWS-Dienstes.

FSx ONTAP bietet funktionsreichen, schnellen und flexiblen gemeinsamen Dateispeicher, der von Linux-, Windows- und macOS-Recheninstanzen, die in AWS oder vor Ort ausgeführt werden, umfassend zugänglich ist. FSx ONTAP bietet leistungsstarken Solid-State-Drive-Speicher (SSD) mit Latenzen im Submillisekundenbereich. Mit FSx ONTAP können Sie für Ihre Arbeitslast eine SSD-Leistung erzielen und gleichzeitig nur für einen kleinen Teil Ihrer Daten SSD-Speicher bezahlen.

Die Verwaltung Ihrer Daten mit FSx ONTAP ist einfacher, da Sie Ihre Dateien per Mausklick als Snapshot

erstellen, klonen und replizieren können. Darüber hinaus verteilt FSx ONTAP Ihre Daten automatisch auf kostengünstigeren, elastischen Speicher, sodass Sie weniger Kapazität bereitstellen oder verwalten müssen.

FSx ONTAP bietet außerdem hochverfügbaren und langlebigen Speicher mit vollständig verwalteten Backups und Unterstützung für regionsübergreifende Notfallwiederherstellung. Um den Schutz und die Sicherung Ihrer Daten zu vereinfachen, unterstützt FSx ONTAP gängige Datensicherheits- und Antivirenanwendungen.

FSx ONTAP als Gastspeicher

▼ **Konfigurieren Sie Amazon FSx ONTAP mit VMware Cloud auf AWS**

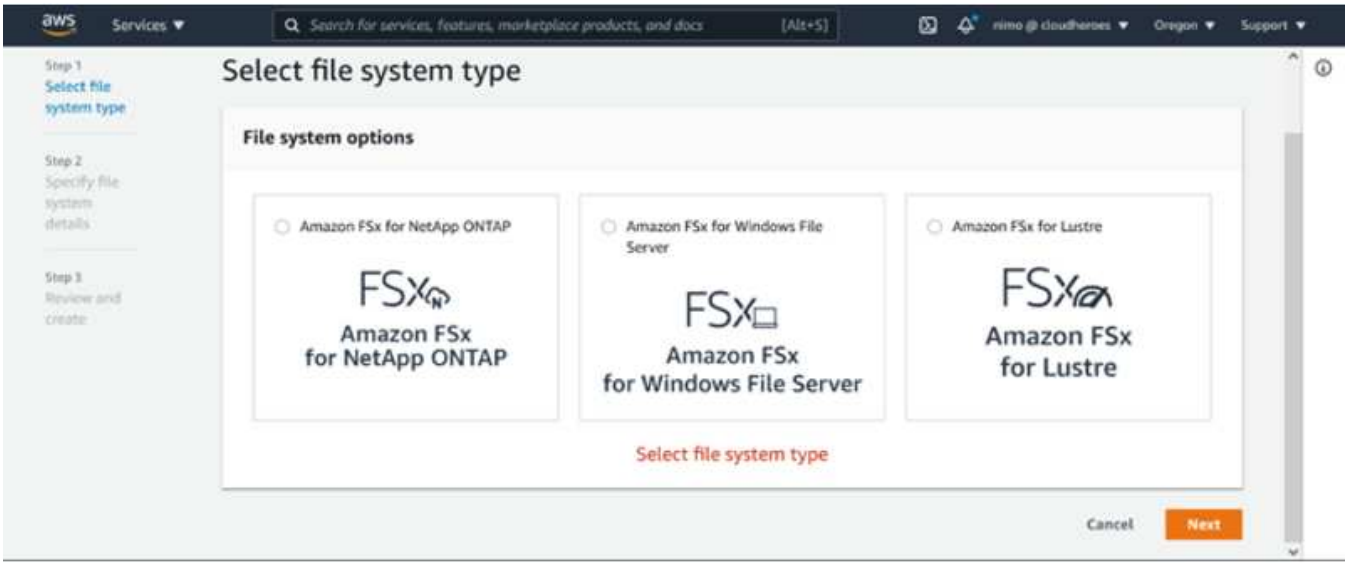
Amazon FSx ONTAP Dateifreigaben und LUNs können von VMs gemountet werden, die innerhalb der VMware SDDC-Umgebung bei VMware Cloud bei AWS erstellt wurden. Die Volumes können auch auf dem Linux-Client gemountet und auf dem Windows-Client mithilfe des NFS- oder SMB-Protokolls zugeordnet werden. Auf LUNS kann auf Linux- oder Windows-Clients als Blockgeräte zugegriffen werden, wenn sie über iSCSI gemountet sind. Amazon FSx für das NetApp ONTAP Dateisystem kann mit den folgenden Schritten schnell eingerichtet werden.

Amazon FSx ONTAP und VMware Cloud on AWS müssen sich in derselben Verfügbarkeitszone befinden, um eine bessere Leistung zu erzielen und Datenübertragungsgebühren zwischen Verfügbarkeitszonen zu vermeiden.

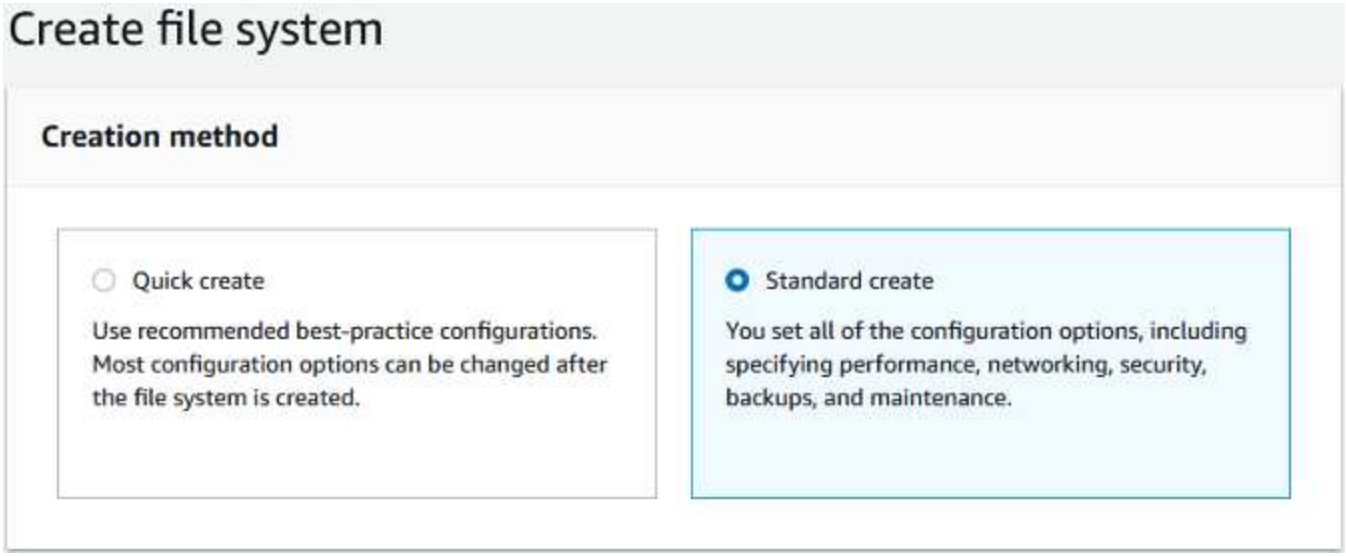
▼ **Erstellen und Mounten von Amazon FSx ONTAP -Volumes**

Führen Sie die folgenden Schritte aus, um ein Amazon FSx ONTAP Dateisystem zu erstellen und bereitzustellen:

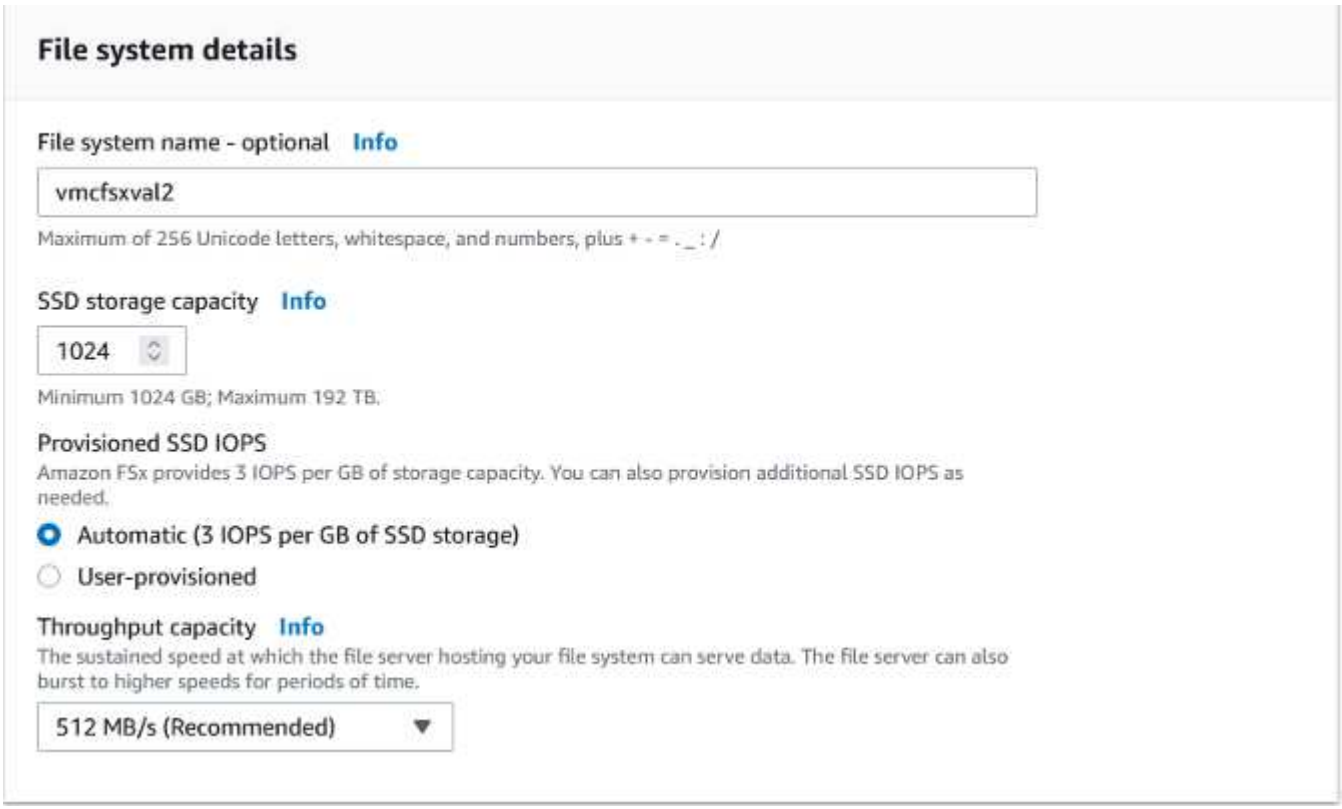
1. Öffnen Sie die"Amazon FSx Konsole" und wählen Sie „Dateisystem erstellen“, um den Assistenten zum Erstellen von Dateisystemen zu starten.
2. Wählen Sie auf der Seite „Dateisystemtyp auswählen“ die Option Amazon FSx ONTAP und anschließend Weiter aus. Die Seite „Dateisystem erstellen“ wird angezeigt.



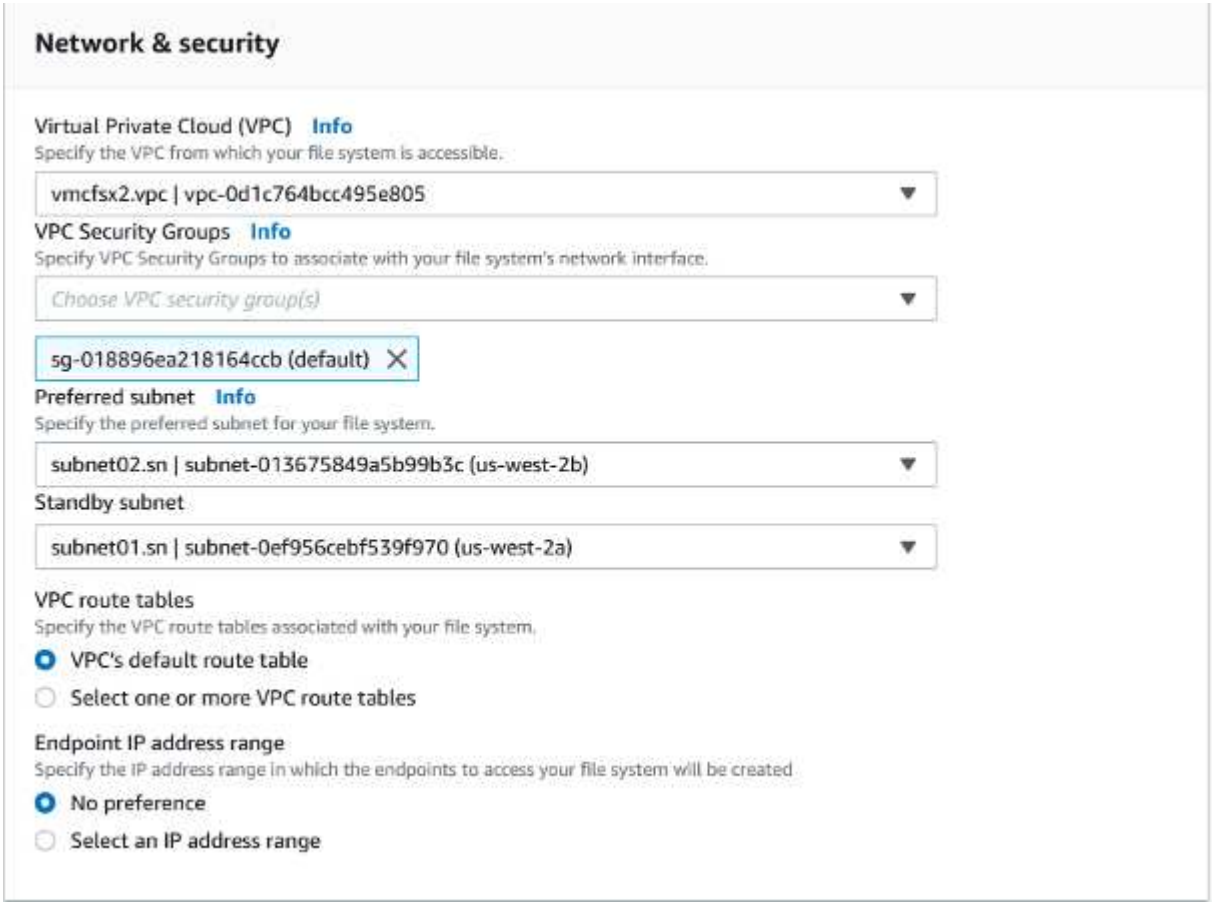
1. Wählen Sie im Abschnitt „Netzwerk“ für Virtual Private Cloud (VPC) die entsprechende VPC und die bevorzugten Subnetze zusammen mit der Routentabelle aus. In diesem Fall wird vmcfsx2.vpc aus der Dropdown-Liste ausgewählt.



1. Wählen Sie als Erstellungsmethode „Standarderstellung“ aus. Sie können auch „Schnell erstellen“ wählen, dieses Dokument verwendet jedoch die Option „Standard erstellen“.

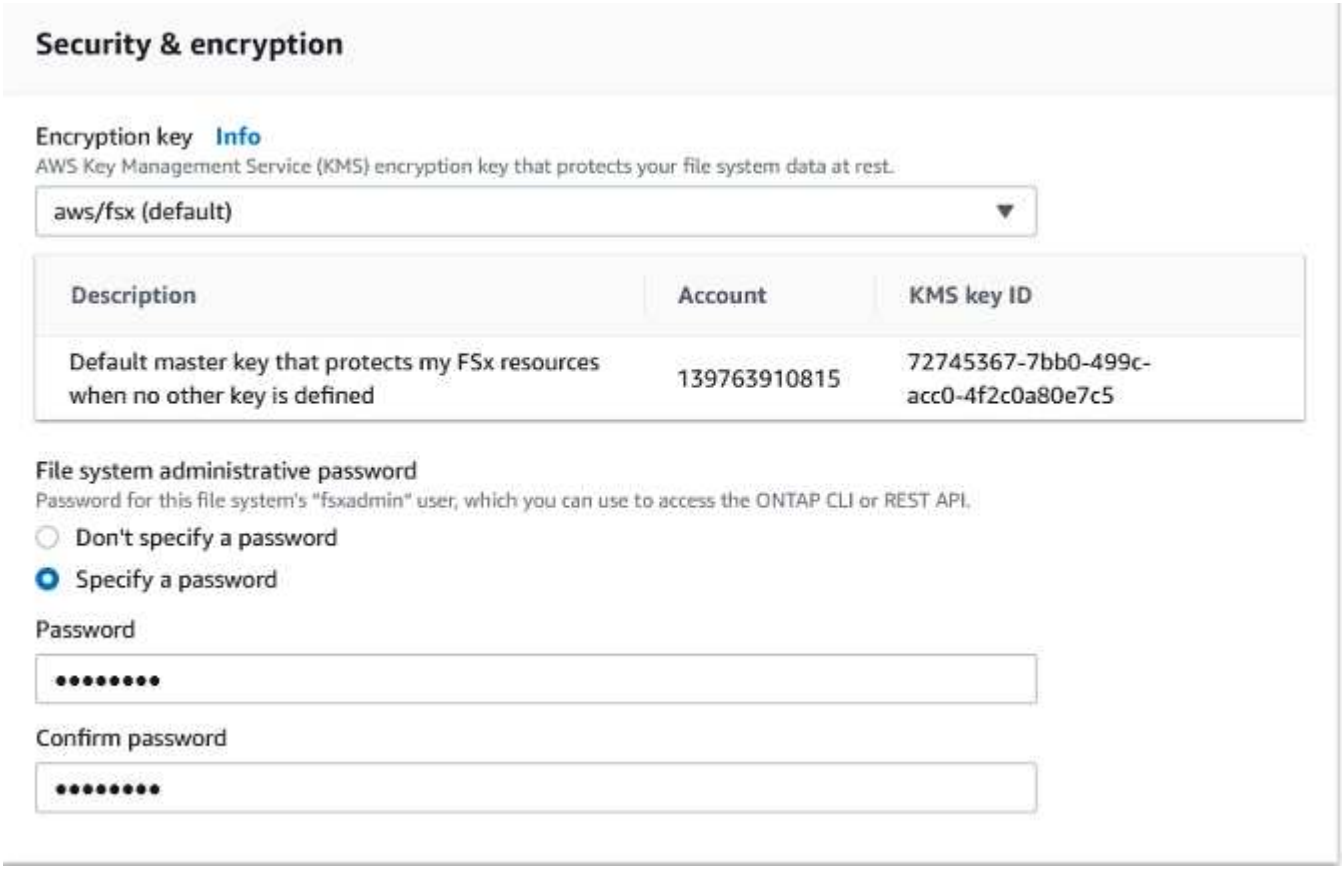


1. Wählen Sie im Abschnitt „Netzwerk“ für Virtual Private Cloud (VPC) die entsprechende VPC und die bevorzugten Subnetze zusammen mit der Routentabelle aus. In diesem Fall wird vmcfsx2.vpc aus der Dropdown-Liste ausgewählt.

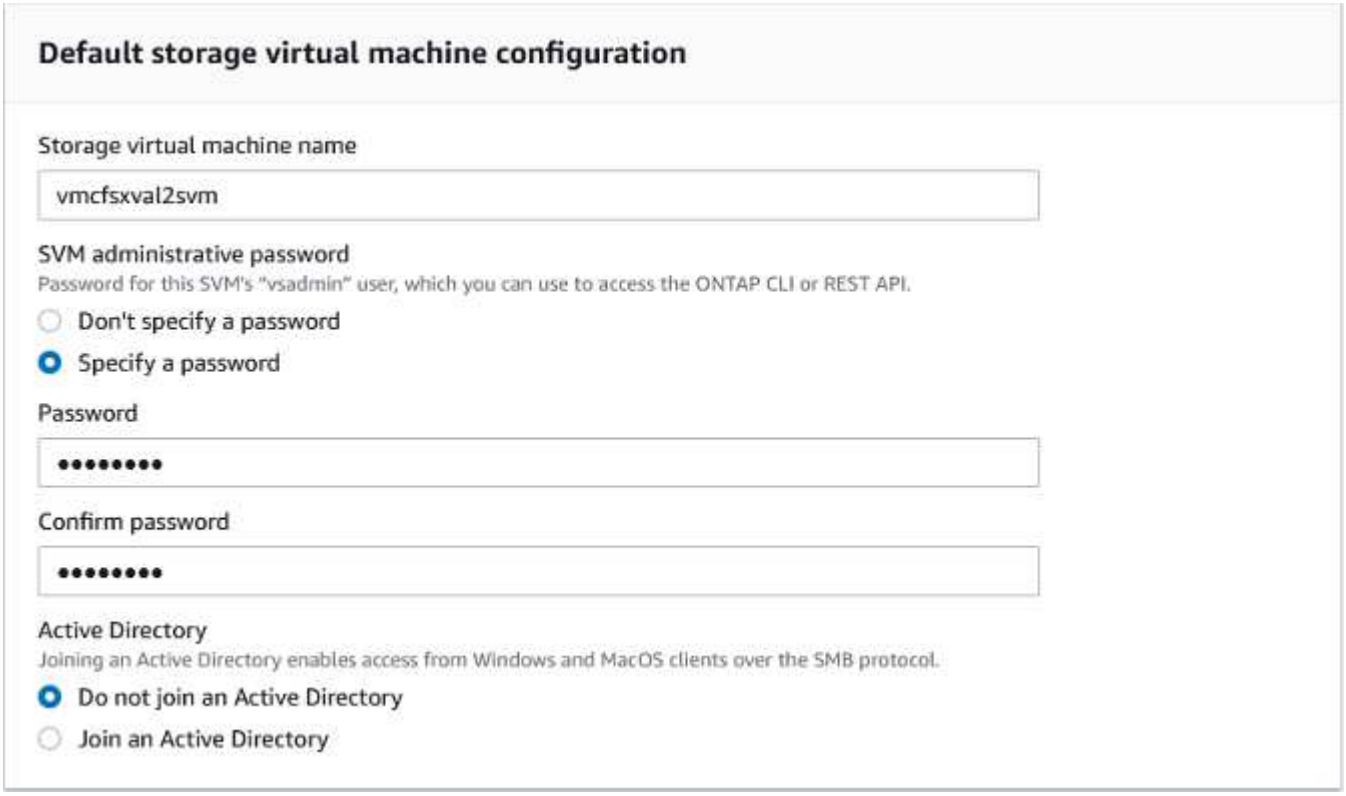


Wählen Sie im Abschnitt „Netzwerk“ für Virtual Private Cloud (VPC) die entsprechende VPC und die bevorzugten Subnetze zusammen mit der Routentabelle aus. In diesem Fall wird vmcfsx2.vpc aus der Dropdown-Liste ausgewählt.

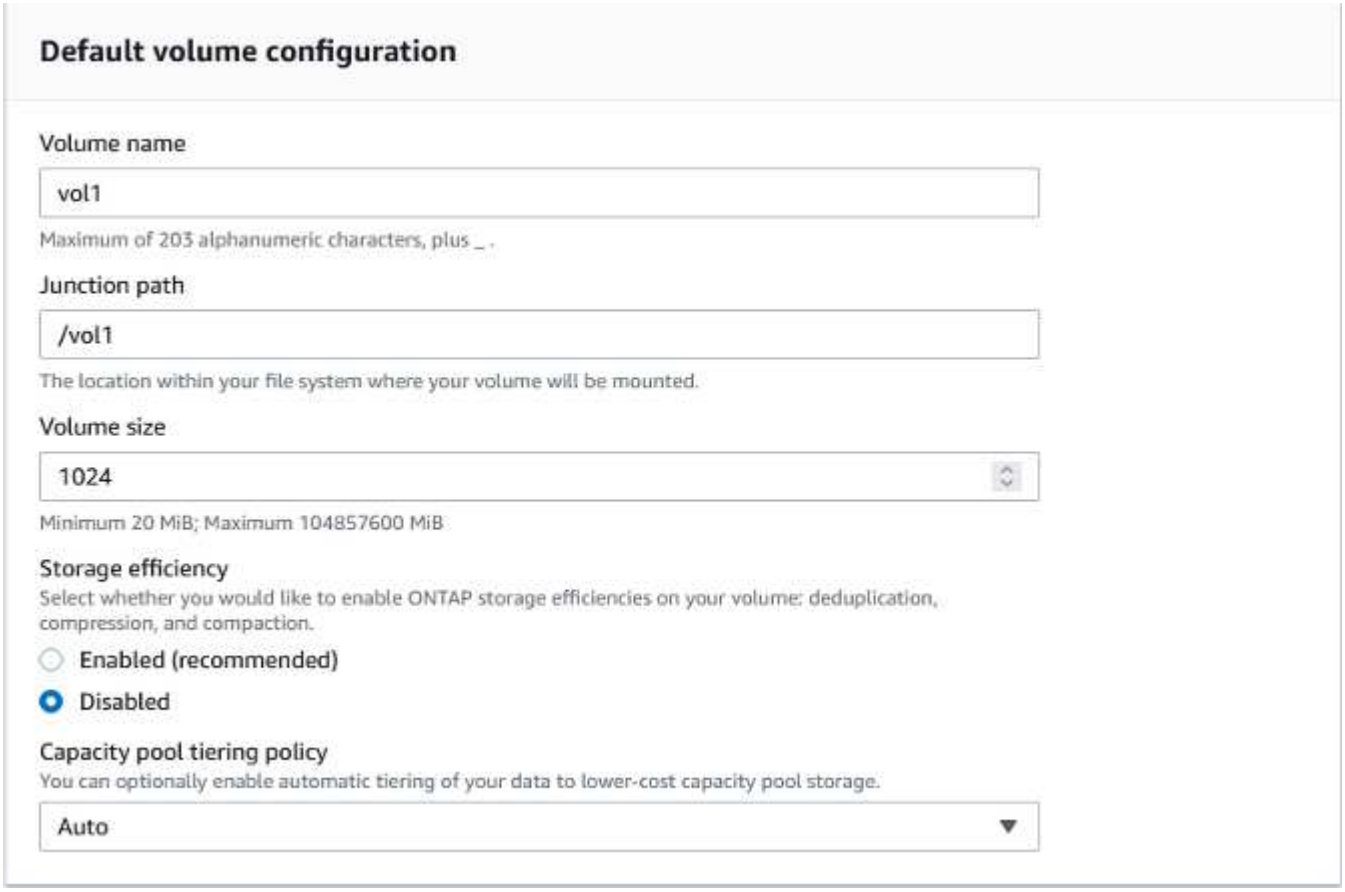
1. Wählen Sie im Abschnitt „Sicherheit und Verschlüsselung“ für den Verschlüsselungsschlüssel den Verschlüsselungsschlüssel des AWS Key Management Service (AWS KMS) aus, der die ruhenden Daten des Dateisystems schützt. Geben Sie als Administratorkennwort des Dateisystems ein sicheres Kennwort für den Benutzer fsxadmin ein.



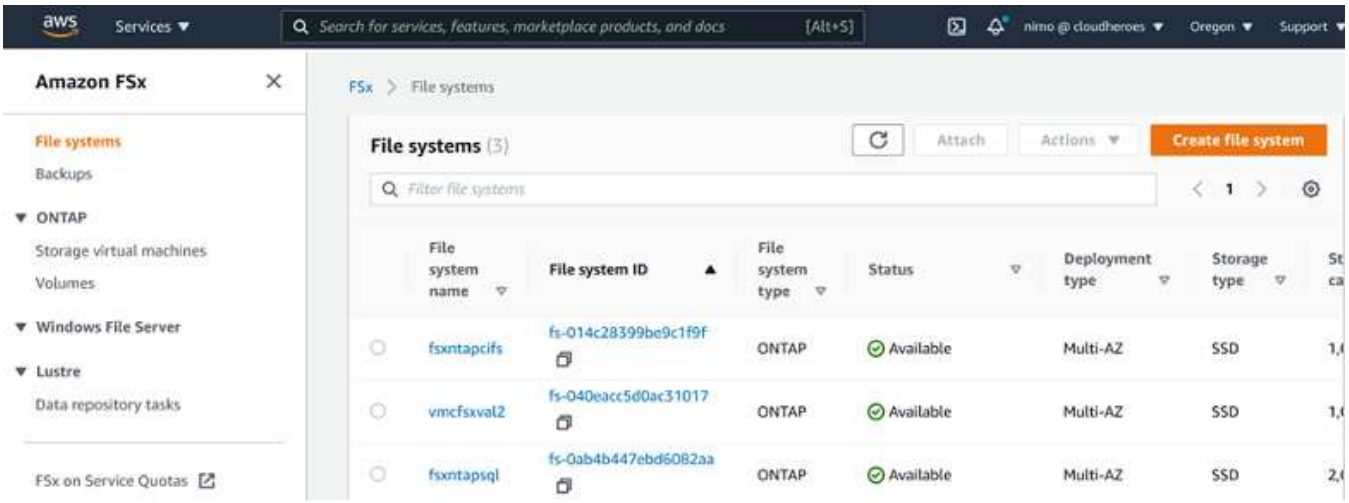
1. Geben Sie in der virtuellen Maschine das Kennwort an, das mit vsadmin für die Verwaltung von ONTAP mithilfe von REST-APIs oder der CLI verwendet werden soll. Wenn kein Passwort angegeben wird, kann ein fsxadmin-Benutzer zur Verwaltung der SVM verwendet werden. Stellen Sie im Abschnitt „Active Directory“ sicher, dass Sie Active Directory mit der SVM verknüpfen, um SMB-Freigaben bereitzustellen. Geben Sie im Abschnitt „Standardkonfiguration der virtuellen Speichermaschine“ einen Namen für den Speicher in dieser Validierung an. SMB-Freigaben werden mithilfe einer selbstverwalteten Active Directory-Domäne bereitgestellt.

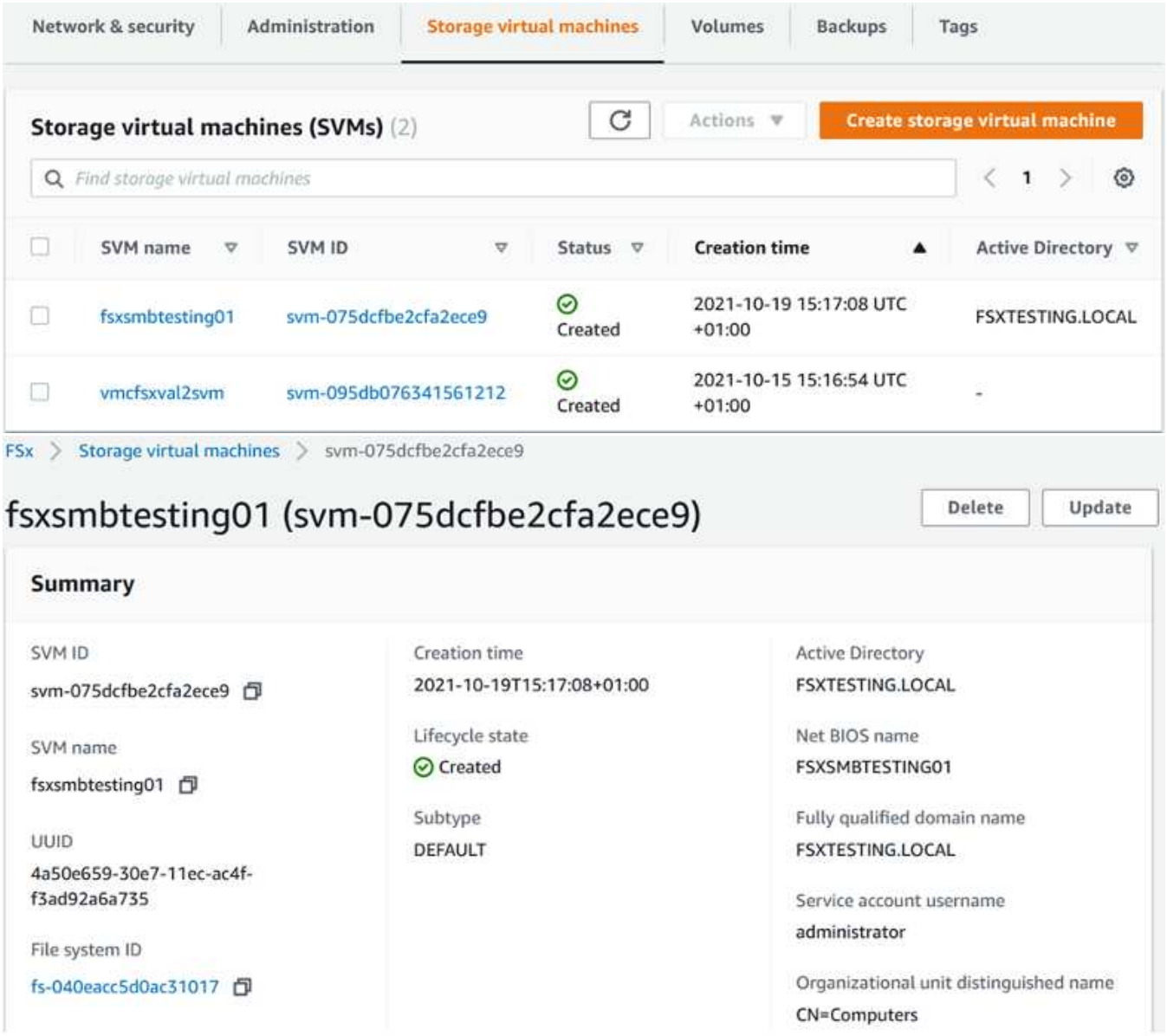


1. Geben Sie im Abschnitt „Standardvolume-Konfiguration“ den Volumenamen und die Volumegröße an. Dies ist ein NFS-Volume. Wählen Sie für die Speichereffizienz „Aktiviert“, um die ONTAP Speichereffizienzfunktionen (Komprimierung, Deduplizierung und Kompaktierung) zu aktivieren, oder „Deaktiviert“, um sie zu deaktivieren.



1. Überprüfen Sie die Dateisystemkonfiguration, die auf der Seite „Dateisystem erstellen“ angezeigt wird.
2. Klicken Sie auf „Dateisystem erstellen“.





Weitere Informationen finden Sie unter"Erste Schritte mit Amazon FSx ONTAP" .

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

1. Öffnen Sie die"Amazon FSx Konsole" .
2. Wählen Sie im linken Navigationsbereich „Dateisysteme“ und dann 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“ aus.
5. Das Dialogfeld „Volume erstellen“ wird angezeigt.

Zu Demozwecken wird in diesem Abschnitt ein NFS-Volume erstellt, das problemlos auf VMs gemountet werden kann, die in der VMware Cloud auf AWS ausgeführt werden. nfsdemovol01 wird wie unten dargestellt erstellt:



▼ **Mounten Sie das FSx ONTAP -Volume auf dem Linux-Client**

Um das im vorherigen Schritt erstellte FSx ONTAP Volume von den Linux-VMs innerhalb von VMC auf AWS SDDC zu mounten, führen Sie die folgenden Schritte aus:

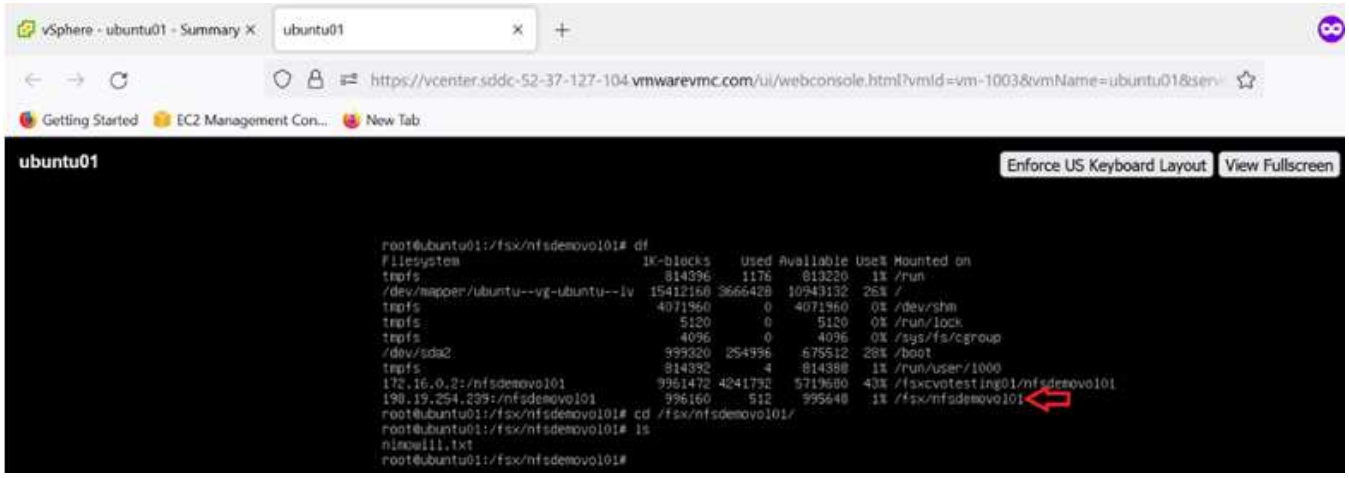
1. Stellen Sie eine Verbindung zur angegebenen Linux-Instanz her.
2. Öffnen Sie mit Secure Shell (SSH) ein Terminal auf der Instanz und melden Sie sich mit den entsprechenden Anmeldeinformationen an.
3. Erstellen Sie mit dem folgenden Befehl ein Verzeichnis für den Einhängepunkt des Datenträgers:

```
 $ sudo mkdir /fsx/nfsdemovol01
. Hängen Sie das Amazon FSx ONTAP NFS-Volume in das Verzeichnis ein,
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 nach der Ausführung den Befehl df aus, um die Bereitstellung zu validieren.



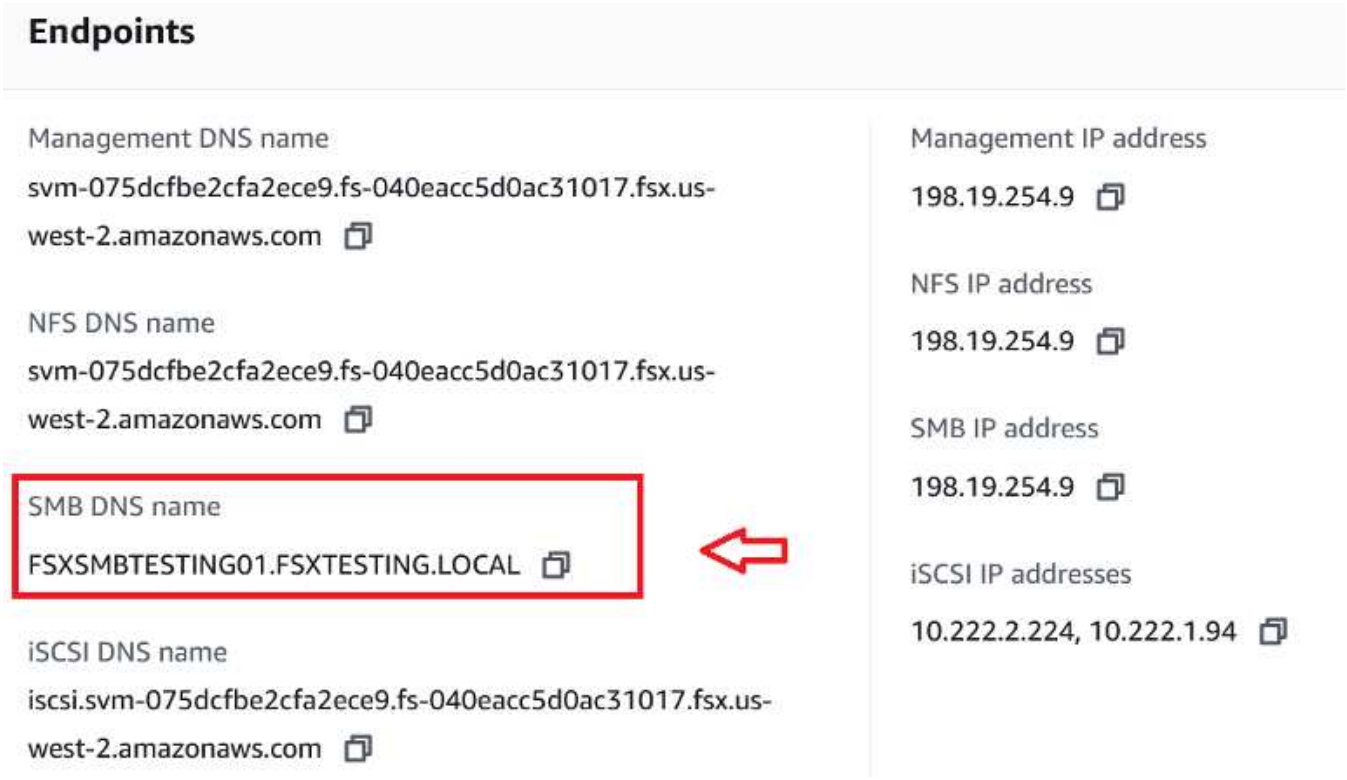
Mounten Sie das FSx ONTAP -Volume auf dem Linux-Client

▼ **Anhängen von FSx ONTAP Volumes an Microsoft Windows-Clients**

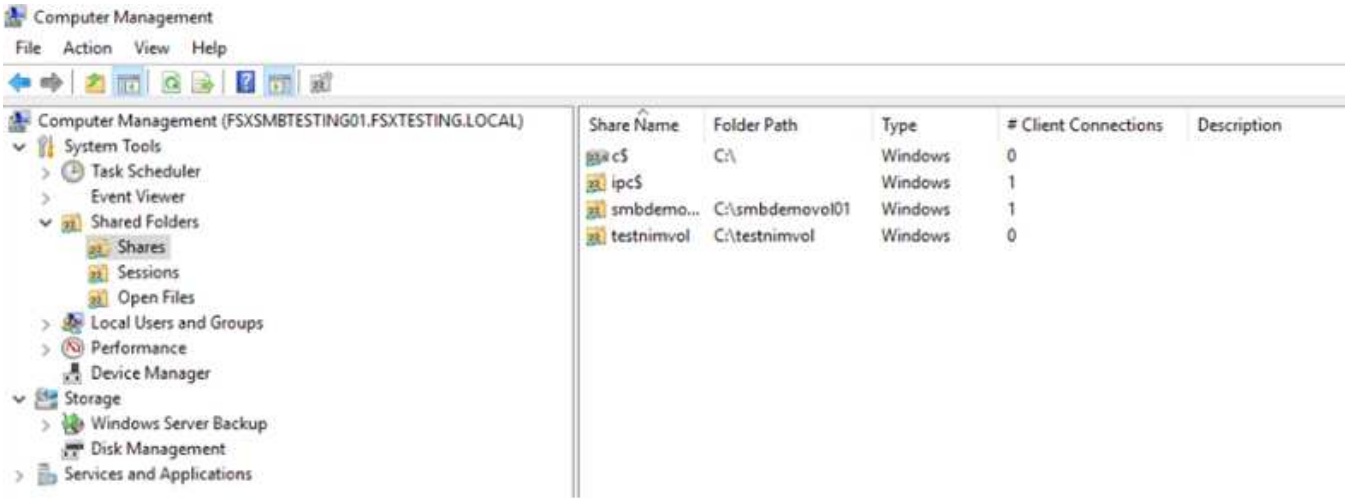
Zum Verwalten und Zuordnen von Dateifreigaben auf einem Amazon FSx Dateisystem muss die GUI „Shared Folders“ verwendet werden.

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

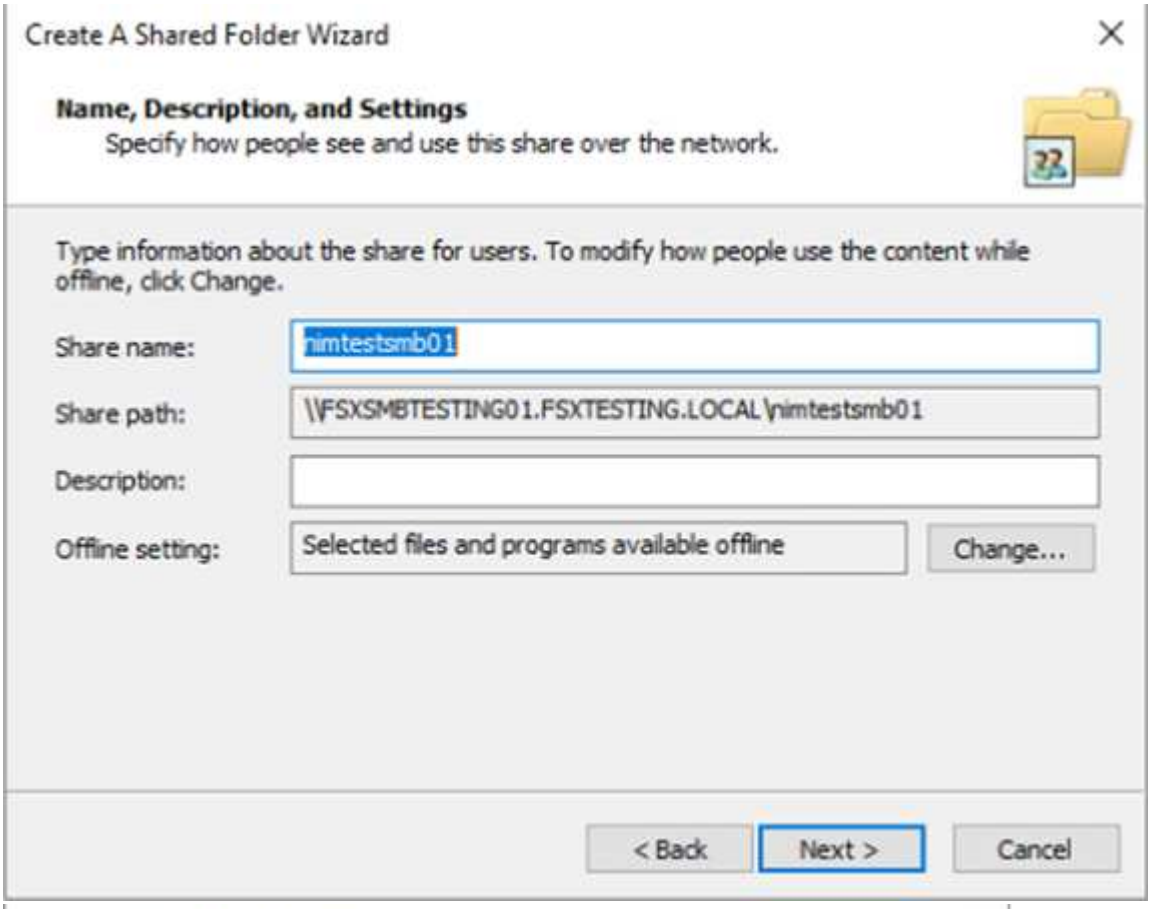
ⓘ Um den DNS-Namen der SVM auf der Amazon FSx Konsole zu finden, wählen Sie „Storage Virtual Machines“, wählen Sie „SVM“ und scrollen Sie dann nach unten zu „Endpoints“, um den SMB-DNS-Namen zu finden. Klicken Sie auf OK. Das Amazon FSx Dateisystem wird in der Liste der freigegebenen Ordner angezeigt.



1. Wählen Sie im Tool „Freigegebene Ordner“ im linken Bereich „Freigaben“ aus, um die aktiven Freigaben für das Amazon FSx Dateisystem anzuzeigen.



1. Wählen Sie nun eine neue Freigabe aus und schließen Sie den Assistenten „Freigegebenen Ordner erstellen“ ab.

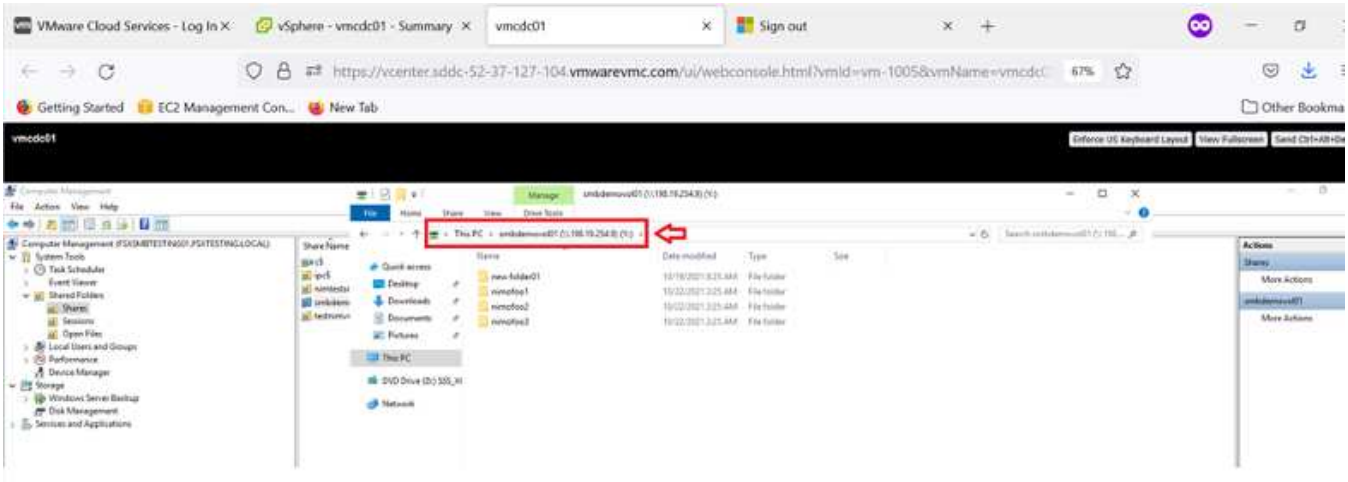




Weitere Informationen zum Erstellen und Verwalten von SMB-Freigaben auf einem Amazon FSx Dateisystem finden Sie unter"Erstellen von SMB-Freigaben" .

1. Nachdem die Verbindung hergestellt ist, kann die SMB-Freigabe angeschlossen und für

Anwendungsdaten verwendet werden. Kopieren Sie hierzu den Freigabepfad und verwenden Sie die Option „Netzlaufwerk zuordnen“, um das Volume auf der VM zu mounten, die auf VMware Cloud auf dem AWS SDDC ausgeführt wird.



▼ **Verbinden Sie ein FSx ONTAP LUN über iSCSI mit einem Host**

Verbinden Sie ein FSx ONTAP LUN über iSCSI mit einem Host

Der iSCSI-Verkehr für FSx durchläuft das VMware Transit Connect/AWS Transit Gateway über die im vorherigen Abschnitt angegebenen Routen. Um eine LUN in Amazon FSx ONTAP zu konfigurieren, folgen Sie der Dokumentation"hier," .

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

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

▼ **Bereitstellen einer LUN in FSx ONTAP:**

1. Greifen Sie über den Verwaltungsport des FSx für das ONTAP -Dateisystem auf die NetApp ONTAP CLI zu.
2. Erstellen Sie die LUNs mit der erforderlichen Größe, wie in der Größenausgabe 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 igroups, um zu steuern, welche Hosts Zugriff auf bestimmte LUNs haben.

```
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 mit dem folgenden Befehl den igroups 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
```

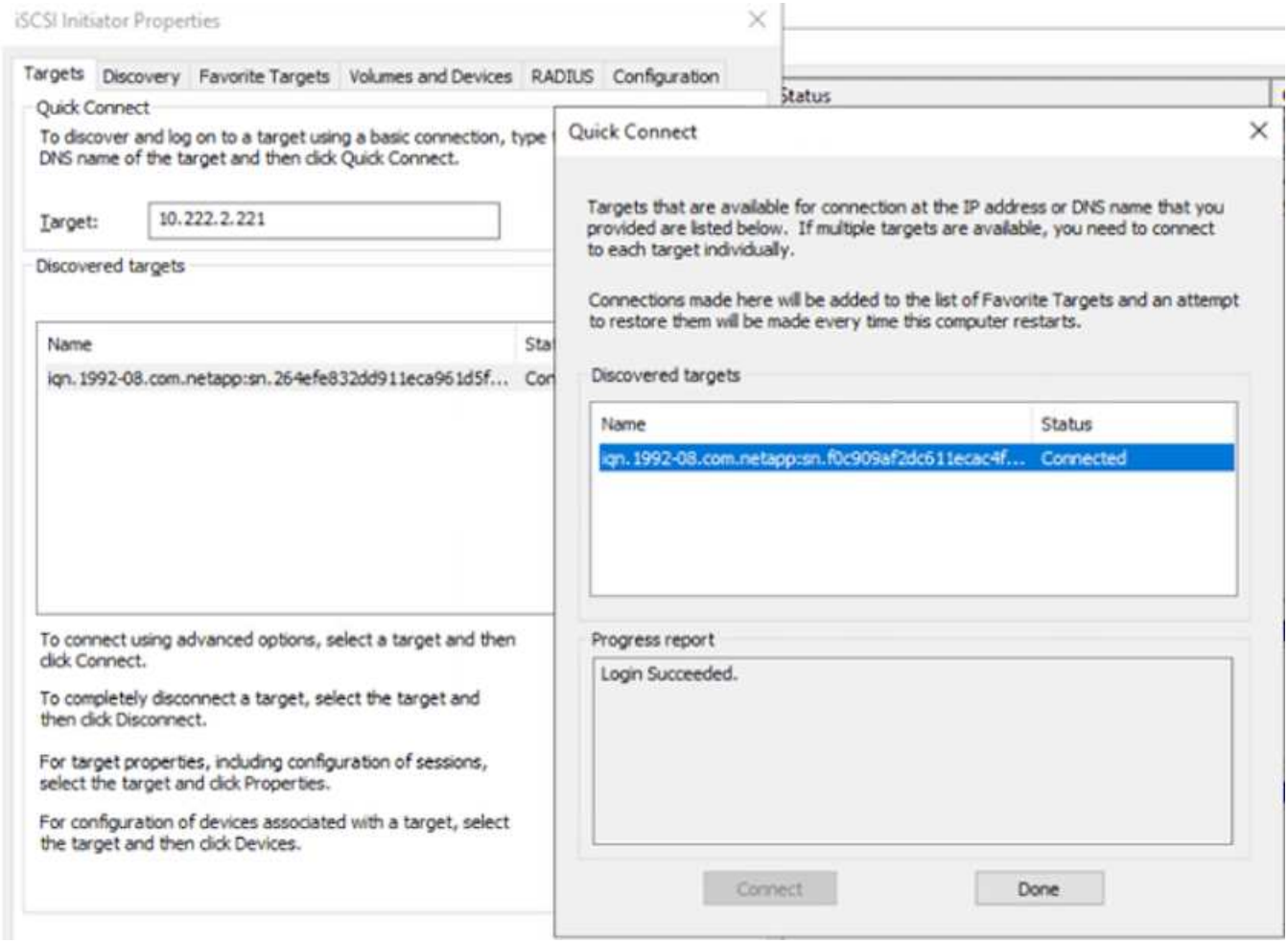
Es wurden zwei Einträge angezeigt.

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

Führen Sie die folgenden Schritte aus, um die neue LUN mit einem Windows-Host zu verbinden, der sich auf VMware Cloud auf AWS SDDC befindet:

1. RDP zur Windows-VM, die auf der VMware Cloud auf AWS SDDC gehostet wird.
2. Navigieren Sie zu Server Manager > Dashboard > Tools > iSCSI-Initiator, um das Dialogfeld „Eigenschaften des iSCSI-Initiators“ zu öffnen.
3. Klicken Sie auf der Registerkarte „Erkennung“ 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 dann „Diese Verbindung beim Start des Computers automatisch wiederherstellen“ oder „Diese Verbindung zur Liste der bevorzugten Ziele hinzufügen“. Klicken Sie auf „Erweitert“.

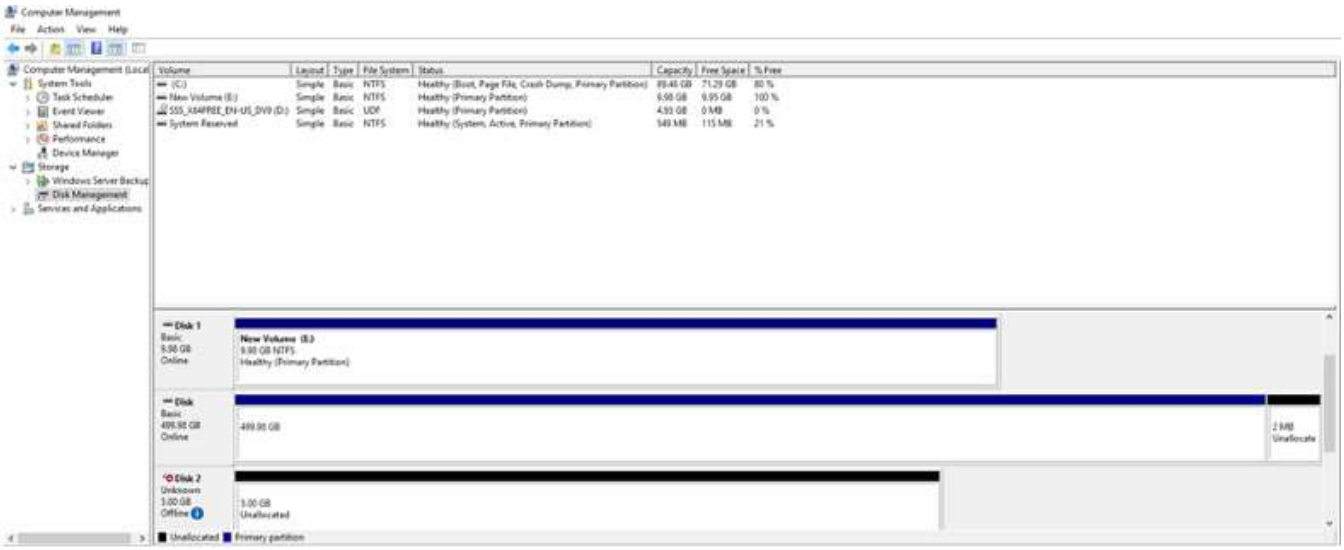
Der Windows-Host muss über eine iSCSI-Verbindung zu jedem Knoten im Cluster verfügen. Das native DSM wählt die besten zu verwendenden Pfade aus.



LUNs auf der Storage Virtual Machine (SVM) werden dem Windows-Host als Datenträger angezeigt. Alle neu hinzugefügten Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen erneuten Scan aus, um die Datenträger zu ermitteln, indem Sie die folgenden Schritte ausführen:

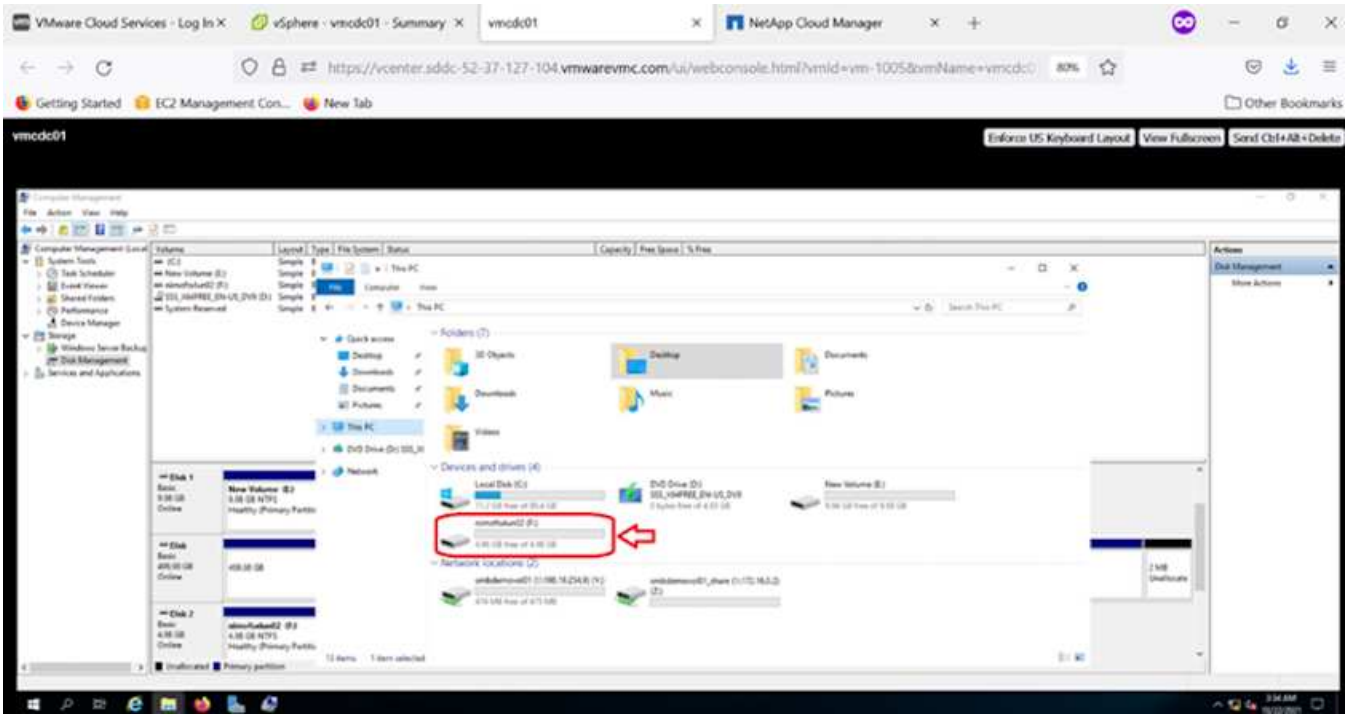
1. Öffnen Sie das Windows-Dienstprogramm „Computerverwaltung“: Start > Verwaltung > Computerverwaltung.

2. Erweitern Sie den Knoten „Speicher“ im Navigationsbaum.
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, verfügt diese über keine Partition oder kein Dateisystem. Initialisieren Sie die LUN und formatieren Sie die LUN optional mit einem Dateisystem, indem Sie die folgenden Schritte ausführen:

1. Starten Sie die Windows-Datenträgerverwaltung.
2. Klicken Sie mit der rechten Maustaste auf die LUN und wählen Sie dann den erforderlichen Datenträger- oder Partitionstyp aus.
3. Folgen Sie den Anweisungen des Assistenten. In diesem Beispiel ist Laufwerk F: gemountet.



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenverwaltungslösung, die auf der ONTAP -Speichersoftware von NetApp basiert und nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar ist.

Es handelt sich um eine softwaredefinierte Version von ONTAP , die Cloud-nativen Speicher nutzt. Dadurch können Sie in der Cloud und vor Ort dieselbe Speichersoftware verwenden und müssen Ihr IT-Personal nicht mehr in völlig neuen Methoden zur Verwaltung Ihrer Daten schulen.

CVO bietet Kunden die Möglichkeit, Daten nahtlos vom Edge zum Rechenzentrum, in die Cloud und zurück zu verschieben und so Ihre Hybrid Cloud zusammenzuführen – alles verwaltet über eine zentrale Verwaltungskonsole, den NetApp Cloud Manager.

CVO bietet von Haus aus extreme Leistung und erweiterte Datenverwaltungsfunktionen, um selbst Ihre anspruchsvollsten Anwendungen in der Cloud zu erfüllen

Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher

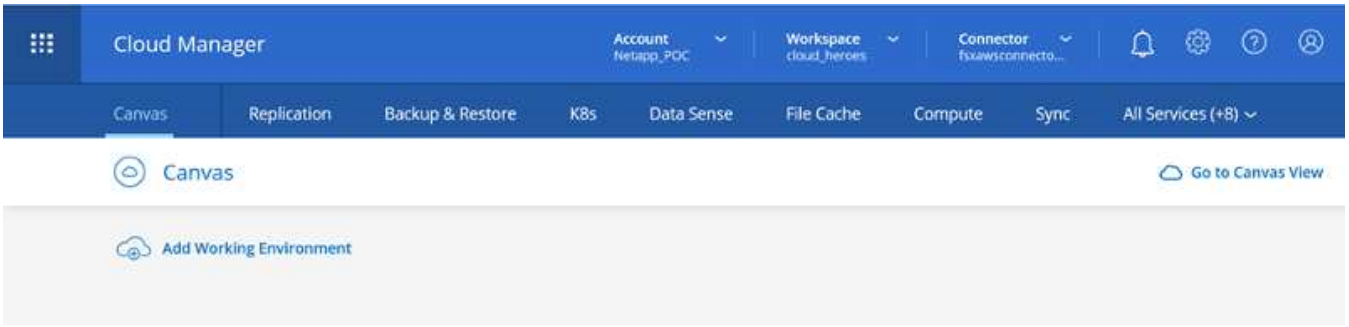
▼ **Neue Cloud Volumes ONTAP Instanz in AWS bereitstellen (selbst machen)**

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 gemountet werden, und auf LUNS kann auf Linux- oder Windows-Clients als Blockgeräte zugegriffen werden, wenn sie über iSCSI gemountet werden, da Cloud Volumes ONTAP die Protokolle iSCSI, SMB und NFS unterstützt. Cloud Volumes ONTAP -Volumes können in wenigen einfachen Schritten eingerichtet werden.

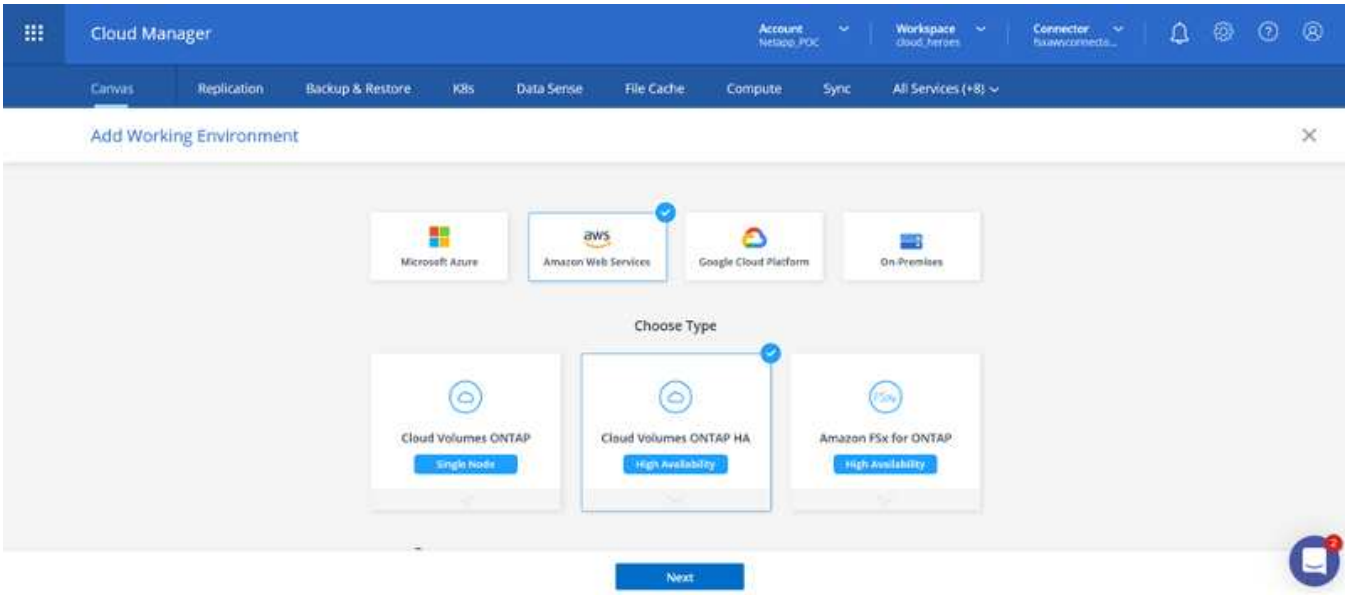
Um Volumes aus einer lokalen Umgebung zur Notfallwiederherstellung oder Migration in die Cloud zu replizieren, stellen Sie eine Netzwerkverbindung zu AWS her, entweder über ein Site-to-Site-VPN oder DirectConnect. Das Replizieren von Daten von lokalen Standorten auf Cloud Volumes ONTAP fällt nicht in den Geltungsbereich dieses Dokuments. Informationen zum Replizieren von Daten zwischen lokalen und Cloud Volumes ONTAP Systemen finden Sie unter"Einrichten der Datenreplikation zwischen Systemen" .

Mit dem "Cloud Volumes ONTAP Sizer" lassen sich die Cloud Volumes ONTAP Instanzen präzise dimensionieren. Außerdem dient die Überwachung der On-Premises-Performance als Eingabe für den Cloud Volumes ONTAP sizer.

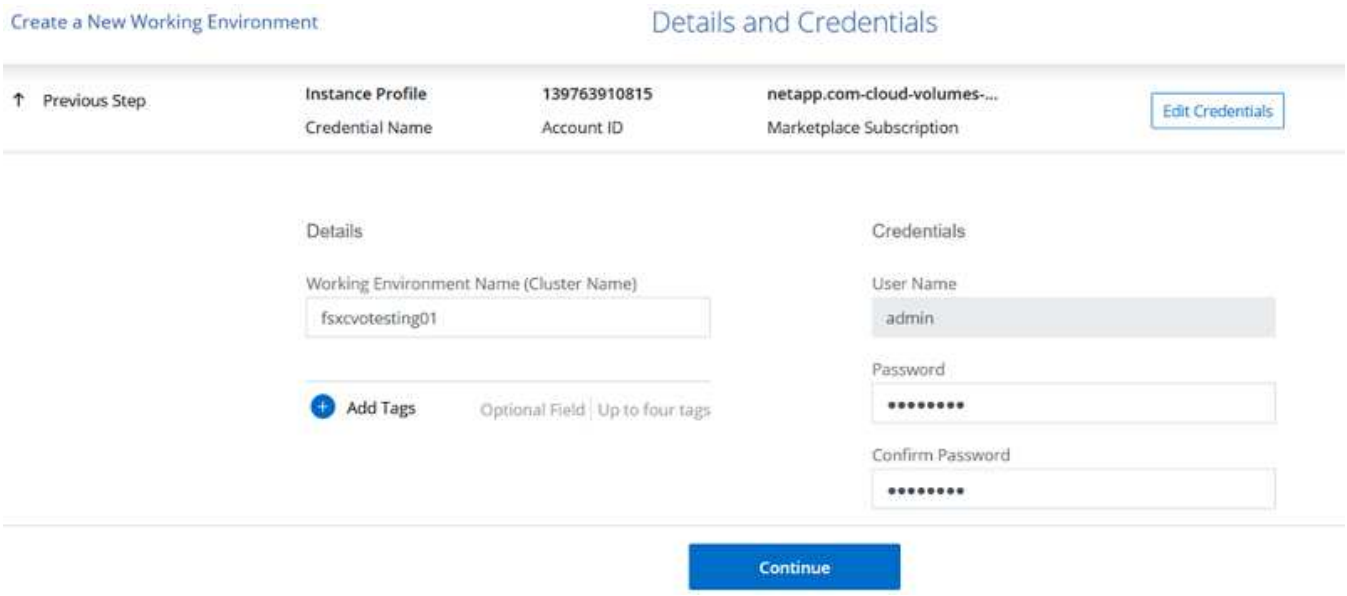
1. Melden Sie sich bei NetApp Cloud Central an. Der Fabric View-Bildschirm wird angezeigt. Suchen Sie die Registerkarte „Cloud Volumes ONTAP“ und wählen Sie „Gehe zu Cloud Manager“ aus. Nachdem Sie sich angemeldet haben, wird der Canvas-Bildschirm angezeigt.



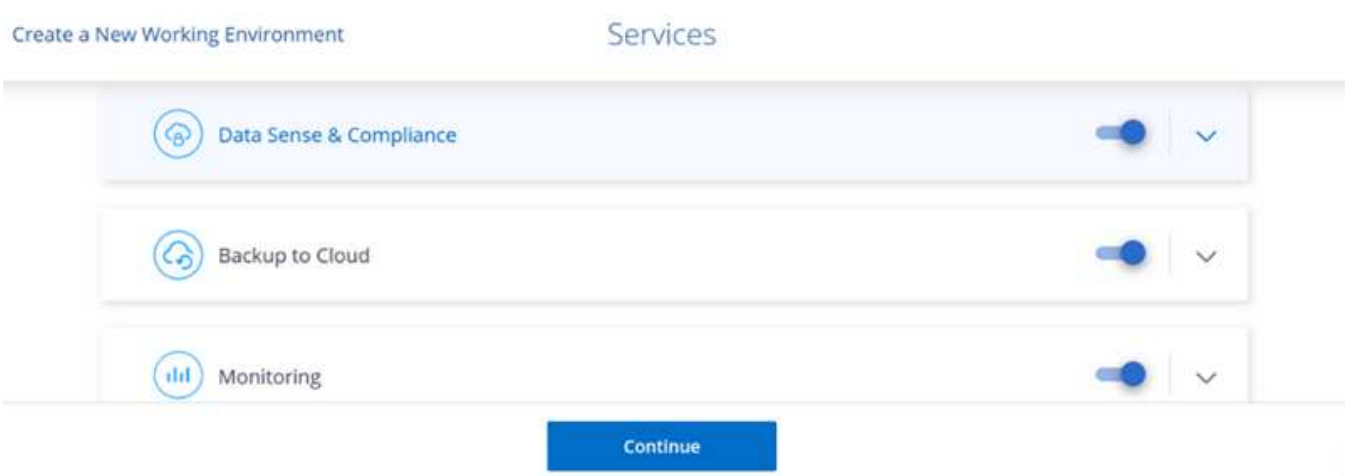
1. Klicken Sie auf der Cloud Manager-Startseite auf „Arbeitsumgebung hinzufügen“ und wählen Sie dann AWS als Cloud und den Typ der Systemkonfiguration aus.



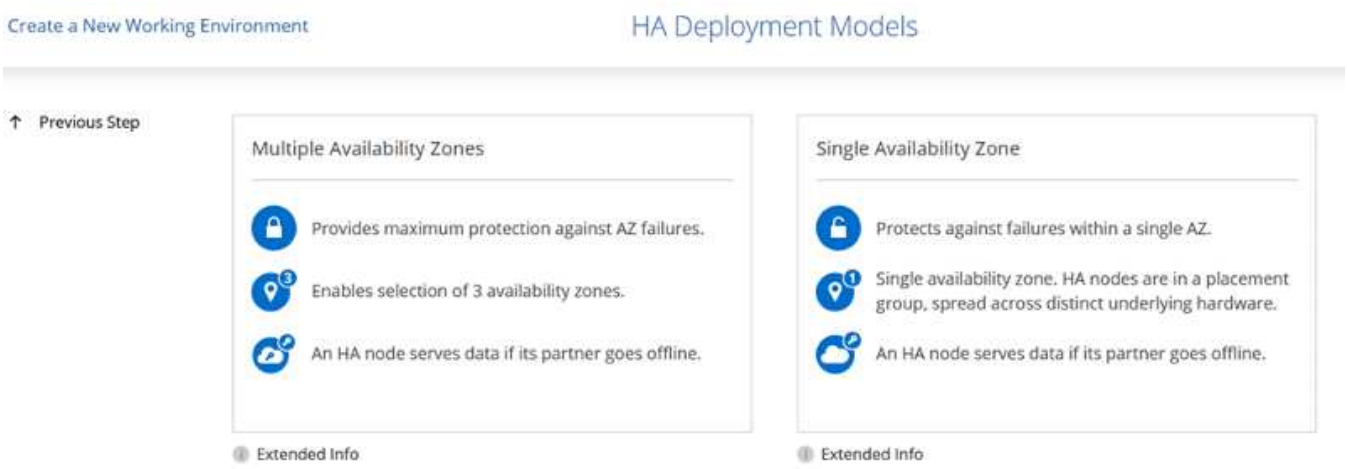
1. Geben Sie die Details der zu erstellenden Umgebung an, einschließlich Umgebungsname und Administratoranmeldeinformationen. Klicken Sie auf „Weiter“.



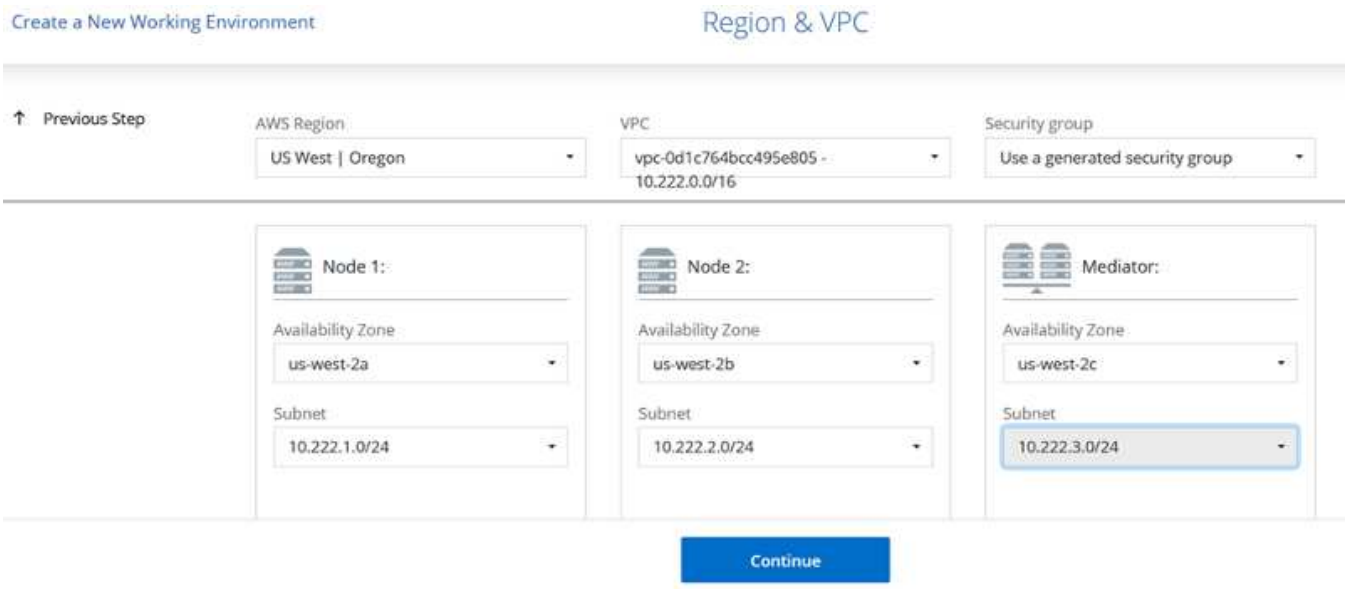
1. Auswahl der Add-on-Services für das Cloud Volumes ONTAP Deployment, einschließlich NetApp Data Classification, NetApp Backup and Recovery und Data Infrastructure Insights. Anschließend wird Continue ausgewählt.



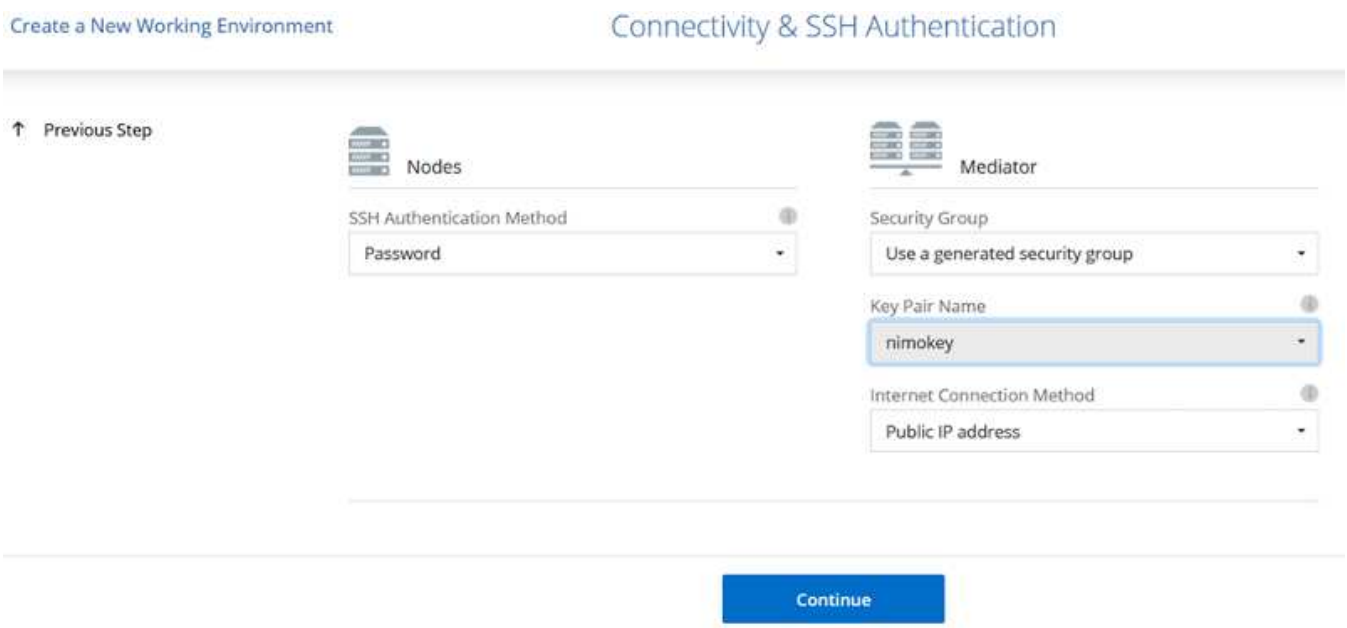
1. Wählen Sie auf der Seite „HA-Bereitstellungsmodelle“ die Konfiguration „Mehrere Verfügbarkeitszonen“ aus.



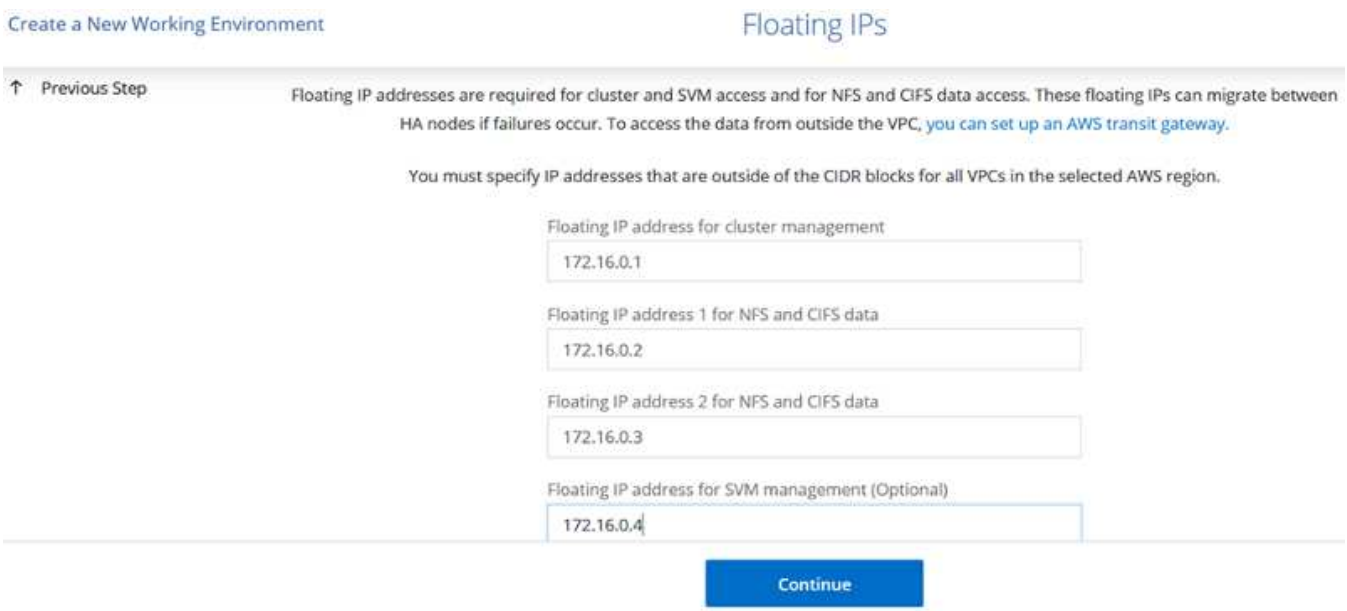
1. Geben Sie auf der Seite „Region und VPC“ die Netzwerkinformationen ein und klicken Sie dann auf „Weiter“.



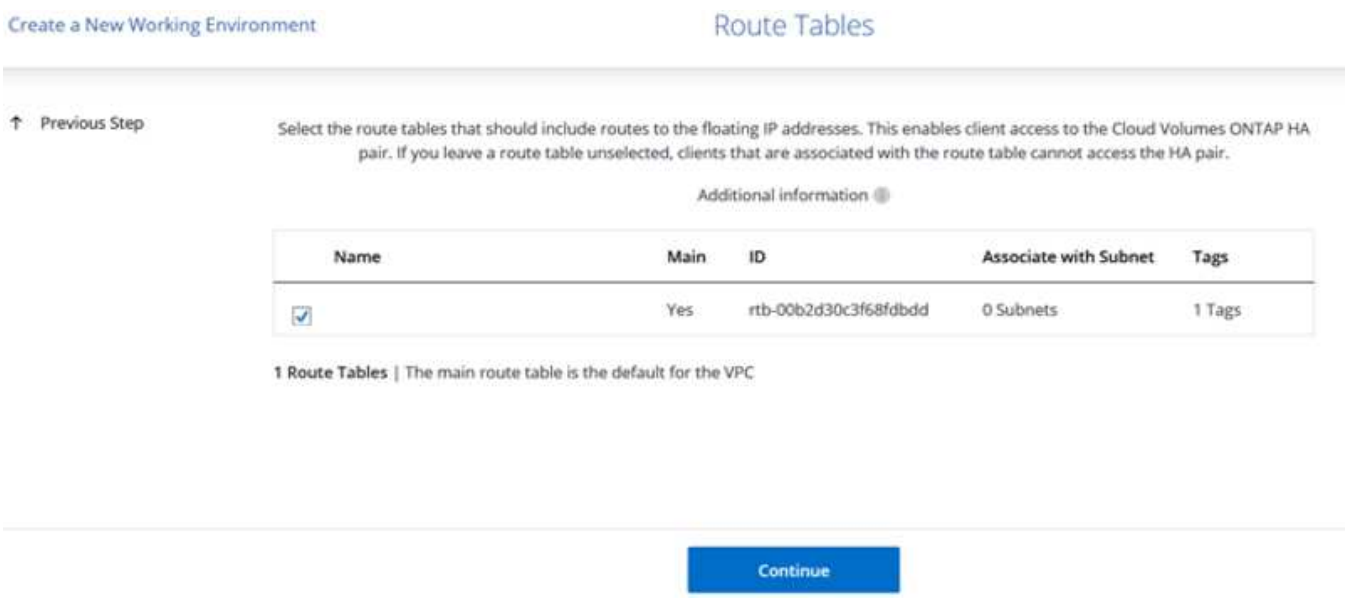
1. Wählen Sie auf der Seite „Konnektivität und SSH-Authentifizierung“ Verbindungsmethoden für das HA-Paar und den Mediator aus.



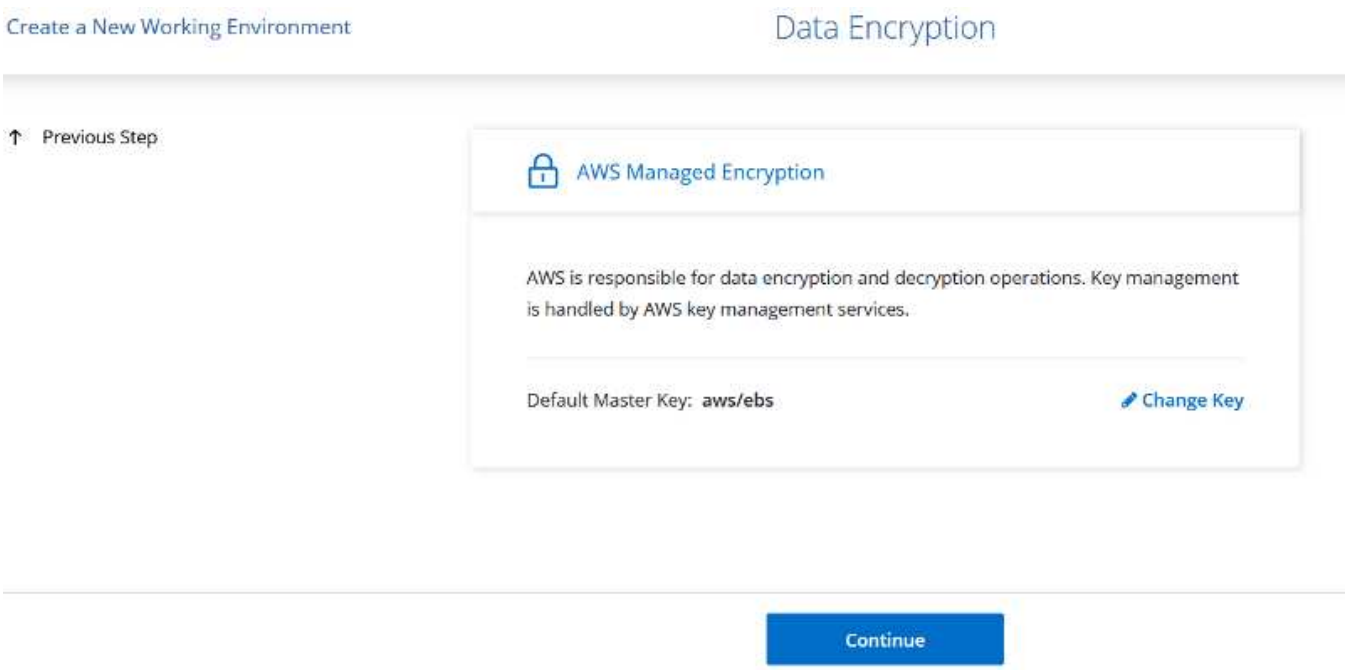
1. Geben Sie die Floating-IP-Adressen an und klicken Sie dann auf „Weiter“.



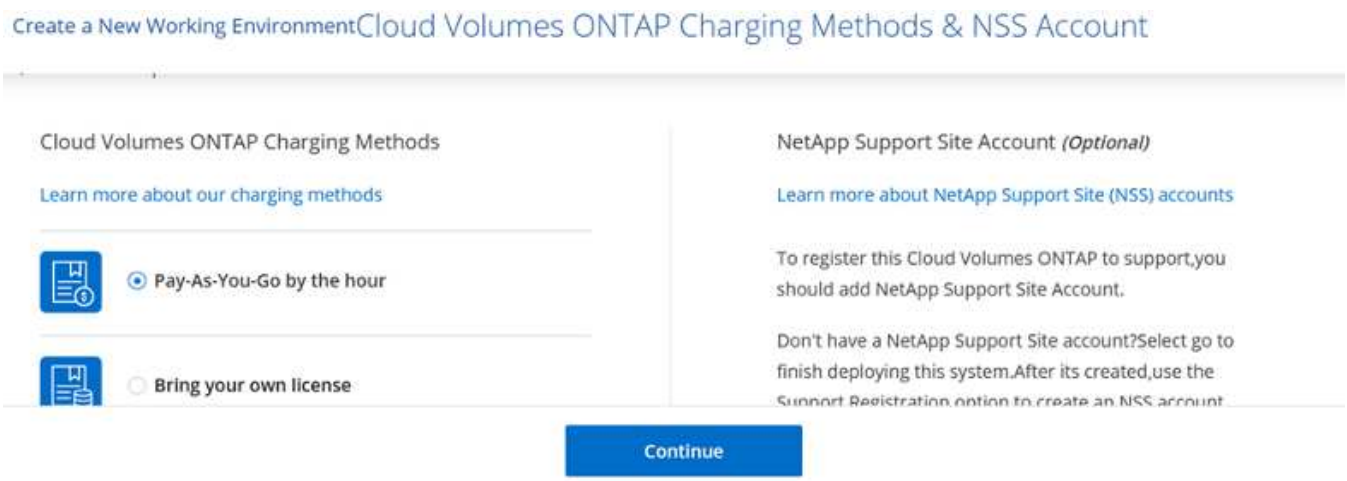
1. Wählen Sie die entsprechenden Routentabellen aus, um Routen zu den Floating-IP-Adressen einzuschließen, und klicken Sie dann auf „Weiter“.



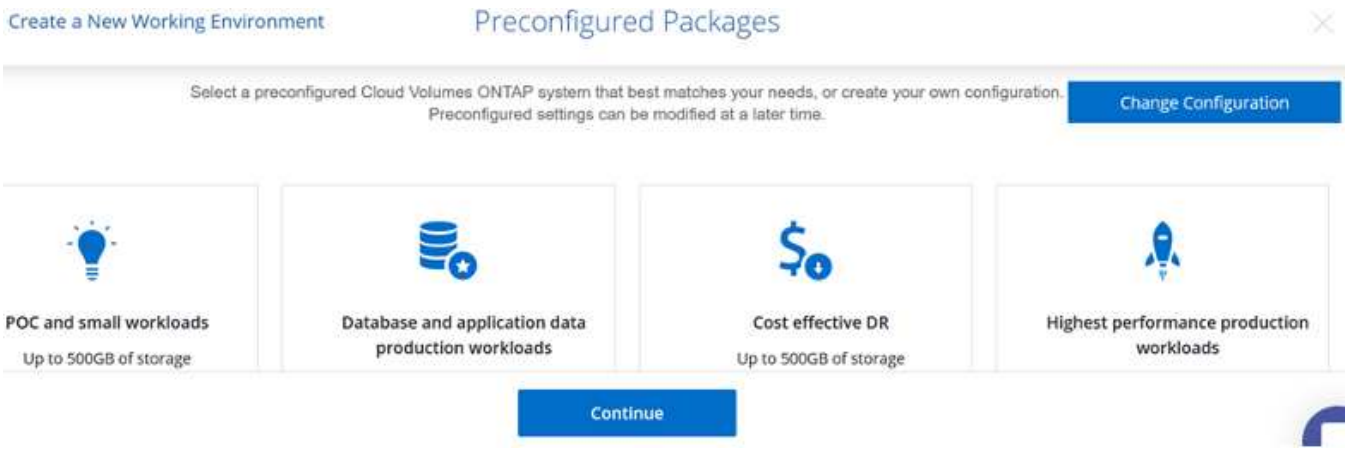
1. Wählen Sie auf der Seite „Datenverschlüsselung“ die von AWS verwaltete Verschlüsselung aus.



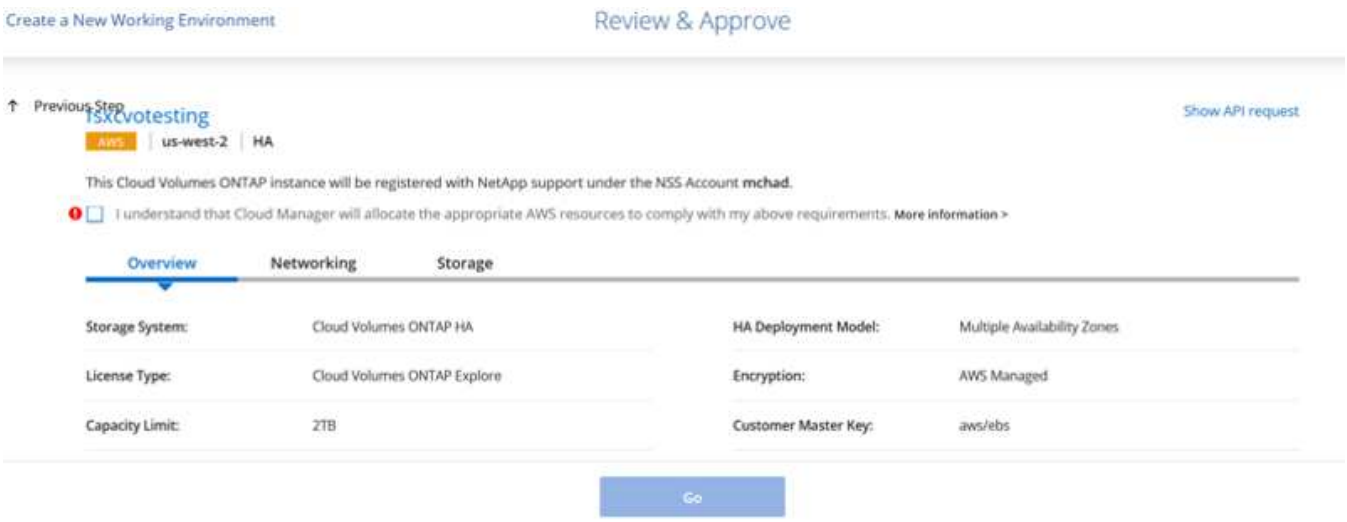
1. Wählen Sie die Lizenzoption: Pay-As-You-Go oder BYOL zur Verwendung einer vorhandenen Lizenz. In diesem Beispiel wird die Pay-As-You-Go-Option verwendet.



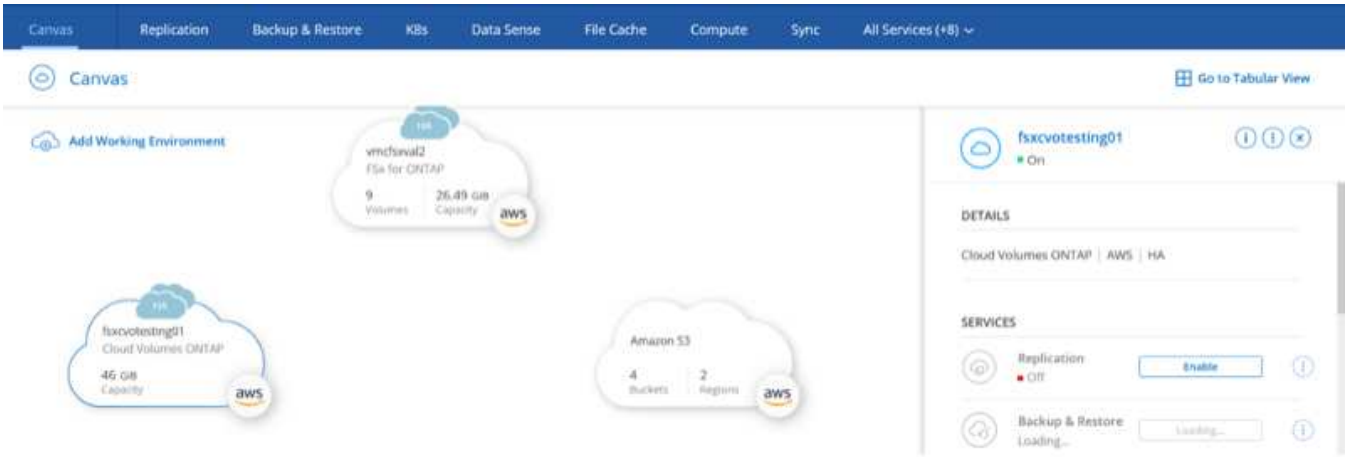
1. Wählen Sie je nach Art der Arbeitslast, die auf den VMs bereitgestellt werden soll, die in der VMware Cloud auf AWS SDDC ausgeführt werden, zwischen mehreren verfügbaren vorkonfigurierten Paketen.



1. Überprüfen und bestätigen Sie die Auswahl auf der Seite „Überprüfen und genehmigen“. Klicken Sie auf „Los“, um die Cloud Volumes ONTAP -Instanz zu erstellen.

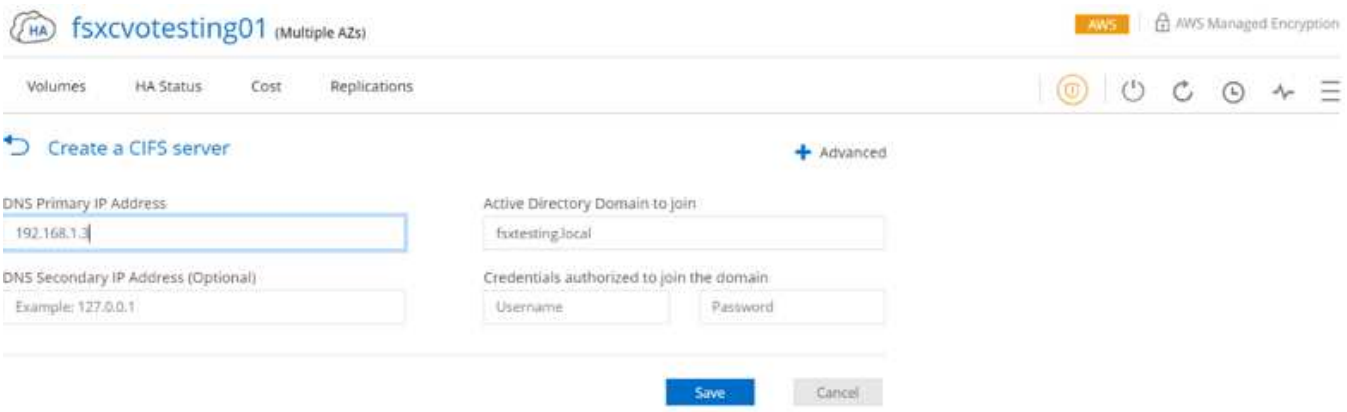


1. Nachdem Cloud Volumes ONTAP bereitgestellt wurde, wird es in den Arbeitsumgebungen auf der Canvas-Seite aufgeführt.

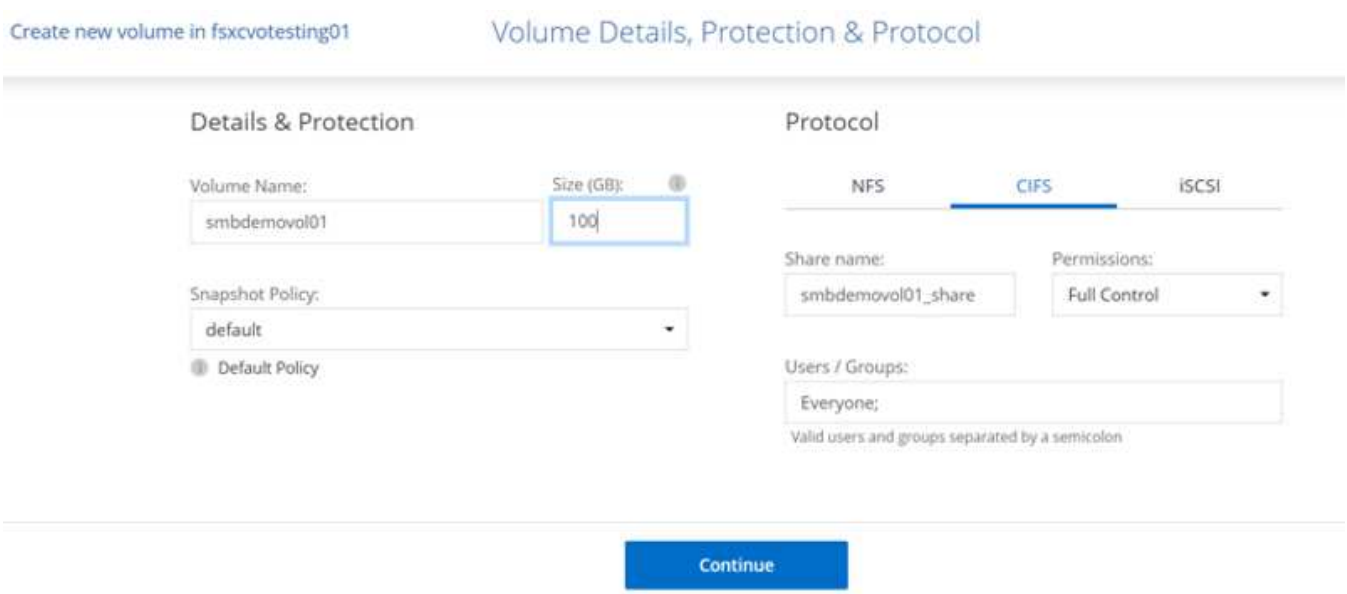


▼ **Zusätzliche Konfigurationen für SMB-Volumes**

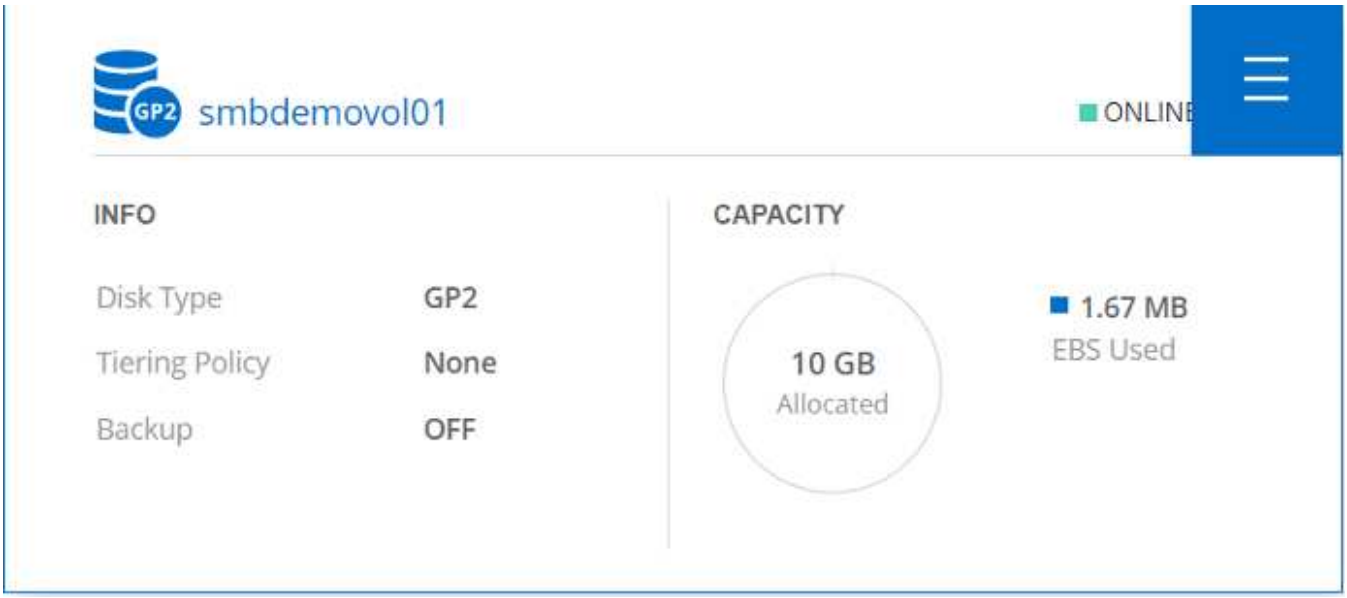
1. Nachdem die Arbeitsumgebung bereit ist, stellen Sie sicher, dass der CIFS-Server mit den entsprechenden DNS- und Active Directory-Konfigurationsparametern konfiguriert ist. Dieser Schritt ist erforderlich, bevor Sie das SMB-Volume erstellen können.



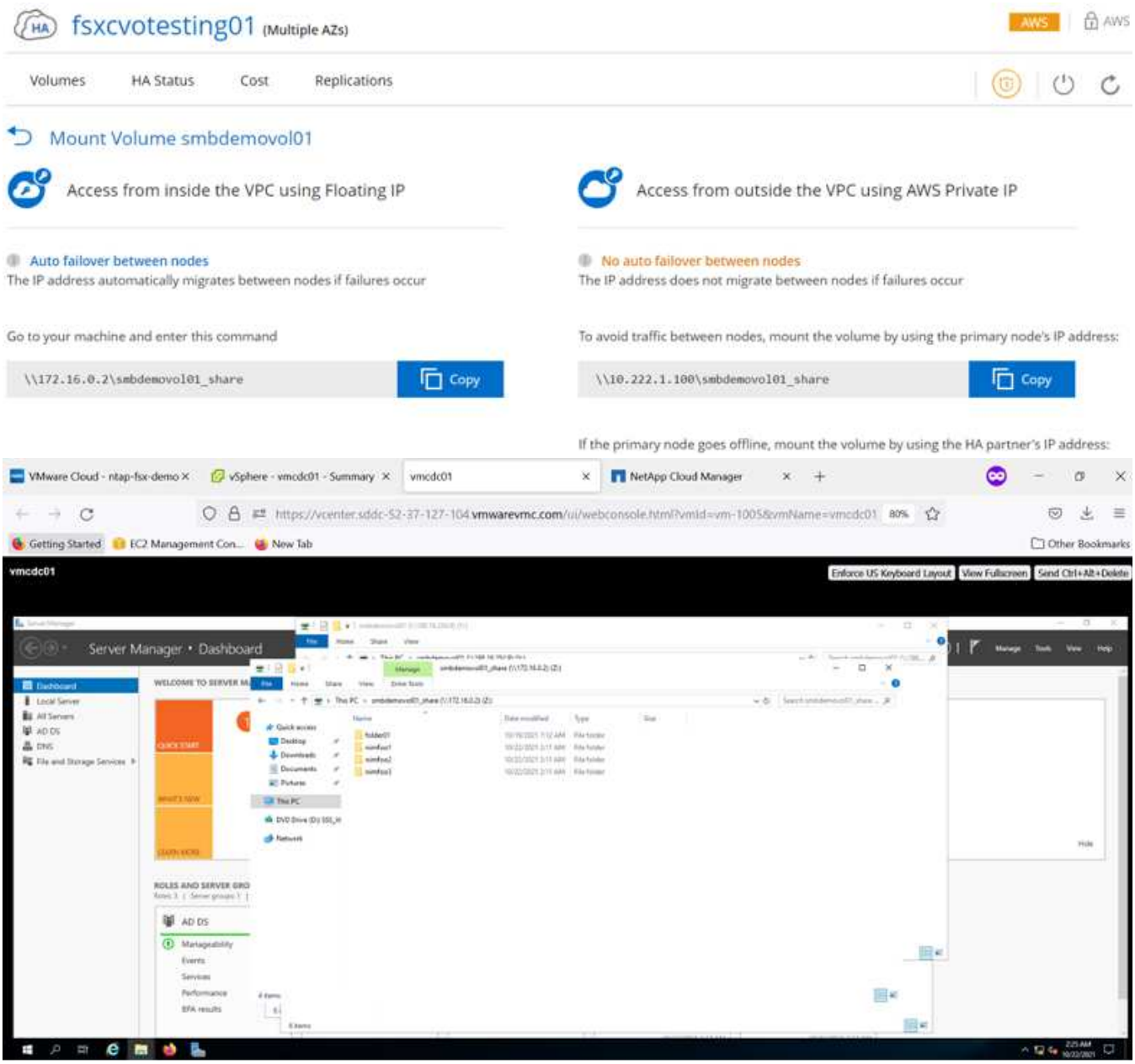
1. Wählen Sie die CVO-Instanz aus, um das Volume zu erstellen, und klicken Sie auf die Option „Volume erstellen“. Wählen Sie die entsprechende Größe und der Cloud-Manager wählt das enthaltene Aggregat aus oder verwenden Sie einen erweiterten Zuordnungsmechanismus, um die Platzierung auf einem bestimmten Aggregat vorzunehmen. Für diese Demo wurde SMB als Protokoll ausgewählt.



1. Nachdem das Volume bereitgestellt wurde, ist es im Bereich „Volumes“ verfügbar. Da eine CIFS-Freigabe bereitgestellt wird, sollten Sie Ihren Benutzern oder Gruppen Berechtigungen für die Dateien und Ordner erteilen und sicherstellen, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können.



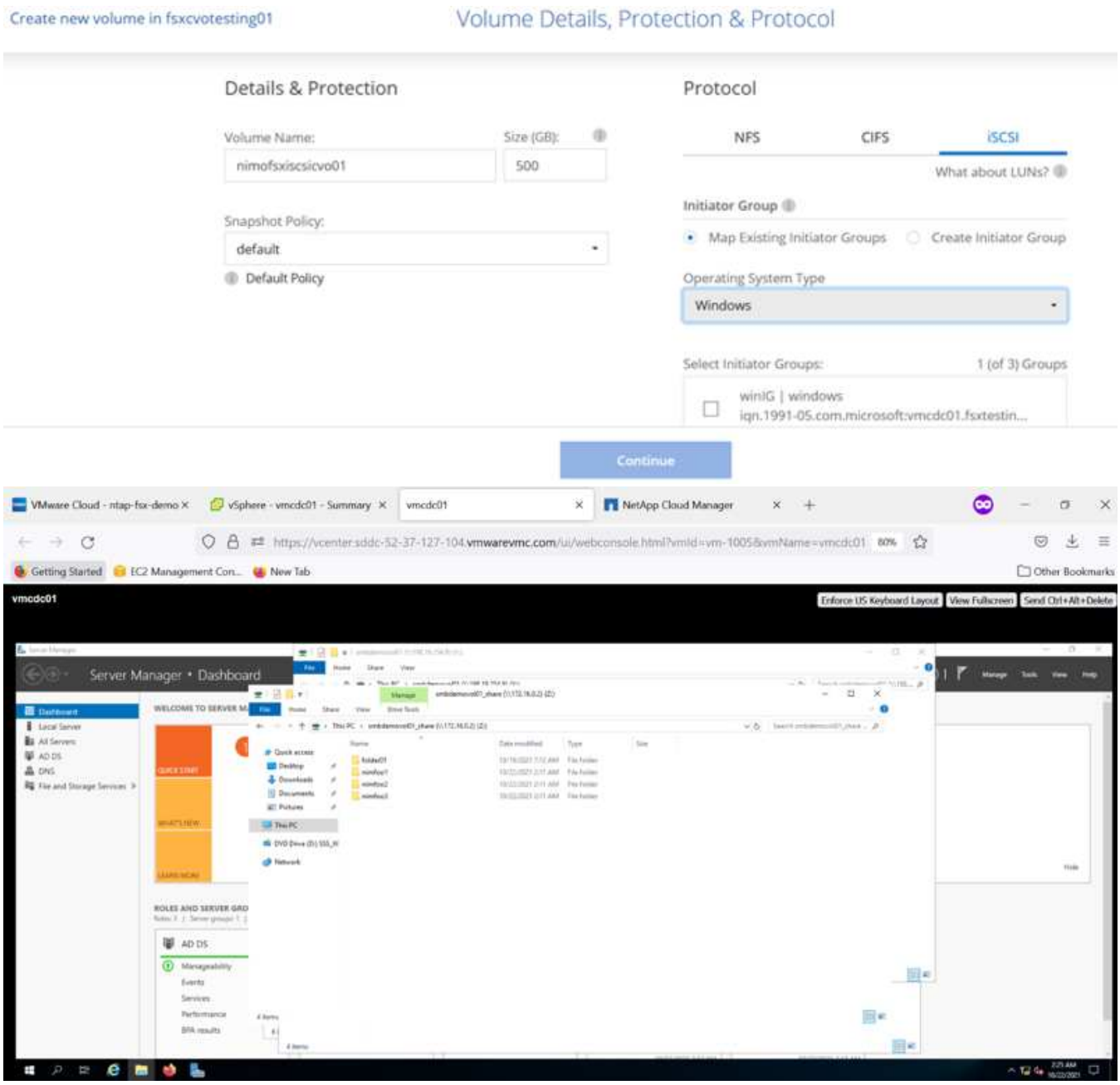
1. Nachdem das Volume erstellt wurde, verwenden Sie den Mount-Befehl, um von der VM, die auf den VMware Cloud- in AWS SDDC-Hosts ausgeführt wird, eine Verbindung zur Freigabe herzustellen.
2. Kopieren Sie den folgenden Pfad und verwenden Sie die Option „Netzlaufwerk zuordnen“, um das Volume auf der VM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



▼ **Verbinden Sie die LUN mit einem Host**

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

1. Doppelklicken Sie auf der Canvas-Seite von Cloud Manager auf die Arbeitsumgebung 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. Nachdem das Volume bereitgestellt wurde, wählen Sie das Volume aus und klicken Sie dann auf Ziel-IQN. Um den iSCSI Qualified Name (IQN) zu kopieren, klicken Sie auf „Kopieren“. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.

Um dasselbe für den Host zu erreichen, der sich auf dem VMware Cloud on AWS SDDC befindet, führen Sie die folgenden Schritte aus:

1. RDP zur VM, die in der VMware Cloud auf AWS gehostet wird.
2. Öffnen Sie das Dialogfeld „Eigenschaften des iSCSI-Initiators“: Server-Manager > Dashboard > Tools > iSCSI-Initiator.
3. Klicken Sie auf der Registerkarte „Erkennung“ 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“.

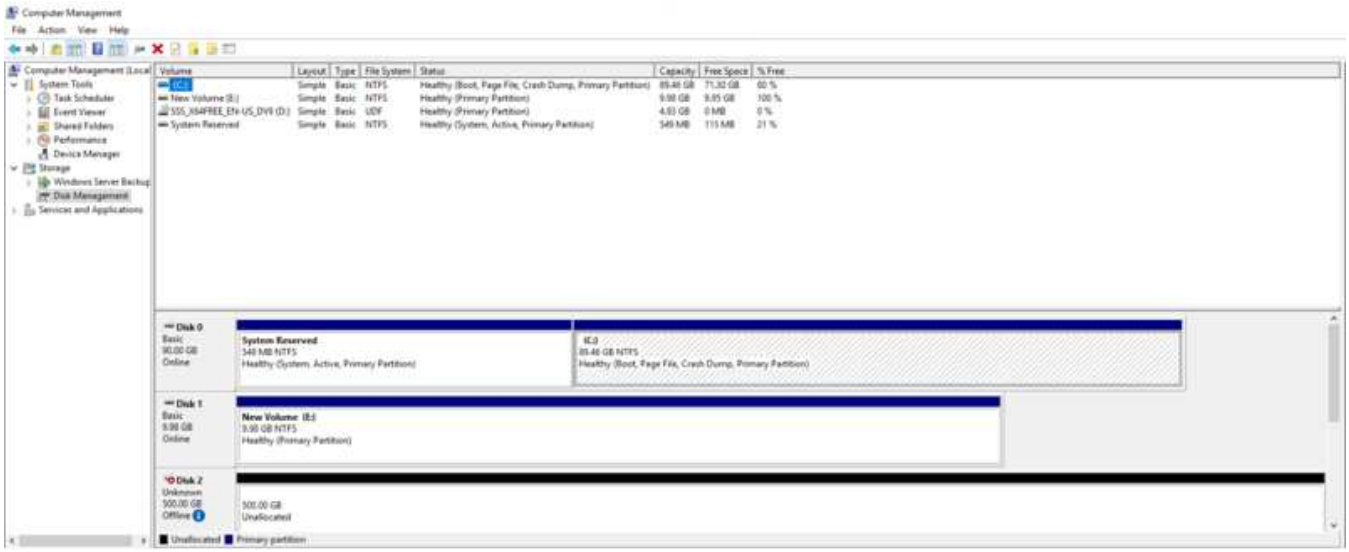
5. Wählen Sie „Multipfad aktivieren“ und dann „Diese Verbindung beim Start des Computers automatisch wiederherstellen“ oder „Diese Verbindung zur Liste der bevorzugten Ziele hinzufügen“. Klicken Sie auf „Erweitert“.

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



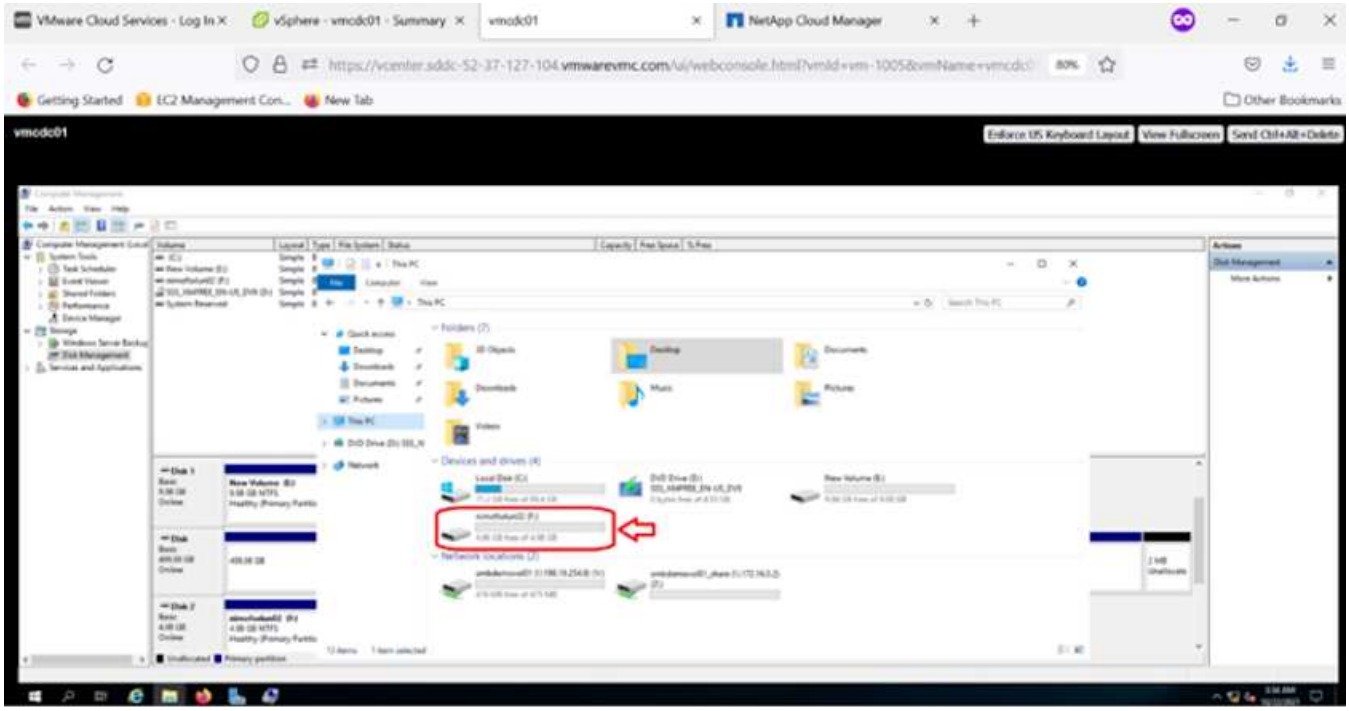
LUNs vom SVM werden dem Windows-Host als Datenträger angezeigt. Alle neu hinzugefügten Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen erneuten Scan aus, um die Datenträger zu ermitteln, indem Sie die folgenden Schritte ausführen:

1. Öffnen Sie das Windows-Dienstprogramm „Computerverwaltung“: Start > Verwaltung > Computerverwaltung.
2. Erweitern Sie den Knoten „Speicher“ im Navigationsbaum.
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, verfügt diese über keine Partition oder kein Dateisystem. Initialisieren Sie die LUN und formatieren Sie die LUN optional mit einem Dateisystem, indem Sie die folgenden Schritte ausführen:

1. Starten Sie die Windows-Datenträgerverwaltung.
2. Klicken Sie mit der rechten Maustaste auf die LUN und wählen Sie dann den erforderlichen Datenträger- oder Partitionstyp aus.
3. Folgen Sie den Anweisungen des Assistenten. In diesem Beispiel ist Laufwerk F: gemountet.



Stellen Sie sicher, dass auf den Linux-Clients der iSCSI-Daemon ausgeführt wird. Nachdem die LUNs bereitgestellt wurden, lesen Sie die ausführliche Anleitung zur iSCSI-Konfiguration für Ihre Linux-Distribution. Beispielsweise finden Sie die Ubuntu iSCSI-Konfiguration"hier," . Führen Sie zur Überprüfung den Befehl lsblk von der Shell aus.

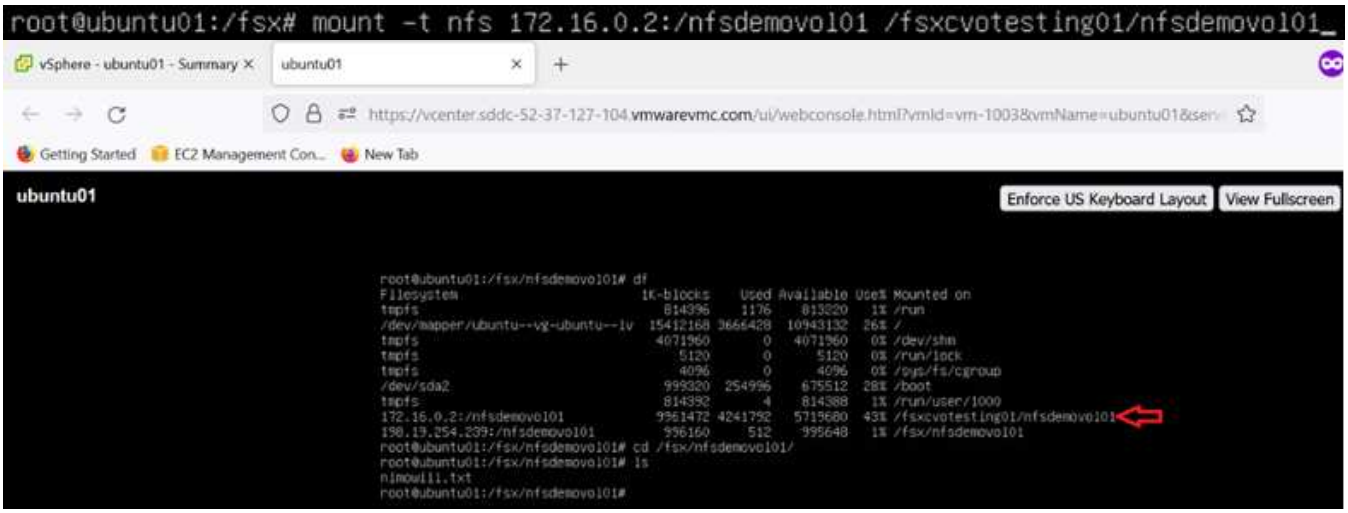
▼ **Mounten Sie das Cloud Volumes ONTAP NFS-Volume auf dem Linux-Client**

Führen Sie die folgenden Schritte aus, um das Cloud Volumes ONTAP (DIY)-Dateisystem von VMs innerhalb von VMC auf AWS SDDC zu mounten:

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

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. Hängen Sie das Amazon FSx ONTAP NFS-Volume in das Verzeichnis ein,
das im vorherigen Schritt erstellt wurde.
```

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



Azure Virtualization Service: Optionen für die Nutzung von NetApp -Speicher

NetApp -Speicher kann entweder als Gastspeicher oder als Zusatzspeicher an den Azure VMware-Dienst angeschlossen werden.

Azure NetApp Files (ANF) als ergänzender NFS-Datenspeicher

Die Unterstützung für NFS-Datenspeicher wurde mit ESXi Version 3 in lokalen Bereitstellungen eingeführt, wodurch die Speicherfunktionen von vSphere erheblich erweitert wurden.

Die Ausführung von vSphere auf NFS ist eine weit verbreitete Option für Virtualisierungsbereitstellungen vor Ort, da sie eine hohe Leistung und Stabilität bietet. Wenn Sie über umfangreiche Network Attached Storage (NAS) in einem lokalen Rechenzentrum verfügen, sollten Sie die Bereitstellung eines Azure VMware Solution SDDC in Azure mit Azure NetApp File-Datenspeichern in Betracht ziehen, um Kapazitäts- und Leistungsprobleme zu überwinden.

Azure NetApp Files basiert auf der branchenführenden, hochverfügbaren Datenverwaltungssoftware NetApp ONTAP . Microsoft Azure-Dienste werden in drei Kategorien eingeteilt: grundlegend, Mainstream und

spezialisiert. Azure NetApp Files gehört zur Kategorie „Spezialisiert“ und wird durch Hardware unterstützt, die in vielen Regionen bereits im Einsatz ist. Mit integrierter Hochverfügbarkeit (HA) schützt Azure NetApp Files Ihre Daten vor den meisten Ausfällen und bietet Ihnen ein branchenführendes SLA mit einer Verfügbarkeit von 99,99 %^.

Weitere Informationen zu ANF als ergänzendem NFS-Datenspeicher finden Sie unter:

- "ANF als ergänzender NFS-Datenspeicher: Übersicht"
- "Ergänzende NFS-Datenspeicheroption in Azure"

Azure NetApp Files (ANF) als mit dem Gast verbundener Speicher

Azure NetApp Files bringt Datenverwaltung und -speicherung auf Unternehmensniveau zu Azure, sodass Sie Ihre Workloads und Anwendungen problemlos verwalten können. Migrieren Sie Ihre Workloads in die Cloud und führen Sie sie ohne Leistungseinbußen aus.

Azure NetApp Files beseitigt Hindernisse, sodass Sie alle Ihre dateibasierten Anwendungen in die Cloud verschieben können. Zum ersten Mal müssen Sie Ihre Anwendungen nicht neu strukturieren und erhalten dauerhaften Speicher für Ihre Anwendungen ohne Komplexität.

Da der Dienst über das Microsoft Azure-Portal bereitgestellt wird, profitieren Benutzer im Rahmen ihres Microsoft Enterprise Agreement von einem vollständig verwalteten Dienst. Dank des erstklassigen Supports von Microsoft können Sie sich vollkommen beruhigt zurücklehnen. Mit dieser Einzellösung können Sie schnell und einfach Multiprotokoll-Workloads hinzufügen. Sie können sowohl dateibasierte Windows- als auch Linux-Anwendungen erstellen und bereitstellen, sogar für Legacy-Umgebungen.

Weitere Informationen finden Sie unter"ANF als Gastverbundener Speicher" .

Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher

Cloud Volumes ONTAP (CVO) ist die branchenführende Cloud-Datenmanagementlösung, die auf der ONTAP -Speichersoftware von NetApp basiert und nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar ist.

Es handelt sich um eine softwaredefinierte Version von ONTAP , die Cloud-nativen Speicher nutzt. Dadurch können Sie in der Cloud und vor Ort dieselbe Speichersoftware verwenden und müssen Ihr IT-Personal nicht mehr in völlig neuen Methoden zur Verwaltung Ihrer Daten schulen.

CVO bietet Kunden die Möglichkeit, Daten nahtlos vom Edge zum Rechenzentrum, in die Cloud und zurück zu verschieben und so Ihre Hybrid Cloud zusammenzuführen – alles verwaltet über eine zentrale Verwaltungskonsole, den NetApp Cloud Manager.

CVO bietet von Haus aus extreme Leistung und erweiterte Datenverwaltungsfunktionen, um selbst Ihre anspruchsvollsten Anwendungen in der Cloud zu erfüllen

Weitere Informationen finden Sie unter"CVO als Gastverbundener Speicher" .

Übersicht über ANF Datastore-Lösungen

Jede erfolgreiche Organisation befindet sich auf dem Weg der Transformation und Modernisierung. Im Rahmen dieses Prozesses nutzen Unternehmen in der Regel ihre vorhandenen VMware-Investitionen, während sie gleichzeitig die Vorteile der Cloud nutzen und Möglichkeiten erkunden, Migrations-, Burst-, Erweiterungs- und Notfallwiederherstellungsprozesse so nahtlos wie möglich zu gestalten. Kunden, die in

die Cloud migrieren, müssen die Probleme der Elastizität und Burst, des Ausstiegs aus Rechenzentren, der Konsolidierung von Rechenzentren, End-of-Life-Szenarien, Fusionen, Übernahmen usw. bewerten. Der von jeder Organisation gewählte Ansatz kann je nach den jeweiligen Geschäftsprioritäten unterschiedlich sein. Bei der Entscheidung für Cloud-basierte Vorgänge ist die Auswahl eines kostengünstigen Modells mit entsprechender Leistung und minimalen Einschränkungen ein wichtiges Ziel. Neben der Auswahl der richtigen Plattform ist die Speicher- und Workflow-Orchestrierung besonders wichtig, um die Leistungsfähigkeit und Elastizität der Cloud-Bereitstellung zu entfalten.

Anwendungsfälle

Obwohl die Azure VMware-Lösung dem Kunden einzigartige Hybridfunktionen bietet, ist ihre Nützlichkeit für Unternehmen mit speicherintensiven Workloads aufgrund der begrenzten nativen Speicheroptionen eingeschränkt. Da der Speicher direkt an Hosts gebunden ist, besteht die einzige Möglichkeit zur Skalierung des Speichers darin, weitere Hosts hinzuzufügen, was bei speicherintensiven Workloads zu einer Kostensteigerung von 35–40 % oder mehr führen kann. Diese Arbeitslasten erfordern zusätzlichen Speicher, nicht zusätzliche Leistung, aber das bedeutet, dass für zusätzliche Hosts bezahlt werden muss.

Betrachten wir das folgende Szenario: Ein Kunde benötigt sechs Hosts für die Leistung (vCPU/vMem), hat aber auch einen erheblichen Speicherbedarf. Ihrer Einschätzung nach sind 12 Hosts erforderlich, um die Speicheranforderungen zu erfüllen. Dies erhöht die Gesamtbetriebskosten, da sie die ganze zusätzliche Leistung kaufen müssen, obwohl sie eigentlich nur mehr Speicherplatz benötigen. Dies gilt für alle Anwendungsfälle, einschließlich Migration, Notfallwiederherstellung, Bursting, Entwicklung/Test usw.

Ein weiterer häufiger Anwendungsfall für Azure VMware Solution ist die Notfallwiederherstellung (DR). Die meisten Organisationen verfügen über keine narrensichere DR-Strategie oder haben möglicherweise Schwierigkeiten, den Betrieb eines Ghost-Rechenzentrums nur für DR zu rechtfertigen. Administratoren können Zero-Footprint-DR-Optionen mit einem Pilot-Light-Cluster oder einem On-Demand-Cluster erkunden. Sie könnten dann den Speicher skalieren, ohne zusätzliche Hosts hinzuzufügen, was möglicherweise eine attraktive Option ist.

Zusammenfassend können die Anwendungsfälle auf zwei Arten klassifiziert werden:

- Skalieren der Speicherkapazität mit ANF-Datenspeichern
- Verwenden von ANF-Datenspeichern als Notfallwiederherstellungsziel für einen kostenoptimierten Wiederherstellungsworkflow vor Ort oder innerhalb von Azure-Regionen zwischen den softwaredefinierten Rechenzentren (SDDCs). Dieses Handbuch bietet Einblicke in die Verwendung von Azure NetApp Files zur Bereitstellung von optimiertem Speicher für Datenspeicher (derzeit in der öffentlichen Vorschau) zusammen mit erstklassigen Datenschutz- und DR-Funktionen in einer Azure VMware-Lösung, mit der Sie Speicherkapazität vom vSAN-Speicher auslagern können.



Wenden Sie sich an die NetApp oder Microsoft-Lösungsarchitekten in Ihrer Region, um weitere Informationen zur Verwendung von ANF-Datenspeichern zu erhalten.

VMware Cloud-Optionen in Azure

Azure VMware-Lösung

Die Azure VMware Solution (AVS) ist ein Hybrid-Cloud-Dienst, der voll funktionsfähige VMware SDDCs innerhalb einer öffentlichen Microsoft Azure-Cloud bereitstellt. AVS ist eine First-Party-Lösung, die vollständig von Microsoft verwaltet und unterstützt und von VMware verifiziert wird und die Azure-Infrastruktur nutzt. Daher

erhalten Kunden VMware ESXi für die Computervirtualisierung, vSAN für hyperkonvergenten Speicher und NSX für Netzwerke und Sicherheit und profitieren gleichzeitig von der globalen Präsenz von Microsoft Azure, den erstklassigen Rechenzentrumseinrichtungen und der Nähe zum umfangreichen Ökosystem nativer Azure-Dienste und -Lösungen. Eine Kombination aus Azure VMware Solution SDDC und Azure NetApp Files bietet die beste Leistung bei minimaler Netzwerklatenz.

Unabhängig von der verwendeten Cloud umfasst der anfängliche Cluster bei der Bereitstellung eines VMware SDDC die folgenden Komponenten:

- VMware ESXi-Hosts für die Computervirtualisierung mit einer vCenter-Server-Appliance für die Verwaltung.
- Hyperkonvergenter VMware vSAN-Speicher, der die physischen Speicherressourcen jedes ESXi-Hosts integriert.
- VMware NSX für virtuelle Netzwerke und Sicherheit mit einem NSX Manager-Cluster für die Verwaltung.

Abschluss

Unabhängig davon, ob Sie eine reine Cloud oder eine Hybrid-Cloud anstreben, bieten Azure NetApp Dateien hervorragende Optionen zum Bereitstellen und Verwalten der Anwendungs-Workloads zusammen mit Dateidiensten und senken gleichzeitig die Gesamtbetriebskosten, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden. Wählen Sie für jeden Anwendungsfall Azure VMware Solution zusammen mit Azure NetApp Files, um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und Vorgänge vor Ort und in mehreren Clouds zu gewährleisten, Workloads in beide Richtungen zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen. Es handelt sich um denselben bekannten Prozess und dieselben bekannten Verfahren, die zum Verbinden des Speichers verwendet werden. Denken Sie daran, dass sich neben den neuen Namen nur die Position der Daten geändert hat. Die Tools und Prozesse bleiben alle gleich und Azure NetApp Files hilft bei der Optimierung der gesamten Bereitstellung.

Imbiss

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können jetzt Azure NetApp Files als Datenspeicher auf AVS SDDC verwenden.
- Verbessern Sie die Reaktionszeiten der Anwendung und sorgen Sie für eine höhere Verfügbarkeit, um Zugriff auf Workload-Daten zu ermöglichen, wann und wo immer diese benötigt werden.
- Vereinfachen Sie die Gesamtkomplexität des vSAN-Speichers mit einfachen und sofortigen Größenänderungsfunktionen.
- Garantierte Leistung für unternehmenskritische Workloads durch dynamische Umgestaltungsfunktionen.
- Wenn Azure VMware Solution Cloud das Ziel ist, ist Azure NetApp Files die richtige Speicherlösung für eine optimierte Bereitstellung.

Wo Sie weitere Informationen finden

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

- Dokumentation zur 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/"

- Anfügen von Azure NetApp Files -Datenspeichern an Azure VMware Solution-Hosts (Vorschau)

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

Erstellen eines zusätzlichen NFS-Datenspeichers in Azure

Die Unterstützung für NFS-Datenspeicher wurde mit ESXi Version 3 in lokalen Bereitstellungen eingeführt, wodurch die Speicherfunktionen von vSphere erheblich erweitert wurden.

Die Ausführung von vSphere auf NFS ist eine weit verbreitete Option für Virtualisierungsbereitstellungen vor Ort, da sie eine hohe Leistung und Stabilität bietet. Wenn Sie über umfangreiche Network Attached Storage (NAS) in einem lokalen Rechenzentrum verfügen, sollten Sie die Bereitstellung eines Azure VMware Solution SDDC in Azure mit Azure NetApp File-Datenspeichern in Betracht ziehen, um Kapazitäts- und Leistungsprobleme zu überwinden.

Azure NetApp Files basiert auf der branchenführenden, hochverfügbaren Datenverwaltungssoftware NetApp ONTAP . Microsoft Azure-Dienste werden in drei Kategorien eingeteilt: grundlegend, Mainstream und spezialisiert. Azure NetApp Files gehört zur Kategorie „Spezialisiert“ und wird durch Hardware unterstützt, die in vielen Regionen bereits im Einsatz ist. Mit integrierter Hochverfügbarkeit (HA) schützt Azure NetApp Files Ihre Daten vor den meisten Ausfällen und bietet Ihnen ein branchenführendes SLA von "99,99 %" Betriebszeit.

Vor der Einführung der Azure NetApp Files -Datenspeicherfunktion war für den Scale-Out-Betrieb bei Kunden, die leistungs- und speicherintensive Workloads hosten wollten, eine Erweiterung sowohl der Rechenleistung als auch des Speichers erforderlich.

Beachten Sie die folgenden Punkte:

- Unausgeglichene Clusterkonfigurationen werden in einem SDDC-Cluster nicht empfohlen. Daher bedeutet eine Speichererweiterung das Hinzufügen weiterer Hosts, was wiederum höhere Gesamtbetriebskosten bedeutet.
- Es ist nur eine vSAN-Umgebung möglich. Daher steht der gesamte Speicherverkehr in direkter Konkurrenz zu den Produktionsarbeitslasten.
- Es besteht keine Möglichkeit, mehrere Leistungsstufen bereitzustellen, um Anwendungsanforderungen, Leistung und Kosten aufeinander abzustimmen.
- Bei auf Cluster-Hosts basierendem vSAN kann die Speicherkapazität schnell an ihre Grenzen stoßen. Durch die Integration von Azure-nativen Platform-as-a-Service-Angeboten (PaaS) wie Azure NetApp Files als Datenspeicher haben Kunden die Möglichkeit, ihren Speicher unabhängig voneinander zu skalieren und dem SDDC-Cluster nur bei Bedarf Compute-Knoten hinzuzufügen. Diese Fähigkeit überwindet die oben genannten Herausforderungen.

Azure NetApp Files ermöglicht Ihnen außerdem die Bereitstellung mehrerer Datenspeicher. Dadurch können Sie ein lokales Bereitstellungsmodell nachahmen, indem Sie virtuelle Maschinen im entsprechenden Datenspeicher platzieren und das erforderliche Servicelevel zuweisen, um die Leistungsanforderungen der Workloads zu erfüllen. Mit der einzigartigen Fähigkeit zur Multiprotokollunterstützung ist der Gastspeicher eine zusätzliche Option für Datenbank-Workloads wie SQL und Oracle, während gleichzeitig die zusätzliche NFS-Datenspeicherfunktion zur Unterbringung der verbleibenden VMDKs genutzt wird. Darüber hinaus ermöglicht Ihnen die native Snapshot-Funktion die Durchführung schneller Backups und granularer Wiederherstellungen.

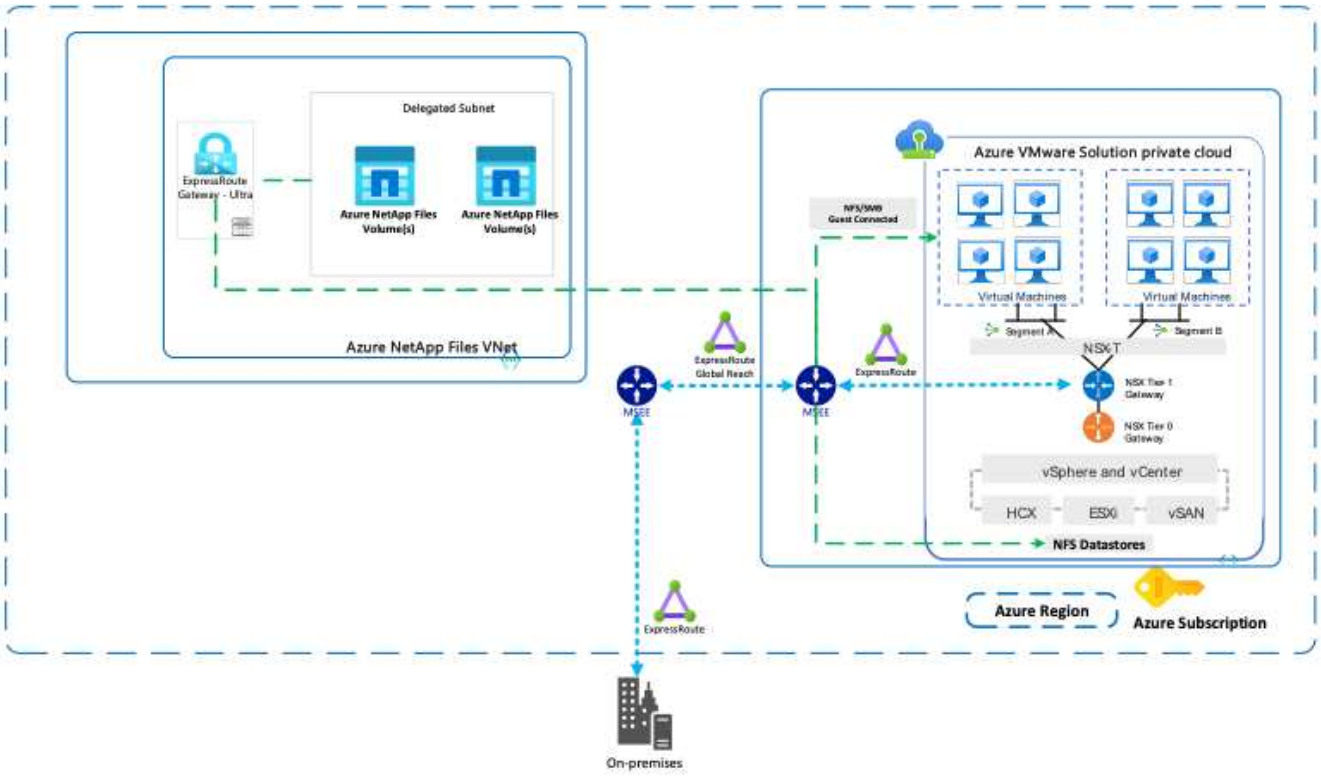


Wenden Sie sich an Azure und NetApp Solution Architects, um die Speicherplanung und -dimensionierung durchzuführen und die erforderliche Anzahl an Hosts zu bestimmen. NetApp

empfiehlt, die Speicherleistungsanforderungen zu ermitteln, bevor das Datastore-Layout für Test-, POC- und Produktionsbereitstellungen finalisiert wird.

Detaillierte Architektur

Aus einer übergeordneten Perspektive beschreibt diese Architektur, wie Hybrid-Cloud-Konnektivität und App-Portabilität zwischen lokalen Umgebungen und Azure erreicht werden. Außerdem wird die Verwendung von Azure NetApp Files als zusätzlicher NFS-Datenspeicher und als In-Guest-Speicheroption für virtuelle Gastcomputer beschrieben, die auf der Azure VMware-Lösung gehostet werden.



Größen

Der wichtigste Aspekt bei der Migration oder Notfallwiederherstellung ist die Bestimmung der richtigen Größe für die Zielumgebung. Es ist sehr wichtig zu verstehen, wie viele Knoten erforderlich sind, um eine Lift-and-Shift-Übung von lokalen Standorten zur Azure VMware-Lösung durchzuführen.

Verwenden Sie zur Größenbestimmung historische Daten aus der lokalen Umgebung mithilfe von RVTools (bevorzugt) oder anderen Tools wie Live Optics oder Azure Migrate. RVTools ist ein ideales Tool zum Erfassen von vCPU, vMem, vDisk und allen erforderlichen Informationen, einschließlich ein- oder ausgeschalteter VMs, um die Zielumgebung zu charakterisieren.

Führen Sie die folgenden Schritte aus, um RVtools auszuführen:

1. Laden Sie RVTools herunter und installieren Sie es.
2. Führen Sie RVTools aus, geben Sie die erforderlichen Informationen ein, um eine Verbindung zu Ihrem lokalen vCenter-Server herzustellen, und drücken Sie auf „Anmelden“.
3. Exportieren Sie das Inventar in eine Excel-Tabelle.
4. Bearbeiten Sie die Tabelle und entfernen Sie alle VMs, die keine idealen Kandidaten sind, aus der Registerkarte „vInfo“. Dieser Ansatz liefert eine klare Ausgabe zu den Speicheranforderungen, die

verwendet werden kann, um die richtige Größe des Azure VMware SDDC-Clusters mit der erforderlichen Anzahl von Hosts festzulegen.

> Gast-VMs, die mit In-Guest-Speicher verwendet werden, müssen separat berechnet werden. Azure NetApp Files kann die zusätzliche Speicherkapazität jedoch problemlos abdecken und so die Gesamtbetriebskosten niedrig halten.

Bereitstellen und Konfigurieren der Azure VMware-Lösung

Wie bei der lokalen Bereitstellung ist die Planung einer Azure VMware-Lösung entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen virtueller Maschinen und für die Migration.

In diesem Abschnitt wird beschrieben, wie AVS für die Verwendung in Kombination mit Azure NetApp Files als Datenspeicher mit In-Guest-Speicher eingerichtet und verwaltet wird.

Der Einrichtungsprozess kann in drei Teile unterteilt werden:

- Registrieren Sie den Ressourcenanbieter und erstellen Sie eine private Cloud.
- Stellen Sie eine Verbindung mit einem neuen oder vorhandenen virtuellen ExpressRoute-Netzwerkgateway her.
- Überprüfen Sie die Netzwerkkonnektivität und greifen Sie auf die private Cloud zu. Siehe hierzu"Link" für eine schrittweise Anleitung des SDDC-Bereitstellungsprozesses der Azure VMware-Lösung.

Konfigurieren von Azure NetApp Files mit Azure VMware Solution

Die neue Integration zwischen Azure NetApp Files ermöglicht Ihnen, NFS-Datenspeicher über die APIs/CLI des Azure VMware Solution-Ressourcenanbieters mit Azure NetApp Files -Volumes zu erstellen und die Datenspeicher auf den Clustern Ihrer Wahl in einer privaten Cloud bereitzustellen. Neben der Unterbringung der VM- und App-VMDKs können Azure NetApp Dateivolumes auch von VMs bereitgestellt werden, die in der Azure VMware Solution SDDC-Umgebung erstellt wurden. Die Volumes können auf dem Linux-Client bereitgestellt und auf einem Windows-Client zugeordnet werden, da Azure NetApp Files die Protokolle Server Message Block (SMB) und Network File System (NFS) unterstützt.

> Um eine optimale Leistung zu erzielen, stellen Sie die Azure NetApp Files in derselben Verfügbarkeitszone wie die private Cloud bereit. Die Colocation mit dem Express Route Fastpath bietet die beste Leistung bei minimaler Netzwerklatenz.

Um ein Azure NetApp File-Volume als VMware-Datenspeicher einer privaten Azure VMware Solution-Cloud anzufügen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind.

▼ Voraussetzungen

1. Verwenden Sie „az login“ und überprüfen Sie, ob das Abonnement für die CloudSanExperience-Funktion im Microsoft.AVS-Namespace registriert ist.

```
az login –tenant xcvxcvxc- vxcv- xcvx- cvxc- vxcvxcvxcv
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

1. Wenn es nicht registriert ist, registrieren Sie es.

```
az feature register --name "CloudSanExperience" --namespace
```

```
"Microsoft.AVS"
```

Die Registrierung kann etwa 15 Minuten dauern.

1. Um den Status der Registrierung zu überprüfen, führen Sie den folgenden Befehl aus.

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
--query properties.state
```

1. Wenn die Registrierung länger als 15 Minuten in einem Zwischenzustand festhängt, melden Sie das Flag ab und registrieren Sie es anschließend erneut.

```
az feature unregister --name "CloudSanExperience" --namespace
"Microsoft.AVS"
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

1. Überprüfen Sie, ob das Abonnement für die Funktion „AnfDatastoreExperience“ im Namespace „Microsoft.AVS“ registriert ist.

```
az feature show --name "AnfDatastoreExperience" --namespace
"Microsoft.AVS" --query properties.state
```

1. Stellen Sie sicher, dass die VMware-Erweiterung installiert ist.

```
az extension show --name vmware
```

1. Wenn die Erweiterung bereits installiert ist, überprüfen Sie, ob die Version 3.0.0 ist. Wenn eine ältere Version installiert ist, aktualisieren Sie die Erweiterung.

```
az extension update --name vmware
```

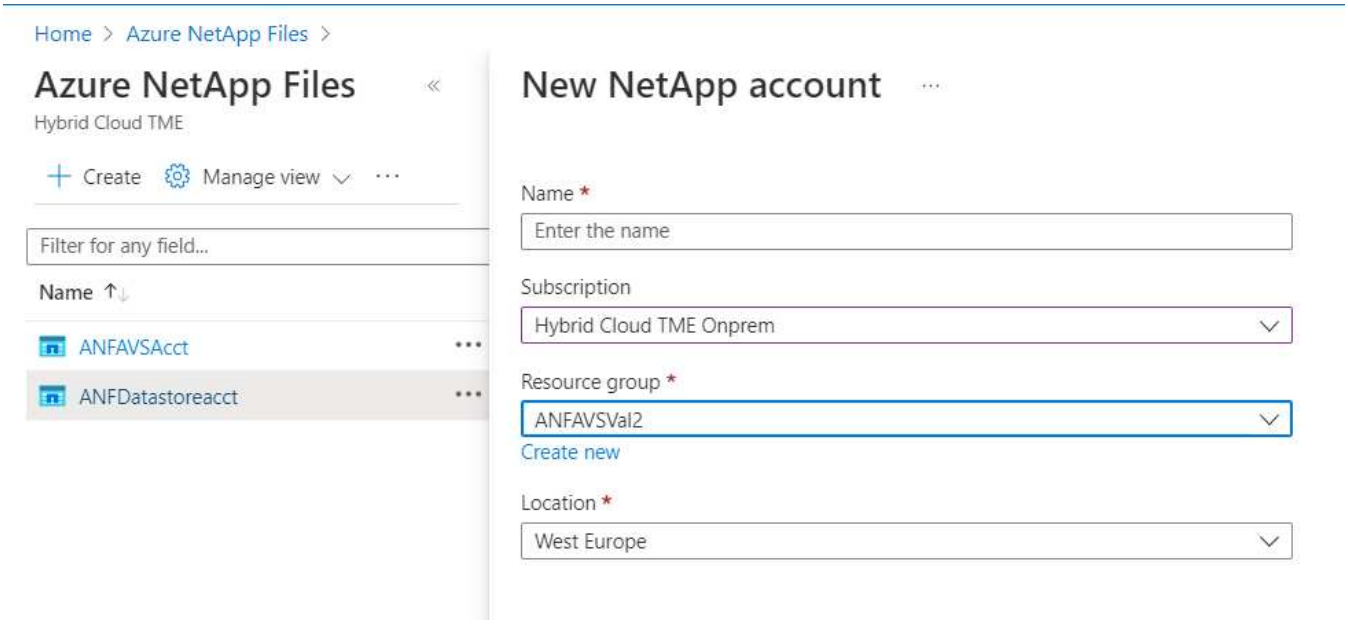
1. Wenn die Erweiterung noch nicht installiert ist, installieren Sie sie.

```
az extension add --name vmware
```

▼ Erstellen und Einbinden von Azure NetApp Files Volumes

1. Melden Sie sich beim 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 mithilfe des `az provider register --namespace Microsoft.NetApp --wait` Befehl. Erstellen Sie nach der Registrierung ein NetApp -Konto. Siehe hierzu "Link" für

detaillierte Schritte.



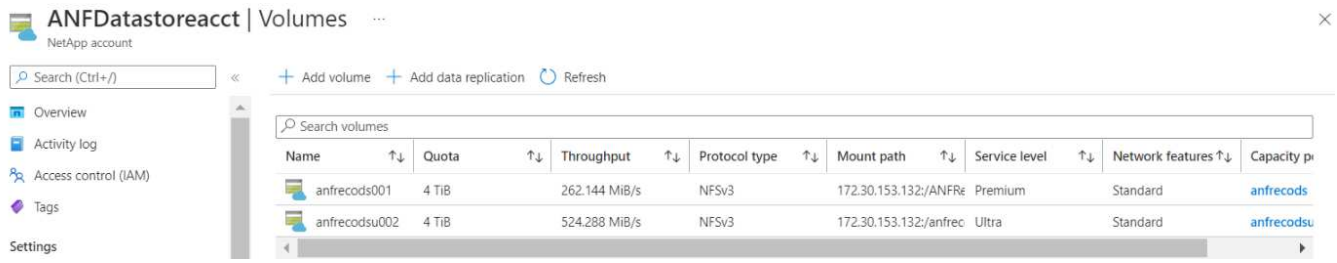
1. Nachdem ein NetApp -Konto erstellt wurde, richten Sie Kapazitätspools mit dem erforderlichen Servicelevel und der erforderlichen Größe ein. Ausführliche Informationen finden Sie hier "Link" .



Wichtige Punkte

- NFSv3 wird für Datenspeicher auf Azure NetApp Files unterstützt.
- Verwenden Sie die Premium- oder Standardstufe für kapazitätsgebundene Workloads und die Ultra-Stufe für leistungsgebundene Workloads, wo nötig, und ergänzen Sie gleichzeitig den standardmäßigen vSAN-Speicher.

1. Konfigurieren Sie ein delegiertes Subnetz für Azure NetApp Files und geben Sie dieses Subnetz beim Erstellen von Volumes an. Ausführliche Schritte zum Erstellen eines delegierten Subnetzes finden Sie hier "Link" .
2. Fügen Sie mithilfe des Blatts „Volumes“ unter dem Blatt „Kapazitätspools“ ein NFS-Volume für den Datenspeicher hinzu.



Weitere Informationen zur Volumeleistung von Azure NetApp Files nach Größe oder Kontingent finden Sie unter"Leistungsüberlegungen für Azure NetApp Files" .

▼ Azure NetApp Files-Datenspeicher zur privaten Cloud hinzufügen

Das Azure NetApp Files Volume kann über das Azure-Portal an Ihre private Cloud angehängt werden. Folgen Sie diesem"Link von Microsoft" für eine schrittweise Anleitung zur Verwendung des Azure-Portals zum Einbinden eines Azure NetApp Dateidatenspeichers.

Führen Sie die folgenden Schritte aus, um einer privaten Cloud einen Azure NetApp Files-Datenspeicher hinzuzufügen:

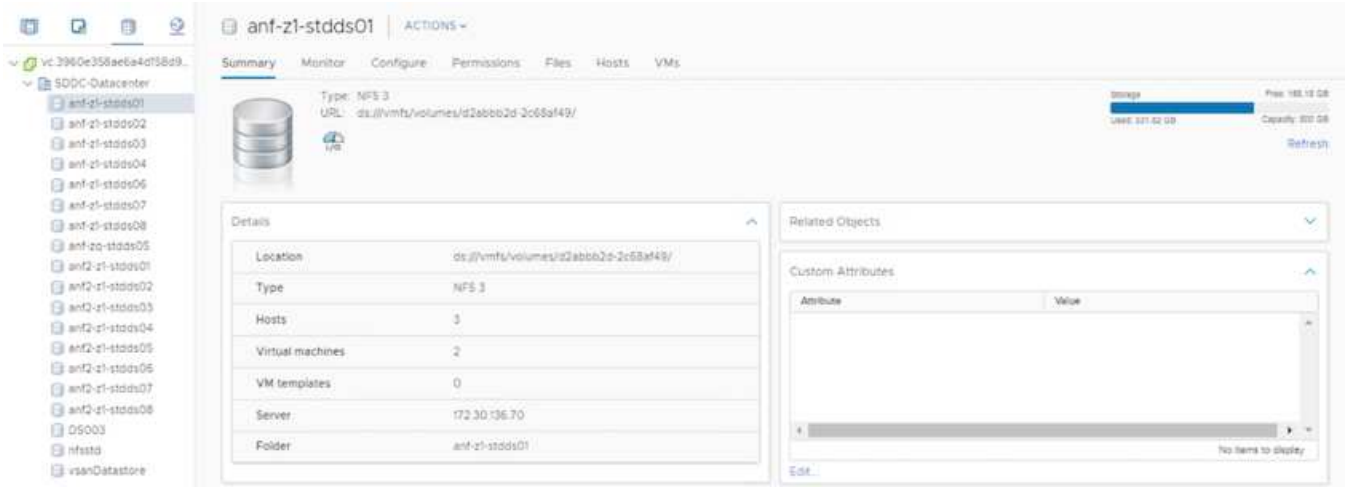
1. Nachdem die erforderlichen Funktionen registriert wurden, fügen Sie einen NFS-Datenspeicher an den privaten Cloudcluster von Azure VMware Solution an, indem Sie den entsprechenden Befehl ausführen.
2. Erstellen Sie einen Datenspeicher mithilfe eines vorhandenen ANF-Volumes im privaten Cloudcluster von Azure VMware Solution.

```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}
```

```
. List all the datastores in a private cloud cluster.
```

C:\Benutzer\niyaz>az vmware datastore list --resource-group anfavsval2 --cluster Cluster-1 --private-cloud ANFDataClus [{ "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDS001", "name": "ANFRecoDS001", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001", "resourceGroup": "anfavsval2" }, "provisioningState": "Erfolgreich", "resourceGroup": "anfavsval2", "Typ": "Microsoft.AVS/privateClouds/clusters/datastores" }, { "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002", "resourceGroup": "anfavsval2" }, "provisioningState": "NetApp", "resourceGroup": "anfavsval2", "Typ": "Microsoft.AVS/privateClouds/clusters/datastores" }]

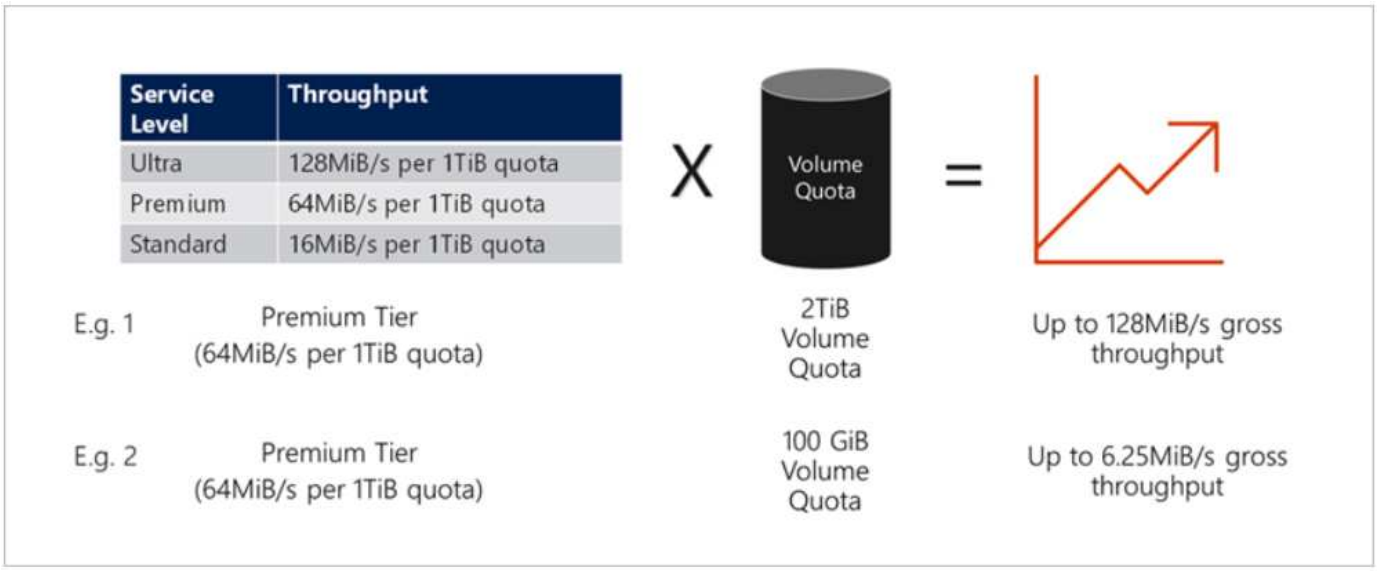
1. Nachdem die erforderliche Konnektivität hergestellt ist, werden die Volumes als Datenspeicher bereitgestellt.



Dimensionierung und Leistungsoptimierung

Azure NetApp Files unterstützt drei Servicelevel: Standard (16 MBit/s pro Terabyte), Premium (64 MBit/s pro Terabyte) und Ultra (128 MBit/s pro Terabyte). Für eine optimale Leistung der Datenbank-Workload ist die Bereitstellung der richtigen Volume-Größe wichtig. Bei Azure NetApp Files werden die Volumeleistung und das Durchsatzlimit anhand der folgenden Faktoren bestimmt:

- Der Servicelevel des Kapazitätspools, zu dem das Volume gehört
- Das dem Volume zugewiesene Kontingent
- Der Quality of Service (QoS)-Typ (automatisch oder manuell) des Kapazitätspools



Weitere Informationen finden Sie unter "Servicelevel für Azure NetApp Files" .

Siehe hierzu"Link von Microsoft" für detaillierte Leistungsbenchmarks, die bei einer Größenbestimmung verwendet werden können.

Wichtige Punkte
• Verwenden Sie für Datenspeichervolumes die Premium- oder Standardstufe, um optimale Kapazität und Leistung zu erzielen. Wenn Leistung erforderlich ist, kann die Ultra-Stufe verwendet werden. • Verwenden Sie für die Anforderungen zur Gastbereitstellung die Premium- oder Ultra-Stufe und für die Dateifreigabeanforderungen für Gast-VMs die Volumes der Standard- oder Premium-Stufe.

Überlegungen zur Leistung

Es ist wichtig zu verstehen, dass es bei NFS Version 3 nur eine aktive Pipe für die Verbindung zwischen dem ESXi-Host und einem einzelnen Speicherziel gibt. Dies bedeutet, dass zwar möglicherweise alternative Verbindungen für ein Failover verfügbar sind, die Bandbreite für einen einzelnen Datenspeicher und den zugrunde liegenden Speicher jedoch auf das beschränkt ist, was eine einzelne Verbindung bereitstellen kann.

Um mit Azure NetApp Files Volumes mehr verfügbare Bandbreite zu nutzen, muss ein ESXi-Host über mehrere Verbindungen zu den Speicherzielen verfügen. Um dieses Problem zu beheben, können Sie mehrere Datenspeicher konfigurieren, wobei jeder Datenspeicher separate Verbindungen zwischen dem ESXi-Host und dem Speicher verwendet.

Für eine höhere Bandbreite empfiehlt es sich, mehrere Datenspeicher mit mehreren ANF-Volumes zu erstellen, VMDKs zu erstellen und die logischen Volumes über VMDKs zu verteilen.

Siehe hierzu"Link von Microsoft" für detaillierte Leistungsbenchmarks, die bei einer Größenbestimmung verwendet werden können.

Wichtige Punkte

- Die Azure VMware-Lösung ermöglicht standardmäßig acht NFS-Datenspeicher. Dieser kann über eine Supportanfrage erhöht werden.
- Nutzen Sie ER Fastpath zusammen mit Ultra SKU für höhere Bandbreite und geringere Latenz. Weitere Informationen
- Mit den „grundlegenden“ Netzwerkfunktionen in Azure NetApp Dateien ist die Konnektivität von Azure VMware Solution an die Bandbreite des ExpressRoute-Schaltkreises und des ExpressRoute-Gateways gebunden.
- Für Azure NetApp Files Volumes mit „Standard“-Netzwerkfunktionen wird ExpressRoute FastPath unterstützt. Wenn FastPath aktiviert ist, sendet es den Netzwerkverkehr direkt an Azure NetApp Files Volumes und umgeht dabei das Gateway, wodurch eine höhere Bandbreite und geringere Latenz erreicht wird.

Erhöhen der Größe des Datenspeichers

Die Neugestaltung des Volumes und dynamische Service-Level-Änderungen sind für das SDDC vollständig transparent. In Azure NetApp Files sorgen diese Funktionen für kontinuierliche Leistungs-, Kapazitäts- und Kostenoptimierungen. Erhöhen Sie die Größe von NFS-Datenspeichern, indem Sie die Größe des Volumes über das Azure-Portal oder mithilfe der CLI ändern. Wenn Sie fertig sind, greifen Sie auf vCenter zu, gehen Sie zur Registerkarte „Datenspeicher“, klicken Sie mit der rechten Maustaste auf den entsprechenden Datenspeicher und wählen Sie „Kapazitätsinformationen aktualisieren“. Mit diesem Ansatz können Sie die Kapazität des Datenspeichers erhöhen und die Leistung des Datenspeichers dynamisch und ohne Ausfallzeiten steigern. Dieser Vorgang ist für Anwendungen außerdem völlig transparent.

Wichtige Punkte

- Durch Volume-Reshaping und dynamische Service-Level-Funktionen können Sie die Kosten optimieren, indem Sie die Größe auf stabile Arbeitslasten abstimmen und so eine Überbereitstellung vermeiden.
- VAAI ist nicht aktiviert.

Arbeitslasten

▼ **Migration**

Einer der häufigsten Anwendungsfälle ist die Migration. Verwenden Sie VMware HCX oder vMotion, um lokale VMs zu verschieben. Alternativ können Sie Rivermeadow verwenden, um VMs in Azure NetApp Files -Datenspeicher zu migrieren.

▼ **Datensicherung**

Das Sichern und schnelle Wiederherstellen von VMs gehört zu den großen Stärken von ANF-Datenspeichern. Verwenden Sie Snapshot-Kopien, um schnell Kopien Ihrer VM oder Ihres Datenspeichers zu erstellen, ohne die Leistung zu beeinträchtigen, und senden Sie diese dann zum längerfristigen Datenschutz an den Azure-Speicher oder mithilfe der regionsübergreifenden Replikation zur Notfallwiederherstellung an eine sekundäre Region. Dieser Ansatz minimiert Speicherplatz und Netzwerkbandbreite, indem nur geänderte Informationen gespeichert werden.

Verwenden Sie Azure NetApp Files Snapshot-Kopien zum allgemeinen Schutz und verwenden Sie Anwendungstools zum Schutz von Transaktionsdaten wie SQL Server oder Oracle, die sich auf den Gast-VMs befinden. Diese Snapshot-Kopien unterscheiden sich von VMware-(Konsistenz-)Snapshots und eignen sich für einen längerfristigen Schutz.

Bei ANF-Datenspeichern kann mit der Option „Auf neuem Volume wiederherstellen“ ein

gesamtes Datenspeichervolume geklont werden. Das wiederhergestellte Volume kann dann als weiterer Datenspeicher auf Hosts innerhalb von AVS SDDC bereitgestellt werden. Nachdem ein Datenspeicher bereitgestellt wurde, können darin enthaltene VMs registriert, neu konfiguriert und angepasst werden, als wären sie einzeln geklonte VMs.

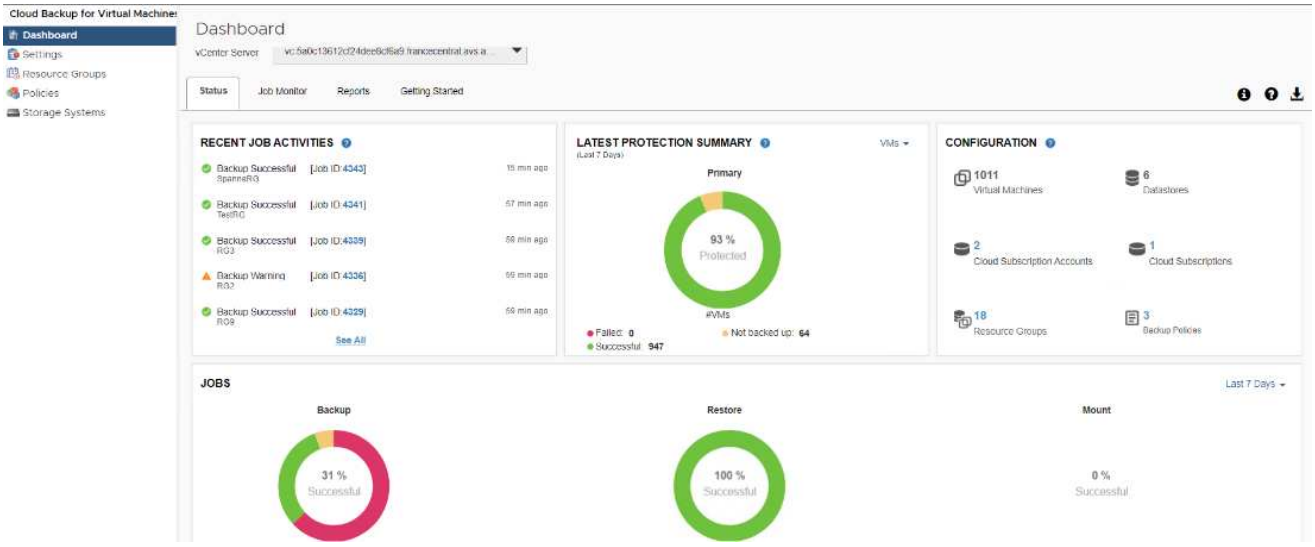
▼ NetApp Backup und Recovery für virtuelle Maschinen

NetApp Backup and Recovery for Virtual Machines bietet eine vSphere Web Client-GUI auf vCenter, um virtuelle Azure VMware Solution Maschinen und Azure NetApp Files Datastores über Backup-Richtlinien zu schützen. Diese Richtlinien können Zeitpläne, Aufbewahrung und weitere Funktionen definieren. Die Funktionalität von NetApp Backup and Recovery for Virtual Machines lässt sich über den Befehl „Run“ einsetzen.

Die Installation der Setup- und Schutzrichtlinien kann durch Ausführen der folgenden Schritte erfolgen:

1. Die Installation von NetApp Backup and Recovery for Virtual Machine in der Azure VMware Solution Private Cloud erfolgt mithilfe des Befehls „Run“.
2. Fügen Sie Anmeldeinformationen für das Cloud-Abonnement (Client und geheimer Wert) hinzu und fügen Sie dann ein Cloud-Abonnementkonto (NetApp -Konto und zugehörige Ressourcengruppe) hinzu, das die Ressourcen enthält, die Sie schützen möchten.
3. Erstellen Sie eine oder mehrere Sicherungsrichtlinien, die die Aufbewahrung, Häufigkeit und andere Einstellungen für Ressourcengruppensicherungen verwalten.
4. Erstellen Sie einen Container, um eine oder mehrere Ressourcen hinzuzufügen, die mit Sicherungsrichtlinien geschützt werden müssen.
5. Stellen Sie im Falle eines Fehlers die gesamte VM oder bestimmte einzelne VMDKs am selben Speicherort wieder her.

Mit der Azure NetApp Files Snapshot-Technologie sind Backups und Wiederherstellungen sehr schnell.



▼ Notfallwiederherstellung mit Azure NetApp Files, JetStream DR und Azure VMware Solution

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Site-Ausfällen und Datenbeschädigungen (z. B. Ransomware) zu schützen. Mithilfe des VMware VAIO-Frameworks können lokale VMware-Workloads in den Azure Blob-Speicher repliziert und wiederhergestellt werden, wodurch ein minimaler oder nahezu kein Datenverlust und eine RTO von nahezu null möglich sind. Mit JetStream DR können die vom lokalen Standort auf AVS und insbesondere

auf Azure NetApp Files replizierten Workloads nahtlos wiederhergestellt werden. Es ermöglicht eine kostengünstige Notfallwiederherstellung durch die Nutzung minimaler Ressourcen am DR-Standort und kostengünstigen Cloud-Speicher. JetStream DR automatisiert die Wiederherstellung in ANF-Datenspeichern über Azure Blob Storage. JetStream DR stellt unabhängige VMs oder Gruppen verwandter VMs gemäß der Netzwerkzuordnung in der Infrastruktur des Wiederherstellungsstandorts wieder her und bietet eine zeitpunktbezogene Wiederherstellung zum Schutz vor Ransomware.

"DR-Lösung mit ANF, JetStream und AVS" .

NetApp -Gastspeicheroptionen für Azure

Azure unterstützt über Gäste verbundene NetApp -Speicher mit dem nativen Azure NetApp Files (ANF)-Dienst oder mit Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure netApp Files bringt Datenverwaltung und -speicherung auf Unternehmensniveau zu Azure, sodass Sie Ihre Workloads und Anwendungen problemlos verwalten können. Migrieren Sie Ihre Workloads in die Cloud und führen Sie sie ohne Leistungseinbußen aus.

Azure netApp Files beseitigt Hindernisse, sodass Sie alle Ihre dateibasierten Anwendungen in die Cloud verschieben können. Zum ersten Mal müssen Sie Ihre Anwendungen nicht neu strukturieren und erhalten dauerhaften Speicher für Ihre Anwendungen ohne Komplexität.

Da der Dienst über das Microsoft Azure-Portal bereitgestellt wird, profitieren Benutzer im Rahmen ihres Microsoft Enterprise Agreement von einem vollständig verwalteten Dienst. Dank des erstklassigen Supports von Microsoft können Sie sich vollkommen beruhigt zurücklehnen. Mit dieser Einzellösung können Sie schnell und einfach Multiprotokoll-Workloads hinzufügen. Sie können sowohl dateibasierte Windows- als auch Linux-Anwendungen erstellen und bereitstellen, sogar für Legacy-Umgebungen.

Azure NetApp Files (ANF) als mit dem Gast verbundener Speicher

▼ **Konfigurieren von Azure NetApp Files mit Azure VMware Solution (AVS)**

Azure NetApp Files Freigaben können von VMs bereitgestellt werden, die in der Azure VMware Solution SDDC-Umgebung erstellt wurden. Die Volumes können auch auf dem Linux-Client gemountet und auf dem Windows-Client zugeordnet werden, da Azure NetApp Files SMB- und NFS-Protokolle unterstützt. Azure NetApp Files Volumes können in fünf einfachen Schritten eingerichtet werden.

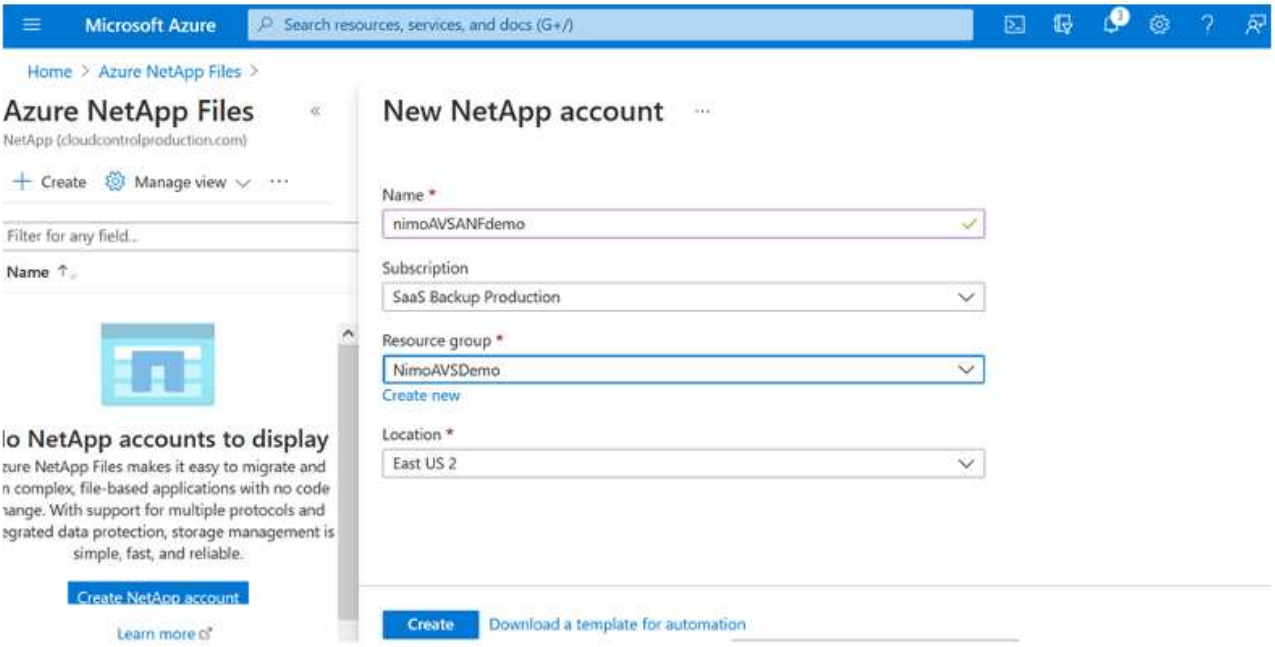
Azure NetApp Files und Azure VMware Solution müssen sich in derselben Azure-Region befinden.

▼ **Erstellen und Einbinden von Azure NetApp Files Volumes**

Führen Sie die folgenden Schritte aus, um Azure NetApp Files Volumes zu erstellen und einzubinden:

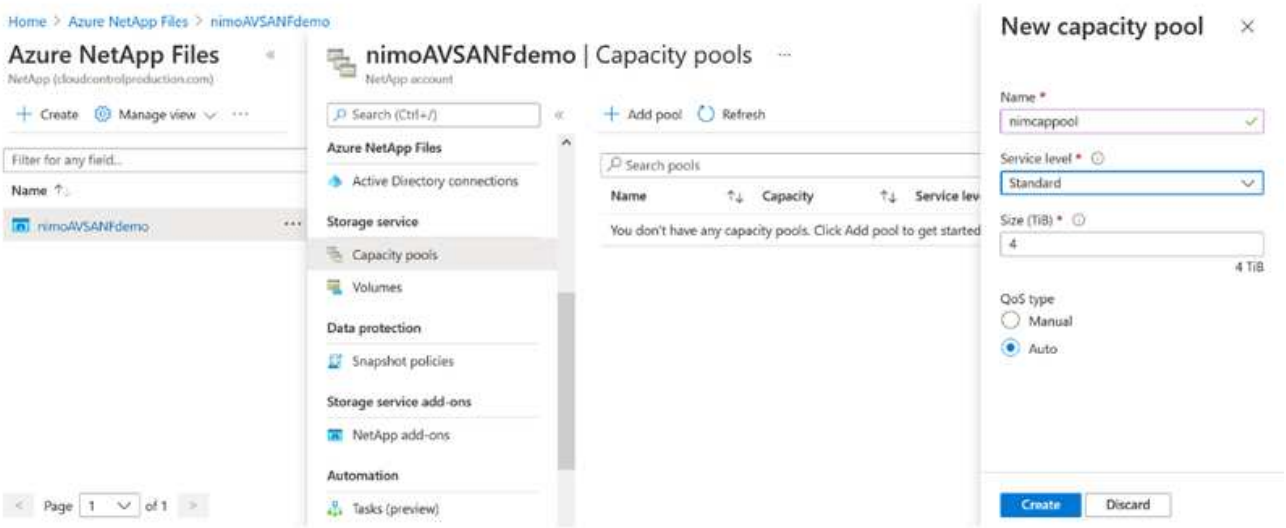
1. Melden Sie sich beim Azure-Portal an und greifen Sie auf Azure NetApp Files zu. Überprüfen Sie den Zugriff auf den Azure NetApp Files -Dienst und registrieren Sie den Azure NetApp Files Ressourcenanbieter mit dem Befehl *az provider register --namespace Microsoft. NetApp –wait*. Erstellen Sie nach Abschluss der Registrierung ein NetApp -Konto.

   Ausführliche Schritte finden Sie unter"Azure NetApp Files Freigaben" . Diese Seite führt Sie Schritt für Schritt durch den Prozess.

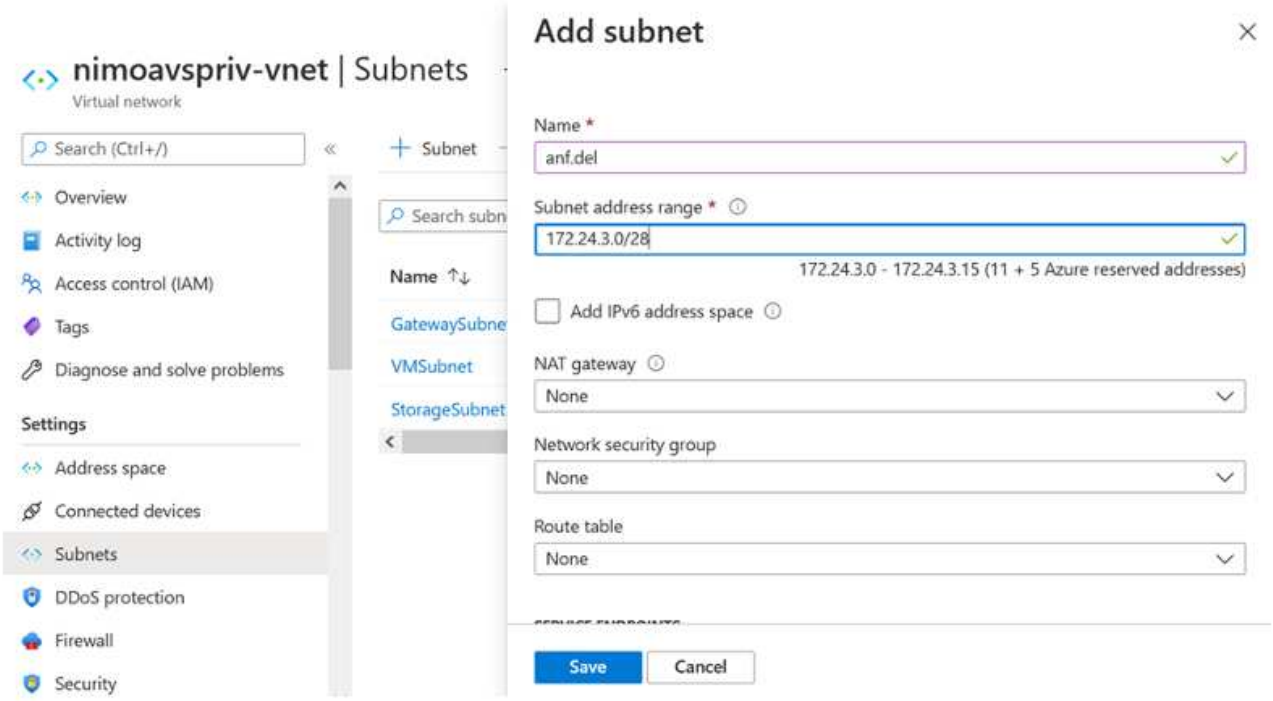


2. Nachdem das NetApp -Konto erstellt wurde, richten Sie die Kapazitätspools mit dem erforderlichen Servicelevel und der erforderlichen Größe ein.

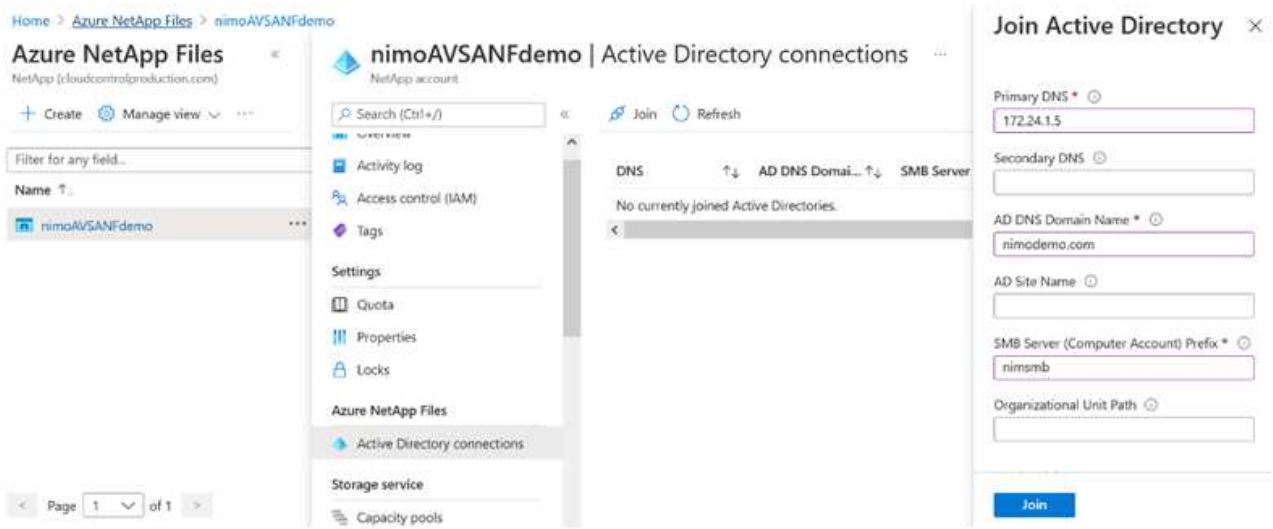
   Weitere Informationen finden Sie unter "Einrichten eines Kapazitätspools" .



3. Konfigurieren Sie das delegierte Subnetz für Azure NetApp Files und geben Sie dieses Subnetz beim Erstellen der Volumes an. Ausführliche Schritte zum Erstellen eines delegierten Subnetzes finden Sie unter"Delegieren eines Subnetzes an Azure NetApp Files" .

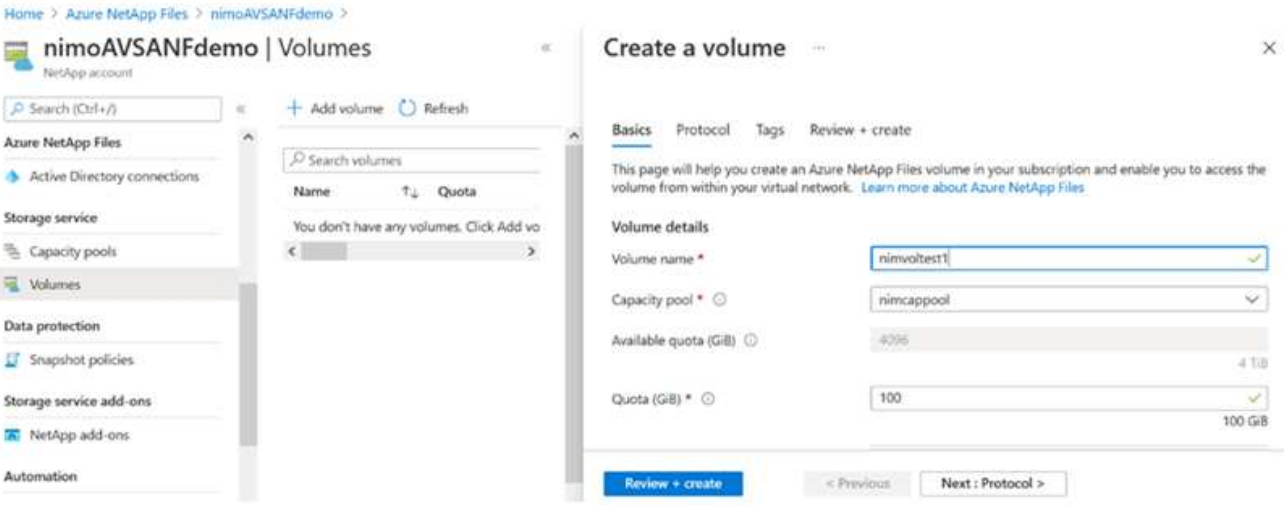


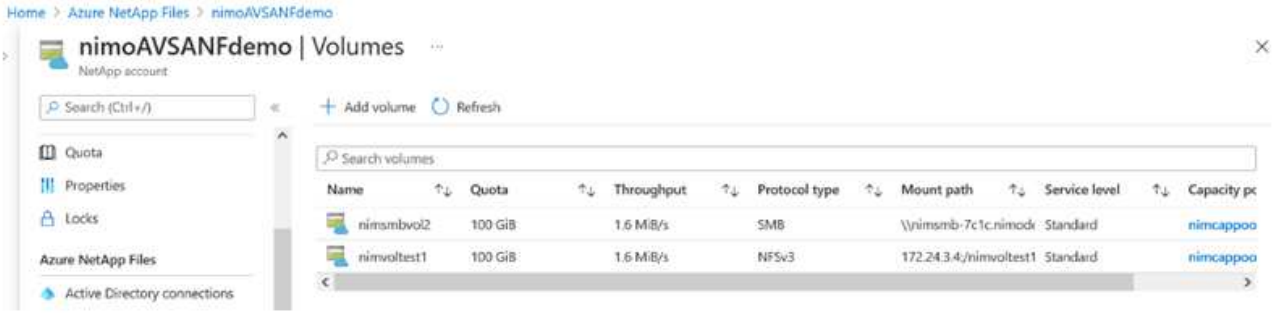
4. Fügen Sie mithilfe des Blatts „Volumes“ unter dem Blatt „Kapazitätspools“ ein SMB-Volume hinzu. Stellen Sie sicher, dass der Active Directory-Connector konfiguriert ist, bevor Sie das SMB-Volume erstellen.



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

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

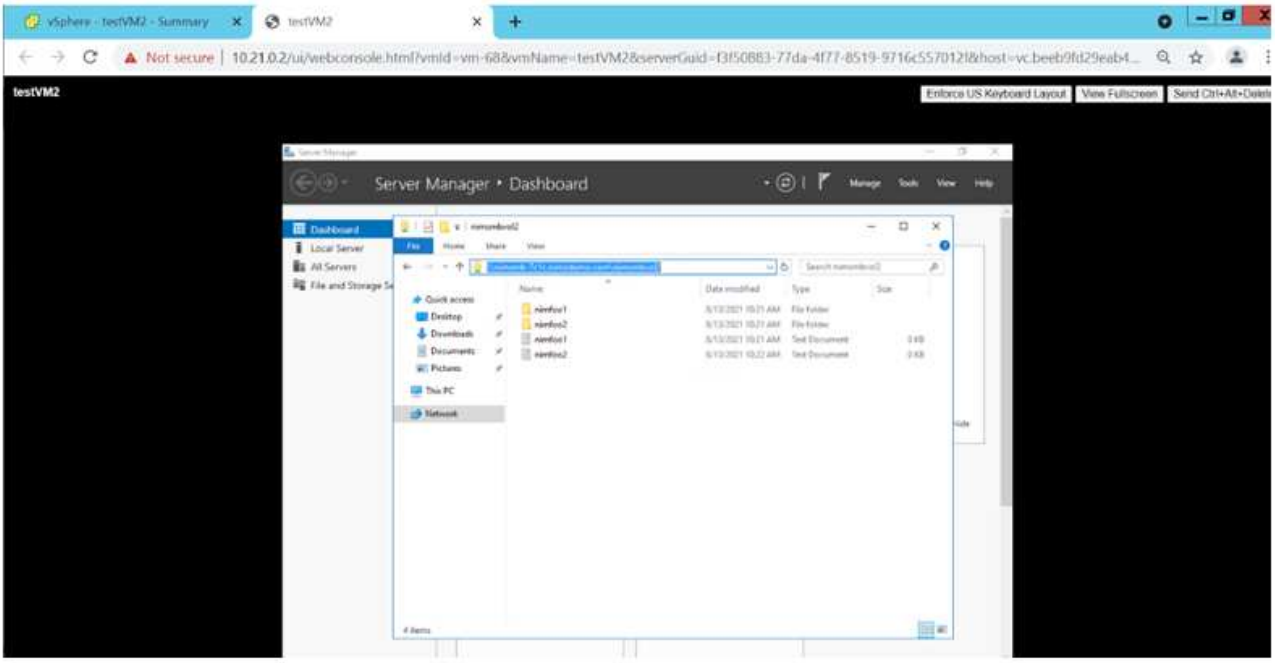


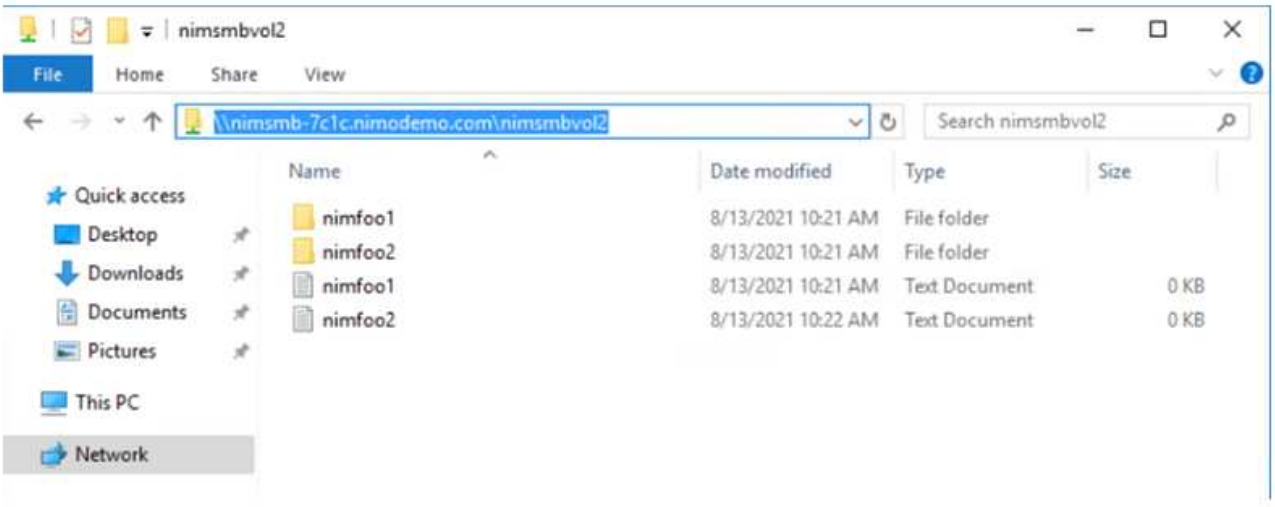


Weitere Informationen zur Volumeleistung von Azure NetApp Files nach Größe oder Kontingent finden Sie unter"Leistungsüberlegungen für Azure NetApp Files" .

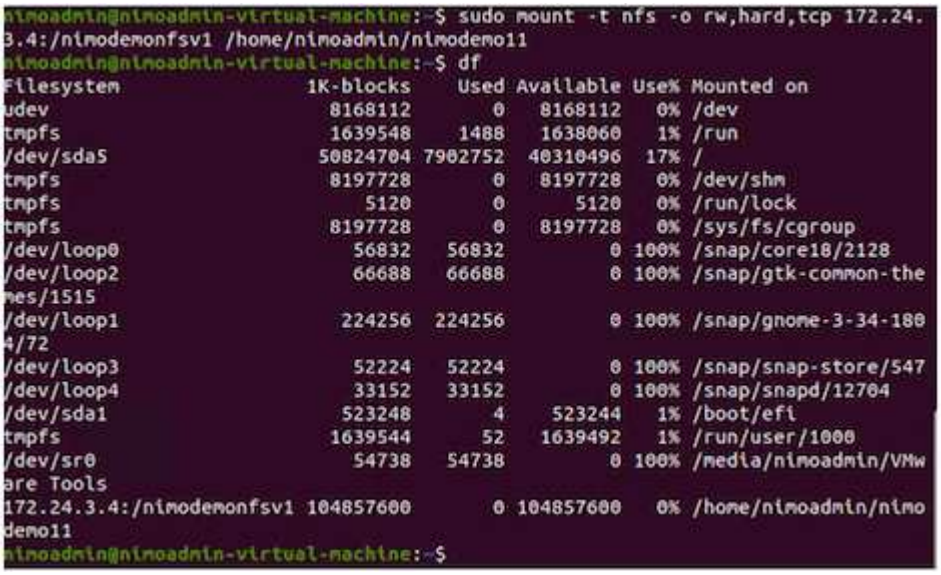
6. Nachdem die Verbindung hergestellt ist, kann das Volume gemountet und für Anwendungsdaten verwendet werden.

   Klicken Sie hierzu im Azure-Portal auf das Blatt „Volumes“, wählen Sie dann das zu mountende Volume aus und greifen Sie auf die Mount-Anweisungen zu. Kopieren Sie den Pfad und verwenden Sie die Option „Netzlaufwerk zuordnen“, um das Volume auf der VM bereitzustellen, die auf Azure VMware Solution SDDC ausgeführt wird.





7. Verwenden Sie denselben Prozess, um NFS-Volumes auf Linux-VMs bereitzustellen, die auf Azure VMware Solution SDDC ausgeführt werden. Nutzen Sie Volume-Reshaping oder dynamische Service-Level-Funktionen, um die Workload-Anforderungen zu erfüllen.



Weitere Informationen finden Sie unter "Dynamisches Ändern des Servicelevels eines Volumes" .

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenverwaltungslösung, die auf der ONTAP -Speichersoftware von NetApp basiert und nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar ist.

Es handelt sich um eine softwaredefinierte Version von ONTAP , die Cloud-nativen Speicher nutzt. Dadurch können Sie in der Cloud und vor Ort dieselbe Speichersoftware verwenden und müssen Ihr IT-Personal nicht mehr in völlig neuen Methoden zur Verwaltung Ihrer Daten schulen.

CVO bietet Kunden die Möglichkeit, Daten nahtlos vom Edge zum Rechenzentrum, in die Cloud und zurück zu verschieben und so Ihre Hybrid Cloud zusammenzuführen – alles verwaltet über eine zentrale Verwaltungskonsole, den NetApp Cloud Manager.

CVO bietet von Haus aus extreme Leistung und erweiterte Datenverwaltungsfunktionen, um selbst Ihre anspruchsvollsten Anwendungen in der Cloud zu erfüllen

Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher

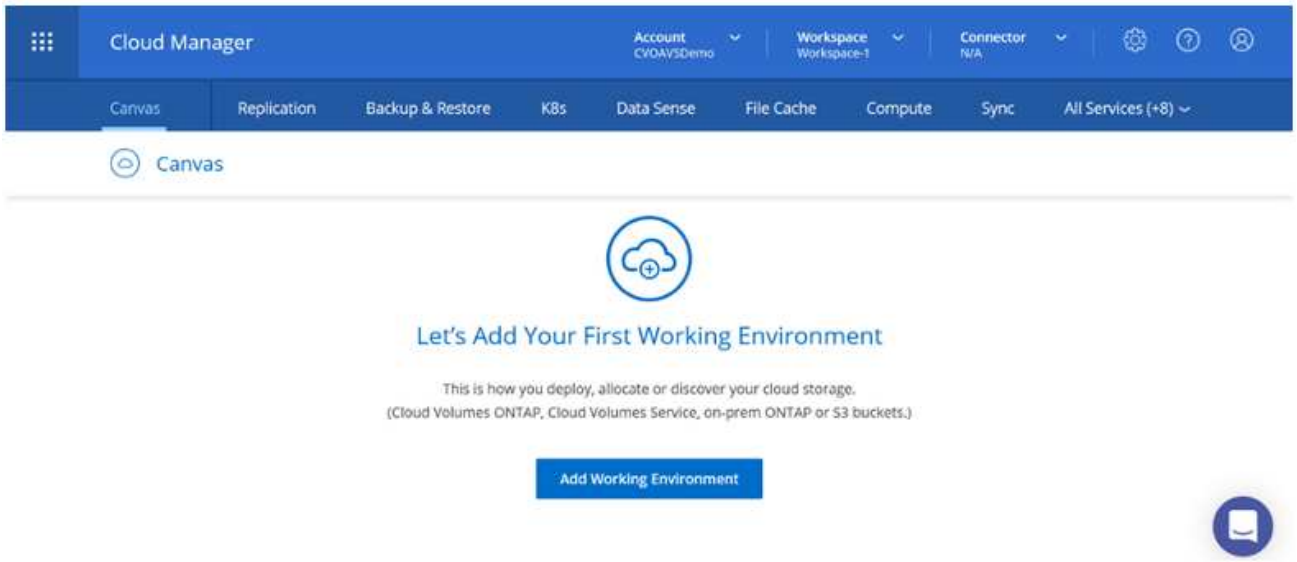
▼ **Stellen Sie das neue Cloud Volumes ONTAP in Azure bereit**

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

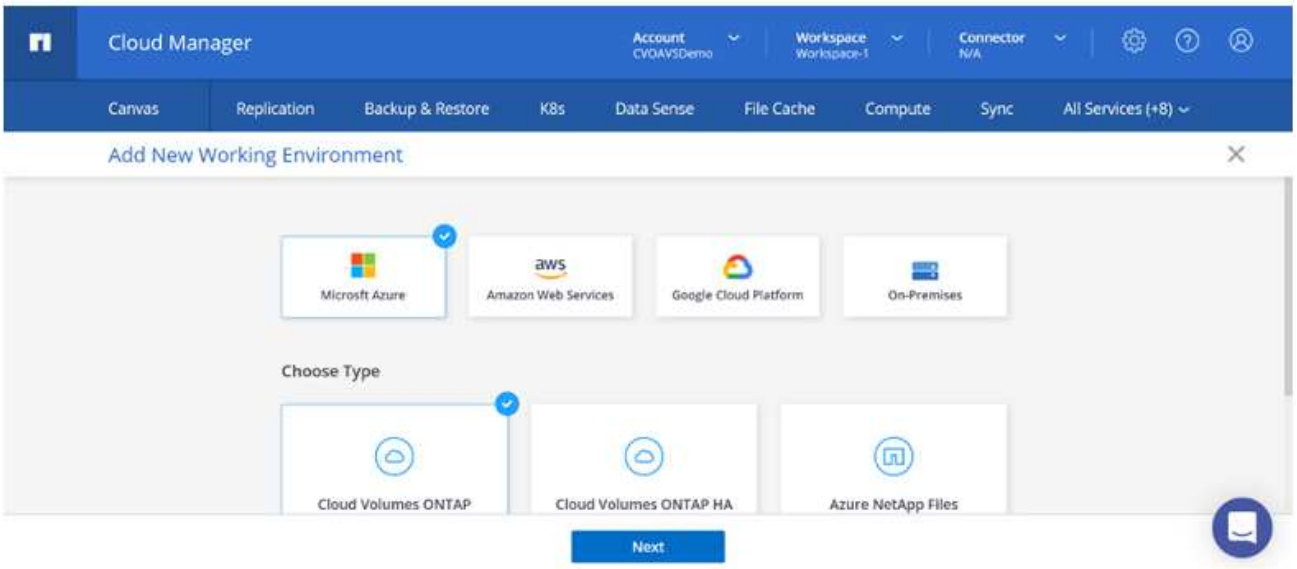
Um Volumes aus einer lokalen Umgebung zur Notfallwiederherstellung oder Migration in die Cloud zu replizieren, stellen Sie eine Netzwerkverbindung zu Azure her, entweder über ein Site-to-Site-VPN oder ExpressRoute. Das Replizieren von Daten von lokalen Standorten auf Cloud Volumes ONTAP fällt nicht in den Geltungsbereich dieses Dokuments. Informationen zum Replizieren von Daten zwischen lokalen und Cloud Volumes ONTAP Systemen finden Sie unter"Einrichten der Datenreplikation zwischen Systemen" .

Mit "Cloud Volumes ONTAP Sizer" lassen sich die Cloud Volumes ONTAP Instanzen präzise dimensionieren. Außerdem dient die Überwachung der On-Premises-Performance als Eingabedaten für den Cloud Volumes ONTAP Sizer.

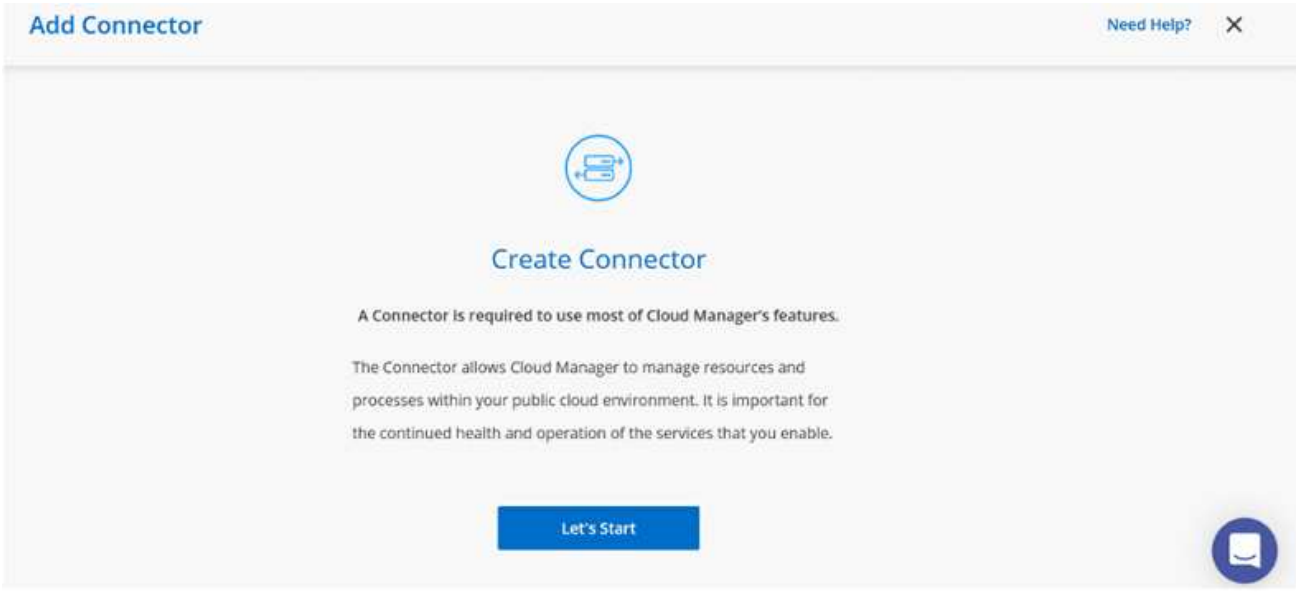
1. Melden Sie sich bei NetApp Cloud Central an – der Fabric View-Bildschirm wird angezeigt. Suchen Sie die Registerkarte „Cloud Volumes ONTAP“ und wählen Sie „Gehe zu Cloud Manager“ aus. Nachdem Sie sich angemeldet haben, wird der Canvas-Bildschirm angezeigt.



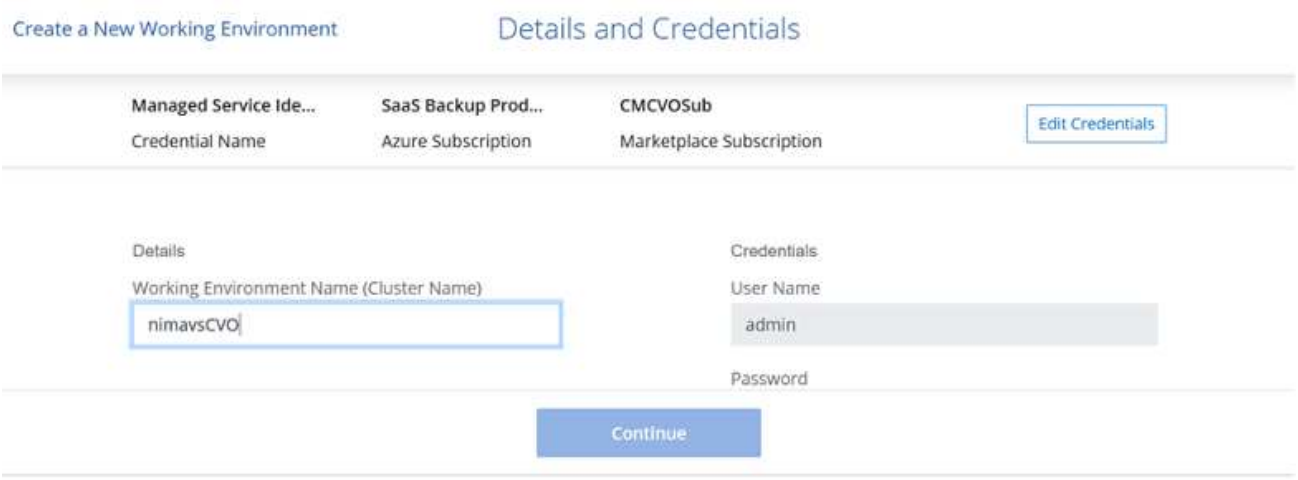
2. Klicken Sie auf der Cloud Manager-Startseite auf „Arbeitsumgebung hinzufügen“ und wählen Sie dann Microsoft Azure als Cloud und den Typ der Systemkonfiguration aus.



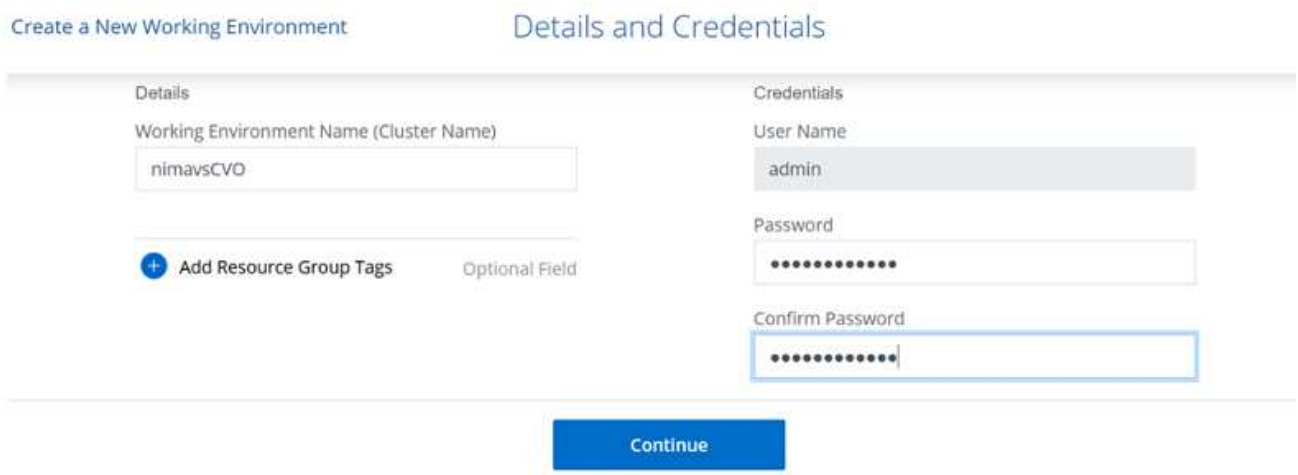
3. Beim Erstellen der ersten Cloud Volumes ONTAP Arbeitsumgebung fordert Cloud Manager Sie auf, einen Connector bereitzustellen.



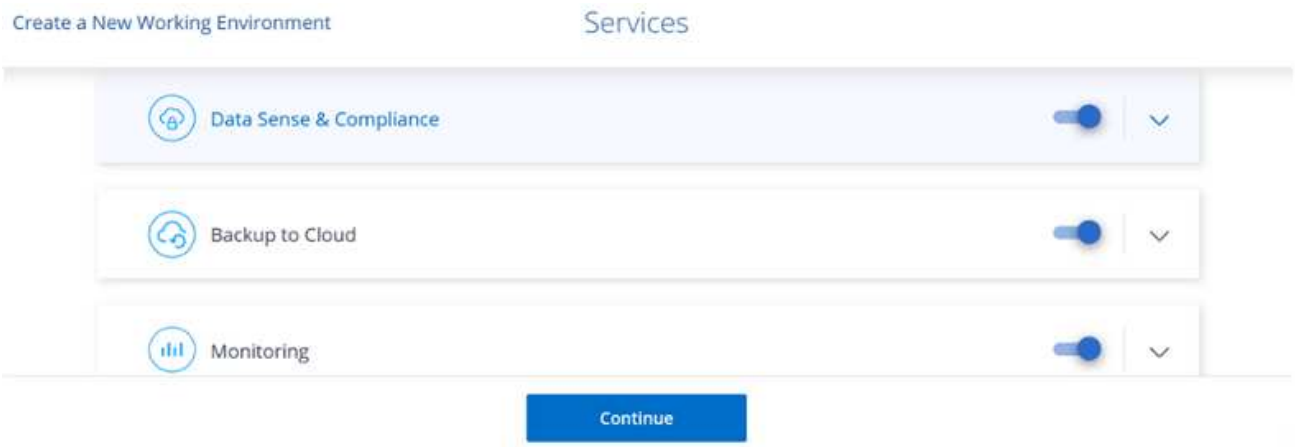
4. Aktualisieren Sie nach der Erstellung des Connectors die Felder „Details“ und „Anmeldeinformationen“.



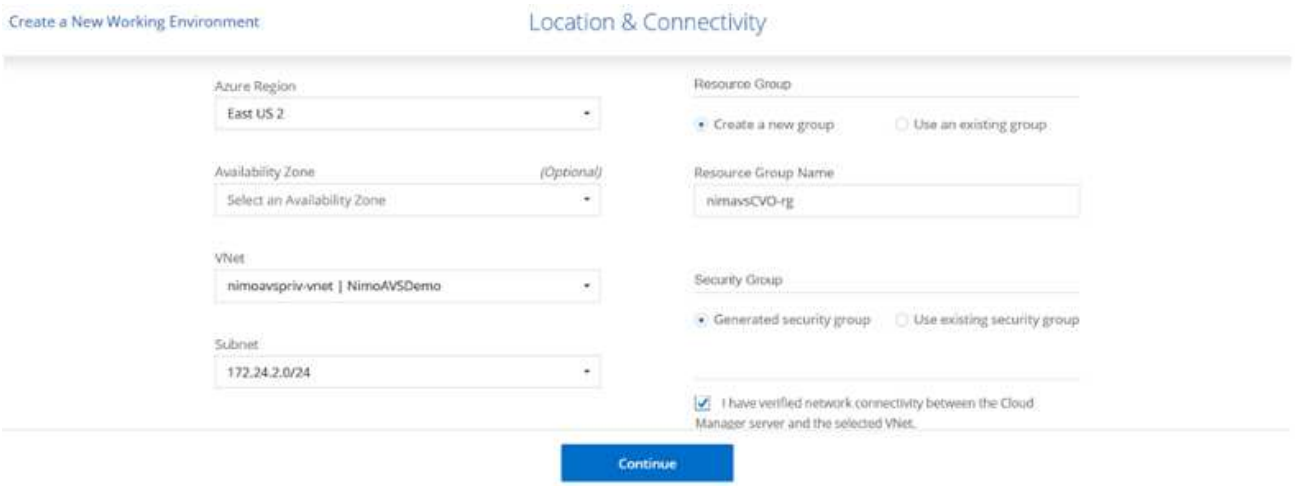
5. Geben Sie die Details der zu erstellenden Umgebung an, einschließlich Umgebungsname und Administratoranmeldeinformationen. Fügen Sie Ressourcengruppen-Tags für die Azure-Umgebung als optionalen Parameter hinzu. Wenn Sie fertig sind, klicken Sie auf „Weiter“.



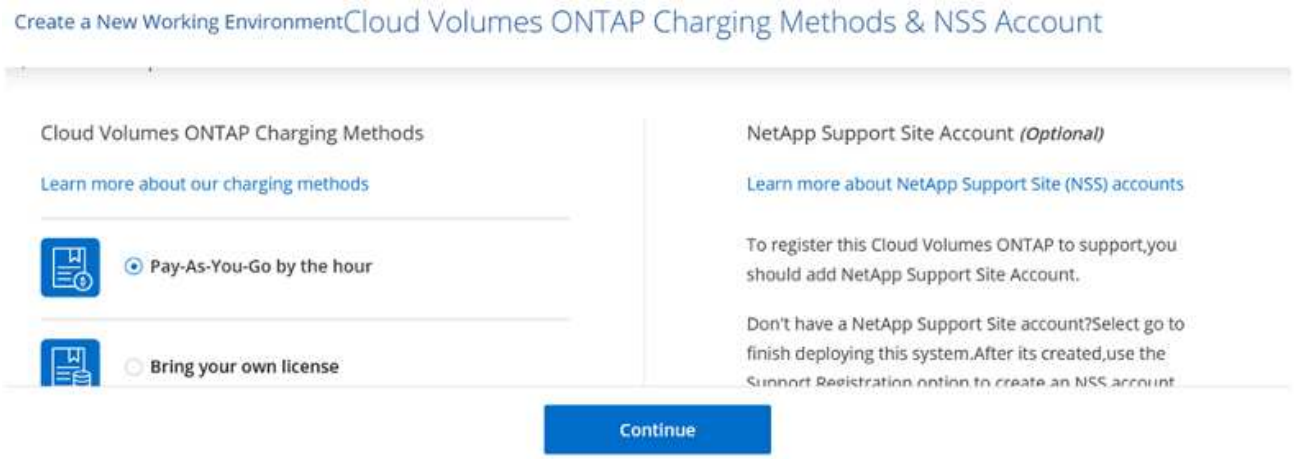
6. Es sind die Add-on Services für das Deployment von Cloud Volumes ONTAP auszuwählen, darunter NetApp Data Classification, NetApp Backup and Recovery und Data Infrastructure Insights. Die Services sind auszuwählen, und anschließend ist auf „Weiter“ zu klicken.



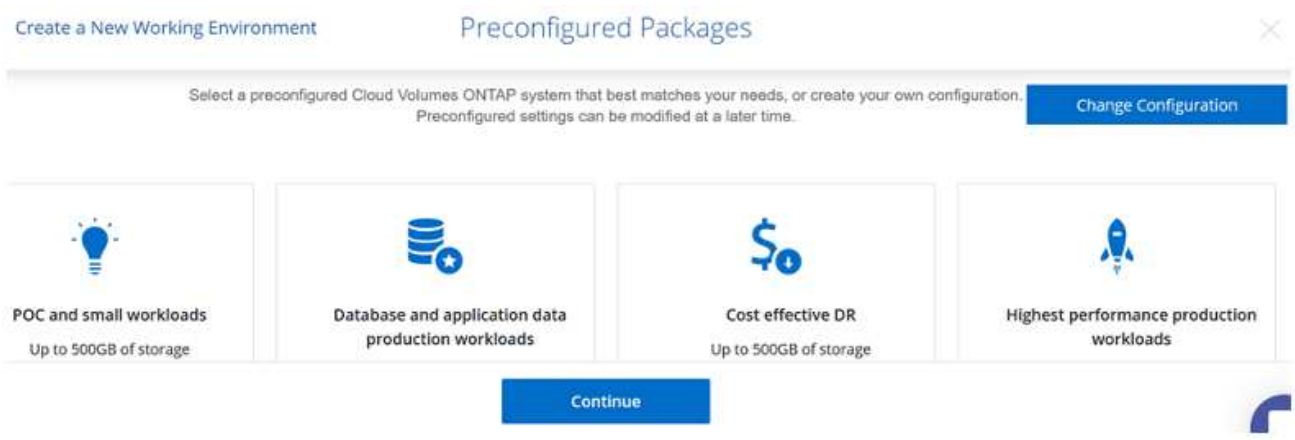
7. Konfigurieren Sie den Azure-Standort und die Konnektivität. Wählen Sie die zu verwendende Azure-Region, Ressourcengruppe, das VNet und das Subnetz aus.



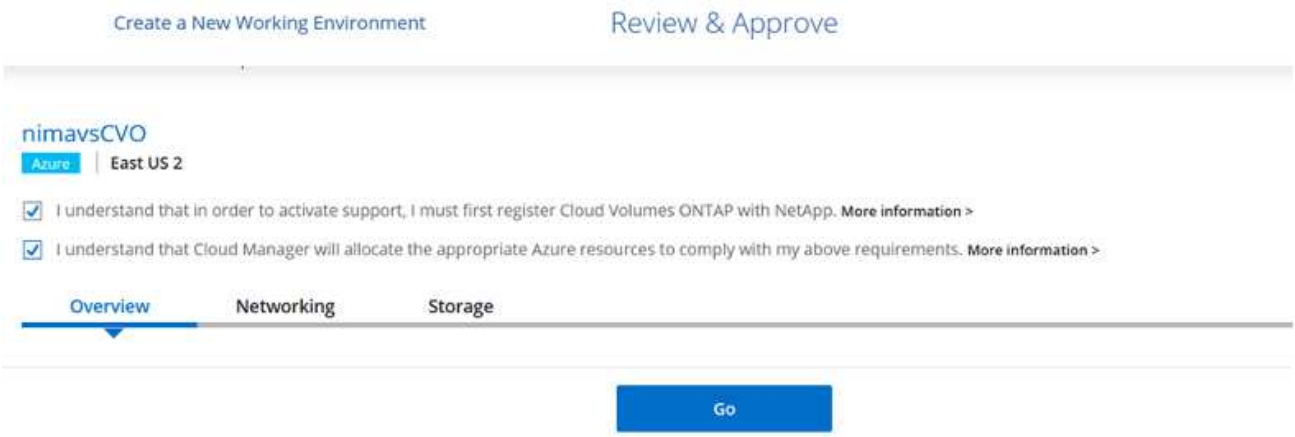
8. Wählen Sie die Lizenzoption: Pay-As-You-Go oder BYOL zur Verwendung einer vorhandenen Lizenz. In diesem Beispiel wird die Pay-As-You-Go-Option verwendet.



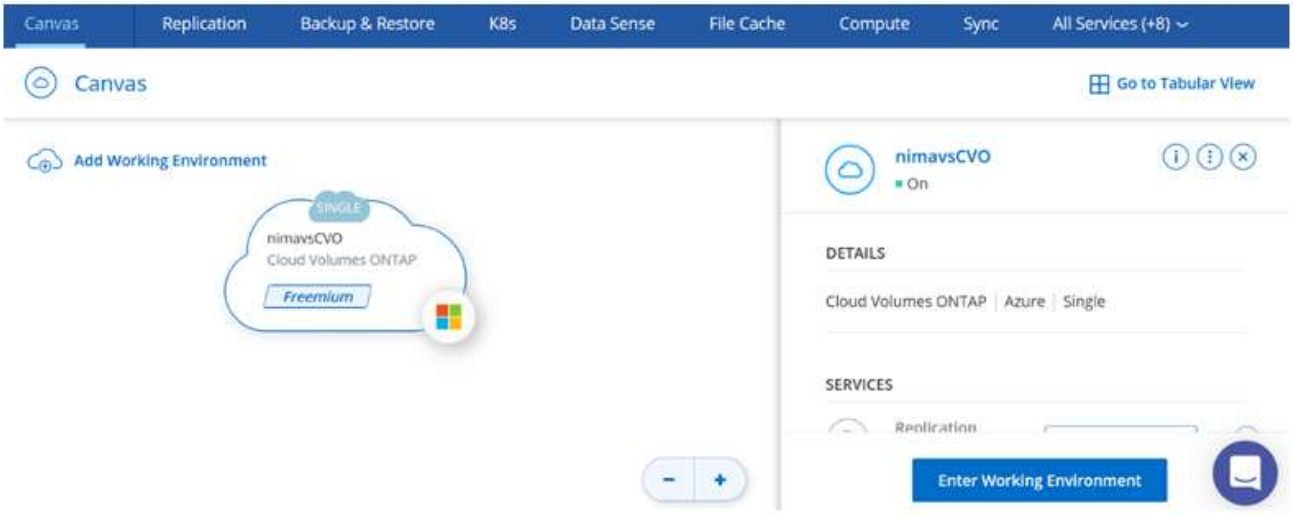
9. Wählen Sie zwischen mehreren vorkonfigurierten Paketen, die für die verschiedenen Arten von Workloads verfügbar sind.



10. Akzeptieren Sie die beiden Vereinbarungen bezüglich der Aktivierung des Supports und der Zuweisung von Azure-Ressourcen. Klicken Sie auf „Los“, um die Cloud Volumes ONTAP -Instanz zu erstellen.

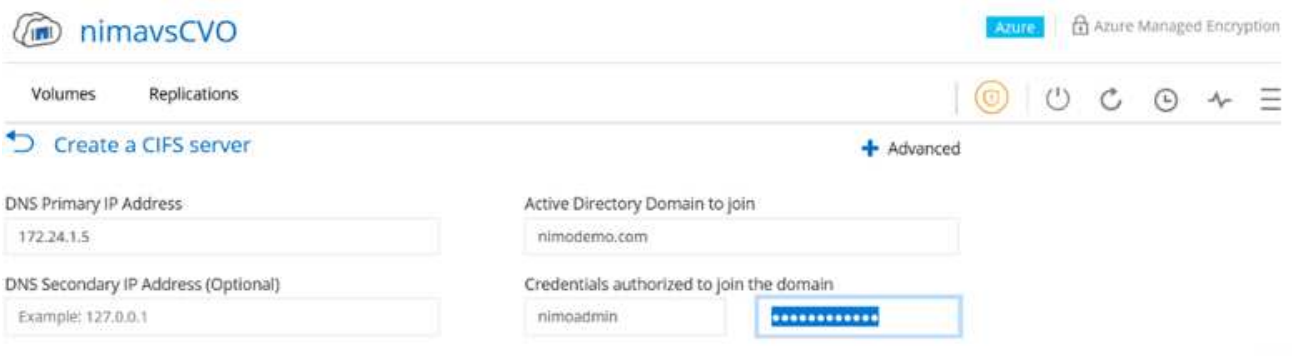


11. Nachdem Cloud Volumes ONTAP bereitgestellt wurde, wird es in den Arbeitsumgebungen auf der Canvas-Seite aufgeführt.

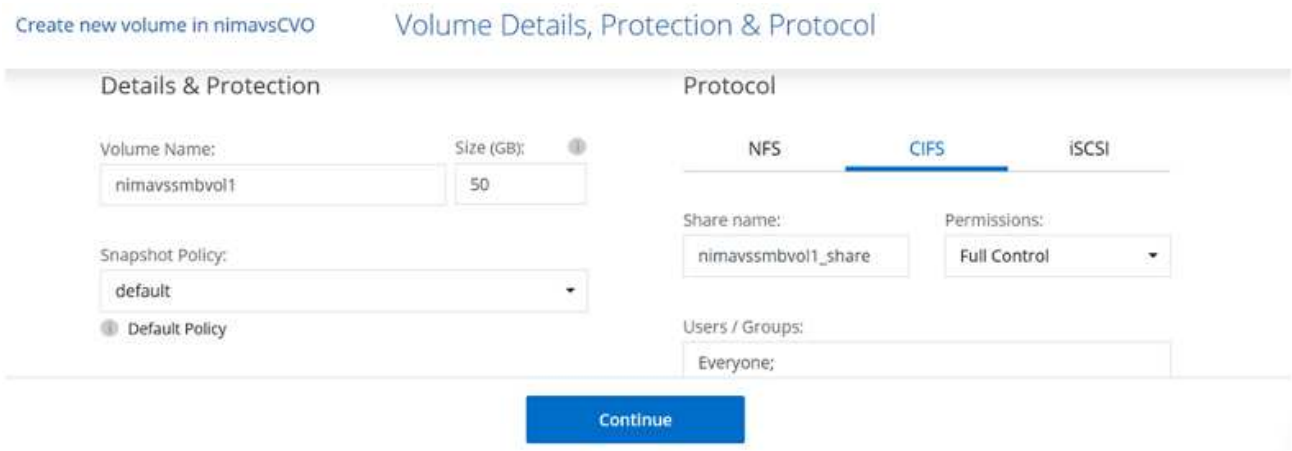


▼ Zusätzliche Konfigurationen für SMB-Volumes

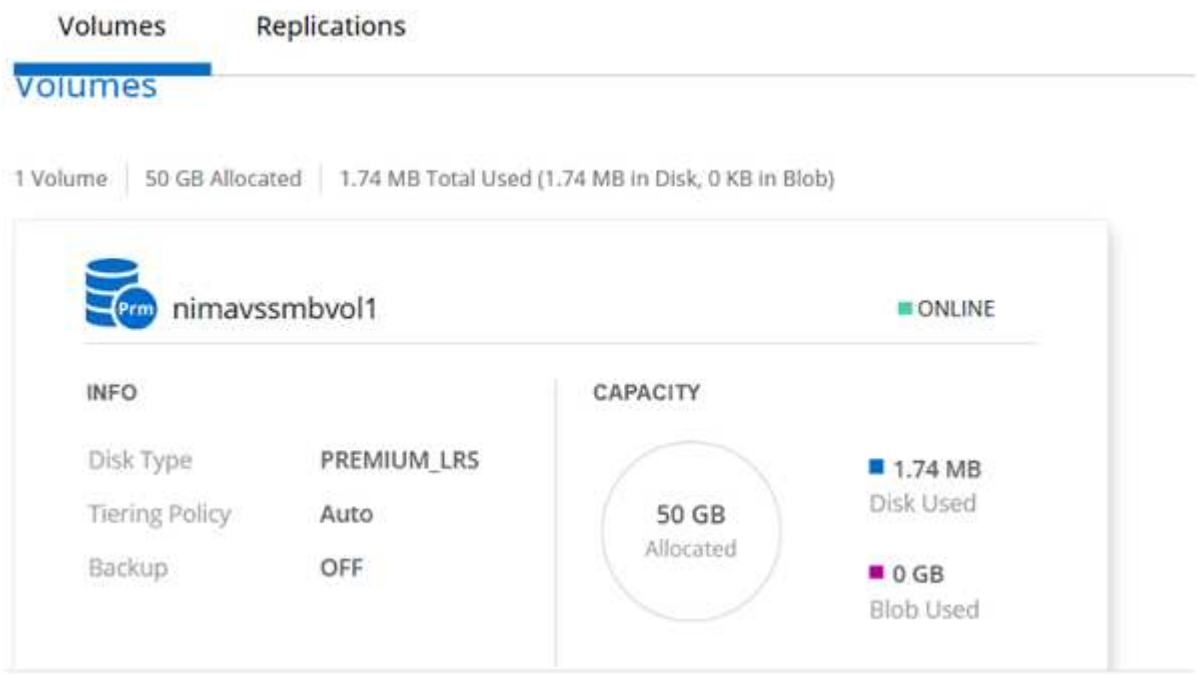
1. Nachdem die Arbeitsumgebung bereit ist, stellen Sie sicher, dass der CIFS-Server mit den entsprechenden DNS- und Active Directory-Konfigurationsparametern konfiguriert ist. Dieser Schritt ist erforderlich, bevor Sie das SMB-Volume erstellen können.



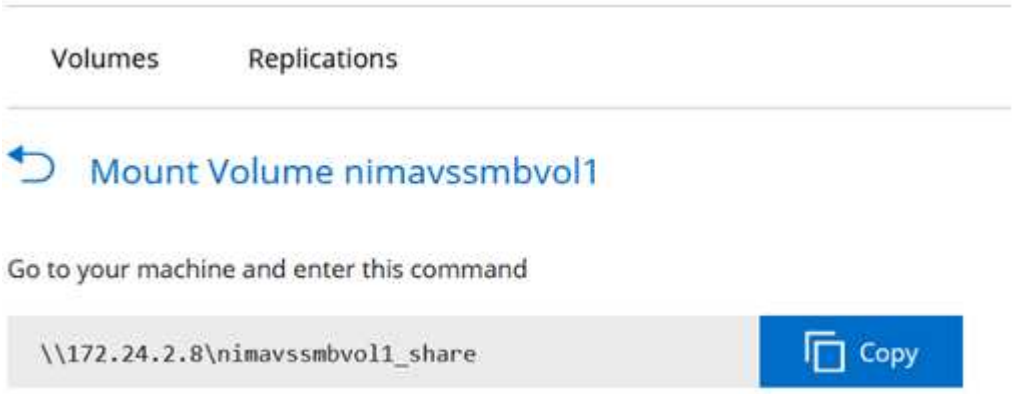
2. Das Erstellen des SMB-Volumes ist ein einfacher Vorgang. Wählen Sie die CVO-Instanz aus, um das Volume zu erstellen, und klicken Sie auf die Option „Volume erstellen“. Wählen Sie die entsprechende Größe und der Cloud-Manager wählt das enthaltene Aggregat aus oder verwenden Sie einen erweiterten Zuordnungsmechanismus, um die Platzierung auf einem bestimmten Aggregat vorzunehmen. Für diese Demo wird SMB als Protokoll ausgewählt.

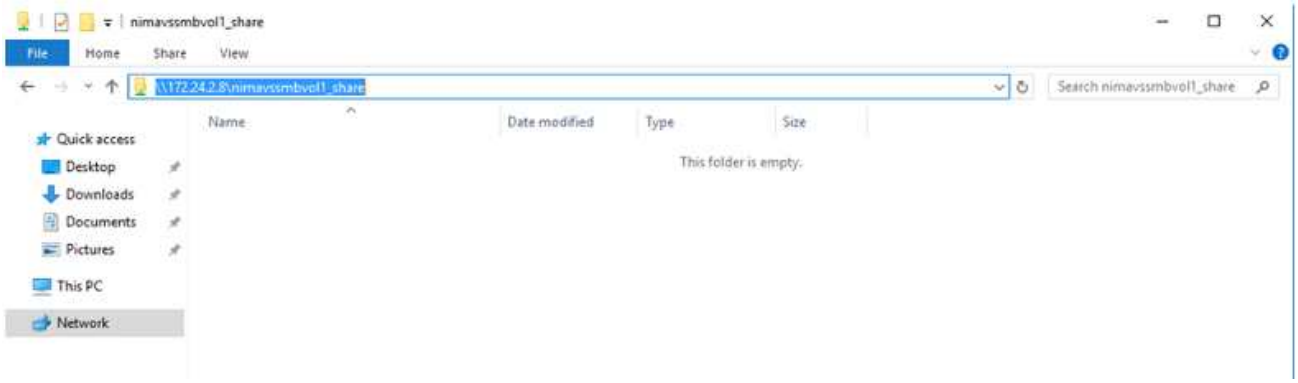


3. Nachdem das Volume bereitgestellt wurde, ist es im Bereich „Volumes“ verfügbar. Da eine CIFS-Freigabe bereitgestellt wird, erteilen Sie Ihren Benutzern oder Gruppen die Berechtigung für die Dateien und Ordner und stellen Sie sicher, dass diese Benutzer auf die Freigabe zugreifen und eine Datei erstellen können. Dieser Schritt ist nicht erforderlich, wenn das Volume aus einer lokalen Umgebung repliziert wird, da alle Datei- und Ordnerberechtigungen als Teil der SnapMirror Replikation beibehalten werden.



4. Nachdem das Volume erstellt wurde, verwenden Sie den Mount-Befehl, um von der VM, die auf den Azure VMware Solution SDDC-Hosts ausgeführt wird, eine Verbindung mit der Freigabe herzustellen.
5. Kopieren Sie den folgenden Pfad und verwenden Sie die Option „Netzlaufwerk zuordnen“, um das Volume auf der VM bereitzustellen, die auf Azure VMware Solution SDDC ausgeführt wird.

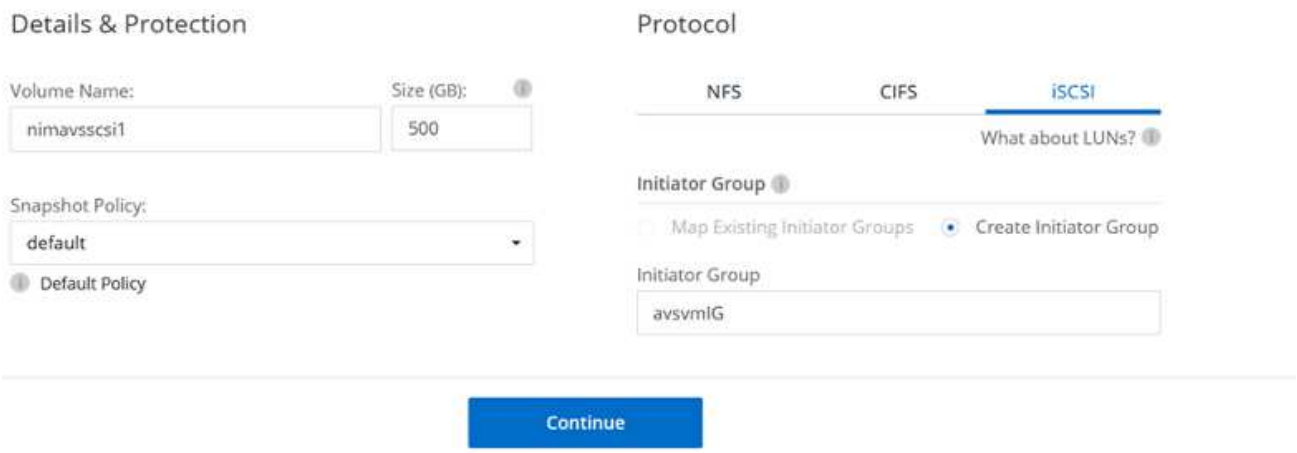




▼ Verbinden Sie die LUN mit einem Host

Führen Sie die folgenden Schritte aus, um die LUN mit einem Host zu verbinden:

1. Doppelklicken Sie auf der Canvas-Seite auf die Arbeitsumgebung 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“.



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

   So erreichen Sie dasselbe für den Host, der sich auf Azure VMware Solution SDDC befindet:

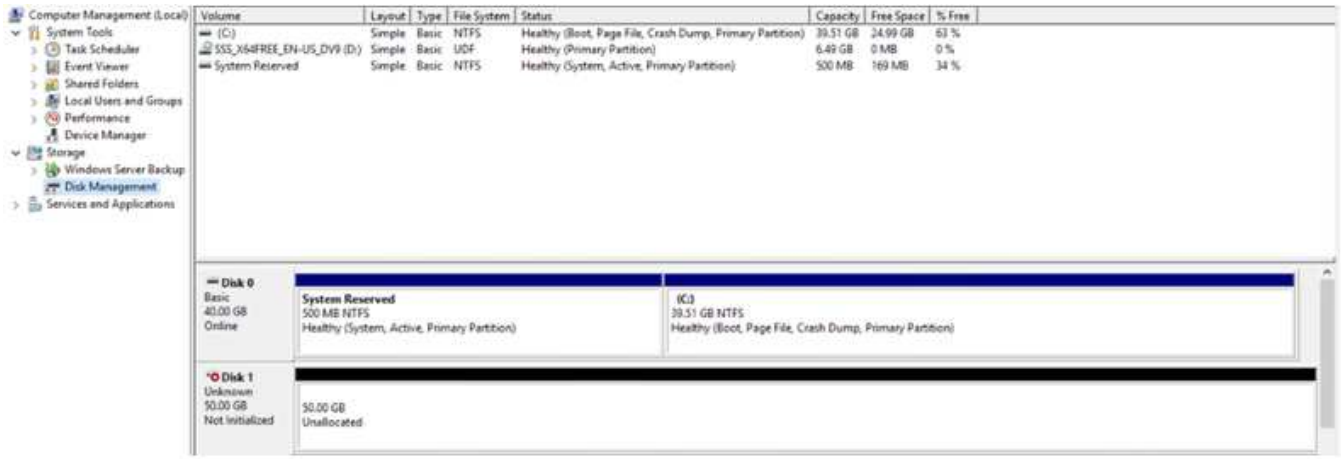
   a. RDP zur VM, die auf Azure VMware Solution SDDC gehostet wird.
   b. Öffnen Sie das Dialogfeld „Eigenschaften des iSCSI-Initiators“: Server-Manager > Dashboard > Tools > iSCSI-Initiator.
   c. Klicken Sie auf der Registerkarte „Erkennung“ auf „Portal erkennen“ oder „Portal hinzufügen“ und geben Sie 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 „Multipfad aktivieren“ und dann „Diese Verbindung beim Start des Computers automatisch wiederherstellen“ oder „Diese Verbindung zur Liste der bevorzugten Ziele hinzufügen“. Klicken Sie auf „Erweitert“.

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



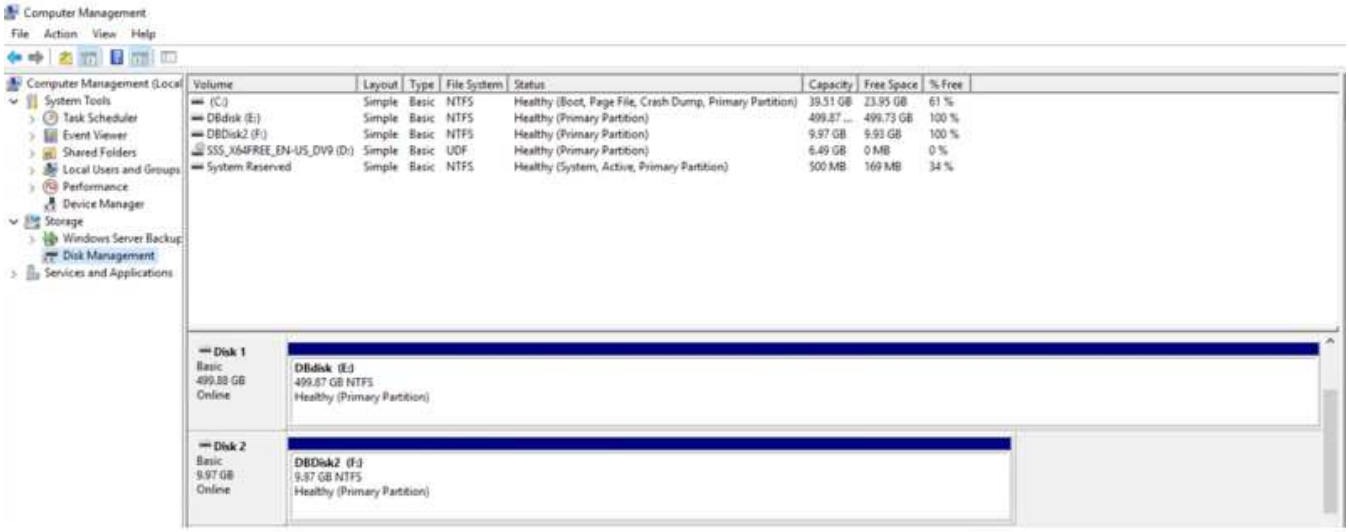
LUNs auf der Storage Virtual Machine (SVM) werden dem Windows-Host als Datenträger angezeigt. Alle neu hinzugefügten Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen erneuten Scan aus, um die Datenträger zu ermitteln, indem Sie die folgenden Schritte ausführen:

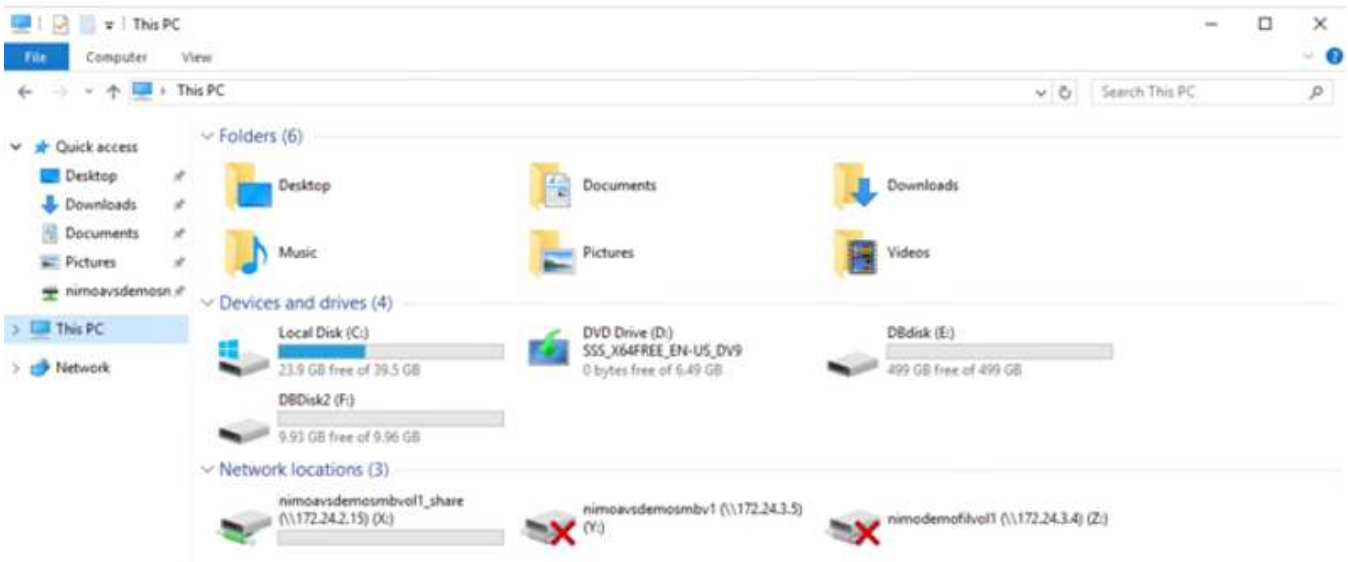
1. Öffnen Sie das Windows-Dienstprogramm „Computerverwaltung“: Start > Verwaltung > Computerverwaltung.
2. Erweitern Sie den Knoten „Speicher“ im Navigationsbaum.
3. Klicken Sie auf Datenträgerverwaltung.
4. Klicken Sie auf „Aktion“ > „Datenträger erneut scannen“.



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

1. Starten Sie die Windows-Datenträgerverwaltung.
2. Klicken Sie mit der rechten Maustaste auf die LUN und wählen Sie dann den erforderlichen Datenträger- oder Partitionstyp aus.
3. Folgen Sie den Anweisungen des Assistenten. In diesem Beispiel ist Laufwerk E: gemountet





Google Cloud VMware Engine: Optionen für die Verwendung von NetApp -Speicher

NetApp -Speicher kann entweder als Gastspeicher oder als Zusatzspeicher an die Google Cloud Virtualization Engine angeschlossen werden.

Google Cloud NetApp Volumes (NetApp Volumes) als ergänzender NFS-Datenspeicher

Kunden, die zusätzliche Speicherkapazität in ihrer Google Cloud VMware Engine (GCVE)-Umgebung benötigen, können Google Cloud NetApp Volumes als zusätzlichen NFS-Datenspeicher nutzen. Durch die Speicherung von Daten auf Google Cloud NetApp Volumes können Kunden zum Schutz vor Katastrophen eine Replikation zwischen Regionen durchführen.

Weitere Informationen finden Sie unter"Google Cloud NetApp Volumes (NetApp Volumes) als ergänzender NFS-Datenspeicher"

NetApp CVO als Gast-Connected-Storage

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenverwaltungslösung, die auf der ONTAP -Speichersoftware von NetApp basiert und nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar ist.

Es handelt sich um eine softwaredefinierte Version von ONTAP , die Cloud-nativen Speicher nutzt. Dadurch können Sie in der Cloud und vor Ort dieselbe Speichersoftware verwenden und müssen Ihr IT-Personal nicht mehr in völlig neuen Methoden zur Verwaltung Ihrer Daten schulen.

CVO bietet Kunden die Möglichkeit, Daten nahtlos vom Edge zum Rechenzentrum, in die Cloud und zurück zu verschieben und so Ihre Hybrid Cloud zusammenzuführen – alles verwaltet über eine zentrale Verwaltungskonsole, den NetApp Cloud Manager.

CVO bietet von Haus aus extreme Leistung und erweiterte Datenverwaltungsfunktionen, um selbst Ihre anspruchsvollsten Anwendungen in der Cloud zu erfüllen.

Weitere Informationen finden Sie unter"NetApp CVO als Gast-Connected-Storage"

Google Cloud NetApp Volumes (NetApp Volumes) als Gast-verbundener Speicher

Google Cloud NetApp Volumes Freigaben können von VMs bereitgestellt werden, die in der VMware Engine-Umgebung erstellt wurden. Die Volumes können auch auf dem Linux-Client gemountet und auf dem Windows-Client zugeordnet werden, da Google Cloud NetApp Volumes die Protokolle SMB und NFS unterstützt. Google Cloud NetApp Volumes Volumes können in einfachen Schritten eingerichtet werden.

Die private Cloud von Google Cloud NetApp Volumes und Google Cloud VMware Engine muss sich in derselben Region befinden.

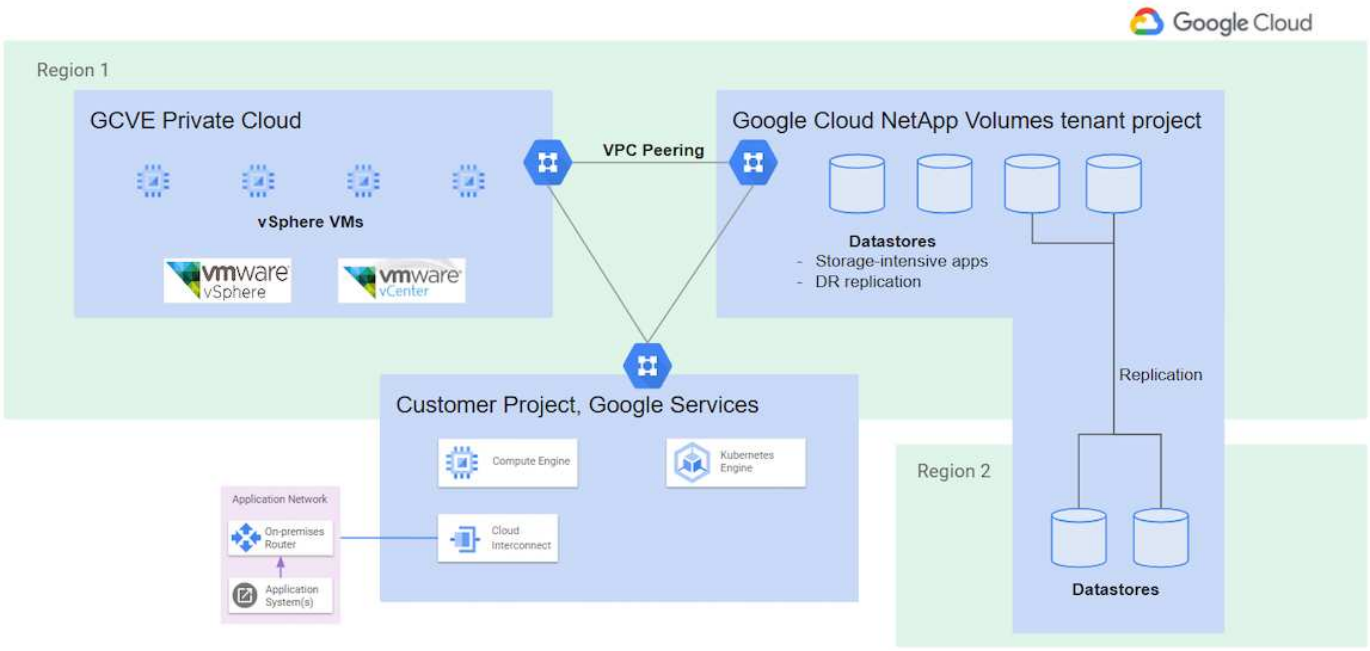
Weitere Informationen finden Sie unter"Google Cloud NetApp Volumes (NetApp Volumes) als Gast-verbundener Speicher"

Ergänzender NFS-Datenspeicher für Google Cloud VMware Engine mit Google Cloud NetApp Volumes

Kunden können die Speicherkapazität auf Google Cloud VMware Engine mithilfe des zusätzlichen NFS-Datenspeichers mit Google Cloud NetApp Volumes erweitern.

Überblick

Kunden, die zusätzliche Speicherkapazität in ihrer Google Cloud VMware Engine (GCVE)-Umgebung benötigen, können den Netapp Cloud Volume Service zur Bereitstellung als zusätzlichen NFS-Datenspeicher nutzen. Durch die Speicherung von Daten auf Google Cloud NetApp Volumes können Kunden zum Schutz vor Katastrophen eine Replikation zwischen Regionen durchführen.



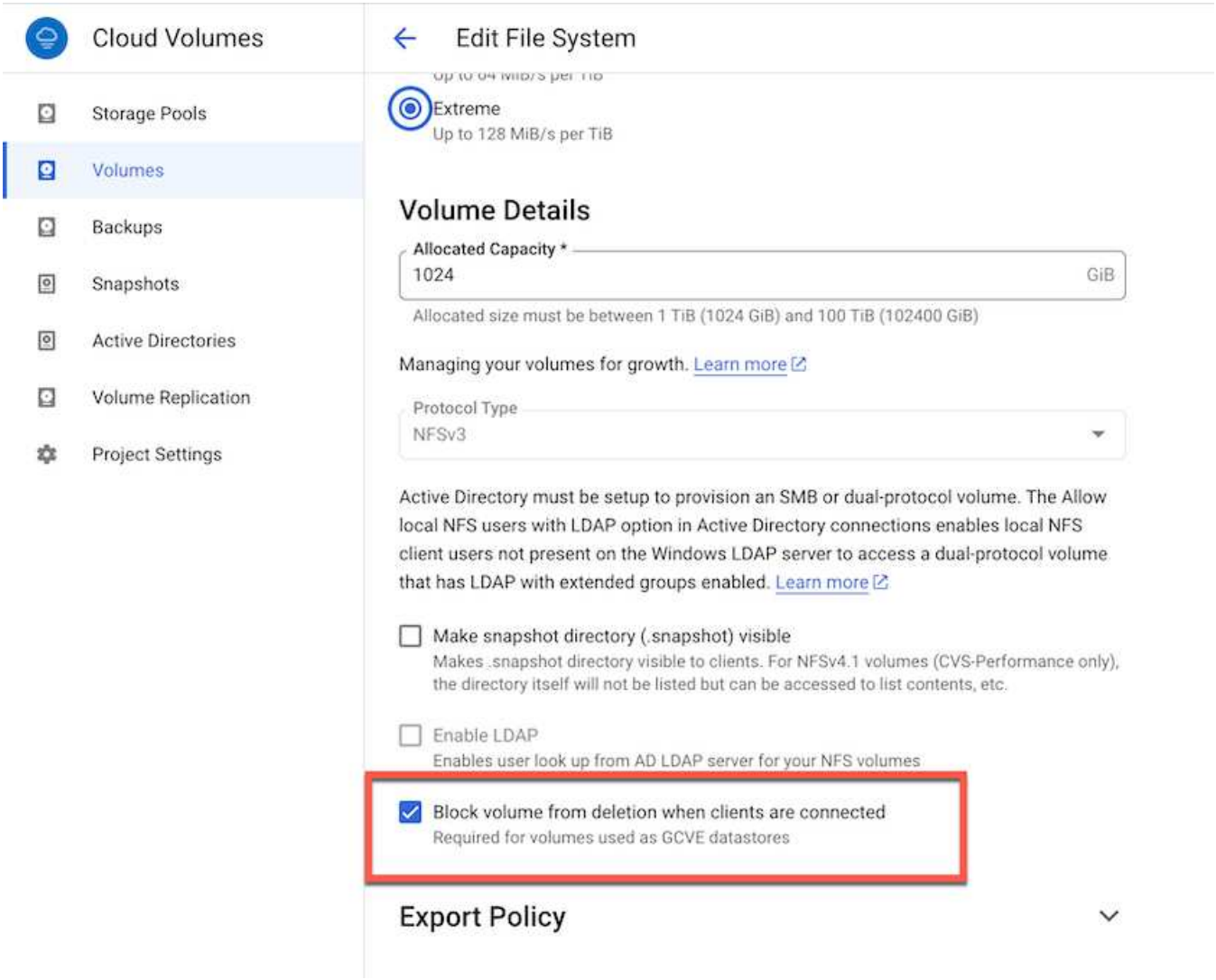
Bereitstellungsschritte zum Mounten des NFS-Datenspeichers von Google Cloud NetApp Volumes (NetApp Volumes) auf GCVE

▼ **Bereitstellung von NetApp Volumes – Performance Volume**

Das Volume von Google Cloud NetApp Volumes kann entweder durch "Verwenden der Google Cloud Console" "Verwendung der Google Cloud CLI oder API" bereitgestellt werden

▼ **Markieren Sie das NetApp Volumes-Volume als nicht löschbar**

Um ein versehentliches Löschen des Volumes zu vermeiden, während die VM ausgeführt wird, sollte das Volume wie im Screenshot unten dargestellt als nicht löschbar markiert sein.



Weitere Informationen finden sich in der "NFS-Volume erstellen" Dokumentation.

▼ **Stellen Sie sicher, dass für NetApp Volumes Tenant VPC eine private Verbindung auf GCVE besteht.**

Um den NFS-Datenspeicher zu mounten, muss eine private Verbindung zwischen GCVE und dem NetApp Volumes-Projekt bestehen. Weitere Informationen finden Sie unter"So richten Sie den privaten Servicezugriff ein"

▼ **Mounten Sie den NFS-Datenspeicher**

Anweisungen zum Mounten eines NFS-Datenspeichers auf GCVE finden Sie unter"So erstellen Sie einen NFS-Datenspeicher mit NetApp Volumes"

Da vSphere-Hosts von Google verwaltet werden, haben Sie keinen Zugriff auf die Installation des 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, beachten Sie bitte"Maximal unterstützte MTU-Größen auf GCP"

Einsparungen mit Google Cloud NetApp Volumes

Weitere Informationen zu Ihren potenziellen Einsparungen mit Google Cloud NetApp Volumes für Ihren Storage Bedarf auf GCVE finden Sie unter "NetApp ROI-Rechner"

Referenzlinks

- "Google Blog – So verwenden Sie NetApp Volumes als Datenspeicher für Google Cloud VMware Engine"
- "NetApp Blog – Eine bessere Möglichkeit, Ihre speicherintensiven Apps in die Google Cloud zu migrieren"

NetApp Storage-Optionen für GCP

GCP unterstützt über Gäste verbundene NetApp -Speicher mit Cloud Volumes ONTAP (CVO) oder Google Cloud NetApp Volumes (NetApp Volumes).

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP oder CVO ist die branchenführende Cloud-Datenverwaltungslösung, die auf der ONTAP -Speichersoftware von NetApp basiert und nativ auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) verfügbar ist.

Es handelt sich um eine softwaredefinierte Version von ONTAP , die Cloud-nativen Speicher nutzt. Dadurch können Sie in der Cloud und vor Ort dieselbe Speichersoftware verwenden und müssen Ihr IT-Personal nicht mehr in völlig neuen Methoden zur Verwaltung Ihrer Daten schulen.

CVO bietet Kunden die Möglichkeit, Daten nahtlos vom Edge zum Rechenzentrum, in die Cloud und zurück zu verschieben und so Ihre Hybrid Cloud zusammenzuführen – alles verwaltet über eine zentrale Verwaltungskonsole, den NetApp Cloud Manager.

CVO bietet von Haus aus extreme Leistung und erweiterte Datenverwaltungsfunktionen, um selbst Ihre anspruchsvollsten Anwendungen in der Cloud zu erfüllen

Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher

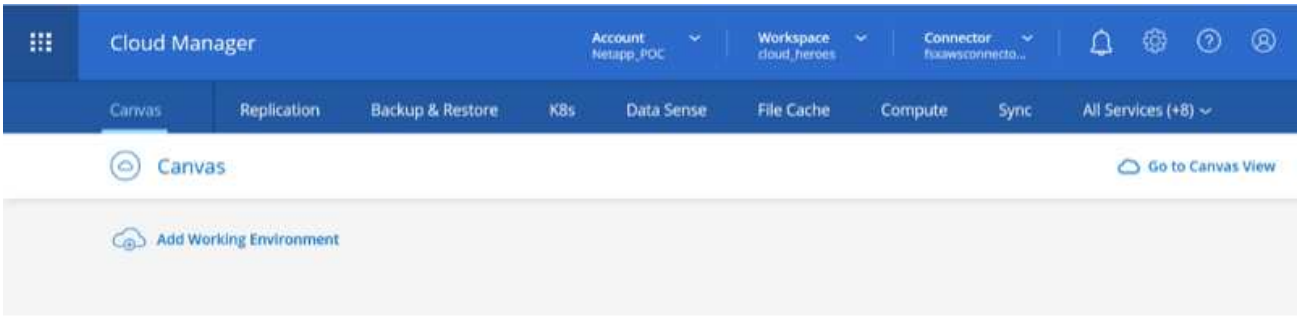
▼ **Cloud Volumes ONTAP in Google Cloud bereitstellen (Do It Yourself)**

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

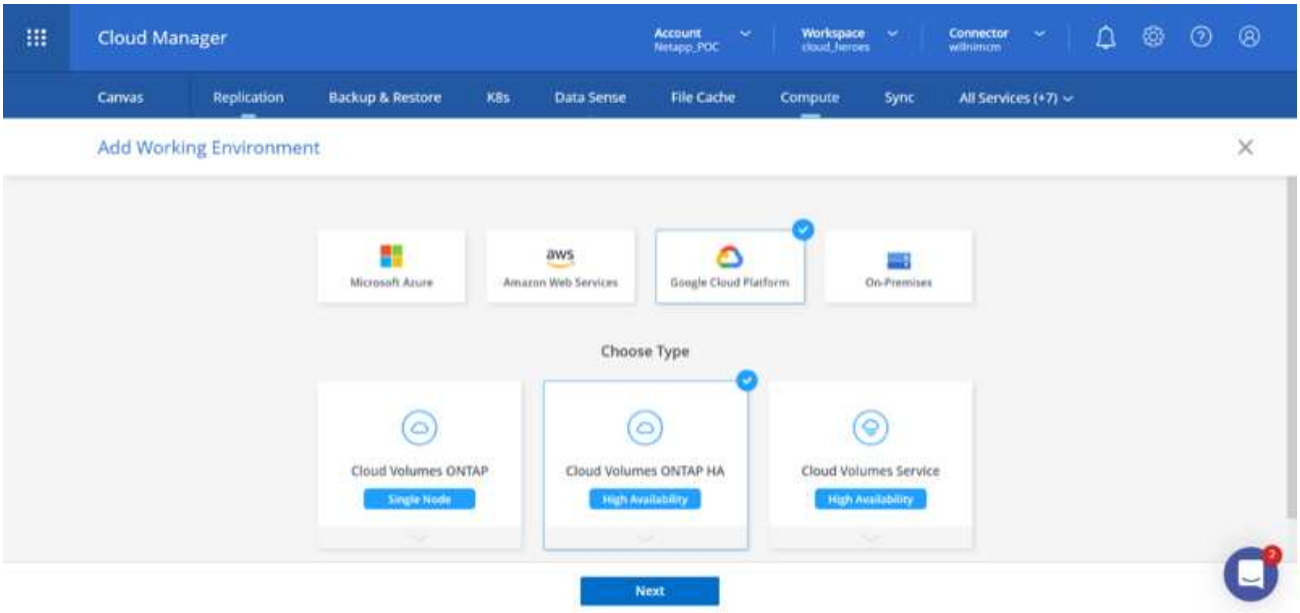
Um Volumes aus einer lokalen Umgebung zur Notfallwiederherstellung oder Migration in die Cloud zu replizieren, stellen Sie eine Netzwerkverbindung zu Google Cloud her, entweder über ein Site-to-Site-VPN oder Cloud Interconnect. Das Replizieren von Daten von lokalen Standorten auf Cloud Volumes ONTAP fällt nicht in den Geltungsbereich dieses Dokuments. Informationen zum Replizieren von Daten zwischen lokalen und Cloud Volumes ONTAP Systemen finden Sie unter"Einrichten der Datenreplikation zwischen Systemen" .

> ⓘ Mit "Cloud Volumes ONTAP Sizer" lassen sich die Cloud Volumes ONTAP Instanzen präzise dimensionieren. Außerdem dient die Überwachung der On-Premises-Performance als Eingabedaten für den Cloud Volumes ONTAP Sizer.

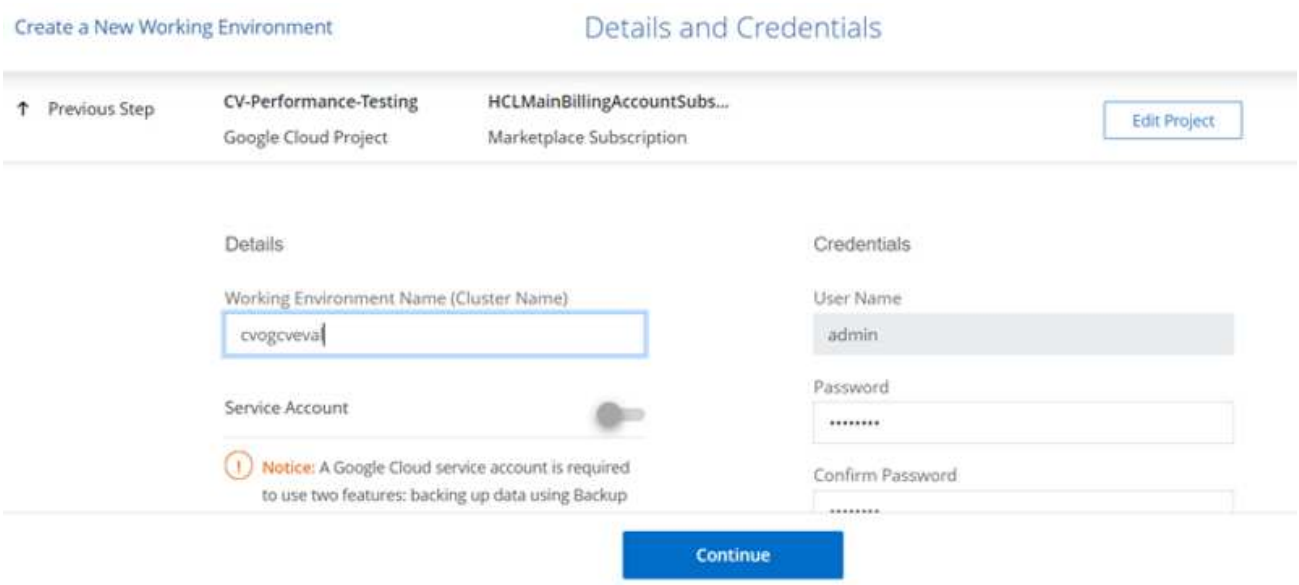
1. Melden Sie sich bei NetApp Cloud Central an – der Fabric View-Bildschirm wird angezeigt. Suchen Sie die Registerkarte „Cloud Volumes ONTAP“ und wählen Sie „Gehe zu Cloud Manager“ aus. Nachdem Sie sich angemeldet haben, wird der Canvas-Bildschirm angezeigt.



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

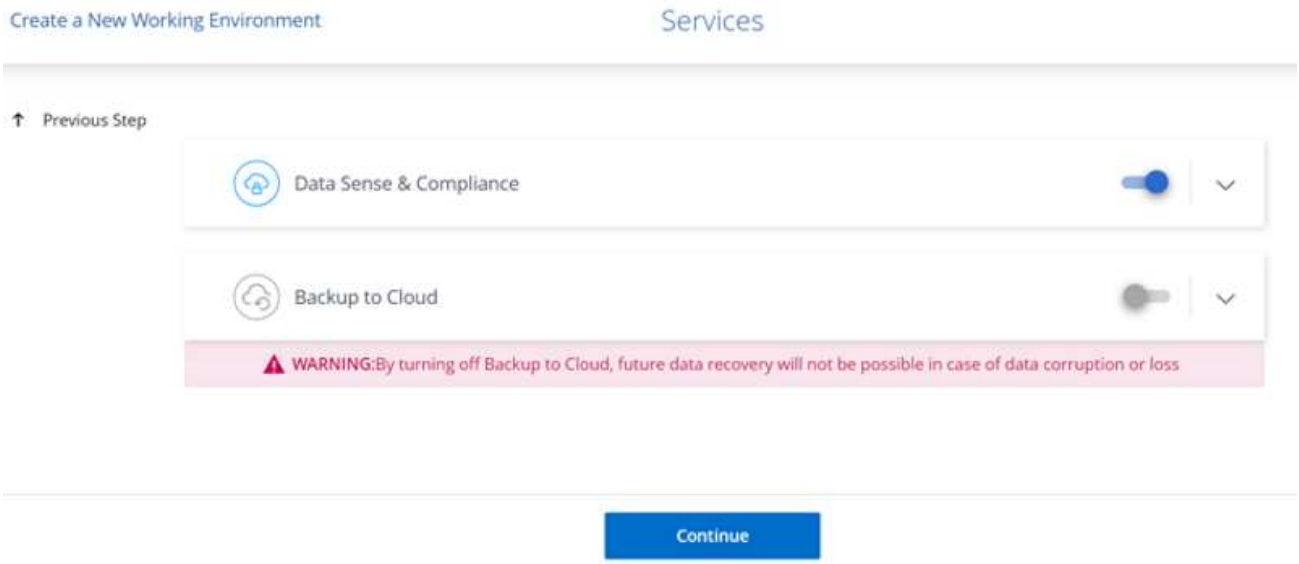


3. Geben Sie die Details der zu erstellenden Umgebung an, einschließlich Umgebungsname und Administratoranmeldeinformationen. Wenn Sie fertig sind, klicken Sie auf „Weiter“.

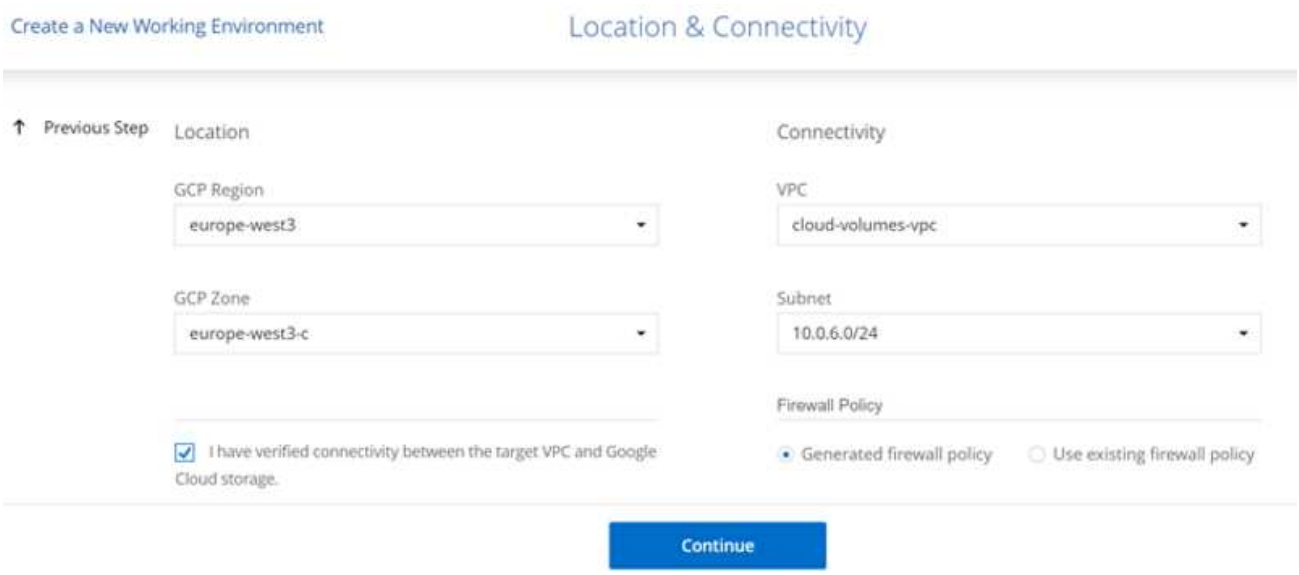


4. Aktivieren oder deaktivieren Sie die Zusatzdienste für die Bereitstellung von Cloud Volumes ONTAP , einschließlich Data Sense & Compliance oder Backup to Cloud. Klicken Sie dann auf „Weiter“.

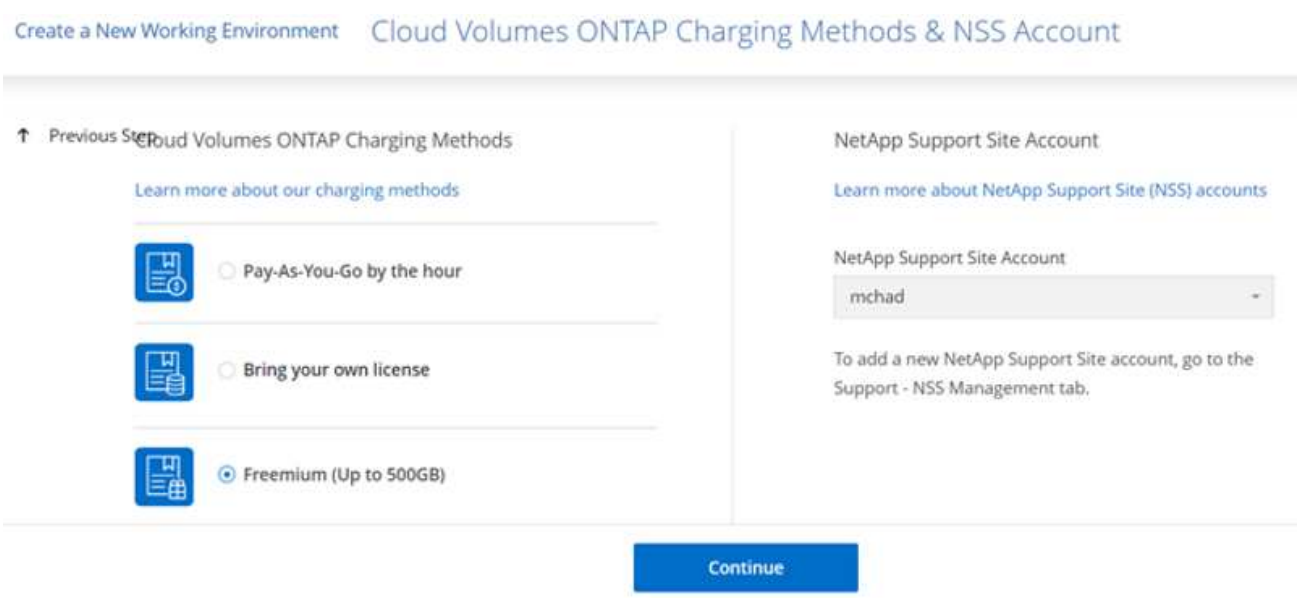
   HINWEIS: Beim Deaktivieren von Zusatzdiensten wird eine Popup-Nachricht zur Bestätigung angezeigt. Zusatzdienste können nach der CVO-Bereitstellung hinzugefügt/entfernt werden. Um Kosten zu vermeiden, sollten Sie sie von Anfang an deaktivieren, wenn sie nicht benötigt werden.



5. Wählen Sie einen Standort und eine Firewall-Richtlinie aus und aktivieren Sie das Kontrollkästchen, um die Netzwerkkonnektivität zum Google Cloud-Speicher zu bestätigen.

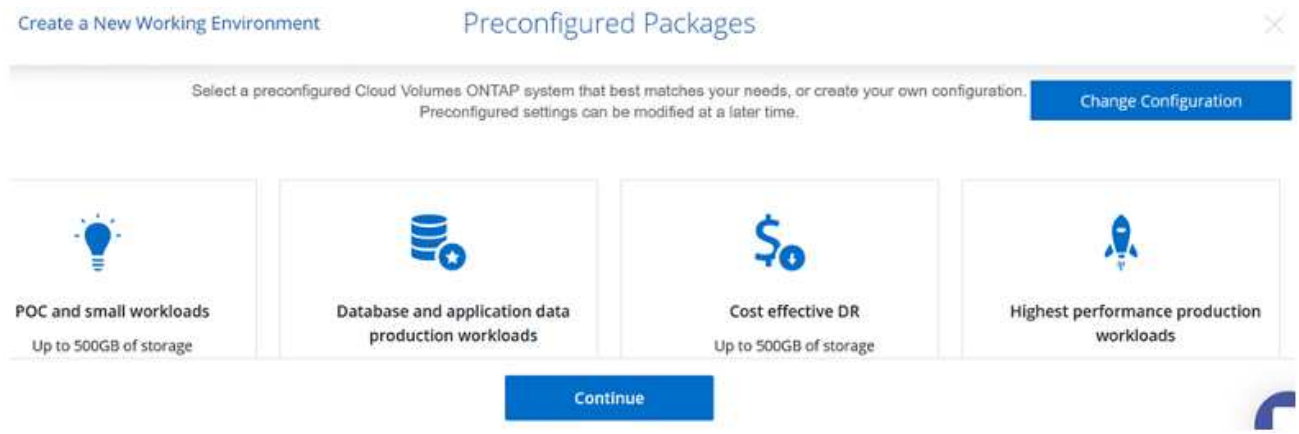


6. Wählen Sie die Lizenzoption: Pay-As-You-Go oder BYOL zur Verwendung einer vorhandenen Lizenz. In diesem Beispiel wird die Freemium-Option verwendet. Klicken Sie dann auf Weiter.

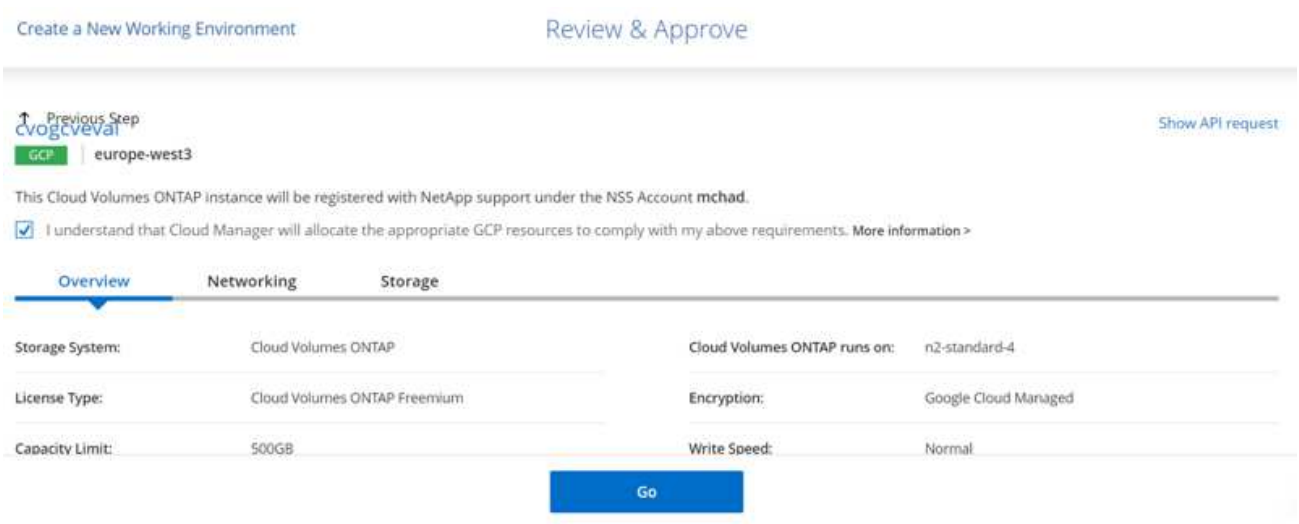


7. Wählen Sie je nach Art der Arbeitslast, die auf den VMs bereitgestellt wird, die auf VMware Cloud auf AWS SDDC ausgeführt werden, zwischen mehreren verfügbaren vorkonfigurierten Paketen.

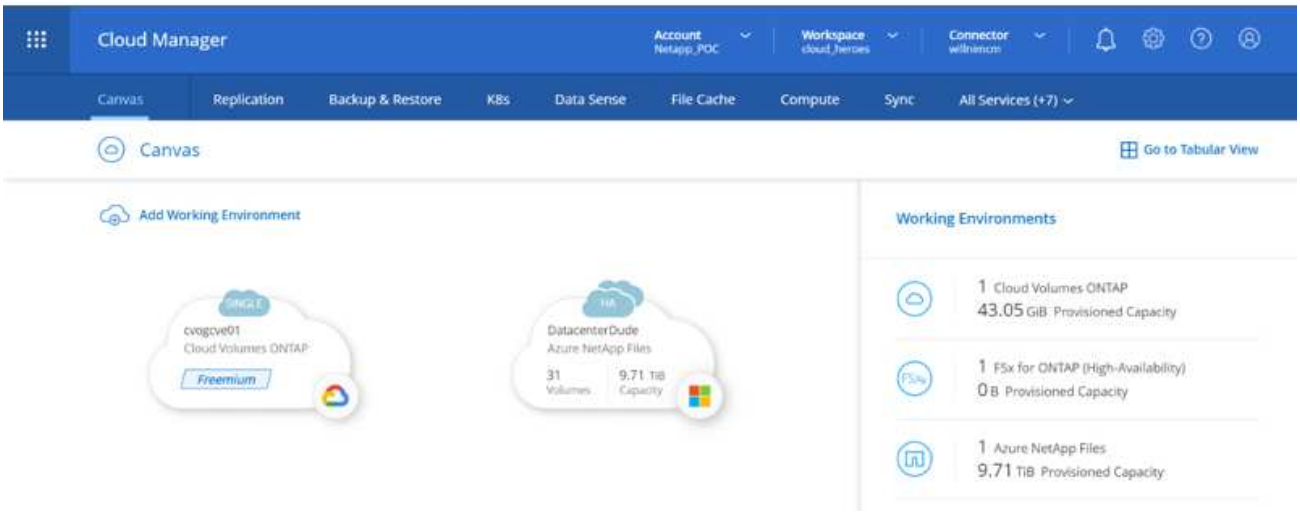
   TIPP: Bewegen Sie den Mauszeiger über die Kacheln, um Details anzuzeigen, oder passen Sie CVO-Komponenten und ONTAP -Version an, indem Sie auf „Konfiguration ändern“ klicken.



8. Überprüfen und bestätigen Sie die Auswahl auf der Seite „Überprüfen und genehmigen“. Klicken Sie auf „Los“, um die Cloud Volumes ONTAP -Instanz zu erstellen.



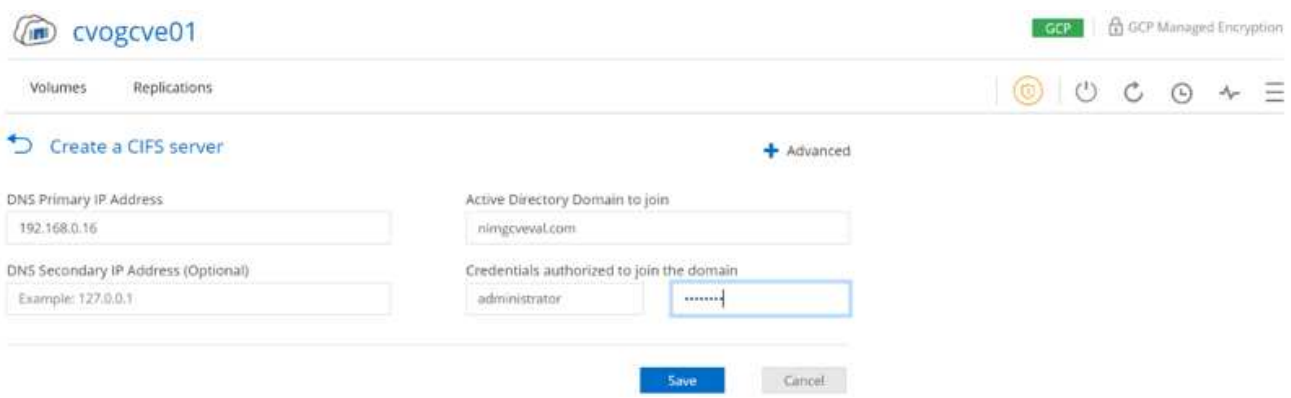
9. Nachdem Cloud Volumes ONTAP bereitgestellt wurde, wird es in den Arbeitsumgebungen auf der Canvas-Seite aufgeführt.



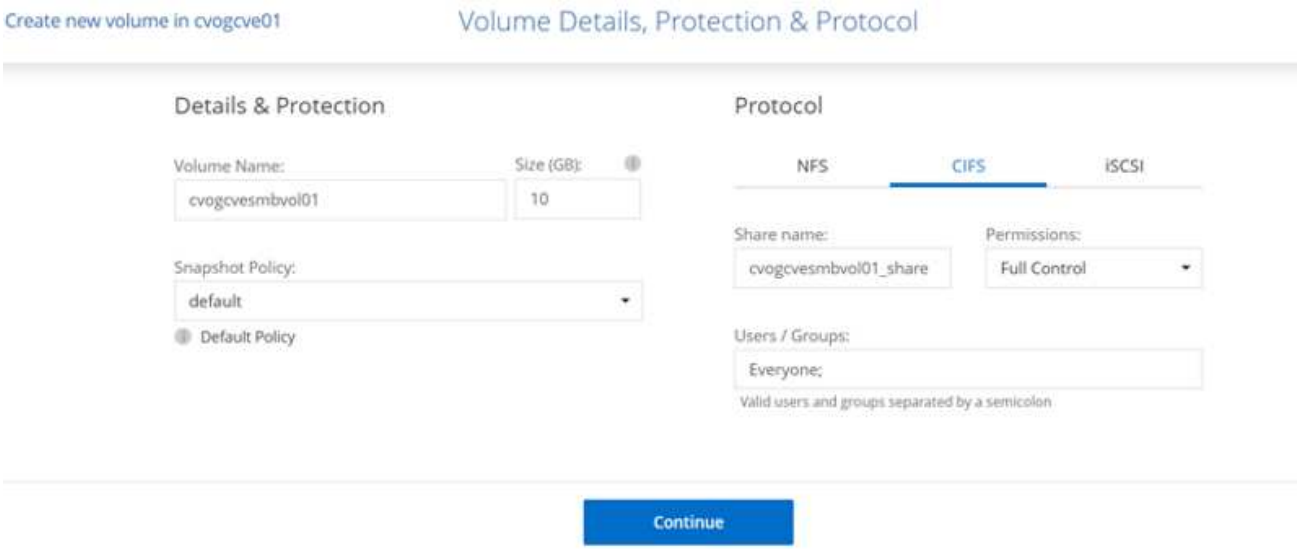
▼ Zusätzliche Konfigurationen für SMB-Volumes

1. Nachdem die Arbeitsumgebung bereit ist, stellen Sie 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.

   TIPP: Klicken Sie auf das Menüsymbol (º), wählen Sie „Erweitert“, um weitere Optionen anzuzeigen, und wählen Sie „CIFS-Setup“.



2. Das Erstellen des SMB-Volumes ist ein einfacher Vorgang. Doppelklicken Sie in Canvas auf die Arbeitsumgebung Cloud Volumes ONTAP , um Volumes zu erstellen und zu verwalten, und klicken Sie auf die Option „Volume erstellen“. Wählen Sie die entsprechende Größe und der Cloud-Manager wählt das enthaltene Aggregat aus oder verwenden Sie einen erweiterten Zuordnungsmechanismus, um die Platzierung auf einem bestimmten Aggregat vorzunehmen. Für diese Demo wird CIFS/SMB als Protokoll ausgewählt.



3. Nachdem das Volume bereitgestellt wurde, ist es im Bereich „Volumes“ verfügbar. Da eine CIFS-Freigabe bereitgestellt wird, erteilen Sie Ihren Benutzern oder Gruppen die Berechtigung für die Dateien und Ordner und stellen Sie sicher, dass 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 alle Datei- und Ordnerberechtigungen als Teil der SnapMirror Replikation beibehalten werden.

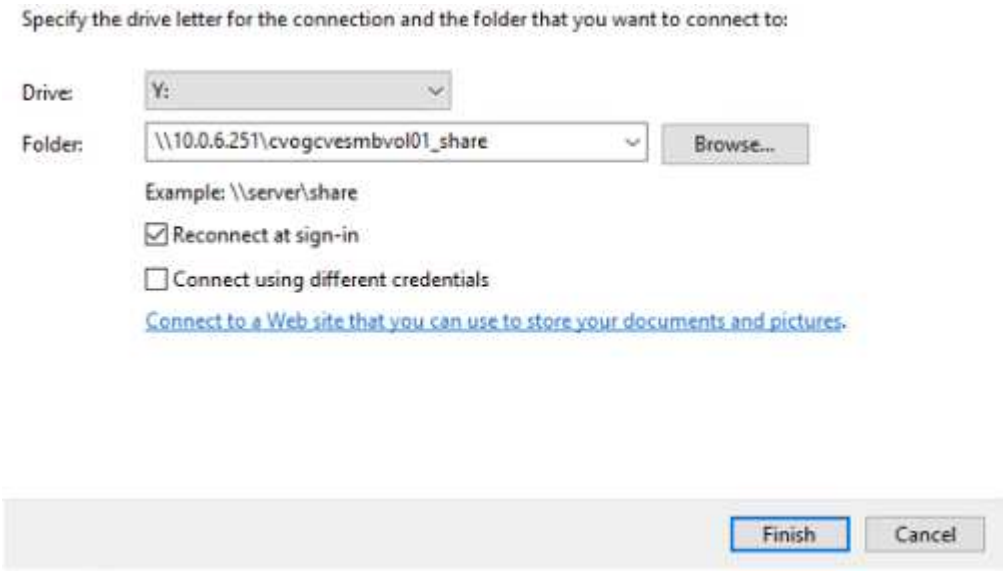
   TIPP: Klicken Sie auf das Lautstärkemenü (º), um die Optionen anzuzeigen.



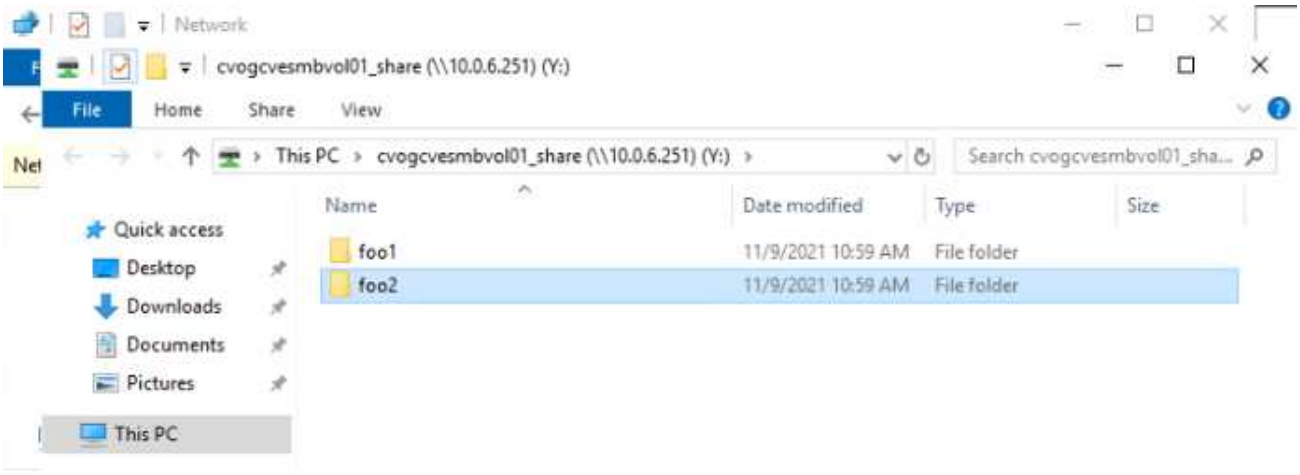
4. Nachdem das Volume erstellt wurde, verwenden Sie den Mount-Befehl, um die Anweisungen zur Volume-Verbindung anzuzeigen, und stellen Sie dann von den VMs auf Google Cloud VMware Engine aus eine Verbindung zur Freigabe her.



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



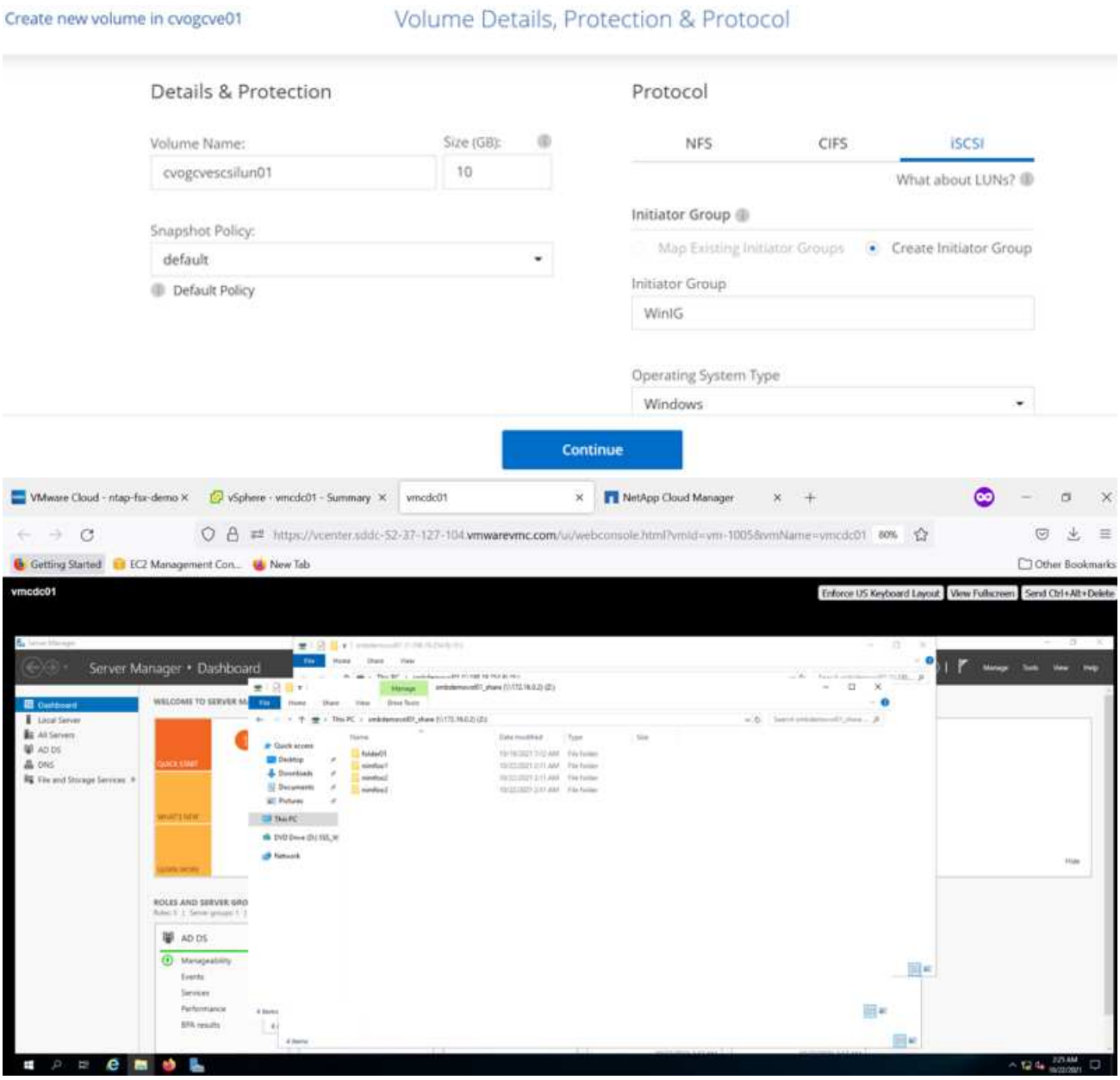
Nach der Zuordnung ist ein einfacher Zugriff möglich und die NTFS-Berechtigungen können entsprechend festgelegt werden.



▼ 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 Canvas-Seite auf die Arbeitsumgebung 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“.



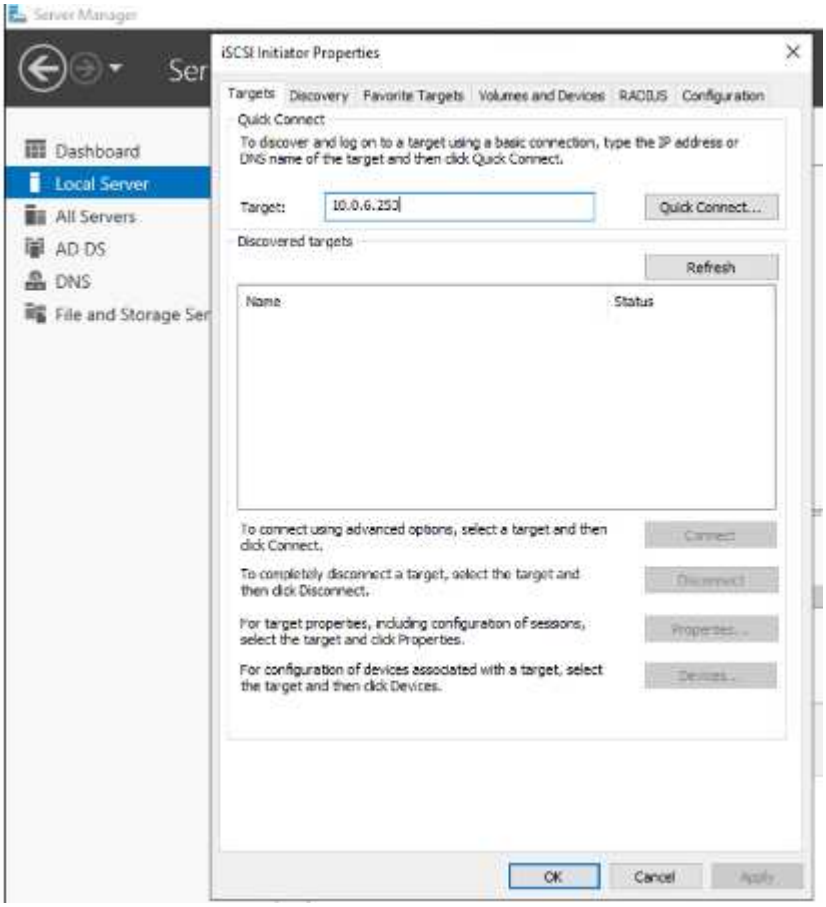
3. Nachdem das Volume bereitgestellt wurde, wählen Sie das Volume-Menü (º) und klicken Sie dann auf „Ziel-iQN“. Um den iSCSI Qualified Name (iQN) zu kopieren, klicken Sie auf „Kopieren“. Richten Sie eine iSCSI-Verbindung vom Host zur LUN ein.

So erreichen Sie dasselbe für den Host, der sich auf Google Cloud VMware Engine befindet:

1. RDP zur VM, die auf Google Cloud VMware Engine gehostet wird.
2. Öffnen Sie das Dialogfeld „Eigenschaften des iSCSI-Initiators“: Server-Manager > Dashboard > Tools > iSCSI-Initiator.

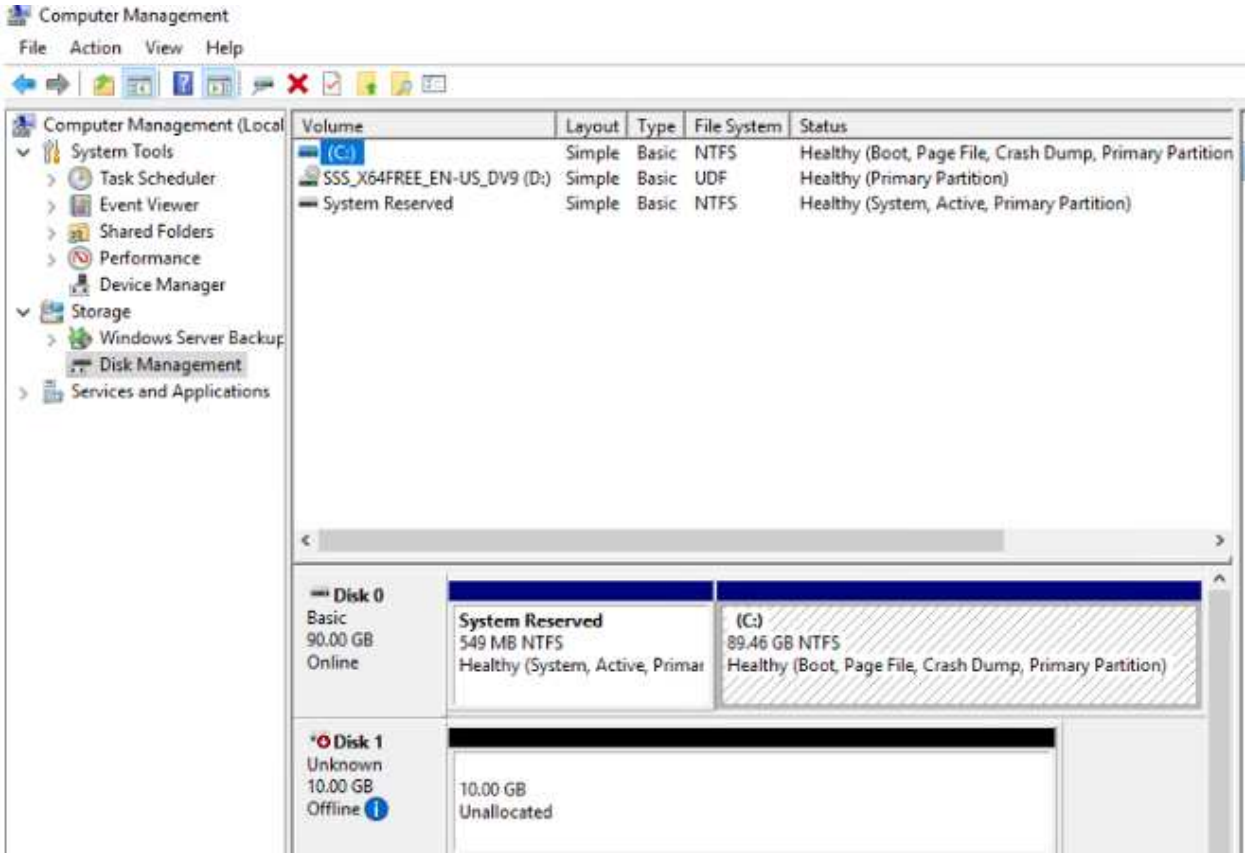
3. Klicken Sie auf der Registerkarte „Erkennung“ auf „Portal erkennen“ oder „Portal hinzufügen“ und geben Sie dann die IP-Adresse des iSCSI-Zielports ein.
4. Wählen Sie auf der Registerkarte „Ziele“ das erkannte Ziel aus und klicken Sie dann auf „Anmelden“ oder „Verbinden“.
5. Wählen Sie „Multipfad aktivieren“ und dann „Diese Verbindung beim Start des Computers automatisch wiederherstellen“ 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 zu verwendenden Pfade aus.



LUNs auf der Storage Virtual Machine (SVM) werden dem Windows-Host als Datenträger angezeigt. Alle neu hinzugefügten Festplatten werden vom Host nicht automatisch erkannt. Lösen Sie einen manuellen erneuten Scan aus, um die Datenträger zu ermitteln, indem Sie die folgenden Schritte ausführen:

a. Öffnen Sie das Windows-Dienstprogramm „Computerverwaltung“: Start > Verwaltung > Computerverwaltung.
b. Erweitern Sie den Knoten „Speicher“ im Navigationsbaum.
c. Klicken Sie auf Datenträgerverwaltung.
d. Klicken Sie auf „Aktion“ > „Datenträger erneut scannen“.

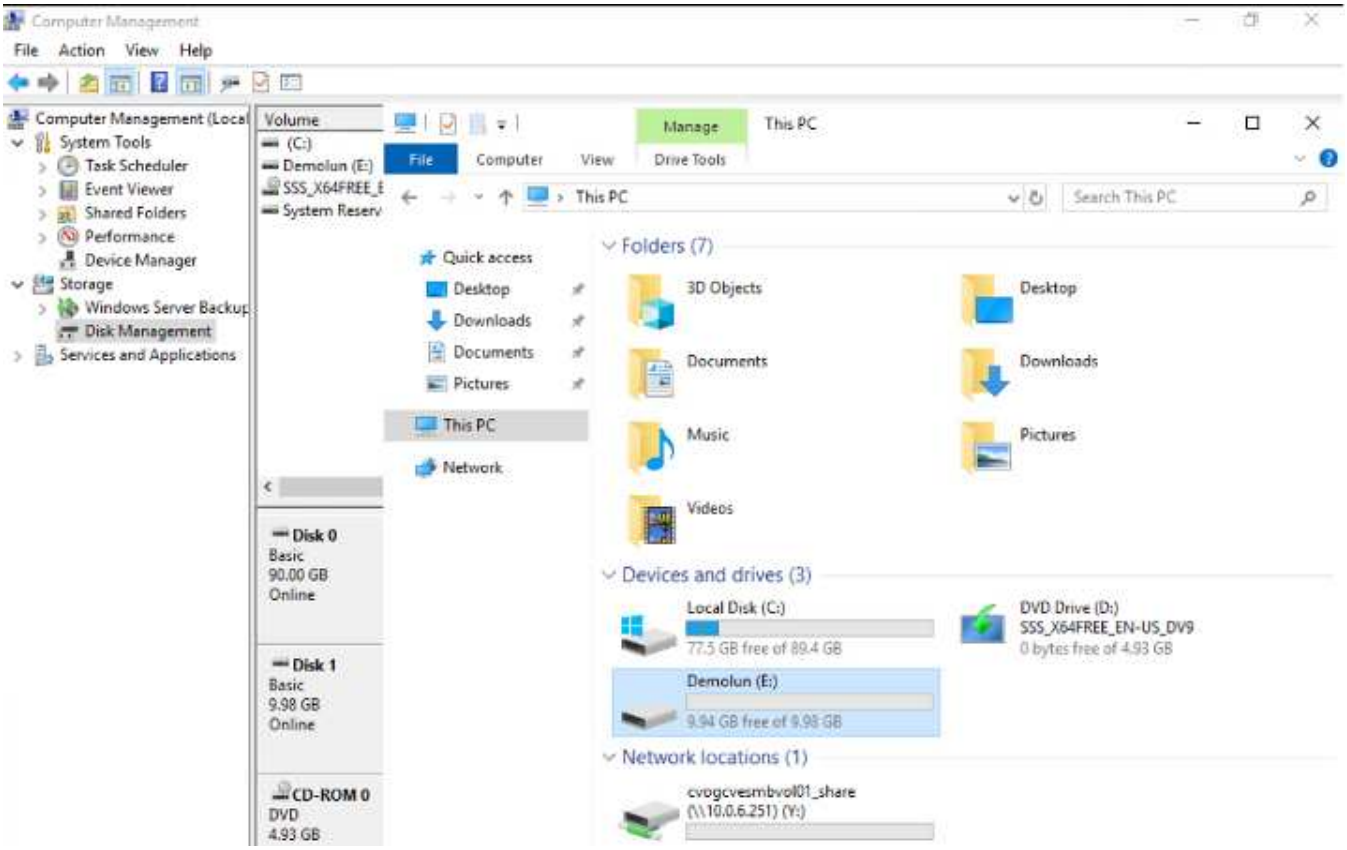


Wenn der Windows-Host zum ersten Mal auf eine neue LUN zugreift, verfügt diese über keine Partition oder kein Dateisystem. Initialisieren Sie die LUN und formatieren Sie die LUN optional mit einem Dateisystem, indem Sie die folgenden Schritte ausführen:

a. Starten Sie die Windows-Datenträgerverwaltung.

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

c. Folgen Sie den Anweisungen des Assistenten. In diesem Beispiel ist Laufwerk F: gemountet.



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

```
nlyaz@nlmubu01:~$ 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
```

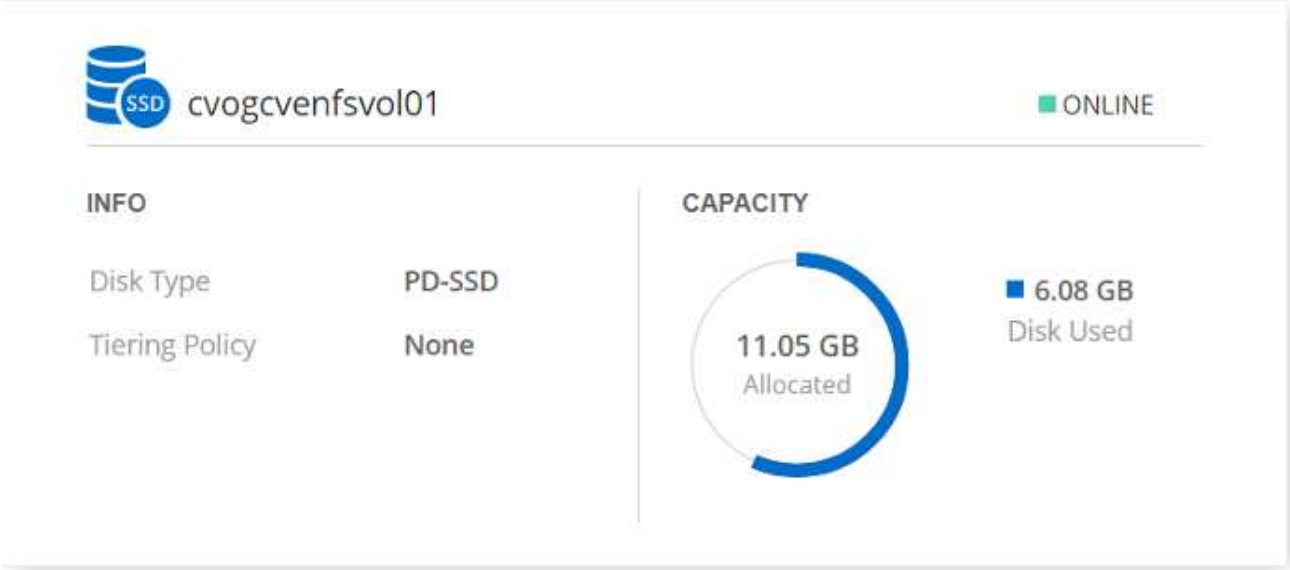
```
nlyaz@nlnubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           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**

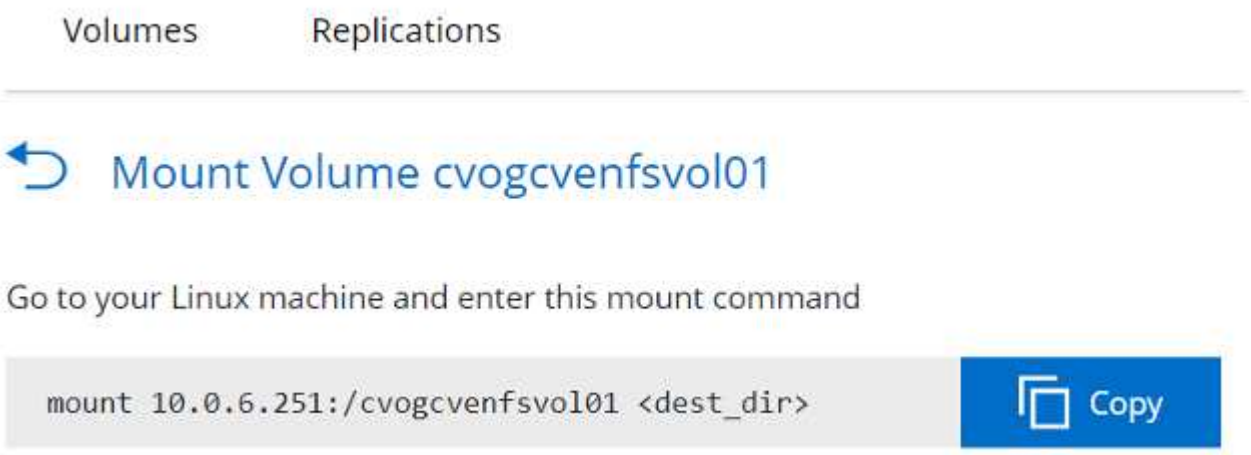
Um das Cloud Volumes ONTAP (DIY)-Dateisystem von VMs innerhalb der Google Cloud VMware Engine zu mounten, führen Sie die folgenden Schritte aus:

Stellen Sie das Volume bereit, indem Sie die folgenden Schritte ausführen

1. Klicken Sie auf der Registerkarte „Volumes“ auf „Neues Volume erstellen“.
2. Wählen Sie auf der Seite „Neues Volume erstellen“ einen Volumetyp aus:



3. Platzieren Sie auf der Registerkarte „Volumes“ den Mauszeiger über dem Volume, wählen Sie das Menüsymbol (º) aus und klicken Sie dann auf „Mount Command“.



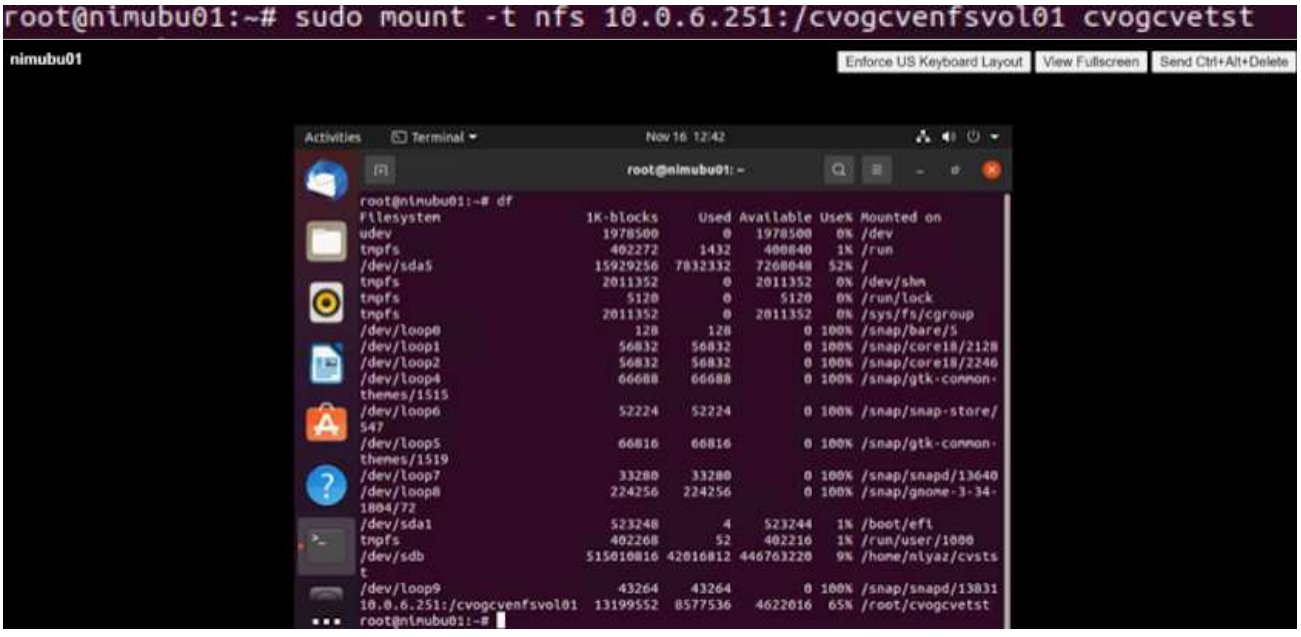
4. Klicken Sie auf „Kopieren“.
5. Stellen Sie eine Verbindung zur angegebenen Linux-Instanz her.
6. Öffnen Sie mithilfe von Secure Shell (SSH) ein Terminal auf der Instanz und melden Sie sich mit den entsprechenden Anmeldeinformationen an.
7. Erstellen Sie mit dem folgenden Befehl ein Verzeichnis für den Einhängepunkt des Datenträgers.

```
$ sudo mkdir /cvogcvetst
```

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

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

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



Google Cloud NetApp Volumes (NetApp Volumes)

Google Cloud NetApp Volumes (NetApp Volumes) ist ein komplettes Portfolio an Datendiensten zur Bereitstellung fortschrittlicher Cloud-Lösungen. NetApp Volumes unterstützt mehrere Dateizugriffsprotokolle für große Cloud-Anbieter (NFS- und SMB-Unterstützung).

Zu den weiteren Vorteilen und Funktionen gehören: Datenschutz und -wiederherstellung mit Snapshot, spezielle Funktionen zum Replizieren, Synchronisieren und Migrieren von Datenzielen vor Ort oder in der Cloud sowie konstant hohe Leistung auf dem Niveau eines dedizierten Flash-Speichersystems.

Google Cloud NetApp Volumes (NetApp Volumes) als mit dem Gast verbundener Speicher

▼ Konfigurieren von NetApp Volumes mit VMware Engine

Google Cloud NetApp Volumes Freigaben können von VMs bereitgestellt werden, die in der VMware Engine-Umgebung erstellt wurden. Die Volumes können auch auf dem Linux-Client gemountet und auf dem Windows-Client zugeordnet werden, da Google Cloud NetApp Volumes die Protokolle SMB und NFS unterstützt. Google Cloud NetApp Volumes Volumes können in einfachen Schritten eingerichtet werden.

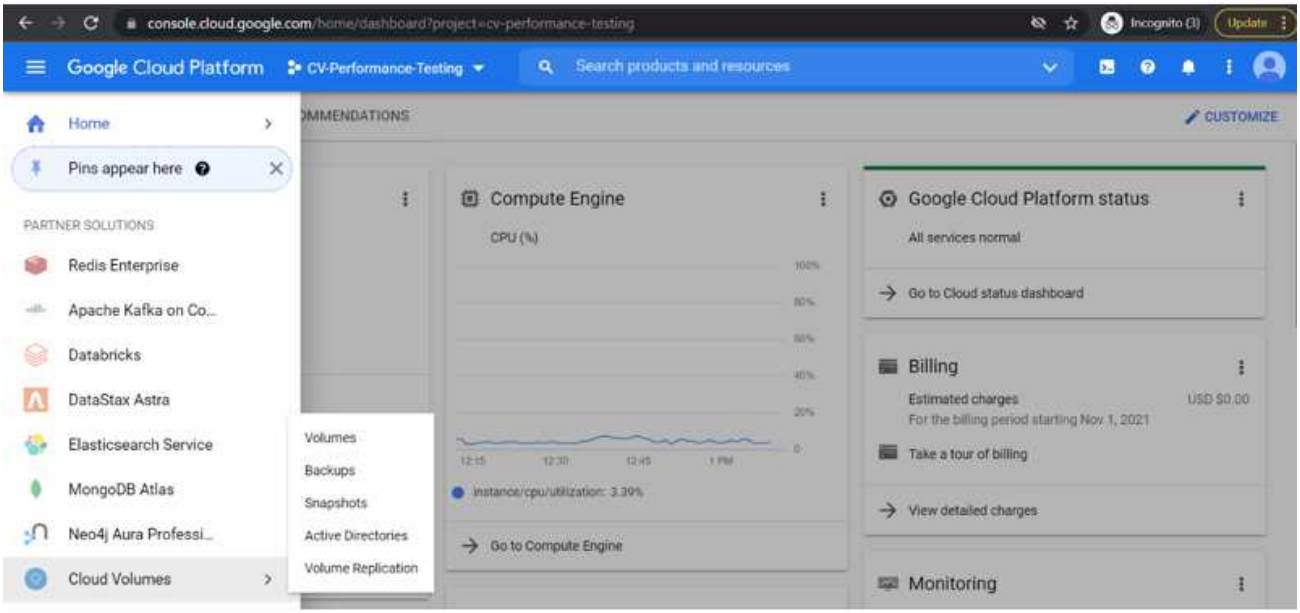
Die private Cloud von Google Cloud NetApp Volumes und Google Cloud VMware Engine muss sich in derselben Region befinden.

Um Google Cloud NetApp Volumes für Google Cloud vom Google Cloud Marketplace zu kaufen, zu aktivieren und zu konfigurieren, folgen Sie diesen detaillierten"Führung" .

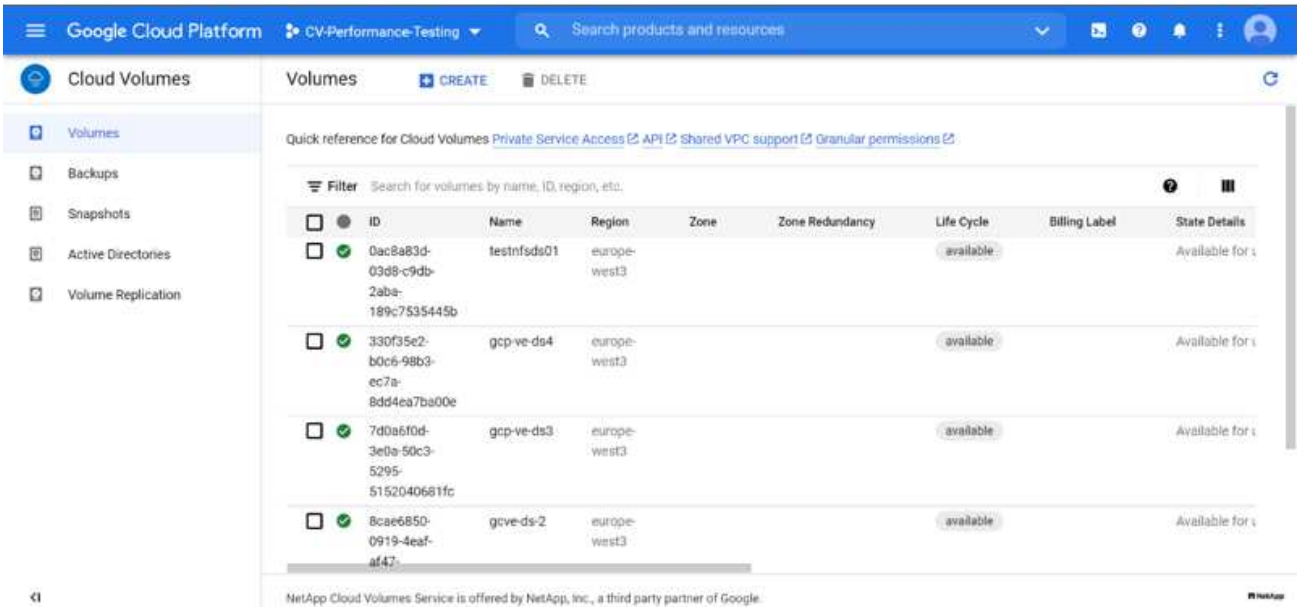
▼ Erstellen Sie ein NetApp Volumes NFS-Volume für die private GCVE-Cloud

Führen Sie die folgenden Schritte aus, um NFS-Volumes zu erstellen und bereitzustellen:

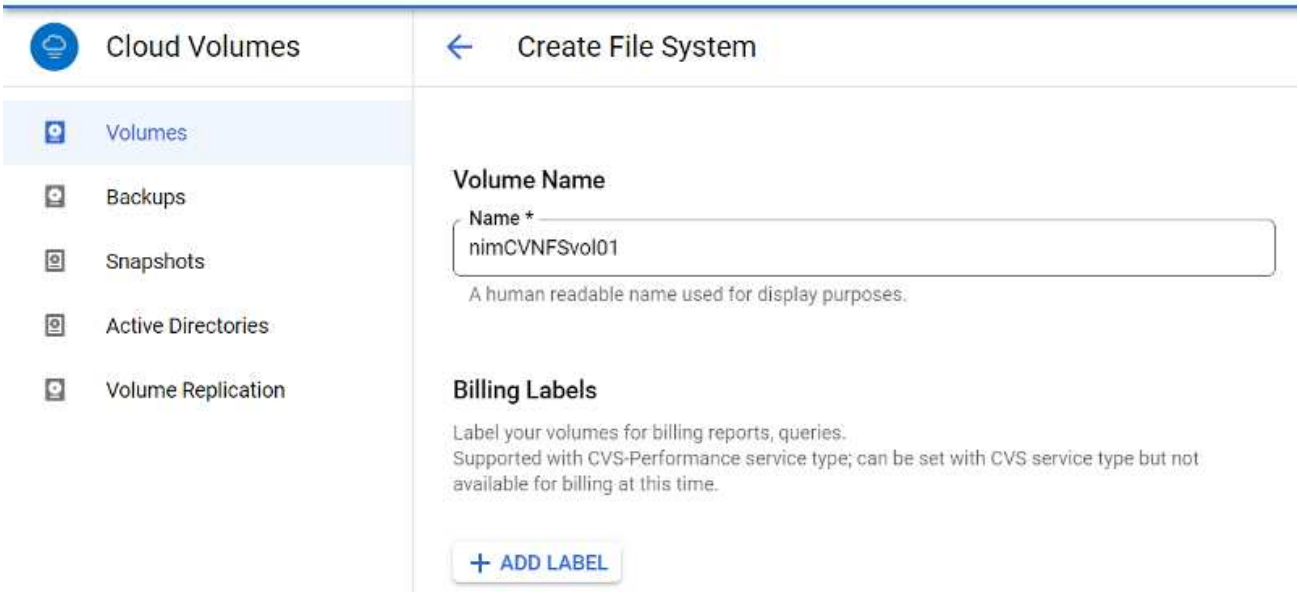
1. Greifen Sie über die Google Cloud-Konsole auf Cloud Volumes von Partner Solutions zu.



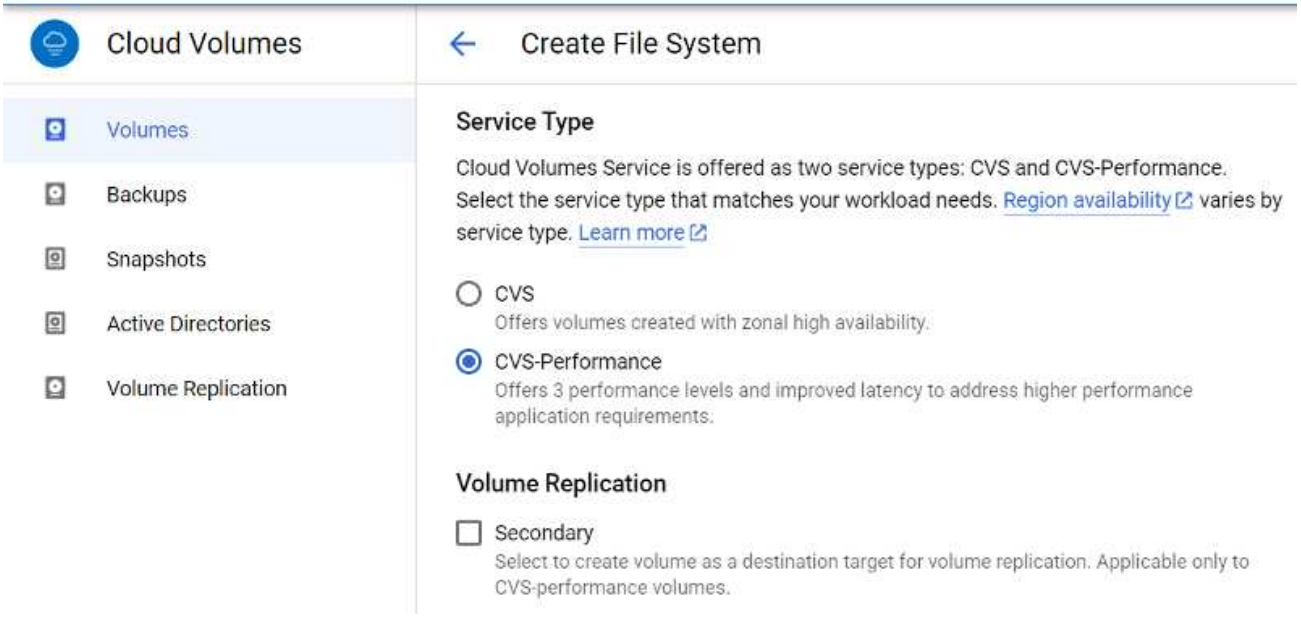
2. Gehen Sie in der Cloud Volumes-Konsole zur Seite „Volumes“ und klicken Sie auf „Erstellen“.



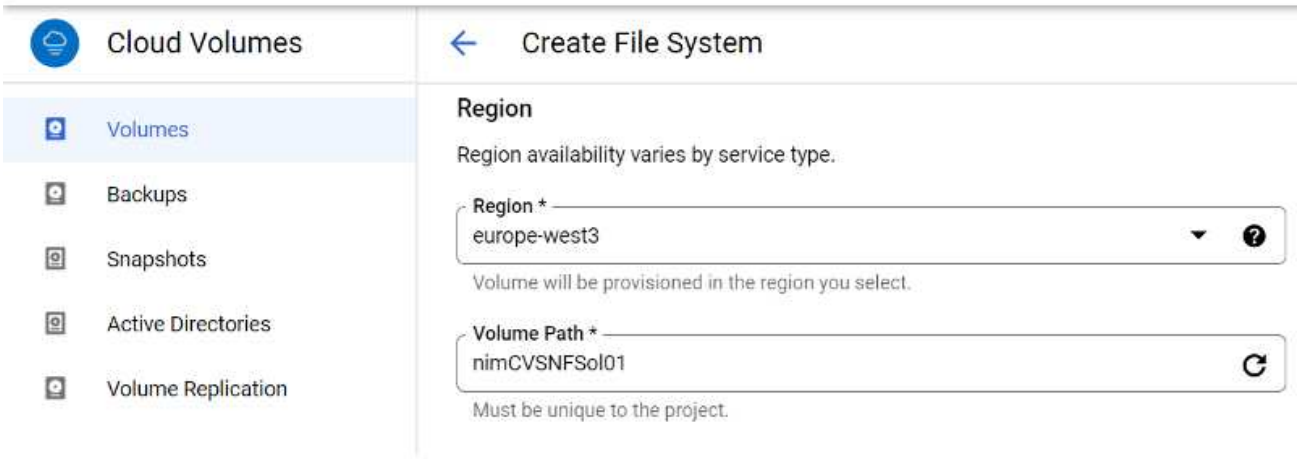
3. Geben Sie auf der Seite „Dateisystem erstellen“ den Datenträgernamen und die Abrechnungsbezeichnungen nach Bedarf für Rückbuchungsmechanismen an.



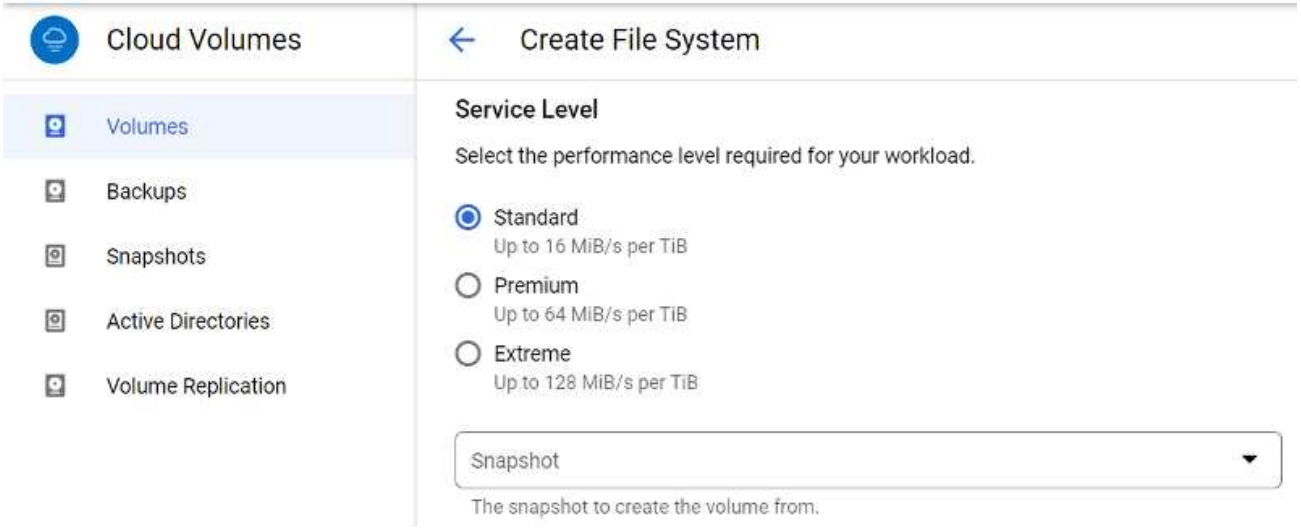
4. Wählen Sie den entsprechenden Dienst aus. Wählen Sie für GCVE NetApp Volumes-Performance und das gewünschte Servicelevel für verbesserte Latenz und höhere Leistung basierend auf den Workload-Anforderungen der Anwendung.



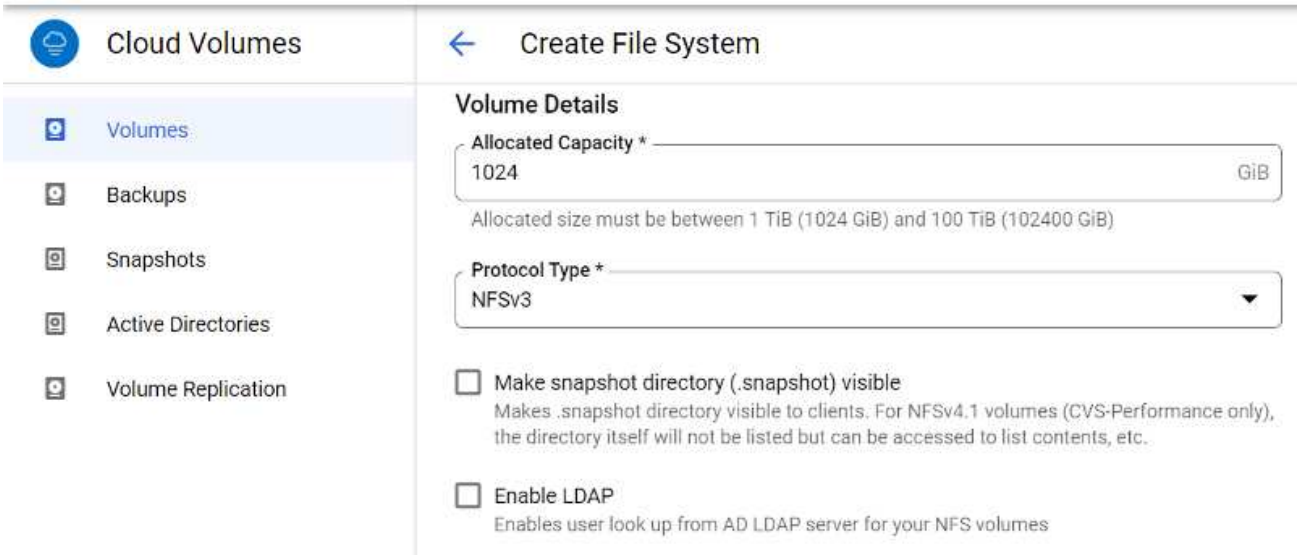
5. Geben Sie die Google Cloud-Region für das Volume und den Volume-Pfad an (der Volume-Pfad muss für alle Cloud-Volumes im Projekt eindeutig sein).



6. Wählen Sie die Leistungsstufe für das Volume aus.

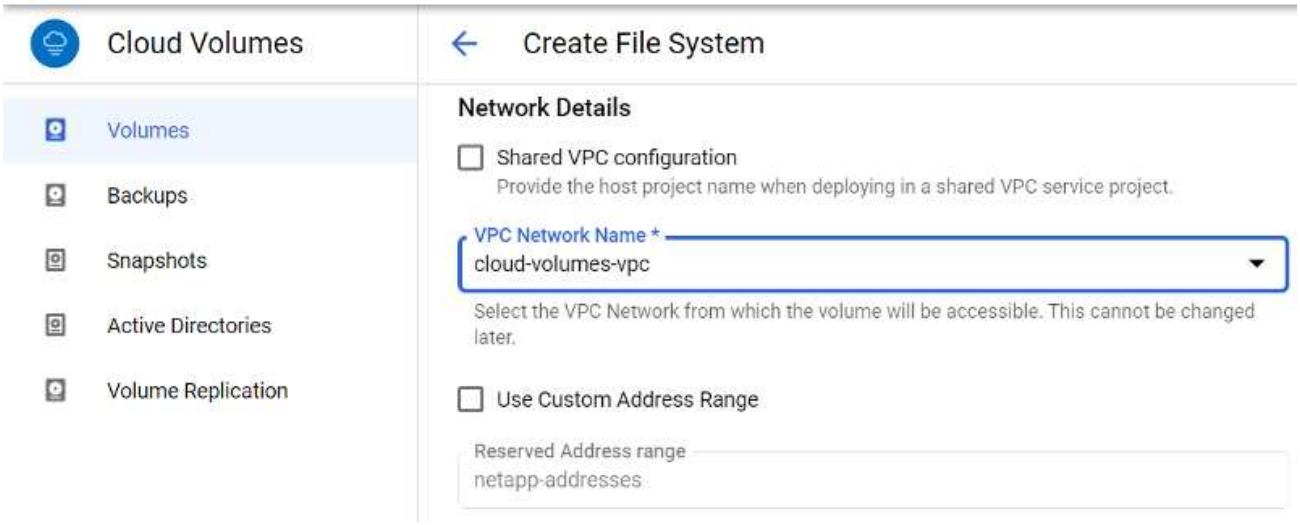


7. Geben Sie die Größe des Volumes und den Protokolltyp an. Bei diesem Test wird NFSv3 verwendet.



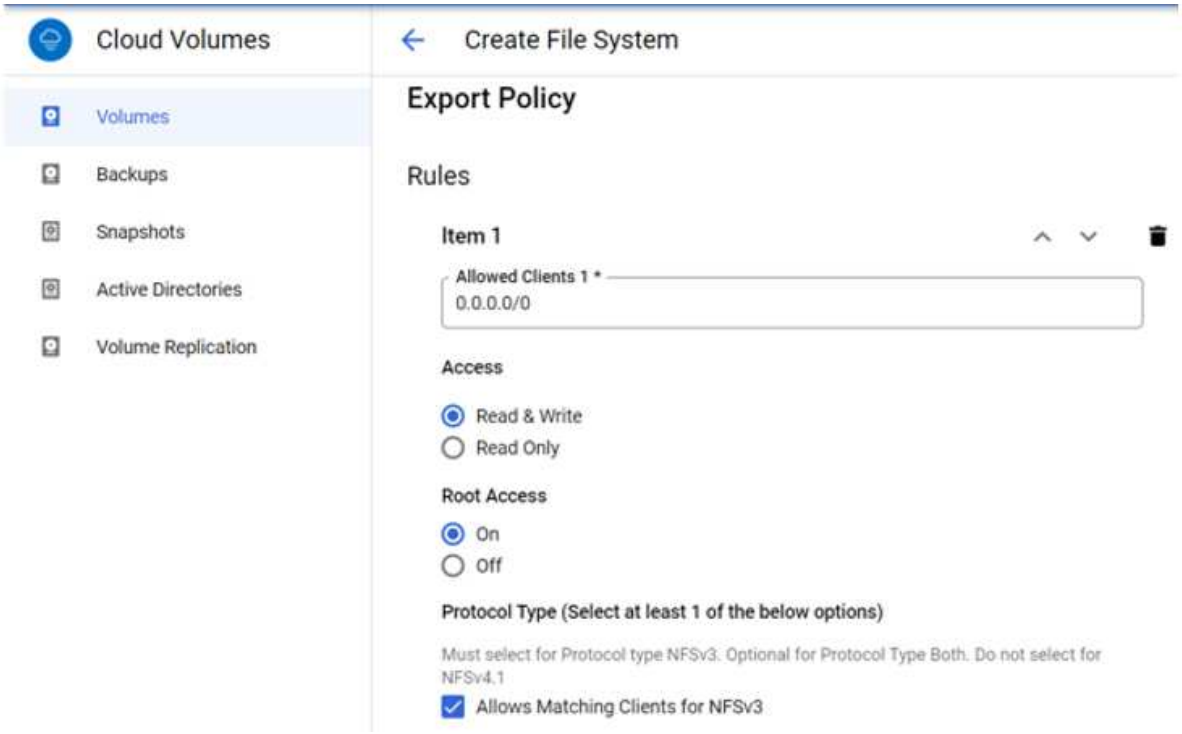
8. Wählen Sie in diesem Schritt das VPC-Netzwerk aus, von dem aus auf das Volume zugegriffen werden soll. Stellen Sie sicher, dass VPC-Peering vorhanden ist.

   HINWEIS: Wenn kein VPC-Peering durchgeführt wurde, wird eine Popup-Schaltfläche angezeigt, die Sie durch die Peering-Befehle führt. Öffnen Sie eine Cloud Shell-Sitzung und führen Sie die entsprechenden Befehle aus, um Ihr VPC mit dem Google Cloud NetApp Volumes Producer zu verbinden. Falls Sie sich entscheiden, das VPC-Peering im Voraus vorzubereiten, lesen Sie diese Anweisungen.



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

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



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



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

Stellen Sie vor der Vorbereitung zum Mounten des NFS-Volumes sicher, dass der Peering-Status der privaten Verbindung als „Aktiv“ aufgeführt ist. Sobald der Status „Aktiv“ ist, verwenden Sie den Mount-Befehl.

Um ein NFS-Volume zu mounten, gehen Sie wie folgt vor:

1. Gehen Sie in der Cloud Console zu Cloud Volumes > Volumes.
2. Zur Seite „Volumes“ gehen
3. Klicken Sie auf das NFS-Volume, für das Sie NFS-Exporte mounten möchten.
4. Scrollen Sie nach rechts und klicken Sie unter „Mehr anzeigen“ auf „Montageanweisungen“.

Um den Mountvorgang innerhalb des Gastbetriebssystems der VMware-VM durchzuführen, führen Sie die folgenden Schritte aus:

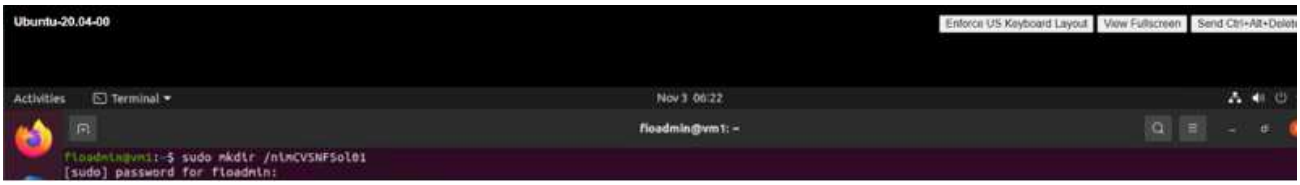
1. Verwenden Sie den SSH-Client und stellen Sie eine SSH-Verbindung zur virtuellen Maschine her.
2. Installieren Sie den NFS-Client auf der Instanz.
   a. Auf einer Red Hat Enterprise Linux- oder SuSE Linux-Instanz:

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

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

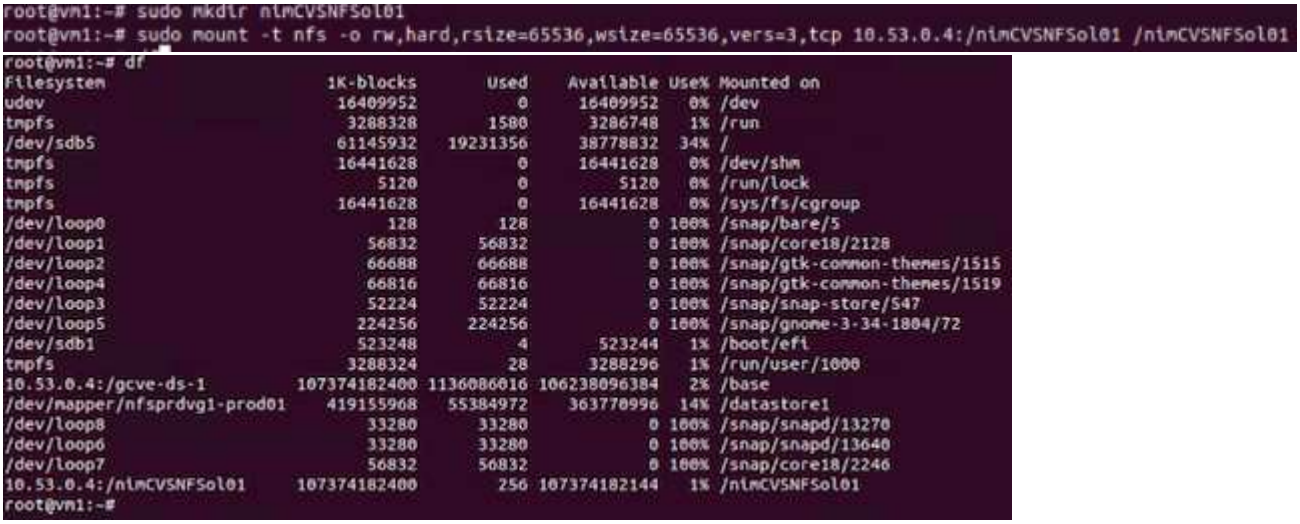
3. Erstellen Sie ein neues Verzeichnis auf der Instanz, beispielsweise „/nimCVSNFSol01“:

```
sudo mkdir /nimCVSNFSol01
```



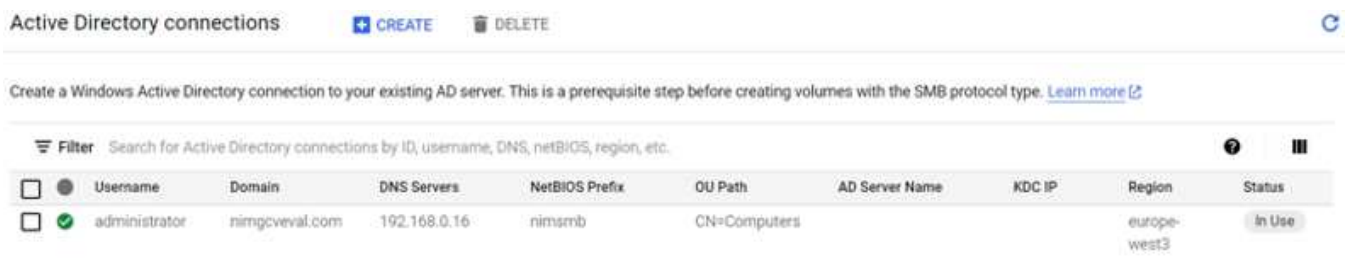
4. Mounten Sie das Volume mit dem entsprechenden Befehl. Nachfolgend sehen Sie einen Beispielbefehl aus dem Labor:

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



▼ **Erstellen und Mounten einer SMB-Freigabe auf VMs, die auf VMware Engine ausgeführt werden**

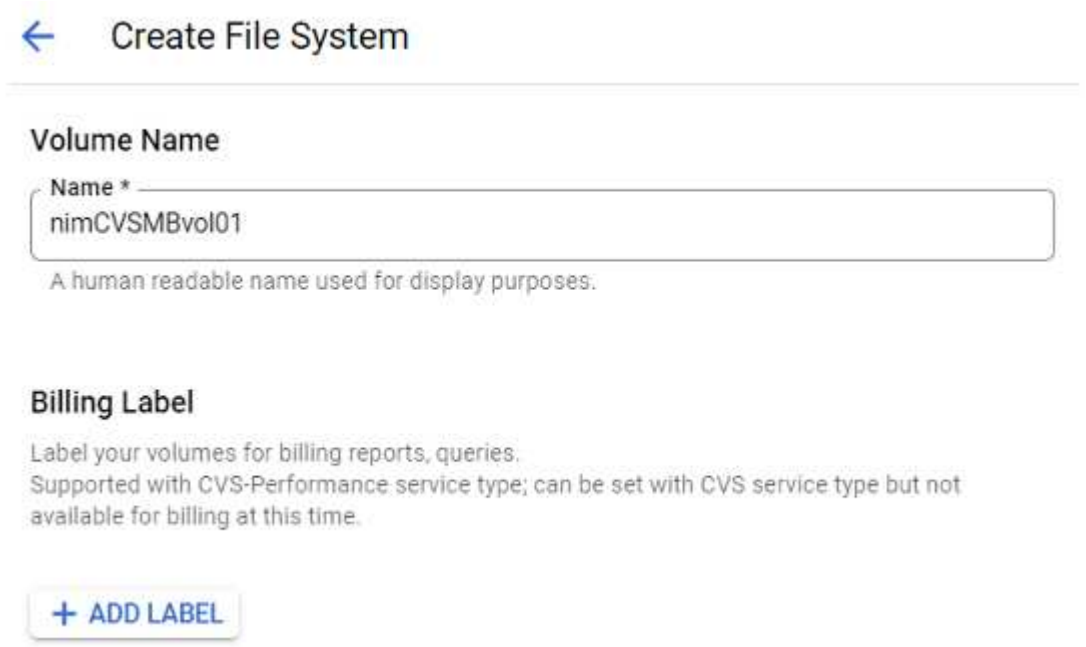
Stellen Sie bei SMB-Volumes sicher, dass die Active Directory-Verbindungen vor dem Erstellen des SMB-Volumes konfiguriert sind.



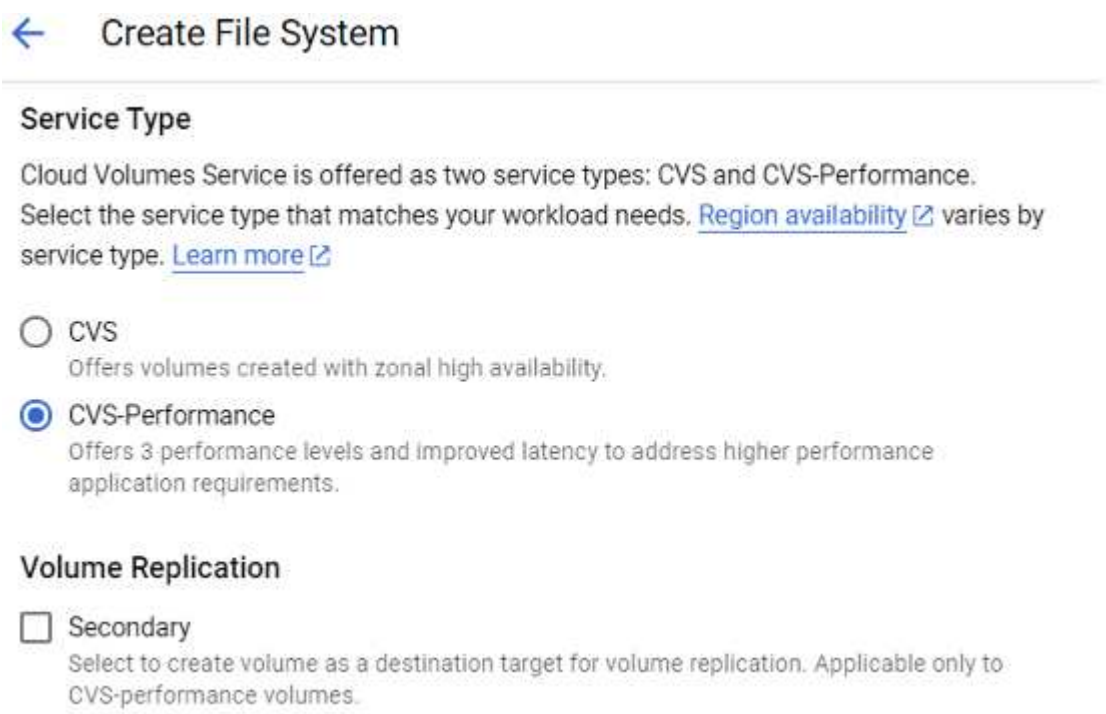
Sobald die AD-Verbindung hergestellt ist, erstellen Sie das Volume mit dem gewünschten Servicelevel. Die Schritte sind dieselben wie beim Erstellen eines NFS-Volumes, außer dass das entsprechende Protokoll

ausgewählt wird.

1. Gehen Sie in der Cloud Volumes-Konsole zur Seite „Volumes“ und klicken Sie auf „Erstellen“.
2. Geben Sie auf der Seite „Dateisystem erstellen“ den Datenträgernamen und die Abrechnungsbezeichnungen nach Bedarf für Rückbuchungsmechanismen an.



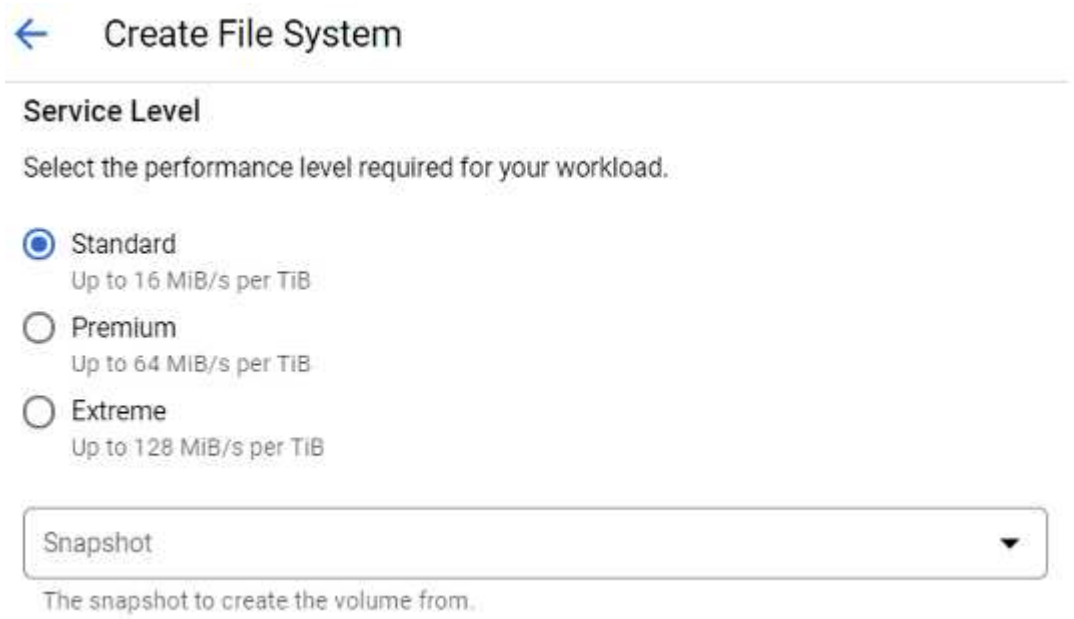
3. Wählen Sie den entsprechenden Dienst aus. Wählen Sie für GCVE NetApp Volumes-Performance und das gewünschte Servicelevel für verbesserte Latenz und höhere Leistung basierend auf den Workload-Anforderungen.



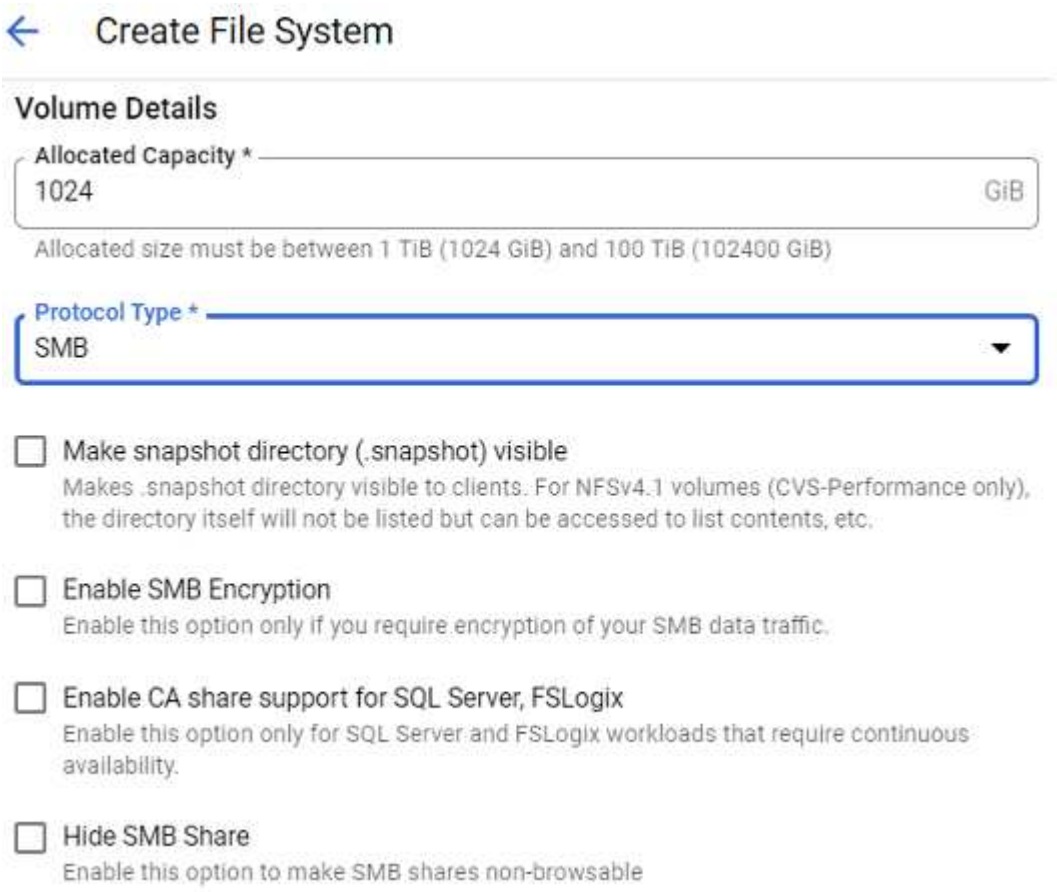
4. Geben Sie die Google Cloud-Region für das Volume und den Volume-Pfad an (der Volume-Pfad muss für alle Cloud-Volumes im Projekt eindeutig sein).



5. Wählen Sie die Leistungsstufe für das Volume aus.

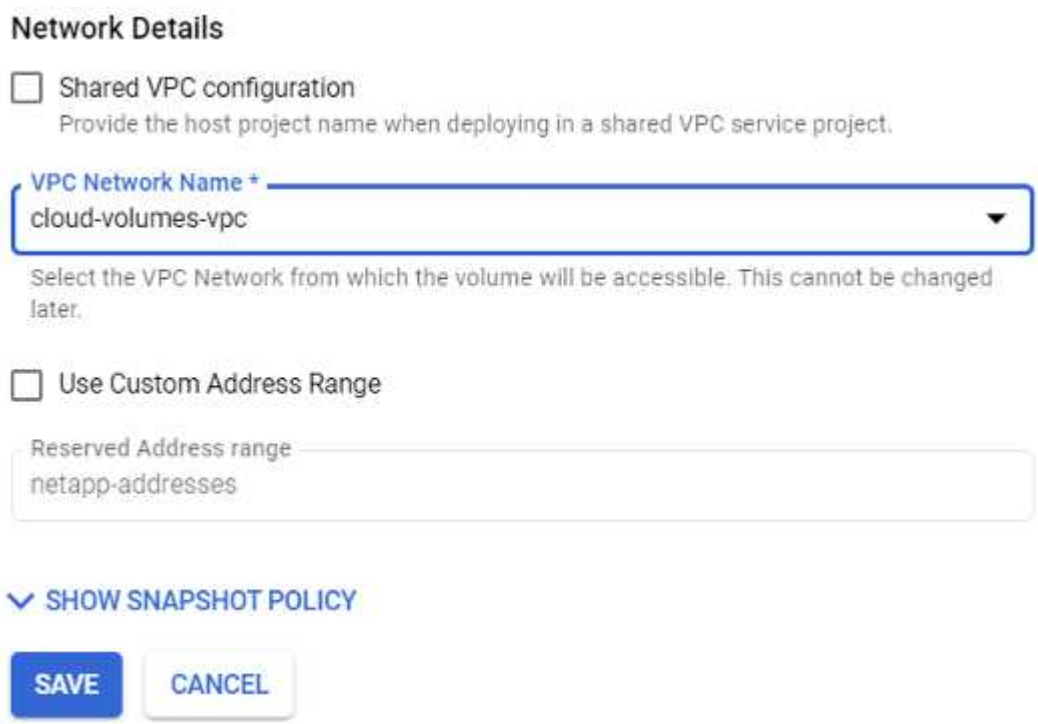


6. Geben Sie die Größe des Volumes und den Protokolltyp an. Bei diesem Test wird SMB verwendet.



7. Wählen Sie in diesem Schritt das VPC-Netzwerk aus, von dem aus auf das Volume zugegriffen werden soll. Stellen Sie sicher, dass VPC-Peering vorhanden ist.

   HINWEIS: Wenn VPC Peering noch nicht eingerichtet wurde, wird eine Pop-up-Schaltfläche angezeigt, die Sie durch die Peering-Befehle führt. Eine Cloud Shell-Sitzung kann geöffnet und die entsprechenden Befehle können ausgeführt werden, um Ihre VPC mit dem Google Cloud NetApp Volumes producer zu verbinden. Falls Sie sich dafür entscheiden, VPC Peering im Voraus vorzubereiten, finden Sie weitere Informationen in diesen "Anweisungen".



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



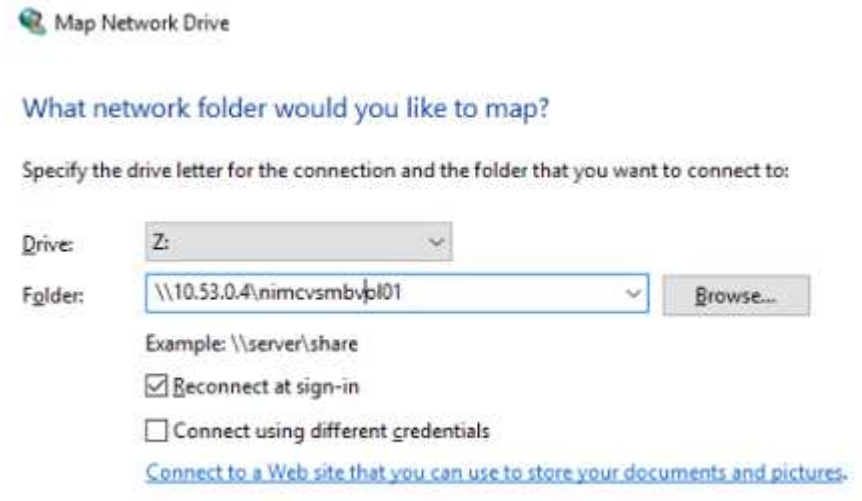
Um das SMB-Volume zu mounten, gehen Sie wie folgt vor:

1. Gehen Sie in der Cloud Console zu Cloud Volumes > Volumes.
2. Zur Seite „Volumes“ gehen
3. Klicken Sie auf das SMB-Volume, für das Sie eine SMB-Freigabe zuordnen möchten.
4. Scrollen Sie nach rechts und klicken Sie unter „Mehr anzeigen“ auf „Montageanweisungen“.

Um den Mountvorgang innerhalb des Windows-Gastbetriebssystems der VMware-VM durchzuführen, führen Sie die folgenden Schritte aus:

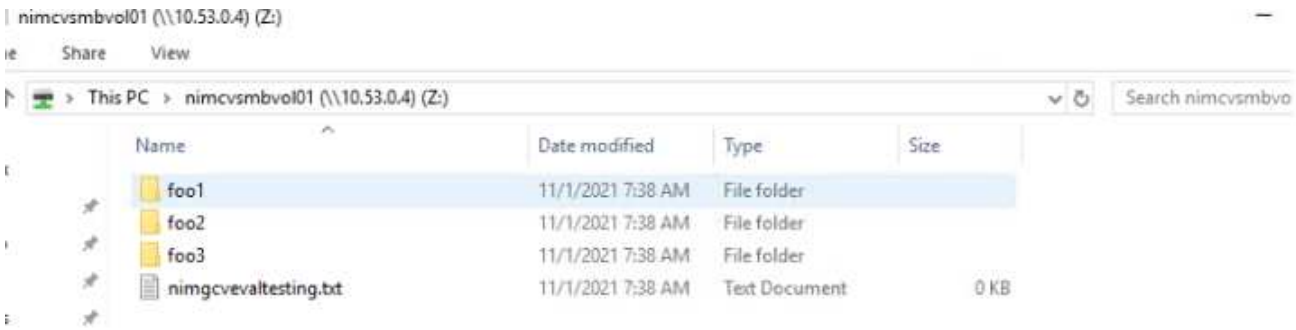
1. Klicken Sie auf die Schaltfläche „Start“ und dann auf „Computer“.
2. Klicken Sie auf „Netzlaufwerk verbinden“.
3. Klicken Sie in der Laufwerksliste auf einen beliebigen verfügbaren Laufwerksbuchstaben.
4. Geben Sie im Ordnerfeld Folgendes ein:

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



Um bei jeder Anmeldung an Ihrem Computer eine Verbindung herzustellen, aktivieren Sie das Kontrollkästchen „Bei Anmeldung erneut verbinden“.

5. Klicken Sie auf Fertig stellen.



Zusammenfassung und Fazit: Warum NetApp Hybrid Multicloud mit VMware

NetApp Cloud Volumes bietet zusammen mit VMware-Lösungen für die großen Hyperscaler großes Potenzial für Unternehmen, die die Hybrid Cloud nutzen möchten. Der Rest dieses Abschnitts enthält Anwendungsfälle, die zeigen, dass die Integration von NetApp Cloud Volumes echte Hybrid-Multicloud-Funktionen ermöglicht.

Anwendungsfall Nr. 1: Speicheroptimierung

Bei der Durchführung einer Größenbestimmung mit der RVtools-Ausgabe ist immer ersichtlich, dass die Leistungsskala (vCPU/vMem) parallel zum Speicher verläuft. Unternehmen geraten häufig in die Situation, dass der Speicherplatz, der die Größe des Clusters erfordert, weit über die erforderliche Leistung hinausgeht.

Durch die Integration von NetApp Cloud Volumes können Unternehmen mit einem einfachen Migrationsansatz eine vSphere-basierte Cloud-Lösung realisieren, ohne dass eine Neuplattformierung, IP-Änderungen oder Architekturänderungen erforderlich sind. Darüber hinaus können Sie mit dieser Optimierung den Speicherbedarf skalieren und gleichzeitig die Anzahl der Hosts in vSphere auf dem Mindestwert halten, ohne dass sich an der Speicherhierarchie, der Sicherheit oder den bereitgestellten Dateien etwas ändert. Dadurch können Sie die Bereitstellung optimieren und die Gesamtbetriebskosten um 35–45 % senken. Diese Integration ermöglicht Ihnen außerdem, den Speicher in Sekundenschnelle von Warm Storage auf

Produktionsleistung zu skalieren.

Anwendungsfall Nr. 2: Cloud-Migration

Unternehmen stehen aus mehreren Gründen unter Druck, Anwendungen von lokalen Rechenzentren in die Public Cloud zu migrieren: ein bevorstehender Ablauf des Mietvertrags, eine Finanzrichtlinie, die von Investitionsausgaben (Capex) auf Betriebsausgaben (Opex) umstellt, oder einfach ein Top-Down-Mandat, alles in die Cloud zu verschieben.

Wenn Geschwindigkeit entscheidend ist, ist nur ein optimierter Migrationsansatz praktikabel, da die Neuplattformierung und Umgestaltung von Anwendungen zur Anpassung an die jeweilige IaaS-Plattform der Cloud langsam und teuer ist und oft Monate dauert. Durch die Kombination von NetApp Cloud Volumes mit der bandbreiteneffizienten SnapMirror -Replikation für mit Gästen verbundenen Speicher (einschließlich RDMs in Verbindung mit anwendungskonsistenten Snapshot-Kopien und HCX, Cloud-spezifischer Migration (z. B. Azure Migrate) oder Produkten von Drittanbietern zum Replizieren von VMs) ist dieser Übergang sogar noch einfacher, als wenn man sich auf zeitaufwändige E/A-Filtermechanismen verlässt.

Anwendungsfall Nr. 3: Rechenzentrumserweiterung

Wenn ein Rechenzentrum aufgrund saisonaler Nachfragespitzen oder einfach aufgrund stetigen organischen Wachstums seine Kapazitätsgrenzen erreicht, ist die Umstellung auf das in der Cloud gehostete VMware zusammen mit NetApp Cloud Volumes eine einfache Lösung. Durch die Nutzung von NetApp Cloud Volumes können Sie Speicher ganz einfach erstellen, replizieren und erweitern, indem Sie hohe Verfügbarkeit über Verfügbarkeitszonen hinweg und dynamische Skalierungsfunktionen bereitstellen. Durch die Nutzung von NetApp Cloud Volumes können Sie die Hostclusterkapazität minimieren, da keine Stretchcluster mehr erforderlich sind.

Anwendungsfall Nr. 4: Notfallwiederherstellung in der Cloud

Bei einem herkömmlichen Ansatz müssten im Katastrophenfall die in die Cloud replizierten VMs auf die eigene Hypervisor-Plattform der Cloud konvertiert werden, bevor sie wiederhergestellt werden könnten – eine Aufgabe, die während einer Krise nicht zu bewältigen ist.

Durch die Verwendung von NetApp Cloud Volumes für mit Gästen verbundenen Speicher mithilfe von SnapCenter und SnapMirror -Replikation vor Ort zusammen mit Virtualisierungslösungen aus der öffentlichen Cloud kann ein besserer Ansatz für die Notfallwiederherstellung entwickelt werden, der die Wiederherstellung von VM-Replikaten auf einer vollständig konsistenten VMware SDDC-Infrastruktur zusammen mit Cloud-spezifischen Wiederherstellungstools (z. B. Azure Site Recovery) oder gleichwertigen Tools von Drittanbietern wie Veeam ermöglicht. Mit diesem Ansatz können Sie außerdem schnell Notfallwiederherstellungsübungen und Wiederherstellungen nach Ransomware durchführen. Dadurch können Sie auch zu Testzwecken oder im Katastrophenfall durch Hinzufügen von Hosts nach Bedarf auf die volle Produktion skalieren.

Anwendungsfall Nr. 5: Anwendungsmodernisierung

Nachdem sich Anwendungen in der öffentlichen Cloud befinden, möchten Unternehmen die Vorteile der Hunderte leistungsstarker Cloud-Dienste nutzen, um sie zu modernisieren und zu erweitern. Durch die Verwendung von NetApp Cloud Volumes ist die Modernisierung ein einfacher Prozess, da die Anwendungsdaten nicht in vSAN gesperrt sind und Datenmobilität für eine Vielzahl von Anwendungsfällen, einschließlich Kubernetes, ermöglicht wird.

Abschluss

Unabhängig davon, ob Sie eine reine Cloud oder eine Hybrid-Cloud anstreben, bietet NetApp Cloud Volumes hervorragende Optionen zum Bereitstellen und Verwalten der Anwendungs-Workloads zusammen mit

Dateidiensten und Blockprotokollen. Gleichzeitig werden die Gesamtbetriebskosten gesenkt, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden.

Wählen Sie für jeden Anwendungsfall Ihren bevorzugten Cloud-/Hyperscaler zusammen mit NetApp Cloud Volumes, um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und konsistente Abläufe vor Ort und in mehreren Clouds zu gewährleisten, Workloads bidirektional zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen.

Es handelt sich um dieselben bekannten Prozesse und Verfahren, die zum Verbinden des Speichers verwendet werden. Denken Sie daran, dass sich mit den neuen Namen nur die Position der Daten geändert hat. Die Tools und Prozesse bleiben alle gleich und NetApp Cloud Volumes hilft bei der Optimierung der gesamten Bereitstellung.

Anwendungsfälle für VMware Hybrid Cloud

Anwendungsfälle für NetApp Hybrid Multicloud mit VMware

Eine Übersicht über die Anwendungsfälle, die für die IT-Organisation bei der Planung von Hybrid-Cloud- oder Cloud-First-Bereitstellungen von Bedeutung sind.

Beliebte Anwendungsfälle

Anwendungsfälle umfassen:

- Notfallwiederherstellung,
- Hosting von Workloads während der Wartung des Rechenzentrums, * kurze Auslastungsspitzen, bei denen zusätzliche Ressourcen benötigt werden, die über die im lokalen Rechenzentrum bereitgestellten hinausgehen,
- VMware-Site-Erweiterung,
- Schnelle Migration in die Cloud,
- Entwicklung/Test und
- Modernisierung von Apps durch Nutzung ergänzender Cloud-Technologien.

In dieser Dokumentation werden Verweise auf Cloud-Workloads anhand der VMware-Anwendungsfälle detailliert beschrieben. Diese Anwendungsfälle sind:

- Schützen (beinhaltet sowohl Disaster Recovery als auch Backup/Wiederherstellung)
- Wandern
- Verlängern

Einblicke in die IT-Reise

Die meisten Organisationen befinden sich auf dem Weg der Transformation und Modernisierung. Im Rahmen dieses Prozesses versuchen Unternehmen, ihre vorhandenen VMware-Investitionen zu nutzen, gleichzeitig die Vorteile der Cloud zu nutzen und nach Möglichkeiten zu suchen, den Migrationsprozess so nahtlos wie möglich zu gestalten. Dieser Ansatz würde ihre Modernisierungsbemühungen sehr einfach machen, da sich die Daten bereits in der Cloud befinden.

Die einfachste Antwort auf dieses Szenario sind VMware-Angebote in jedem Hyperscaler. Wie NetApp Cloud Volumes bietet VMware eine Möglichkeit, lokale VMware-Umgebungen in jede beliebige Cloud zu verschieben

oder zu erweitern. So können Sie vorhandene lokale Ressourcen, Kenntnisse und Tools beibehalten und gleichzeitig Workloads nativ in der Cloud ausführen. Dies reduziert das Risiko, da es zu keinen Dienstunterbrechungen oder IP-Änderungen kommt und das IT-Team mit vorhandenen Kenntnissen und Tools wie vor Ort arbeiten kann. Dies kann zu beschleunigten Cloud-Migrationen und einem wesentlich reibungsloseren Übergang zu einer hybriden Multicloud-Architektur führen.

Die Bedeutung zusätzlicher NFS-Speicheroptionen verstehen

Während VMware in jeder Cloud jedem Kunden einzigartige Hybridfunktionen bietet, ist die Nützlichkeit von VMware für Unternehmen mit speicherintensiven Workloads aufgrund der begrenzten zusätzlichen NFS-Speicheroptionen eingeschränkt. Da der Speicher direkt an Hosts gebunden ist, besteht die einzige Möglichkeit zur Skalierung des Speichers darin, weitere Hosts hinzuzufügen – und das kann die Kosten bei speicherintensiven Workloads um 35–40 Prozent oder mehr erhöhen. Diese Arbeitslasten benötigen lediglich zusätzlichen Speicher, nicht zusätzliche Leistung. Das bedeutet jedoch, dass für zusätzliche Hosts bezahlt werden muss.

Betrachten wir folgendes Szenario:

Ein Kunde benötigt nur fünf Hosts für CPU und Speicher, hat jedoch einen großen Speicherbedarf und braucht 12 Hosts, um den Speicherbedarf zu decken. Diese Anforderung führt letztendlich zu einem erheblichen finanziellen Problem, da zusätzliche Leistung gekauft werden muss, obwohl lediglich der Speicher erweitert werden muss.

Wenn Sie die Einführung und Migration in die Cloud planen, ist es immer wichtig, den besten Ansatz zu ermitteln und den einfachsten Weg zu wählen, der die Gesamtinvestitionen reduziert. Der gängigste und einfachste Ansatz für jede Anwendungsmigration ist das Rehosting (auch als „Lift and Shift“ bezeichnet), bei dem keine virtuelle Maschine (VM) oder Datenkonvertierung stattfindet. Die Verwendung von NetApp Cloud Volumes mit VMware Software-Defined Data Center (SDDC) bietet als Ergänzung zu vSAN eine einfache Lift-and-Shift-Option.

NetApp -Lösungen für VMware in Hyperscalern

Erfahren Sie mehr über die Lösungen, die NetApp in die VMware-Umgebung jedes Hyperscalers einbringt – von der Migration von Workflows über die Erweiterung/Ausweitung in die Cloud bis hin zu Backup/Wiederherstellung und Notfallwiederherstellung.

NetApp -Lösungen für VMware-Umgebungen

Unabhängig davon, ob Sie in einem Hybrid-Cloud-Modell oder einem „Cloud First“-Modell arbeiten, bietet NetApp eine große Vielfalt an Lösungen für die gängigsten Anwendungsfälle zur Verwaltung von Workloads in einem Cloud- oder Hybrid-Cloud-Modell.

NetApp bietet außerdem Lösungen für Speicher, der als In-Guest-Speicher (mit Gast verbunden) oder als zusätzlicher NFS-Datenspeicher in jedem der Hyperscaler bereitgestellt wird. Alle Lösungen werden im Einklang mit der VMware-Klassifizierung von Cloud-Workloads kategorisiert. Zu diesen Klassifizierungen gehören:

- Schützen (beinhaltet sowohl Disaster Recovery als auch Backup/Wiederherstellung)
- Wandern
- Verlängern

Weitere Einzelheiten zu den für jeden Hyperscaler verfügbaren Lösungen finden Sie unter:

- "Lösungen für AWS / VMC"
- "Lösungen für Azure / AVS"
- "Lösungen für GCP / GCVE"

NetApp -Lösungen für Amazon VMware Managed Cloud (VMC)

Erfahren Sie mehr über die Lösungen, die NetApp für AWS bereitstellt.

VMware unterteilt die Cloud-Workloads in eine von drei Kategorien:

- Schützen (einschließlich Notfallwiederherstellung und Sicherung/Wiederherstellung)
- Wandern
- Verlängern

Durchsuchen Sie die verfügbaren Lösungen in den folgenden Abschnitten.

Schützen

- "Notfallwiederherstellung mit VMC auf AWS (Gastverbindung)"
- "Veeam Backup Restore in VMC mit FSx ONTAP"
- "Disaster Recovery (DRO) mit FSx ONTAP und VMC"
- "Verwenden von Veeam Replication und FSx ONTAP für die Notfallwiederherstellung in VMware Cloud auf AWS"

Wandern

- "Migrieren Sie Workloads mit VMware HCX in den FSx ONTAP Datenspeicher"

Verlängern

DEMNÄCHST KOMMT!!

NetApp -Lösungen für Azure VMware Solution (AVS)

Erfahren Sie mehr über die Lösungen, die NetApp für Azure bereitstellt.

VMware unterteilt die Cloud-Workloads in eine von drei Kategorien:

- Schützen (einschließlich Notfallwiederherstellung und Sicherung/Wiederherstellung)
- Wandern
- Verlängern

Durchsuchen Sie die verfügbaren Lösungen in den folgenden Abschnitten.

Schützen

- "Disaster Recovery mit ANF und JetStream (zusätzlicher NFS-Datenspeicher)"
- "Disaster Recovery mit ANF und CVO (Guest Connected Storage)"
- "Disaster Recovery (DRO) mit ANF und AVS"

- "Verwenden der Veeam-Replikation und des Azure NetApp Files -Datenspeichers für die Notfallwiederherstellung in Azure VMware Solution"

Wandern

- "Migrieren Sie Workloads mit VMware HCX zum Azure NetApp Files Datenspeicher"

Verlängern

DEMNÄCHST KOMMT!!

NetApp -Lösungen für Google Cloud VMware Engine (GCVE)

Erfahren Sie mehr über die Lösungen, die NetApp für GCP bereitstellt.

VMware unterteilt die Cloud-Workloads in eine von drei Kategorien:

- Schützen (einschließlich Notfallwiederherstellung und Sicherung/Wiederherstellung)
- Wandern
- Verlängern

Durchsuchen Sie die verfügbaren Lösungen in den folgenden Abschnitten.

Schützen

- "Anwendungs-Notfallwiederherstellung mit SnapCenter, Cloud Volumes ONTAP und Veeam Replication"
- "Anwendungskonsistente Notfallwiederherstellung mit NetApp SnapCenter und Veeam-Replikation auf NetApp Volumes auf GCVE"

Wandern

- "Workload-Migration mit VMware HCX zum NFS-Datenspeicher von Google Cloud NetApp Volumes"
- "VM-Replikation mit Veeam zum NFS-Datenspeicher von Google Cloud NetApp Volumes"

Verlängern

DEMNÄCHST KOMMT!!

NetApp für AWS/VMC

NetApp -Funktionen für AWS VMC

Erfahren Sie mehr über die Funktionen, die NetApp in die AWS VMware Cloud (VMC) einbringt – von NetApp als an einen Gast angeschlossenes Speichergerät oder als zusätzlicher NFS-Datenspeicher bis hin zur Migration von Workflows, Erweiterung/Bursting in die Cloud, Sicherung/Wiederherstellung und Notfallwiederherstellung.

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

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

Konfigurieren von VMC in AWS

Wie bei der lokalen Umgebung ist die Planung einer Cloud-basierten Virtualisierungsumgebung entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen und Migrieren von VMs.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud on AWS SDDC einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp -Speicher verwenden.



In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP mit AWS VMC.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von VMware Cloud für AWS
- Verbinden Sie VMware Cloud mit FSx ONTAP

Sehen Sie sich die detaillierte"Konfigurationsschritte für VMC" .

NetApp Storage-Optionen für VMC

NetApp Speicher kann innerhalb von AWS VMC auf verschiedene Weise genutzt werden – entweder als verbundener oder als zusätzlicher NFS-Datenspeicher.

Bitte besuchen Sie"Unterstützte NetApp -Speicheroptionen" für weitere Informationen.

AWS unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- FSx ONTAP als Gastspeicher
- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- FSx ONTAP als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungs-Speicheroptionen für VMC" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für VMC" .

Anwendungsfälle der Lösung

Mit den Cloud-Lösungen von NetApp und VMware lassen sich viele Anwendungsfälle ganz einfach in Ihrem AWS VMC bereitstellen. Für jeden der von VMware definierten Cloud-Bereiche werden Anwendungsfälle definiert:

- Schützen (beinhaltet sowohl Disaster Recovery als auch Backup/Wiederherstellung)
- Verlängern
- Wandern

"Durchsuchen Sie die NetApp -Lösungen für AWS VMC"

Schützen Sie Workloads auf AWS/VMC

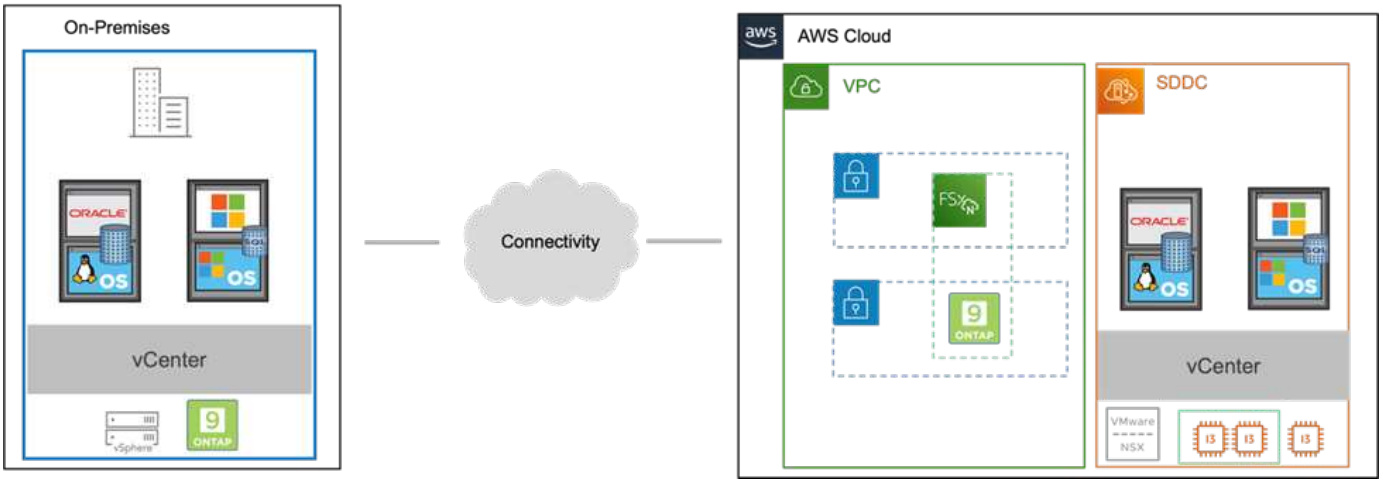
TR-4931: Notfallwiederherstellung mit VMware Cloud auf Amazon Web Services und Guest Connect

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

Überblick

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

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



Annahmen, Voraussetzungen und Komponentenübersicht

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

"Anforderungen, Voraussetzungen und Planung der DR-Lösung"

Durchführen von DR mit SnapCenter

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

Maschinen.

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

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

Konfigurieren Sie SnapMirror -Beziehungen und Aufbewahrungspläne

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

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

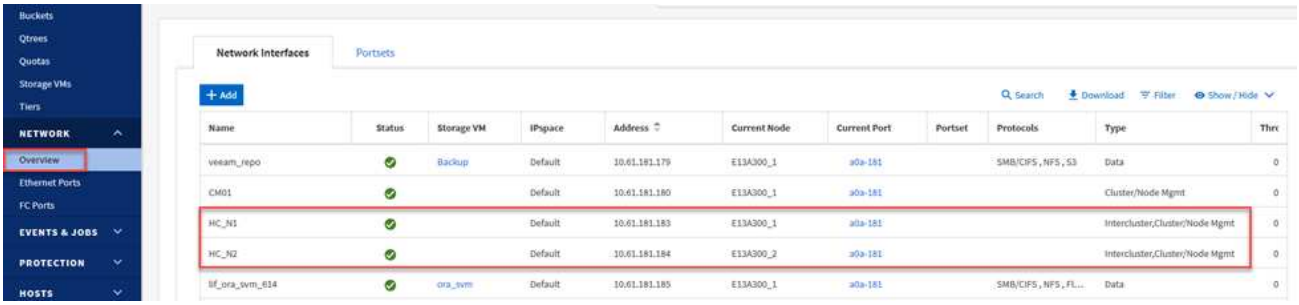
Zum Einrichten von SnapMirror -Beziehungen zwischen einem lokalen ONTAP System und FSx ONTAP sind die folgenden Schritte erforderlich:

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

▼ **Notieren Sie die logischen Quell- und Zielschnittstellen zwischen Clustern.**

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

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



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

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

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

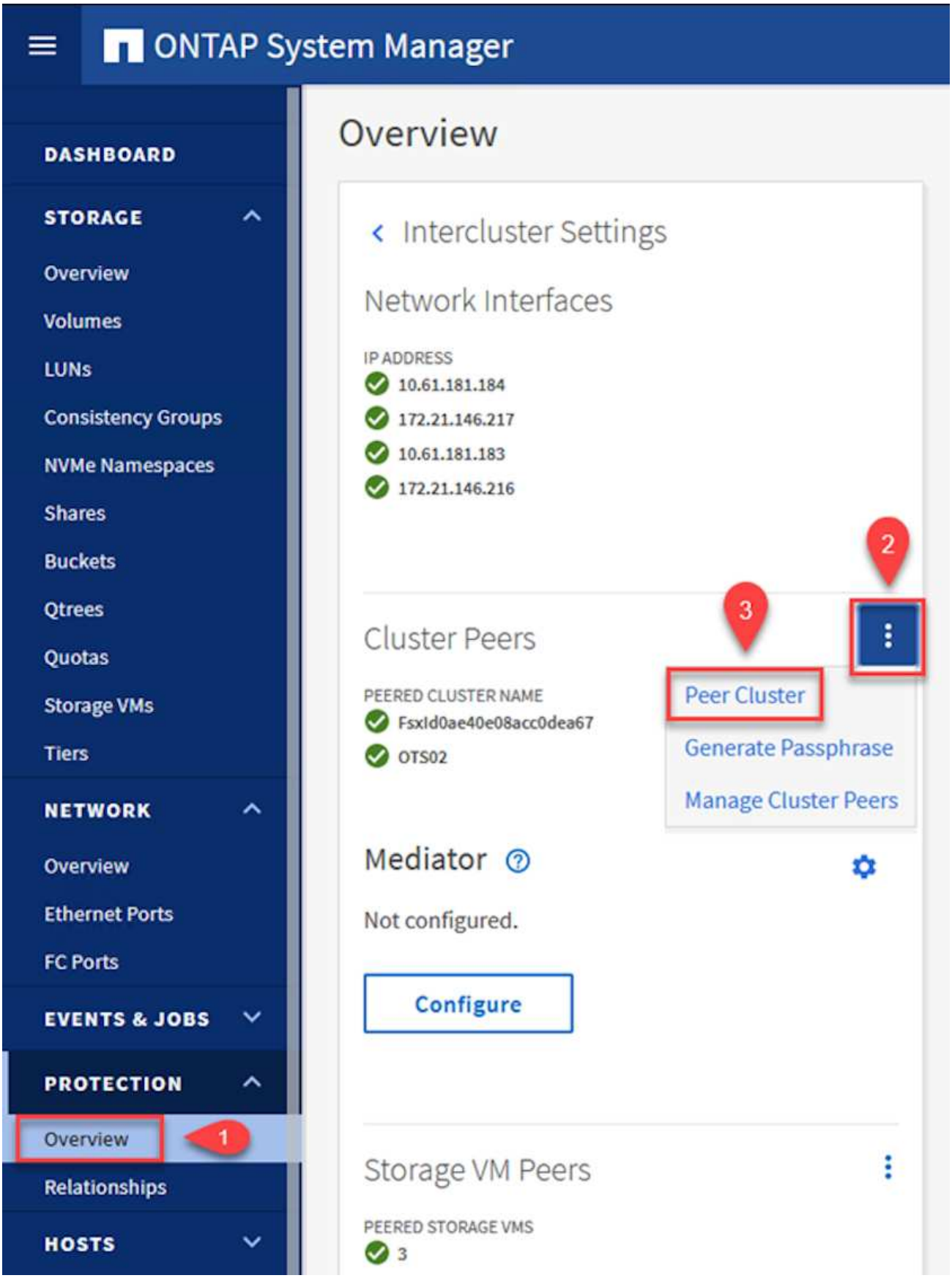
▼ **Cluster-Peering zwischen ONTAP und FSx einrichten**

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

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

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

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



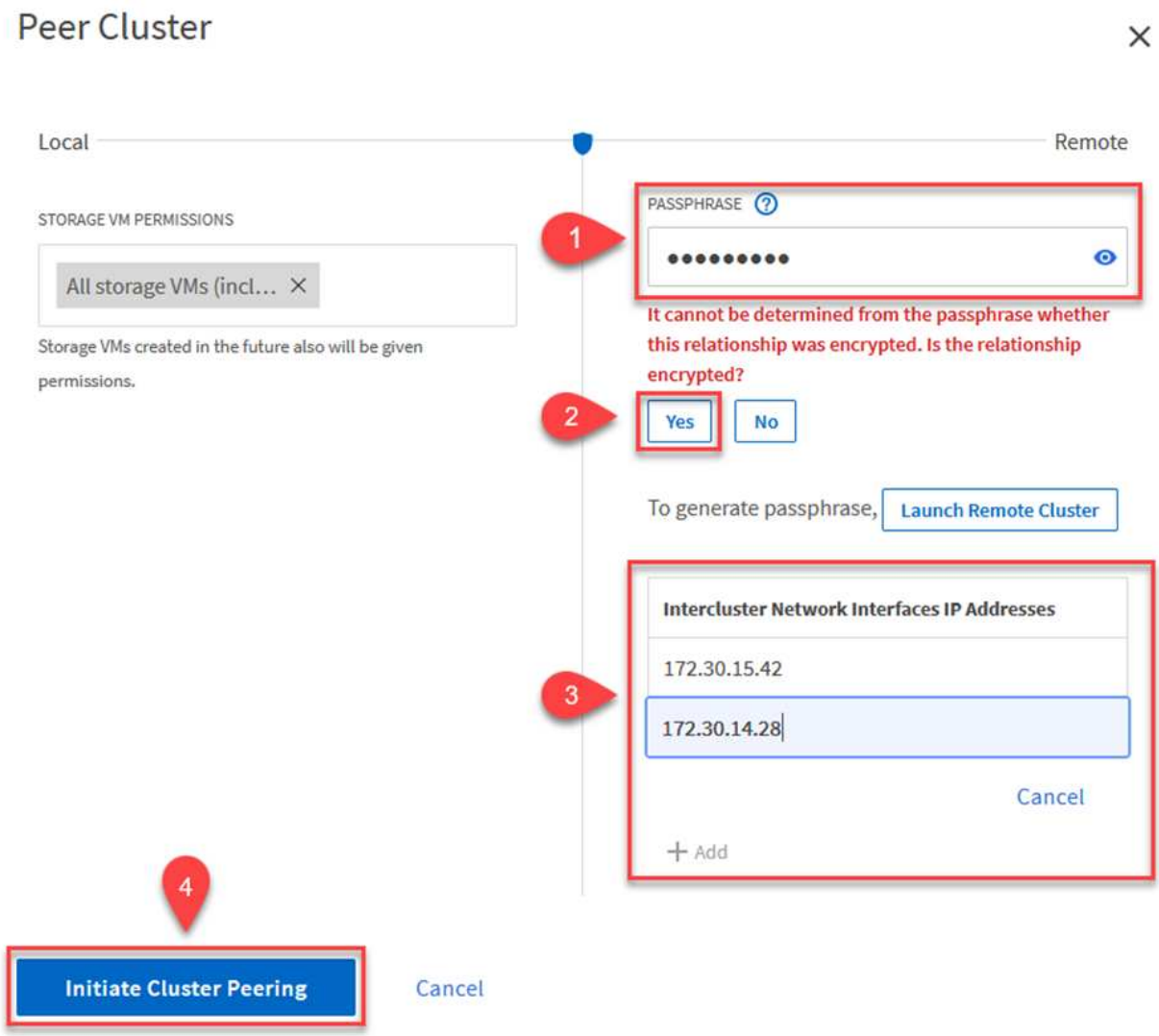
3. Geben Sie im Dialogfeld „Peer-Cluster“ die erforderlichen Informationen ein:
   a. Geben Sie die Passphrase ein, die zum Herstellen der Peer-Cluster-Beziehung im Ziel-FSx-Cluster

verwendet wurde.

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

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

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



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

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

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

▼ **Herstellen einer SVM-Peering-Beziehung**

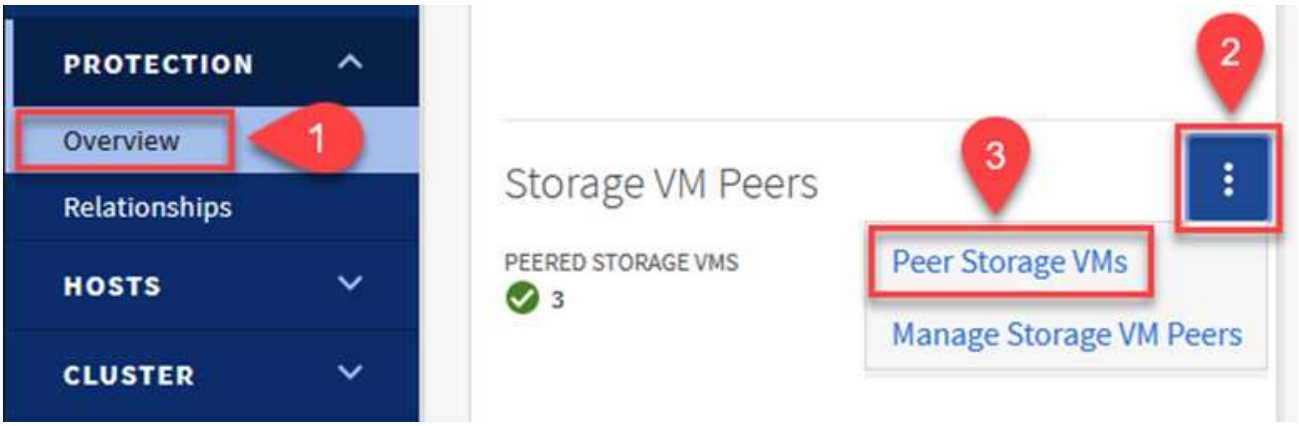
Der nächste Schritt besteht darin, eine SVM-Beziehung zwischen den virtuellen Ziel- und

Quellspeichermaschinen einzurichten, die die Volumes enthalten, die in SnapMirror -Beziehungen enthalten sein werden.

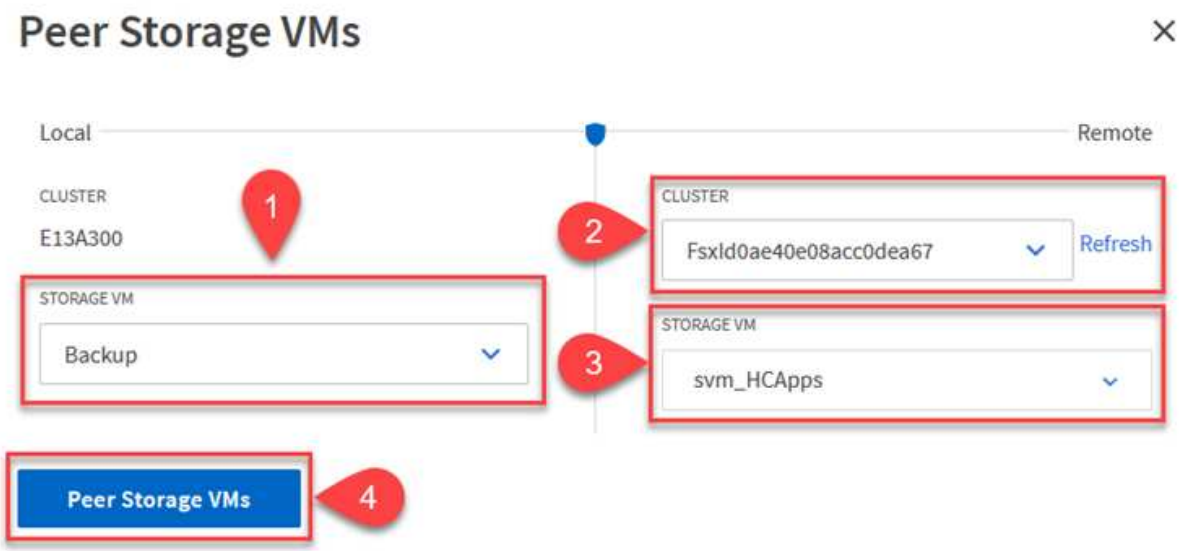
1. Verwenden Sie im Quell-FSx-Cluster den folgenden Befehl aus der CLI, um die SVM-Peer-Beziehung zu erstellen:

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

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



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



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

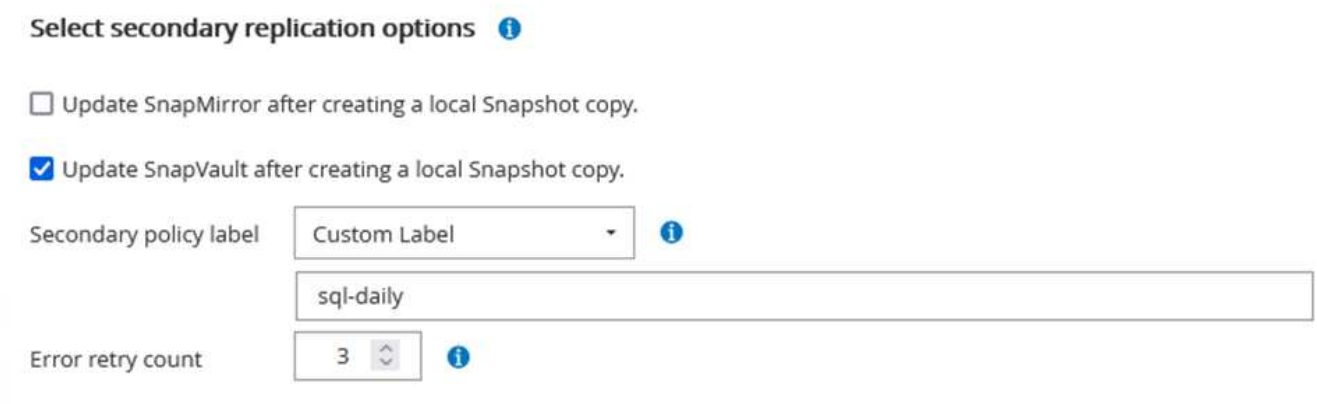
▼ **Erstellen einer Snapshot-Aufbewahrungsrichtlinie**

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

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

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

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



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

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

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

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

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

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

```
#ofSnapshotsToRetain
```

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

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

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

▼ **Zielvolumes erstellen**

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

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

▼ **Erstellen Sie die SnapMirror -Beziehungen zwischen Quell- und Zielvolumes**

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

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

▼ **Initialisieren Sie die SnapMirror -Beziehungen**

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

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

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

▼ **Bereitstellen von Windows SnapCenter Server vor Ort**

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

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

Die SnapCenter software ist erhältlich unter "dieser Link" .

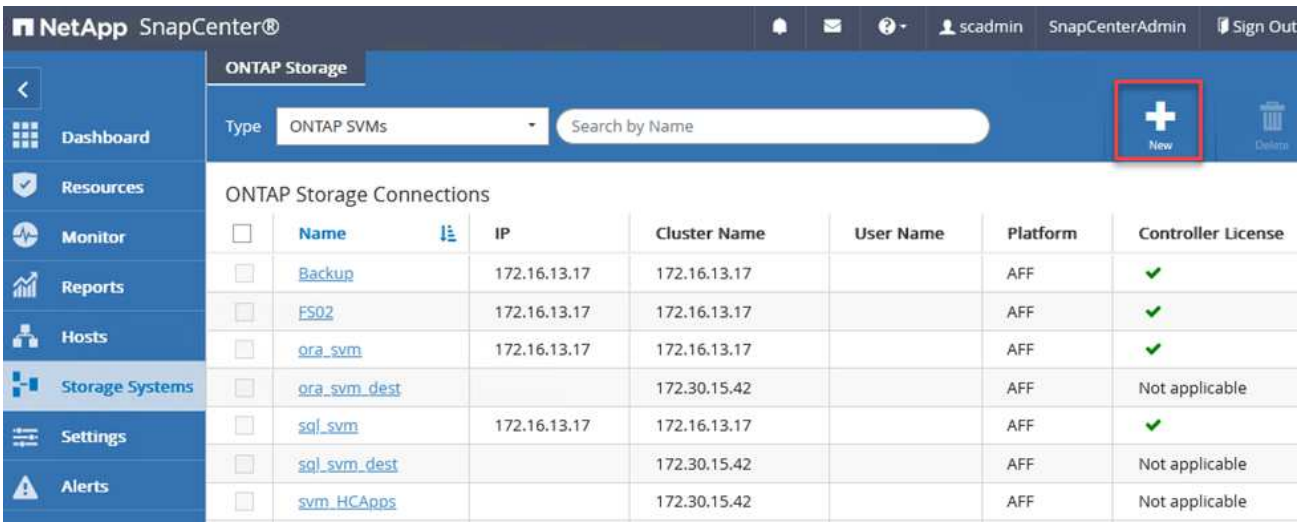
Nach der Installation können Sie über einen Webbrowser mit *https://Virtual_Cluster_IP_or_FQDN:8146* auf die SnapCenter -Konsole zugreifen.

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

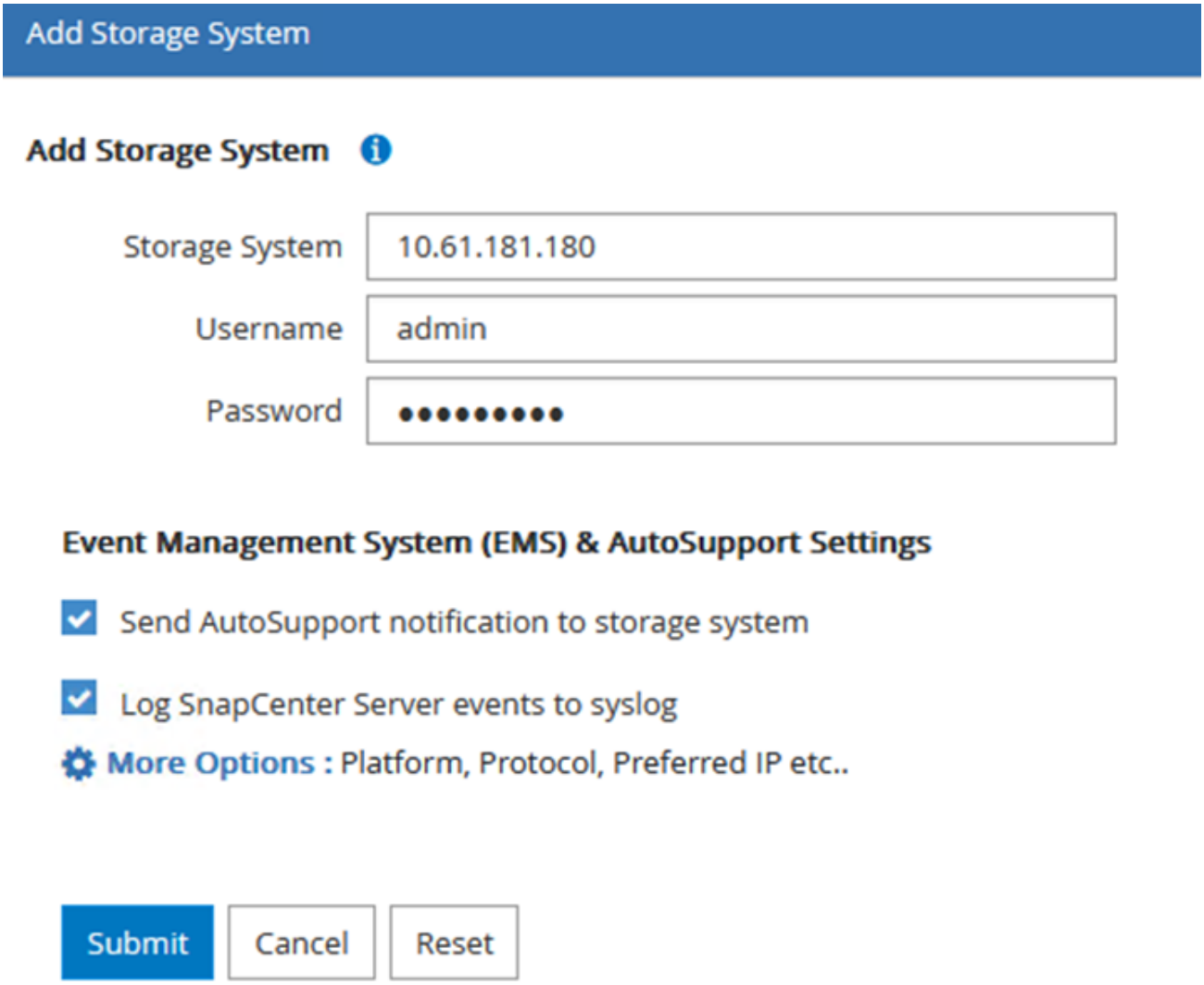
▼ **Speichercontroller zu SnapCenter hinzufügen**

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

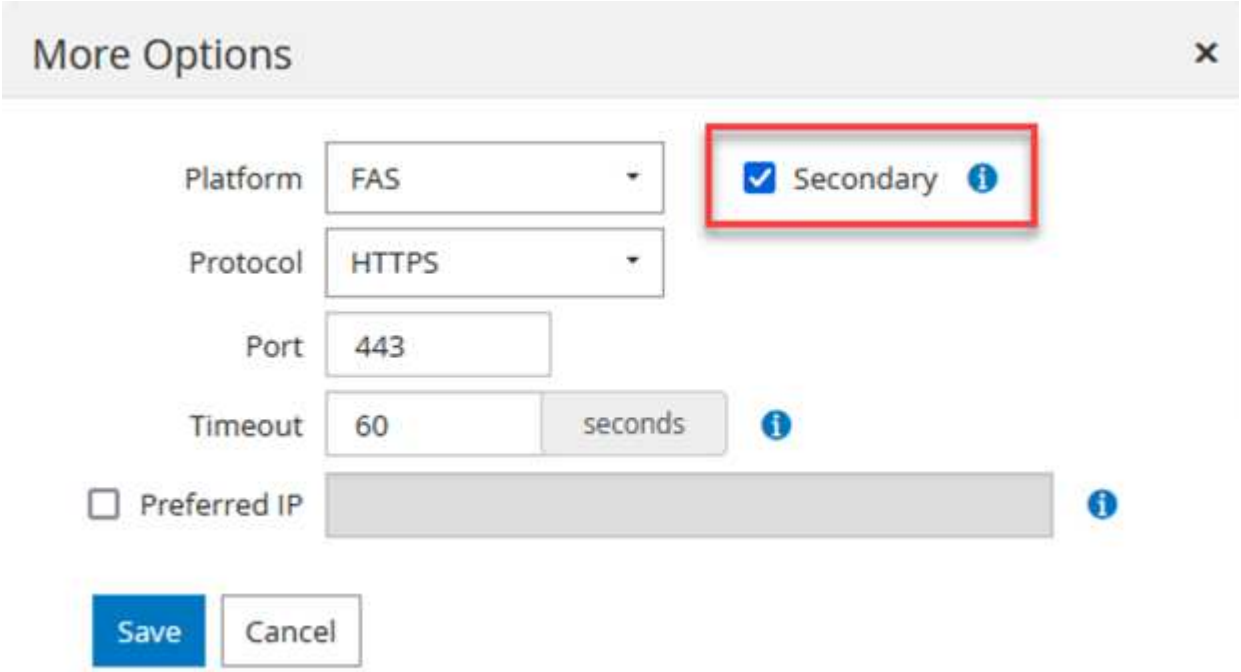
1. Wählen Sie im linken Menü „Speichersysteme“ aus und klicken Sie dann auf „Neu“, um mit dem Hinzufügen Ihrer Speichercontroller zu SnapCenter zu beginnen.



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



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

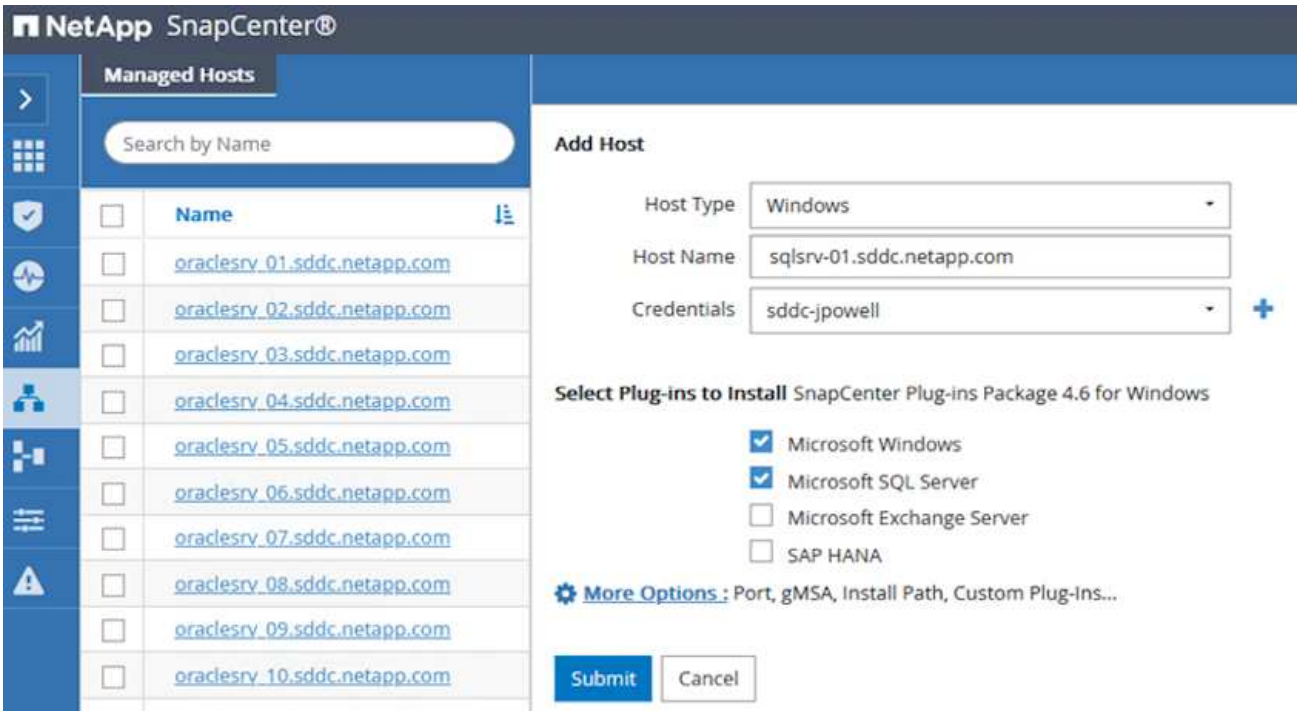


Weitere Informationen zum Hinzufügen von Speichersystemen zu SnapCenter finden Sie in der Dokumentation unter "dieser Link" .

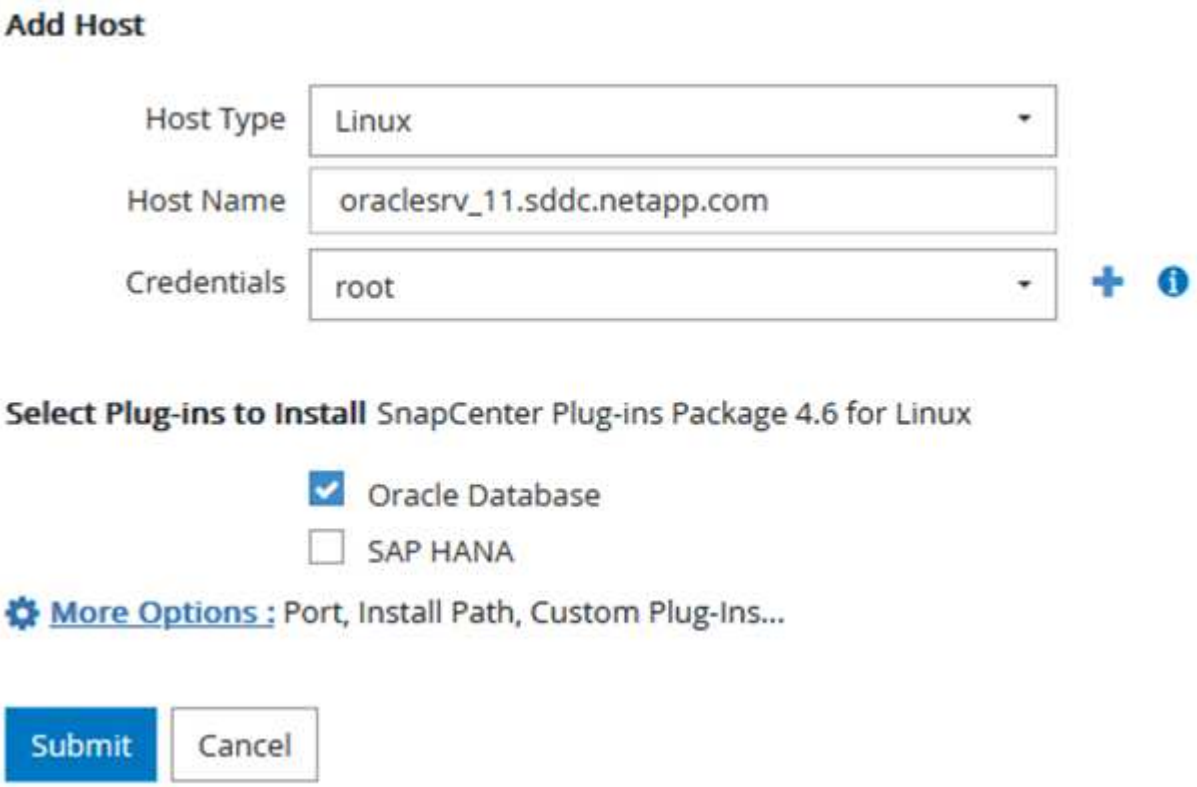
▼ **Hosts zu SnapCenter hinzufügen**

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

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



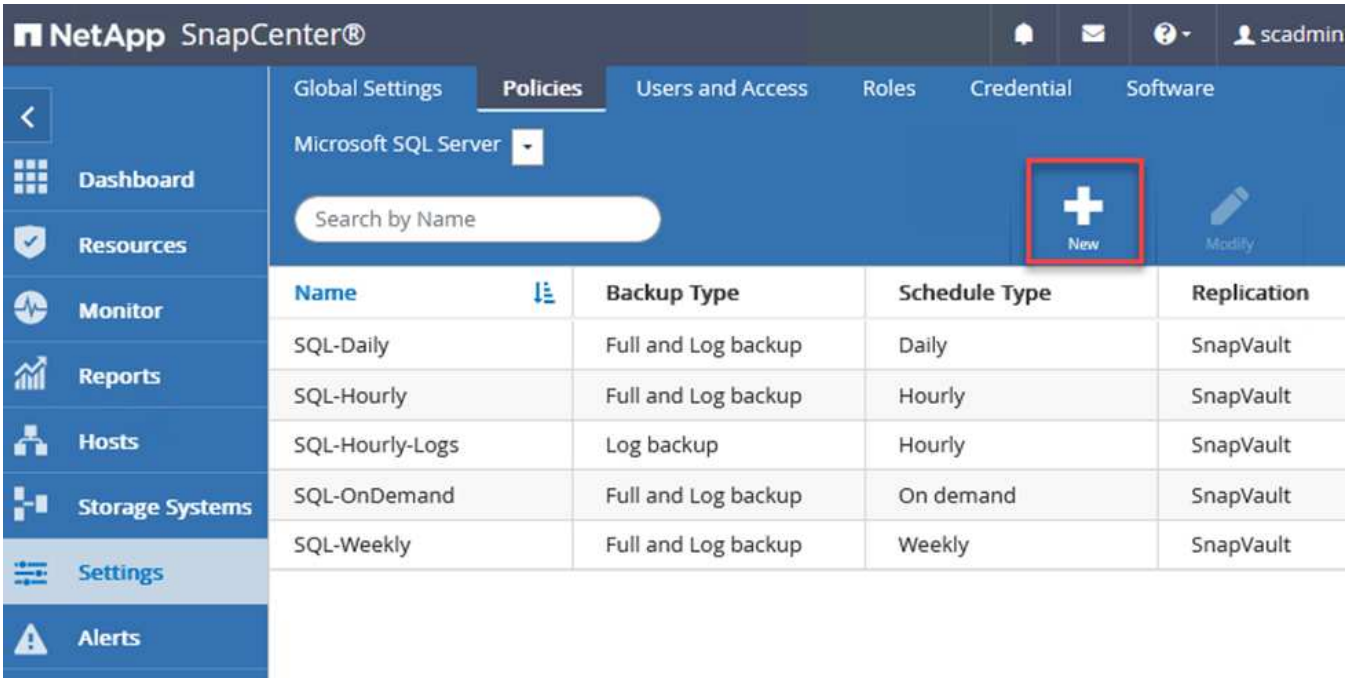
3. Füllen Sie für Oracle die erforderlichen Felder im Dialogfeld „Host hinzufügen“ aus und aktivieren Sie das Kontrollkästchen für das Oracle-Datenbank-Plug-In. Klicken Sie anschließend auf „Senden“, um den Erkennungsprozess zu starten und den Host zu SnapCenter hinzuzufügen.



▼ **Erstellen von SnapCenter -Richtlinien**

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

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



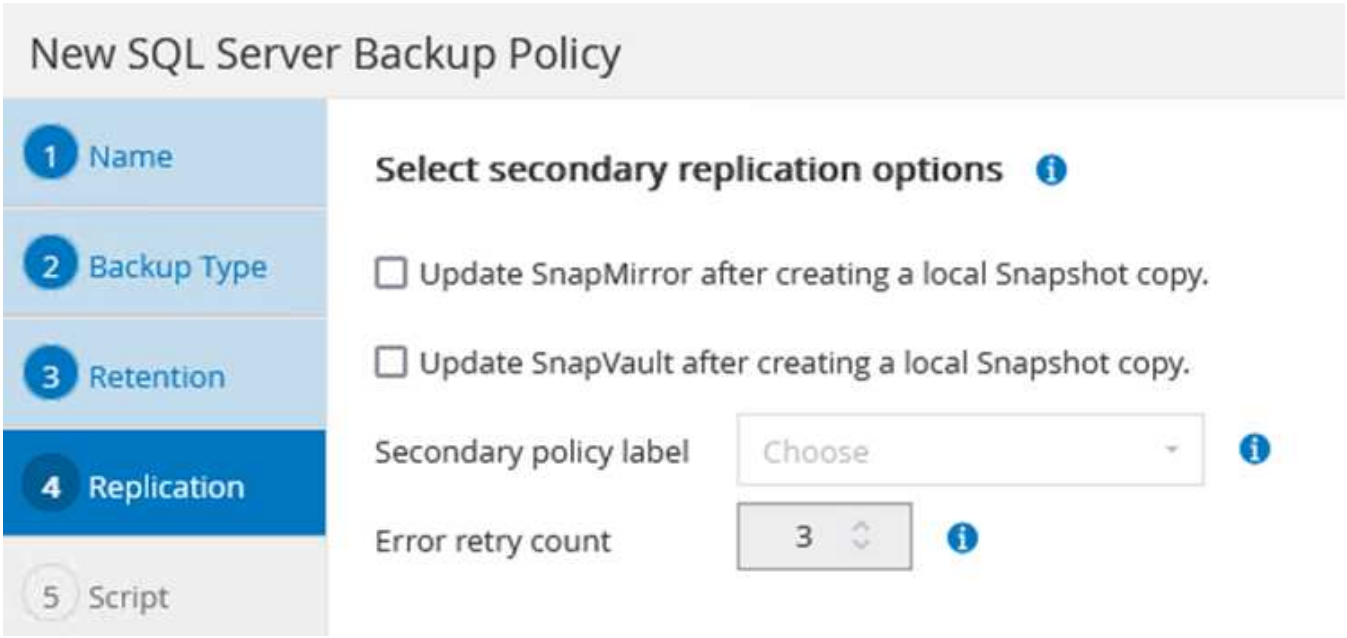
Ausführliche Informationen zum Erstellen von Richtlinien für SQL Server-Backups finden Sie im "SnapCenter -Dokumentation" .

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

Anmerkungen:

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

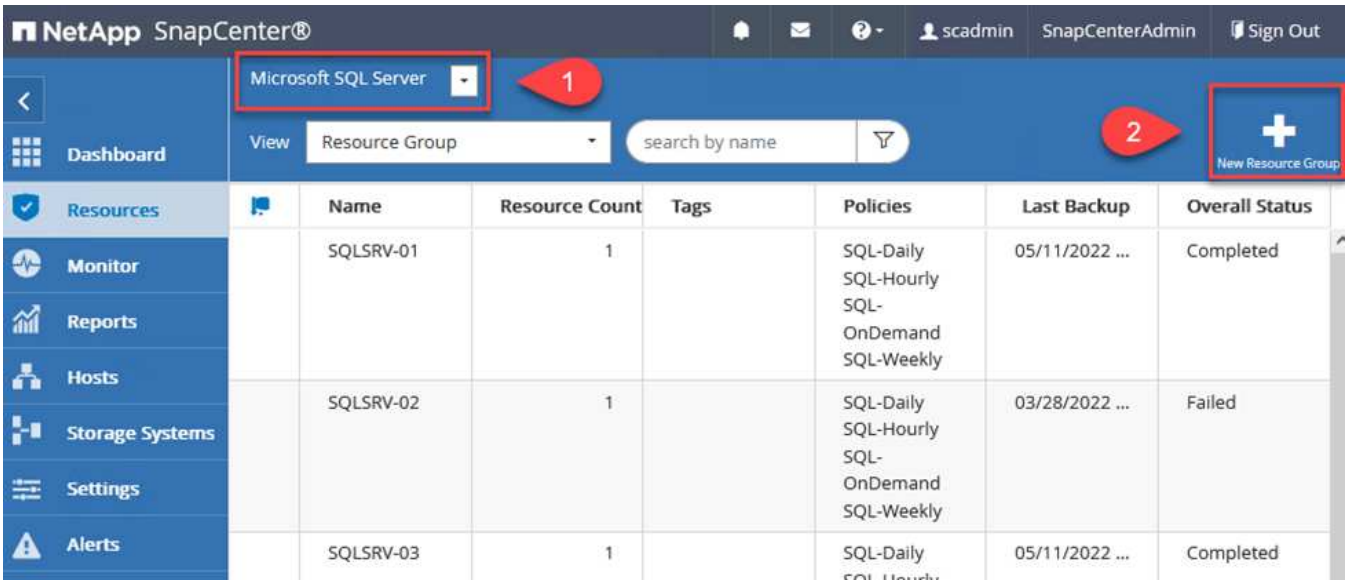
Das folgende Bild zeigt die vorhergehenden Optionen und wie sie im Assistenten für Sicherungsrichtlinien aussehen.



▼ Erstellen von SnapCenter -Ressourcengruppen

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

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



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

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

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

Bereitstellen und Konfigurieren des Veeam Backup Servers

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

▼ Konfigurieren des Veeam Scale-Out-Backup-Repository

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

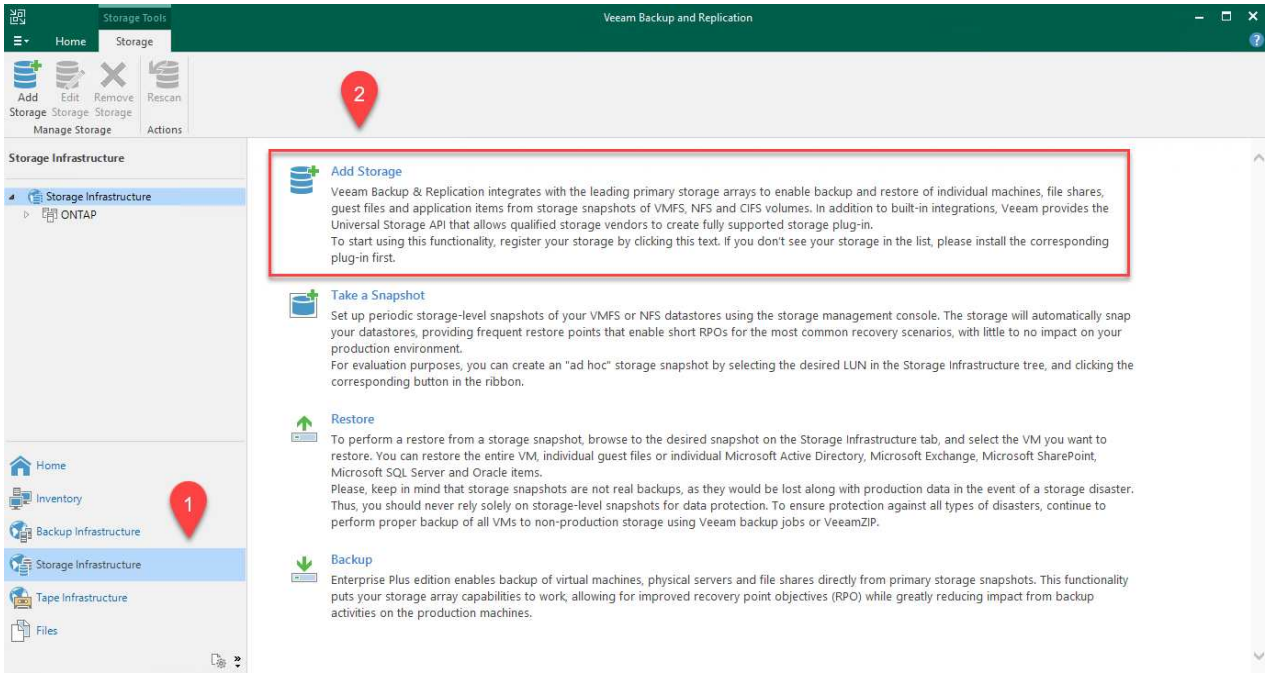
Sehen Sie sich die folgenden Voraussetzungen an, bevor Sie beginnen.

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

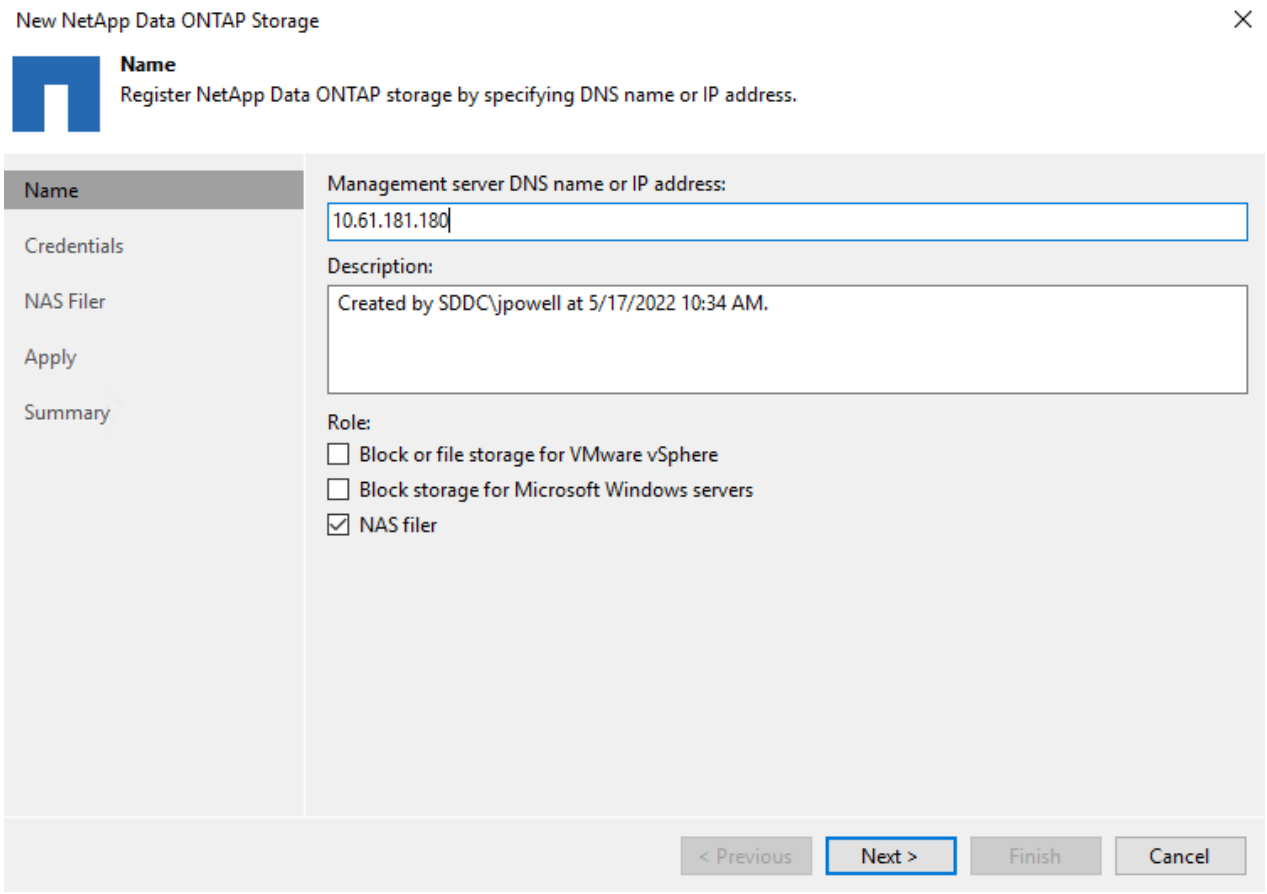
▼ Fügen Sie ONTAP -Speicher zu Veeam hinzu

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

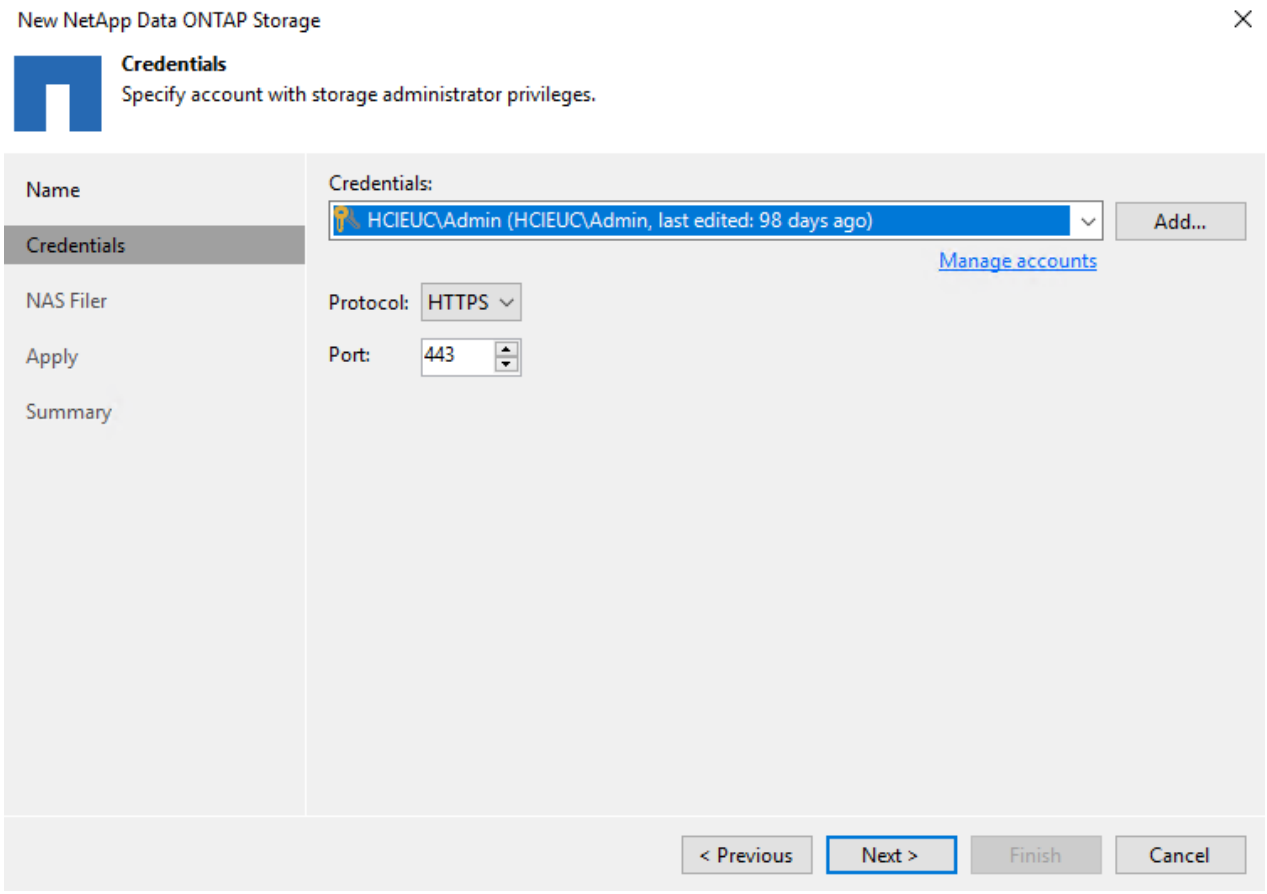
1. Öffnen Sie die Veeam-Konsole und melden Sie sich an. Navigieren Sie zu „Speicherinfrastruktur“ und wählen Sie dann „Speicher hinzufügen“ aus.



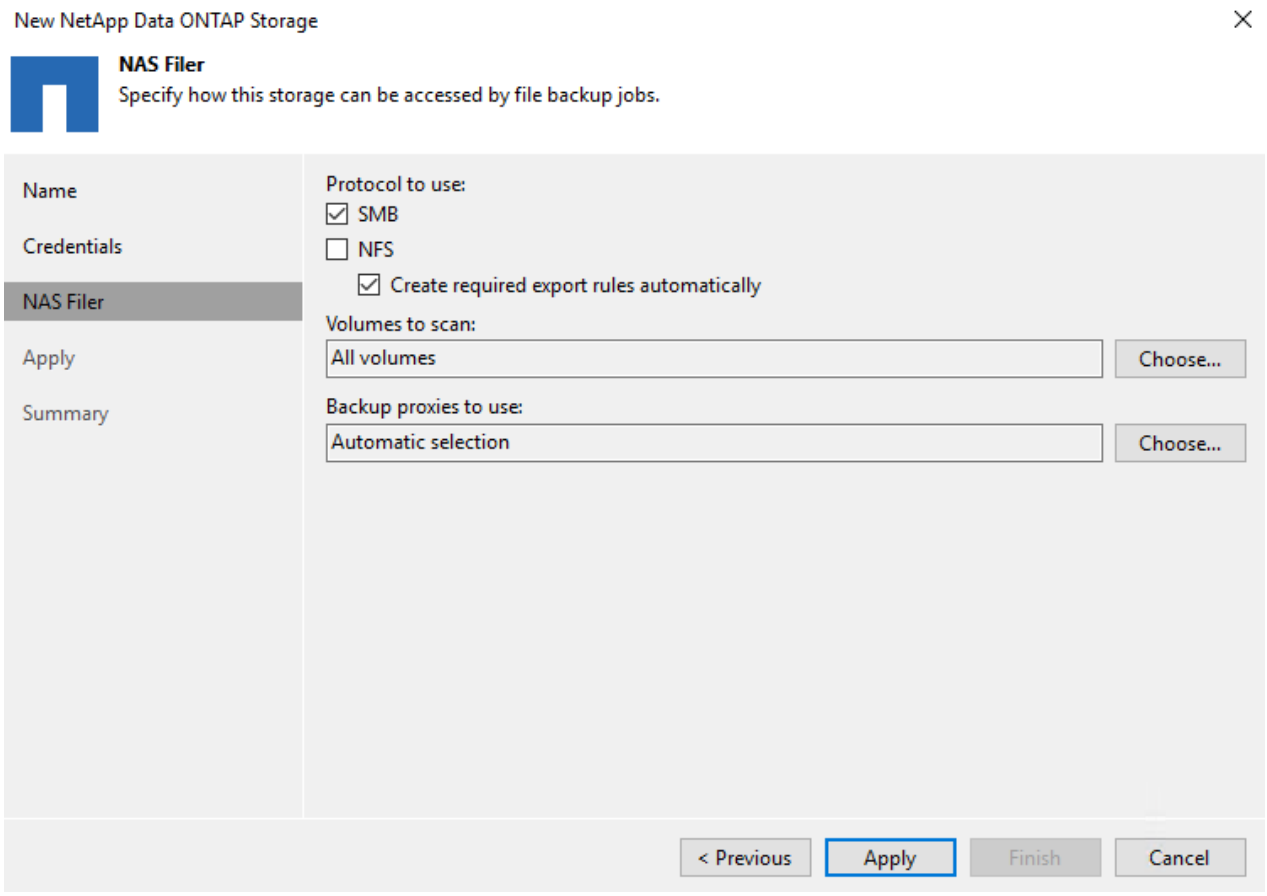
2. Wählen Sie im Assistenten „Speicher hinzufügen“ NetApp als Speicheranbieter und dann Data ONTAP aus.
3. Geben Sie die Verwaltungs-IP-Adresse ein und aktivieren Sie das Kontrollkästchen „NAS-Filer“. Klicken Sie auf Weiter.



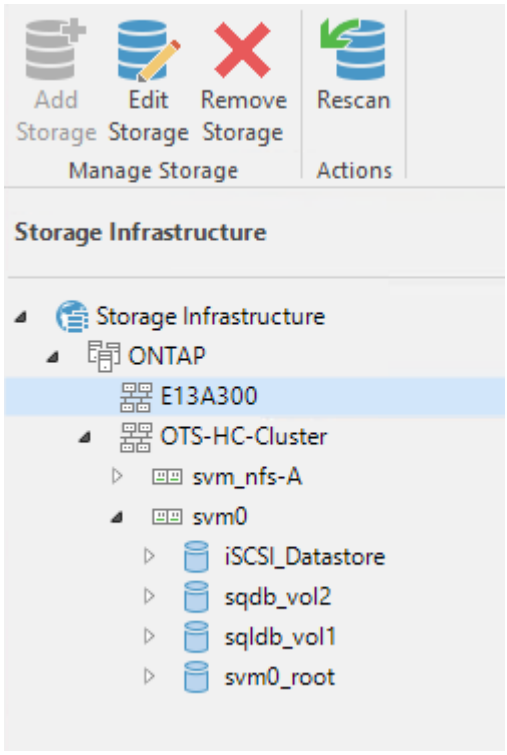
4. Fügen Sie Ihre Anmeldeinformationen hinzu, um auf den ONTAP Cluster zuzugreifen.



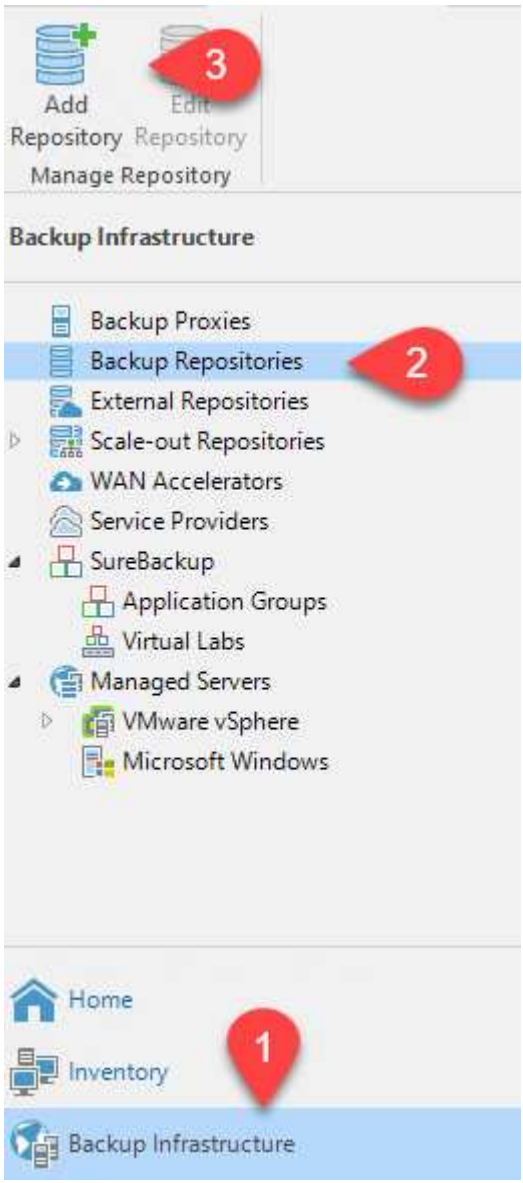
5. Wählen Sie auf der NAS-Filer-Seite die gewünschten Protokolle zum Scannen aus und klicken Sie auf „Weiter“.



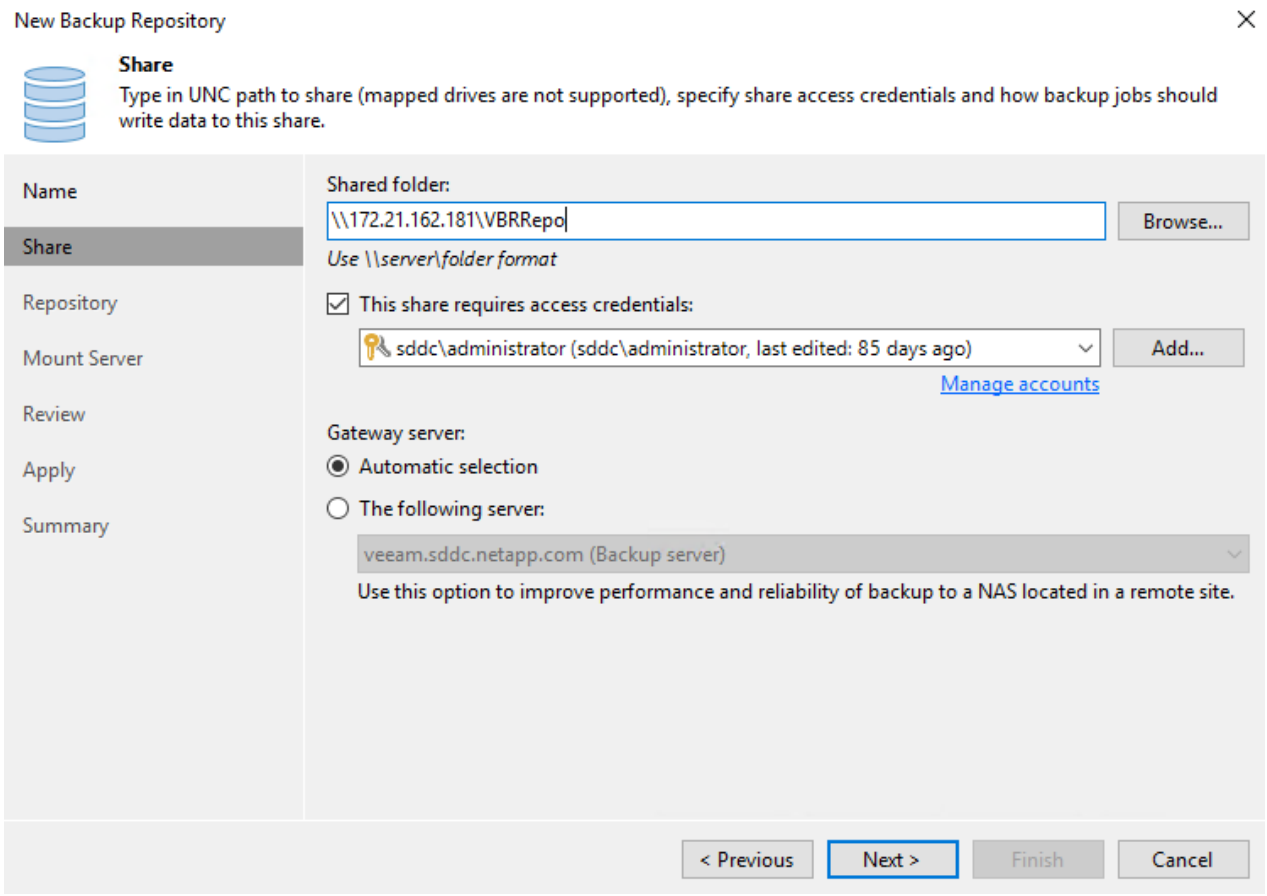
6. Füllen Sie die Seiten „Übernehmen“ und „Zusammenfassung“ des Assistenten aus und klicken Sie auf „Fertig stellen“, um mit der Speichererkennung zu beginnen. Nach Abschluss des Scans wird der ONTAP Cluster zusammen mit den NAS-Filern als verfügbare Ressourcen hinzugefügt.



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



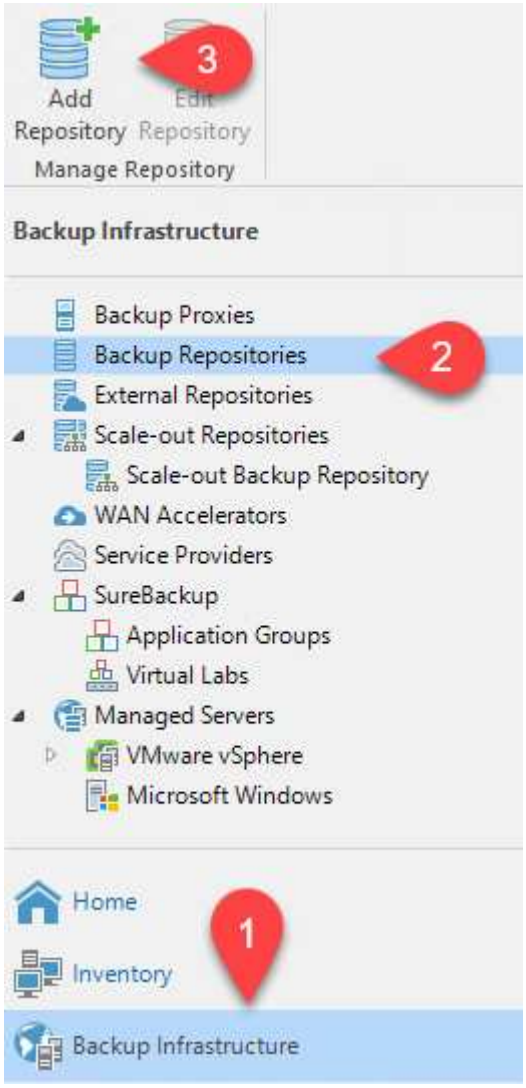
8. Befolgen Sie alle Schritte im Assistenten „Neues Sicherungsrepository“, um das Repository zu erstellen. Ausführliche Informationen zum Erstellen von Veeam Backup Repositories finden Sie im "Veeam-Dokumentation" .



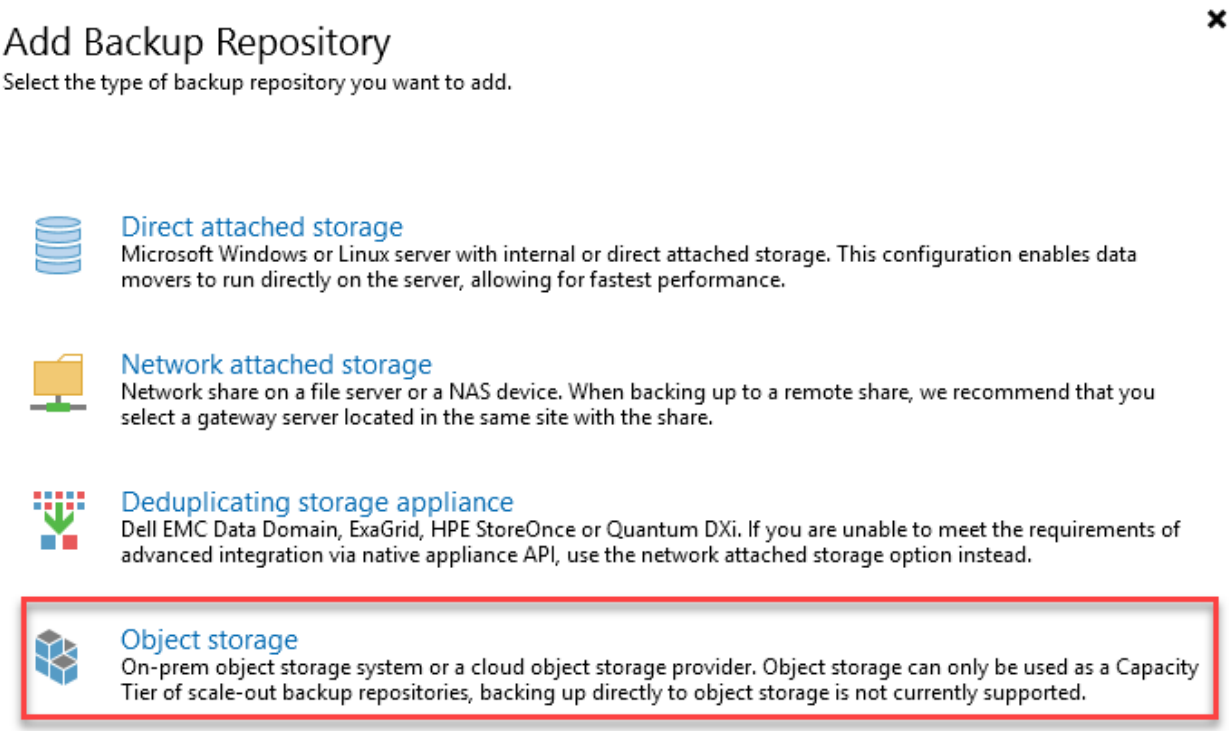
▼ **Fügen Sie den Amazon S3-Bucket als Backup-Repository hinzu**

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

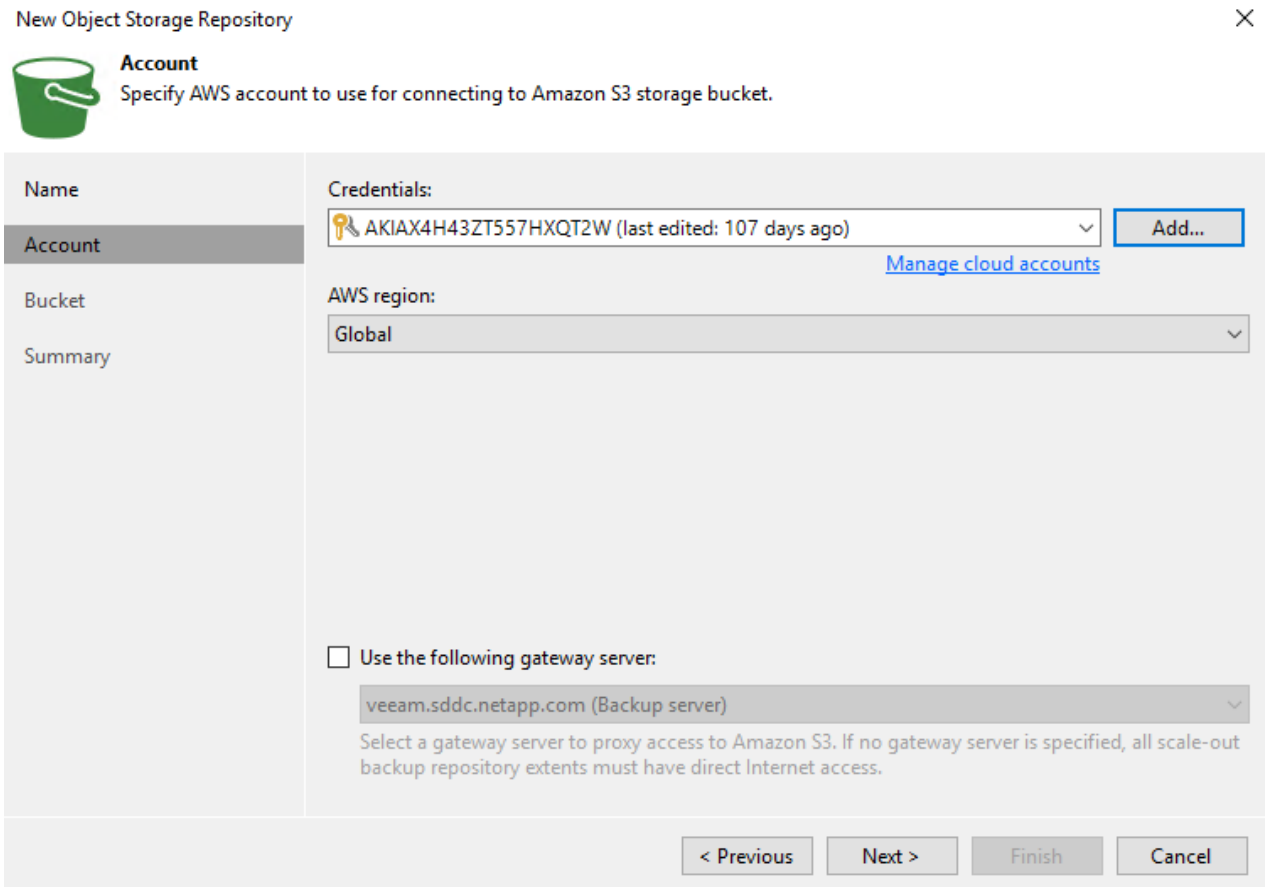
1. Navigieren Sie zu Backup-Infrastruktur > Backup-Repositorys. Klicken Sie auf Repository hinzufügen.



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



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

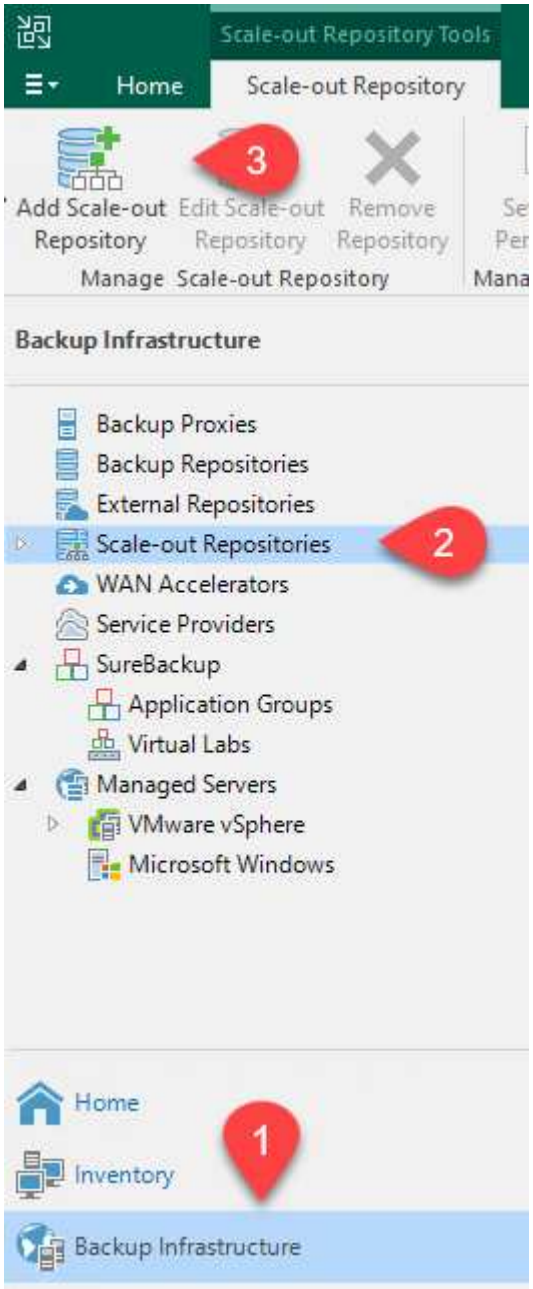


5. Nachdem die Amazon-Konfiguration geladen wurde, wählen Sie Ihr Rechenzentrum, Ihren Bucket und Ihren Ordner aus und klicken Sie auf „Übernehmen“. Klicken Sie abschließend auf „Fertig stellen“, um den Assistenten zu schließen.

▼ **Erstellen eines Scale-Out-Sicherungsrepositorys**

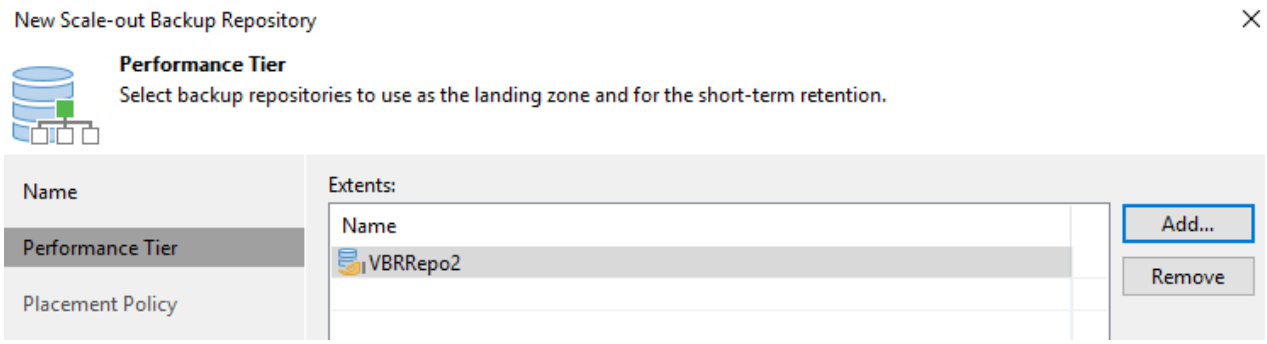
Nachdem wir nun unsere Speicher-Repositories zu Veeam hinzugefügt haben, können wir den SOBR erstellen, um Sicherungskopien zur Notfallwiederherstellung automatisch in unseren externen Amazon S3-Objektspeicher zu verschieben.

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

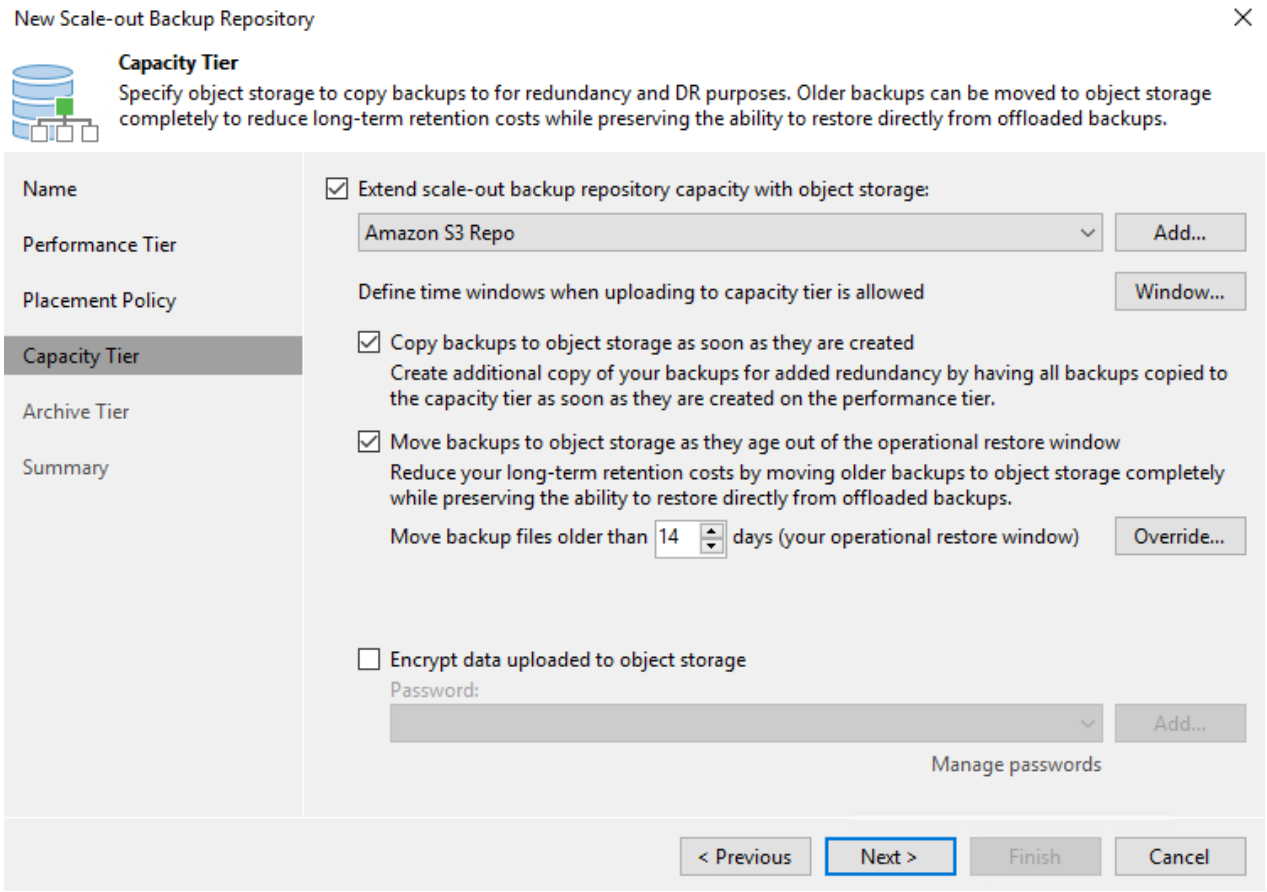


2. Geben Sie im neuen Scale-Out-Backup-Repository einen Namen für das SOBR ein und klicken Sie auf „Weiter“.
3. Wählen Sie für die Leistungsstufe das Sicherungsrepository aus, das die SMB-Freigabe enthält, die

sich auf Ihrem lokalen ONTAP Cluster befindet.



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



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

▼ Erstellen der Scale-Out-Backup-Repository-Jobs

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

Help Center Technische Dokumentation" .

NetApp Backup und Recovery Tools und Konfiguration

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

▼ **Bereitstellen eines sekundären Windows SnapCenter -Servers**

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

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

Sie finden die SnapCenter software unter "dieser Link" .

▼ **Konfigurieren des sekundären Windows SnapCenter -Servers**

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

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

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

▼ **Bereitstellen eines sekundären Veeam Backup & Replication-Servers**

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

▼ **Konfigurieren Sie den sekundären Veeam Backup & Replication-Server**

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

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

1. Konfigurieren Sie das Netzwerk für die Kommunikation mit VMware Cloud, FSx ONTAP und dem S3-

Bucket, das das ursprüngliche Sicherungsrepository enthält.

2. Konfigurieren Sie eine SMB-Freigabe auf FSx ONTAP als neues Backup-Repository.
3. Mounten Sie den ursprünglichen S3-Bucket, der als Teil des Scale-Out-Backup-Repositorys vor Ort verwendet wurde.
4. Richten Sie nach der Wiederherstellung der VM neue Sicherungsaufträge ein, um SQL- und Oracle-VMs zu schützen.

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

SnapCenter -Datenbanksicherung für die Notfallwiederherstellung

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

▼ **Voraussetzungen für SnapCenter -Backups**

Für die SnapCenter Sicherung sind die folgenden Voraussetzungen erforderlich:

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

▼ **Zusammenfassung des SnapCenter -Sicherungs- und Wiederherstellungsprozesses**

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

▼ **Sichern Sie die SnapCenter -Datenbank und -Konfiguration**

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

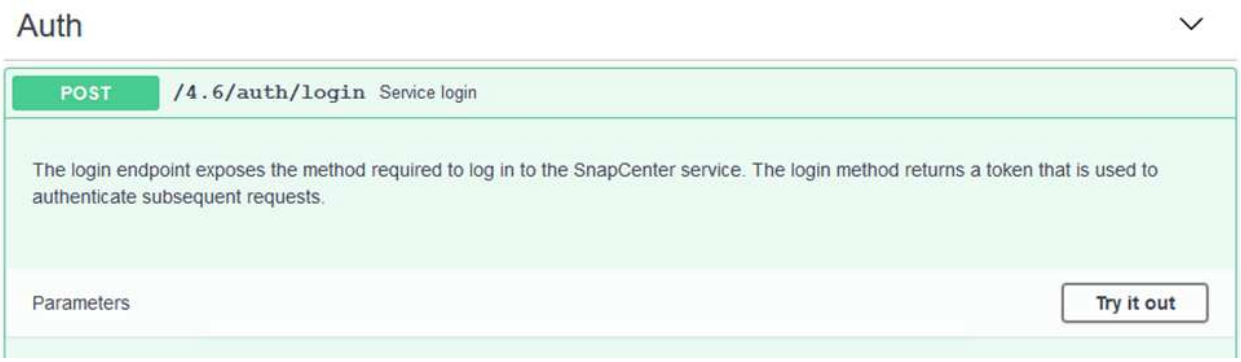
▼ **Melden Sie sich bei Swagger an und erhalten Sie ein Autorisierungstoken**

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

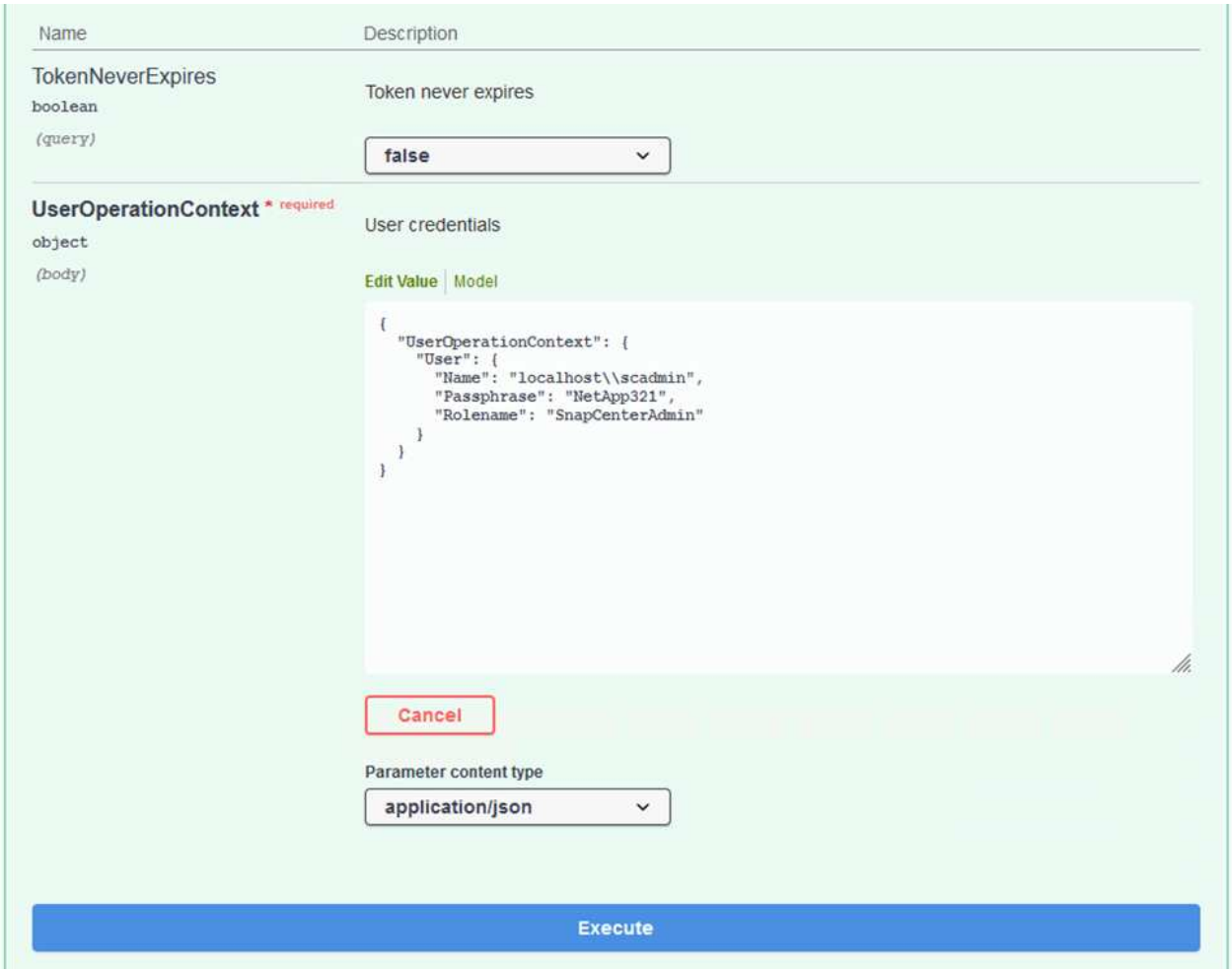
1. Greifen Sie auf die SnapCenter Swagger API-Webseite unter *https://< SnapCenter Server IP>:8146/swagger/* zu.



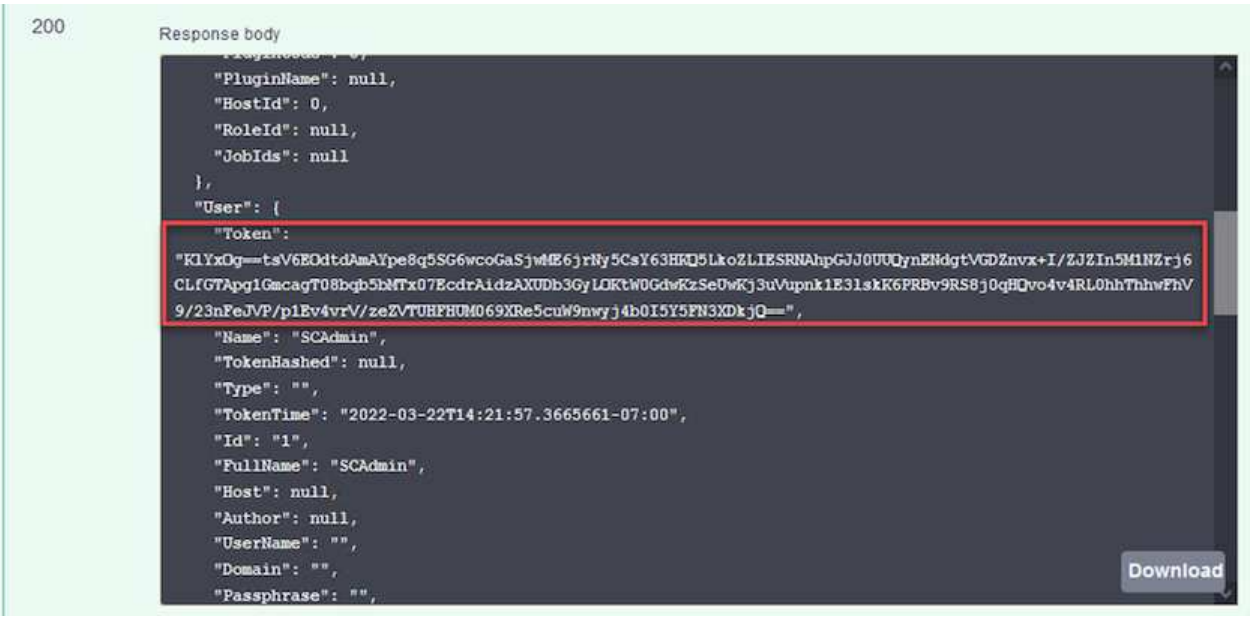
2. Erweitern Sie den Abschnitt „Auth“ und klicken Sie auf „Ausprobieren“.



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



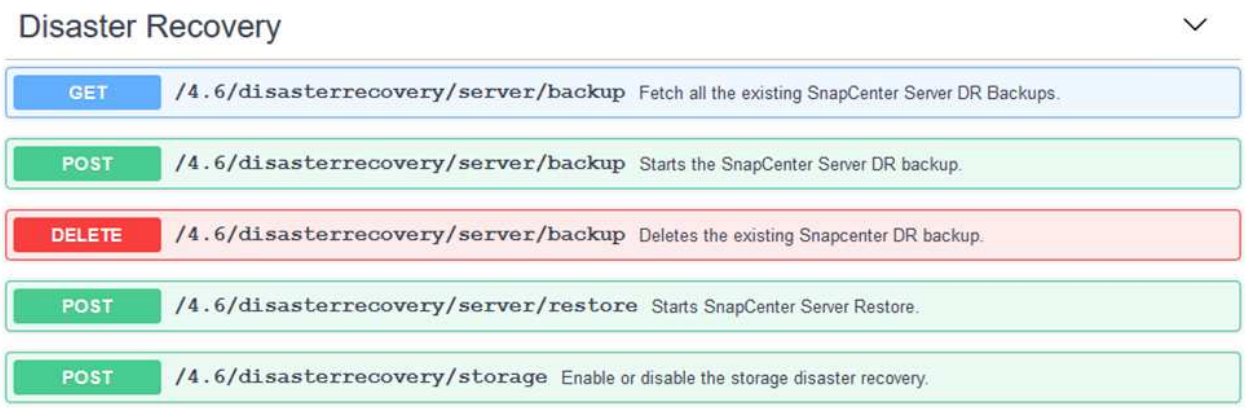
4. Im Antworttext unten können Sie das Token sehen. Kopieren Sie den Token-Text zur Authentifizierung beim Ausführen des Sicherungsvorgangs.



▼ **Führen Sie eine SnapCenter -Datenbanksicherung durch**

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

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

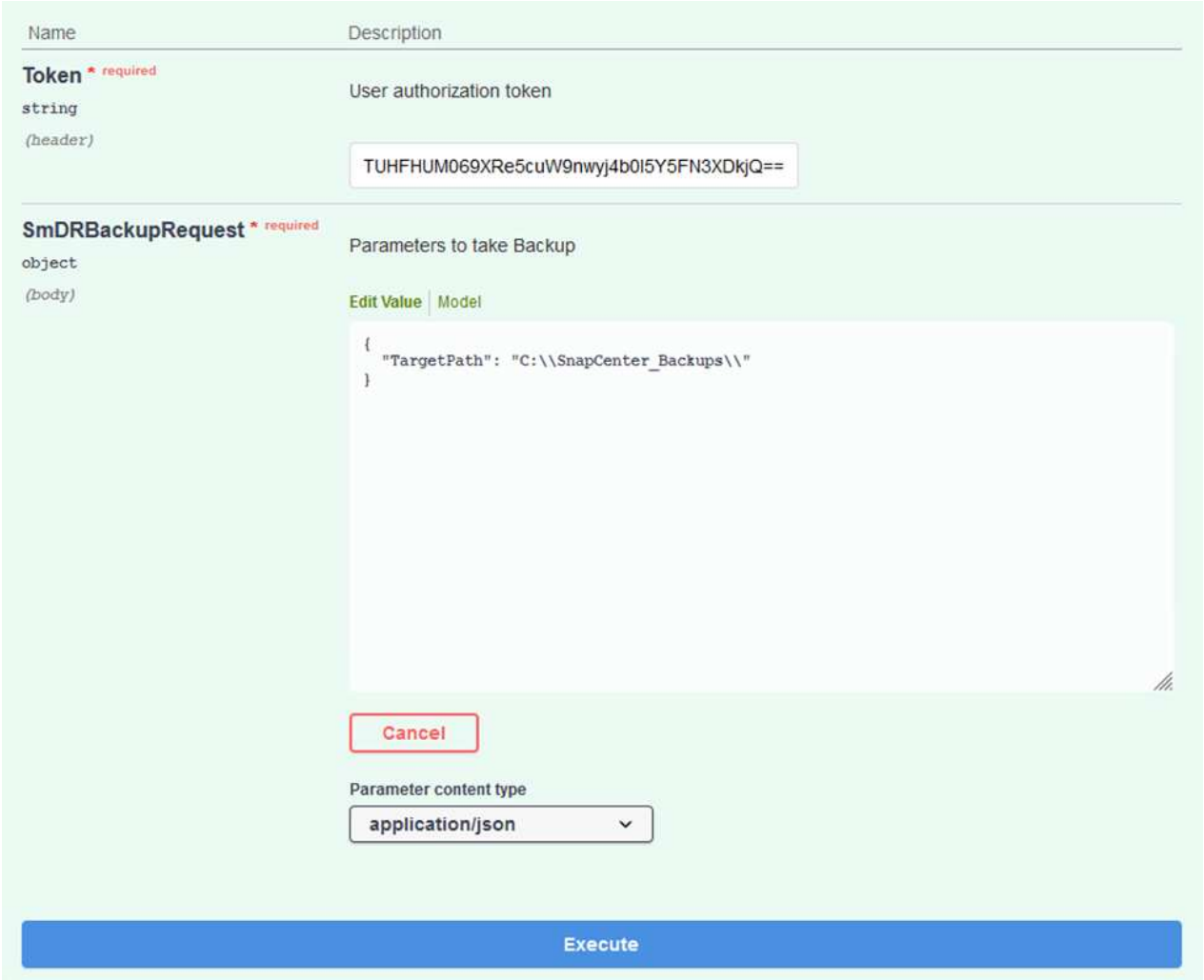


2. Erweitern Sie die `/4.6/disasterrecovery/server/backup` und klicken Sie auf „Ausprobieren“.



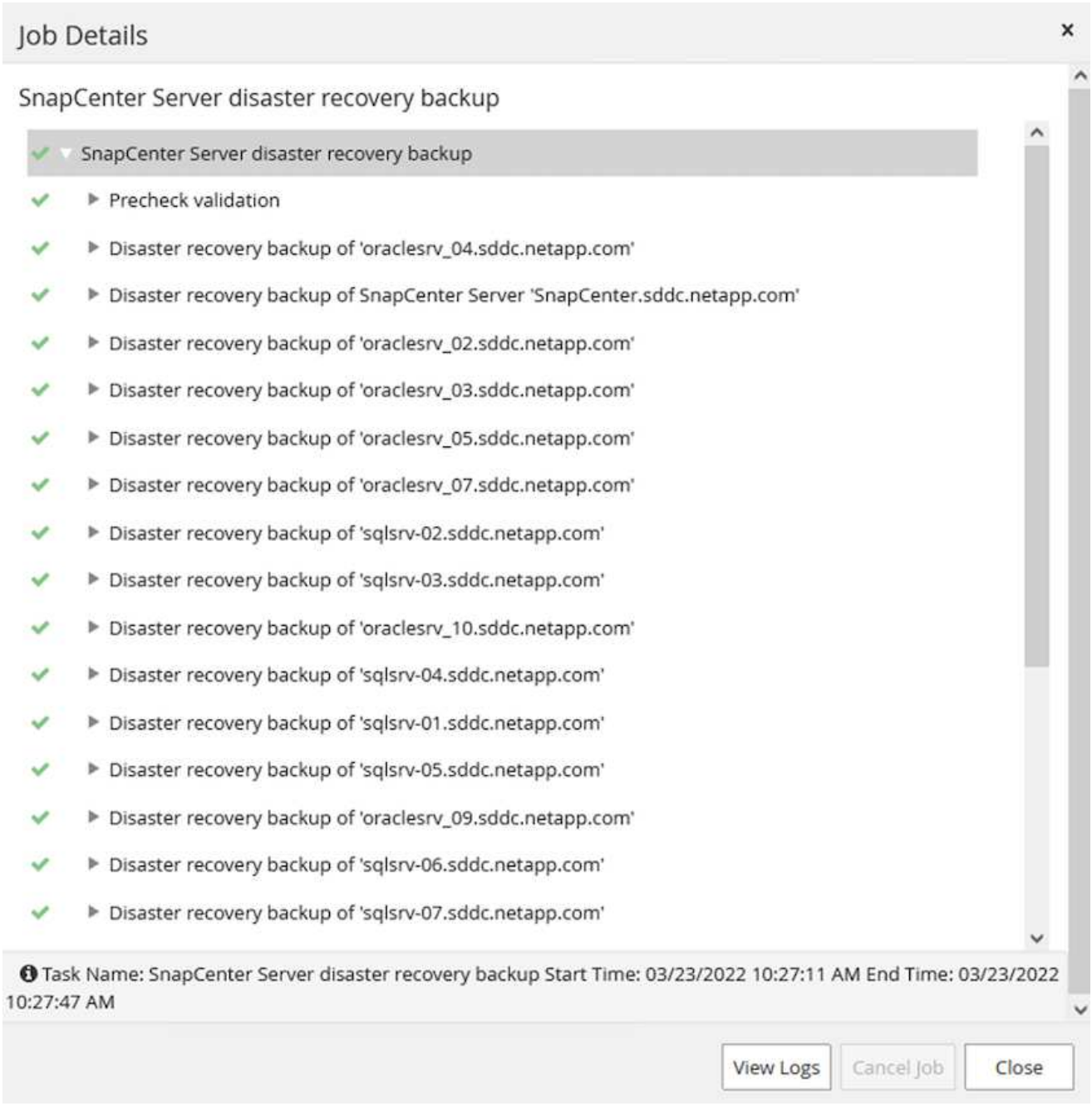
3. Fügen Sie im Abschnitt „SmDRBackupRequest“ den richtigen lokalen Zielpfad hinzu und wählen Sie „Ausführen“, um die Sicherung der SnapCenter -Datenbank und -Konfiguration zu starten.

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



▼ **Überwachen Sie den Sicherungsauftrag von SnapCenter**

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



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

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

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

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

```
/E /H /K
```

Ausfallsicherung

▼ Katastrophe am Primärstandort

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

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

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

▼ SnapCenter -Datenbankwiederherstellungsprozess

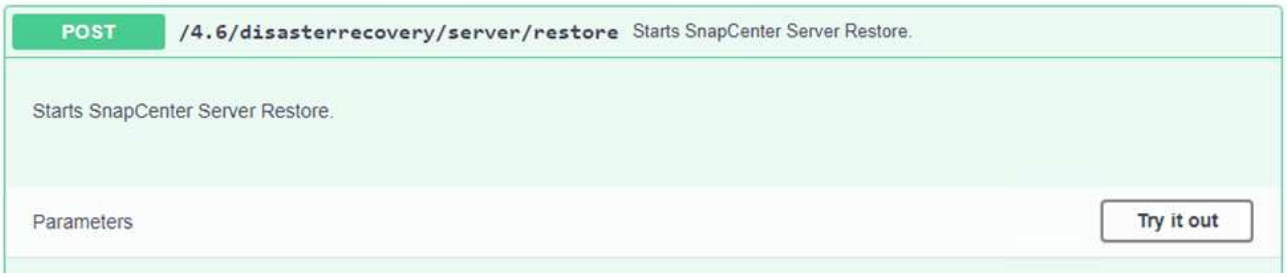
SnapCenter unterstützt Notfallwiederherstellungsszenarien, indem es die Sicherung und Wiederherstellung seiner MySQL-Datenbank und Konfigurationsdateien ermöglicht. Auf diese Weise kann ein Administrator regelmäßige Sicherungen der SnapCenter -Datenbank im lokalen Rechenzentrum durchführen und diese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

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

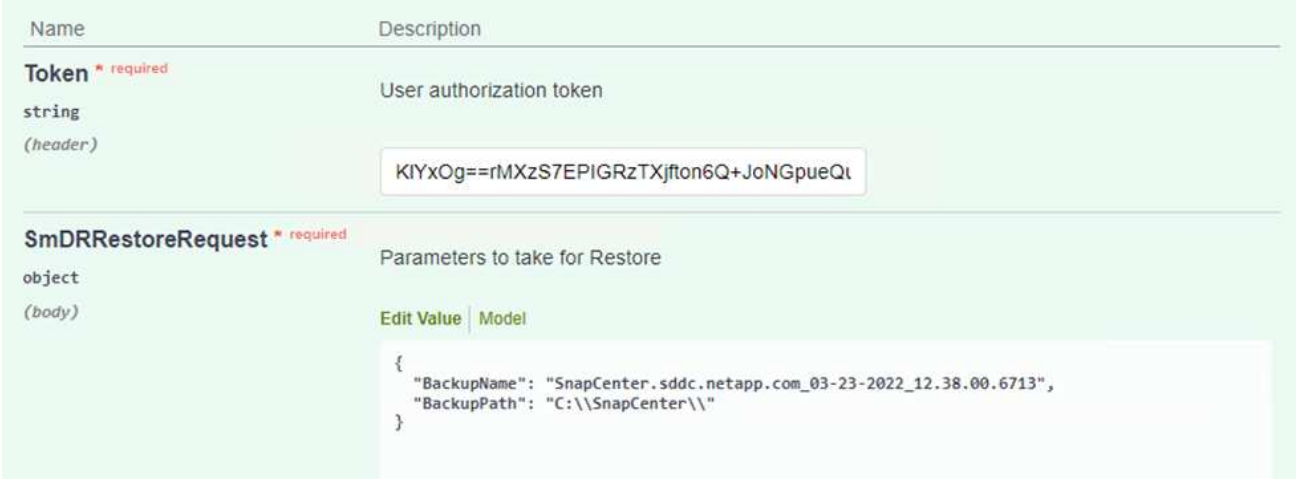
1. Unterbrechen Sie die SnapMirror -Beziehung zum FSx-Cluster, wodurch das Volume Lese-/Schreibzugriff erhält.
2. Erstellen Sie einen CIFS-Server (falls erforderlich) und erstellen Sie eine CIFS-Freigabe, die auf den Verbindungspfad des geklonten Volumes verweist.
3. Verwenden Sie xcopy, um die Sicherungsdateien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

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

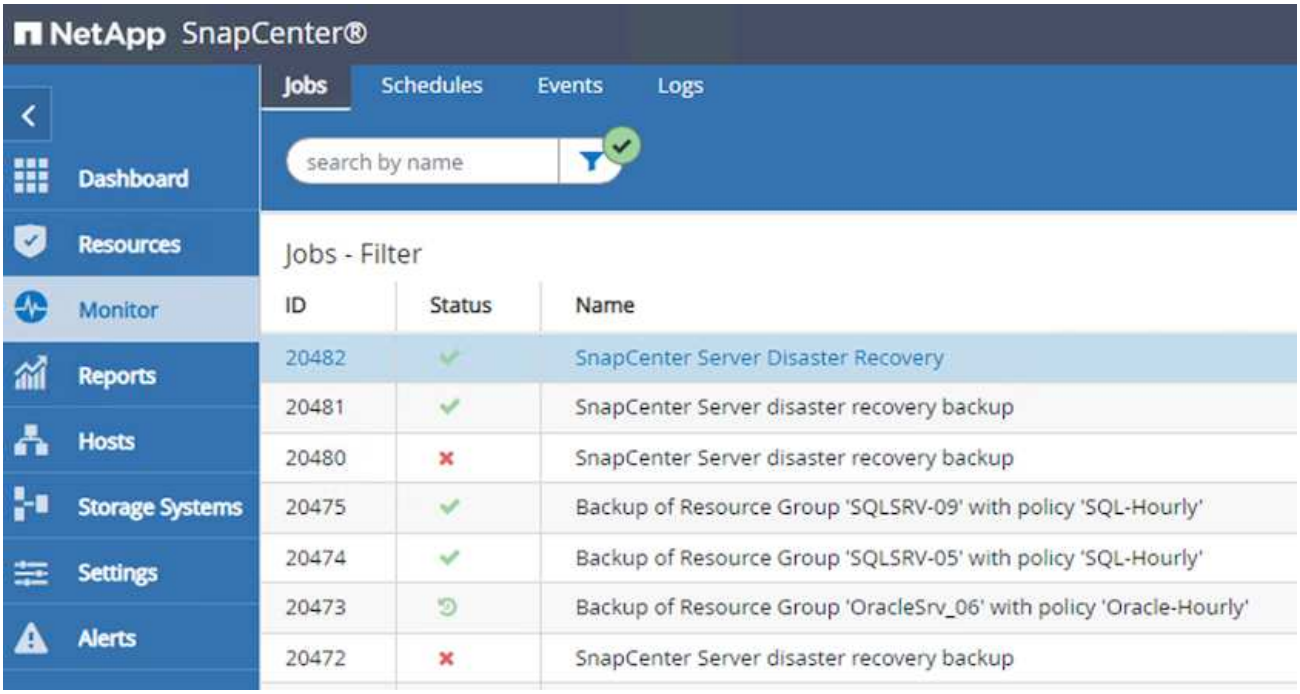
1. Navigieren Sie zur Swagger-API-Webseite für den sekundären SnapCenter Server und befolgen Sie die vorherigen Anweisungen, um ein Autorisierungstoken zu erhalten.
2. Navigieren Sie zum Abschnitt Disaster Recovery der Swagger-Seite, wählen Sie `/4.6/disasterrecovery/server/restore` und klicken Sie auf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

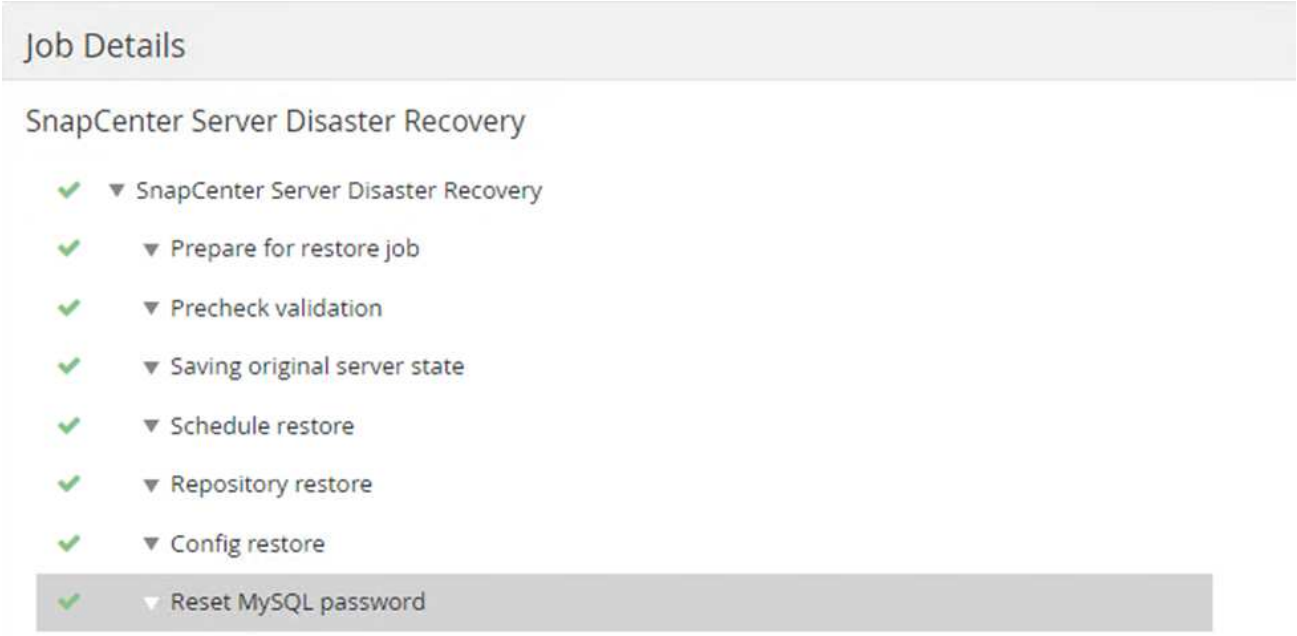


3. Fügen Sie Ihr Autorisierungstoken ein und fügen Sie im Abschnitt „SmDRResterRequest“ den Namen des Backups und des lokalen Verzeichnisses auf dem sekundären SnapCenter -Server ein.



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





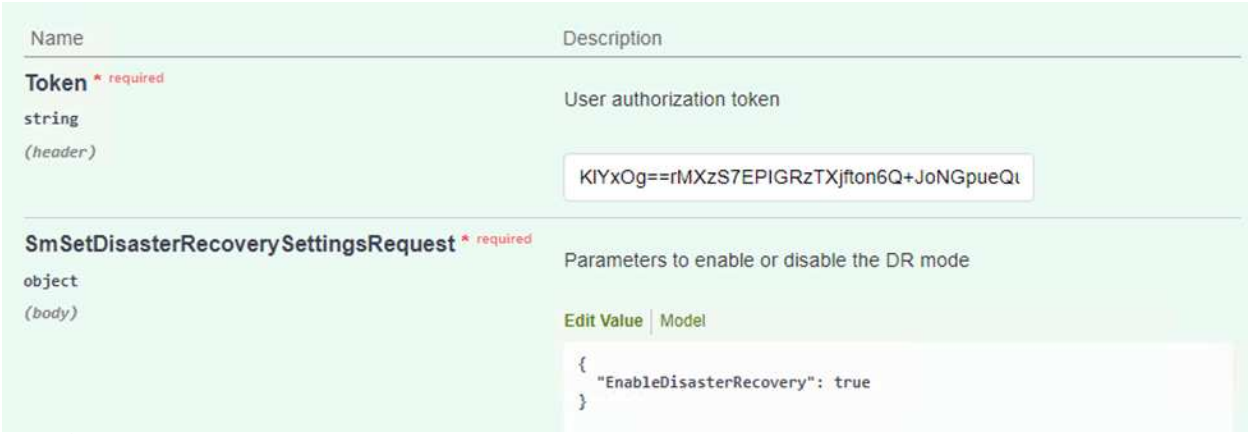
6. Um SQL Server-Wiederherstellungen vom sekundären Speicher zu aktivieren, müssen Sie die SnapCenter Datenbank in den Disaster Recovery-Modus schalten. Dies wird als separater Vorgang durchgeführt und auf der Swagger-API-Webseite initiiert.

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

   b. Fügen Sie das Benutzerautorisierungstoken ein.

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

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



Siehe Kommentare zu zusätzlichen Verfahren.

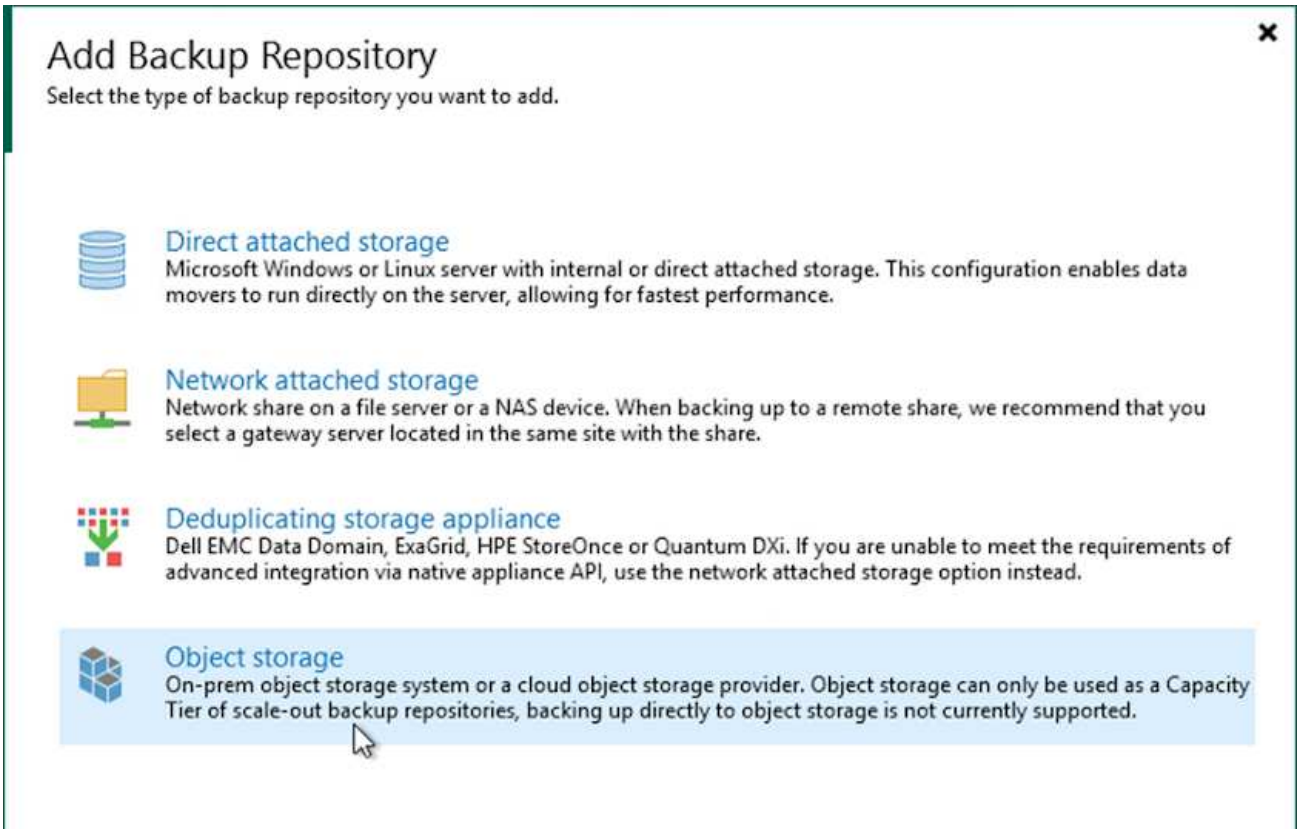
Wiederherstellen von Anwendungs-VMs mit der vollständigen Wiederherstellung von Veeam

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

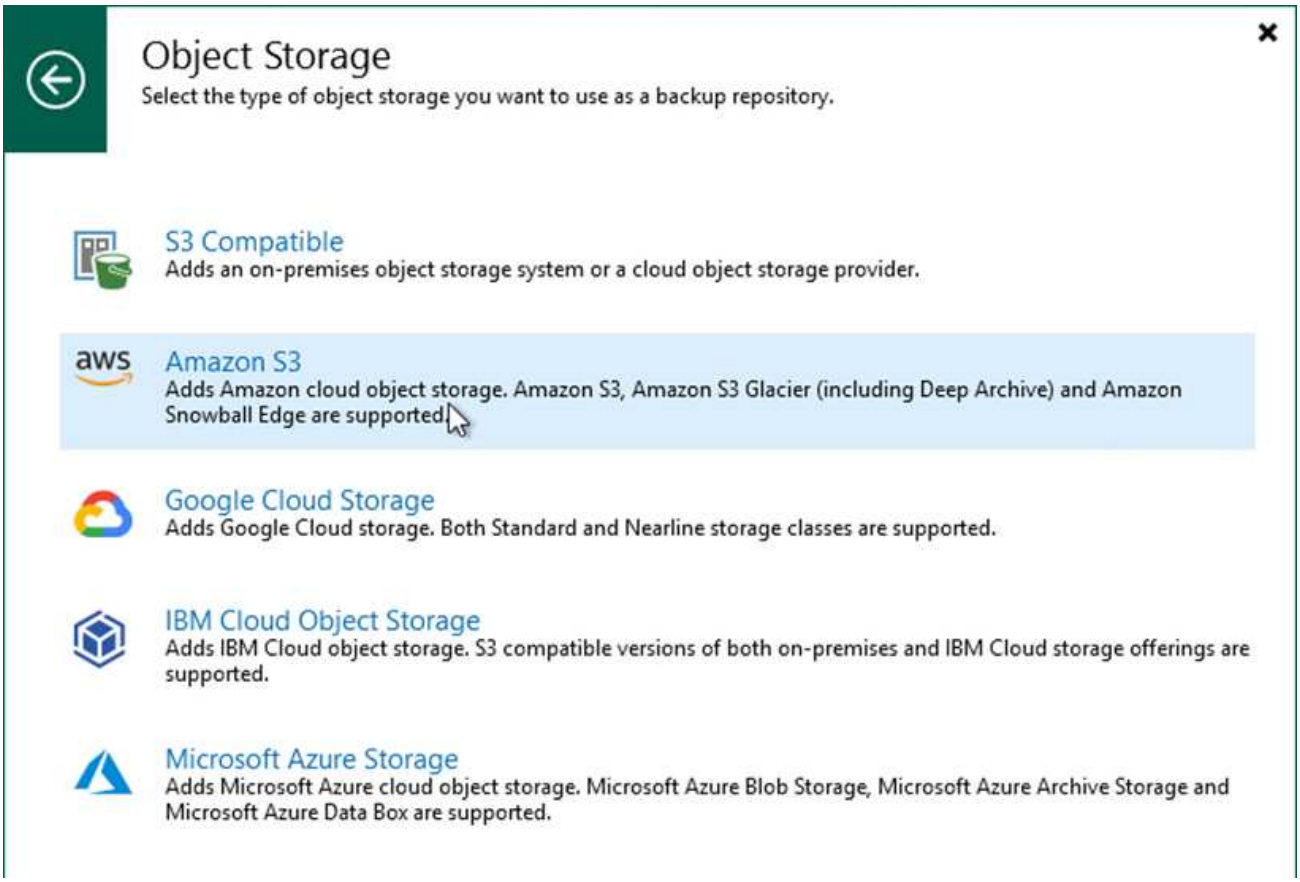
Importieren Sie vom sekundären Veeam-Server die Sicherungen aus dem S3-Speicher und stellen Sie die SQL Server- und Oracle-VMs in Ihrem VMware Cloud-Cluster wieder her.

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

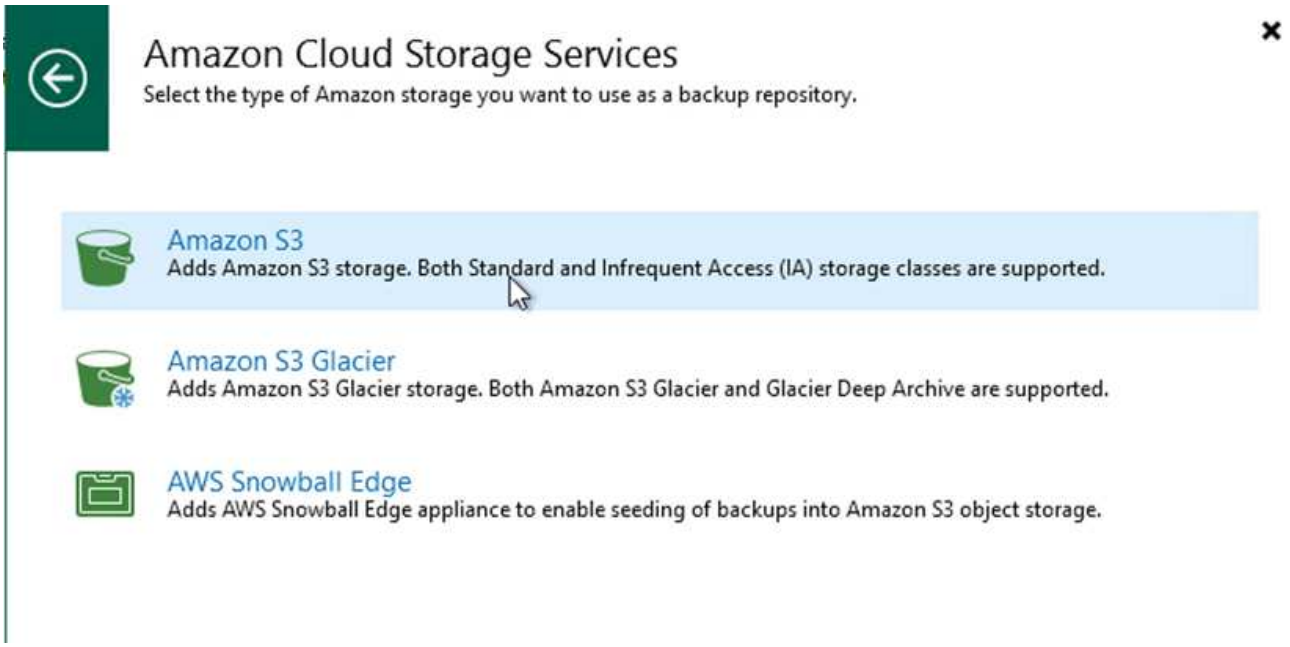
1. Gehen Sie zu „Backup-Repositorys“ und klicken Sie im oberen Menü auf „Repository hinzufügen“, um den Assistenten „Backup-Repository hinzufügen“ zu starten. Wählen Sie auf der ersten Seite des Assistenten „Object Storage“ als Sicherungsrepository-Typ aus.



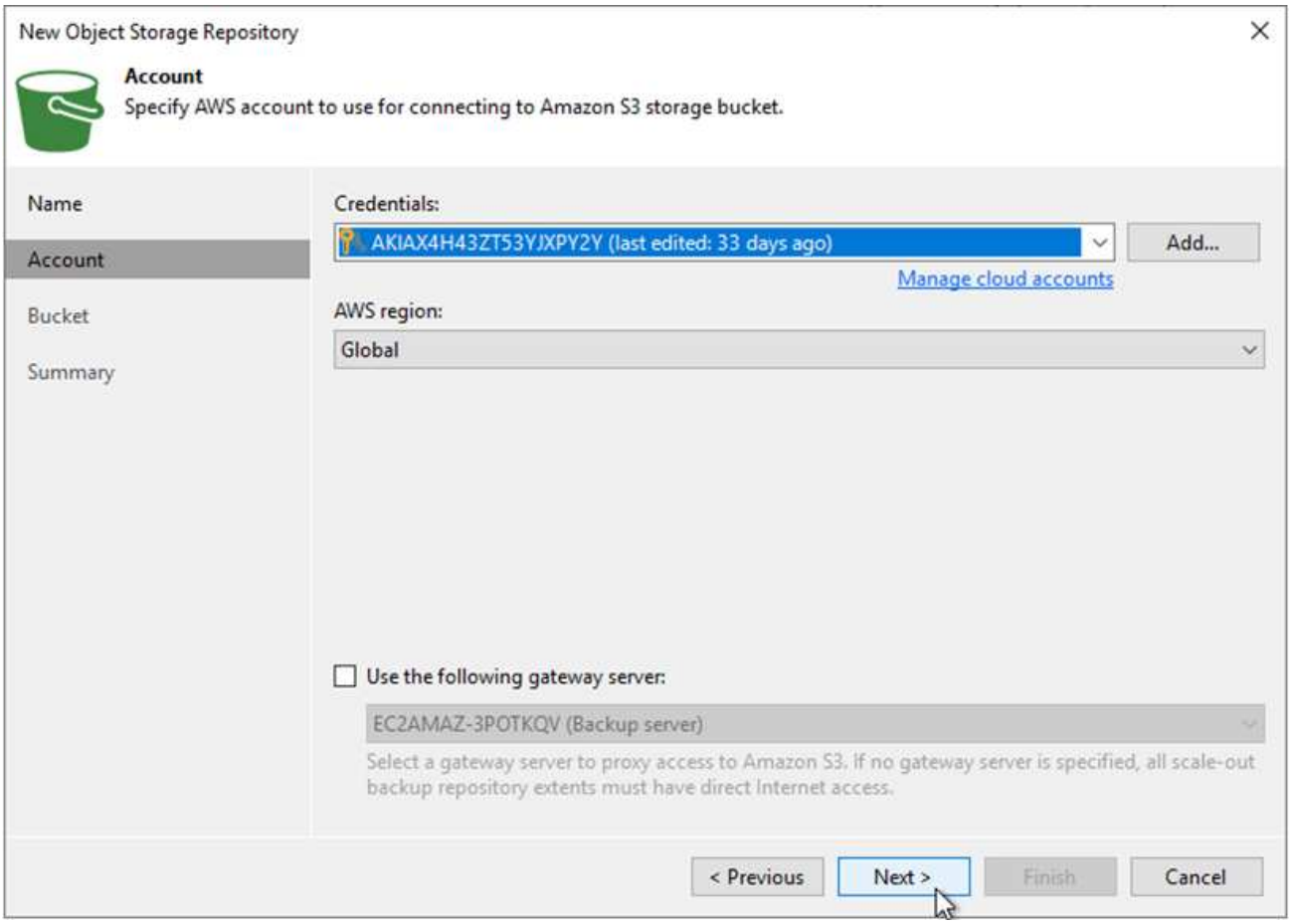
2. Wählen Sie Amazon S3 als Objektspeichertyp aus.



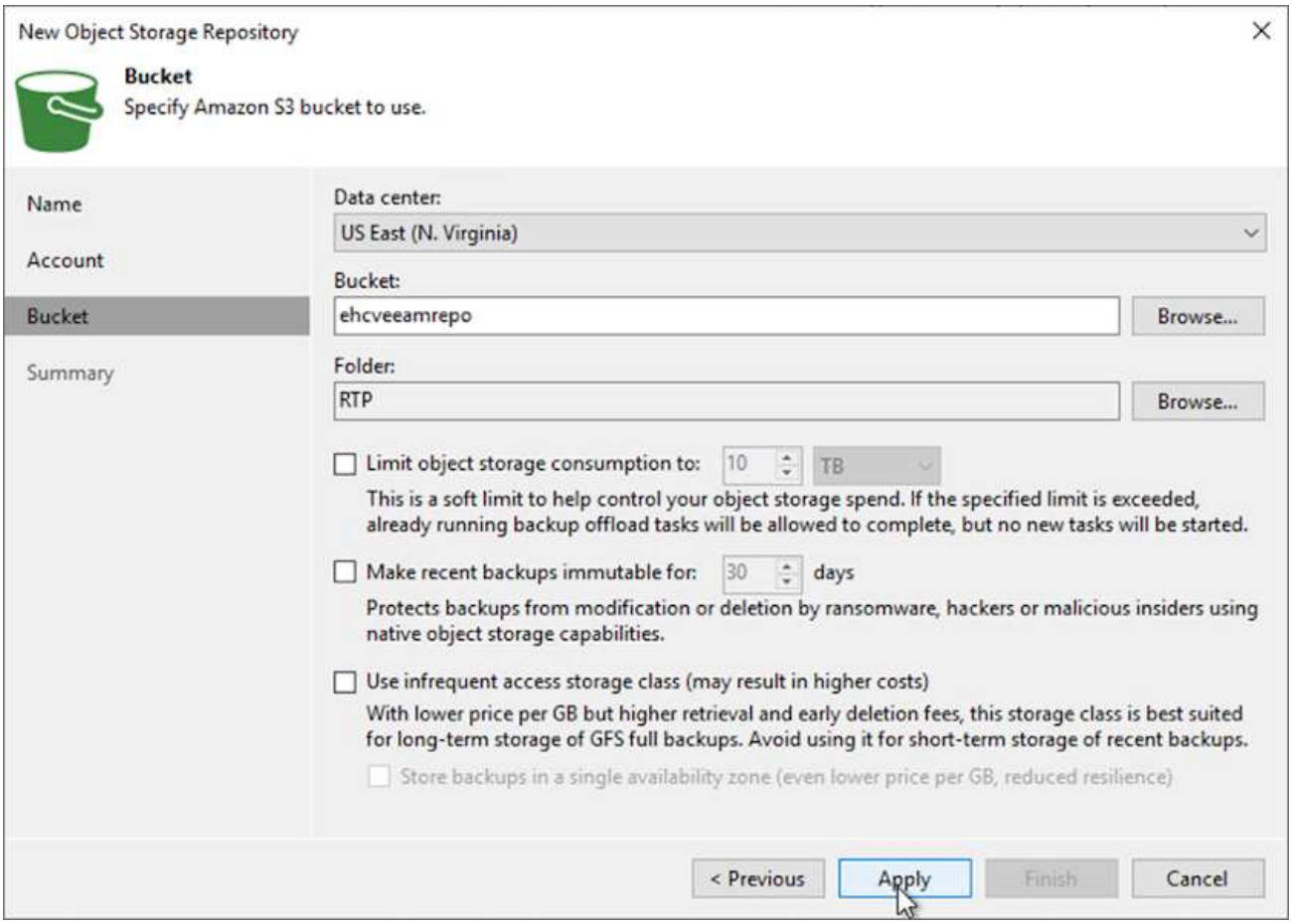
3. Wählen Sie aus der Liste der Amazon Cloud Storage Services Amazon S3 aus.



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



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

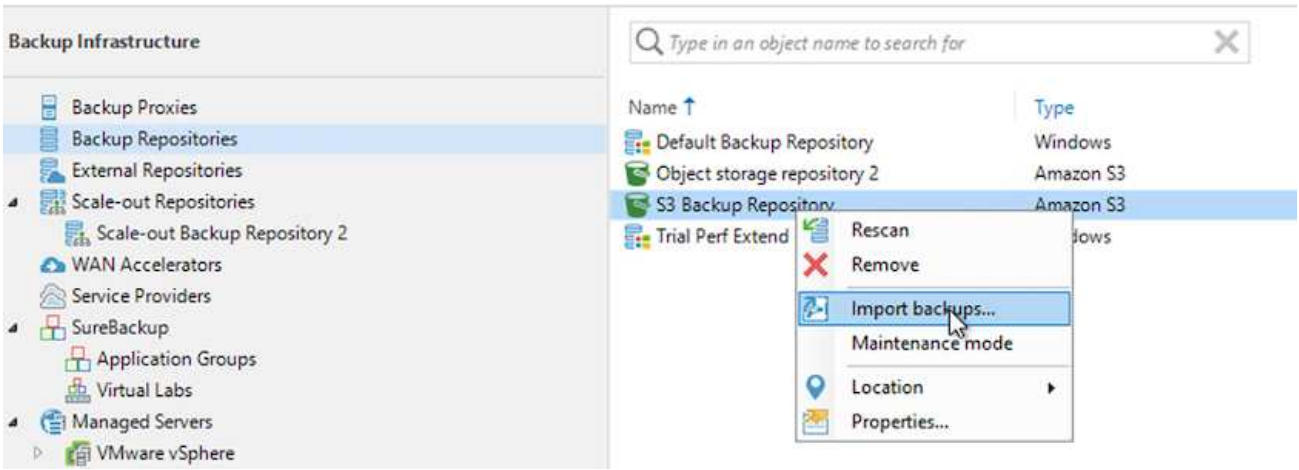


6. Wählen Sie abschließend „Fertig stellen“, um den Vorgang abzuschließen und das Repository hinzuzufügen.

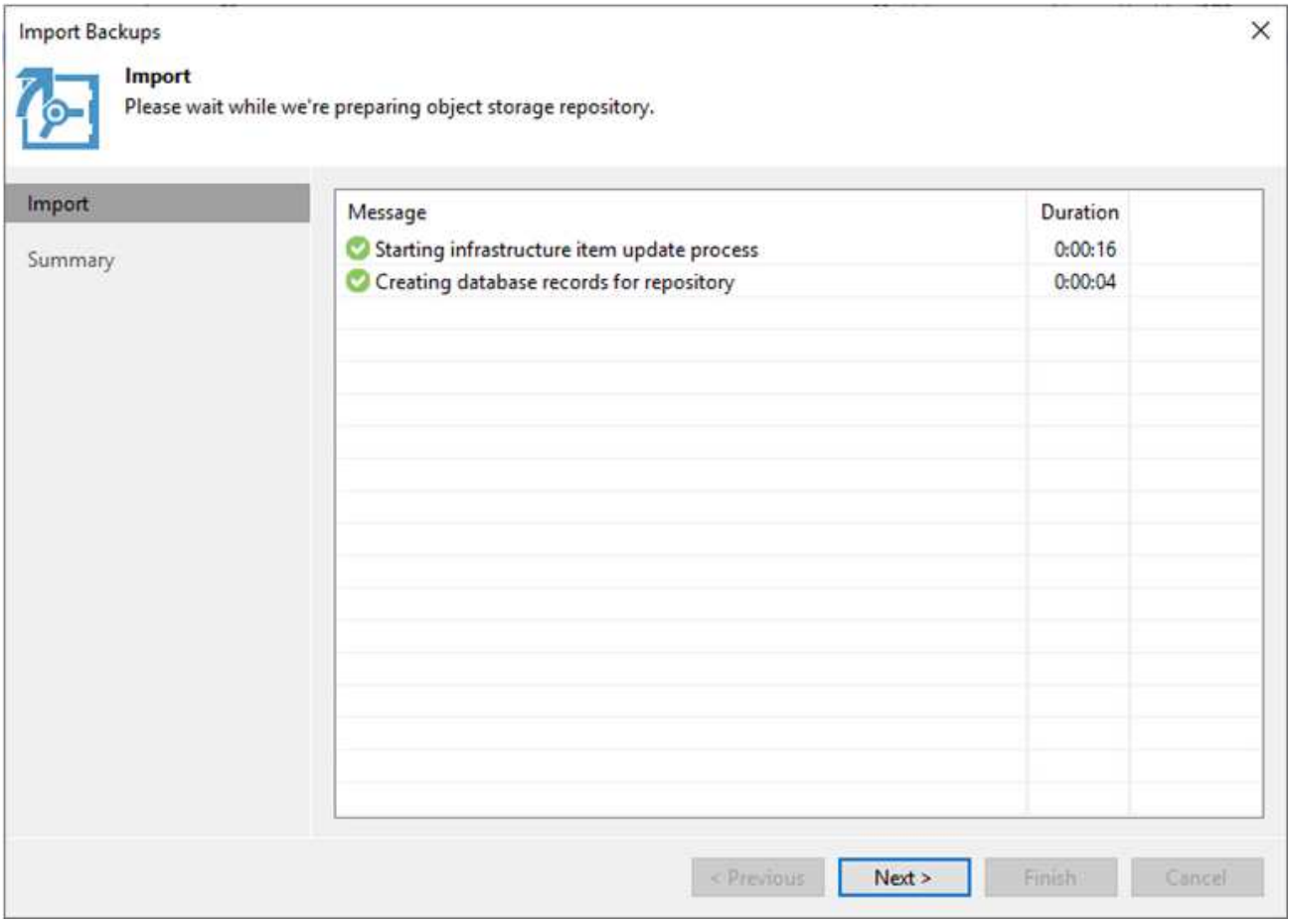
▼ Importieren von Backups aus dem S3-Objektspeicher

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

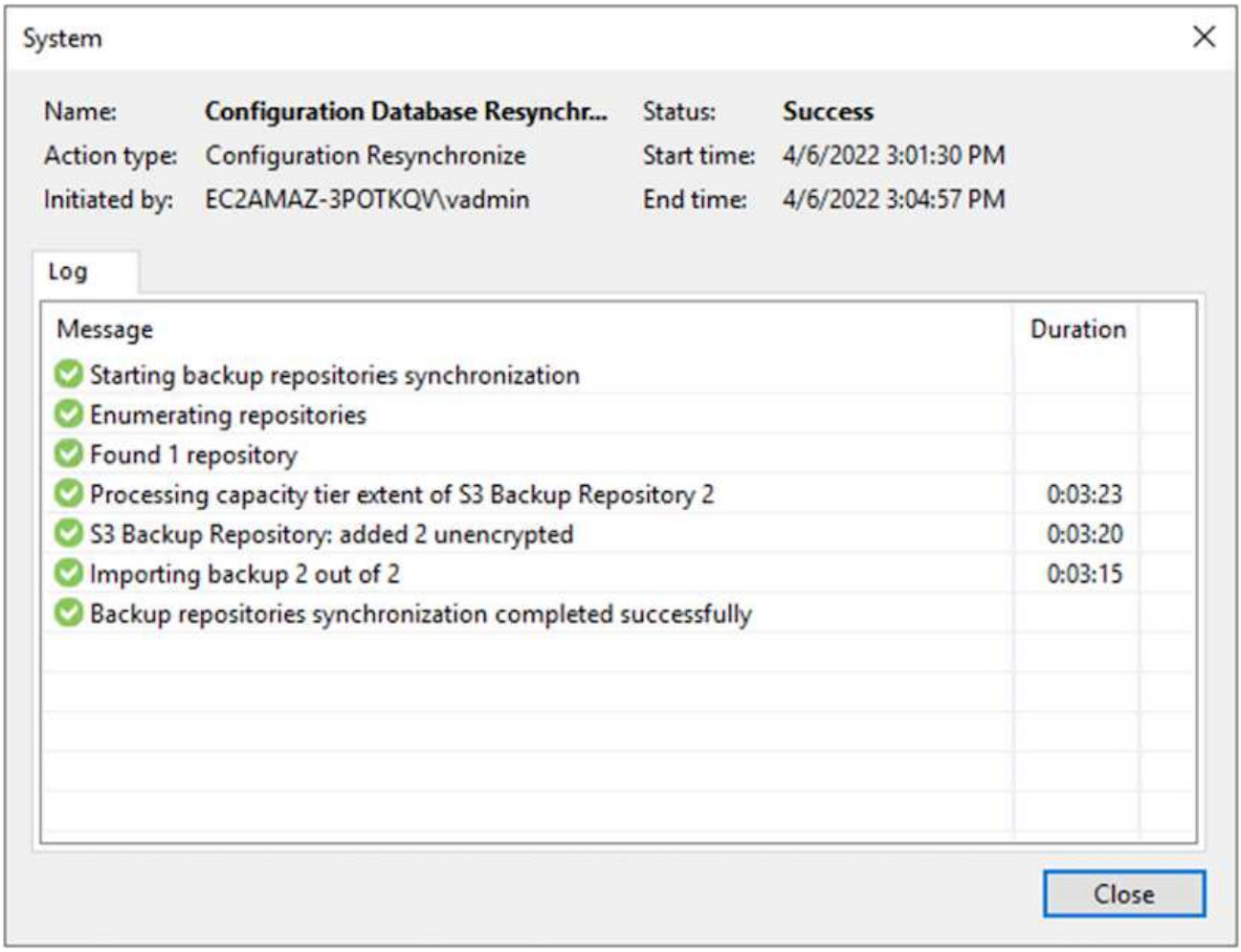
1. Wählen Sie im S3-Sicherungsrepository „Sicherungen importieren“ aus, um den Assistenten „Sicherungen importieren“ zu starten.



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



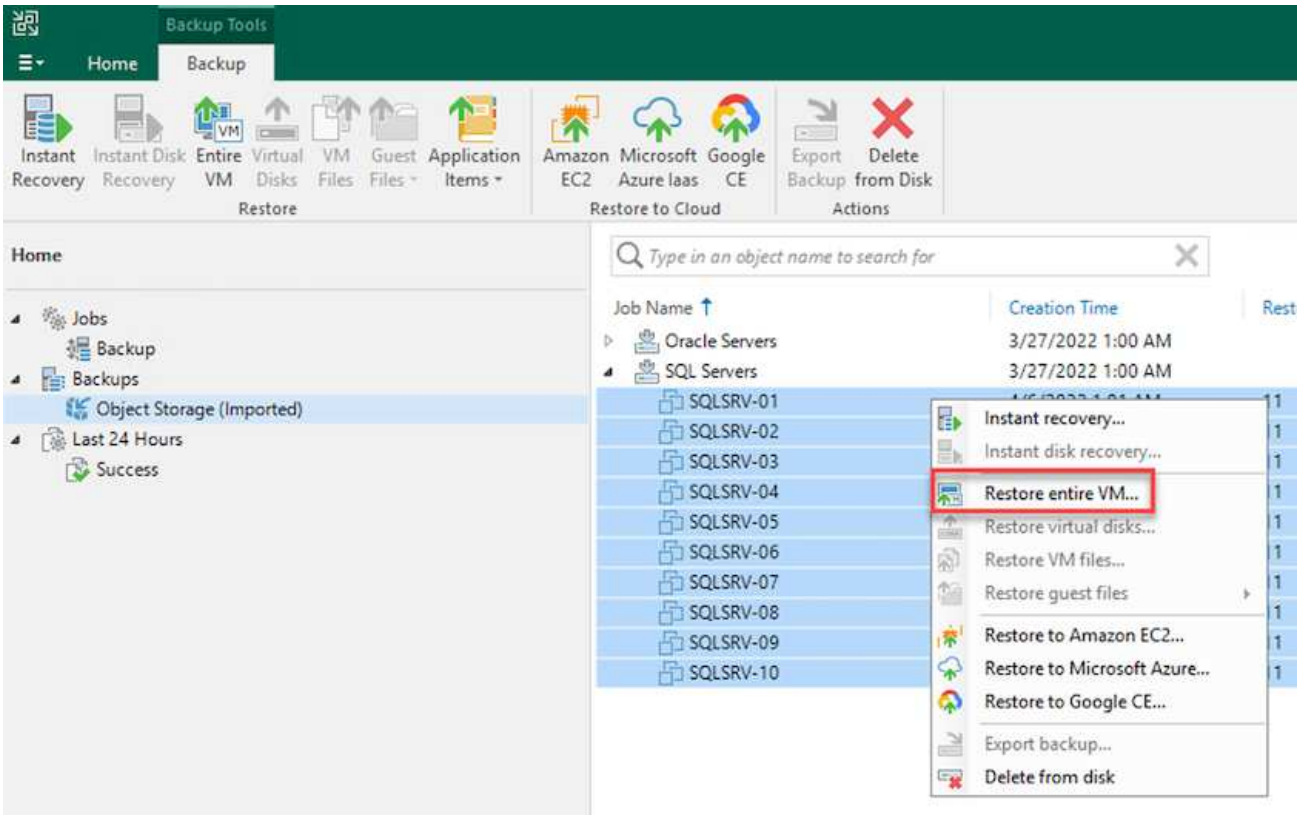
3. Nachdem der Import abgeschlossen ist, können Sie VMs im VMware Cloud-Cluster wiederherstellen.



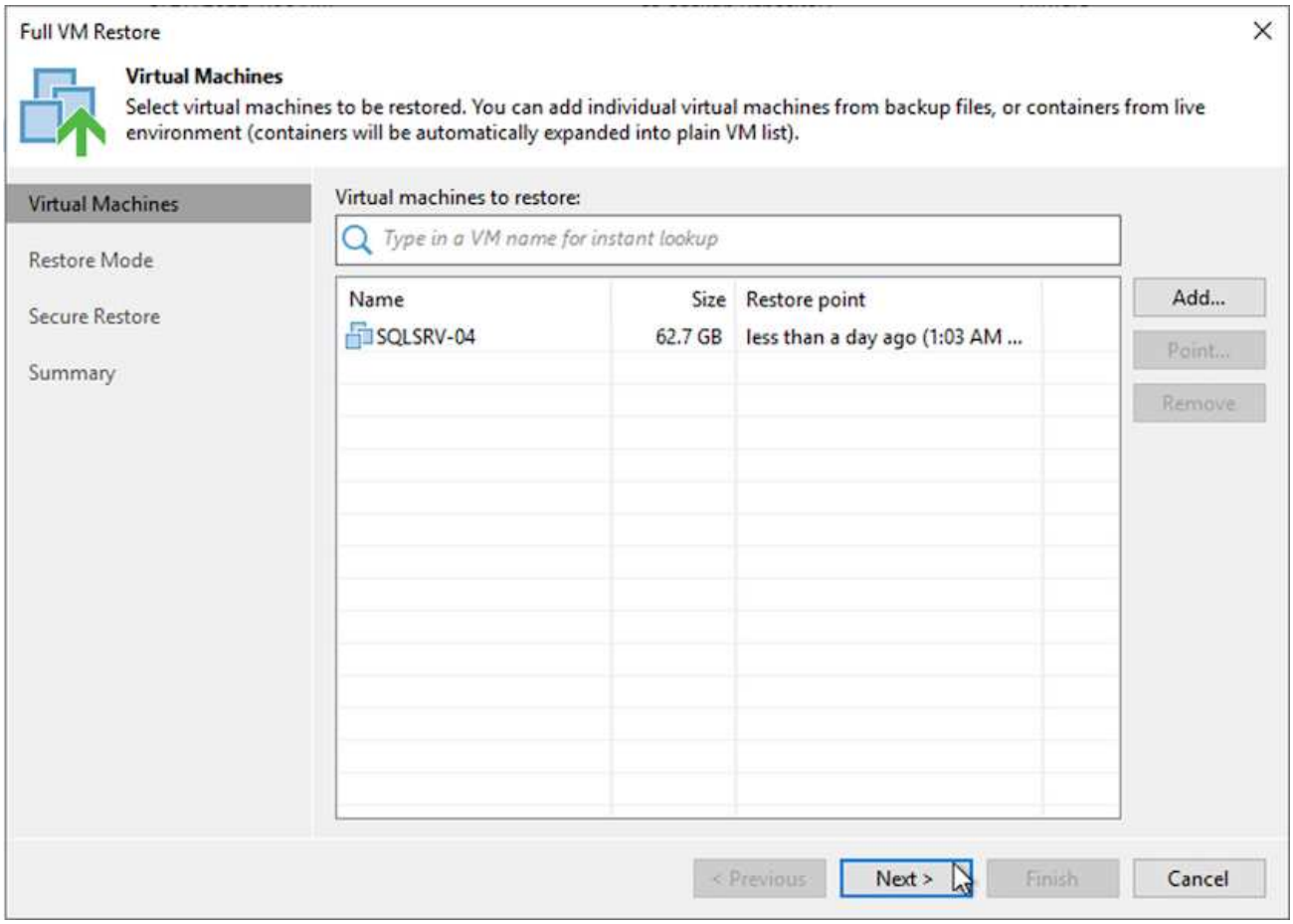
▼ Stellen Sie Anwendungs-VMs mit der vollständigen Wiederherstellung von Veeam in der VMware Cloud wieder her

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

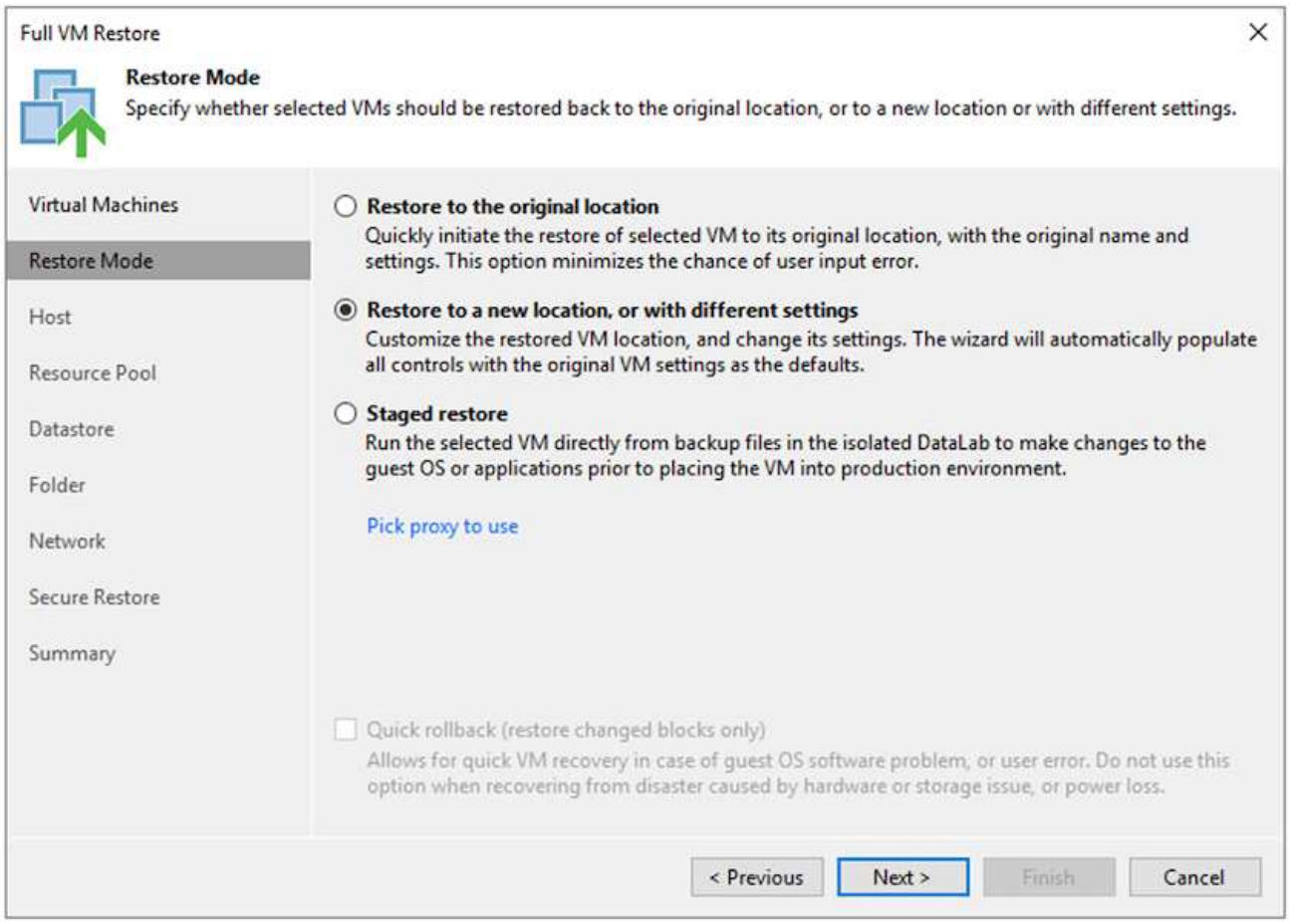
1. Wählen Sie auf der Veeam-Startseite den Objektspeicher mit den importierten Sicherungen aus, wählen Sie die wiederherzustellenden VMs aus, klicken Sie dann mit der rechten Maustaste und wählen Sie „Gesamte VM wiederherstellen“ aus.



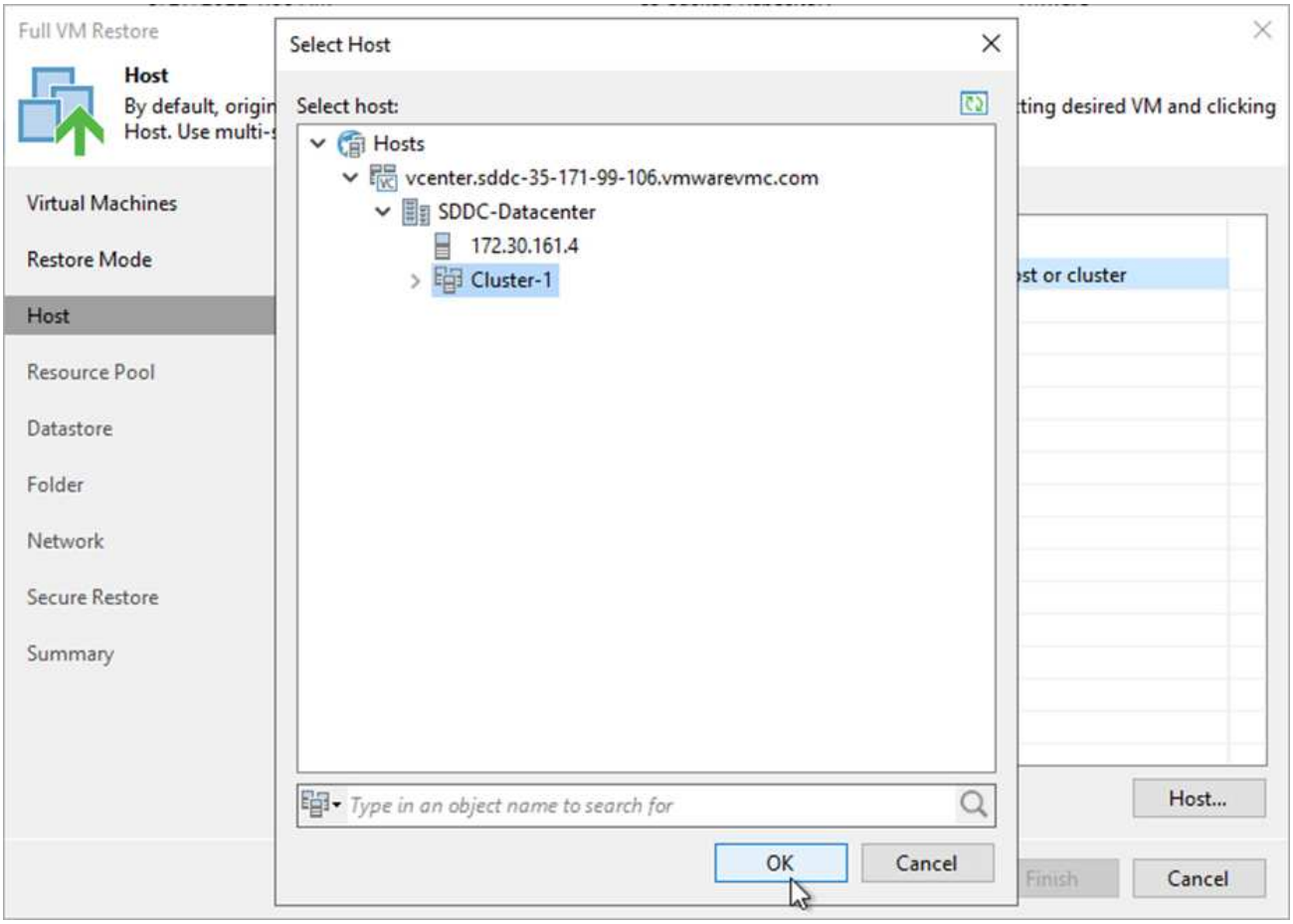
2. Ändern Sie auf der ersten Seite des Assistenten zur vollständigen VM-Wiederherstellung bei Bedarf die zu sichernden VMs und wählen Sie „Weiter“ aus.



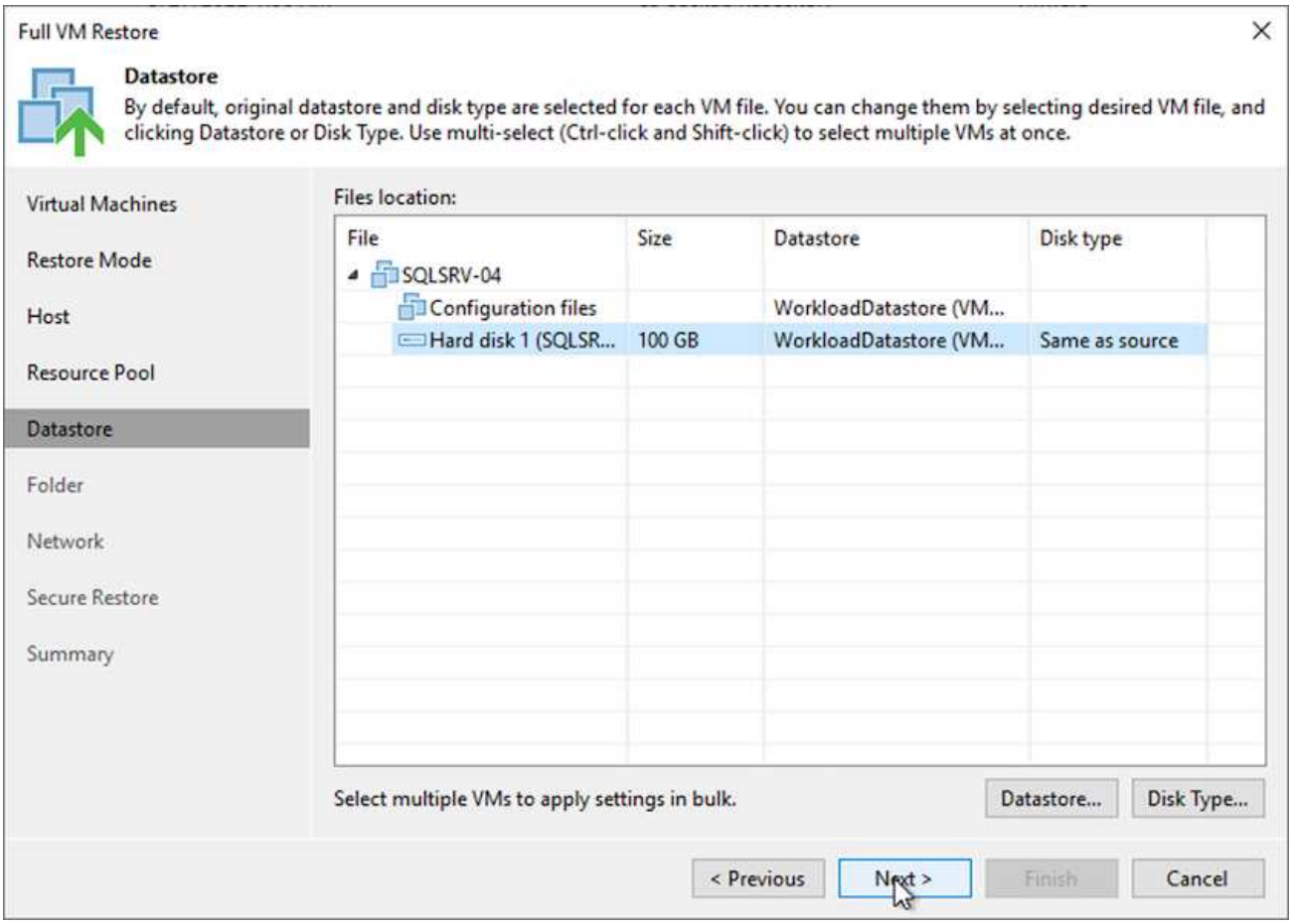
3. Wählen Sie auf der Seite „Wiederherstellungsmodus“ die Option „An einem neuen Speicherort oder mit anderen Einstellungen wiederherstellen“ aus.



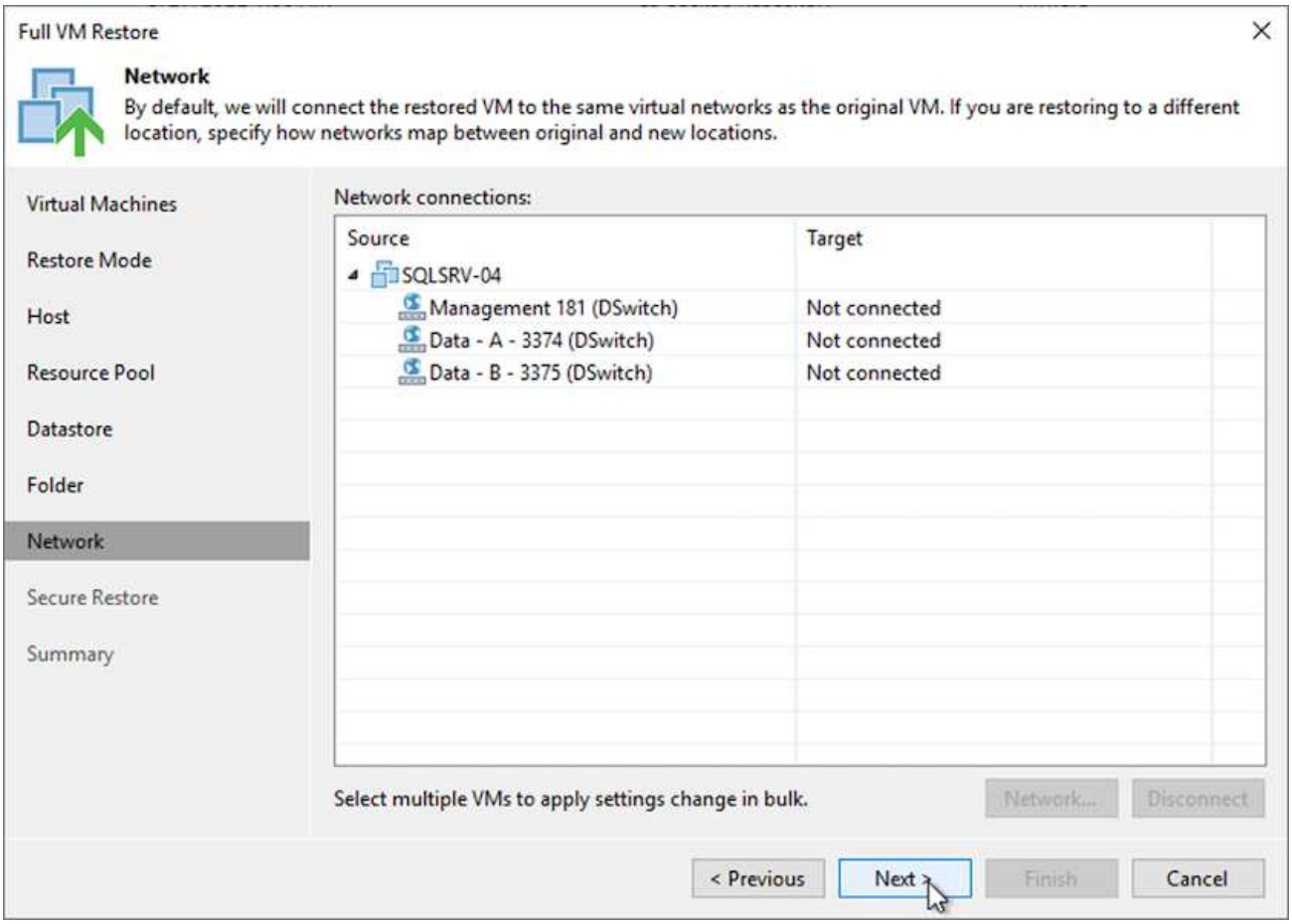
4. Wählen Sie auf der Hostseite den Ziel-ESXi-Host oder -Cluster aus, auf dem die VM wiederhergestellt werden soll.

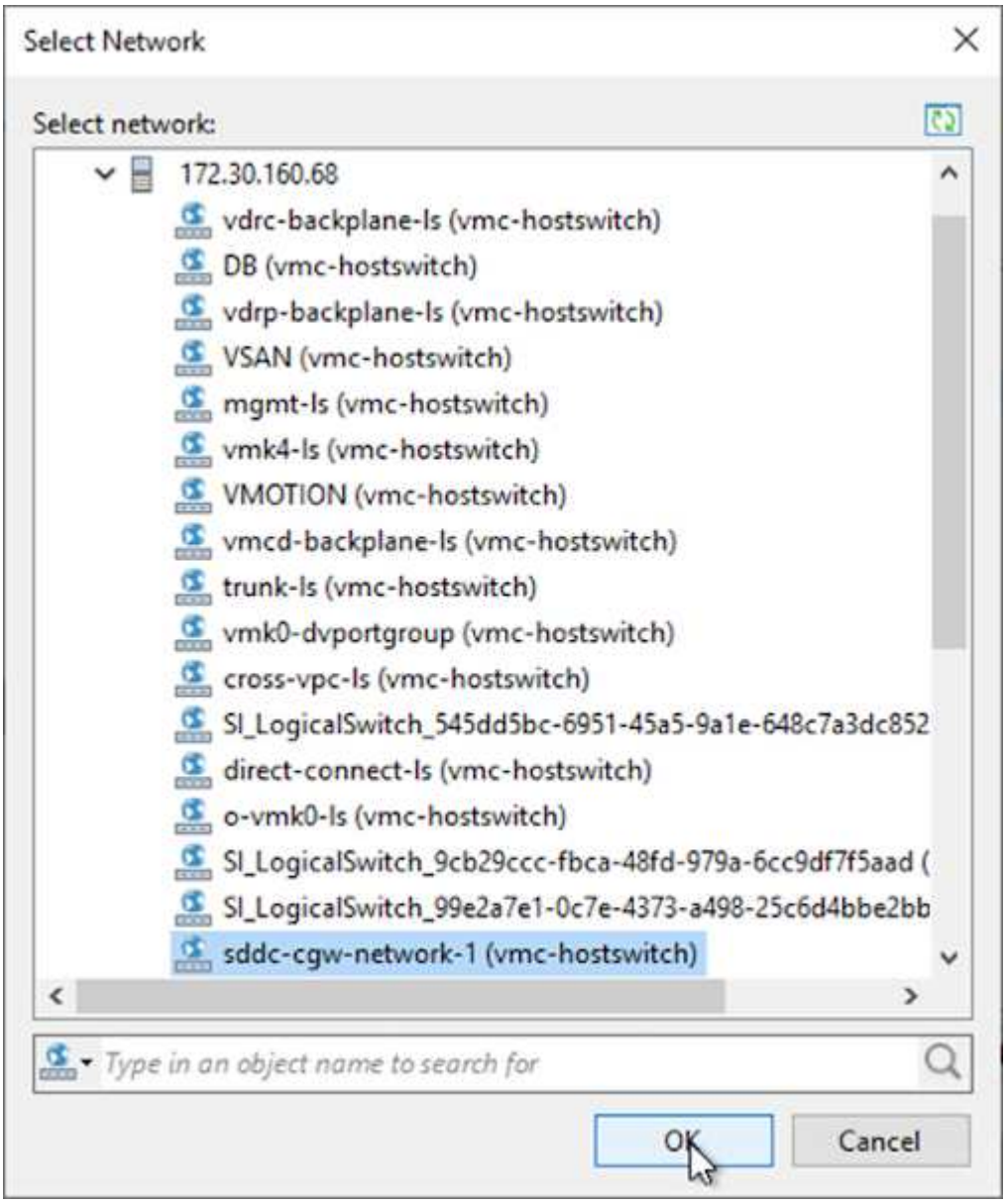


5. Wählen Sie auf der Seite „Datenspeicher“ den Zielspeicherort für die Konfigurationsdateien und die Festplatte aus.



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


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



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

Wiederherstellen von SQL Server-Anwendungsdaten

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

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

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

▼ VM: Konfiguration nach der Wiederherstellung für SQL Server-VM

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

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

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

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

▼ **Konfigurieren des FSx-Speichers für die SQL Server-Wiederherstellung**

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

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

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

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

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

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

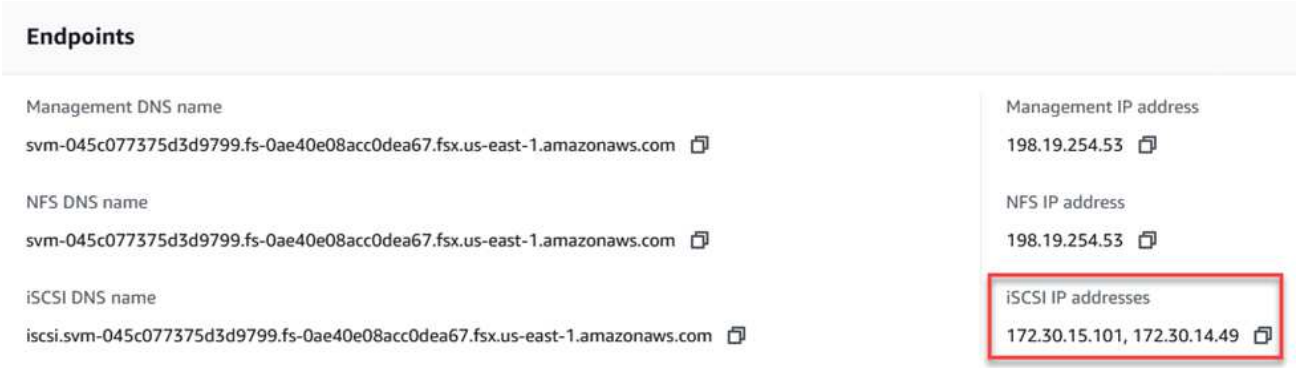
```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

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

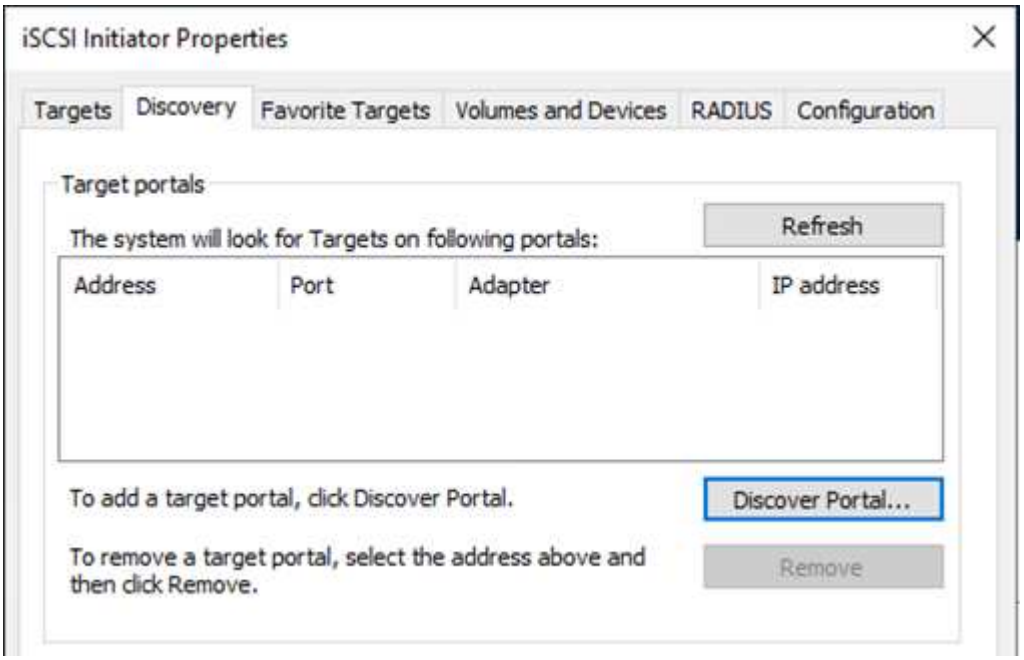
▼ **Einrichten der Windows-VM für den iSCSI-Zugriff und Ermitteln der Dateisysteme**

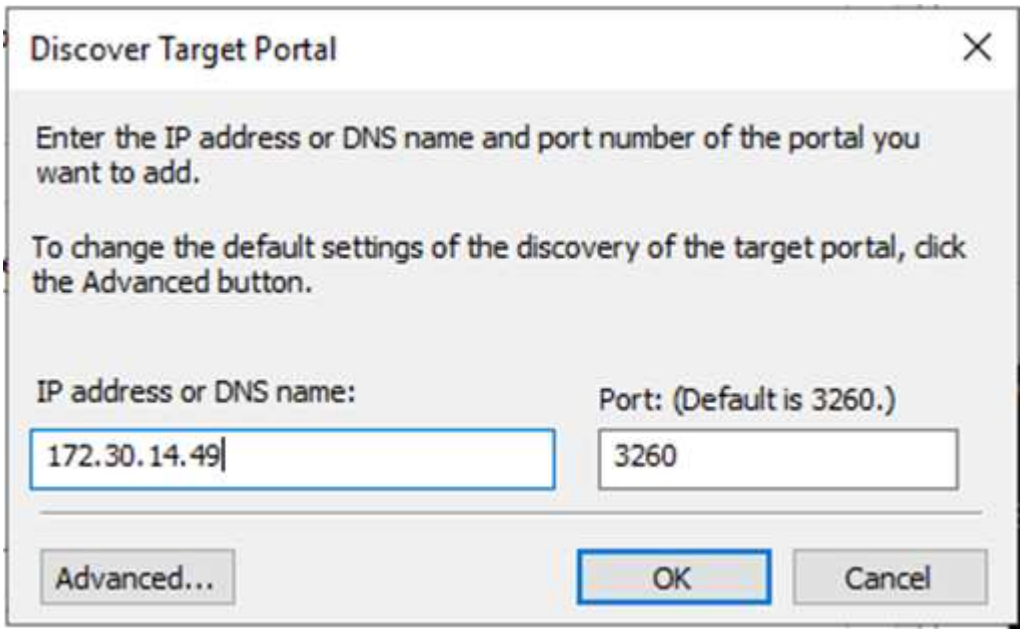
1. Richten Sie von der SQL Server-VM aus Ihren iSCSI-Netzwerkadapter für die Kommunikation mit der VMware-Portgruppe ein, die mit Konnektivität zu den iSCSI-Zielschnittstellen auf Ihrer FSx-Instanz eingerichtet wurde.
2. Öffnen Sie das Dienstprogramm „iSCSI-Initiator-Eigenschaften“ und löschen Sie die alten Konnektivitätseinstellungen auf den Registerkarten „Erkennung“, „Favoritenziele“ und „Ziele“.

3. Suchen Sie die IP-Adresse(n) für den Zugriff auf die logische iSCSI-Schnittstelle auf der FSx-Instanz/dem FSx-Cluster. Dies finden Sie in der AWS-Konsole unter Amazon FSx > ONTAP > Storage Virtual Machines.

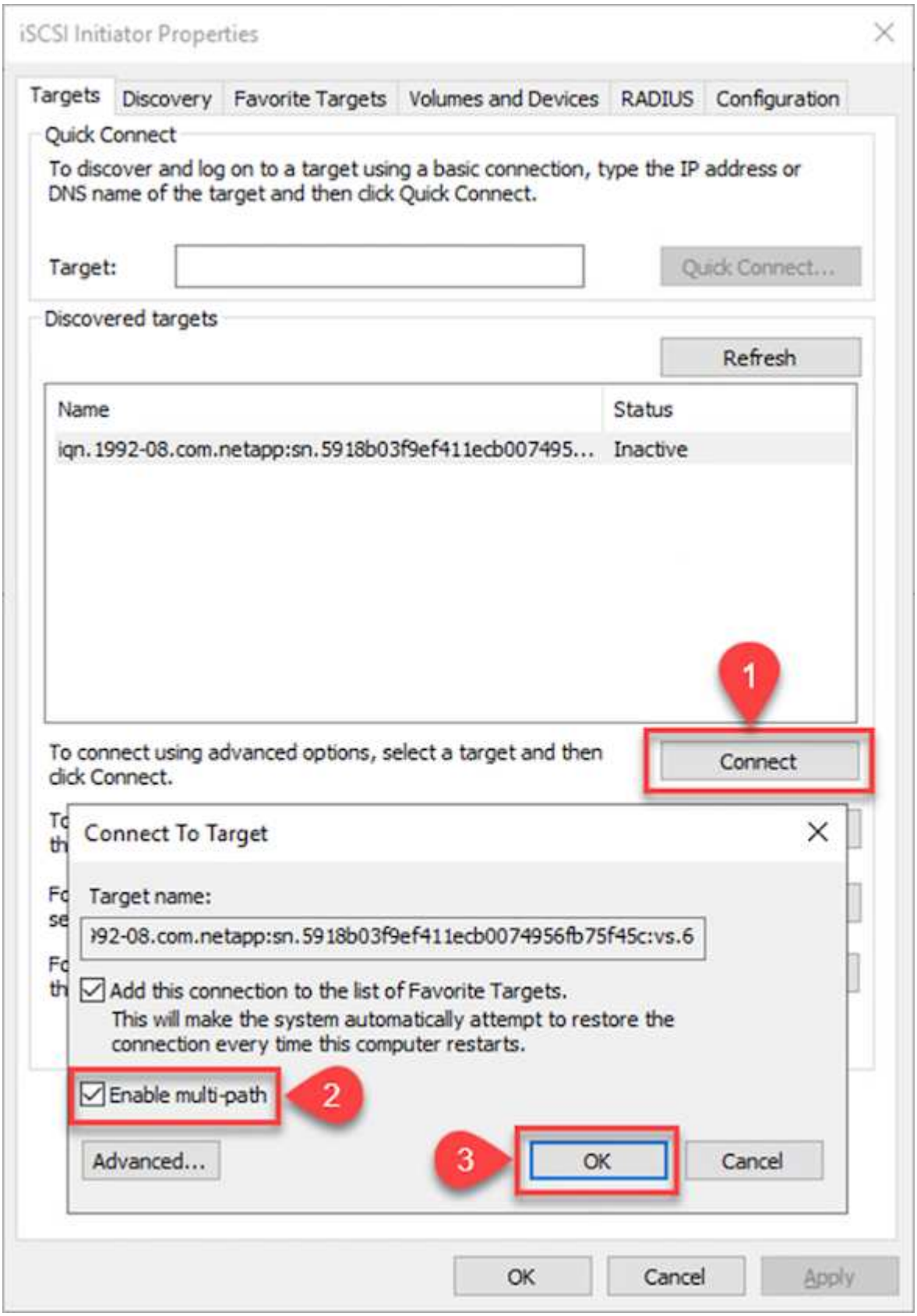


4. Klicken Sie auf der Registerkarte „Discovery“ auf „Discover Portal“ und geben Sie die IP-Adressen für Ihre FSx-iSCSI-Ziele ein.

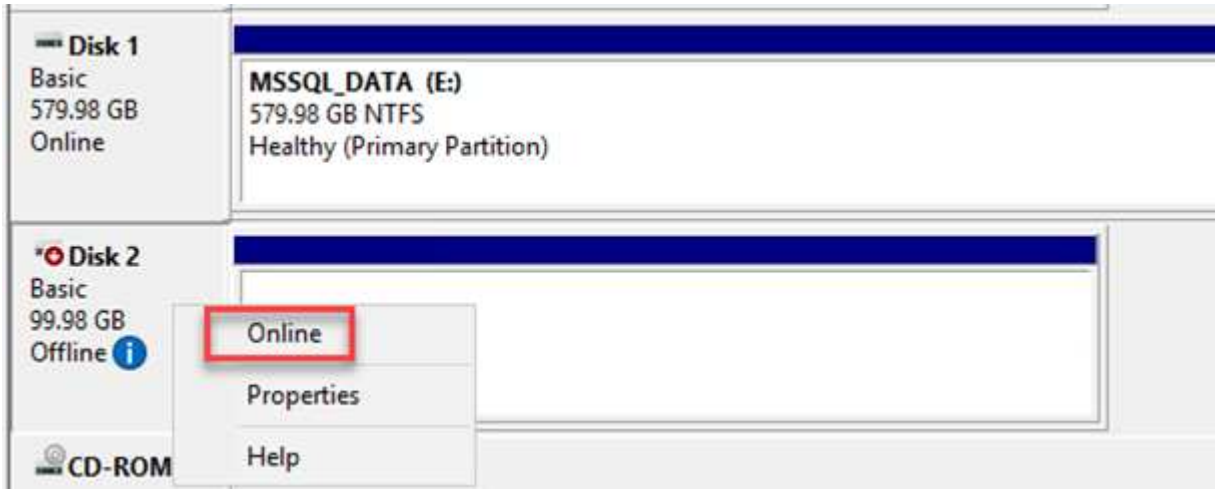




5. Klicken Sie auf der Registerkarte „Ziel“ auf „Verbinden“, wählen Sie „Mehrere Pfade aktivieren“ aus, falls dies für Ihre Konfiguration geeignet ist, und klicken Sie dann auf „OK“, um eine Verbindung mit dem Ziel herzustellen.

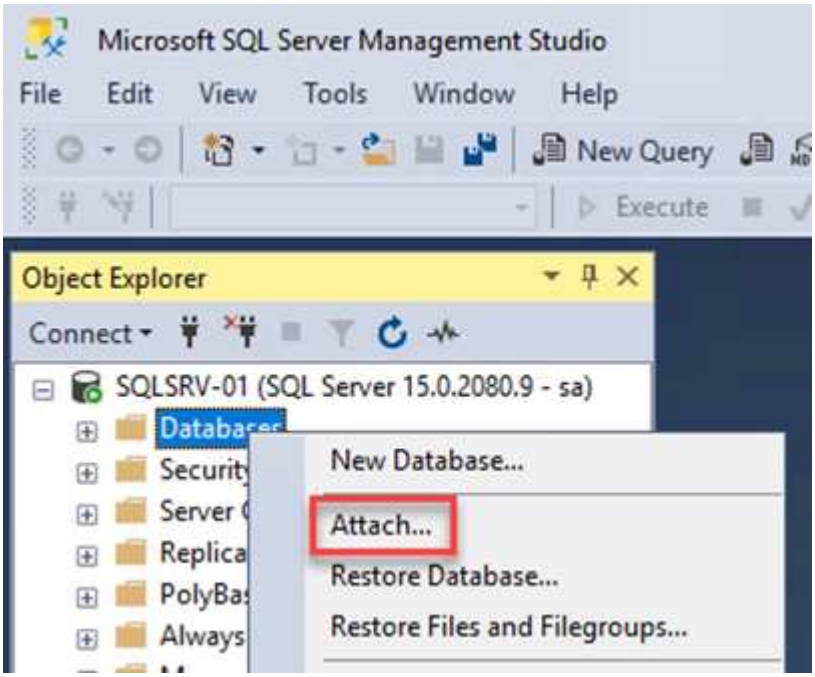


6. Öffnen Sie das Dienstprogramm „Computerverwaltung“ und schalten Sie die Festplatten online. Stellen Sie sicher, dass sie dieselben Laufwerksbuchstaben behalten, die sie zuvor hatten.

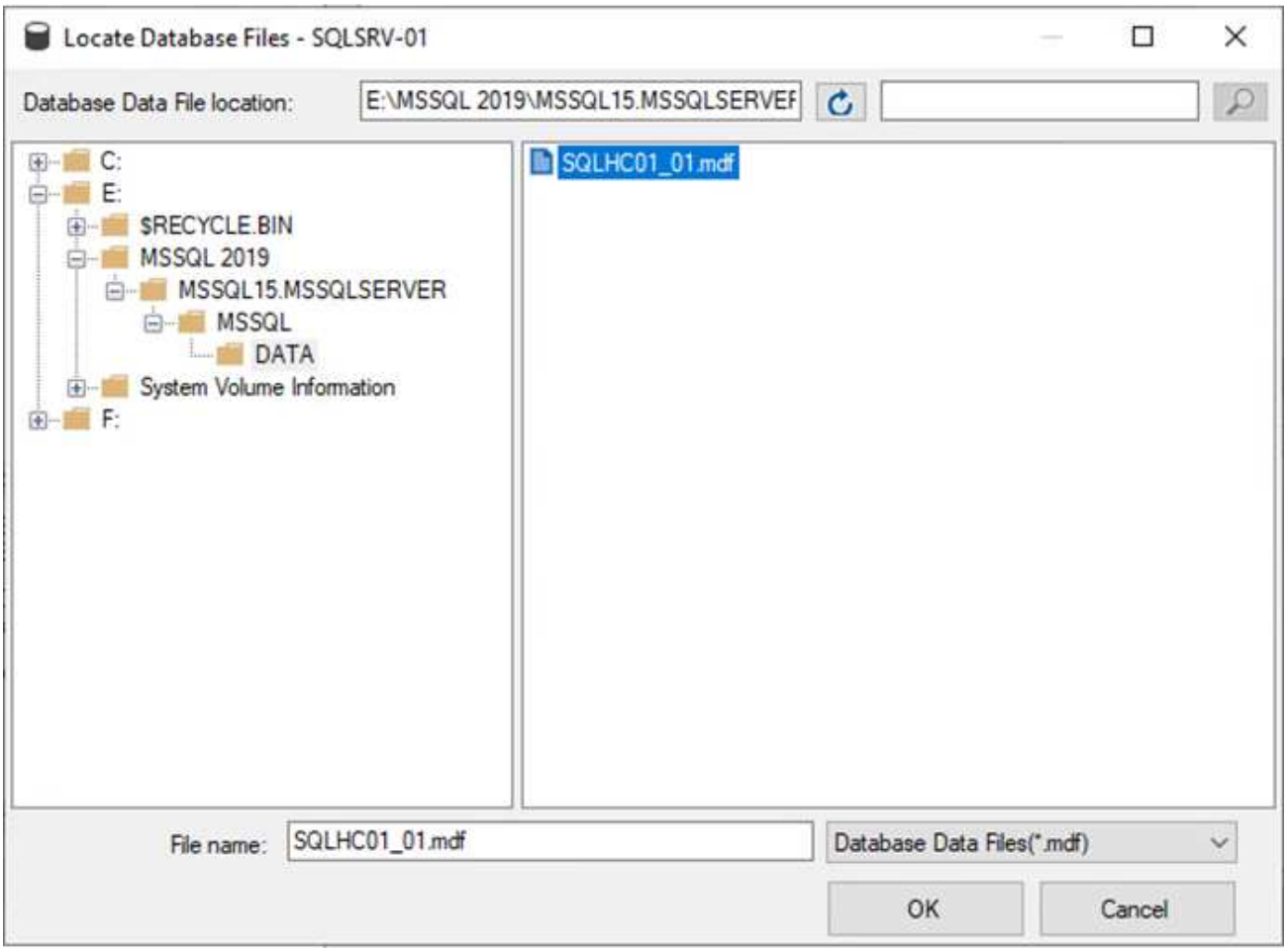


▼ **Anfügen der SQL Server-Datenbanken**

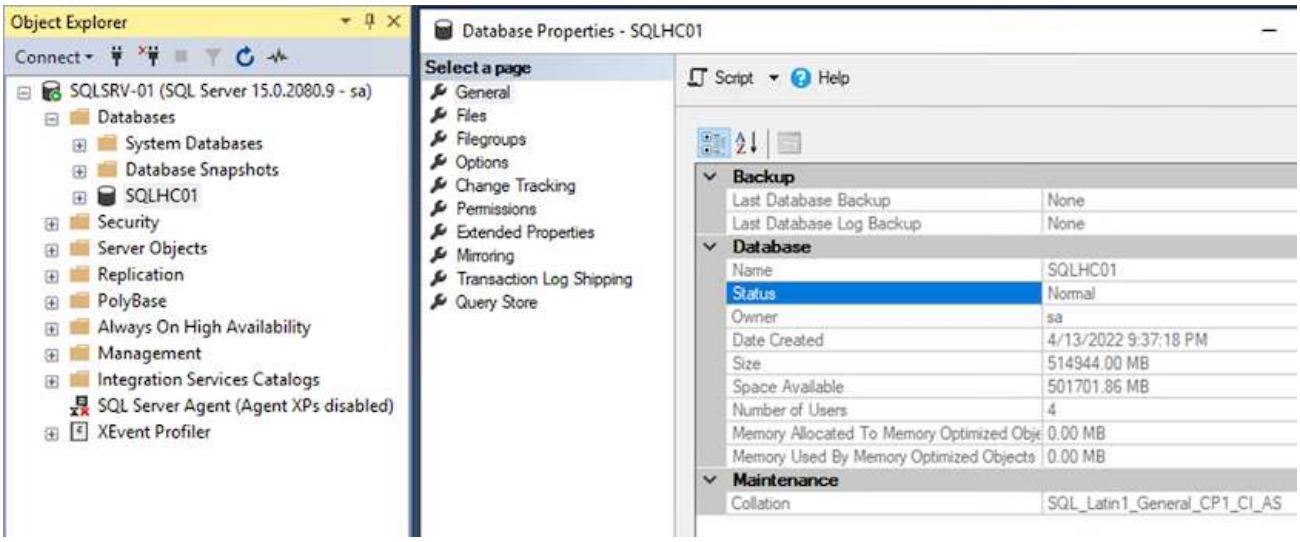
1. Öffnen Sie von der SQL Server-VM aus Microsoft SQL Server Management Studio und wählen Sie „Anhängen“ aus, um den Verbindungsvorgang mit der Datenbank zu starten.



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



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

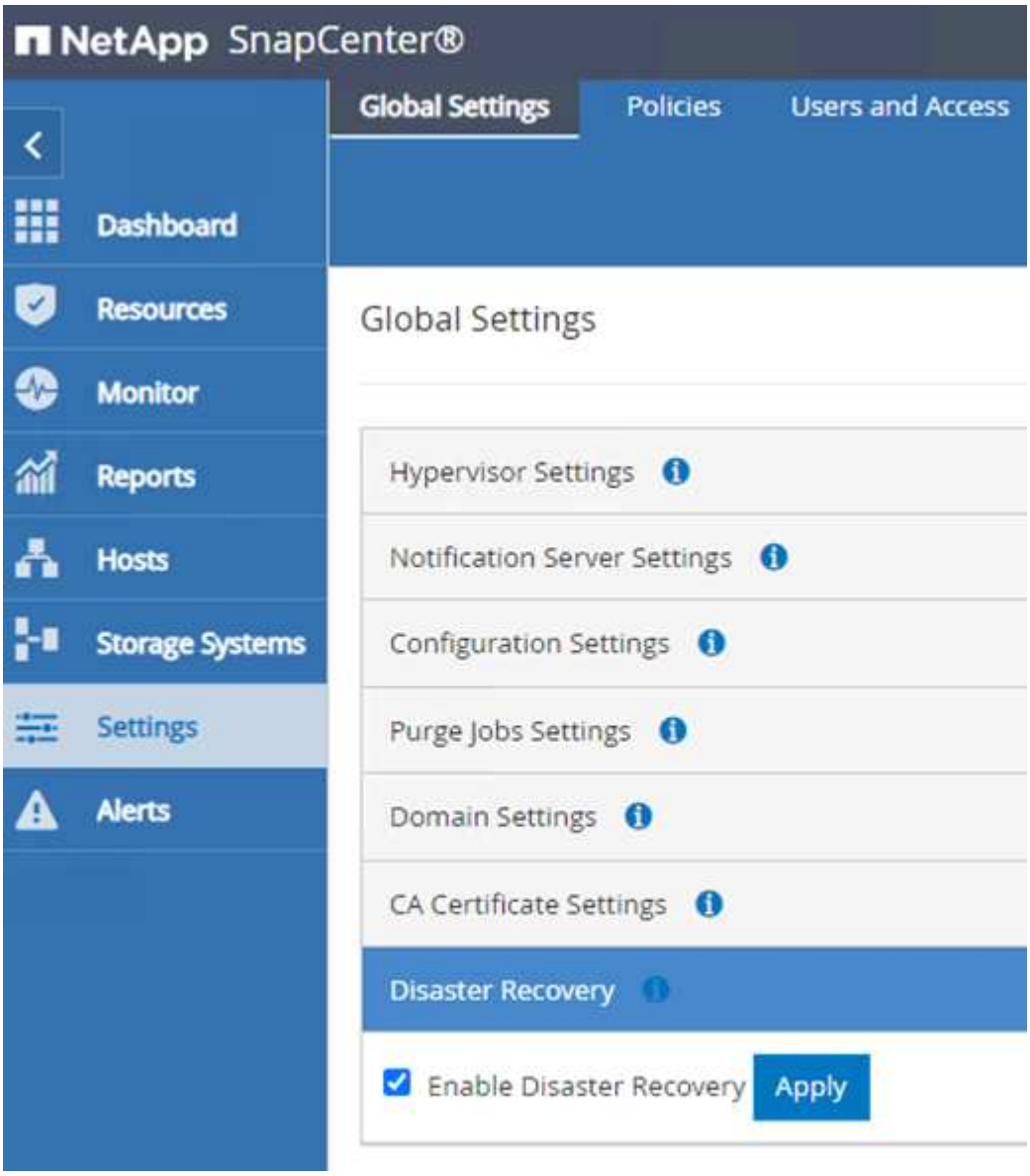


▼ **Bestätigen Sie die SnapCenter -Kommunikation mit dem SQL Server-Plug-in**

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

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

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



Wiederherstellen von Oracle-Anwendungsdaten

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

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

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

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

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

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

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

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

FsxId0ae40e08acc0dea67::>
```

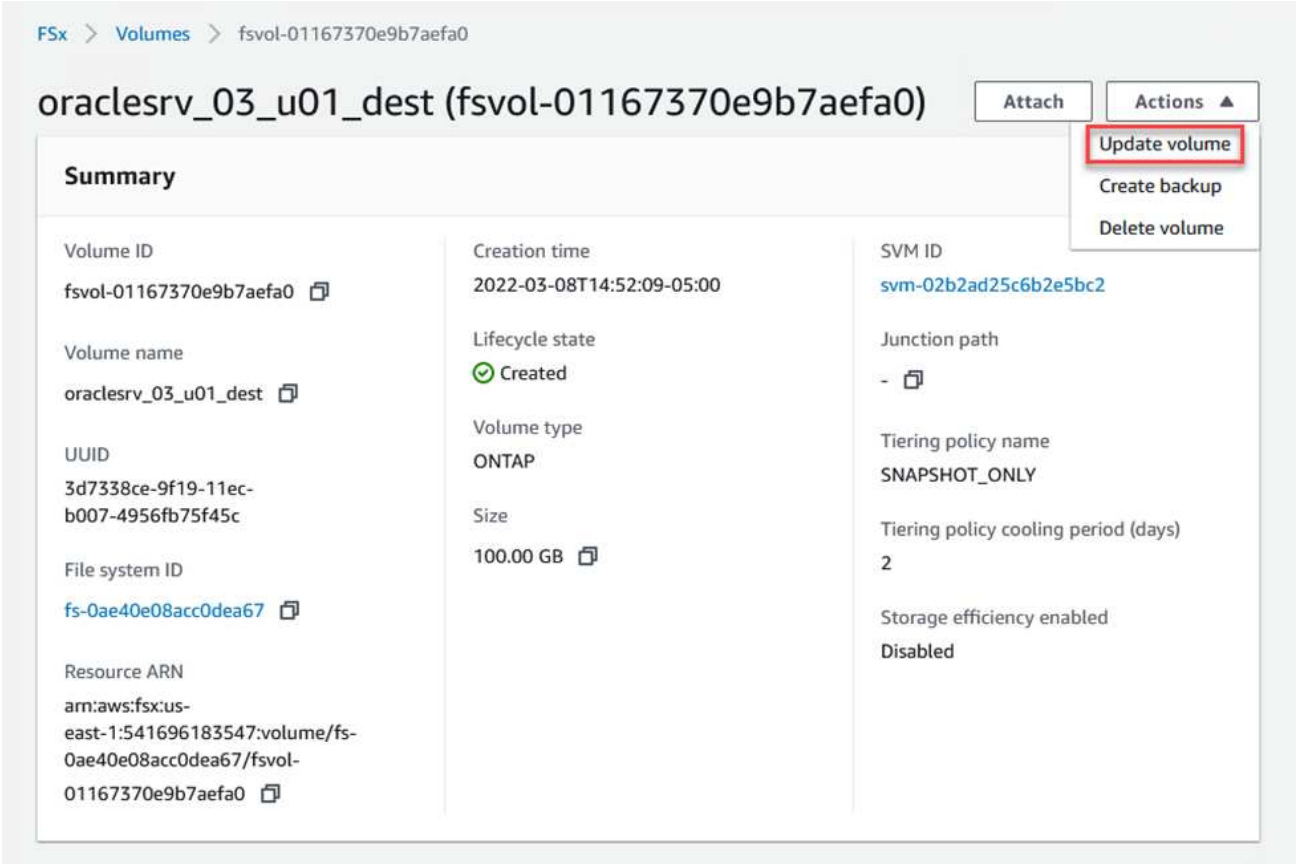
2. Führen Sie den folgenden Befehl aus, um die vorhandenen SnapMirror -Beziehungen aufzuheben.

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

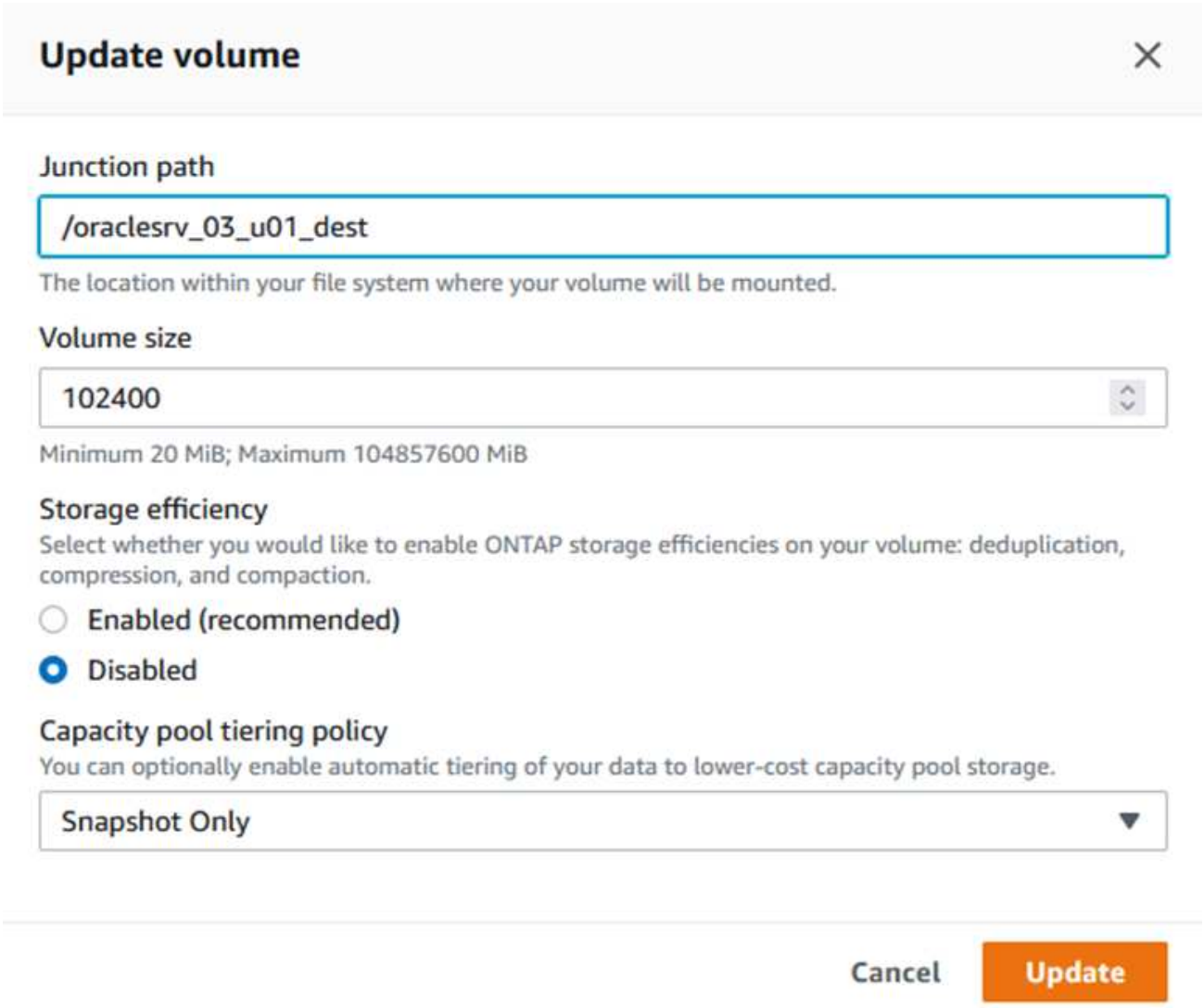
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

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

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



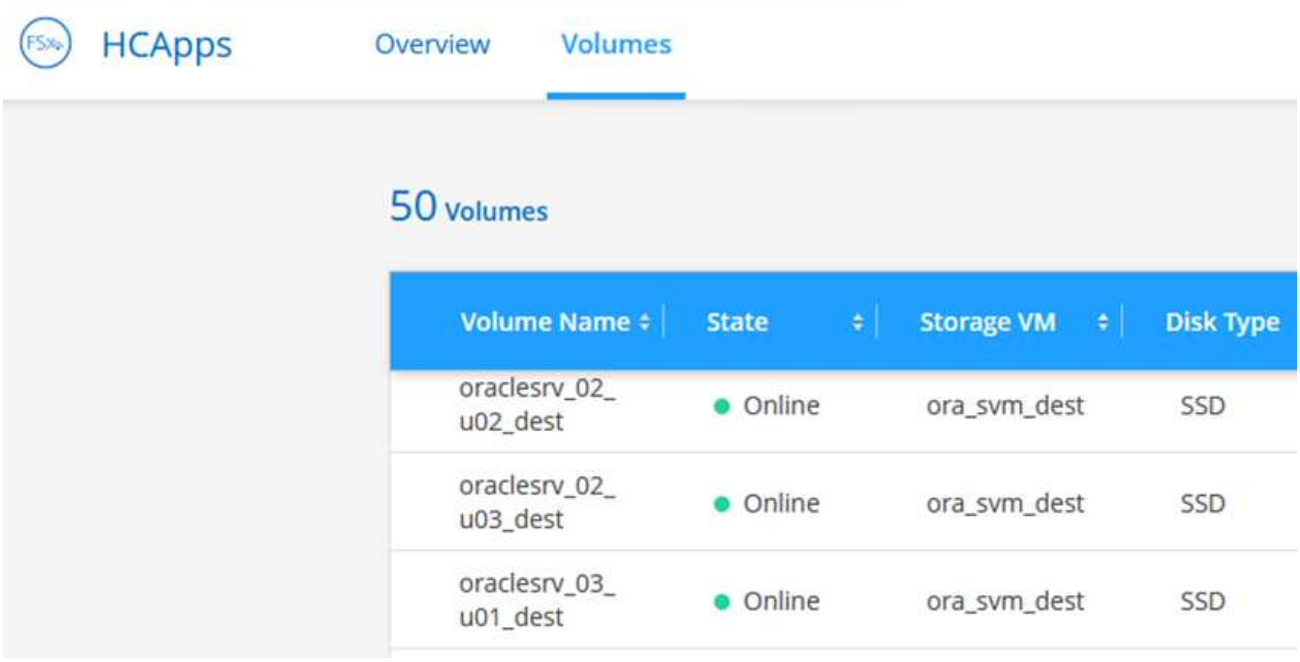
4. Fügen Sie den Namen des Kreuzungspfads hinzu und klicken Sie auf „Aktualisieren“. Geben Sie diesen Verbindungspfad an, wenn Sie das NFS-Volume vom Oracle-Server mounten.



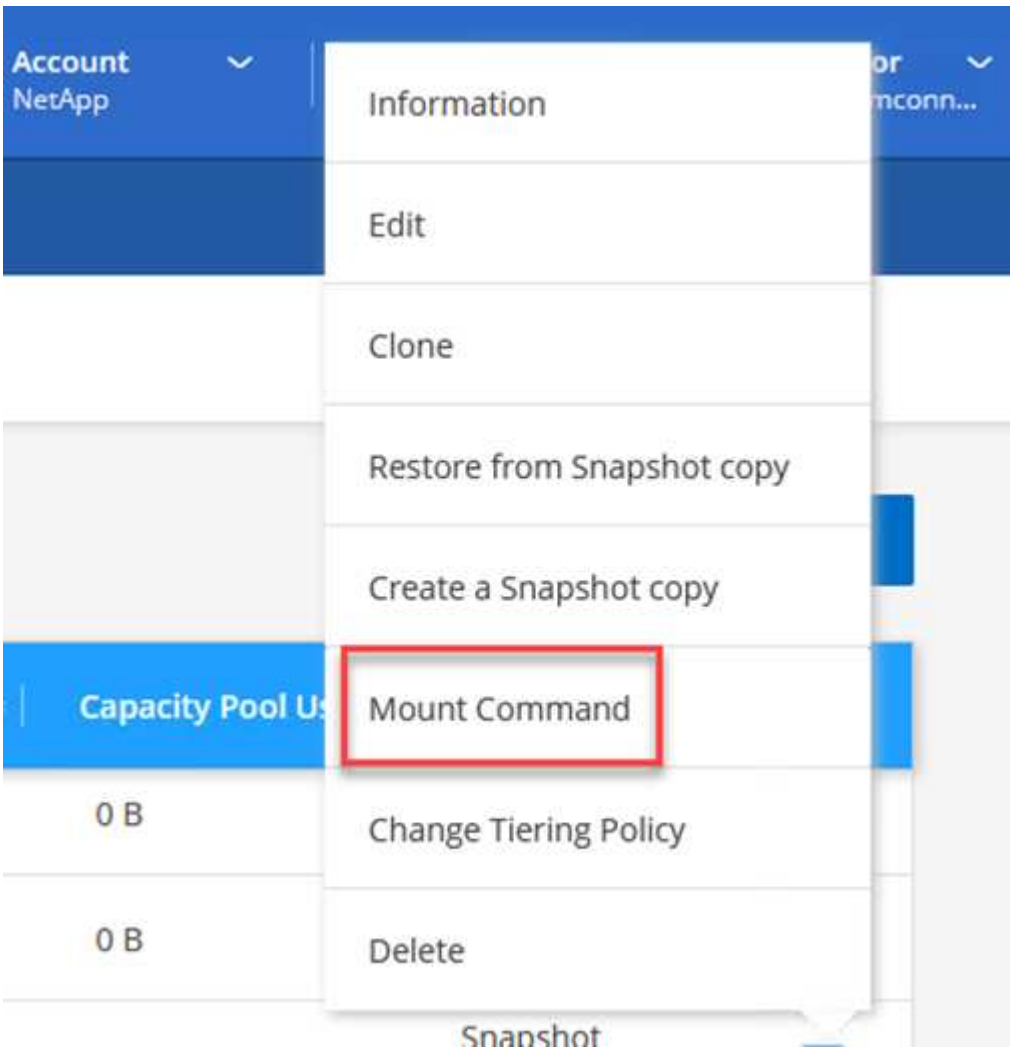
▼ **Mounten Sie NFS-Volumes auf Oracle Server**

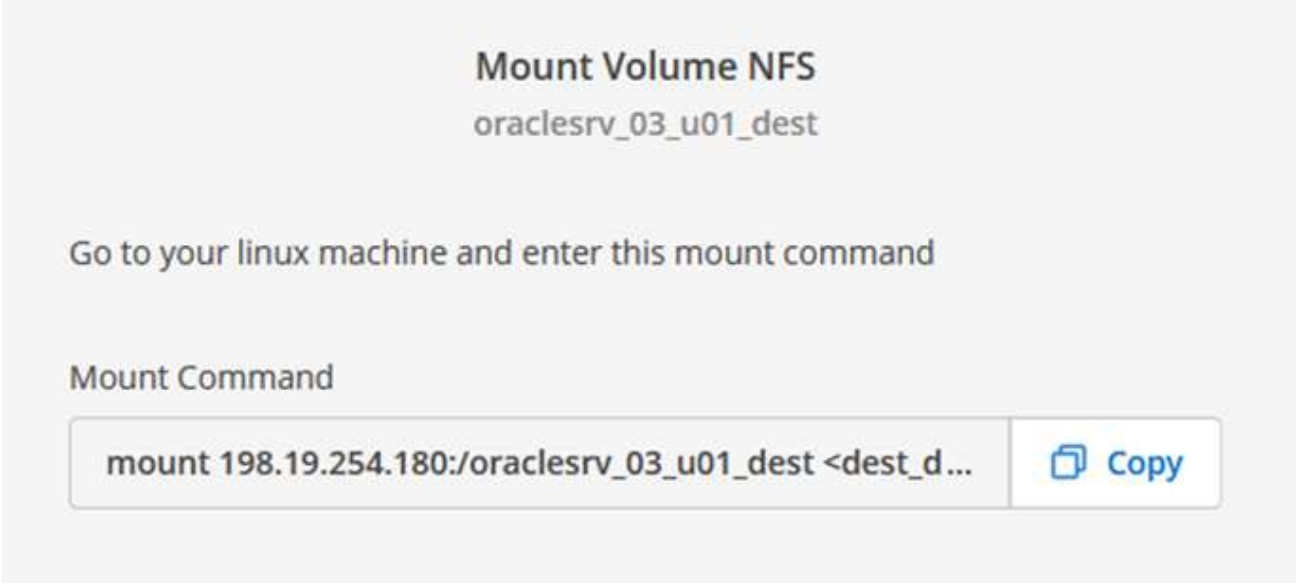
In Cloud Manager können Sie den Mount-Befehl mit der richtigen NFS-LIF-IP-Adresse zum Mounten der NFS-Volumes abrufen, die die Oracle-Datenbankdateien und -Protokolle enthalten.

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



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





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

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

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

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

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

Failback

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

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

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

Abschluss

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

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

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

Veeam Backup & Restore in VMware Cloud, mit Amazon FSx ONTAP

Veeam Backup & Replication ist eine effektive und zuverlässige Lösung zum Schutz von Daten in VMware Cloud. Diese Lösung demonstriert die richtige Einrichtung und Konfiguration für die Verwendung von Veeam Backup and Replication zum Sichern und Wiederherstellen von Anwendungs-VMs, die sich auf FSx ONTAP NFS-Datenspeichern in VMware Cloud befinden.

Überblick

VMware Cloud (in AWS) unterstützt die Verwendung von NFS-Datenspeichern als zusätzlichen Speicher und FSx ONTAP ist eine sichere Lösung für Kunden, die große Datenmengen für ihre Cloud-Anwendungen speichern müssen, die unabhängig von der Anzahl der ESXi-Hosts im SDDC-Cluster skaliert werden können. Dieser integrierte AWS-Speicherdienst bietet hocheffizienten Speicher mit allen herkömmlichen NetApp ONTAP Funktionen.

Anwendungsfälle

Diese Lösung ist für die folgenden Anwendungsfälle geeignet:

- Sicherung und Wiederherstellung von in VMC gehosteten virtuellen Windows- und Linux-Maschinen unter Verwendung von FSx ONTAP als Sicherungsrepository.
- Sicherung und Wiederherstellung von Microsoft SQL Server-Anwendungsdaten mit FSx ONTAP als Sicherungsrepository.
- Sicherung und Wiederherstellung von Oracle-Anwendungsdaten mit FSx ONTAP als Sicherungsrepository.

NFS-Datenspeicher mit Amazon FSx ONTAP

Alle virtuellen Maschinen in dieser Lösung befinden sich auf zusätzlichen NFS-Datenspeichern von FSx ONTAP . Die Verwendung von FSx ONTAP als ergänzender NFS-Datenspeicher bietet mehrere Vorteile. Sie können damit beispielsweise:

- Erstellen Sie ein skalierbares und hochverfügbares Dateisystem in der Cloud, ohne dass eine komplexe Einrichtung und Verwaltung erforderlich ist.

- Integrieren Sie es in Ihre vorhandene VMware-Umgebung, sodass Sie vertraute Tools und Prozesse zur Verwaltung Ihrer Cloud-Ressourcen verwenden können.
- Profitieren Sie von den erweiterten Datenverwaltungsfunktionen von ONTAP, wie Snapshots und Replikation, um Ihre Daten zu schützen und ihre Verfügbarkeit sicherzustellen.

▼ Übersicht über die Lösungsbereitstellung

Diese Liste enthält die grundlegenden Schritte zum Konfigurieren von Veeam Backup & Replication, zum Ausführen von Sicherungs- und Wiederherstellungsaufträgen mit FSx ONTAP als Sicherungsrepository und zum Durchführen von Wiederherstellungen von SQL Server- und Oracle-VMs und -Datenbanken:

1. Erstellen Sie das FSx ONTAP Dateisystem, das als iSCSI-Sicherungsrepository für Veeam Backup & Replication verwendet werden soll.
2. Stellen Sie Veeam Proxy bereit, um Backup-Workloads zu verteilen und auf FSx ONTAP gehostete iSCSI-Backup-Repositorys bereitzustellen.
3. Konfigurieren Sie Veeam-Sicherungsjobs zum Sichern von virtuellen SQL Server-, Oracle-, Linux- und Windows-Maschinen.
4. Stellen Sie virtuelle SQL Server-Maschinen und einzelne Datenbanken wieder her.
5. Stellen Sie virtuelle Oracle-Maschinen und einzelne Datenbanken wieder her.

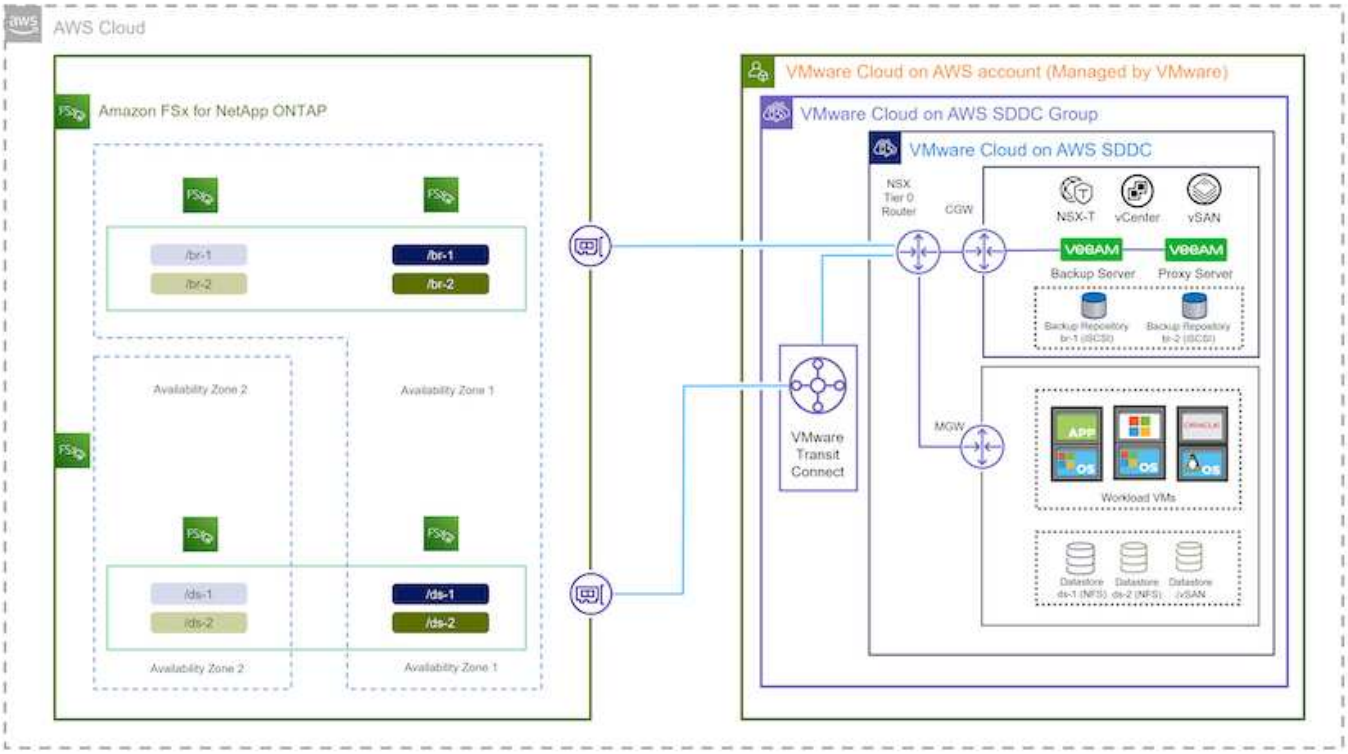
▼ Voraussetzungen

Der Zweck dieser Lösung besteht darin, den Datenschutz von virtuellen Maschinen zu demonstrieren, die in VMware Cloud ausgeführt werden und sich auf von FSx ONTAP gehosteten NFS-Datenspeichern befinden. Diese Lösung setzt voraus, dass die folgenden Komponenten konfiguriert und einsatzbereit sind:

1. FSx ONTAP -Dateisystem mit einem oder mehreren NFS-Datenspeichern, die mit VMware Cloud verbunden sind.
2. Microsoft Windows Server-VM mit installierter Veeam Backup & Replication-Software.
    - Der vCenter-Server wurde vom Veeam Backup & Replication-Server anhand seiner IP-Adresse oder seines vollqualifizierten Domänennamens erkannt.
3. Während der Bereitstellung der Lösung muss eine Microsoft Windows Server-VM mit Veeam Backup Proxy-Komponenten installiert werden.
4. Microsoft SQL Server-VMs mit VMDKs und Anwendungsdaten, die sich auf FSx ONTAP NFS-Datenspeichern befinden. Für diese Lösung hatten wir zwei SQL-Datenbanken auf zwei separaten VMDKs.
    - Hinweis: Als bewährte Methode werden Datenbank- und Transaktionsprotokolldateien auf separaten Laufwerken abgelegt, da dies die Leistung und Zuverlässigkeit verbessert. Dies liegt teilweise daran, dass Transaktionsprotokolle sequenziell geschrieben werden, während Datenbankdateien zufällig geschrieben werden.
5. Oracle-Datenbank-VMs mit VMDKs und Anwendungsdaten, die sich auf FSx ONTAP NFS-Datenspeichern befinden.
6. Linux- und Windows-Dateiserver-VMs mit VMDKs, die sich auf FSx ONTAP NFS-Datenspeichern befinden.
7. Veeam benötigt bestimmte TCP-Ports für die Kommunikation zwischen Servern und Komponenten in der Backup-Umgebung. Auf den Komponenten der Veeam-Backup-Infrastruktur werden die erforderlichen Firewall-Regeln automatisch erstellt. Eine vollständige Liste der Netzwerk-Port-Anforderungen finden Sie im Abschnitt „Ports“ der "Veeam Backup and Replication-Benutzerhandbuch für VMware vSphere" .

High-Level-Architektur

Die Prüfung/Validierung dieser Lösung wurde in einem Labor durchgeführt, das möglicherweise nicht der endgültigen Bereitstellungsumgebung entspricht. Weitere Informationen finden Sie in den folgenden Abschnitten.



▼ **Hardware-/Softwarekomponenten**

Der Zweck dieser Lösung besteht darin, den Datenschutz von virtuellen Maschinen zu demonstrieren, die in VMware Cloud ausgeführt werden und sich auf von FSx ONTAP gehosteten NFS-Datenspeichern befinden. Diese Lösung setzt voraus, dass die folgenden Komponenten bereits konfiguriert und einsatzbereit sind:

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

Lösungsbereitstellung

In dieser Lösung bieten wir detaillierte Anweisungen zum Bereitstellen und Validieren einer Lösung unter Verwendung der Veeam Backup and Replication-Software zum Durchführen von Backups und Wiederherstellungen von virtuellen Maschinen mit SQL Server, Oracle sowie Windows- und Linux-Dateiservern in einem VMware Cloud SDDC auf AWS. Die virtuellen Maschinen in dieser Lösung befinden sich auf einem zusätzlichen NFS-Datenspeicher, der von FSx ONTAP gehostet wird. Darüber hinaus wird ein separates FSx ONTAP Dateisystem zum Hosten von iSCSI-Volumes verwendet, die für Veeam-Backup-Repositorys verwendet werden.

Wir werden die Erstellung des FSx ONTAP Dateisystems durchgehen, iSCSI-Volumes mounten, die als Backup-Repositorys verwendet werden sollen, Backup-Jobs erstellen und ausführen und VM- und

Datenbankwiederherstellungen durchführen.

Ausführliche Informationen zu FSx ONTAP finden Sie im "FSx ONTAP Benutzerhandbuch" .

Ausführliche Informationen zu Veeam Backup und Replication finden Sie im "Veeam Help Center Technische Dokumentation" Website.

Hinweise und Einschränkungen zur Verwendung von Veeam Backup and Replication mit VMware Cloud on AWS finden Sie unter "VMware Cloud auf AWS und VMware Cloud auf Dell EMC-Support. Überlegungen und Einschränkungen" .

Veeam-Proxyserver bereitstellen

Ein Veeam-Proxyserver ist eine Komponente der Veeam Backup & Replication-Software, die als Vermittler zwischen der Quelle und dem Backup- oder Replikationsziel fungiert. Der Proxyserver trägt zur Optimierung und Beschleunigung der Datenübertragung während Sicherungsaufträgen bei, indem er die Daten lokal verarbeitet und verschiedene Transportmodi für den Datenzugriff mithilfe von VMware vStorage-APIs für den Datenschutz oder über direkten Speicherzugriff nutzen kann.

Bei der Auswahl eines Veeam-Proxyserver-Designs ist es wichtig, die Anzahl gleichzeitiger Aufgaben und den gewünschten Transportmodus bzw. Typ des Speicherzugriffs zu berücksichtigen.

Informationen zur Dimensionierung der Anzahl der Proxy-Server 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 Transportmodus als Methode zum Abrufen von VM-Daten von der Quelle und zum Übertragen an das Ziel. Der Transportmodus wird während der Konfiguration des Sicherungsauftrags angegeben. Durch die Verwendung des direkten Speicherzugriffs ist es möglich, die Effizienz von Backups aus NFS-Datenspeichern zu steigern.

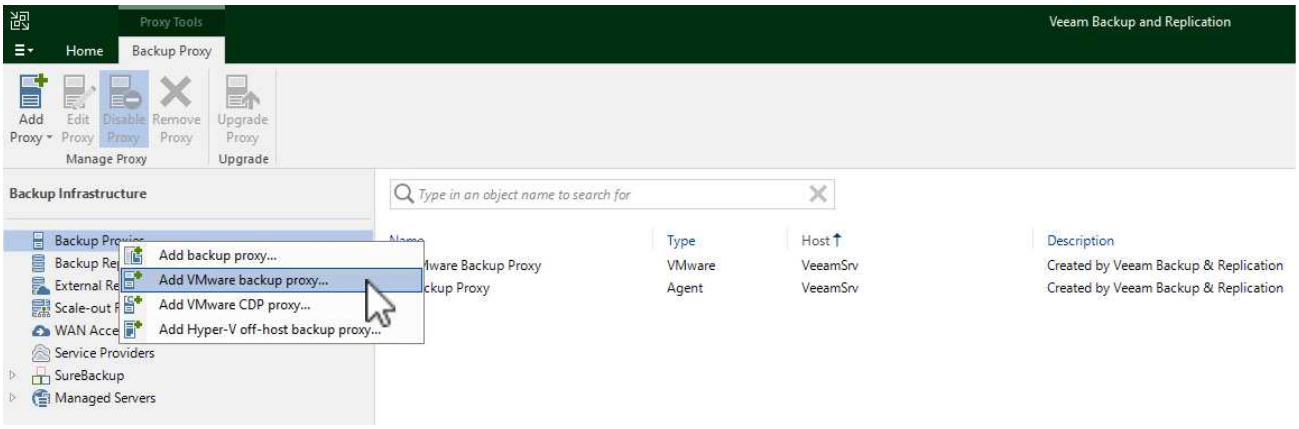
Weitere Informationen zu den Transportarten finden Sie im "Veeam Backup and Replication-Benutzerhandbuch für VMware vSphere" .

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

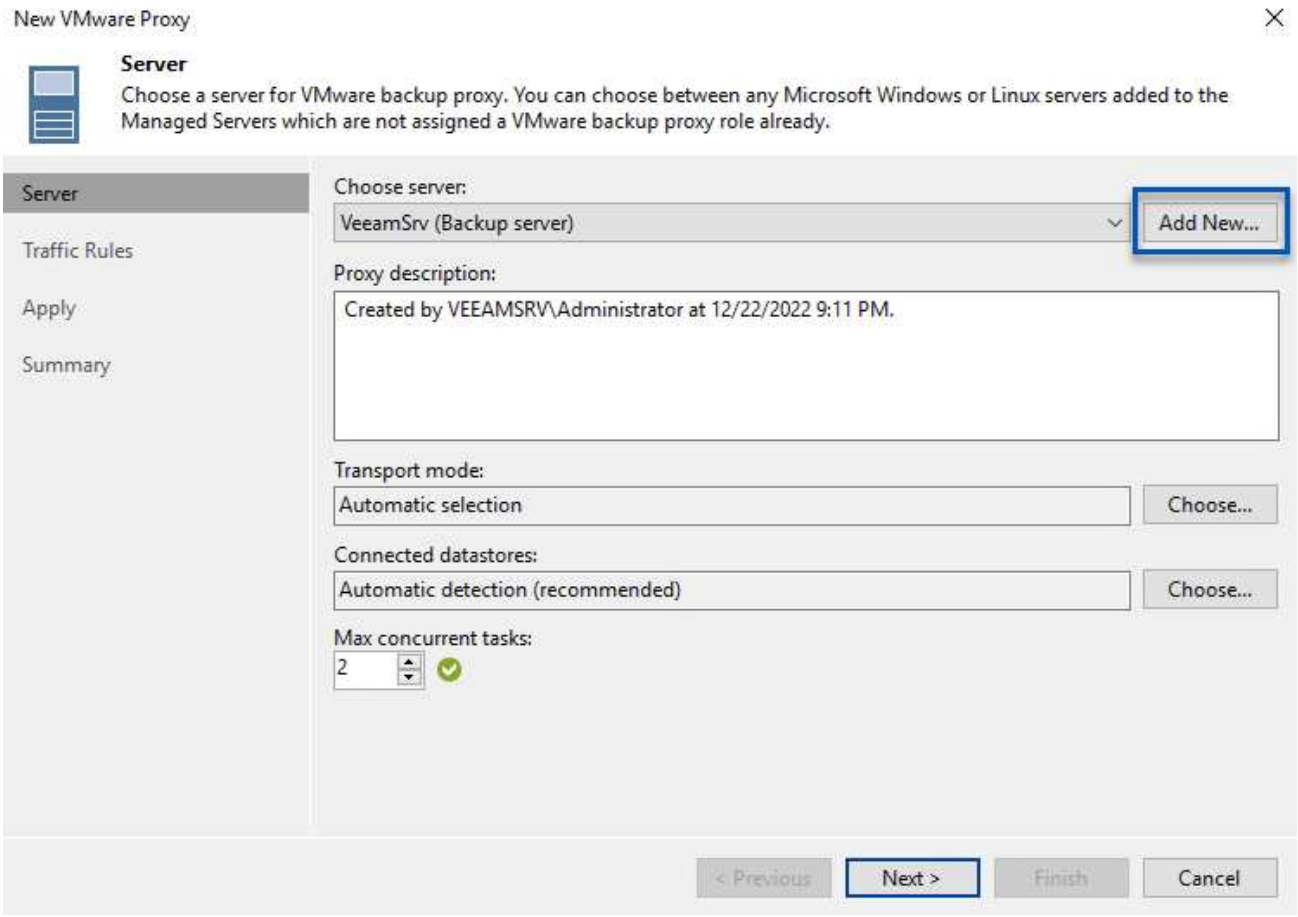
▼ **Bereitstellen von Veeam Proxy zur Verteilung von Backup-Workloads**

In diesem Schritt wird der Veeam-Proxy auf einer vorhandenen Windows-VM bereitgestellt. Dadurch können Sicherungsaufträge zwischen dem primären Veeam-Sicherungsserver und dem Veeam-Proxy verteilt werden.

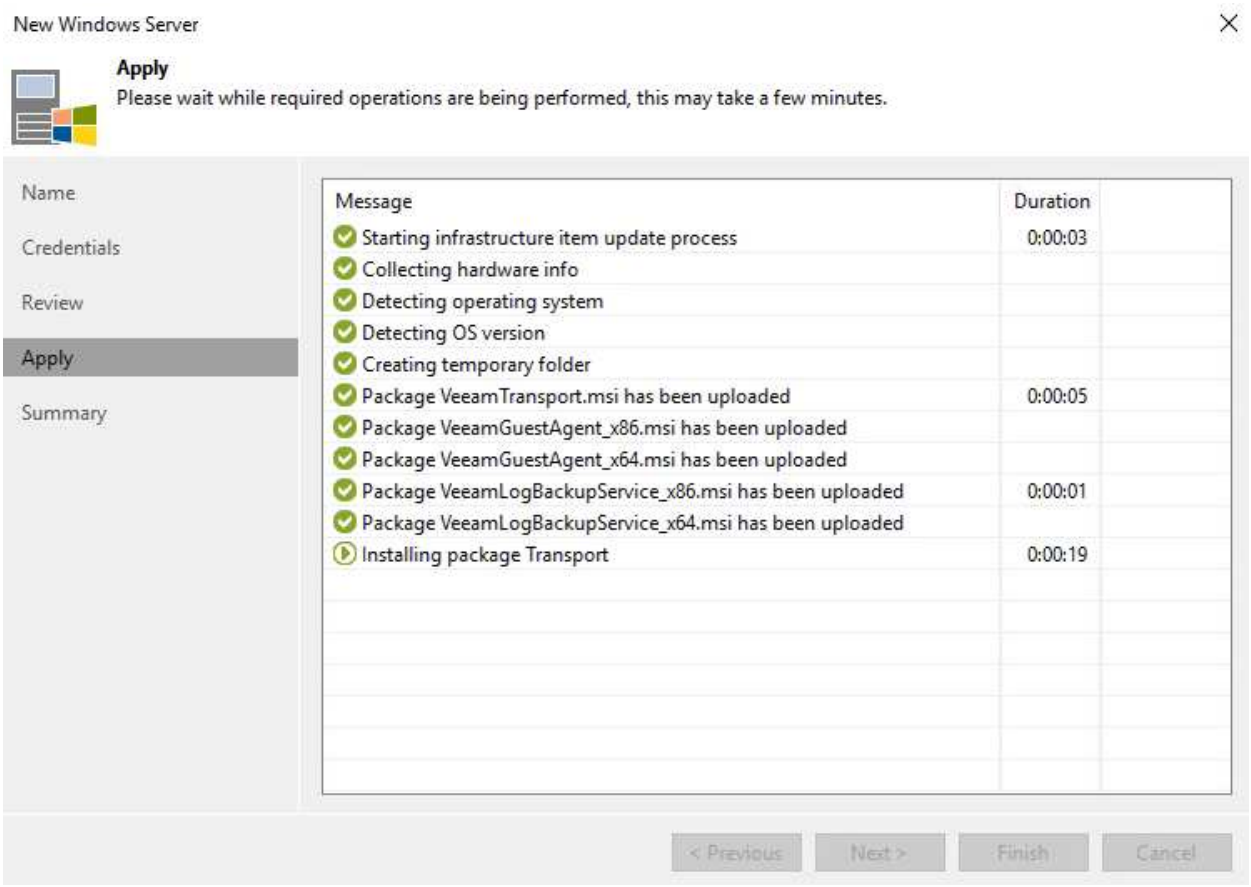
1. Öffnen Sie auf dem Veeam Backup and Replication-Server die Verwaltungskonsole und wählen Sie im Menü unten links **Backup Infrastructure** aus.
2. Klicken Sie mit der rechten Maustaste auf **Backup-Proxys** und klicken Sie auf **VMware-Backup-Proxy hinzufügen…**, um den Assistenten zu öffnen.



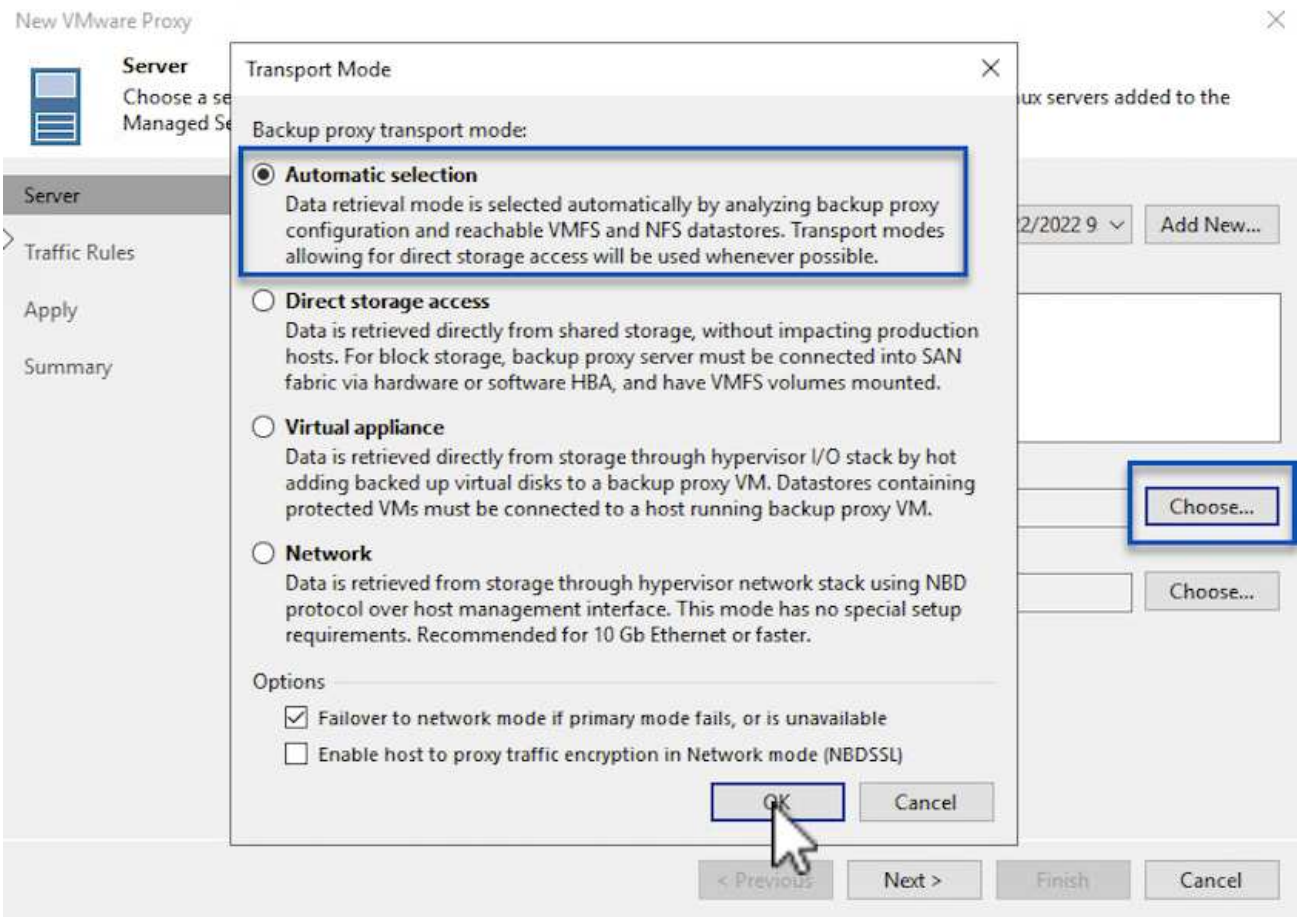
3. Klicken Sie im Assistenten **VMware-Proxy hinzufügen** auf die Schaltfläche **Neu hinzufügen…**, um einen neuen Proxyserver hinzuzufügen.



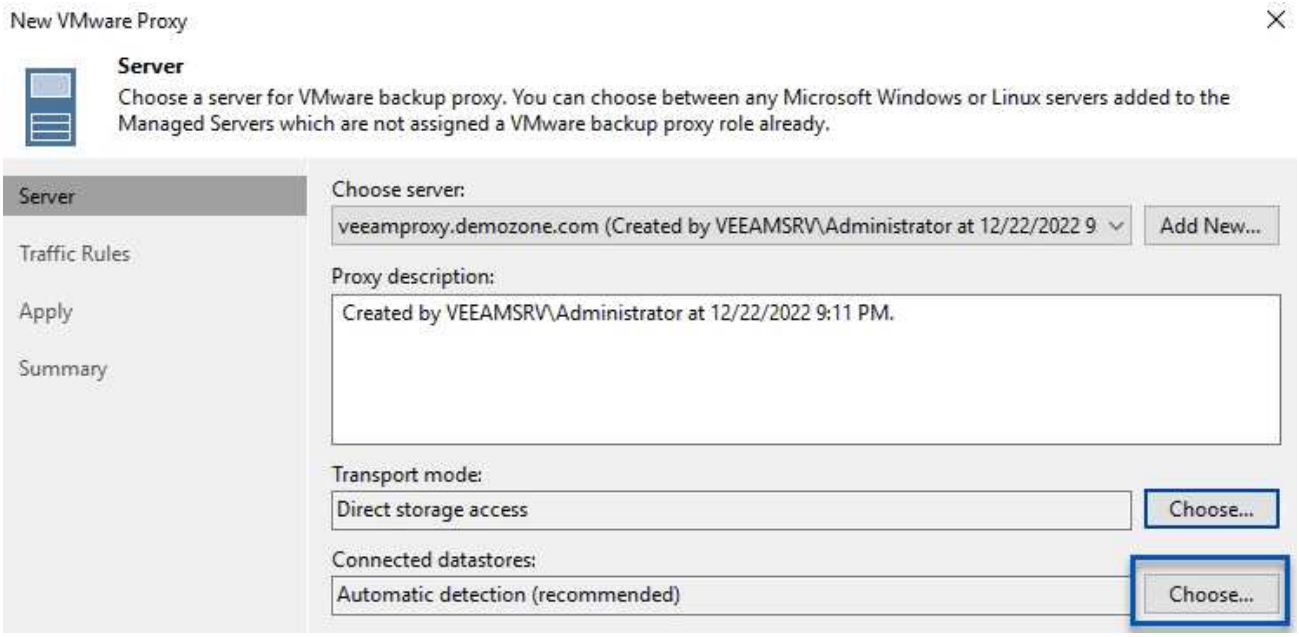
4. Wählen Sie „Microsoft Windows hinzufügen“ aus und folgen Sie den Anweisungen zum Hinzufügen des Servers:
   - Füllen Sie den DNS-Namen oder die IP-Adresse aus
   - Wählen Sie ein Konto für die Anmeldeinformationen auf dem neuen System aus oder fügen Sie neue Anmeldeinformationen hinzu
   - Überprüfen Sie die zu installierenden Komponenten und klicken Sie dann auf **Übernehmen**, um mit der Bereitstellung zu beginnen

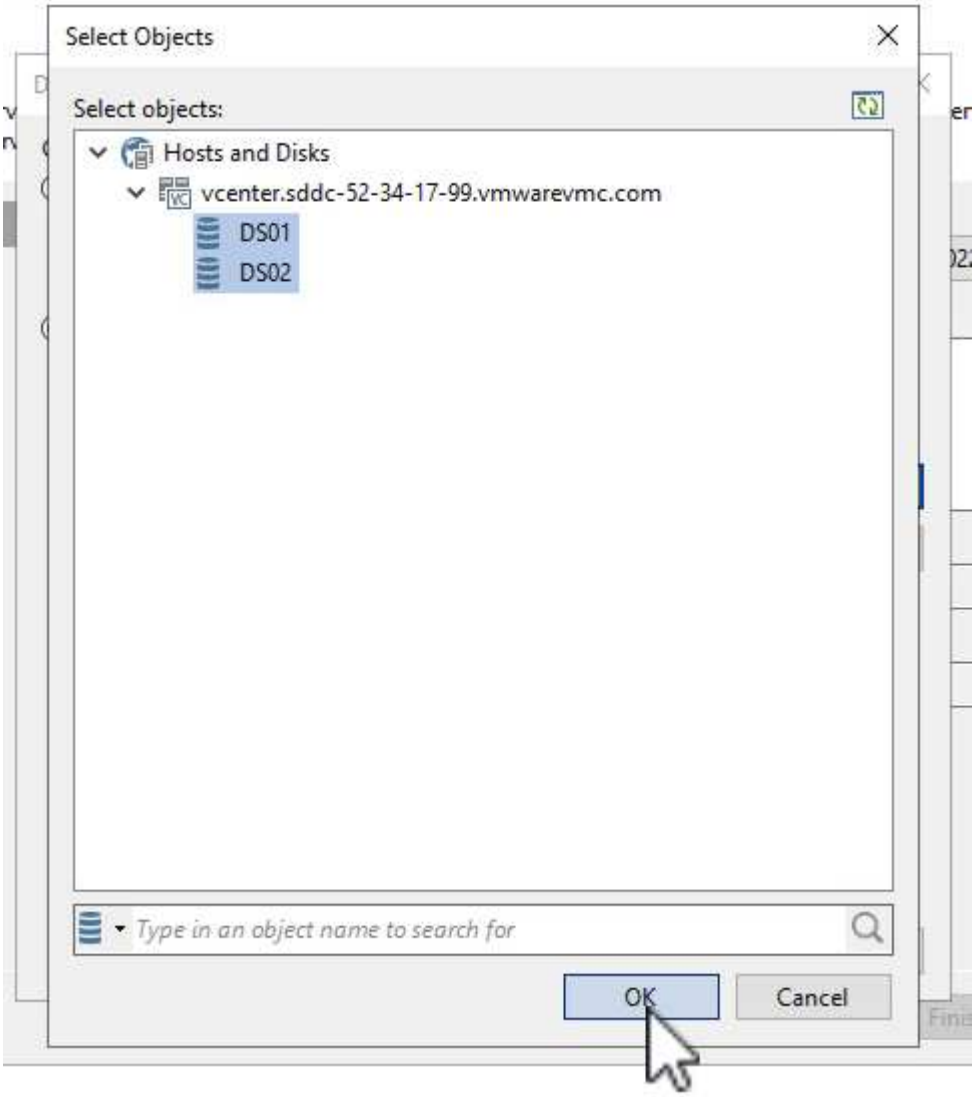


5. Wählen Sie im Assistenten **Neuer VMware-Proxy** einen Transportmodus aus. In unserem Fall haben wir **Automatische Auswahl** gewählt.

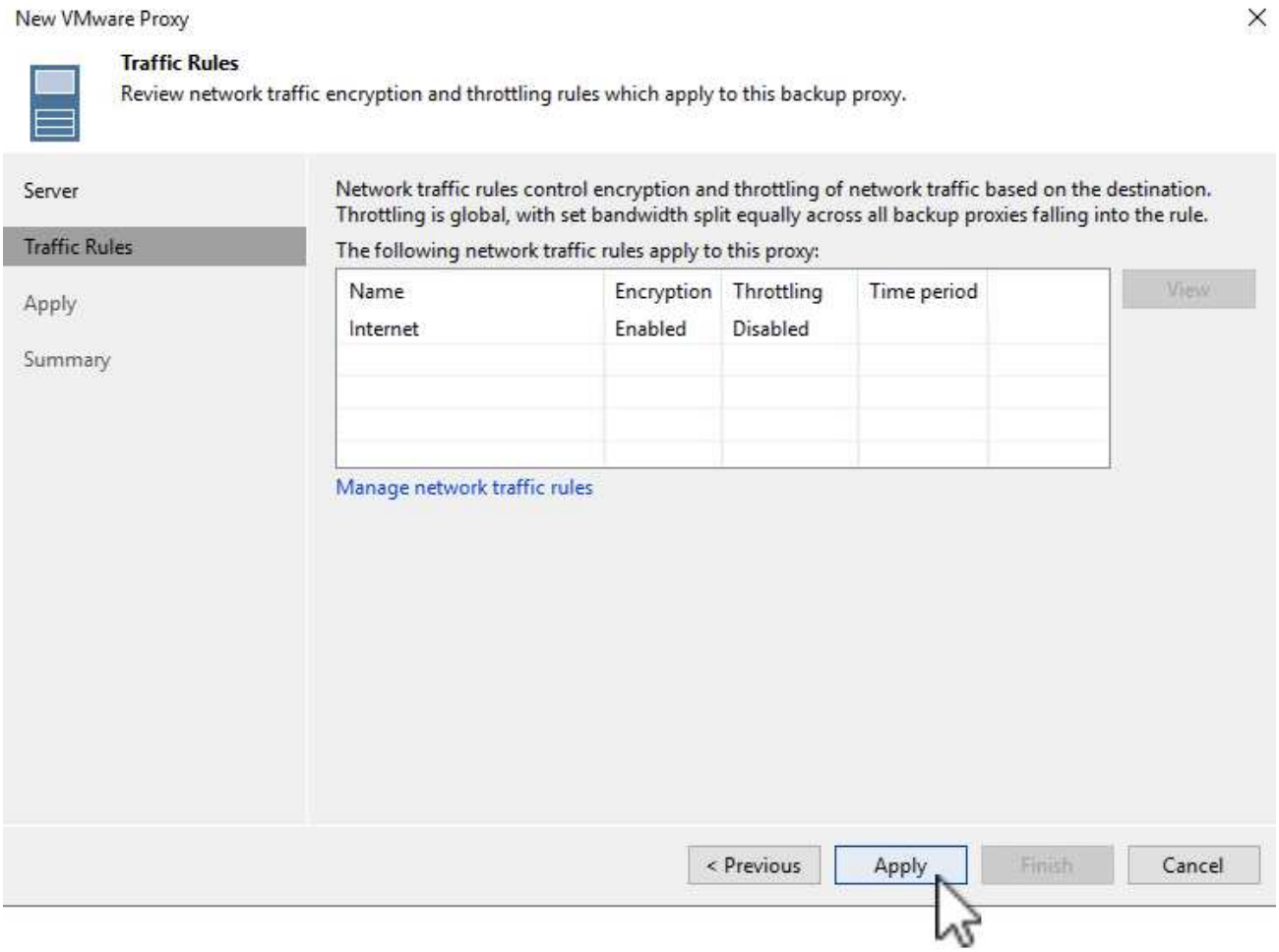


6. Wählen Sie die verbundenen Datenspeicher aus, auf die der VMware-Proxy direkten Zugriff haben soll.





7. Konfigurieren und wenden Sie alle gewünschten spezifischen Netzwerkverkehrsregeln wie Verschlüsselung oder Drosselung an. Wenn Sie fertig sind, klicken Sie auf die Schaltfläche **Übernehmen**, um die Bereitstellung abzuschließen.



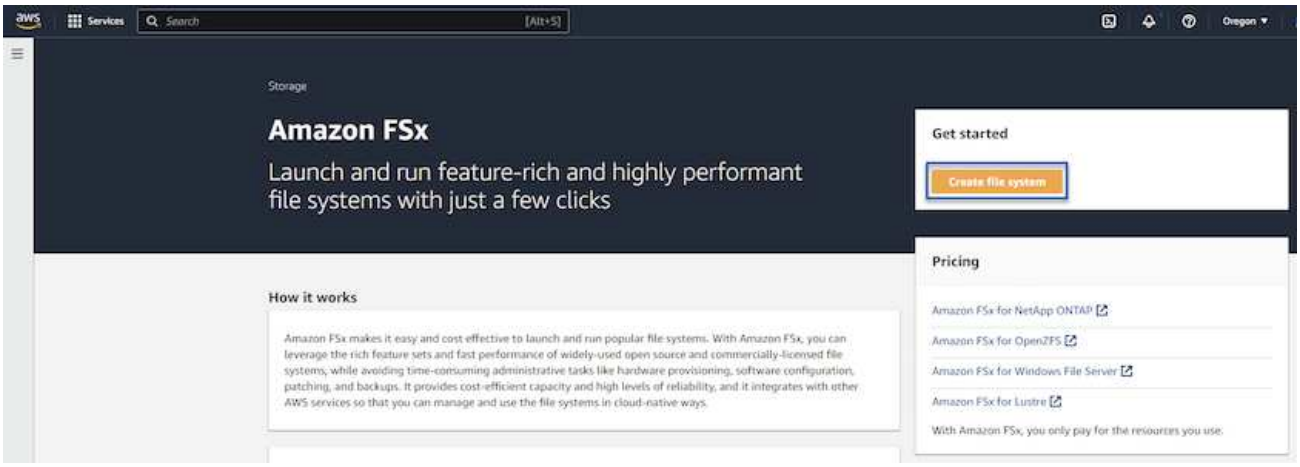
Konfigurieren von Speicher- und Sicherungsrepositorys

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 behandeln wir das Erstellen eines FSx ONTAP Dateisystems, das Mounten von iSCSI-LUNs auf den Veeam-Servern und das Erstellen von Backup-Repositorys.

▼ Erstellen Sie ein FSx ONTAP Dateisystem

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

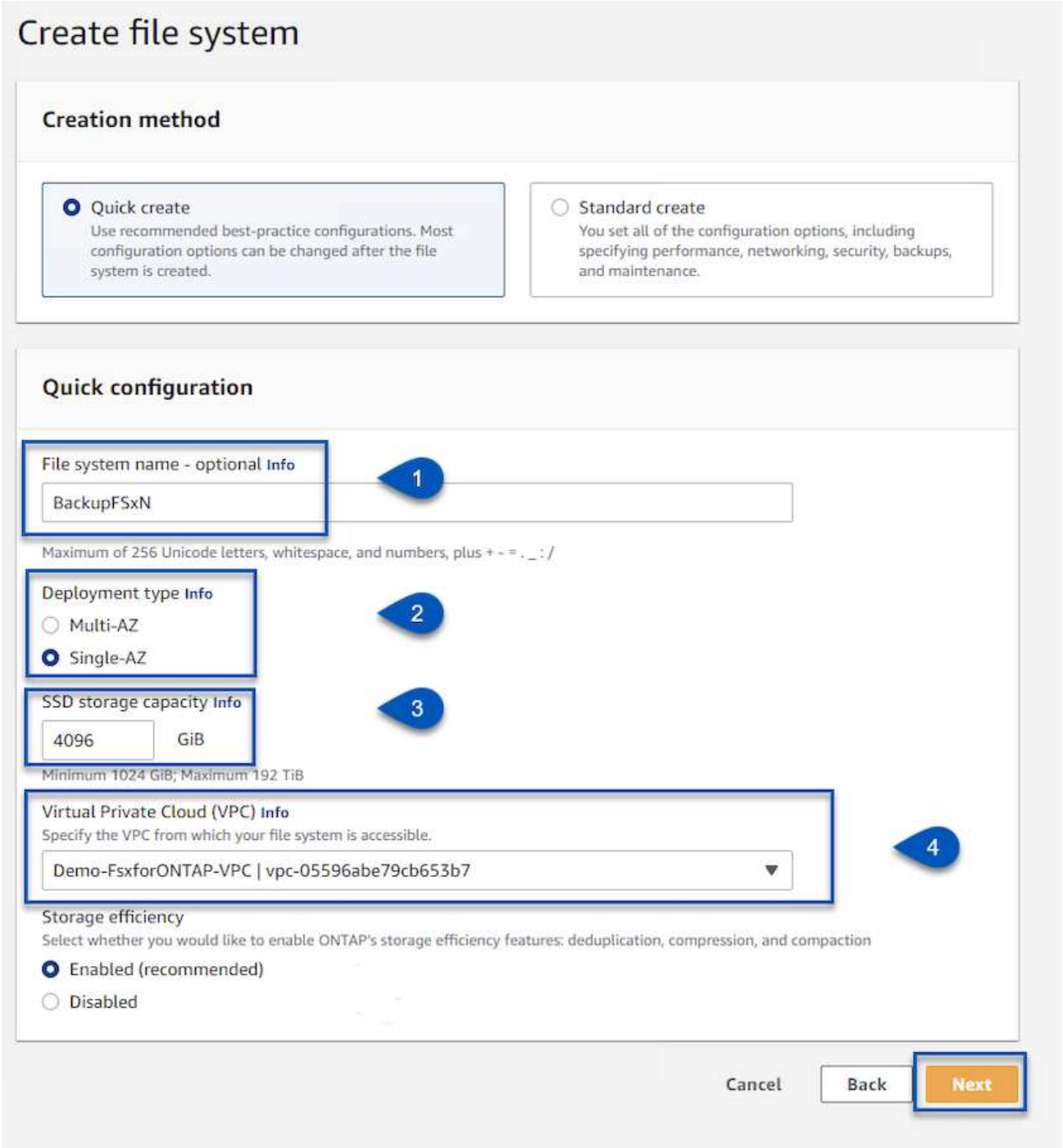
1. Gehen Sie in der AWS-Konsole zu FSx und dann zu **Dateisystem erstellen**



2. Wählen Sie * Amazon FSx ONTAP* und dann **Weiter**, um fortzufahren.



3. Geben Sie den Dateisystemnamen, den Bereitstellungstyp, die SSD-Speicherkapazität und die VPC ein, in der sich der FSx ONTAP Cluster befinden wird. Dies muss ein VPC sein, das für die Kommunikation mit dem virtuellen Maschinennetzwerk in VMware Cloud konfiguriert ist. Klicken Sie auf **Weiter**.



4. Überprüfen Sie die Bereitstellungsschritte und klicken Sie auf **Dateisystem erstellen**, um mit der Erstellung des Dateisystems zu beginnen.

▼ Konfigurieren und Mounten von iSCSI-LUNs

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

ⓘ Das Erstellen einer iSCSI-LUN auf FSx ONTAP ist ein mehrstufiger Prozess. Der erste Schritt zum Erstellen der Volumes kann in der Amazon FSx Konsole oder mit der NetApp ONTAP CLI durchgeführt werden.

Weitere Informationen zur Verwendung von FSx ONTAP finden Sie im "FSx ONTAP Benutzerhandbuch" .

1. Erstellen Sie über die NetApp ONTAP CLI die ersten 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 im vorherigen Schritt erstellten Volumes:

```
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:

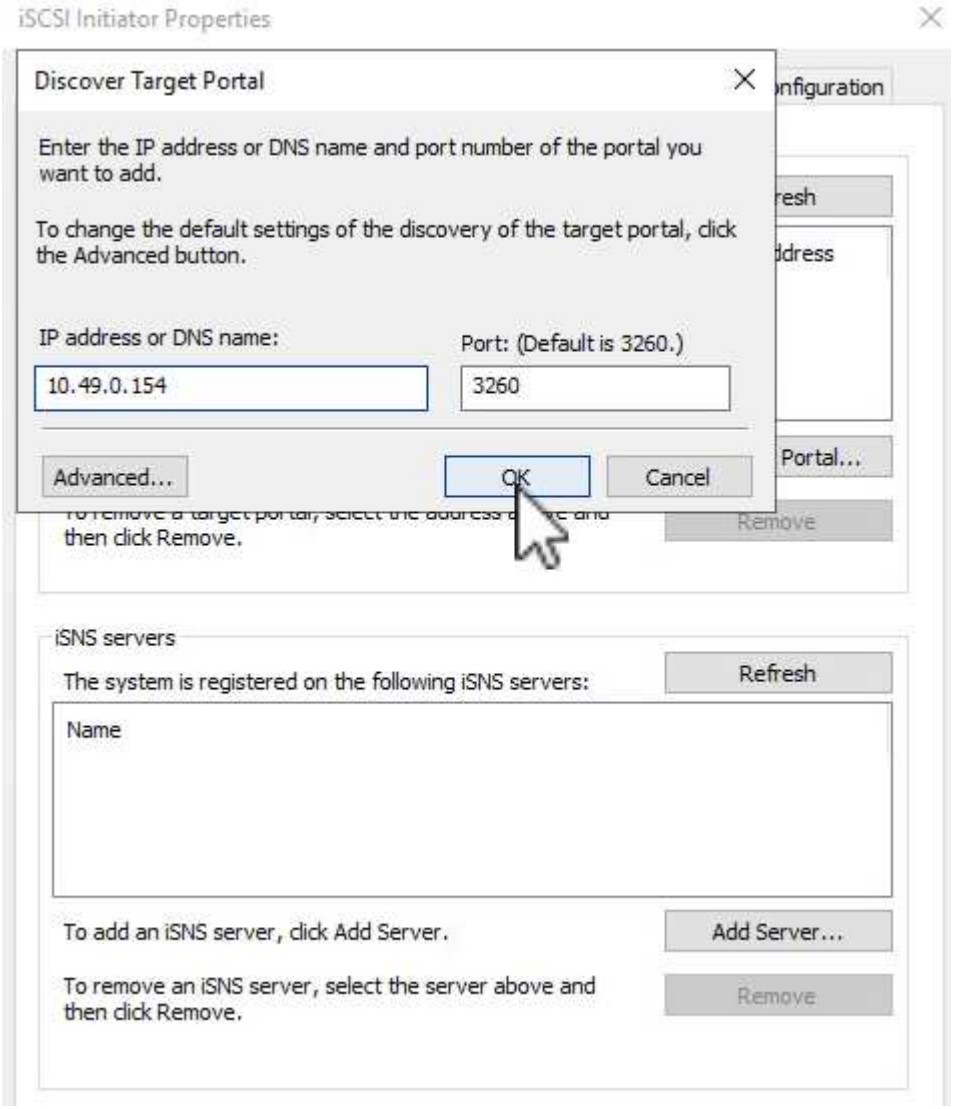
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

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

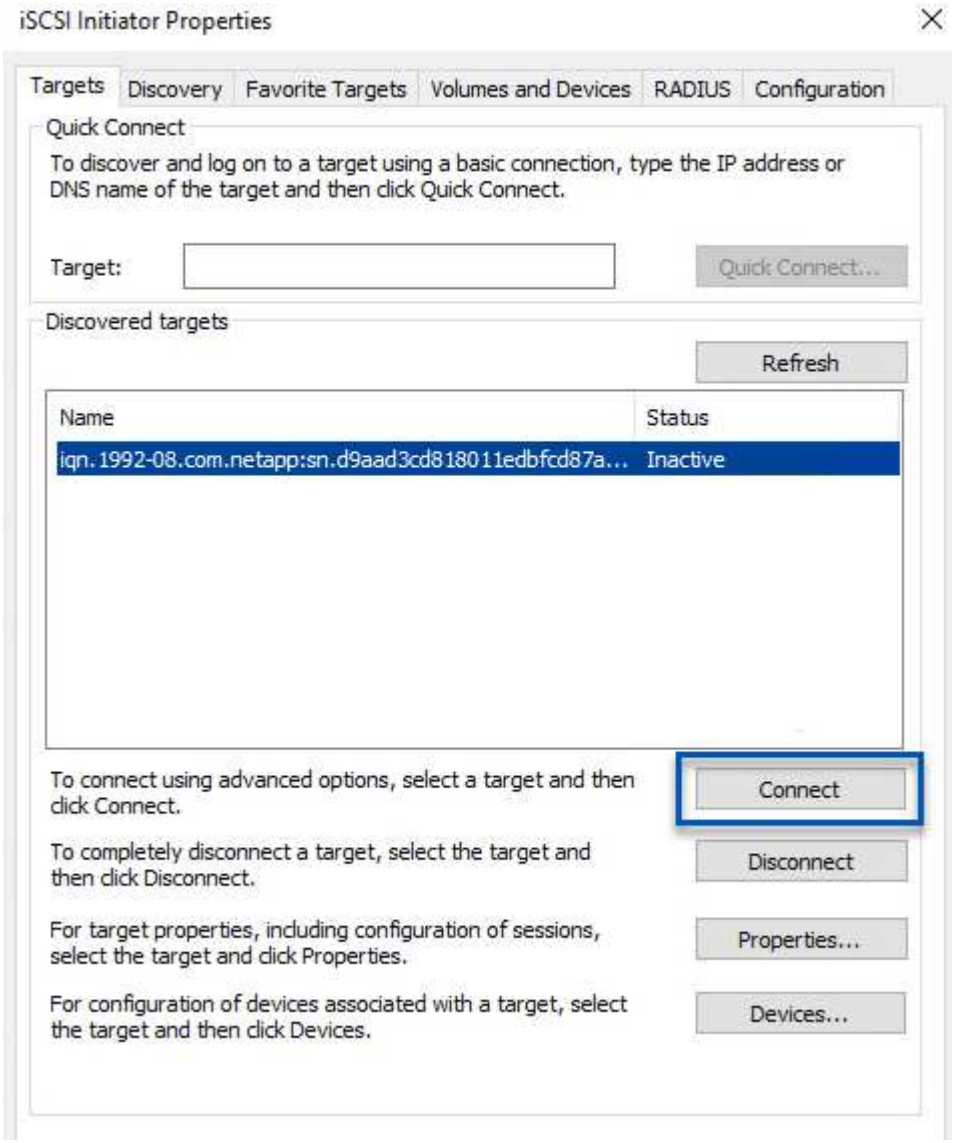
4. Ordnen Sie abschließend die LUNs der Initiatorgruppe zu, die Sie gerade erstellt haben:

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

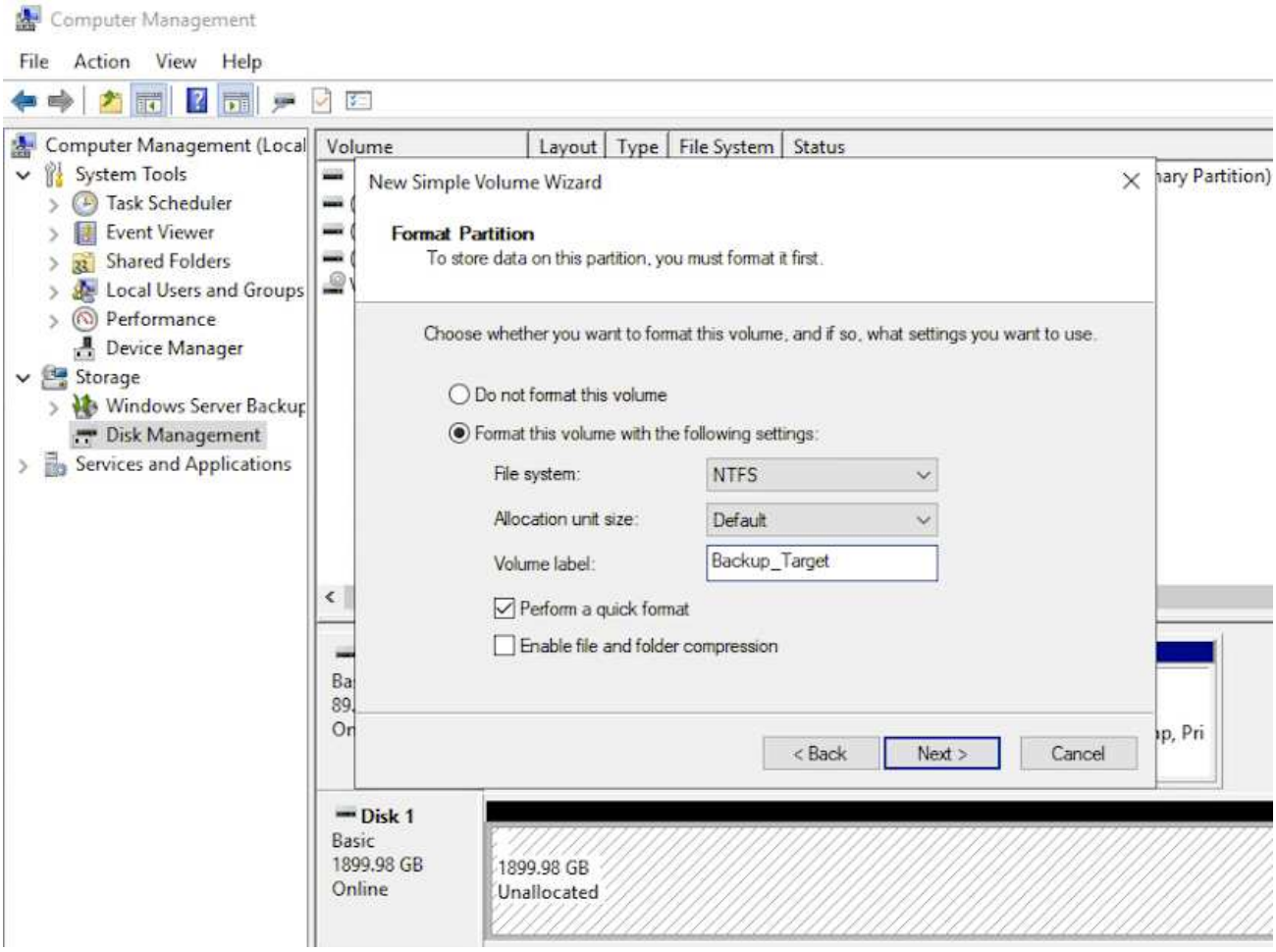
5. Um die iSCSI-LUNs zu mounten, melden Sie sich beim Veeam Backup & Replication Server an und öffnen Sie die iSCSI-Initiator-Eigenschaften. Gehen Sie zur Registerkarte **Erkennen** und geben Sie die IP-Adresse des iSCSI-Ziels ein.



6. Markieren Sie auf der Registerkarte **Ziele** die inaktive LUN und klicken Sie auf **Verbinden**. Aktivieren Sie das Kontrollkästchen **Multipfad aktivieren** und klicken Sie auf **OK**, um eine Verbindung mit der LUN herzustellen.



7. Initialisieren Sie im Dienstprogramm „Datenträgerverwaltung“ die neue LUN und erstellen Sie ein Volume mit dem gewünschten Namen und Laufwerksbuchstaben. Aktivieren Sie das Kontrollkästchen **Multipfad aktivieren** und klicken Sie auf **OK**, um eine Verbindung mit der LUN herzustellen.

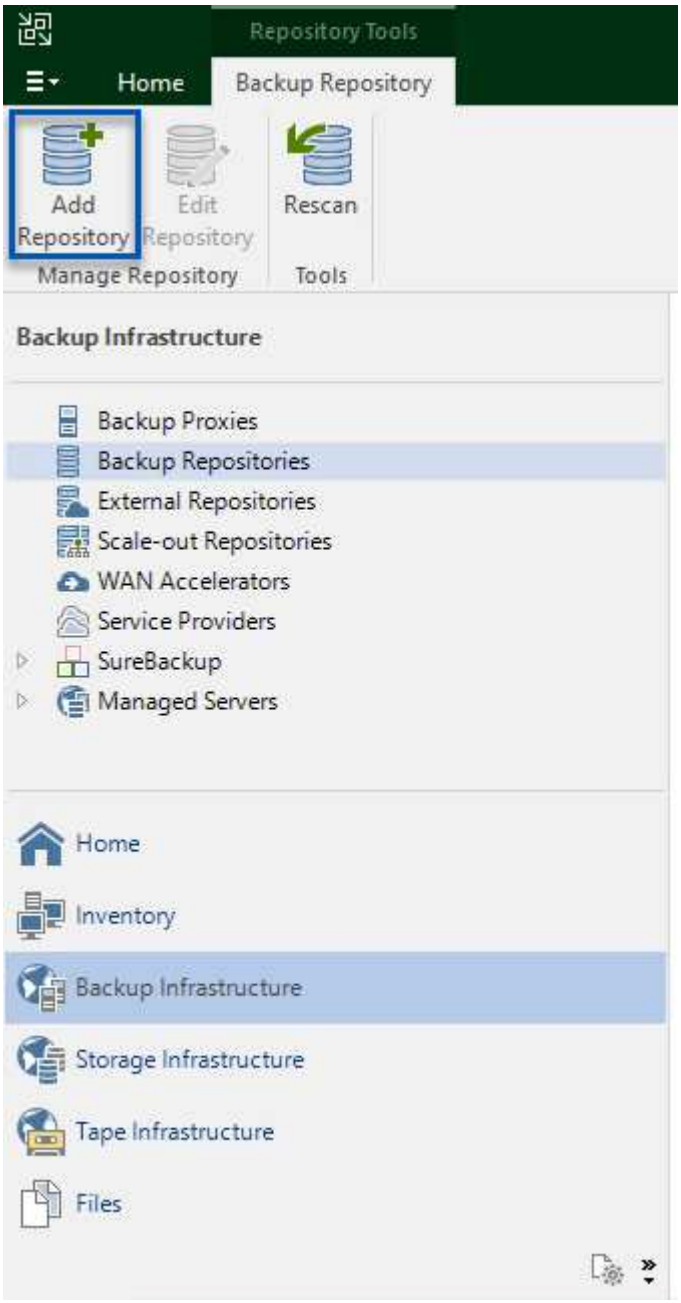


8. Wiederholen Sie diese Schritte, um die iSCSI-Volumes auf dem Veeam-Proxyserver zu mounten.

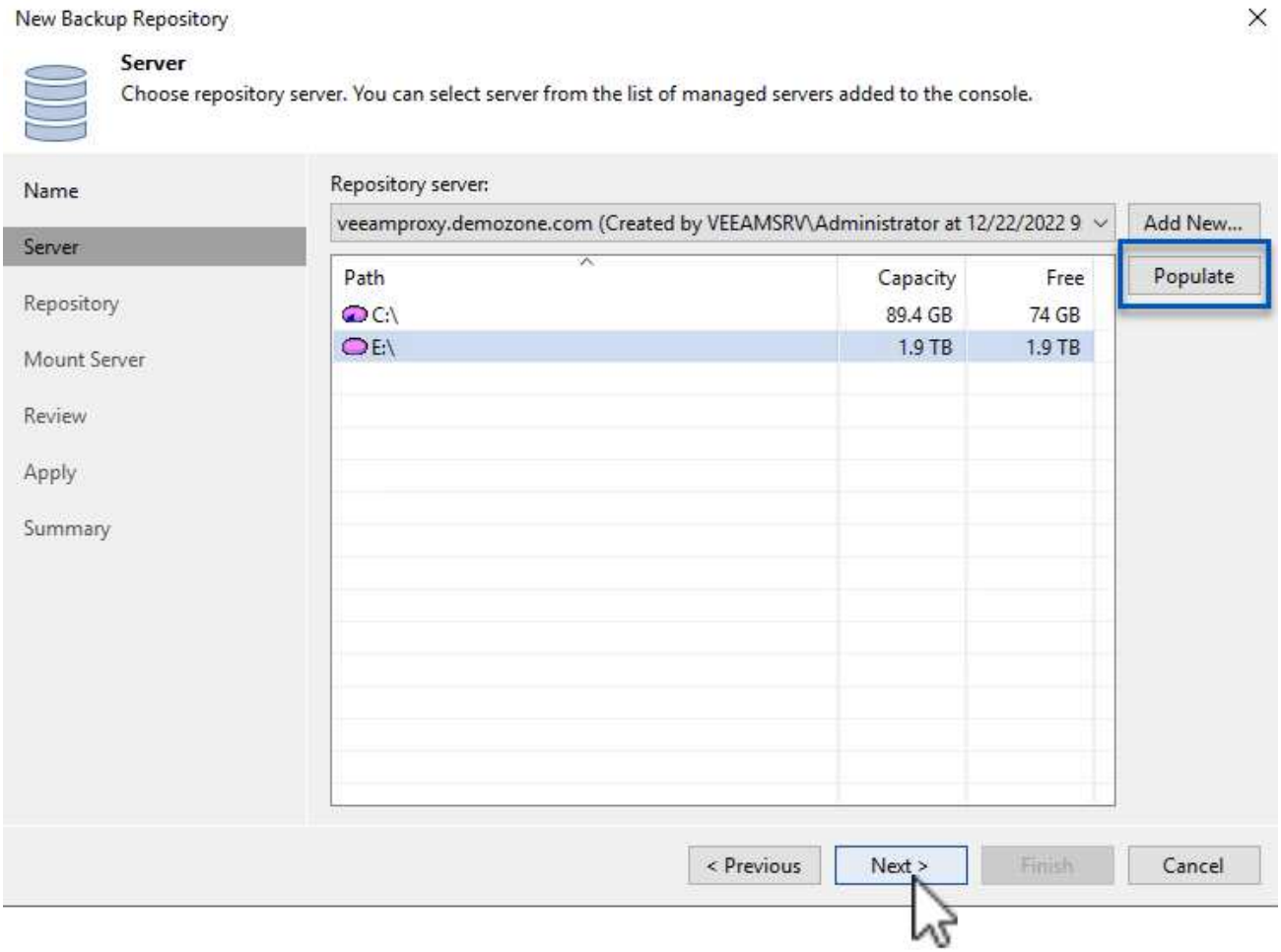
▼ **Erstellen Sie Veeam-Backup-Repositorys**

Erstellen Sie in der Veeam Backup and Replication-Konsole Sicherungsrepositorys für die Veeam Backup- und Veeam Proxy-Server. Diese Repositories werden als Sicherungsziele für die Sicherungen der virtuellen Maschinen verwendet.

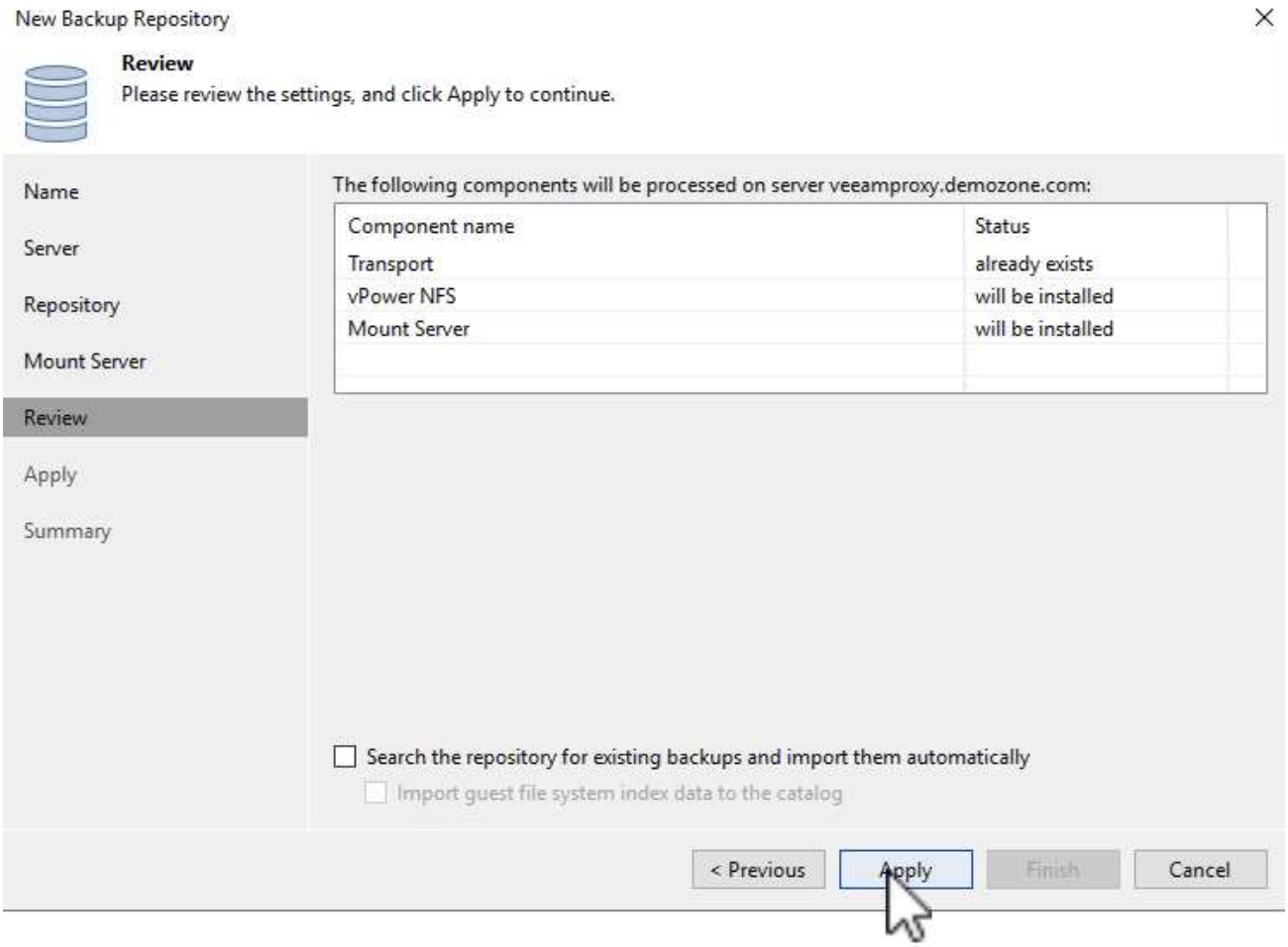
1. Klicken Sie in der Veeam Backup and Replication-Konsole unten links auf **Backup Infrastructure** und wählen Sie dann **Add Repository**



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



3. Wählen Sie auf der nächsten Seite einen Mount-Server aus, der zum Mounten von Backups bei der Durchführung erweiterter Wiederherstellungen verwendet wird. Standardmäßig ist dies derselbe Server, mit dem der Repository-Speicher verbunden ist.
4. Überprüfen Sie Ihre Auswahl und klicken Sie auf **Übernehmen**, um mit der Erstellung des Sicherungsrepositorys zu beginnen.



5. Wiederholen Sie diese Schritte für alle weiteren Proxyserver.

Konfigurieren von Veeam-Sicherungsaufträgen

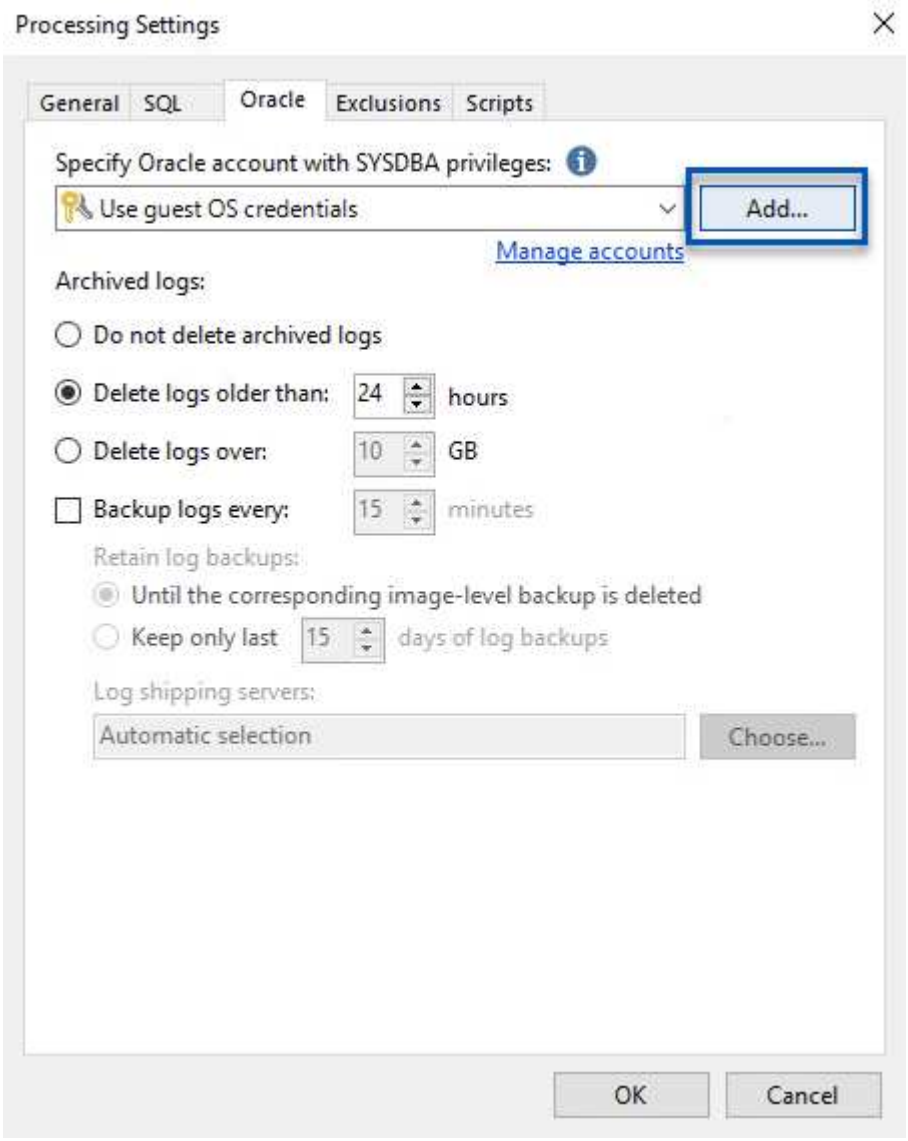
Sicherungsaufträge sollten unter Verwendung der Sicherungsrepositorys im vorherigen Abschnitt erstellt werden. Das Erstellen von Sicherungsaufträgen gehört zum normalen Repertoire eines jeden Speicheradministrators und wir behandeln hier nicht alle Schritte. Ausführlichere Informationen zum Erstellen von Sicherungsaufträgen in Veeam finden Sie im "Veeam Help Center Technische Dokumentation" .

In dieser Lösung wurden separate Sicherungsaufträge erstellt für:

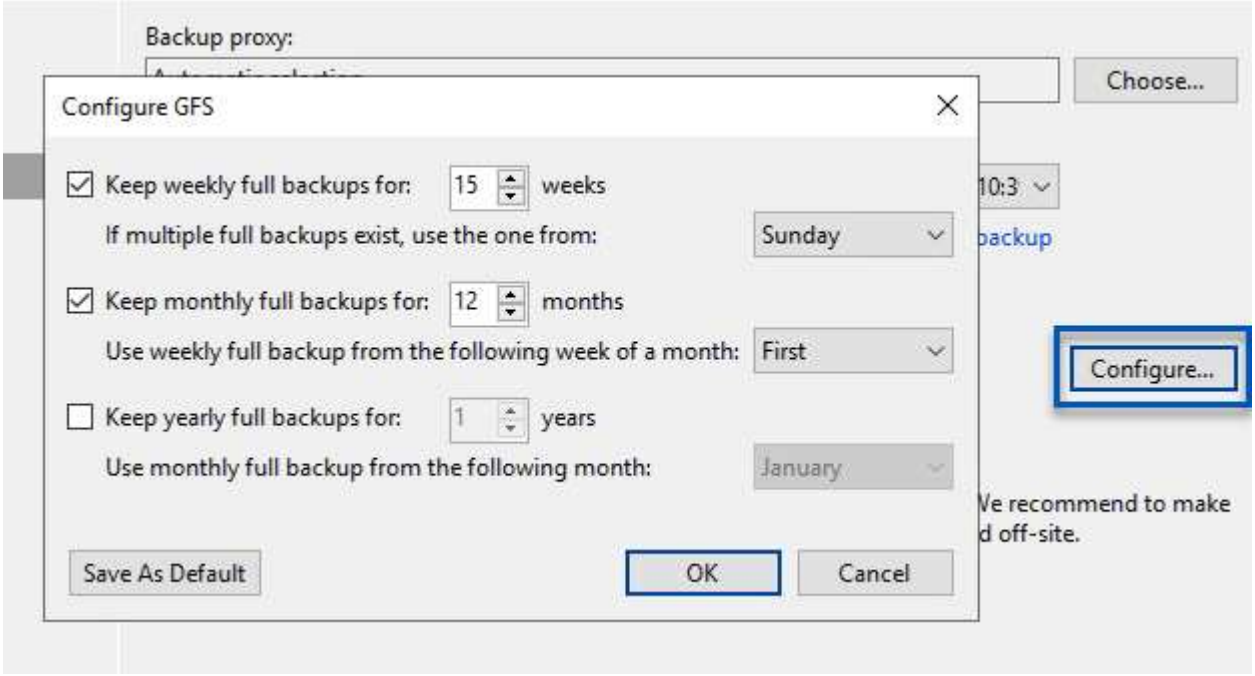
- Microsoft Windows SQL Server
- Oracle-Datenbankserver
- Windows-Dateiserver
- Linux-Dateiserver

▼ Allgemeine Überlegungen zur Konfiguration von Veeam-Sicherungsjobs

1. Aktivieren Sie die anwendungsbewusste Verarbeitung, um konsistente Sicherungen zu erstellen und die Transaktionsprotokollverarbeitung durchzuführen.
2. Fügen Sie nach der Aktivierung der anwendungsbewussten Verarbeitung die richtigen Anmeldeinformationen mit Administratorrechten zur Anwendung hinzu, da diese sich von den Anmeldeinformationen des Gastbetriebssystems unterscheiden können.



3. Um die Aufbewahrungsrichtlinie für die Sicherung zu verwalten, aktivieren Sie **Bestimmte vollständige Sicherungen zu Archivierungszwecken länger aufbewahren** und klicken Sie auf die Schaltfläche **Konfigurieren…**, um die Richtlinie zu konfigurieren.



Wiederherstellen von Anwendungs-VMs mit der vollständigen Wiederherstellung von Veeam

Die Durchführung einer vollständigen Wiederherstellung mit Veeam ist der erste Schritt bei der Wiederherstellung einer Anwendung. Wir haben überprüft, dass die vollständige Wiederherstellung unserer VMs aktiviert war und alle Dienste normal ausgeführt wurden.

Das Wiederherstellen von Servern gehört zum normalen Repertoire eines jeden Speicheradministrators und wir behandeln hier nicht alle Schritte. Ausführlichere Informationen zur Durchführung vollständiger Wiederherstellungen in Veeam finden Sie im "Veeam Help Center Technische Dokumentation" .

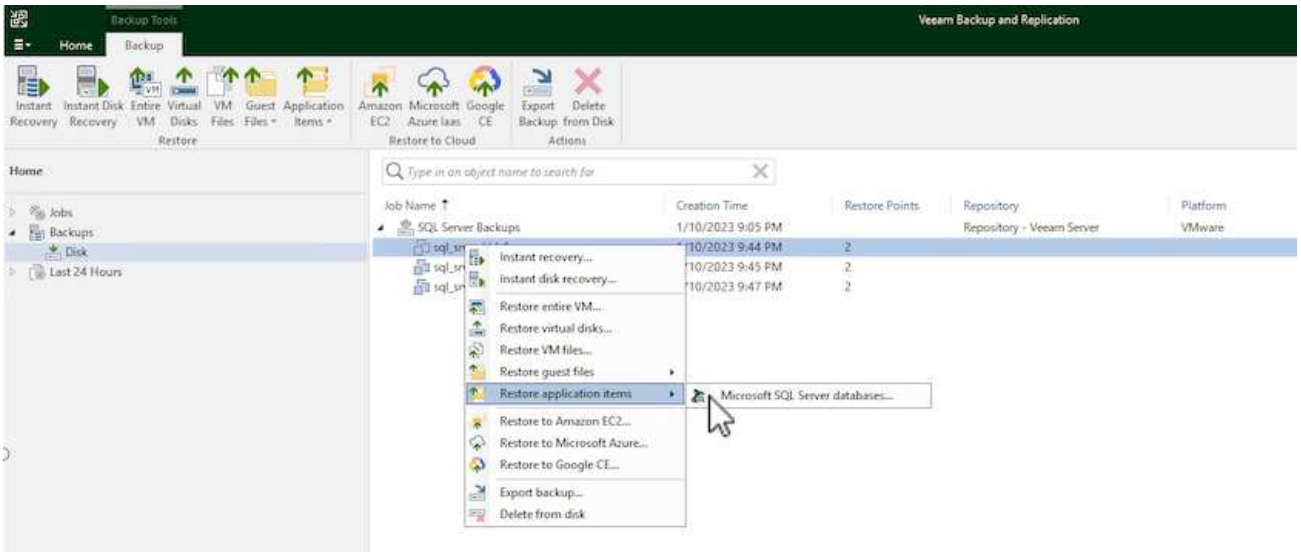
Wiederherstellen von SQL Server-Datenbanken

Veeam Backup & Replication bietet mehrere Optionen zum Wiederherstellen von SQL Server-Datenbanken. Für diese Validierung haben wir den Veeam Explorer für SQL Server mit Instant Recovery verwendet, um Wiederherstellungen unserer SQL Server-Datenbanken durchzuführen. SQL Server Instant Recovery ist eine Funktion, mit der Sie SQL Server-Datenbanken schnell wiederherstellen können, ohne auf eine vollständige Datenbankwiederherstellung warten zu müssen. Dieser schnelle Wiederherstellungsprozess minimiert Ausfallzeiten und gewährleistet die Geschäftskontinuität. So funktioniert es:

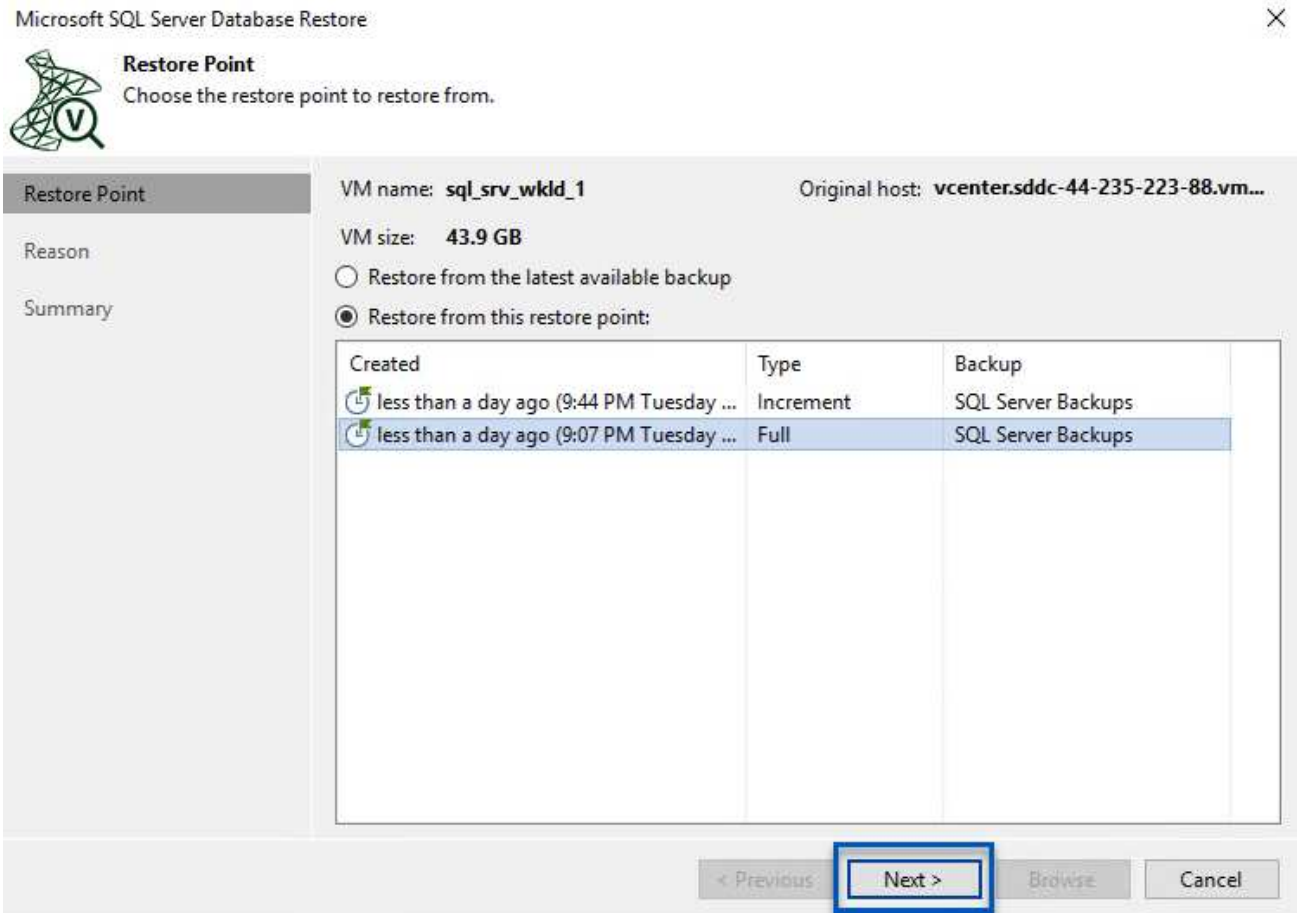
- Veeam Explorer **mountet das Backup**, das die wiederherzustellende SQL Server-Datenbank enthält.
- Die Software **veröffentlicht die Datenbank** direkt aus den bereitgestellten Dateien und macht sie als temporäre Datenbank auf der Ziel-SQL-Server-Instanz zugänglich.
- Während die temporäre Datenbank verwendet wird, leitet Veeam Explorer Benutzerabfragen an diese Datenbank um und stellt so sicher, 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 Datenbankspeicherort.
- Sobald die vollständige Datenbankwiederherstellung abgeschlossen ist, **schaltet Veeam Explorer Benutzerabfragen zurück auf die ursprüngliche** Datenbank und entfernt die temporäre Datenbank.

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

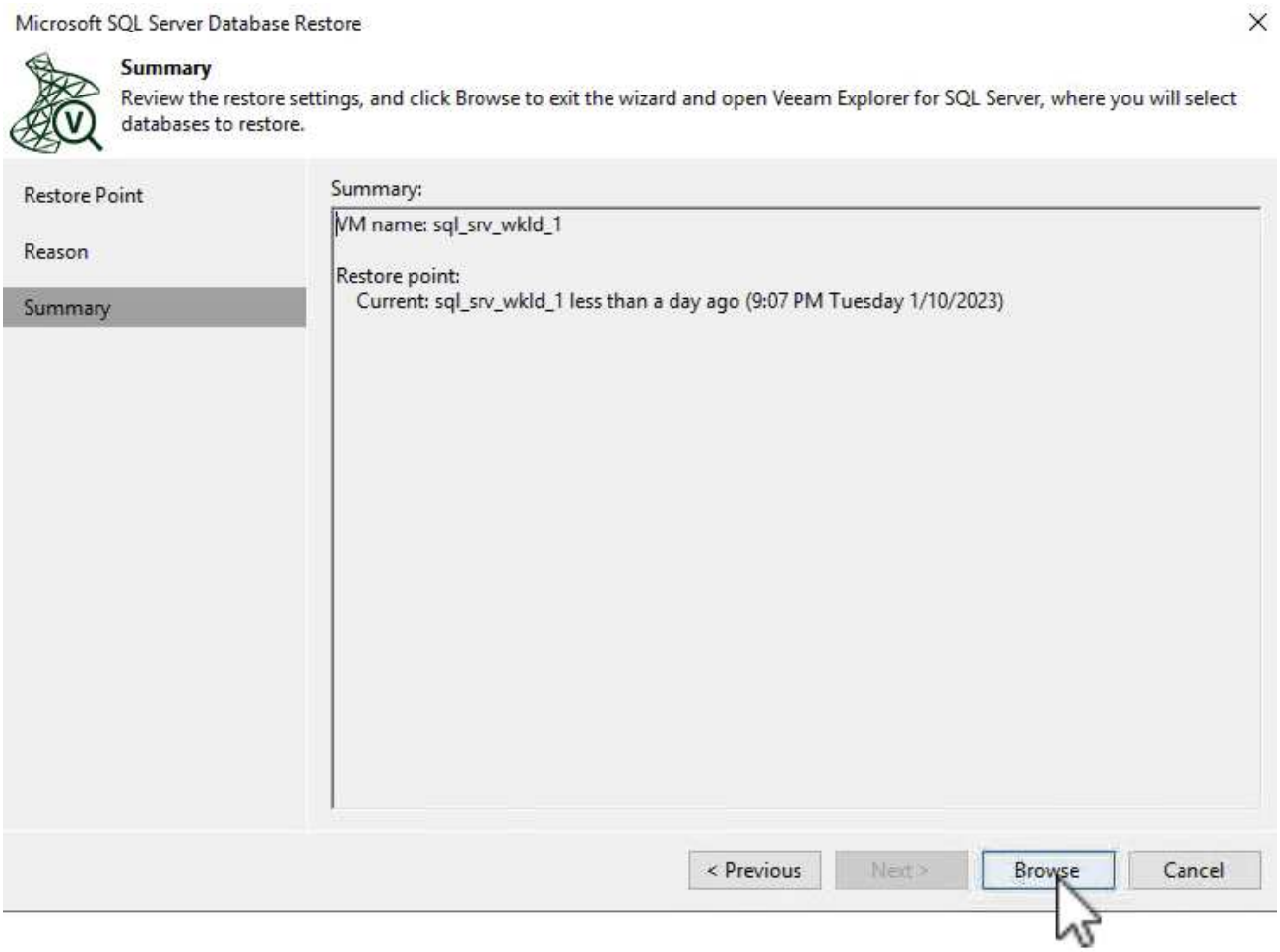
1. Navigieren Sie in der Veeam Backup and Replication-Konsole zur Liste der SQL Server-Backups, klicken Sie mit der rechten Maustaste auf einen Server und wählen Sie **Anwendungselemente wiederherstellen** und dann **Microsoft SQL Server-Datenbanken…**.



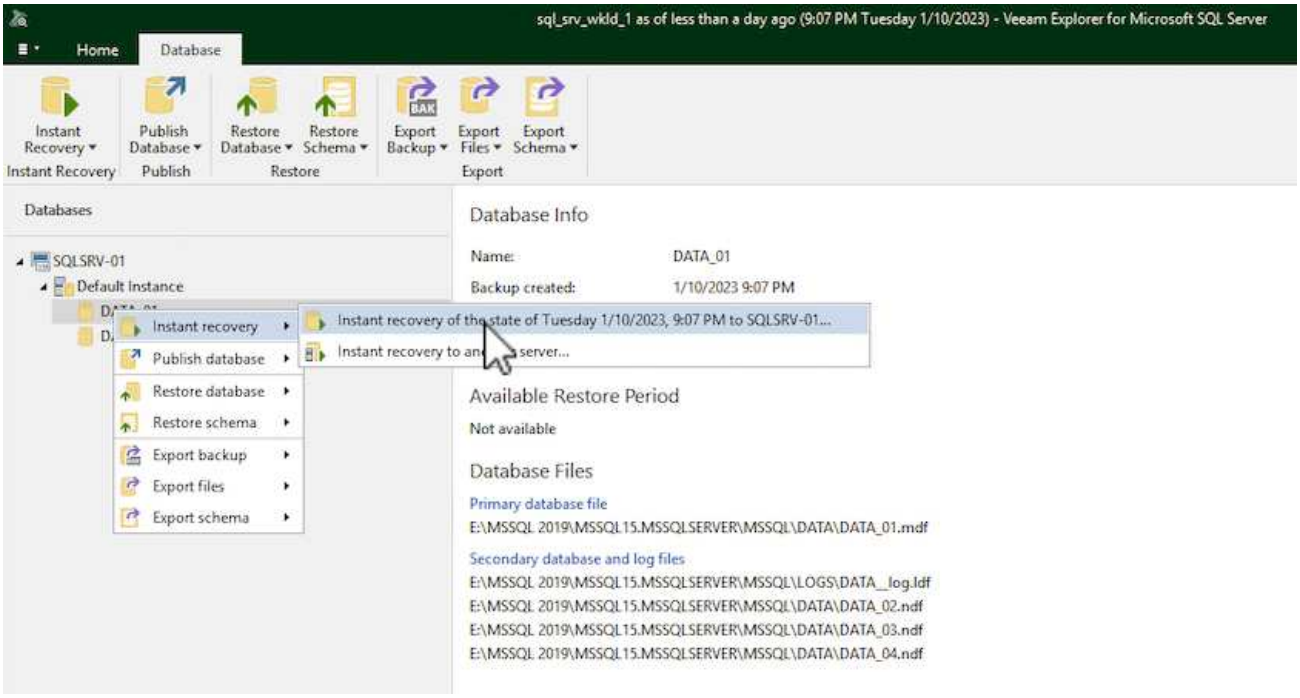
2. Wählen Sie im Assistenten zur Wiederherstellung der Microsoft SQL Server-Datenbank einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.



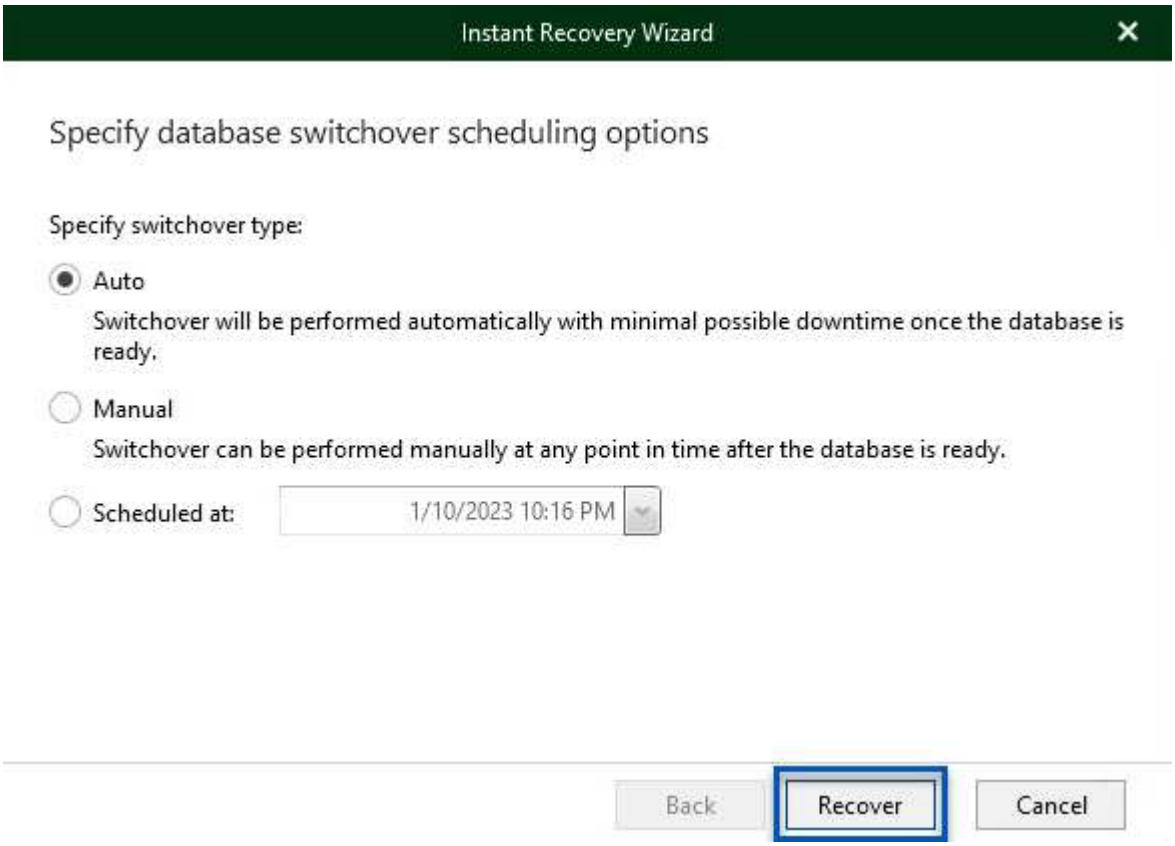
3. Geben Sie bei Bedarf einen **Wiederherstellungsgrund** ein und klicken Sie dann auf der Seite „Zusammenfassung“ auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Microsoft SQL Server zu starten.



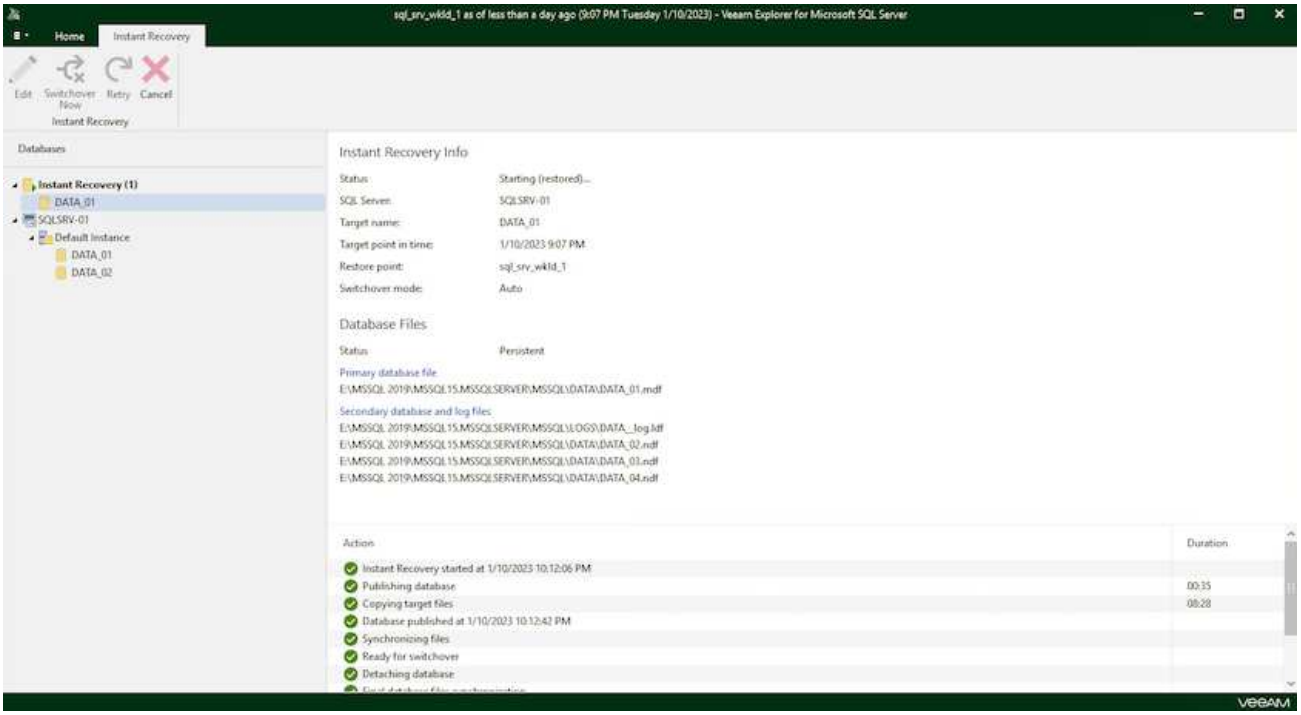
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie mit der rechten Maustaste und wählen Sie **Sofortige Wiederherstellung** und dann den spezifischen Wiederherstellungspunkt, zu dem die Wiederherstellung erfolgen soll.



5. Geben Sie im Instant Recovery-Assistenten den Switchover-Typ an. Dies kann entweder automatisch mit minimaler Ausfallzeit, manuell oder zu einem festgelegten Zeitpunkt erfolgen. Klicken Sie dann auf die Schaltfläche **Wiederherstellen**, um den Wiederherstellungsvorgang zu starten.



6. Der Wiederherstellungsprozess kann vom Veeam Explorer aus überwacht werden.



Ausführlichere Informationen zum Durchführen von SQL Server-Wiederherstellungsvorgängen mit Veeam

Explorer finden Sie im Abschnitt „Microsoft SQL Server“ im "Veeam Explorers-Benutzerhandbuch" .

Wiederherstellen von Oracle-Datenbanken mit Veeam Explorer

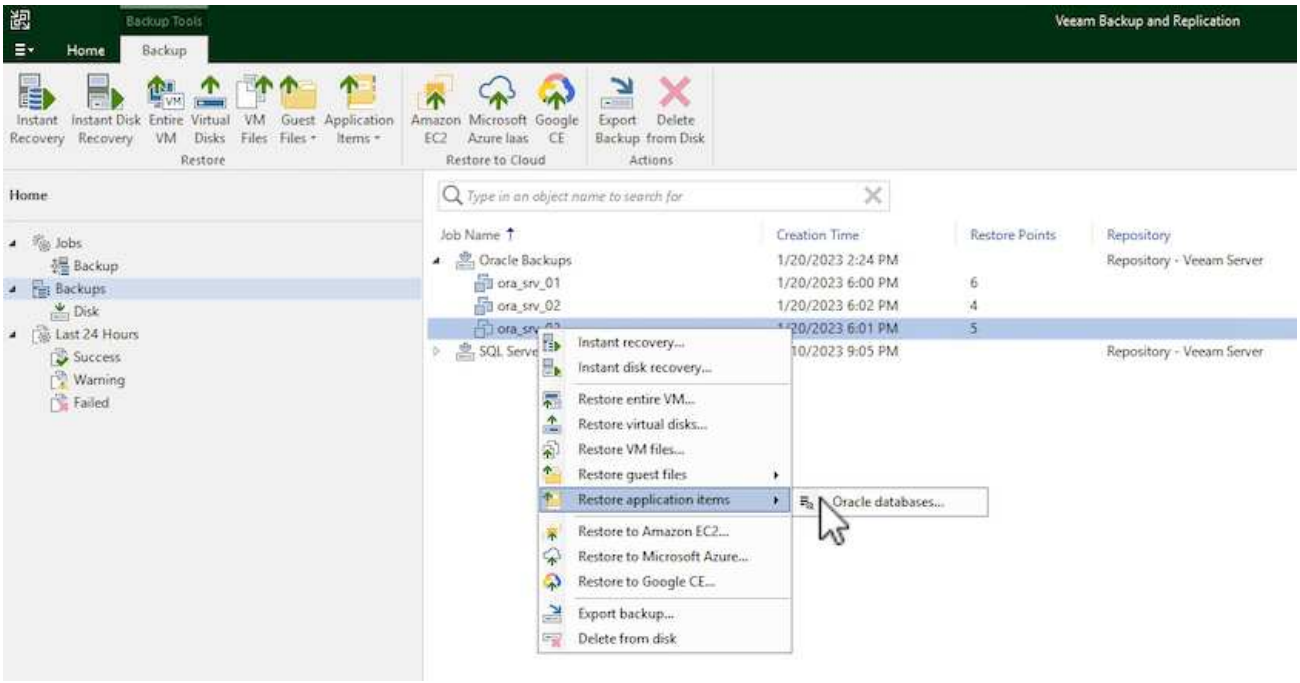
Veeam Explorer für Oracle-Datenbanken bietet die Möglichkeit, eine Standardwiederherstellung der Oracle-Datenbank oder eine unterbrechungsfreie Wiederherstellung mithilfe von Instant Recovery durchzuführen. Es unterstützt auch die Veröffentlichung von Datenbanken für schnellen Zugriff, die Wiederherstellung von Data Guard-Datenbanken und die Wiederherstellung aus RMAN-Backups.

Ausführlichere Informationen zum Durchführen von Oracle-Datenbankwiederherstellungsvorgängen mit Veeam Explorer finden Sie im Abschnitt „Oracle“ im "Veeam Explorers-Benutzerhandbuch" .

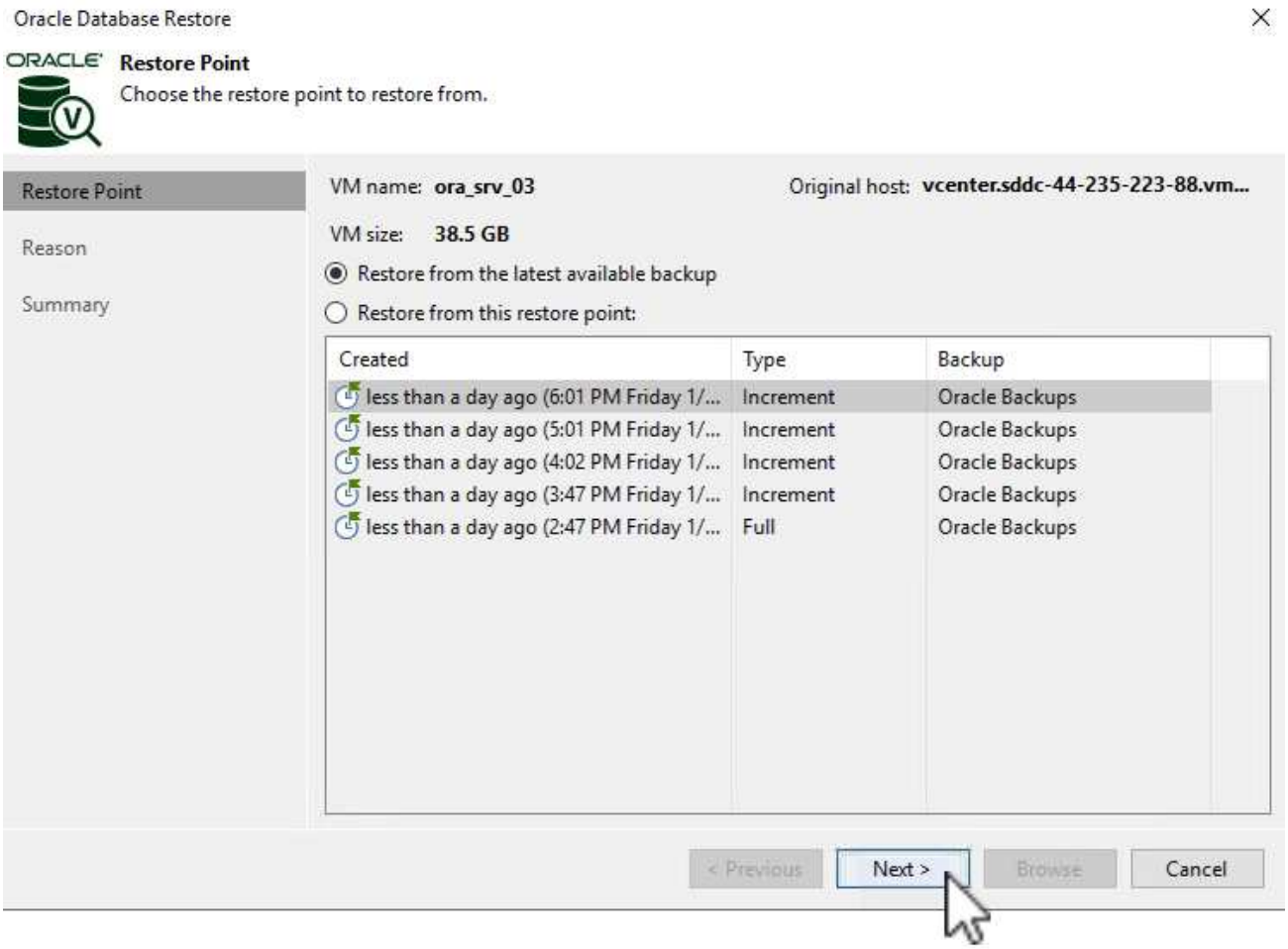
▼ **Stellen Sie die Oracle-Datenbank mit Veeam Explorer wieder her**

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

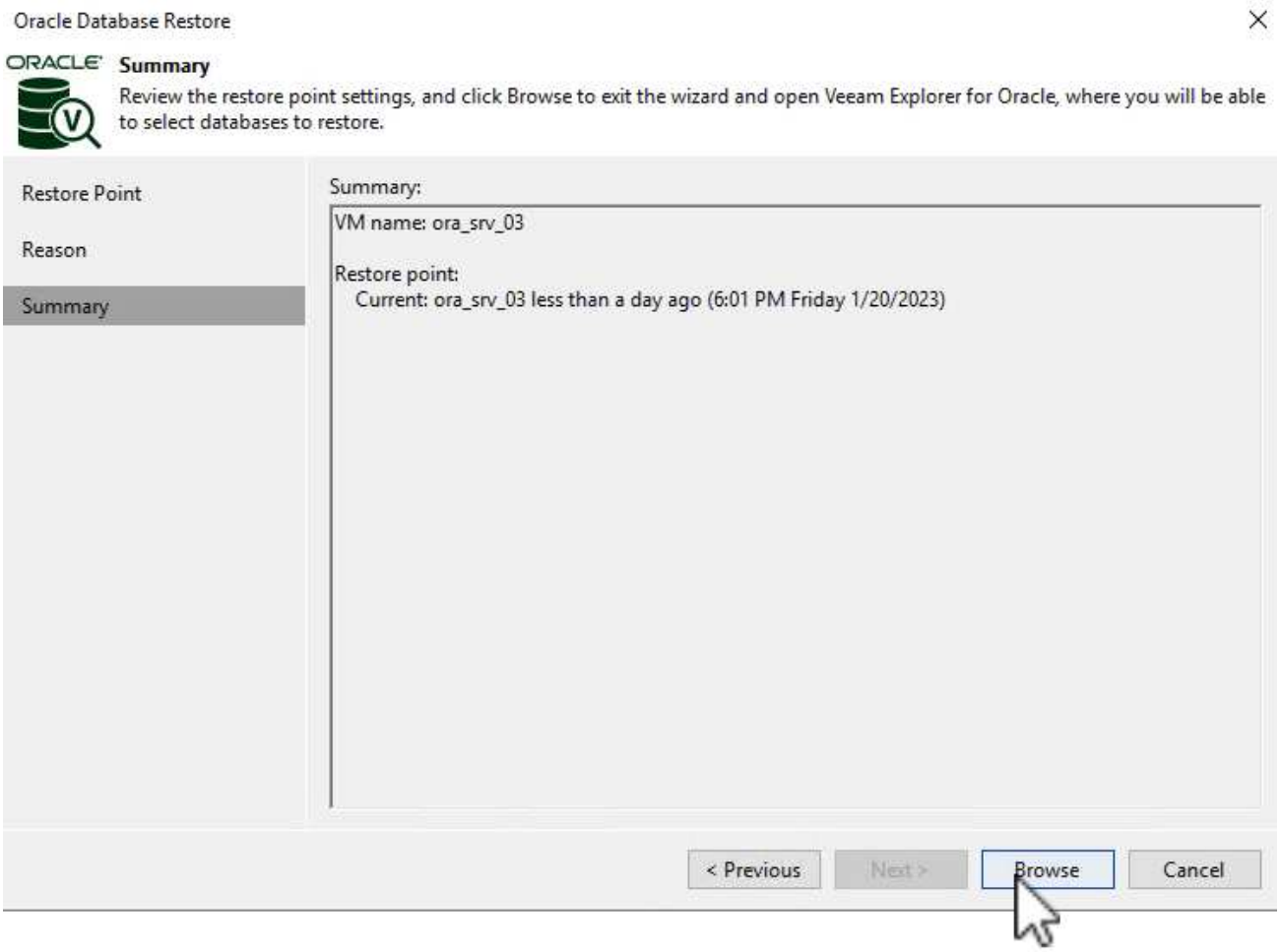
1. Navigieren Sie in der Veeam Backup and Replication-Konsole zur Liste der Oracle-Backups, klicken Sie mit der rechten Maustaste auf einen Server und wählen Sie **Anwendungselemente wiederherstellen** und dann **Oracle-Datenbanken…**.



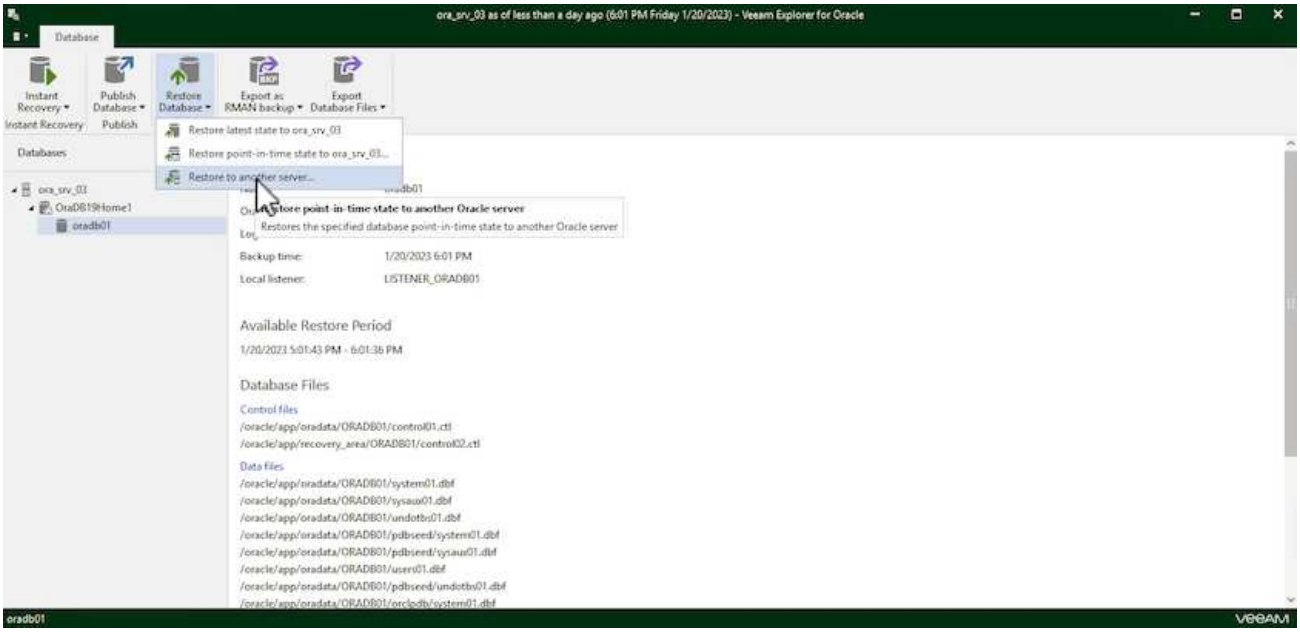
2. Wählen Sie im Oracle Database Restore Wizard einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.



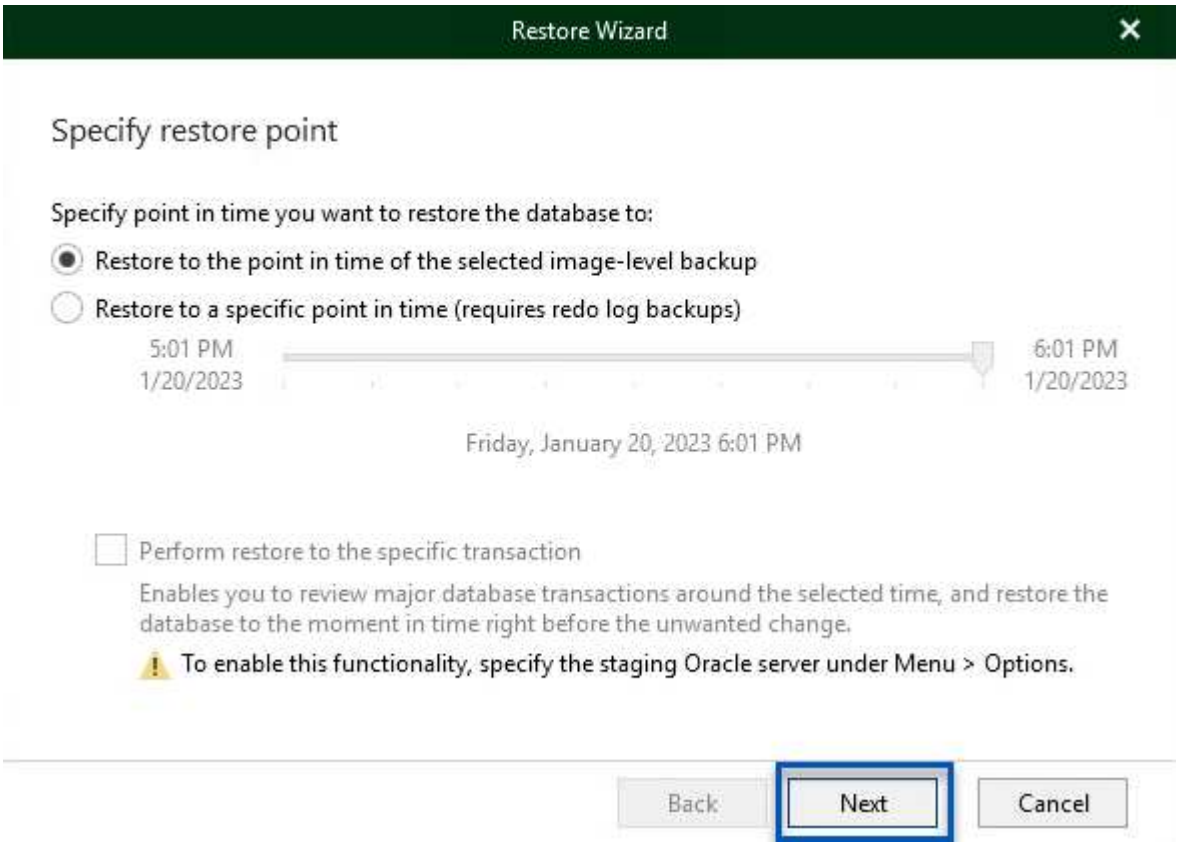
3. Geben Sie bei Bedarf einen **Wiederherstellungsgrund** ein und klicken Sie dann auf der Seite „Zusammenfassung“ auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Oracle zu starten.



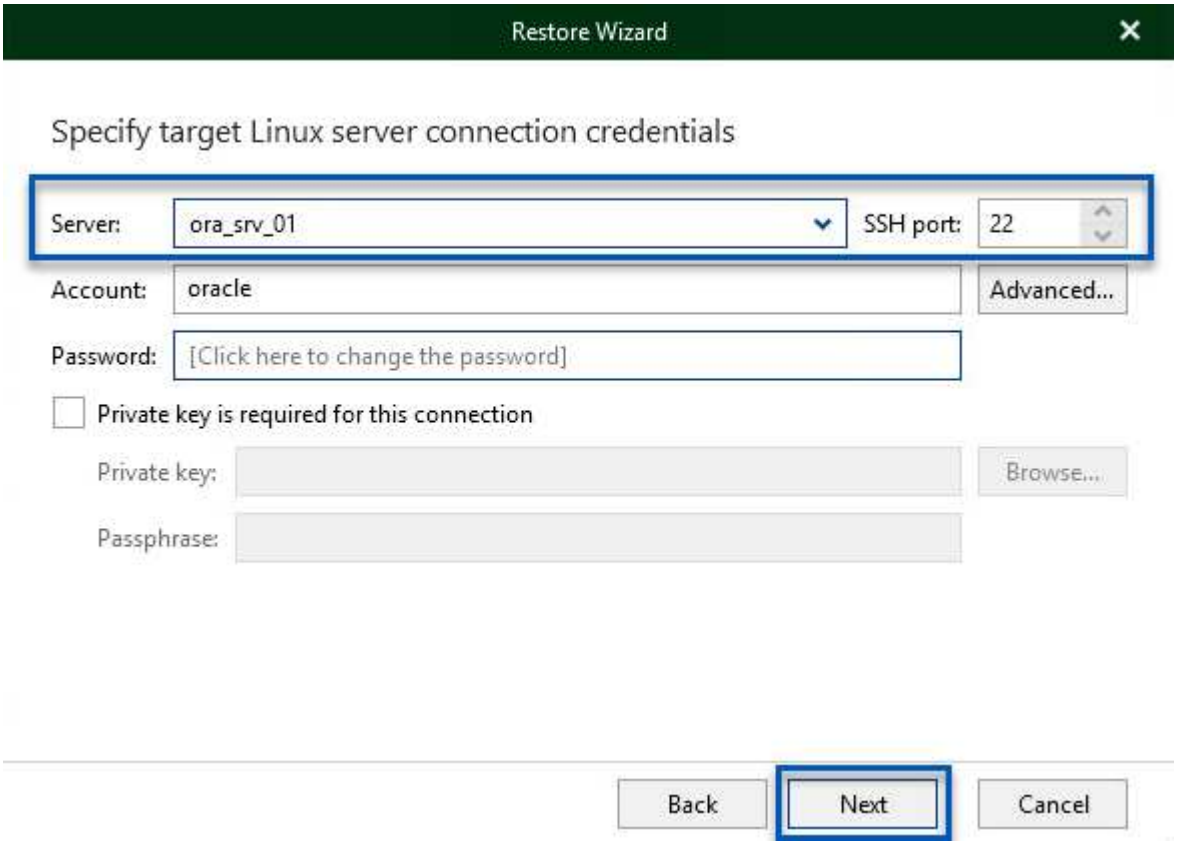
4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie auf die wiederherzustellende Datenbank und wählen Sie dann oben im Dropdown-Menü **Datenbank wiederherstellen** die Option **Auf einem anderen Server wiederherstellen…**.



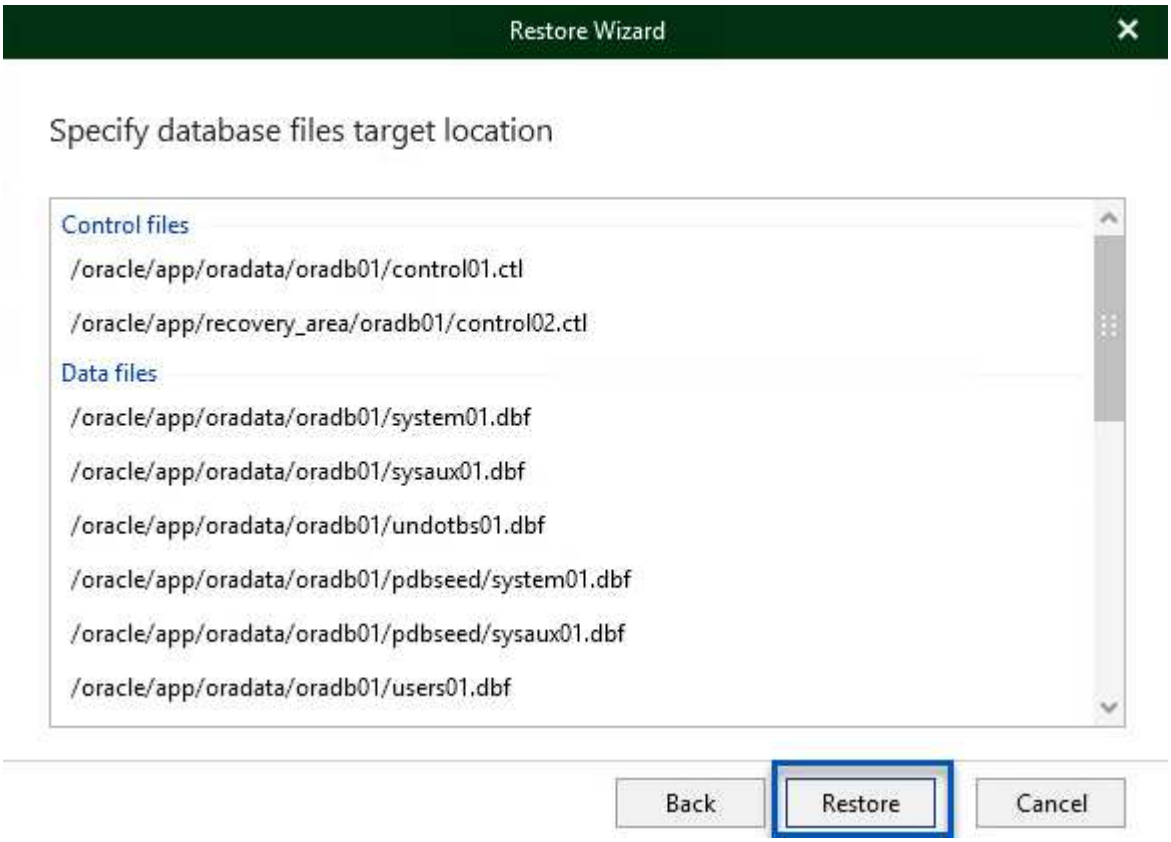
5. Geben Sie im Wiederherstellungsassistenten den Wiederherstellungspunkt an, von dem aus die Wiederherstellung erfolgen soll, und klicken Sie auf **Weiter**.



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



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

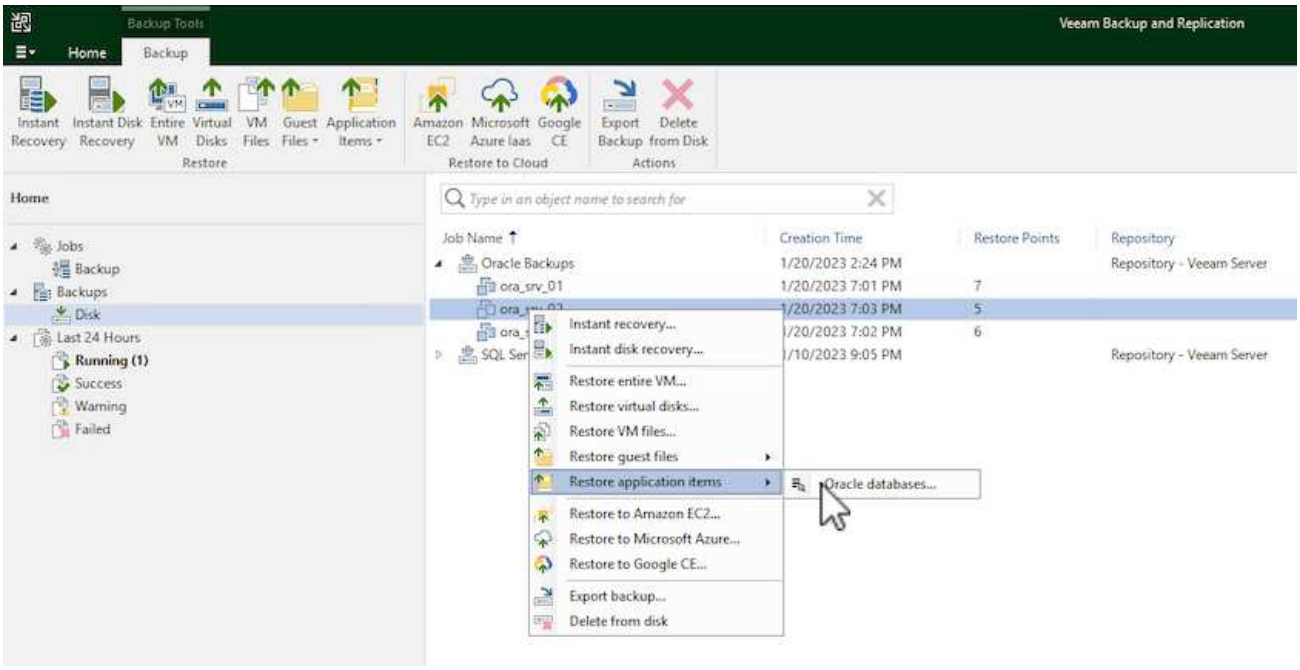


8. Überprüfen Sie nach Abschluss der Datenbankwiederherstellung, ob die Oracle-Datenbank auf dem Server ordnungsgemäß gestartet wird.

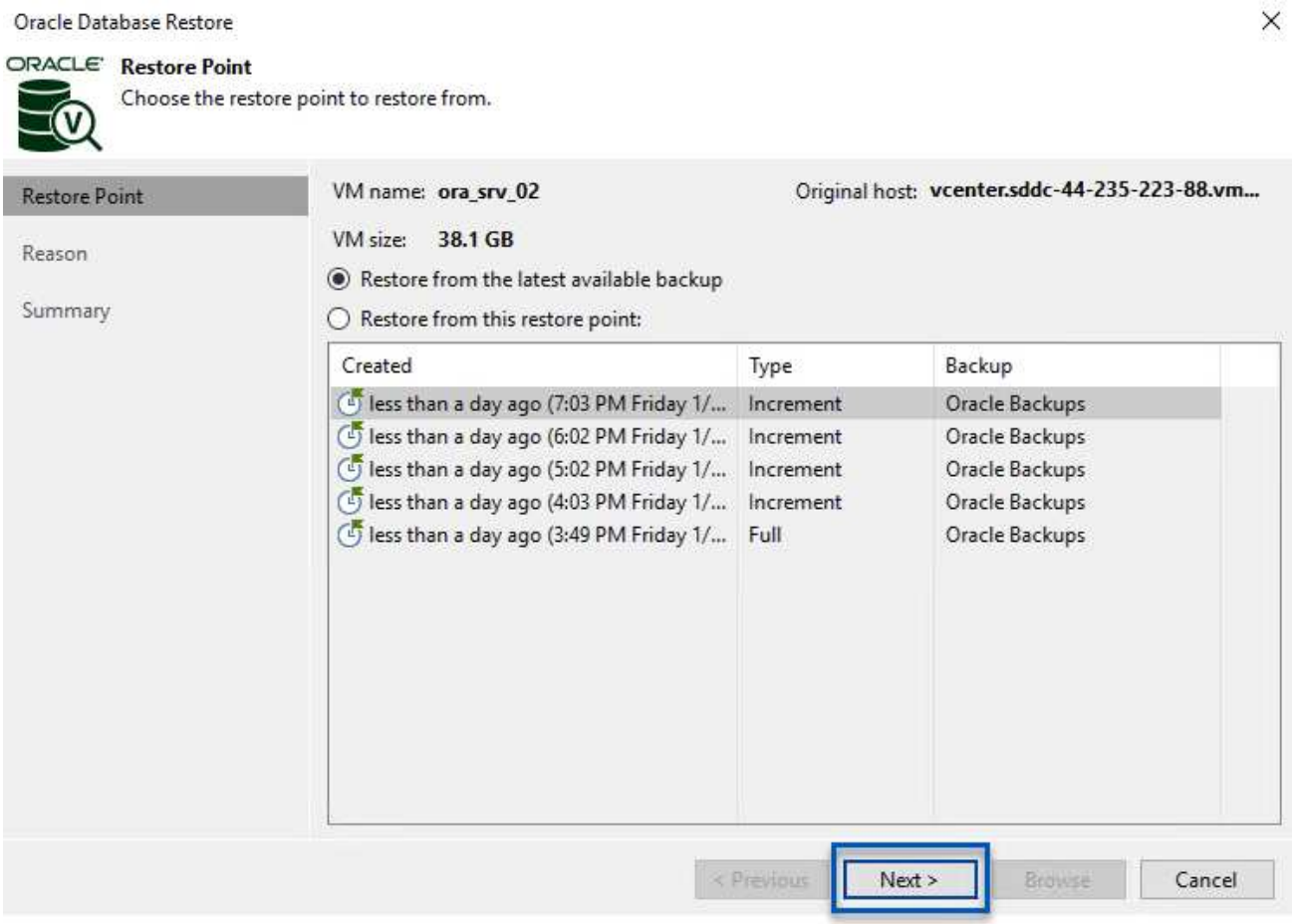
▼ **Veröffentlichen Sie die Oracle-Datenbank auf einem alternativen Server**

In diesem Abschnitt wird eine Datenbank auf einem alternativen Server veröffentlicht, um einen schnellen Zugriff zu ermöglichen, 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 **Anwendungselemente wiederherstellen** und dann **Oracle-Datenbanken…**.

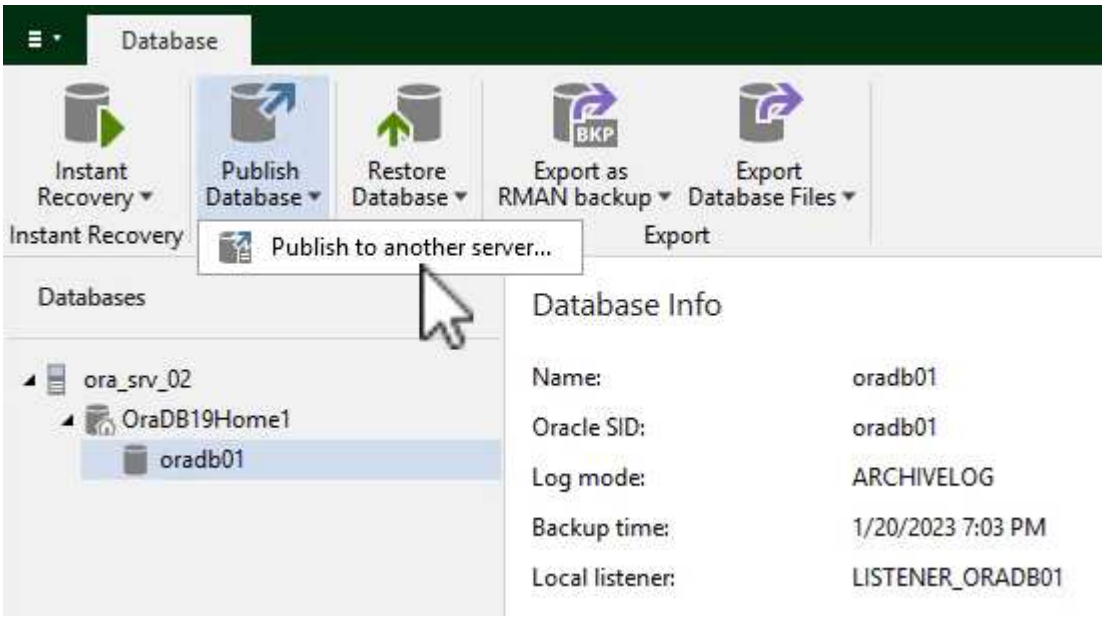


2. Wählen Sie im Oracle Database Restore Wizard einen Wiederherstellungspunkt aus der Liste aus und klicken Sie auf **Weiter**.

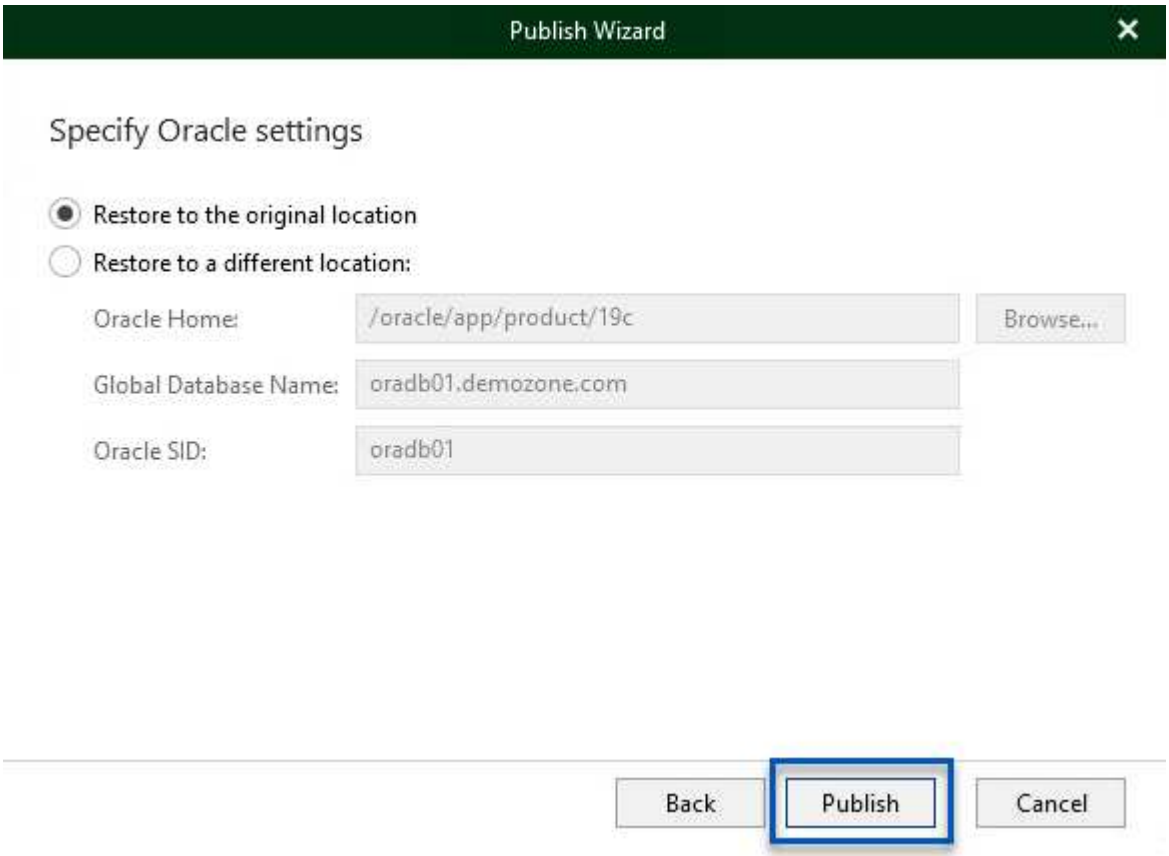


3. Geben Sie bei Bedarf einen **Wiederherstellungsgrund** ein und klicken Sie dann auf der Seite „Zusammenfassung“ auf die Schaltfläche **Durchsuchen**, um Veeam Explorer für Oracle zu starten.

4. Erweitern Sie im Veeam Explorer die Liste der Datenbankinstanzen, klicken Sie auf die wiederherzustellende Datenbank und wählen Sie dann oben im Dropdown-Menü **Datenbank veröffentlichen** die Option **Auf einem anderen Server veröffentlichen…**.



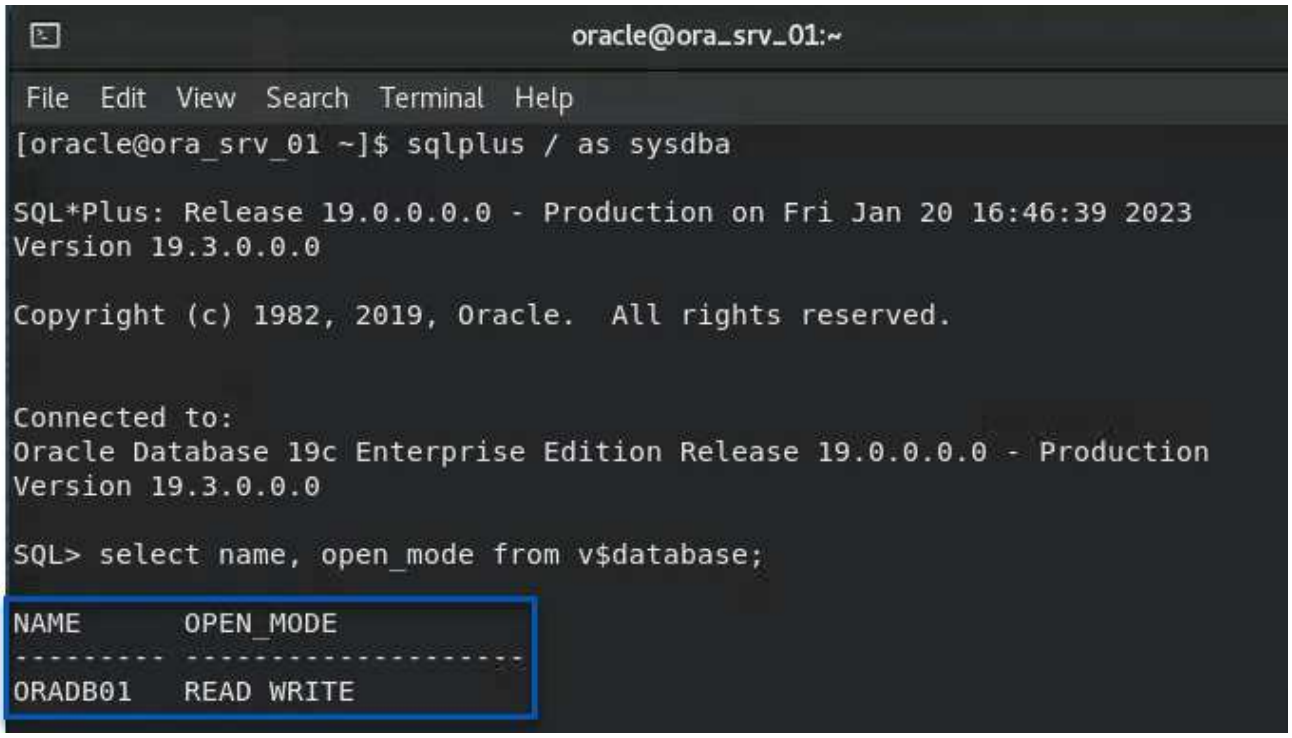
5. Geben Sie im Veröffentlichungsassistenten den Wiederherstellungspunkt an, von dem aus die Datenbank veröffentlicht werden soll, und klicken Sie auf **Weiter**.
6. Geben Sie abschließend den Zielspeicherort des Linux-Dateisystems an und klicken Sie auf **Veröffentlichen**, um den Wiederherstellungsprozess zu starten.



7. Sobald die Veröffentlichung abgeschlossen ist, melden Sie sich 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;
```



Abschluss

VMware Cloud ist eine leistungsstarke Plattform zum Ausführen geschäftskritischer Anwendungen und zum Speichern vertraulicher Daten. Für Unternehmen, die auf VMware Cloud angewiesen sind, ist eine sichere Datenschutzlösung unerlässlich, um die Geschäftskontinuität sicherzustellen und zum Schutz vor Cyberbedrohungen und Datenverlust beizutragen. Durch die Wahl einer zuverlässigen und robusten Datenschutzlösung können Unternehmen darauf vertrauen, dass ihre kritischen Daten unter allen Umständen sicher sind.

Der in dieser Dokumentation vorgestellte Anwendungsfall konzentriert sich auf bewährte Datenschutztechnologien, die die Integration zwischen NetApp, VMware und Veeam hervorheben. FSx ONTAP wird als ergänzender NFS-Datenspeicher für VMware Cloud in AWS unterstützt und für alle virtuellen Maschinen- und Anwendungsdaten verwendet. Veeam Backup & Replication ist eine umfassende Datensicherungslösung, die Unternehmen dabei unterstützt, ihre Sicherungs- und Wiederherstellungsprozesse zu verbessern, zu automatisieren und zu optimieren. Veeam wird in Verbindung mit iSCSI-Backup-Zielvolumes verwendet, die auf FSx ONTAP gehostet werden, um eine sichere und einfach zu verwaltende Datenschutzlösung für Anwendungsdaten in der VMware Cloud bereitzustellen.

Weitere Informationen

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

- "FSx ONTAP Benutzerhandbuch"
- "Veeam Help Center Technische Dokumentation"
- "VMware Cloud auf AWS-Support. Überlegungen und Einschränkungen"

TR-4955: Notfallwiederherstellung mit FSx ONTAP und VMC (AWS VMware Cloud)

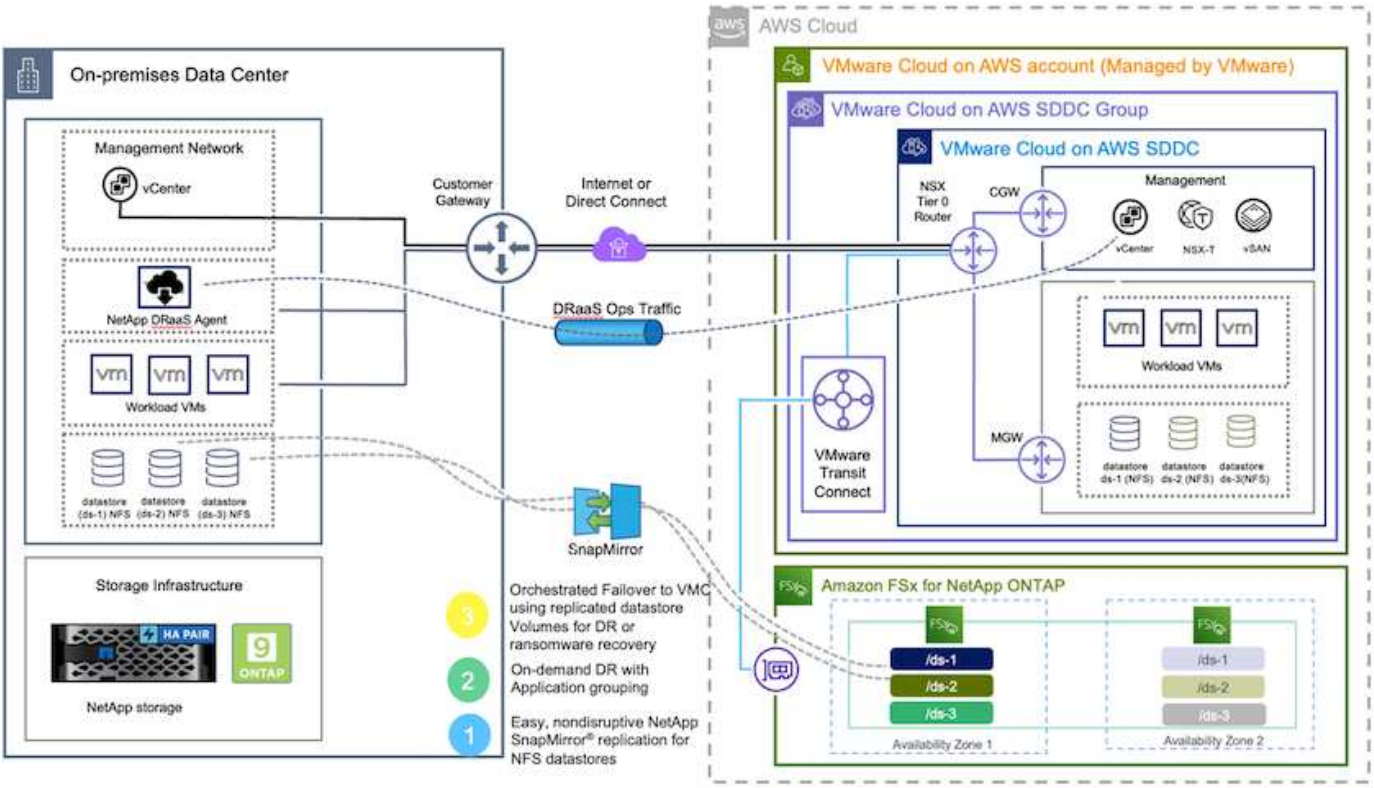
Mit Disaster Recovery Orchestrator (DRO; eine Skriptlösung mit Benutzeroberfläche) können Workloads, die vor Ort auf FSx ONTAP repliziert wurden, nahtlos wiederhergestellt werden. DRO automatisiert die Wiederherstellung von der SnapMirror Ebene über die VM-Registrierung bei VMC bis hin zu Netzwerkzuordnungen direkt auf NSX-T. Diese Funktion ist in allen VMC-Umgebungen enthalten.

Niyaz Mohamed, NetApp

Überblick

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Site-Ausfällen und Datenbeschädigungen (z. B. Ransomware) zu schützen. Mit der NetApp SnapMirror -Technologie können lokale VMware-Workloads auf FSx ONTAP repliziert werden, das in AWS ausgeführt wird.

Mit Disaster Recovery Orchestrator (DRO; eine Skriptlösung mit Benutzeroberfläche) können Workloads, die vor Ort auf FSx ONTAP repliziert wurden, nahtlos wiederhergestellt werden. DRO automatisiert die Wiederherstellung von der SnapMirror Ebene über die VM-Registrierung bei VMC bis hin zu Netzwerkzuordnungen direkt auf NSX-T. Diese Funktion ist in allen VMC-Umgebungen enthalten.



Bereitstellen und Konfigurieren von VMware Cloud auf AWS

"VMware Cloud auf AWS"bietet eine Cloud-native Erfahrung für VMware-basierte Workloads im AWS-Ökosystem. Jedes VMware Software-Defined Data Center (SDDC) läuft in einer Amazon Virtual Private Cloud (VPC) und bietet einen vollständigen VMware-Stack (einschließlich vCenter Server), NSX-T Software-Defined Networking, vSAN Software-Defined Storage und einen oder mehrere ESXi-Hosts, die den Workloads Rechen- und Speicherressourcen bereitstellen. Um eine VMC-Umgebung auf AWS zu konfigurieren, folgen Sie den Schritten hier"Link" . Ein Pilotlichtcluster kann auch für DR-Zwecke verwendet werden.

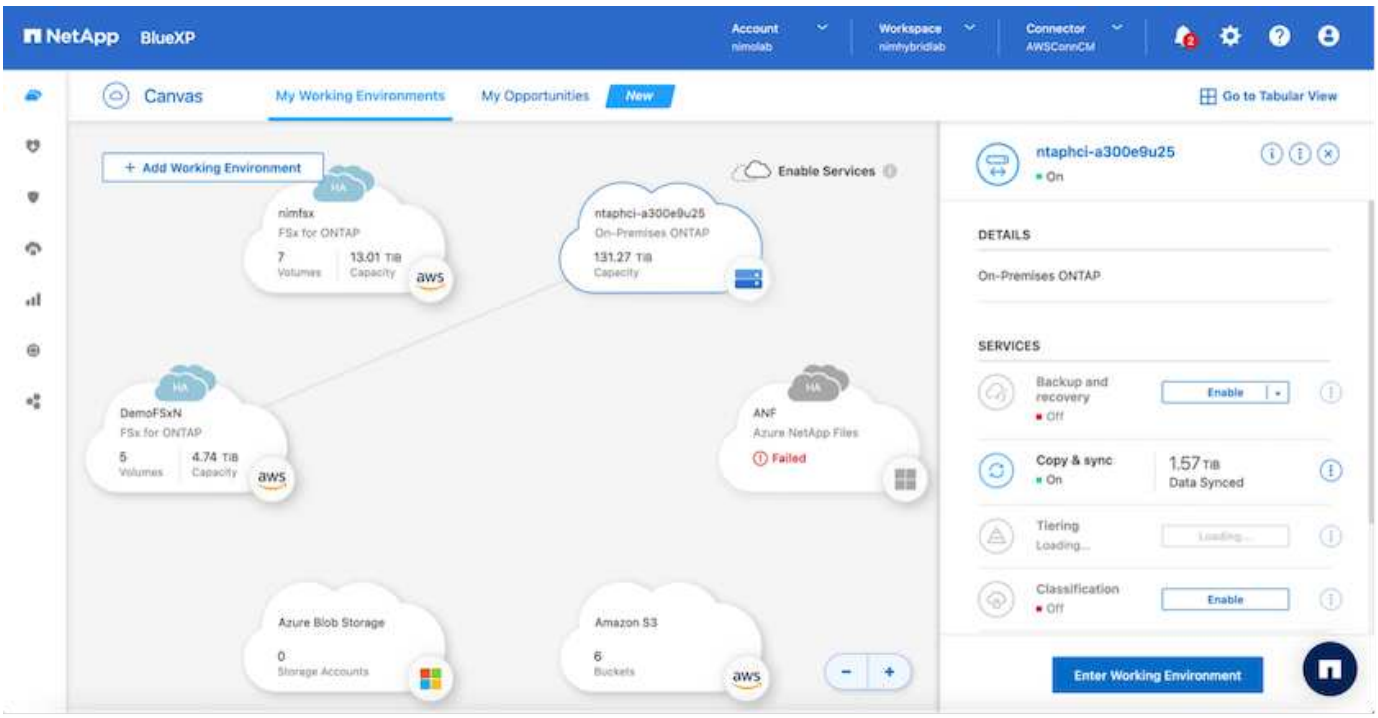
In der ersten Version unterstützt DRO einen vorhandenen Pilotlichtcluster. Die On-Demand-SDDC-Erstellung wird in einer kommenden Version verfügbar sein.

Bereitstellen und Konfigurieren von FSx ONTAP

Amazon FSx ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher bietet, der auf dem beliebten NetApp ONTAP Dateisystem basiert. Befolgen Sie die Schritte in diesem"Link" zum Bereitstellen und Konfigurieren von FSx ONTAP.

Bereitstellen und Konfigurieren von SnapMirror für FSx ONTAP

Im nächsten Schritt erfolgt mit NetApp Console die Identifizierung der bereitgestellten FSx ONTAP on AWS Instanz, und die gewünschten Datastore Volumes werden mit der entsprechenden Häufigkeit und NetApp Snapshot-Kopien-Aufbewahrung aus einer lokalen Umgebung nach FSx ONTAP repliziert:



Die Schritte zur Konfiguration von DRO finden Sie unter diesem Link. Die Planung der Replikation kann auch über die NetApp ONTAP CLI unter diesem Link erfolgen.

Eine SnapMirror -Beziehung ist Voraussetzung und muss vorher erstellt werden.

DRO-Installation

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

Voraussetzungen

- Stellen Sie sicher, dass eine Verbindung zum Quell- und Ziel-vCenter und den Speichersystemen besteht.
- Wenn Sie DNS-Namen verwenden, sollte eine DNS-Auflösung vorhanden sein. Andernfalls sollten Sie IP-Adressen für das vCenter und die Speichersysteme verwenden.
- Erstellen Sie einen Benutzer mit Root-Berechtigungen. Sie können sudo auch mit einer EC2-Instanz verwenden.

OS Anforderungen

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

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

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

Installieren des Pakets

1. Laden Sie das Installationspaket auf die angegebene virtuelle Maschine herunter:

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

   Der Agent kann vor Ort 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 Bereitstellungsskript wie folgt aus:

```
sudo sh deploy.sh
```

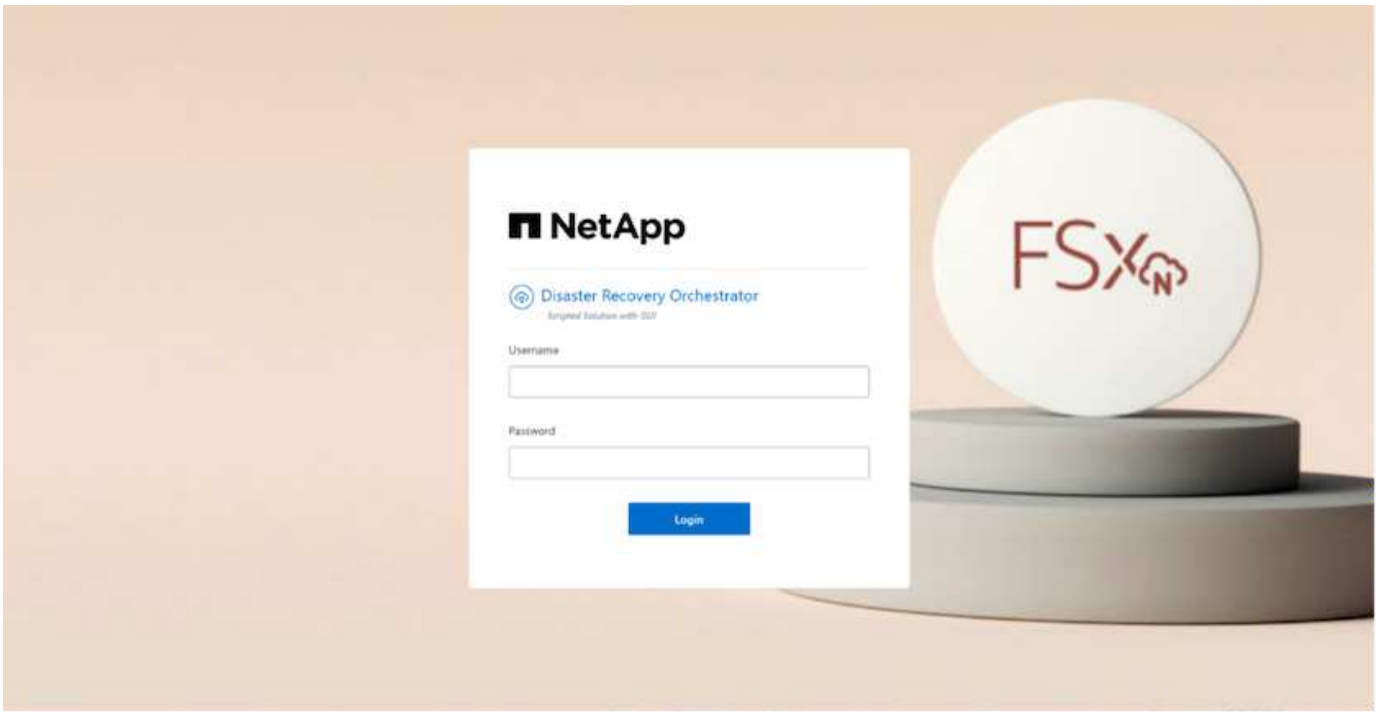
4. Greifen Sie auf die Benutzeroberfläche zu, indem Sie Folgendes verwenden:

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

mit den folgenden Standardanmeldeinformationen:

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

Das Passwort kann über die Option „Passwort ändern“ geändert werden.



DRO-Konfiguration

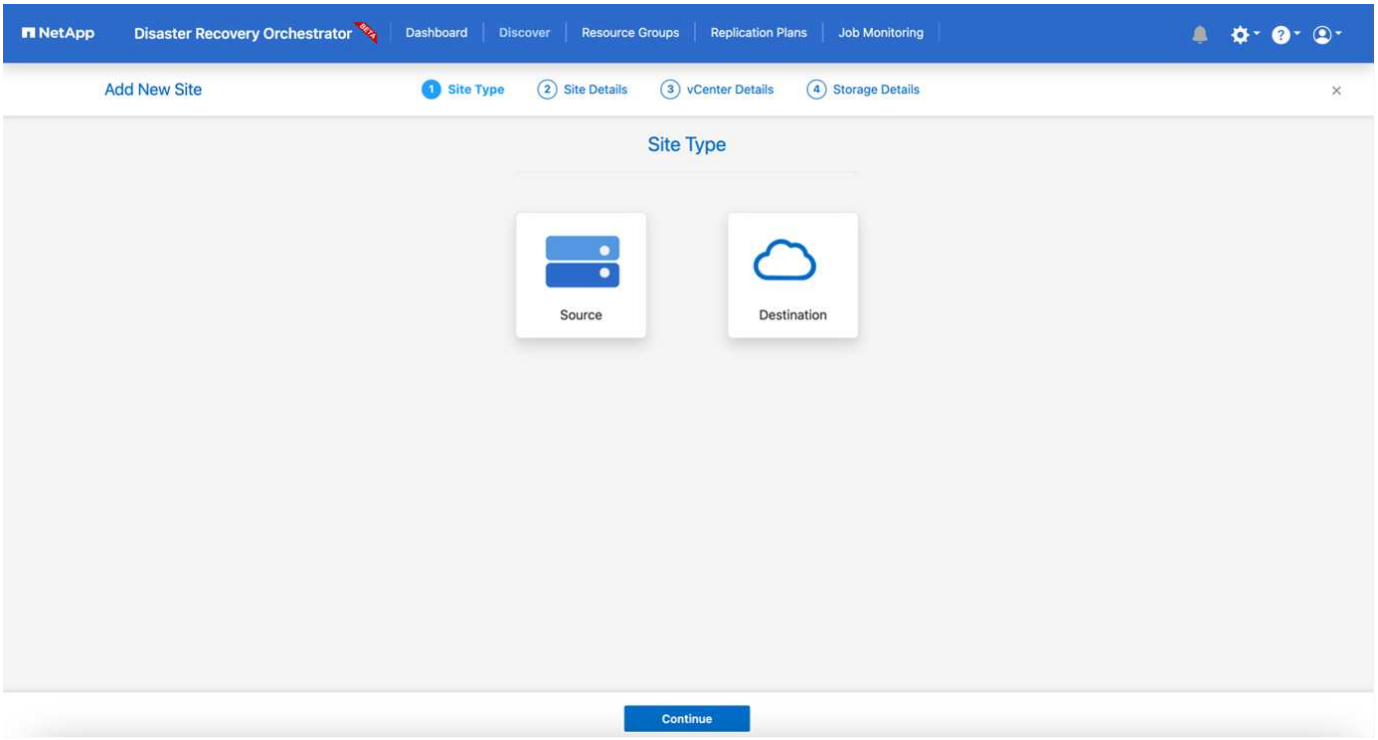
Nachdem FSx ONTAP und VMC ordnungsgemäß konfiguriert wurden, können Sie mit der Konfiguration von DRO beginnen, um die Wiederherstellung lokaler Workloads auf VMC mithilfe der schreibgeschützten SnapMirror -Kopien auf FSx ONTAP zu automatisieren.

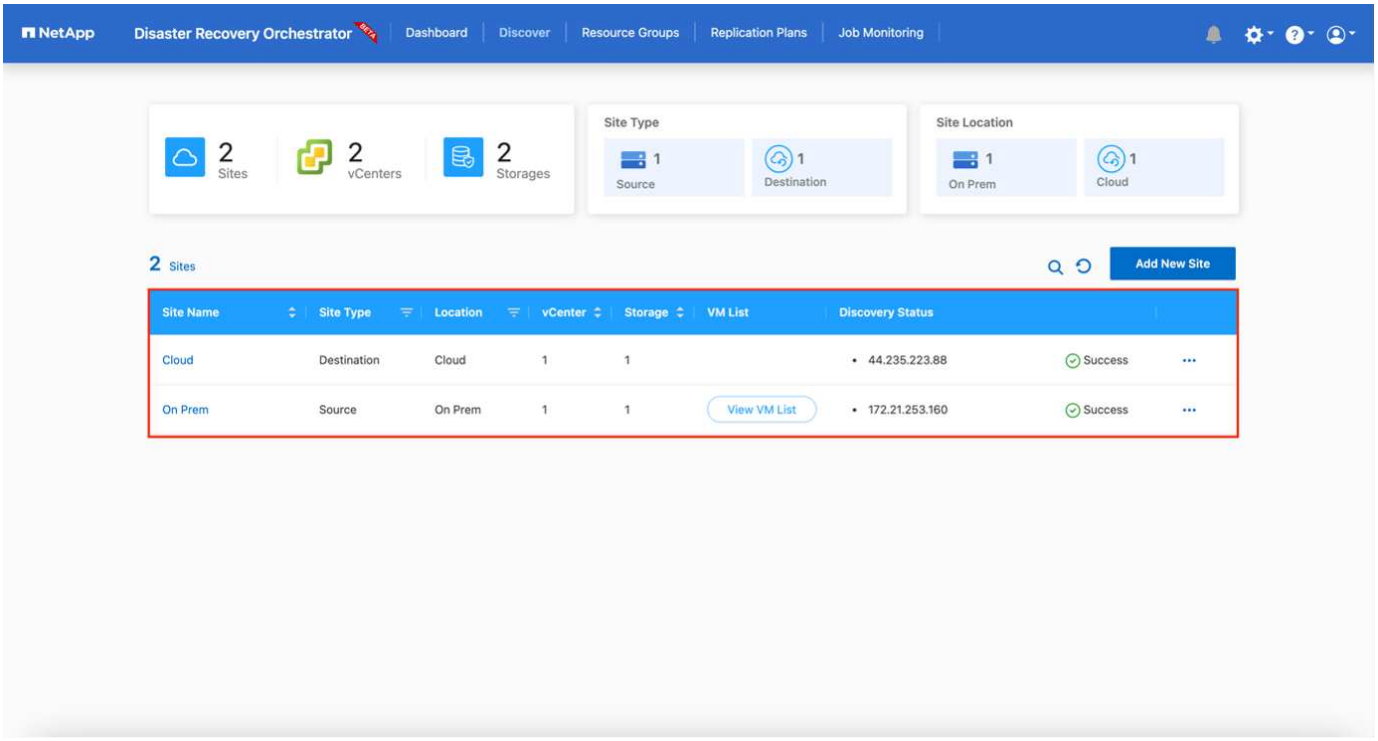
NetApp empfiehlt, den DRO-Agenten in AWS und auch in derselben VPC bereitzustellen, in der FSx ONTAP bereitgestellt wird (es kann auch eine Peer-Verbindung bestehen), damit der DRO-Agent über das Netzwerk mit Ihren lokalen Komponenten sowie mit den FSx ONTAP und VMC-Ressourcen kommunizieren kann.

Der erste Schritt besteht darin, die lokalen und Cloud-Ressourcen (sowohl vCenter als auch Speicher) zu ermitteln und zu DRO hinzuzufügen. Öffnen Sie DRO in einem unterstützten Browser, verwenden Sie den Standardbenutzernamen und das Standardkennwort (admin/admin) und fügen Sie Sites hinzu. Websites können auch mithilfe der Option „Entdecken“ hinzugefügt werden. Fügen Sie die folgenden Plattformen hinzu:

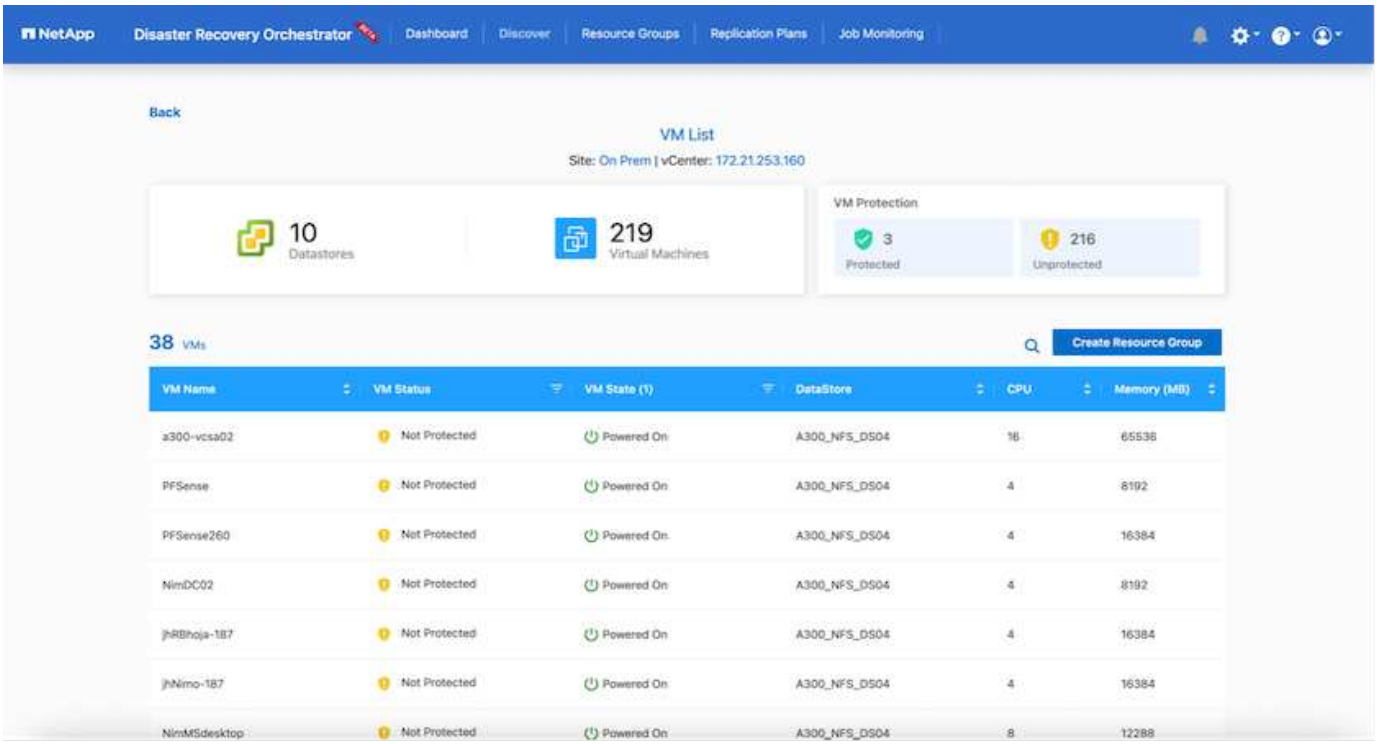
- Vor Ort
  - Lokales vCenter
  - ONTAP -Speichersystem

- Wolke
  - VMC vCenter
  - FSx ONTAP





Nach dem Hinzufügen führt DRO eine automatische Erkennung durch und zeigt die VMs an, die über entsprechende SnapMirror Replikate vom Quellspeicher bis zu FSx ONTAP verfügen. DRO erkennt automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie.



Der nächste Schritt besteht darin, die erforderlichen VMs in Funktionsgruppen zu gruppieren, die als Ressourcengruppen dienen.

Ressourcengruppierungen

Nachdem die Plattformen hinzugefügt wurden, können Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen gruppieren. Mit DRO-Ressourcengruppen können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen, Startverzögerungen und optionalen Anwendungsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

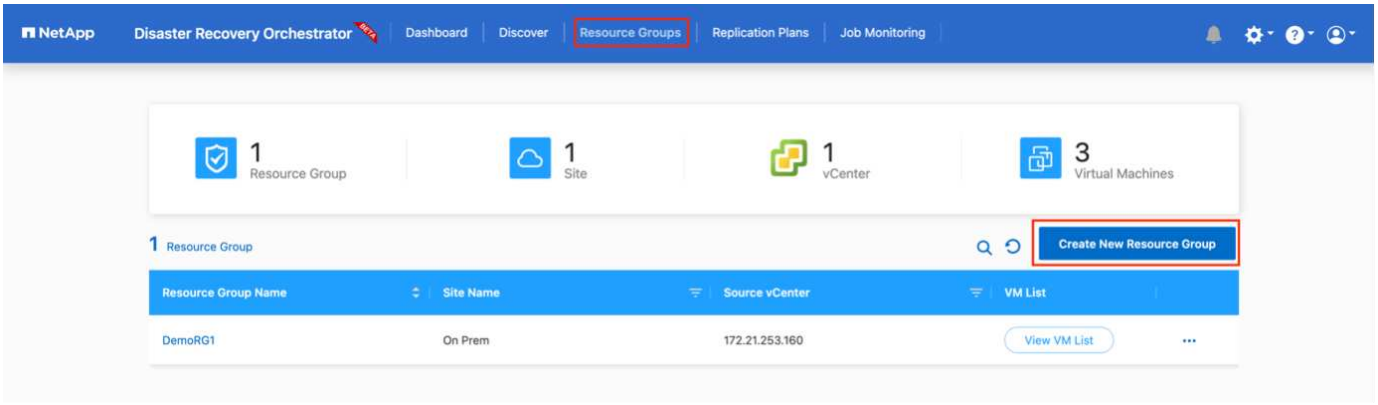
Führen Sie die folgenden Schritte aus, um mit der Erstellung von Ressourcengruppen zu beginnen:

1. Greifen Sie auf **Ressourcengruppen** zu und klicken Sie auf **Neue Ressourcengruppe erstellen**.
2. Wählen Sie unter **Neue Ressourcengruppe** die Quellsite aus der Dropdown-Liste aus und klicken Sie auf **Erstellen**.
3. Geben Sie **Ressourcengruppendetails** ein und klicken Sie auf **Weiter**.
4. Wählen Sie mithilfe der Suchoption die entsprechenden VMs aus.
5. Wählen Sie die Startreihenfolge und Startverzögerung (Sek.) für die ausgewählten VMs aus. Legen Sie die Reihenfolge der Einschaltsequenz fest, indem Sie jede VM auswählen und die Priorität dafür festlegen. Drei ist der Standardwert für alle VMs.

   Die Optionen sind wie folgt:

   1 – Die erste virtuelle Maschine, die eingeschaltet wird. 3 – Standard. 5 – Die letzte virtuelle Maschine, die eingeschaltet wird.

6. Klicken Sie auf **Ressourcengruppe erstellen**.

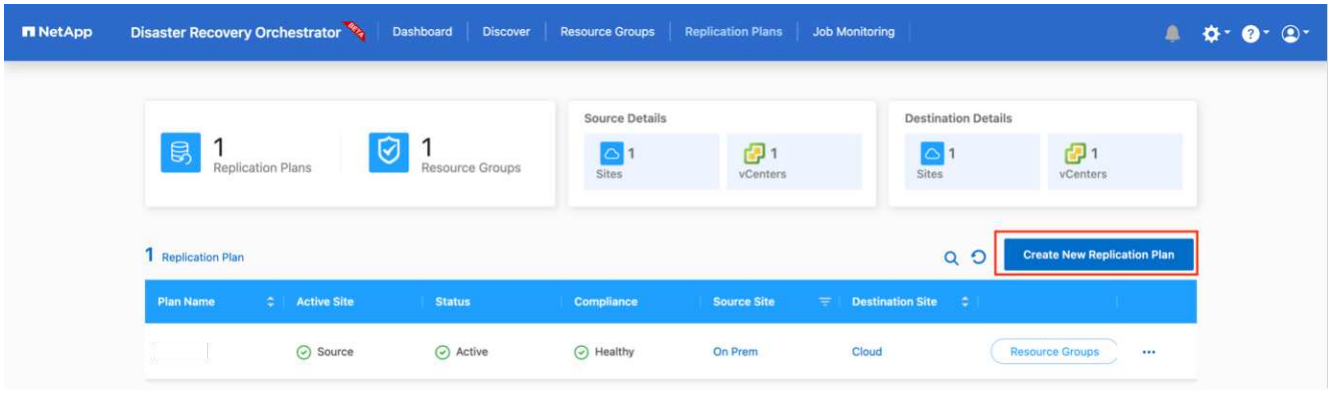


Replikationspläne

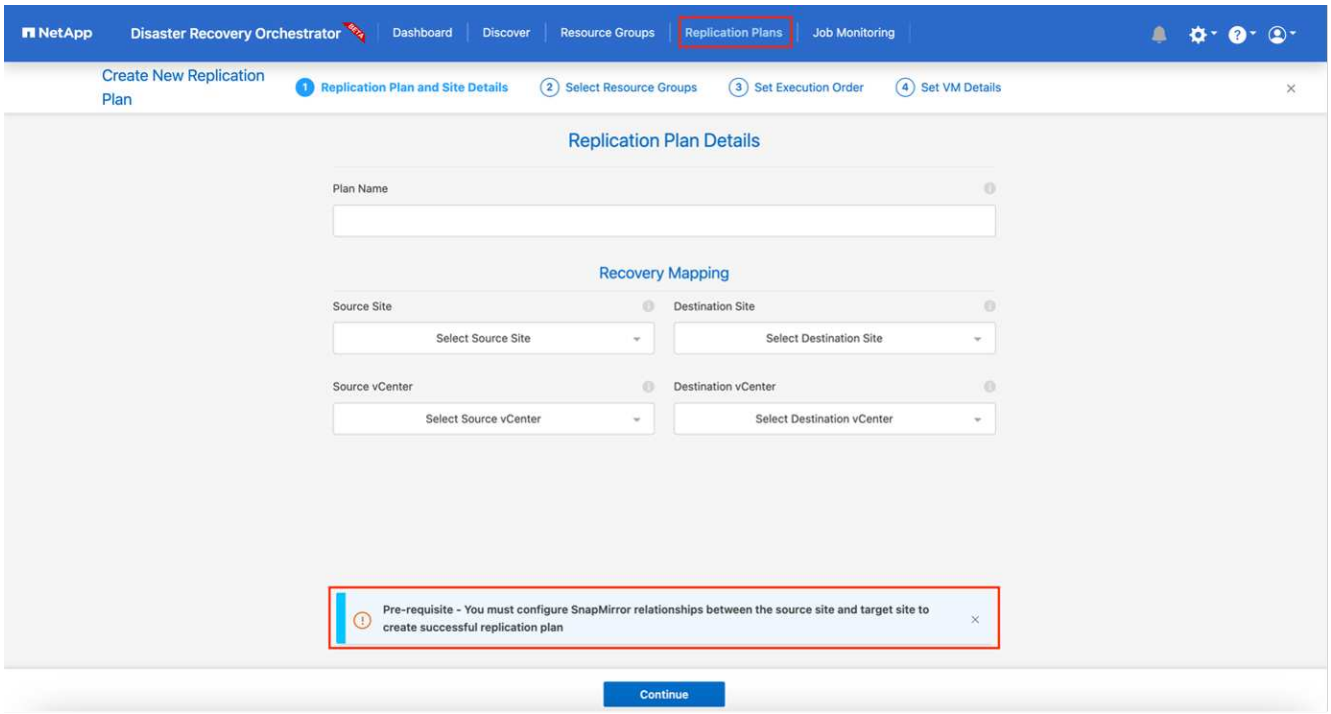
Sie benötigen einen Plan zur Wiederherstellung von Anwendungen im Katastrophenfall. Wählen Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste aus und wählen Sie die Ressourcengruppen aus, die in diesen Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen (z. B. Domänencontroller, dann Tier-1, dann Tier-2 usw.). Solche Pläne werden manchmal auch als Blaupausen bezeichnet. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Neuer Replikationsplan**.

Führen Sie die folgenden Schritte aus, um mit der Erstellung eines Replikationsplans zu beginnen:

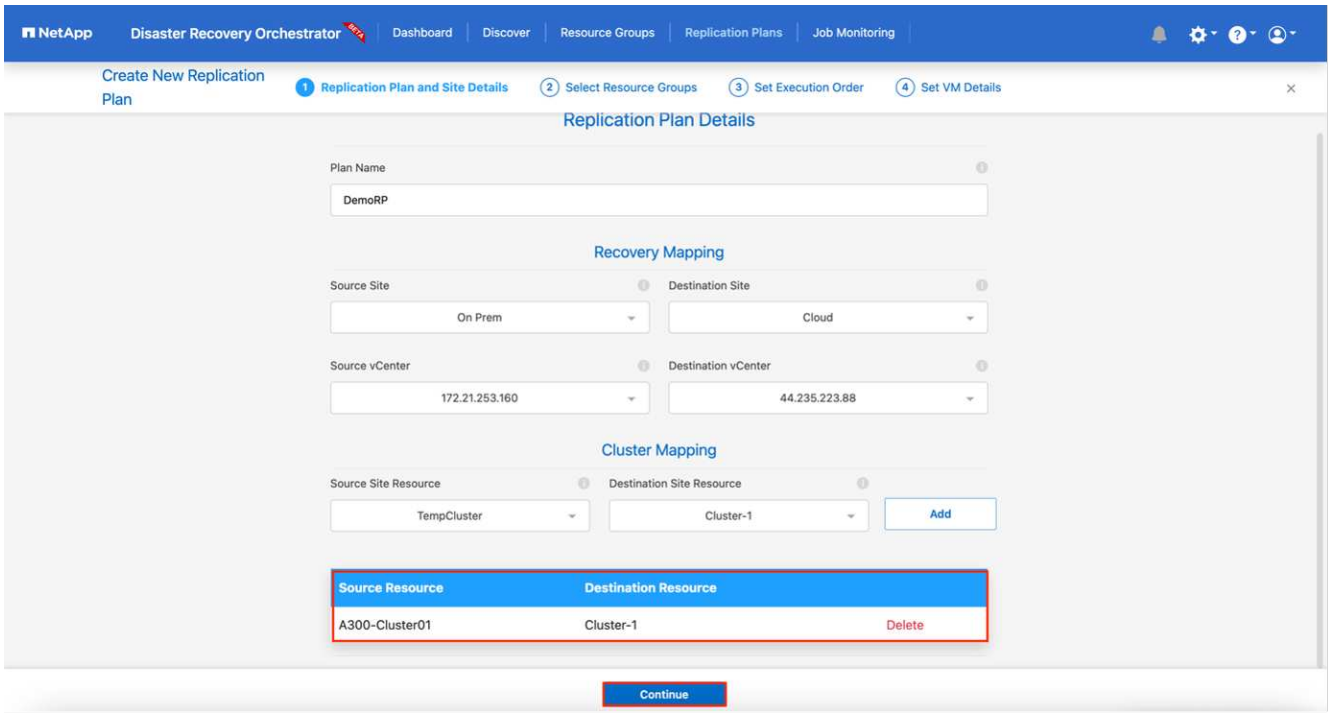
1. Greifen Sie auf **Replikationspläne** zu und klicken Sie auf **Neuen Replikationsplan erstellen**.



2. Geben Sie unter **Neuer Replikationsplan** einen Namen für den Plan ein und fügen Sie Wiederherstellungszuordnungen hinzu, indem Sie die Quellsite, das zugehörige vCenter, die Zielsite und das zugehörige vCenter auswählen.

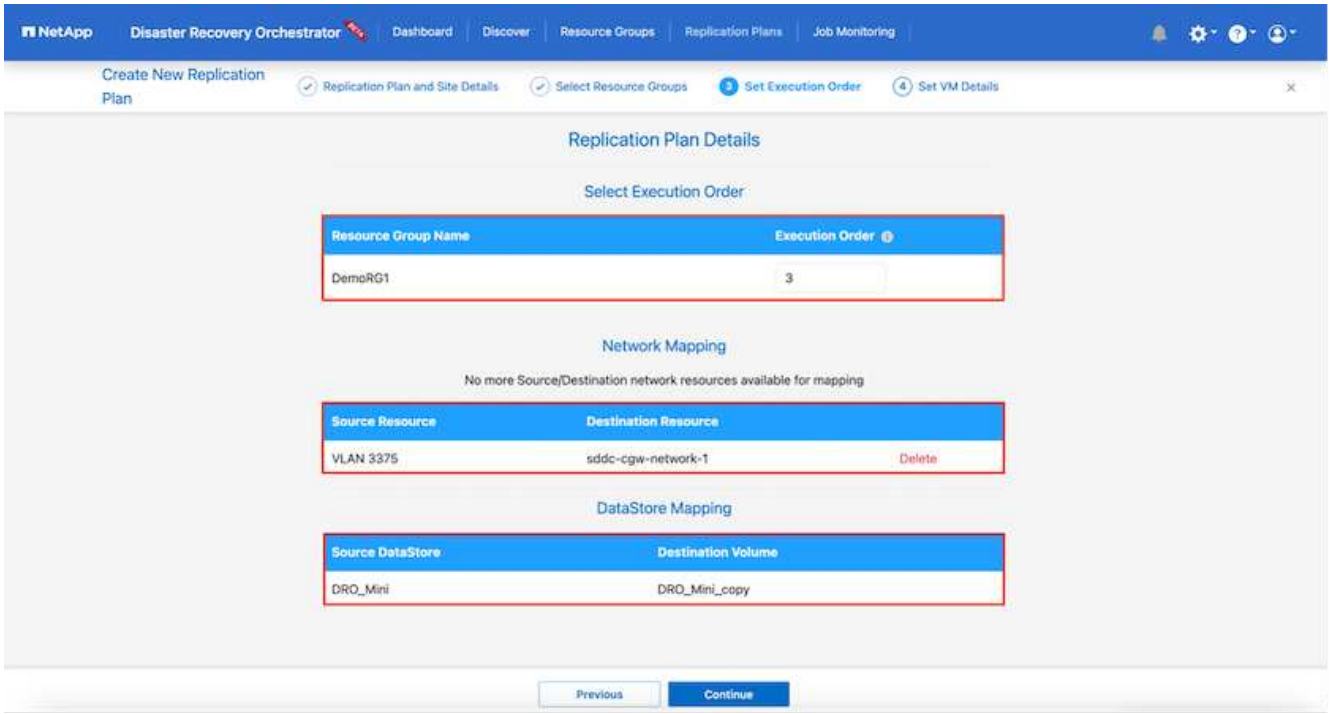


3. Wählen Sie nach Abschluss der Wiederherstellungszuordnung die Clusterzuordnung aus.

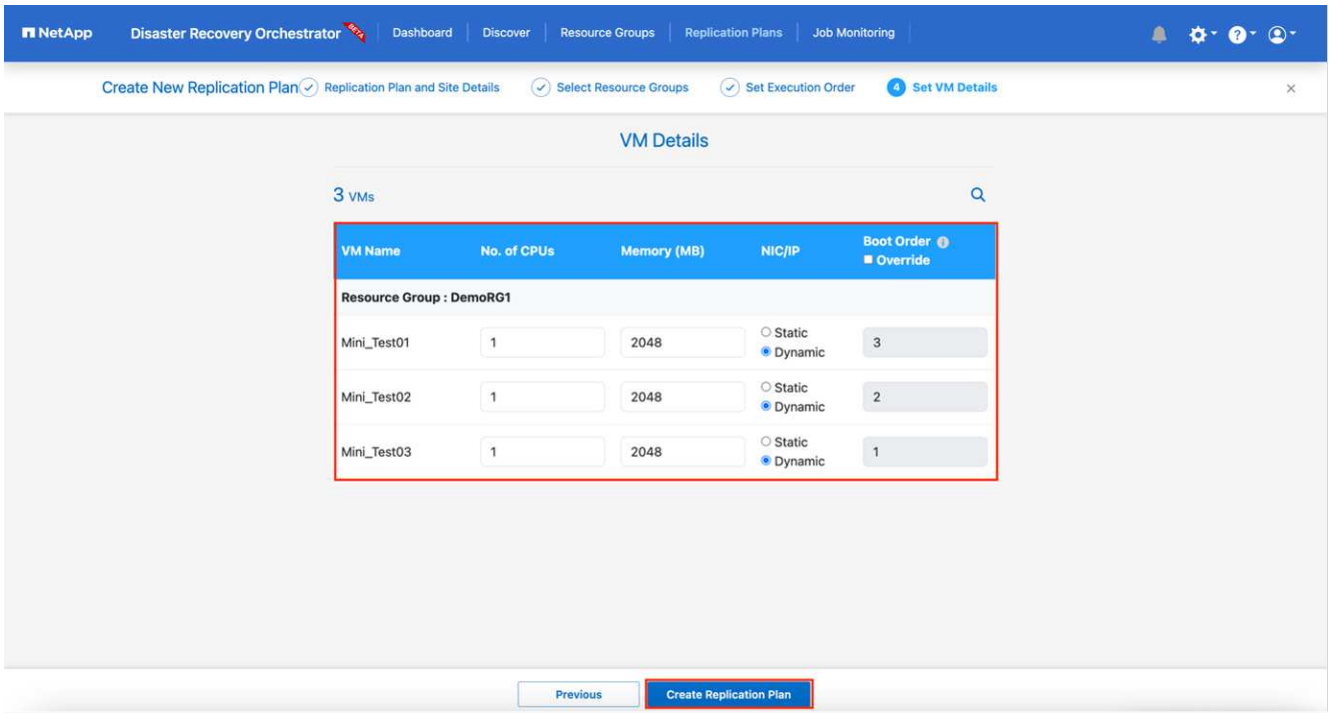


4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
6. Wenn Sie fertig sind, wählen Sie die Netzwerkzuordnung zum entsprechenden Segment aus. Die Segmente sollten bereits in VMC bereitgestellt sein. Wählen Sie daher das entsprechende Segment aus, um die VM zuzuordnen.
7. Basierend auf der Auswahl der VMs werden Datenspeicherzuordnungen automatisch ausgewählt.

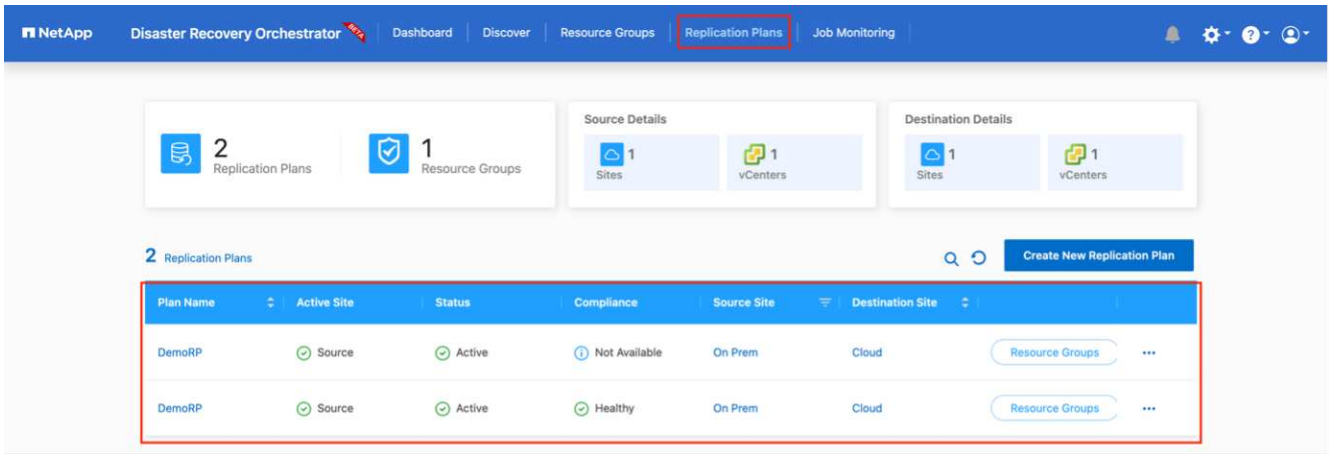
SnapMirror ist auf Lautstärke eingestellt. Daher werden alle VMs zum Replikationsziel repliziert. Stellen Sie sicher, dass Sie alle VMs auswählen, die Teil des Datenspeichers sind. Wenn sie nicht ausgewählt sind, werden nur die VMs verarbeitet, die Teil des Replikationsplans sind.



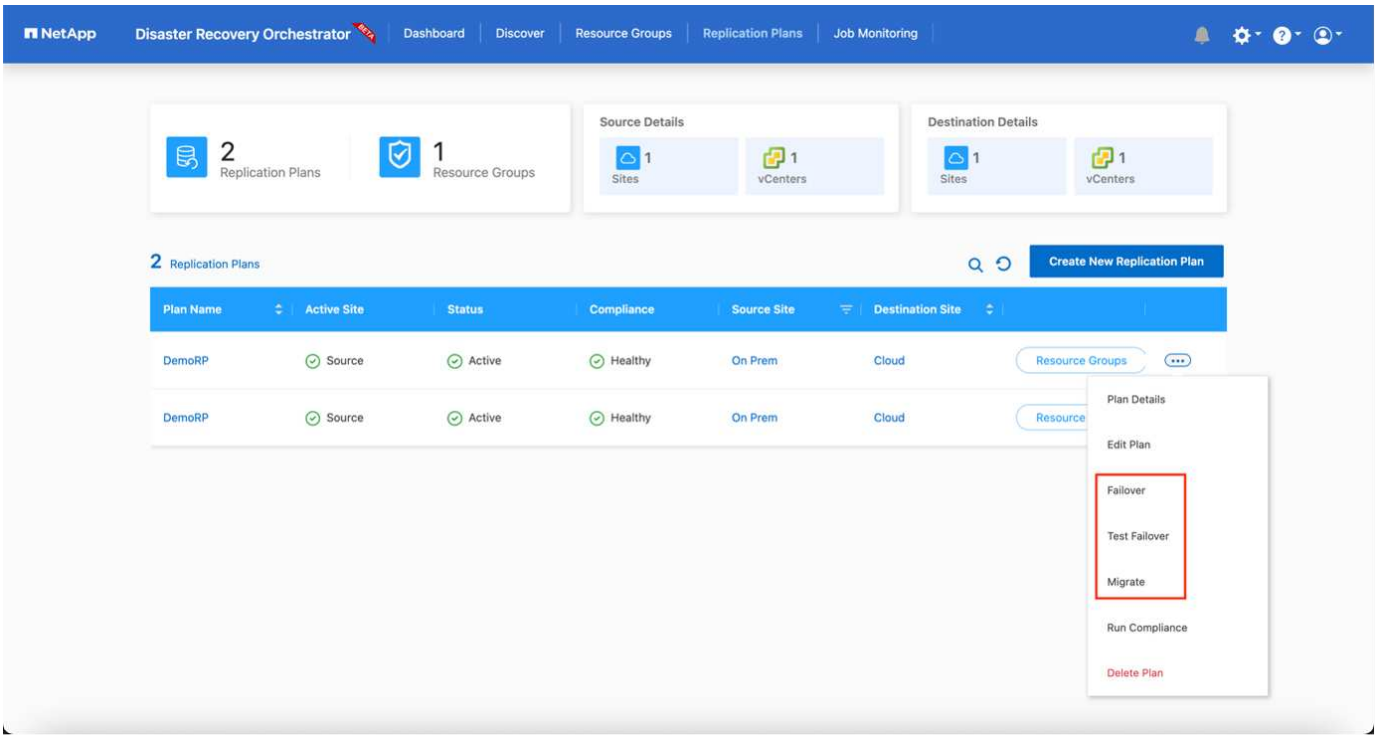
8. Unter den VM-Details können Sie optional die CPU- und RAM-Parameter der VM anpassen. Dies kann sehr hilfreich sein, wenn Sie große Umgebungen auf kleineren Zielclustern wiederherstellen oder DR-Tests durchführen, ohne eine 1:1-physikalische VMware-Infrastruktur bereitstellen zu müssen. Darüber hinaus können Sie die Startreihenfolge und die Startverzögerung (Sekunden) für alle ausgewählten VMs in den Ressourcengruppen ändern. Es gibt eine zusätzliche Option zum Ändern der Startreihenfolge, wenn Änderungen an den bei der Auswahl der Startreihenfolge der Ressourcengruppe ausgewählten vorgenommen werden müssen. Standardmäßig wird die bei der Ressourcengruppenauswahl festgelegte Startreihenfolge verwendet. In dieser Phase können jedoch beliebige Änderungen vorgenommen werden.

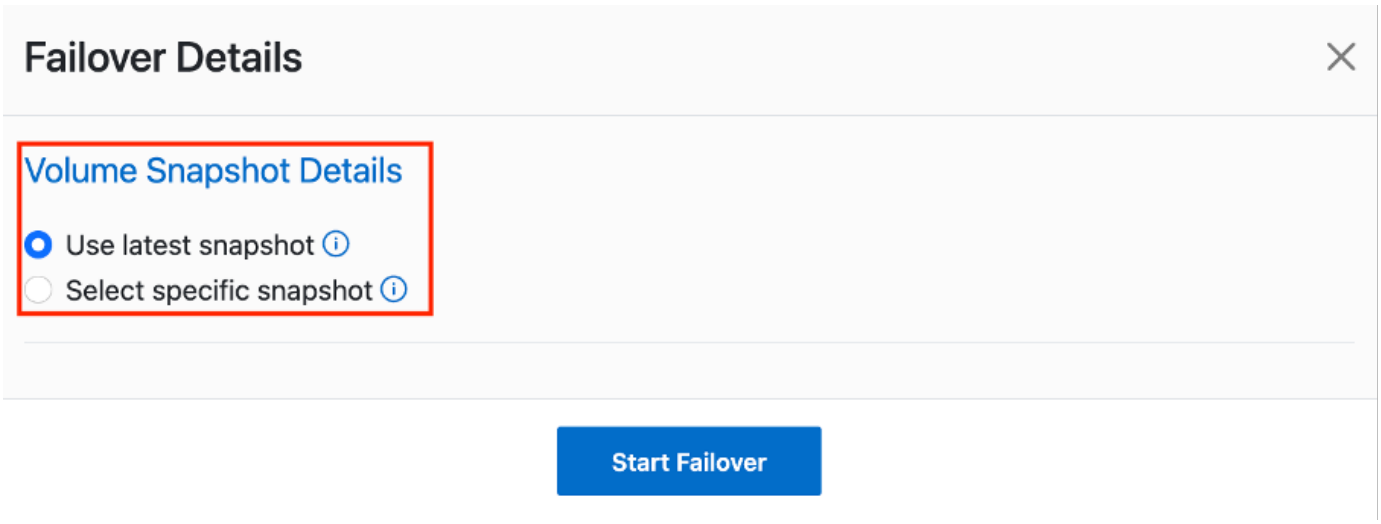


9. Klicken Sie auf **Replikationsplan erstellen**.

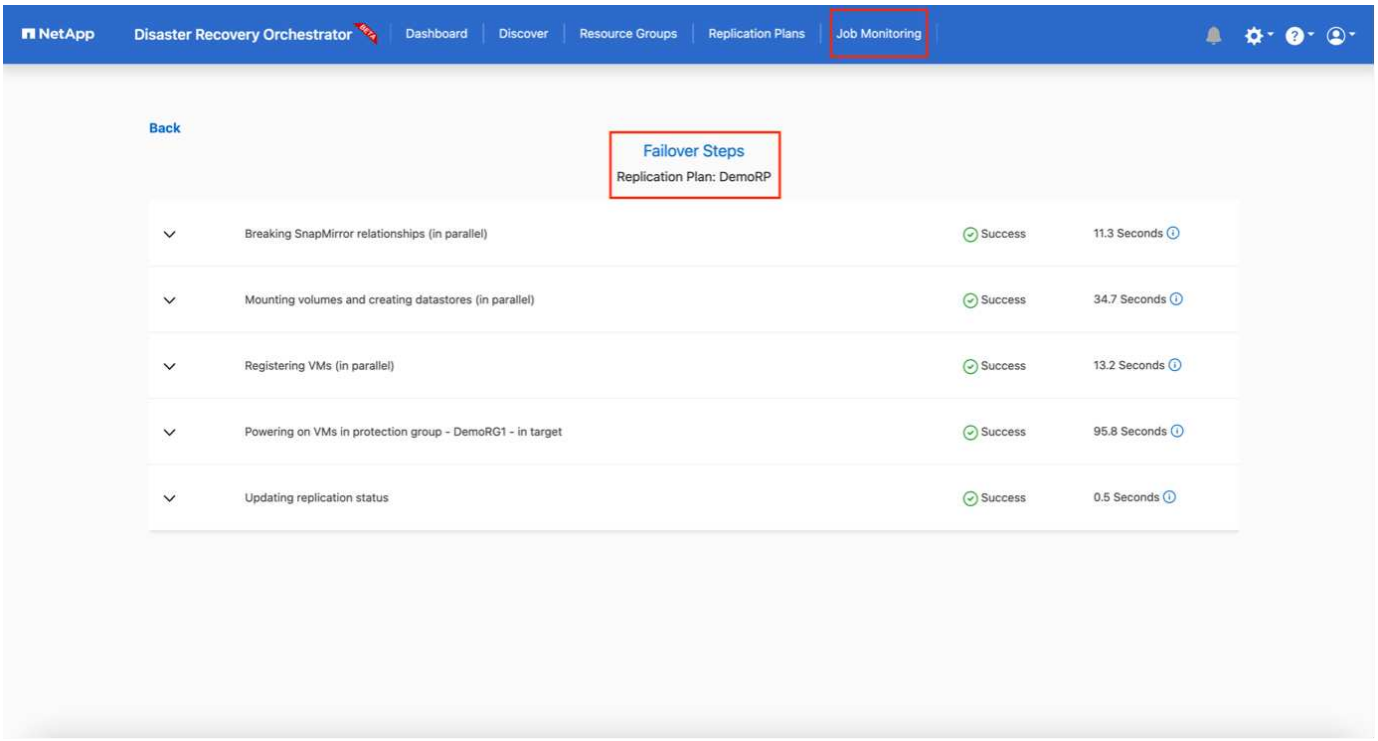


Nachdem der Replikationsplan erstellt wurde, kann je nach Bedarf die Failover-Option, die Test-Failover-Option oder die Migrationsoption ausgeführt werden. Während der Failover- und Test-Failover-Optionen wird die aktuellste SnapMirror -Snapshot-Kopie verwendet, oder es kann eine bestimmte Snapshot-Kopie aus einer Point-in-Time-Snapshot-Kopie ausgewählt werden (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die Point-in-Time-Option kann sehr hilfreich sein, wenn Sie mit einem Korruptionsereignis wie Ransomware konfrontiert sind, bei dem die aktuellsten Replikate bereits kompromittiert oder verschlüsselt sind. DRO zeigt alle verfügbaren Zeitpunkte an. Um ein Failover auszulösen oder ein Failover mit der im Replikationsplan angegebenen Konfiguration zu testen, können Sie auf **Failover** oder **Failover testen** klicken.

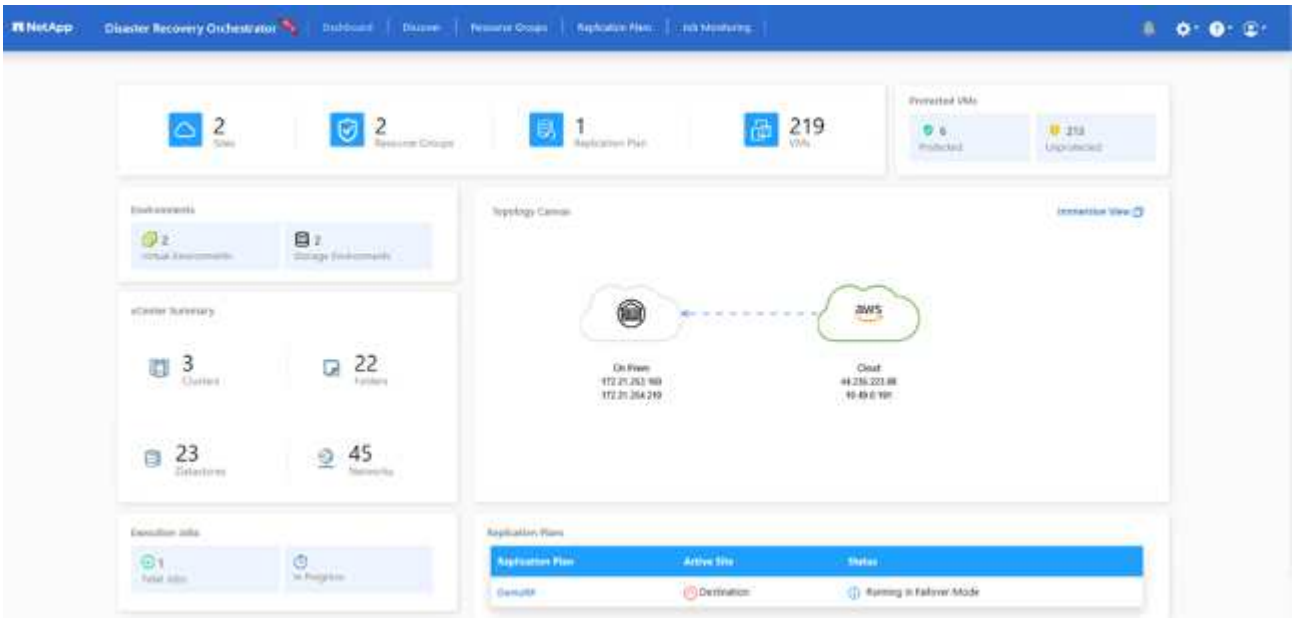




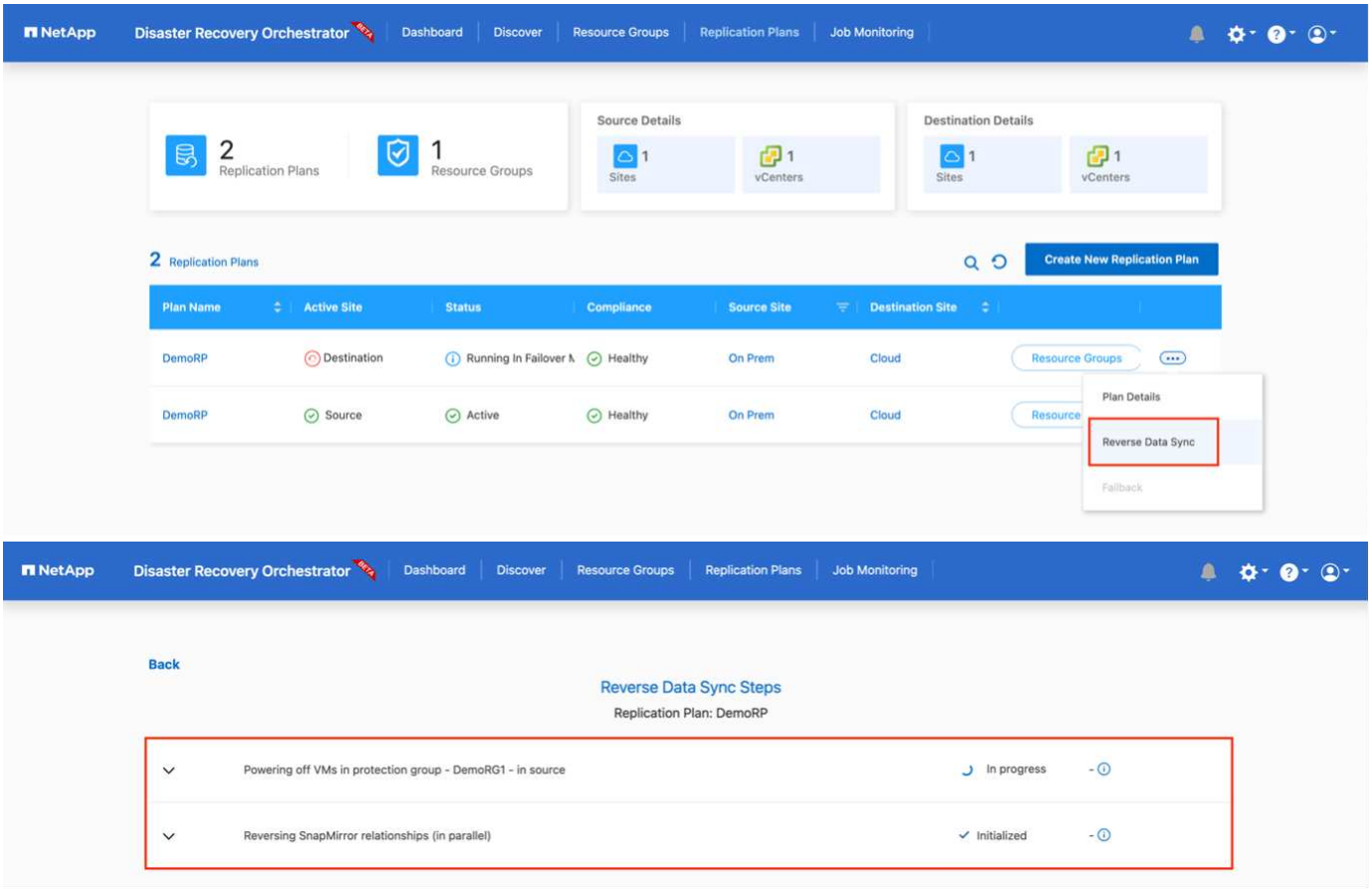
Der Replikationsplan kann im Aufgabenmenü überwacht werden:



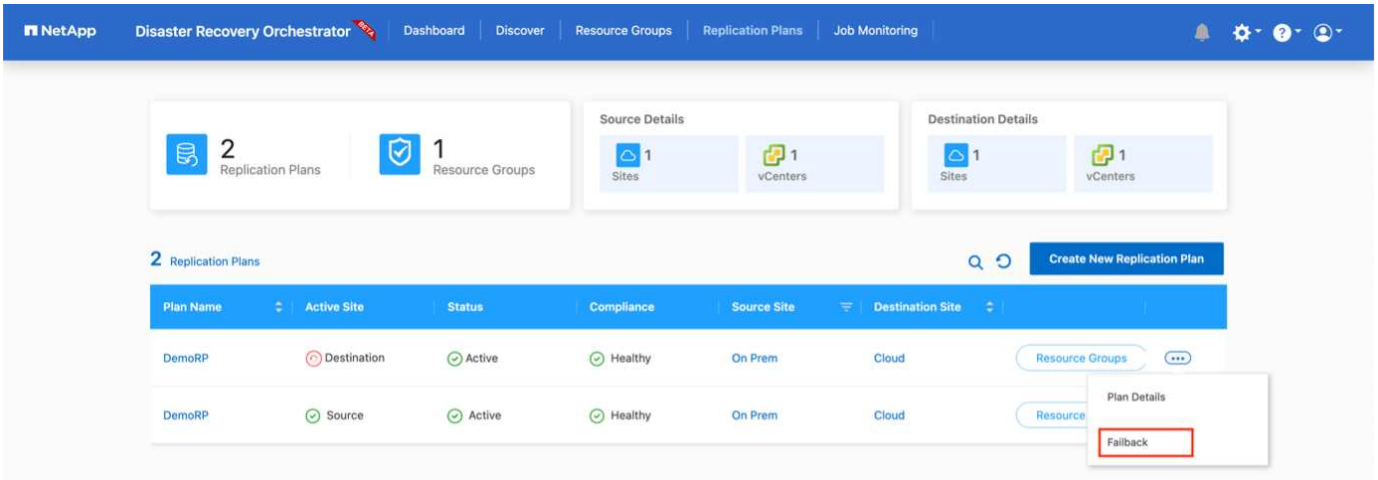
Nachdem das Failover ausgelöst wurde, können die wiederhergestellten Elemente im VMC vCenter (VMs, Netzwerke, Datenspeicher) angezeigt werden. Standardmäßig werden die VMs im Workload-Ordner wiederhergestellt.

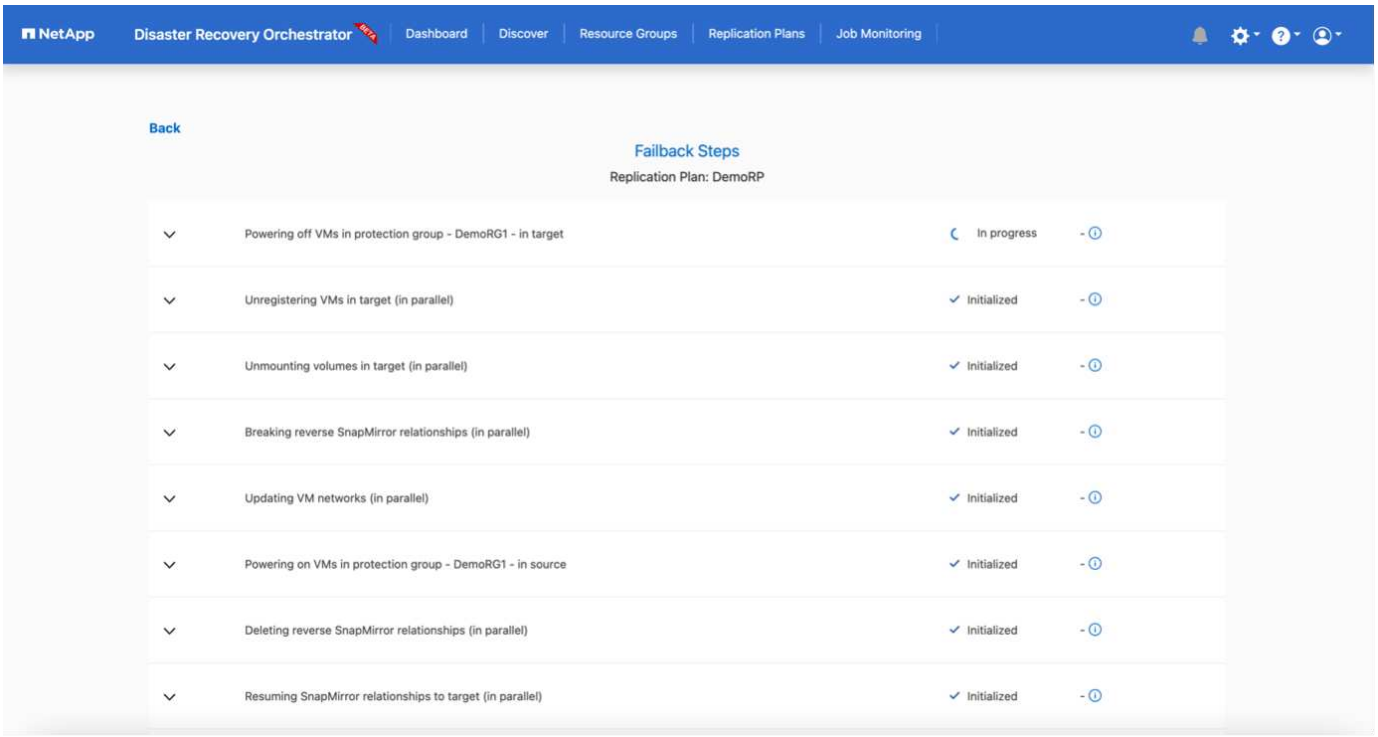


Failback kann auf Replikationsplanebene ausgelöst werden. Für ein Test-Failover kann die Teardown-Option verwendet werden, um die Änderungen rückgängig zu machen und die FlexClone -Beziehung zu entfernen. Das mit dem Failover verbundene Failback ist ein zweistufiger Prozess. Wählen Sie den Replikationsplan und dann **Datensynchronisierung umkehren** aus.

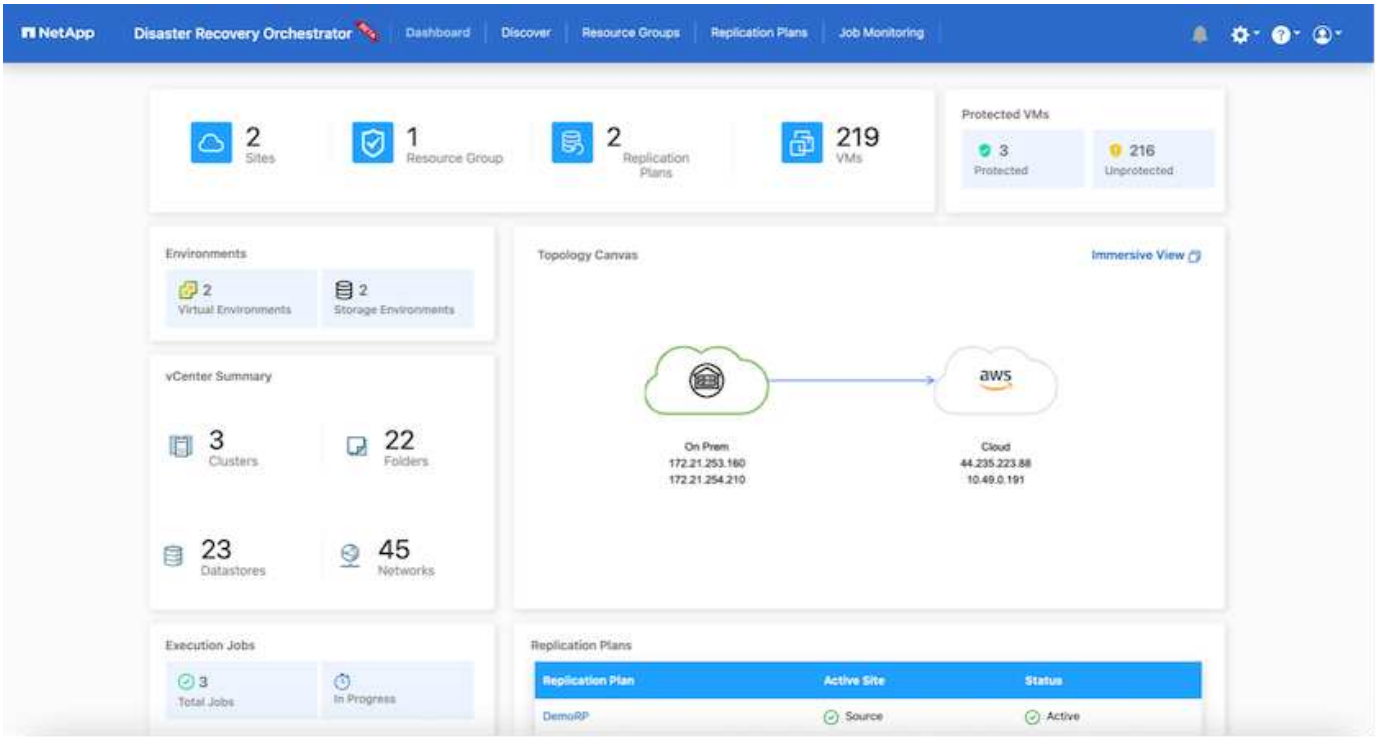


Nach Abschluss können Sie ein Failback auslösen, um zum ursprünglichen Produktionsstandort zurückzukehren.





In NetApp Console ist ersichtlich, dass der Replikations-Systemstatus für die entsprechenden Volumes (diejenigen, die VMC als Lese-/Schreib-Volumes zugeordnet wurden) unterbrochen ist. Während des Test-Failovers erfasst DRO weder das Ziel- noch das Replikat-Volume. Stattdessen erstellt es eine FlexClone-Kopie der erforderlichen SnapMirror- (oder Snapshot-)Instanz und stellt die FlexClone-Instanz bereit, wodurch keine zusätzliche physische Kapazität für FSx ONTAP verbraucht wird. Dieser Prozess stellt sicher, dass das Volume nicht geändert wird und Replikationsjobs auch während DR-Tests oder Triage-Workflows fortgesetzt werden können. Darüber hinaus stellt dieser Prozess sicher, dass die Recovery, falls Fehler auftreten oder beschädigte Daten wiederhergestellt werden, bereinigt werden kann, ohne dass das Risiko besteht, dass das Replikat zerstört wird.



Ransomware-Wiederherstellung

Die Wiederherstellung nach Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Organisationen schwierig sein, den sicheren Zeitpunkt der Rückkehr zu bestimmen und, sobald dieser ermittelt ist, wiederhergestellte Workloads vor wiederkehrenden Angriffen beispielsweise durch ruhende Malware oder anfällige Anwendungen zu schützen.

DRO geht auf diese Probleme ein, indem es Ihnen ermöglicht, Ihr System von jedem verfügbaren Zeitpunkt aus wiederherzustellen. Sie können Workloads auch in funktionsfähige und dennoch isolierte Netzwerke zurückverlagern, sodass Anwendungen an einem Standort funktionieren und miteinander kommunizieren können, an dem sie keinem Nord-Süd-Verkehr ausgesetzt sind. Dies bietet Ihrem Sicherheitsteam einen sicheren Ort, um forensische Untersuchungen durchzuführen und sicherzustellen, dass keine versteckte oder schlafende Malware vorhanden ist.

Vorteile

- Nutzung der effizienten und belastbaren SnapMirror -Replikation.
- Wiederherstellung zu jedem verfügbaren Zeitpunkt mit Aufbewahrung der Snapshot-Kopie.
- Vollständige Automatisierung aller erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs aus den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung.
- Workload-Wiederherstellung mit ONTAP FlexClone -Technologie unter Verwendung einer Methode, die das replizierte Volume nicht ändert.
  - Vermeidet das Risiko einer Datenbeschädigung bei Volumes oder Snapshot-Kopien.
  - Vermeidet Replikationsunterbrechungen während DR-Test-Workflows.
  - Mögliche Verwendung von DR-Daten mit Cloud-Computing-Ressourcen für Workflows über DR hinaus, wie z. B. DevTest, Sicherheitstests, Patch- oder Upgrade-Tests und Fehlerbehebungstests.
- CPU- und RAM-Optimierung zur Senkung der Cloud-Kosten durch die Möglichkeit der Wiederherstellung auf kleineren Computerclustern.

Verwenden von Veeam Replication und FSx ONTAP für die Notfallwiederherstellung in VMware Cloud auf AWS

Die Amazon FSx ONTAP Integration mit VMware Cloud auf AWS ist ein von AWS verwalteter externer NFS-Datenspeicher, der auf dem ONTAP -Dateisystem von NetApp basiert und an einen Cluster im SDDC angehängt werden kann. Es bietet Kunden eine flexible, leistungsstarke virtualisierte Speicherinfrastruktur, die unabhängig von den Rechenressourcen skaliert.

Überblick

Kunden, die VMware Cloud on AWS SDDC als Disaster Recovery-Ziel verwenden möchten, können FSx ONTAP Datenspeicher verwenden, um Daten vor Ort mithilfe jeder validierten Drittanbieterlösung zu replizieren, die VM-Replikationsfunktionen bietet. Durch das Hinzufügen des FSx ONTAP Datenspeichers wird eine kostenoptimierte Bereitstellung ermöglicht, als beim Aufbau einer VMware Cloud auf AWS SDDC mit einer enormen Anzahl von ESXi-Hosts, nur um den Speicher unterzubringen.

Dieser Ansatz hilft Kunden auch dabei, Pilot Light Cluster in VMC zusammen mit FSx ONTAP -Datenspeichern zum Hosten der VM-Replikate zu verwenden. Derselbe Prozess kann auch als Migrationsoption auf VMware Cloud auf AWS erweitert werden, indem ein ordnungsgemäßes Failover des Replikationsplans durchgeführt wird.

Problemstellung

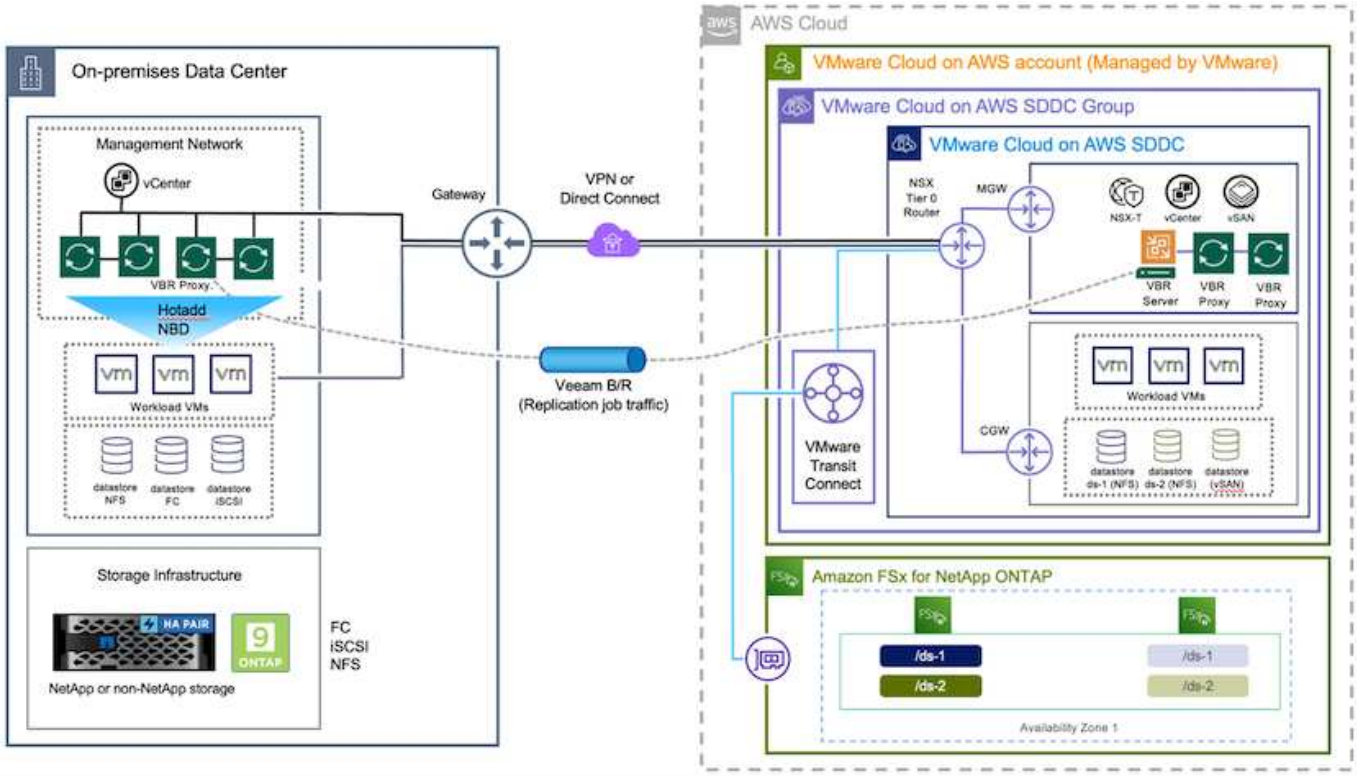
In diesem Dokument wird beschrieben, wie Sie mithilfe des FSx ONTAP Datenspeichers und der Veeam-Sicherung und -Replikation die Notfallwiederherstellung für lokale VMware-VMs in VMware Cloud auf AWS unter Verwendung der VM-Replikationsfunktion einrichten.

Veeam Backup & Replication ermöglicht die Vor-Ort- und Remote-Replikation für die Notfallwiederherstellung (DR). Wenn virtuelle Maschinen repliziert werden, erstellt Veeam Backup & Replication eine exakte Kopie der VMs im nativen VMware vSphere-Format auf dem Ziel-VMware Cloud on AWS SDDC-Cluster und hält die Kopie mit der ursprünglichen VM synchronisiert.

Durch die Replikation werden die besten RTO-Werte (Recovery Time Objective) erzielt, da eine Kopie einer VM im startbereiten Zustand vorliegt. Dieser Replikationsmechanismus stellt sicher, dass die Workloads im Katastrophenfall schnell in VMware Cloud on AWS SDDC gestartet werden können. Die Veeam Backup & Replication-Software optimiert außerdem die Verkehrsübertragung für die Replikation über WAN und langsame Verbindungen. Darüber hinaus filtert es auch doppelte Datenblöcke, Null-Datenblöcke, Auslagerungsdateien und ausgeschlossene VM-Gastbetriebssystemdateien heraus und komprimiert den Replikationsverkehr.

Um zu verhindern, dass Replikationsaufträge die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Netzwerkdrosselungsregeln eingerichtet werden. Der Replikationsprozess in Veeam Backup & Replication ist auftragsgesteuert, d. h. die Replikation wird durch die Konfiguration von Replikationsaufträgen durchgeführt. Im Katastrophenfall kann ein Failover ausgelöst werden, um die VMs durch ein Failover auf ihre Replikatkopie wiederherzustellen.

Beim Failover übernimmt eine replizierte VM die Rolle der ursprünglichen VM. Ein Failover kann auf den neuesten Stand einer Replik oder auf einen ihrer bekannten Wiederherstellungspunkte durchgeführt werden. Dies ermöglicht bei Bedarf eine Ransomware-Wiederherstellung oder isolierte Tests. Bei Veeam Backup & Replication sind Failover und Failback temporäre Zwischenschritte, die weiter finalisiert werden sollten. Veeam Backup & Replication bietet mehrere Optionen zur Handhabung verschiedener Notfallwiederherstellungsszenarien.



Schritte auf hohem Niveau

1. Die Veeam Backup- und Replication-Software wird in einer lokalen Umgebung mit entsprechender Netzwerkkonnektivität ausgeführt.
2. Informationen zur Konfiguration von VMware Cloud on AWS sind im VMware Cloud Tech Zone-Artikel "VMware Cloud auf AWS-Integration mit Amazon FSx ONTAP – Bereitstellungshandbuch" zum Einsetzen und Konfigurieren von VMware Cloud on AWS SDDC und FSx ONTAP als NFS-Datenspeicher zu finden. (Eine Pilot-Light-Umgebung mit einer minimalen Konfiguration kann für DR-Zwecke verwendet werden. Im Falle eines Incident erfolgt das Failover der VMs auf diesen Cluster, und zusätzliche Knoten können hinzugefügt werden.)
3. Richten Sie Replikationsjobs ein, um VM-Replikate mit Veeam Backup and Replication zu erstellen.
4. Erstellen Sie einen Failover-Plan und führen Sie das Failover durch.
5. Wechseln Sie zurück zu Produktions-VMs, sobald das Notfallereignis abgeschlossen ist und die primäre Site aktiv ist.

Voraussetzungen für die Veeam VM-Replikation auf VMC- und FSx ONTAP Datenspeicher

1. Stellen Sie sicher, dass die Sicherungs-VM von Veeam Backup & Replication mit dem Quell-vCenter sowie den Ziel-VMware-Cloud-on-AWS-SDDC-Clustern verbunden ist.
2. Der Sicherungsserver muss in der Lage sein, Kurznamen aufzulösen und eine Verbindung zu Quell- und Ziel-vCentern herzustellen.
3. Der Ziel-FSx ONTAP -Datenspeicher muss über genügend freien Speicherplatz verfügen, um VMDKs replizierter VMs zu speichern

Weitere Informationen finden Sie unter "Überlegungen und Einschränkungen""hier," .

Bereitstellungsdetails

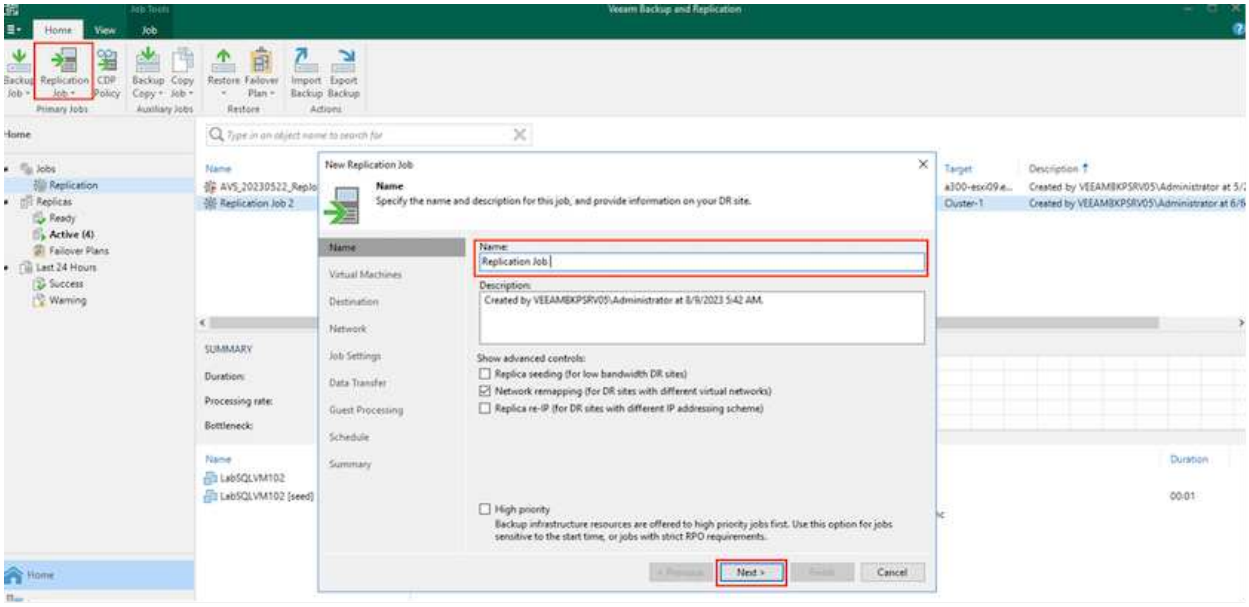
▼ **Schritt 1: VMs replizieren**

Veeam Backup & Replication nutzt die Snapshot-Funktionen von VMware vSphere und fordert während der Replikation VMware vSphere auf, einen VM-Snapshot zu erstellen. Der VM-Snapshot ist die zeitpunktbezogene Kopie einer VM, die virtuelle Festplatten, Systemstatus, Konfiguration usw. enthält. Veeam Backup & Replication verwendet den Snapshot als Datenquelle für die Replikation.

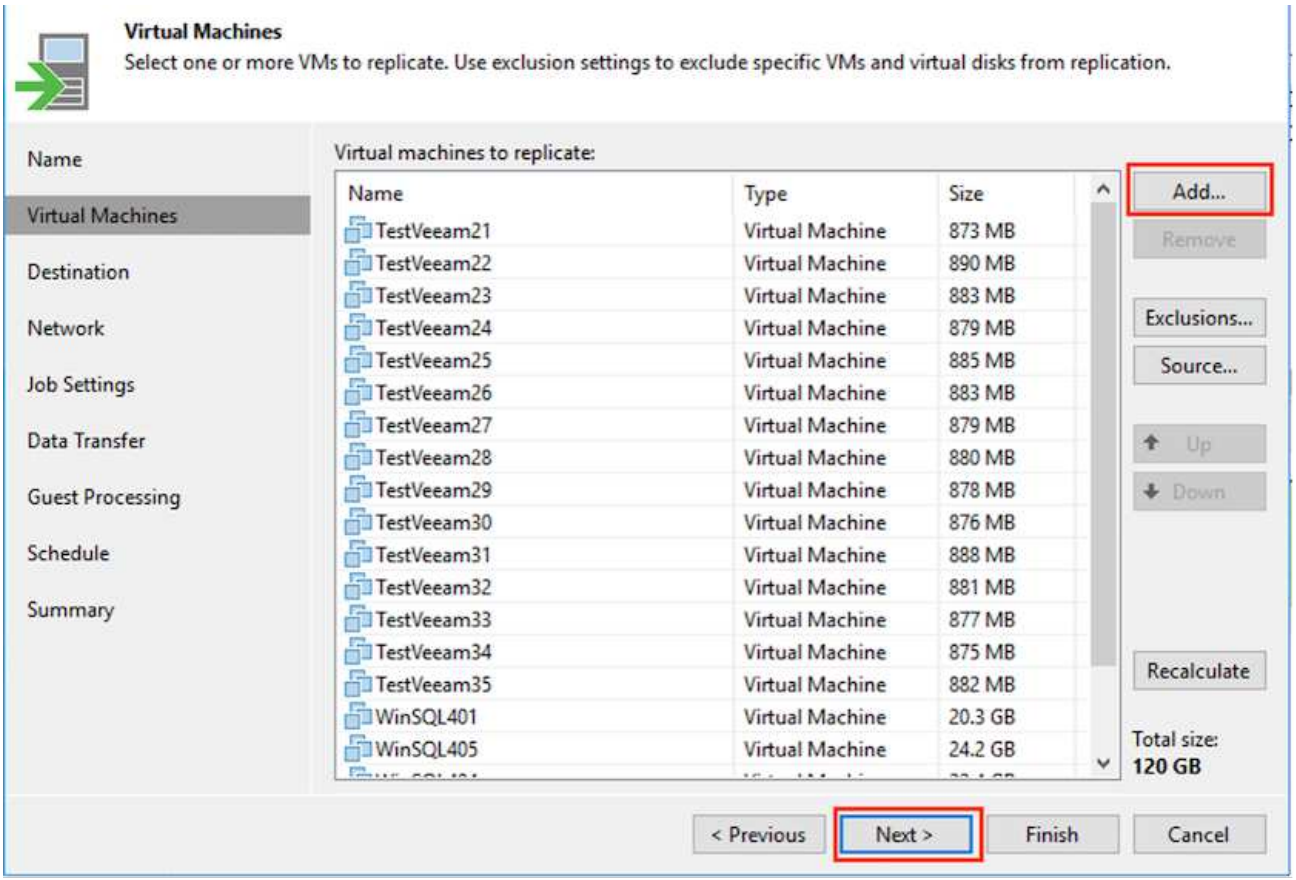
Führen Sie zum Replizieren von VMs die folgenden Schritte aus:

1. Öffnen Sie die Veeam Backup & Replication-Konsole.
2. Wählen Sie in der Home-Ansicht Replikationsauftrag > Virtuelle Maschine > VMware vSphere aus.
3. Geben Sie einen Auftragsnamen an und aktivieren Sie das entsprechende Kontrollkästchen für die erweiterte Steuerung. Klicken Sie auf Weiter.
   - Aktivieren Sie das Kontrollkästchen „Replica Seeding“, wenn die Bandbreite der Konnektivität zwischen lokalen Standorten und AWS eingeschränkt ist.
   - Aktivieren Sie das Kontrollkästchen „Netzwerkneuzuordnung (für AWS VMC-Sites mit unterschiedlichen Netzwerken), wenn die Segmente auf VMware Cloud on AWS SDDC nicht mit denen der lokalen Site-Netzwerke übereinstimmen.
   - Wenn sich das IP-Adressschema am lokalen Produktionsstandort vom Schema am AWS VMC-Standort unterscheidet, aktivieren Sie das Kontrollkästchen „Replikat-Re-IP (für DR-Standorte mit

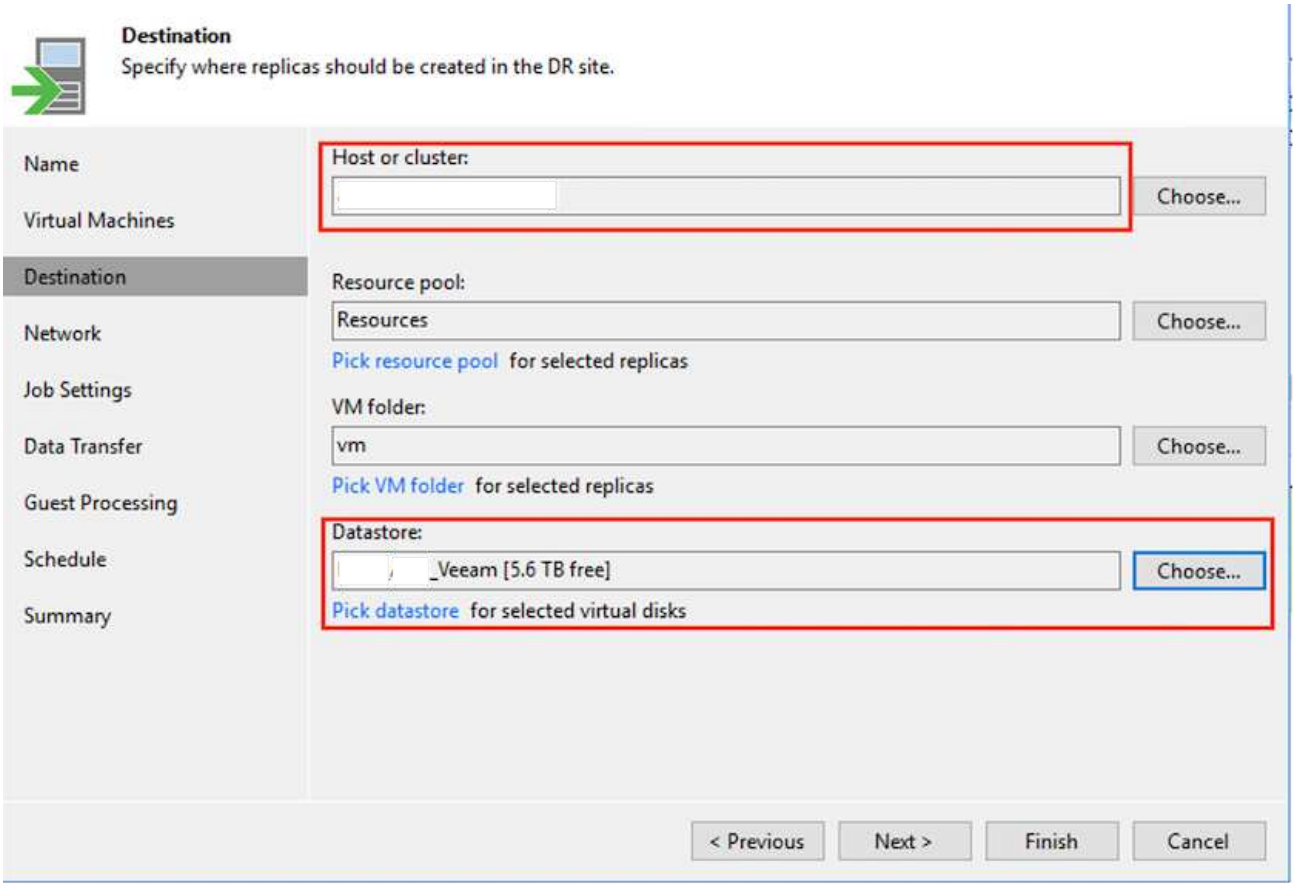
anderem IP-Adressschema)“.



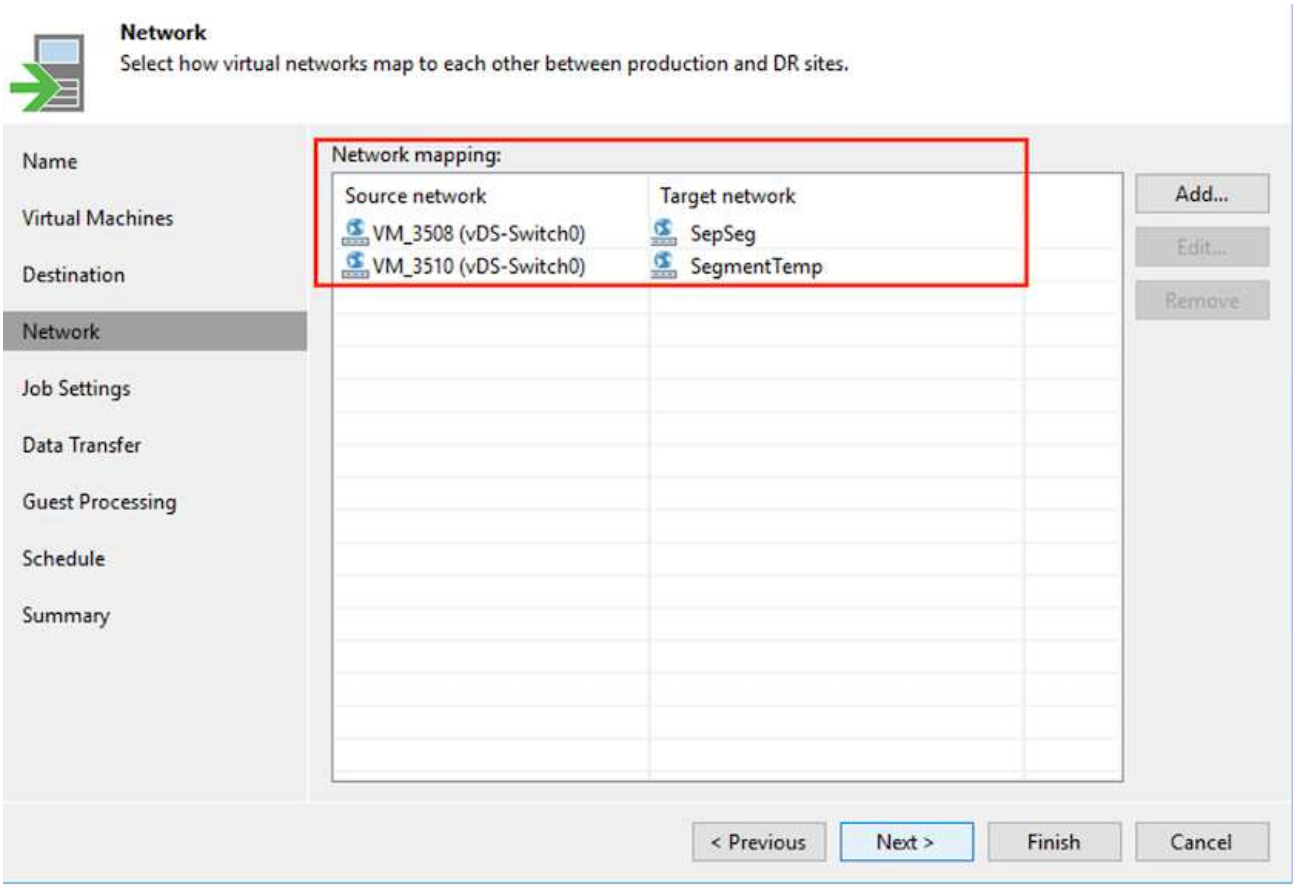
4. Wählen Sie im Schritt **Virtuelle Maschinen** die VMs aus, die in den FSx ONTAP -Datenspeicher repliziert werden müssen, der an VMware Cloud on AWS SDDC angeschlossen ist. Die virtuellen Maschinen können auf vSAN platziert werden, um die verfügbare vSAN-Datenspeicherkapazität zu füllen. In einem Pilotlichtcluster ist die nutzbare Kapazität eines 3-Knoten-Clusters begrenzt. Die restlichen Daten können auf FSx 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**.



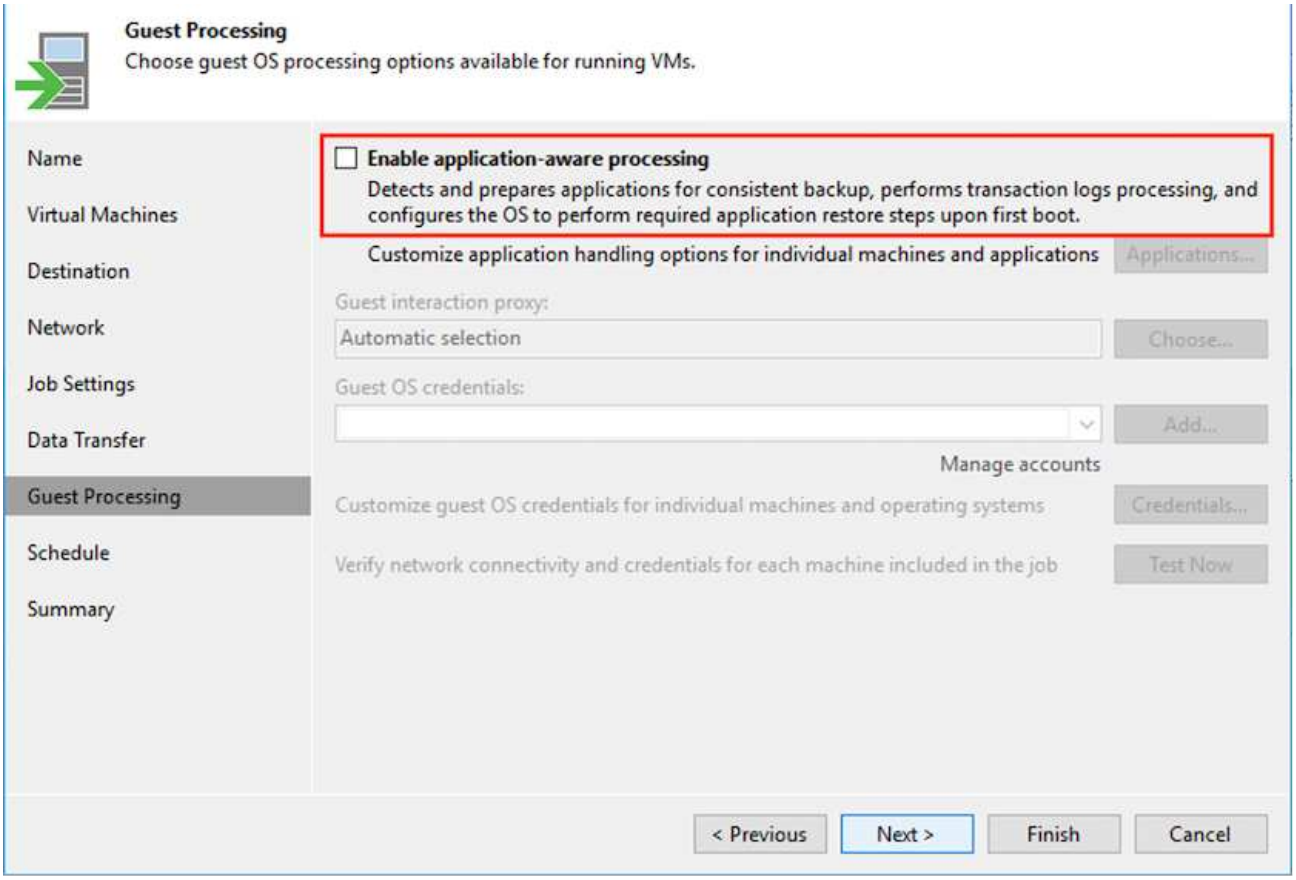
5. Wählen Sie anschließend das Ziel als VMware Cloud on AWS SDDC-Cluster/Host und den entsprechenden Ressourcenpool, VM-Ordner und FSx ONTAP -Datenspeicher für VM-Replikate aus. Klicken Sie dann auf **Weiter**.



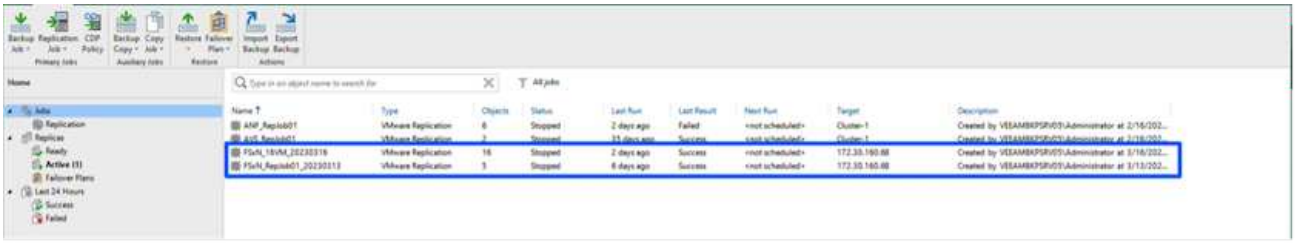
6. Erstellen Sie im nächsten Schritt nach Bedarf die Zuordnung zwischen Quell- und Ziel-Virtual-Network.



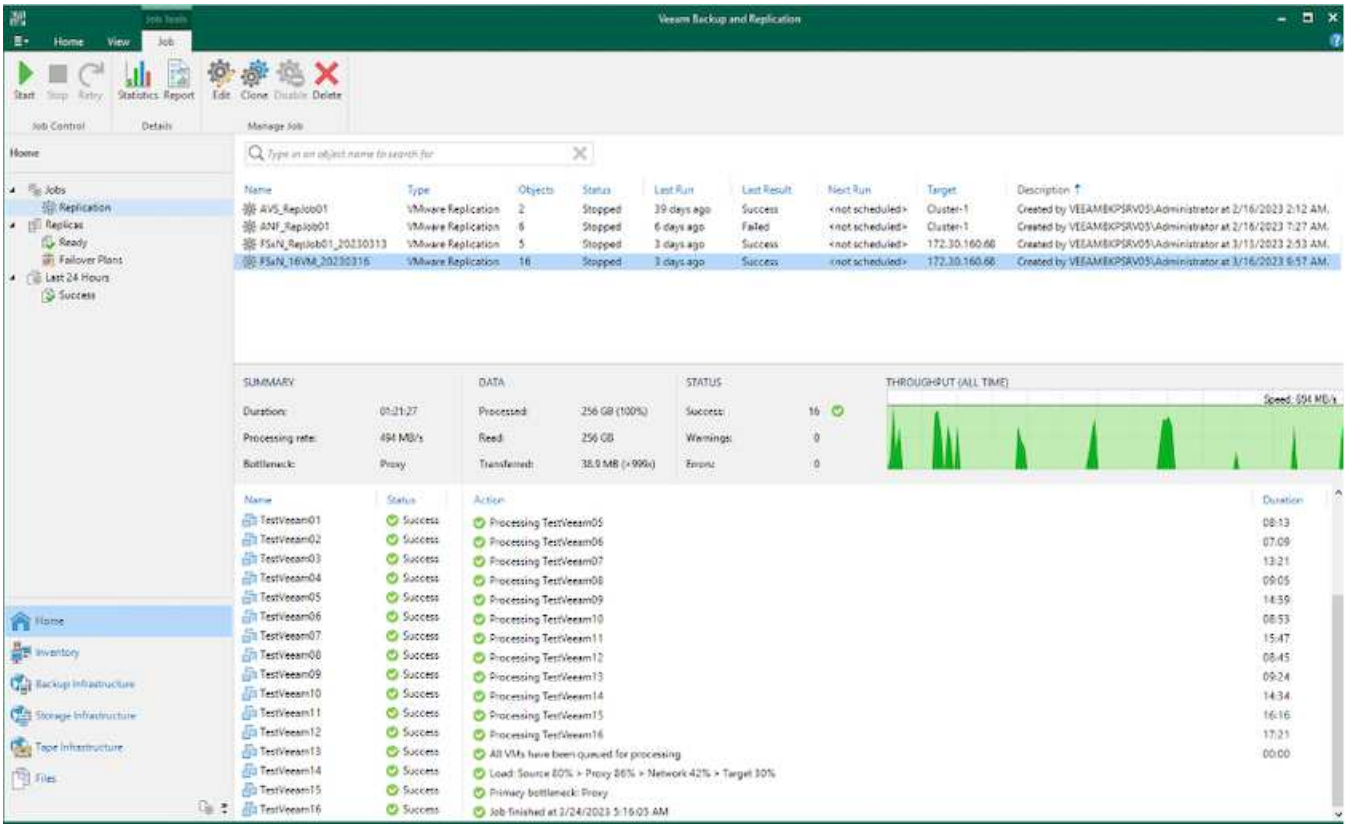
7. Geben Sie im Schritt **Jobeinstellungen** das Sicherungsrepository an, in dem Metadaten für VM-Replikate, Aufbewahrungsrichtlinien usw. gespeichert werden.
8. Aktualisieren Sie die **Quell**- und **Ziel**-Proxyserver im Schritt **Datenübertragung**, belassen Sie die Auswahl **Automatisch** (Standard), lassen Sie die Option **Direkt** ausgewählt und klicken Sie auf **Weiter**.
9. Wählen Sie im Schritt **Gastverarbeitung** nach Bedarf die Option **Anwendungsbewusste Verarbeitung aktivieren**. Klicken Sie auf **Weiter**.



10. Wählen Sie den Replikationszeitplan aus, um den Replikationsauftrag regelmäßig auszuführen.
11. Überprüfen Sie im Schritt **Zusammenfassung** des Assistenten die Details des Replikationsauftrags. 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**, um den Assistenten zu schließen.



Sobald der Replikationsauftrag startet, werden die VMs mit dem angegebenen Suffix auf dem Ziel-VMC-SDDC-Cluster/-Host aufgefüllt.



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

▼ Schritt 2: Erstellen eines Failoverplans

Wenn die erste Replikation oder das Seeding abgeschlossen ist, erstellen Sie den Failover-Plan. Der Failover-Plan hilft dabei, das Failover für abhängige VMs einzeln oder als Gruppe automatisch durchzuführen. Der Failover-Plan ist die Blaupause für die Reihenfolge, in der die VMs verarbeitet werden, einschließlich der Startverzögerungen. Der Failover-Plan hilft auch sicherzustellen, dass kritische abhängige VMs bereits ausgeführt werden.

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 zum Starten von VM-Replikaten.

ⓘ Der Failover-Plan kann erst hinzugefügt werden, wenn die erste Replikation abgeschlossen ist und sich die VM-Replikate im Status „Bereit“ befinden.

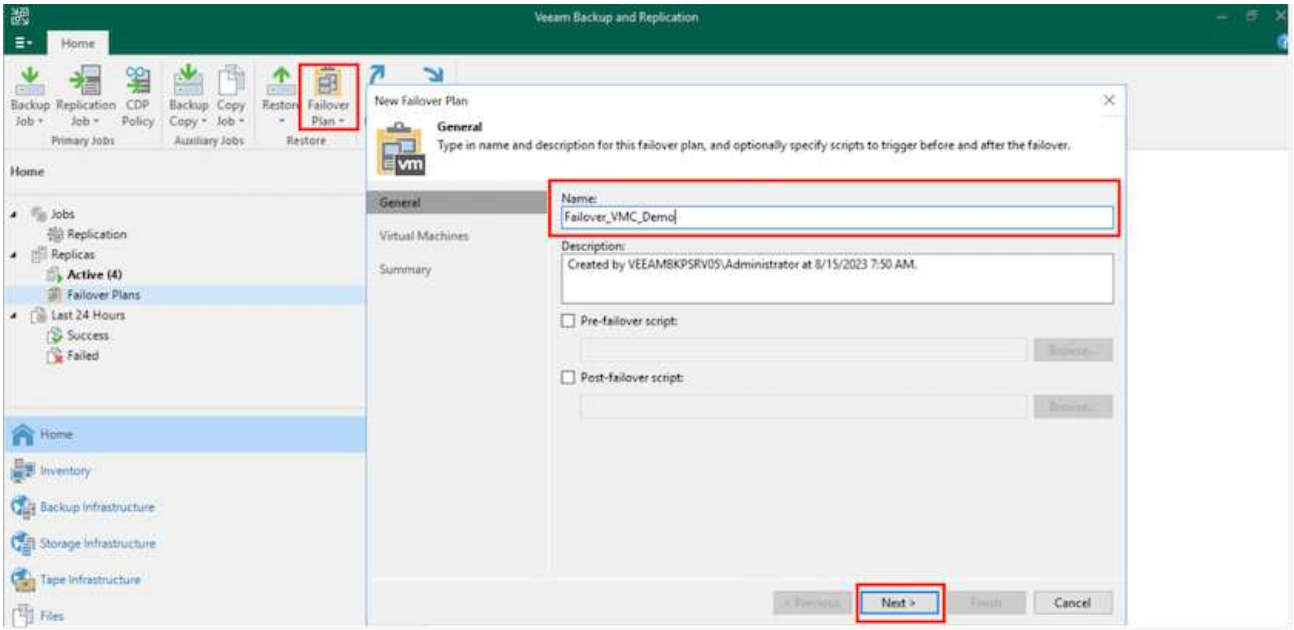
ⓘ Die maximale Anzahl an VMs, die beim Ausführen eines Failover-Plans gleichzeitig gestartet werden können, beträgt 10.

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

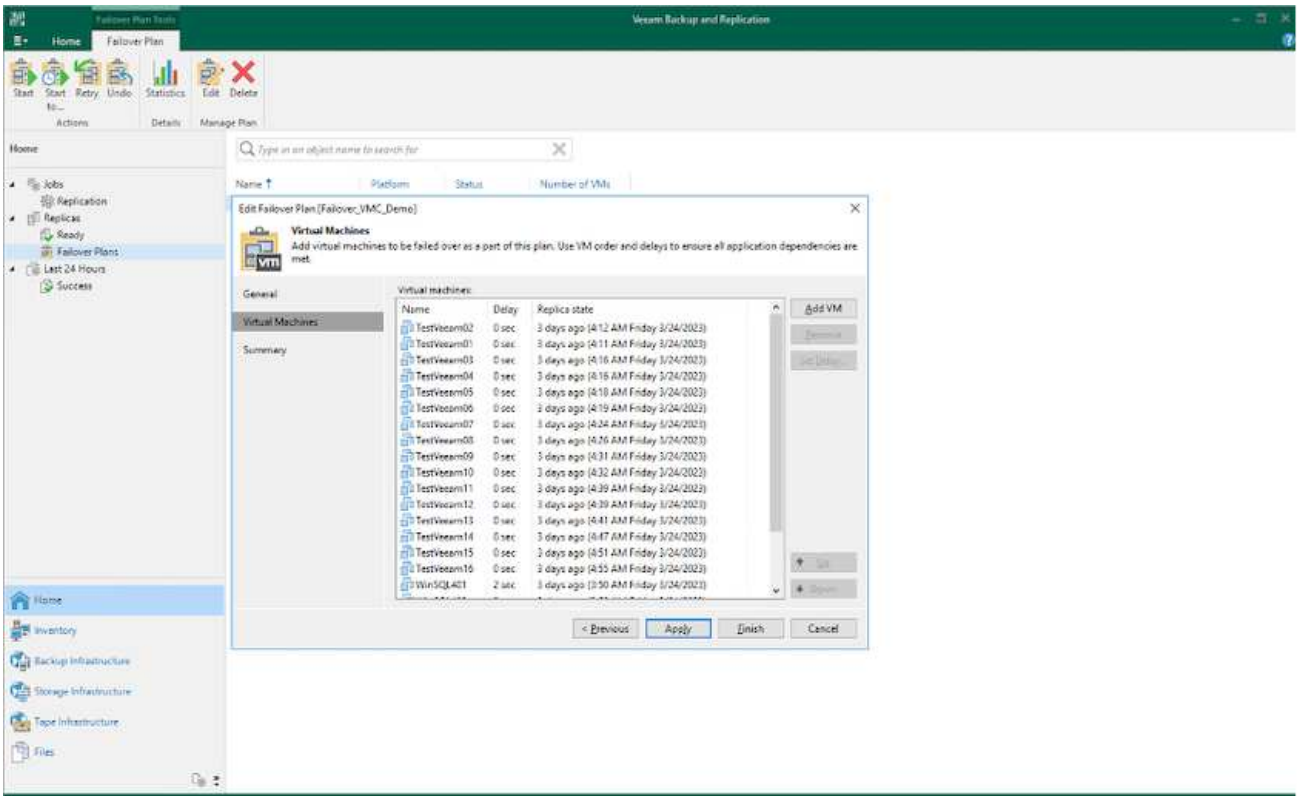
Um den **Failover-Plan** zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie in der Home-Ansicht **Failover-Plan > VMware vSphere**.
2. Geben Sie als Nächstes einen Namen und eine Beschreibung für den Plan ein. Bei Bedarf können Skripte vor und nach dem Failover hinzugefügt werden. Führen Sie beispielsweise ein Skript aus, um

VMs herunterzufahren, bevor Sie die replizierten VMs starten.



3. Fügen Sie die VMs zum Plan hinzu und ändern Sie die Startreihenfolge und Startverzögerungen der VM, um die Anwendungsabhängigkeiten zu erfüllen.



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

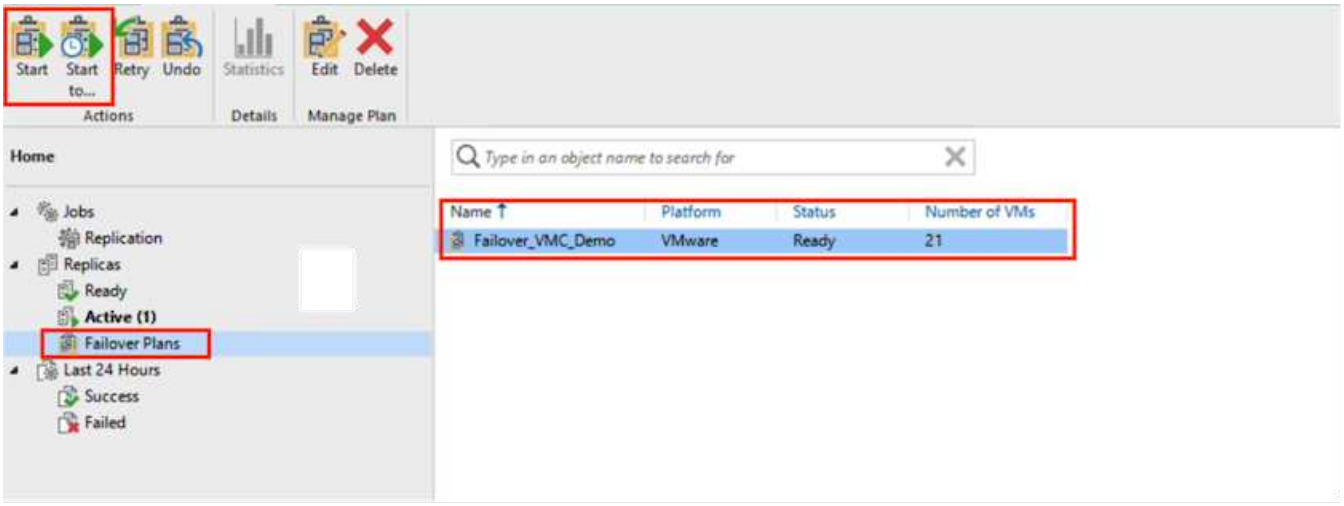
▼ Schritt 3: Ausführen des Failoverplans

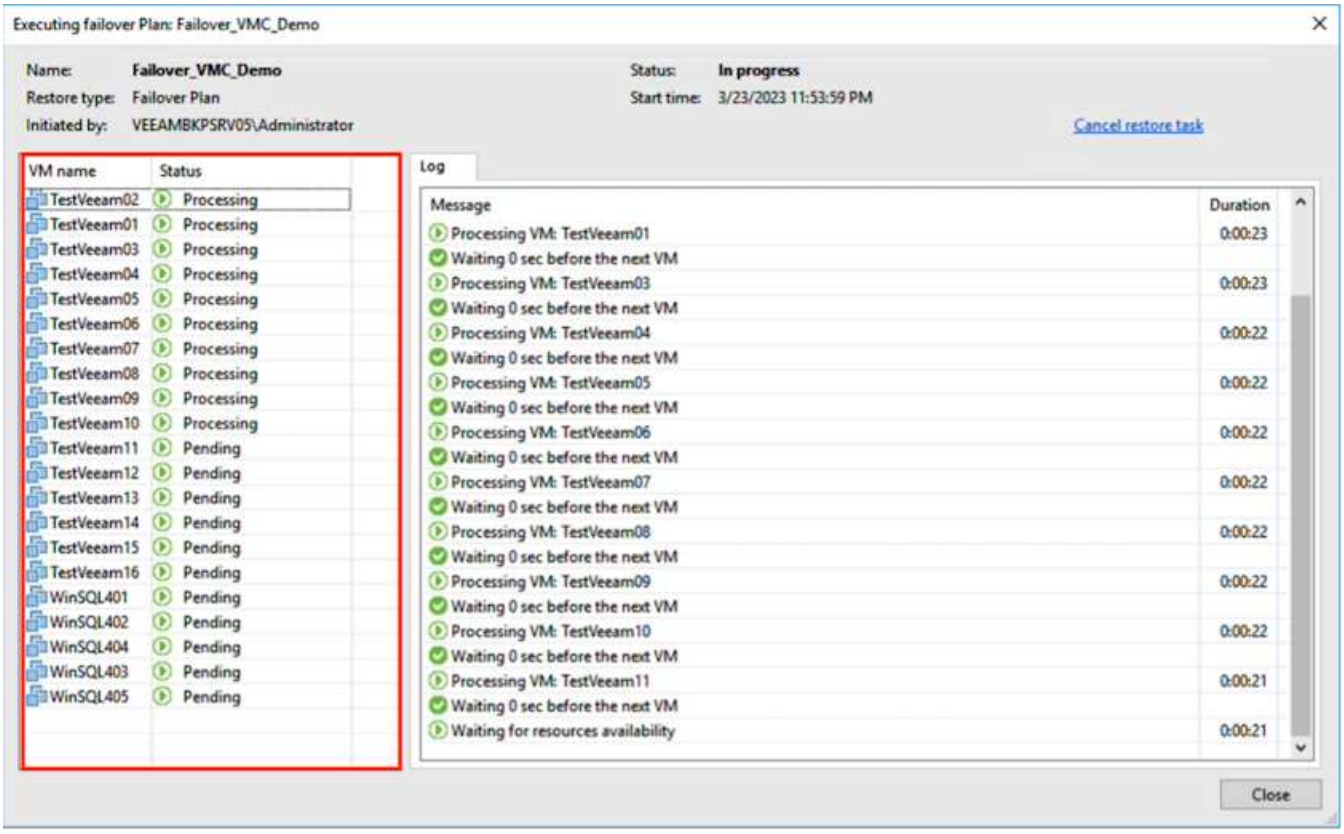
Während des Failovers wird die Quell-VM am Produktionsstandort auf ihre Replik am Disaster-Recovery-Standort umgeschaltet. Als Teil des Failover-Prozesses stellt Veeam Backup & Replication die VM-Replik

am erforderlichen Wiederherstellungspunkt wieder her und verschiebt alle E/A-Aktivitäten von der Quell-VM auf ihre Replik. Replikate können nicht nur im Katastrophenfall, sondern auch zur Simulation von DR-Übungen verwendet werden. Während der Failover-Simulation läuft die Quell-VM weiter. Sobald alle erforderlichen Tests durchgeführt wurden, können Sie das Failover rückgängig machen und zum Normalbetrieb zurückkehren.

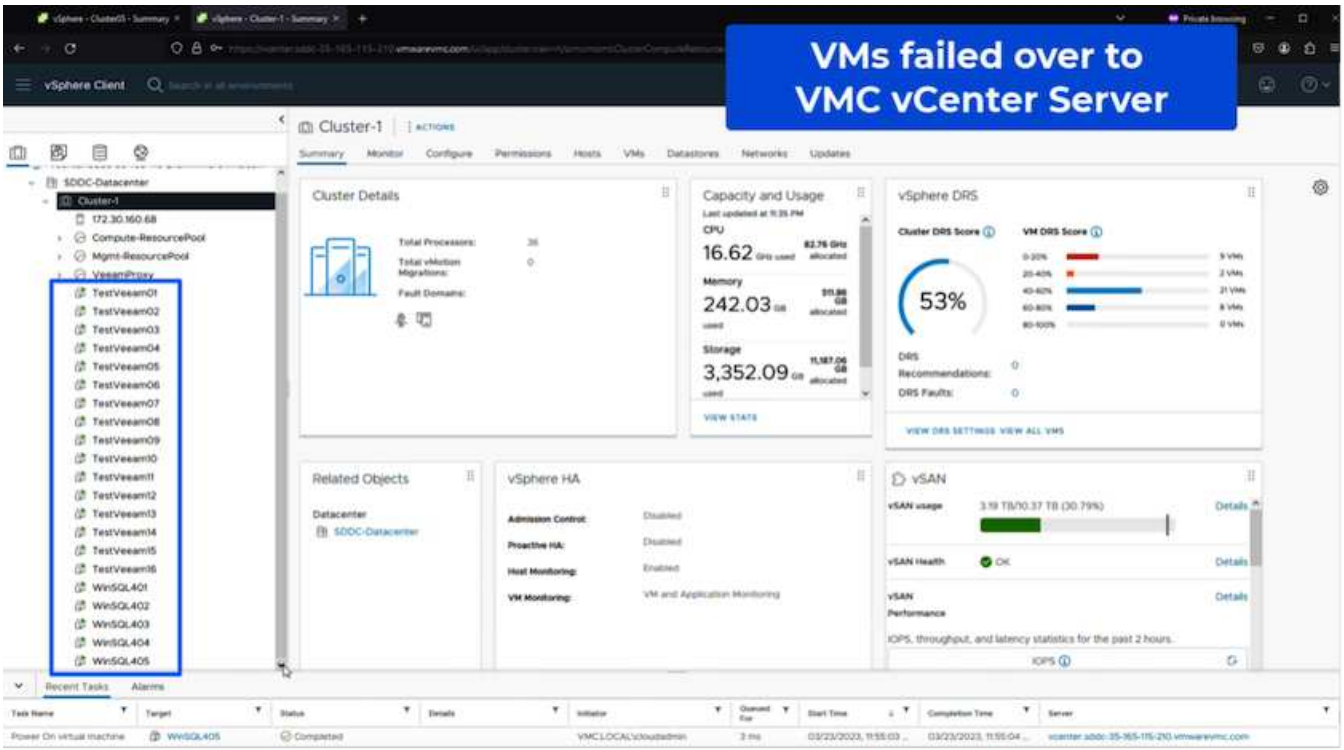
Stellen Sie sicher, dass eine Netzwerksegmentierung vorhanden ist, um IP-Konflikte während DR-Übungen zu vermeiden.

Um den Failover-Plan zu starten, klicken Sie einfach auf die Registerkarte **Failover-Pläne** und klicken Sie mit der rechten Maustaste auf den Failover-Plan. Wählen Sie **Start**. Dabei wird ein Failover unter Verwendung der neuesten Wiederherstellungspunkte der VM-Replikate durchgeführt. Um ein Failover auf bestimmte Wiederherstellungspunkte von VM-Replikaten durchzuführen, wählen Sie **Starten mit**.

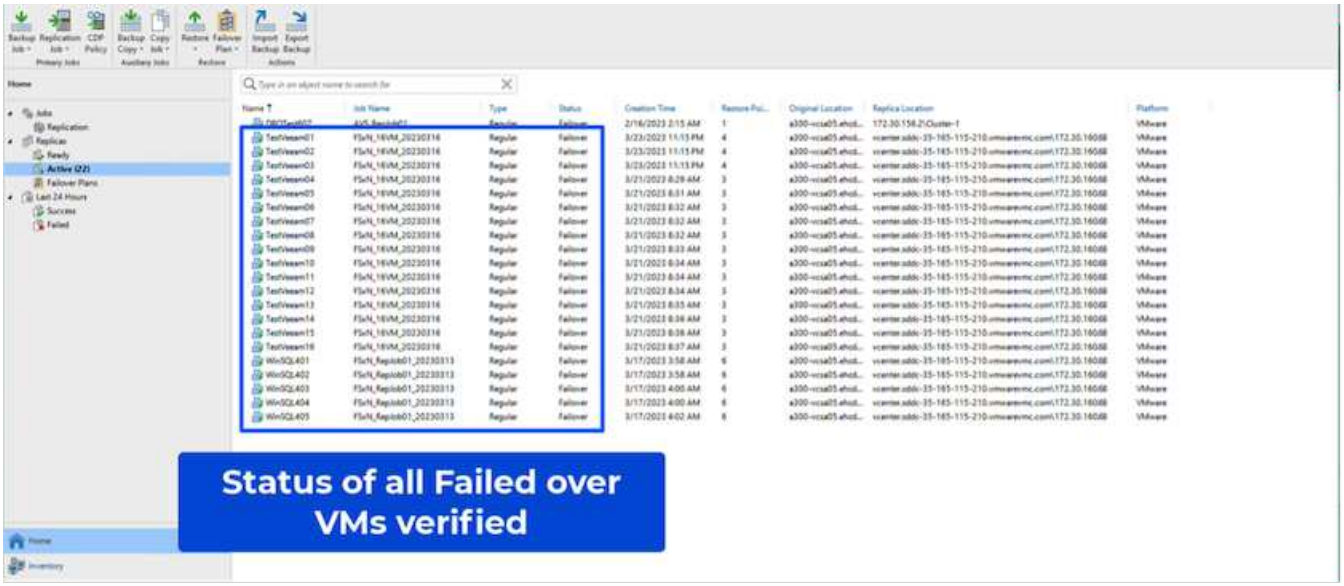




Der Status der VM-Replik ändert sich von „Bereit“ in „Failover“ und VMs werden auf dem Zielcluster/-host von VMware Cloud on AWS SDDC gestartet.



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



Veeam Backup & Replication stoppt alle Replikationsaktivitäten für die Quell-VM, bis deren Replikat wieder in den Zustand „Bereit“ versetzt wird.

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

▼ Schritt 4: Failback zur Produktionssite

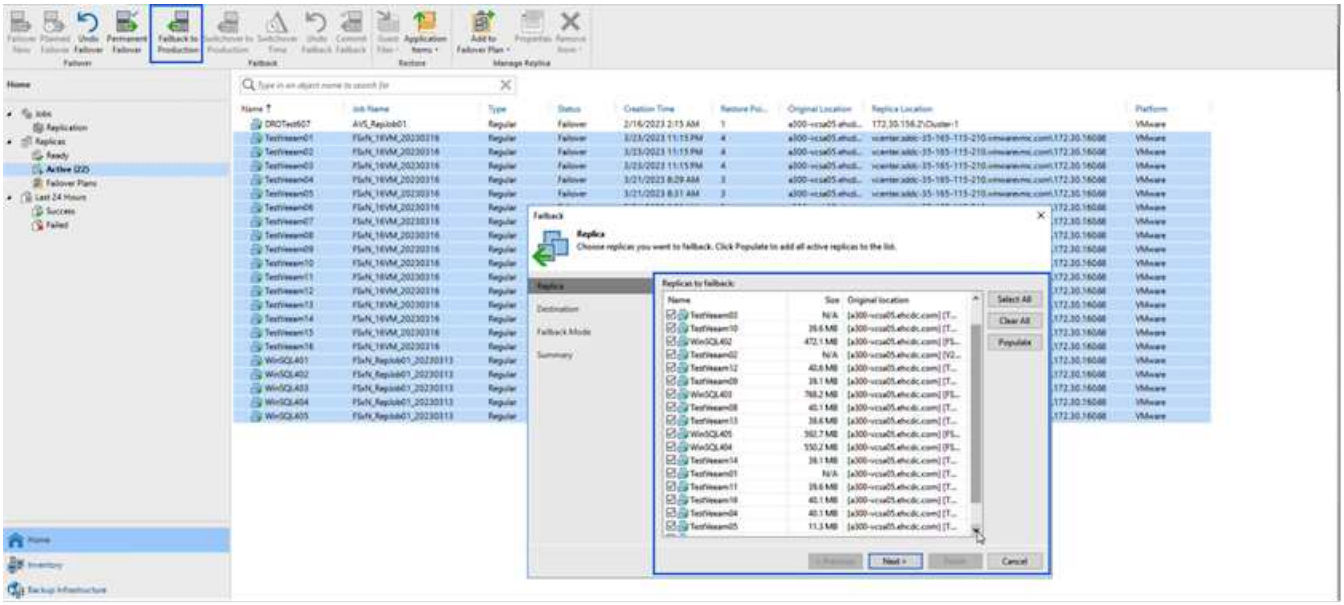
Wenn der Failover-Plan ausgeführt wird, wird er als Zwischenschritt betrachtet und muss je nach Bedarf abgeschlossen werden. Zu den Optionen gehören die folgenden:

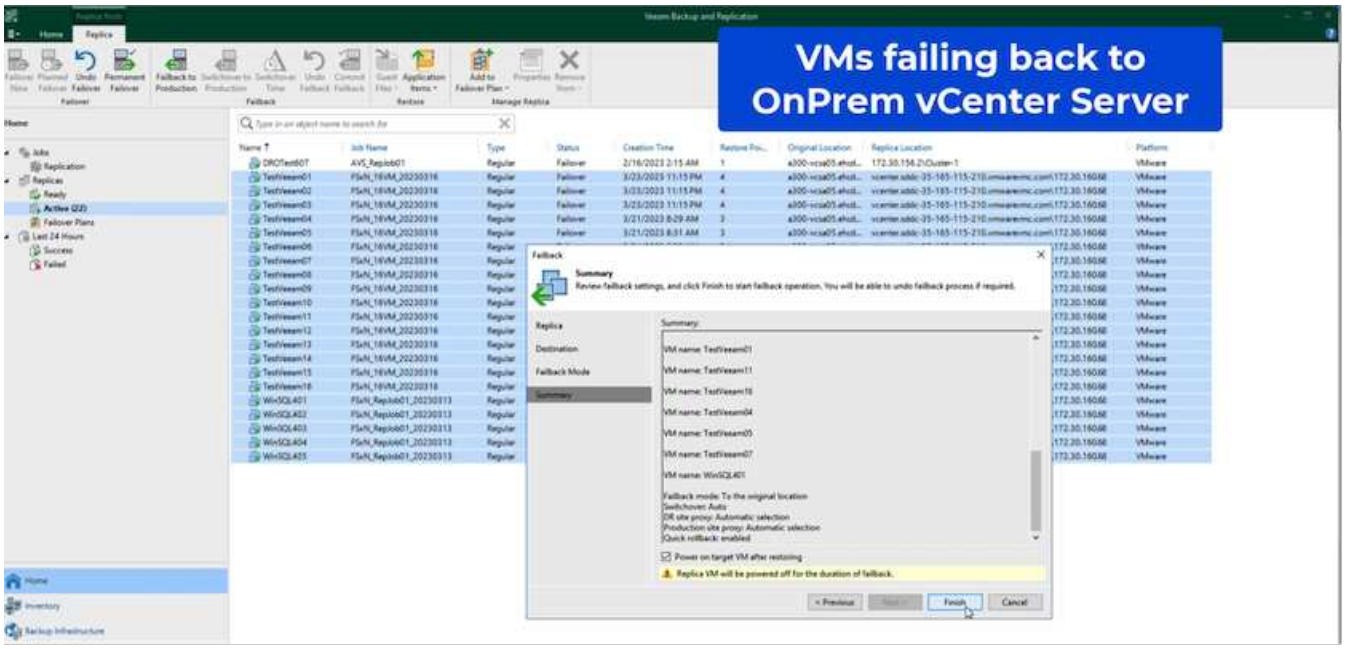
- **Failback zur Produktion** – Wechseln Sie zurück zur ursprünglichen VM und übertragen Sie alle Änderungen, die während der Ausführung der VM-Replik vorgenommen wurden, auf die ursprüngliche VM.

> Wenn Sie ein Failback durchführen, werden Änderungen nur übertragen, aber nicht veröffentlicht. Wählen Sie **Failback festschreiben** (sobald bestätigt wurde, dass die ursprüngliche VM wie erwartet funktioniert) oder **Failback rückgängig machen**, um zur VM-Replik zurückzukehren, wenn die ursprüngliche VM nicht wie erwartet funktioniert.

- **Failover rückgängig machen** – Wechseln Sie zurück zur ursprünglichen VM und verwerfen Sie alle Änderungen, die während der Ausführung an der VM-Replik vorgenommen wurden.
- **Permanentes Failover** – Wechseln Sie dauerhaft von der Original-VM zu einer VM-Replik und verwenden Sie diese Replik als Original-VM.

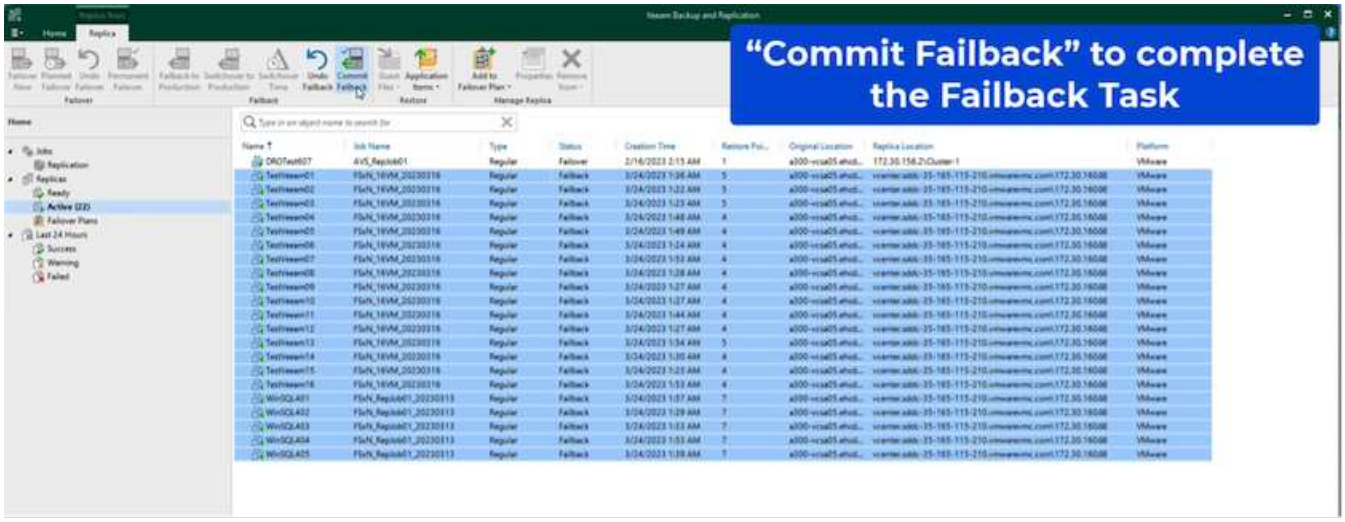
In dieser Demo wurde Failback zur Produktion ausgewählt. Im Schritt „Ziel“ des Assistenten wurde ein Failback zur ursprünglichen VM ausgewählt und das Kontrollkästchen „VM nach der Wiederherstellung einschalten“ aktiviert.

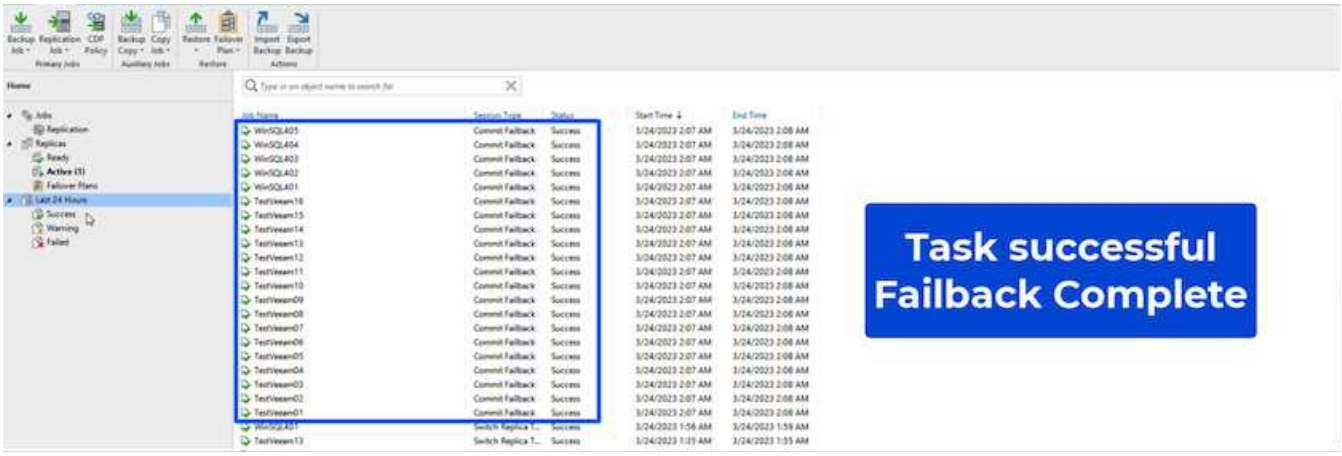




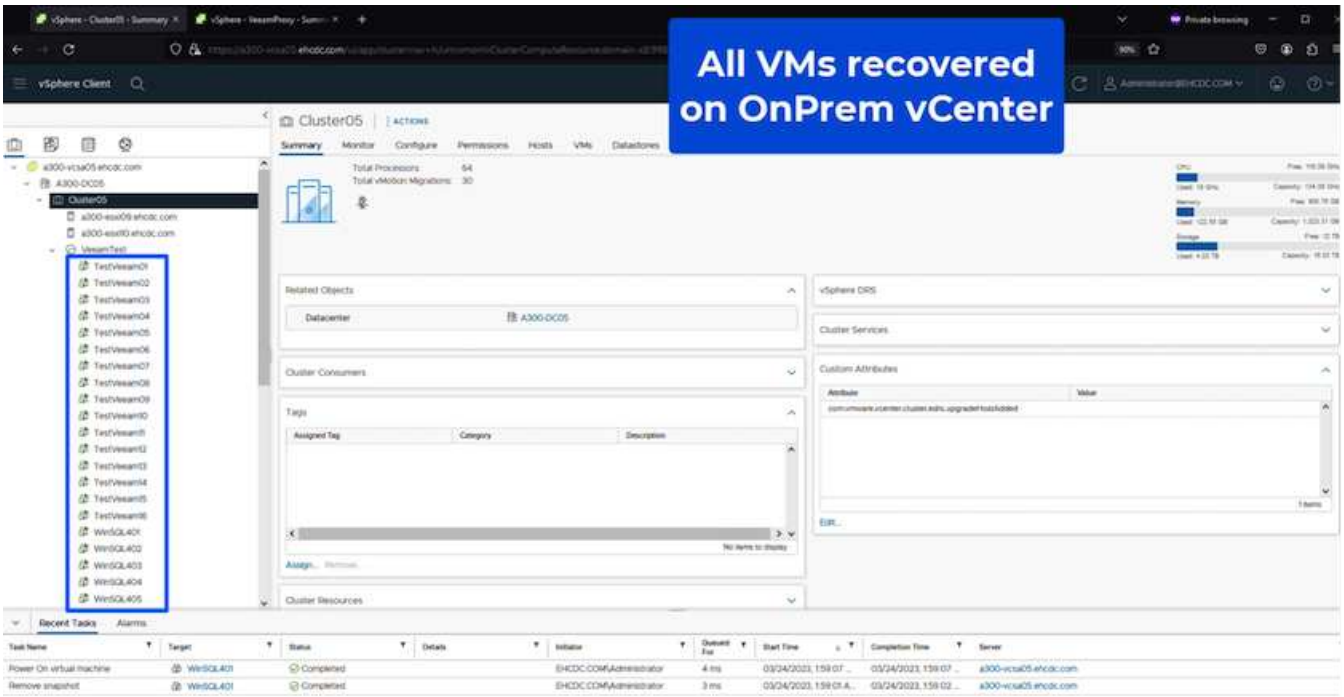
Failback-Commit ist eine der Möglichkeiten, den Failback-Vorgang abzuschließen. Wenn das Failback ausgeführt wird, wird bestätigt, dass die an die VM gesendeten Änderungen, für die das Failback ausgeführt wird (die Produktions-VM), wie erwartet funktionieren. Nach dem Commit-Vorgang nimmt Veeam Backup & Replication die Replikationsaktivitäten für die Produktions-VM wieder auf.

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





Nach einem erfolgreichen Failback zur Produktion werden alle VMs wieder am ursprünglichen Produktionsstandort wiederhergestellt.



Abschluss

Die FSx ONTAP Datenspeicherfunktion ermöglicht es Veeam oder jedem validierten Drittanbietertool, eine kostengünstige DR-Lösung mithilfe des Pilot Light Clusters bereitzustellen, ohne eine große Anzahl von Hosts im Cluster bereitstellen zu müssen, nur um die VM-Replikatkopie unterzubringen. Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten, individuellen Notfallwiederherstellungsplans und ermöglicht außerdem die Wiederverwendung vorhandener Backup-Produkte im Unternehmen, um die DR-Anforderungen zu erfüllen. Dadurch wird eine Cloud-basierte Notfallwiederherstellung durch Verlassen der DR-Rechenzentren vor Ort ermöglicht. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Um mehr über diesen Vorgang zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen.

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

Migrieren Sie Workloads auf AWS/VMC

TR 4942: Migrieren Sie Workloads mit VMware HCX zum FSx ONTAP Datenspeicher

Ein häufiger Anwendungsfall für VMware Cloud (VMC) auf Amazon Web Services (AWS) mit seinem zusätzlichen NFS-Datenspeicher auf Amazon FSx ONTAP ist die Migration von VMware-Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmethoden zum Verschieben lokaler virtueller Maschinen (VMs) und ihrer Daten, die auf allen von VMware unterstützten Datenspeichern ausgeführt werden, in VMC-Datenspeicher, einschließlich zusätzlicher NFS-Datenspeicher auf FSx ONTAP.

Übersicht: Migrieren virtueller Maschinen mit VMware HCX, FSx ONTAP -Zusatzdatenspeichern und VMware Cloud

VMware HCX ist in erster Linie eine Mobilitätsplattform, die die Workload-Migration, die Workload-Neuverteilung und die Geschäftskontinuität über Clouds hinweg vereinfachen soll. Es ist Teil von VMware Cloud auf AWS und bietet zahlreiche Möglichkeiten zur Migration von Workloads und kann für Disaster Recovery (DR)-Vorgänge verwendet werden.

Dieses Dokument bietet eine Schritt-für-Schritt-Anleitung zum Bereitstellen und Konfigurieren von VMware HCX, einschließlich aller Hauptkomponenten, vor Ort und auf der Cloud-Rechenzentrumsseite, wodurch verschiedene VM-Migrationsmechanismen ermöglicht werden.

Weitere Informationen finden Sie unter "VMware HCX-Benutzerhandbuch" Und "Checkliste B installieren – HCX mit einer VMware Cloud on AWS SDDC-Zielumgebung" .

▼ **Schritte auf hoher Ebene**

Diese Liste enthält die wichtigsten Schritte zum Installieren und Konfigurieren von VMware HCX:

1. Aktivieren Sie HCX für das VMC-Software-Defined Data Center (SDDC) über die VMware Cloud Services Console.
2. Laden Sie das OVA-Installationsprogramm für den HCX Connector herunter und stellen Sie es auf dem lokalen vCenter Server bereit.
3. Aktivieren Sie HCX mit einem Lizenzschlüssel.
4. Koppeln Sie den lokalen VMware HCX Connector mit VMC HCX Cloud Manager.
5. Konfigurieren Sie das Netzwerkprofil, das Computeprofil und das Service Mesh.
6. (Optional) Führen Sie eine Netzwerkerweiterung durch, um das Netzwerk zu erweitern und eine erneute IP-Vergabe zu vermeiden.
7. Überprüfen Sie den Gerätestatus und stellen Sie sicher, dass eine Migration möglich ist.
8. Migrieren Sie die VM-Workloads.

▼ **Voraussetzungen**

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

Die folgenden Installationsschritte müssen abgeschlossen sein, bevor Sie mit der Aktivierung und

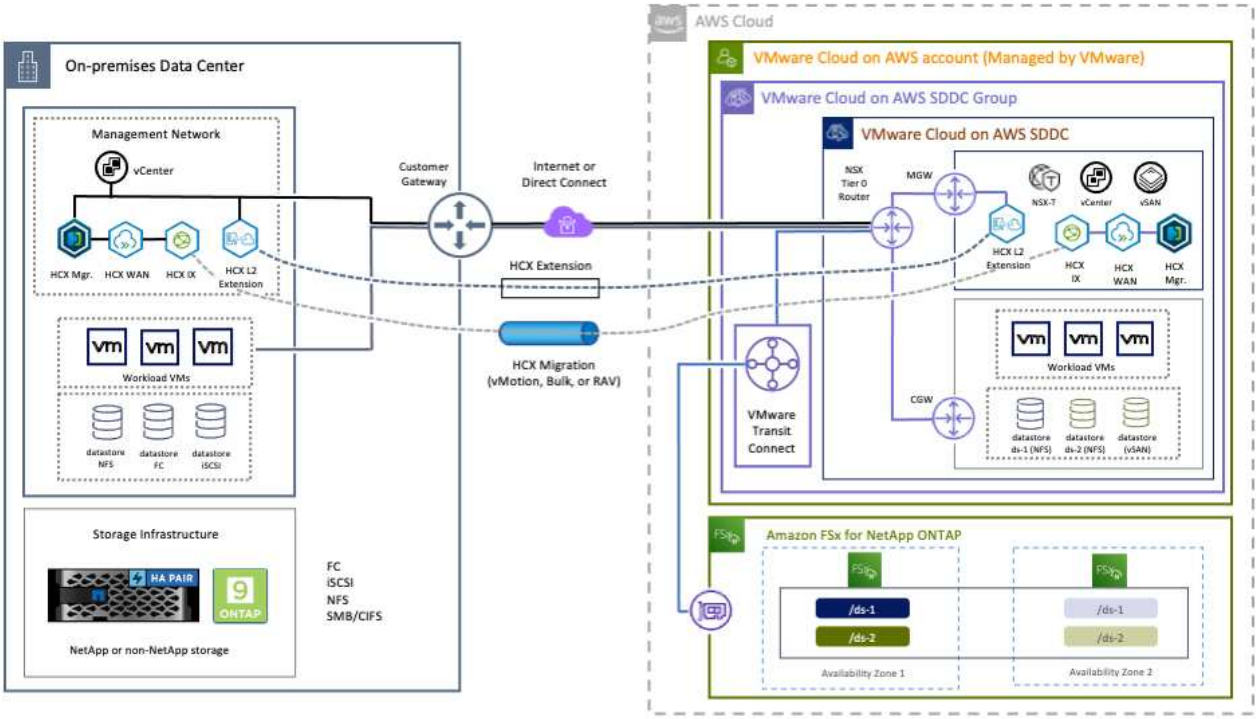
Bereitstellung von HCX fortfahren:

1. Verwenden Sie ein vorhandenes VMC SDDC oder erstellen Sie ein neues SDDC, indem Sie Folgendes befolgen:"NetApp Link" oder das "VMware-Link" .
2. Der Netzwerkpfad von der lokalen vCenter-Umgebung zum VMC SDDC muss die Migration von VMs mithilfe von vMotion unterstützen.
3. Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und Ports" sind für vMotion-Datenverkehr zwischen dem lokalen vCenter Server und dem SDDC vCenter zulässig.
4. Das FSx ONTAP NFS-Volume sollte als zusätzlicher Datenspeicher im VMC SDDC gemountet werden. Um die NFS-Datenspeicher an den entsprechenden Cluster anzuhängen, folgen Sie den Schritten in diesem"NetApp Link" oder das "VMware-Link" .

▼ High-Level-Architektur

Zu Testzwecken wurde die für diese Validierung verwendete lokale Laborumgebung über ein Site-to-Site-VPN mit AWS VPC verbunden, was eine lokale Konnektivität mit AWS und mit VMware Cloud SDDC über ein externes Transit-Gateway ermöglichte. Der Datenverkehr für die HCX-Migration und Netzwerkerweiterung fließt über das Internet zwischen lokalen Standorten und dem VMware Cloud-Ziel-SDDC. Diese Architektur kann so geändert werden, dass private virtuelle Schnittstellen von Direct Connect verwendet werden.

Das folgende Bild zeigt die Architektur auf hoher Ebene.



Lösungsbereitstellung

Befolgen Sie die Schritte, um die Bereitstellung dieser Lösung abzuschließen:

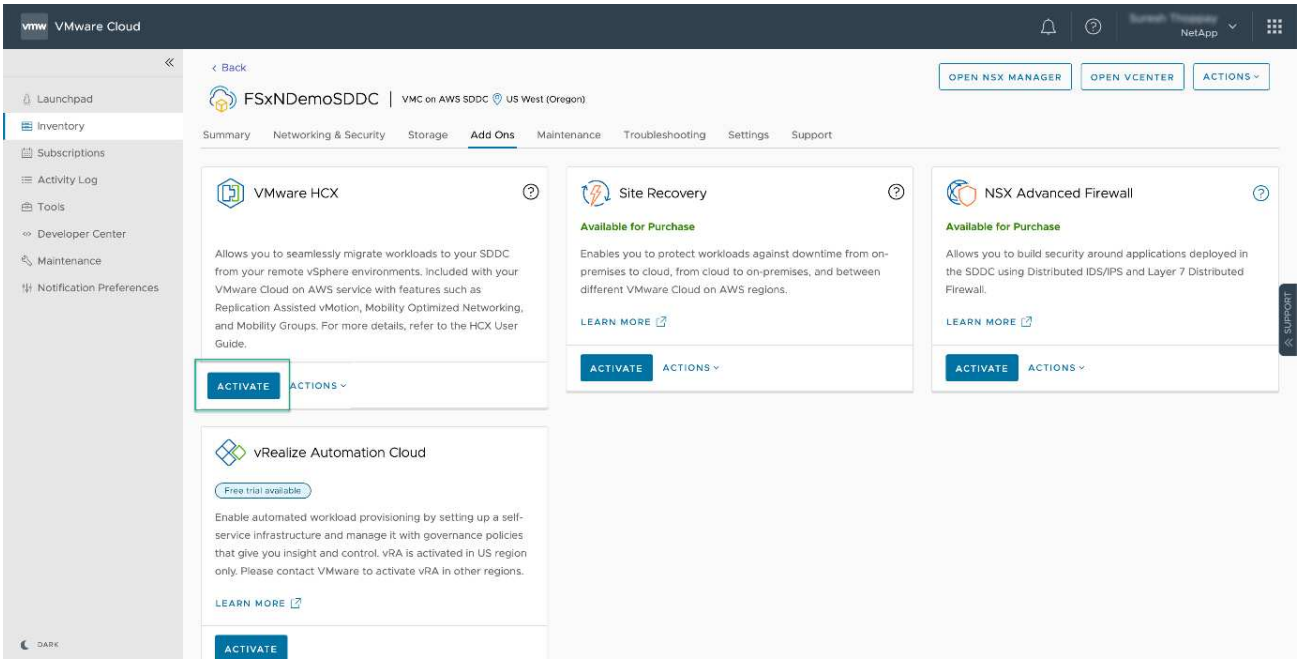
▼ Schritt 1: Aktivieren Sie HCX über VMC SDDC mithilfe der Add-Ons-Option

Führen Sie zur Durchführung der Installation die folgenden Schritte aus:

1. Melden Sie sich bei der VMC-Konsole an unter "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 zum SDDC anzeigen“ und wählen Sie die Registerkarte „Add-Ons“ aus.
3. Klicken Sie auf „Für VMware HCX aktivieren“.

Dieser Schritt kann bis zu 25 Minuten dauern.

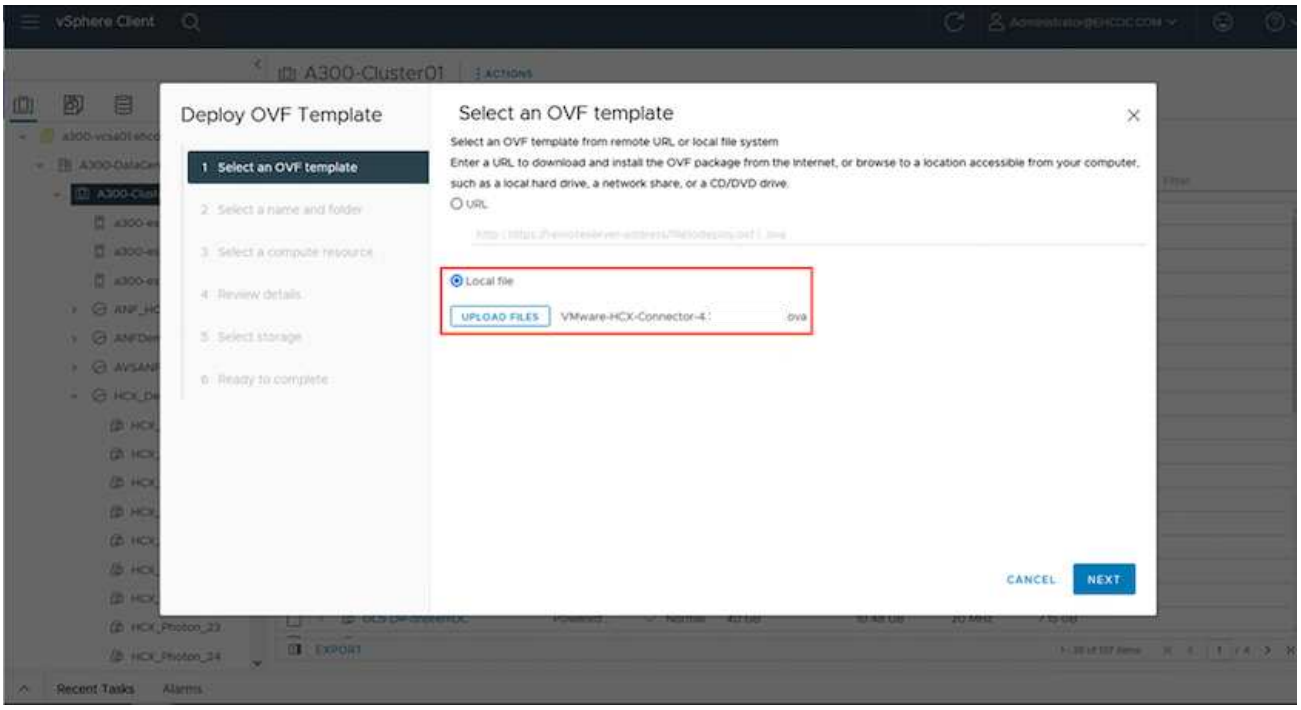


4. Nachdem die Bereitstellung abgeschlossen ist, validieren Sie die Bereitstellung, indem Sie bestätigen, dass HCX Manager und die zugehörigen Plug-Ins in der vCenter-Konsole verfügbar sind.
5. Erstellen Sie die entsprechenden Management Gateway-Firewalls, um die für den Zugriff auf HCX Cloud Manager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

▼ Schritt 2: Bereitstellen der OVA-Installationsdatei im lokalen vCenter Server

Damit der lokale Connector mit dem HCX Manager in VMC kommunizieren kann, stellen Sie sicher, dass die entsprechenden Firewall-Ports in der lokalen 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-Image des HCX Connector anfordern“.
2. Nachdem Sie den HCX Connector heruntergeladen haben, stellen Sie die OVA auf dem lokalen vCenter Server bereit. Klicken Sie mit der rechten Maustaste auf „vSphere-Cluster“ und wählen Sie die Option „OVF-Vorlage bereitstellen“.

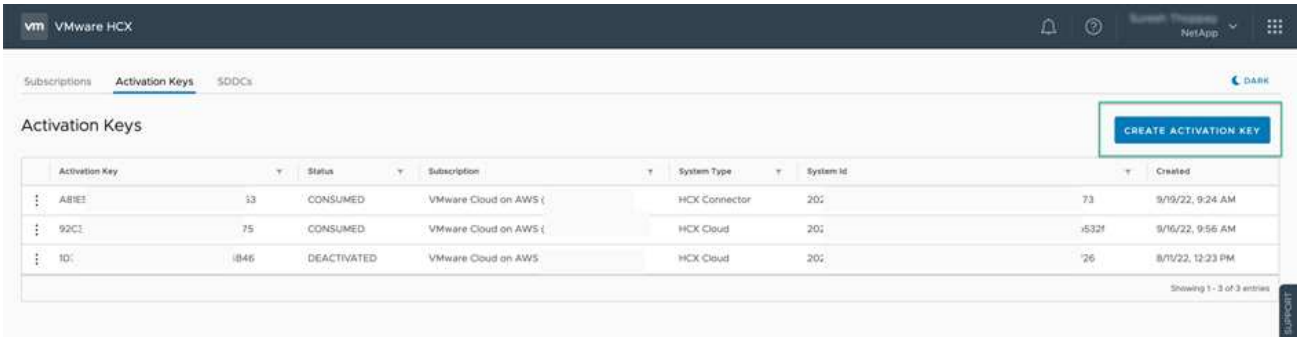


3. Geben Sie die erforderlichen Informationen in den Assistenten „OVF-Vorlage bereitstellen“ ein, klicken Sie auf „Weiter“ und dann auf „Fertig stellen“, um die VMware HCX Connector OVA bereitzustellen.
4. Schalten Sie die virtuelle Appliance manuell ein. Eine Schritt-für-Schritt-Anleitung finden Sie unter "VMware HCX-Benutzerhandbuch" .

▼ **Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren**

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

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



Für jeden vor Ort bereitgestellten HCX-Connector ist ein separater Schlüssel erforderlich.

3. Melden Sie sich beim lokalen VMware HCX Connector an unter "`https://hcxconnectorIP:9443`" mit Administratoranmeldeinformationen.

   Verwenden Sie das während der OVA-Bereitstellung definierte Kennwort.

4. Geben Sie im Abschnitt „Lizenzierung“ den in Schritt 2 kopierten Aktivierungsschlüssel ein und klicken Sie auf „Aktivieren“.

   Damit die Aktivierung erfolgreich abgeschlossen werden kann, muss der lokale HCX-Connector über einen Internetzugang verfügen.

5. Geben Sie unter „Rechenzentrumsstandort“ den gewünschten Speicherort für die lokale Installation des VMware HCX Managers an. Klicken Sie auf „Weiter“.
6. Aktualisieren Sie unter „Systemname“ den Namen und klicken Sie auf „Fortfahren“.
7. Wählen Sie „Ja“ und dann „Weiter“.
8. Geben Sie unter „Verbinden Sie Ihr vCenter“ die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) und die Anmeldeinformationen für den vCenter-Server ein und klicken Sie auf „Fortfahren“.

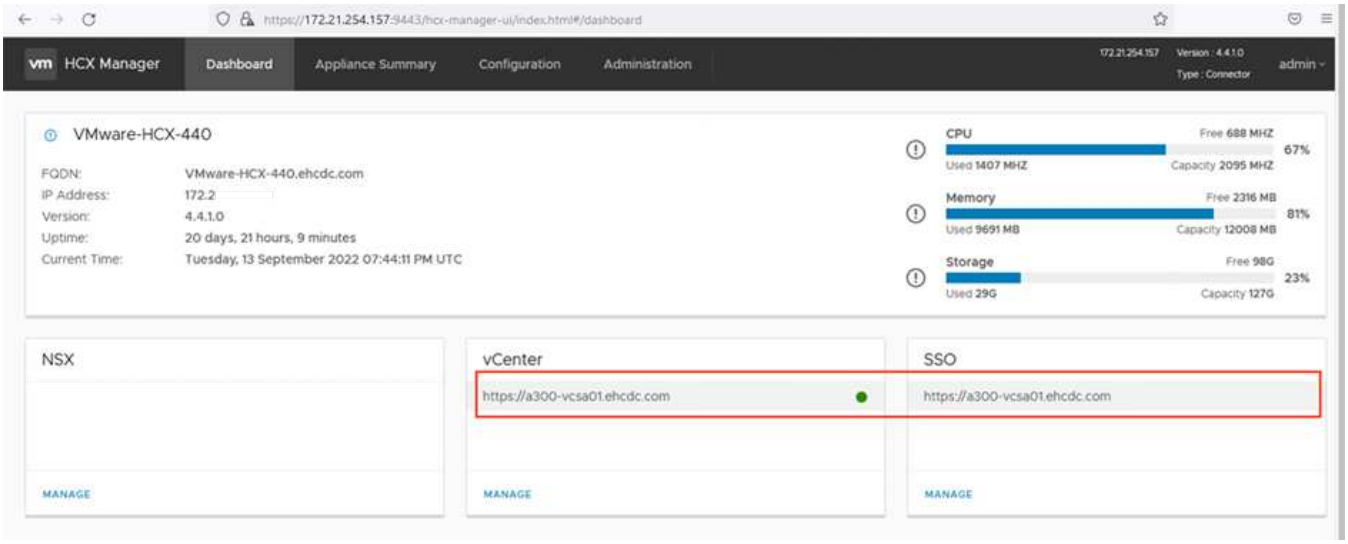
   Verwenden Sie den FQDN, um spätere Kommunikationsprobleme zu vermeiden.

9. Geben Sie unter „SSO/PSC konfigurieren“ den FQDN oder die IP-Adresse des Platform Services Controllers ein und klicken Sie auf „Fortfahren“.

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

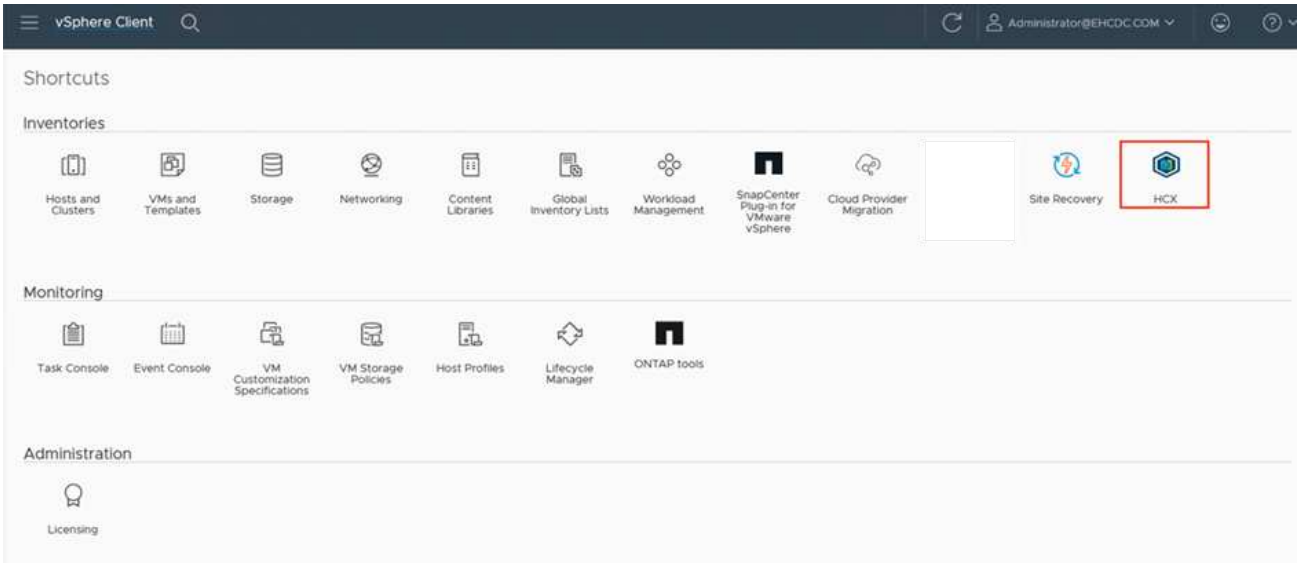
10. Überprüfen Sie, ob die Informationen richtig eingegeben wurden, und klicken Sie auf „Neu starten“.
11. Nach Abschluss wird der vCenter Server grün angezeigt. Sowohl der vCenter Server als auch SSO müssen über die richtigen Konfigurationsparameter verfügen, die mit denen auf der vorherigen Seite übereinstimmen sollten.

    Dieser Vorgang sollte etwa 10–20 Minuten dauern und das Plug-In sollte dem vCenter Server hinzugefügt werden.

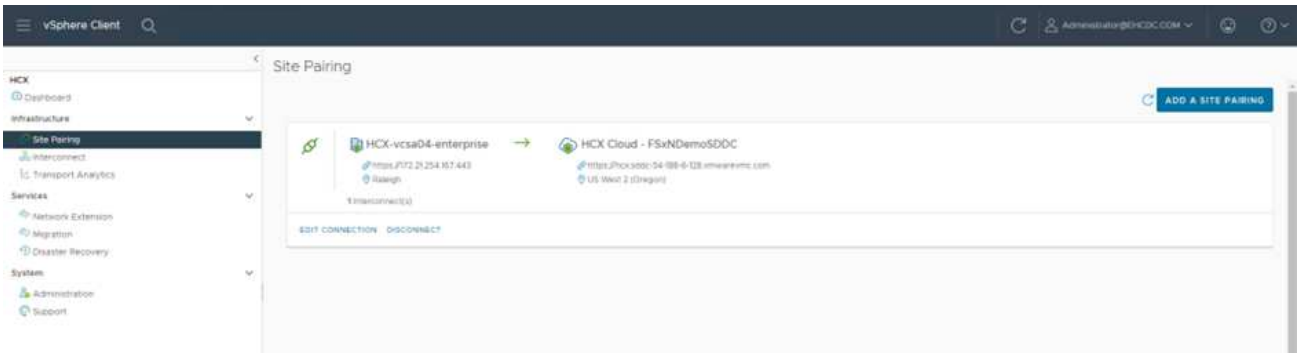


▼ Schritt 4: Koppeln Sie den lokalen VMware HCX Connector mit dem VMC HCX Cloud Manager

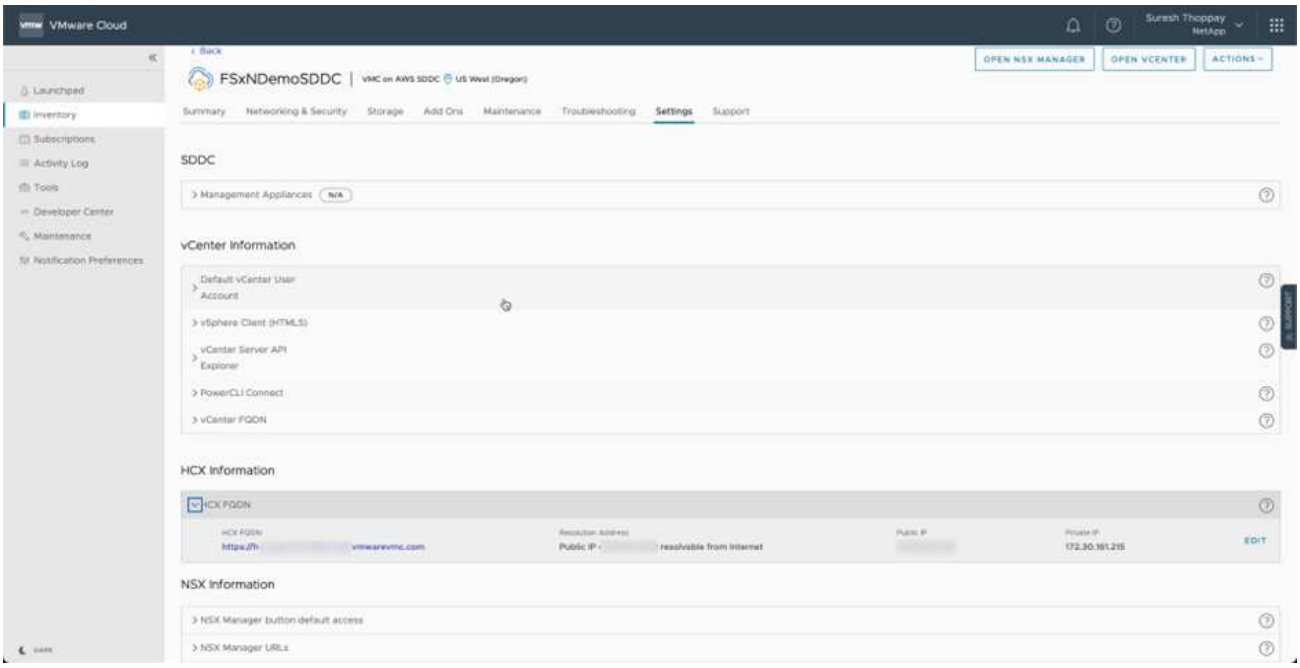
1. Um ein Site-Paar zwischen dem lokalen vCenter Server und dem VMC SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das HCX vSphere Web Client Plug-in zu.

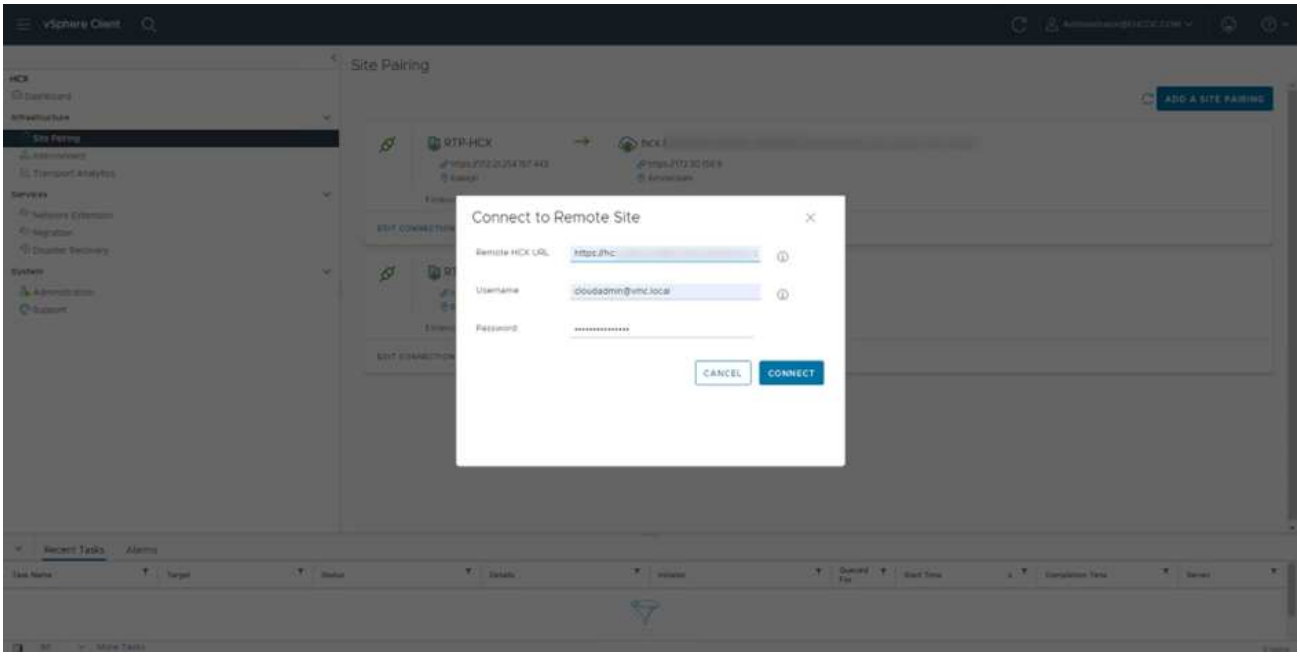


2. Klicken Sie unter „Infrastruktur“ auf „Site-Paarung hinzufügen“. Geben Sie zur Authentifizierung der Remote-Site die URL oder IP-Adresse des VMC HCX Cloud Managers und die Anmeldeinformationen für die CloudAdmin-Rolle ein.



HCX-Informationen können von der SDDC-Einstellungsseite abgerufen werden.





3. Klicken Sie auf „Verbinden“, um die Site-Kopplung zu starten.

> VMware HCX Connector muss über Port 443 mit der HCX Cloud Manager-IP kommunizieren können.

4. Nachdem die Kopplung erstellt wurde, ist die neu konfigurierte Site-Kopplung auf dem HCX-Dashboard verfügbar.

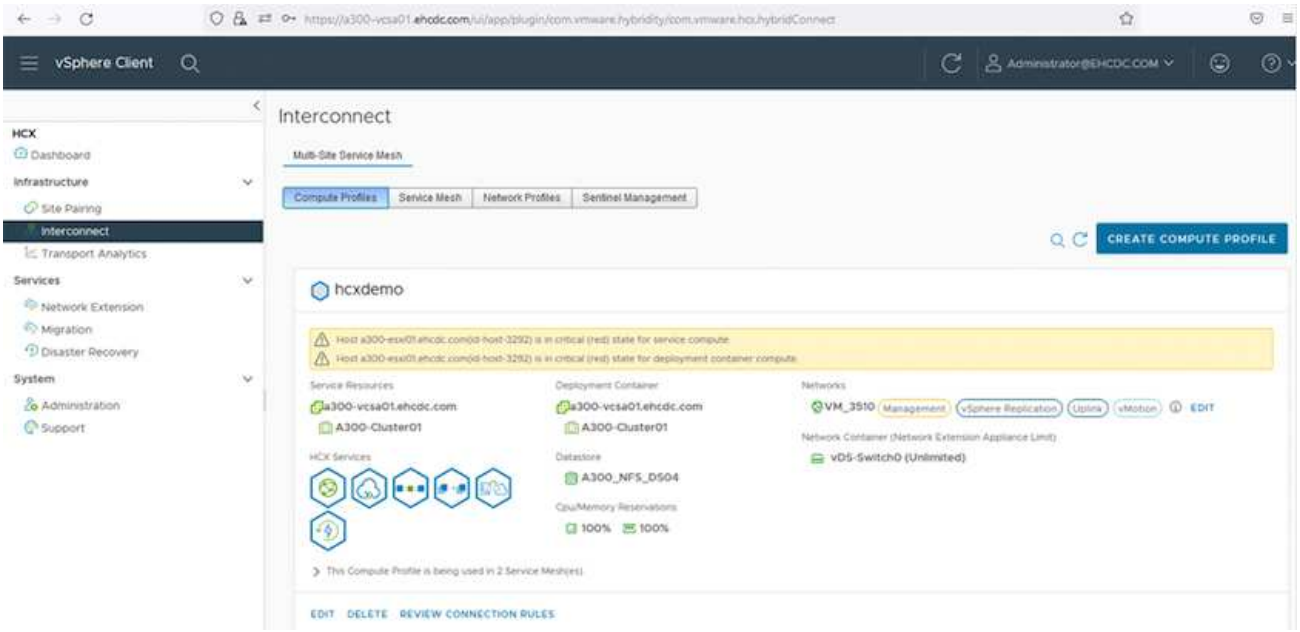
▼ Schritt 5: Konfigurieren Sie das Netzwerkprofil, das Compute-Profil und das Service Mesh

Das VMware HCX Interconnect (HCX-IX)-Gerät bietet sichere Tunnelfunktionen über das Internet und private Verbindungen zum Zielstandort, die Replikations- und vMotion-basierte Funktionen ermöglichen. Die Verbindung bietet Verschlüsselung, Verkehrstechnik und ein SD-WAN. Führen Sie die folgenden Schritte aus, um die HCI-IX Interconnect Appliance zu erstellen:

1. Wählen Sie unter „Infrastruktur“ die Optionen „Interconnect“ > „Multi-Site Service Mesh“ > „Compute-Profile“ > „Compute-Profil erstellen“ aus.

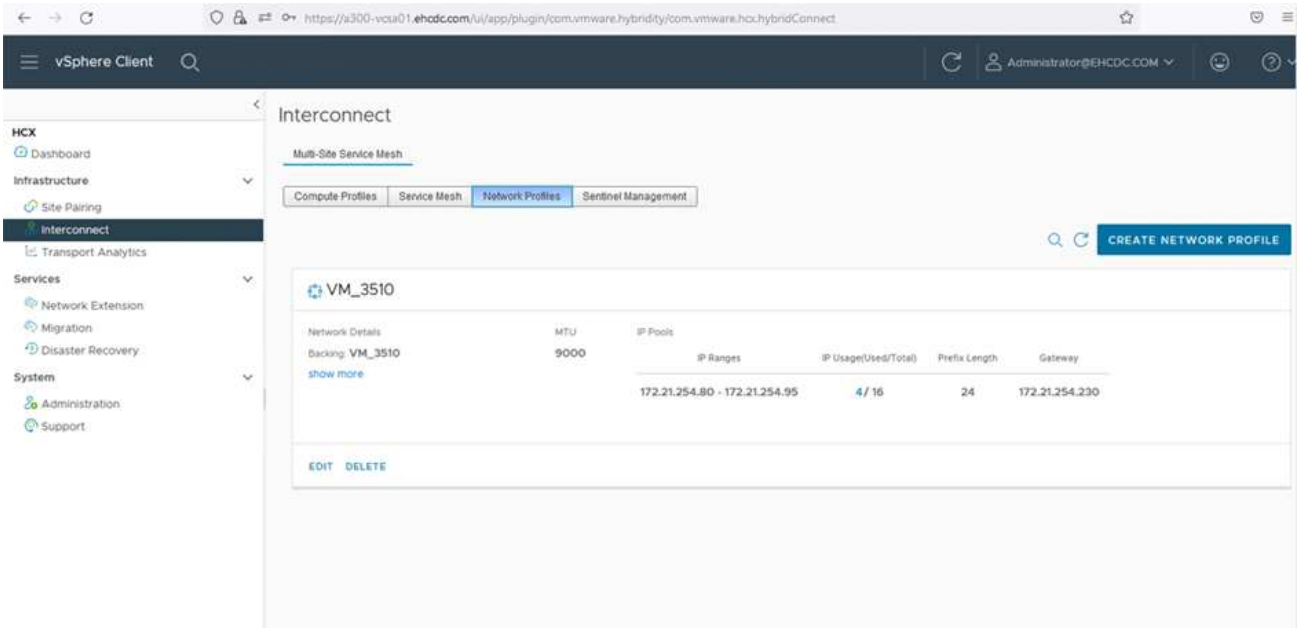
   Rechenprofile enthalten die Rechen-, Speicher- und Netzwerkbereitstellungsparameter, die zum Bereitstellen einer virtuellen Interconnect-Appliance erforderlich sind. Sie geben auch an, auf welchen Teil des VMware-Rechenzentrums der HCX-Dienst zugreifen kann.

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



2. Nachdem das Compute-Profil erstellt wurde, erstellen Sie 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.

   Dies erfordert zwei oder mehr IP-Adressen. Diese IP-Adressen werden vom Verwaltungsnetzwerk an virtuelle Appliances zugewiesen.

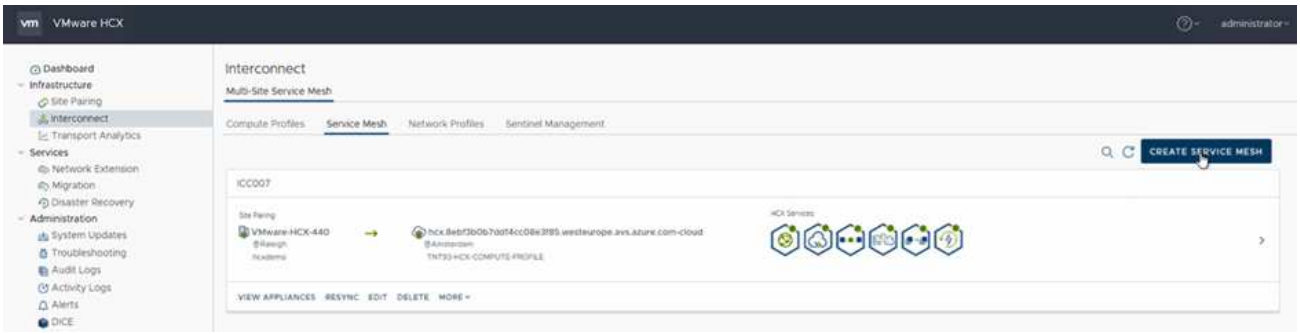


Ausführliche Anweisungen finden Sie unter "Erstellen eines Netzwerkprofils" .

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

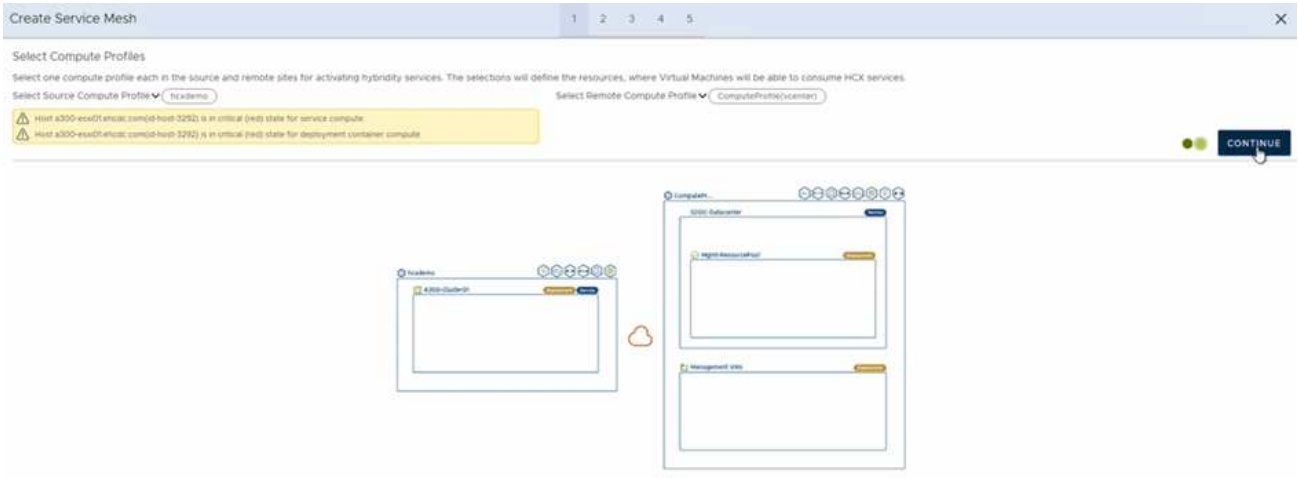
4. Um ein Service Mesh zu erstellen, wählen Sie die Registerkarte „Service Mesh“ innerhalb der Option „Interconnect“ und wählen Sie lokale und VMC SDDC-Sites aus.

   Das Service-Mesh erstellt ein lokales und ein Remote-Compute- und Netzwerkprofilpaar.

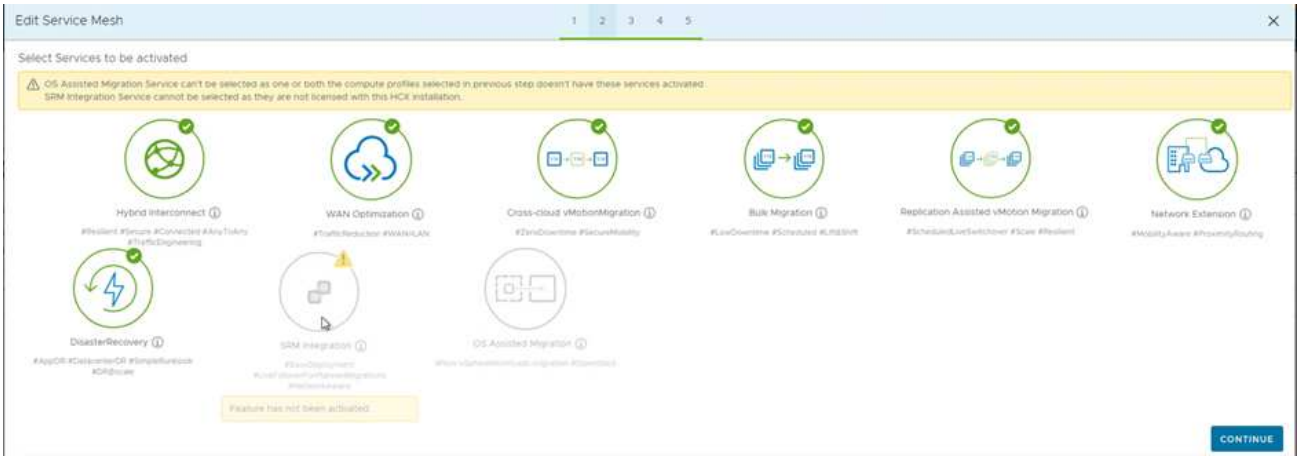


Teil dieses Prozesses ist die Bereitstellung von HCX-Geräten, die sowohl auf den Quell- als auch auf den Zielstandorten automatisch konfiguriert werden und so ein sicheres Transport-Fabric erstellen.

5. Wählen Sie die Quell- und Remote-Compute-Profile aus und klicken Sie auf „Fortfahren“.

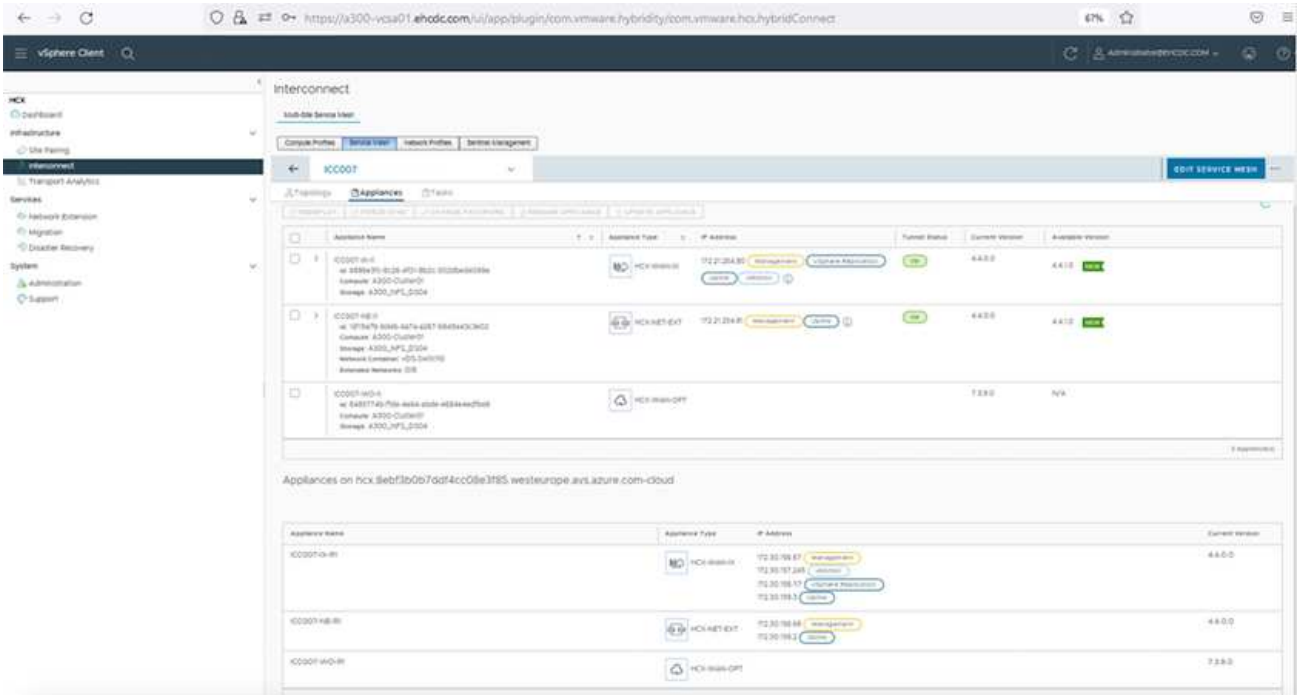


6. Wählen Sie den zu aktivierenden Dienst aus und klicken Sie auf „Weiter“.



> Für Replication Assisted vMotion Migration, SRM Integration und OS Assisted Migration ist eine HCX Enterprise-Lizenz erforderlich.

7. Geben Sie dem Service Mesh einen Namen und klicken Sie auf „Fertig stellen“, um mit dem Erstellungsprozess zu beginnen. Die Bereitstellung sollte etwa 30 Minuten dauern. Nachdem das Service Mesh konfiguriert wurde, wurden die virtuelle Infrastruktur und das Netzwerk erstellt, die zum Migrieren der Workload-VMs erforderlich sind.



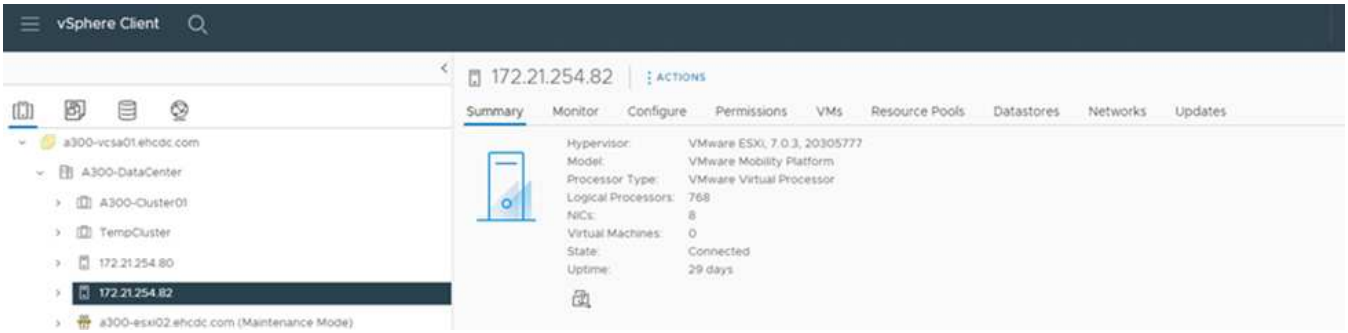
▼ Schritt 6: Migrieren von Workloads

HCX bietet bidirektionale Migrationsdienste zwischen zwei oder mehr unterschiedlichen Umgebungen wie lokalen Umgebungen und VMC SDDCs. Anwendungs-Workloads können mithilfe einer Vielzahl von Migrationstechnologien wie HCX-Massenmigration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (verfügbar mit HCX Enterprise Edition) und HCX OS Assisted Migration (verfügbar mit HCX Enterprise Edition) zu und von HCX-aktivierten Sites migriert werden.

Weitere Informationen zu verfügbaren HCX-Migrationstechnologien finden Sie unter "VMware HCX-Migrationstypen"

Das HCX-IX-Gerät verwendet den Mobility Agent-Dienst, um vMotion-, Cold- und Replication Assisted vMotion (RAV)-Migrationen durchzuführen.

ⓘ Die HCX-IX-Appliance fügt den Mobility Agent-Dienst als Hostobjekt im vCenter Server hinzu. Die in diesem Objekt angezeigten Prozessor-, Speicher-, Speicher- und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch auf dem physischen Hypervisor dar, auf dem die IX-Appliance gehostet wird.



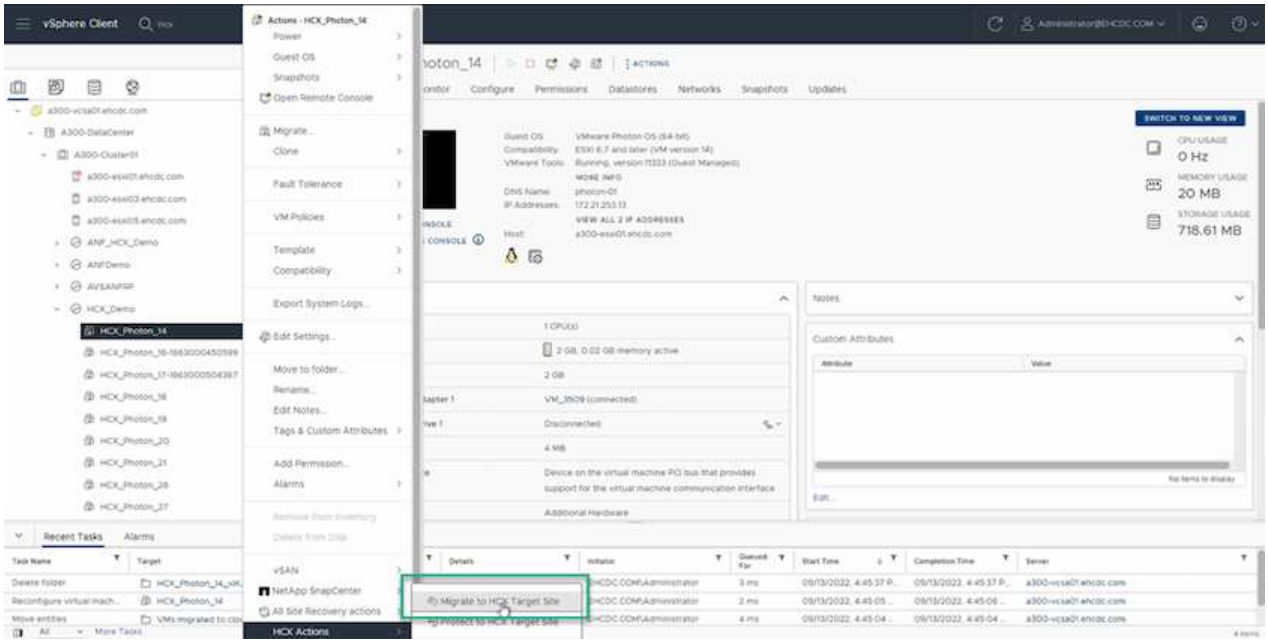
▼ VMware HCX vMotion

In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie verwendet das VMware vMotion-Protokoll, um eine VM zu VMC SDDC zu migrieren. Die Migrationsoption vMotion wird zum Migrieren des VM-Status jeweils einer einzelnen VM verwendet. Bei

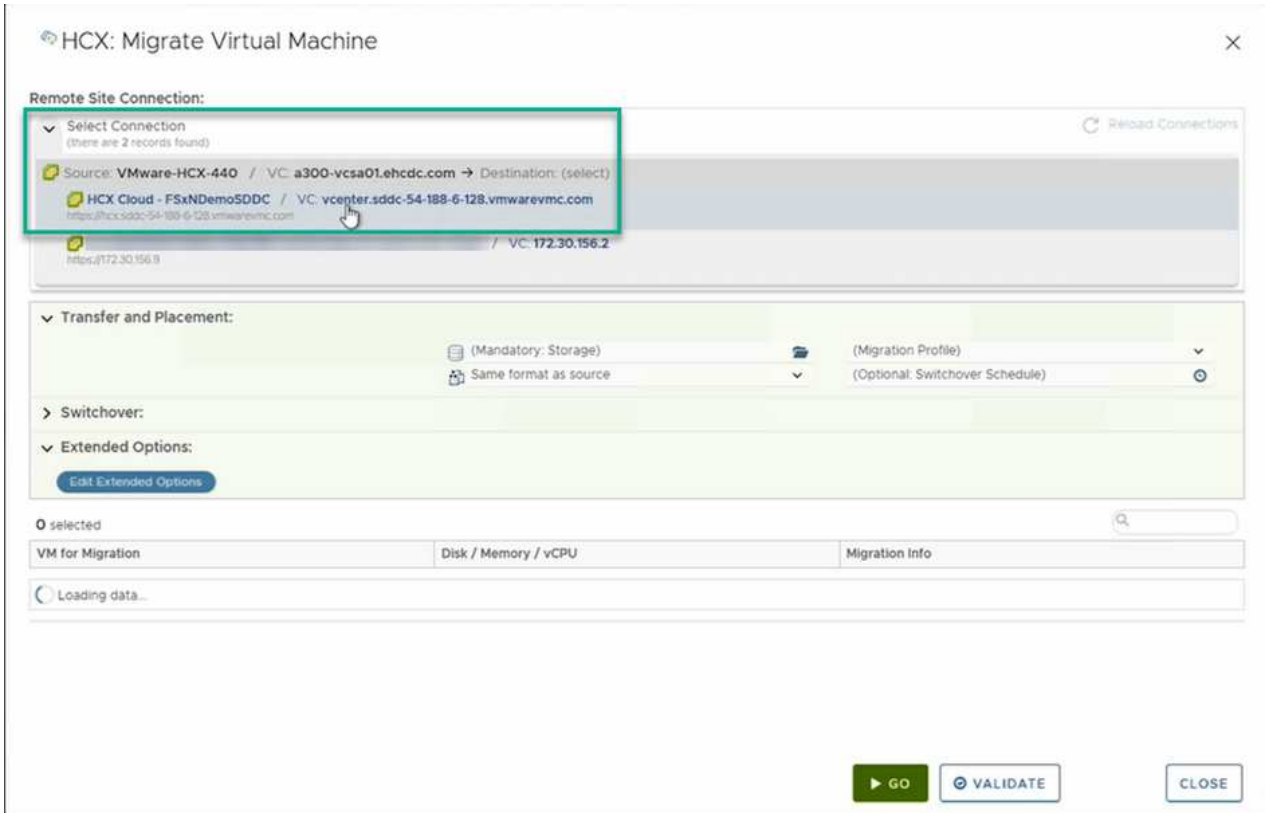
dieser Migrationsmethode kommt es zu keiner Dienstunterbrechung.

> Die Netzwerkerweiterung sollte vorhanden sein (für die Portgruppe, an die die VM angeschlossen ist), um die VM zu migrieren, ohne dass eine Änderung der IP-Adresse erforderlich ist.

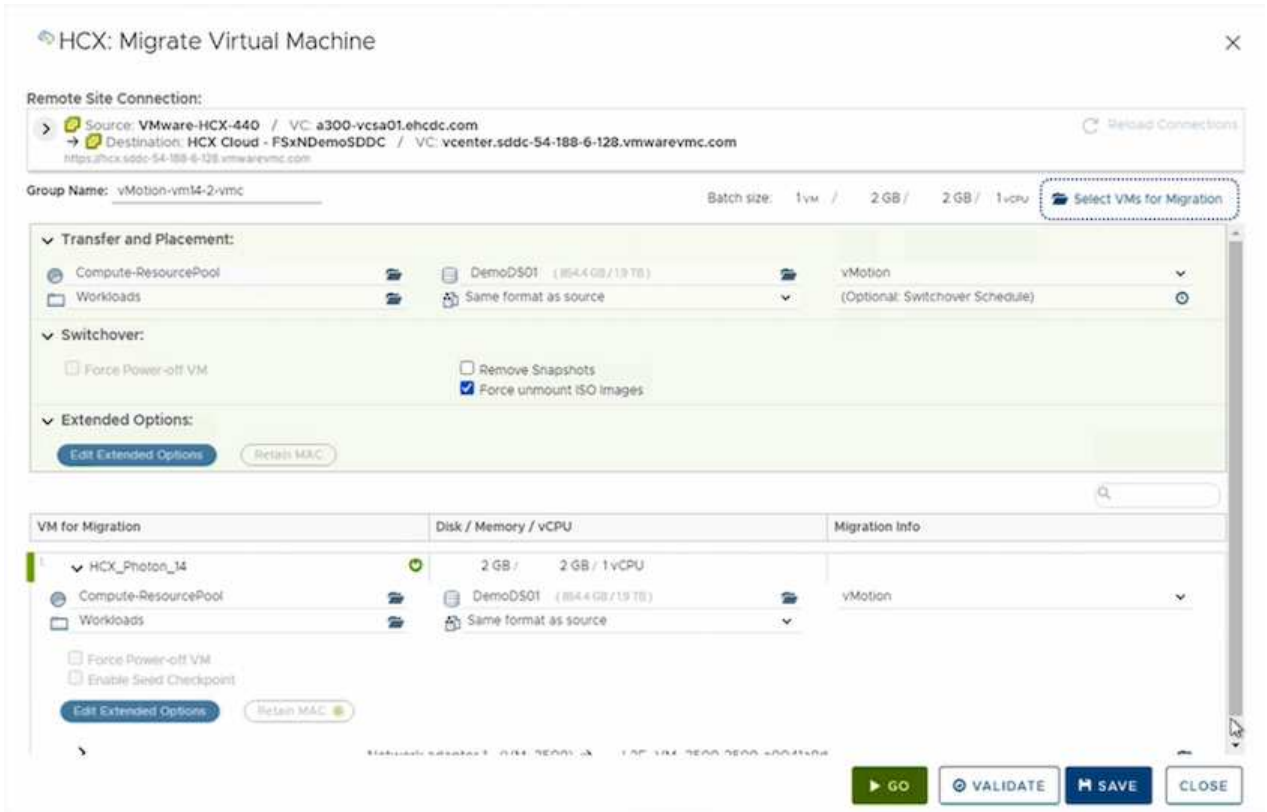
1. Gehen Sie im lokalen vSphere-Client zu „Inventar“, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie „HCX-Aktionen“ > „Zu HCX-Zielsite migrieren“.



2. Wählen Sie im Assistenten „Virtuelle Maschine migrieren“ die Remote-Site-Verbindung (Ziel-VMC-SDDC) aus.



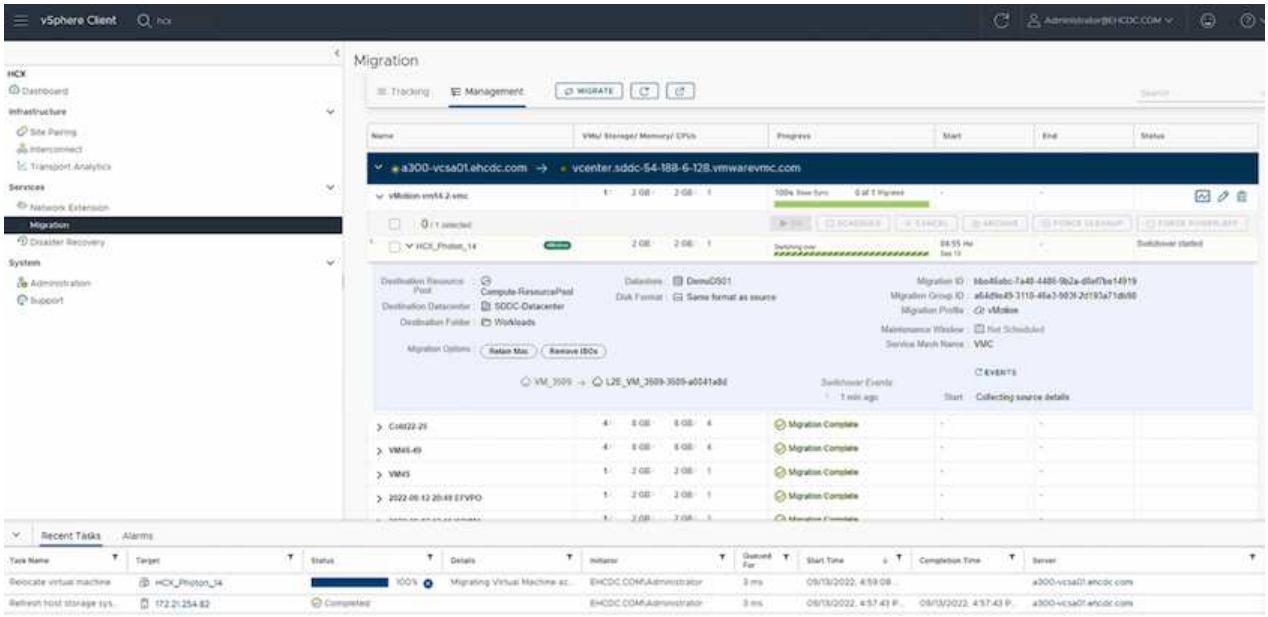
3. Fügen Sie einen Gruppennamen hinzu und aktualisieren Sie unter „Übertragung und Platzierung“ die Pflichtfelder (Cluster, Speicher und Zielnetzwerk). Klicken Sie auf „Validieren“.



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

Die vMotion-Übertragung erfasst den aktiven Speicher der VM, ihren Ausführungsstatus, ihre IP-Adresse und ihre MAC-Adresse. Weitere Informationen zu den Anforderungen und Einschränkungen von HCX vMotion finden Sie unter "VMware HCX vMotion und Cold Migration verstehen" .

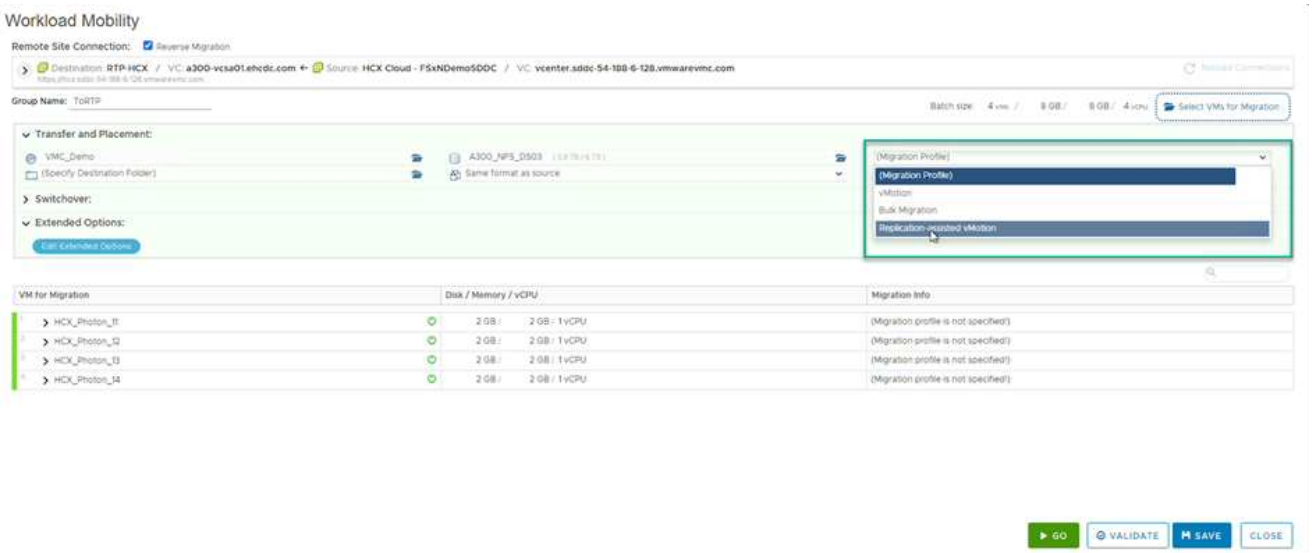
5. Sie können den Fortschritt und den Abschluss von vMotion über das Dashboard „HCX > Migration“ überwachen.



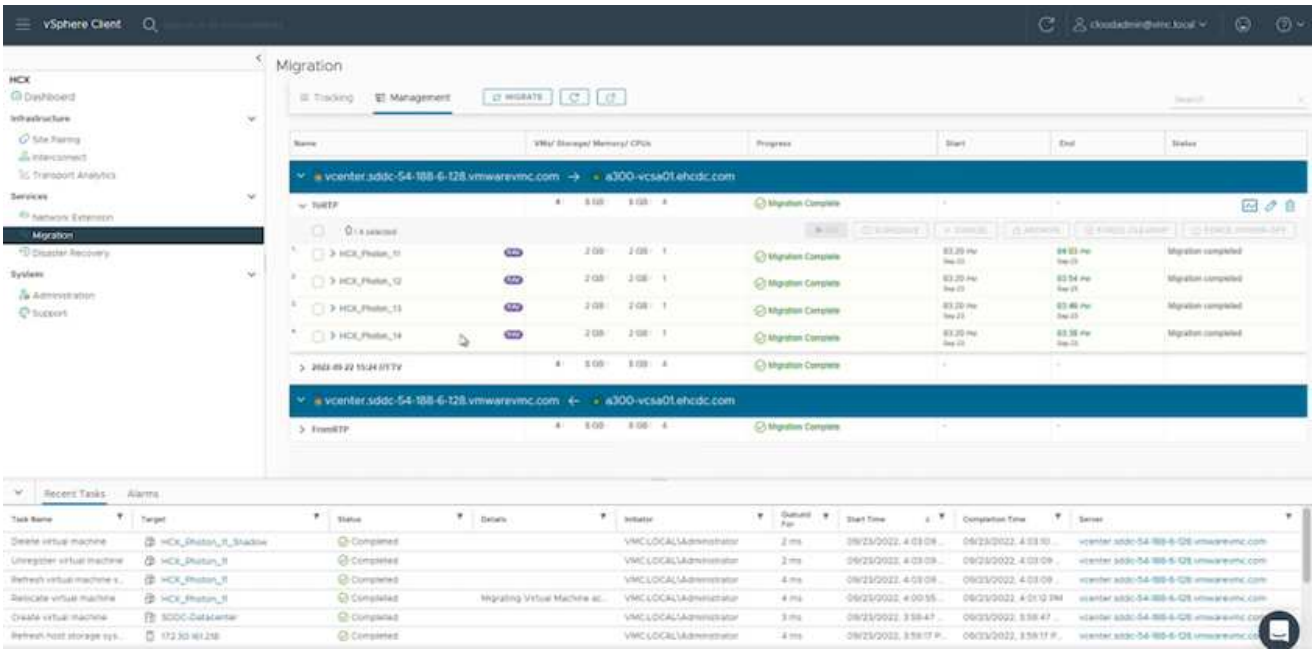
▼ VMware Replication Assisted vMotion

Wie Sie vielleicht der VMware-Dokumentation entnommen haben, kombiniert VMware HCX Replication Assisted vMotion (RAV) die Vorteile von Massenmigration und vMotion. Bei der Massenmigration wird vSphere Replication verwendet, um mehrere VMs parallel zu migrieren. Die VM wird während der Umschaltung neu gestartet. HCX vMotion migriert ohne Ausfallzeiten, wird jedoch seriell jeweils eine VM in einer Replikationsgruppe durchgeführt. RAV repliziert die VM parallel und hält sie bis zum Umschaltfenster synchron. Während des Umschaltvorgangs wird jeweils eine VM migriert, ohne dass es zu Ausfallzeiten für die VM kommt.

Der folgende Screenshot zeigt das Migrationsprofil als Replication Assisted vMotion.



Die Dauer der Replikation kann im Vergleich zur vMotion einer kleinen Anzahl von VMs länger sein. Synchronisieren Sie mit RAV nur die Deltas und schließen Sie den Speicherinhalt ein. Nachfolgend sehen Sie einen Screenshot des Migrationsstatus. Er zeigt, dass die Startzeit der Migration für jede VM gleich ist, die Endzeit jedoch unterschiedlich ist.



Weitere Informationen zu den HCX-Migrationsoptionen und zur Migration von Workloads von lokalen Standorten zu VMware Cloud on AWS mithilfe von HCX finden Sie im "VMware HCX-Benutzerhandbuch" .

VMware HCX vMotion erfordert eine Durchsatzkapazität von 100 Mbit/s oder mehr.

Der Zieldatenspeicher von VMC FSx ONTAP muss über ausreichend Speicherplatz für die Migration verfügen.

Abschluss

Unabhängig davon, ob Sie eine reine Cloud oder eine Hybrid-Cloud anstreben und Ihre Daten sich auf Speichersystemen beliebiger Art/Anbieter vor Ort befinden, bieten Amazon FSx ONTAP und HCX hervorragende Optionen zum Bereitstellen und Migrieren der Workloads bei gleichzeitiger Reduzierung der Gesamtbetriebskosten, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden. Wählen Sie für jeden Anwendungsfall VMC zusammen mit dem FSx ONTAP -Datenspeicher, um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und Vorgänge vor Ort und in mehreren Clouds zu nutzen, Workloads in beide Richtungen zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen. Es handelt sich um denselben bekannten Prozess und dieselben bekannten Verfahren, die zum Verbinden des Speichers und Migrieren von VMs mithilfe der VMware vSphere-Replikation, VMware vMotion oder sogar NFC-Kopie verwendet werden.

Imbiss

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können jetzt Amazon FSx ONTAP als Datenspeicher mit VMC SDDC verwenden.
- Sie können Daten problemlos von jedem lokalen Rechenzentrum zu VMC migrieren, das mit FSx ONTAP -Datenspeicher läuft

- Sie können den FSx ONTAP Datenspeicher problemlos vergrößern und verkleinern, um die Kapazitäts- und Leistungsanforderungen während der Migrationsaktivität zu erfüllen.

Wo Sie weitere Informationen finden

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

- VMware Cloud-Dokumentation

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

- Amazon FSx ONTAP Dokumentation

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

  VMware HCX-Benutzerhandbuch

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

NetApp für AWS / EVS

Mounten Sie FSx ONTAP als externen Datenspeicher für EVS

So mounten Sie Amazon FSx for NetApp ONTAP als externen Datenspeicher für Amazon Elastic VMware Service

Dieses Dokument enthält detaillierte Schritte zum Erstellen eines FSx für ONTAP -Dateisystems und zum Anhängen zur Verwendung als Internet Small Computer System Interface (iSCSI)- oder Network File System (NFS)-Datenspeicher zur Verwendung mit Amazon EVS.

Einführung

Organisationen mit bestehenden VMware-Investitionen vor Ort, die nach effizienten und kostengünstigen Möglichkeiten zur Modernisierung ihrer Bereitstellungen durch Migration, Bursting, Erweiterung oder Schutz (Backup, Notfallwiederherstellung) von Kopien auf AWS suchen, sind mit mehreren Herausforderungen konfrontiert. Mit der Veröffentlichung von Amazon Elastic VMware Service (Amazon EVS) gibt es jetzt einen nativen AWS-Dienst, der es ermöglicht, VMware Cloud Foundation (VCF) direkt in einer Amazon Virtual Private Cloud (VPC) auszuführen.

Amazon EVS ermöglicht die Erweiterung vorhandener VCF-Bereitstellungen auf AWS, den Wechsel in AWS zur Leistungssteigerung bei Spitzenauslastung und die vollständige Ausführung von VCF-Workloads auf AWS, um Modernisierungen, Rechenzentrumsausstiege, Konsolidierungen und andere Anwendungsfälle zu erleichtern.

Obwohl Amazon EVS große Vorteile bietet, koppelt die standardmäßige hyperkonvergente Architektur Rechenleistung und Speicher und verhindert so eine unabhängige Skalierung des einen oder anderen, je nach Geschäftsanforderungen. In der heutigen datenzentrierten Welt ist der Speicherbedarf vieler Unternehmen höher als der Rechenbedarf. Bei der hyperkonvergenten Architektur von VMware sind Speicherressourcen jedoch mit Rechenressourcen gekoppelt. Das bedeutet, dass die Skalierung des Speichers nur durch das Hinzufügen von Rechenhosts erfolgen kann, die nie verwendet werden. Dies ist eine Situation, die die Kosten

erheblich erhöhen kann, insbesondere bei speicherintensiven Arbeitslasten.

Um dieses Problem zu lösen, bieten AWS und NetApp Amazon FSx for NetApp ONTAP (FSx für ONTAP) als externen Speicherdienst für Amazon EVS an. FSx für ONTAP ist ein AWS-nativer Speicherdienst, der die hohe Leistung, Datenausfallsicherheit und Kosteneffizienzfunktionen der NetApp ONTAP Software bietet. Durch die Verwendung von FSx für ONTAP als externer Speicher können Amazon EVS-Benutzer Rechen- und Speicherressourcen unabhängig voneinander skalieren und so optimale Gesamtbetriebskosten (TCO) erzielen.

Überblick

Dieses Dokument enthält detaillierte Schritte zum Erstellen eines FSx für ONTAP -Dateisystems und zum Anhängen zur Verwendung als Internet Small Computer System Interface (iSCSI)- oder Network File System (NFS)-Datenspeicher zur Verwendung mit Amazon EVS.

Zweck dieses Handbuchs

Dieses Handbuch enthält Anweisungen zum Einrichten eines FSx for ONTAP -Datenspeichers für Amazon EVS sowie Best Practices, Supportanforderungen, Größenüberlegungen und andere Informationen, die Ihnen bei der Planung, Gestaltung und Implementierung der Integration helfen.

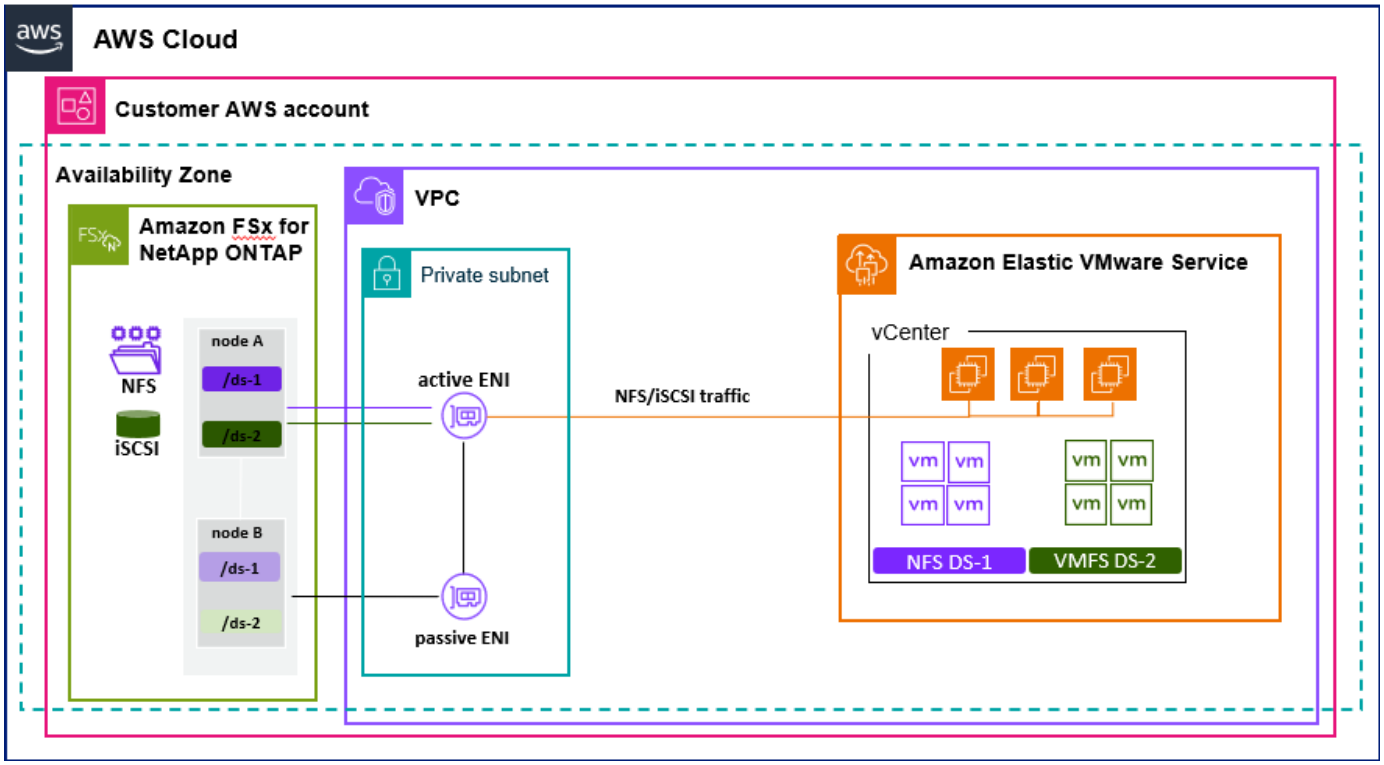
Publikum

Dieses Tutorial richtet sich an Cloud-Architekten und Cloud-Administratoren, die mit VMware vSphere, Amazon EVS, der AWS-Konsole und FSx für ONTAP vertraut sind.

Architektur auf hoher Ebene

In diesem Abschnitt geben wir einen Überblick über die Lösungsarchitektur für die Verwendung von FSx for ONTAP als Datenspeicher für Amazon EVS.

Unten sehen Sie eine Übersicht über die Architektur des FSx for ONTAP -Datenspeichers mit einer Amazon EVS-Umgebung innerhalb einer AWS VPC.



Bereitstellungsverfahren für die Verwendung von FSx for ONTAP als NFS-Datenspeicher

In diesem Abschnitt werden die Schritte zum Bereitstellen von FSx für ONTAP als NFS-Datenspeicher gezeigt. Die Schritte zum Bereitstellen eines iSCSI-Datenspeichers werden im nächsten Abschnitt ausführlich beschrieben.

Allgemeine Bereitstellungsschritte

Die Bereitstellung des FSx for ONTAP Dateisystems zur Verwendung als NFS-Datenspeicher für Amazon EVS und die Herstellung der Konnektivität zwischen den beiden Diensten umfasst die folgenden Schritte:

- Einrichten eines FSx für ONTAP Dateisystems in derselben VPC, in der sich die Amazon EVS VCF-Umgebung befindet.
- Validieren der Sicherheitsgruppen und der Routingtabelle.
- Anschließen eines FSx für ONTAP Speichervolumes zur Verwendung als NFS-Datenspeicher für Amazon EVS.

Voraussetzungen

Die folgenden Voraussetzungen sollten erfüllt sein, bevor Sie mit der Einrichtung eines FSx for ONTAP als NFS-Datenspeicher für Amazon EVS beginnen:

- Eine Amazon EVS-Virtualisierungsumgebung. Weitere Informationen hierzu finden Sie in der Dokumentation zu"Leitfaden „Erste Schritte mit Amazon EVS“" .
- Erstellen Sie eine Single-Availability Zone (AZ) FSx für ONTAP mit entsprechender SSD-Speicherkapazität, bereitgestellten IOPS und Durchsatz.
- Für optimale Leistung platzieren Sie das FSx for ONTAP -Dateisystem im selben VPC wie die Amazon EVS-Instance. Beachten Sie, dass VPC-Peering auch für den Fall unterstützt wird, dass FSx für ONTAP in einer anderen VPC bereitgestellt wird.

- Wählen Sie basierend auf den Leistungsanforderungen die richtigen IOPS und den richtigen Durchsatz aus, die für ein Single-AZ FSx für ONTAP Dateisystem erforderlich sind. Sehen"Details zu den Leistungsspezifikationen für FSx für ONTAP" um den Durchsatz und die IOPS zu verstehen, die jede verfügbare Option bietet.

> Für diese Anleitung stellen wir das FSx for ONTAP -Dateisystem im selben Subnetz wie das Servicezugriffssubnetz bereit.

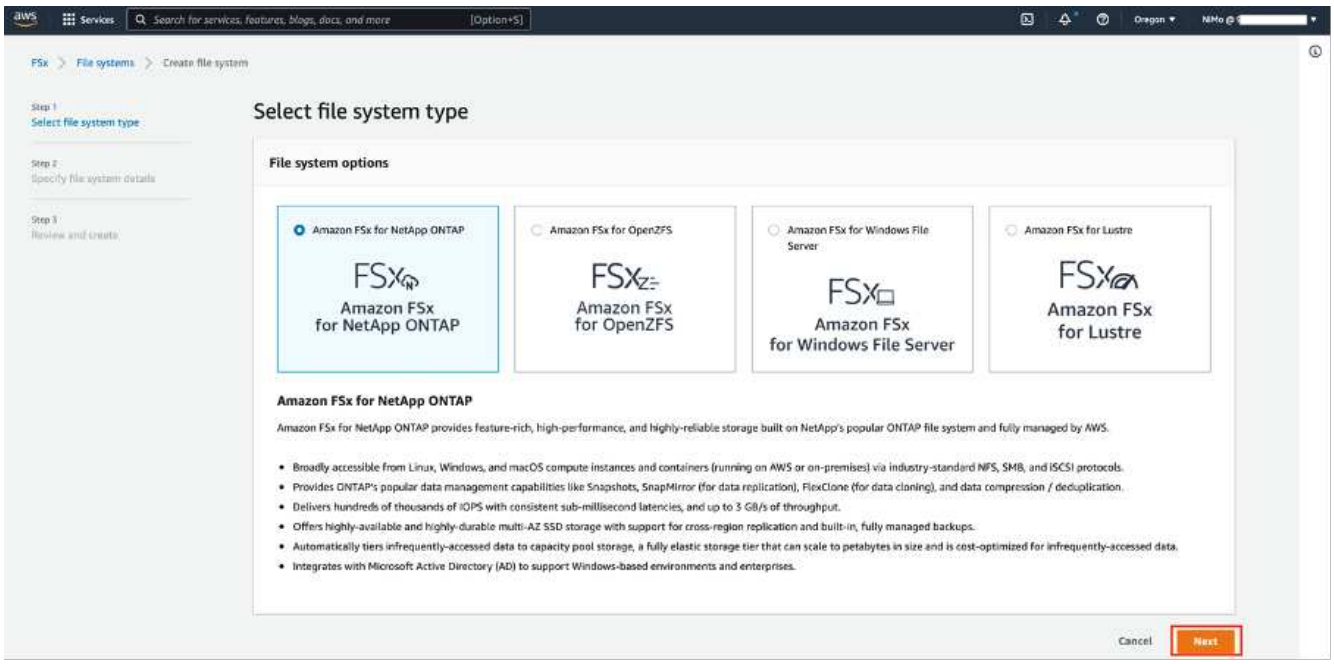
Sobald die Amazon EVS-Virtualisierungsumgebung in der VPC bereitgestellt wurde, können Sie mit der Einrichtung des Single-AZ FSx für ONTAP -Dateisystems fortfahren, das als NFS-Datenspeicher verwendet wird.

> Ihr FSx for ONTAP -Dateisystem sollte in derselben AZ wie das Amazon EVS SDDC bereitgestellt werden.

Erstellen Sie ein FSx für ONTAP -Dateisystem

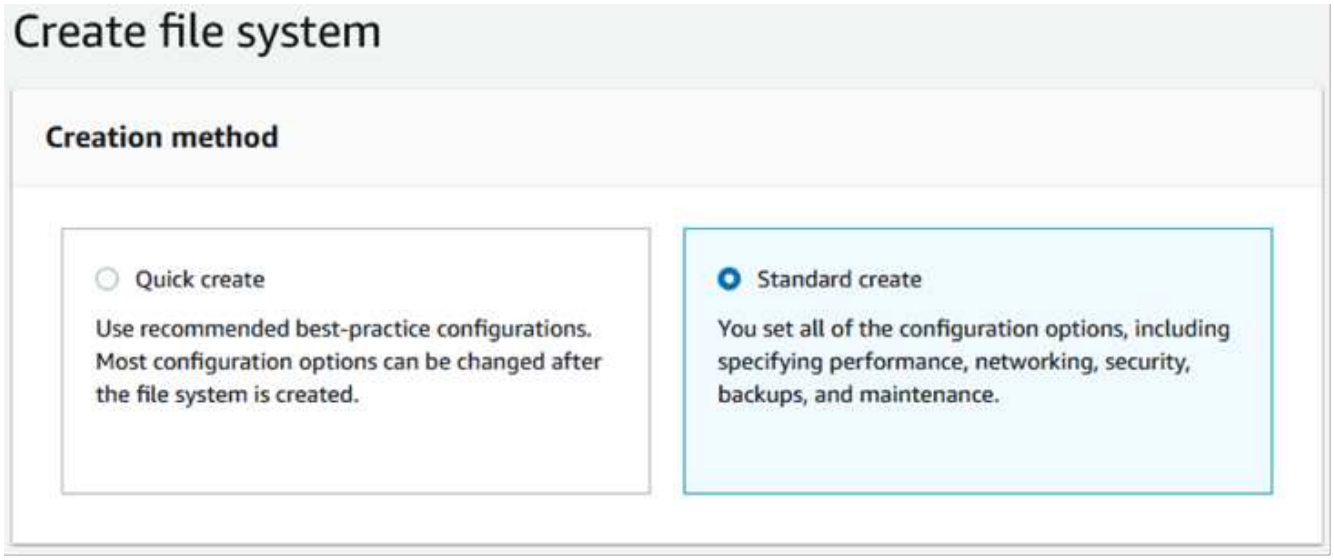
Die folgenden Schritte zeigen Ihnen, wie Sie ein FSx für ONTAP Dateisystem bereitstellen und mounten:

1. Gehen Sie zur Amazon FSx Konsole unter `https://console.aws.amazon.com/fsx/` Verwenden Sie Ihren Internetbrowser und melden Sie sich mit Ihren Anmeldeinformationen an.
2. Wählen Sie in der Konsole „Dateisystem erstellen“ aus. Dadurch wird der Setup-Assistent zum Erstellen eines FSx für ONTAP Dateisystems gestartet.
3. Wählen Sie zunächst den Dateisystemtyp aus. Wählen Sie aus den verfügbaren Dateisystemoptionen „Amazon FSx for NetApp ONTAP“ aus und fahren Sie fort, indem Sie auf die Schaltfläche „Weiter“ klicken.

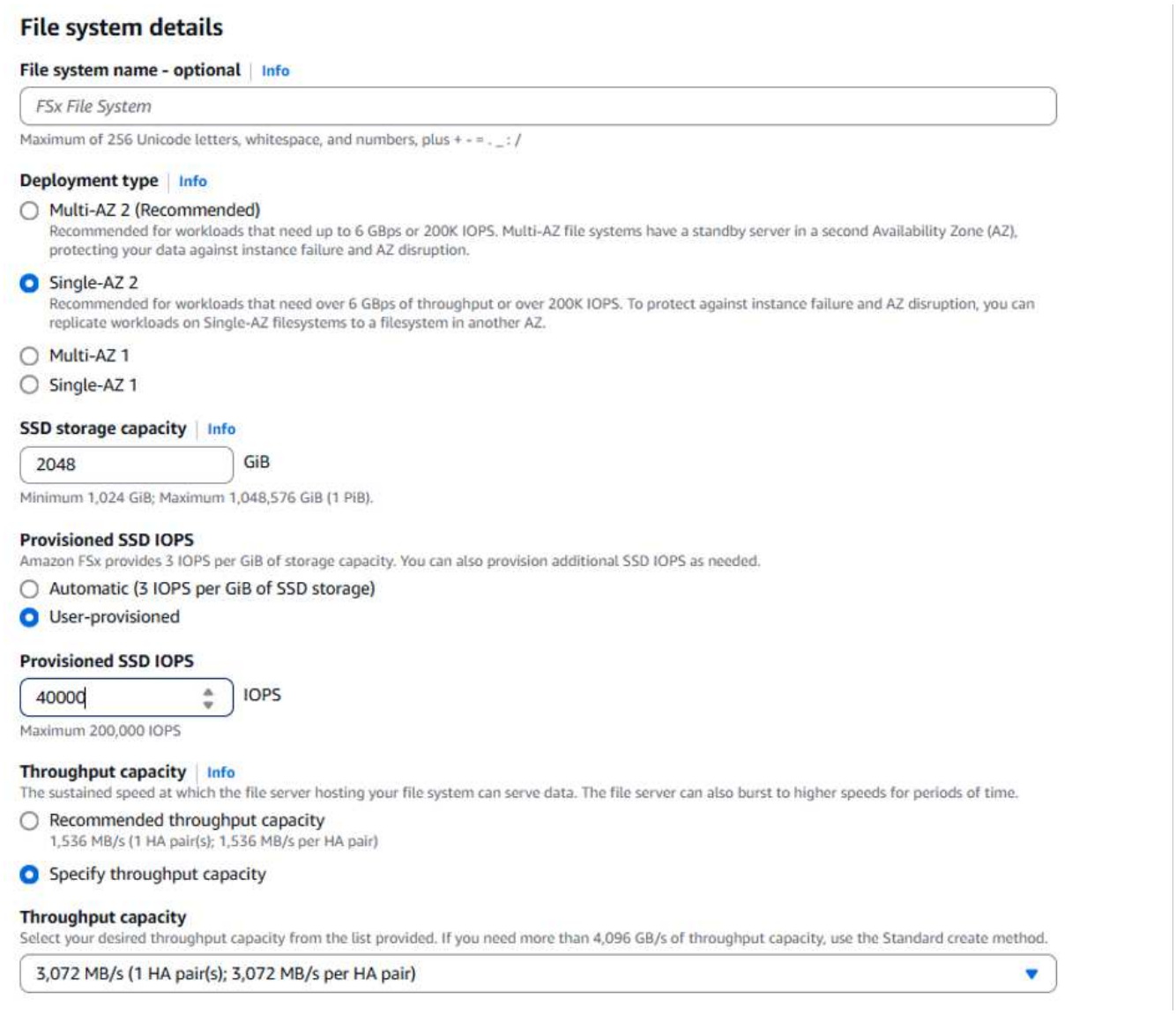


4. Ihnen wird die Auswahl zwischen den Optionen „Schnell erstellen“ und „Standard erstellen“ angeboten. „Quick Create“ bietet vordefinierte Konfigurationen und „Standard Create“ ermöglicht Ihnen, Ihre eigenen Konfigurationen zu definieren.

   Wählen Sie die Option „Standard erstellen“.

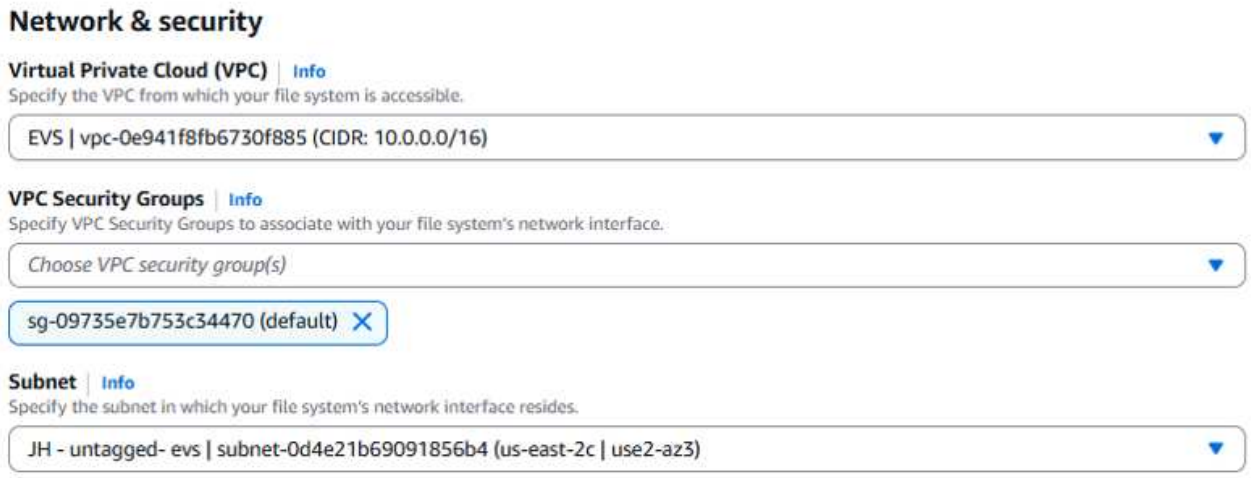


Sie befinden sich jetzt im Standard-Setup-Assistenten zum Erstellen eines Dateisystems. Wählen Sie auf der Seite mit den Dateisystemdetails dieselben Informationen aus und geben Sie sie ein, wie im Bild unten gezeigt:



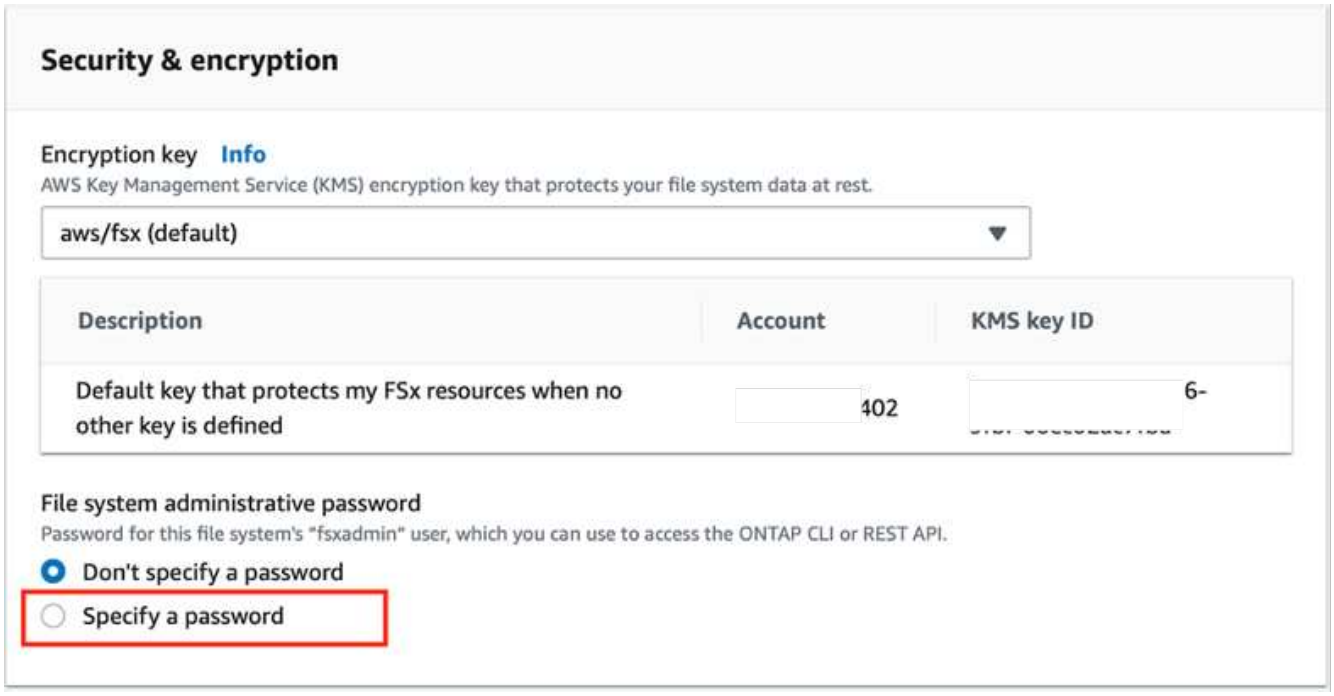
5. Scrollen Sie nach unten, bis Sie den Abschnitt „Netzwerk und Sicherheit“ finden. In diesem Abschnitt legen Sie die Details für das Subnetz und die VPC fest. Für die Zwecke dieses Handbuchs haben wir „EVS-VPC“ aus dem Dropdown-Menü ausgewählt und das Servicezugriffssubnetz (untagged VLAN) als Subnetz für die virtuelle EVS-Umgebung ausgewählt.

   Das Subnetz kann jedes beliebige private Subnetz ohne Tag in der VPC sein. Es kann sich auch in einem anderen VPC/Subnetz befinden, das über VPC-Peering verbunden ist, solange das richtige Routing konfiguriert wurde.

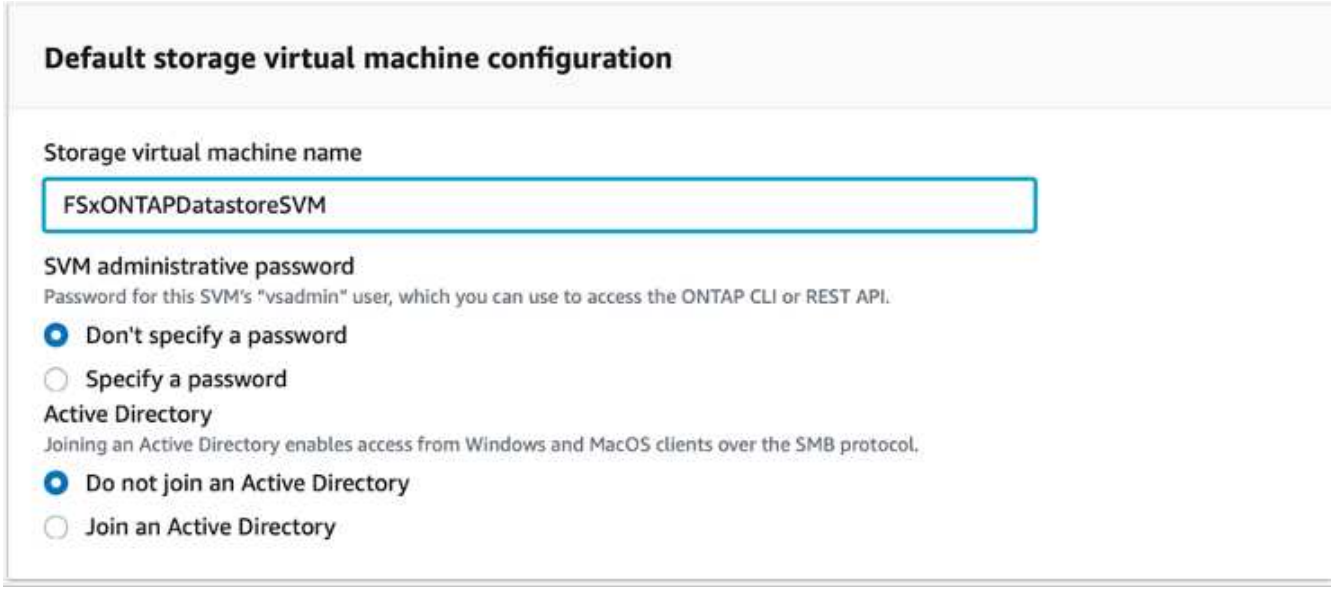


6. Wenn Sie nach unten scrollen, finden Sie den Abschnitt „Sicherheit und Verschlüsselung“. Wählen Sie hier den Verschlüsselungsschlüssel aus dem Dropdown-Menü aus. Diese Schlüssel werden vom AWS Key Management Service (AWS KMS) bereitgestellt und schützen die ruhenden Daten in Ihrem FSx for ONTAP -Dateisystem.

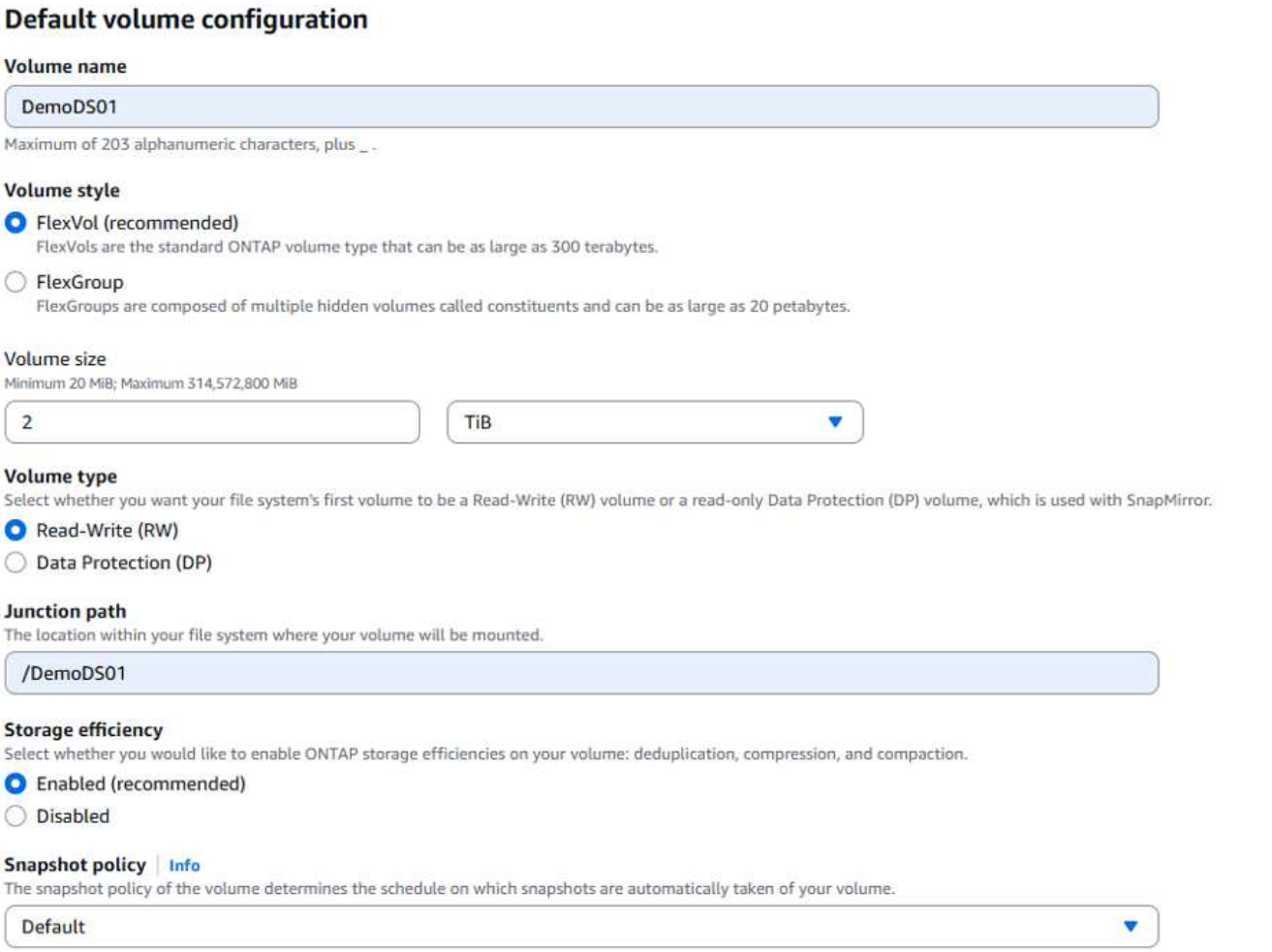
   Geben Sie als Nächstes in der Einstellung „Administratorkennwort für Dateisystem“ ein eindeutiges Kennwort für den Benutzer fsxadmin an, der das Dateisystem verwalten wird.



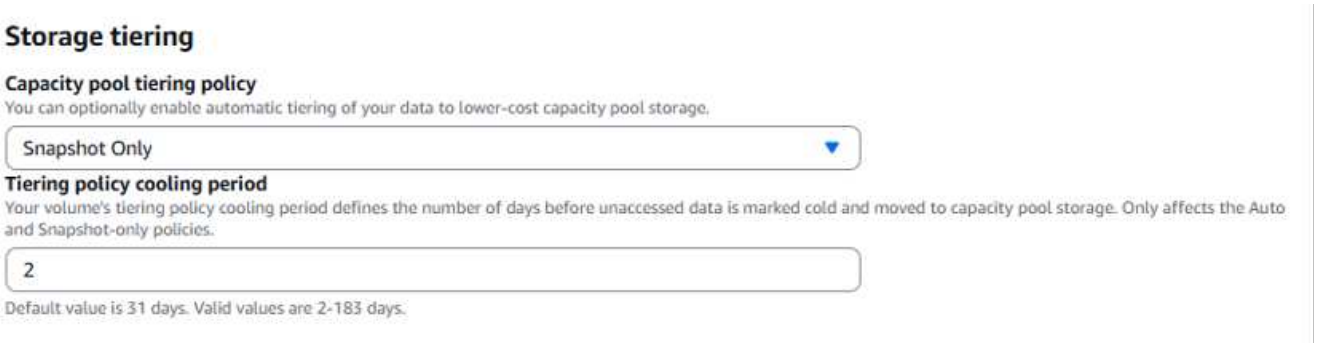
7. Als Nächstes scrollen Sie nach unten zu einem Abschnitt mit dem Titel „Standardkonfiguration der virtuellen Speichermaschine“. Hier müssen Sie einen Namen für die Storage Virtual Machine (SVM) angeben.



8. Scrollen Sie anschließend nach unten zum Abschnitt „Standard-Volume-Konfiguration“. Hier geben Sie dem Volume einen Namen und legen die Volumegröße fest. Das Volume-Protokoll sollte NFS v3 sein (standardmäßig aktiviert). Klicken Sie auf die Option zum Aktivieren von Speichereffizienzfunktionen (Komprimierung, Deduplizierung und Kompaktierung), um Ihre allgemeine Speichernutzung und -kosten zu reduzieren.



9. Wählen Sie für die Speicher-Tiering-Option „Nur Snapshot“ aus dem Dropdown-Menü und legen Sie eine Kühlperiode für die Tiering-Richtlinie fest. Der Standardwert beträgt 31 Tage, für dieses Beispiel legen wir jedoch eine Abkühlungsperiode von zwei Tagen fest.



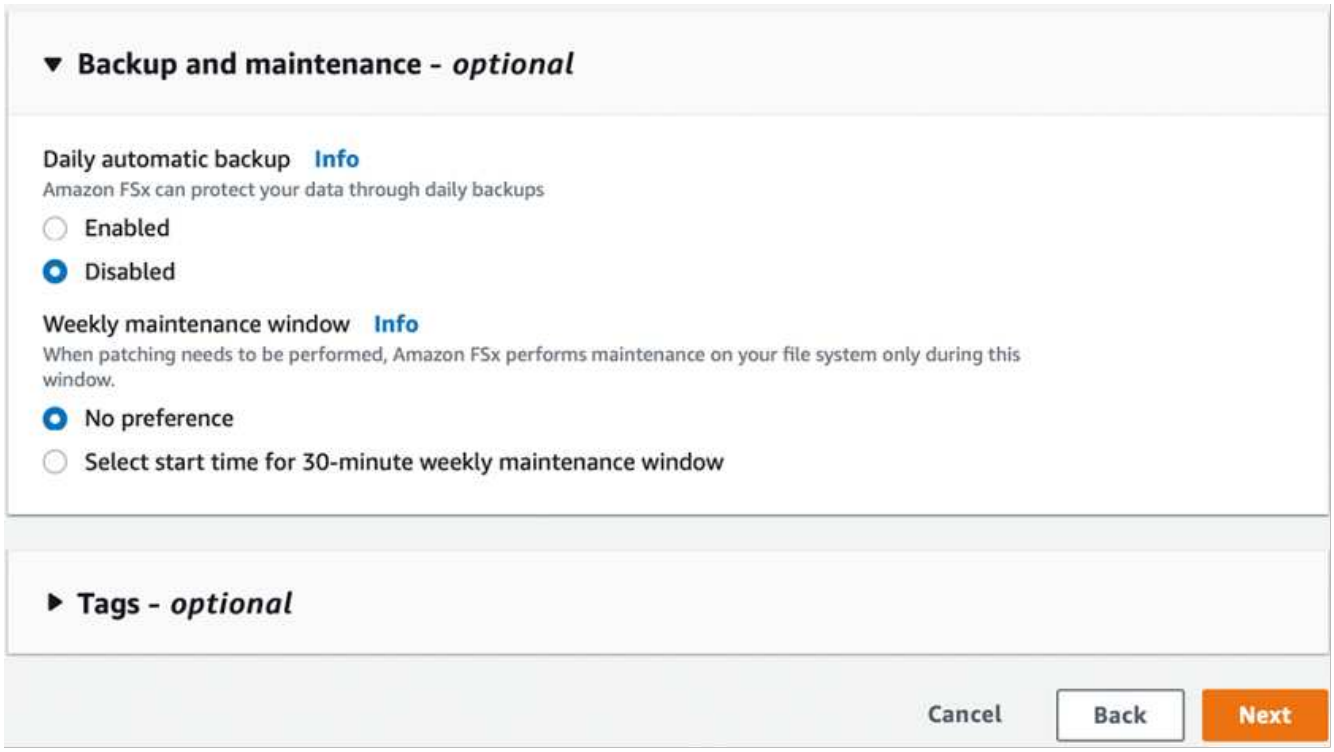
10. Nachdem Sie das Volume erstellt haben, ändern Sie die folgenden Parameter mithilfe der ONTAP Befehlszeilenschnittstelle (ONTAP CLI):

Einstellung	Konfiguration
Volumengarantie	Keine (Thin Provisioning)
Teilreserve	0 %
snap_reserve	0 %

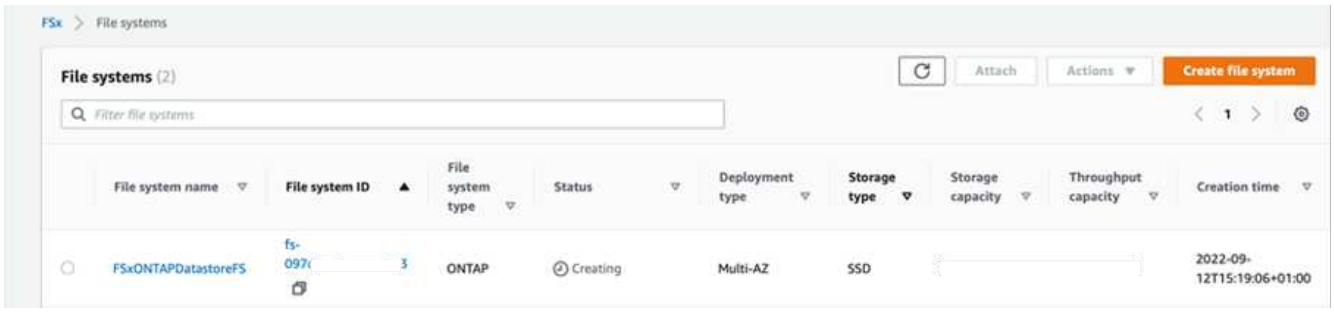
Einstellung	Konfiguration
Automatische Größe	wachsen_schrumpfen
Speichereffizienz	Ermöglicht
Volume-Tiering-Richtlinie	Nur Schnappschuss
Aktualisierung der Zugriffszeit (-atime-update)	FALSCH
Minimaler Readahead (-min-readahead)	FALSCH
Snapshot-Richtlinie	Keine

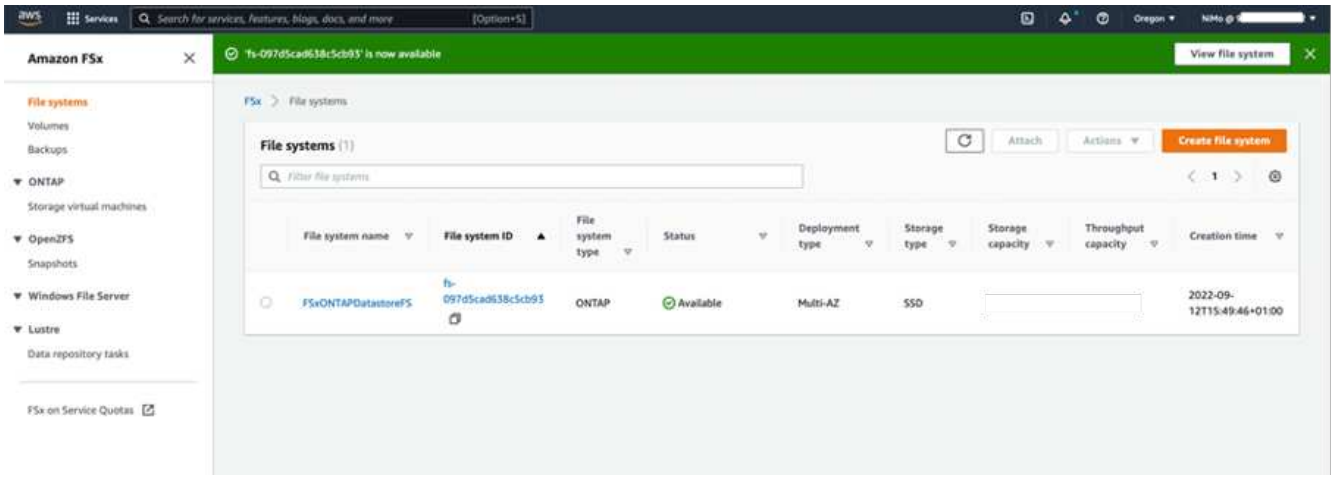
11. Deaktivieren Sie im optionalen Schritt „Sicherung und Wartung“ die täglichen automatischen Sicherungen und wählen Sie „Keine Präferenz“ für das wöchentliche Wartungsfenster.

    Klicken Sie auf „Weiter“, wenn Sie fertig sind.



12. Sie erhalten nun eine Übersicht über die gesamte Dateisystemkonfiguration, die Sie in den vorherigen Schritten eingerichtet haben. Überprüfen Sie, ob alle Parameter korrekt sind, und klicken Sie dann auf die Schaltfläche „Dateisystem erstellen“, um die Einrichtung abzuschließen.



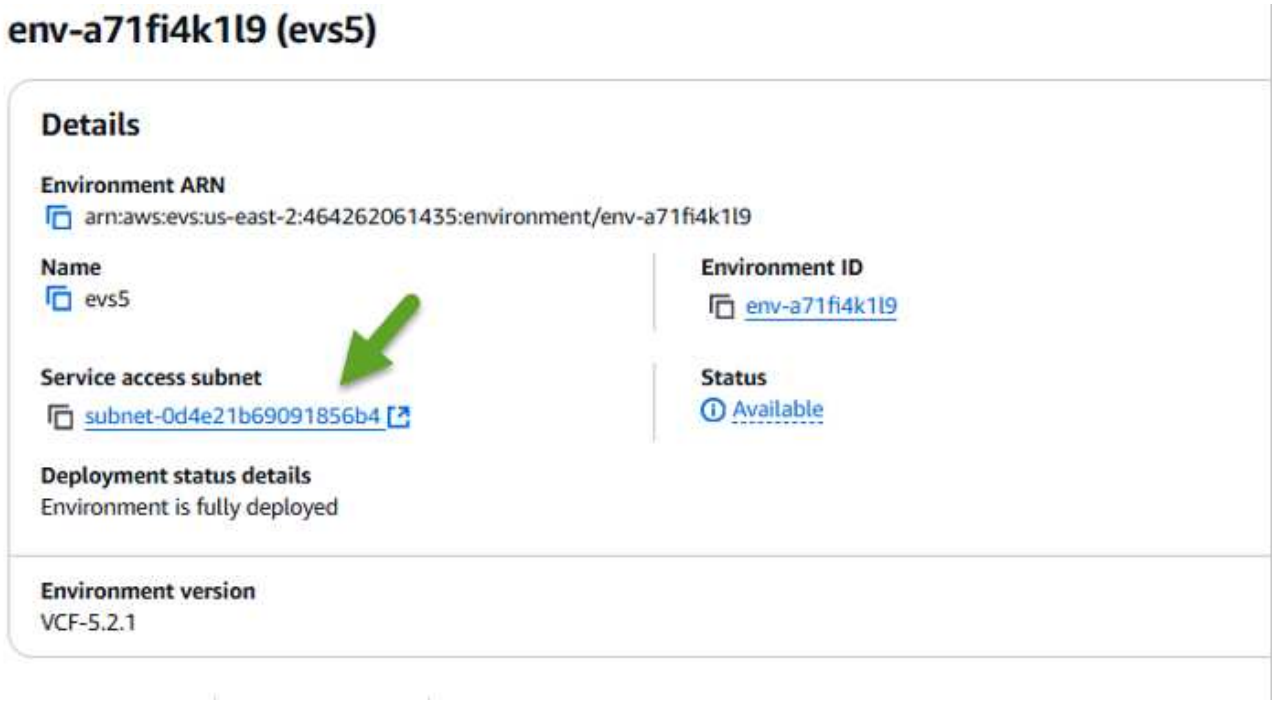


Um zusätzliche FSx für ONTAP Dateisysteme zu erstellen, können Sie die oben beschriebenen Schritte befolgen und die Werte, die sich auf die Leistung und die Festplattenkapazität auswirken, nach Bedarf anpassen. Weitere Informationen zu den Leistungsoptionen für FSx for ONTAP finden Sie unter"diese Dokumentationsseite" .

Validieren von Routing- und Sicherheitsgruppen für VPC- und Virtualisierungsumgebungen

Die Validierung der VPC- und SDDC-Routing- und Sicherheitsgruppen ist wichtig, um sicherzustellen, dass die Amazon EVS-Virtualisierungsumgebung und die FSx for ONTAP Dateisystemkomponenten ordnungsgemäß zusammenarbeiten können.

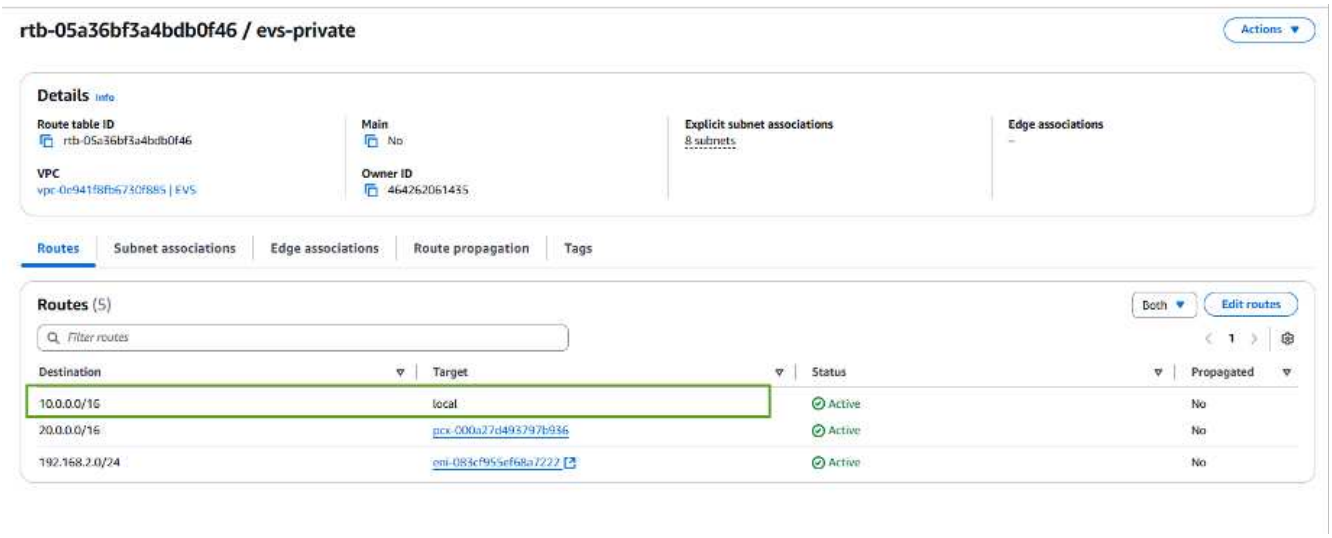
1. Navigieren Sie zu Elastic VMware Service > Virtualization Environments > [Ihre Amazon EVS-Umgebung] und wählen Sie das Service-Zugriffssubnetz aus, wie unten durch den grünen Pfeil angezeigt:



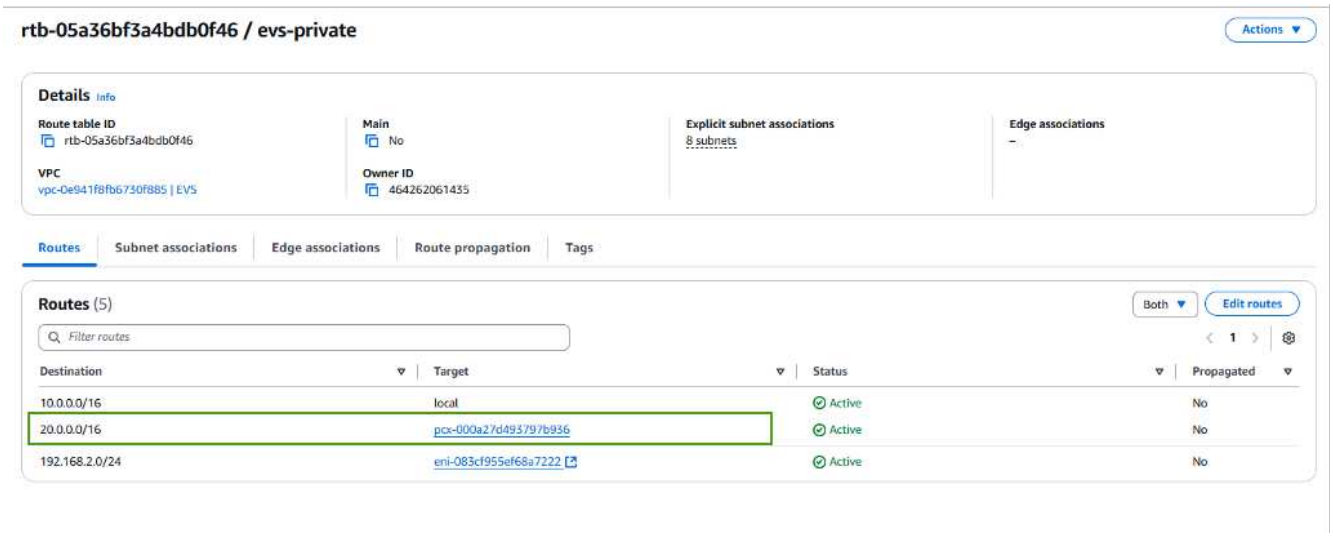
2. Dadurch wird das Subnetz-Panel geöffnet. Suchen Sie in diesem Bereich nach der Routentabelle und klicken Sie darauf.

   In diesem Beispiel befindet sich das FSxN ONTAP Dateisystem im selben VPC wie die Amazon EVS VCF-

Umgebung, daher sind die Standardrouten ausreichend.



Wenn sich das FSx for ONTAP -Dateisystem in einer anderen VPC befindet, überprüfen Sie, ob die Routen zu dieser VPC hinzugefügt wurden. In diesem Beispiel wurden Routen für VPC-Peering zum VPC hinzugefügt, in dem sich das FSx for ONTAP -System befindet.

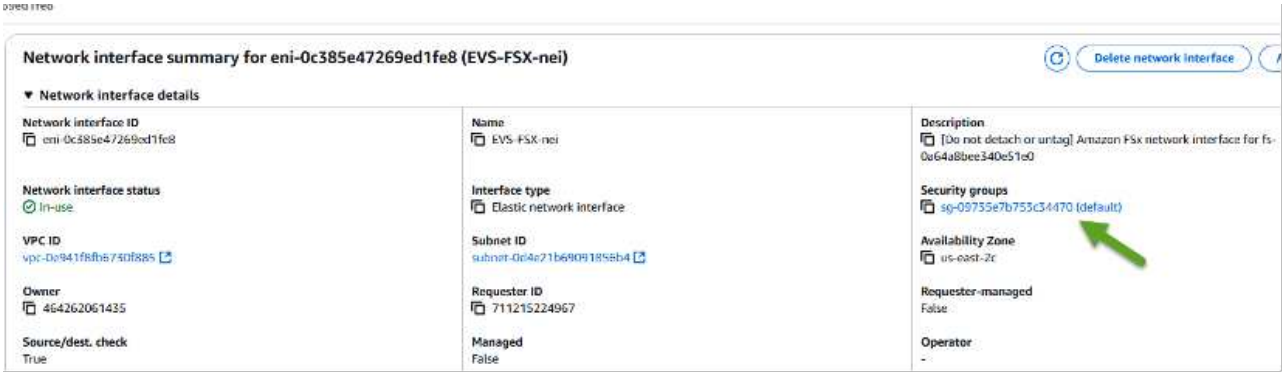


3. Als Nächstes müssen Sie überprüfen, ob die mit dem FSx for ONTAP Dateisystem verbundene Sicherheitsgruppe (d. h. die mit der Elastic Network Interface (ENI) verbundene) Zugriff auf NFS-Ports ermöglicht.

   Eine vollständige Liste der NFS- und iSCSI-Protokollports finden Sie unter folgendem Link: https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]File System Access Control mit Amazon VPC-Dokumentation].

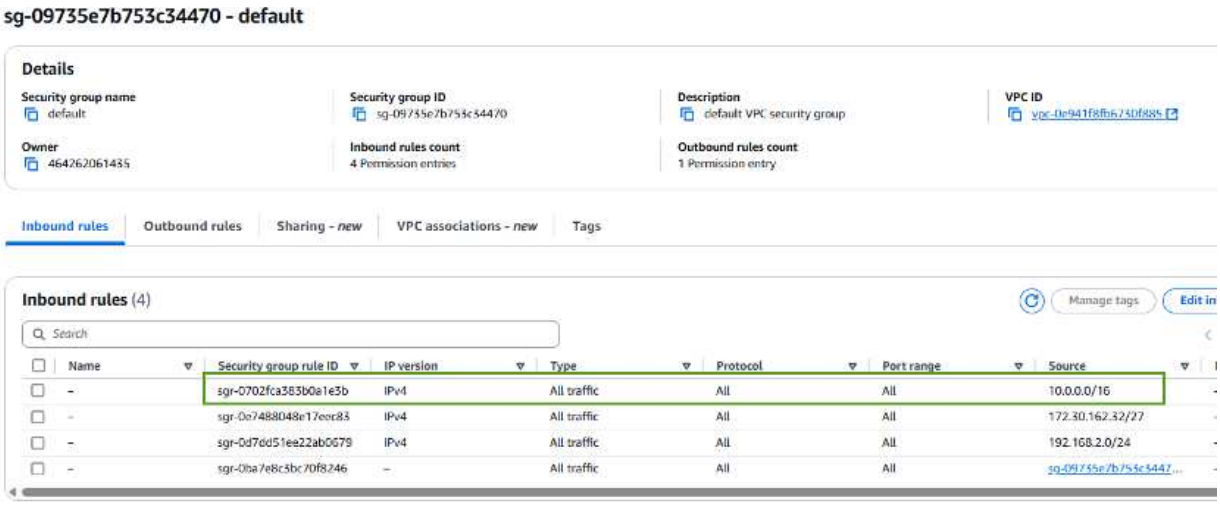
   So überprüfen Sie, ob Ihr FSx for ONTAP -Dateisystem mit der Sicherheitsgruppe verknüpft ist:

   a. Navigieren Sie in der AWS-Konsole zu FSx > Dateisysteme > [Ihr FSx for ONTAP -Dateisystem].
   b. Klicken Sie auf der Registerkarte „Netzwerk und Sicherheit“ auf die ENI.
   c. Suchen Sie die Sicherheitsgruppe, die unter den Netzwerkschnittstellendetails aufgeführt ist und mit der ENI verknüpft ist (im Bild unten durch den grünen Pfeil gekennzeichnet).



d. Validieren Sie die Ports. In diesem im folgenden Bildschirm gezeigten Beispiel ist der gesamte Datenverkehr zulässig. Sie können diese jedoch auf NFS-Ports beschränken. Hier ist die Liste der Ports:

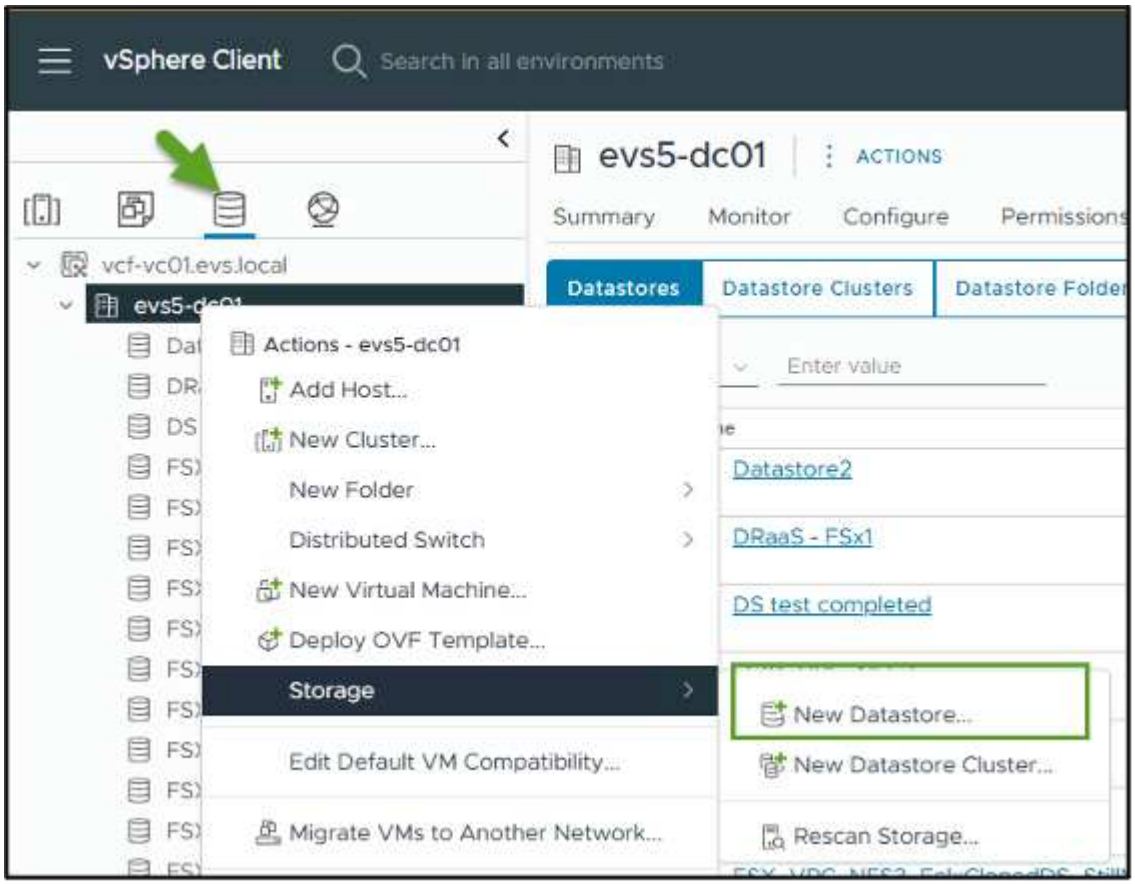
- Port 111 TCP: Portmapper, wird verwendet, um auszuhandeln, welche Ports in NFS-Anfragen verwendet werden.
- Port 635 TCP: Mountd, der zum Empfangen eingehender Mount-Anfragen dient.
- Port 2049 TCP: NFS, der den NFS-Verkehr abwickelt.
- Port 4045 TCP: Network Lock Manager (NLM), der sich um Sperranforderungen kümmert.
- Port 4046 TCP: Network Status Monitor (NSM), der NFS-Clients Benachrichtigungen sendet, wenn der Server zur Sperrverwaltung neu gestartet wird.



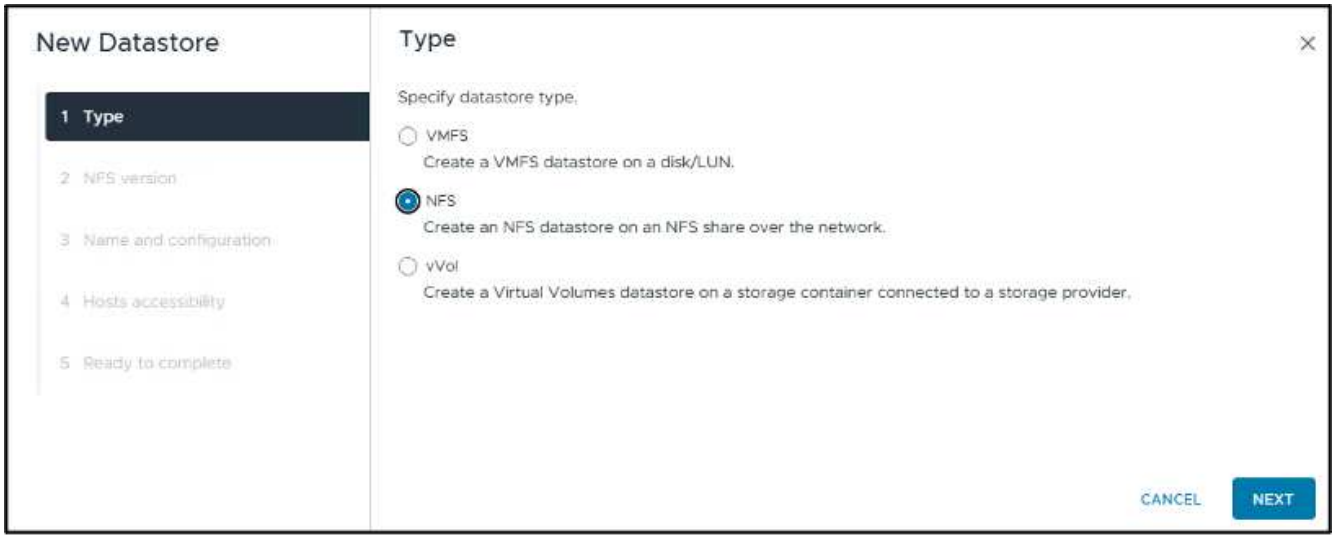
Anhängen eines FSx for ONTAP NFS-Volumes an Amazon EVS zur Verwendung als Datenspeicher

Nachdem Ihr FSx for ONTAP Dateisystem bereitgestellt und alle erforderlichen Konnektivitätsparameter validiert wurden, ist es an der Zeit, ein FSx for ONTAP -Speichervolume an Amazon EVS anzuhängen. Die folgenden Schritte zeigen, wie Sie auf vCenter zugreifen und das FSx for ONTAP Volume als NFS-Datenspeicher mounten:

1. Gehen Sie im vSphere-Client auf die Registerkarte „Datastore“. Suchen Sie das Rechenzentrum und navigieren Sie zu Speicher > Neuer Datenspeicher, wie unten gezeigt:

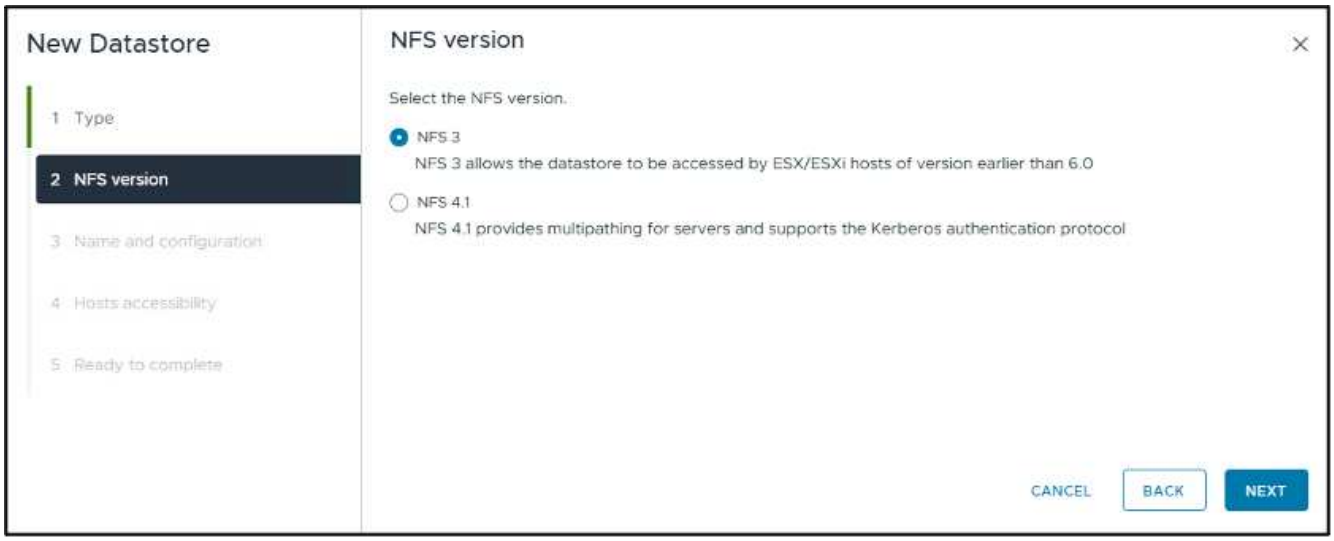


2. Sie befinden sich jetzt im Assistenten „Neuer Datenspeicher“. Im Schritt „Typ“ wählen Sie einen Datenspeichertyp aus. Wählen Sie „NFS“ und klicken Sie auf „WEITER“, um fortzufahren.



3. Im Schritt „NFS-Version“ wählen Sie eine NFS-Version aus.

   Für dieses Beispiel wählen wir „NFS 3“, beachten Sie jedoch, dass auch NFS v4.1 verwendet werden kann.



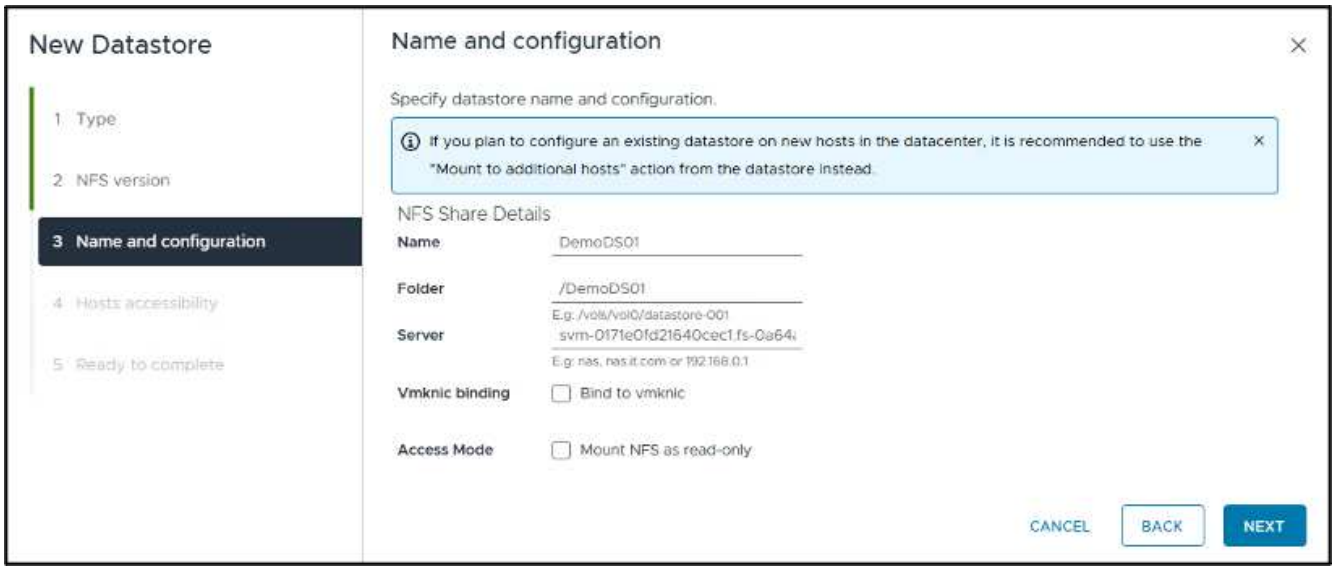
4. Im Schritt „Name und Konfiguration“ werden Sie:

   a. Geben Sie dem Datenspeicher einen Namen.

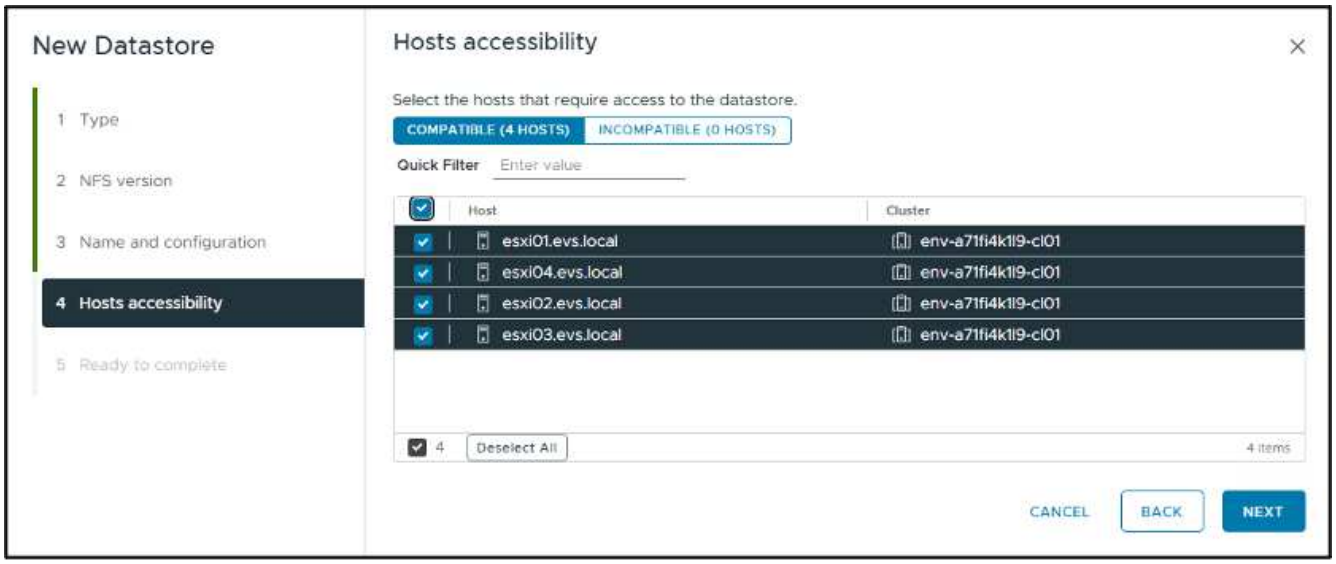
   b. Geben Sie dem Ordner einen Namen. Verwenden Sie den Verbindungspfad zu Ihrem NFS-Volume.

   c. Geben Sie dem Server einen Namen. Verwenden Sie entweder den NFS-DNS-Namen Ihres SVM oder die IP-Adresse des NFS.

      Klicken Sie auf „WEITER“, um fortzufahren.



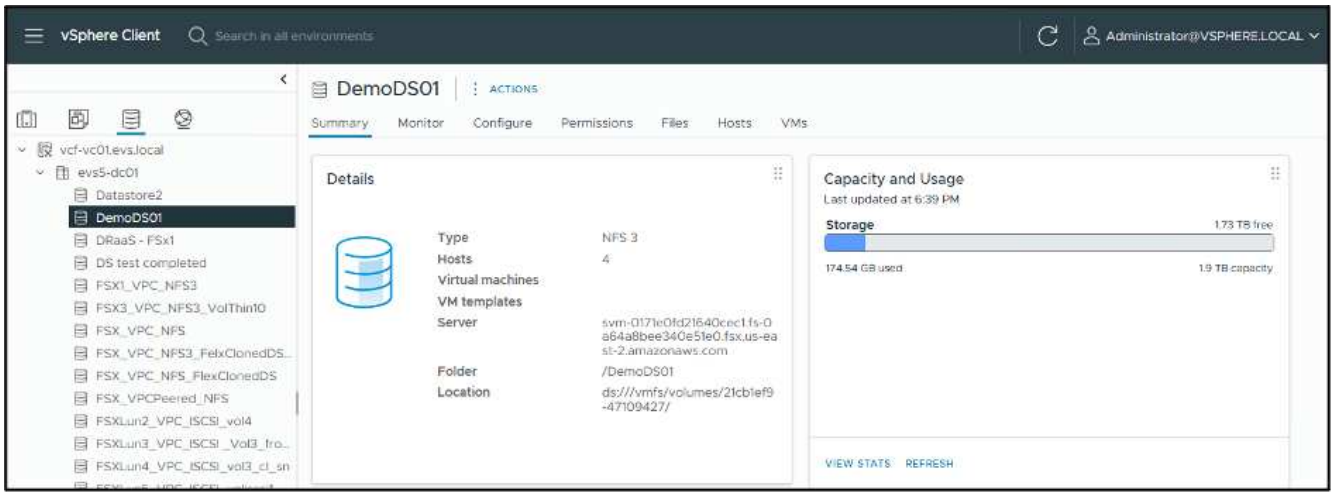
5. Wählen Sie im Schritt „Host-Zugriff“ alle Hosts aus, die Zugriff auf den Datenspeicher benötigen, und klicken Sie dann auf „WEITER“, um fortzufahren.



6. Überprüfen Sie im Schritt „Bereit zum Abschließen“ die Daten und klicken Sie auf „FERTIGSTELLEN“, um die Einrichtung abzuschließen.



7. Überprüfen Sie, ob der NFS-Datenspeicher verbunden wurde, indem Sie wie unten gezeigt auf vCenter zugreifen:



Bereitstellungsverfahren für die Verwendung von FSx for ONTAP als iSCSI-Datenspeicher

In diesem Abschnitt werden die Schritte zum Konfigurieren eines iSCSI-Datenspeichers mit FSx für ONTAP beschrieben.

Voraussetzungen

Bevor Sie FSx für ONTAP als iSCSI-Datenspeicher bereitstellen und anschließen, müssen Sie zunächst eine Amazon EVS-Virtualisierungsumgebung bereitstellen. Weitere Informationen finden Sie in der Dokumentation zum Handbuch „Erste Schritte mit Amazon EVS“. In diesem Abschnitt wird außerdem davon ausgegangen, dass Sie ein FSx für ONTAP Dateisystem bereitgestellt haben. Die entsprechenden Schritte finden Sie im Abschnitt „Detaillierte Vorgehensweise“ oben.

Allgemeine Bereitstellungsschritte

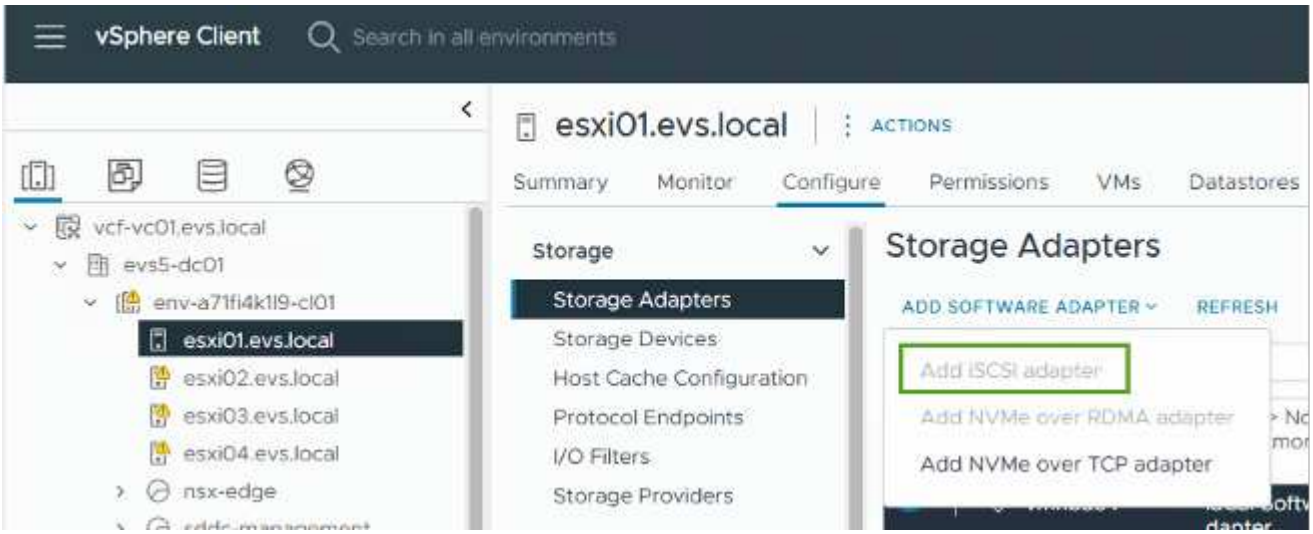
Die Bereitstellung des FSx for ONTAP Dateisystems zur Verwendung als iSCSI-Datenspeicher für Amazon EVS und die Herstellung der Konnektivität zwischen den beiden Diensten umfasst die folgenden Schritte:

- Einrichten eines iSCSI-Netzwerkadapters für jeden ESXi-Host.
- Erstellen und Konfigurieren des FSx für ONTAP Dateisystem, Volume, LUN usw.
- Verbinden der ESXi-Hosts mit dem FSx for ONTAP Dateisystemserver.
- Erstellen eines iSCSI-Datenspeicher-Dateisystems für virtuelle Maschinen (VMFS).

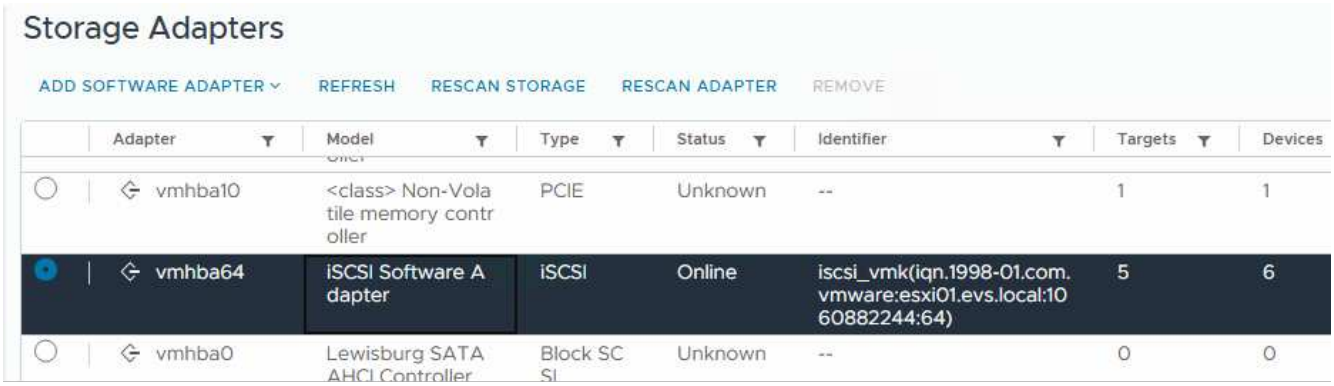
iSCSI-Netzwerkadapter hinzufügen

Die folgenden Schritte müssen auf jedem ESXi-Host in Ihrer Umgebung ausgeführt werden.

1. Rufen Sie den vSphere-Client auf und wählen Sie den ESXi-Host aus. Wählen Sie auf der Registerkarte „Konfigurieren“ die Option „Softwareadapter hinzufügen“ und dann im Dropdown-Menü „iSCSI-Adapter hinzufügen“, wie hier gezeigt:

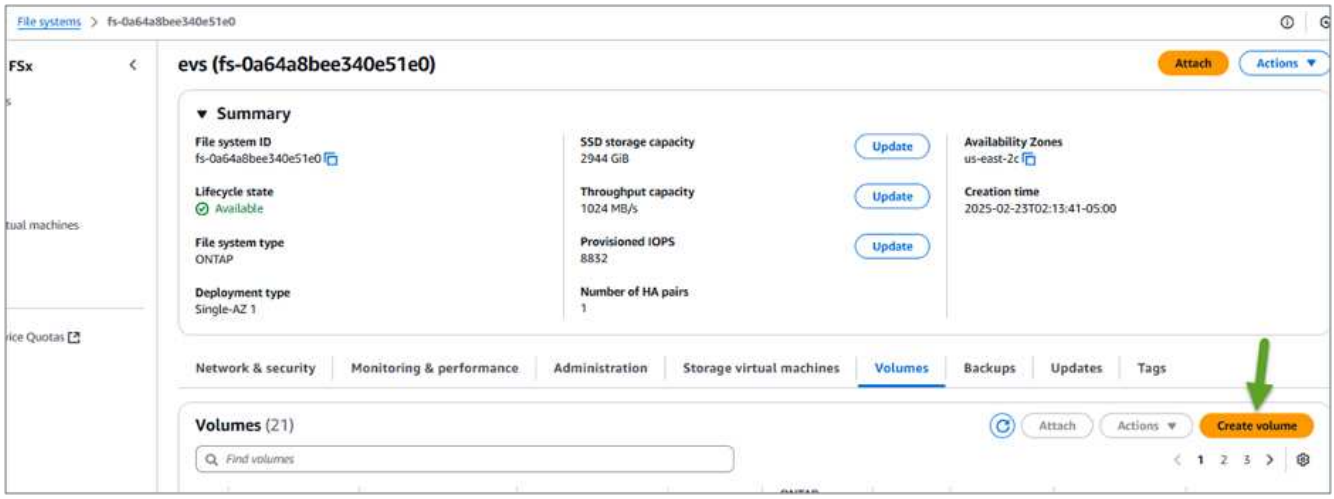


2. Sobald die Installation abgeschlossen ist, befinden Sie sich auf dem Bildschirm „Speicheradapter“. Wählen Sie „Adapter erneut scannen“ aus der Menüleiste. Notieren Sie den IQN des iSCSI-Adapters: iqn.xxxx. Dieser Wert wird später im LUN-Mapping-Schritt verwendet.



Erstellen Sie ein FSx für ONTAP -Volume

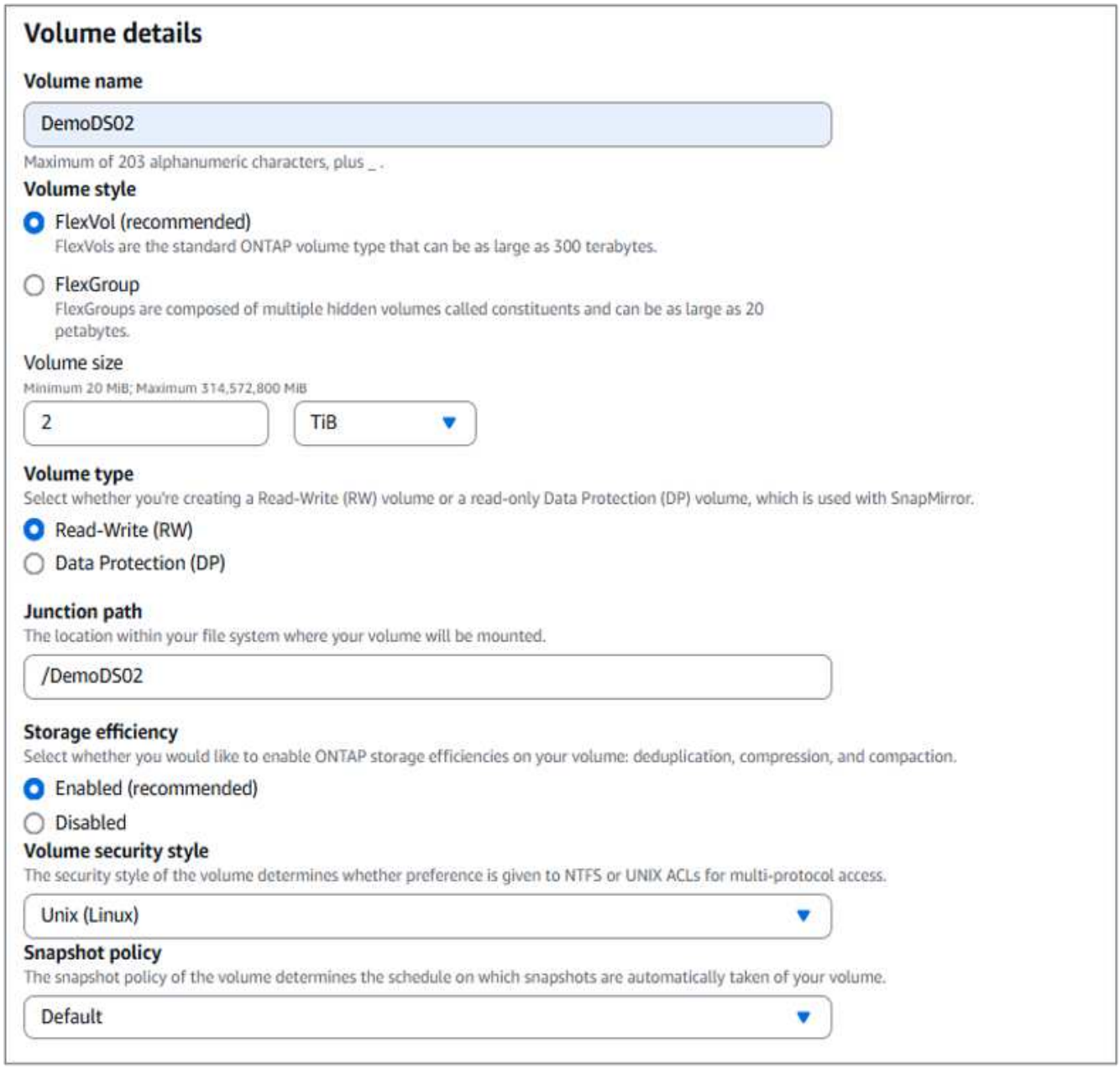
1. Gehen Sie zur AWS-Konsole, rufen Sie die Seite für Ihr FSx for ONTAP -Dateisystem auf und klicken Sie auf „Volume erstellen“.



2. Wählen Sie die SVM aus, auf der Sie das Volume erstellen möchten.



3. Geben Sie auf der Seite „Volumedetails“ die Details wie im folgenden Screenshot gezeigt ein. Wenn Sie fertig sind, klicken Sie auf „Erstellen“, um das Volume einzurichten. Wählen Sie „Aktiviert“, um die ONTAP Speichereffizienzfunktionen (Komprimierung, Deduplizierung und Kompaktierung) zu aktivieren.



4. Wählen Sie für die Speicher-Tiering-Option „Nur Snapshot“ aus dem Dropdown-Menü und legen Sie eine Kühlperiode für die Tiering-Richtlinie fest. Der Standardwert beträgt 31 Tage, für dieses Beispiel legen wir jedoch eine Abkühlungsperiode von zwei Tagen fest.



5. Nachdem das Volume erstellt wurde, legen Sie mit der ONTAP CLI die folgenden Werte fest:

Einstellung	Konfiguration
Volumengarantie	Keine (Thin Provisioning)
Teilreserve	0 %
snap_reserve	0 %
Automatische Größe	wachsen_schrumpfen
Speichereffizienz	Ermöglicht
Volume-Tiering-Richtlinie	Nur Schnappschuss
Aktualisierung der Zugriffszeit (-atime-update)	FALSCH
Minimaler Readahead (-min-readahead)	FALSCH
Snapshot-Richtlinie	Keine
LUN-Speicherplatzreservierung	Deaktiviert
LUN-Speicherplatzzuweisung	Ermöglicht

Erstellen Sie eine LUN, eine igroup und ordnen Sie die LUN zu

In diesem Abschnitt zeigen wir, wie Sie die LUN erstellen, die in vSphere als Festplatte angezeigt wird. Wir zeigen auch, wie eine Initiatorgruppe (igroup) erstellt wird, also die Liste der Initiatoren, die Zugriff auf die LUN haben. Die igroup ermöglicht den Zugriff auf die LUN von den vSphere ESXi-Hosts. Abschließend zeigen wir, wie die igroup der LUN zugeordnet wird.

1. Um auf die ONTAP CLI zuzugreifen, richten Sie eine SSH-Sitzung auf dem Verwaltungsport des FSx for ONTAP -Dateisystems oder SVM ein, indem Sie den folgenden Befehl ausführen:

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. Erstellen Sie die LUN. Stellen Sie sicher, dass die Speicherzuweisung und Speicherreservierung aktiviert sind. Die Größe sollte bis zu 90 % der Volumengröße betragen:

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. Erstellen Sie die Igroup und fügen Sie den IQN aller ESXi-Hosts innerhalb des Clusters hinzu.

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. Ordnen Sie die LUN mit dem folgenden Code zu:

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. Überprüfen Sie die LUN-Zuordnung und stellen Sie sicher, dass der Status in „Zugeordnet“ geändert wurde. Dies ist eine notwendige doppelte Überprüfung, um sicherzustellen, dass sich die LUN in einem zugeordneten Zustand befindet:

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

Abrufen von iSCSI-Konfigurationsinformationen vom SVM

1. Führen Sie „iSCSI show“ aus und notieren Sie den Zielnamen. Dies wird bei der vSphere-Erkennung der FSx für ONTAP Festplatten verwendet (Hinweis: Dieser Zielname ist für Ihre SVM eindeutig):

```
Fsxid::> iscsi show -vserver fsx
                Vserver: fsx
            Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
           Target Alias: fsx
   Administrative Status: up
```

2. Notieren Sie die iSCSI-IP-Adressen:

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

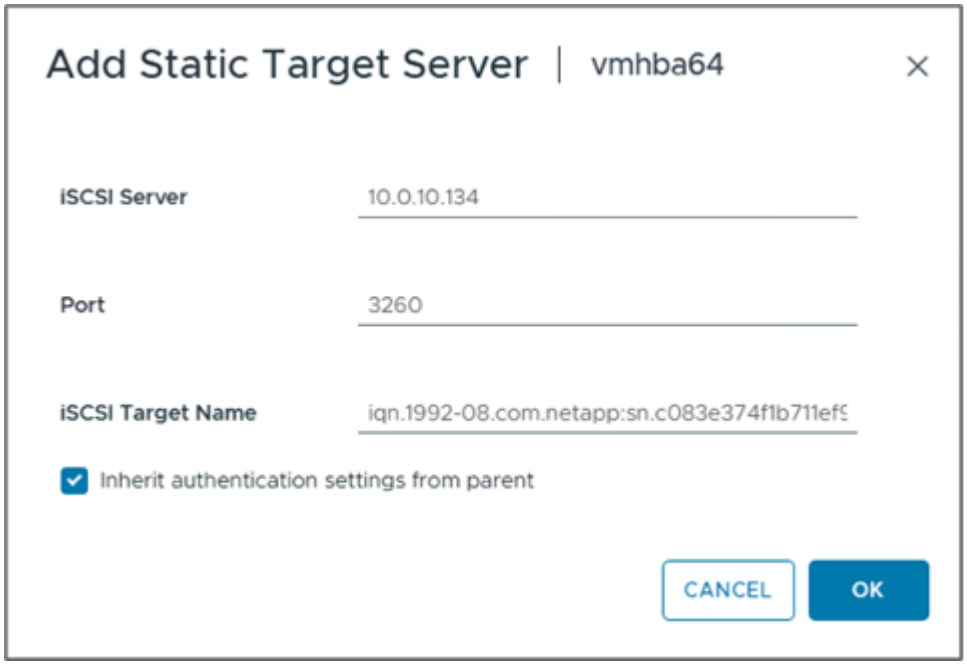
Entdecken Sie den FSx für ONTAP iSCSI-Server

Nachdem wir nun die LUN zugeordnet haben, können wir den FSx for ONTAP iSCSI-Server für die SVM ermitteln. Beachten Sie, dass Sie die hier aufgeführten Schritte für jeden ESXi-Host wiederholen müssen, der in Ihrem SDDC vorhanden ist.

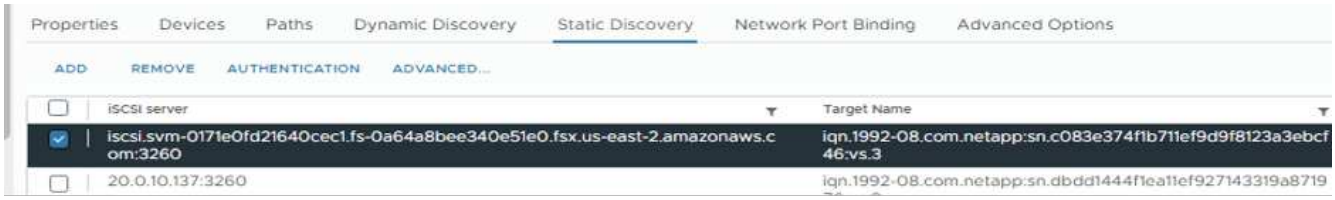
1. Stellen Sie zunächst sicher, dass die mit dem FSx for ONTAP Dateisystem verknüpfte Sicherheitsgruppe (d. h. die mit dem ENI verbundene) iSCSI-Ports zulässt.

   Eine vollständige Liste der iSCSI-Protokollports und deren Anwendung finden Sie unter"Dateisystem-Zugriffskontrolle mit Amazon VPC" .

2. Gehen Sie im vSphere-Client zu ESXi-Host > Speicheradapter > Statische Erkennung und klicken Sie auf „Hinzufügen“.
3. Geben Sie die IP-Adresse des iSCSI-Servers von oben ein (Port ist 3260). Der iSCSI-Zielname ist der IQN aus dem iSCSI-Show-Befehl. Klicken Sie auf „OK“, um fortzufahren.



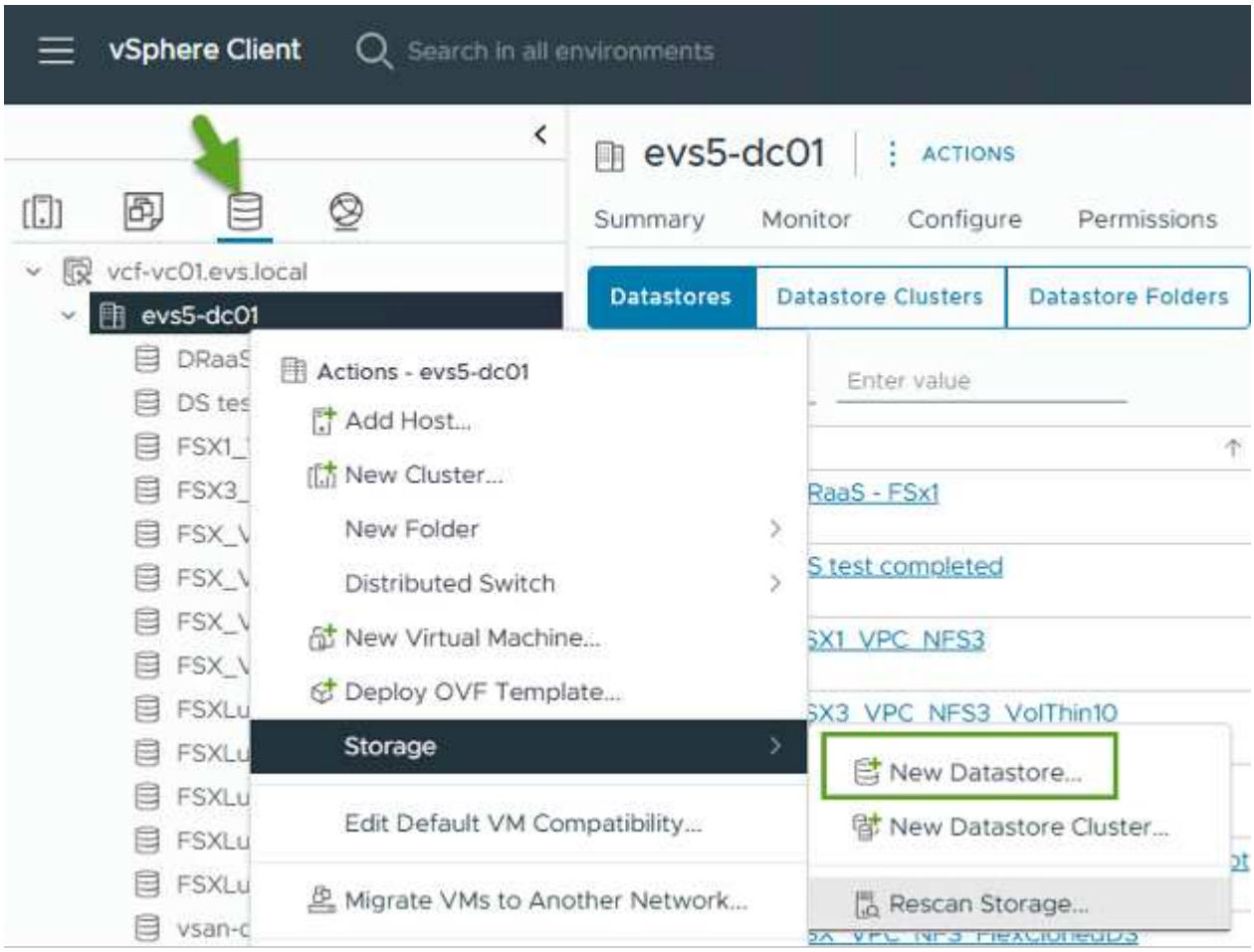
4. Der Assistent wird geschlossen und Sie gelangen zum Bildschirm „Statische Datenspeichererkennung“. In der Tabelle auf dieser Seite können Sie überprüfen, ob das Ziel erkannt wurde.



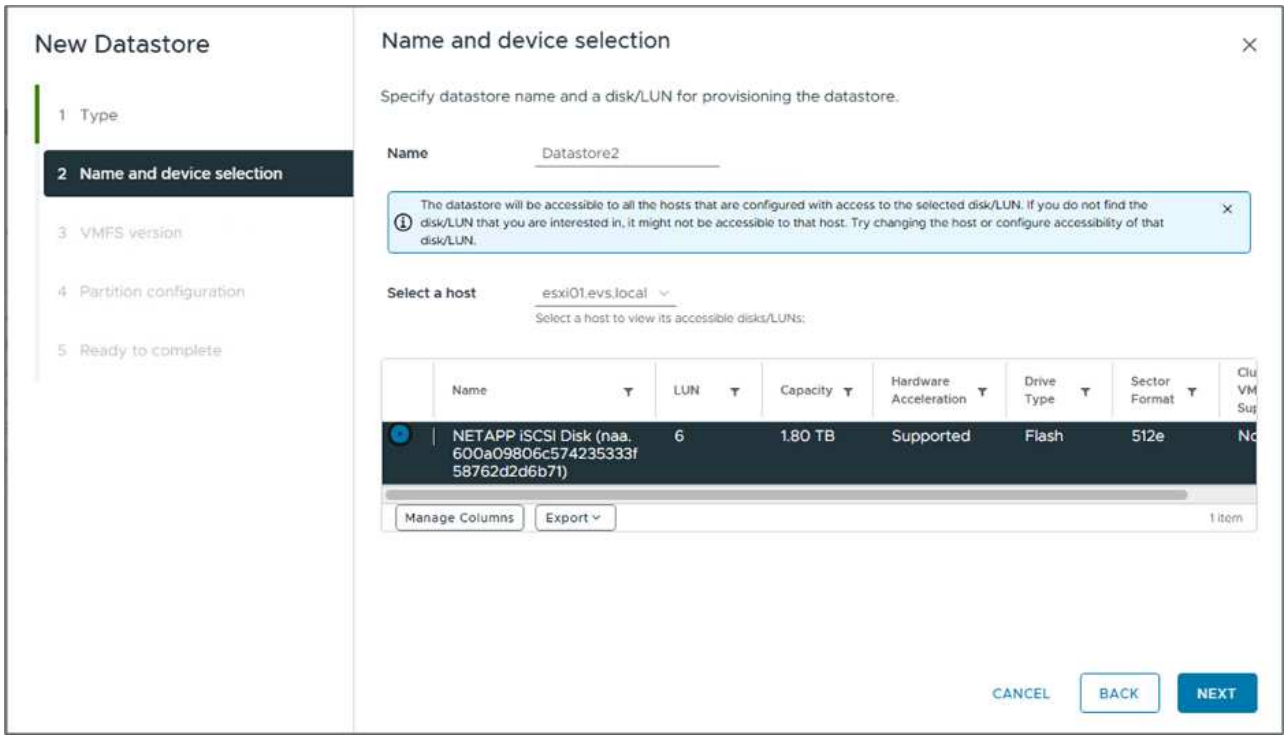
Erstellen eines iSCSI-Datenspeichers

Nachdem wir den iSCSI-Server ermittelt haben, können wir einen iSCSI-Datenspeicher erstellen.

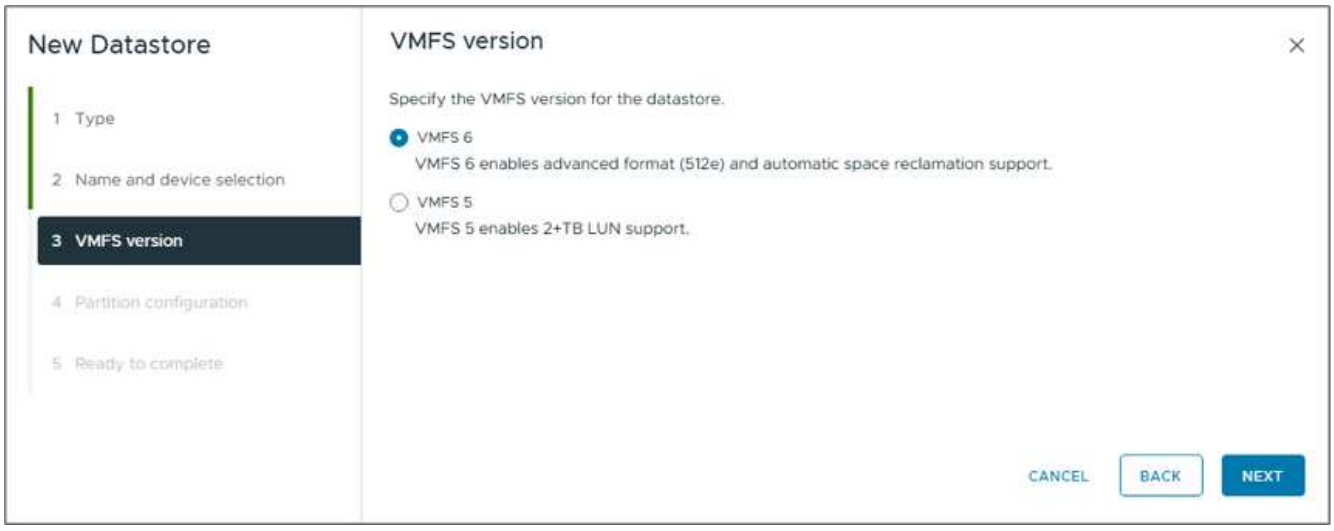
1. Gehen Sie im vSphere-Client zur Registerkarte „Datastore“ und wählen Sie das SDDC aus, in dem Sie den Datastore bereitstellen möchten. Klicken Sie mit der rechten Maustaste und wählen Sie das Speichersymbol (im Screenshot unten durch den grünen Pfeil gekennzeichnet) aus. Wählen Sie dann „Neuer Datenspeicher“ aus dem Dropdown-Menü:



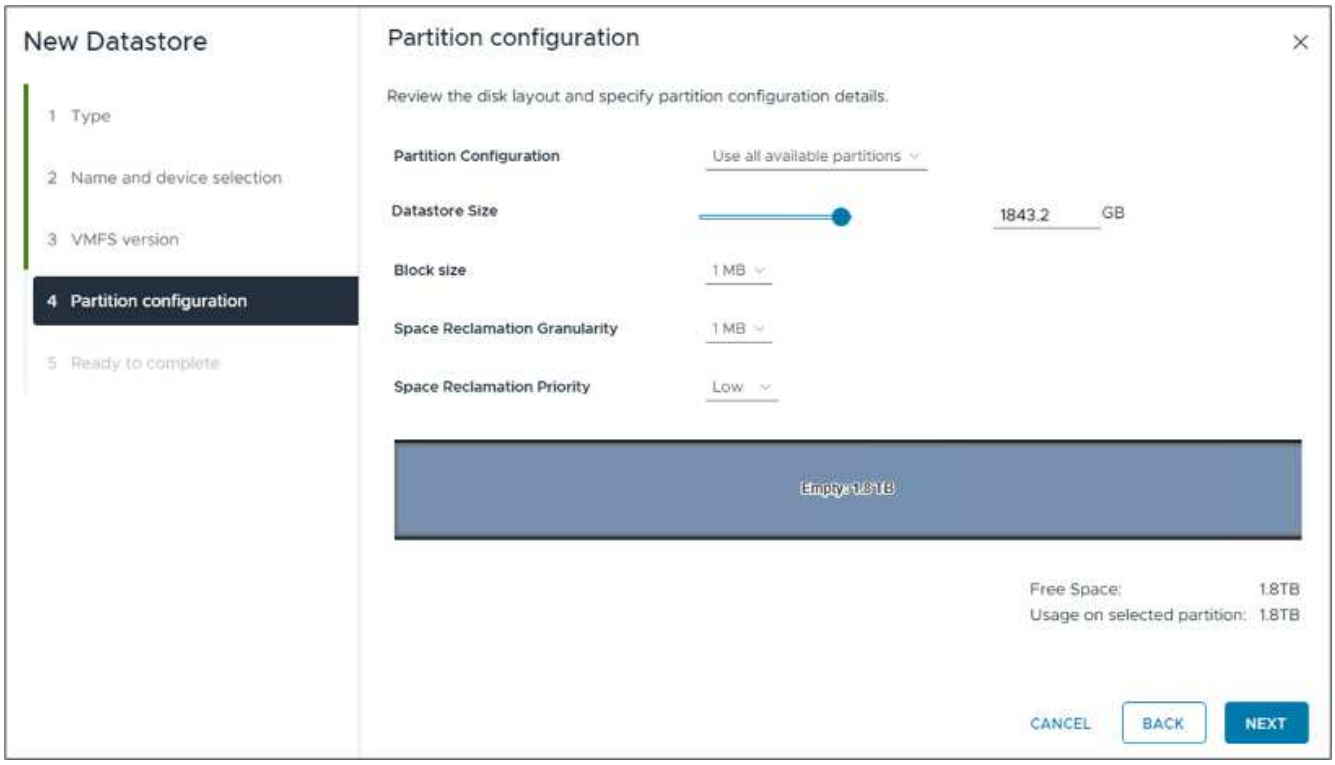
2. Sie befinden sich jetzt im Assistenten „Neuer Datenspeicher“. Wählen Sie im Schritt „Typ“ die Option VMFS aus.
3. Im Schritt „Namens- und Geräteauswahl“:
   a. Geben Sie einen Namen für Ihren Datenspeicher ein.
   b. Wählen Sie aus, welchen ESXi-Host Sie mit dem Datenspeicher verbinden möchten.
   c. Wählen Sie die erkannte Festplatte (LUN) aus und klicken Sie auf „Weiter“.



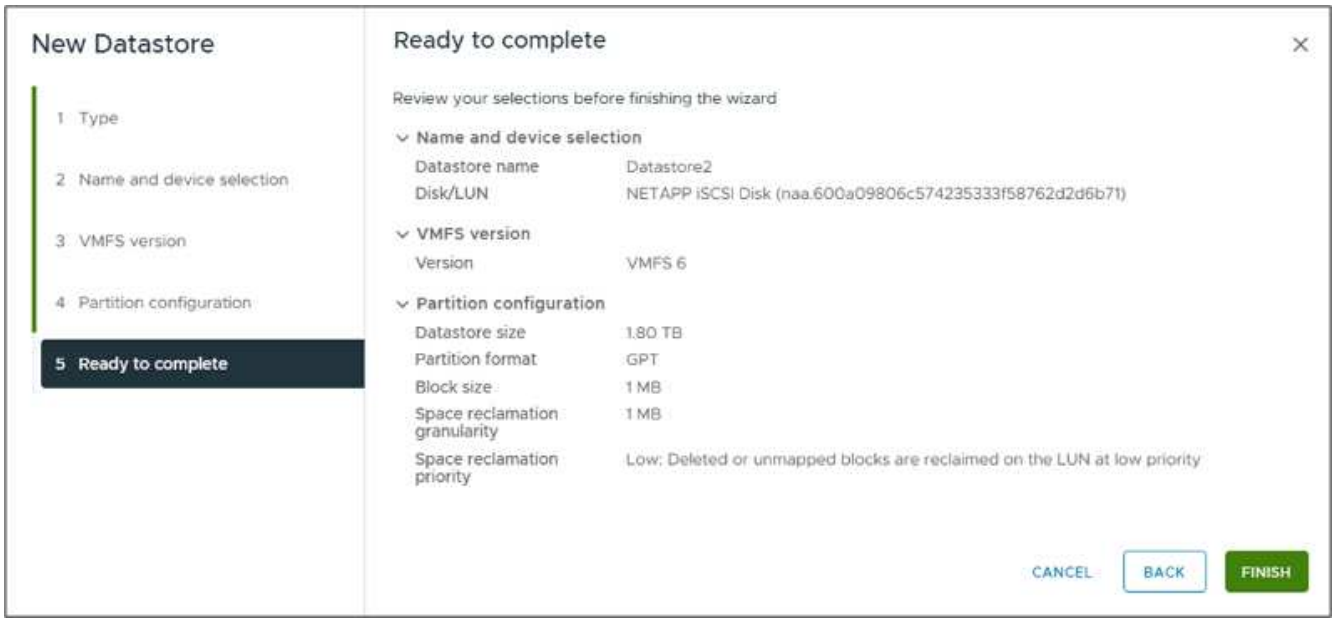
4. Wählen Sie im Schritt „VMFS-Version“ „VMFS 6“ aus.



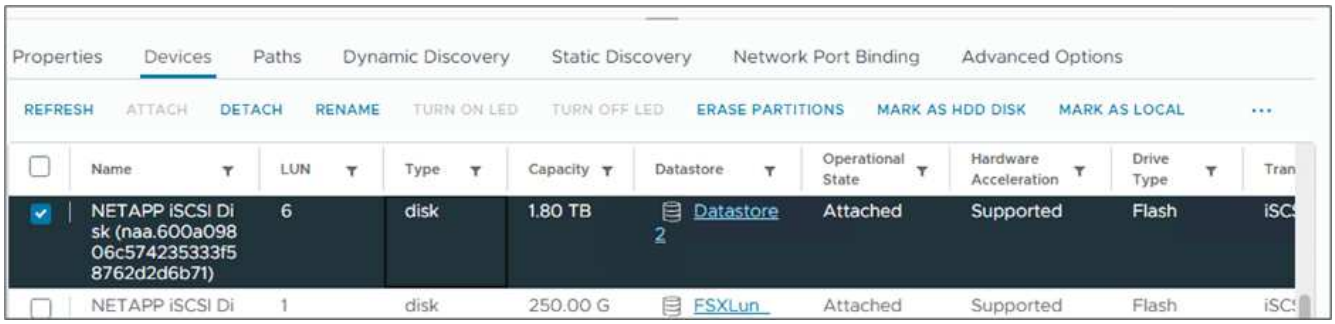
5. Lassen Sie im Schritt „Partitionskonfiguration“ die Standardeinstellungen unverändert, einschließlich der Option „Alle verfügbaren Partitionen verwenden“. Klicken Sie auf „Weiter“, um fortzufahren.



6. Stellen Sie im Schritt „Bereit zum Abschließen“ sicher, dass die Einstellungen korrekt sind. Wenn Sie fertig sind, klicken Sie auf „FERTIGSTELLEN“, um die Einrichtung abzuschließen.



7. Kehren Sie zur Seite „Geräte“ zurück und überprüfen Sie, ob der Datenspeicher angeschlossen wurde.



Abschluss

Dieses Dokument enthält Anweisungen zum Einrichten von FSx für ONTAP als externer Speicher für Amazon EVS zur Verwendung mit den Protokollen NFS und iSCSI.

Die Verwendung von FSx für ONTAP als externer Speicher für Amazon EVS bietet klare betriebliche und geschäftliche Vorteile. Es bietet durch die ONTAP Technologie eine bessere Datenausfallsicherheit, besseren Schutz, bessere Replikation und Kosteneffizienz und sorgt dank der Entkopplung der hyperkonvergenten VMware-Architektur für optimierte Gesamtbetriebskosten. Mit FSx für ONTAP können Amazon EVS-Benutzer den Speicher skalieren, ohne Rechenressourcen hinzuzufügen und ohne die Kosten in die Höhe zu treiben. Dadurch wird das volle Elastizitäts- und Skalierbarkeitspotenzial der AWS Cloud erschlossen.

Weitere Informationen finden Sie in der Ankündigung zu den Neuerungen von Amazon:"Amazon EVS ist jetzt in FSx für ONTAP integriert" und im NetApp -Blog:"Amazon EVS kündigt Unterstützung für FSx für ONTAP an" .

FSx ONTAP Datenspeicher für EVS schützen

Wie Sie Amazon FSx for NetApp ONTAP-Datastores mit Amazon Elastic VMware Service mithilfe des NetApp SnapCenter Plug-in for VMware schützen

Dieser Leitfaden zeigt einen einfachen Bereitstellungsansatz zum Schutz von FSx for ONTAP Network File System (NFS) und iSCSI Amazon EVS-Datenspeichern und zugehörigen VMs mithilfe der NetApp SnapCenter Plug-in for VMware vSphere (SCV) Backup und Recovery-Lösung für VMs.

Einführung

Amazon FSx for NetApp ONTAP (FSx for ONTAP)-basierte zusätzliche Datenspeicher für Amazon Elastic VMware Service (Amazon EVS) bieten eine hervorragende Lösung für die Ausführung sowohl leistungsintensiver Workloads – wie etwa durch die Nutzung von nConnect, Amazon Virtual Private Cloud (Amazon VPC) Peering und die Verwendung mehrerer Netzwerkverbindungen pro Datenspeicher-Mount – als auch speicherintensiver Workloads.

Diese Funktion ermöglicht es Kunden, die Einschränkungen des lokalen Instanzspeichers, der von einem virtuellen storage area network (vSAN) bereitgestellt wird, zu überwinden, den Speicher unabhängig von der Rechenleistung zu skalieren und die Gesamtbetriebskosten zu senken. Neben den Vorteilen bei den Gesamtbetriebskosten (TCO) bietet FSx for ONTAP Amazon EVS mit Funktionen der Enterprise-Klasse, die Kunden von On-Premises ONTAP kennen, und trägt so zur Optimierung und Vereinfachung von Bereitstellungen bei. Mit FSx for ONTAP erhalten Sie Zugriff auf NetApp Snapshot, SnapMirror und SnapVault -Technologien, die Backup- und Recovery-Operationen für virtuelle Maschinen (VMs), Datastores und virtuelle Festplatten (VMDKs) unterstützen. Ein zentrales Merkmal ist der Snapshot-basierte Schutz.

Überblick

Mit der Skalierung und Konsolidierung von IT-Umgebungen in Unternehmen gewinnt der Schutz dieser Workloads und des zugrunde liegenden Speichers zunehmend an Bedeutung. SCV kann verwendet werden, um Datenspeicher und virtuelle Maschinen direkt über den Amazon EVS vSphere Client zu sichern.

Zweck dieses Handbuchs

Dieser Leitfaden enthält Anweisungen zum Schutz eines FSx for ONTAP Datastores für Amazon EVS mithilfe von SCV. Beispielszenarien zum Schutz von VMs und Datenbanken sowie zur Wiederherstellung werden ebenfalls bereitgestellt.

Publikum

Dieses Tutorial richtet sich an Cloud-Architekten und Cloud-Administratoren, die mit VMware vSphere, Amazon EVS, der AWS-Konsole und FSx für ONTAP vertraut sind.

Wichtige Schritte für die Bereitstellung und Konfiguration

Nachfolgend sind die wichtigsten Schritte für die Bereitstellung und Konfiguration von SCV zum Schutz Ihrer VMs und Datastores auf Amazon EVS aufgeführt:

1. Laden Sie die SCV Open Virtual Appliance (OVA) herunter.
2. Melden Sie sich mit den vSphere Client-Zugangsdaten bei Amazon EVS an.
3. Stellen Sie eine Open Virtualization Format (OVF)-Vorlage bereit, um den VMware-Bereitstellungsassistenten zu starten.
4. Um auf das Plug-in zuzugreifen, wählen Sie SnapCenter Plug-in für VMware aus dem Menü aus.
5. Speicher hinzufügen.
6. Backup-Richtlinien erstellen.
7. Ressourcengruppen erstellen.
8. Backup-Ressourcengruppen.
9. Stellen Sie die gesamte virtuelle Maschine oder eine bestimmte virtuelle Festplatte oder Gastdateien wieder her.

Einrichtungsprozedur für SnapCenter Plug-in für VMware

In diesem Abschnitt werden die Schritte zur Einrichtung des SnapCenter Plug-in für VMware beschrieben.

Voraussetzungen

Folgende Voraussetzungen sind erforderlich, bevor Sie beginnen:

1. Für die Registrierung des vCenter Servers während der Bereitstellung der OVA geben Sie den vollqualifizierten Domainnamen (FQDN) oder die IP-Adresse des vCenter an.
2. Für die vCenter-Anmeldeinformationen verwenden Sie ein Konto mit minimal erforderlichen Berechtigungen
3. Firewall-Ports für den vCenter Serverzugriff öffnen.
4. Aktualisieren Sie die Sicherheitsgruppe der Amazon VPC, in der FSx for ONTAP ausgeführt wird, um SCV den Zugriff auf FSx for ONTAP zu ermöglichen.

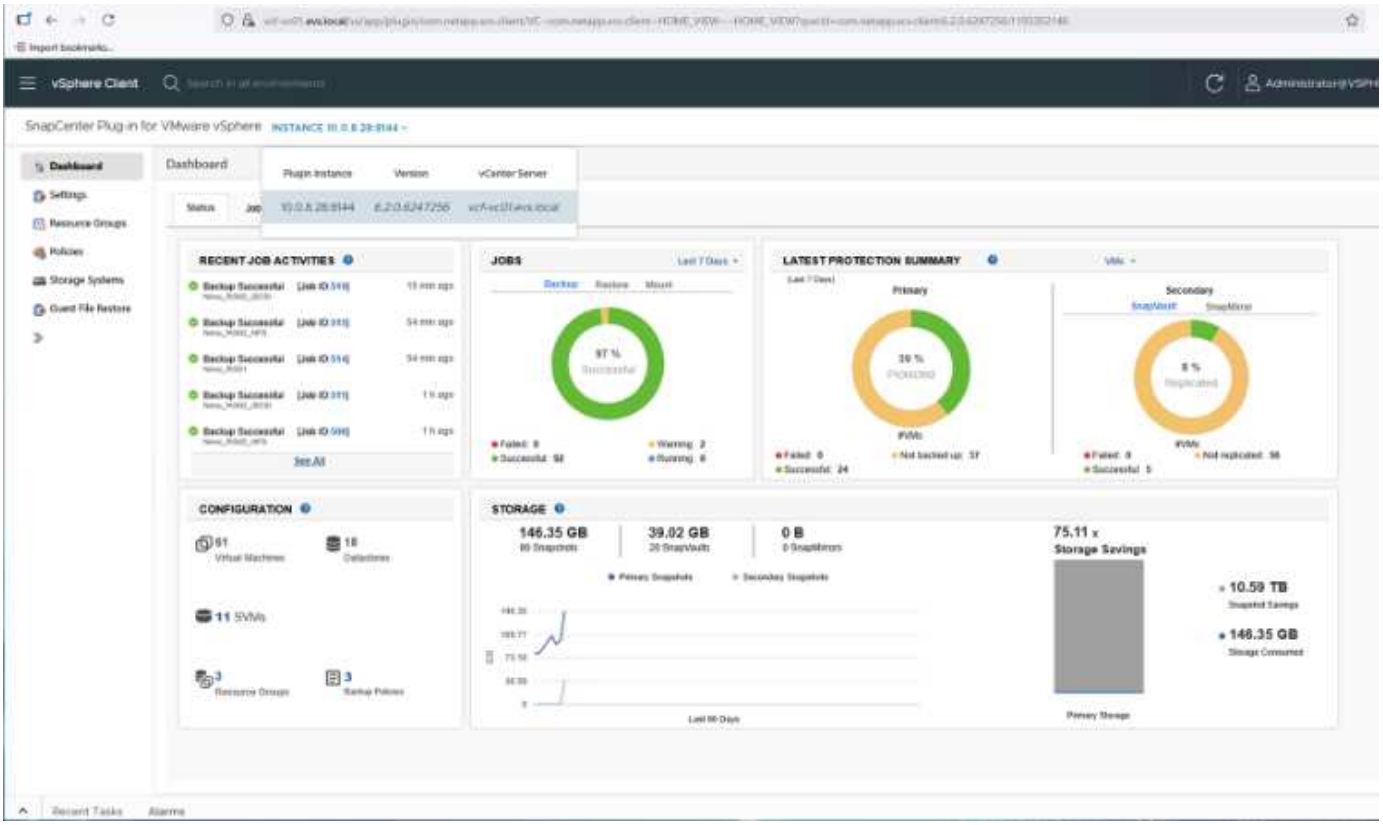
SCV ist kostenlos erhältlich.

Einrichten des SnapCenter Plug-ins für VMware

Zum Schutz von VMs und NFS/iSCSI-basierten Datenspeichern, auf denen sie gehostet werden, muss SCV bereitgestellt werden. Es ist ein einfacher OVF-Import.

Die Schritte zur Bereitstellung sind wie folgt:

1. Lade die OVA von "NetApp Support Site" herunter.
2. Melden Sie sich bei Amazon EVS vCenter an.
3. Klicken Sie innerhalb von vCenter mit der rechten Maustaste auf ein beliebiges Inventarobjekt wie ein Rechenzentrum, einen Ordner, einen Cluster oder einen Host und wählen Sie „OVF-Vorlage bereitstellen“.
4. Wählen Sie die korrekten Einstellungen, einschließlich Speicher, Segment, und passen Sie die Vorlage an, um das vCenter und dessen Zugangsdaten zu aktualisieren, SCV-Zugangsdaten und IP-Details zu erstellen. Nachdem Sie alles überprüft haben, wählen Sie „Fertigstellen“.
5. Warten Sie, bis die OVF-Import- und Bereitstellungsaufgaben abgeschlossen sind.
6. Sobald SCV erfolgreich bereitgestellt wurde, wird es innerhalb von vCenter registriert.
7. Um auf das Plug-in zuzugreifen, navigieren Sie zur linken Seitenleiste der vCenter Webclient-Seite und wählen Sie „SnapCenter Plug-in for VMware“.



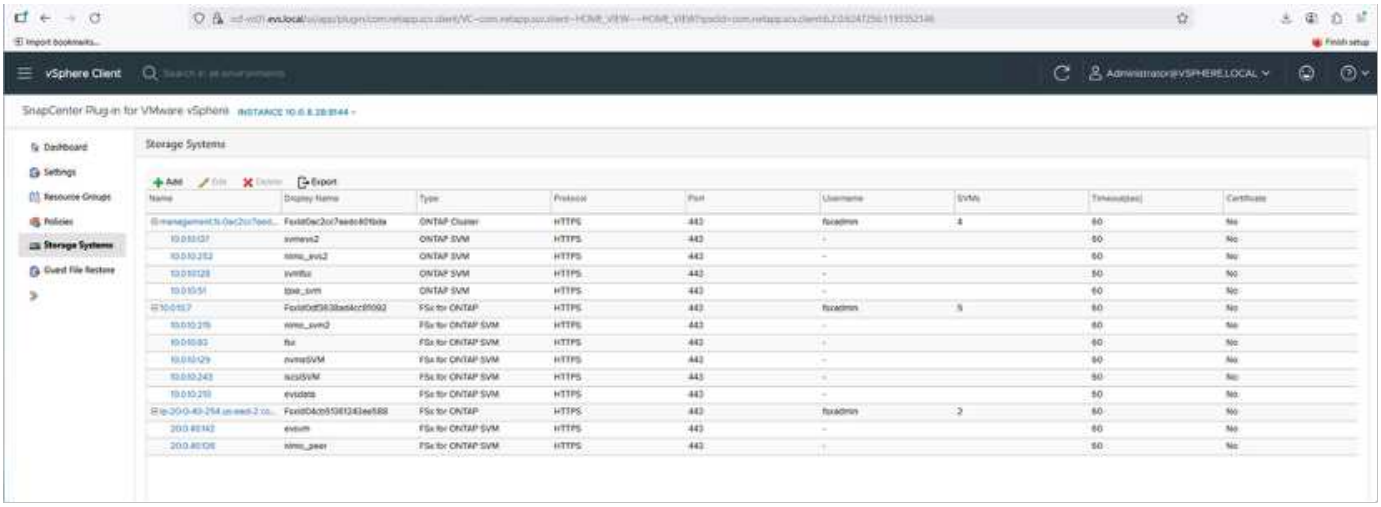
Konfigurationsverfahren für das SnapCenter Plug-in für VMware

Dieser Abschnitt beschreibt die Schritte zur Konfiguration des SnapCenter Plug-in für VMware. Die folgenden Abschnitte erläutern, wie Speicher hinzugefügt, eine Sicherungsrichtlinie erstellt und Ressourcengruppen erstellt werden.

Hinzufügen des Speichersystems

Der nächste Schritt zum Schutz von Workloads mit Switched Virtual Connection ist das Hinzufügen von "Speichersystem". Durch das Hinzufügen von Speicher kann SCV Sicherungs- und Wiederherstellungsvorgänge innerhalb von vCenter erkennen und verwalten. Fügen Sie den FSx for NetApp ONTAP Management-Endpunkt oder die IP-Adresse des Verwaltungsendpunkts der Storage Virtual Machine (SVM) als Speichersystem hinzu, um die Sicherung und Wiederherstellung von VMs zu aktivieren.

1. Wählen Sie im linken Navigationsmenü des EVS vCenter die Option „SnapCenter Plug-in for VMware“.
2. Wählen Sie „Storage System“.
3. Wählen Sie „Add“, um die FSx for ONTAP Details hinzuzufügen.
4. Verwenden Sie die Methode „Credentials as the Authentication“ und geben Sie FSxadmin als Benutzernamen und Passwort ein. Wählen Sie dann „Add“, um die Einstellungen zu speichern.



Alle SVMs werden automatisch hinzugefügt, wenn das Dateisystem hinzugefügt wird.

Wenn die SCV-Version 6.2 ist, gehen Sie zu "die SCV Support-Seite" und laden Sie die SCV 6.2P1-Version herunter.

Erstellen Sie eine Sicherungsrichtlinie

Eine robuste Backup-Strategie sollte Schlüsselfaktoren wie den Backup-Zeitplan, die zu sichernden Daten und die Aufbewahrungsdauer der Backups definieren. Snapshot-Kopien können stündlich oder täglich geplant werden, um ganze Datastores zu schützen. Durch diese Art der Backup-Planung werden nicht nur die Datastores gesichert, sondern auch Backup- und Wiederherstellungsvorgänge für die darin enthaltenen VMs und VMDKs unterstützt.

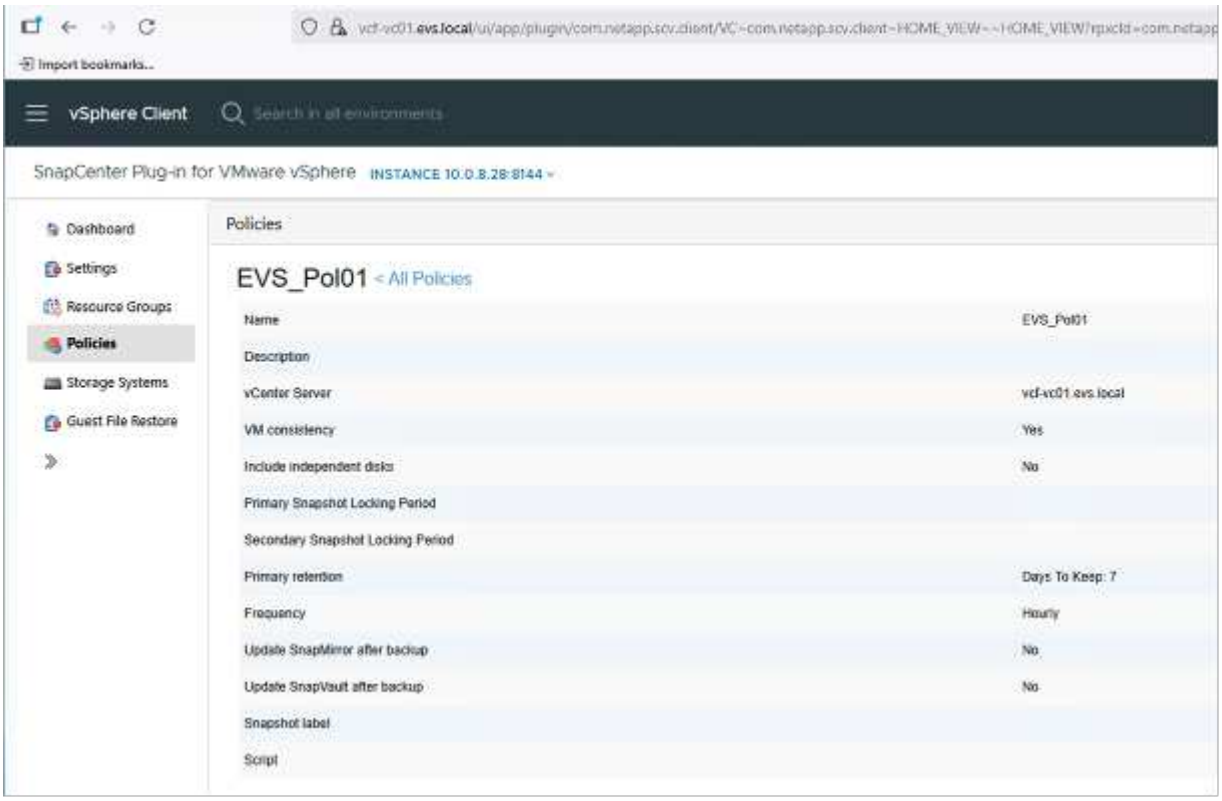
Bevor Sie Backups für VMs und Datenspeicher starten, erstellen Sie eine "Sicherungsrichtlinie" und eine Ressourcengruppe. Die Backup-Richtlinie legt Parameter wie den Backup-Zeitplan und die Aufbewahrungseinstellungen fest.

Hier sind die Schritte zum Erstellen einer Backup-Richtlinie:

1. Gehen Sie im Navigationsbereich auf der linken Seite in SCV und wählen Sie „Richtlinien“.
2. Wählen Sie auf der Seite „Policies“ die Option „Create“, um den Assistenten zu starten.
3. Geben Sie auf der Seite „New Backup Policy“ einen Namen für die Richtlinie ein.

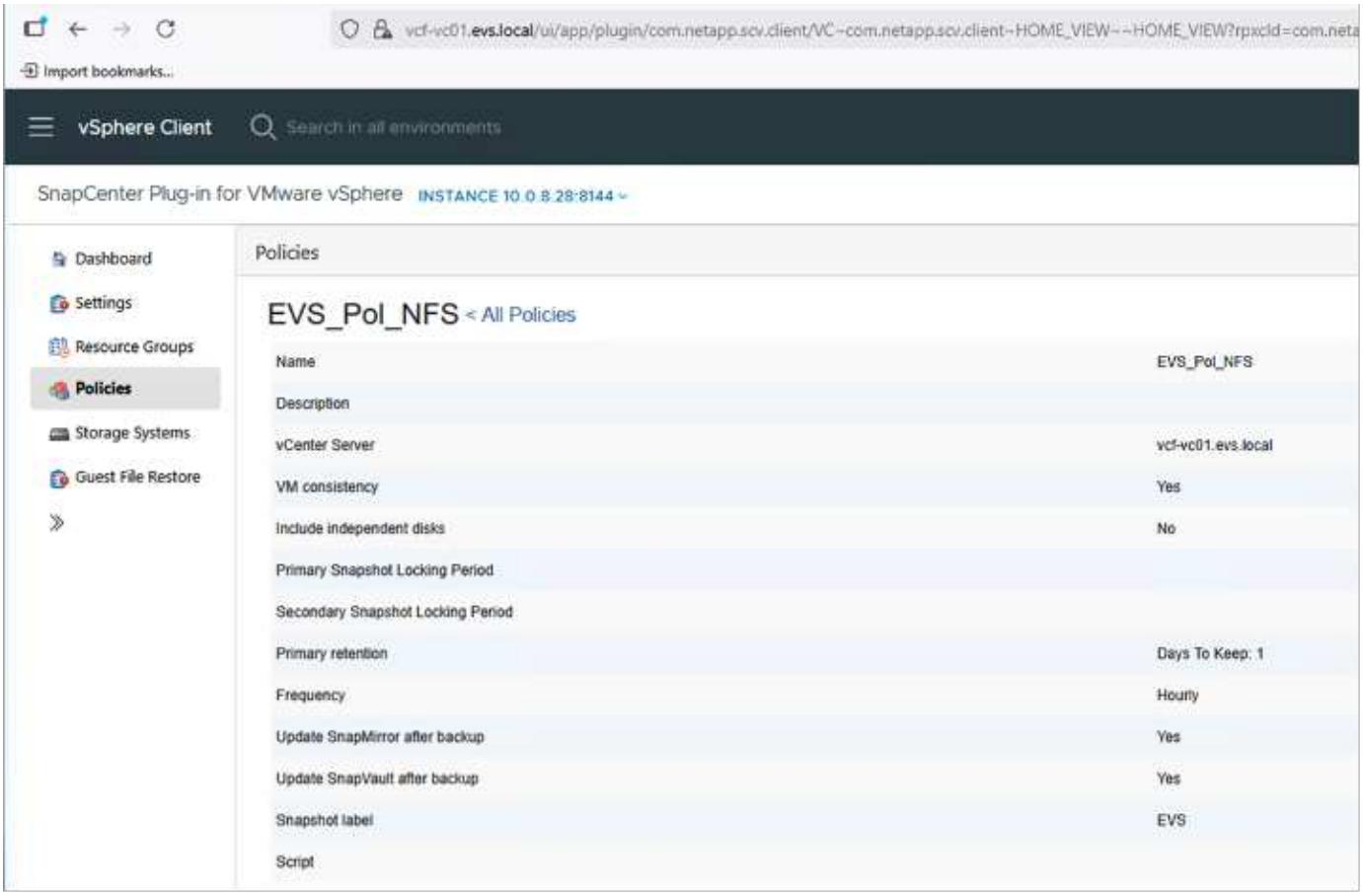
4. Geben Sie die Aufbewahrungsfrist, die Sicherungshäufigkeit und die Replikationseinstellungen an.
5. Aktivieren Sie das Kontrollkästchen „Sperrzeitraum“, um die Snapshot-Sperre zu aktivieren. Sie können die primären und sekundären Snapshot-Sperrzeiträume als Tage/Monate/Jahre auswählen.

Ungeachtet des in der SnapMirror-Richtlinie definierten Aufbewahrungswerts bleibt die sekundäre Snapshot-Kopie so lange intakt, bis die angegebene Sperrfrist für den sekundären Snapshot abläuft.



Um VM-konsistente Backups zu aktivieren, müssen die VMware tools installiert und ausgeführt werden. Wenn das VM-Konsistenz-Kästchen aktiviert ist, werden die VMs zunächst in den Ruhezustand versetzt, dann erstellt VMware einen VM-konsistenten Snapshot (ohne Arbeitsspeicher), anschließend führt SCV die Backup-Operation durch und danach wird der VM-Betrieb fortgesetzt.

Um Snapshot-Kopien auf ein sekundäres Spiegel- oder Vault-Dateisystem zu replizieren, müssen die Beziehungen vorher konfiguriert werden.



Sobald die Richtlinie erstellt ist, besteht der nächste Schritt darin, die Ressourcengruppe zu erstellen, die die entsprechenden NFS- oder iSCSI-Datastores und VMs definiert, die gesichert werden sollen.

Erstellen Sie eine Ressourcengruppe

Eine Ressourcengruppe dient als Container für VMs und Datenspeicher, die Schutz benötigen. Ressourcen können jederzeit zu oder aus einer Ressourcengruppe hinzugefügt oder entfernt werden, was Flexibilität bei der Verwaltung von Sicherungskonfigurationen bietet.

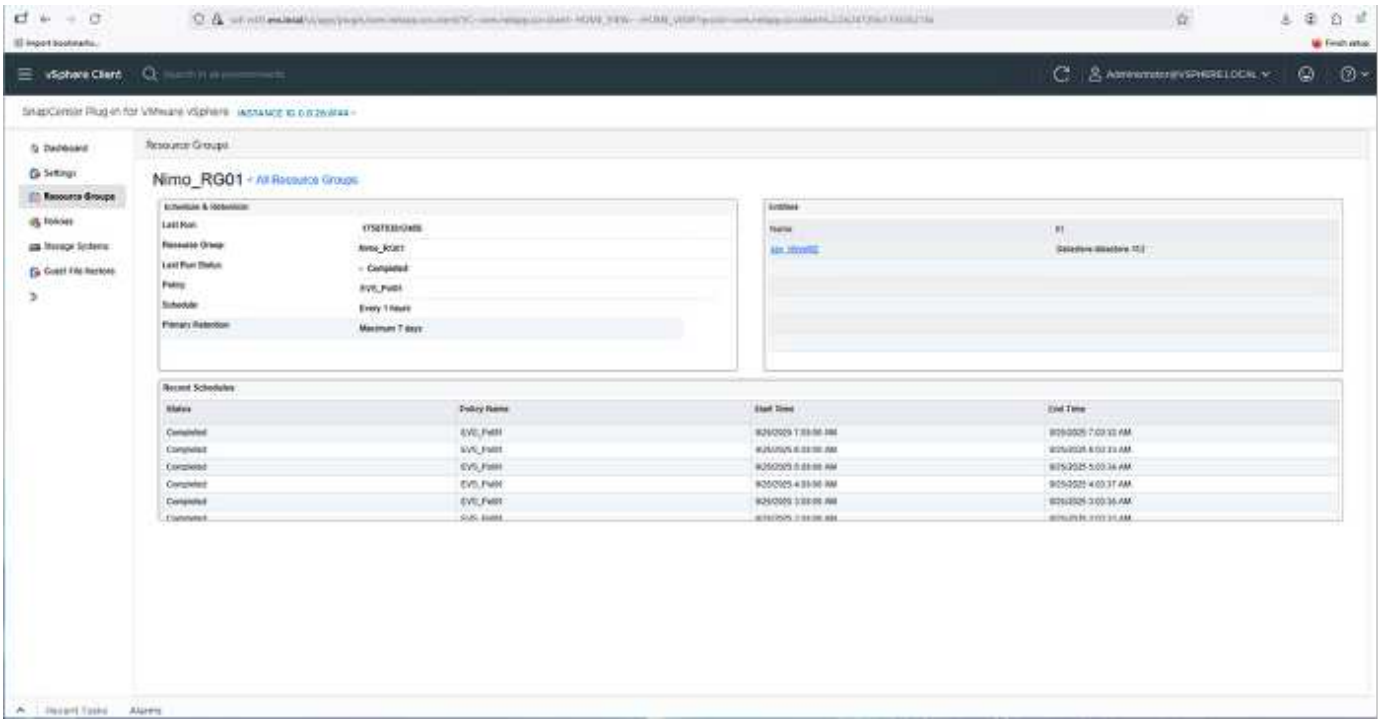
Sie können ein "Ressourcengruppe" mit den folgenden Schritten erstellen:

1. Gehen Sie im Navigationsbereich auf der linken Seite in SCV zu „Ressourcengruppen“.
2. Wählen Sie auf der Seite Ressourcengruppen „Erstellen“, um den Assistenten zur Erstellung von Ressourcengruppen zu starten.

> Eine weitere Option zum Erstellen von Ressourcengruppen besteht darin, eine einzelne VM oder einen Datenspeicher auszuwählen und eine Ressourcengruppe zu erstellen, die nur diese Ressource enthält.

3. Wählen Sie auf der Seite „Resources“ den Scope (VMs oder Datastores) und das Data Center aus.
4. Wählen Sie auf der Seite „Spanning disks“ die Option „Virtual Machines with multiple VMDKs across multiple datastores“.
5. Als Nächstes ordnen Sie eine Sicherungsrichtlinie zu. Wählen Sie eine vorhandene Richtlinie aus oder erstellen Sie eine neue Sicherungsrichtlinie.
6. Konfigurieren Sie auf der "Zeitpläne"-Seite den Sicherungszeitplan für jede ausgewählte Richtlinie.

7. Sobald Sie die entsprechenden Auswahlen getroffen haben, wählen Sie „Fertigstellen“. Dadurch wird eine neue Ressourcengruppe erstellt und der Ressourcengruppe hinzugefügt.



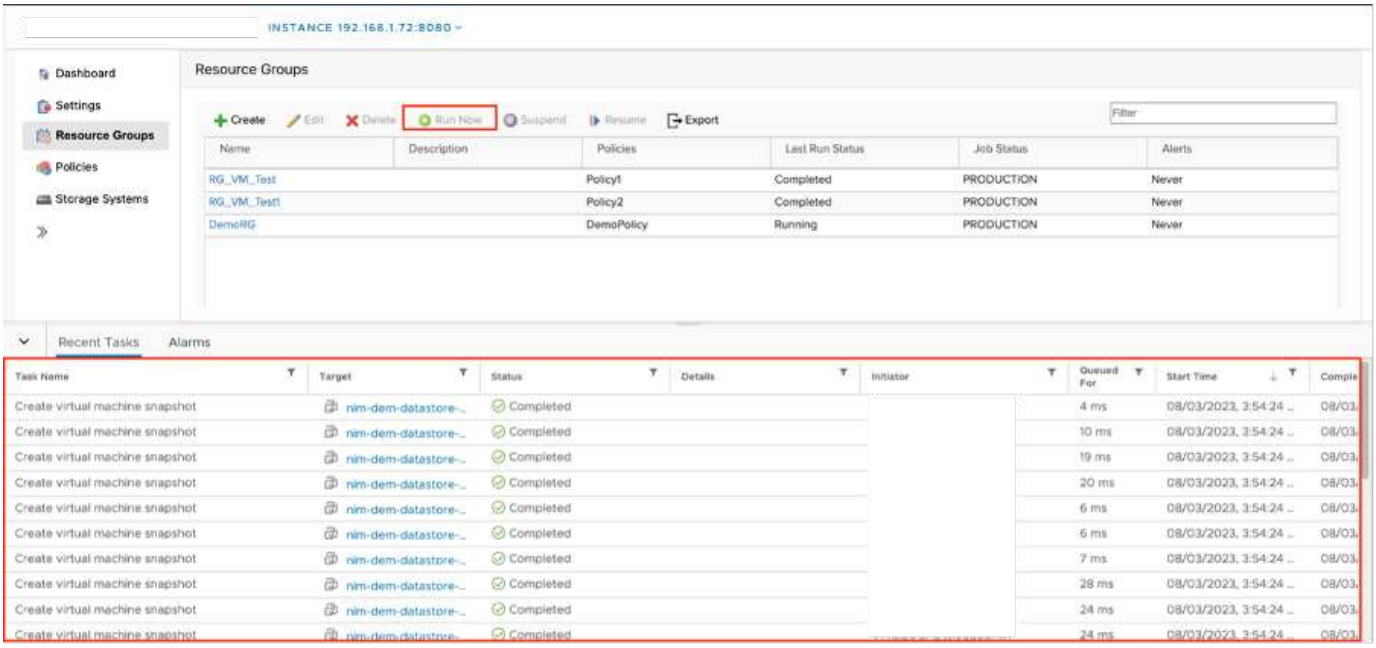
Backup von Ressourcengruppen

Sicherungsvorgänge werden für alle Ressourcen innerhalb einer Ressourcengruppe ausgeführt. Wenn einer Ressourcengruppe eine Richtlinie zugewiesen und ein Zeitplan konfiguriert ist, werden Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

1. Wählen Sie in der linken Navigation der vCenter Webclient-Seite „SnapCenter Plug-in for VMware“ und dann „Resource Groups“ aus.
2. Suchen Sie auf der Seite Ressourcengruppen die gewünschte Ressourcengruppe und wählen Sie „Jetzt ausführen“, um das manuelle Backup zu starten.



3. Wenn für die Ressourcengruppe mehrere Richtlinien konfiguriert sind, wählen Sie die Richtlinie für den Sicherungsvorgang im Dialogfeld „Jetzt sichern“ aus.
4. Wählen Sie „OK“, um die Sicherung zu starten.

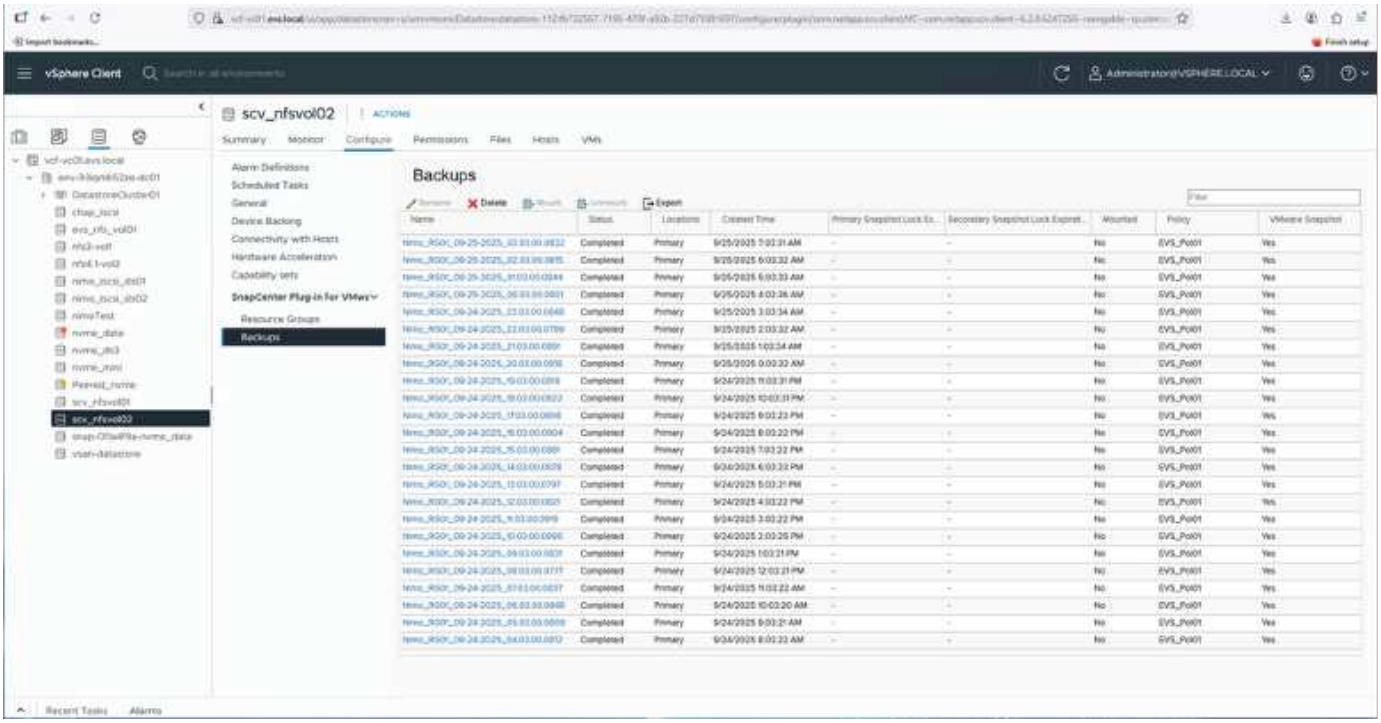


Überwachen Sie den Fortschritt des Vorgangs, indem Sie unten im Fenster „Recent Tasks“ auswählen oder, für weitere Details, im Dashboard „Job Monitor“ auswählen.

Der Prozess zum Erstellen von Sicherungsrichtlinien, Konfigurieren von Ressourcengruppen und Durchführen von Sicherungsvorgängen ist bei verschiedenen Speicherprotokollen, einschließlich NFS und iSCSI, konsistent.

Backups werden gemäß dem in der Richtlinie definierten Zeitplan durchgeführt.

Nach Abschluss der Sicherung kann sie auf Datenspeicherebene oder für einzelne VMs angezeigt werden, indem „SnapCenter Plug-in for VMware vSphere“ in der Dropdown-Liste ausgewählt und anschließend „Wiederherstellen“ gewählt wird.



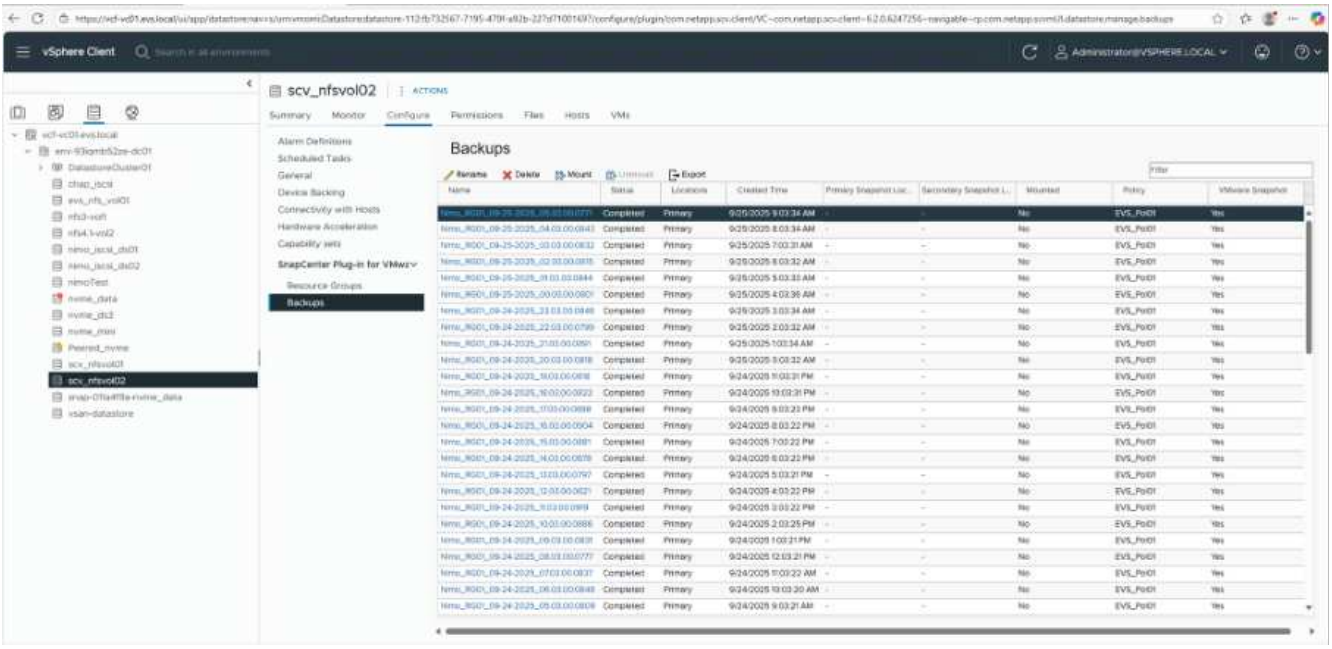
Wiederherstellungsverfahren für VMs, die durch das SnapCenter Plug-in für VMware geschützt sind

Dieser Abschnitt beschreibt die Schritte zur Wiederherstellung von VMs aus Backups. SCV kann verwendet werden, um VMs innerhalb von vCenter wiederherzustellen. Dadurch können sie auf dem ursprünglichen Datenspeicher des ursprünglichen ESXi-Hosts (wobei vorhandene Inhalte überschrieben werden), gelöschte oder umbenannte VMs aus einer Backup-Kopie, auf einem anderen Datenspeicher des ursprünglichen ESXi-Hosts, auf dem ursprünglichen Datenspeicher eines anderen vom selben vCenter verwalteten ESXi-Hosts oder auf einem anderen Datenspeicher eines anderen ESXi-Hosts innerhalb derselben vCenter-Umgebung wiederhergestellt werden.

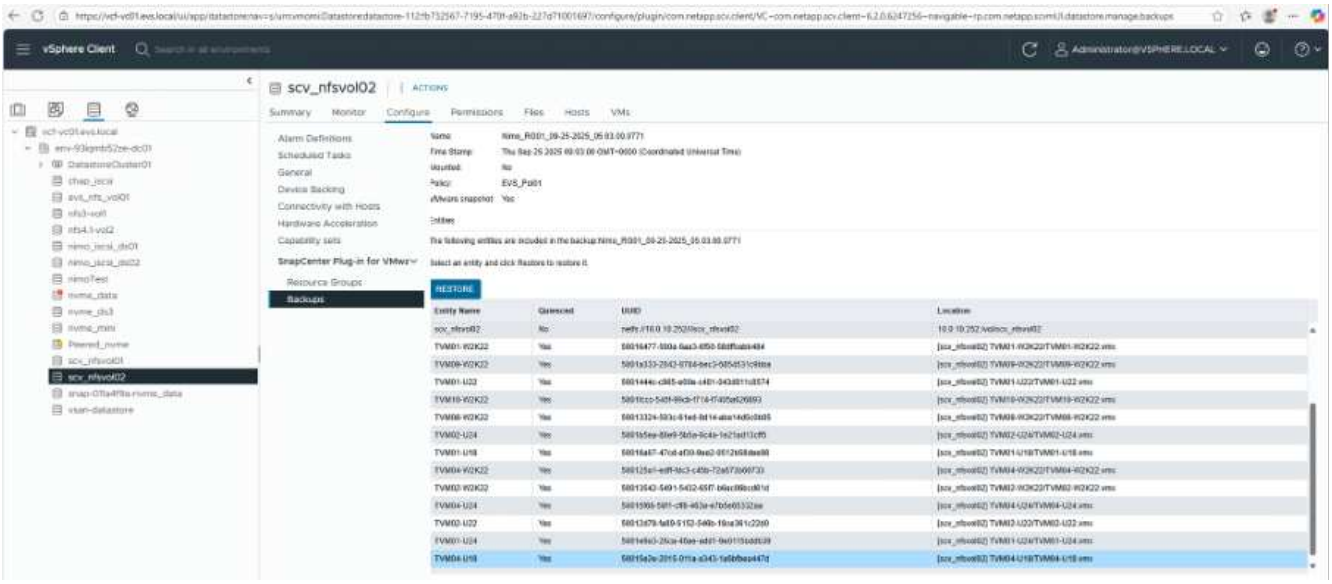
Schritte zur Durchführung der Restore-Operation

Um die Restore-Operation durchzuführen, befolgen Sie diese Schritte:

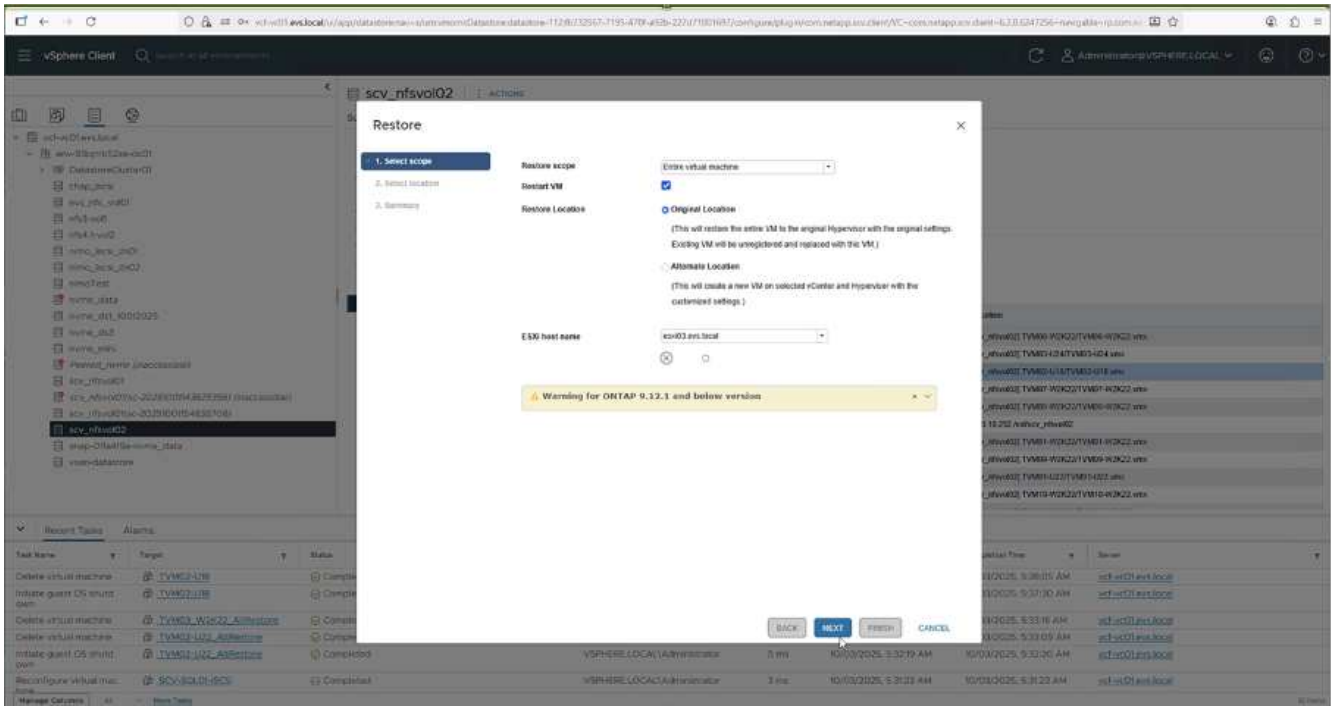
1. In der EVS vSphere Web-Client-GUI gehen Sie zu „Inventory > Datastores“ und wählen Sie den gewünschten Datastore aus. Navigieren Sie dann im Abschnitt „SnapCenter Plug-in for VMware vSphere“ zu „Configure > Backups“.



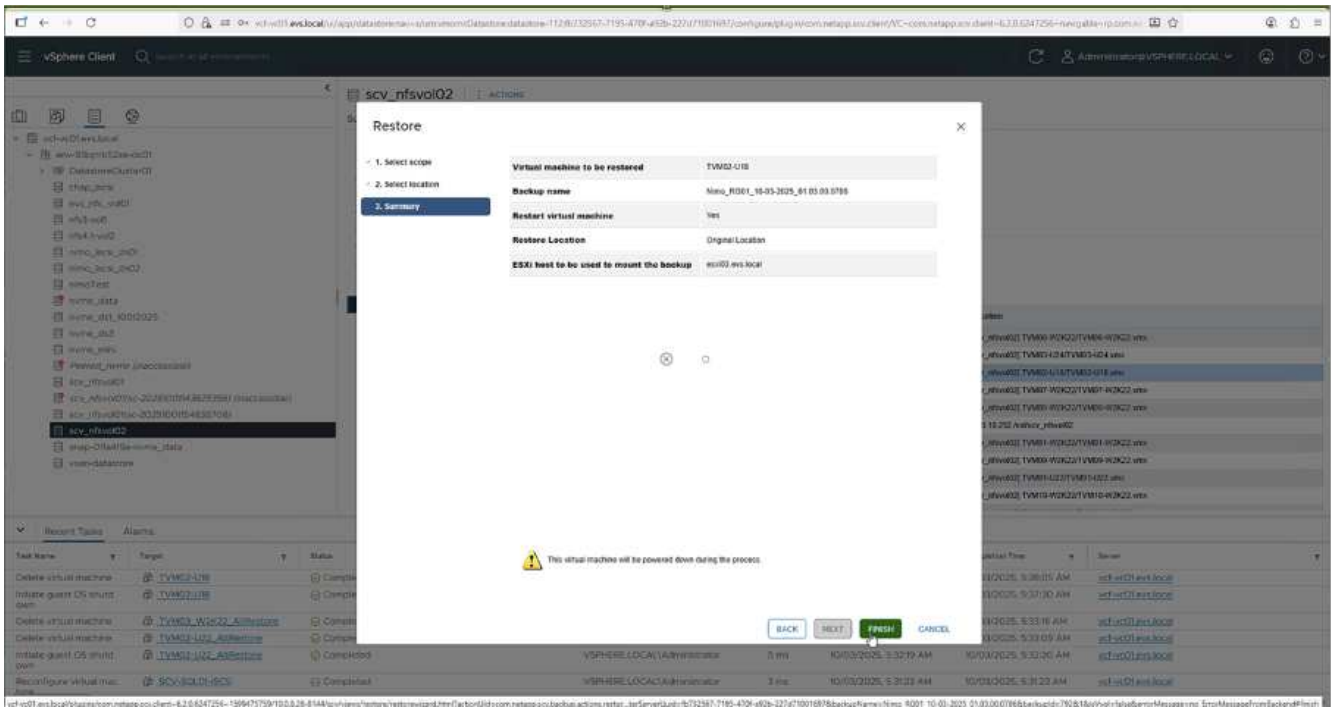
2. Doppelklicken Sie auf eine Sicherung, um alle in dieser Sicherung enthaltenen VMs anzuzeigen. Suchen Sie die wiederherzustellende VM in der Liste und wählen Sie "Wiederherstellen".



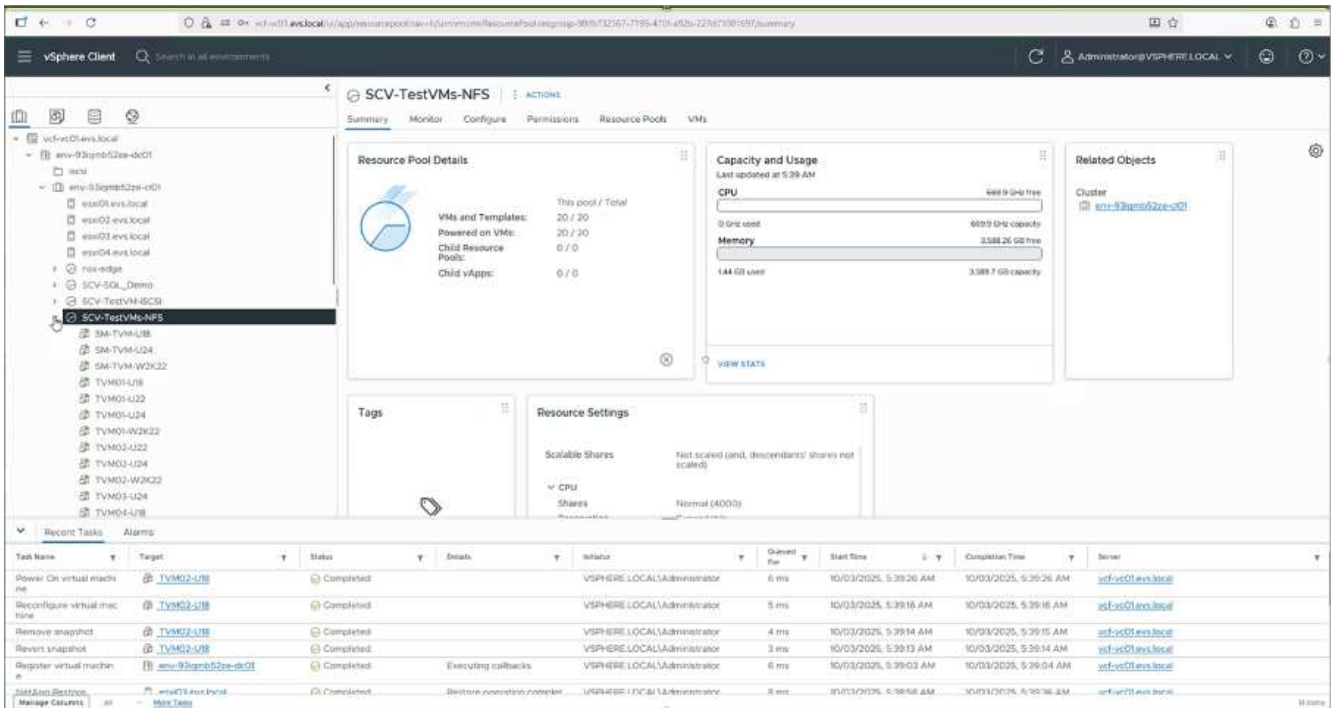
3. Wählen Sie auf der Seite „Bereich auswählen“ im Feld „Wiederherstellungsbereich“ die Option „Gesamte virtuelle Maschine“ aus, wählen Sie dann „Wiederherstellungsort“ aus und geben Sie die Ziel-ESXi-Informationen ein, unter denen das Backup eingebunden werden soll.
4. Aktivieren Sie das Kontrollkästchen „Restart VM“, wenn die VM nach dem Restore-Vorgang eingeschaltet werden muss.
5. Wählen Sie auf der "Select Location page" einen primären Standort aus.



6. Überprüfen Sie die Seite „Summary“ und wählen Sie dann „Finish“.



7. Überwachen Sie den Fortschritt des Vorgangs, indem Sie unten auf dem Bildschirm „Recent Tasks“ auswählen.



Obwohl die VMs wiederhergestellt wurden, werden sie nicht automatisch ihren vorherigen Ressourcengruppen hinzugefügt. Wenn Sie diese VMs schützen möchten, fügen Sie sie manuell den entsprechenden Ressourcengruppen hinzu.

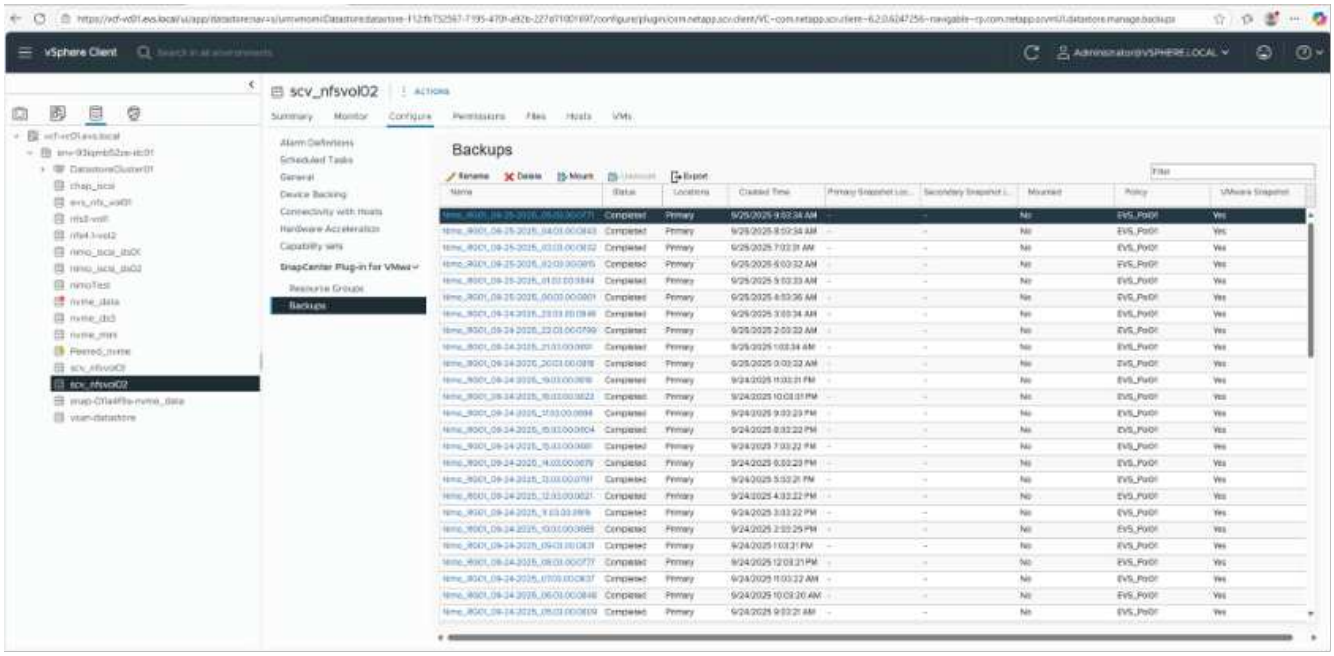
Der Restore-Vorgang kann auch auf Ebene einzelner VMs ausgelöst werden.

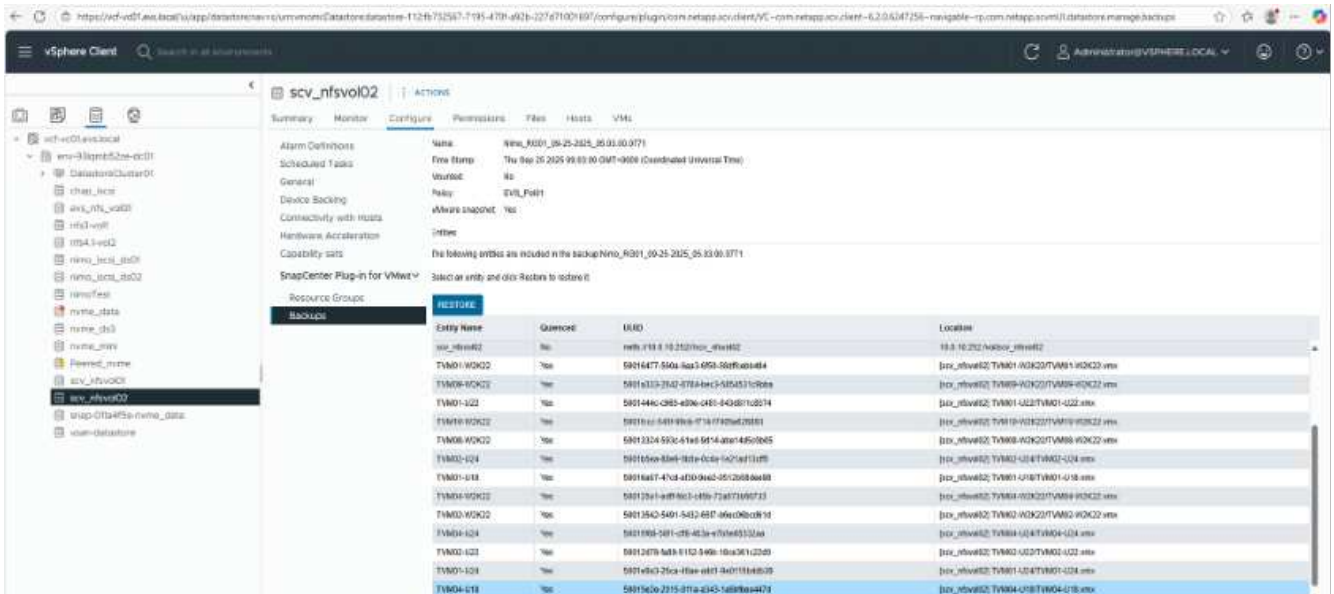
Schritte zur Wiederherstellung einer gelöschten VM

Das Wiederherstellen einer gelöschten VM ist mit SCV ein einfacher Prozess.

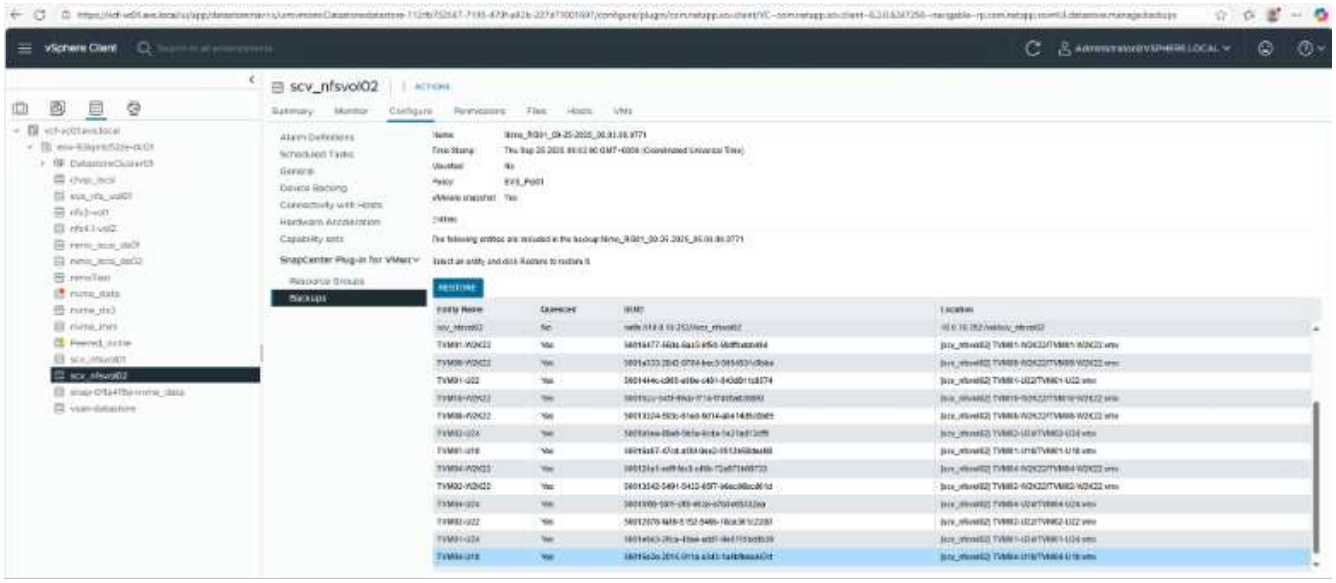
Die Wiederherstellung einer gelöschten VM kann auf Datenspeicherebene durchgeführt werden.

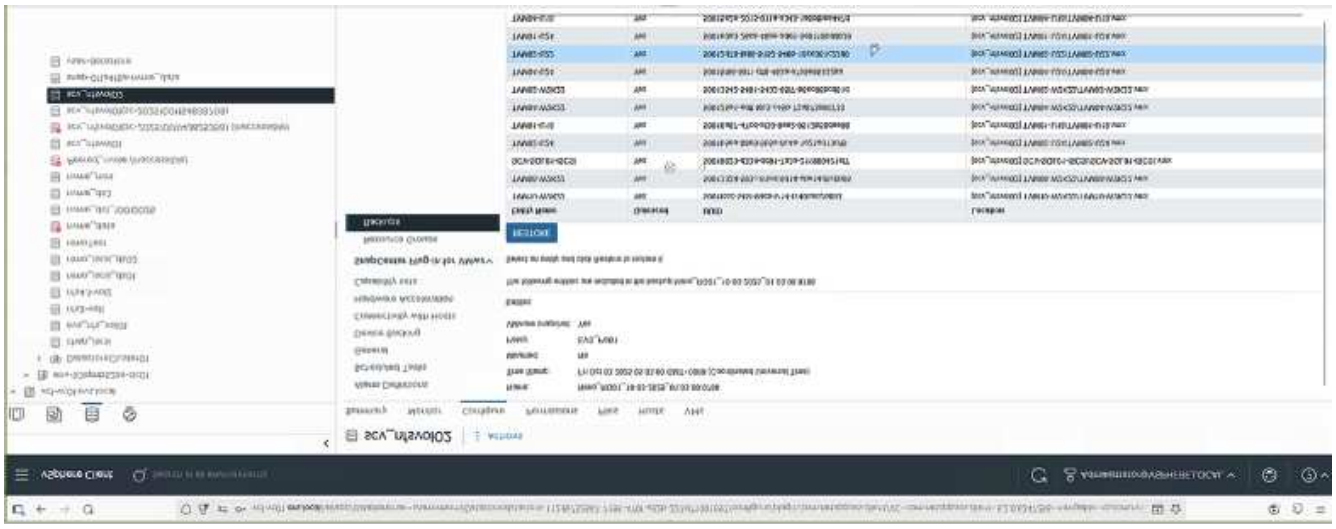
1. Gehen Sie zum jeweiligen Datastore > Configure > Backups. Wählen Sie dort die gelöschte VM aus und wählen Sie „Restore“.

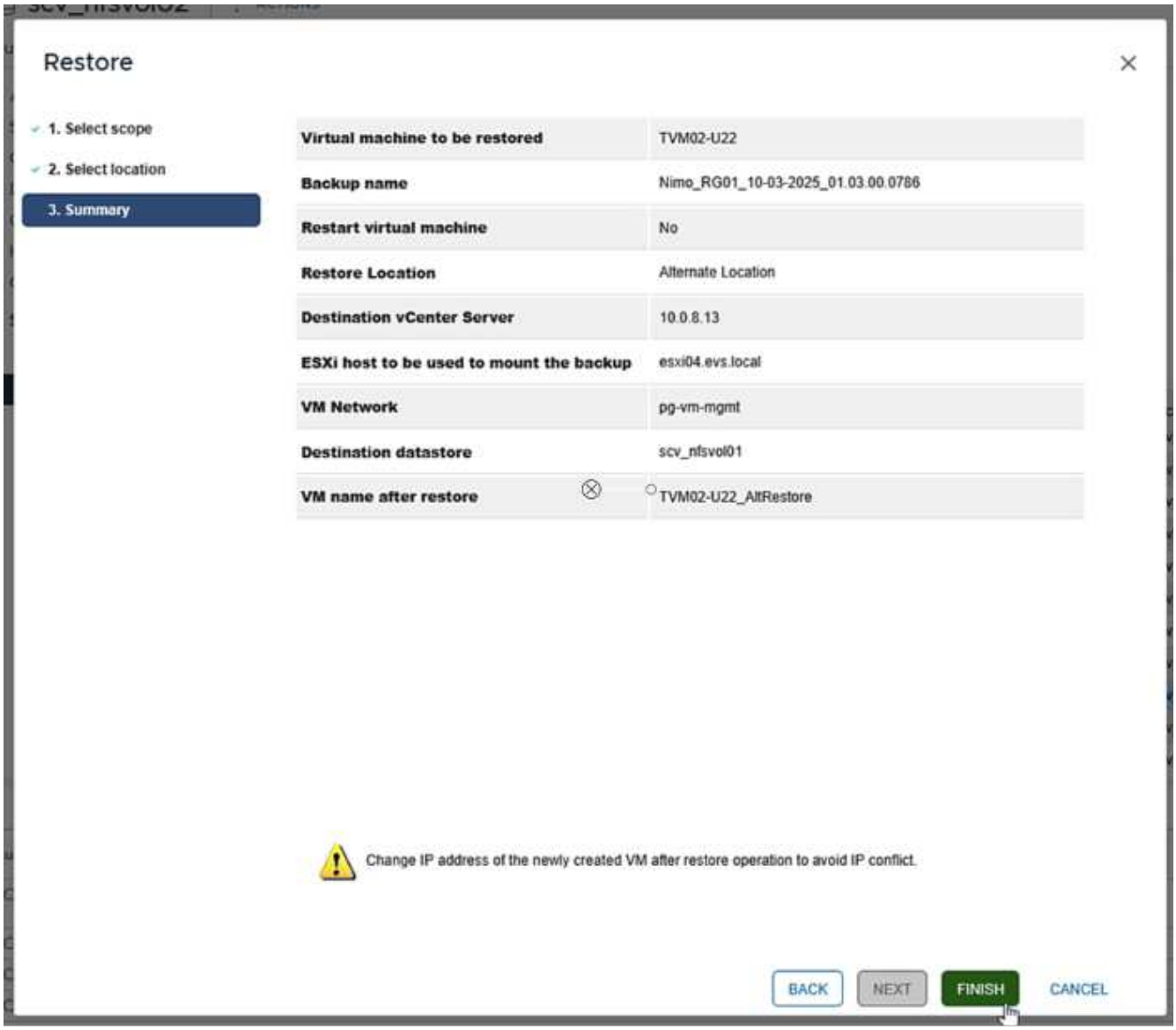


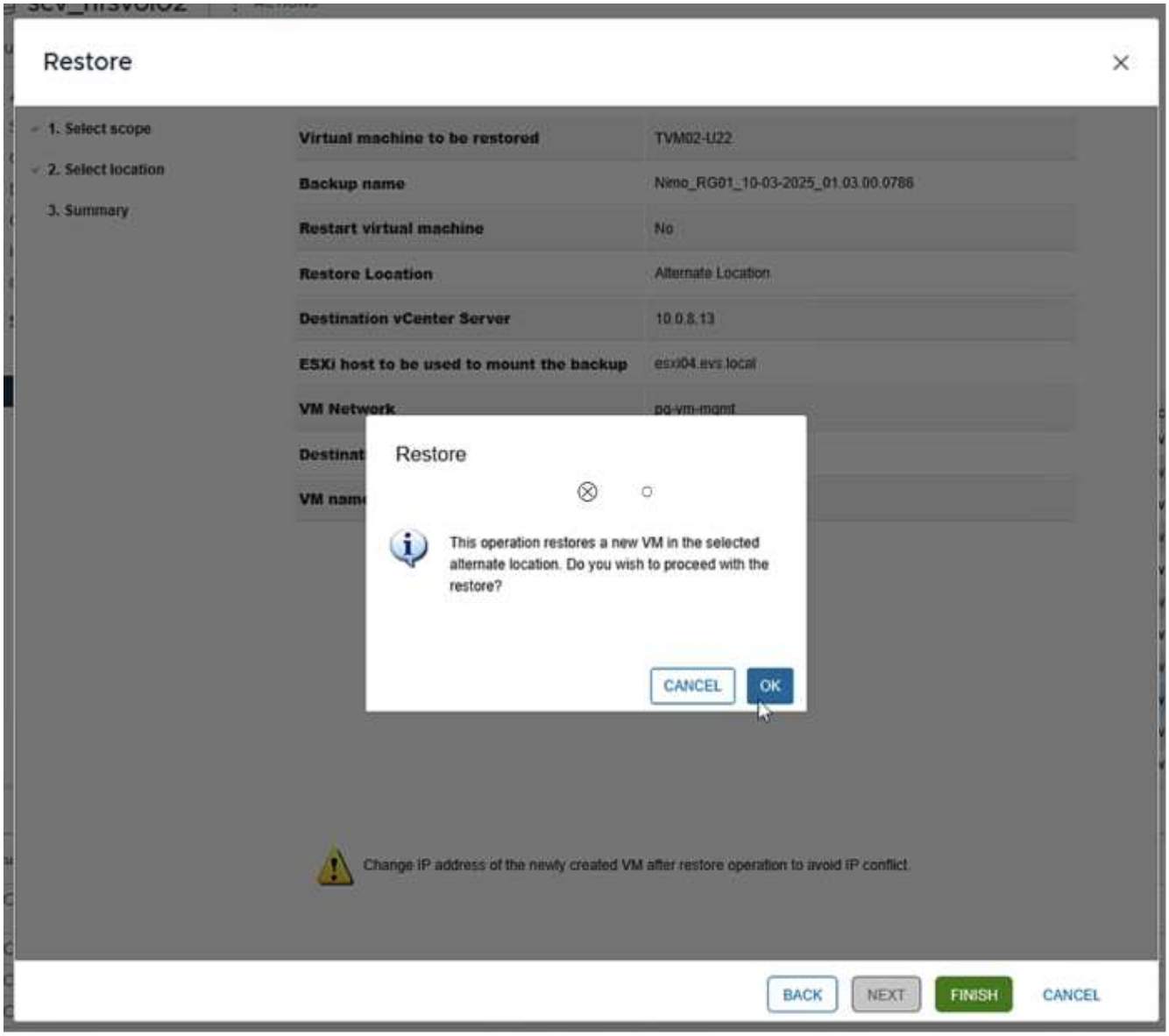


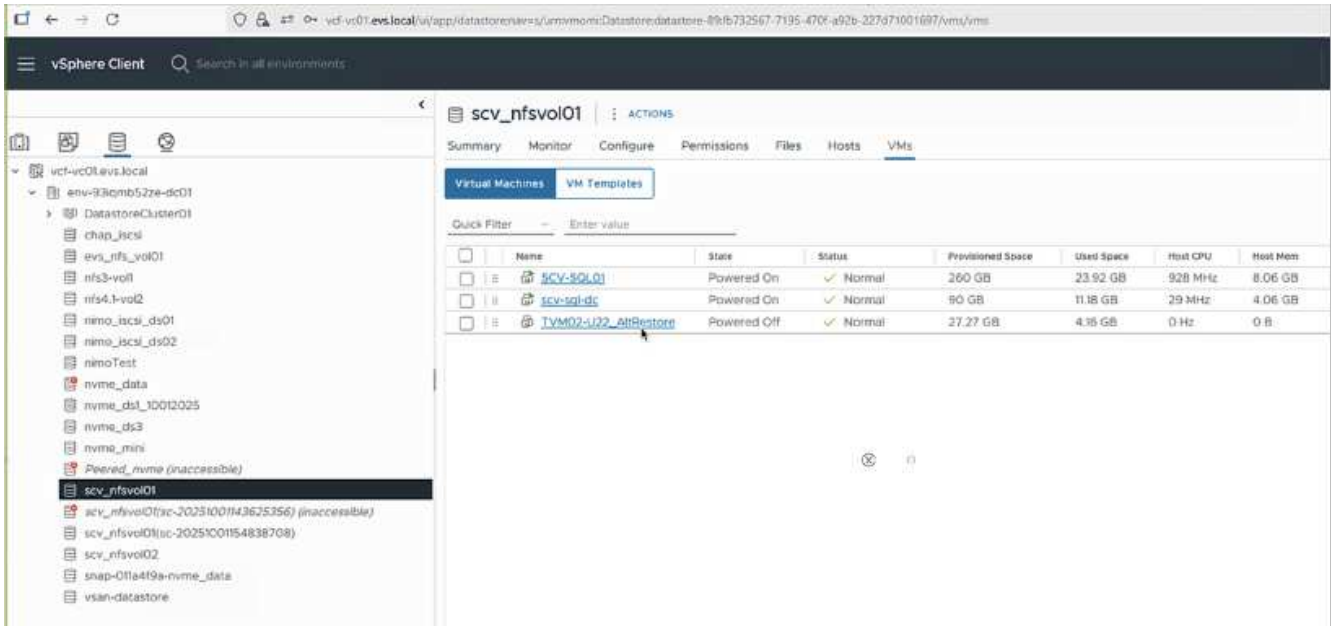
2. Der nachfolgende Screenshot-Ablauf beschreibt die Wiederherstellung einer VM auf einen alternativen ESXi-Host und einen anderen Datenspeicher.


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE




Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

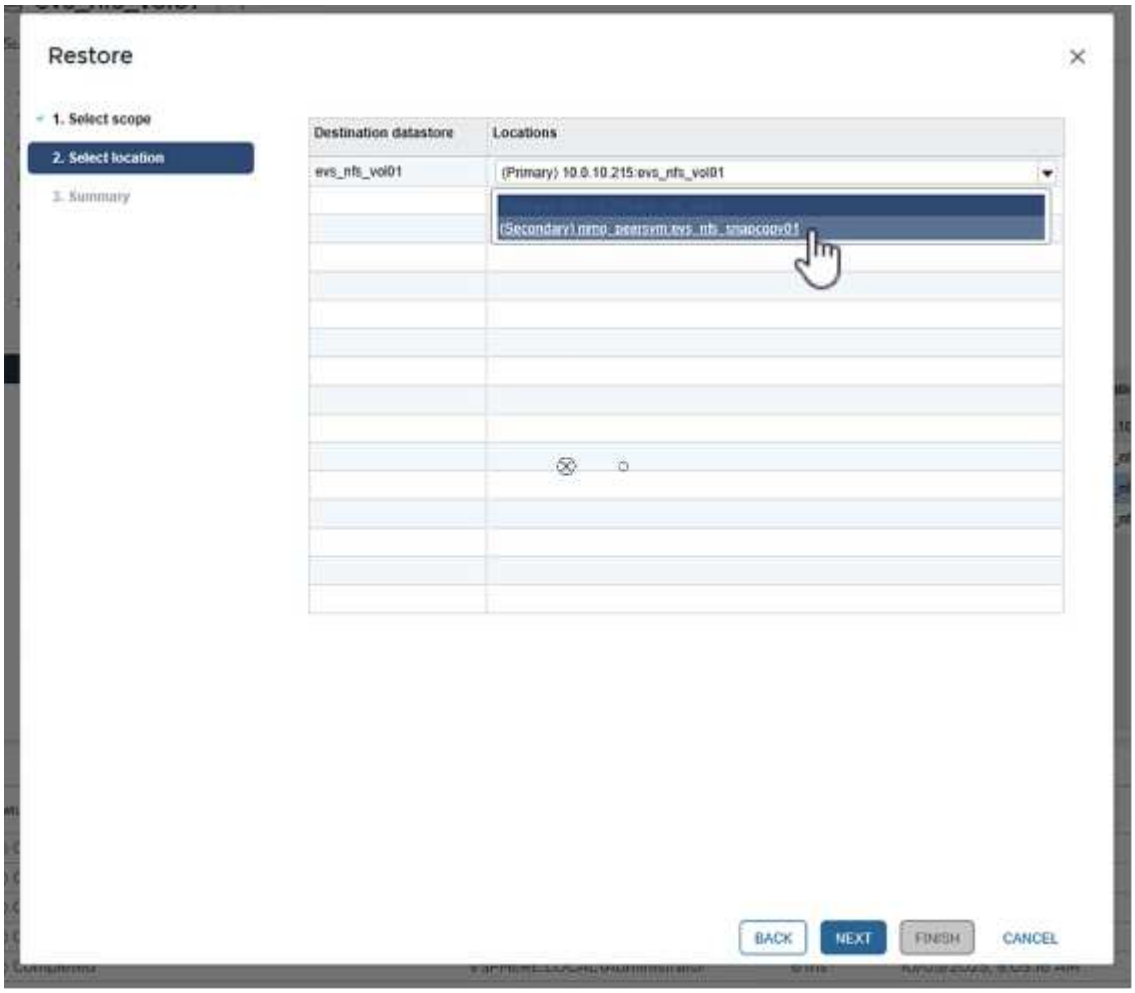

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

Der Zieldatenspeicher muss über ausreichend freien Speicherplatz verfügen und der im Feld „Wiederherstellung an alternativem Speicherort“ angegebene vCenter muss per DNS auflösbar sein.

Um die Wiederherstellungseffizienz in NFS-Umgebungen zu verbessern, aktivieren Sie die VMware vStorage API for Array Integration (VAAI).

Wiederherstellungen können auch von sekundären Standorten aus durchgeführt werden, wie zum Beispiel von einem SnapMirror Ziel.



+

Wiederherstellungsverfahren für Gastdateien und -ordner, die durch das SnapCenter Plug-in für VMware geschützt sind

Im folgenden Abschnitt wird gezeigt, wie Gastdateien und -ordner aus VMDKs wiederhergestellt werden.

SnapCenter unterstützt die Wiederherstellung von Dateien und Ordnern aus VMDKs nur, wenn das Gastbetriebssystem Windows ist.

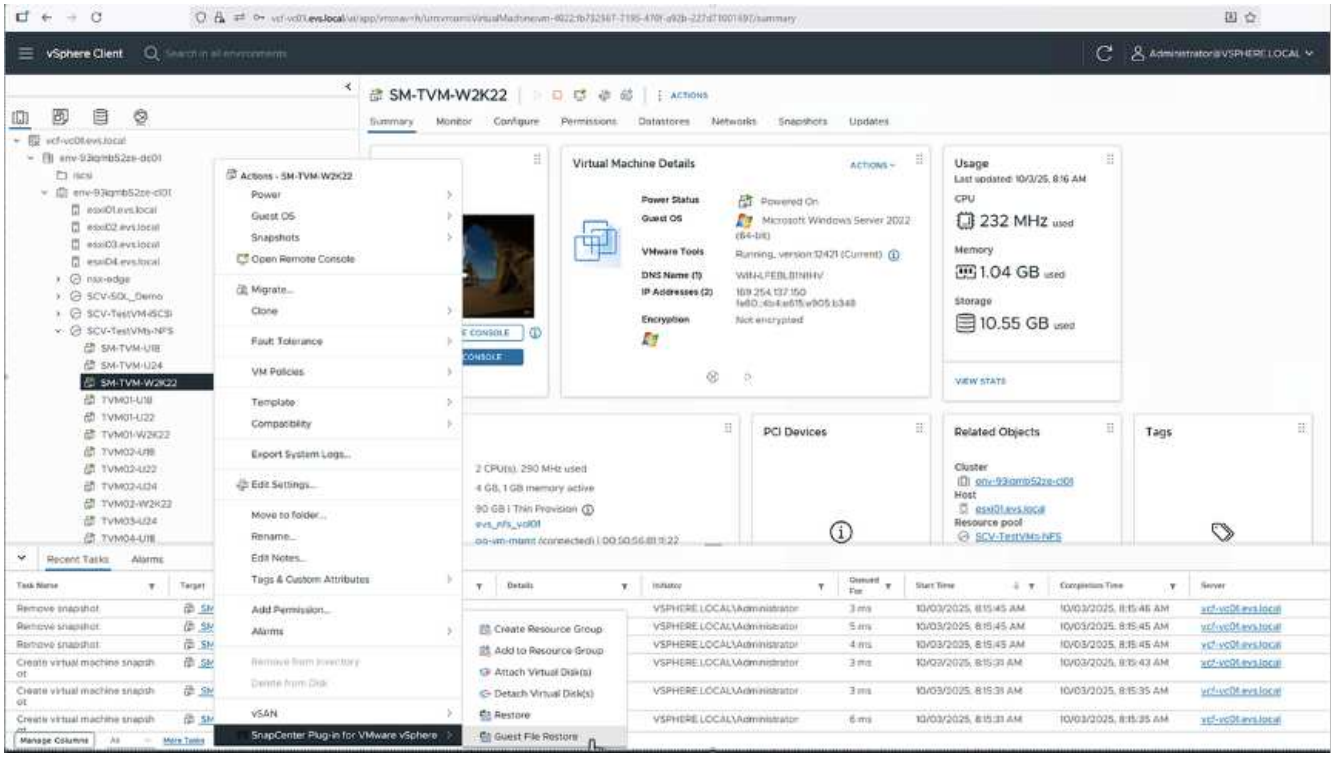
Überlegungen zur Wiederherstellung von Gastdateien und -ordnern mit SCV:

- VMware Tools müssen auf der VM ausgeführt werden.

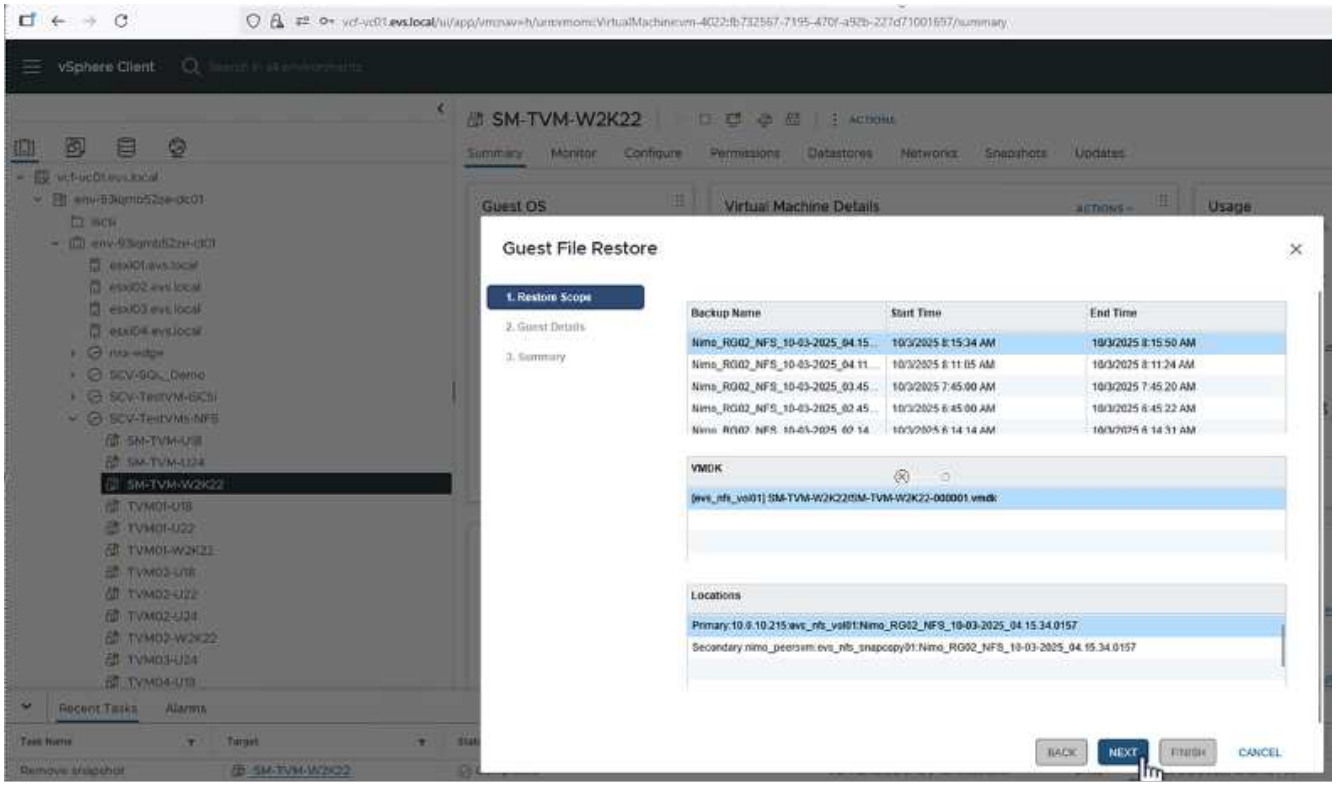
- Die beigefügte VMDK ist standardmäßig 24 Stunden lang zugänglich.
- Es kann jeweils nur ein Restore- oder Attach-Vorgang an einer virtuellen Maschine durchgeführt werden.
- Systemdateien, versteckte Dateien und verschlüsselte Dateien können wiederhergestellt werden; jedoch werden ihre ursprünglichen Eigenschaften nicht beibehalten.
- Vermeiden Sie, verschlüsselte Dateien in verschlüsselte Ordner wiederherzustellen oder Systemdateien zu überschreiben.

Schritte für die Wiederherstellung von Gastdateien und -ordnern:

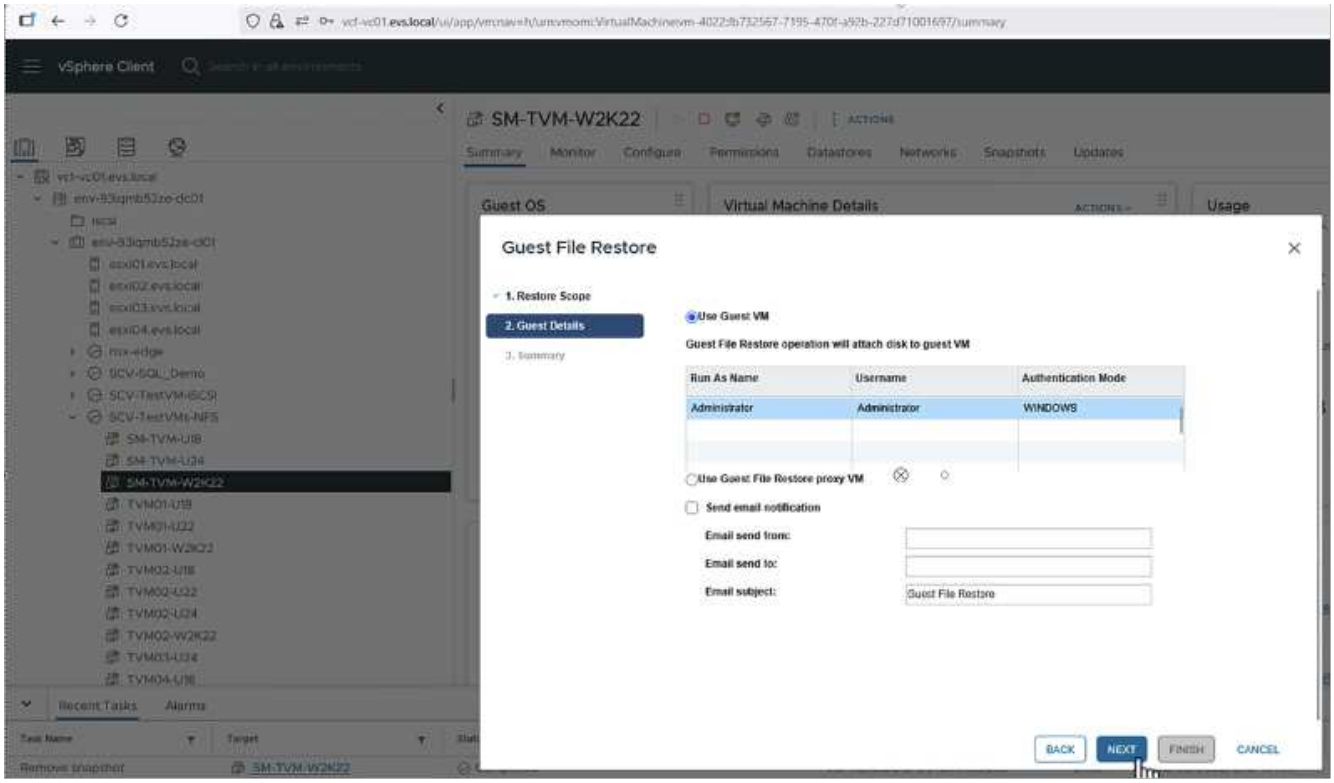
1. Klicken Sie mit der rechten Maustaste auf die Ziel-VM und wählen Sie „NetApp SnapCenter > Guest File Restore“.



2. Wählen Sie die Sicherung aus, die die benötigte VMDK enthält. Geben Sie die VMDK und ihren Speicherort (primär oder sekundär) an.

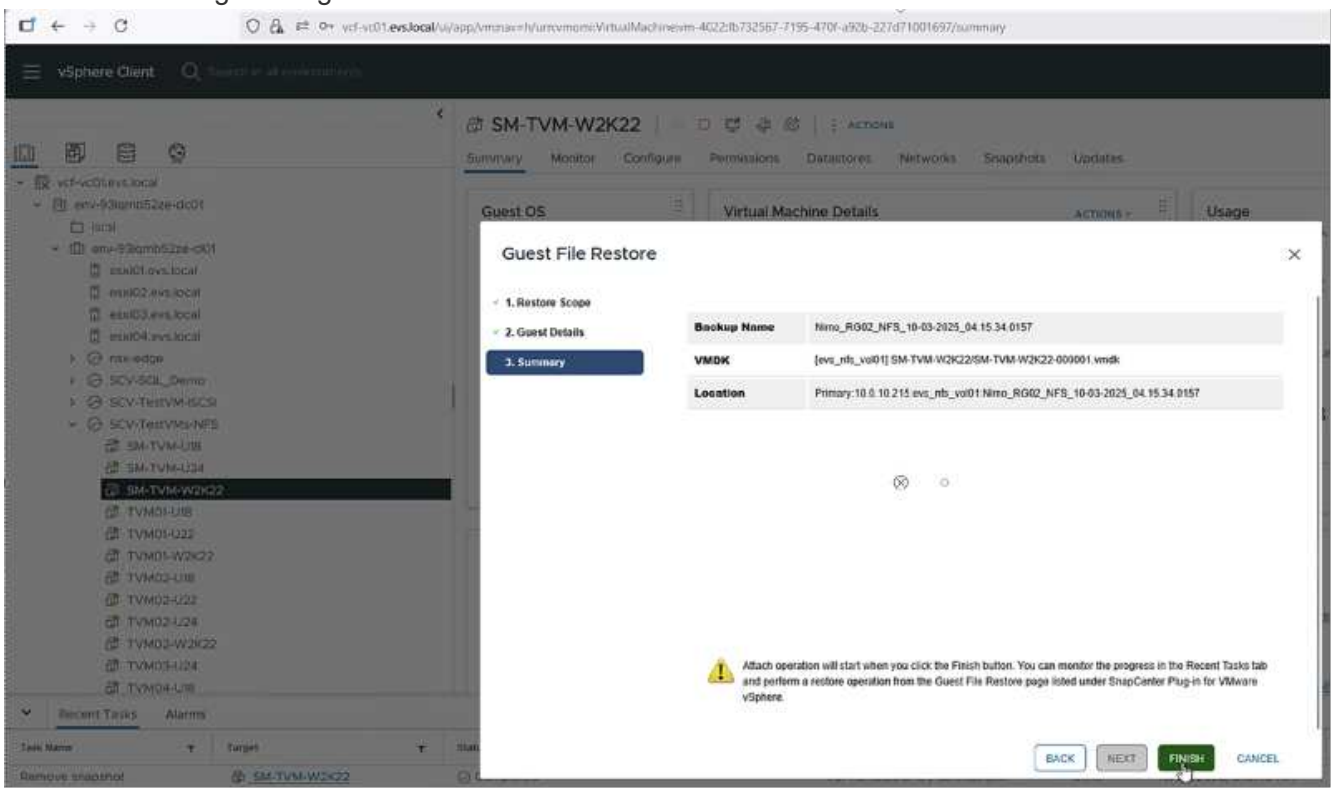


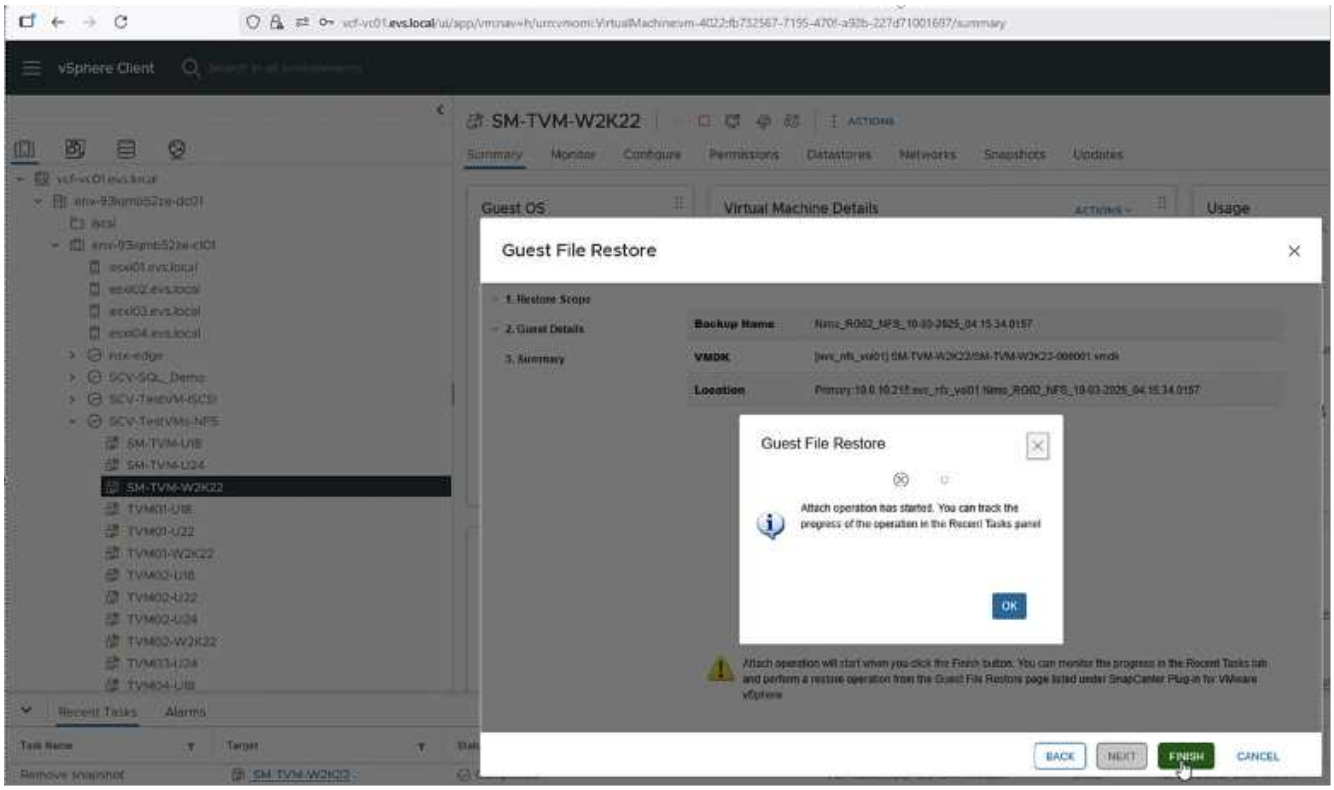
3. Wählen Sie „Disk Attachment Method“.



- Gast-VM-Option: Die Festplatte an die ursprüngliche VM anhängen (erfordert vorkonfigurierte Anmeldeinformationen). Diese Option wird in dieser Demonstration verwendet.
- Proxy VM Option: Die Festplatte wird an eine bestimmte Proxy-VM angehängt (muss im Voraus konfiguriert werden).

4. Warten Sie, bis der Einfügevorgang abgeschlossen ist, bevor Sie Dateien durchsuchen und wiederherstellen. Nach Abschluss des Vorgangs erstellt SnapCenter automatisch eine Gastdatei-Wiederherstellungssitzung.





5. Navigieren Sie in der Guest File Restore-Sitzung zur VMDK, wählen Sie die erforderlichen Dateien oder Ordner aus und stellen Sie sie am angegebenen Speicherort wieder her.

Schutzverfahren für Datenbanken, die auf VMware VMDKs mit SnapCenter for SQL (SCSQL) ausgeführt werden

Im folgenden Abschnitt wird gezeigt, wie Sie Datenbanken, die auf VMware VMDKs laufen, mit SnapCenter für SQL (SCSQL) schützen.

SCSQL einrichten

Die Einrichtung für die Verwendung von SCSQL zum Schutz von Datenbanken auf VMDKs ist wie folgt:

1. "Installieren und konfigurieren" SnapCenter Server.
2. Melden Sie sich bei SnapCenter an.
3. Konfigurieren Sie die SnapCenter Umgebung:
   - "Hinzufügen oder zuweisen" Anschlüsse des Speichersystems.
   - "Erstellen"Zugangsdaten.
4. Für Microsoft SQL Server-Datenbanken auf VMware VMDKs:
   - "SCV bereitstellen" (bereits im Abschnitt „Einrichtung“ behandelt).
   - Registrieren Sie das Plug-in bei SnapCenter.
5. Fügen Sie "SQL Server Hosts und Plug-ins installieren" hinzu:
   - "Konfigurieren Sie die SQL-Plug-ins".
   - "Konfigurieren Sie den Schutzplan und die Zeitpläne für Datenbank und Protokolle".

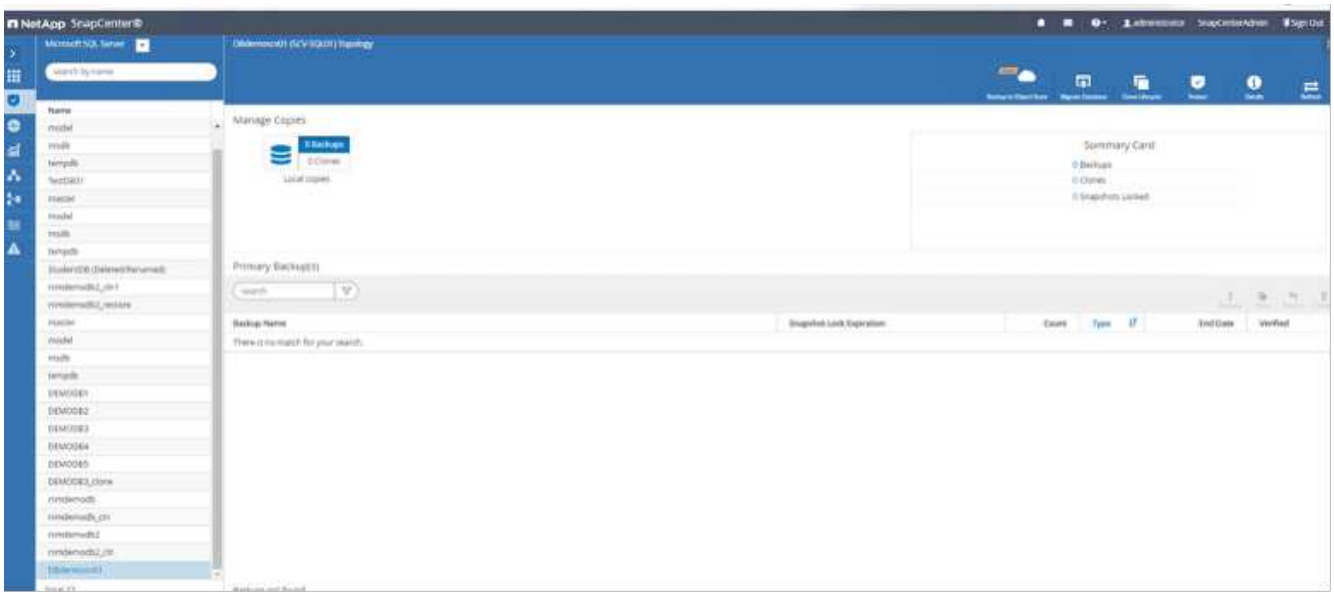


Einrichten einer Backup-Richtlinie

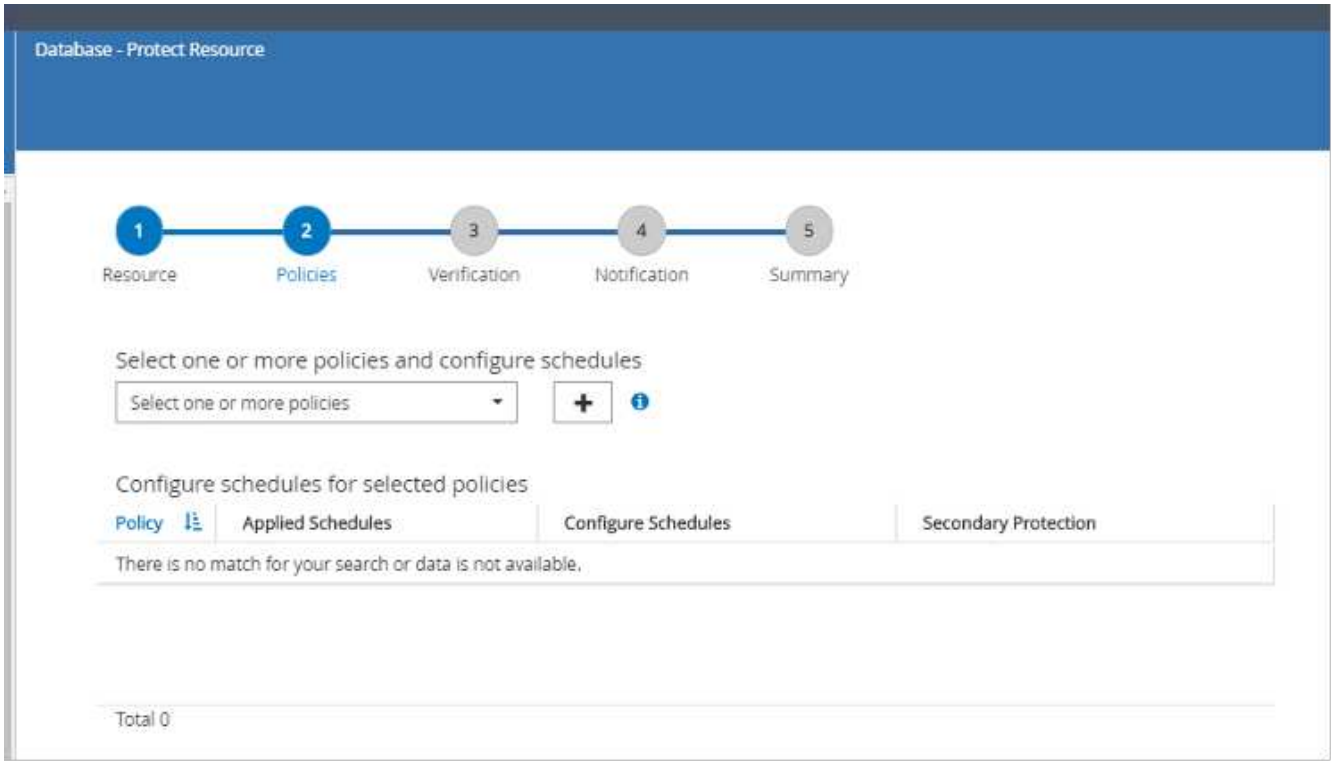
Die folgenden Schritte zeigen, wie Sie eine Backup-Richtlinie einrichten.

1. Wählen Sie die Datenbank auf der Registerkarte „Ressourcen“ aus und wählen Sie „Schützen“ in der oberen rechten Ecke.

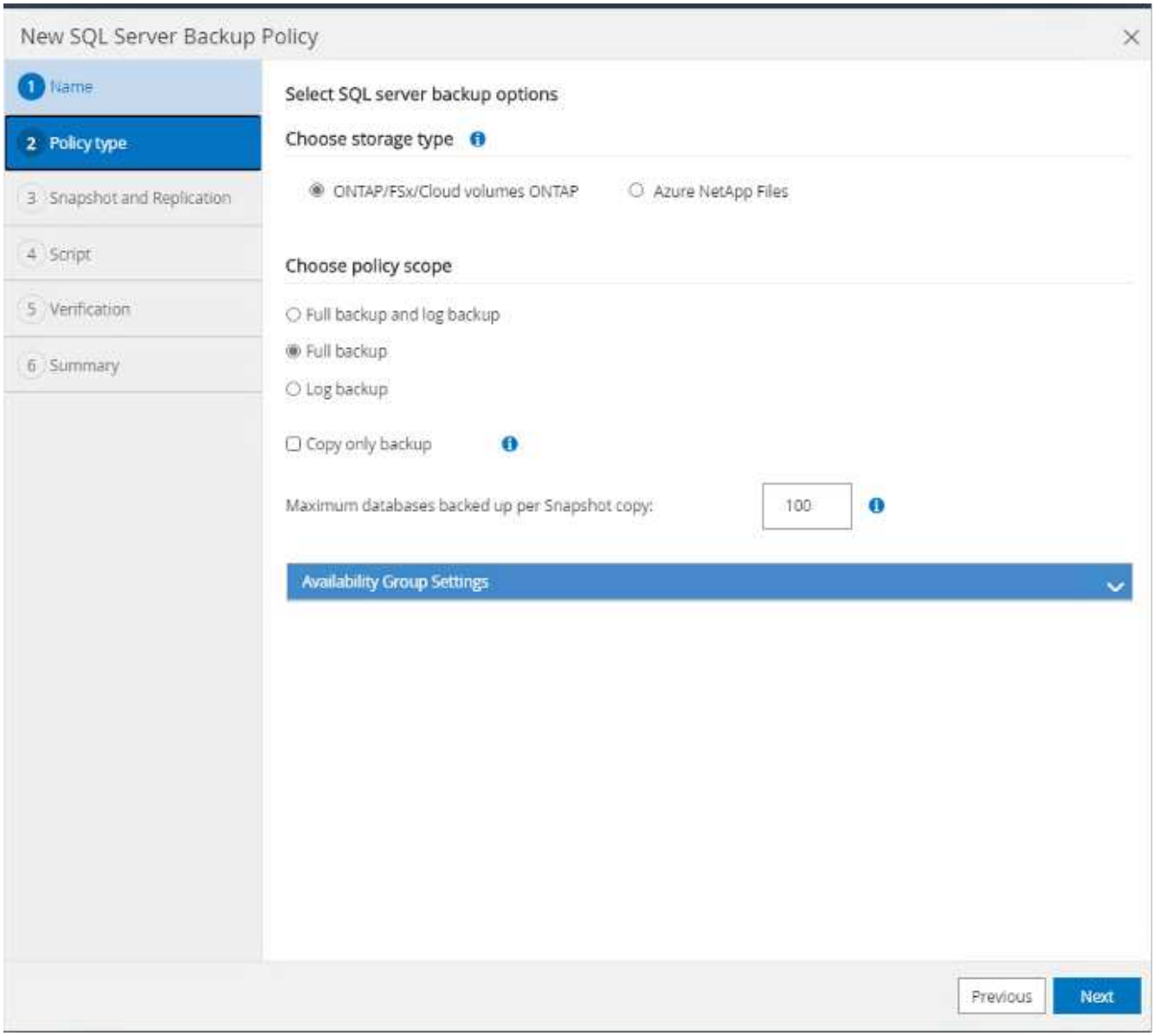
   Validierungen werden an einer SQL Server Datenbank durchgeführt, die auf der Gast-VM läuft.



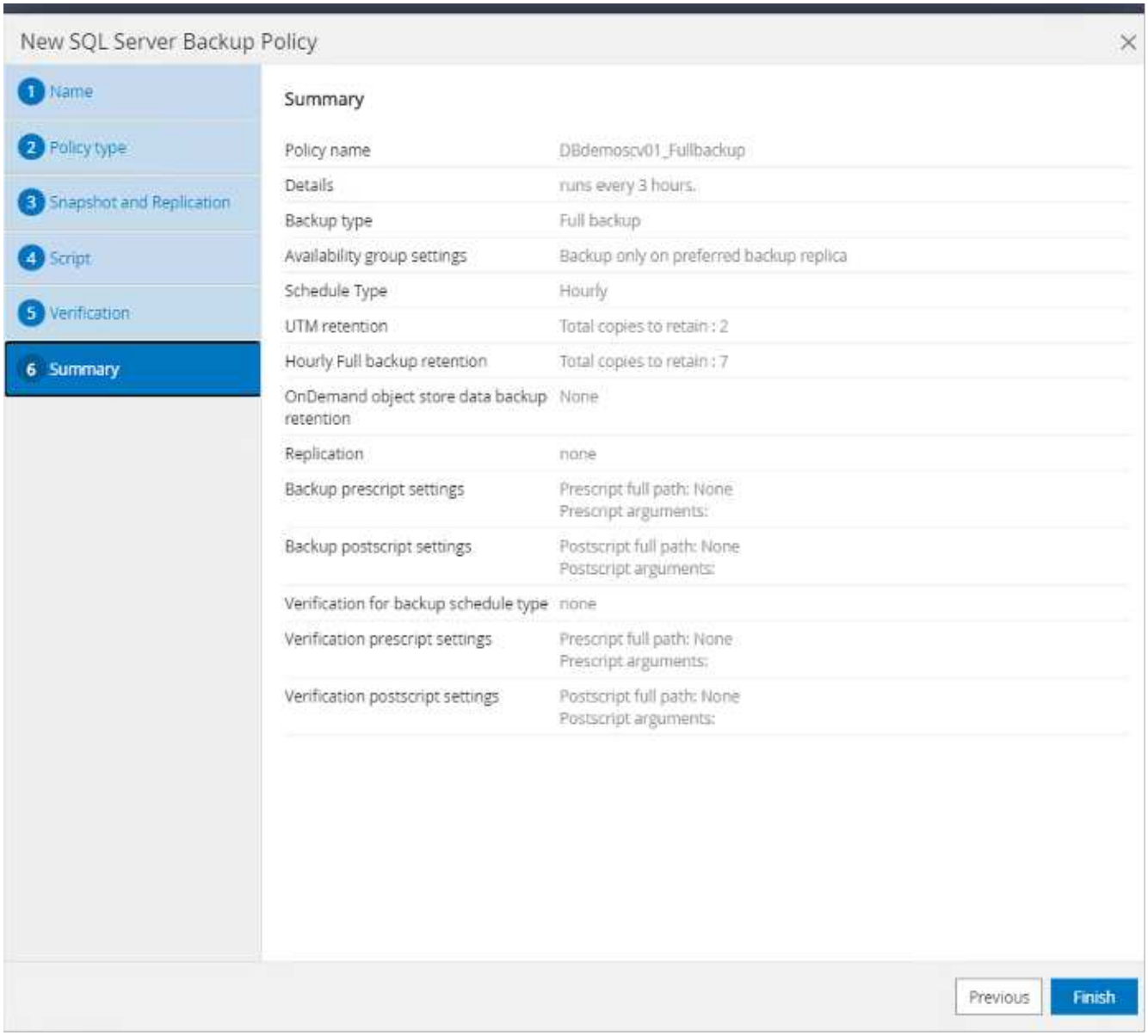
2. Klicken Sie auf das Pluszeichen-Symbol, um eine SQL Server-Backup-Richtlinie zu konfigurieren.



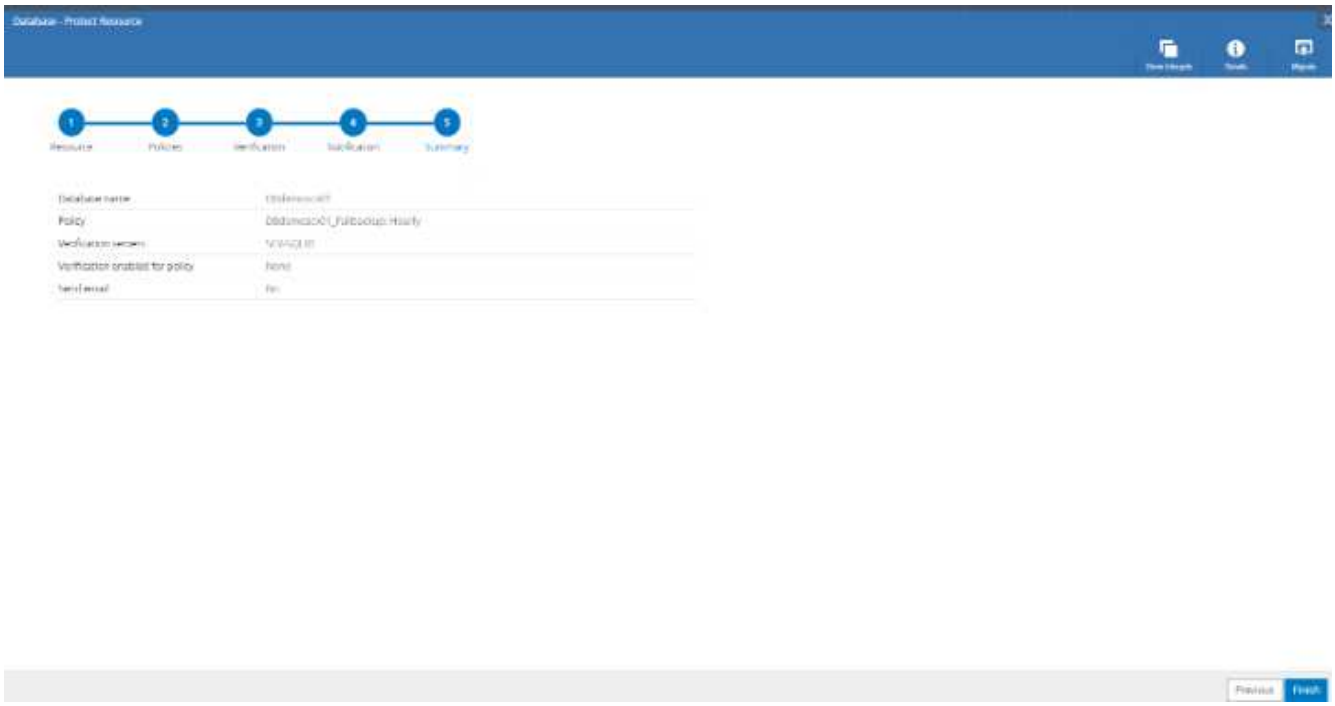
3. In dieser Demo ist „Full backup“ ausgewählt. Wählen Sie „Next“, um fortzufahren.



4. Wählen Sie auf der Zusammenfassungsseite „Fertigstellen“.



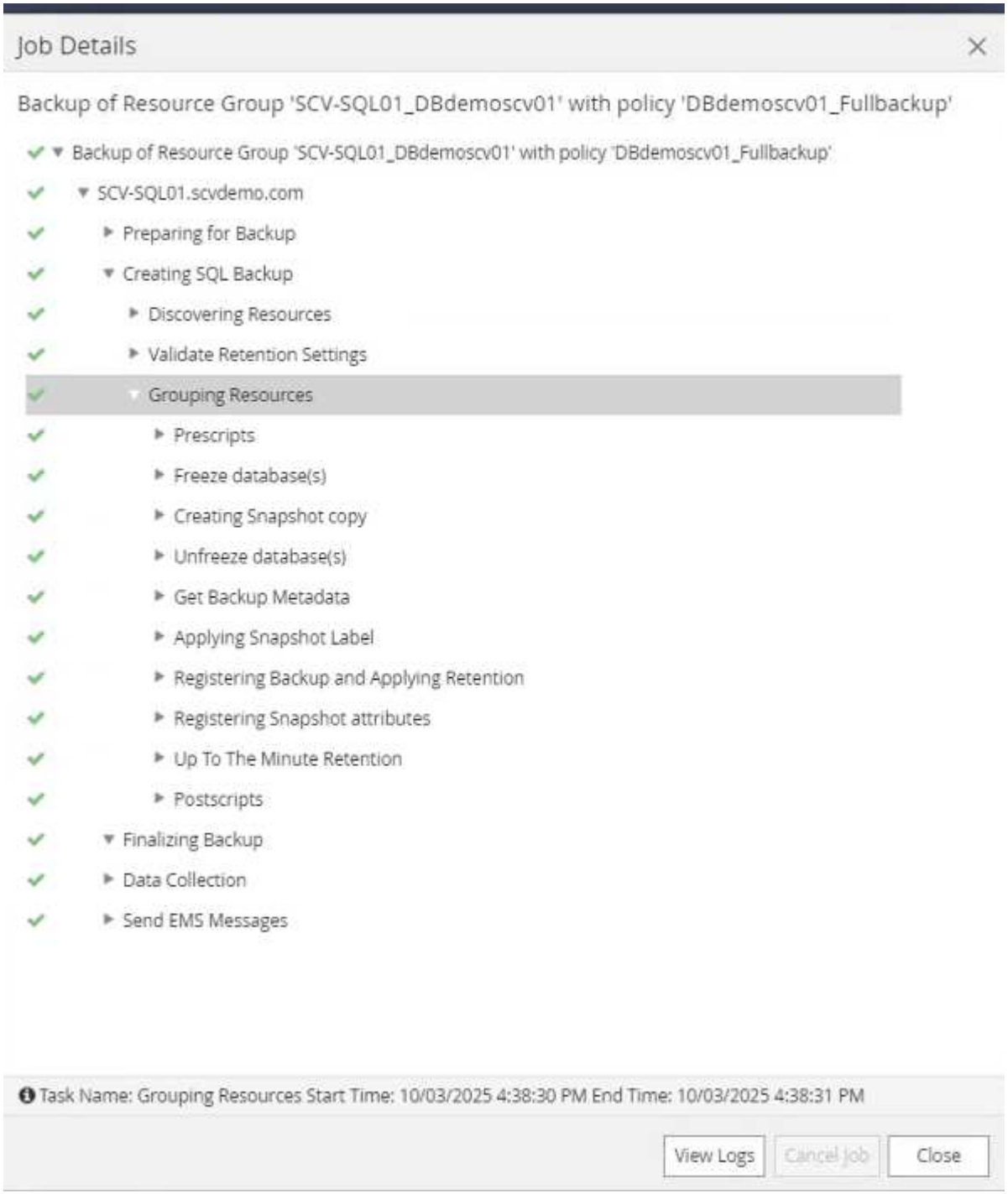
5. Fahren Sie mit "Finish" fort.



Überwachung eines Backups

Sobald Sie eine Backup-Richtlinie eingerichtet haben, können Sie Ihre Backup-Vorgänge überwachen, während sie stattfinden. Sie können dies entweder tun, indem Sie auf Backup now klicken, um eine On-Demand-Backup-Operation auszulösen, oder indem Sie warten, bis Ihre geplante Backup-Richtlinie aktiviert wird.

1. Überwachen Sie den Fortschritt des Jobs mit „Monitor > Jobs“.
2. Wählen Sie den Sicherungsauftrag aus und klicken Sie dann auf „Details“, um die Auftragsdetails wie unten anzuzeigen.

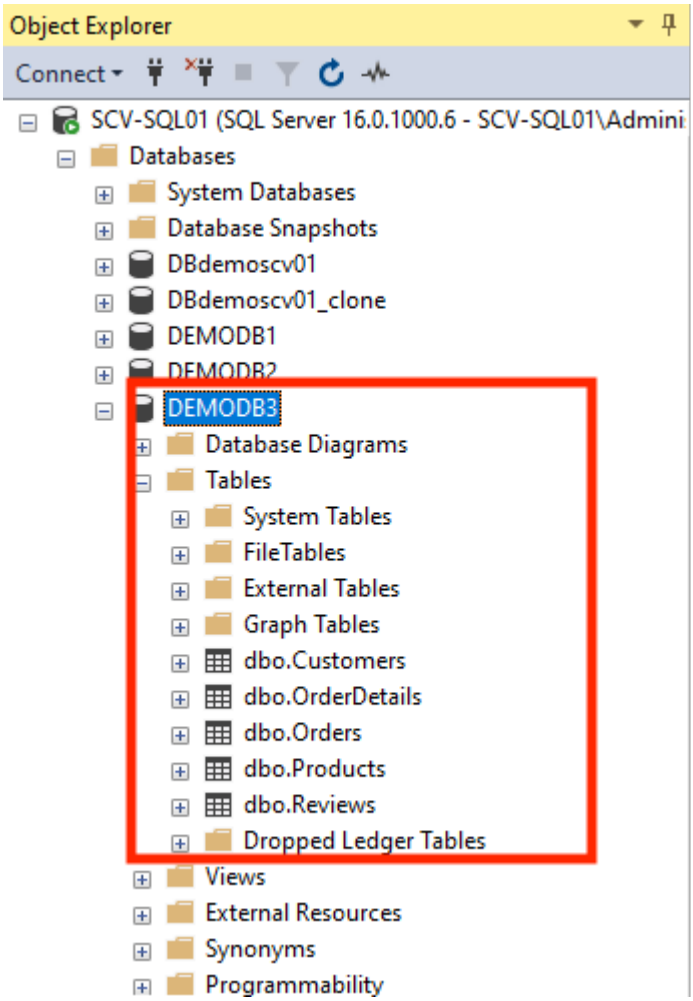


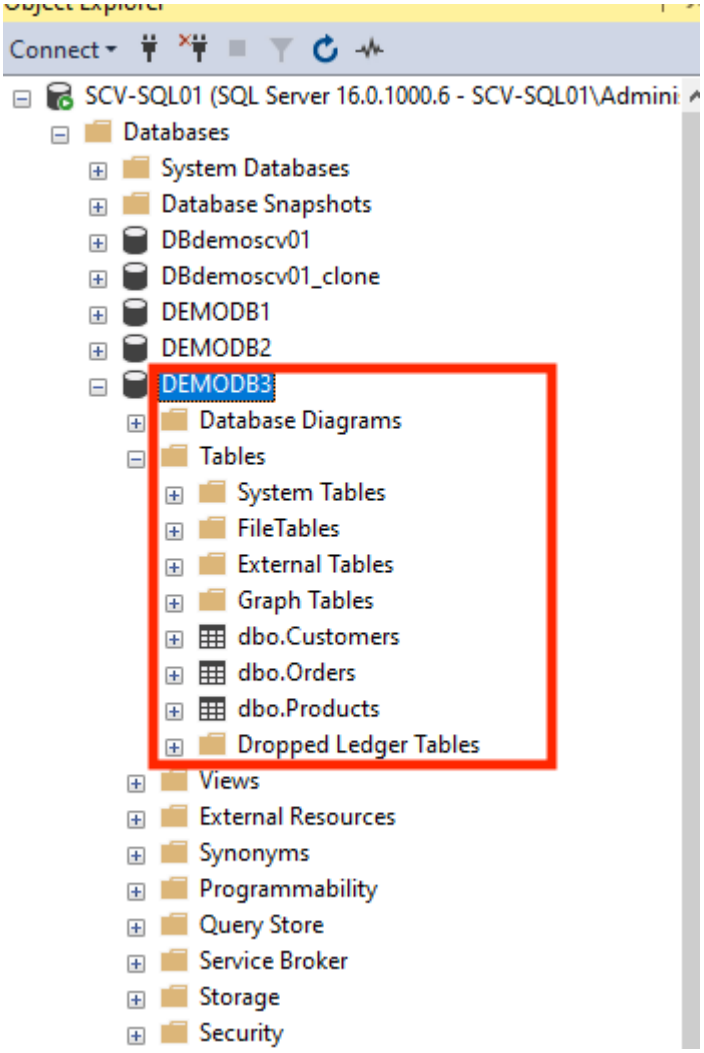
Wiederherstellung von Datenbanken, die sich auf den VMDKs befinden

Die Datenbank auf der VMDK kann zu einem bestimmten Zeitpunkt wiederhergestellt werden.

Wir können die Bedeutung dessen simulieren, indem wir einige Tabellen in Ihrer Datenbank löschen, was dann durch einen zeitpunktgenauen Restore korrigiert wird.

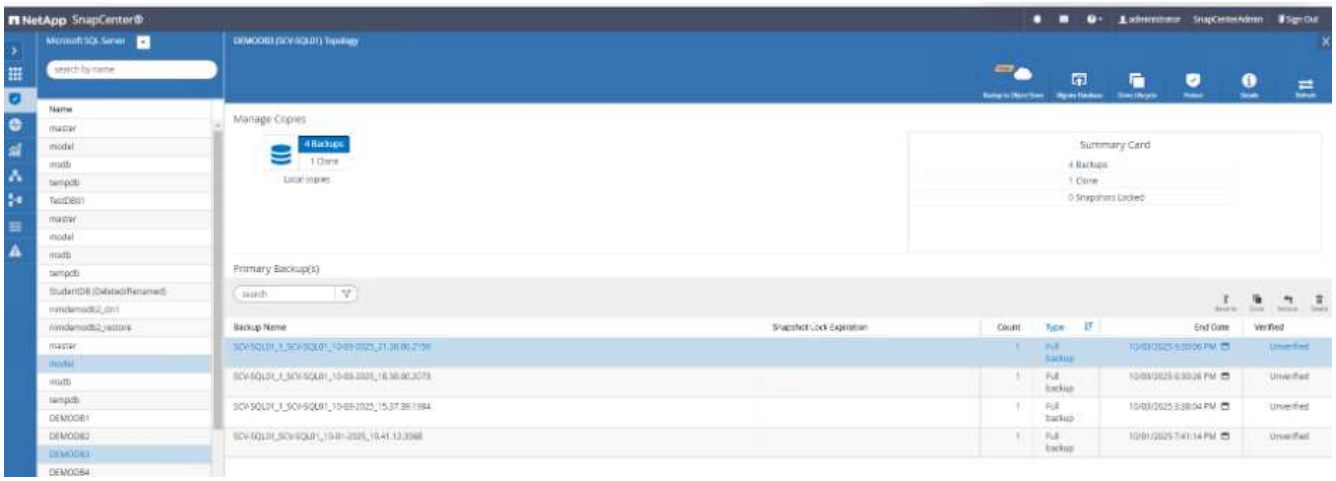
Im Folgenden sehen Sie, dass mehrere Tabellen aus unserer Datenbank, die im ersten Screenshot angezeigt wurden, im zweiten Screenshot gelöscht wurden:


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

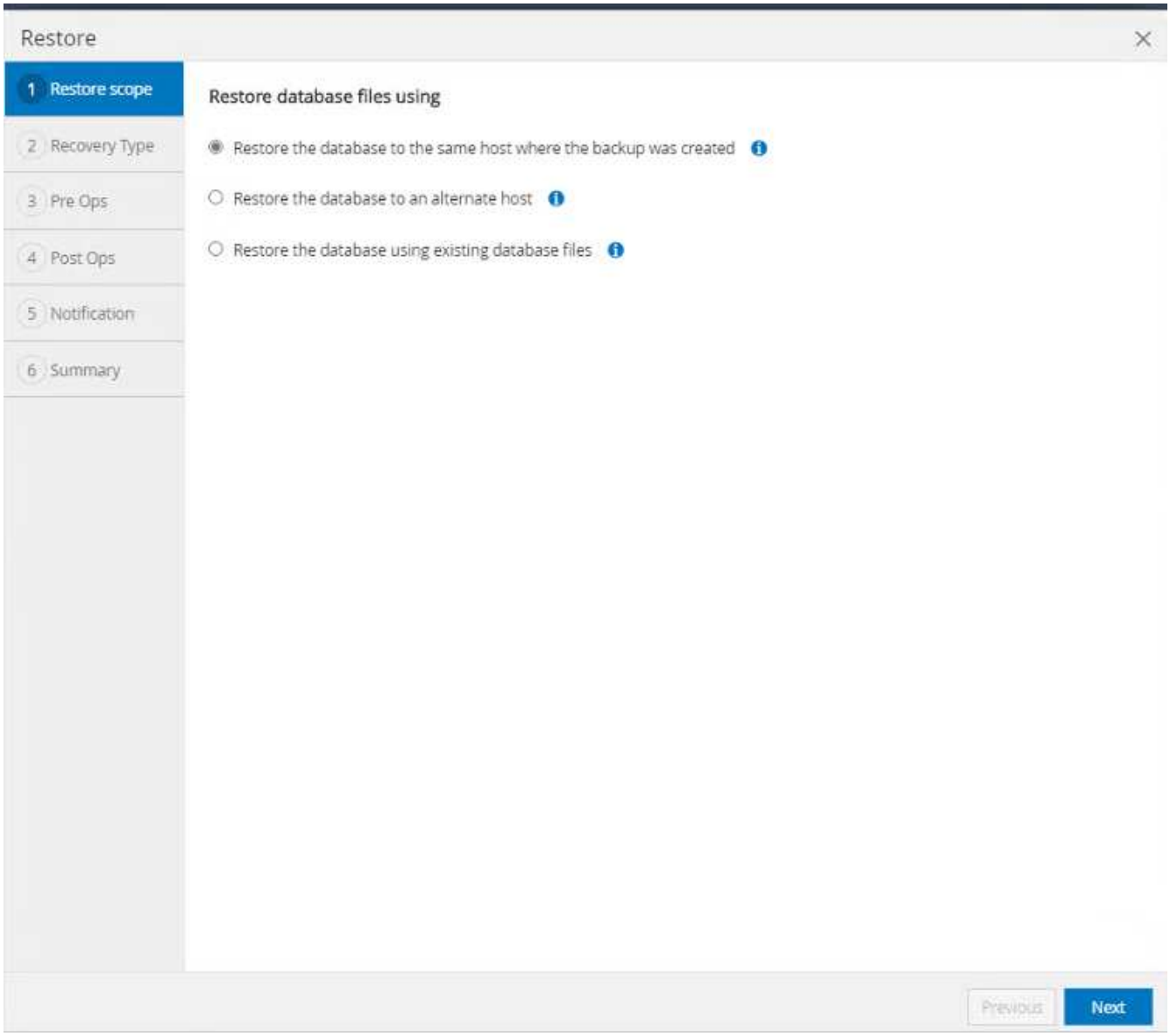


Die folgenden Schritte zeigen, wie eine Wiederherstellung durchgeführt wird, um diese gelöschten Tabellen wiederherzustellen:

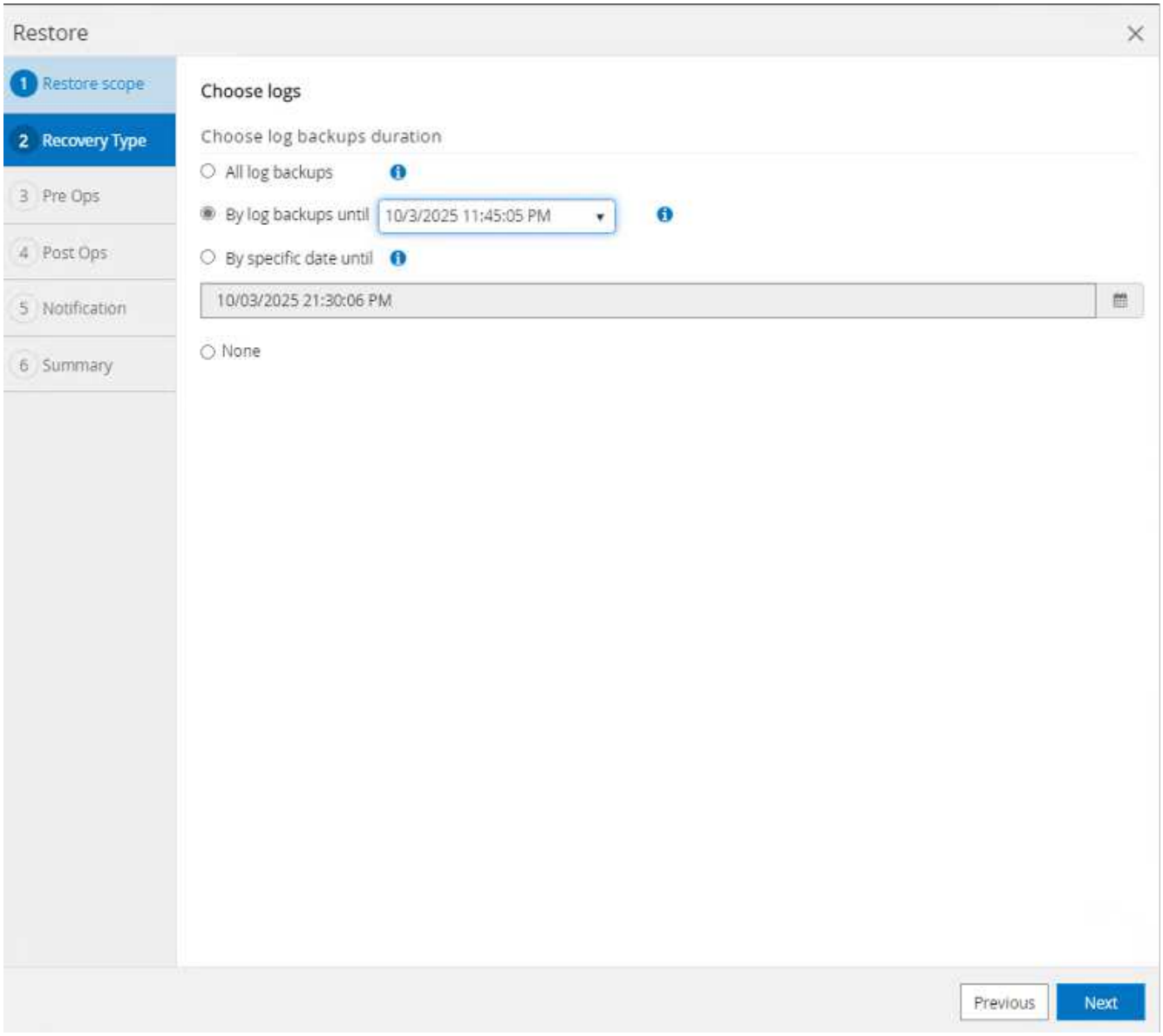
1. Wählen Sie die Datenbank aus der Ressourcengruppe.



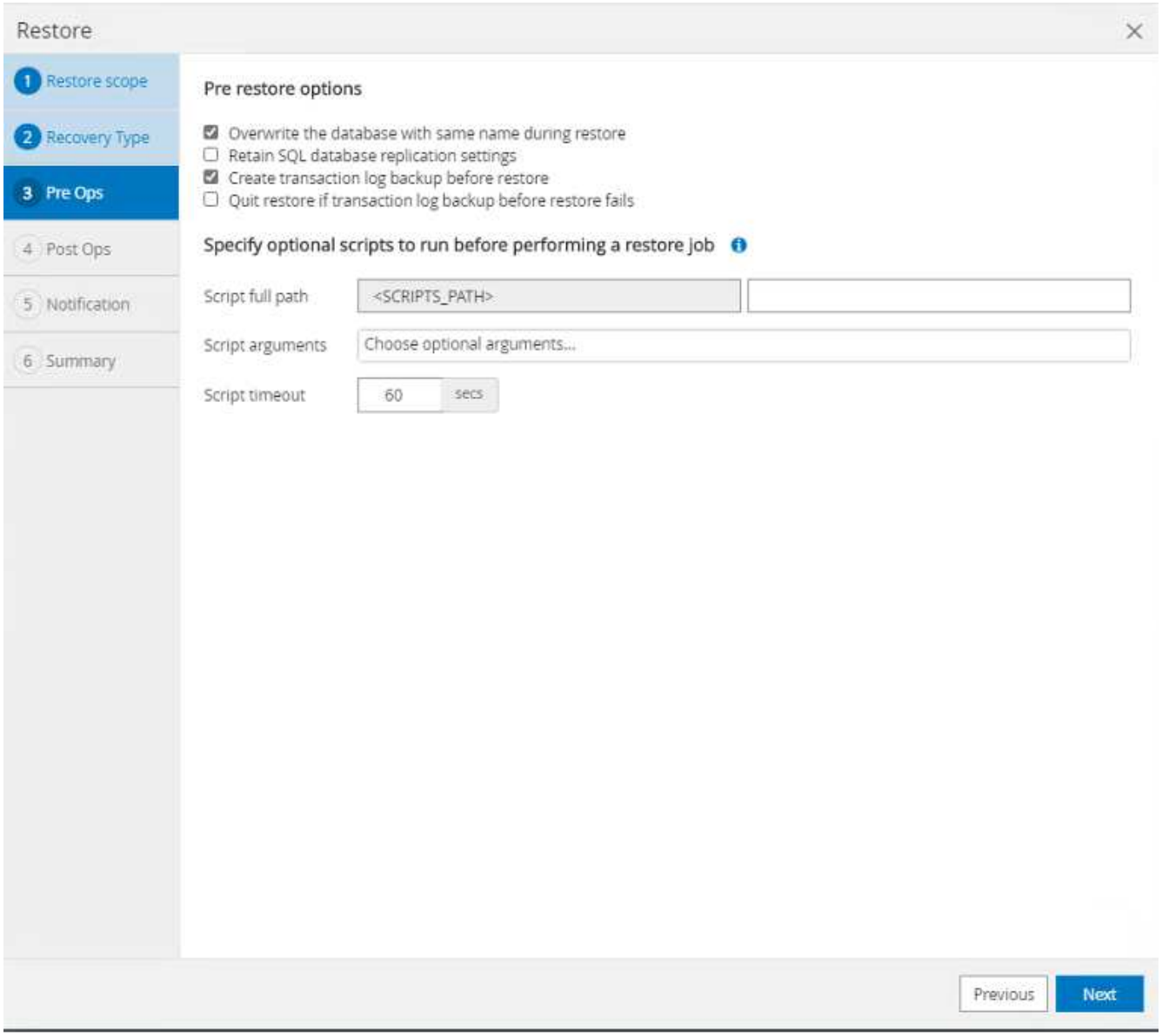
2. Wählen Sie auf der Seite „Wiederherstellen“ die Option „Die Datenbank auf demselben Host wiederherstellen, auf dem das Backup erstellt wurde“.



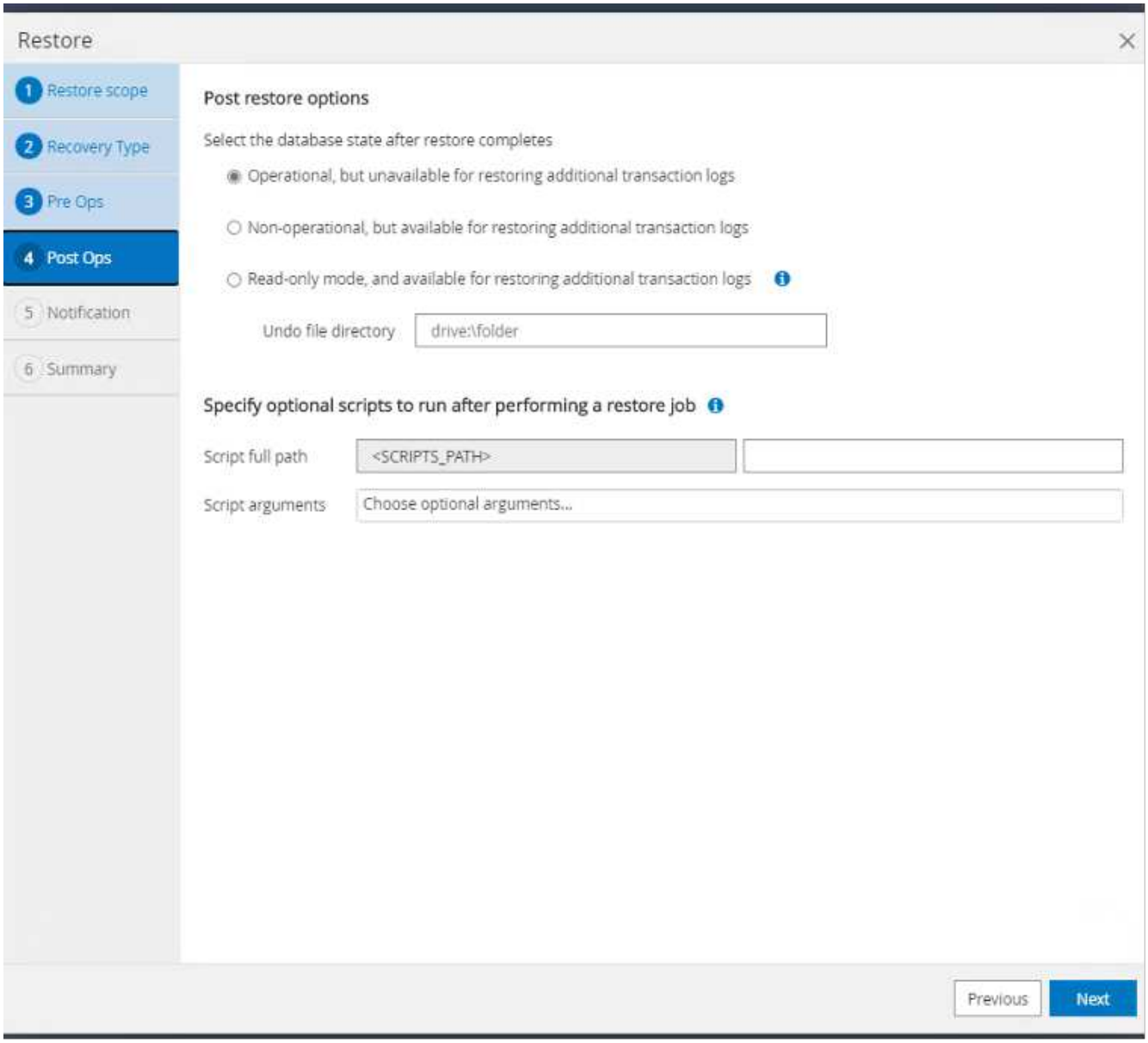
3. Wählen Sie die Option, ein Log-Backup zu einem bestimmten Zeitpunkt zu verwenden.



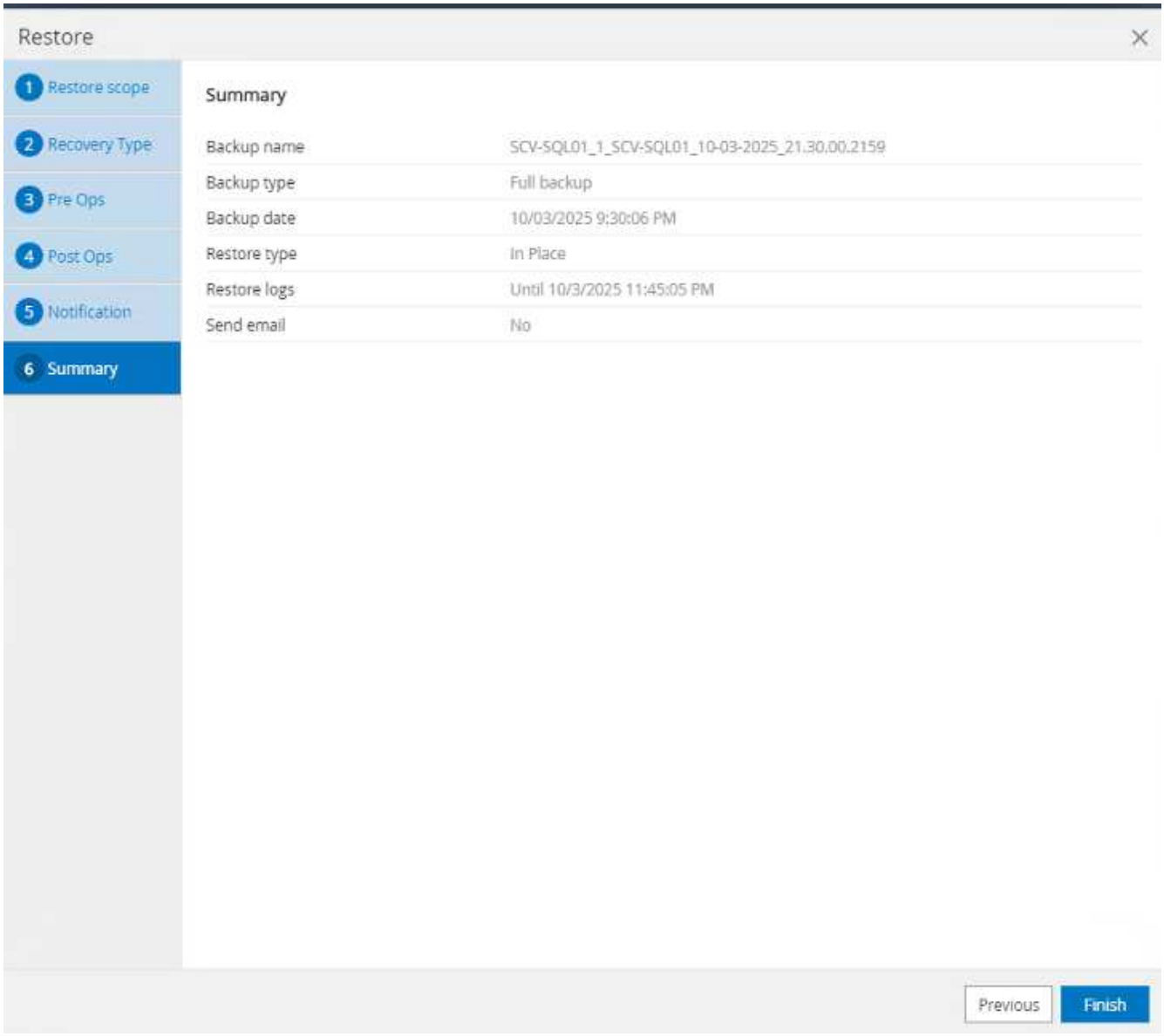
4. Wählen Sie „Datenbank mit gleichem Namen während der Wiederherstellung überschreiben, Transaktionsprotokollsicherung vor der Wiederherstellung erstellen“ und wählen Sie „Weiter“.



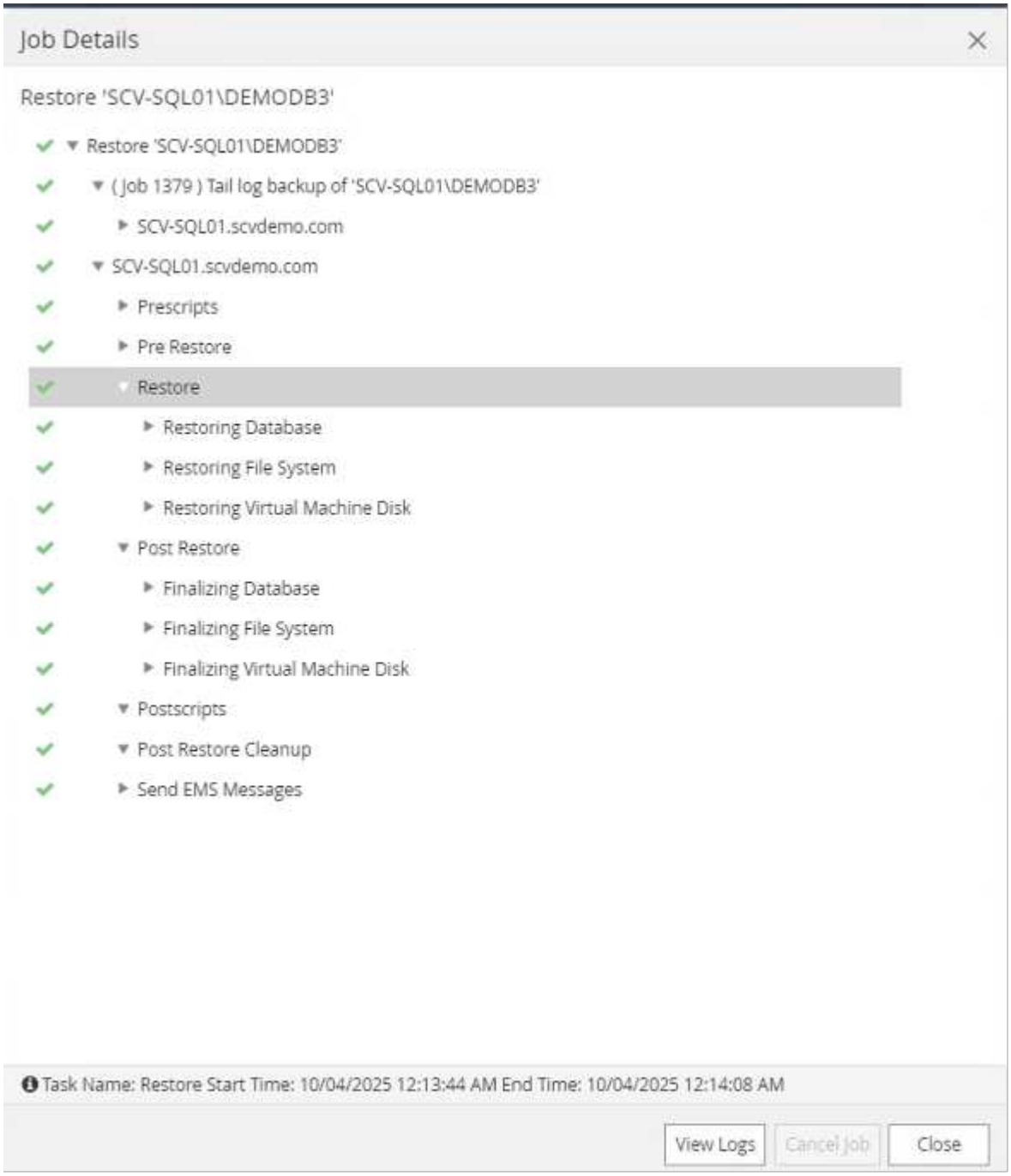
5. Wählen Sie den Zustand aus, den die Datenbank nach der Wiederherstellung annehmen soll, aus den Listenoptionen aus und wählen Sie „Weiter“.



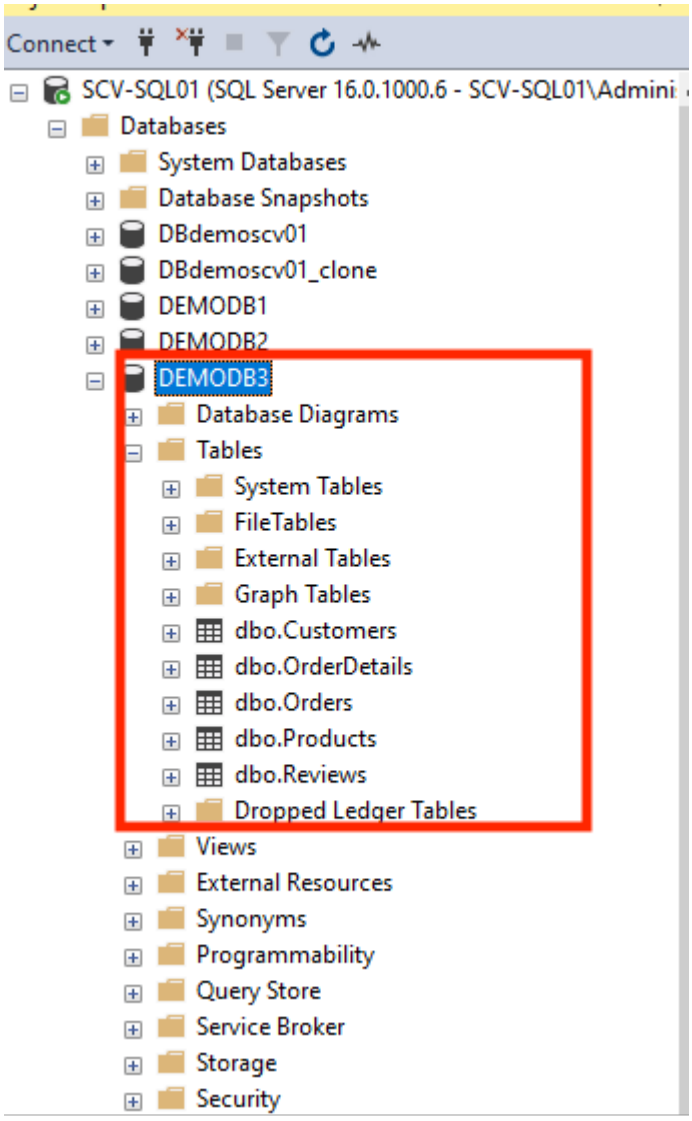
6. Wählen Sie auf der Zusammenfassungsseite „Finish“.



7. Überwachen Sie den Job bis zum Abschluss.



8. Überprüfen Sie, ob die gelöschten Tabellen erfolgreich wiederhergestellt wurden.



Abschluss

In diesem Dokument geben wir eine detaillierte Schritt-für-Schritt-Anleitung für die Bereitstellung, Konfiguration und Verwendung von SCV und "SnapCenter Plug-in für SQL Server (SCSQL)" bei Verwendung von FSx for ONTAP als zusätzlichem Datenspeicher mit Amazon EVS-Clustern.

Abschluss

Zusammenfassend lässt sich sagen, dass bei der Verwendung von FSx für ONTAP zur Optimierung der Gesamtbetriebskosten (TCO) einer Amazon EVS-Bereitstellung SCV eine einfache und effiziente Methode zur Sicherung von VMs bietet. Es kann VMs nahtlos und schnell sichern und wiederherstellen, da es auf Snapshot-Kopien basiert, deren Erstellung buchstäblich nur Sekunden dauert.

"Testen Sie das SnapCenter Plug-in für VMware jetzt kostenlos".

NetApp für Azure / AVS

NetApp -Funktionen für Azure AVS

Erfahren Sie mehr über die Funktionen, die NetApp in die Azure VMware Solution (AVS) einbringt – von NetApp als über einen Gast verbundenes Speichergerät oder als zusätzlicher NFS-Datenspeicher bis hin zur Migration von Workflows, Erweiterung/Bursting in die Cloud, Sicherung/Wiederherstellung und Notfallwiederherstellung.

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

- "Konfigurieren von AVS in Azure"
- "NetApp Storage-Optionen für AVS"
- "NetApp / VMware Cloud-Lösungen"

Konfigurieren von AVS in Azure

Wie bei der lokalen Umgebung ist die Planung einer Cloud-basierten Virtualisierungsumgebung entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen und Migrieren von VMs.

In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Solution einrichten und verwalten und in Kombination mit den verfügbaren Optionen zum Anbinden von NetApp -Speicher verwenden.

> In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP mit Azure VMware Solution.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Registrieren des Ressourcenanbieters und Erstellen einer privaten Cloud
- Herstellen einer Verbindung mit einem neuen oder vorhandenen virtuellen ExpressRoute-Netzwerkgateway
- Überprüfen Sie die Netzwerkkonnektivität und greifen Sie auf die private Cloud zu

Sehen Sie sich die detaillierte"Konfigurationsschritte für AVS" .

NetApp Storage-Optionen für AVS

NetApp Speicher kann innerhalb von Azure AVS auf verschiedene Weise genutzt werden – entweder als verbundener Speicher oder als zusätzlicher NFS-Datenspeicher.

Bitte besuchen Sie"Unterstützte NetApp -Speicheroptionen" für weitere Informationen.

Azure unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- Azure NetApp Files (ANF) als mit dem Gast verbundener Speicher
- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- Azure NetApp Files (ANF) als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungs-Speicheroptionen für AVS" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für AVS" .

Anwendungsfälle der Lösung

Mit NetApp und VMware-Cloudlösungen lassen sich viele Anwendungsfälle einfach in Azure AVS bereitstellen. Diese Fälle sind für jeden der von VMware definierten Cloudbereiche definiert:

- Schützen (beinhaltet sowohl Disaster Recovery als auch Backup/Wiederherstellung)
- Verlängern
- Wandern

"Durchsuchen Sie die NetApp -Lösungen für Azure AVS"

Schützen Sie Workloads auf Azure/AVS

Disaster Recovery mit ANF und JetStream

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Site-Ausfällen und Datenbeschädigungen (z. B. Ransomware) zu schützen. Mithilfe des VMware VAIO-Frameworks können lokale VMware-Workloads in den Azure Blob-Speicher repliziert und wiederhergestellt werden, wodurch ein minimaler oder nahezu kein Datenverlust und eine RTO von nahezu null möglich sind.

Mit JetStream DR können die vom lokalen Standort auf AVS und insbesondere auf Azure NetApp Files replizierten Workloads nahtlos wiederhergestellt werden. Es ermöglicht eine kostengünstige Notfallwiederherstellung durch die Nutzung minimaler Ressourcen am DR-Standort und kostengünstigen Cloud-Speicher. JetStream DR automatisiert die Wiederherstellung in ANF-Datenspeichern über Azure Blob Storage. JetStream DR stellt unabhängige VMs oder Gruppen verwandter VMs gemäß der Netzwerkzuordnung in der Infrastruktur des Wiederherstellungsstandorts wieder her und bietet eine zeitpunktbezogene Wiederherstellung zum Schutz vor Ransomware.

Dieses Dokument vermittelt ein Verständnis der Betriebsprinzipien und Hauptkomponenten von JetStream DR.

▼ Übersicht über die Lösungsbereitstellung

1. Installieren Sie die JetStream DR-Software im lokalen Rechenzentrum.
    a. Laden Sie das JetStream DR-Softwarepaket vom Azure Marketplace (ZIP) herunter und stellen Sie das JetStream DR MSA (OVA) im vorgesehenen Cluster bereit.
    b. Konfigurieren Sie den Cluster mit dem E/A-Filterpaket (installieren Sie JetStream VIB).
    c. Stellen Sie Azure Blob (Azure Storage-Konto) in derselben Region wie der DR AVS-Cluster bereit.
    d. Stellen Sie DRVA-Geräte bereit und weisen Sie Replikationsprotokollvolumes zu (VMDK aus vorhandenem Datenspeicher oder gemeinsam genutztem iSCSI-Speicher).
    e. Erstellen Sie geschützte Domänen (Gruppen verwandter VMs) und weisen Sie DRVAs und Azure Blob Storage/ANF zu.
    f. Schutz starten.
2. Installieren Sie die JetStream DR-Software in der privaten Azure VMware Solution-Cloud.
    a. Verwenden Sie den Befehl „Ausführen“, um JetStream DR zu installieren und zu konfigurieren.
    b. Fügen Sie denselben Azure Blob-Container hinzu und ermitteln Sie Domänen mithilfe der Option „Domänen scannen“.

c. Stellen Sie die erforderlichen DRVA-Geräte bereit.

d. Erstellen Sie Replikationsprotokollvolumes mithilfe verfügbarer vSAN- oder ANF-Datenspeicher.

e. Importieren Sie geschützte Domänen und konfigurieren Sie RocVA (Recovery VA), um den ANF-Datenspeicher für VM-Platzierungen zu verwenden.

f. Wählen Sie die entsprechende Failover-Option aus und starten Sie die kontinuierliche Rehydrierung für Domänen oder VMs mit nahezu null RTO.

3. Lösen Sie während eines Notfallereignisses ein Failover zu Azure NetApp Files Datenspeichern am angegebenen AVS DR-Standort aus.
4. Rufen Sie das Failback zur geschützten Site auf, nachdem die geschützte Site wiederhergestellt wurde. Stellen Sie vor dem Start sicher, dass die Voraussetzungen erfüllt sind, wie in diesem Abschnitt angegeben. "Link" und führen Sie außerdem das von JetStream Software bereitgestellte Bandwidth Testing Tool (BWT) aus, um die potenzielle Leistung des Azure Blob-Speichers und seine Replikationsbandbreite bei Verwendung mit der JetStream DR-Software zu bewerten. Nachdem die Voraussetzungen, einschließlich der Konnektivität, erfüllt sind, richten Sie JetStream DR für AVS ein und abonnieren Sie es über die "Azure Marketplace" . Nachdem das Softwarepaket 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. Stellen Sie eine Liste der zu schützenden VMs zusammen mit ihren RTO- und Wiederherstellungsgruppeneinstellungen bereit und führen Sie dann CPT aus.

CPT erfüllt die folgenden Funktionen:

- Kombinieren Sie VMs entsprechend ihrer RTO in Schutzdomänen.
- Festlegen der optimalen Anzahl von DRVAs und ihrer Ressourcen.
- Schätzung der erforderlichen Replikationsbandbreite.
- Identifizieren der Merkmale des Replikationsprotokollvolumens (Kapazität, Bandbreite usw.).
- Schätzen der erforderlichen Objektspeicherkapazität und mehr.

> ⓘ Die Anzahl und der Inhalt der vorgeschriebenen Domänen hängen von verschiedenen VM-Eigenschaften ab, wie z. B. durchschnittlichen IOPS, Gesamtkapazität, Priorität (die die Failover-Reihenfolge definiert), RTO und anderen.

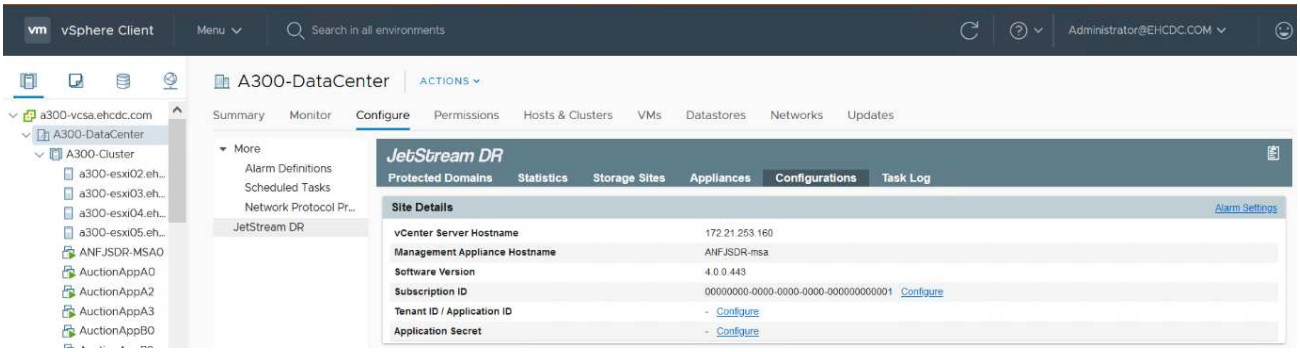
Installieren Sie JetStream DR im lokalen Rechenzentrum

Die JetStream DR-Software besteht aus drei Hauptkomponenten: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) und Hostkomponenten (E/A-Filterpakete). MSA wird verwendet, um Hostkomponenten auf dem Computercluster zu installieren und zu konfigurieren und anschließend die JetStream DR-Software zu verwalten. Die folgende Liste bietet eine allgemeine Beschreibung des Installationsvorgangs:

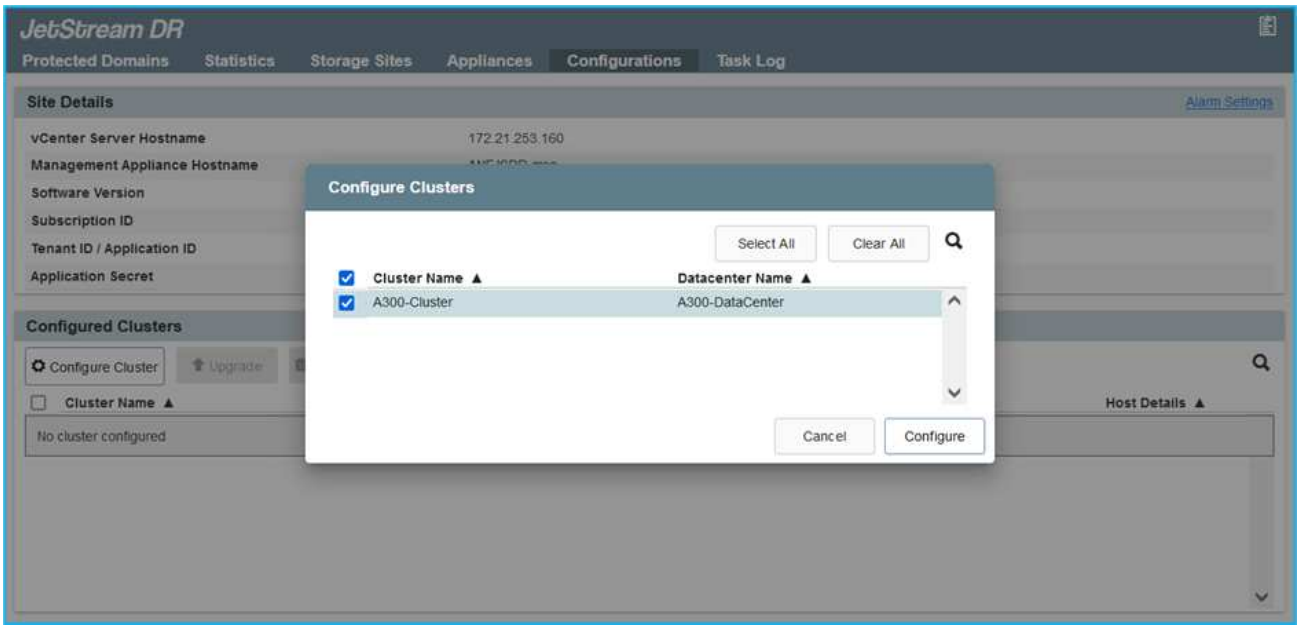
▼ So installieren Sie JetStream DR vor Ort

1. Voraussetzungen prüfen.
2. Führen Sie das Kapazitätsplanungstool aus, um Empfehlungen zu Ressourcen und Konfigurationen zu erhalten (optional, aber für Proof-of-Concept-Tests empfohlen).
3. Stellen Sie den JetStream DR MSA auf einem vSphere-Host im vorgesehenen Cluster bereit.
4. Starten Sie das MSA mit seinem DNS-Namen in einem Browser.

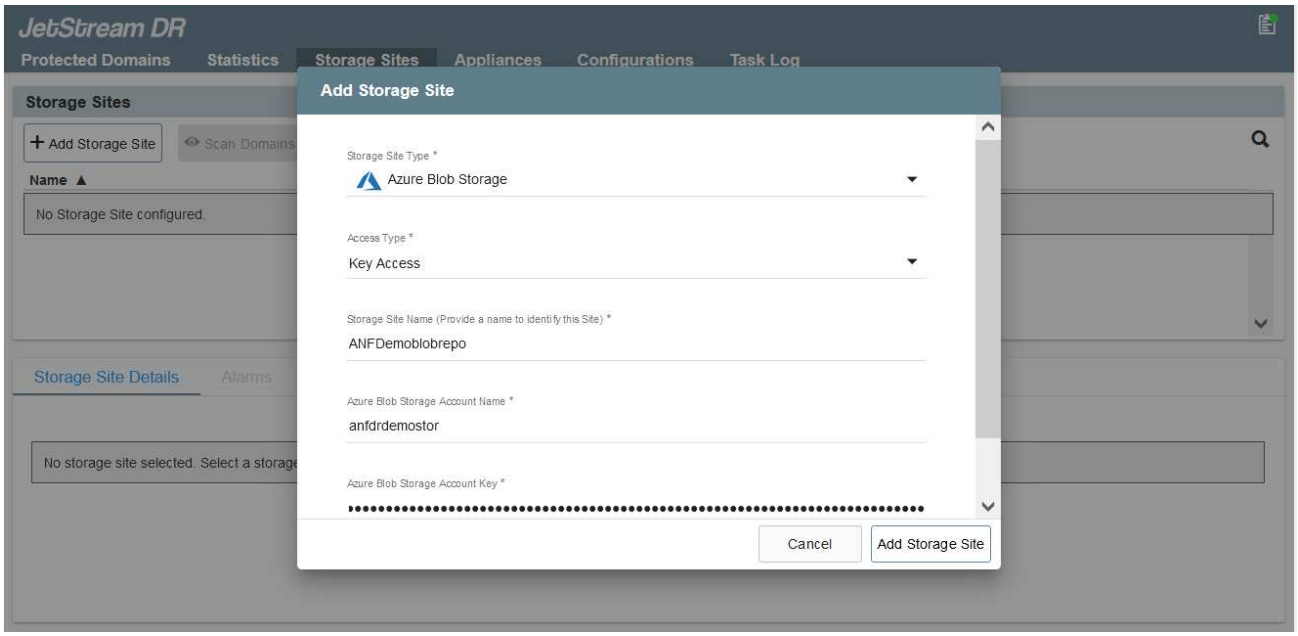
5. Registrieren Sie den vCenter-Server beim MSA. Führen Sie zur Durchführung der Installation die folgenden detaillierten Schritte aus:
6. Nachdem JetStream DR MSA bereitgestellt und der vCenter Server registriert wurde, greifen Sie über den vSphere Web Client auf das JetStream DR-Plug-In zu. Dies kann durch Navigieren zu Rechenzentrum > Konfigurieren > JetStream DR erfolgen.



7. Wählen Sie in der JetStream DR-Schnittstelle den entsprechenden Cluster aus.



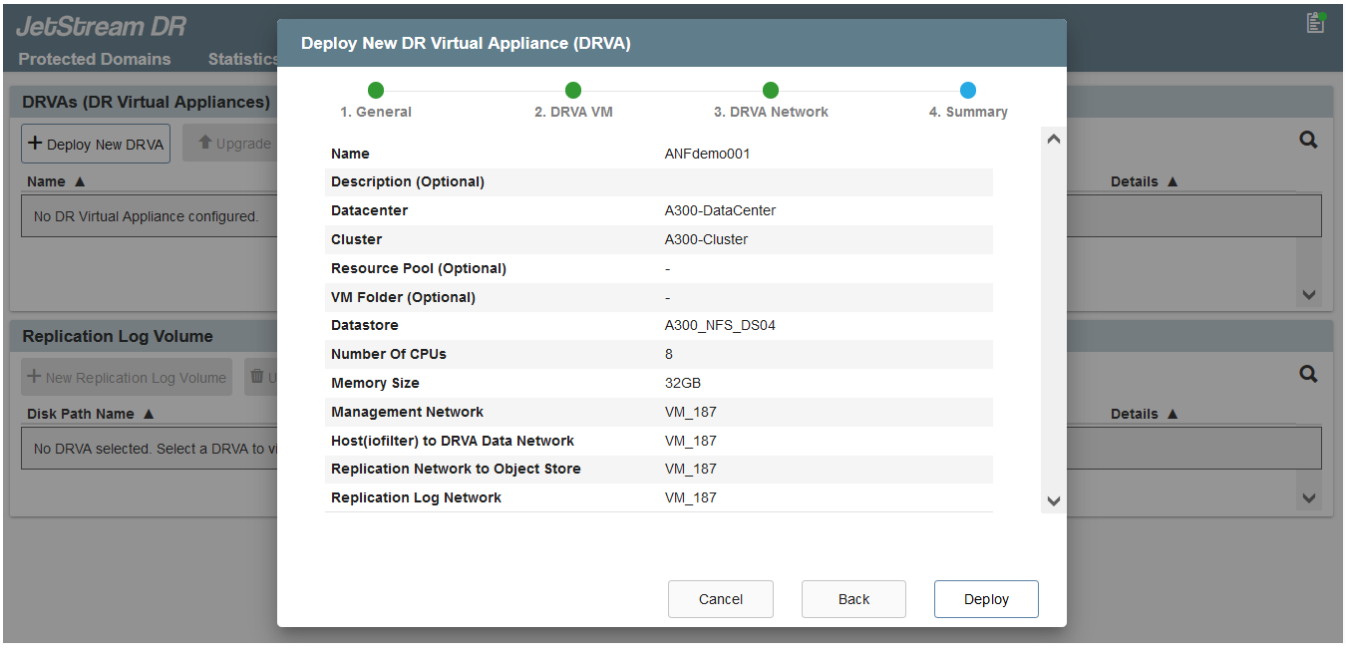
8. Konfigurieren Sie den Cluster mit dem E/A-Filterpaket.



9. Fügen Sie Azure Blob Storage am Wiederherstellungsstandort hinzu.
10. Stellen Sie eine DR Virtual Appliance (DRVA) über die Registerkarte „Appliances“ bereit.

> DRVAs können automatisch von CPT erstellt werden, für POC-Tests empfehlen wir jedoch, den DR-Zyklus manuell zu konfigurieren und auszuführen (Schutz starten > Failover > Failback).

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

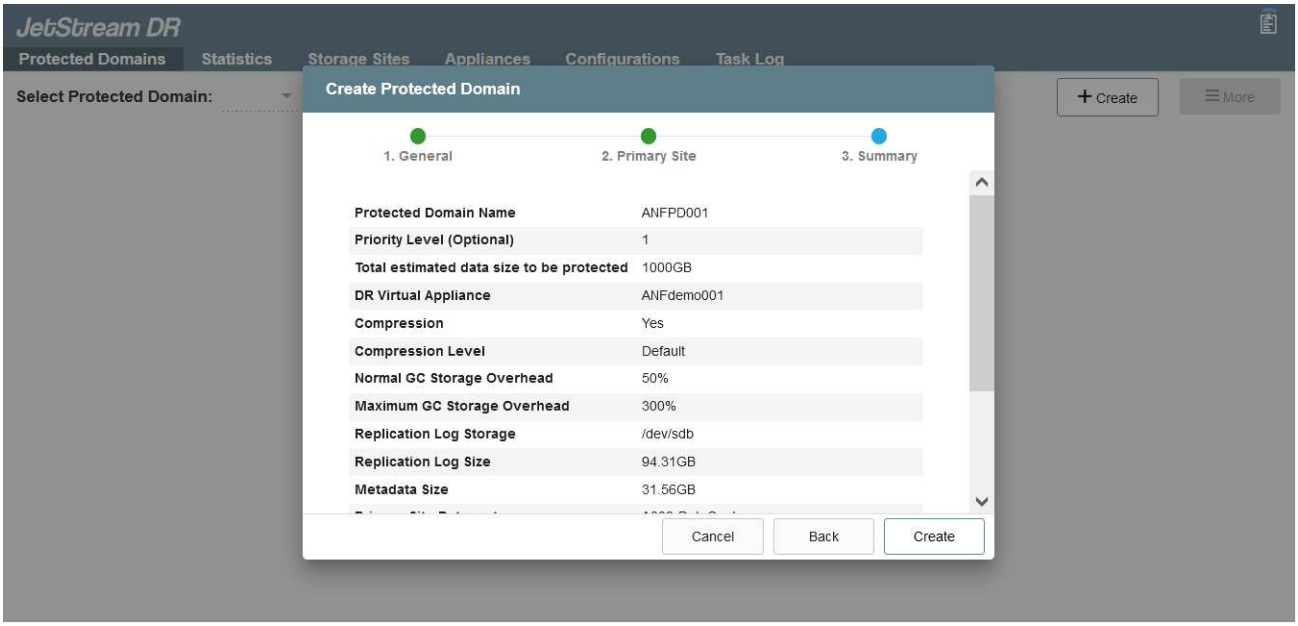


In diesem Beispiel wurden vier DRVAs für 80 virtuelle Maschinen erstellt.

1. Erstellen Sie Replikationsprotokollvolumes für jeden DRVA mithilfe von VMDK aus den verfügbaren

Datenspeichern oder unabhängigen gemeinsam genutzten iSCSI-Speicherpools.

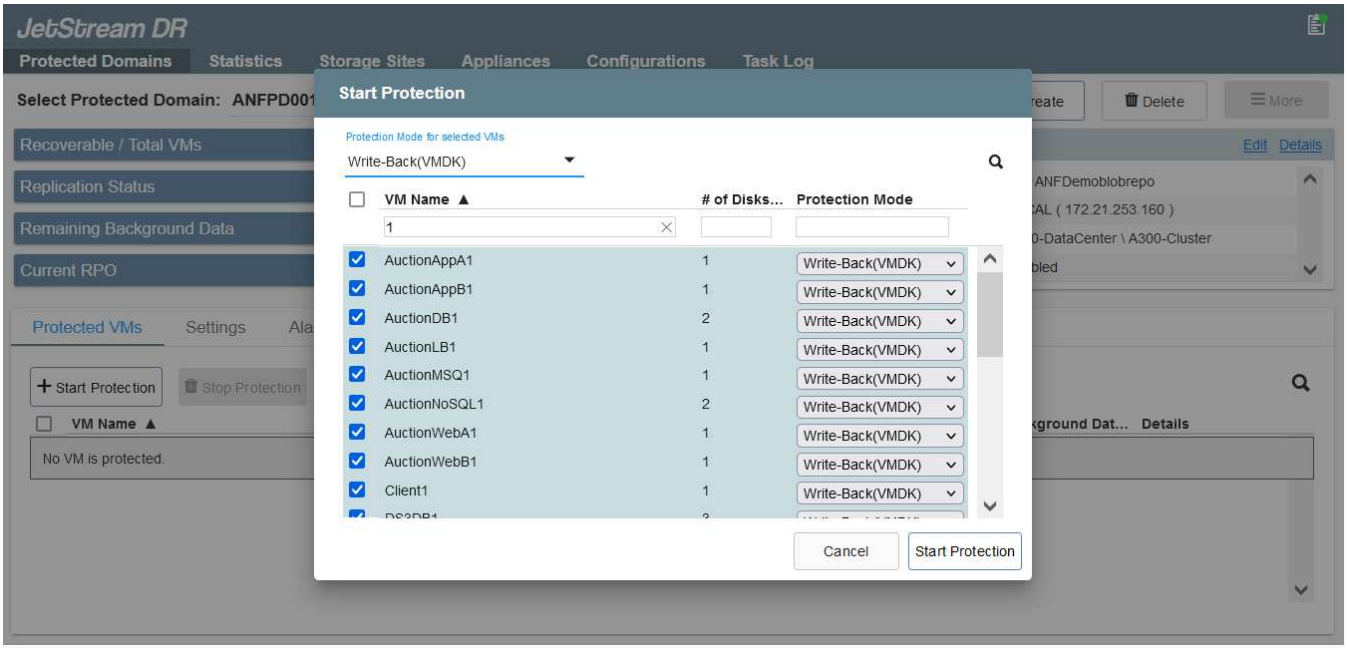
2. Erstellen Sie auf der Registerkarte „Geschützte Domänen“ die erforderliche Anzahl geschützter Domänen mithilfe von Informationen zur Azure Blob Storage-Site, der DRVA-Instanz und dem Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder eine Gruppe von VMs innerhalb des Clusters, die gemeinsam geschützt werden und denen eine Prioritätsreihenfolge für Failover-/Failback-Vorgänge zugewiesen wird.



3. Wählen Sie die VMs aus, die Sie schützen möchten, und starten Sie den VM-Schutz der geschützten Domäne. Dadurch wird die Datenreplikation in den angegebenen Blob Store gestartet.

ⓘ Stellen Sie sicher, dass für alle VMs in einer geschützten Domäne derselbe Schutzmodus verwendet wird.

ⓘ Der Write-Back-Modus (VMDK) kann eine höhere Leistung bieten.



Stellen Sie sicher, dass Replikationsprotokollvolumes auf Hochleistungsspeichern abgelegt werden.

> Failover-Runbooks können so konfiguriert werden, dass sie die VMs gruppieren (sogenannte Wiederherstellungsgruppen), die Startreihenfolge festlegen und die CPU-/Speichereinstellungen zusammen mit den IP-Konfigurationen ändern.

Installieren Sie JetStream DR für AVS in einer privaten Azure VMware Solution-Cloud mit dem Befehl „Ausführen“

Eine bewährte Methode für eine Wiederherstellungssite (AVS) besteht darin, im Voraus einen Pilot-Light-Cluster mit drei Knoten zu erstellen. Dadurch kann die Infrastruktur des Wiederherstellungsstandorts vorkonfiguriert werden, einschließlich der folgenden Elemente:

- Zielnetzwerksegmente, Firewalls, Dienste wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF-Volumes als Datenspeicher und mehr. JetStream DR unterstützt den RTO-Modus nahezu Null für unternehmenskritische Domänen. Für diese Domänen sollte der Zielspeicher vorinstalliert sein. In diesem Fall ist ANF ein empfohlener Speichertyp.

> Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster so konfiguriert werden, dass sie den lokalen Anforderungen entspricht.

Abhängig von den SLA- und RTO-Anforderungen kann ein kontinuierliches Failover oder ein regulärer (Standard-)Failover-Modus verwendet werden. Um eine RTO von nahezu Null zu erreichen, sollte am Wiederherstellungsort mit der kontinuierlichen Rehydration begonnen werden.

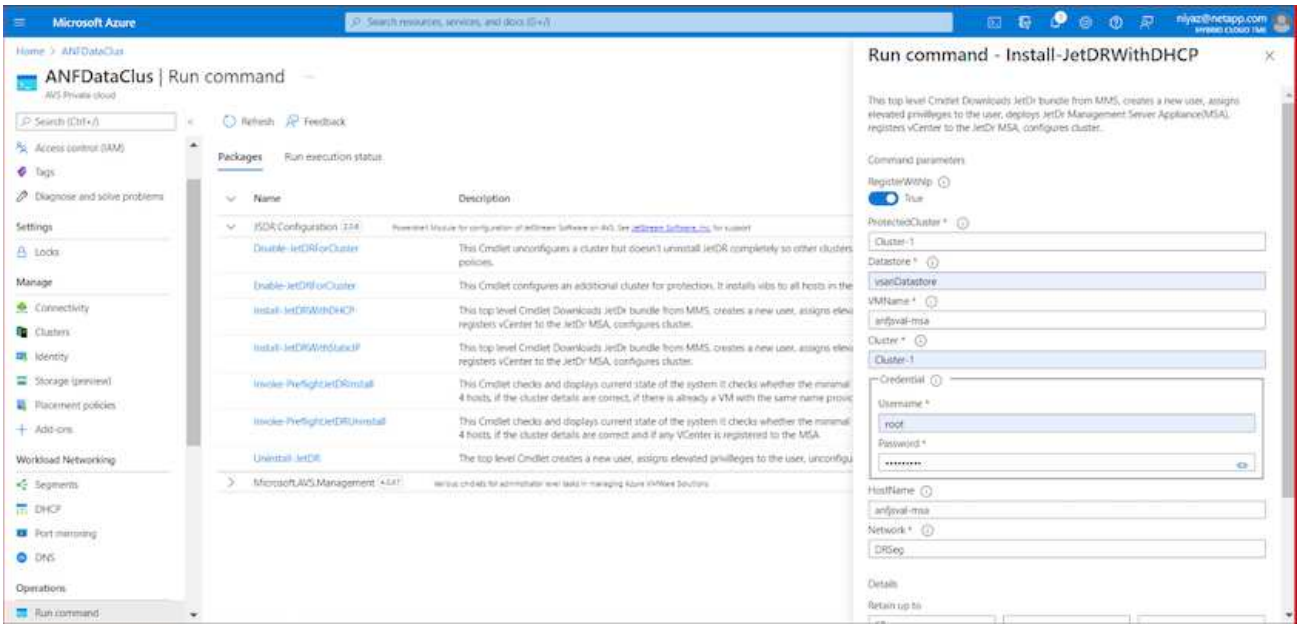
▼ **So installieren Sie JetStream DR für AVS in einer privaten Cloud**

Führen Sie die folgenden Schritte aus, um JetStream DR für AVS in einer privaten Azure VMware Solution-Cloud zu installieren:

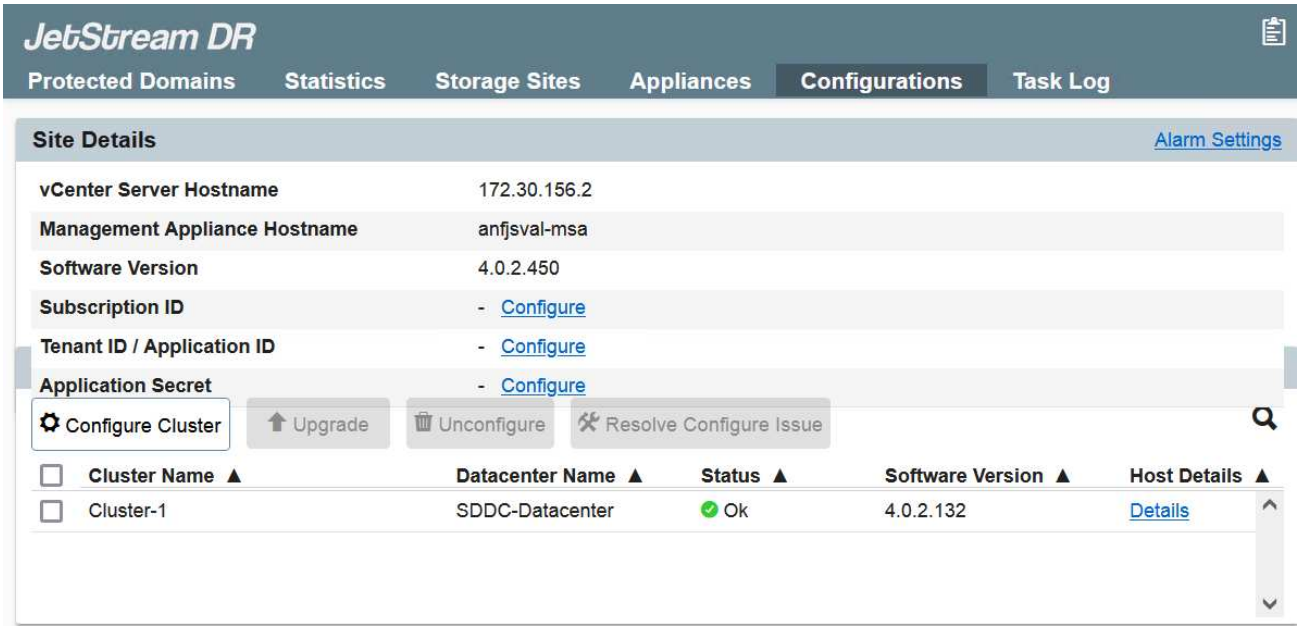
1. Gehen Sie im Azure-Portal zur Azure VMware-Lösung, wählen Sie die private Cloud aus und wählen Sie „Befehl ausführen“ > „Pakete“ > „JSDR.Configuration“.

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

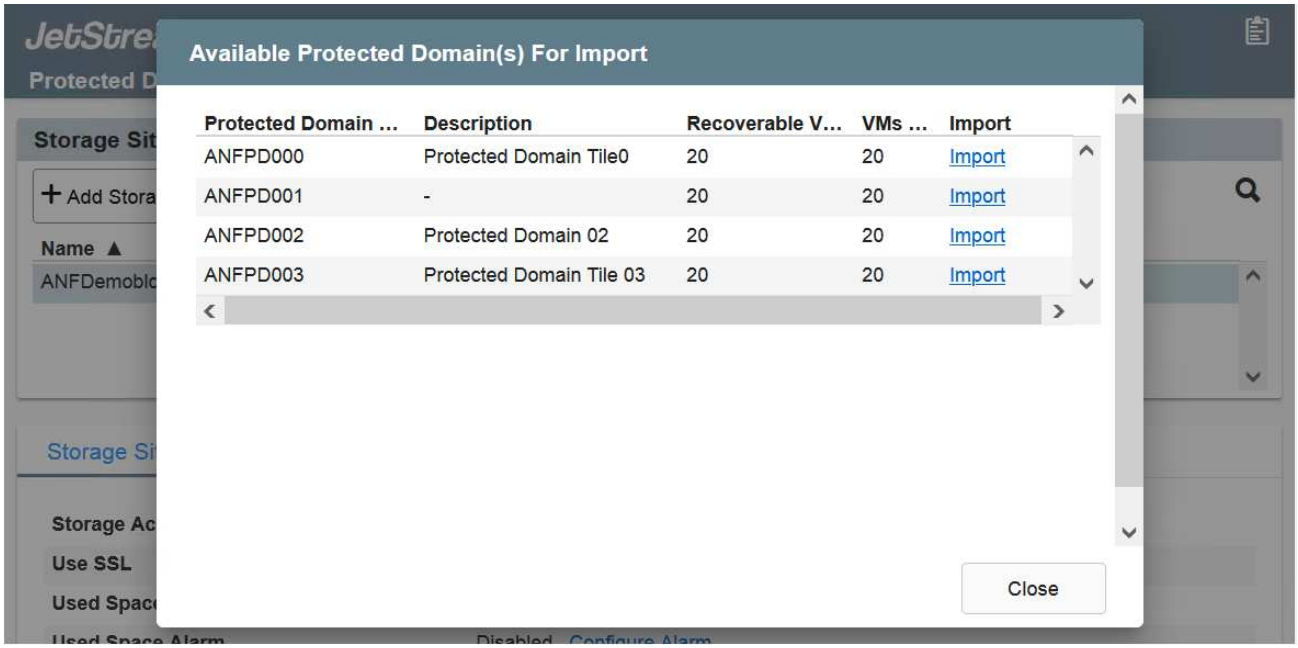
   Der folgende Screenshot zeigt die Installation mit einer DHCP-basierten IP-Adresse.



2. Aktualisieren Sie den Browser, nachdem die Installation von JetStream DR für AVS abgeschlossen ist. Um auf die JetStream DR-Benutzeroberfläche zuzugreifen, gehen Sie zu SDDC Datacenter > Konfigurieren > JetStream DR.



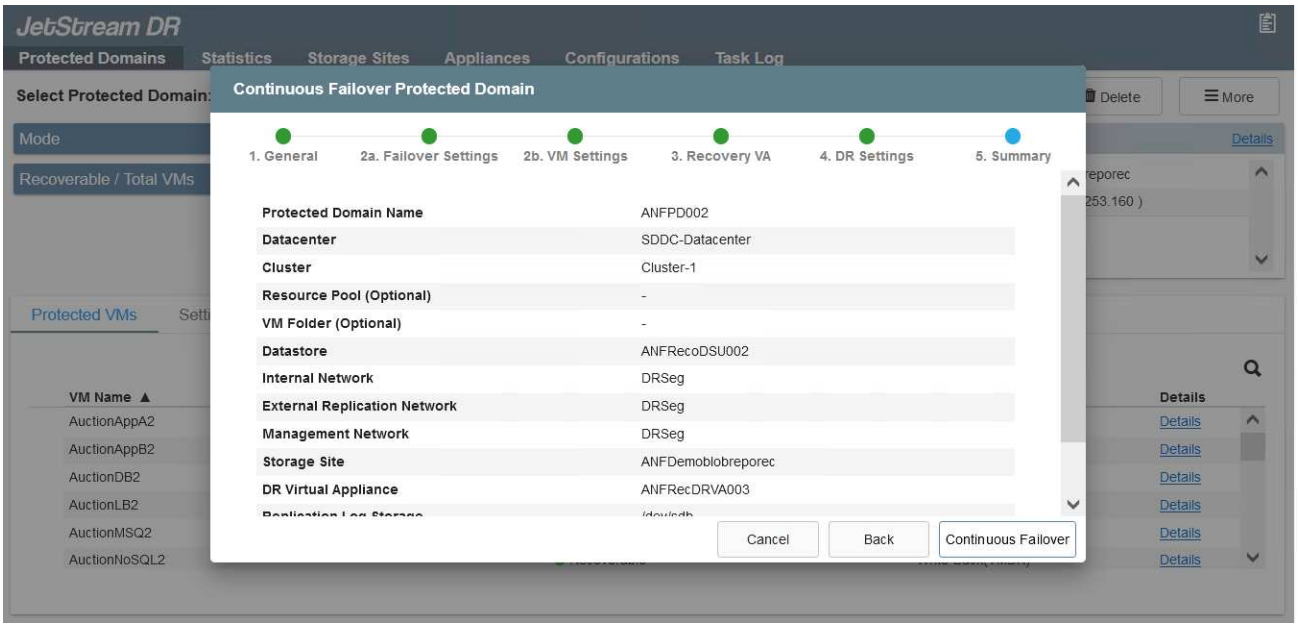
3. Fügen Sie über die JetStream DR-Schnittstelle das Azure Blob Storage-Konto hinzu, das zum Schutz des lokalen Clusters als Speicherort verwendet wurde, und führen Sie dann die Option „Domänen scannen“ aus.



4. Nachdem die geschützten Domänen importiert wurden, stellen Sie DRVA-Geräte bereit. In diesem Beispiel wird die kontinuierliche Rehydrierung manuell vom Wiederherstellungsstandort aus mithilfe der JetStream DR-Benutzeroberfläche gestartet.

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

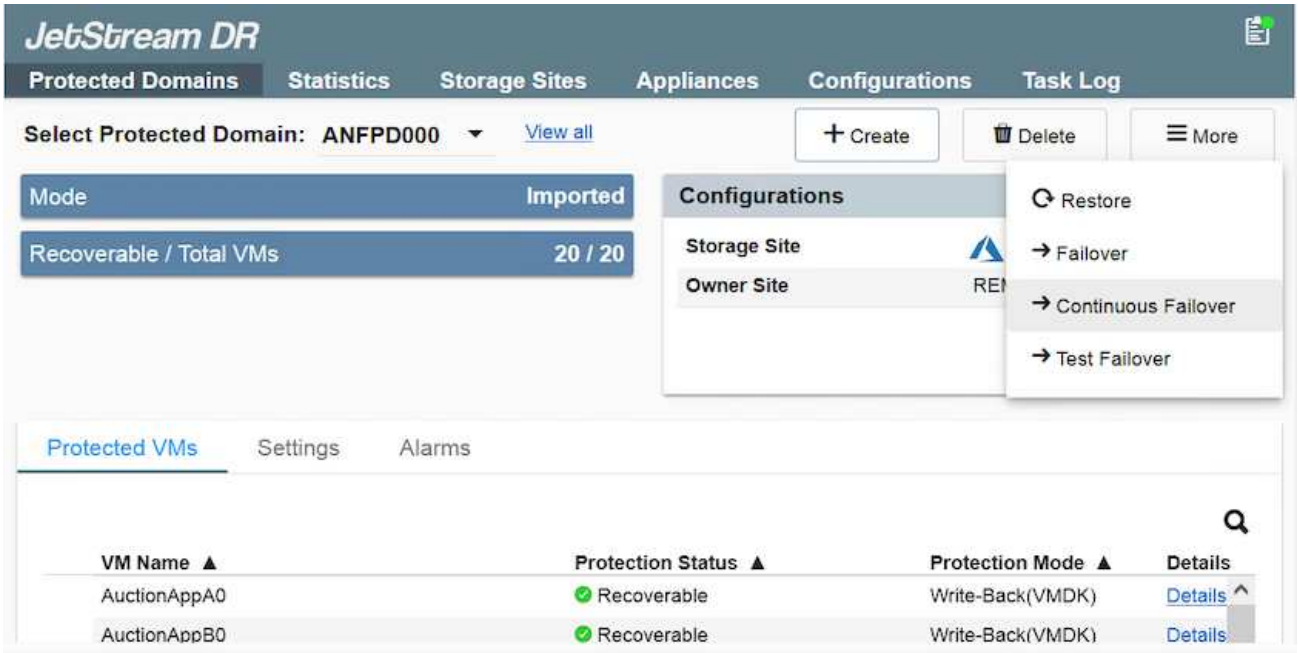
5. Erstellen Sie Replikationsprotokollvolumes mithilfe verfügbarer vSAN- oder ANF-Datenspeicher.
6. Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery VA so, dass der ANF-Datenspeicher für VM-Platzierungen verwendet wird.



> Stellen Sie sicher, dass DHCP im ausgewählten Segment aktiviert ist und genügend IPs verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen wiederhergestellt werden. Jede wiederherzustellende VM (einschließlich kontinuierlicher Rehydration) erfordert eine individuelle dynamische IP. Nach Abschluss der

Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

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



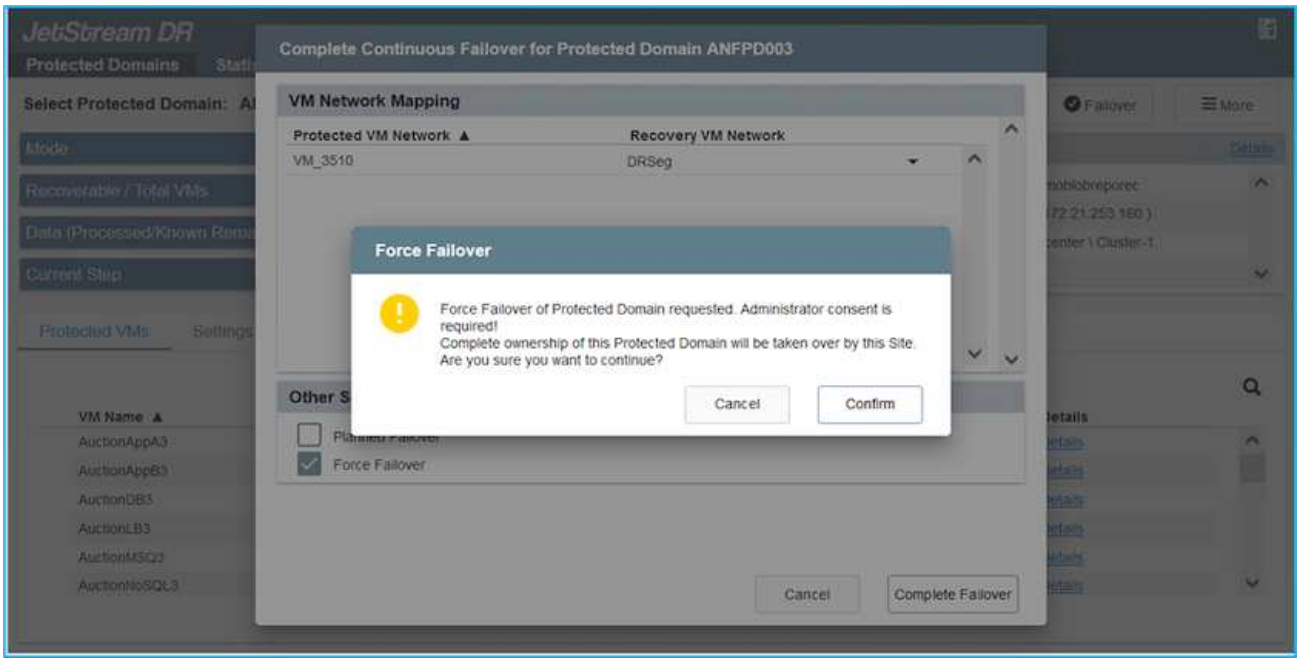
Durchführen eines Failovers/Failbacks

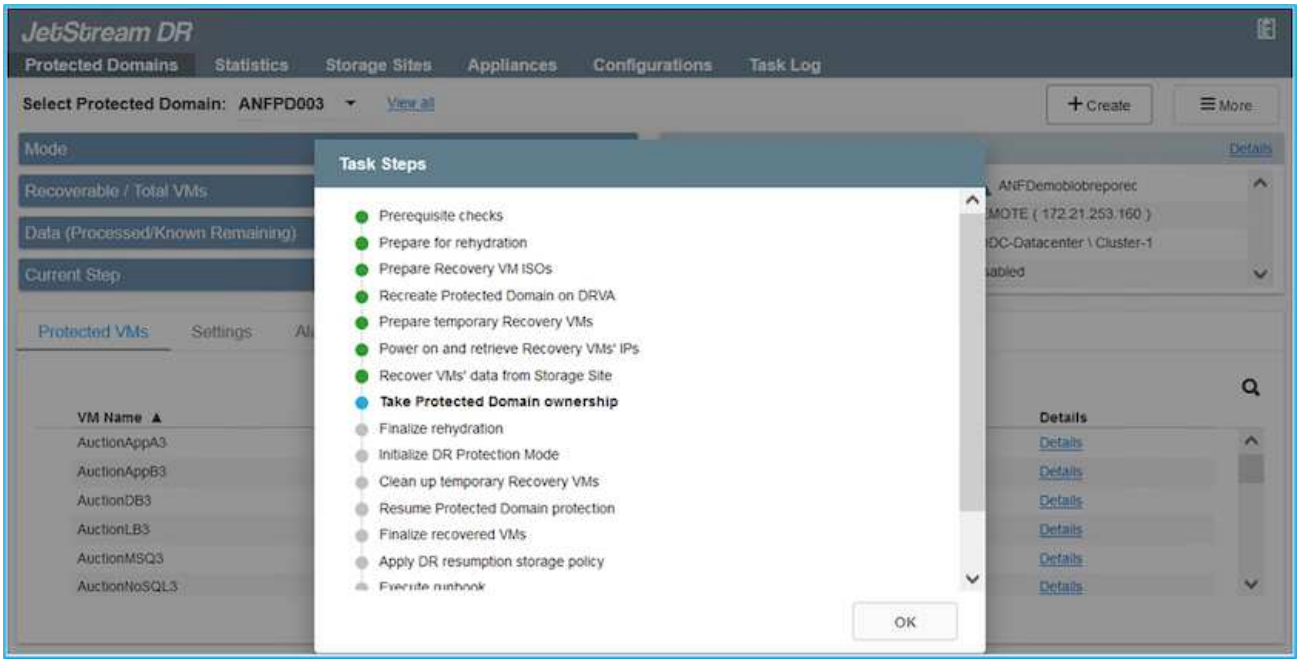
▼ So führen Sie ein Failover/Failback durch

1. Nachdem im geschützten Cluster der lokalen Umgebung ein Notfall (Teil- oder Vollausfall) aufgetreten ist, lösen Sie das Failover aus.

CPT kann verwendet werden, um den Failoverplan auszuführen und die VMs aus Azure Blob Storage in der AVS-Cluster-Wiederherstellungssite wiederherzustellen.

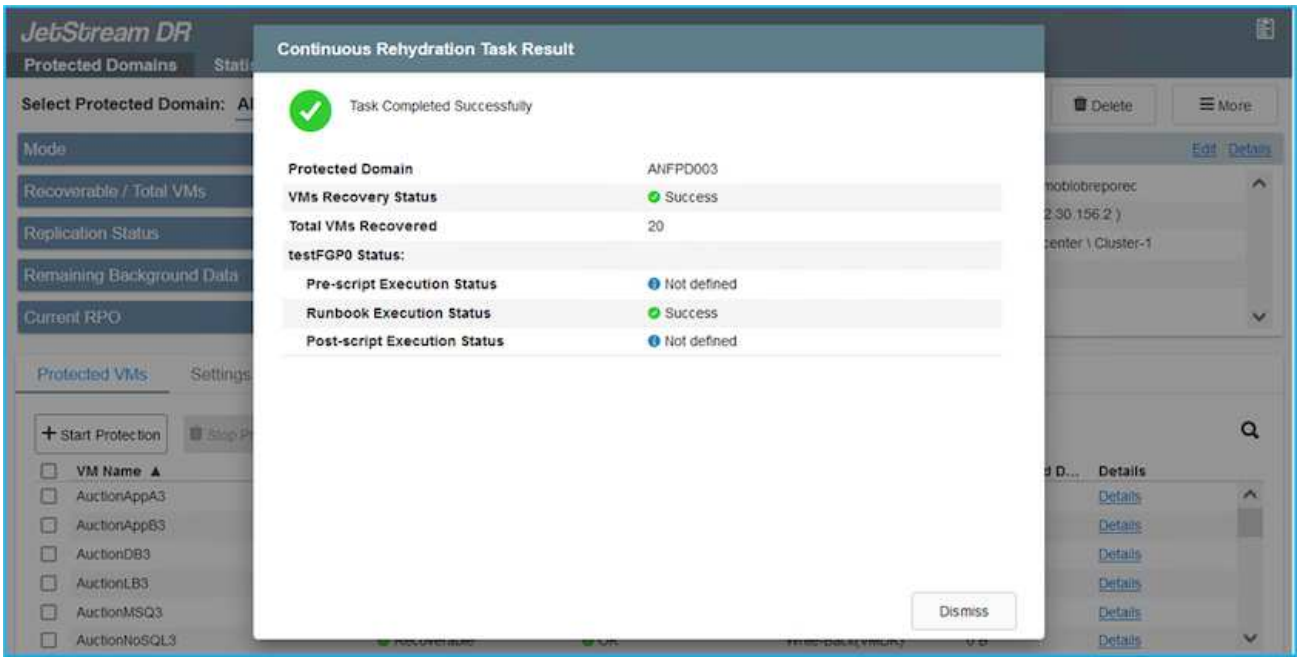
Nach dem Failover (für kontinuierliche oder standardmäßige Rehydrierung), wenn die geschützten VMs in AVS gestartet wurden, wird der Schutz automatisch fortgesetzt und JetStream DR repliziert ihre Daten weiterhin in die entsprechenden/ursprünglichen Container in Azure Blob Storage.





Die Taskleiste zeigt den Fortschritt der Failover-Aktivitäten an.

2. Wenn die Aufgabe abgeschlossen ist, greifen Sie auf die wiederhergestellten VMs zu und das Geschäft wird wie gewohnt fortgesetzt.

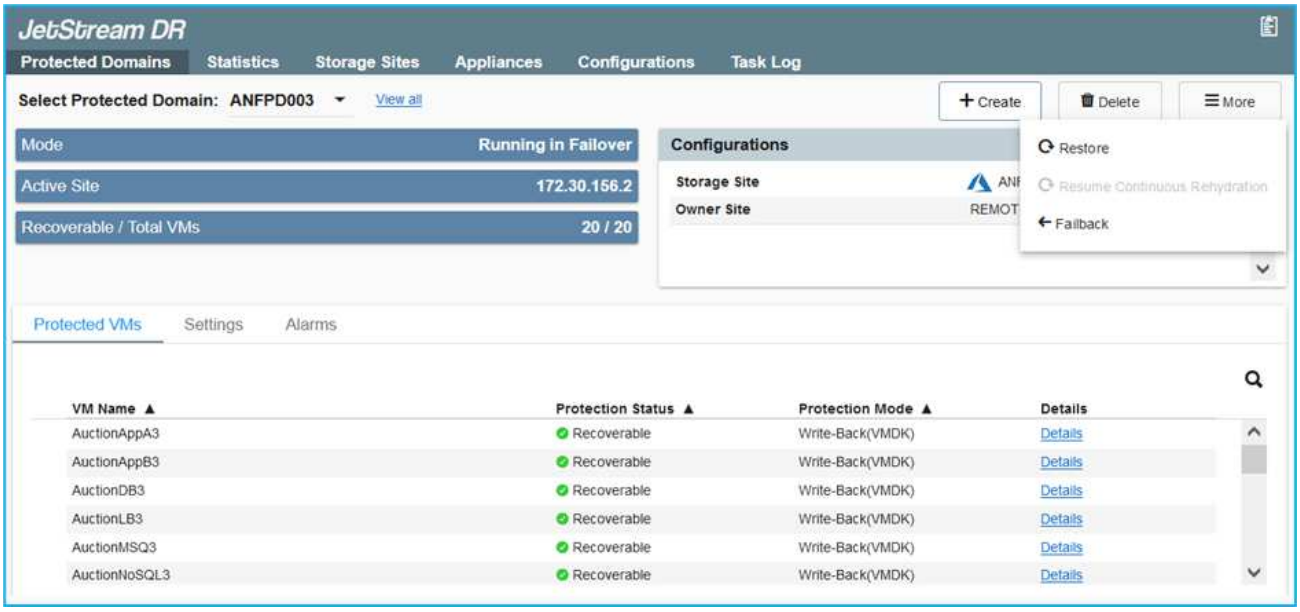


Nachdem die primäre Site wieder betriebsbereit ist, kann ein Failback durchgeführt werden. Der VM-Schutz wird fortgesetzt und die Datenkonsistenz sollte überprüft werden.

3. Stellen Sie die lokale Umgebung wieder her. Je nach Art des Katastrophenfalls kann es erforderlich sein, die Konfiguration des geschützten Clusters wiederherzustellen und/oder zu überprüfen. Gegebenenfalls muss die JetStream DR-Software neu installiert werden.

> Hinweis: Die `recovery_utility_prepare_failback` Das im Automation Toolkit bereitgestellte Skript kann verwendet werden, um die ursprünglich geschützte Site von veralteten VMs, Domäneninformationen usw. zu bereinigen.

4. Greifen Sie auf die wiederhergestellte lokale Umgebung zu, gehen Sie zur Jetstream DR-Benutzeroberfläche und wählen Sie die entsprechende geschützte Domäne aus. Nachdem die geschützte Site für das Failback bereit ist, wählen Sie die Failback-Option in der Benutzeroberfläche aus.



Der von CPT generierte Failback-Plan kann auch verwendet werden, um die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher zurück in die ursprüngliche VMware-Umgebung zu initiieren.

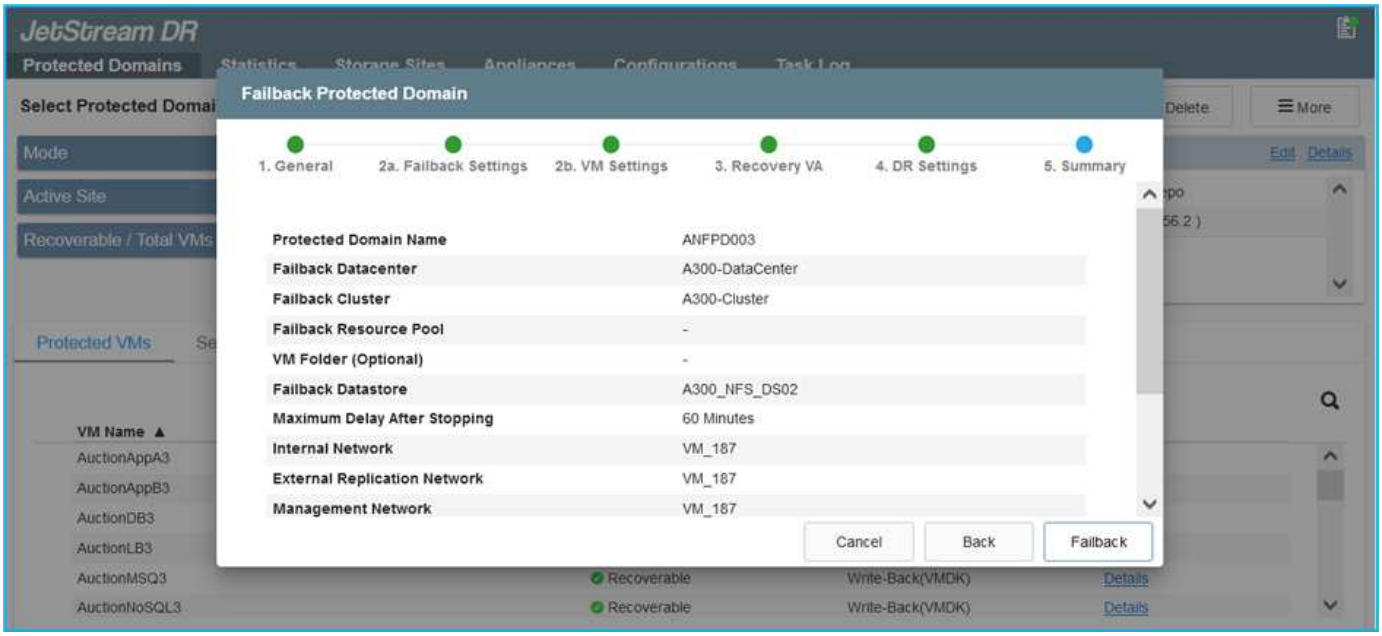
Geben Sie die maximale Verzögerung nach dem Anhalten von VMs am Wiederherstellungsstandort und dem Neustart am geschützten Standort an. Diese Zeit umfasst das Abschließen der Replikation nach dem Stoppen der Failover-VMs, die Zeit zum Bereinigen der Wiederherstellungssite und die Zeit zum Neuerstellen der VMs an der geschützten Site. 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.

Ransomware-Wiederherstellung

Die Wiederherstellung nach Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Organisationen schwierig sein, den sicheren Zeitpunkt der Rückkehr zu bestimmen und, nachdem dieser ermittelt wurde, sicherzustellen, dass wiederhergestellte Workloads vor erneuten Angriffen (durch schlafende Malware oder über anfällige Anwendungen) geschützt sind.

JetStream DR für AVS kann zusammen mit Azure NetApp Files -Datenspeichern diese Probleme lösen, indem es Unternehmen die Wiederherstellung von verfügbaren Zeitpunkten aus ermöglicht, sodass Workloads bei Bedarf in einem funktionsfähigen, isolierten Netzwerk wiederhergestellt werden. Durch die Wiederherstellung können Anwendungen weiterhin funktionieren und miteinander kommunizieren, ohne dass sie dem Nord-Süd-Verkehr ausgesetzt sind. Dadurch erhalten Sicherheitsteams einen sicheren Ort, um forensische Untersuchungen und andere notwendige Sanierungsmaßnahmen durchzuführen.



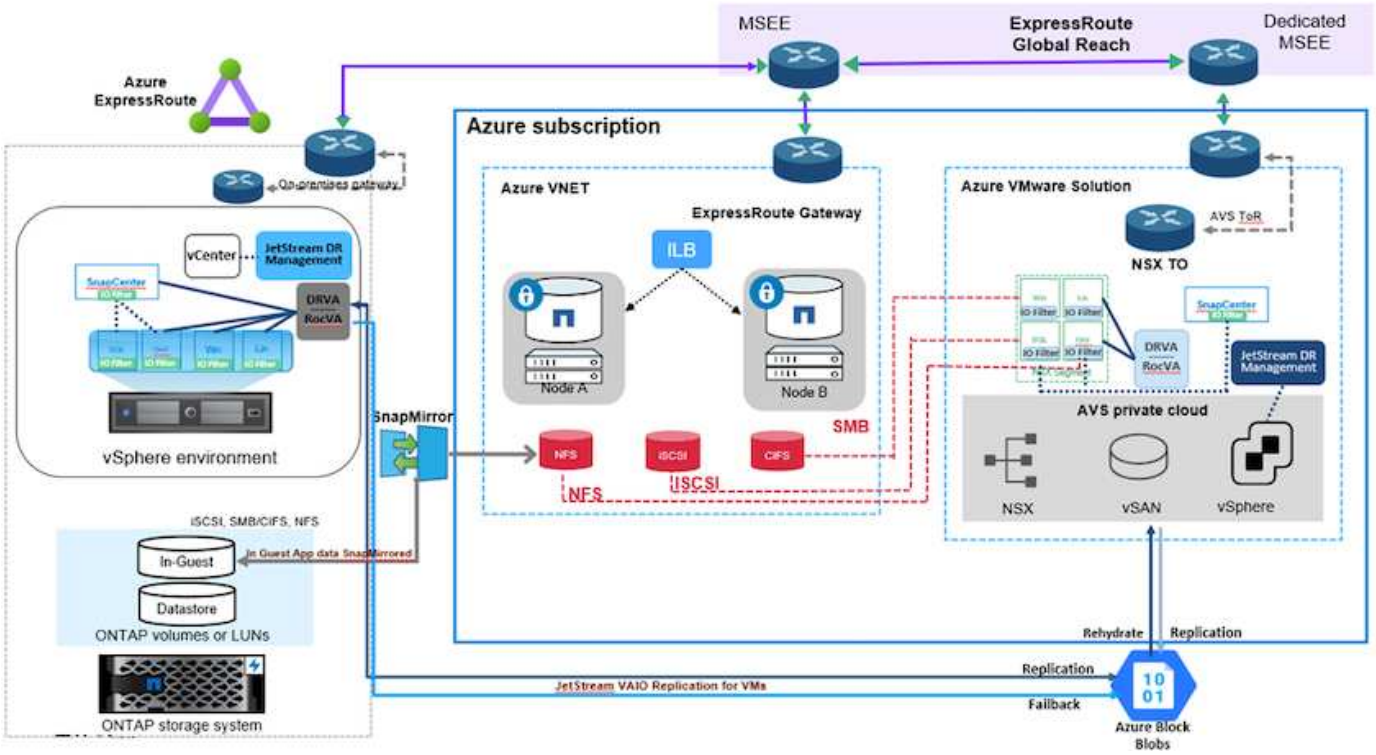
Disaster Recovery mit CVO und AVS (Gastspeicher)

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, Workloads vor Site-Ausfällen und Datenbeschädigungen wie Ransomware zu schützen. Mit NetApp SnapMirror können lokale VMware-Workloads, die über den Gast verbundenen Speicher verwenden, auf NetApp Cloud Volumes ONTAP repliziert

werden, das in Azure ausgeführt wird.

Überblick

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
Dieses Dokument bietet eine schrittweise Anleitung zum Einrichten und
Durchführen einer Notfallwiederherstellung unter Verwendung von NetApp
SnapMirror, JetStream und der Azure VMware Solution (AVS).
```



Annahmen

Dieses Dokument konzentriert sich auf die In-Guest-Speicherung für Anwendungsdaten (auch als Gastverbindung bezeichnet) und wir gehen davon aus, dass die lokale Umgebung SnapCenter für anwendungskonsistente Sicherungen verwendet.

> Dieses Dokument gilt für alle Sicherungs- oder Wiederherstellungslösungen von Drittanbietern. Befolgen Sie je nach der in der Umgebung verwendeten Lösung Best Practices, um Sicherungsrichtlinien zu erstellen, die den SLAs des Unternehmens entsprechen.

Verwenden Sie für die Konnektivität zwischen der lokalen Umgebung und dem virtuellen Azure-Netzwerk die Express Route Global Reach oder ein virtuelles WAN mit einem VPN-Gateway. Segmente sollten basierend

auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen zum Verbinden lokaler Rechenzentren mit Azure, weshalb wir in diesem Dokument keinen bestimmten Workflow beschreiben können. Informationen zur geeigneten Methode zur Konnektivität zwischen lokalen Standorten und Azure finden Sie in der Azure-Dokumentation.

Bereitstellen der DR-Lösung

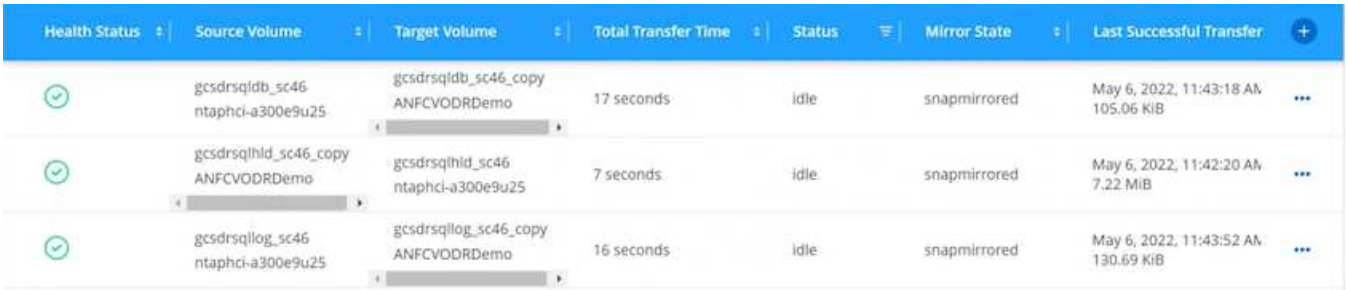
Übersicht über die Lösungsbereitstellung

1. Stellen Sie sicher, dass Anwendungsdaten mit SnapCenter unter Einhaltung der erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie Cloud Volumes ONTAP mit der richtigen Instanzgröße bereit, indem Sie den Cloud Manager innerhalb des entsprechenden Abonnements und virtuellen Netzwerks verwenden.
   a. Konfigurieren Sie SnapMirror für die relevanten Anwendungsvolumes.
   b. Aktualisieren Sie die Sicherungsrichtlinien in SnapCenter , um SnapMirror -Updates nach den geplanten Jobs auszulösen.
3. Installieren Sie die JetStream DR-Software im lokalen Rechenzentrum und starten Sie den Schutz für virtuelle Maschinen.
4. Installieren Sie die JetStream DR-Software in der privaten Azure VMware Solution-Cloud.
5. Unterbrechen Sie während eines Katastrophenfalls die SnapMirror Beziehung mithilfe von Cloud Manager und lösen Sie ein Failover virtueller Maschinen zu Azure NetApp Files oder zu vSAN-Datenspeichern am angegebenen AVS DR-Standort aus.
   a. Verbinden Sie die ISCSI-LUNs und NFS-Mounts für die Anwendungs-VMs erneut.
6. Rufen Sie ein Failback zur geschützten Site auf, indem Sie SnapMirror nach der Wiederherstellung der primären Site rückwärts neu synchronisieren.

Bereitstellungsdetails

▼ Konfigurieren Sie CVO auf Azure und replizieren Sie Volumes nach CVO

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



▼ Konfigurieren Sie AVS-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Bereitstellung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der Azure VMware-Lösung und die Dauer des Betriebs des SDDC. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann aus nur drei Hosts bestehen, bei einer vollständigen Bereitstellung kann es aber auch

ein Cluster mit mehreren Hosts sein.

Die Entscheidung zur Bereitstellung eines AVS-Clusters basiert in erster Linie auf den RPO/RTO-Anforderungen. Mit der Azure VMware-Lösung kann das SDDC rechtzeitig bereitgestellt werden, um es entweder auf Tests oder einen tatsächlichen Katastrophenfall vorzubereiten. Ein Just-in-Time bereitgestelltes SDDC spart ESXi-Hostkosten, wenn Sie nicht mit einer Katastrophe zu kämpfen haben. Diese Art der Bereitstellung beeinträchtigt die RTO jedoch um einige Stunden, während SDDC bereitgestellt wird.

Die am häufigsten eingesetzte Option besteht darin, SDDC im ständig eingeschalteten Pilotlichtmodus laufen zu lassen. Diese Option bietet einen kleinen Platzbedarf von drei Hosts, die immer verfügbar sind. Darüber hinaus beschleunigt sie die Wiederherstellungsvorgänge, indem sie eine laufende Basislinie für Simulationsaktivitäten und Konformitätsprüfungen bereitstellt und so das Risiko einer Betriebsabweichung zwischen den Produktions- und DR-Standorten vermeidet. Der Pilotlicht-Cluster kann bei Bedarf schnell auf das gewünschte Niveau hochskaliert werden, um ein tatsächliches DR-Ereignis zu bewältigen.

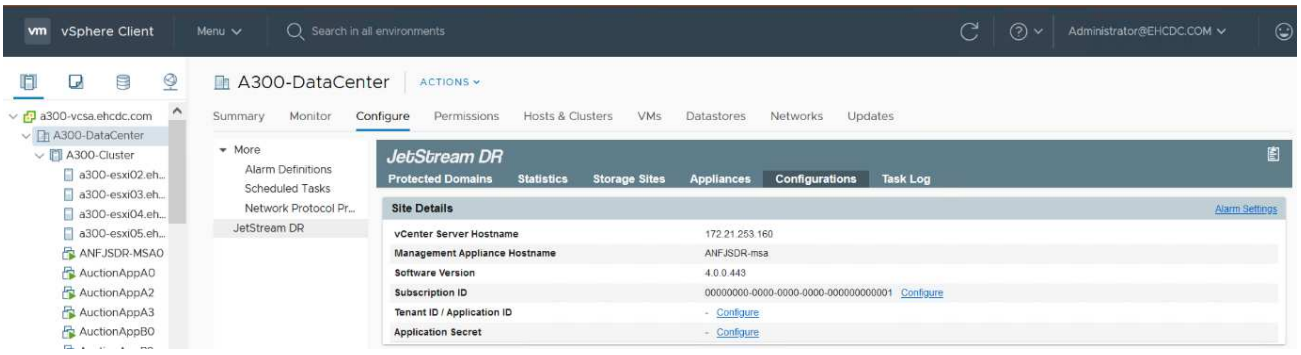
Informationen zum Konfigurieren von AVS SDDC (sei es auf Abruf oder im Pilotlichtmodus) finden Sie unter"Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf Azure" . Stellen Sie als Voraussetzung sicher, dass die auf den AVS-Hosts befindlichen Gast-VMs nach dem Herstellen der Verbindung Daten von Cloud Volumes ONTAP nutzen können.

Nachdem Cloud Volumes ONTAP und AVS ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Jetstream, um die Wiederherstellung lokaler Workloads auf AVS (VMs mit Anwendungs-VMDKs und VMs mit In-Guest-Speicher) zu automatisieren. Verwenden Sie dazu den VAIO-Mechanismus und nutzen Sie SnapMirror für Anwendungs-Volume-Kopien auf Cloud Volumes ONTAP.

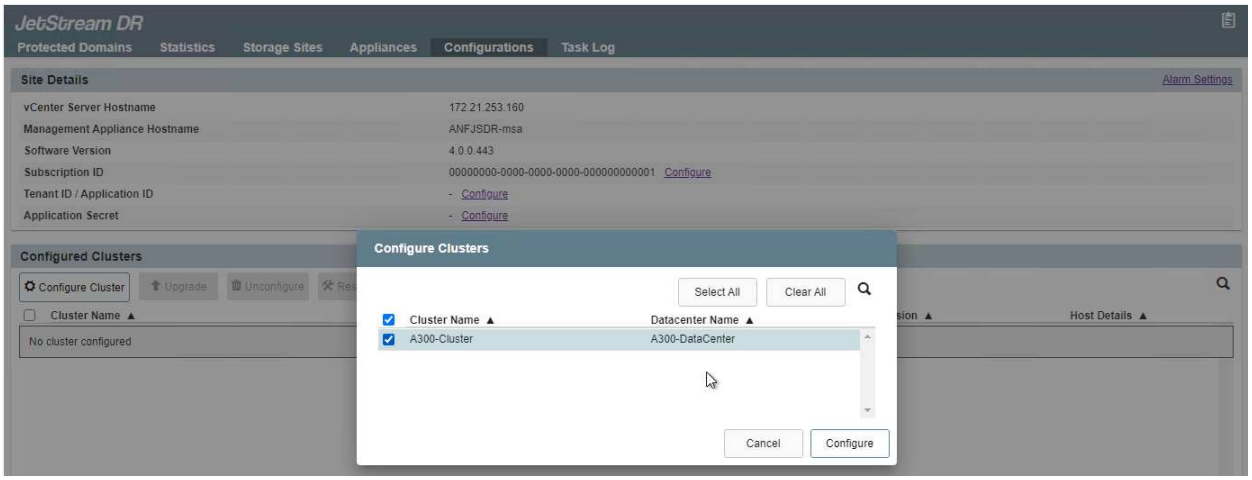
▼ Installieren Sie JetStream DR im lokalen Rechenzentrum

Die JetStream DR-Software besteht aus drei Hauptkomponenten: der JetStream DR Management Server Virtual Appliance (MSA), der DR Virtual Appliance (DRVA) und Hostkomponenten (E/A-Filterpakete). Das MSA wird verwendet, um Hostkomponenten auf dem Computercluster zu installieren und zu konfigurieren und anschließend die JetStream DR-Software zu verwalten. Der Installationsvorgang läuft wie folgt ab:

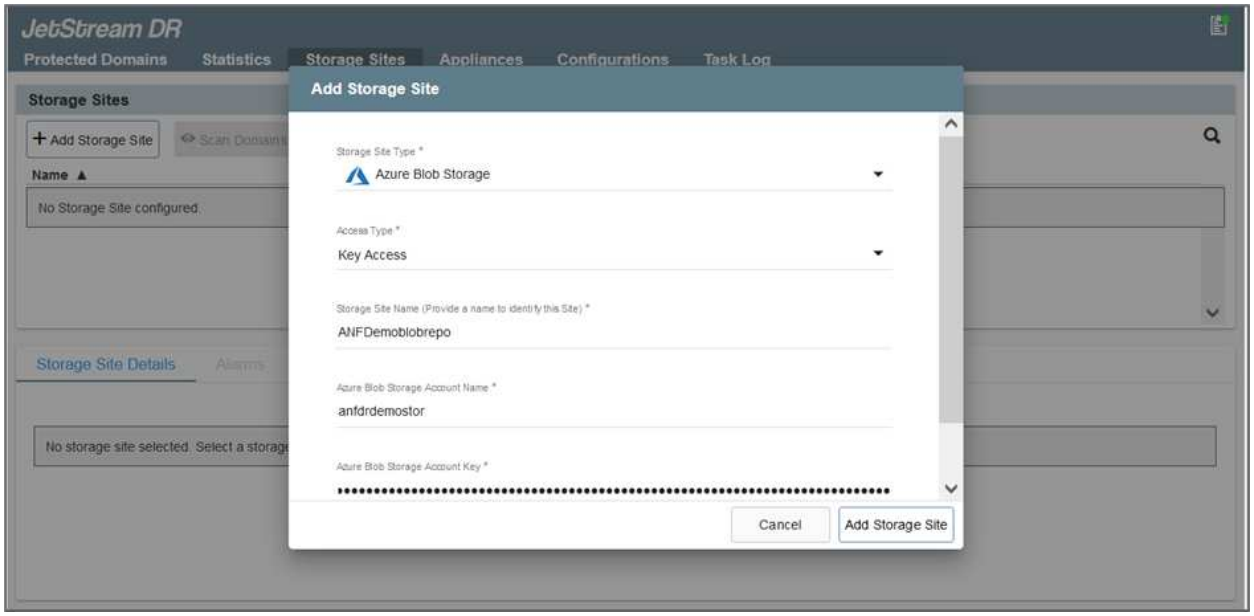
1. Prüfen Sie die Voraussetzungen.
2. Führen Sie das Kapazitätsplanungstool aus, um Empfehlungen zu Ressourcen und Konfigurationen zu erhalten.
3. Stellen Sie den JetStream DR MSA auf jedem vSphere-Host im vorgesehenen Cluster bereit.
4. Starten Sie das MSA mit seinem DNS-Namen in einem Browser.
5. Registrieren Sie den vCenter-Server beim MSA.
6. Nachdem JetStream DR MSA bereitgestellt und der vCenter Server registriert wurde, navigieren Sie mit dem vSphere Web Client zum JetStream DR-Plug-In. Dies kann durch Navigieren zu Rechenzentrum > Konfigurieren > JetStream DR erfolgen.



7. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
   a. Konfigurieren Sie den Cluster mit dem E/A-Filterpaket.



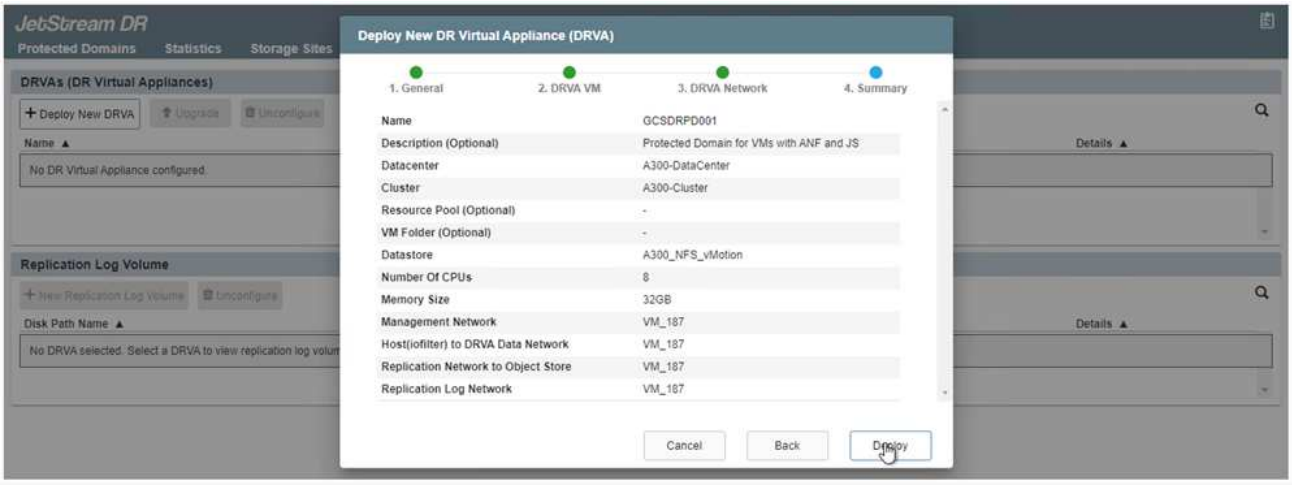
   b. Fügen Sie den Azure Blob-Speicher am Wiederherstellungsstandort hinzu.



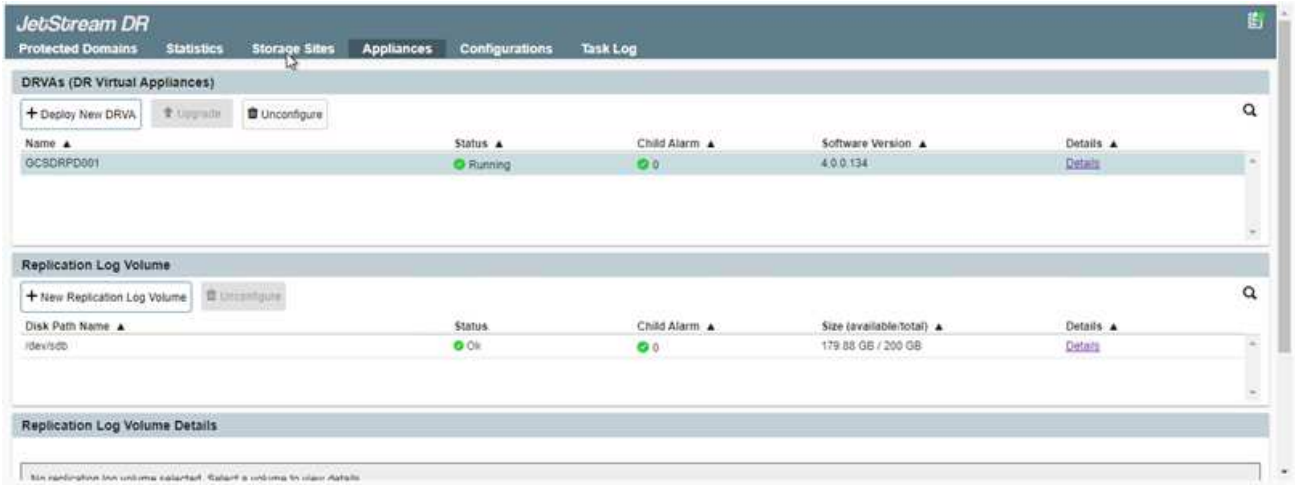
8. Stellen Sie die erforderliche Anzahl von DR Virtual Appliances (DRVAs) über die Registerkarte „Appliances“ bereit.

> Verwenden Sie das Kapazitätsplanungstool, um die Anzahl der erforderlichen DRVAs zu schätzen.

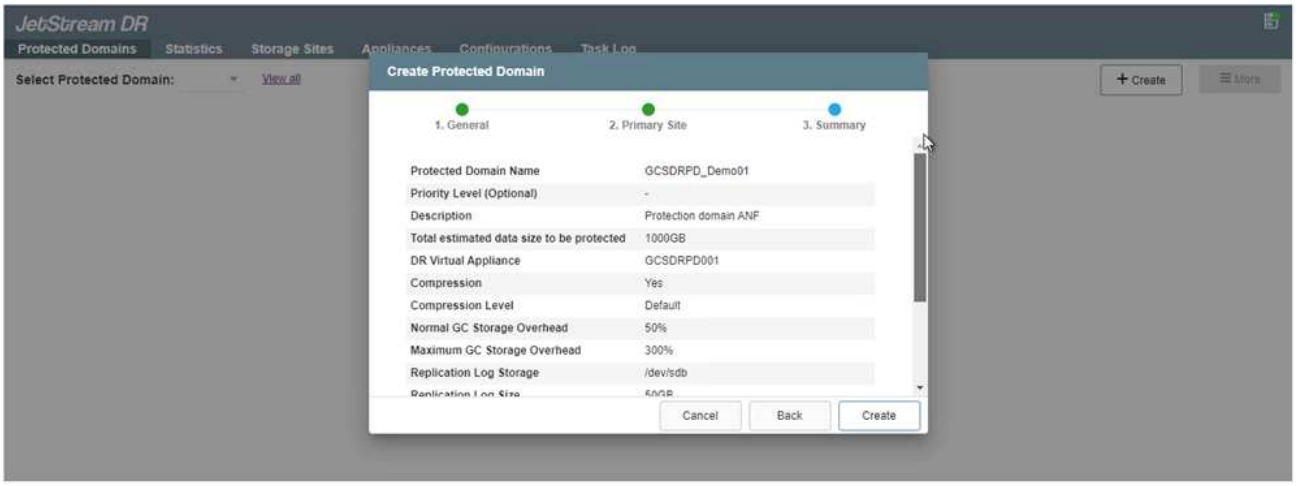


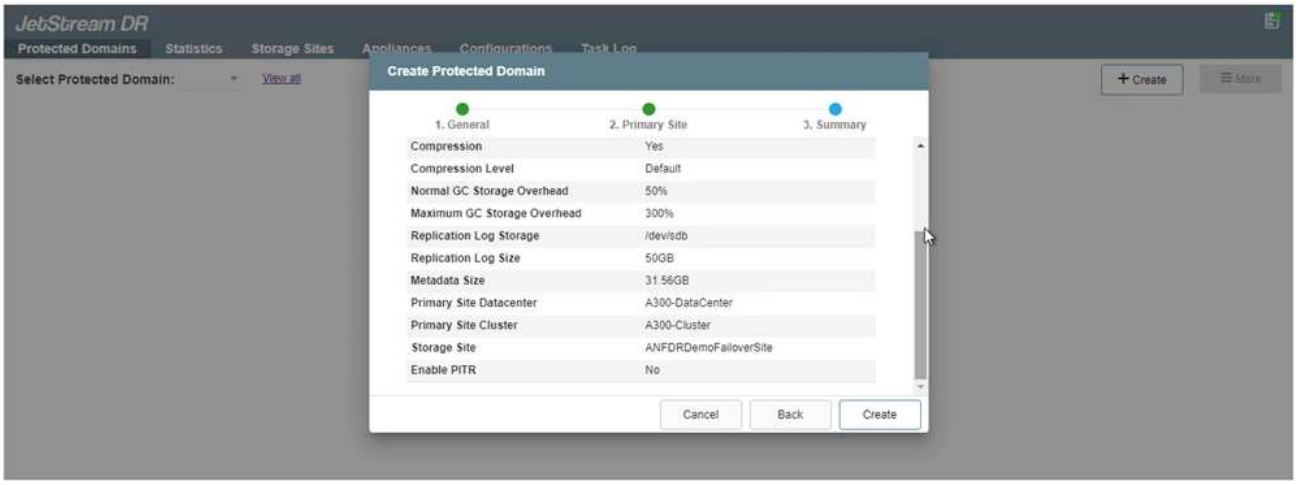


9. Erstellen Sie Replikationsprotokollvolumes für jeden DRVA mithilfe des VMDK aus den verfügbaren Datenspeichern oder dem unabhängigen gemeinsam genutzten iSCSI-Speicherpool.



10. Erstellen Sie auf der Registerkarte „Geschützte Domänen“ die erforderliche Anzahl geschützter Domänen mithilfe von Informationen zur Azure Blob Storage-Site, der DRVA-Instanz und dem Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder einen Satz von Anwendungs-VMs innerhalb des Clusters, die gemeinsam geschützt werden und denen eine Prioritätsreihenfolge für Failover-/Failback-Vorgänge zugewiesen wird.

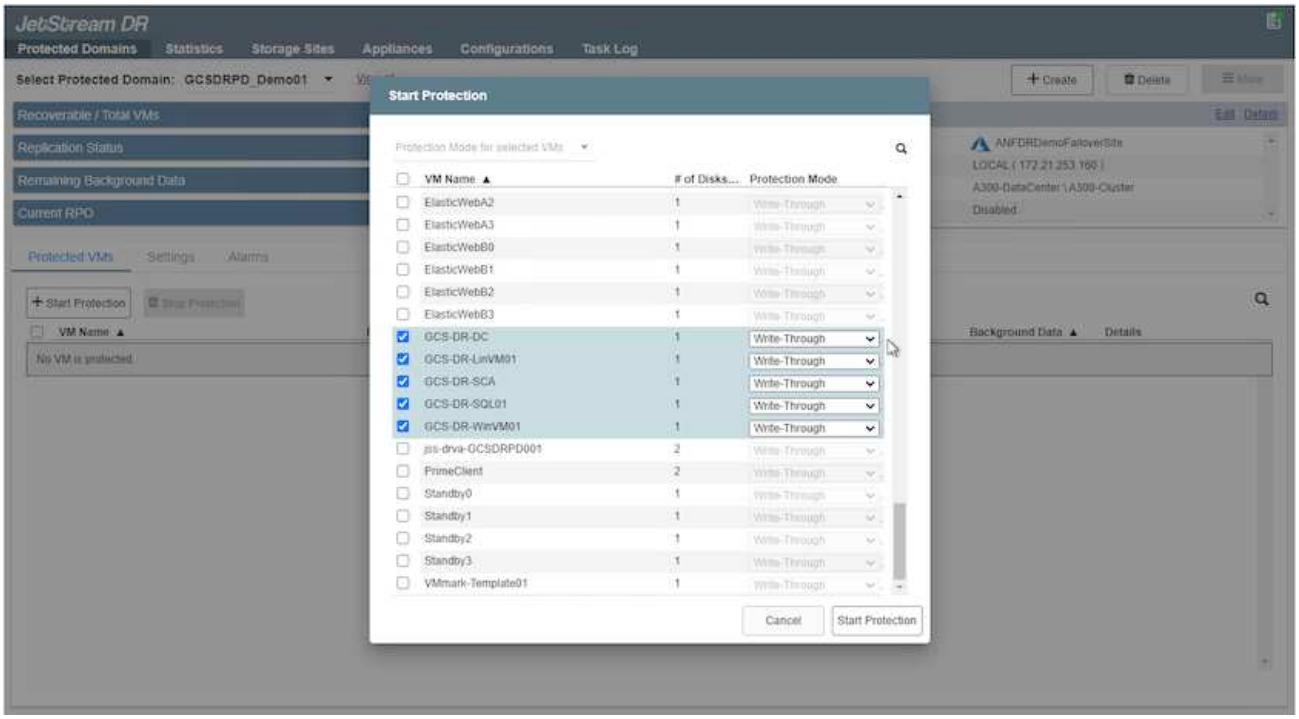




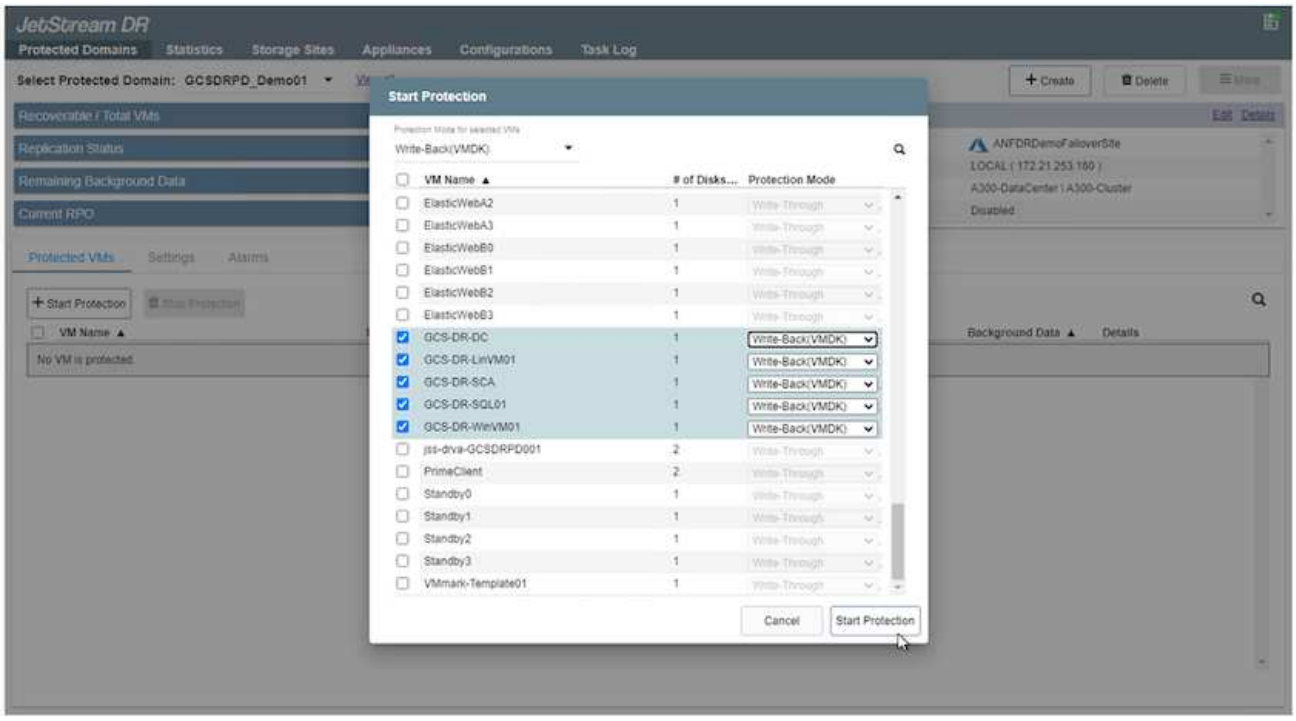
11. Wählen Sie die zu schützenden VMs aus und gruppieren Sie die VMs basierend auf der Abhängigkeit in Anwendungsgruppen. Mithilfe von Anwendungsdefinitionen können Sie VM-Sätze in logische Gruppen gruppieren, die deren Startreihenfolge, Startverzögerungen und optionale Anwendungsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

> Stellen Sie sicher, dass für alle VMs in einer geschützten Domäne derselbe Schutzmodus verwendet wird.

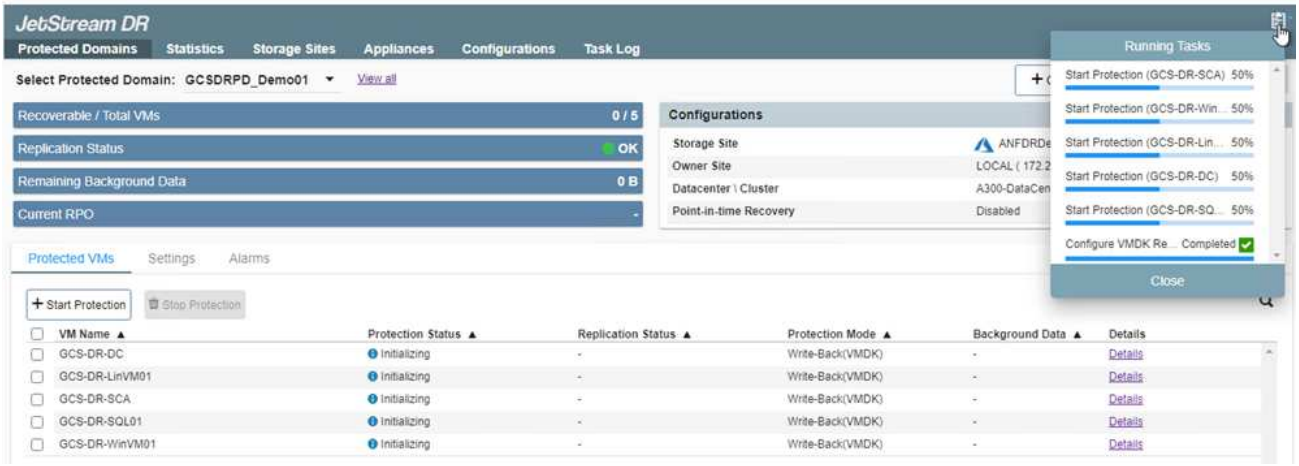
> Der Write-Back-Modus (VMDK) bietet eine höhere Leistung.



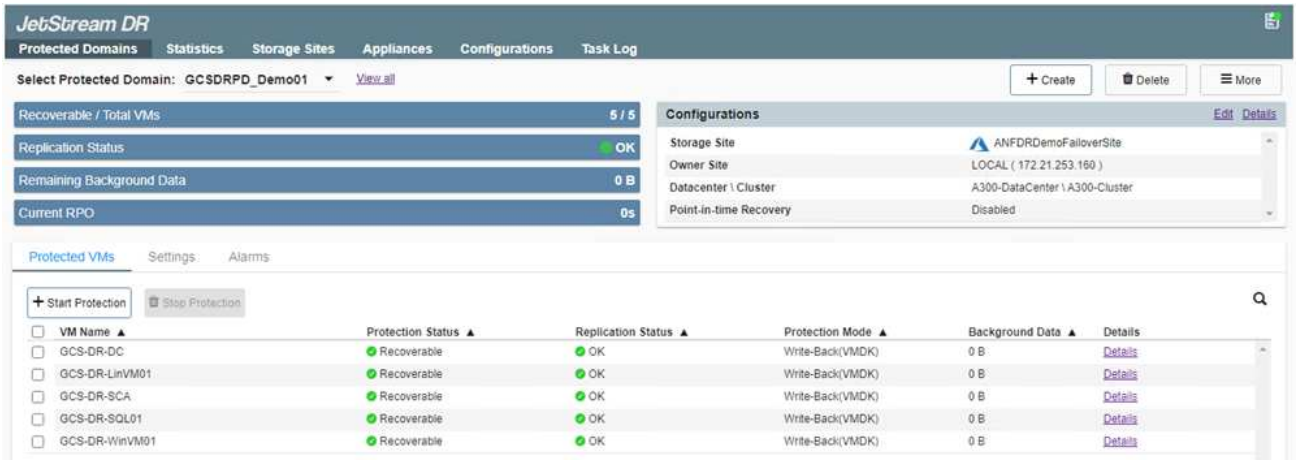
12. Stellen Sie sicher, dass Replikationsprotokollvolumes auf Hochleistungsspeichern abgelegt werden.



13. Wenn Sie fertig sind, klicken Sie auf „Schutz starten“ für die geschützte Domäne. Dadurch wird die Datenreplikation für die ausgewählten VMs in den angegebenen Blob-Speicher gestartet.



14. Nach Abschluss der Replikation wird der VM-Schutzstatus als „Wiederherstellbar“ gekennzeichnet.



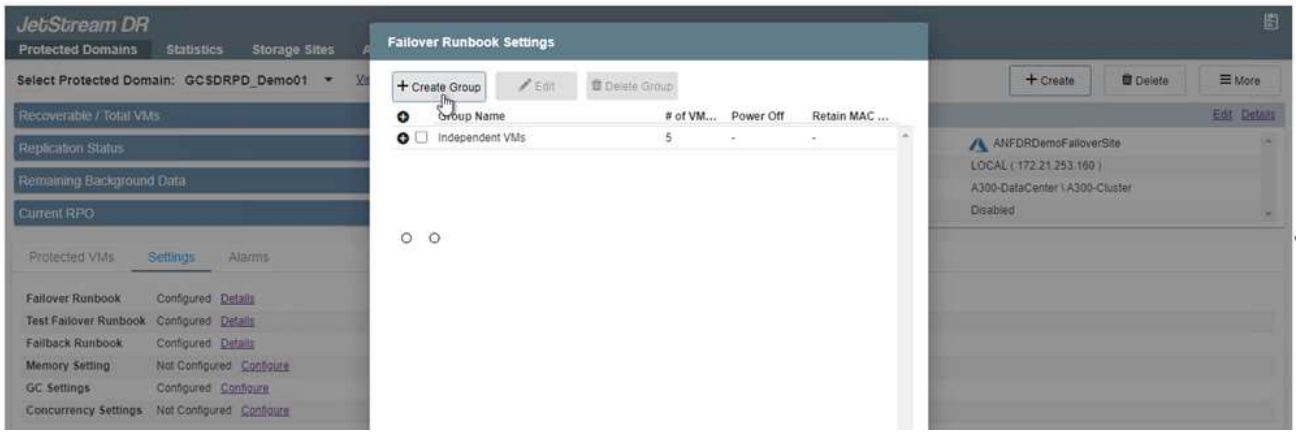
> Failover-Runbooks können so konfiguriert werden, dass sie die VMs gruppieren (eine sogenannte Wiederherstellungsgruppe), die Startreihenfolge festlegen und die CPU-/Speichereinstellungen zusammen mit den IP-Konfigurationen ändern.

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

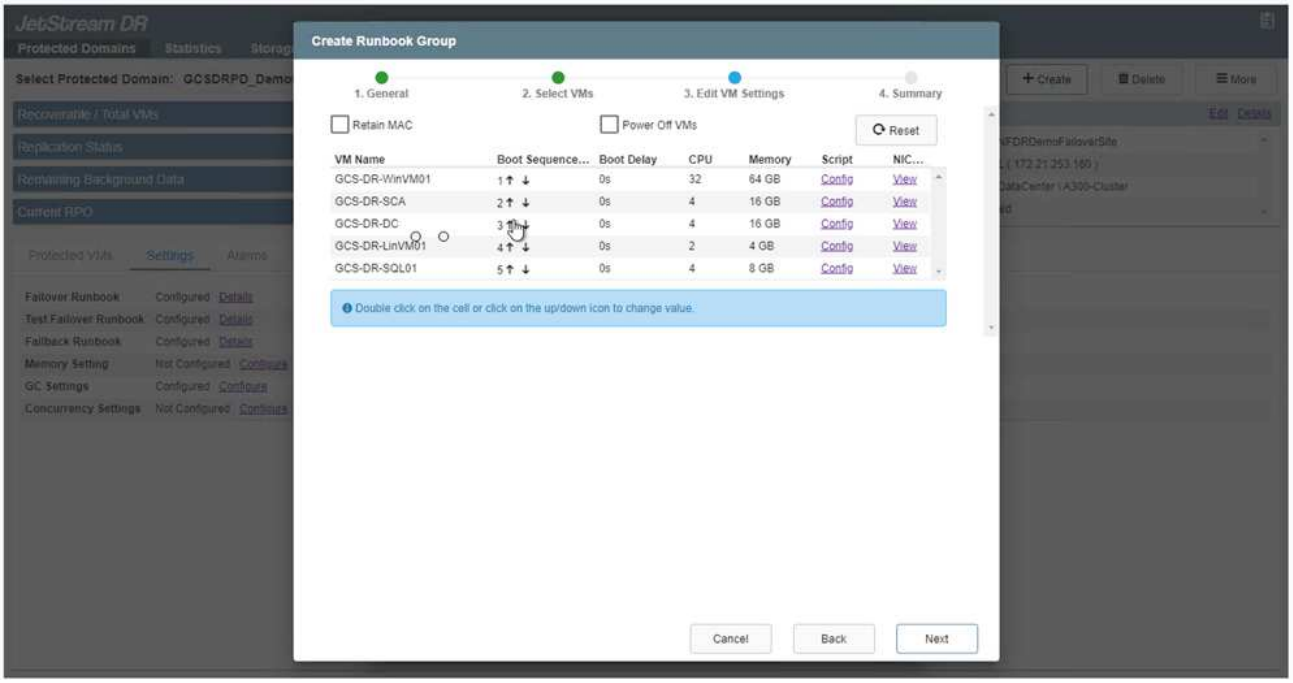


16. Klicken Sie auf die Schaltfläche „Gruppe erstellen“, um mit der Erstellung einer neuen Runbook-Gruppe zu beginnen.

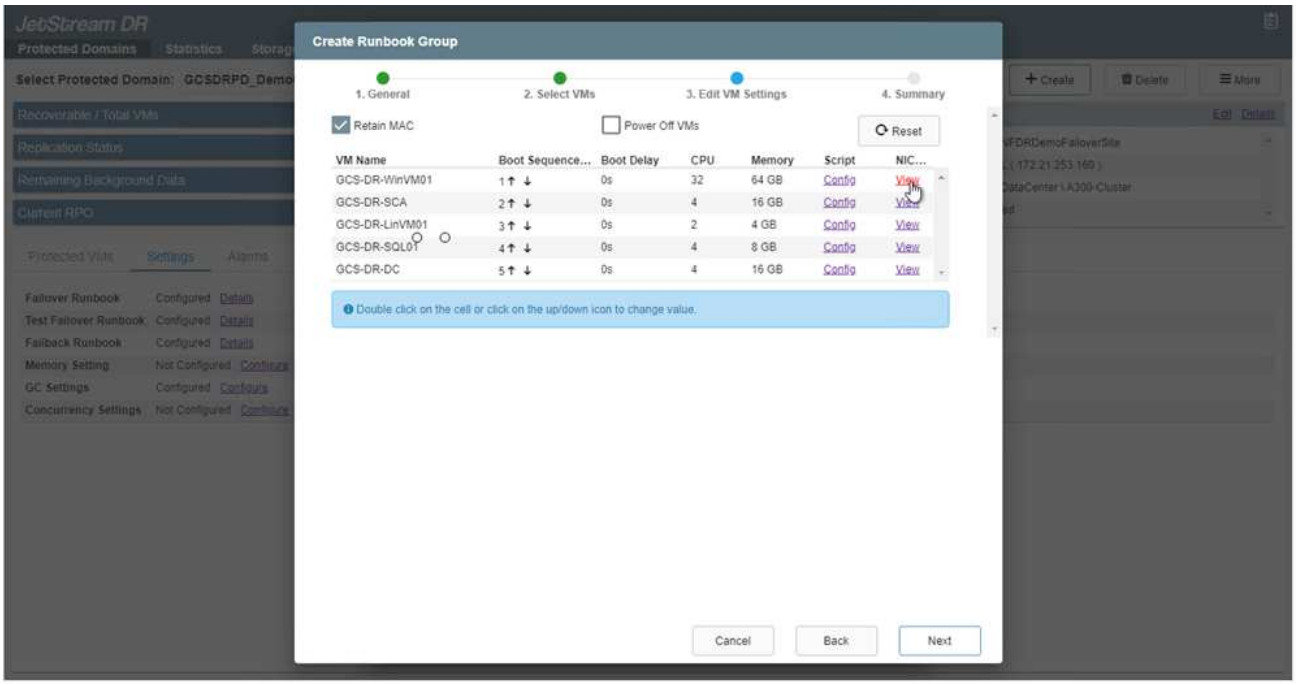
Wenden Sie bei Bedarf im unteren Teil des Bildschirms benutzerdefinierte Vor- und Nachskripte an, die vor und nach dem Betrieb der Runbook-Gruppe automatisch ausgeführt werden. Stellen Sie sicher, dass sich die Runbook-Skripte auf dem Verwaltungsserver befinden.



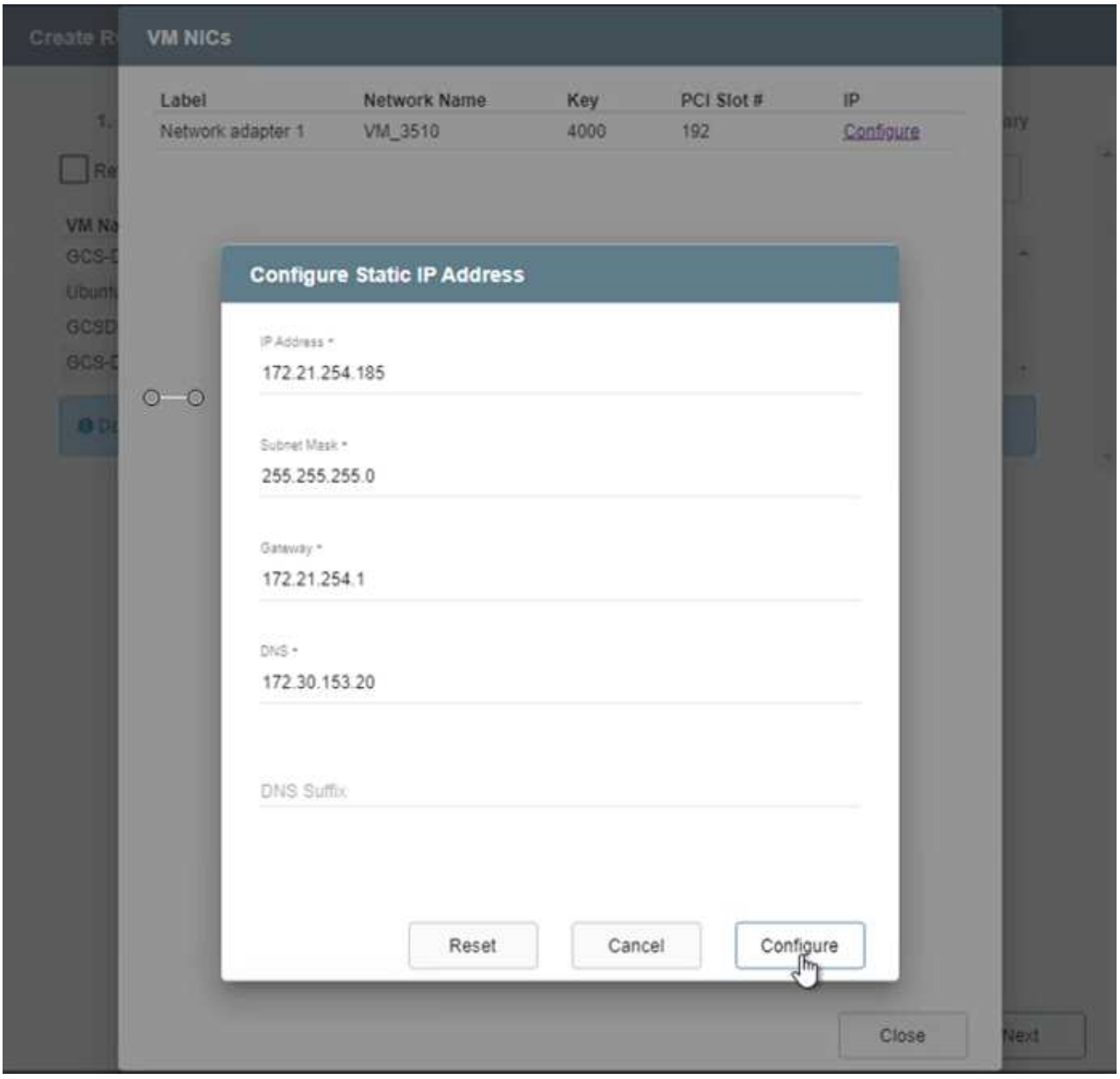
17. Bearbeiten Sie die VM-Einstellungen nach Bedarf. Geben Sie die Parameter für die Wiederherstellung der VMs an, einschließlich der Startreihenfolge, der Startverzögerung (angegeben in Sekunden), der Anzahl der CPUs und der Menge des zuzuweisenden Speichers. Ändern Sie die Startreihenfolge der VMs, indem Sie auf die Aufwärts- oder Abwärtspfeile klicken. Es werden auch Optionen zum Beibehalten des MAC bereitgestellt.

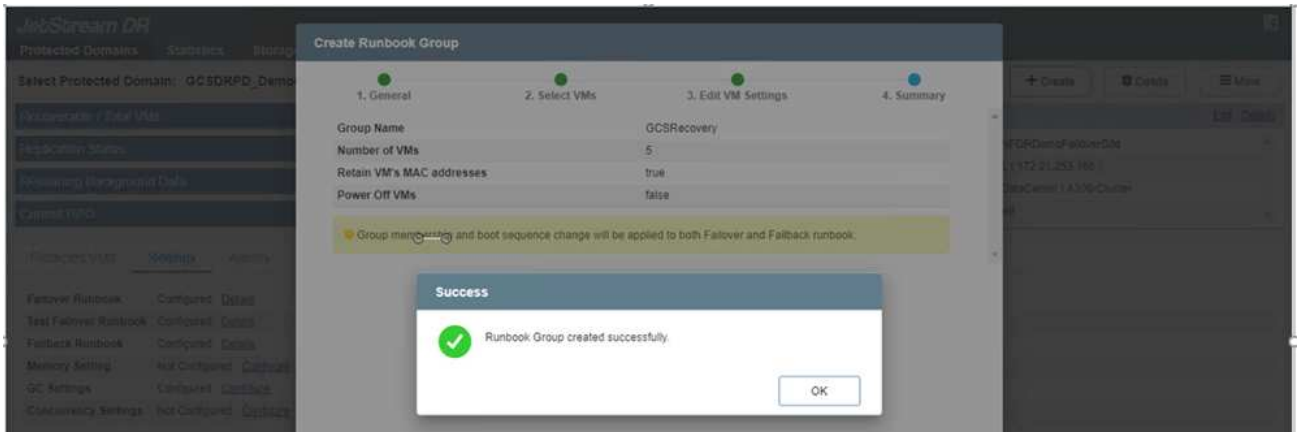


18. Für die einzelnen VMs der Gruppe können statische IP-Adressen manuell konfiguriert werden. Klicken Sie auf den Link „NIC-Ansicht“ einer VM, um ihre IP-Adresseinstellungen manuell zu konfigurieren.



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 jetzt als „Konfiguriert“ aufgeführt. Failover- und Failback-Runbookgruppen werden paarweise unter Verwendung derselben anfänglichen Gruppe von VMs und Einstellungen erstellt. Bei Bedarf können die Einstellungen jeder Runbook-Gruppe individuell angepasst werden, indem Sie auf den entsprechenden Link „Details“ klicken und Änderungen vornehmen.

▼ **Installieren Sie JetStream DR für AVS in der privaten Cloud**

Eine bewährte Methode für eine Wiederherstellungssite (AVS) besteht darin, im Voraus einen Pilot-Light-Cluster mit drei Knoten zu erstellen. Dadurch kann die Infrastruktur des Wiederherstellungsstandorts vorkonfiguriert werden, einschließlich der folgenden Punkte:

- Zielnetzwerksegmente, Firewalls, Dienste wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF-Volumes als Datenspeicher und mehr

JetStream DR unterstützt einen RTO-Modus nahezu Null für unternehmenskritische Domänen. Für diese Domänen sollte der Zielspeicher vorinstalliert sein. In diesem Fall ist ANF ein empfohlener Speichertyp.

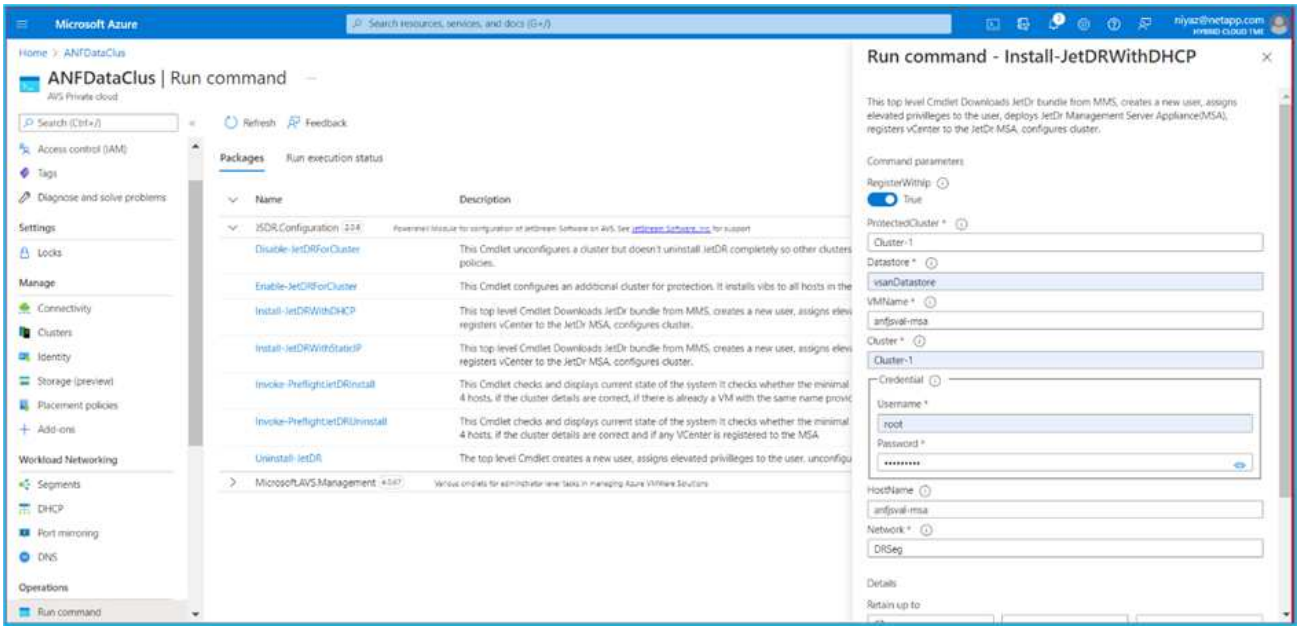
ⓘ Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster so konfiguriert werden, dass sie den lokalen Anforderungen entspricht.

ⓘ Abhängig von den SLA- und RTO-Anforderungen können Sie kontinuierliches Failover oder den regulären (Standard-)Failover-Modus verwenden. Um eine RTO von nahezu Null zu erreichen, sollten Sie am Wiederherstellungsort mit der kontinuierlichen Rehydrierung beginnen.

1. Um JetStream DR für AVS in einer privaten Azure VMware Solution-Cloud zu installieren, verwenden Sie den Befehl „Ausführen“. Gehen Sie im Azure-Portal zur Azure VMware-Lösung, wählen Sie die private Cloud aus und wählen Sie „Befehl ausführen“ > „Pakete“ > „JSDR.Configuration“.

   ⓘ Der Standard-CloudAdmin-Benutzer der Azure VMware-Lösung verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Solution ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Azure VMware Solution-Ausführungsbefehls für JetStream DR.

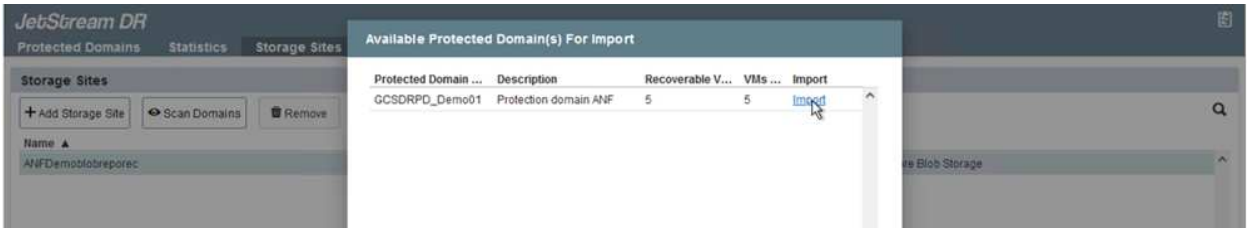
   Der folgende Screenshot zeigt die Installation mit einer DHCP-basierten IP-Adresse.



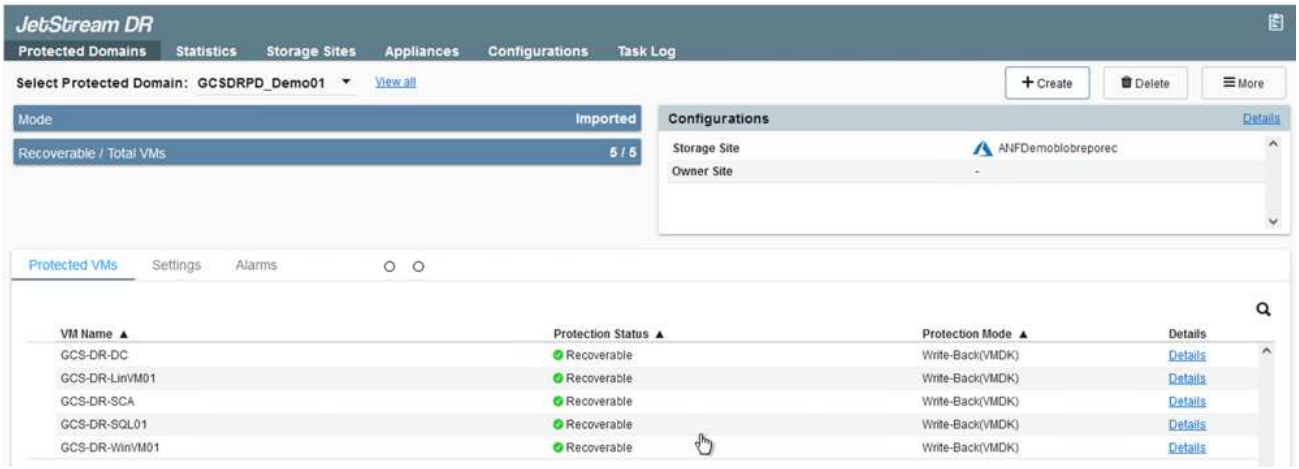
2. Aktualisieren Sie den Browser, nachdem die Installation von JetStream DR für AVS abgeschlossen ist. Um auf die JetStream DR-Benutzeroberfläche zuzugreifen, gehen Sie zu SDDC Datacenter > Konfigurieren > JetStream DR.



3. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
   a. Fügen Sie das Azure Blob Storage-Konto, das zum Schutz des lokalen Clusters verwendet wurde, als Speicherstandort hinzu und führen Sie dann die Option „Domänen scannen“ aus.
   b. Wählen Sie im angezeigten Popup-Dialogfenster die zu importierende geschützte Domäne aus und klicken Sie dann auf den Link „Importieren“.



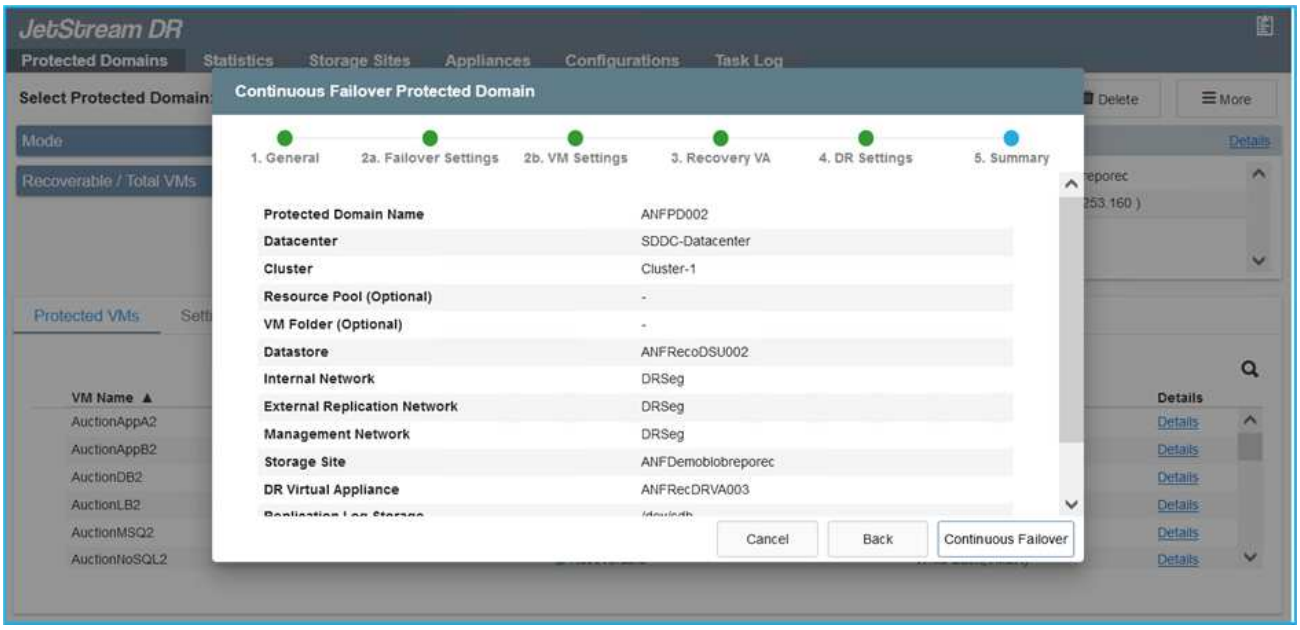
4. Die Domäne wird zur Wiederherstellung importiert. Gehen Sie zur Registerkarte „Geschützte Domänen“ und überprüfen Sie, ob die gewünschte Domäne ausgewählt wurde, oder wählen Sie die gewünschte Domäne aus dem Menü „Geschützte Domäne auswählen“ aus. Es wird eine Liste der wiederherstellbaren VMs in der geschützten Domäne angezeigt.



5. Nachdem die geschützten Domänen importiert wurden, stellen Sie DRVA-Geräte bereit.

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

6. Erstellen Sie Replikationsprotokollvolumes mithilfe verfügbarer vSAN- oder ANF-Datenspeicher.
7. Importieren Sie die geschützten Domänen und konfigurieren Sie die Wiederherstellungs-VA so, dass ein ANF-Datenspeicher für VM-Platzierungen verwendet wird.

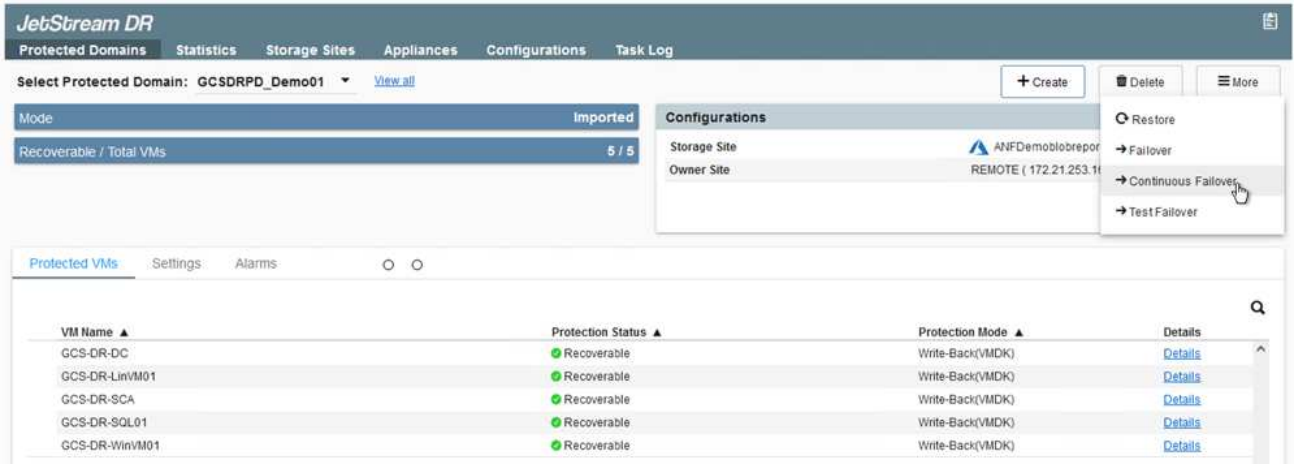


Stellen Sie sicher, dass DHCP im ausgewählten Segment aktiviert ist und genügend IPs verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen wiederhergestellt werden. Jede wiederherzustellende VM (einschließlich kontinuierlicher Rehydration) erfordert eine individuelle dynamische IP. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

8. Wählen Sie die entsprechende Failover-Option (kontinuierliches Failover oder Failover). In diesem Beispiel wird die kontinuierliche Rehydration (kontinuierliches Failover) ausgewählt.

Obwohl sich die Modi „Continuous Failover“ und „Failover“ hinsichtlich des Zeitpunkts der Konfiguration unterscheiden, werden beide Failover-Modi mit denselben Schritten

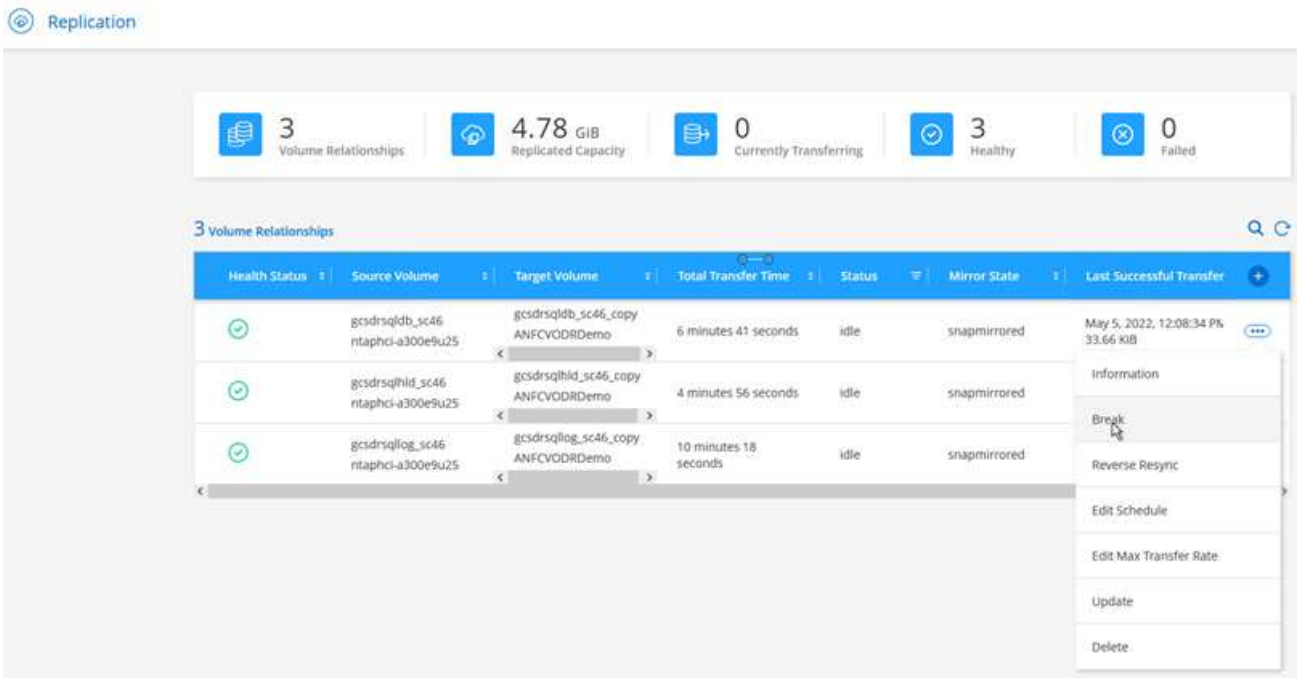
konfiguriert. Als Reaktion auf ein Katastrophenereignis werden Failover-Schritte konfiguriert und gemeinsam ausgeführt. Ein kontinuierliches Failover kann jederzeit konfiguriert und dann während des normalen Systembetriebs im Hintergrund ausgeführt werden. Nach dem Auftreten eines Katastrophenereignisses wird ein kontinuierliches Failover durchgeführt, um den Besitz der geschützten VMs sofort auf den Wiederherstellungsstandort zu übertragen (RTO nahe Null).

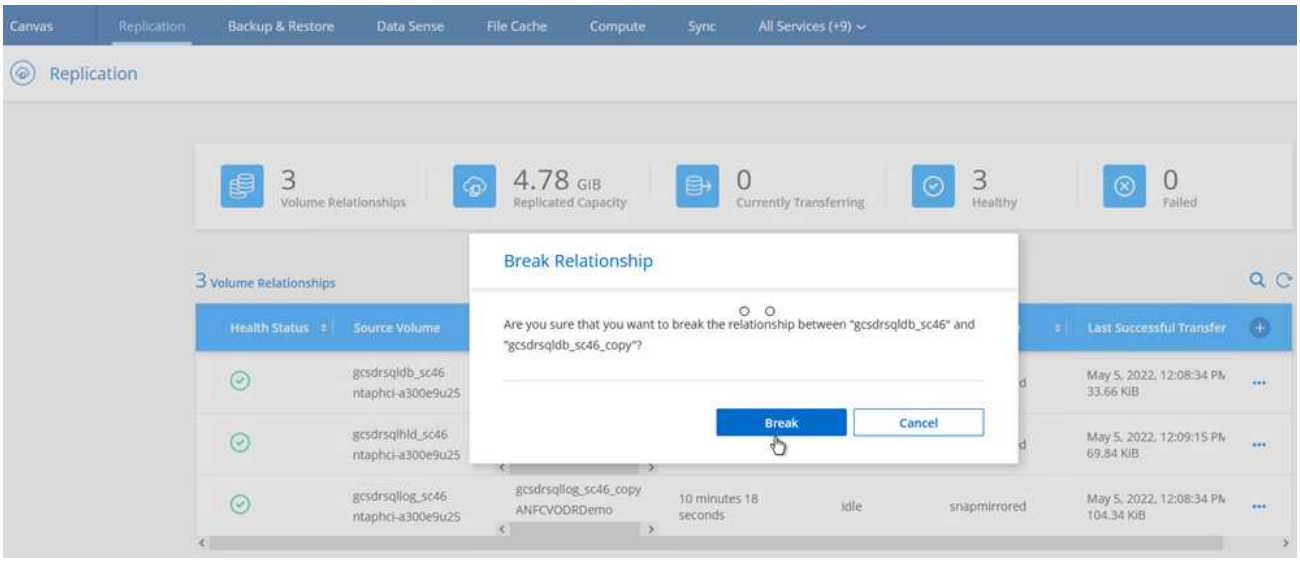


Der kontinuierliche Failover-Prozess beginnt und sein Fortschritt kann über die Benutzeroberfläche überwacht werden. Wenn Sie im Abschnitt „Aktueller Schritt“ auf das blaue Symbol klicken, wird ein Popup-Fenster mit Details zum aktuellen Schritt des Failover-Prozesses angezeigt.

▼ **Failover und Failback**

1. Nach einem Desaster im geschützten Cluster der On-Premises-Umgebung (Teil- oder Komplettausfall) können Sie nach Aufhebung der SnapMirror -Beziehung für die jeweiligen Anwendungsvolumes das Failover für VMs mit Jetstream auslösen.

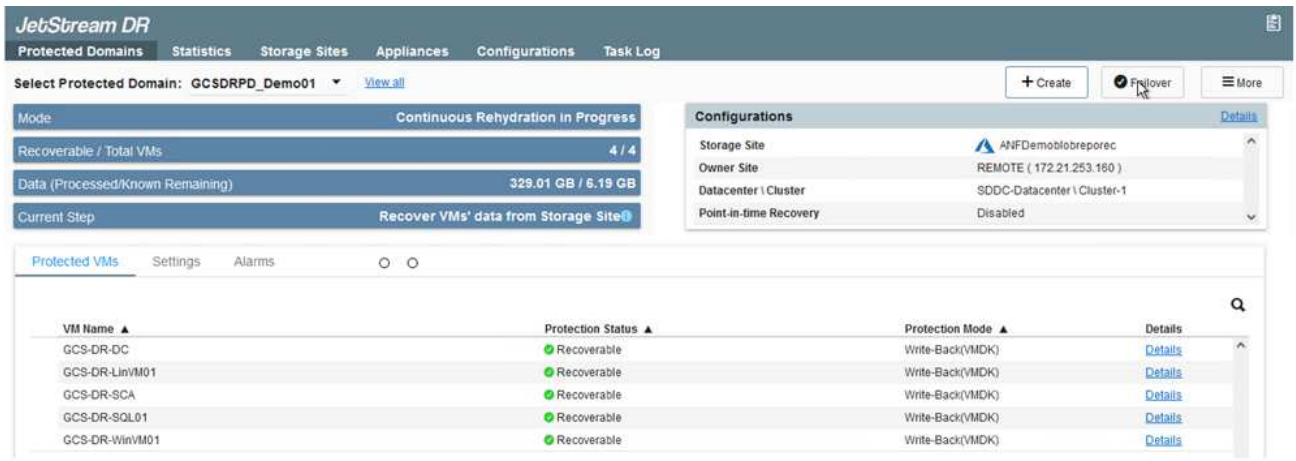


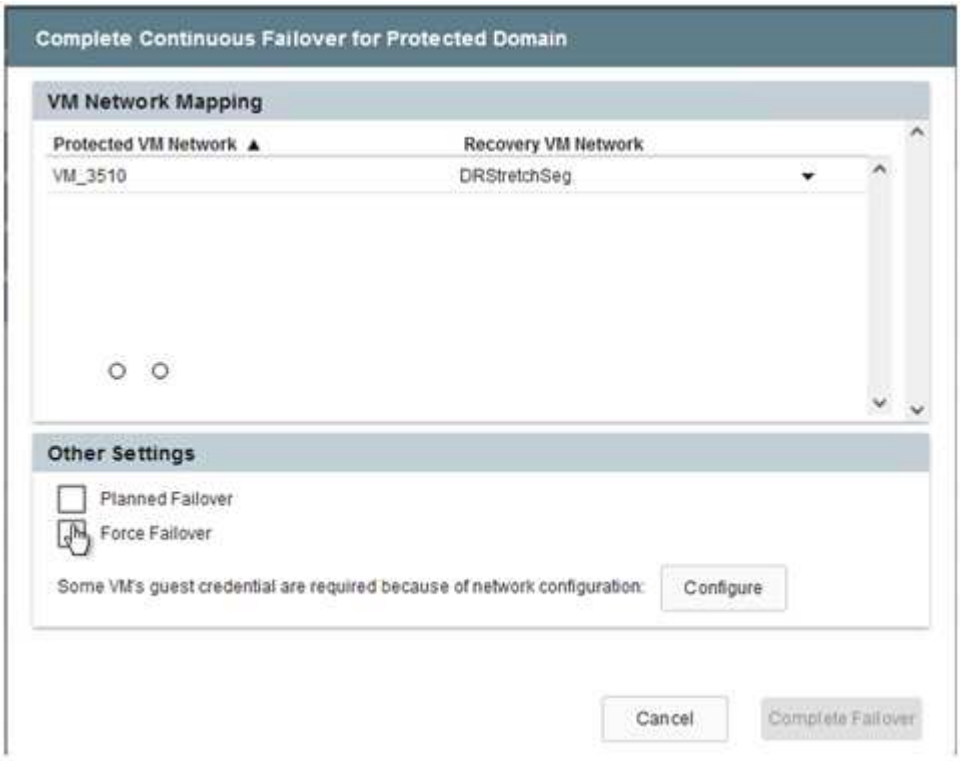


Dieser Schritt kann leicht automatisiert werden, um den Wiederherstellungsprozess zu erleichtern.

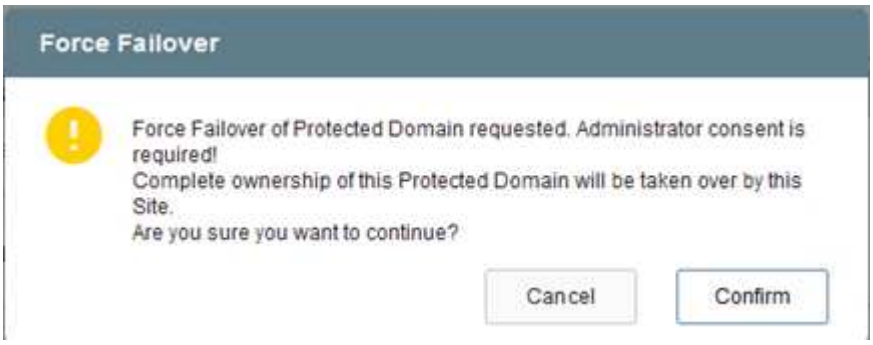
2. Greifen Sie auf die Jetstream-Benutzeroberfläche auf AVS SDDC (Zielseite) zu und lösen Sie die Failover-Option aus, um das Failover abzuschließen. Die Taskleiste zeigt den Fortschritt der Failover-Aktivitäten an.

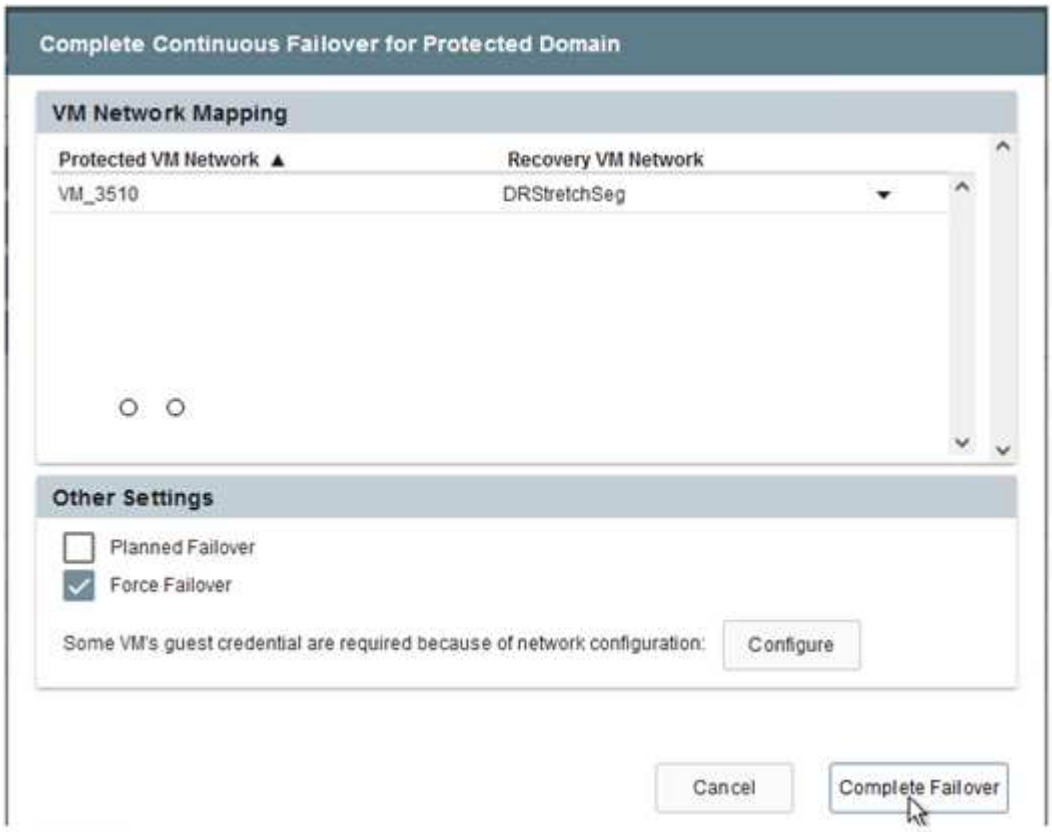
   Im Dialogfenster, das nach Abschluss des Failovers angezeigt wird, kann die Failover-Aufgabe als geplant angegeben oder als erzwungen angenommen werden.





Beim erzwungenen Failover wird davon ausgegangen, dass auf den primären Standort nicht mehr zugegriffen werden kann und der Besitz der geschützten Domäne direkt vom Wiederherstellungsstandort übernommen werden sollte.





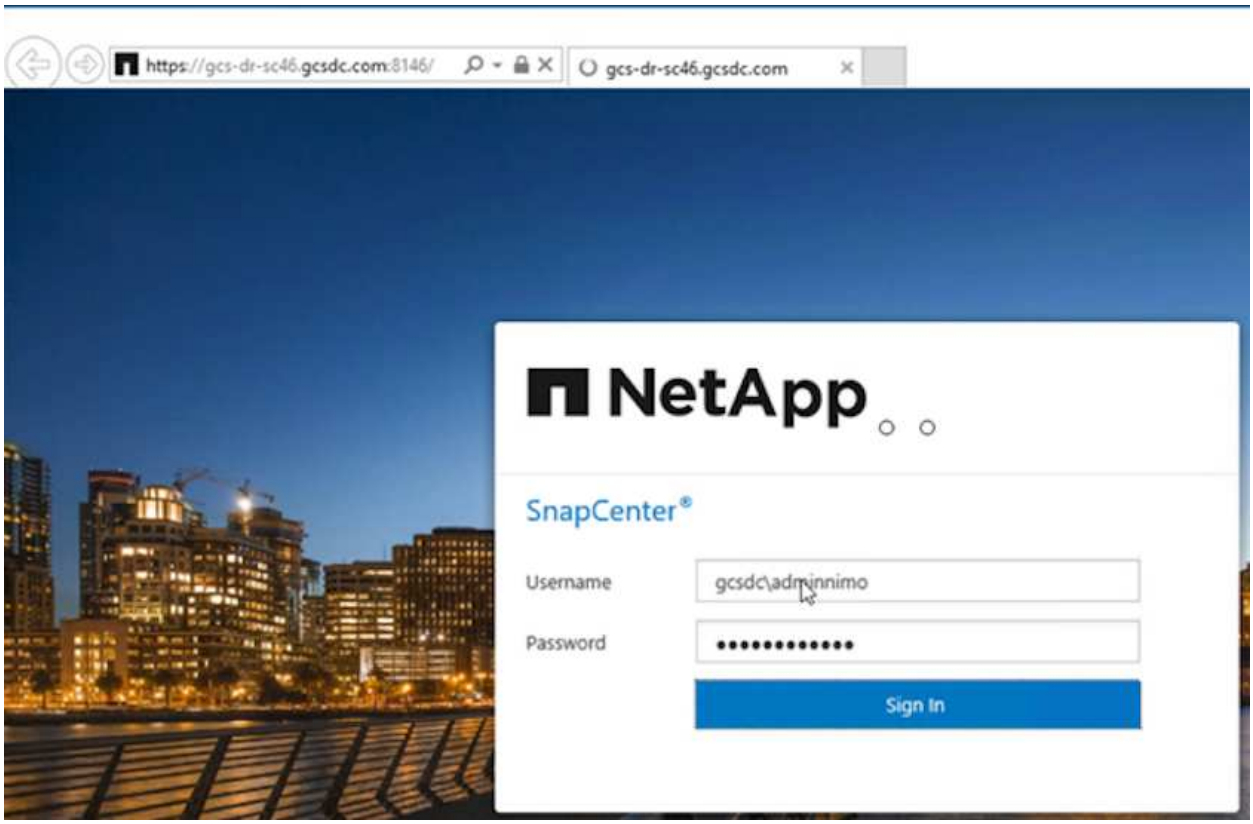
3. Nach Abschluss des kontinuierlichen Failovers wird eine Meldung angezeigt, die den Abschluss der Aufgabe bestätigt. Wenn die Aufgabe abgeschlossen ist, greifen Sie auf die wiederhergestellten VMs zu, um ISCSI- oder NFS-Sitzungen zu konfigurieren.

Der Failover-Modus ändert sich in „Wird im Failover ausgeführt“ und der VM-Status ist „Wiederherstellbar“. Alle VMs der geschützten Domäne werden jetzt am Wiederherstellungsstandort in dem durch die Failover-Runbook-Einstellungen angegebenen Zustand ausgeführt.

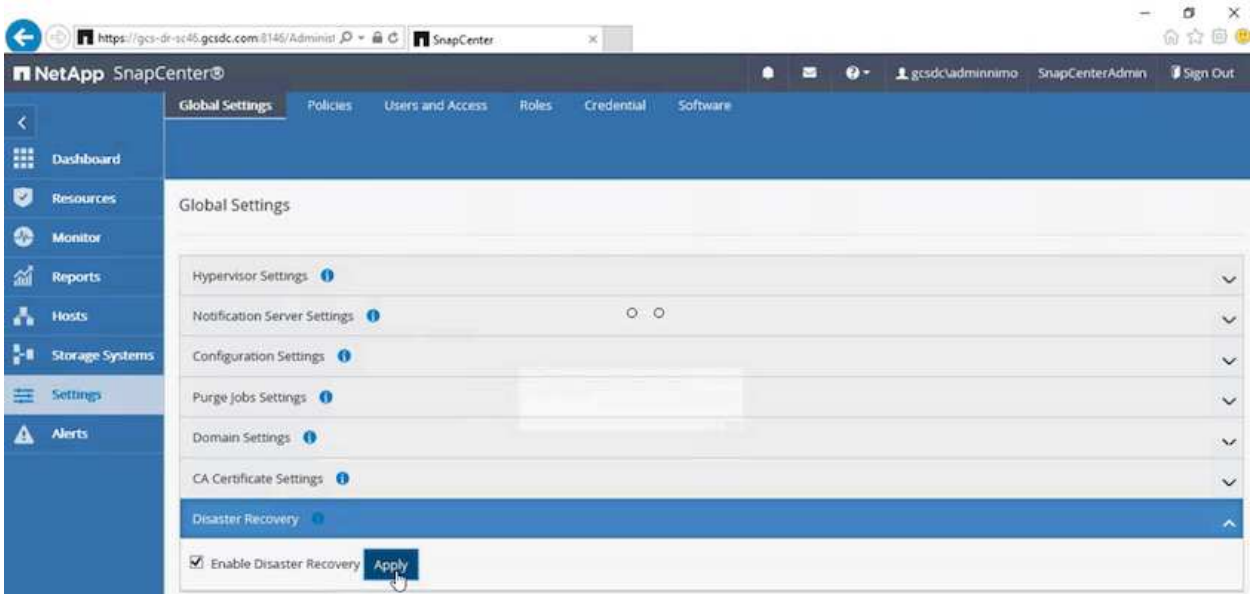
Um die Failover-Konfiguration und -Infrastruktur zu überprüfen, kann JetStream DR im Testmodus (Option „Test-Failover“) betrieben werden, um die Wiederherstellung virtueller Maschinen und ihrer Daten aus dem Objektspeicher in eine Testwiederherstellungsumgebung zu beobachten. Wenn ein Failover-Verfahren im Testmodus ausgeführt wird, ähnelt sein Ablauf einem tatsächlichen Failover-Prozess.



4. Nachdem die virtuellen Maschinen wiederhergestellt wurden, verwenden Sie die Speicher-Notfallwiederherstellung für den In-Guest-Speicher. Um diesen Prozess zu demonstrieren, wird in diesem Beispiel ein SQL-Server verwendet.
5. Melden Sie sich bei der wiederhergestellten SnapCenter VM auf AVS SDDC an und aktivieren Sie den DR-Modus.
   a. Greifen Sie über den Browser auf die SnapCenter -Benutzeroberfläche zu.



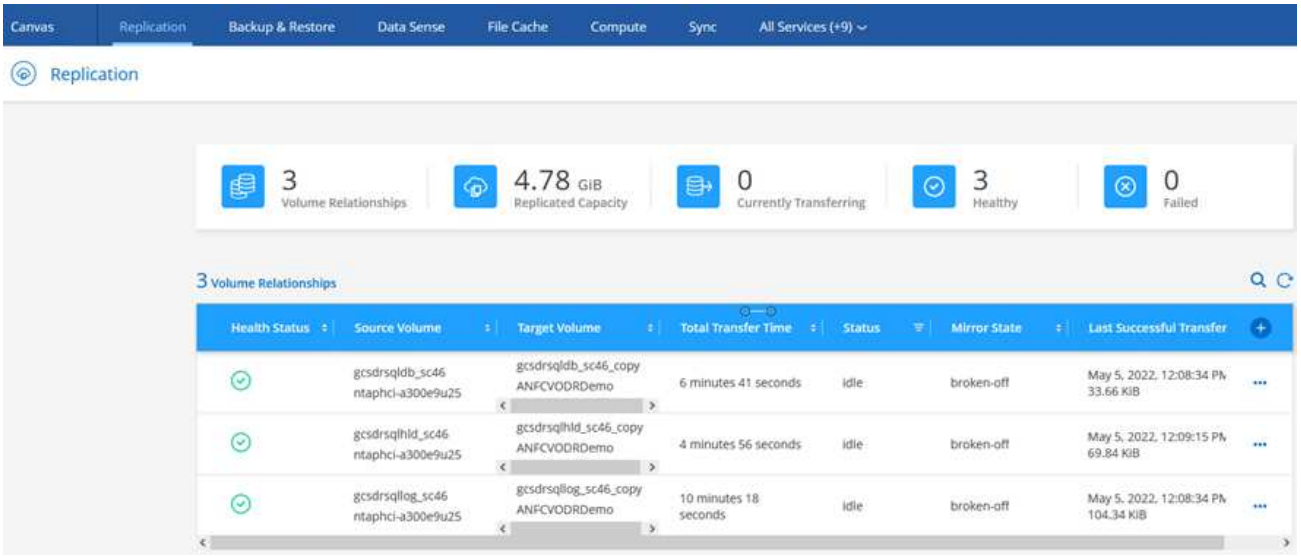
   b. Navigieren Sie auf der Seite „Einstellungen“ zu „Einstellungen > Globale Einstellungen > Notfallwiederherstellung“.
   c. Wählen Sie „Notfallwiederherstellung aktivieren“ aus.
   d. Klicken Sie auf „Übernehmen“.



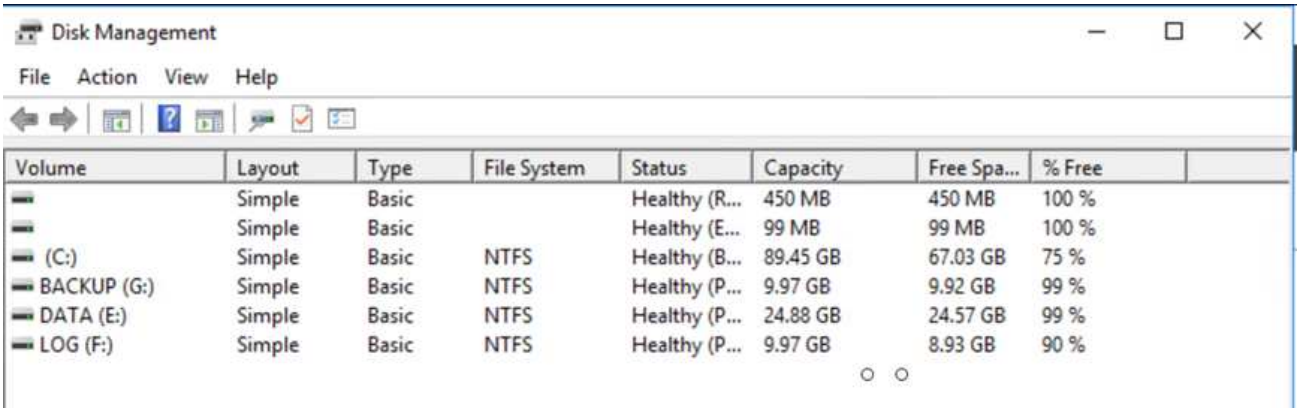
e. Überprüfen Sie, ob der DR-Job aktiviert ist, indem Sie auf Überwachen > Jobs klicken.

> Für die Speicher-Notfallwiederherstellung sollte NetApp SnapCenter 4.6 oder höher verwendet werden. Für frühere Versionen sollten anwendungskonsistente Snapshots (mit SnapMirror repliziert) verwendet und eine manuelle Wiederherstellung durchgeführt werden, falls frühere Sicherungen am Notfallwiederherstellungsstandort wiederhergestellt werden müssen.

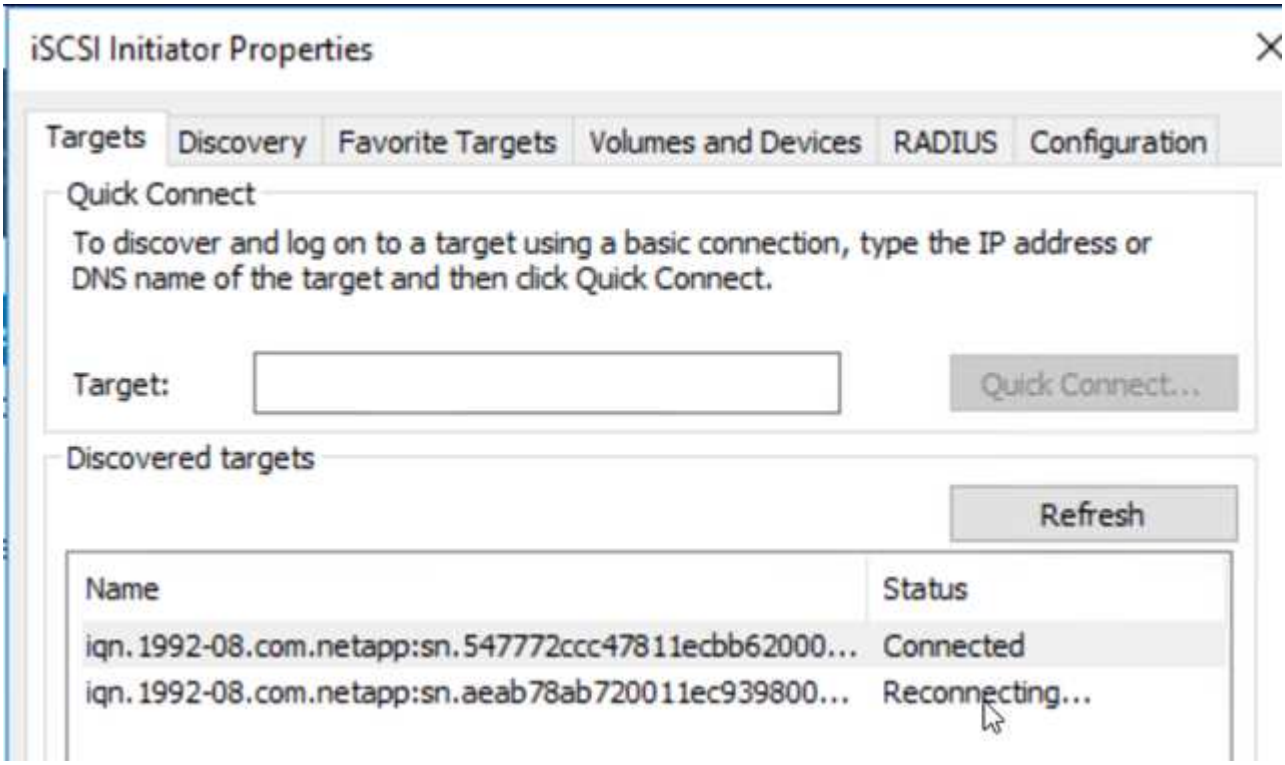
6. Stellen Sie sicher, dass die SnapMirror -Beziehung unterbrochen ist.



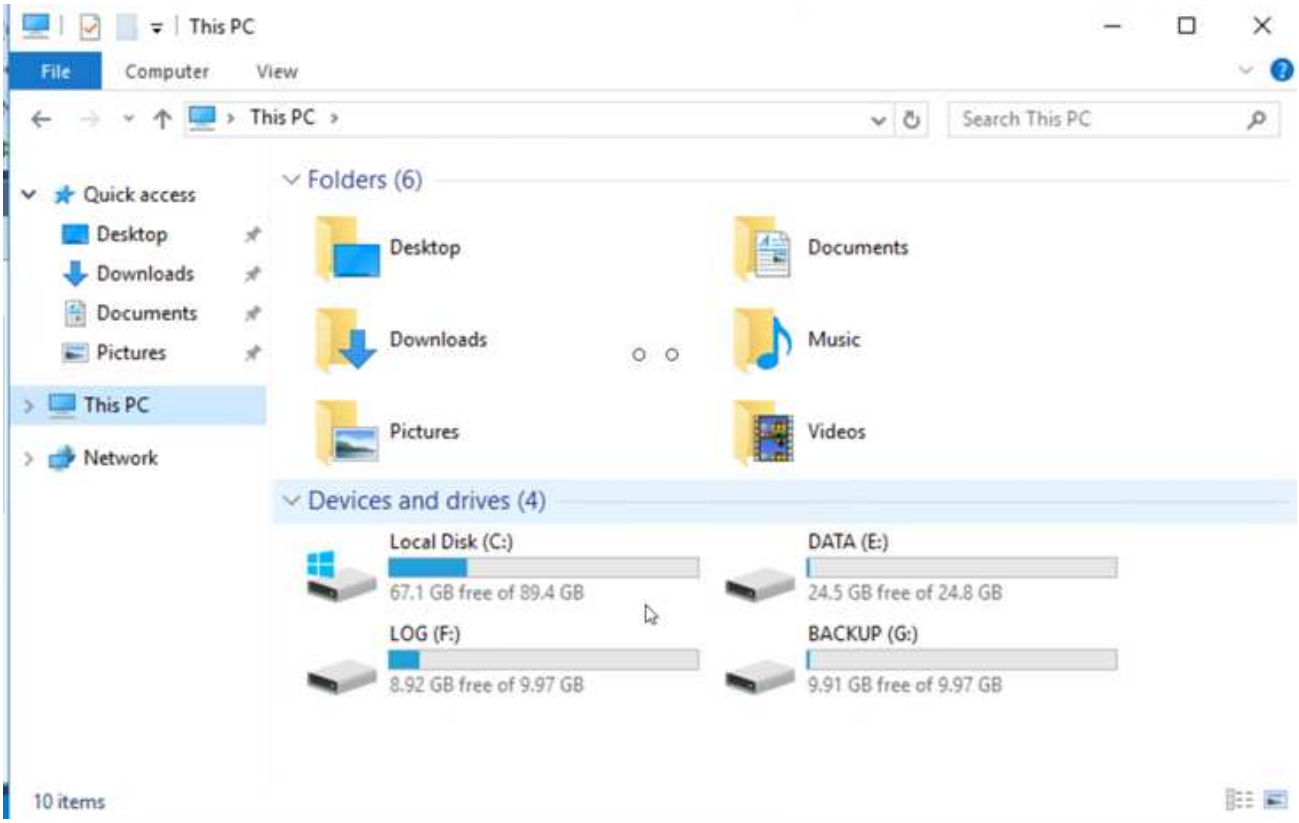
7. Fügen Sie die LUN von Cloud Volumes ONTAP mit denselben Laufwerksbuchstaben an die wiederhergestellte SQL-Gast-VM an.



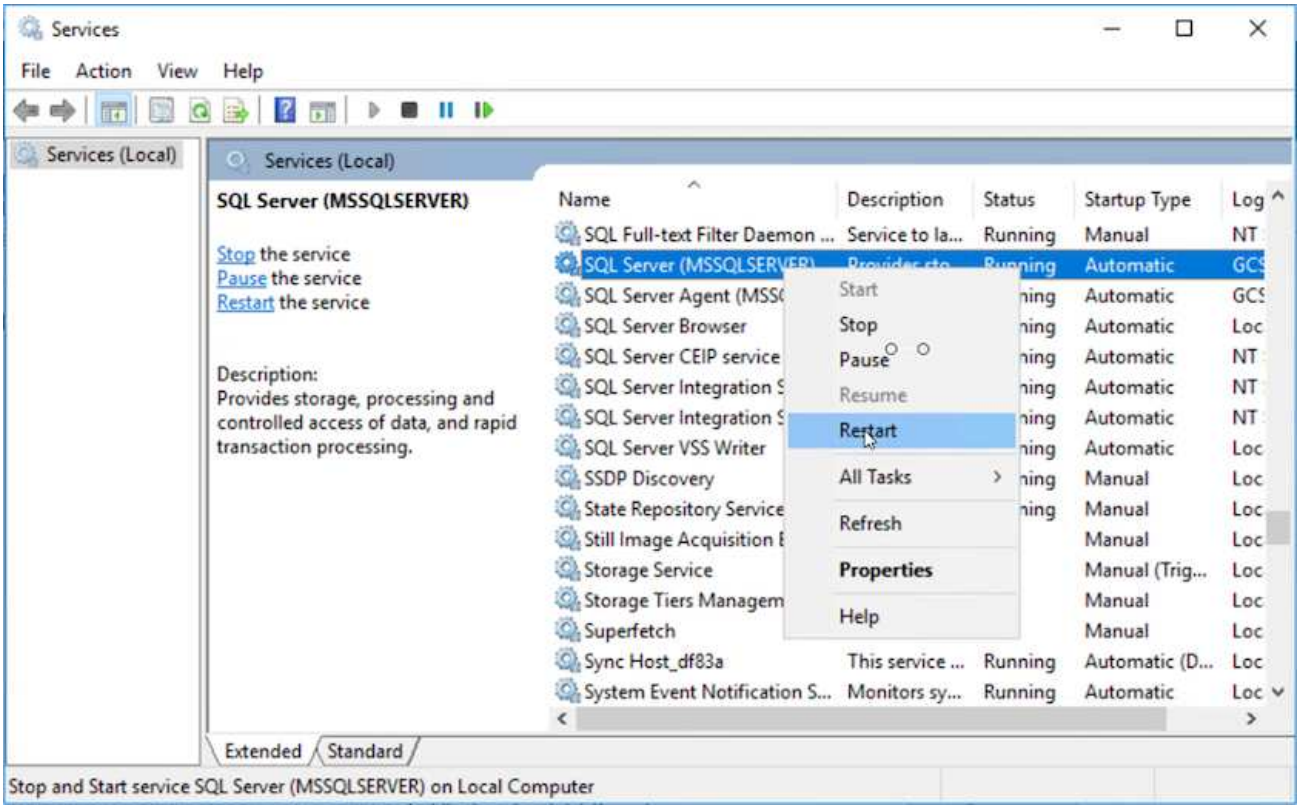
8. Öffnen Sie den iSCSI-Initiator, löschen Sie die vorherige getrennte Sitzung und fügen Sie das neue Ziel zusammen mit Multipath für die replizierten Cloud Volumes ONTAP Volumes hinzu.



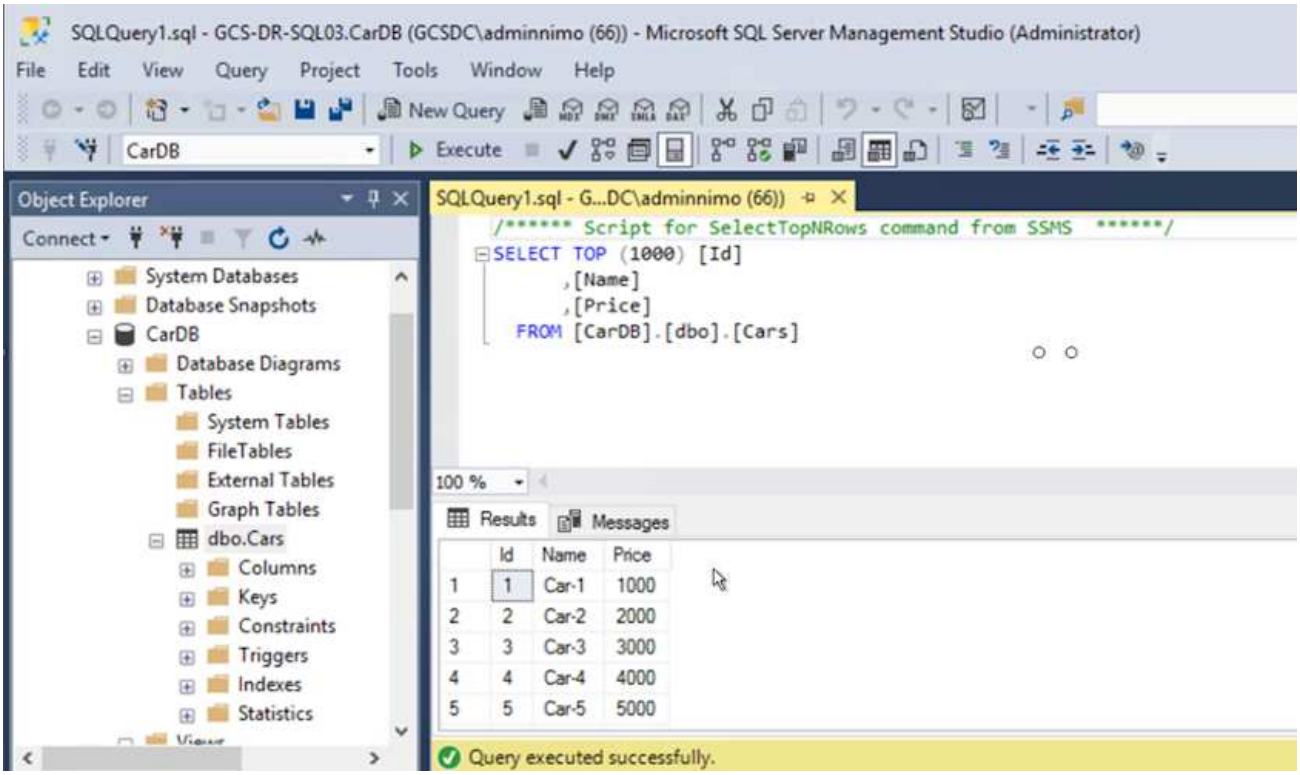
9. Stellen Sie sicher, dass alle Festplatten mit denselben Laufwerksbuchstaben verbunden sind, die vor DR verwendet wurden.



10. Starten Sie den MSSQL-Serverdienst neu.



11. Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.



Im Falle von NFS hängen Sie die Volumes mit dem Mount-Befehl an und aktualisieren Sie die `/etc/fstab` Einträge.

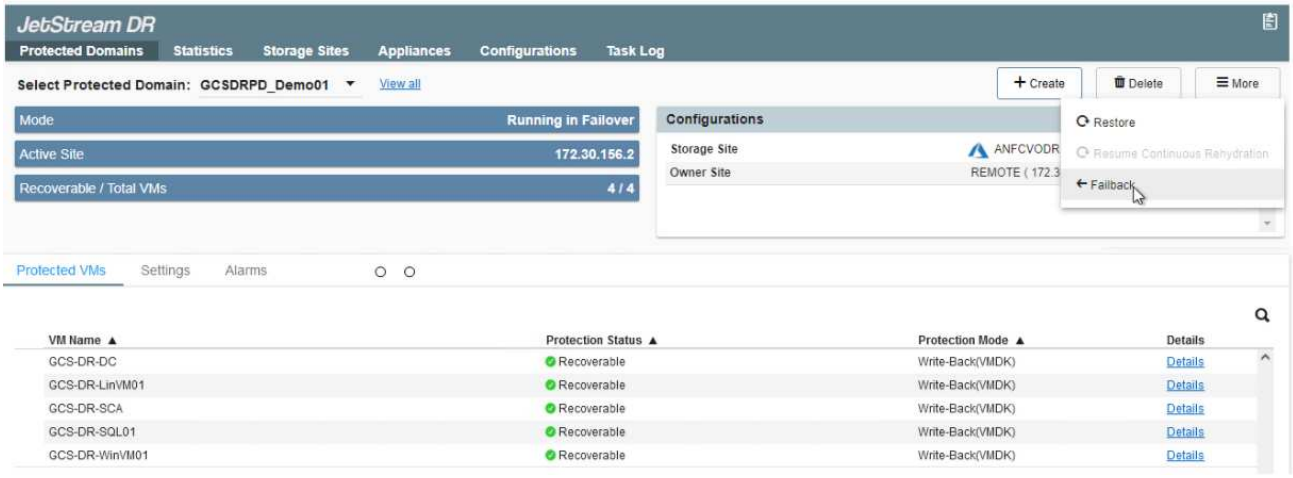
Ab diesem Zeitpunkt kann der Betrieb wieder aufgenommen werden und das Geschäft kann normal weiterlaufen.

Auf der NSX-T-Seite kann ein separates dediziertes Tier-1-Gateway zum Simulieren von Failover-Szenarien erstellt werden. Dadurch wird sichergestellt, dass alle Workloads miteinander kommunizieren können, jedoch kein Datenverkehr in die Umgebung hinein oder aus ihr heraus geleitet werden kann, sodass alle Triage-, Eindämmungs- oder Härtungsaufgaben ohne das Risiko einer Kreuzkontamination durchgeführt werden können. Dieser Vorgang liegt außerhalb des Rahmens dieses Dokuments, kann jedoch problemlos zur Simulation der Isolation durchgeführt werden.

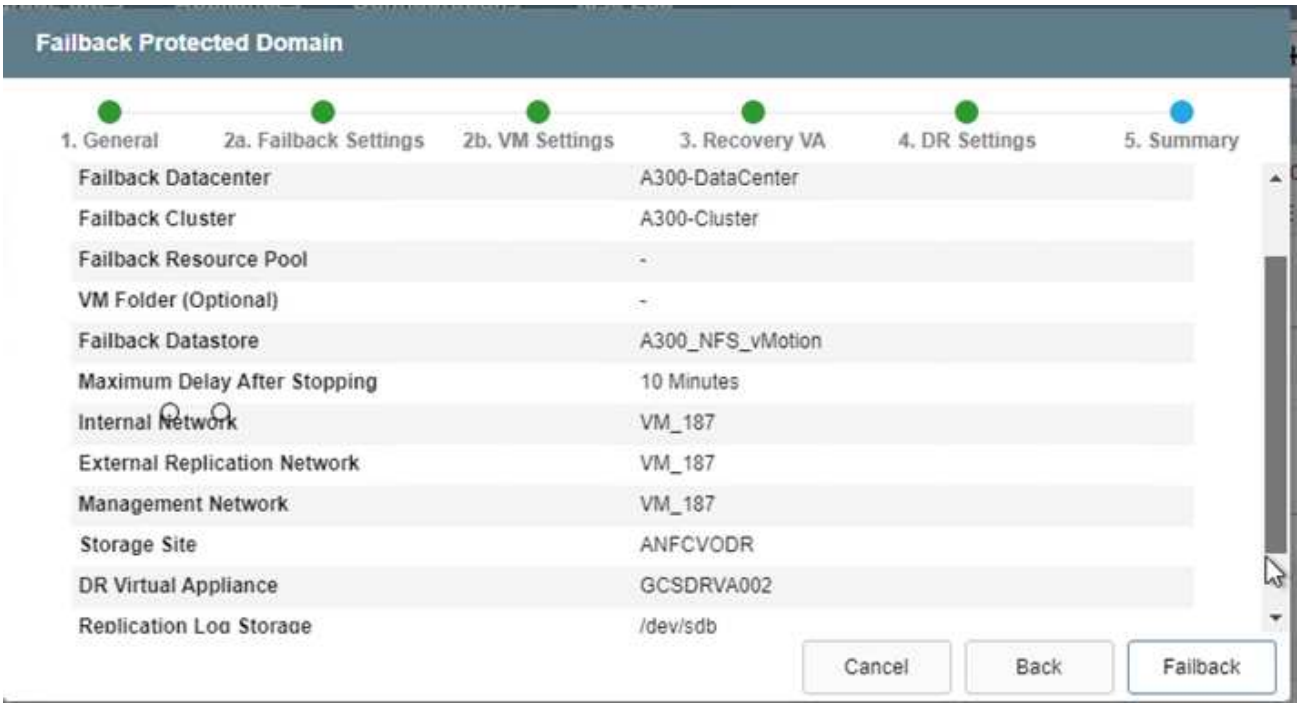
Nachdem die primäre Site wieder betriebsbereit ist, können Sie ein Failback durchführen. Der VM-Schutz wird von Jetstream wieder aufgenommen und die SnapMirror -Beziehung muss umgekehrt werden.

1. Stellen Sie die lokale Umgebung wieder her. Je nach Art des Katastrophenfalls kann es erforderlich sein, die Konfiguration des geschützten Clusters wiederherzustellen und/oder zu überprüfen. Gegebenenfalls muss die JetStream DR-Software neu installiert werden.
2. Greifen Sie auf die wiederhergestellte lokale Umgebung zu, gehen Sie zur Jetstream DR-Benutzeroberfläche und wählen Sie die entsprechende geschützte Domäne aus. Nachdem die geschützte Site für das Failback bereit ist, wählen Sie die Failback-Option in der Benutzeroberfläche aus.

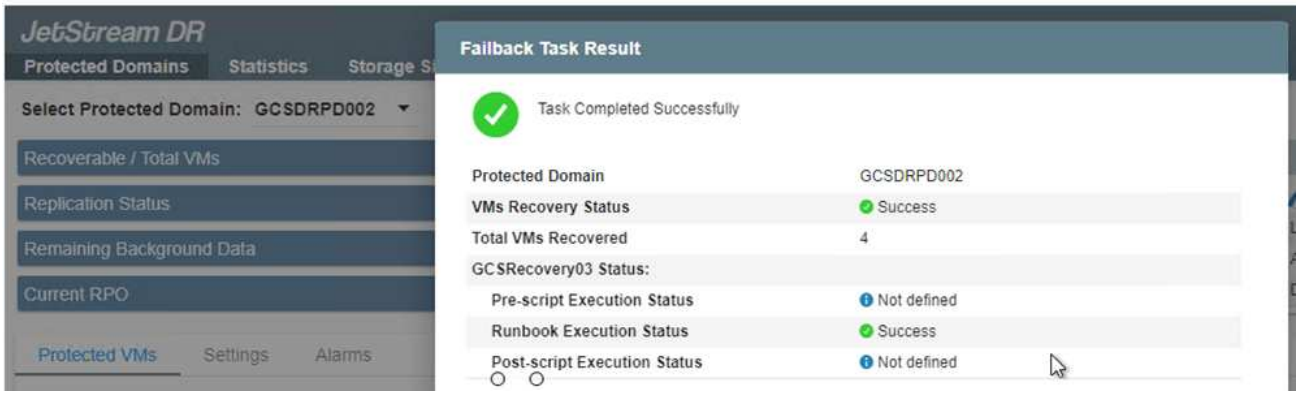
Der vom CPT generierte Failback-Plan kann auch verwendet werden, um die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher zurück in die ursprüngliche VMware-Umgebung zu initiieren.



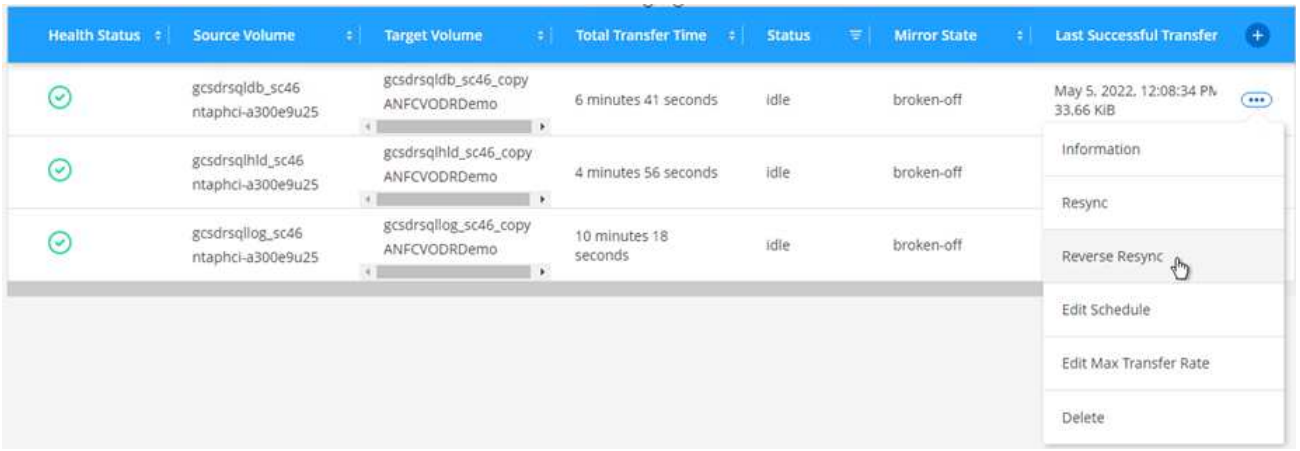
Geben Sie die maximale Verzögerung an, nachdem die VMs am Wiederherstellungsstandort angehalten und am geschützten Standort neu gestartet wurden. Die für diesen Vorgang benötigte Zeit umfasst die Fertigstellung der Replikation nach dem Stoppen der Failover-VMs, die zum Bereinigen der Wiederherstellungssite benötigte Zeit und die zum Neuerstellen der VMs auf der geschützten Site benötigte Zeit. NetApp empfiehlt 10 Minuten.

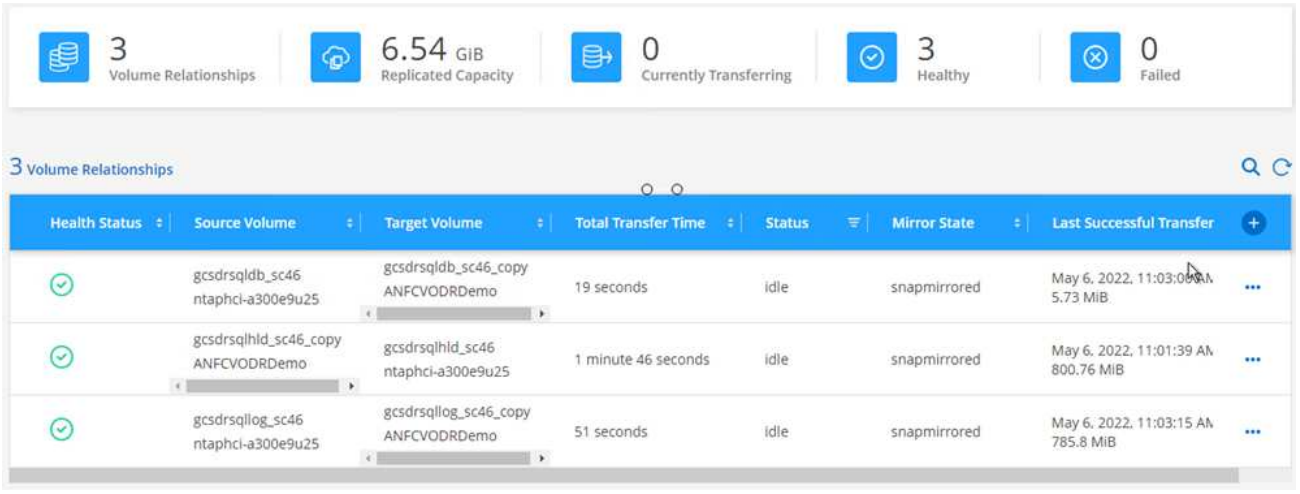


3. Schließen Sie den Failback-Prozess ab und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

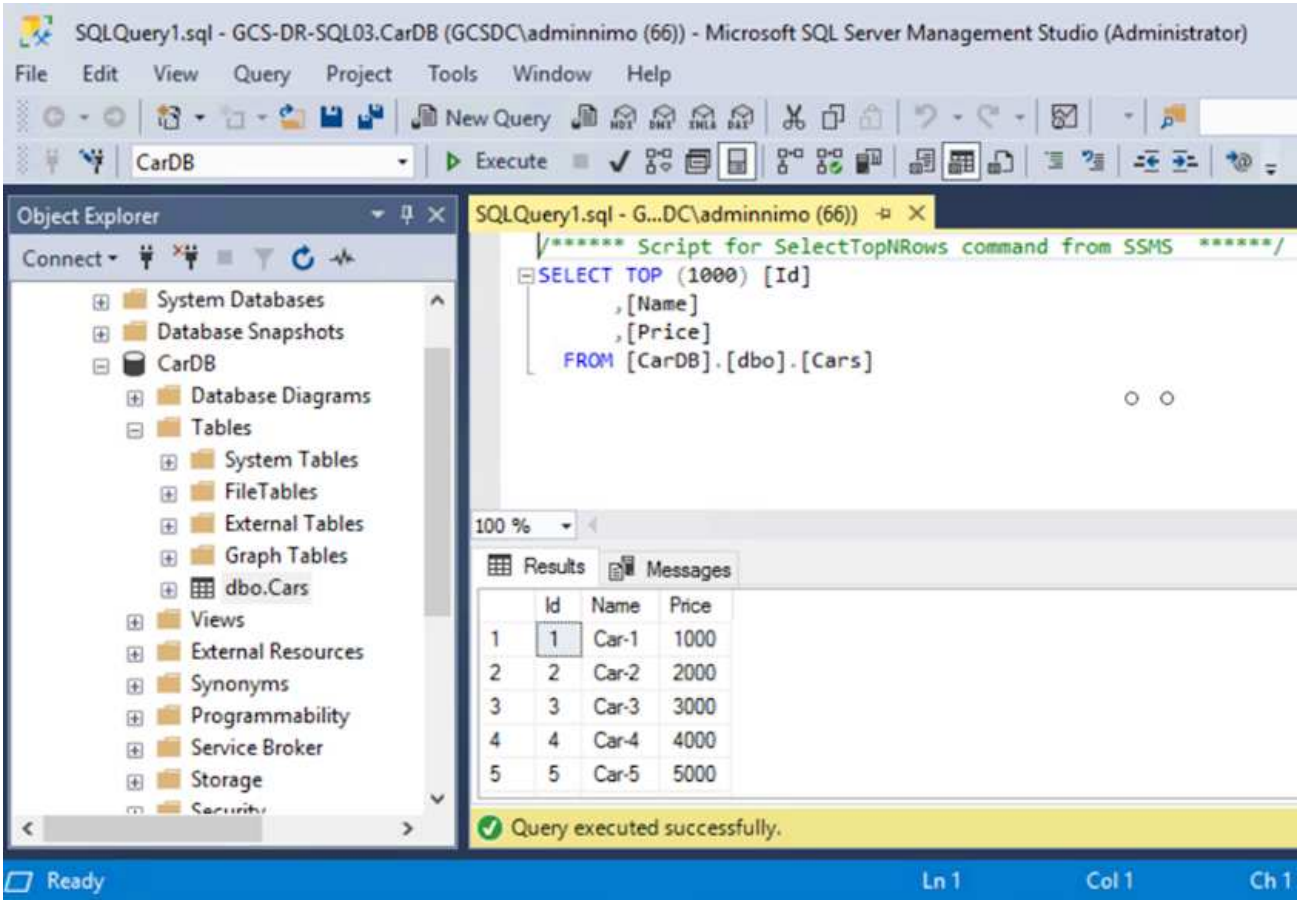


4. Nachdem die VMs wiederhergestellt wurden, trennen Sie den sekundären Speicher vom Host und stellen Sie eine Verbindung zum primären Speicher her.





5. Starten Sie den MSSQL-Serverdienst neu.
6. Überprüfen Sie, ob die SQL-Ressourcen wieder online sind.



Um ein Failback zum primären Speicher durchzuführen, stellen Sie sicher, dass die Beziehungsrichtung dieselbe bleibt wie vor dem Failover, indem Sie einen umgekehrten Resynchronisierungsvorgang durchführen.

Um die Rollen des primären und sekundären Speichers nach dem umgekehrten Resynchronisierungsvorgang beizubehalten, führen Sie den umgekehrten Resynchronisierungsvorgang erneut durch.

Dieser Prozess ist auf andere Anwendungen wie Oracle, ähnliche Datenbankvarianten und alle anderen Anwendungen anwendbar, die über den Gast verbundenen Speicher verwenden.

Testen Sie wie immer die Schritte zur Wiederherstellung der kritischen Workloads, bevor Sie sie in die Produktion portieren.

Vorteile dieser Lösung

- Verwendet die effiziente und stabile Replikation von SnapMirror.
- Stellt mit ONTAP Snapshot-Aufbewahrung alle verfügbaren Zeitpunkte wieder her.
- Für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs ist eine vollständige Automatisierung verfügbar, angefangen bei den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung.
- SnapCenter verwendet Klonmechanismen, die das replizierte Volume nicht ändern.
  - Dadurch wird das Risiko einer Datenbeschädigung bei Volumes und Snapshots vermieden.
  - Vermeidet Replikationsunterbrechungen während DR-Test-Workflows.

- Nutzt die DR-Daten für Workflows, die über DR hinausgehen, wie etwa Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Fehlerbehebungstests.

- Durch die CPU- und RAM-Optimierung können die Cloud-Kosten gesenkt werden, indem die Wiederherstellung auf kleineren Computerclustern ermöglicht wird.

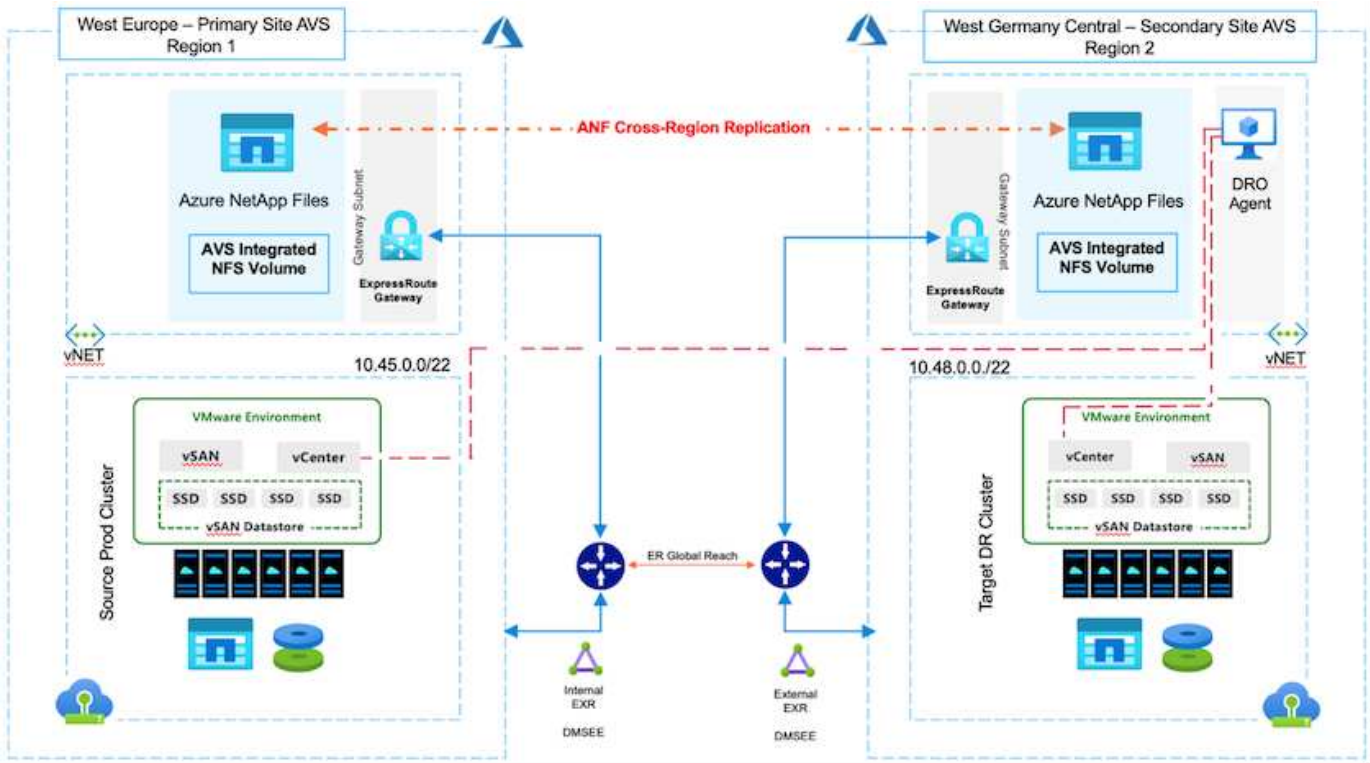
TR-4955: Notfallwiederherstellung mit Azure NetApp Files (ANF) und Azure VMware Solution (AVS)

Die Notfallwiederherstellung mithilfe der Replikation auf Blockebene zwischen Regionen innerhalb der Cloud ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Site-Ausfällen und Datenbeschädigungen (z. B. Ransomware) zu schützen.

Überblick

Mit der regionsübergreifenden Volumereplikation von Azure NetApp Files (ANF) können VMware-Workloads, die auf einem Azure VMware Solution (AVS) SDDC-Standort ausgeführt werden und Azure NetApp Files-Volumes als NFS-Datenspeicher auf dem primären AVS-Standort verwenden, auf einen bestimmten sekundären AVS-Standort in der Zielwiederherstellungsregion repliziert werden.

Mit Disaster Recovery Orchestrator (DRO) (einer Skriptlösung mit Benutzeroberfläche) können Sie Workloads, die von einem AVS SDDC auf ein anderes repliziert wurden, nahtlos wiederherstellen. DRO automatisiert die Wiederherstellung, indem es das Replikations-Peering unterbricht und dann das Zielvolume als Datenspeicher bereitstellt, über die VM-Registrierung bei AVS bis hin zu Netzwerkzuordnungen direkt auf NSX-T (in allen privaten AVS-Clouds enthalten).



Voraussetzungen und allgemeine Empfehlungen

- Stellen Sie sicher, dass Sie die regionsübergreifende Replikation aktiviert haben, indem Sie ein Replikations-Peering erstellen. Sehen "Erstellen einer Volumereplikation für Azure NetApp Files" .

- Sie müssen ExpressRoute Global Reach zwischen den privaten Quell- und Ziel-Clouds der Azure VMware

Solution konfigurieren.

- Sie müssen über einen Dienstprinzipal verfügen, der auf Ressourcen zugreifen kann.
- Die folgende Topologie wird unterstützt: primärer AVS-Standort zu sekundärem AVS-Standort.
- Konfigurieren Sie die "Replikation" Planen Sie für jedes Volume entsprechend den Geschäftsanforderungen und der Datenänderungsrate.

Kaskadierungs- und Fan-In- und Fan-Out-Topologien werden nicht unterstützt.

Erste Schritte

Bereitstellen der Azure VMware-Lösung

Der "Azure VMware-Lösung" (AVS) ist ein Hybrid-Cloud-Dienst, der voll funktionsfähige VMware SDDCs innerhalb einer öffentlichen Microsoft Azure-Cloud bereitstellt. AVS ist eine First-Party-Lösung, die vollständig von Microsoft verwaltet und unterstützt und von VMware verifiziert wird und die Azure-Infrastruktur nutzt. Daher erhalten Kunden VMware ESXi für die Computervirtualisierung, vSAN für hyperkonvergenten Speicher und NSX für Netzwerke und Sicherheit und profitieren gleichzeitig von der globalen Präsenz von Microsoft Azure, den erstklassigen Rechenzentrumseinrichtungen und der Nähe zum umfangreichen Ökosystem nativer Azure-Dienste und -Lösungen. Eine Kombination aus Azure VMware Solution SDDC und Azure NetApp Files bietet die beste Leistung bei minimaler Netzwerklatenz.

Um eine AVS-Private-Cloud auf Azure zu konfigurieren, folgen Sie den Schritten in diesem"Link" für NetApp Dokumentation und in diesem "Link" für Microsoft-Dokumentation. Eine Pilotlichtumgebung mit minimaler Konfiguration kann für DR-Zwecke verwendet werden. Dieses Setup enthält nur Kernkomponenten zur Unterstützung kritischer Anwendungen und kann skaliert werden, sodass im Falle eines Failovers weitere Hosts bereitgestellt werden können, um den Großteil der Last zu übernehmen.

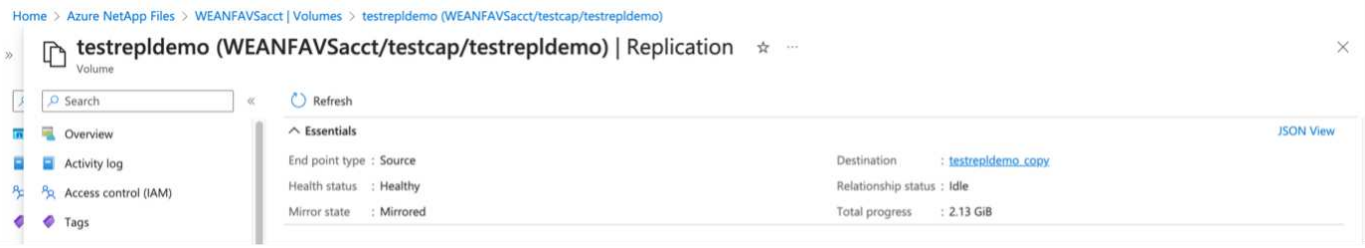
In der ersten Version unterstützt DRO einen vorhandenen AVS SDDC-Cluster. Die On-Demand-SDDC-Erstellung wird in einer kommenden Version verfügbar sein.

Bereitstellen und Konfigurieren von Azure NetApp Files

"Azure NetApp Files"ist ein leistungsstarker, gebührenpflichtiger Dateispeicherdienst der Enterprise-Klasse. Befolgen Sie die Schritte in diesem "Link" zum Bereitstellen und Konfigurieren von Azure NetApp Files als NFS-Datenspeicher zur Optimierung der AVS-Bereitstellungen in privaten Clouds.

Erstellen einer Volumereplikation für Azure NetApp Files-basierte Datenspeichervolumes

Der erste Schritt besteht darin, die regionsübergreifende Replikation für die gewünschten Datenspeichervolumes vom primären AVS-Standort zum sekundären AVS-Standort mit den entsprechenden Frequenzen und Aufbewahrungszeiten einzurichten.



Befolgen Sie die Schritte in diesem "Link" um eine regionsübergreifende Replikation durch Erstellen eines Replikations-Peerings einzurichten. Das Servicelevel für den Zielkapazitätspool kann mit dem des

Quellkapazitätspools übereinstimmen. Für diesen speziellen Anwendungsfall können Sie jedoch das Standard-Service-Level auswählen und dann "Ändern Sie den Service-Level" im Falle einer echten Katastrophe oder DR-Simulationen.

Eine regionsübergreifende Replikationsbeziehung ist Voraussetzung und muss vorher erstellt werden.

DRO-Installation

Um mit DRO zu beginnen, verwenden Sie das Ubuntu-Betriebssystem auf der vorgesehenen virtuellen Azure-Maschine und stellen Sie sicher, dass Sie die Voraussetzungen erfüllen. Installieren Sie dann das Paket.

Voraussetzungen:

- Dienstprinzipal, der auf Ressourcen zugreifen kann.
- Stellen Sie sicher, dass eine entsprechende Verbindung zu den Quell- und Ziel-SDDC- und Azure NetApp Files Instanzen besteht.
- Wenn Sie DNS-Namen verwenden, sollte eine DNS-Auflösung vorhanden sein. Verwenden Sie andernfalls IP-Adressen für vCenter.

Betriebssystemanforderungen:

- Ubuntu Focal 20.04 (LTS)Die folgenden Pakete müssen auf der vorgesehenen virtuellen Agent-Maschine installiert werden:
- Docker
- Docker-Compose
- JqChange `docker.sock` zu dieser neuen Berechtigung: `sudo chmod 666 /var/run/docker.sock .`

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

Die Schritte sind wie folgt:

1. Laden Sie das Installationspaket auf die angegebene virtuelle Maschine herunter:

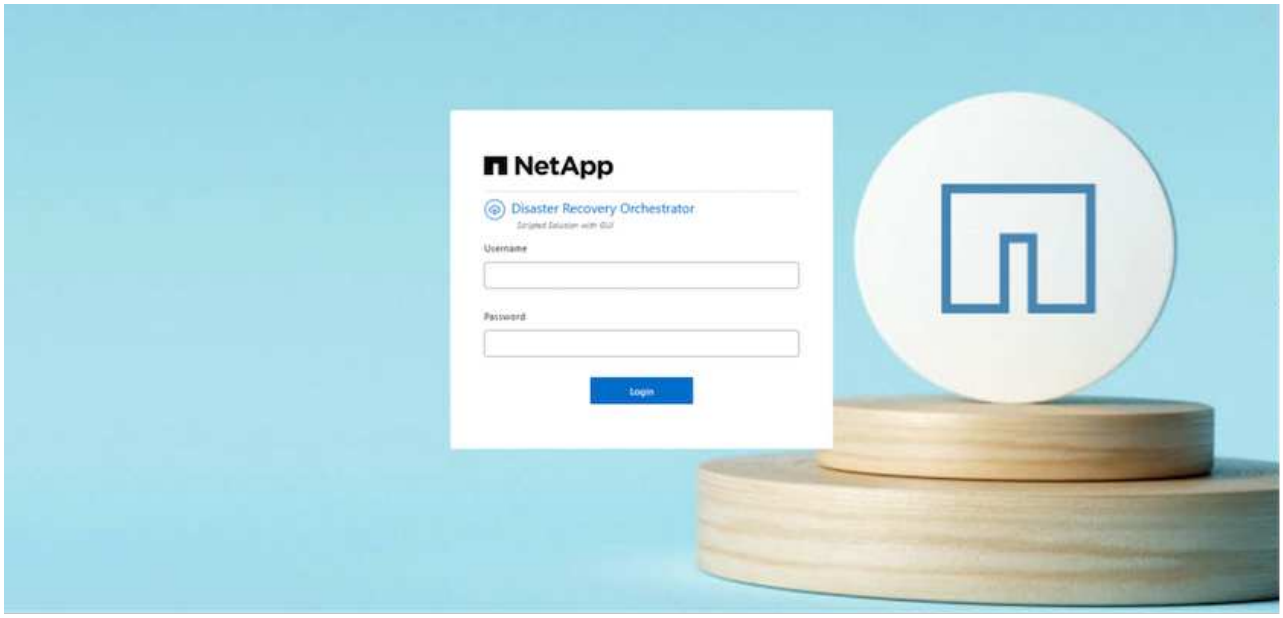
```
git clone https://github.com/NetApp/DRO-Azure.git
```

Der Agent muss in der sekundären AVS-Standortregion oder in der primären AVS-Standortregion in einer anderen 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 Anmeldeinformationen auf die Benutzeroberfläche zu:
    - Benutzername: `admin`
    - Passwort: `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-Agenten am sekundären AVS-Standort bereitzustellen und die ExpressRoute-Gateway-Verbindung so zu konfigurieren, dass der DRO-Agent über das Netzwerk mit den entsprechenden AVS- und Azure NetApp Files Komponenten kommunizieren kann.

Der erste Schritt besteht darin, Anmeldeinformationen hinzuzufügen. DRO benötigt die Berechtigung zum Erkennen von Azure NetApp Files und der Azure VMware-Lösung. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie eine Azure Active Directory (AD)-Anwendung erstellen und einrichten und die von DRO benötigten Azure-Anmeldeinformationen abrufen. Sie müssen den Dienstprinzipal 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 mit dem Dienstprinzipal verknüpften Anmeldeinformationen auszuwählen. Sie müssen diese Anmeldeinformationen zu DRO hinzufügen, bevor Sie auf „Neue Site hinzufügen“ klicken können.

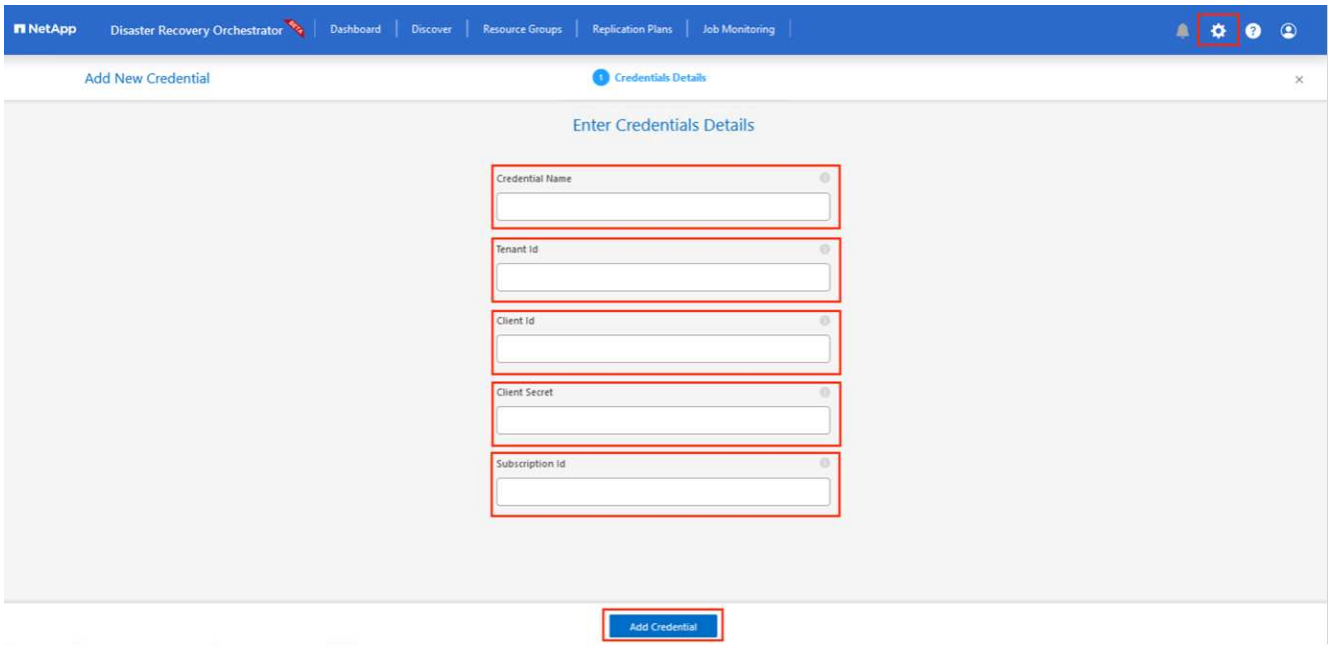
Führen Sie zum Ausführen dieses Vorgangs die folgenden Schritte aus:

1. Öffnen Sie DRO in einem unterstützten Browser und verwenden Sie den Standardbenutzernamen und das Standardkennwort/`admin`/`admin`). Das Passwort kann nach der ersten Anmeldung über die Option „Passwort ändern“ zurückgesetzt werden.
2. Klicken Sie oben rechts in der DRO-Konsole auf das Symbol **Einstellungen** und wählen Sie **Anmeldeinformationen** aus.
3. Klicken Sie auf „Neue Anmeldeinformationen hinzufügen“ und folgen Sie den Schritten des Assistenten.
4. Um die Anmeldeinformationen zu definieren, geben Sie Informationen zum Azure Active Directory-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:

- Anmeldeinformationsname
- Mandanten-ID
- Client-ID
- Clientgeheimnis
- Abonnement-ID

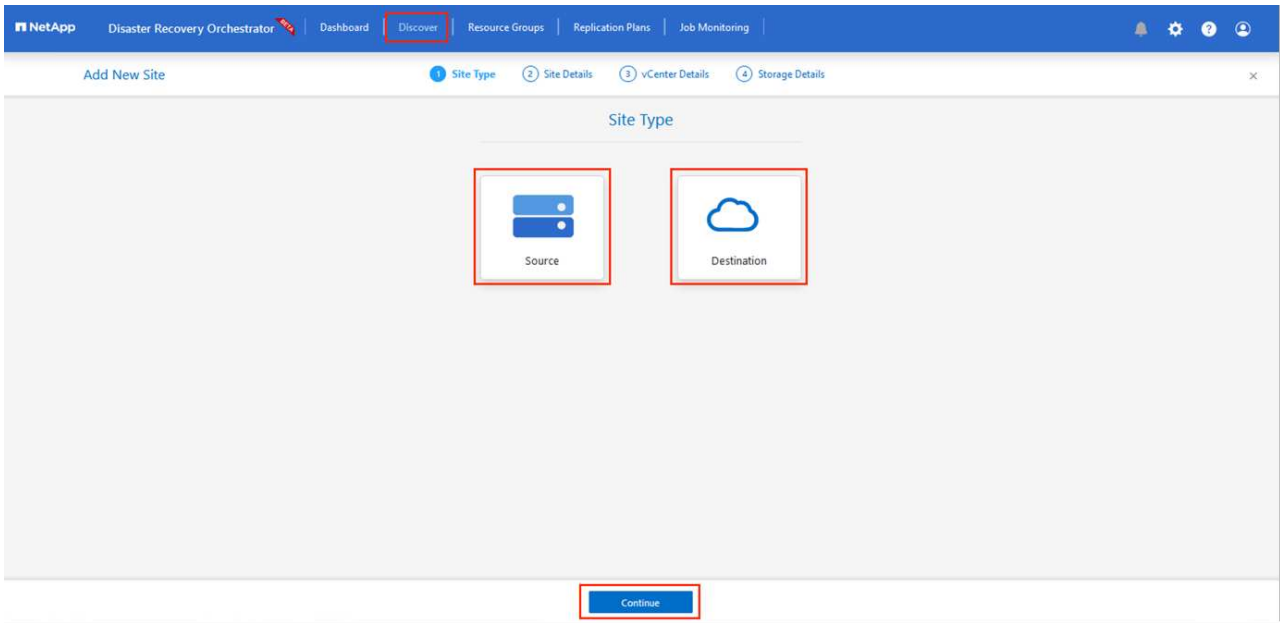
  Sie sollten diese Informationen beim Erstellen der AD-Anwendung erfasst haben.

5. Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und klicken Sie auf „Anmeldeinformationen hinzufügen“.



Nachdem Sie die Anmeldeinformationen hinzugefügt haben, ist es an der Zeit, die primären und sekundären AVS-Sites (sowohl vCenter als auch das Azure NetApp Dateispeicherkonto) zu ermitteln und zu DRO hinzuzufügen. Führen Sie die folgenden Schritte aus, um die Quell- und Zielsite hinzuzufügen:

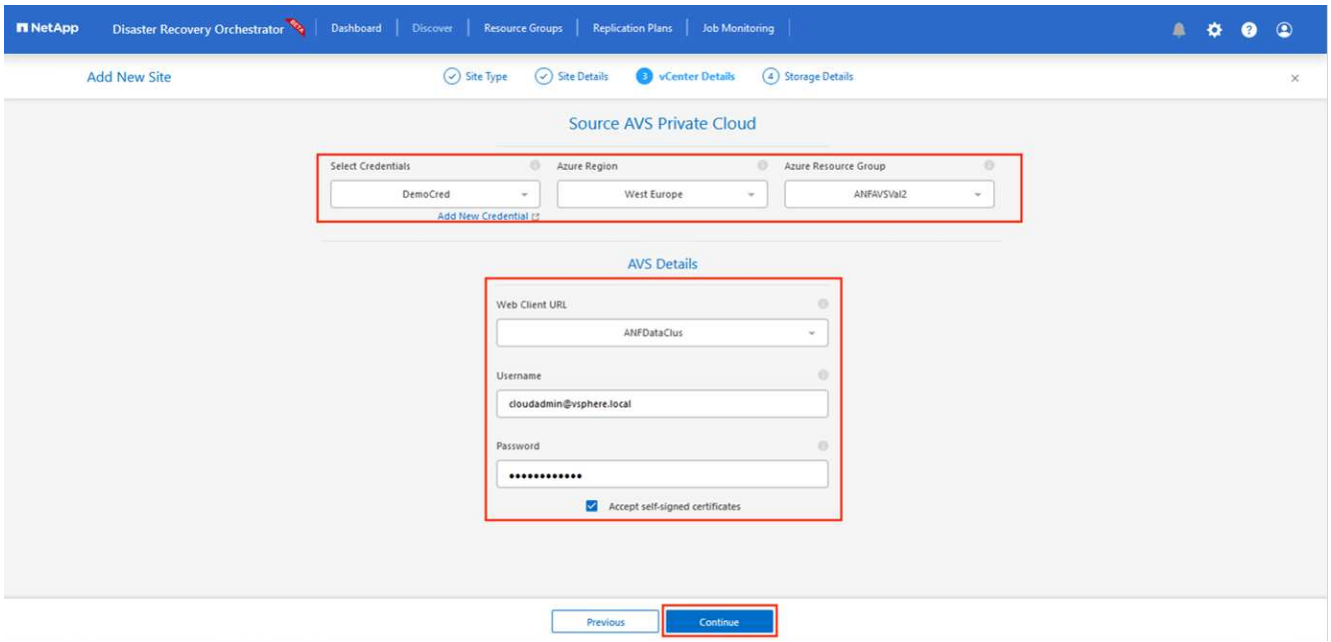
6. Gehen Sie zur Registerkarte **Entdecken**.
7. Klicken Sie auf **Neue Site hinzufügen**.
8. Fügen Sie die folgende primäre AVS-Site hinzu (in der Konsole als **Quelle** bezeichnet).
   - SDDC vCenter
   - Azure NetApp Files Speicherkonto
9. Fügen Sie die folgende sekundäre AVS-Site hinzu (in der Konsole als **Ziel** bezeichnet).
   - SDDC vCenter
   - Azure NetApp Files Speicherkonto



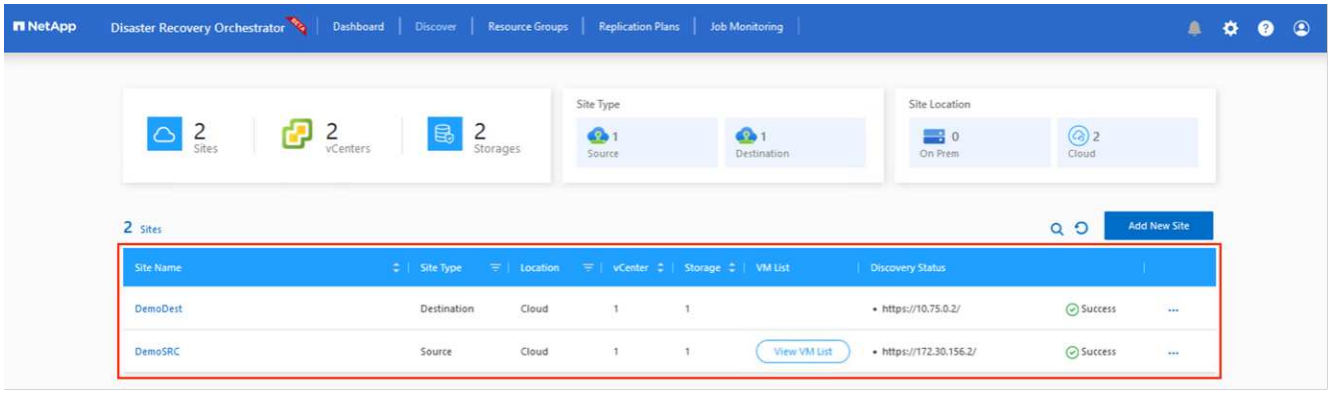
10. Fügen Sie Sitedetails hinzu, indem Sie auf **Quelle** klicken, einen aussagekräftigen Sitenamen eingeben und den Connector auswählen. Klicken Sie dann auf **Weiter**.

> Zu Demonstrationszwecken wird in diesem Dokument das Hinzufügen einer Quellsite behandelt.

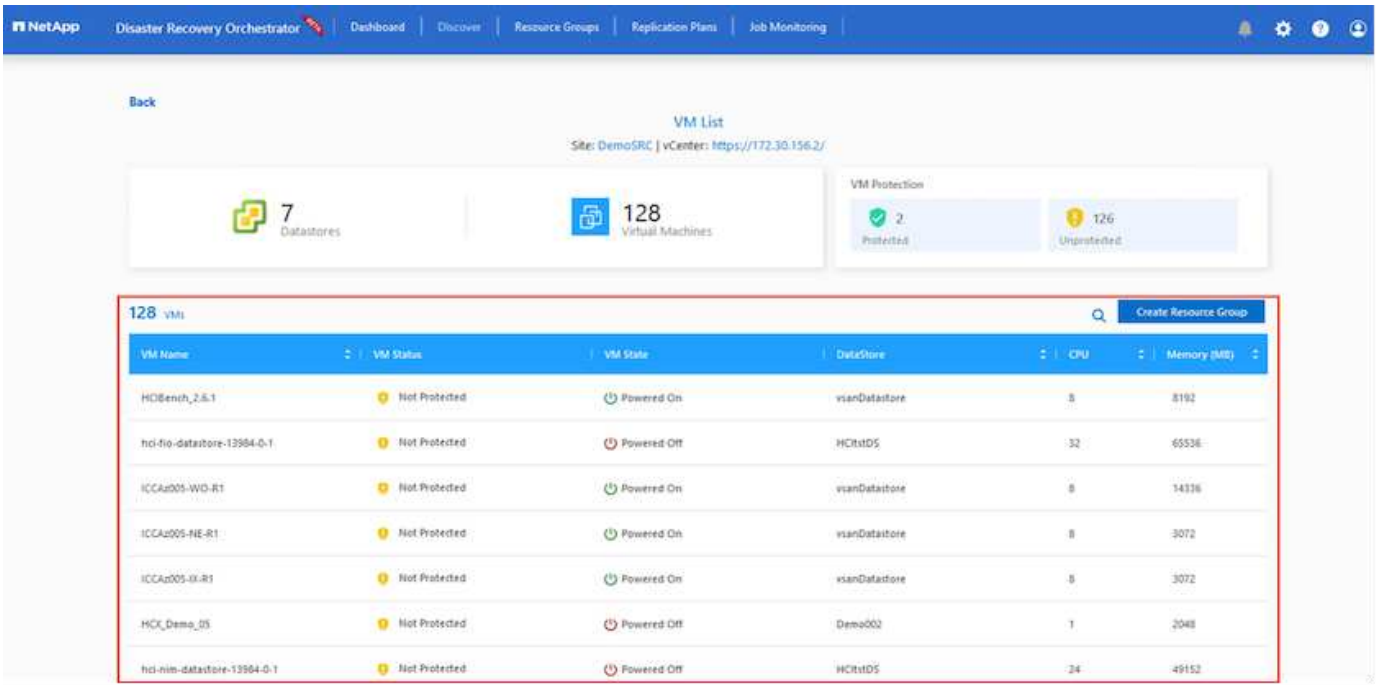
11. Aktualisieren Sie die vCenter-Details. Wählen Sie dazu die Anmeldeinformationen, die Azure-Region und die Ressourcengruppe aus der Dropdown-Liste für das primäre AVS SDDC aus.
12. DRO listet alle verfügbaren SDDCs innerhalb der Region auf. Wählen Sie die gewünschte private Cloud-URL aus der Dropdown-Liste aus.
13. Geben Sie den `cloudadmin@vsphere.local` Benutzeranmeldeinformationen. Der Zugriff ist über das Azure-Portal möglich. Befolgen Sie die in diesem Dokument beschriebenen Schritte "Link" . Klicken Sie anschließend auf **Weiter**.



14. Wählen Sie die Quellspeicherdetails (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 über entsprechende regionsübergreifende Replikate vom Quell- zum Zielstandort verfügen. DRO erkennt automatisch die von den VMs verwendeten Netzwerke und Segmente und füllt sie.



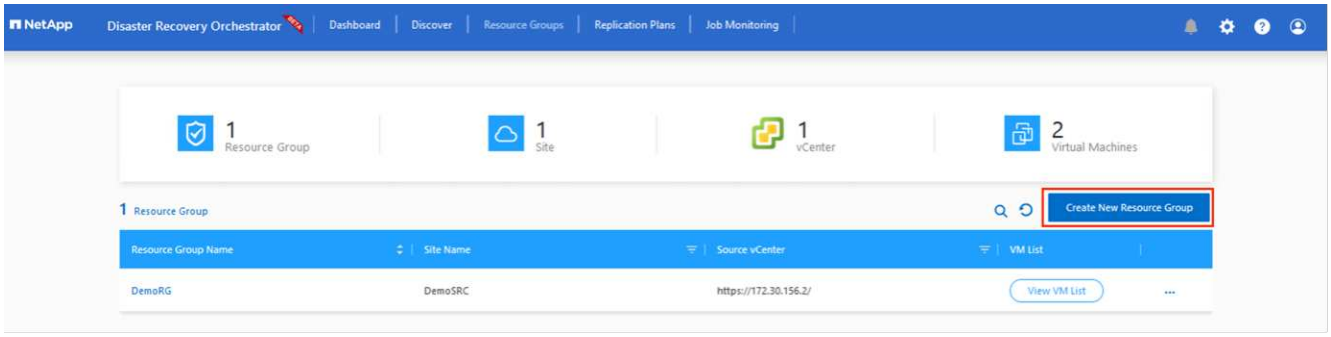
Der nächste Schritt besteht darin, die benötigten VMs in ihren Funktionsgruppen als Ressourcengruppen zu gruppieren.

Ressourcengruppierungen

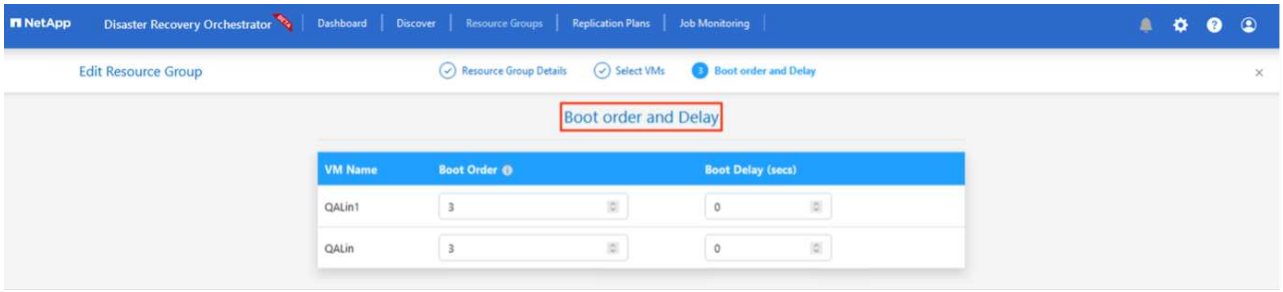
Nachdem die Plattformen hinzugefügt wurden, gruppieren Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen. Mit DRO-Ressourcengruppen können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen, Startverzögerungen und optionalen Anwendungsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

Um mit der Erstellung von Ressourcengruppen zu beginnen, klicken Sie auf das Menüelement **Neue Ressourcengruppe erstellen**.

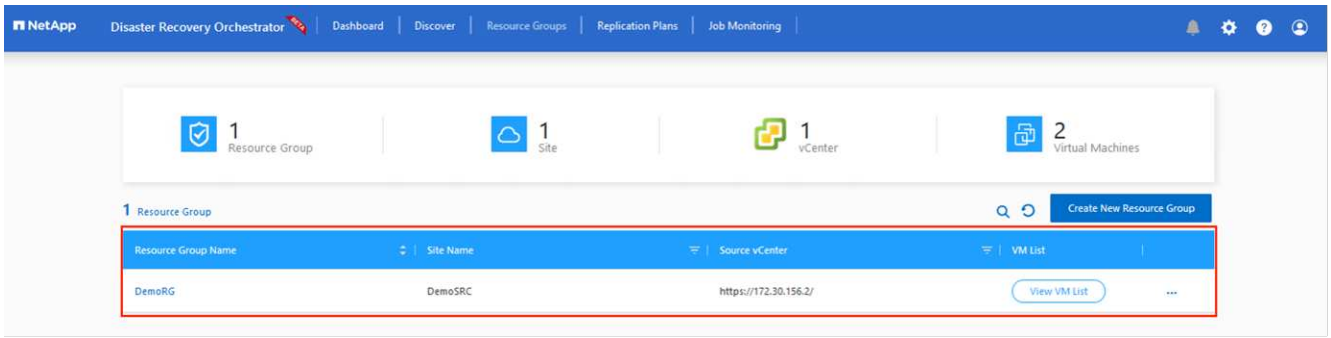
1. Greifen Sie auf **Ressourcengruppen** zu und klicken Sie auf **Neue Ressourcengruppe erstellen**.



2. Wählen Sie unter „Neue Ressourcengruppe“ die Quellsite aus der Dropdown-Liste aus und klicken Sie auf „Erstellen“.
3. Geben Sie die Details der Ressourcengruppe ein und klicken Sie auf **Weiter**.
4. Wählen Sie mithilfe der Suchoption geeignete VMs aus.
5. Wählen Sie die **Startreihenfolge** und **Startverzögerung** (Sek.) für alle ausgewählten VMs aus. Legen Sie die Reihenfolge der Einschaltsequenz fest, indem Sie jede virtuelle Maschine auswählen und die Priorität dafür festlegen. Der Standardwert für alle virtuellen Maschinen ist 3. Die Optionen sind wie folgt:
   - Die erste virtuelle Maschine, die eingeschaltet wird
   - Standard
   - Die letzte eingeschaltete virtuelle Maschine



6. Klicken Sie auf **Ressourcengruppe erstellen**.



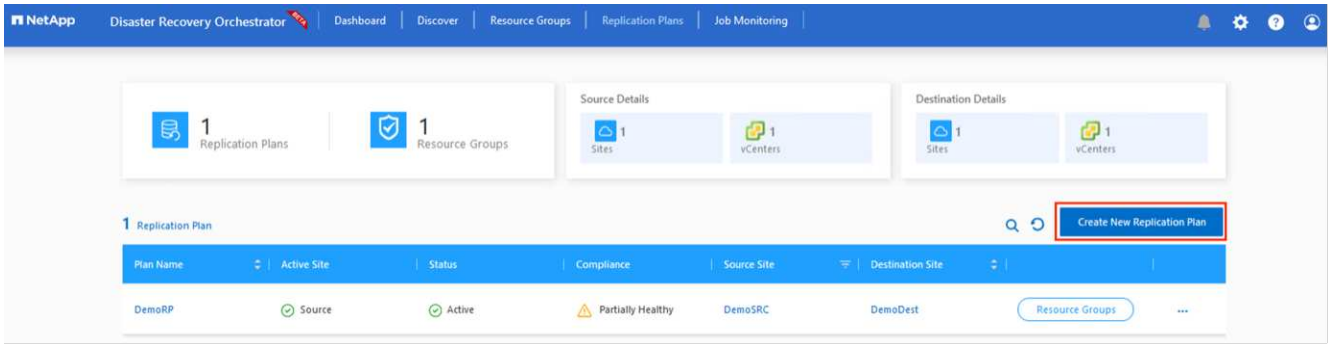
Replikationspläne

Sie müssen über einen Plan zur Wiederherstellung von Anwendungen im Katastrophenfall verfügen. Wählen Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste aus, wählen Sie die Ressourcengruppen aus, die in diesen Plan aufgenommen werden sollen, und geben Sie auch die Gruppierung an, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen (z. B. Domänencontroller, Tier-1, Tier-2

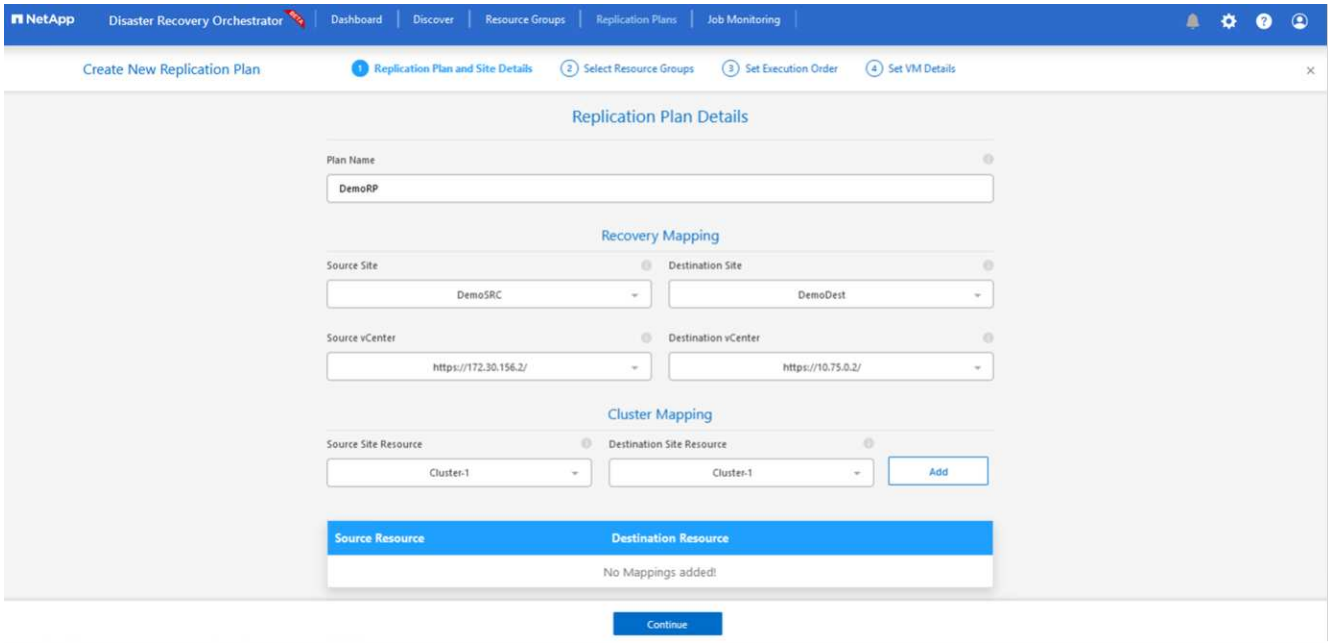
usw.). Pläne werden oft auch als Blaupausen bezeichnet. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte „Replikationsplan“ und klicken Sie auf **Neuer Replikationsplan**.

Führen Sie die folgenden Schritte aus, um mit der Erstellung eines Replikationsplans zu beginnen:

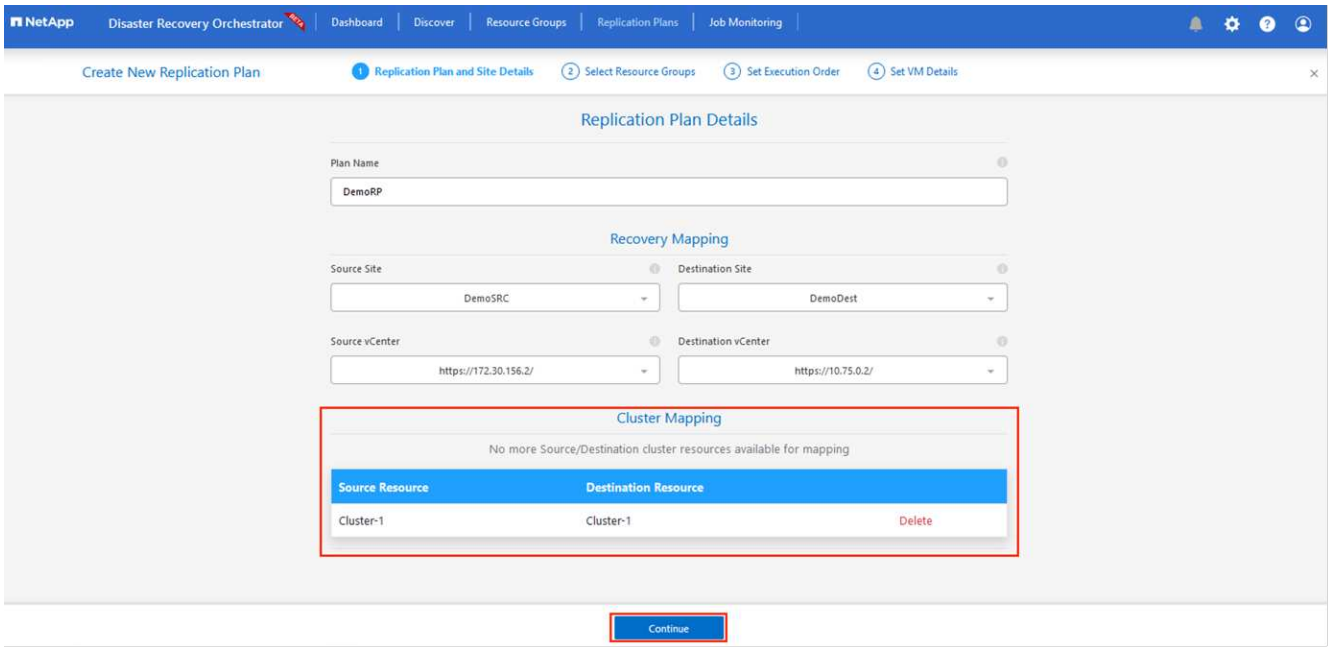
1. Navigieren Sie zu **Replikationsplänen** und klicken Sie auf **Neuen Replikationsplan erstellen**.



2. Geben Sie im **Neuen Replikationsplan** einen Namen für den Plan ein und fügen Sie Wiederherstellungszuordnungen hinzu, indem Sie die Quellsite, das zugehörige vCenter, die Zielsite und das zugehörige vCenter auswählen.

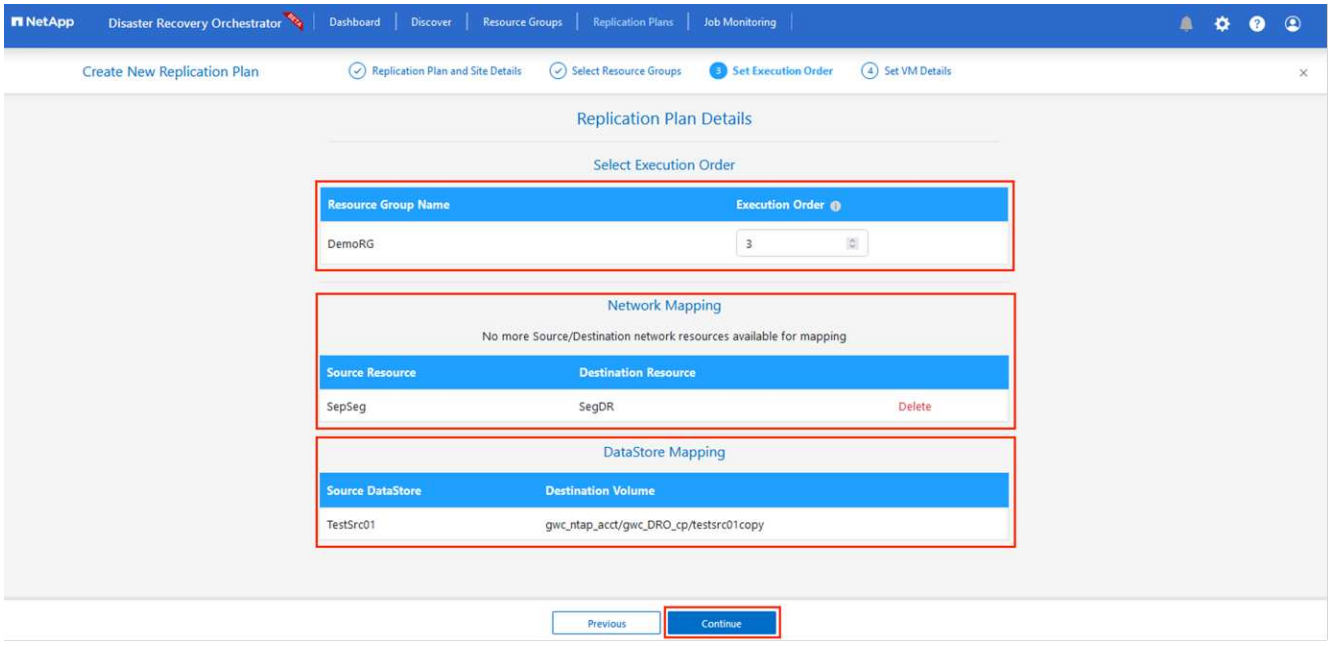


3. Wählen Sie nach Abschluss der Wiederherstellungszuordnung die **Clusterzuordnung** aus.

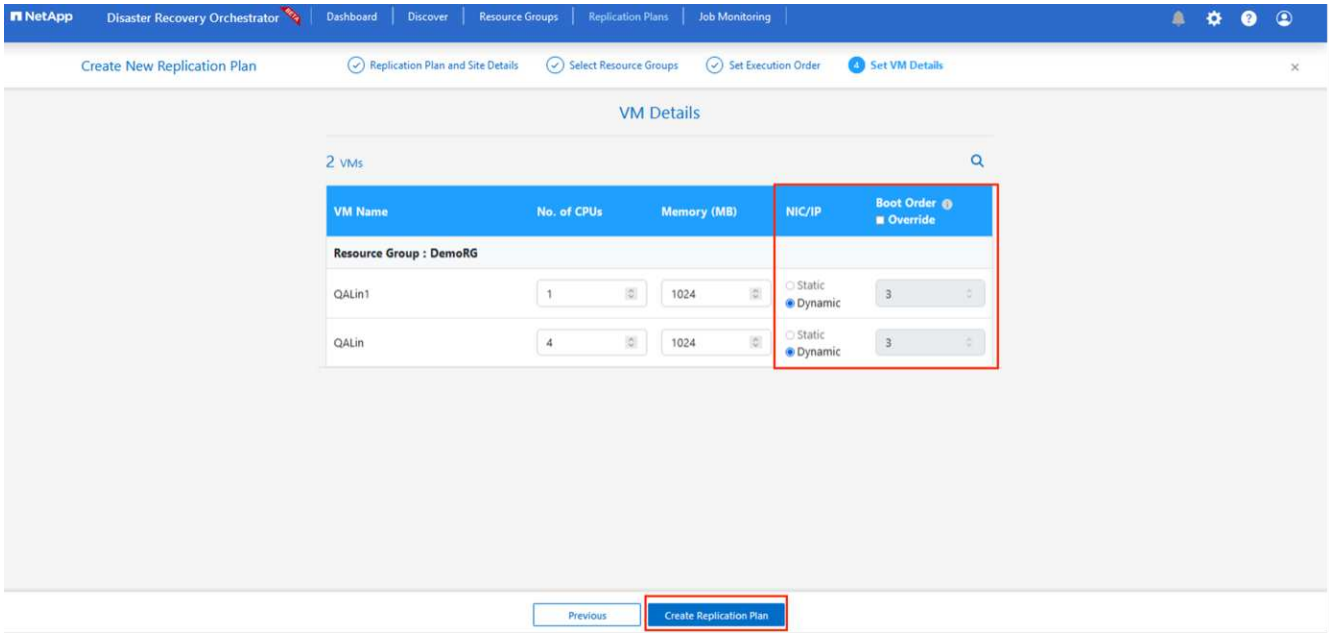


4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
6. Sobald dies erledigt ist, legen Sie die Netzwerkzuordnung auf das entsprechende Segment fest. Die Segmente sollten bereits auf dem sekundären AVS-Cluster bereitgestellt sein. Um die VMs diesen zuzuordnen, wählen Sie das entsprechende Segment aus.
7. Datenspeicherzuordnungen werden automatisch basierend auf der Auswahl der VMs ausgewählt.

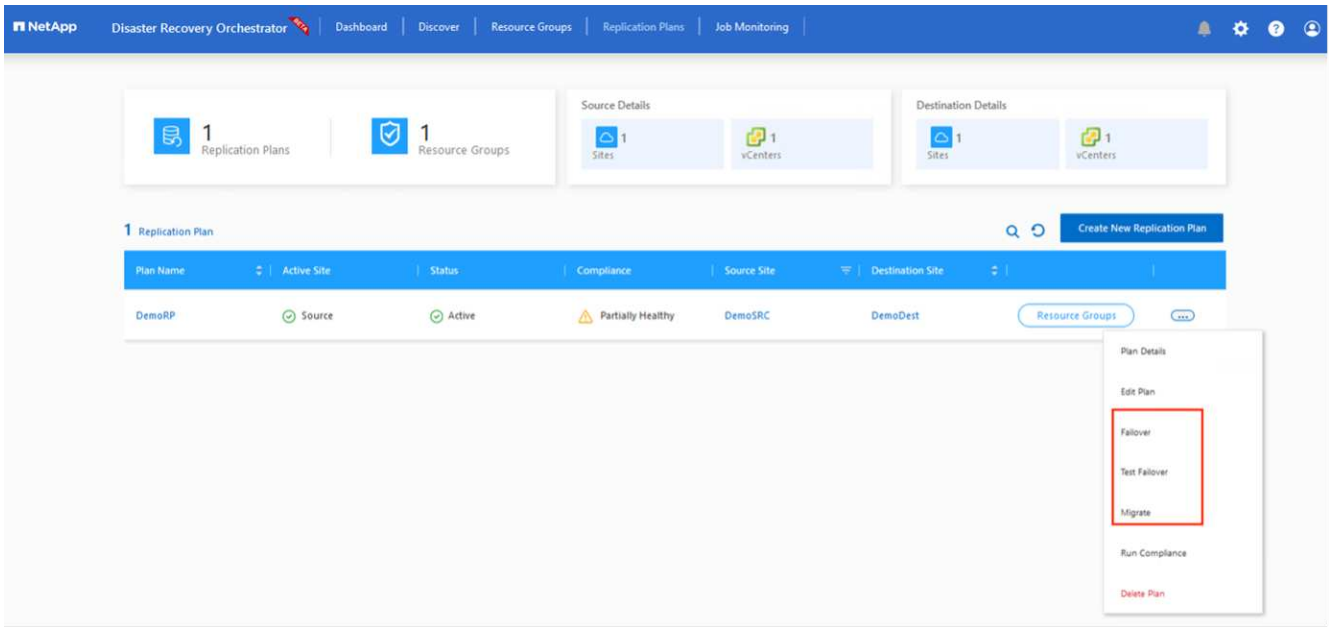
Die regionsübergreifende Replikation (CRR) erfolgt auf Volumeebene. Daher werden alle auf dem jeweiligen Volume befindlichen VMs zum CRR-Ziel repliziert. Achten Sie darauf, alle VMs auszuwählen, die Teil des Datenspeichers sind, da nur virtuelle Maschinen verarbeitet werden, die Teil des Replikationsplans sind.



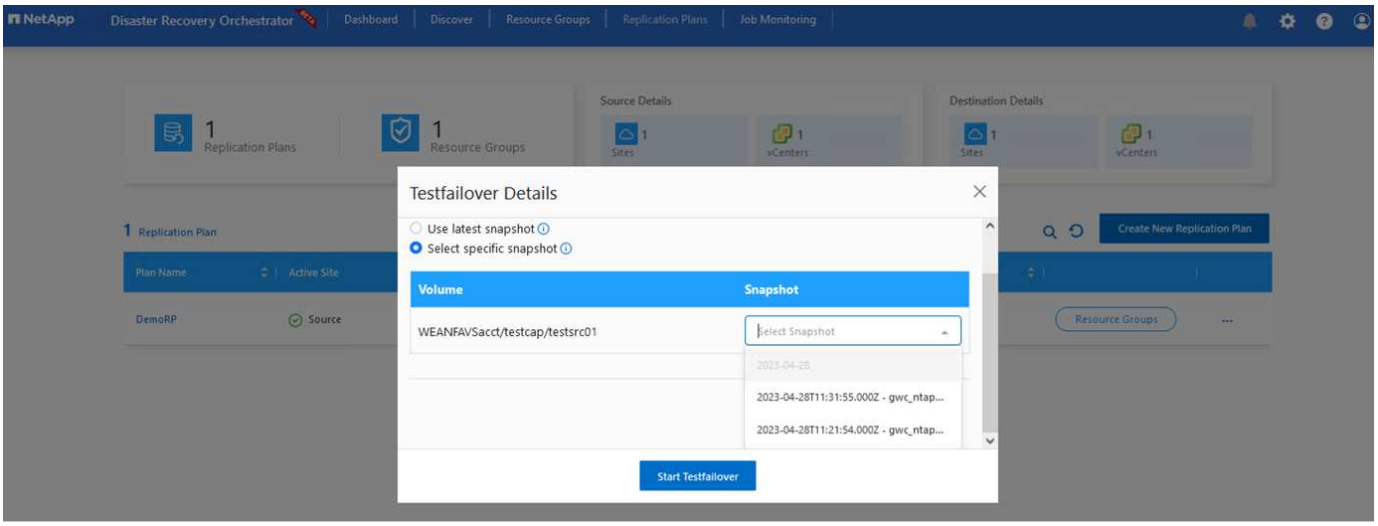
8. Unter VM-Details können Sie optional die CPU- und RAM-Parameter der VMs ändern. Dies kann sehr hilfreich sein, wenn Sie große Umgebungen auf kleineren Zielclustern wiederherstellen oder DR-Tests durchführen, ohne eine physische Eins-zu-eins-VMware-Infrastruktur bereitstellen zu müssen. Ändern Sie außerdem die Startreihenfolge und die Startverzögerung (Sek.) für alle ausgewählten VMs in den Ressourcengruppen. Es gibt eine zusätzliche Option zum Ändern der Startreihenfolge, wenn Änderungen an der von Ihnen bei der Auswahl der Startreihenfolge der Ressourcengruppe ausgewählten Reihenfolge erforderlich sind. Standardmäßig wird die bei der Ressourcengruppenauswahl festgelegte Startreihenfolge verwendet. In dieser Phase können jedoch beliebige Änderungen vorgenommen werden.



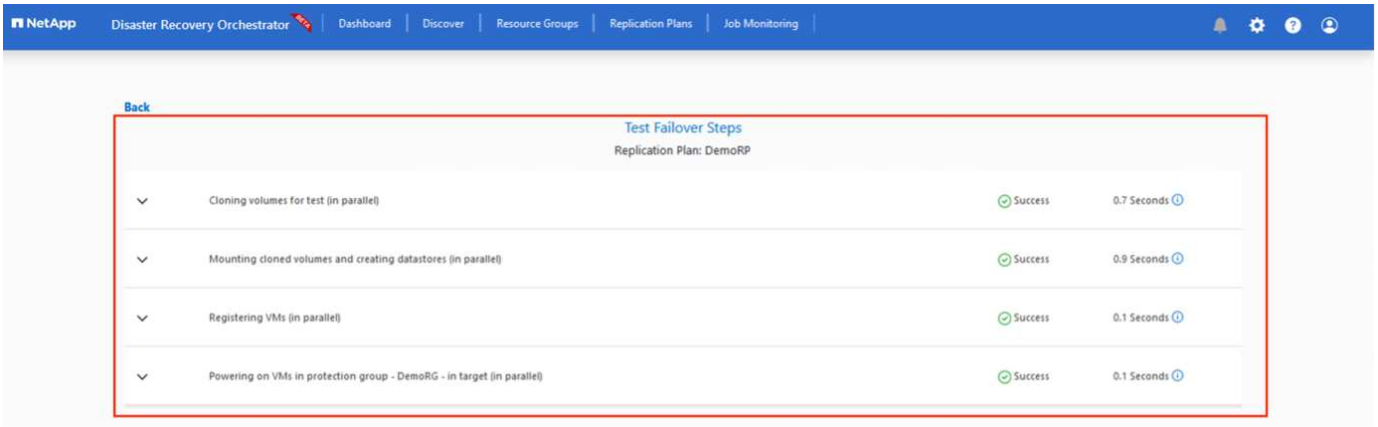
9. Klicken Sie auf **Replikationsplan erstellen**. Nachdem der Replikationsplan erstellt wurde, können Sie je nach Ihren Anforderungen die Optionen Failover, Testfailover oder Migration ausführen.



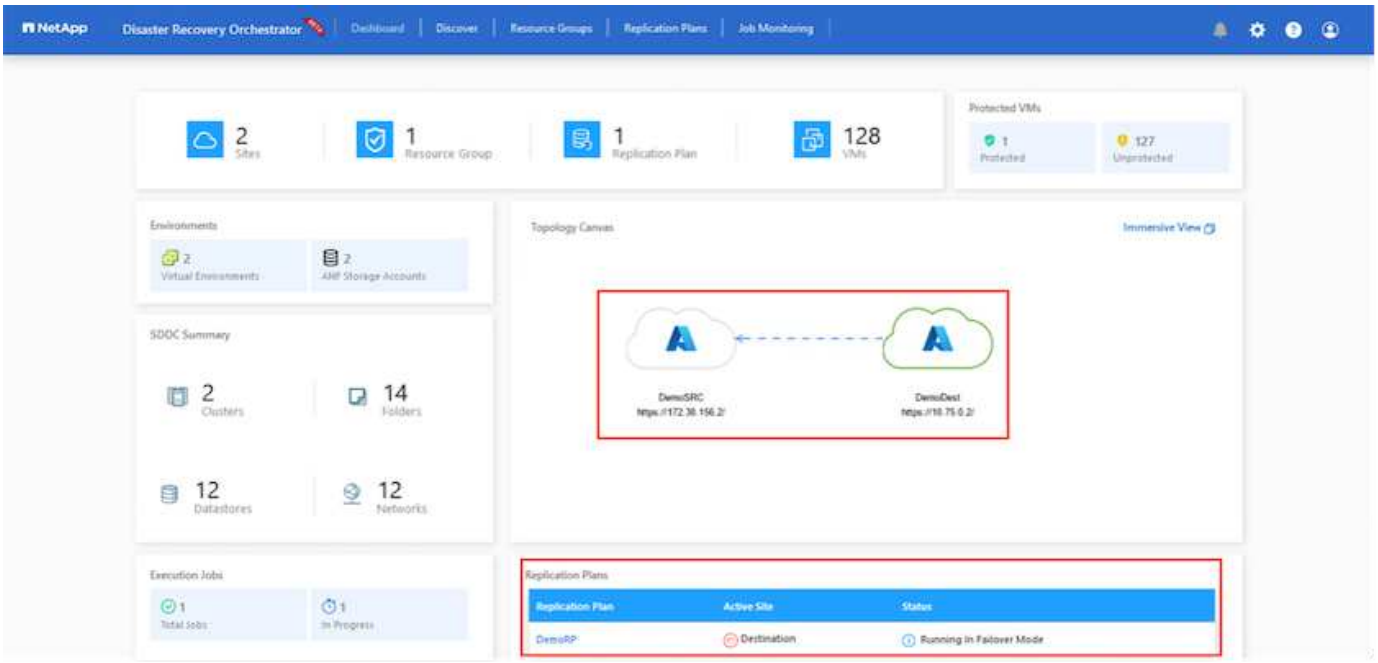
Bei den Failover- und Test-Failover-Optionen wird der aktuellste Snapshot verwendet oder es kann ein bestimmter Snapshot aus einem Point-in-Time-Snapshot ausgewählt werden. Die Point-in-Time-Option kann sehr nützlich sein, wenn Sie mit einem Korruptionsereignis wie Ransomware konfrontiert sind, bei dem die aktuellsten Replikate bereits kompromittiert oder verschlüsselt sind. DRO zeigt alle verfügbaren Zeitpunkte an.



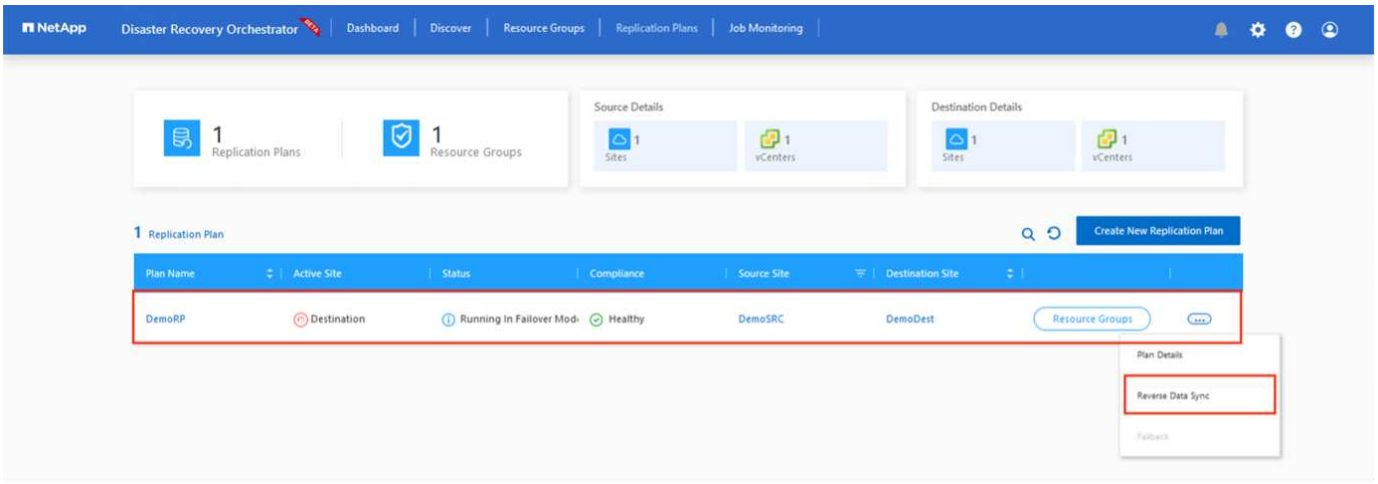
Um ein Failover auszulösen oder ein Failover mit der im Replikationsplan angegebenen Konfiguration zu testen, können Sie auf **Failover** oder **Failover testen** klicken. Sie können den Replikationsplan im Aufgabenmenü überwachen.



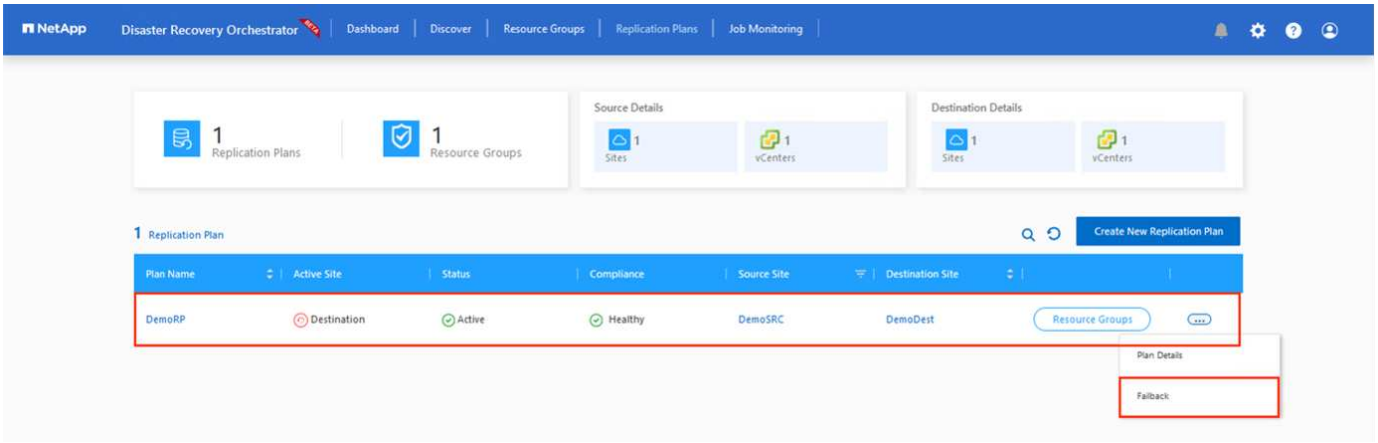
Nachdem das Failover ausgelöst wurde, können die wiederhergestellten Elemente im AVS SDDC vCenter (VMs, Netzwerke und Datenspeicher) des sekundären Standorts angezeigt werden. Standardmäßig werden die VMs im Workload-Ordner wiederhergestellt.

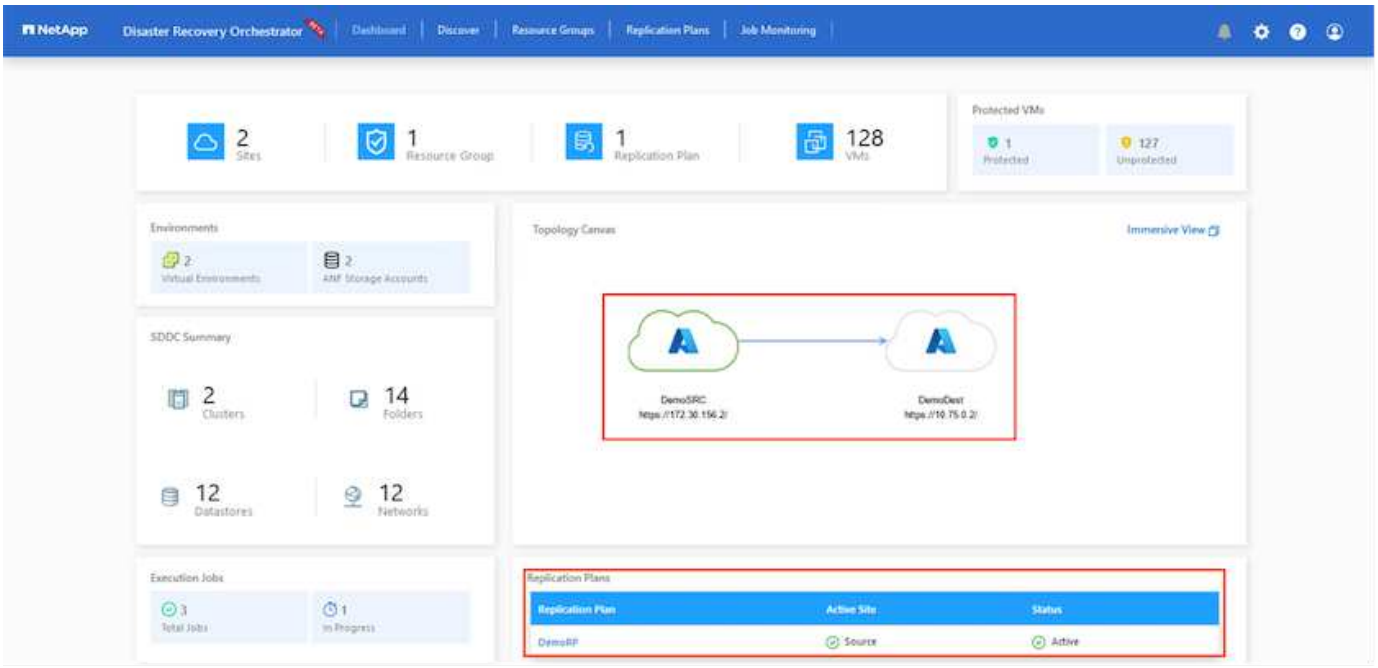


Failback kann auf der Ebene des Replikationsplans ausgelöst werden. Im Falle eines Test-Failovers kann die Teardown-Option verwendet werden, um die Änderungen rückgängig zu machen und das neu erstellte Volume zu entfernen. Failbacks im Zusammenhang mit Failover sind ein zweistufiger Prozess. Wählen Sie den Replikationsplan und dann **Reverse Data Sync** aus.



Nachdem dieser Schritt abgeschlossen ist, lösen Sie ein Failback aus, um zur primären AVS-Site zurückzukehren.





Im Azure-Portal können wir sehen, dass die Replikationsintegrität für die entsprechenden Volumes unterbrochen wurde, die dem AVS SDDC des sekundären Standorts als Lese-/Schreibvolumes zugeordnet wurden. Während des Test-Failovers ordnet DRO das Ziel- oder Replikat-Volume nicht zu. Stattdessen wird ein neues Volume des erforderlichen regionsübergreifenden Replikations-Snapshots erstellt und das Volume als Datenspeicher bereitgestellt, wodurch zusätzliche physische Kapazität aus dem Kapazitätspool verbraucht wird und sichergestellt wird, dass das Quellvolume nicht geändert wird. Insbesondere können Replikationsaufträge während DR-Tests oder Triage-Workflows fortgesetzt werden. 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.

Ransomware-Wiederherstellung

Die Wiederherstellung nach Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Organisationen schwierig sein, den sicheren Zeitpunkt der Rückkehr zu bestimmen und, sobald dieser ermittelt ist, sicherzustellen, dass wiederhergestellte Workloads vor erneuten Angriffen (beispielsweise durch ruhende Malware oder anfällige Anwendungen) geschützt sind.

DRO geht auf diese Bedenken ein, indem es Unternehmen die Wiederherstellung von jedem verfügbaren Zeitpunkt aus ermöglicht. Anschließend werden die Arbeitslasten in funktionsfähige und dennoch isolierte Netzwerke zurückgeführt, sodass die Anwendungen funktionieren und miteinander kommunizieren können,

aber keinem Nord-Süd-Verkehr ausgesetzt sind. Dieser Prozess bietet Sicherheitsteams einen sicheren Ort, um forensische Untersuchungen durchzuführen und versteckte oder schlafende Malware zu identifizieren.

Abschluss

Die Notfallwiederherstellungslösung Azure NetApp Files und Azure VMware bietet Ihnen die folgenden Vorteile:

- Nutzen Sie die effiziente und stabile regionsübergreifende Replikation von Azure NetApp Files .
- Stellen Sie mit Snapshot-Aufbewahrung einen beliebigen verfügbaren Zeitpunkt wieder her.
- Automatisieren Sie alle erforderlichen Schritte vollständig, um Hunderte bis Tausende von VMs aus den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung wiederherzustellen.
- Bei der Workload-Wiederherstellung wird der Prozess „Neue Volumes aus den aktuellsten Snapshots erstellen“ genutzt, bei dem das replizierte Volume nicht manipuliert wird.
- Vermeiden Sie jegliches Risiko einer Datenbeschädigung auf den Volumes oder Snapshots.
- Vermeiden Sie Replikationsunterbrechungen während DR-Test-Workflows.
- Nutzen Sie DR-Daten und Cloud-Rechenressourcen für Workflows, die über DR hinausgehen, wie etwa Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests sowie Fehlerbehebungstests.
- Durch die CPU- und RAM-Optimierung können die Cloud-Kosten gesenkt werden, da die Wiederherstellung auf kleineren Computerclustern möglich ist.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Informationen finden Sie in den folgenden Dokumenten und/oder auf den folgenden Websites:

- Erstellen einer Volumereplikation für Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Regionenübergreifende Replikation 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"

- Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf Azure

  "AVS auf Azure einrichten"

- Bereitstellen und Konfigurieren der Azure VMware-Lösung

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Verwenden der Veeam-Replikation und des Azure NetApp Files -Datenspeichers für die Notfallwiederherstellung in Azure VMware Solution

Azure NetApp Files (ANF)-Datenspeicher entkoppeln Speicher und Rechenleistung und ermöglichen jedem Unternehmen die nötige Flexibilität, um seine Workloads in die Cloud

zu verlagern. Es bietet Kunden eine flexible, leistungsstarke Speicherinfrastruktur, die unabhängig von den Rechenressourcen skaliert. Azure NetApp Files Datenspeicher vereinfachen und optimieren die Bereitstellung neben Azure VMware Solution (AVS) als Notfallwiederherstellungssite für lokale VMWare-Umgebungen.

Überblick

Mit NFS-Datenspeichern auf Azure NetApp Files Volumes (ANF) können Daten aus lokalen Umgebungen mithilfe jeder validierten Drittanbieterlösung, die VM-Replikationsfunktionen bietet, repliziert werden. Durch das Hinzufügen von Azure NetApp Files -Datenspeichern wird eine kostenoptimierte Bereitstellung im Vergleich zum Aufbau eines Azure VMware Solution SDDC mit einer enormen Anzahl von ESXi-Hosts zur Unterbringung des Speichers ermöglicht. Dieser Ansatz wird als „Pilot Light Cluster“ bezeichnet. Ein Pilot Light Cluster ist eine minimale AVS-Hostkonfiguration (3 x AVS-Knoten) zusammen mit der Azure NetApp Files Datastore-Kapazität.

Ziel ist die Aufrechterhaltung einer kostengünstigen Infrastruktur mit allen Kernkomponenten zur Bewältigung eines Failovers. Ein Pilot-Light-Cluster kann skaliert werden und mehr AVS-Hosts bereitstellen, wenn ein Failover auftritt. Und sobald das Failover abgeschlossen ist und der normale Betrieb wiederhergestellt ist, kann der Pilot Light-Cluster wieder auf den kostengünstigen Betriebsmodus herunterskaliert werden.

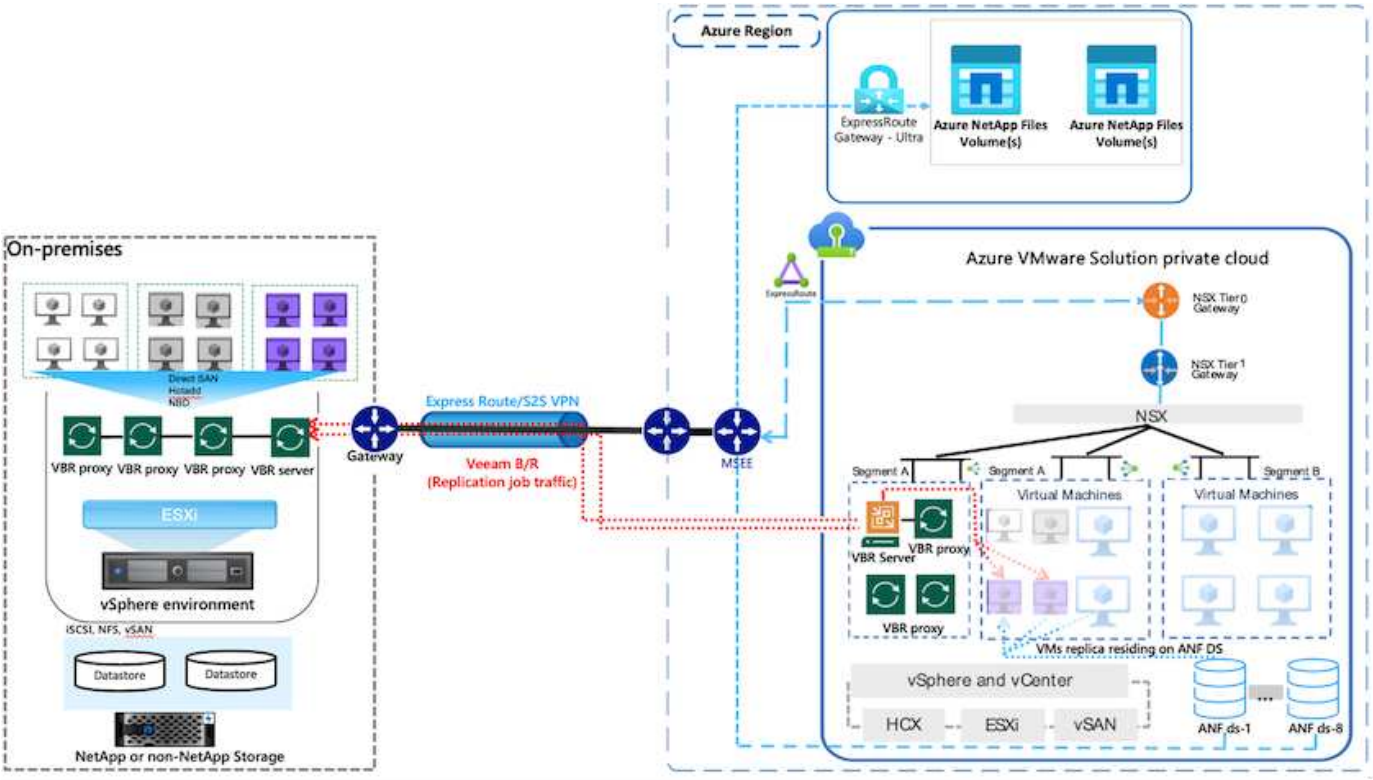
Zweck dieses Dokuments

In diesem Artikel wird beschrieben, wie Sie den Azure NetApp Files -Datenspeicher mit Veeam Backup und Replikation verwenden, um mithilfe der VM-Replikationssoftwarefunktion von Veeam die Notfallwiederherstellung für lokale VMware-VMs (AVS) einzurichten.

Veeam Backup & Replication ist eine Backup- und Replikationsanwendung für virtuelle Umgebungen. Wenn virtuelle Maschinen repliziert werden, wird Veeam Backup & Replication von AVS repliziert. Die Software erstellt 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 synchronisiert. Die Replikation bietet die beste Wiederherstellungszeit (RTO), da am DR-Standort eine bereitgestellte Kopie einer VM in einem startbereiten Zustand vorhanden ist.

Dieser Replikationsmechanismus stellt sicher, dass die Workloads im Katastrophenfall schnell in einem AVS SDDC gestartet werden können. Die Veeam Backup & Replication-Software optimiert außerdem die Verkehrsübertragung für die Replikation über WAN und langsame Verbindungen. Darüber hinaus filtert es auch doppelte Datenblöcke, Null-Datenblöcke, Auslagerungsdateien und „ausgeschlossene VM-Gastbetriebssystemdateien“ heraus. Die Software komprimiert außerdem den Replikationsverkehr. Um zu verhindern, dass Replikationsaufträge die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Netzwerkdrosselungsregeln verwendet werden.

Der Replikationsprozess in Veeam Backup & Replication ist auftragsgesteuert, d. h. die Replikation wird durch die Konfiguration von Replikationsaufträgen durchgeführt. Im Katastrophenfall kann ein Failover ausgelöst werden, um die VMs durch ein Failover auf ihre Replikatkopie wiederherzustellen. Beim Failover übernimmt eine replizierte VM die Rolle der ursprünglichen VM. Das Failover kann auf den neuesten Stand einer Replik oder auf einen ihrer bekannten Wiederherstellungspunkte durchgeführt werden. Dies ermöglicht bei Bedarf eine Ransomware-Wiederherstellung oder isolierte Tests. Veeam Backup & Replication bietet mehrere Optionen zur Handhabung verschiedener Notfallwiederherstellungsszenarien.



Lösungsbereitstellung

Schritte auf hohem Niveau

1. Die Veeam Backup and Replication-Software wird in einer lokalen Umgebung mit entsprechender Netzwerkkonnektivität ausgeführt.
2. "Bereitstellen von Azure VMware Solution (AVS)"Private Cloud und"Azure NetApp Files Datenspeicher anhängen" zu Azure VMware Solution-Hosts.

   Eine Pilot-Light-Umgebung mit minimaler Konfiguration kann für DR-Zwecke verwendet werden. Im Falle eines Vorfalls erfolgt ein Failover der VMs auf diesen Cluster und es können zusätzliche Knoten hinzugefügt werden.

3. Richten Sie einen Replikationsjob ein, um VM-Replikate mit Veeam Backup and Replication zu erstellen.
4. Erstellen Sie einen Failover-Plan und führen Sie das Failover durch.
5. Wechseln Sie zurück zu Produktions-VMs, sobald das Notfallereignis abgeschlossen ist und die primäre Site aktiv ist.

Voraussetzungen für die Veeam VM-Replikation in AVS- und ANF-Datenspeicher

1. Stellen Sie sicher, dass die Veeam Backup & Replication-Sicherungs-VM sowohl mit den Quell- als auch mit den Ziel-AVS-SDDC-Clustern verbunden ist.
2. Der Sicherungsserver muss in der Lage sein, Kurznamen aufzulösen und eine Verbindung zu Quell- und Ziel-vCentern herzustellen.
3. Der Zieldatenspeicher von Azure NetApp Files muss über genügend freien Speicherplatz verfügen, um VMDKs replizierter VMs zu speichern.

Weitere Informationen finden Sie unter "Überlegungen und Einschränkungen""hier," .

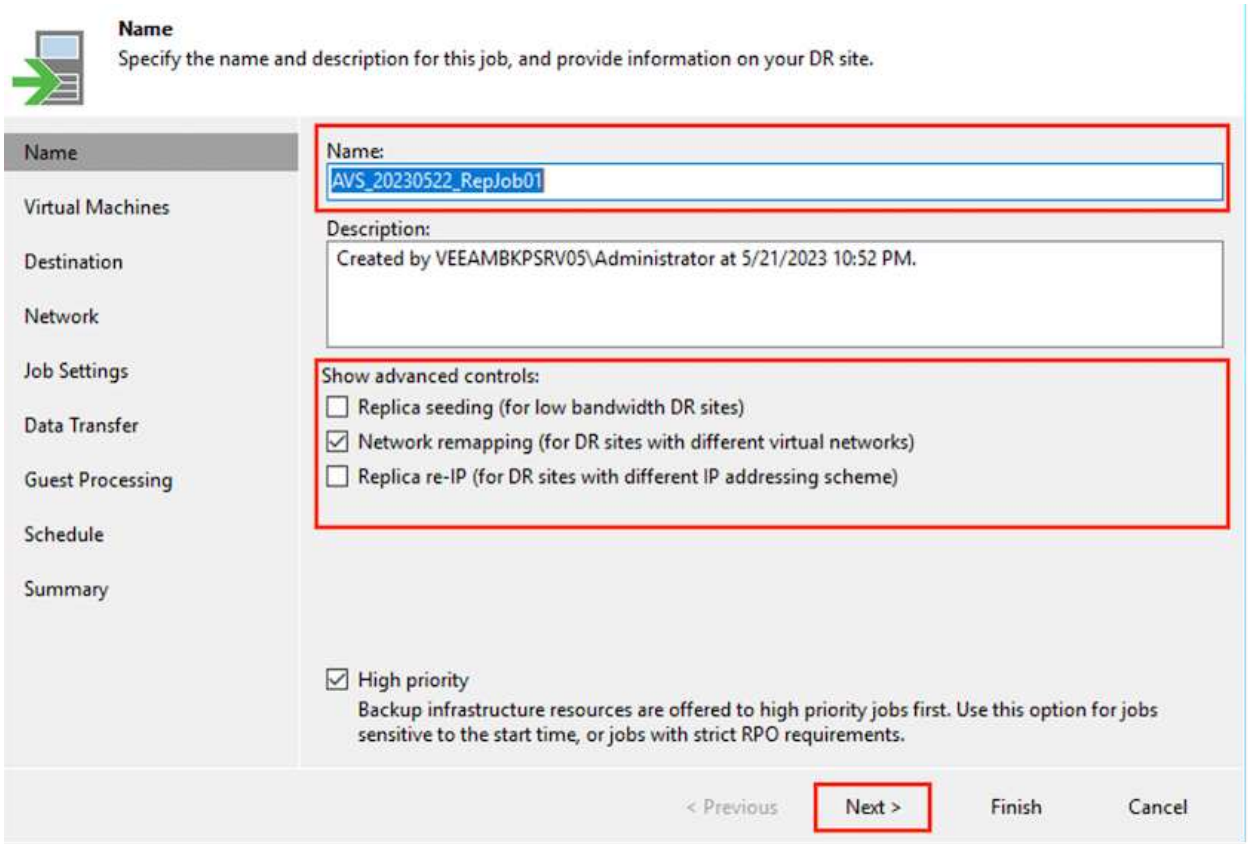
Bereitstellungsdetails

▼ **Schritt 1: VMs replizieren**

Veeam Backup & Replication nutzt die Snapshot-Funktionen von VMware vSphere. Während der Replikation fordert Veeam Backup & Replication VMware vSphere auf, einen VM-Snapshot zu erstellen. Der VM-Snapshot ist die zeitpunktbezogene Kopie einer VM, die virtuelle Festplatten, Systemstatus, Konfiguration und Metadaten enthält. Veeam Backup & Replication verwendet den Snapshot als Datenquelle für die Replikation.

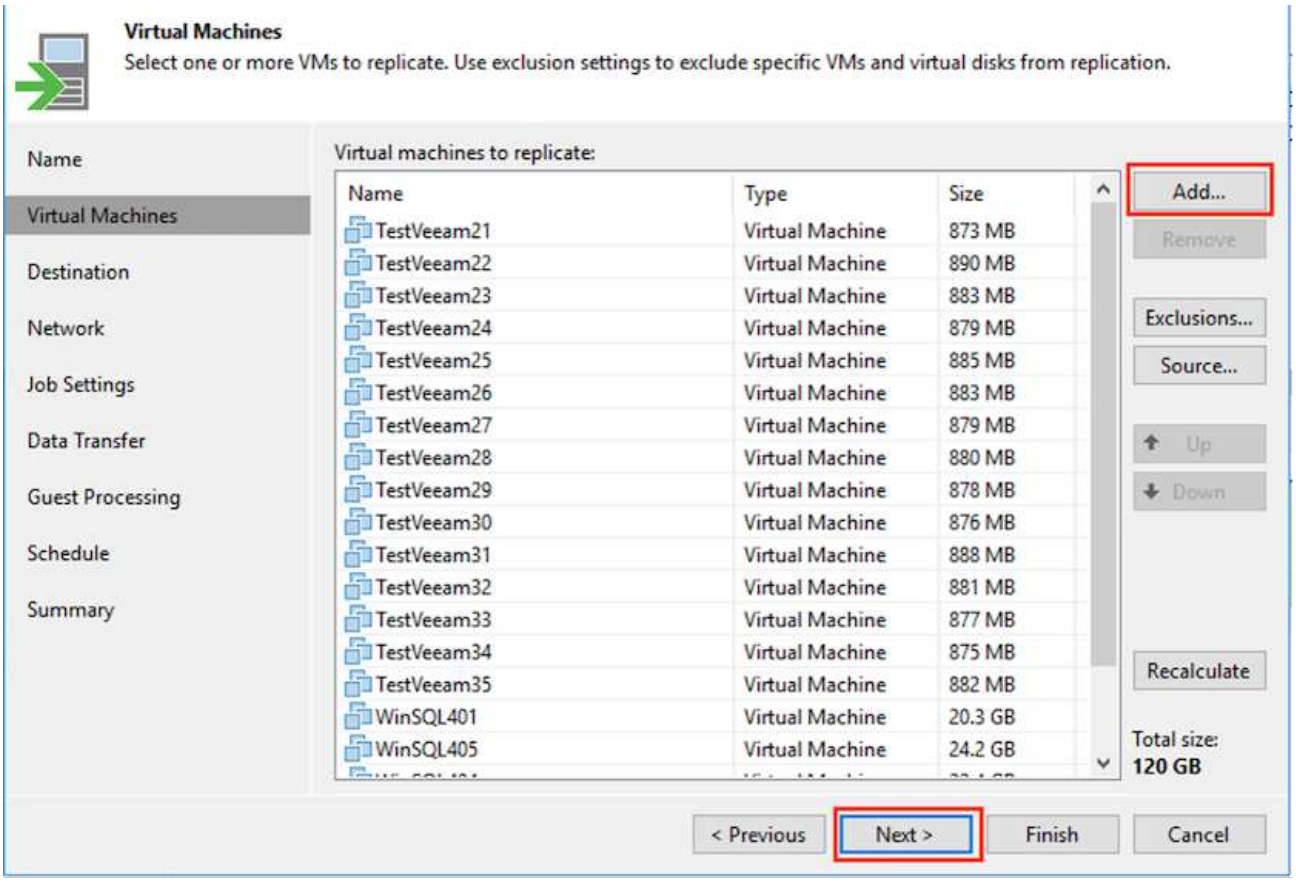
Führen Sie zum Replizieren von VMs die folgenden Schritte aus:

1. Öffnen Sie die Veeam Backup & Replication-Konsole.
2. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Jobknoten und wählen Sie „Replikationsjob“ > „Virtuelle Maschine“.
3. Geben Sie einen Auftragsnamen an und aktivieren Sie das entsprechende Kontrollkästchen für die erweiterte Steuerung. Klicken Sie auf Weiter.
   - Aktivieren Sie das Kontrollkästchen „Replikat-Seeding“, wenn die Bandbreite der Konnektivität zwischen der lokalen Umgebung und Azure eingeschränkt ist. *Aktivieren Sie das Kontrollkästchen „Netzwerkneuzuordnung (für AVS SDDC-Sites mit unterschiedlichen Netzwerken), wenn die Segmente auf Azure VMware Solution SDDC nicht mit denen der lokalen Site-Netzwerke übereinstimmen.
   - Wenn sich das IP-Adressschema am lokalen Produktionsstandort vom Schema am AVS-Zielstandort unterscheidet, aktivieren Sie das Kontrollkästchen „Replikat-Re-IP (für DR-Standorte mit anderem IP-Adressschema)“.

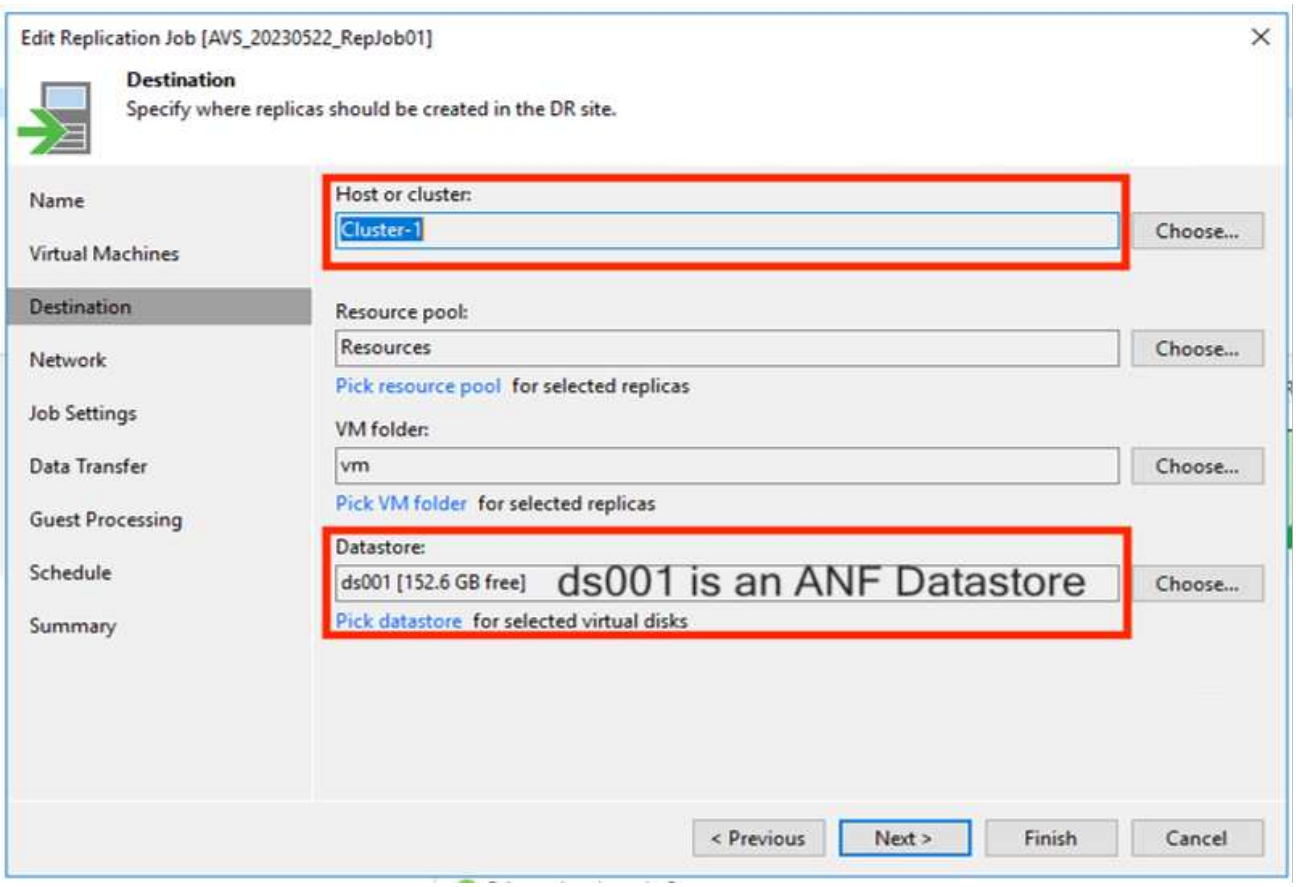


4. Wählen Sie im Schritt „Virtuelle Maschinen“ die VMs aus, die in den Azure NetApp Files -Datenspeicher repliziert werden sollen, der an ein Azure VMware Solution SDDC angehängt ist. Die virtuellen

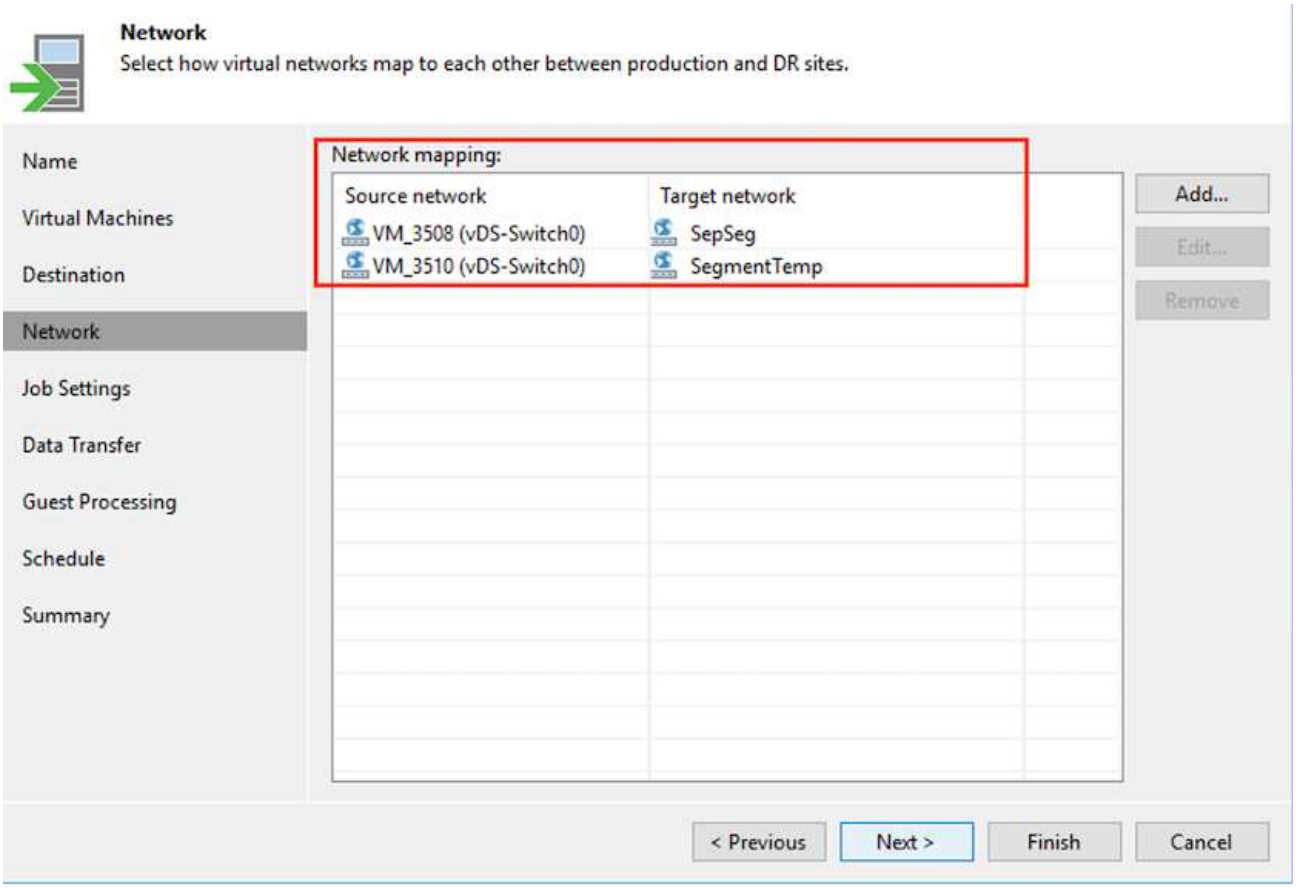
Maschinen können auf vSAN platziert werden, um die verfügbare vSAN-Datenspeicherkapazität zu füllen. In einem Pilotlichtcluster ist die nutzbare Kapazität eines 3-Knoten-Clusters begrenzt. Die restlichen Daten können problemlos in Azure NetApp Files -Datenspeichern abgelegt werden, sodass die VMs wiederhergestellt und der Cluster erweitert werden kann, um die CPU-/Speicheranforderungen 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**.



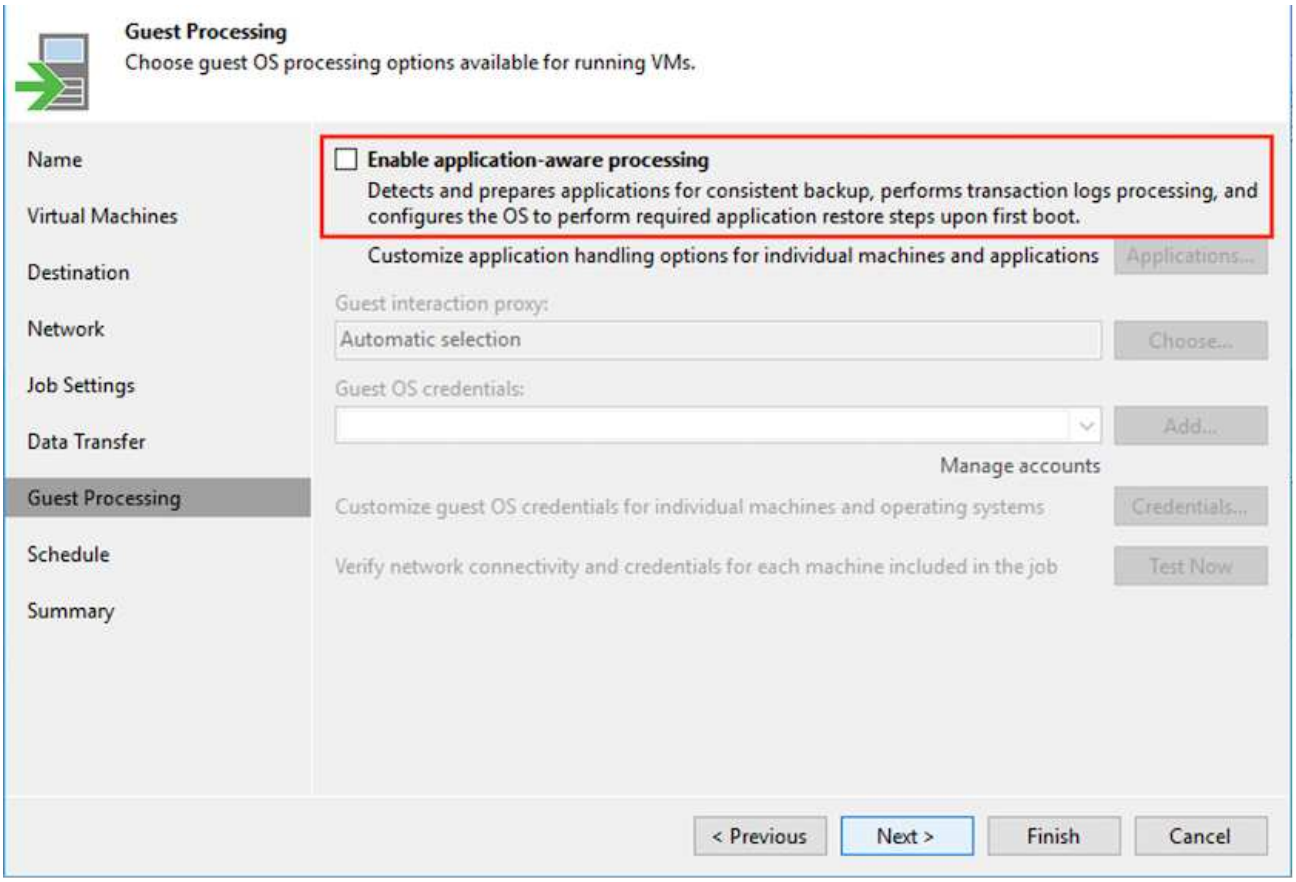
5. Wählen Sie anschließend das Ziel als Azure VMware Solution SDDC-Cluster/Host und den entsprechenden Ressourcenpool, VM-Ordner und FSx ONTAP -Datenspeicher für VM-Replikate aus. Klicken Sie dann auf **Weiter**.



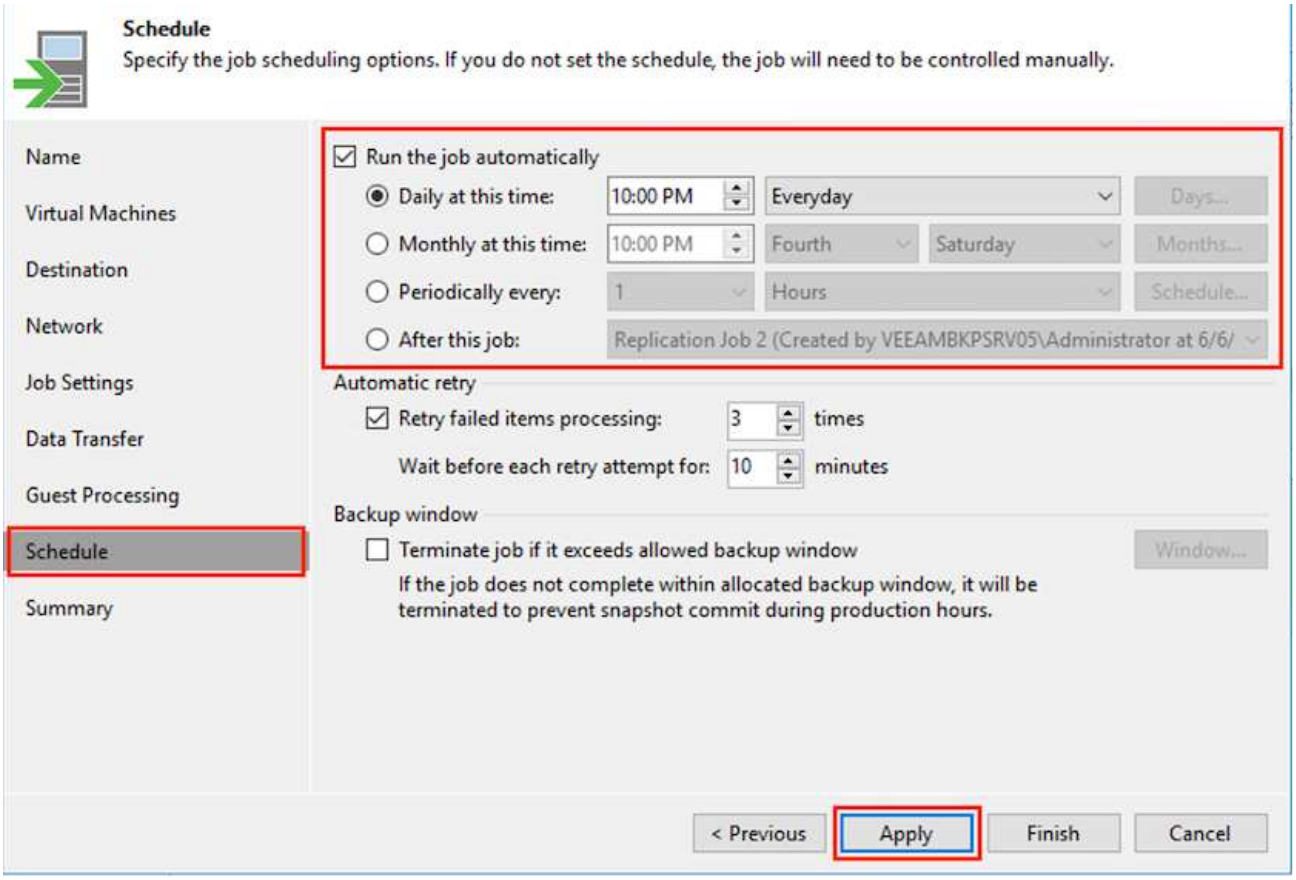
6. Erstellen Sie im nächsten Schritt nach Bedarf die Zuordnung zwischen Quell- und Ziel-Virtual-Network.



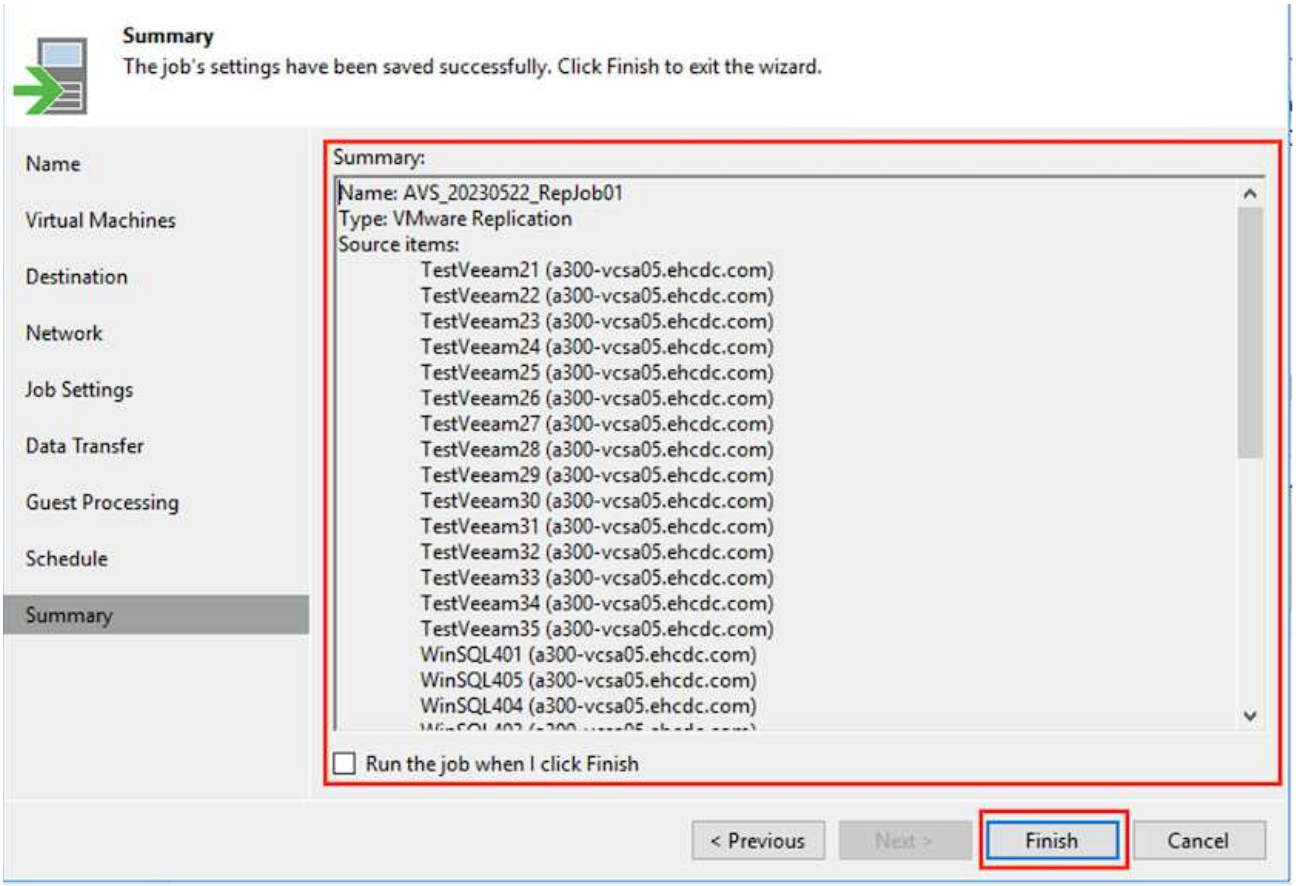
7. Geben Sie im Schritt **Jobeinstellungen** das Sicherungsrepository an, in dem Metadaten für VM-Replikate, Aufbewahrungsrichtlinien usw. gespeichert werden.
8. Aktualisieren Sie die **Quell-** und **Ziel-**Proxyserver im Schritt **Datenübertragung**, belassen Sie die Auswahl **Automatisch** (Standard), lassen Sie die Option **Direkt** ausgewählt und klicken Sie auf **Weiter**.
9. Wählen Sie im Schritt **Gastverarbeitung** nach Bedarf die Option **Anwendungsbewusste Verarbeitung aktivieren**. Klicken Sie auf **Weiter**.



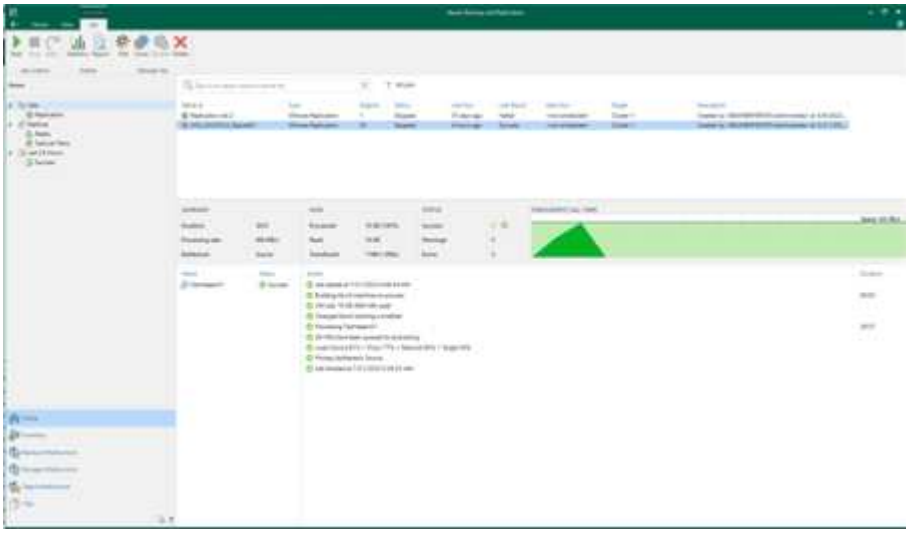
10. Wählen Sie den Replikationszeitplan aus, um den Replikationsauftrag regelmäßig auszuführen.



11. Überprüfen Sie im Schritt **Zusammenfassung** des Assistenten die Details des Replikationsauftrags. 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**, um den Assistenten zu schließen.



Sobald der Replikationsauftrag startet, werden die VMs mit dem angegebenen Suffix auf dem Ziel-AVS-SDDC-Cluster/-Host aufgefüllt.



Weitere Informationen zur Veeam-Replikation finden Sie unter"Funktionsweise der Replikation"

▼ **Schritt 2: Erstellen eines Failoverplans**

Wenn die erste Replikation oder das Seeding abgeschlossen ist, erstellen Sie den Failover-Plan. Der Failover-Plan hilft dabei, das Failover für abhängige VMs einzeln oder als Gruppe automatisch durchzuführen. Der Failover-Plan ist die Blaupause für die Reihenfolge, in der die VMs verarbeitet werden, einschließlich der Startverzögerungen. Der Failover-Plan hilft auch sicherzustellen, dass kritische abhängige VMs bereits ausgeführt werden.

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 zum Starten von VM-Replikaten.

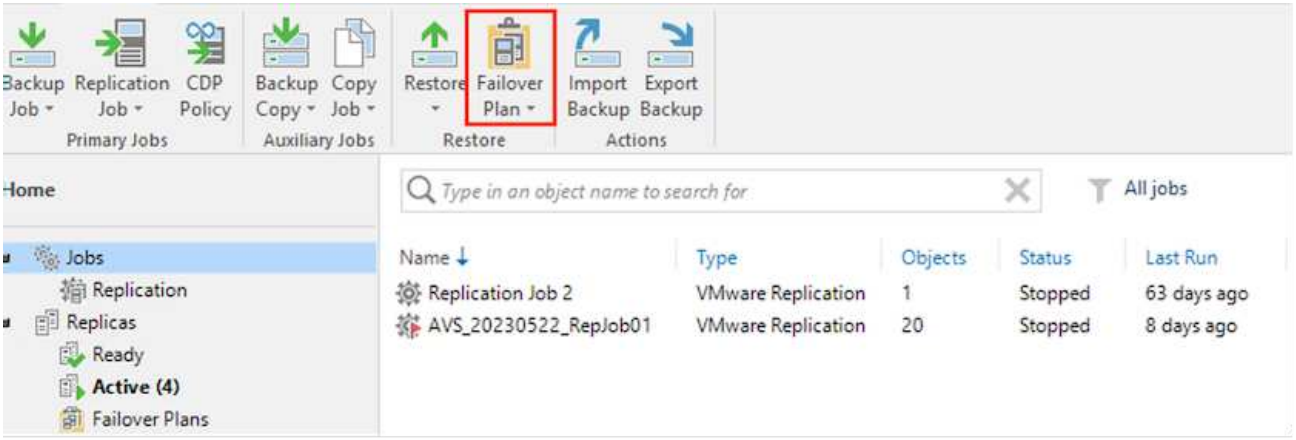
Der Failover-Plan kann erst hinzugefügt werden, wenn die erste Replikation abgeschlossen ist und sich die VM-Replikate im Status „Bereit“ befinden.

Die maximale Anzahl VMs, die beim Ausführen eines Failover-Plans gleichzeitig gestartet werden können, beträgt 10

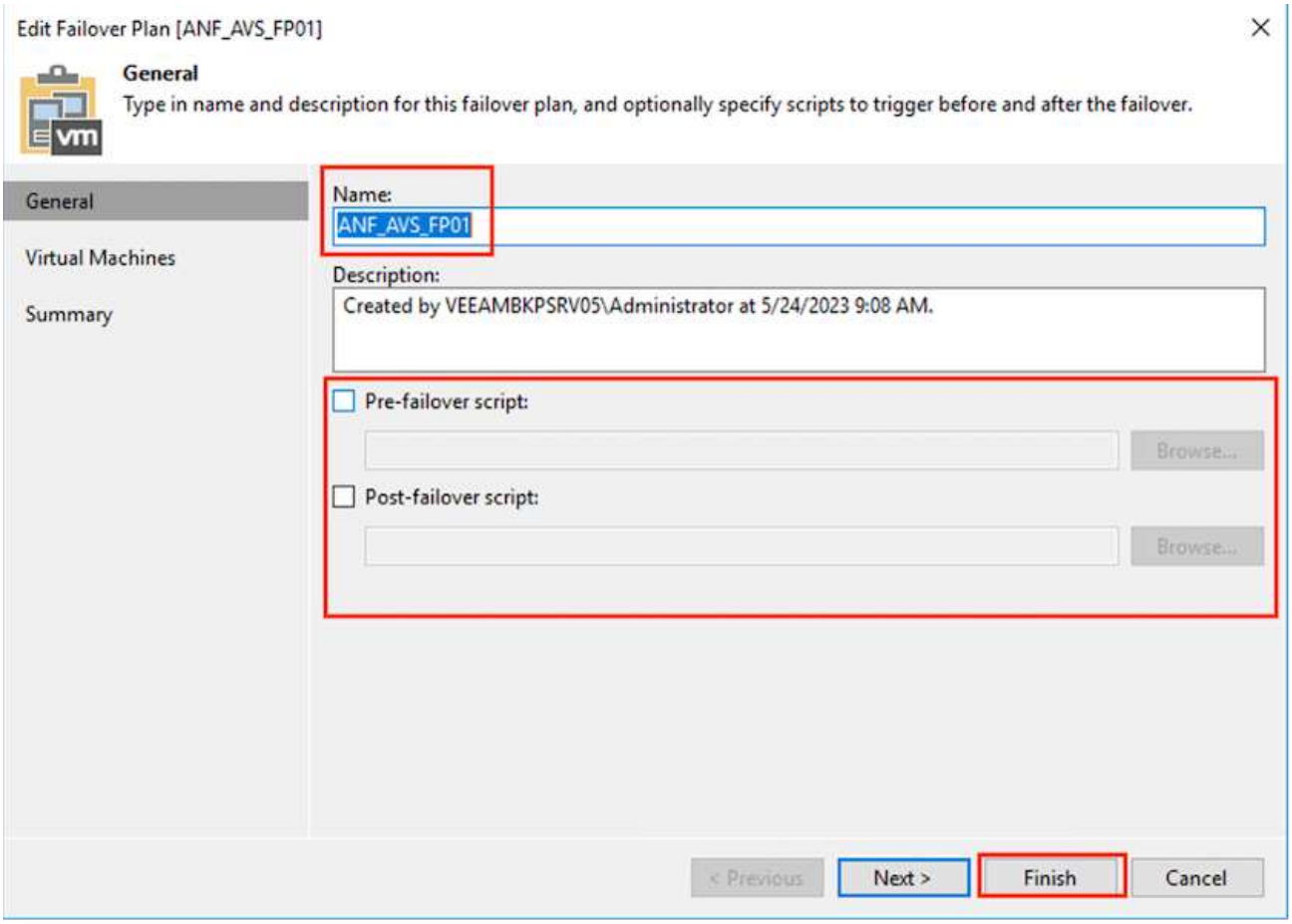
Während des Failover-Prozesses werden die Quell-VMs nicht ausgeschaltet

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

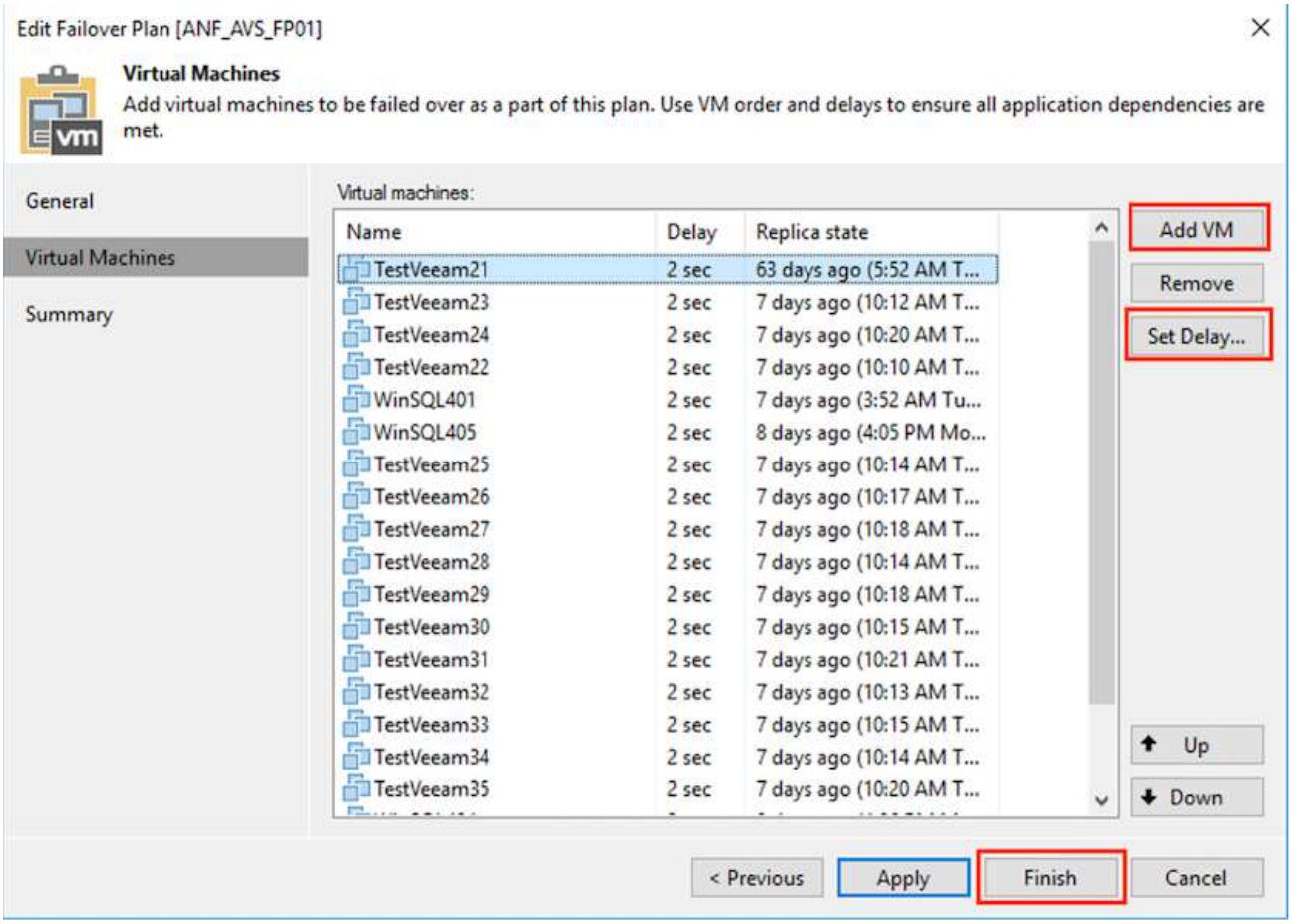
1. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Knoten „Replikate“ und wählen Sie „Failover-Pläne“ > „Failover-Plan“ > „VMware vSphere“.



2. Geben Sie als Nächstes einen Namen und eine Beschreibung für den Plan ein. Bei Bedarf können Skripte vor und nach dem Failover hinzugefügt werden. Führen Sie beispielsweise ein Skript aus, um VMs herunterzufahren, bevor Sie die replizierten VMs starten.



3. Fügen Sie die VMs zum Plan hinzu und ändern Sie die Startreihenfolge und Startverzögerungen der VM, um die Anwendungsabhängigkeiten zu erfüllen.



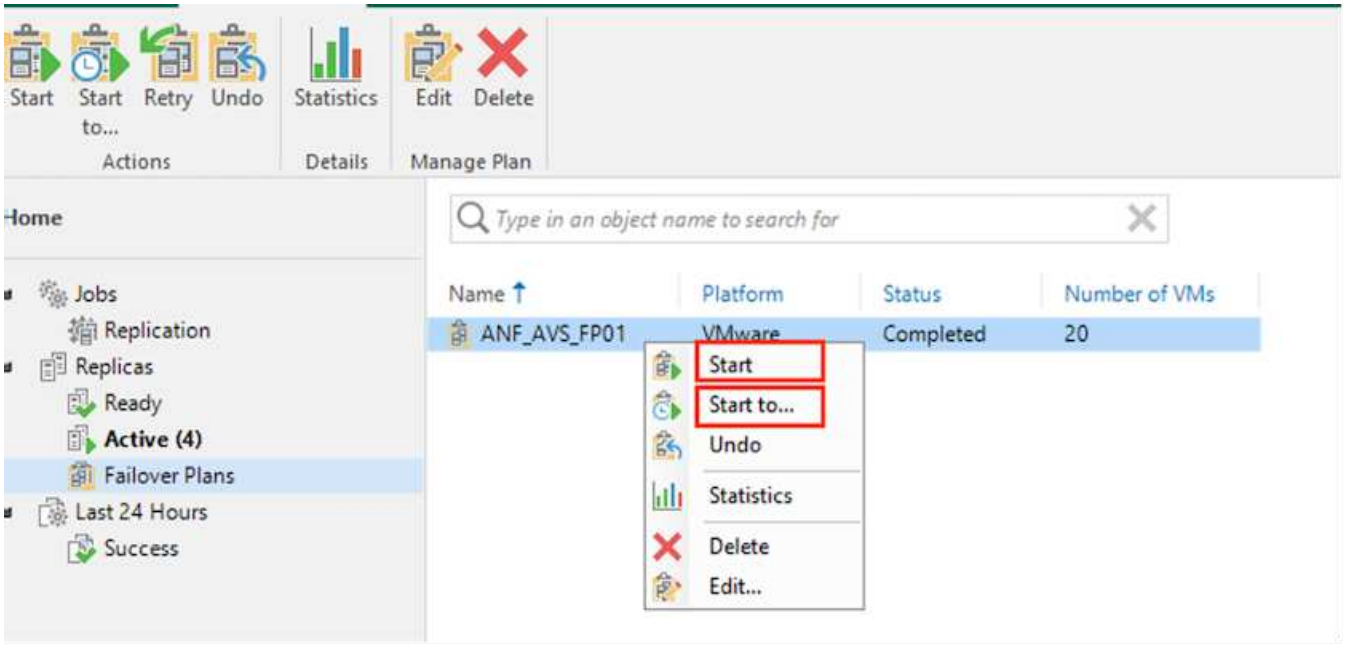
Weitere Informationen zum Erstellen von Replikationsaufträgen finden Sie unter"Erstellen von Replikationsjobs" .

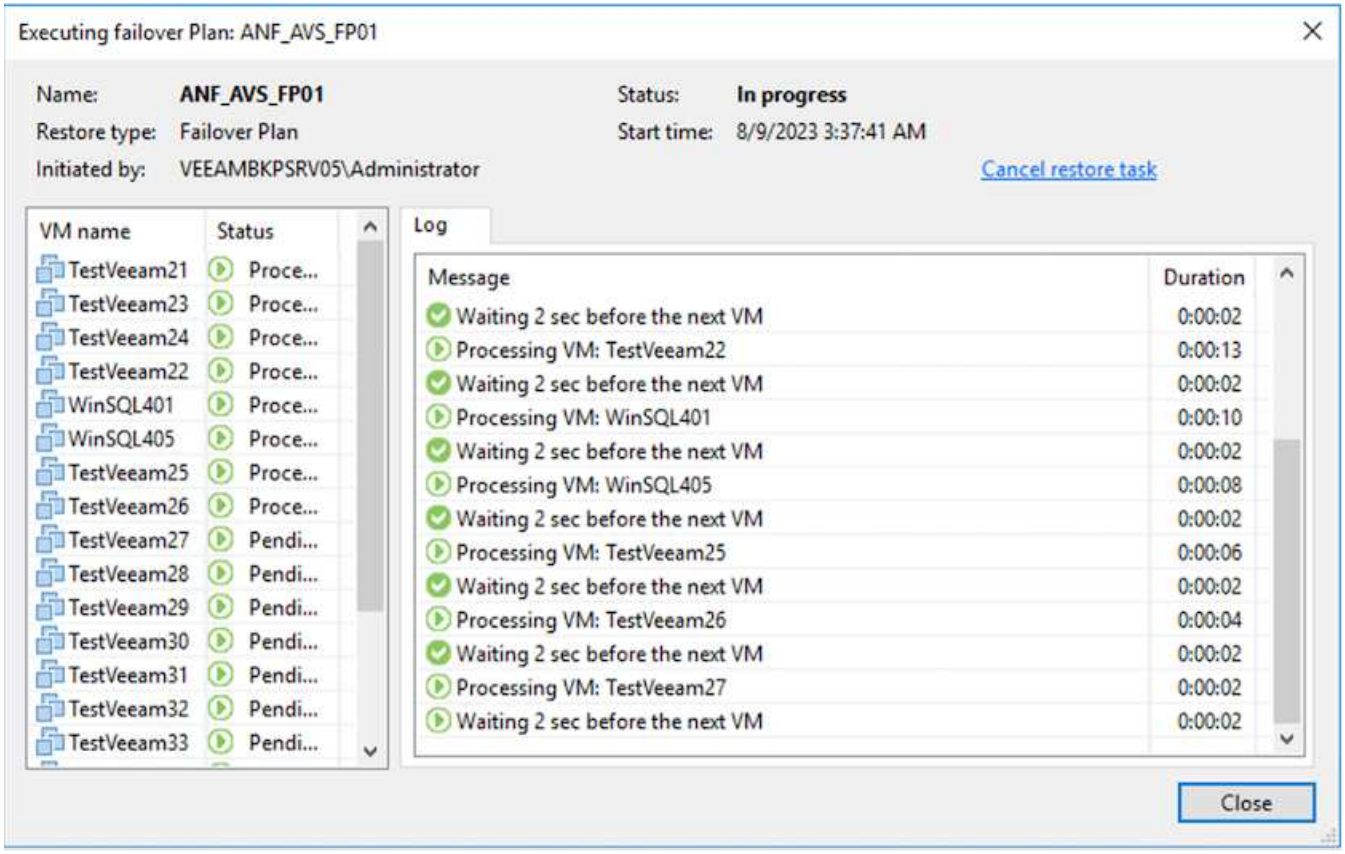
▼ Schritt 3: Ausführen des Failoverplans

Während des Failovers wird die Quell-VM am Produktionsstandort auf ihre Replik am Disaster-Recovery-Standort umgeschaltet. Als Teil des Failover-Prozesses stellt Veeam Backup & Replication die VM-Replik am erforderlichen Wiederherstellungspunkt wieder her und verschiebt alle E/A-Aktivitäten von der Quell-VM auf ihre Replik. Replikate können nicht nur im Katastrophenfall, sondern auch zur Simulation von DR-Übungen verwendet werden. Während der Failover-Simulation läuft die Quell-VM weiter. Sobald alle erforderlichen Tests durchgeführt wurden, können Sie das Failover rückgängig machen und zum Normalbetrieb zurückkehren.

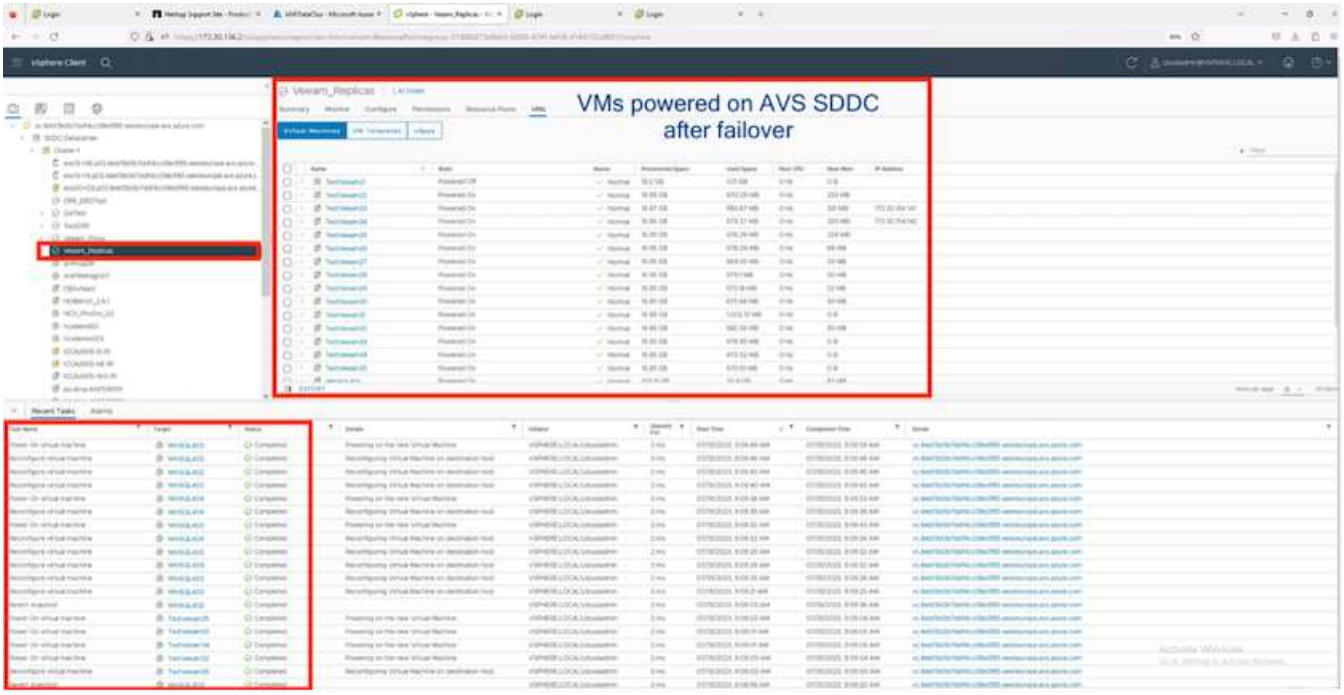
ⓘ Stellen Sie sicher, dass eine Netzwerksegmentierung vorhanden ist, um IP-Konflikte während des Failovers zu vermeiden.

Um den Failover-Plan zu starten, klicken Sie einfach auf die Registerkarte **Failover-Pläne** und klicken Sie mit der rechten Maustaste auf Ihren Failover-Plan. Wählen Sie ***Start**. Dabei wird ein Failover unter Verwendung der neuesten Wiederherstellungspunkte der VM-Replikate durchgeführt. Um ein Failover auf bestimmte Wiederherstellungspunkte von VM-Replikaten durchzuführen, wählen Sie **Starten mit**.

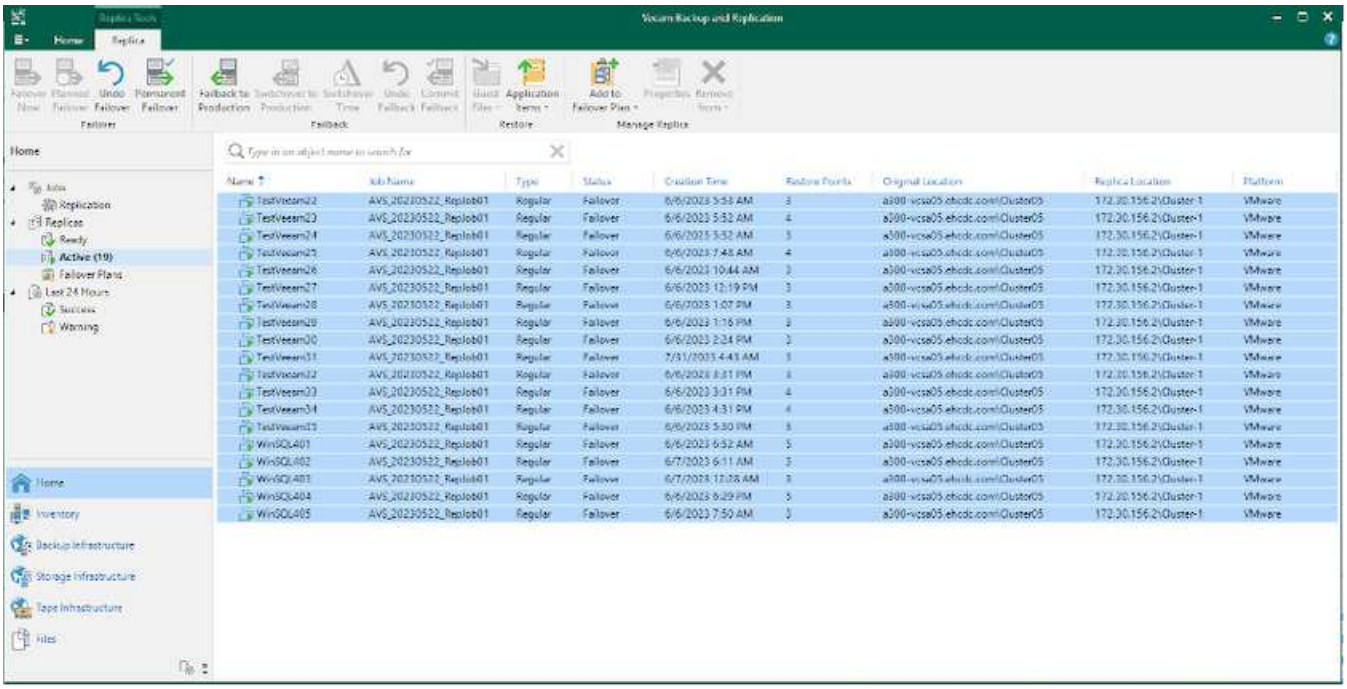




Der Status der VM-Replik ändert sich von „Bereit“ in „Failover“ und die VMs werden auf dem Ziel-SDDC-Cluster/-Host der Azure VMware Solution (AVS) gestartet.



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



Veeam Backup & Replication stoppt alle Replikationsaktivitäten für die Quell-VM, bis deren Replikat wieder in den Zustand „Bereit“ versetzt wird.

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

▼ **Schritt 4: Failback zur Produktionssite**

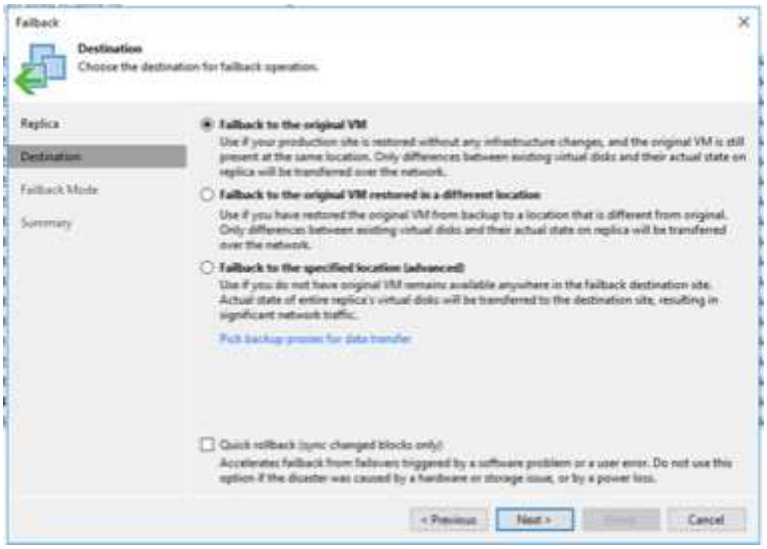
Wenn der Failover-Plan ausgeführt wird, wird er als Zwischenschritt betrachtet und muss je nach Bedarf abgeschlossen werden. Zu den Optionen gehören die folgenden:

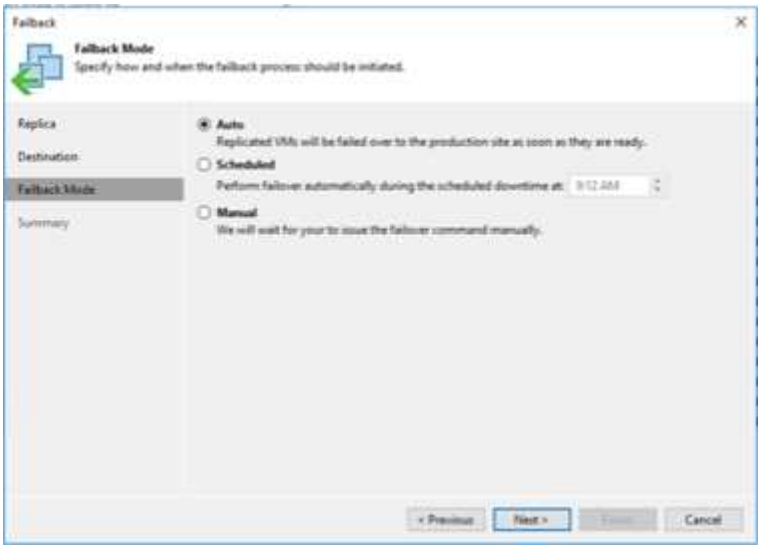
- **Failback zur Produktion** – Wechseln Sie zurück zur ursprünglichen VM und übertragen Sie alle Änderungen, die während der Ausführung der VM-Replik vorgenommen wurden, auf die ursprüngliche VM.

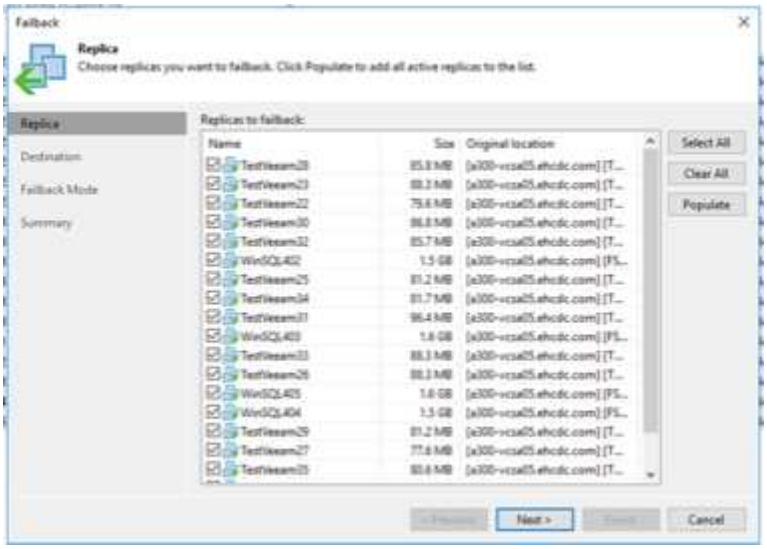
> Wenn Sie ein Failback durchführen, werden Änderungen nur übertragen, aber nicht veröffentlicht. Wählen Sie **Failback festschreiben** (sobald bestätigt wurde, dass die ursprüngliche VM wie erwartet funktioniert) oder „Failback rückgängig machen“, um zur VM-Replik zurückzukehren, wenn die ursprüngliche VM nicht wie erwartet funktioniert.

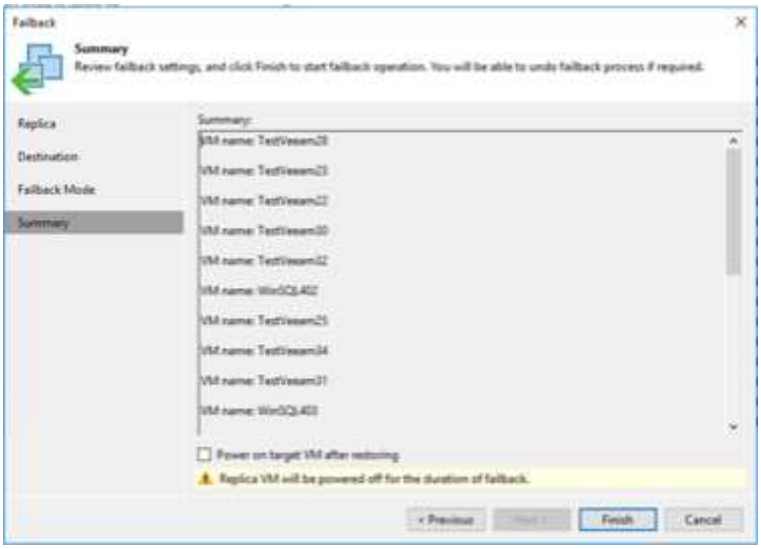
- **Failover rückgängig machen** – Wechseln Sie zurück zur ursprünglichen VM und verwerfen Sie alle Änderungen, die während der Ausführung an der VM-Replik vorgenommen wurden.
- **Permanentes Failover** – Wechseln Sie dauerhaft von der Original-VM zu einer VM-Replik und verwenden Sie diese Replik als Original-VM.

In dieser Demo wurde Failback zur Produktion ausgewählt. Im Schritt „Ziel“ des Assistenten wurde ein Failback zur ursprünglichen VM ausgewählt und das Kontrollkästchen „VM nach der Wiederherstellung einschalten“ aktiviert.



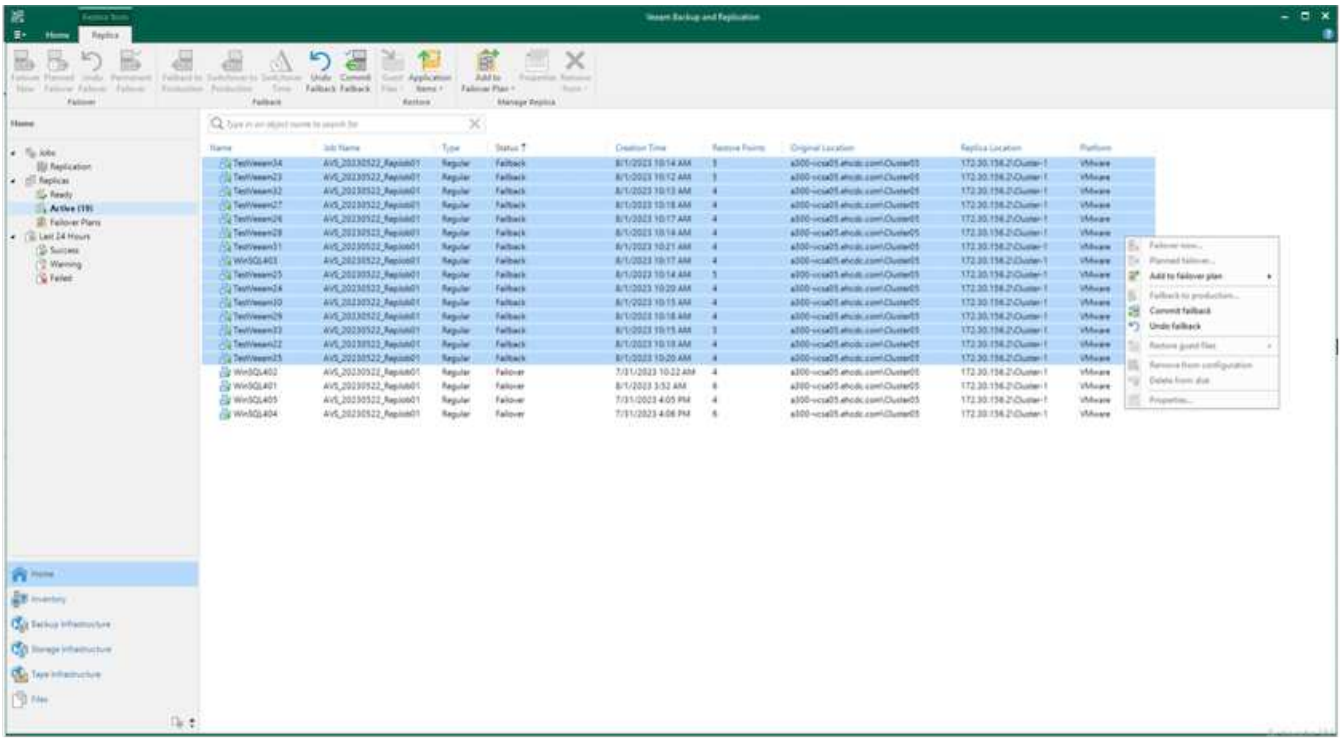




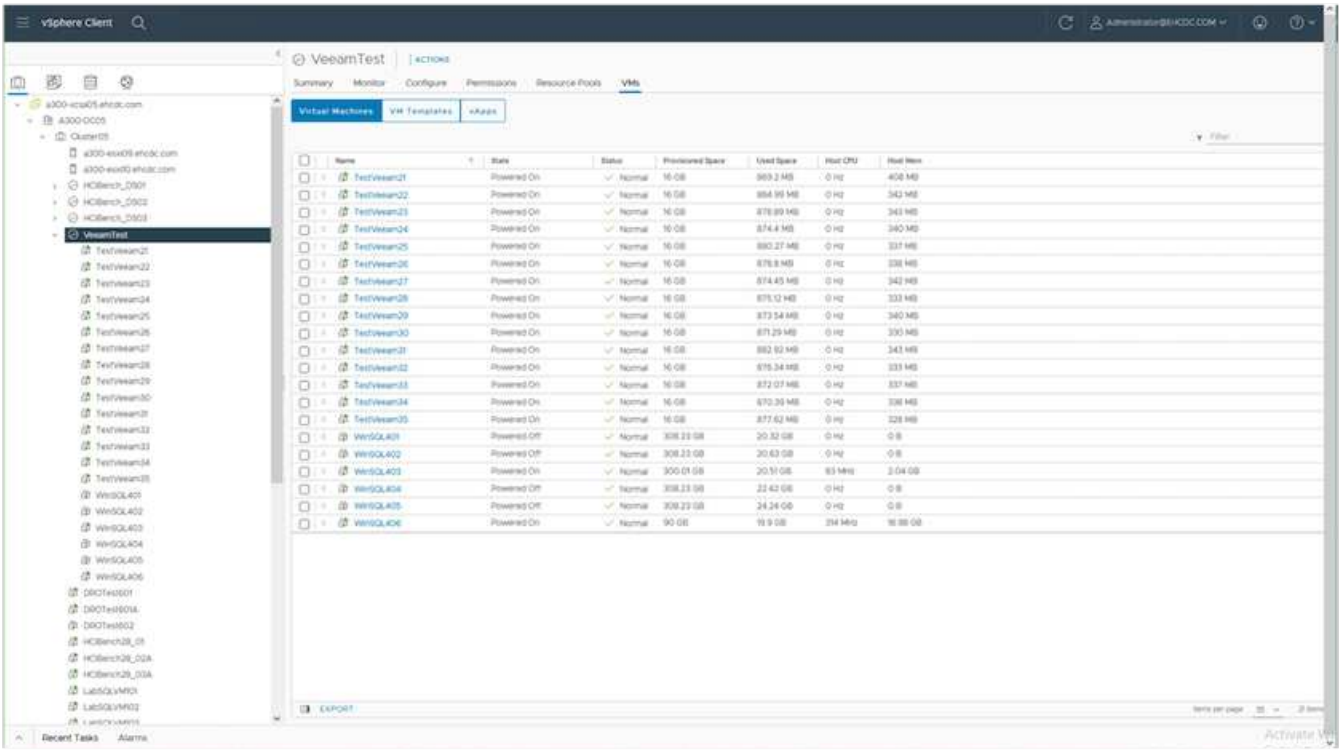


Failback-Commit ist eine der Möglichkeiten, den Failback-Vorgang abzuschließen. Wenn das Failback ausgeführt wird, wird bestätigt, dass die an die VM gesendeten Änderungen, für die das Failback ausgeführt wird (die Produktions-VM), wie erwartet funktionieren. Nach dem Commit-Vorgang nimmt Veeam Backup & Replication die Replikationsaktivitäten für die Produktions-VM wieder auf.

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



Nach einem erfolgreichen Failback zur Produktion werden alle VMs wieder am ursprünglichen Produktionsstandort wiederhergestellt.



Abschluss

Die Azure NetApp Files -Datenspeicherfunktion ermöglicht es Veeam oder jedem validierten Drittanbietertool, eine kostengünstige DR-Lösung bereitzustellen, indem Pilot Light-Cluster genutzt werden, anstatt einen großen Cluster nur zur Aufnahme von VM-Replikaten einzurichten. Dies bietet eine effiziente Möglichkeit, einen maßgeschneiderten Notfallwiederherstellungsplan zu erstellen und vorhandene Backup-Produkte im

Unternehmen für die Notfallwiederherstellung wiederzuverwenden. Dadurch wird eine Cloud-basierte Notfallwiederherstellung durch Verlassen der lokalen Notfallwiederherstellungs-Rechenzentren ermöglicht. Im Katastrophenfall ist ein Failover per Knopfdruck oder im Katastrophenfall ein automatisches Failover möglich.

Um mehr über diesen Vorgang zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Migrieren von Workloads auf Azure/AVS

TR-4940: Migrieren von Workloads zum Azure NetApp Files Datenspeicher mithilfe von VMware HCX – Kurzanleitung

Einer der häufigsten Anwendungsfälle für die Azure VMware Solution und den Azure NetApp Files -Datenspeicher ist die Migration von VMware-Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmechanismen zum Verschieben lokaler virtueller Maschinen (VMs) und ihrer Daten in Azure NetApp Files -Datenspeicher.

Übersicht: Migrieren virtueller Maschinen mit VMware HCX, Azure NetApp Files Datenspeichern und Azure VMware-Lösung

VMware HCX ist in erster Linie eine Migrationsplattform, die die Anwendungsmigration, die Neuverteilung der Arbeitslast und sogar die Geschäftskontinuität über Clouds hinweg vereinfachen soll. Es ist Teil der Azure VMware Solution Private Cloud und bietet viele Möglichkeiten zum Migrieren von Workloads und kann für Disaster Recovery-Vorgänge (DR) verwendet werden.

Dieses Dokument enthält eine Schritt-für-Schritt-Anleitung zum Bereitstellen des Azure NetApp Files -Datenspeichers, gefolgt vom Herunterladen, Bereitstellen und Konfigurieren von VMware HCX, einschließlich aller Hauptkomponenten vor Ort und auf der Azure VMware Solution-Seite, einschließlich Interconnect, Netzwerkerweiterung und WAN-Optimierung zum Aktivieren verschiedener VM-Migrationsmechanismen.

> VMware HCX funktioniert mit jedem Datenspeichertyp, da die Migration auf VM-Ebene erfolgt. Daher ist dieses Dokument für bestehende NetApp -Kunden und Nicht- NetApp -Kunden relevant, die Azure NetApp Files mit Azure VMware Solution für eine kostengünstige VMware-Cloud-Bereitstellung bereitstellen möchten.

▼ Schritte auf hoher Ebene

Diese Liste enthält die allgemeinen Schritte, die zum Installieren und Konfigurieren von HCX Cloud Manager auf der Azure-Cloudseite und zum Installieren von HCX Connector vor Ort erforderlich sind:

1. Installieren Sie HCX über das Azure-Portal.
2. Laden Sie das HCX Connector Open Virtualization Appliance (OVA)-Installationsprogramm herunter und stellen Sie es auf dem lokalen VMware vCenter Server bereit.
3. Aktivieren Sie HCX mit dem Lizenzschlüssel.
4. Koppeln Sie den lokalen VMware HCX Connector mit Azure VMware Solution HCX Cloud Manager.
5. Konfigurieren Sie das Netzwerkprofil, das Computeprofil und das Service Mesh.
6. (Optional) Führen Sie eine Netzwerkerweiterung durch, um eine erneute IP-Zuweisung während der Migration zu vermeiden.

7. Überprüfen Sie den Gerätestatus und stellen Sie sicher, dass eine Migration möglich ist.
8. Migrieren Sie die VM-Workloads.

▼ Voraussetzungen

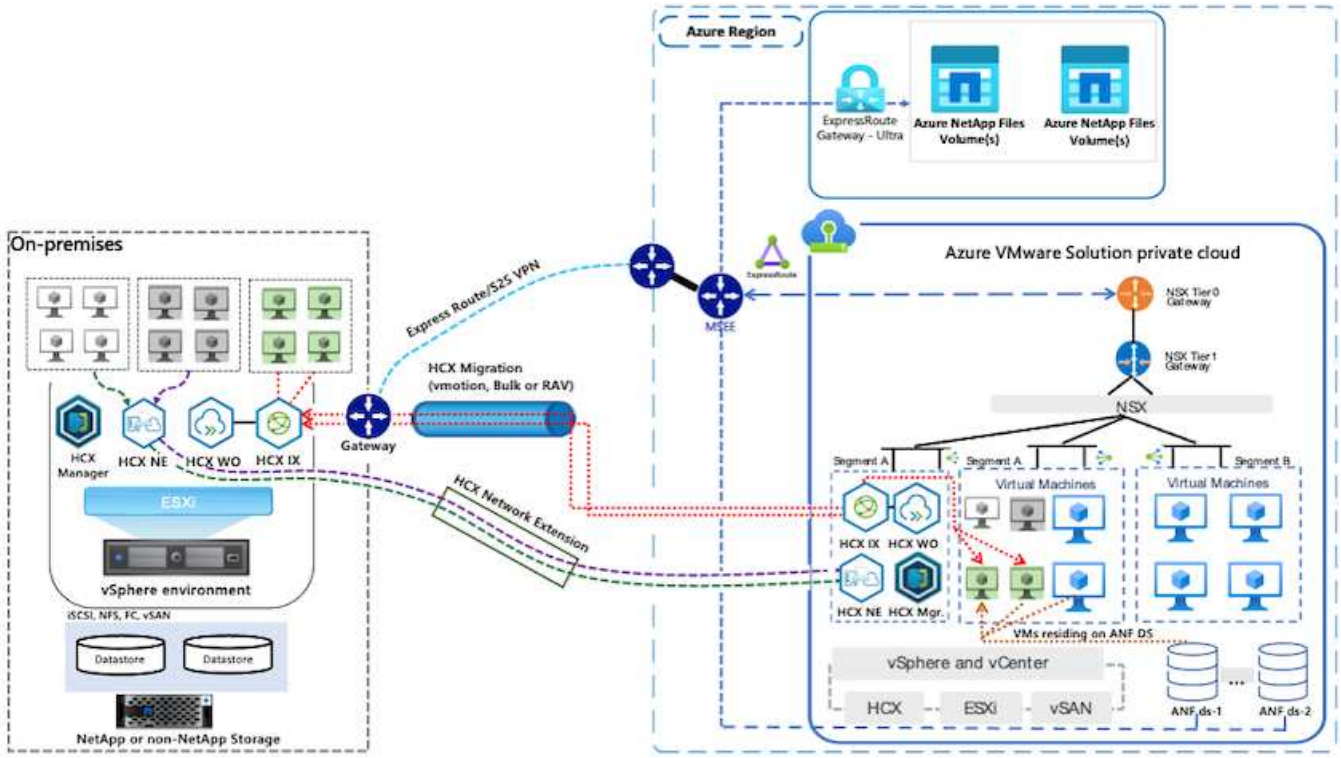
Stellen Sie vor dem Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie hier "Link" . Nachdem die Voraussetzungen, einschließlich der Konnektivität, erfüllt sind, konfigurieren und aktivieren Sie HCX, indem Sie den Lizenzschlüssel aus dem Azure VMware Solution-Portal generieren. Nachdem das OVA-Installationsprogramm heruntergeladen wurde, fahren Sie mit dem Installationsvorgang wie unten beschrieben fort.

ⓘ HCX Advanced ist die Standardoption und die VMware HCX Enterprise Edition ist auch über ein Support-Ticket verfügbar und wird ohne zusätzliche Kosten unterstützt.

- Verwenden Sie ein vorhandenes Azure VMware-Lösungs-Software-Defined Data Center (SDDC) oder erstellen Sie eine private Cloud, indem Sie dieses"NetApp Link" oder das "Microsoft-Link" .
- Die Migration von VMs und zugehörigen Daten aus dem lokalen VMware vSphere-fähigen Rechenzentrum erfordert eine Netzwerkkonnektivität vom Rechenzentrum zur SDDC-Umgebung. Bevor Sie Workloads migrieren, "Richten Sie eine Site-to-Site-VPN- oder Express-Route-Verbindung mit globaler Reichweite ein" zwischen der On-Premises-Umgebung und der jeweiligen privaten Cloud.
- Der Netzwerkpfad von der lokalen VMware vCenter Server-Umgebung zur privaten Azure VMware Solution-Cloud muss die Migration von VMs mithilfe von vMotion unterstützen.
- Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und Ports" sind für vMotion-Datenverkehr zwischen dem lokalen vCenter Server und SDDC vCenter zulässig. In der privaten Cloud ist das Routing im vMotion-Netzwerk standardmäßig konfiguriert.
- Das NFS-Volume von Azure NetApp Files sollte als Datenspeicher in Azure VMware Solution bereitgestellt werden. Befolgen Sie die in diesem Dokument beschriebenen Schritte "Link" Azure NetApp Files -Datenspeicher an Azure VMware Solutions-Hosts anzuhängen.

▼ High-Level-Architektur

Zu Testzwecken wurde die für diese Validierung verwendete lokale Laborumgebung über ein Site-to-Site-VPN verbunden, das eine lokale Konnektivität mit Azure VMware Solution ermöglicht.



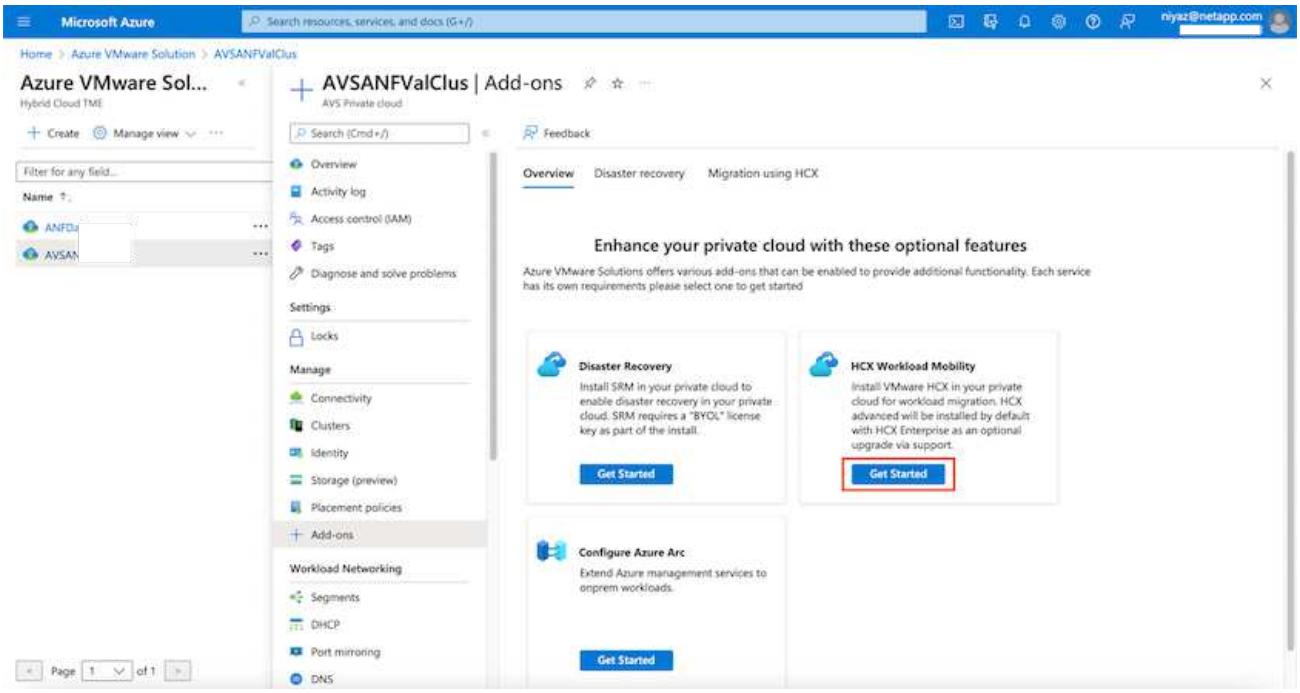
Lösungsbereitstellung

Befolgen Sie die Schritte, um die Bereitstellung dieser Lösung abzuschließen:

▼ **Schritt 1: Installieren Sie HCX über das Azure-Portal mithilfe der Add-Ons-Option**

Führen Sie zur Durchführung der Installation die folgenden Schritte aus:

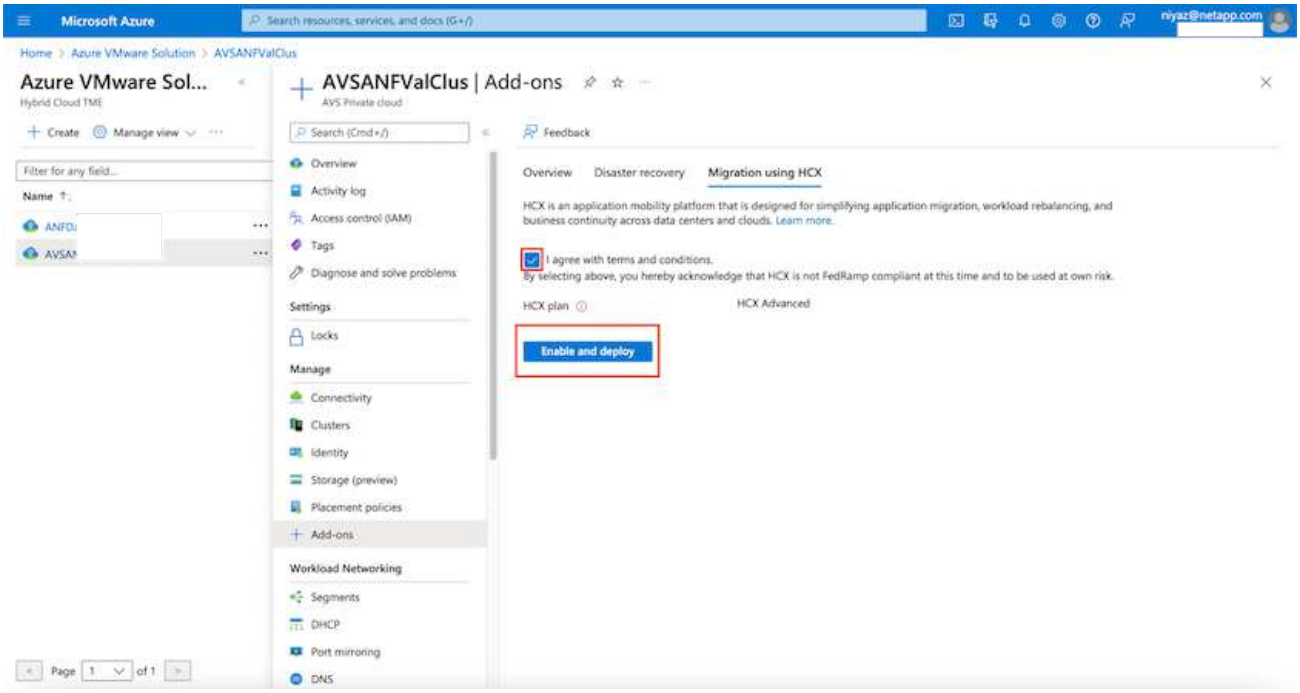
1. Melden Sie sich beim Azure-Portal an und greifen Sie auf die private Cloud der Azure VMware Solution zu.
2. Wählen Sie die entsprechende private Cloud aus und greifen Sie auf Add-ons zu. Dies kann durch Navigieren zu **Verwalten > Add-ons** erfolgen.
3. Klicken Sie im Abschnitt „HCX Workload Mobility“ auf **Erste Schritte**.



4. 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 Supportanfrage, um die Enterprise Edition zu aktivieren.

> Die Bereitstellung dauert ungefähr 25 bis 30 Minuten.



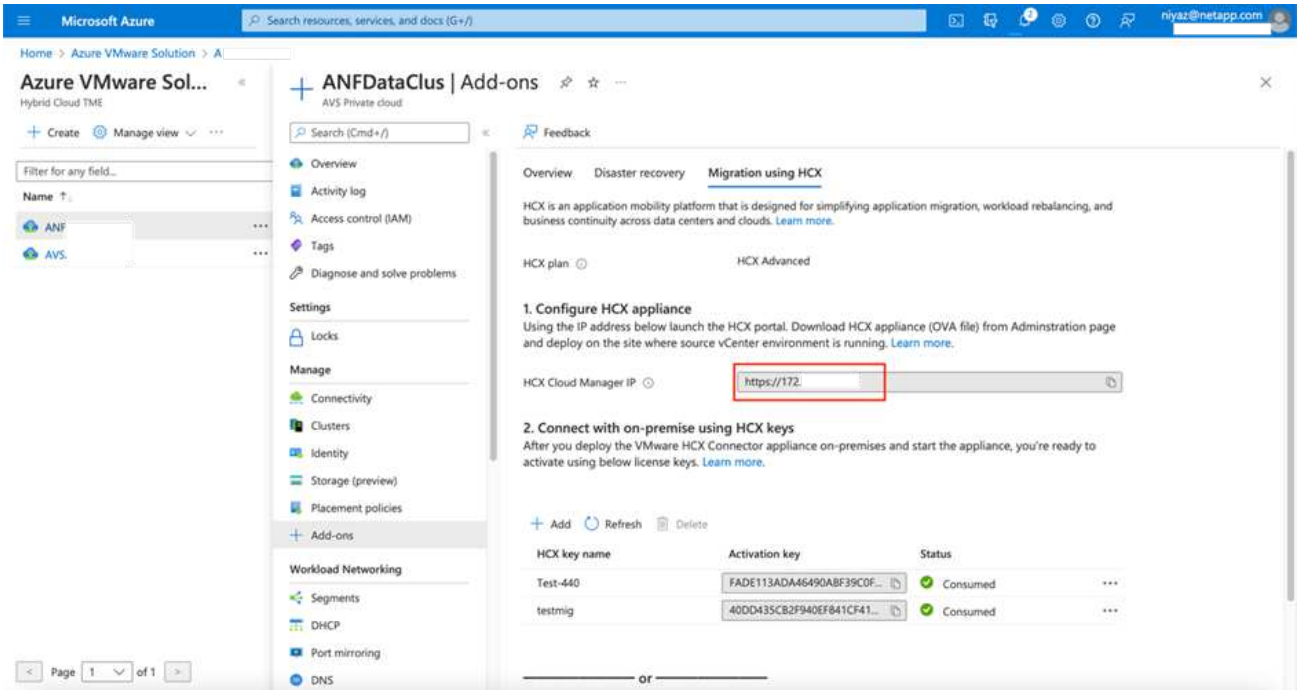
▼ Schritt 2: Bereitstellen der OVA-Installationsdatei im lokalen vCenter Server

Damit der lokale Connector eine Verbindung mit dem HCX Manager in Azure VMware Solution herstellen kann, stellen Sie sicher, dass die entsprechenden Firewall-Ports in der lokalen Umgebung geöffnet sind.

Führen Sie die folgenden Schritte aus, um HCX Connector herunterzuladen und auf dem lokalen vCenter Server zu installieren:

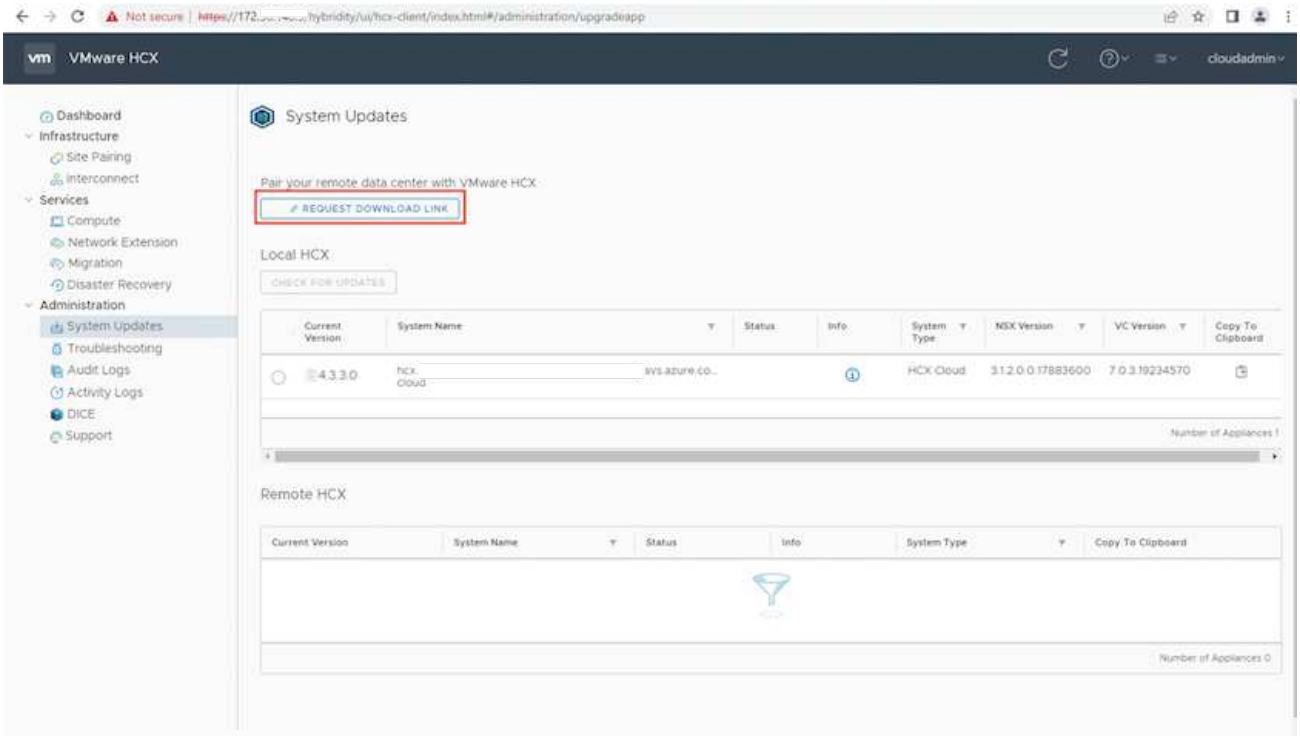
1. Gehen Sie im Azure-Portal zur Azure VMware Solution, wählen Sie die private Cloud aus, wählen Sie „Verwalten > Add-Ons > Migration“ mit HCX und kopieren Sie das HCX Cloud Manager-Portal, um die OVA-Datei herunterzuladen.

   Verwenden Sie die standardmäßigen CloudAdmin-Benutzeranmeldeinformationen, um auf das HCX-Portal zuzugreifen.

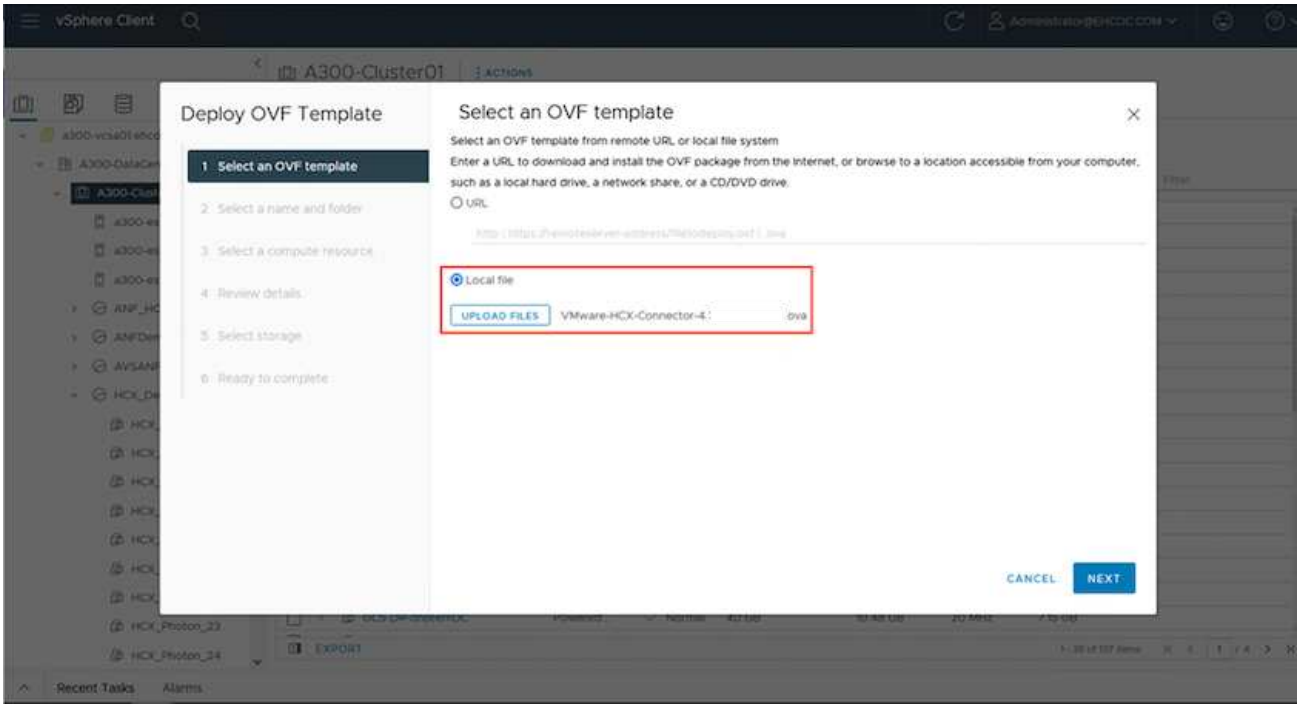


2. Nachdem Sie über den Jumphost mit cloudadmin@vsphere.local auf das HCX-Portal zugegriffen haben, navigieren Sie zu **Administration > Systemupdates** und klicken Sie auf **Download-Link anfordern**.

   Laden Sie den Link zur OVA-Datei herunter oder kopieren Sie ihn und fügen Sie ihn in einen Browser ein, um den Downloadvorgang der VMware HCX Connector-OVA-Datei zur Bereitstellung auf dem lokalen vCenter Server zu starten.



3. Nachdem die OVA heruntergeladen wurde, stellen Sie sie mithilfe der Option **OVF-Vorlage bereitstellen** in der lokalen VMware vSphere-Umgebung bereit.



4. Geben Sie alle erforderlichen Informationen für die OVA-Bereitstellung ein, klicken Sie auf **Weiter** und dann auf **Fertig**, um die OVA des VMware HCX-Connectors bereitzustellen.

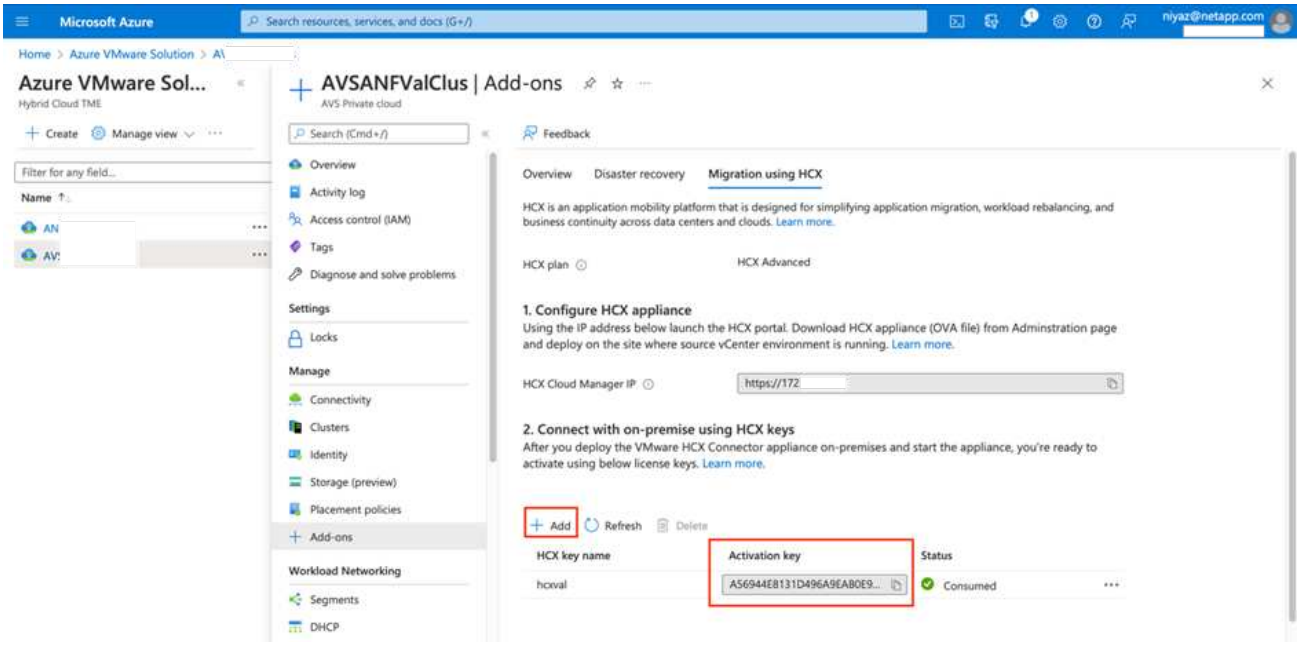
Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "VMware HCX-Benutzerhandbuch" .

▼ Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie die VMware HCX Connector OVA vor Ort bereitgestellt und die Appliance gestartet haben, führen Sie die folgenden Schritte aus, um HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel aus dem Azure VMware Solution-Portal und aktivieren Sie ihn im VMware HCX Manager.

1. Gehen Sie im Azure-Portal zur Azure VMware-Lösung, wählen Sie die private Cloud aus und wählen Sie **Verwalten > Add-Ons > Migration mit HCX**.
2. Klicken Sie unter **Mit HCX-Schlüsseln vor Ort verbinden** auf **Hinzufügen** und kopieren Sie den Aktivierungsschlüssel.



> Für jeden bereitgestellten lokalen HCX-Connector ist ein separater Schlüssel erforderlich.

3. Melden Sie sich beim lokalen VMware HCX Manager an unter "`https://hcxmanagerIP:9443`" mit Administratoranmeldeinformationen.

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

4. Geben Sie in der Lizenzierung den aus Schritt 3 kopierten Schlüssel ein und klicken Sie auf **Aktivieren**.

> Der lokale HCX-Connector sollte über Internetzugang verfügen.

5. Geben Sie unter **Rechenzentrumsstandort** den nächstgelegenen Standort für die lokale Installation des VMware HCX Manager an. Klicken Sie auf **Weiter**.
6. Aktualisieren Sie unter **Systemname** den Namen und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Ja, fortfahren**.
8. Geben Sie unter **Verbinden Sie Ihr vCenter** den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des vCenter-Servers und die entsprechenden Anmeldeinformationen ein und klicken Sie auf **Weiter**.

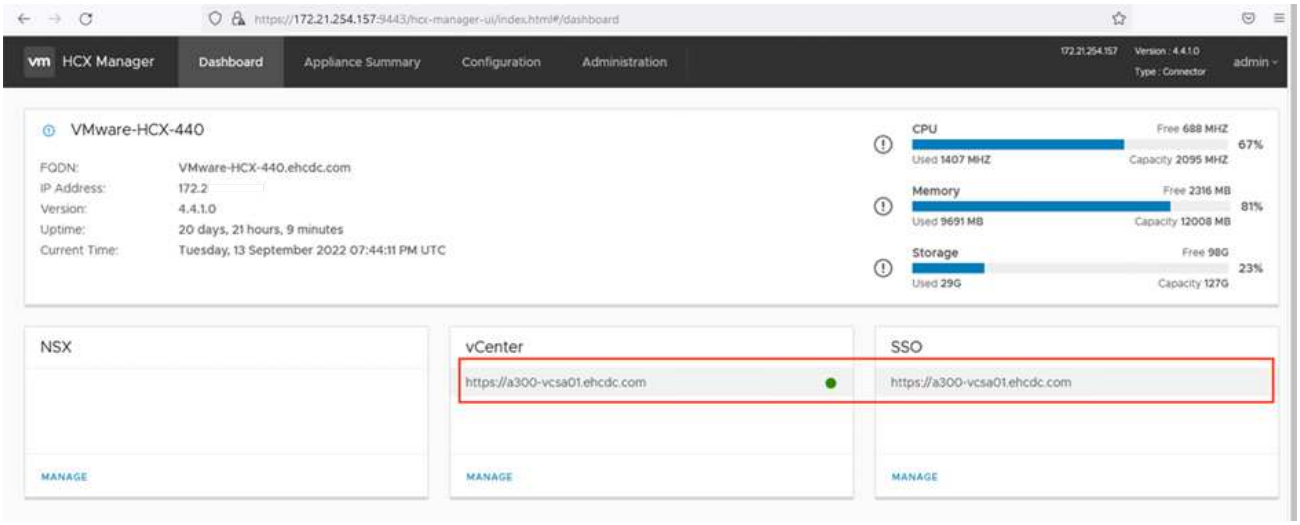
> Verwenden Sie den FQDN, um spätere Verbindungsprobleme zu vermeiden.

9. Geben Sie unter **SSO/PSC konfigurieren** den FQDN oder die IP-Adresse des Platform Services Controllers ein und klicken Sie auf **Weiter**.

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

10. Überprüfen Sie, ob die eingegebenen Informationen korrekt sind, und klicken Sie auf **Neustart**.
11. 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 denen auf der vorherigen Seite übereinstimmen sollten.

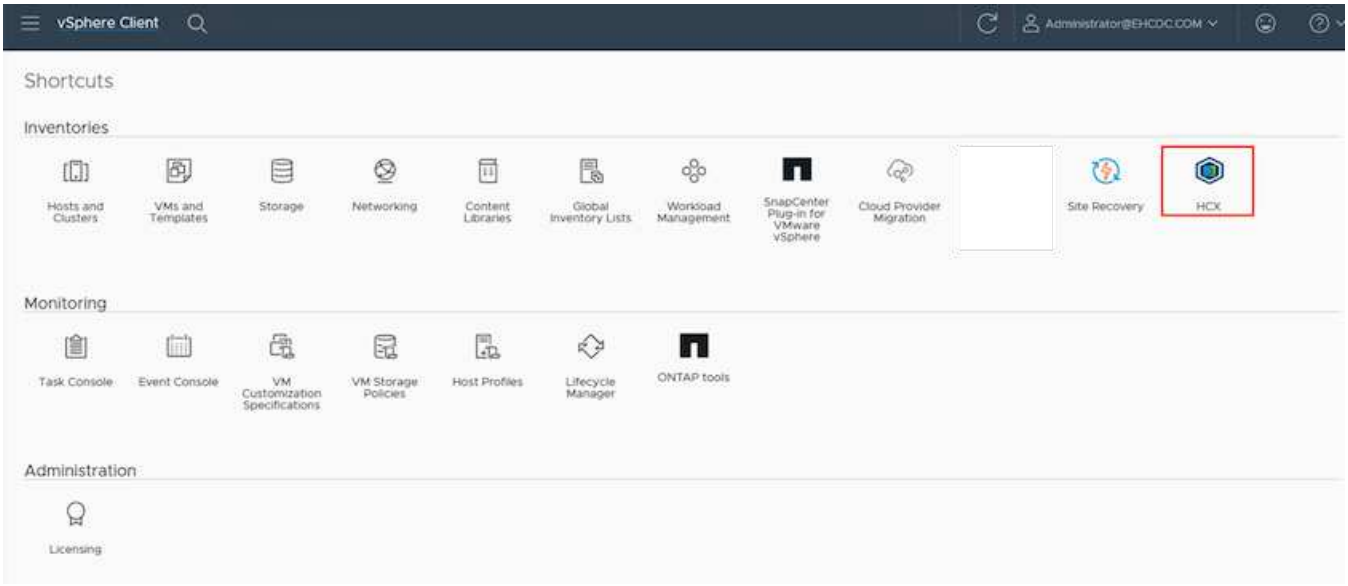
    Dieser Vorgang sollte etwa 10 bis 20 Minuten dauern und das Plug-In sollte dem vCenter Server hinzugefügt werden.



▼ Schritt 4: Koppeln Sie den lokalen VMware HCX Connector mit dem Azure VMware Solution HCX Cloud Manager

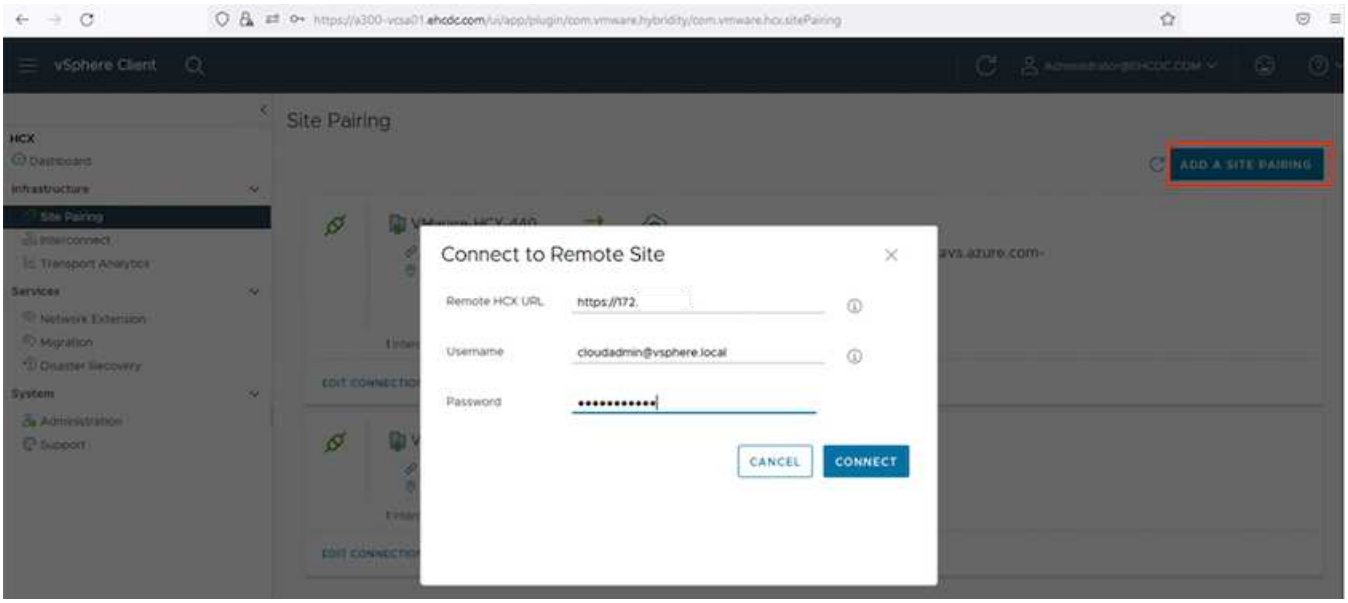
Nachdem der HCX Connector sowohl lokal als auch in Azure VMware Solution installiert wurde, konfigurieren Sie den lokalen VMware HCX Connector für die private Cloud von Azure VMware Solution, indem Sie die Kopplung hinzufügen. Führen Sie die folgenden Schritte aus, um die Site-Kopplung zu konfigurieren:

1. Um ein Site-Paar zwischen der lokalen vCenter-Umgebung und 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-Paarung hinzufügen“*.

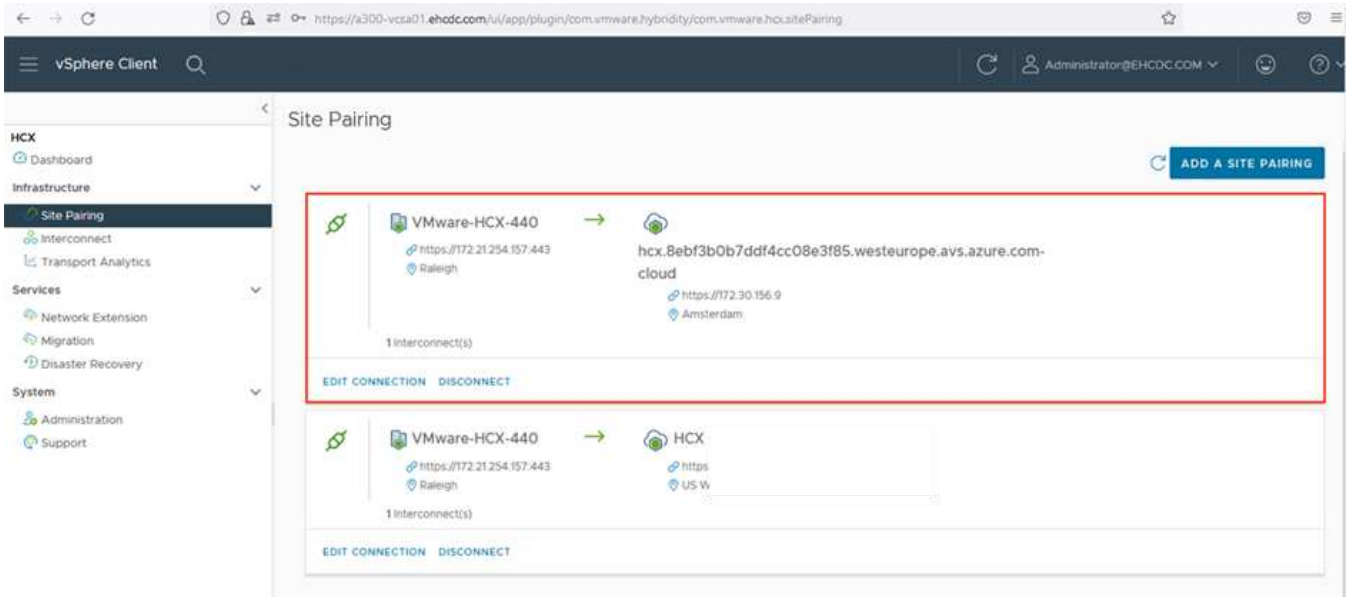
Geben Sie die URL oder IP-Adresse des Azure VMware Solution HCX Cloud Managers und die Anmeldeinformationen für die CloudAdmin-Rolle für den Zugriff auf die private Cloud ein.



1. Klicken Sie auf **Verbinden**.

VMware HCX Connector muss in der Lage sein, über Port 443 an die IP-Adresse des HCX Cloud Managers weiterzuleiten.

1. Nachdem die Kopplung erstellt wurde, ist die neu konfigurierte Site-Kopplung auf dem HCX-Dashboard verfügbar.

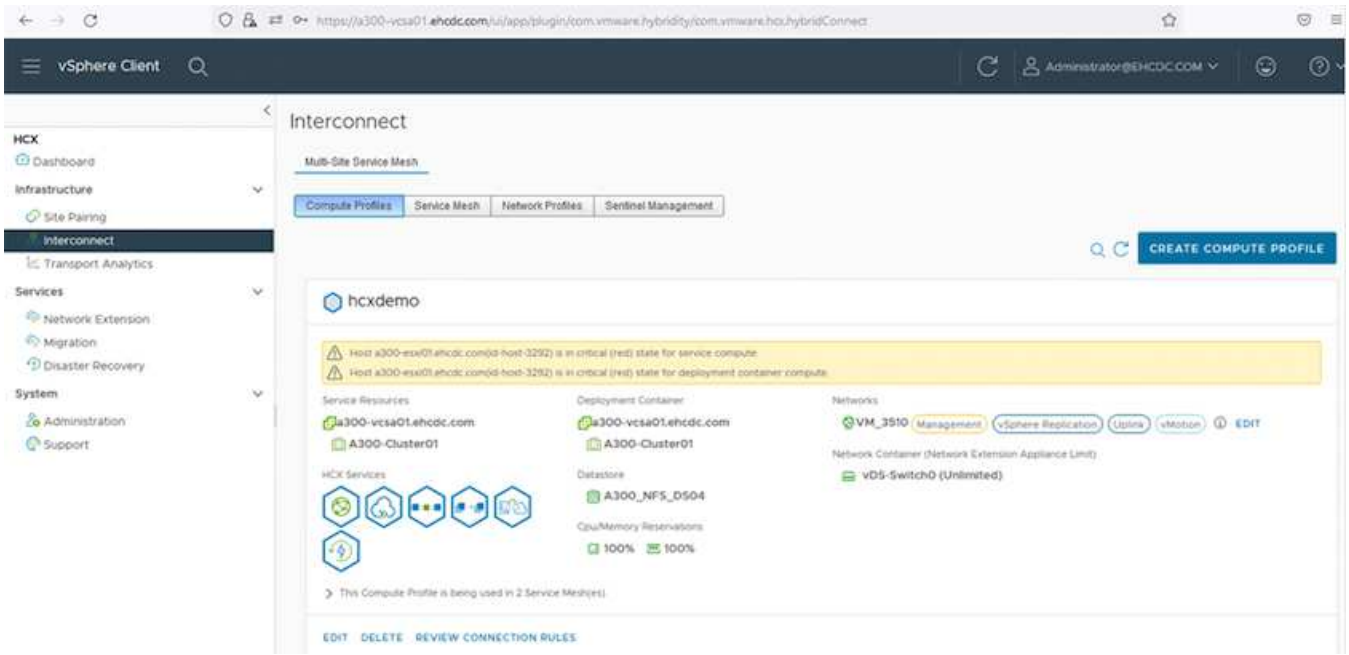


▼ **Schritt 5: Konfigurieren Sie das Netzwerkprofil, das Compute-Profil und das Service Mesh**

Die VMware HCX Interconnect Service Appliance bietet Replikations- und vMotion-basierte Migrationsfunktionen über das Internet und private Verbindungen zum Zielstandort. Die Verbindung bietet Verschlüsselung, Verkehrstechnik und VM-Mobilität. Führen Sie die folgenden Schritte aus, um eine Interconnect-Dienst-Appliance zu erstellen:

1. Wählen Sie unter „Infrastruktur“ die Option „Interconnect > Multi-Site Service Mesh > Compute-Profile > Compute-Profil erstellen“ aus.

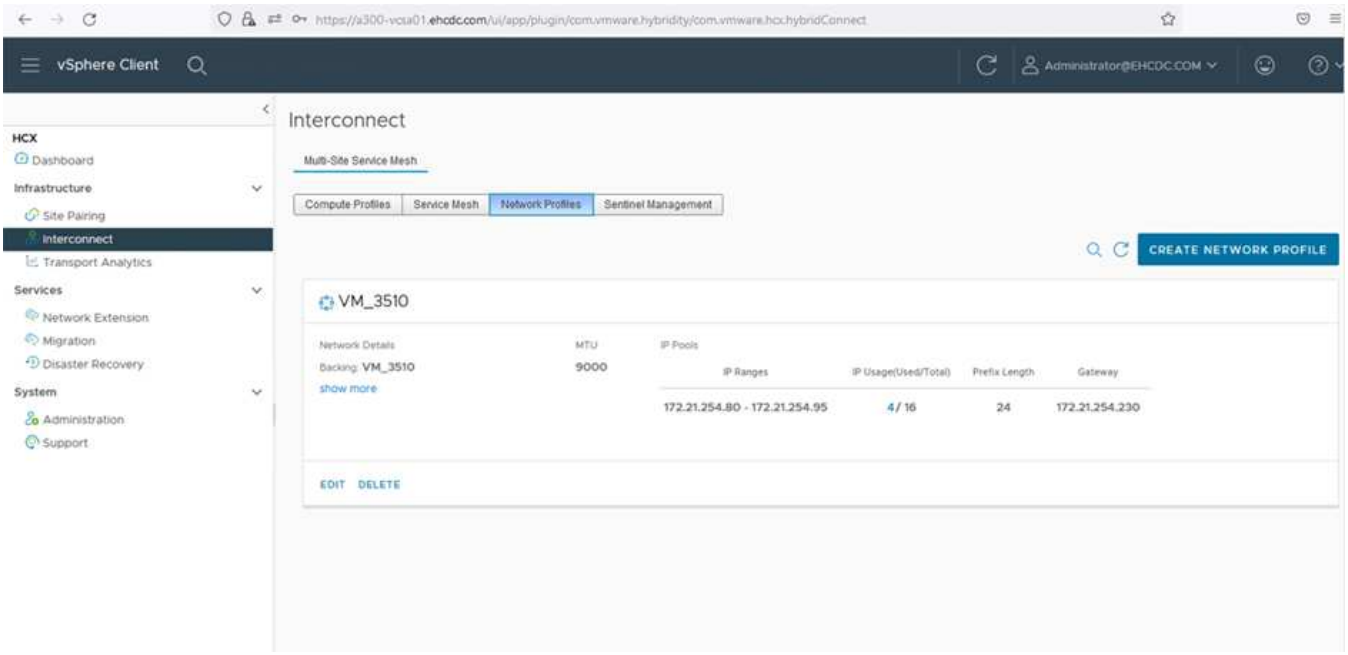
Die Rechenprofile definieren die Bereitstellungsparameter, einschließlich der bereitgestellten Appliances und der Teile des VMware-Rechenzentrums, auf die der HCX-Dienst zugreifen kann.



1. Nachdem das Compute-Profil erstellt wurde, erstellen Sie die Netzwerkprofile, indem Sie **Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen** auswählen.

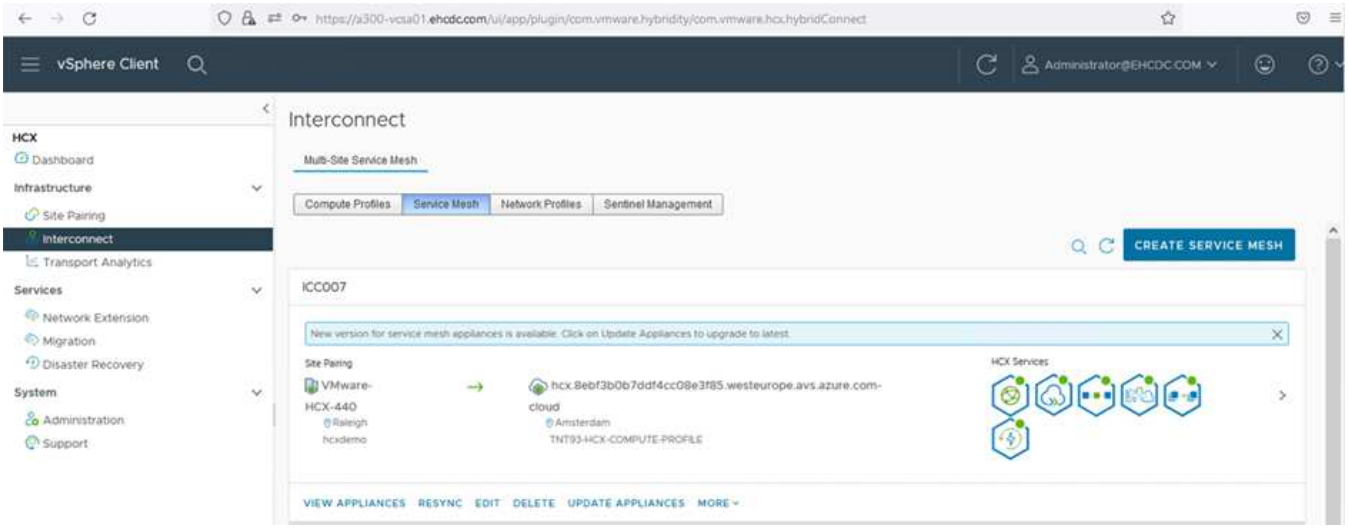
Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

Für diesen Schritt sind zwei oder mehr IP-Adressen erforderlich. Diese IP-Adressen werden vom Verwaltungsnetzwerk den Interconnect Appliances zugewiesen.



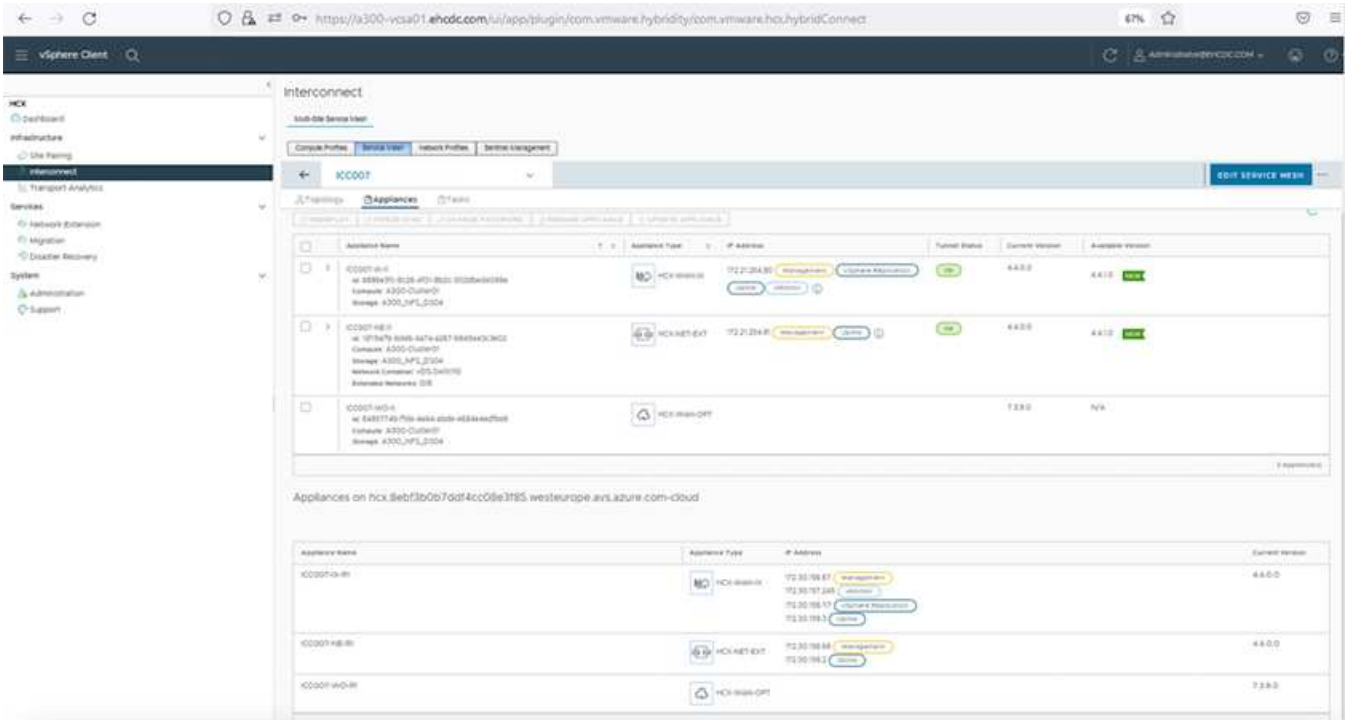
1. Zu diesem Zeitpunkt wurden die Computer- und Netzwerkprofile erfolgreich erstellt.
2. Erstellen Sie das Service Mesh, indem Sie innerhalb der Option **Interconnect** die Registerkarte **Service Mesh** auswählen und die lokalen und Azure SDDC-Sites auswählen.
3. Das Service Mesh gibt ein lokales und ein Remote-Compute- und Netzwerkprofilpaar an.

Im Rahmen dieses Prozesses werden die HCX-Geräte sowohl am Quell- als auch am Zielstandort bereitgestellt und automatisch konfiguriert, um ein sicheres Transport-Fabric zu erstellen.



1. Dies ist der letzte Schritt der Konfiguration. Die Bereitstellung sollte etwa 30 Minuten dauern. Nachdem

das Service-Mesh konfiguriert wurde, ist die Umgebung mit den erfolgreich erstellten IPsec-Tunneln bereit, um die Workload-VMs zu migrieren.



▼ **Schritt 6: Migrieren von Workloads**

Workloads können mithilfe verschiedener VMware HCX-Migrationstechnologien bidirektional zwischen lokalen und Azure SDDCs migriert werden. VMs können mithilfe mehrerer Migrationstechnologien wie HCX-Massenmigration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (verfügbar mit der HCX Enterprise Edition) und HCX OS Assisted Migration (verfügbar mit der HCX Enterprise Edition) zu und von VMware HCX-aktivierten Einheiten verschoben werden.

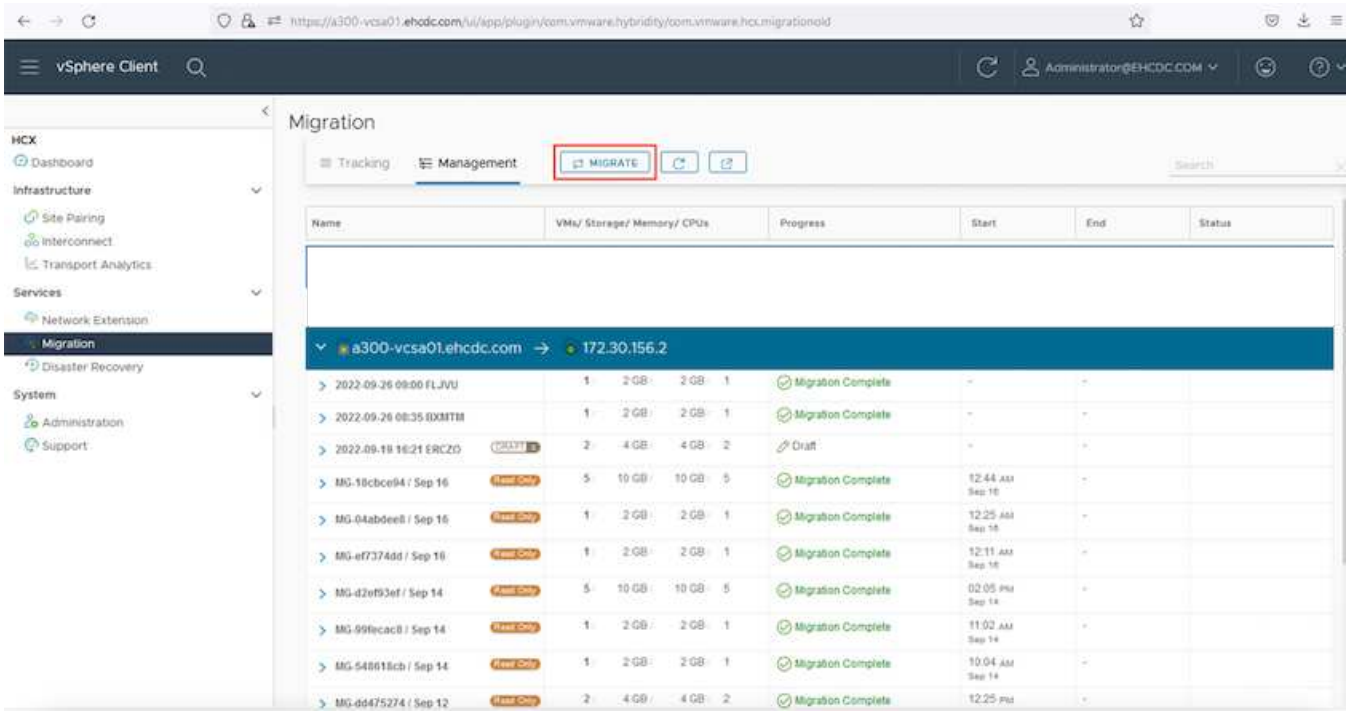
Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter "VMware HCX-Migrationstypen" .

Massenmigration

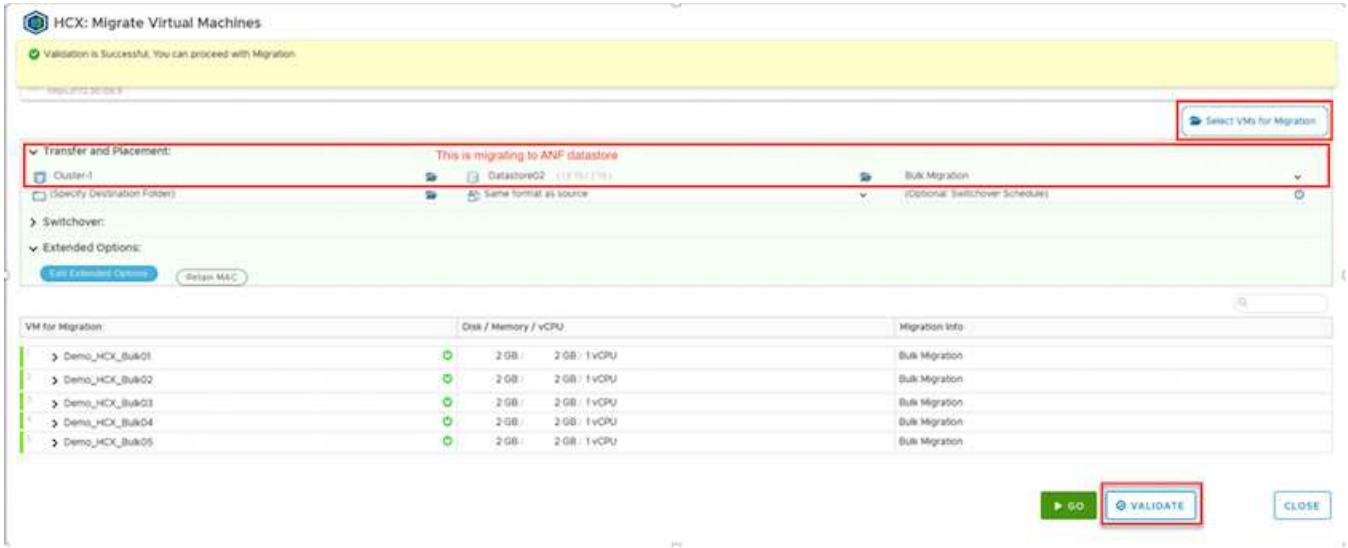
In diesem Abschnitt wird der Massenmigrationsmechanismus ausführlich beschrieben. Während einer Massenmigration verwendet die Massenmigrationsfunktion von HCX vSphere Replication, um Festplattendateien zu migrieren und gleichzeitig die VM auf der vSphere HCX-Zielinstanz neu zu erstellen.

Führen Sie die folgenden Schritte aus, um Massenmigrationen von virtuellen Maschinen zu initiieren:

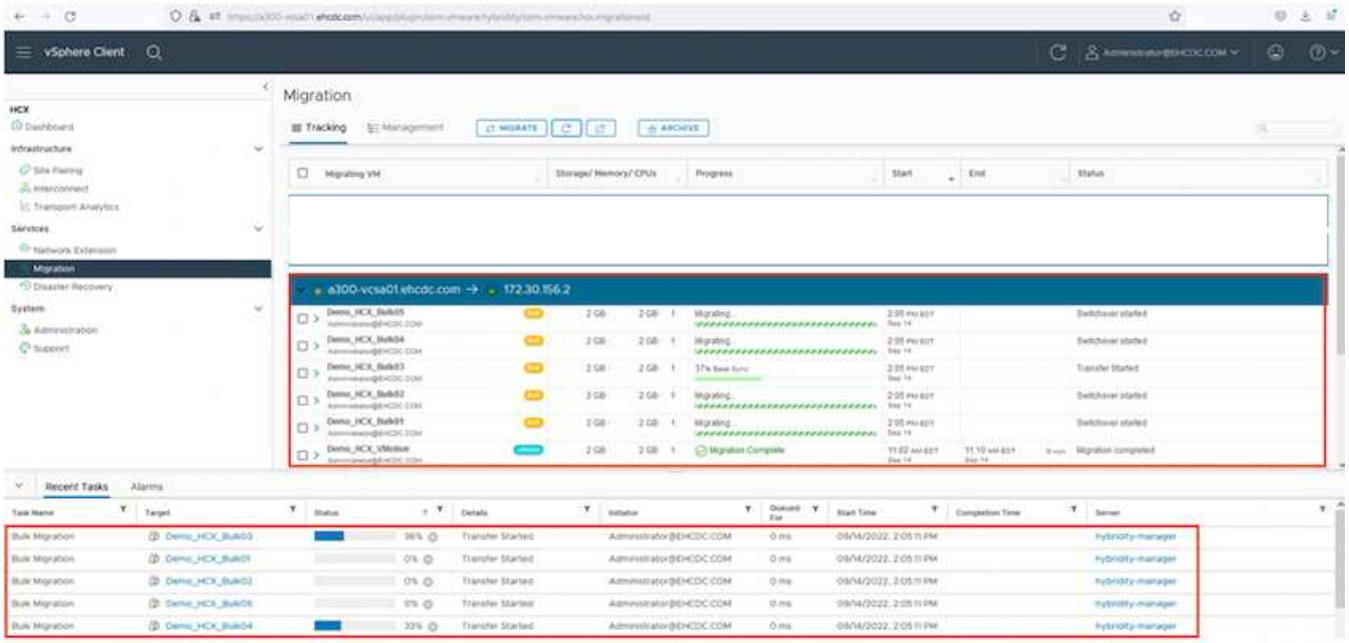
1. Greifen Sie unter **Dienste > Migration** auf die Registerkarte **Migrieren** zu.



1. Wählen Sie unter **Remote-Site-Verbindung** die Remote-Site-Verbindung aus und wählen Sie Quelle und Ziel aus. In diesem Beispiel ist das Ziel der Azure VMware Solution SDDC HCX-Endpunkt.
2. Klicken Sie auf **VMs für die Migration auswählen**. Dadurch wird eine Liste aller lokalen VMs bereitgestellt. Wählen Sie die VMs basierend auf dem Match:Value-Ausdruck aus und klicken Sie auf **Hinzufügen**.
3. Aktualisieren Sie im Abschnitt **Übertragung und Platzierung** die Pflichtfelder (**Cluster**, **Speicher**, **Ziel** und **Netzwerk**), einschließlich des Migrationsprofils, und klicken Sie auf **Validieren**.

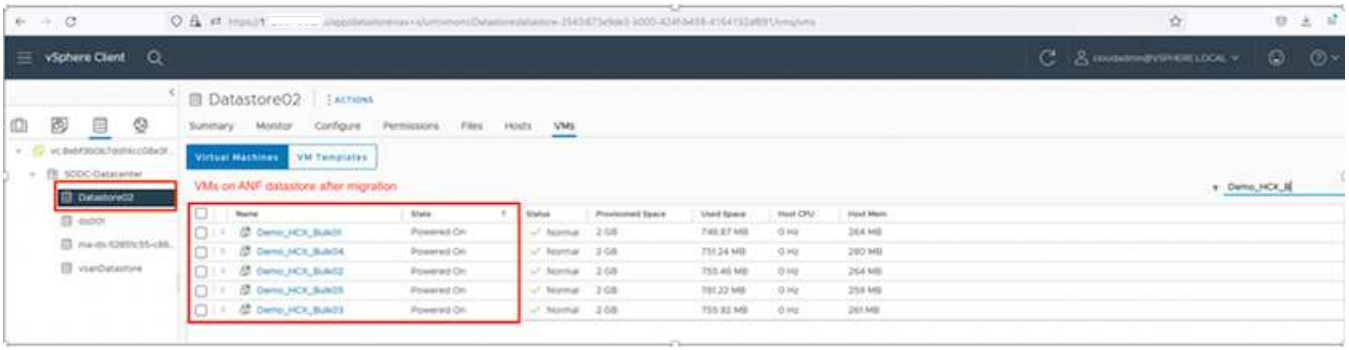


1. Klicken Sie nach Abschluss der Validierungsprüfungen auf **Los**, um die Migration zu starten.



Während dieser Migration wird auf dem angegebenen Azure NetApp Files -Datenspeicher im Ziel-vCenter ein Platzhalterdatenträger erstellt, um die Replikation der Daten des Quell-VM-Datenträgers auf die Platzhalterdatenträger zu ermöglichen. HBR wird für eine vollständige Synchronisierung mit dem Ziel ausgelöst. Nachdem die Baseline abgeschlossen ist, wird eine inkrementelle Synchronisierung basierend auf dem Recovery Point Objective (RPO)-Zyklus durchgeführt. Nachdem die vollständige/inkrementelle Synchronisierung abgeschlossen ist, wird die Umschaltung automatisch ausgelöst, sofern kein bestimmter Zeitplan festgelegt ist.

1. Nachdem die Migration abgeschlossen ist, validieren Sie diese, indem Sie auf das Ziel-SDDC-vCenter zugreifen.

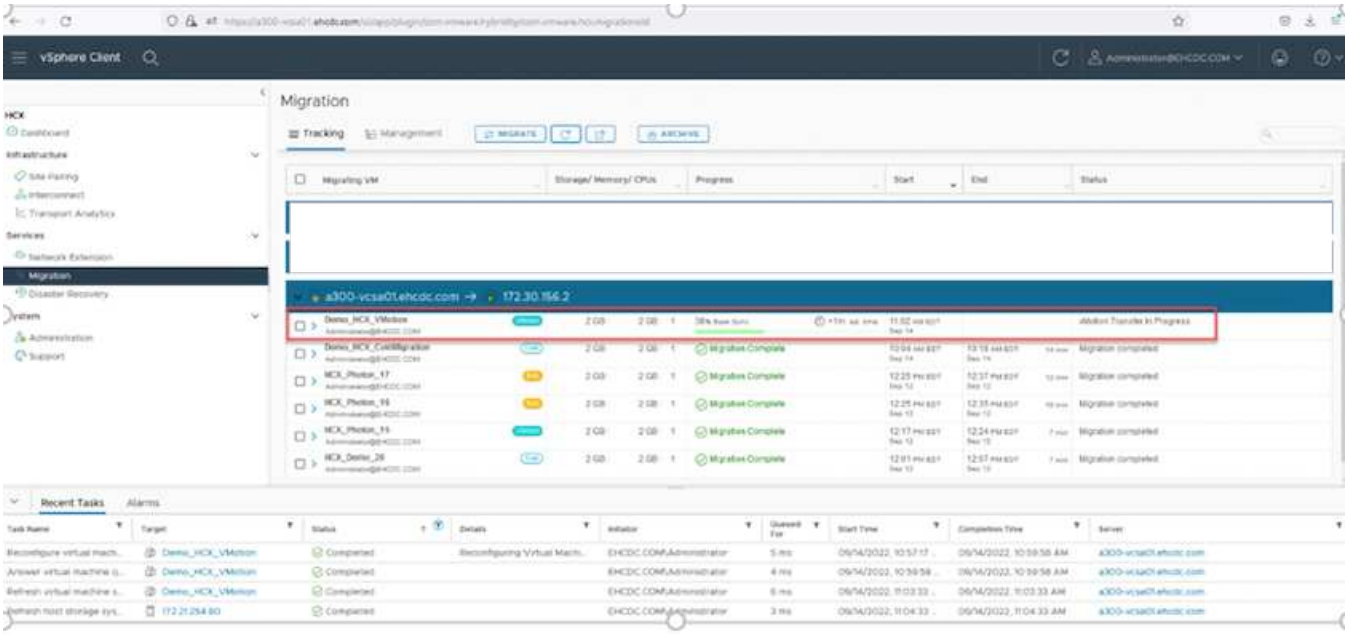


Weitere und ausführliche Informationen zu verschiedenen Migrationsoptionen und zur Migration von Workloads von lokalen Standorten zu Azure VMware Solution mithilfe von HCX finden Sie unter "Überlegungen zur VMware HCX-Migration" .

Um mehr über diesen Prozess zu erfahren, schauen Sie sich das folgende Video an:

Workload-Migration mit HCX

Hier ist ein Screenshot der HCX vMotion-Option.



Um mehr über diesen Prozess zu erfahren, schauen Sie sich das folgende Video an:

HCX vMotion

Stellen Sie sicher, dass für die Migration ausreichend Bandbreite zur Verfügung steht.

Der Ziel-ANF-Datenspeicher sollte über ausreichend Speicherplatz verfügen, um die Migration durchzuführen.

Abschluss

Unabhängig davon, ob Sie eine reine Cloud oder eine Hybrid Cloud anstreben und Ihre Daten sich auf Speichersystemen beliebiger Art/Anbieter vor Ort befinden, bieten Azure NetApp Files und HCX hervorragende Optionen zum Bereitstellen und Migrieren der Anwendungsworkloads und senken gleichzeitig die Gesamtbetriebskosten, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden. Wählen Sie für jeden Anwendungsfall Azure VMware Solution zusammen mit Azure NetApp Files, um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und Vorgänge vor Ort und in mehreren Clouds zu gewährleisten, Workloads bidirektional zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen. Es handelt sich um denselben bekannten Prozess und dieselben bekannten Verfahren, die zum Verbinden des Speichers und Migrieren von VMs mithilfe von VMware vSphere Replication, VMware vMotion oder sogar Network File Copy (NFC) verwendet werden.

Imbiss

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können jetzt Azure NetApp Files als Datenspeicher auf Azure VMware Solution SDDC verwenden.
- Sie können Daten problemlos vom lokalen Standort in den Azure NetApp Files Datenspeicher migrieren.
- Sie können den Azure NetApp Files -Datenspeicher problemlos vergrößern und verkleinern, um die Kapazitäts- und Leistungsanforderungen während der Migrationsaktivität zu erfüllen.

Wo Sie weitere Informationen finden

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

- Dokumentation zur 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/"

- Überlegungen zur VMware HCX-Migration

"https://learn.microsoft.com/en-us/azure/azure-vmware/architecture-migrate"

NetApp für GCP/GCVE

NetApp -Funktionen für die Google Cloud Platform GCVE

Erfahren Sie mehr über die Funktionen, die NetApp der Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) bietet – von NetApp als über einen Gast verbundenes Speichergerät oder als zusätzlicher NFS-Datenspeicher bis hin zur Migration von Workflows, Erweiterung/Bursting in die Cloud, Sicherung/Wiederherstellung und Notfallwiederherstellung.

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

- "Konfigurieren von GCVE in GCP"
- "NetApp Storage-Optionen für GCVE"
- "NetApp / VMware Cloud-Lösungen"

Konfigurieren von GCVE in GCP

Wie bei der lokalen Umgebung ist die Planung einer Cloud-basierten Virtualisierungsumgebung entscheidend für eine erfolgreiche produktionsbereite Umgebung zum Erstellen und Migrieren von VMs.

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und verwalten und es in Kombination mit den verfügbaren Optionen zum Anschließen von NetApp -Speicher verwenden.

> In-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP und Google Cloud NetApp Volumes mit GCVE.

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von GCVE
- Privaten Zugriff auf GCVE aktivieren

Sehen Sie sich die detaillierte"Konfigurationsschritte für GCVE" .

NetApp Storage-Optionen für GCVE

NetApp Speicher kann innerhalb von GCP GCVE auf verschiedene Weise genutzt werden – entweder als verbundener oder als zusätzlicher NFS-Datenspeicher.

Bitte besuchen Sie"Unterstützte NetApp -Speicheroptionen" für weitere Informationen.

Google Cloud unterstützt NetApp -Speicher in den folgenden Konfigurationen:

- Cloud Volumes ONTAP (CVO) als mit dem Gast verbundener Speicher
- Google Cloud NetApp Volumes (NetApp Volumes) als mit dem Gast verbundener Speicher
- Google Cloud NetApp Volumes (NetApp Volumes) als ergänzender NFS-Datenspeicher

Sehen Sie sich die detaillierte"Gastverbindungsspeicheroptionen für GCVE" . Sehen Sie sich die detaillierte"zusätzliche NFS-Datenspeicheroptionen für GCVE" .

Lesen Sie mehr über"Google Cloud NetApp Volumes Datenspeicherunterstützung für Google Cloud VMware Engine (NetApp -Blog)" oder"So verwenden Sie Google Cloud NetApp Volumes als Datenspeicher für Google Cloud VMware Engine (Google-Blog)"

Anwendungsfälle der Lösung

Mit NetApp und VMware-Cloudlösungen lassen sich viele Anwendungsfälle einfach in Azure AVS bereitstellen. Diese Fälle sind für jeden der von VMware definierten Cloudbereiche definiert:

- Schützen (beinhaltet sowohl Disaster Recovery als auch Backup/Wiederherstellung)
- Verlängern
- Wandern

"Durchsuchen Sie die NetApp -Lösungen für Google Cloud GCVE"

Schützen Sie Workloads auf GCP/GCVE

Anwendungskonsistente Notfallwiederherstellung mit NetApp SnapCenter und Veeam Replication

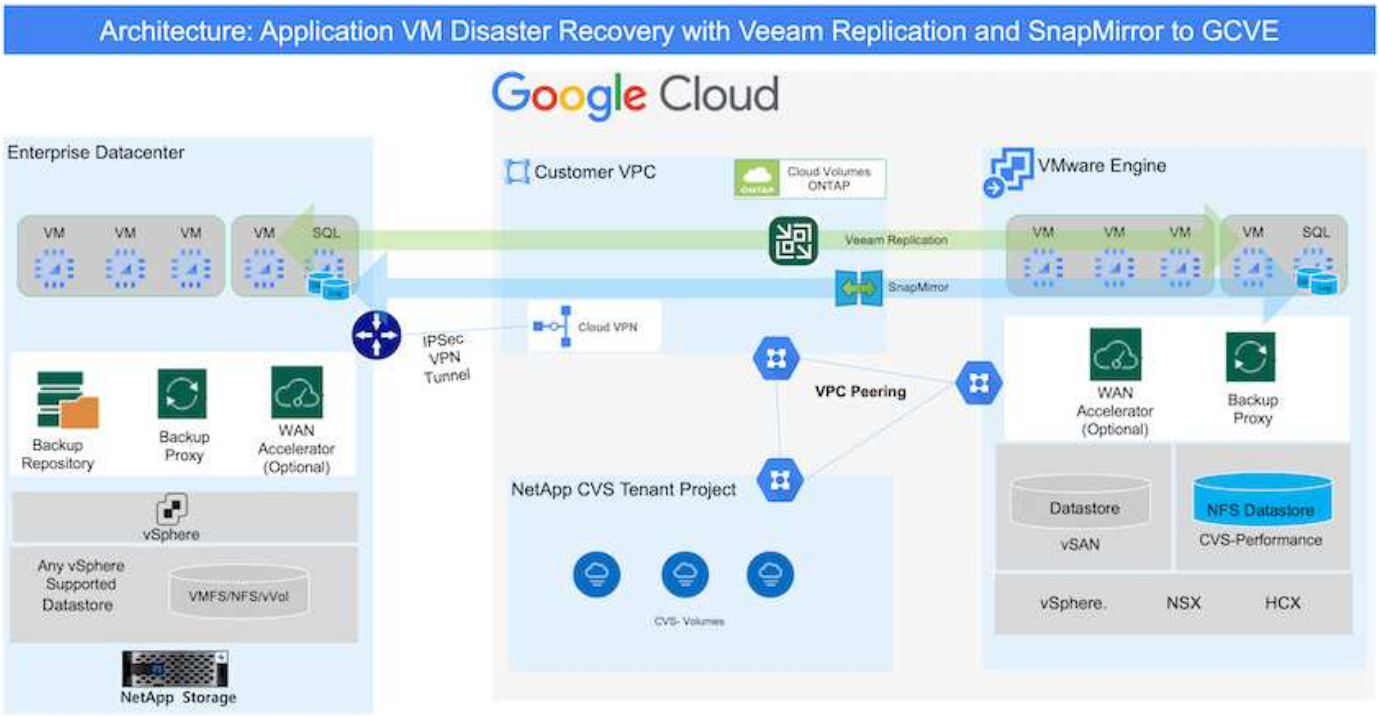
Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, Workloads vor Site-Ausfällen und Datenbeschädigungen wie Ransomware zu schützen. Mit NetApp SnapMirror können lokale VMware-Workloads, die über den Gast verbundenen Speicher verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, das in Google Cloud ausgeführt wird.

Überblick

Viele Kunden suchen nach einer effektiven Disaster-Recovery-Lösung für ihre auf VMware vSphere gehosteten Anwendungs-VMs. Viele von ihnen nutzen ihre vorhandene Backup-Lösung, um im Katastrophenfall eine Wiederherstellung durchzuführen. Oftmals erhöht diese Lösung die RTO und erfüllt nicht die Erwartungen. Um RPO und RTO zu reduzieren, kann die Veeam-VM-Replikation sogar von vor Ort zu GCVE genutzt werden, solange Netzwerkkonnektivität und eine Umgebung mit entsprechenden Berechtigungen verfügbar sind. HINWEIS: Die Veeam VM-Replikation schützt keine mit dem VM-Gast verbundenen Speichergeräte wie iSCSI- oder NFS-Mounts innerhalb der Gast-VM. Diese müssen separat geschützt werden.

Für eine anwendungskonsistente Replikation für SQL VM und zur Reduzierung der RTO haben wir SnapCenter verwendet, um Snapmirror-Vorgänge von SQL-Datenbank- und Protokollvolumes zu orchestrieren.

Dieses Dokument bietet eine schrittweise Anleitung zum Einrichten und Durchführen einer Notfallwiederherstellung unter Verwendung von NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Annahmen

Dieses Dokument konzentriert sich auf die In-Guest-Speicherung für Anwendungsdaten (auch als Gastverbindung bezeichnet) und wir gehen davon aus, dass die lokale Umgebung SnapCenter für anwendungskonsistente Sicherungen verwendet.

> Dieses Dokument gilt für alle Sicherungs- oder Wiederherstellungslösungen von Drittanbietern. Befolgen Sie je nach der in der Umgebung verwendeten Lösung Best Practices, um Sicherungsrichtlinien zu erstellen, die den SLAs des Unternehmens entsprechen.

Verwenden Sie für die Konnektivität zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk Konnektivitätsoptionen wie dedizierte Verbindung oder Cloud-VPN. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen zum Verbinden lokaler Rechenzentren mit Google Cloud, weshalb wir in diesem Dokument keinen bestimmten Arbeitsablauf beschreiben können. Informationen zur entsprechenden Methode zur Konnektivität zwischen lokalen Standorten und Google finden Sie in der Google Cloud-Dokumentation.

Bereitstellen der DR-Lösung

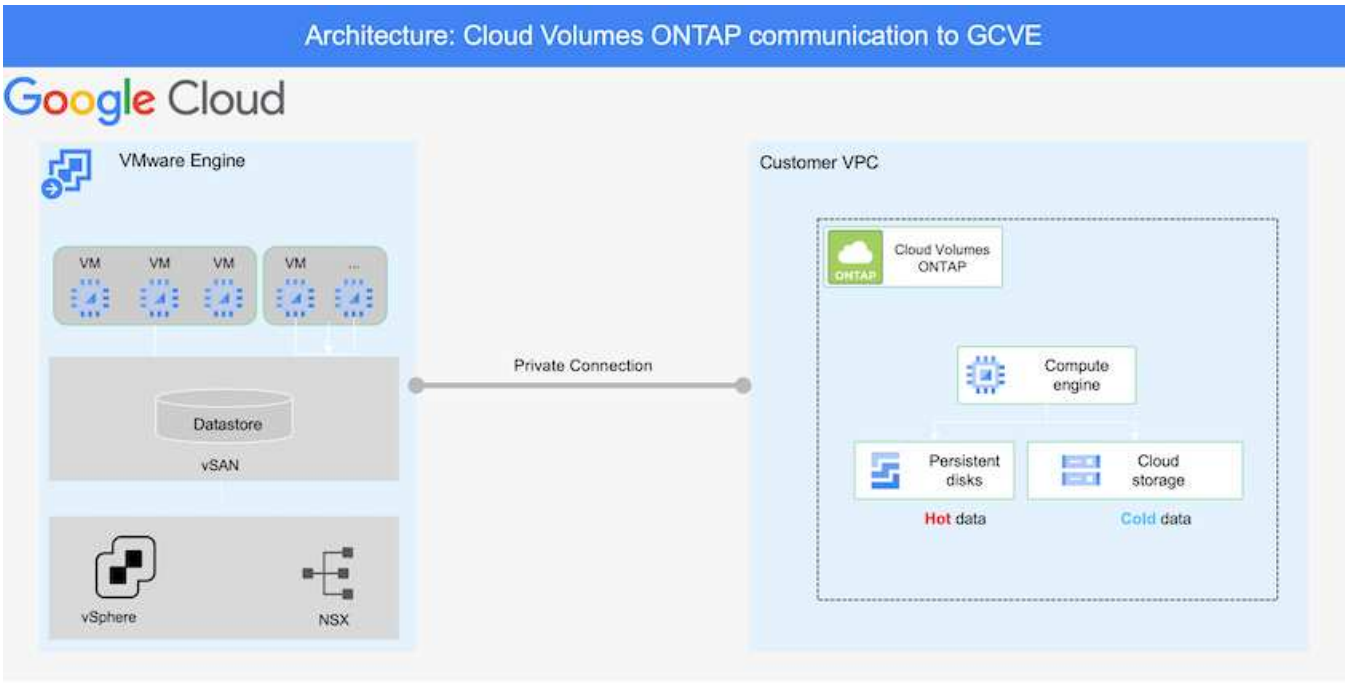
Übersicht über die Lösungsbereitstellung

1. Stellen Sie sicher, dass Anwendungsdaten mit SnapCenter unter Einhaltung der erforderlichen RPO-Anforderungen gesichert werden.
2. Die Bereitstellung von Cloud Volumes ONTAP mit der korrekten Instanzgröße erfolgt über NetApp Console innerhalb des entsprechenden Abonnements und virtuellen Netzwerks.
   a. Konfigurieren Sie SnapMirror für die relevanten Anwendungsvolumes.
   b. Aktualisieren Sie die Sicherungsrichtlinien in SnapCenter , um SnapMirror -Updates nach den geplanten Jobs auszulösen.
3. Installieren Sie die Veeam-Software und beginnen Sie mit der Replikation virtueller Maschinen auf die Google Cloud VMware Engine-Instanz.
4. Im Katastrophenfall lässt sich die SnapMirror Beziehung mit NetApp Console unterbrechen und das Failover der virtuellen Maschinen mit Veeam auslösen.
   a. Verbinden Sie die ISCSI-LUNs und NFS-Mounts für die Anwendungs-VMs erneut.
   b. Rufen Sie Anwendungen online auf.
5. Rufen Sie ein Failback zur geschützten Site auf, indem Sie SnapMirror nach der Wiederherstellung der primären Site rückwärts neu synchronisieren.

Bereitstellungsdetails

▼ **Konfigurieren Sie CVO in Google Cloud und replizieren Sie Volumes nach CVO**

Der erste Schritt besteht darin, Cloud Volumes ONTAP auf Google Cloud zu konfigurieren ("cvo") und replizieren Sie die gewünschten Volumes mit den gewünschten Frequenzen und Snapshot-Aufbewahrungen auf Cloud Volumes ONTAP .



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter"Einrichten der Replikation mit SnapCenter"

Überprüfung des SQL-VM-Schutzes mit SnapCenter

▼ **Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff**

Zwei wichtige Faktoren, die bei der Bereitstellung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer der Betriebsdauer des SDDC. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann aus nur drei Hosts bestehen, bei einer vollständigen Bereitstellung kann es aber auch ein Cluster mit mehreren Hosts sein.

Google Cloud NetApp Volumes für NFS-Datenspeicher und Cloud Volumes ONTAP für SQL-Datenbanken und -Protokolle können in jedem VPC bereitgestellt werden und GCVE sollte über eine private Verbindung zu diesem VPC verfügen, um den NFS-Datenspeicher zu mounten und die VM mit iSCSI-LUNs zu verbinden.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter"Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)" . Stellen Sie als Voraussetzung sicher, dass die auf den GCVE-Hosts befindlichen Gast-VMs nach dem Herstellen der Verbindung Daten von Cloud Volumes ONTAP nutzen können.

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 Anwendungs-VMDKs und VMs mit In-Guest-Speicher) zu automatisieren. Verwenden Sie dazu die Replikationsfunktion von Veeam und nutzen Sie SnapMirror für Anwendungs-Volume-Kopien auf Cloud Volumes ONTAP.

▼ **Veeam-Komponenten installieren**

Basierend auf dem Bereitstellungsszenario müssen der Veeam-Sicherungsserver, das Sicherungsrepository und der Sicherungsproxy bereitgestellt werden. Für diesen Anwendungsfall ist es nicht erforderlich, einen Objektspeicher für Veeam bereitzustellen, und auch ein Scale-Out-Repository ist nicht erforderlich. "Informationen zum Installationsverfahren finden Sie in der Veeam-Dokumentation." Weitere Informationen finden Sie unter"Migration mit Veeam Replication"

▼ **Einrichten der VM-Replikation mit Veeam**

Sowohl das lokale vCenter als auch das GCVE vCenter müssen bei Veeam registriert werden. "Einrichten des vSphere VM-Replikationsjobs" Wählen Sie im Schritt „Gastverarbeitung“ des Assistenten die Option „Anwendungsverarbeitung deaktivieren“, da wir SnapCenter für die anwendungsbewusste Sicherung und Wiederherstellung verwenden werden.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

▼ **Failover der Microsoft SQL Server-VM**

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Vorteile dieser Lösung

- Verwendet die effiziente und stabile Replikation von SnapMirror.
- Stellt mit ONTAP Snapshot-Aufbewahrung alle verfügbaren Zeitpunkte wieder her.
- Für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs ist eine vollständige Automatisierung verfügbar, angefangen bei den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung.
- SnapCenter verwendet Klonmechanismen, die das replizierte Volume nicht ändern.
  - Dadurch wird das Risiko einer Datenbeschädigung bei Volumes und Snapshots vermieden.

- Vermeidet Replikationsunterbrechungen während DR-Test-Workflows.
- Nutzt die DR-Daten für Workflows, die über DR hinausgehen, wie etwa Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Fehlerbehebungstests.

- Die Veeam-Replikation ermöglicht das Ändern von VM-IP-Adressen auf der DR-Site.

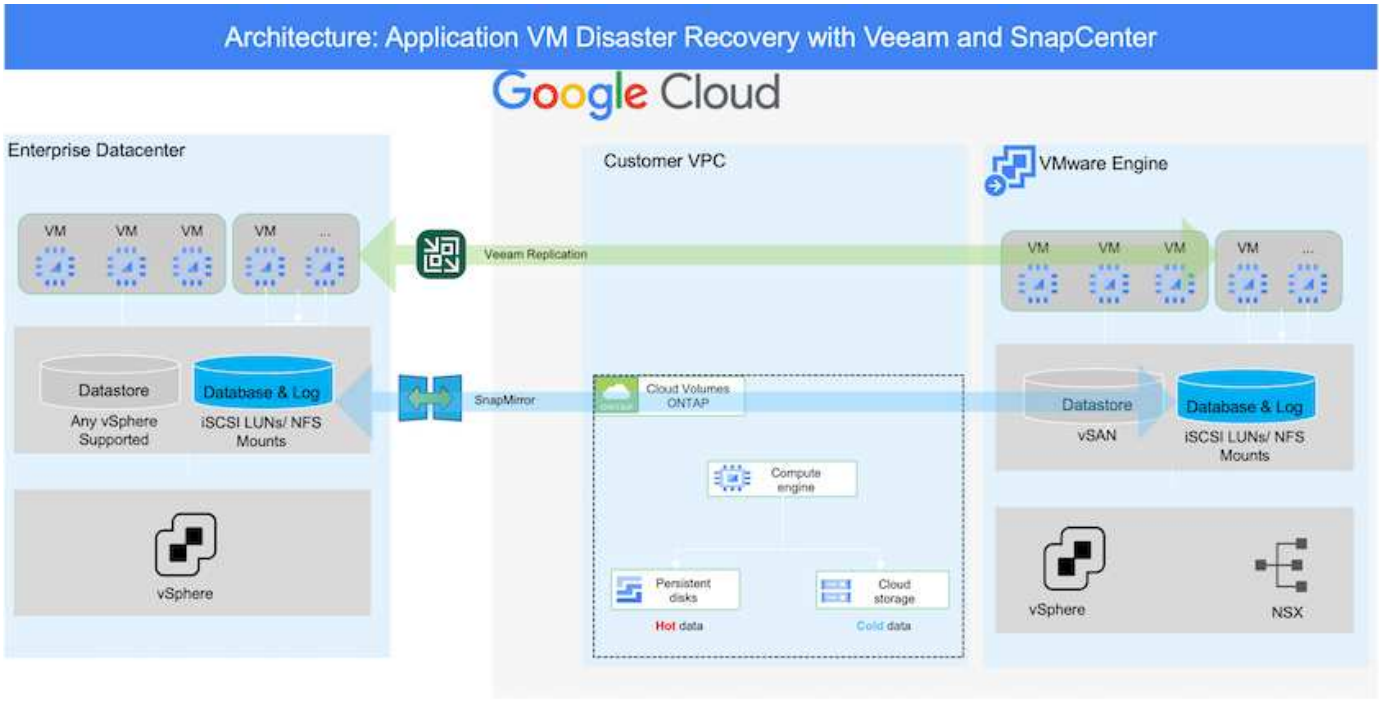
Anwendungs-Notfallwiederherstellung mit SnapCenter, Cloud Volumes ONTAP und Veeam Replication

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, Workloads vor Site-Ausfällen und Datenbeschädigungen wie Ransomware zu schützen. Mit NetApp SnapMirror können lokale VMware-Workloads, die über den Gast verbundenen Speicher verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, das in Google Cloud ausgeführt wird.

Überblick

Dies umfasst Anwendungsdaten. Was ist jedoch mit den eigentlichen VMs selbst? Die Notfallwiederherstellung sollte alle abhängigen Komponenten abdecken, einschließlich virtueller Maschinen, VMDKs, Anwendungsdaten und mehr. Um dies zu erreichen, kann SnapMirror zusammen mit Veeam verwendet werden, um Workloads, die von lokalen Standorten auf Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen, während vSAN-Speicher für VM VMDKs verwendet wird.

Dieses Dokument bietet eine schrittweise Anleitung zum Einrichten und Durchführen einer Notfallwiederherstellung unter Verwendung von NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Annahmen

Dieses Dokument konzentriert sich auf die In-Guest-Speicherung für Anwendungsdaten (auch als Gastverbindung bezeichnet) und wir gehen davon aus, dass die lokale Umgebung SnapCenter für anwendungskonsistente Sicherungen verwendet.

Dieses Dokument gilt für alle Sicherungs- oder Wiederherstellungslösungen von Drittanbietern. Befolgen Sie je nach der in der Umgebung verwendeten Lösung Best Practices, um Sicherungsrichtlinien zu erstellen, die den SLAs des Unternehmens entsprechen.

Verwenden Sie für die Konnektivität zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk Konnektivitätsoptionen wie dedizierte Verbindung oder Cloud-VPN. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

Es gibt mehrere Optionen zum Verbinden lokaler Rechenzentren mit Google Cloud, weshalb wir in diesem Dokument keinen bestimmten Arbeitsablauf beschreiben können. Informationen zur entsprechenden Methode zur Konnektivität zwischen lokalen Standorten und Google finden Sie in der Google Cloud-Dokumentation.

Bereitstellen der DR-Lösung

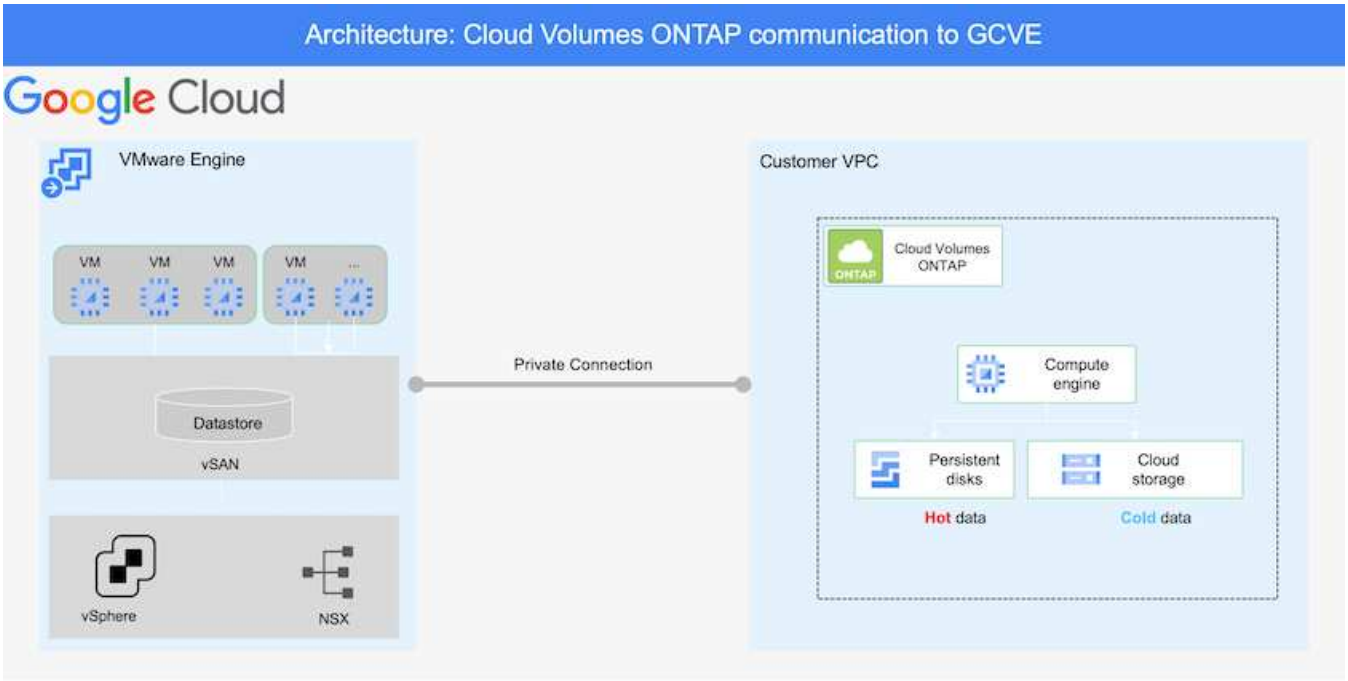
Übersicht über die Lösungsbereitstellung

1. Stellen Sie sicher, dass Anwendungsdaten mit SnapCenter unter Einhaltung der erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie Cloud Volumes ONTAP mit der richtigen Instanzgröße bereit, indem Sie den Cloud Manager innerhalb des entsprechenden Abonnements und virtuellen Netzwerks verwenden.
   a. Konfigurieren Sie SnapMirror für die relevanten Anwendungsvolumes.
   b. Aktualisieren Sie die Sicherungsrichtlinien in SnapCenter , um SnapMirror -Updates nach den geplanten Jobs auszulösen.
3. Installieren Sie die Veeam-Software und beginnen Sie mit der Replikation virtueller Maschinen auf die Google Cloud VMware Engine-Instanz.
4. Unterbrechen Sie im Katastrophenfall die SnapMirror Beziehung mithilfe von Cloud Manager und lösen Sie mit Veeam ein Failover virtueller Maschinen aus.
   a. Verbinden Sie die ISCSI-LUNs und NFS-Mounts für die Anwendungs-VMs erneut.
   b. Rufen Sie Anwendungen online auf.
5. Rufen Sie ein Failback zur geschützten Site auf, indem Sie SnapMirror nach der Wiederherstellung der primären Site rückwärts neu synchronisieren.

Bereitstellungsdetails

▼ **Konfigurieren Sie CVO in Google Cloud und replizieren Sie Volumes nach CVO**

Der erste Schritt besteht darin, Cloud Volumes ONTAP auf Google Cloud zu konfigurieren ("cvo") und replizieren Sie die gewünschten Volumes mit den gewünschten Frequenzen und Snapshot-Aufbewahrungen auf Cloud Volumes ONTAP .



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter"Einrichten der Replikation mit SnapCenter"

Einrichten der Replikation mit SnapCenter

▼ **Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff**

Zwei wichtige Faktoren, die bei der Bereitstellung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer der Betriebsdauer des SDDC. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann aus nur drei Hosts bestehen, bei einer vollständigen Bereitstellung kann es aber auch ein Cluster mit mehreren Hosts sein.

Cloud Volumes ONTAP kann auf jedem VPC bereitgestellt werden und GCVE sollte über eine private Verbindung zu diesem VPC verfügen, damit die VM eine Verbindung zu iSCSI-LUNs herstellen kann.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter"Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)" . Stellen Sie als Voraussetzung sicher, dass die auf den GCVE-Hosts befindlichen Gast-VMs nach dem Herstellen der Verbindung Daten von Cloud Volumes ONTAP nutzen können.

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 Anwendungs-VMDKs und VMs mit In-Guest-Speicher) zu automatisieren. Verwenden Sie dazu die Replikationsfunktion von Veeam und nutzen Sie SnapMirror für Anwendungs-Volume-Kopien auf Cloud Volumes ONTAP.

▼ **Veeam-Komponenten installieren**

Basierend auf dem Bereitstellungsszenario müssen der Veeam-Sicherungsserver, das Sicherungsrepository und der Sicherungsproxy bereitgestellt werden. Für diesen Anwendungsfall ist es nicht erforderlich, einen Objektspeicher für Veeam bereitzustellen, und auch ein Scale-Out-Repository ist nicht erforderlich.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Informationen zum Installationsverfahren finden Sie in der Veeam-Dokumentation."]

▼ **Einrichten der VM-Replikation mit Veeam**

Sowohl das lokale vCenter als auch das GCVE vCenter müssen bei Veeam registriert werden. "Einrichten des vSphere VM-Replikationsjobs" Wählen Sie im Schritt „Gastverarbeitung“ des Assistenten die Option „Anwendungsverarbeitung deaktivieren“, da wir SnapCenter für die anwendungsbewusste Sicherung und Wiederherstellung verwenden werden.

Einrichten des vSphere VM-Replikationsjobs

▼ **Failover der Microsoft SQL Server-VM**

Failover der Microsoft SQL Server-VM

Vorteile dieser Lösung

- Verwendet die effiziente und stabile Replikation von SnapMirror.
- Stellt mit ONTAP Snapshot-Aufbewahrung alle verfügbaren Zeitpunkte wieder her.
- Für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs ist eine vollständige Automatisierung verfügbar, angefangen bei den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung.
- SnapCenter verwendet Klonmechanismen, die das replizierte Volume nicht ändern.
  - Dadurch wird das Risiko einer Datenbeschädigung bei Volumes und Snapshots vermieden.
  - Vermeidet Replikationsunterbrechungen während DR-Test-Workflows.
  - Nutzt die DR-Daten für Workflows, die über DR hinausgehen, wie etwa Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Fehlerbehebungstests.
- Die Veeam-Replikation ermöglicht das Ändern von VM-IP-Adressen auf der DR-Site.

Verwenden von Veeam Replication und Google Cloud NetApp Volumes -Datenspeicher für die Notfallwiederherstellung auf Google Cloud VMware Engine

Ein umfassender Notfallwiederherstellungsplan ist für Unternehmen in Krisenzeiten von entscheidender Bedeutung. Viele Organisationen nutzen Cloud Computing für den täglichen Betrieb und die Notfallwiederherstellung. Dieser proaktive Ansatz kann kostspielige Geschäftsunterbrechungen reduzieren oder vermeiden.

In diesem Artikel wird beschrieben, wie Sie mit Veeam Backup & Replication die Notfallwiederherstellung für lokale VMware-VMs auf Google Cloud VMware Engine (GCVE) mit Google Cloud NetApp Volumes (NetApp Volumes) einrichten.

Überblick

Google Cloud NetApp Volumes ist ein Speicherdienst von Google und NetApp , der für Google Cloud verfügbar ist. Der NetApp Volumes-Dienst bietet leistungsstarken NFS/SMB-Speicher. VMware-zertifizierter NetApp Volumes NFS-Speicher kann als externer Datenspeicher für ESXi-Hosts in GCVE verwendet werden. Benutzer müssen eine Peering-Verbindung zwischen ihrer privaten GCVE-Cloud und dem NetApp Volumes-Projekt herstellen. Innerhalb einer Region fallen keine Netzgebühren für den Speicherzugriff an. Benutzer können NetApp Volumes-Volumes in der Google Cloud-Konsole erstellen und den Löschschutz aktivieren, bevor sie Volumes als Datenspeicher auf ihren ESXi-Hosts bereitstellen.

Auf NetApp Volumes basierende NFS-Datenspeicher können zum Replizieren von Daten vor Ort mithilfe jeder validierten Drittanbieterlösung verwendet werden, die VM-Replikationsfunktionen bietet. Durch das Hinzufügen von NetApp Volumes-Datenspeichern wird eine kostenoptimierte Bereitstellung ermöglicht, anstatt ein auf Google Cloud VMware Engine (GCVE) basierendes SDDC mit einer großen Anzahl von ESXi-Hosts zur

Unterbringung des Speichers aufzubauen. Dieser Ansatz wird als „Pilot Light Cluster“ bezeichnet. Ein Pilot Light Cluster ist eine minimale GCVE-Hostkonfiguration (3 x GCVE ESXi-Hosts) zusammen mit der Kapazität von NetApp Volumes-Datenspeichern, um eine unabhängige Skalierung zur Erfüllung der Kapazitätsanforderungen zu ermöglichen.

Das Ziel besteht darin, eine kostengünstige Infrastruktur aufrechtzuerhalten, die nur die Kernkomponenten zur Verwaltung eines Failovers umfasst. Ein Pilot Light-Cluster kann im Falle eines Failovers erweitert werden und weitere GCVE-Hosts hinzufügen. Sobald das Failover behoben ist und der normale Betrieb wieder aufgenommen wird, kann der Pilot Light Cluster seine Größe reduzieren und in einen kostengünstigen Betriebsmodus zurückkehren.

Zweck dieses Dokuments

In diesem Artikel wird beschrieben, wie Sie mithilfe eines Google Cloud NetApp Volumes -Datenspeichers mit Veeam Backup & Replication die Notfallwiederherstellung für lokale VMware-VMs zu GCVE mithilfe der VM-Replikationssoftwarefunktion von Veeam einrichten.

Veeam Backup & Replication ist eine Backup- und Replikationsanwendung für virtuelle Umgebungen. Wenn virtuelle Maschinen repliziert werden, erstellt Veeam Backup & Replication eine exakte Kopie der VMs im nativen VMware vSphere-Format auf dem Ziel-GCVE-SDDC-Cluster. Veeam Backup & Replication hält die Kopie mit der ursprünglichen VM synchronisiert. Die Replikation bietet die beste Wiederherstellungszeit (RTO), da am DR-Standort eine bereitgestellte Kopie einer VM in einem startbereiten Zustand vorhanden ist.

Dieser Replikationsmechanismus stellt sicher, dass die Workloads im Katastrophenfall schnell in GCVE gestartet werden können. Die Veeam Backup & Replication-Software optimiert außerdem die Verkehrsübertragung für die Replikation über WAN und langsame Verbindungen. Darüber hinaus filtert es auch doppelte Datenblöcke, Null-Datenblöcke, Auslagerungsdateien und „ausgeschlossene VM-Gastbetriebssystemdateien“ heraus. Die Software komprimiert außerdem den Replikationsverkehr. Um zu verhindern, dass Replikationsaufträge die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Netzwerkdrosselungsregeln verwendet werden.

Der Replikationsprozess in Veeam Backup & Replication ist auftragsgesteuert, d. h. die Replikation wird durch die Konfiguration von Replikationsaufträgen durchgeführt. Im Katastrophenfall kann ein Failover ausgelöst werden, um die VMs durch ein Failover auf ihre Replikatkopie wiederherzustellen. Beim Failover übernimmt eine replizierte VM die Rolle der ursprünglichen VM. Das Failover kann auf den neuesten Status einer Replik oder auf einen ihrer bekannten funktionierenden Wiederherstellungspunkte durchgeführt werden. Dies ermöglicht bei Bedarf eine Ransomware-Wiederherstellung oder isolierte Tests. Veeam Backup & Replication bietet mehrere Optionen zur Handhabung verschiedener Notfallwiederherstellungsszenarien.

Lösungsübersicht

Diese Lösung umfasst die folgenden Schritte auf hoher Ebene:

1. Erstellen Sie ein NFS-Volume mit Google Cloud NetApp Volumes
2. Befolgen Sie den GCP-Prozess, um einen GCVE-Datenspeicher aus dem NFS-Volume von NetApp Volumes zu erstellen.
3. Richten Sie einen Replikationsauftrag ein, um VM-Replikate mit Veeam Backup & Replication zu erstellen.
4. Erstellen Sie einen Failover-Plan und führen Sie das Failover durch.
5. Wechseln Sie zurück zu Produktions-VMs, sobald das Notfallereignis abgeschlossen ist und die primäre Site wieder aktiv ist.

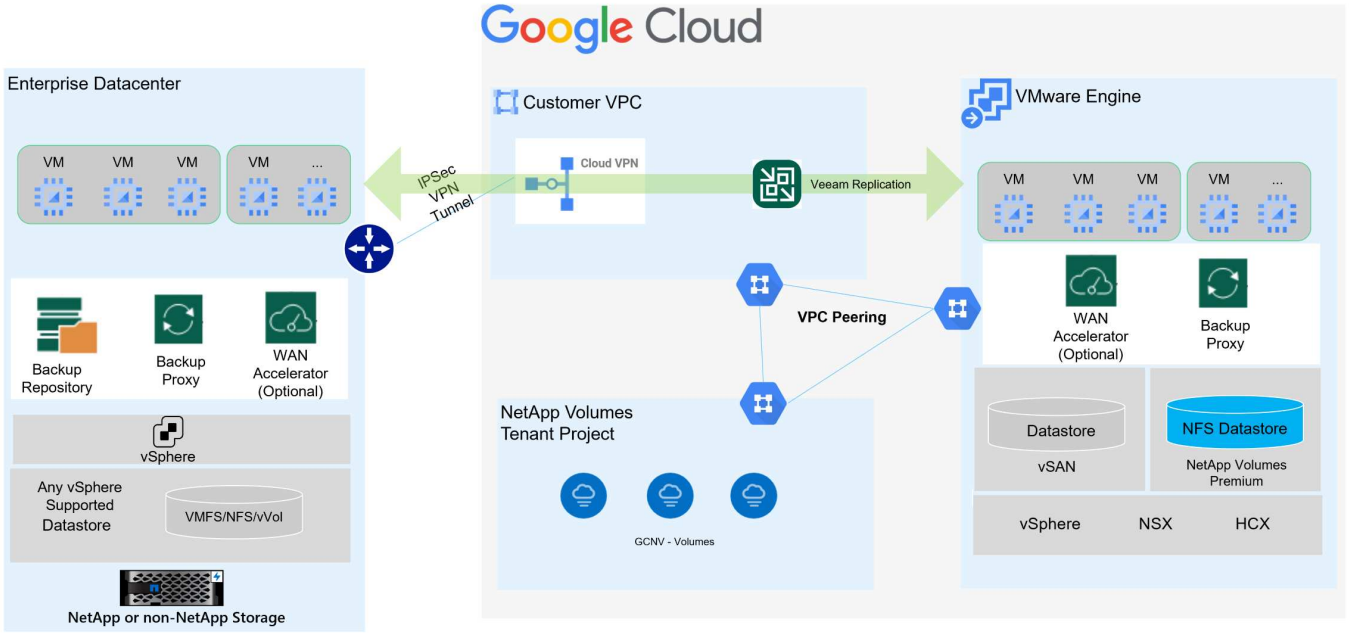


Beim Erstellen eines Volumes in NetApp Volumes zur Verwendung als GCVE-Datenspeicher wird nur NFS v3 unterstützt.

Weitere Informationen zur Verwendung von NetApp Volumes NFS-Volumes als Datenspeicher für GCVE finden Sie unter "Verwenden des NFS-Volumes als vSphere-Datenspeicher, der von Google Cloud NetApp Volumes gehostet wird" .

Architektur

Das folgende Diagramm zeigt die Architektur der in dieser Dokumentation vorgestellten Lösung. Als bewährte Methode wird empfohlen, einen Veeam Backup & Replication-Server sowohl am Standort vor Ort als auch im GCVE SDDC zu haben. Sicherung und Wiederherstellung werden vom Veeam-Server vor Ort durchgeführt und verwaltet, und die Replikation wird vom Veeam-Server im GCVE SDDC verwaltet. Diese Architektur bietet die höchste Verfügbarkeit, wenn im primären Rechenzentrum ein Fehler auftritt.



Voraussetzungen für die Veeam-Replikation in GCVE- und NetApp Volumes-Datenspeichern

Diese Lösung erfordert die folgenden Komponenten und Konfigurationen:

1. NetApp Volumes verfügt über einen Speicherpool mit ausreichend freier Kapazität, um das zu erstellende NFS-Volume aufzunehmen.
2. Die Veeam Backup and Replication-Software wird in einer lokalen Umgebung mit entsprechender Netzwerkkonnektivität ausgeführt.
3. Stellen Sie sicher, dass die Veeam Backup & Replication-Sicherungs-VM sowohl mit den Quell- als auch mit den Ziel-GCVE-SDDC-Clustern verbunden ist.
4. Stellen Sie sicher, dass die Veeam Backup & Replication-Sicherungs-VM mit den Veeam Proxy-Server-VMs sowohl im Quell- als auch im Ziel-GCVE-Cluster verbunden ist.
5. Der Sicherungsserver muss in der Lage sein, Kurznamen aufzulösen und eine Verbindung zu Quell- und Ziel-vCentern herzustellen.

Benutzer müssen eine Peering-Verbindung zwischen ihrer privaten GCVE-Cloud und dem NetApp Volumes-Projekt herstellen, indem sie die Seiten „VPC-Netzwerk-Peering“ oder „Private Verbindungen“ in der Benutzeroberfläche der VMware Engine Cloud-Konsole verwenden.

Veeam benötigt ein GCVE Lösungsbenutzerkonto mit erhöhten Berechtigungen, wenn der

> GCVE vCenter Server zum Veeam Backup and Replication Inventar hinzugefügt wird. Weitere Informationen sind in der Dokumentation der Google Cloud Platform (GCP) "Erhöhen der VMware Engine-Berechtigungen" zu finden.

Weitere Informationen finden Sie unter "Überlegungen und Einschränkungen" in der Veeam Backup & Replication-Dokumentation.

Bereitstellungsschritte

In den folgenden Abschnitten werden die Bereitstellungsschritte zum Erstellen und Einbinden eines NFS-Datenspeichers mithilfe von Google Cloud NetApp Volumes und zur Verwendung von Veeam Backup and Replication zum Implementieren einer vollständigen Notfallwiederherstellungslösung zwischen einem lokalen Rechenzentrum und Google Cloud VMware Engine beschrieben.

Erstellen Sie ein NetApp Volumes NFS-Volume und einen Datenspeicher für GCVE

Siehe "Verwenden des NFS-Volumes als vSphere-Datenspeicher, der von Google Cloud NetApp Volumes gehostet wird" für eine Übersicht zur Verwendung von Google Cloud NetApp Volumes als Datenspeicher für GCVE.

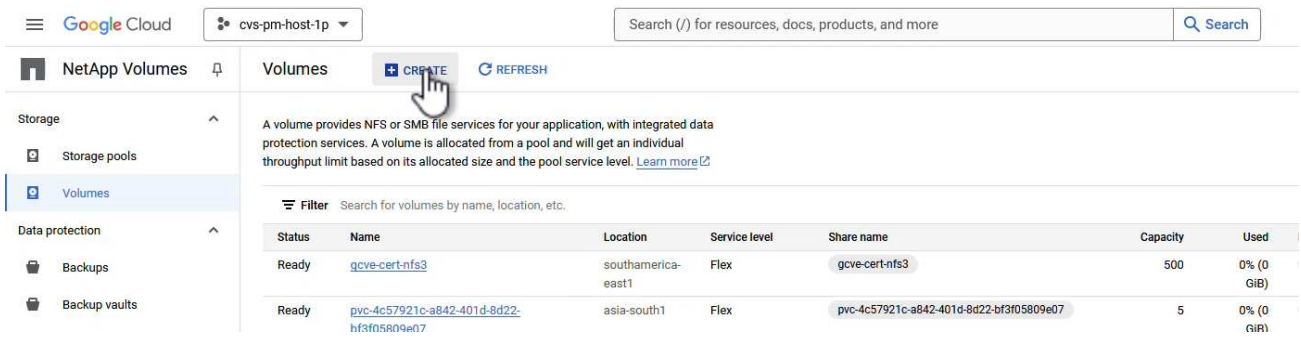
Führen Sie die folgenden Schritte aus, um einen NFS-Datenspeicher für GCVE mit NetApp Volumes zu erstellen und zu verwenden:

▼ **NetApp Volumes NFS-Volume erstellen**

Der Zugriff auf Google Cloud NetApp Volumes erfolgt über die Konsole der Google Cloud Platform (GCP).

Siehe "Erstellen eines Volumes" Ausführliche Informationen zu diesem Schritt finden Sie in der Dokumentation zu Google Cloud NetApp Volumes .

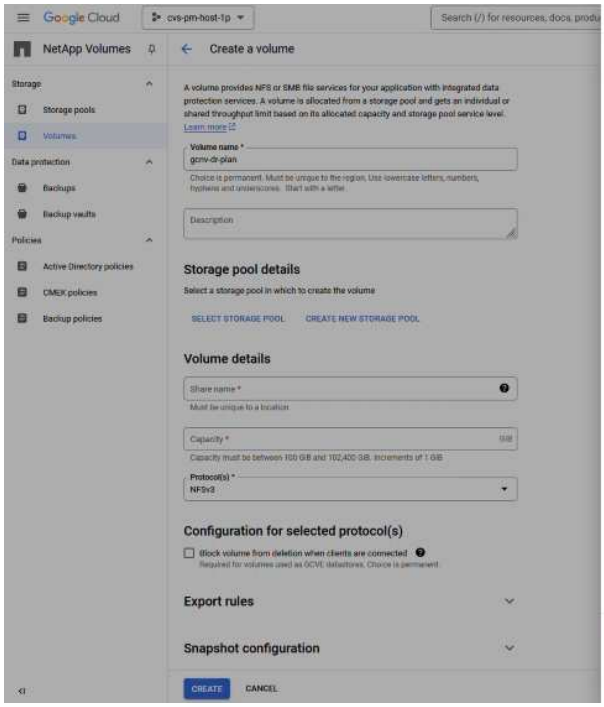
1. Navigieren Sie in einem Webbrowser zu https://console.cloud.google.com/ und melden Sie sich bei Ihrer GCP-Konsole an. Suchen Sie nach * NetApp Volumes*, um zu beginnen.
2. Klicken Sie in der Verwaltungsoberfläche * NetApp Volumes* auf **Erstellen**, um mit der Erstellung eines NFS-Volumes zu beginnen.

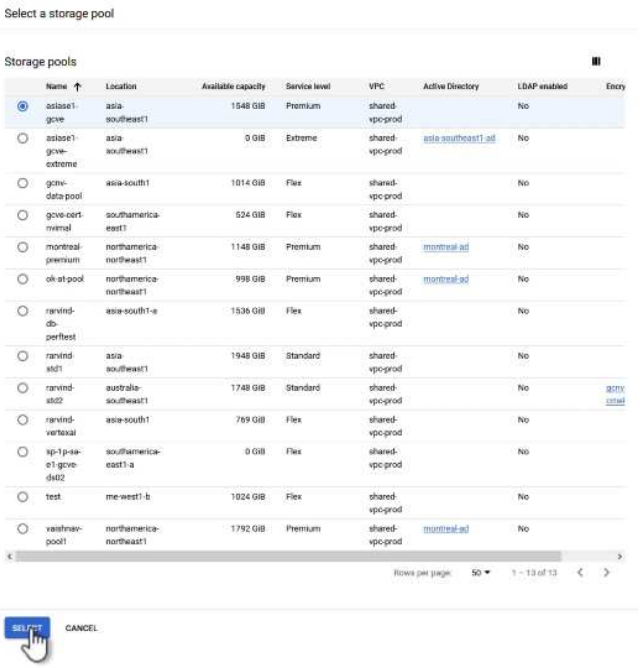


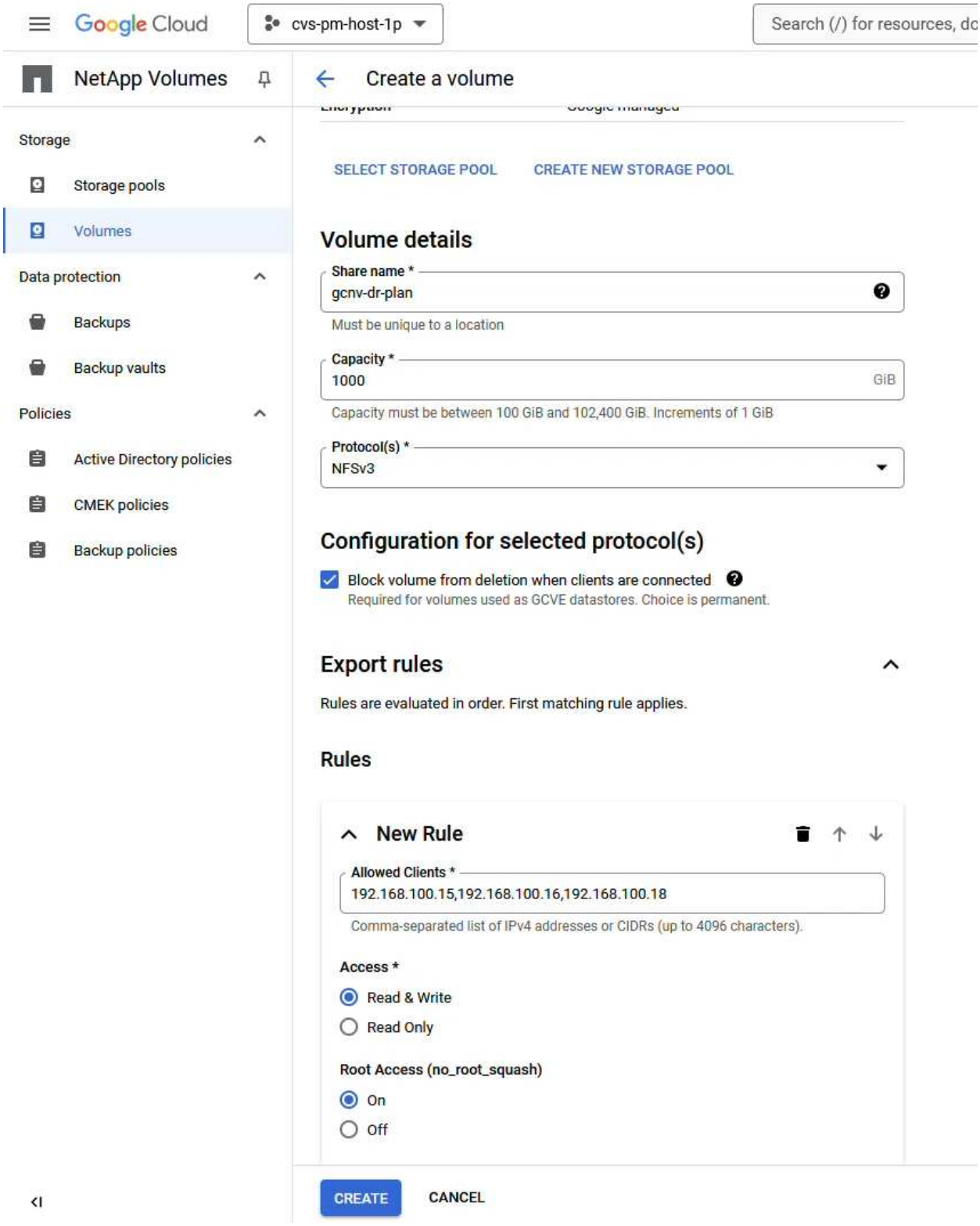
3. Geben Sie im Assistenten „Volume erstellen“ alle erforderlichen Informationen ein:
   - Ein Name für das Volume.
   - Der Speicherpool, auf dem das Volume erstellt werden soll.
   - Ein Freigabename, der beim Mounten des NFS-Volumes verwendet wird.
   - Die Kapazität des Datenträgers in GiB.

- Das zu verwendende Speicherprotokoll.
- Aktivieren Sie das Kontrollkästchen, um **Löschen des Volumes zu verhindern, wenn Clients verbunden sind** (erforderlich für GCVE beim Mounten als Datenspeicher).
- Die Exportregeln für den Zugriff auf das Volume. Dies sind die IP-Adressen der ESXi-Adapter im NFS-Netzwerk.
- Ein Snapshot-Zeitplan, der zum Schutz des Volumes mithilfe lokaler Snapshots verwendet wird.
- Optional können Sie das Volume sichern und/oder Bezeichnungen für das Volume erstellen.

Beim Erstellen eines Volumes in NetApp Volumes zur Verwendung als GCVE-Datenspeicher wird nur NFS v3 unterstützt.

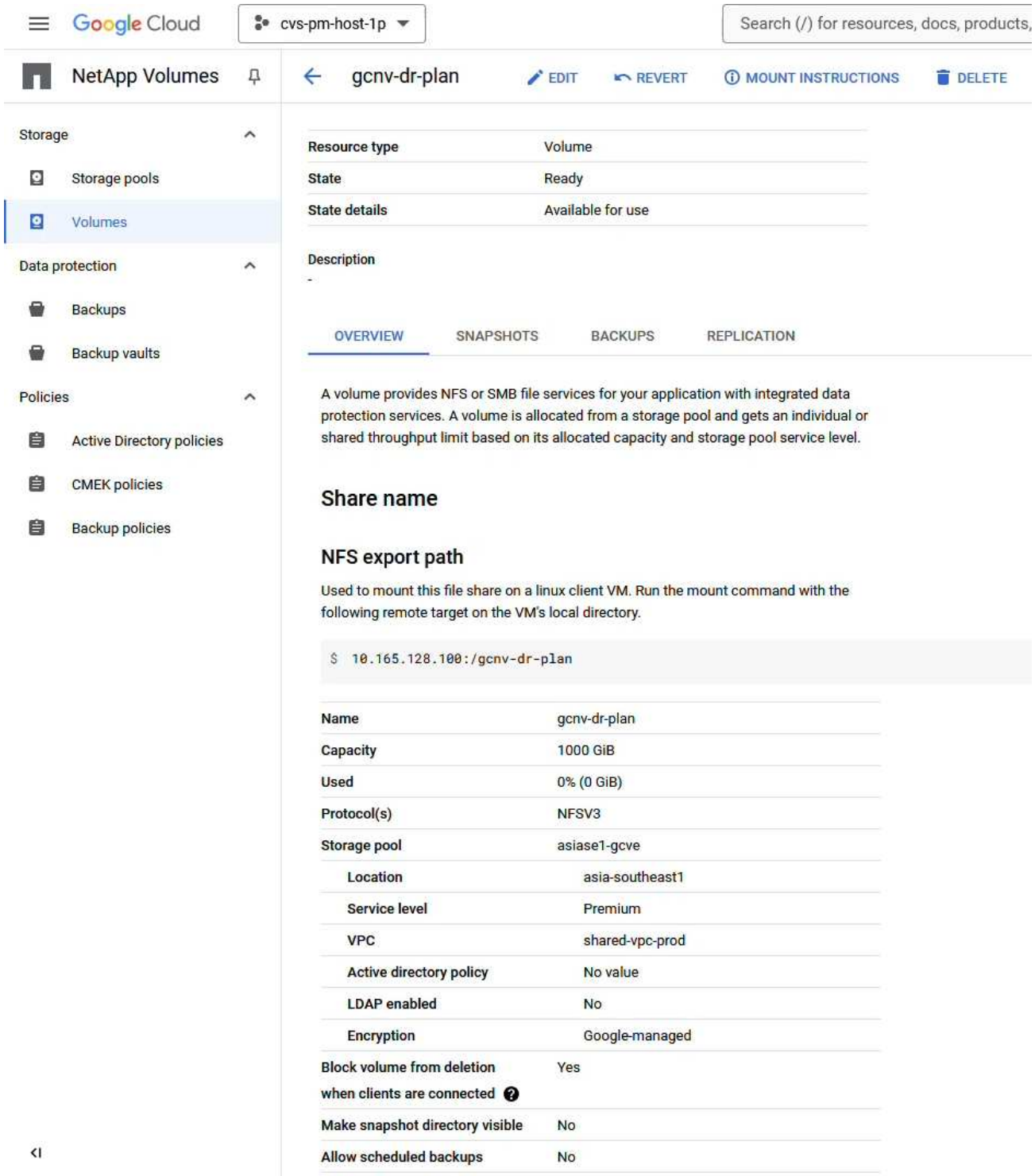






Klicken Sie auf **Erstellen**, um die Erstellung des Volumes abzuschließen.

4. Sobald das Volume erstellt ist, kann der zum Mounten des Volumes erforderliche NFS-Exportpfad auf der Eigenschaftenseite des Volumes angezeigt werden.



▼ **Mounten Sie den NFS-Datenspeicher in GCVE**

Zum Zeitpunkt des Schreibens dieses Artikels erfordert der Vorgang zum Mounten eines Datenspeichers in GCVE das Öffnen eines GCP-Supporttickets, um das Volume als NFS-Datenspeicher mounten zu lassen.

Siehe "Verwenden des NFS-Volumes als vSphere-Datenspeicher, der von Google Cloud NetApp Volumes gehostet wird" für weitere Informationen.

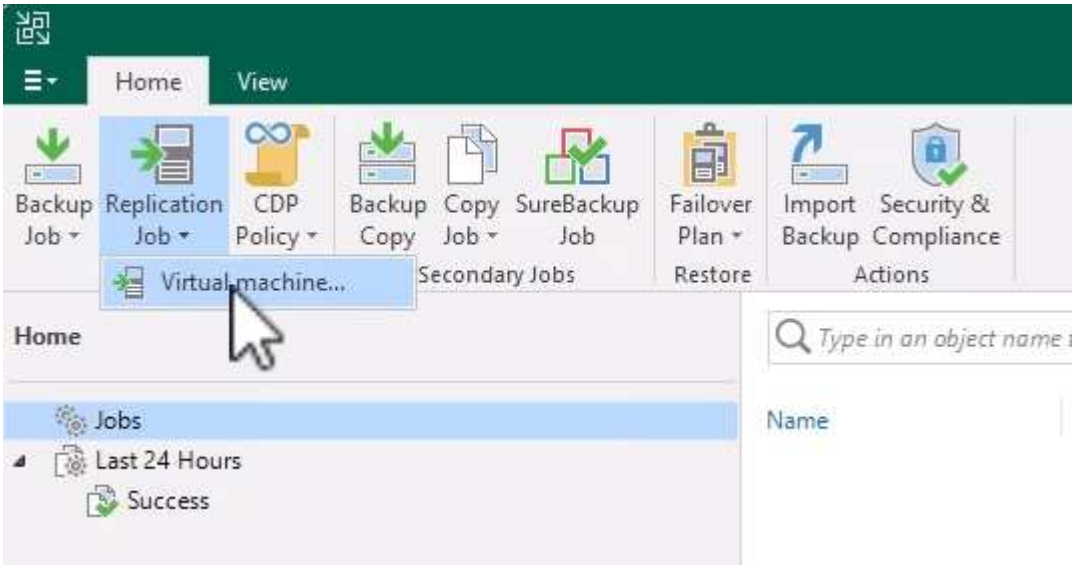
Replizieren Sie VMs zu GCVE und führen Sie einen Failover-Plan und ein Failback aus

▼ **Replizieren Sie VMs in den NFS-Datenspeicher in GCVE**

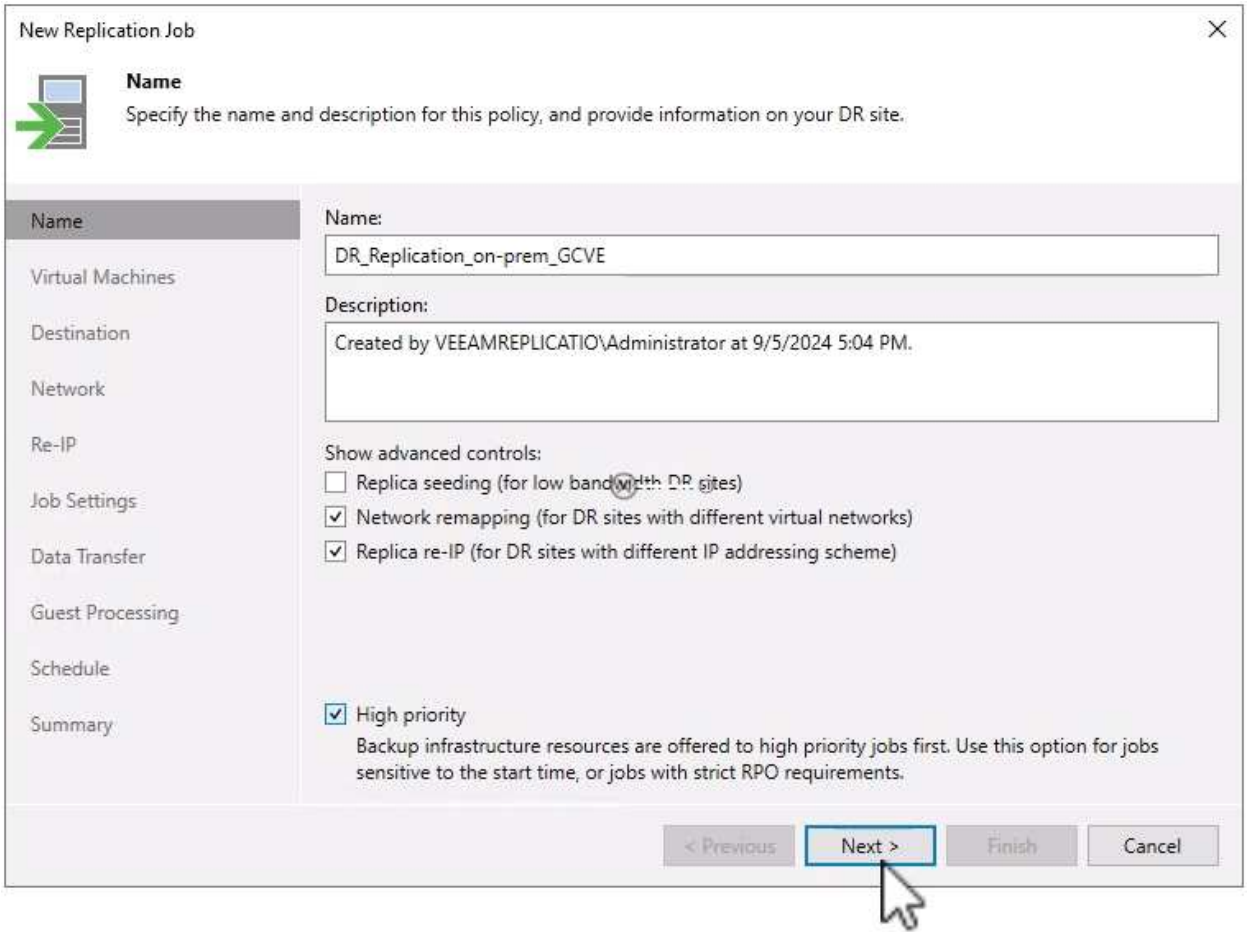
Veeam Backup & Replication nutzt während der Replikation die Snapshot-Funktionen von VMware vSphere. Veeam Backup & Replication fordert VMware vSphere auf, einen VM-Snapshot zu erstellen. Der VM-Snapshot ist die zeitpunktbezogene Kopie einer VM, die virtuelle Festplatten, Systemstatus, Konfiguration und Metadaten enthält. Veeam Backup & Replication verwendet den Snapshot als Datenquelle für die Replikation.

Führen Sie zum Replizieren von VMs die folgenden Schritte aus:

1. Öffnen Sie die Veeam Backup & Replication-Konsole.
2. Klicken Sie auf der Registerkarte **Startseite** auf **Replikationsauftrag > Virtuelle Maschine…**

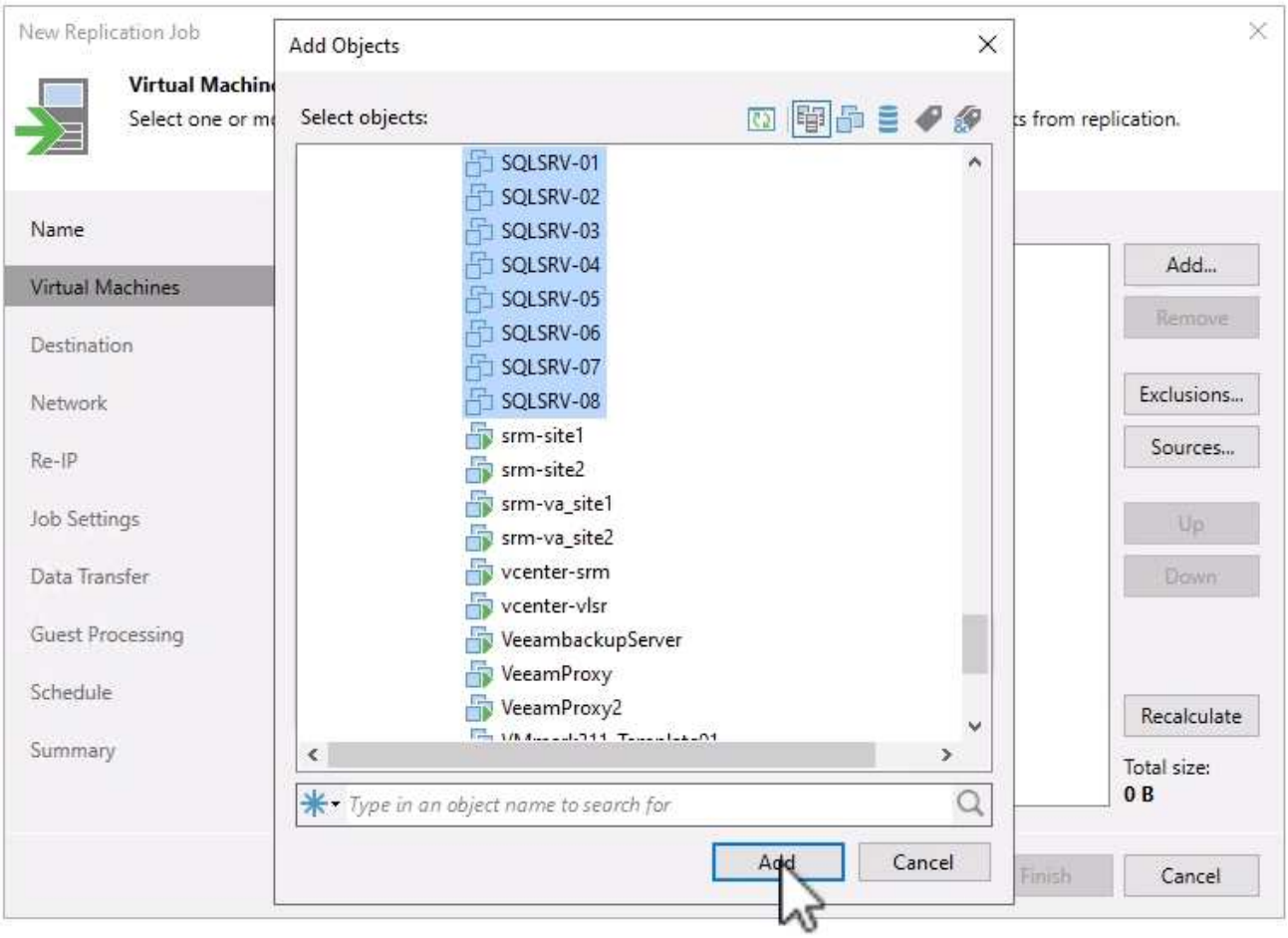


3. Geben Sie auf der Seite **Name** des Assistenten **Neuer Replikationsjob** einen Jobnamen an und aktivieren Sie die entsprechenden Kontrollkästchen für die erweiterte Steuerung.
   - Aktivieren Sie das Kontrollkästchen „Replikat-Seeding“, wenn die Bandbreite der Konnektivität zwischen lokalen Standorten und GCP eingeschränkt ist.
   - Aktivieren Sie das Kontrollkästchen „Netzwerkneuzuordnung (für GCVE SDDC-Sites mit unterschiedlichen Netzwerken), wenn die Segmente auf dem GCVE SDDC nicht mit denen der lokalen Site-Netzwerke übereinstimmen.
   - Aktivieren Sie das Kontrollkästchen „Replikat-Re-IP (für DR-Sites mit unterschiedlichem IP-Adressschema)“, wenn sich das IP-Adressschema am lokalen Produktionsstandort vom Schema am GCVE-Zielstandort unterscheidet.

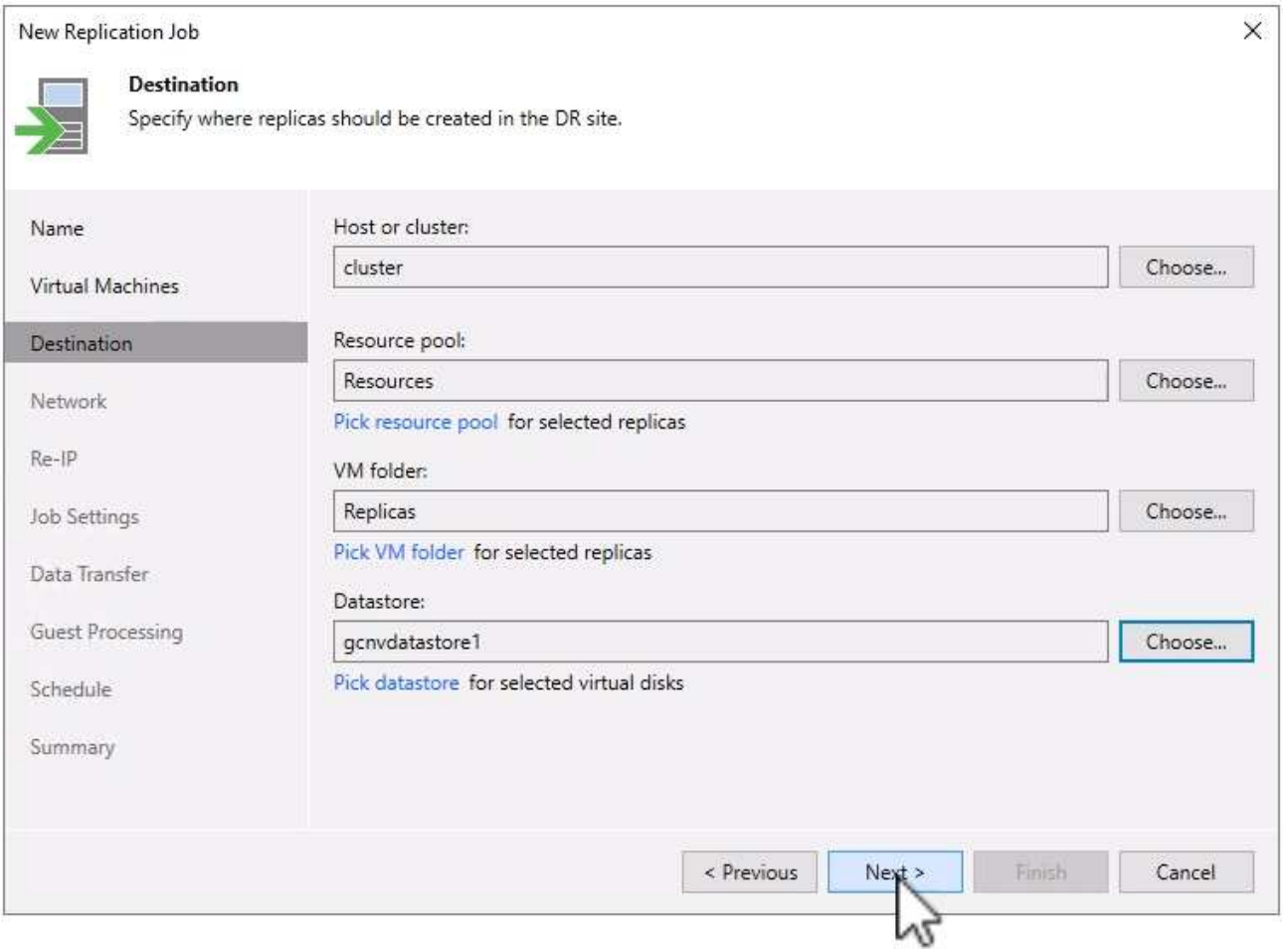


4. Wählen Sie auf der Seite **Virtuelle Maschinen** die VMs aus, die in den NetApp Volumes-Datenspeicher repliziert werden sollen, der an ein GCVE SDDC angeschlossen ist. Klicken Sie auf **Hinzufügen**, wählen Sie dann im Fenster **Objekt hinzufügen** die erforderlichen VMs oder VM-Container aus und klicken Sie auf **Hinzufügen**. Klicken Sie auf **Weiter**.

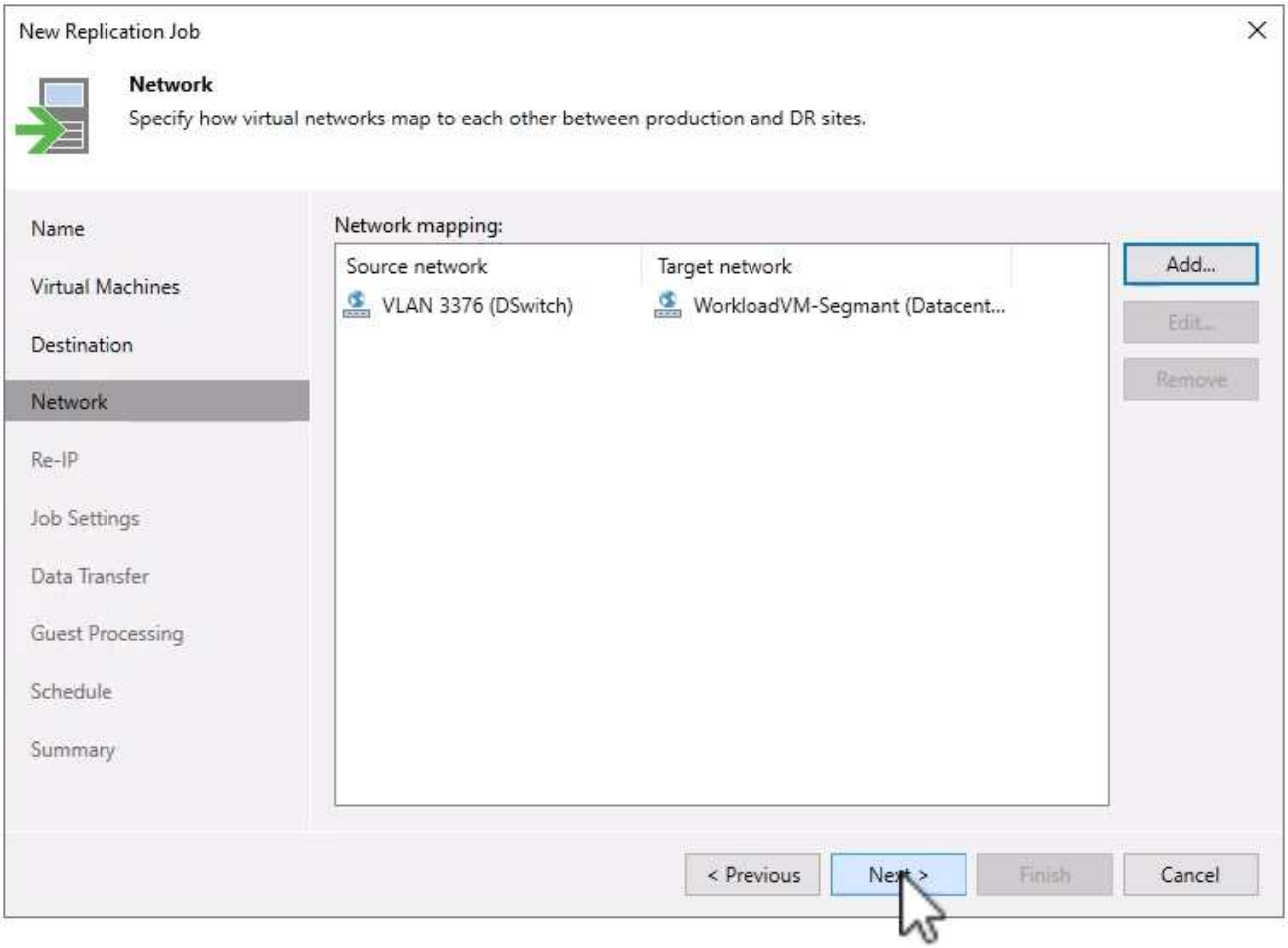
> Die virtuellen Maschinen können auf vSAN platziert werden, um die verfügbare vSAN-Datenspeicherkapazität zu füllen. In einem Pilot-Light-Cluster ist die nutzbare Kapazität eines 3-Knoten-vSAN-Clusters begrenzt. Die restlichen Daten können problemlos in Google Cloud NetApp Volumes -Datenspeichern abgelegt werden, sodass die VMs wiederhergestellt und der Cluster später erweitert werden kann, um die CPU-/Speicheranforderungen zu erfüllen.



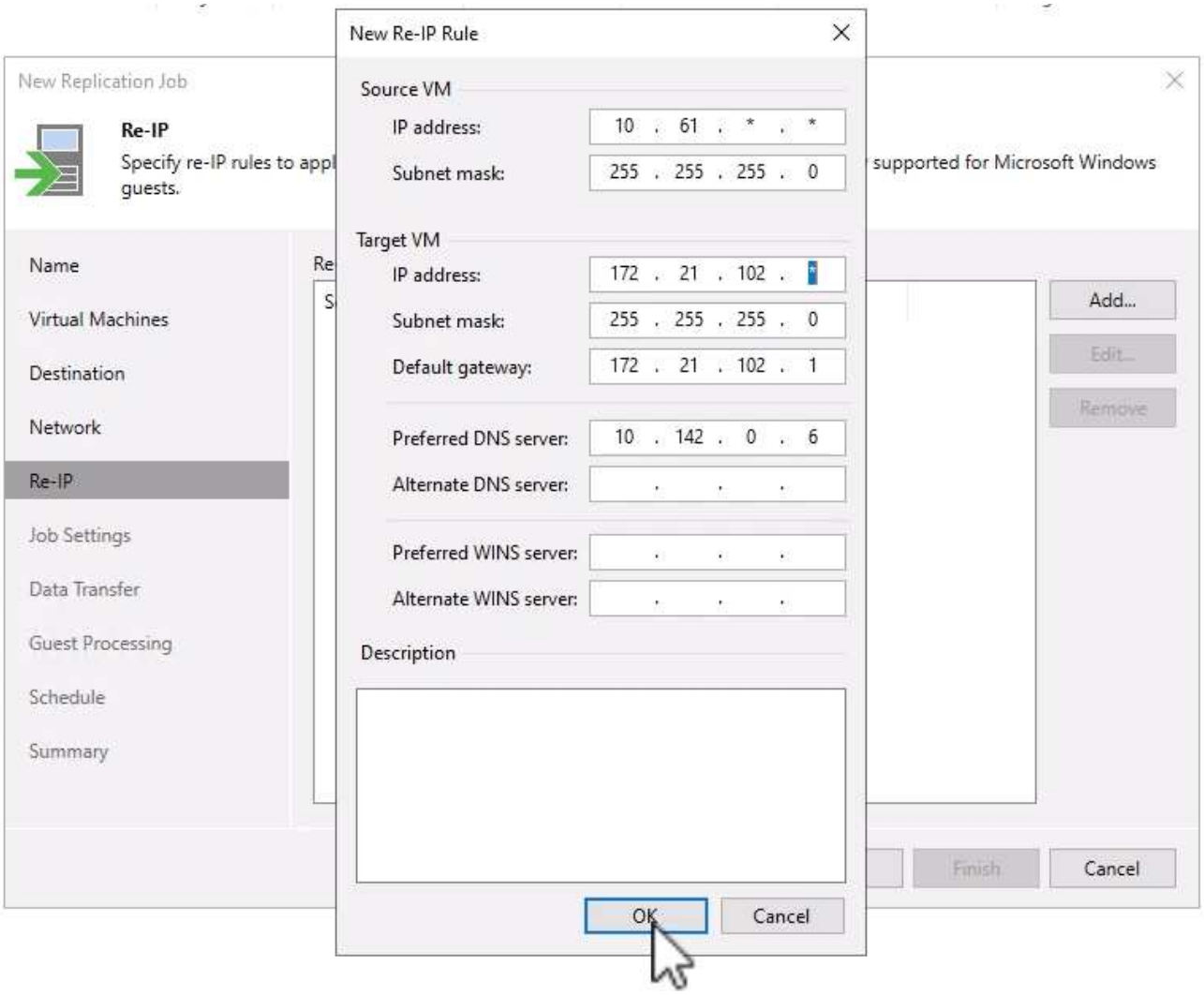
5. Wählen Sie auf der Seite **Ziel** als Ziel den GCVE SDDC-Cluster/Hosts und den entsprechenden Ressourcenpool, VM-Ordner und NetApp Volumes-Datenspeicher für die VM-Replikate aus. Klicken Sie auf **Weiter**, um fortzufahren.



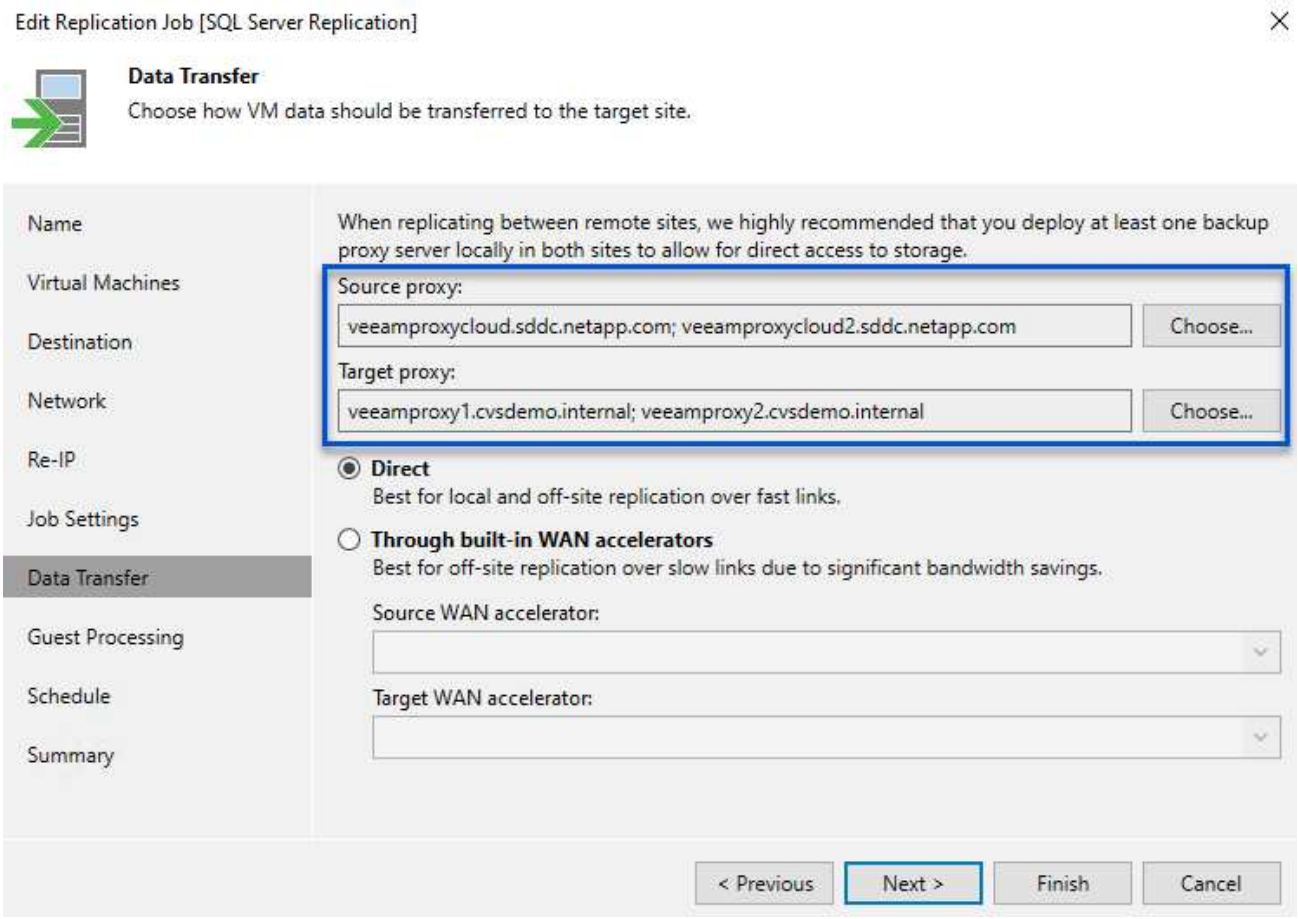
6. Erstellen Sie auf der Seite **Netzwerk** nach Bedarf die Zuordnung zwischen virtuellen Quell- und Zielnetzwerken. Klicken Sie auf **Weiter**, um fortzufahren.



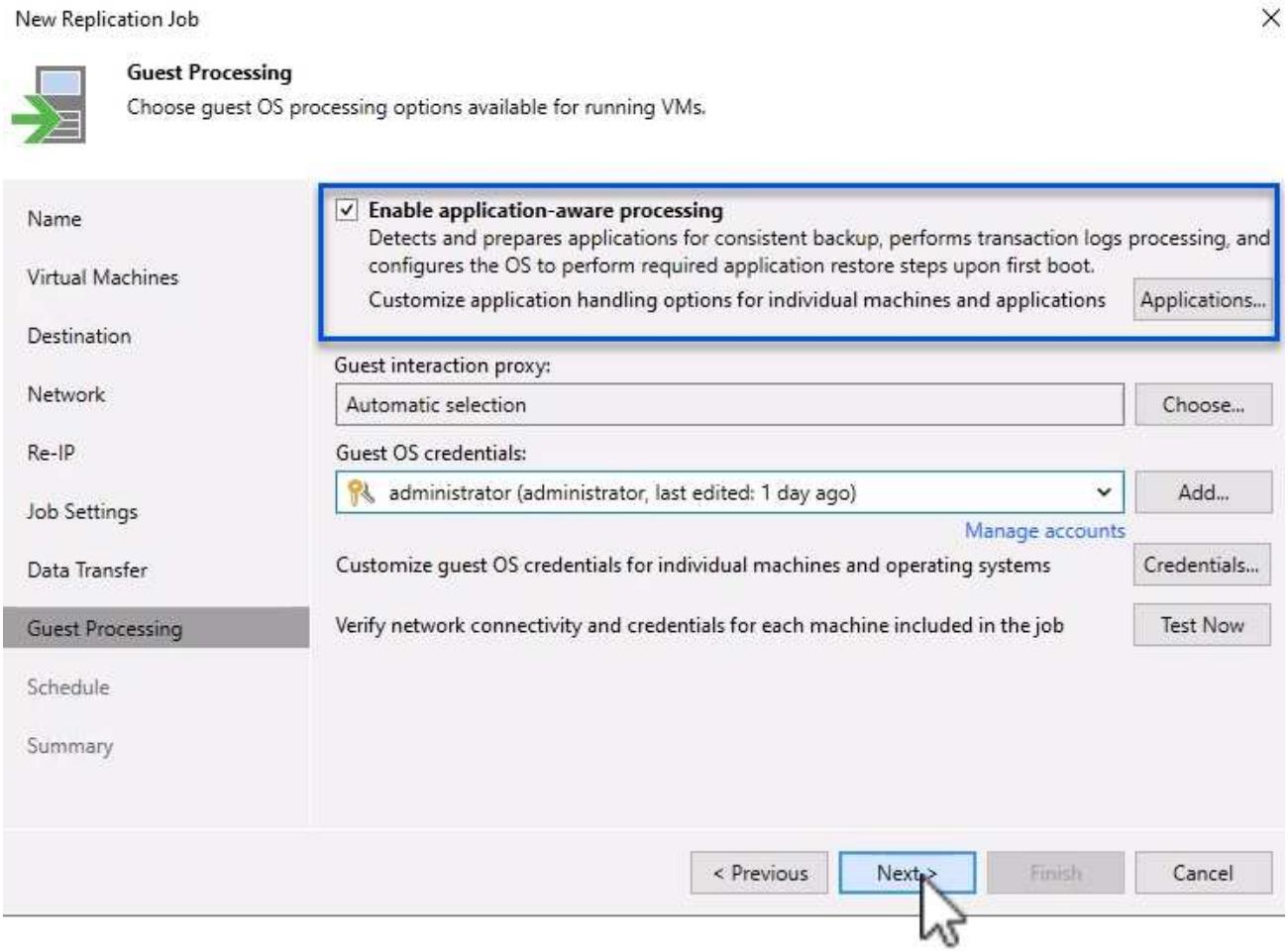
7. Klicken Sie auf der Seite **Re-IP** auf die Schaltfläche **Hinzufügen…**, um eine neue Re-IP-Regel hinzuzufügen. Füllen Sie die IP-Bereiche der Quell- und Ziel-VM aus, um das Netzwerk anzugeben, das im Falle eines Failovers auf die Quell-VMs angewendet wird. Verwenden Sie Sternchen, um einen Adressbereich anzugeben, der für dieses Oktett angegeben ist. Klicken Sie auf **Weiter**, um fortzufahren.



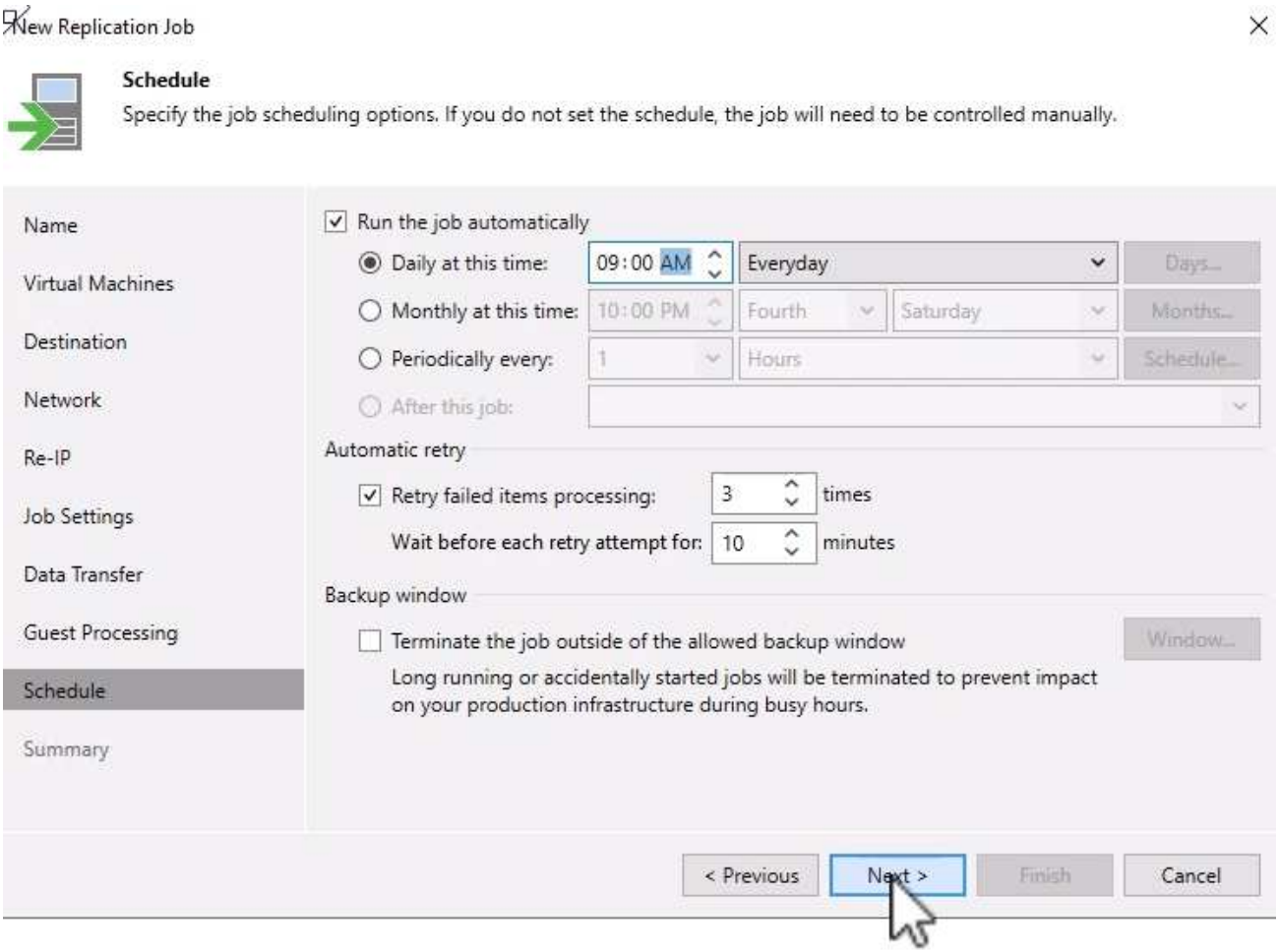
8. Geben Sie auf der Seite **Jobeinstellungen** das Sicherungsrepository an, in dem Metadaten für VM-Replikate gespeichert werden, sowie die Aufbewahrungsrichtlinie und wählen Sie unten die Schaltfläche **Erweitert…** für zusätzliche Jobeinstellungen aus. Klicken Sie auf **Weiter**, um fortzufahren.
9. Wählen Sie bei der **Datenübertragung** die Proxyserver aus, die sich an den Quell- und Zielstandorten befinden, und lassen Sie die Option „Direkt“ ausgewählt. Auch WAN-Beschleuniger können hier ausgewählt werden, sofern konfiguriert. Klicken Sie auf **Weiter**, um fortzufahren.



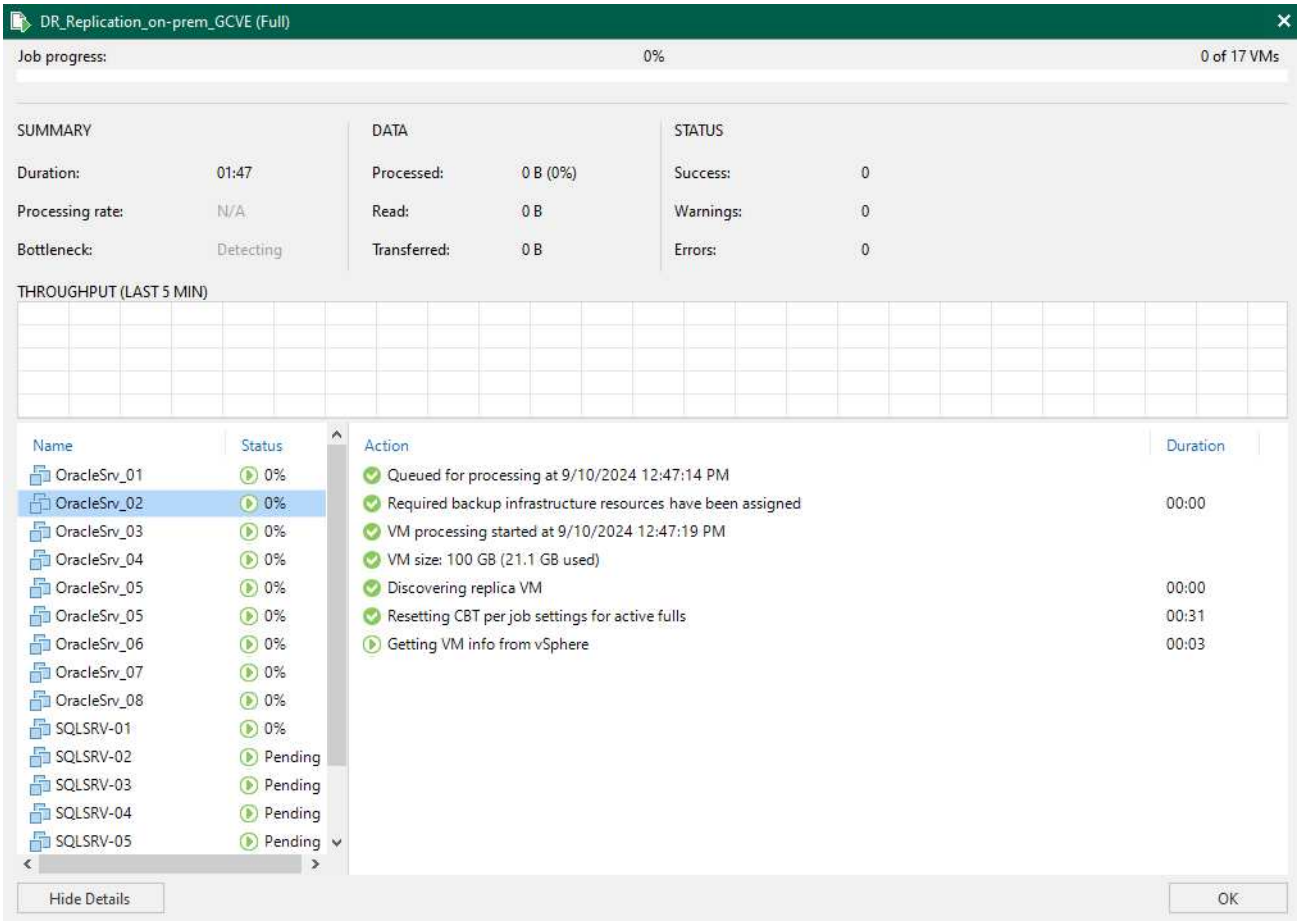
10. Aktivieren Sie auf der Seite **Gastverarbeitung** bei Bedarf das Kontrollkästchen **Anwendungsbewusste Verarbeitung aktivieren** und wählen Sie die **Anmeldeinformationen des Gastbetriebssystems** aus. Klicken Sie auf **Weiter**, um fortzufahren.



11. Definieren Sie auf der Seite **Zeitplan** die Zeiten und die Häufigkeit, mit der der Replikationsauftrag ausgeführt werden soll. Klicken Sie auf **Weiter**, um fortzufahren.



12. Überprüfen Sie abschließend die Jobeinstellungen auf der Seite **Zusammenfassung**. Aktivieren Sie das Kontrollkästchen „Job ausführen, wenn ich auf „Fertig stellen“ klicke“ und klicken Sie auf „Fertig stellen“, um die Erstellung des Replikationsjobs abzuschließen.
13. Nach der Ausführung kann der Replikationsauftrag im Auftragsstatusfenster angezeigt werden.



Weitere Informationen zur Veeam-Replikation finden Sie unter"Funktionsweise der Replikation"

▼ **Erstellen eines Failoverplans**

Wenn die erste Replikation oder das Seeding abgeschlossen ist, erstellen Sie den Failover-Plan. Der Failover-Plan hilft dabei, das Failover für abhängige VMs einzeln oder als Gruppe automatisch durchzuführen. Der Failover-Plan ist die Blaupause für die Reihenfolge, in der die VMs verarbeitet werden, einschließlich der Startverzögerungen. Der Failover-Plan hilft auch sicherzustellen, dass kritische abhängige VMs bereits ausgeführt werden.

Erstellen Sie nach Abschluss der ersten Replikation oder des Seedings einen Failover-Plan. Dieser Plan dient als strategischer Entwurf für die Orchestrierung des Failovers abhängiger VMs, entweder einzeln oder als Gruppe. Es definiert die Verarbeitungsreihenfolge der VMs, berücksichtigt notwendige Startverzögerungen und stellt sicher, dass kritische abhängige VMs vor anderen betriebsbereit sind. Durch die Implementierung eines gut strukturierten Failover-Plans können Unternehmen ihren Disaster-Recovery-Prozess optimieren, Ausfallzeiten minimieren und die Integrität voneinander abhängiger Systeme während eines Failover-Ereignisses aufrechterhalten.

Beim Erstellen des Plans identifiziert und verwendet Veeam Backup & Replication automatisch die aktuellsten Wiederherstellungspunkte, um die VM-Replikate zu initiieren.

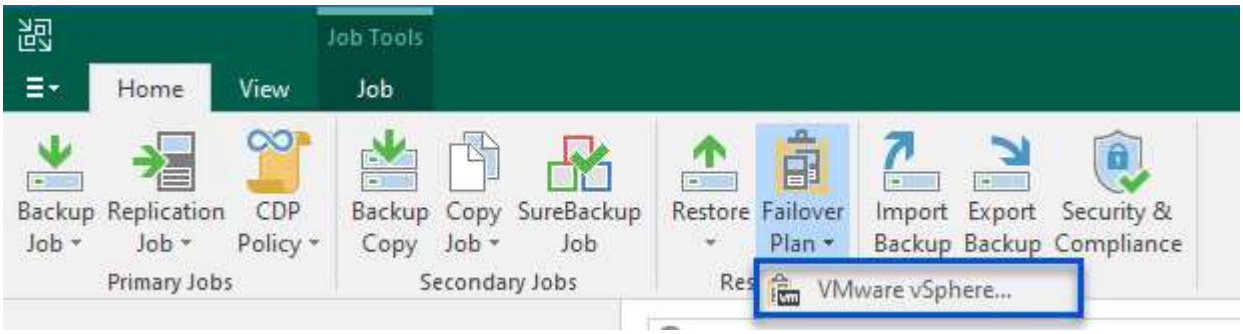
ⓘ Der Failover-Plan kann erst erstellt werden, wenn die erste Replikation abgeschlossen ist und sich die VM-Replikate im Status „Bereit“ befinden.

ⓘ Die maximale Anzahl an VMs, die beim Ausführen eines Failover-Plans gleichzeitig gestartet werden können, beträgt 10.

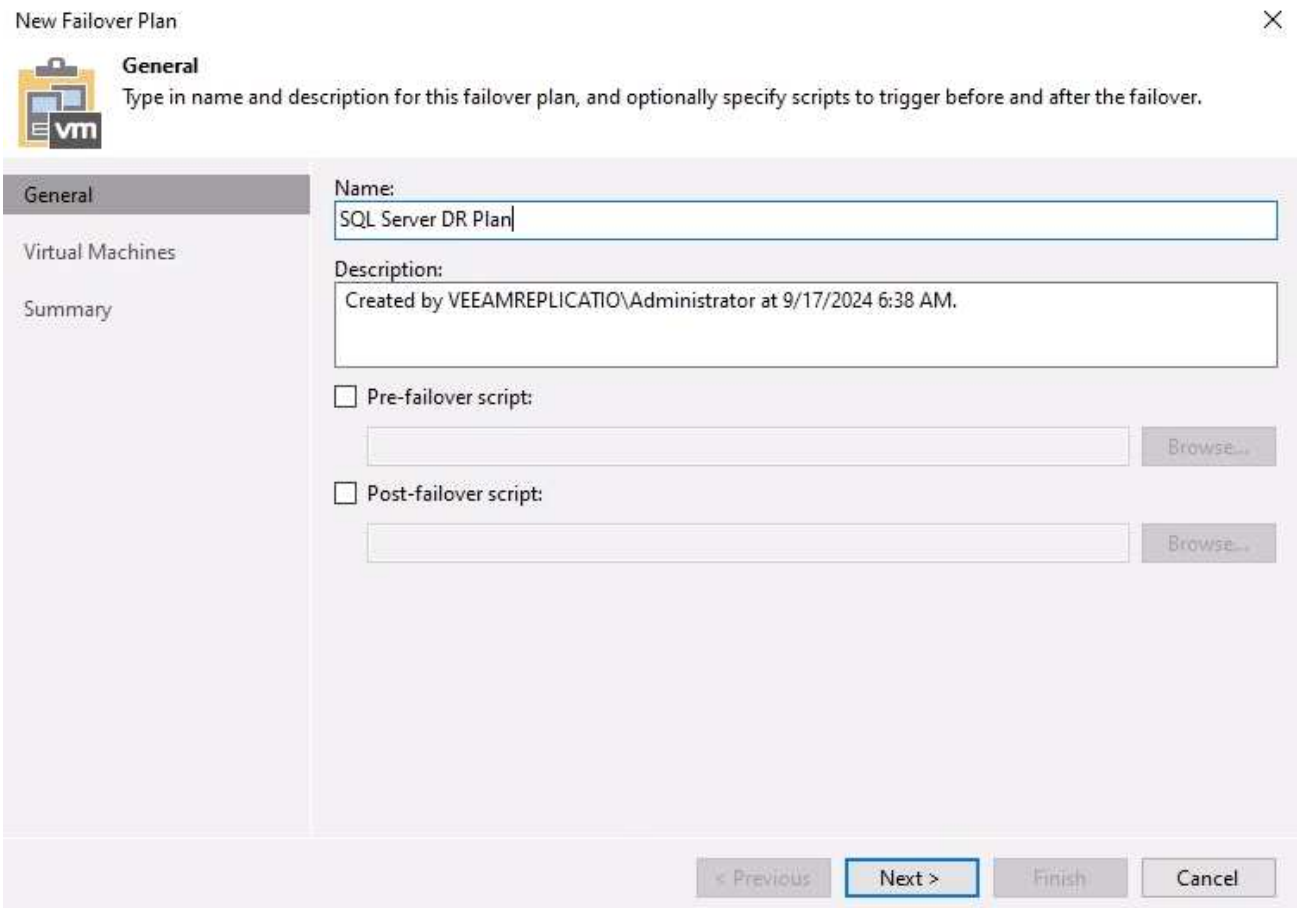
Während des Failover-Prozesses werden die Quell-VMs nicht ausgeschaltet.

Führen Sie die folgenden Schritte aus, um den **Failover-Plan** zu erstellen:

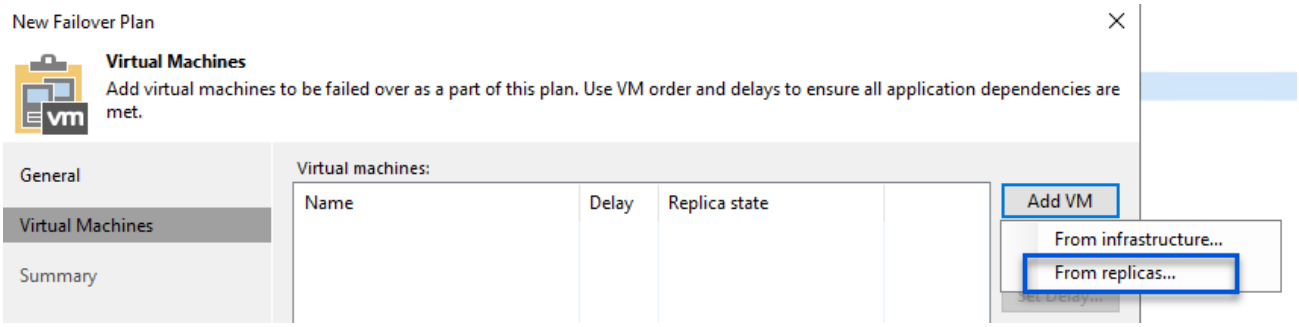
1. Klicken Sie in der **Startseite**-Ansicht im Abschnitt **Wiederherstellen** auf die Schaltfläche **Failover-Plan**. Wählen Sie im Dropdown-Menü **VMware vSphere…** aus.

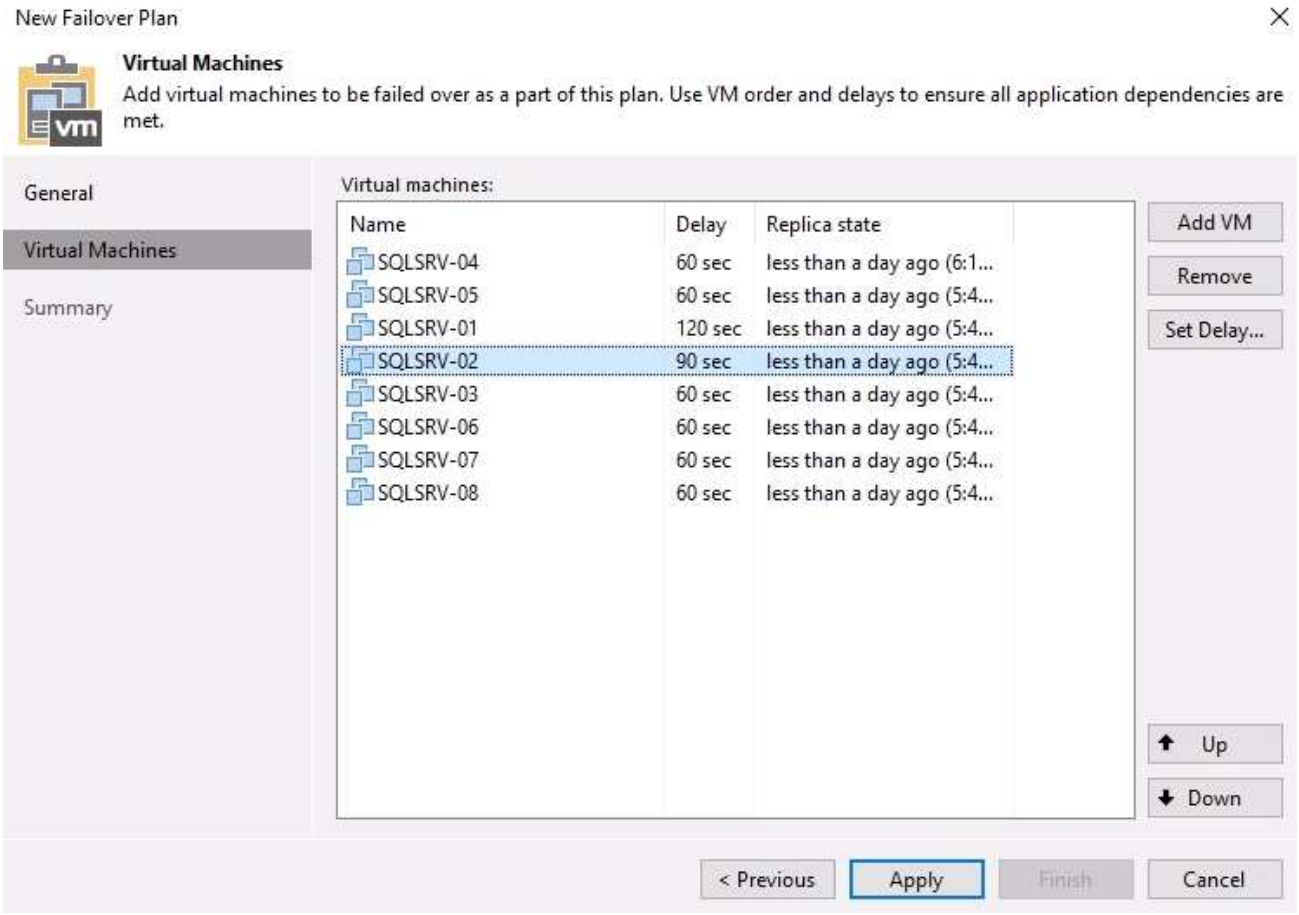


2. Geben Sie auf der Seite **Allgemein** des Assistenten **Neuer Failoverplan** einen Namen und eine Beschreibung für den Plan ein. Bei Bedarf können Skripte vor und nach dem Failover hinzugefügt werden. Führen Sie beispielsweise ein Skript aus, um VMs herunterzufahren, bevor Sie die replizierten VMs starten.



3. Klicken Sie auf der Seite **Virtuelle Maschinen** auf die Schaltfläche **VM hinzufügen** und wählen Sie **Aus Replikaten…**. Wählen Sie die VMs aus, die Teil des Failover-Plans sein sollen, und ändern Sie dann die VM-Startreihenfolge und alle erforderlichen Startverzögerungen, um Anwendungsabhängigkeiten zu erfüllen.





Klicken Sie auf **Übernehmen**, um fortzufahren.

4. Überprüfen Sie abschließend alle Failover-Planeinstellungen und klicken Sie auf **Fertig**, um den Failover-Plan zu erstellen.

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

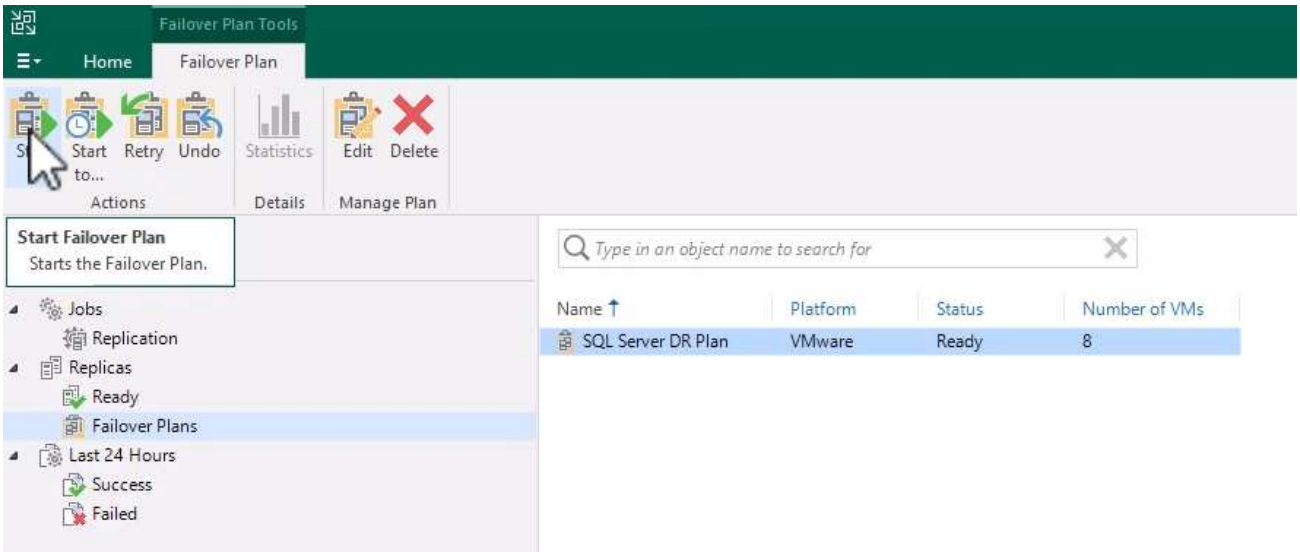
▼ Ausführen des Failoverplans

Während des Failovers wechselt die Quell-VM am Produktionsstandort zu ihrer Replik am Notfallwiederherstellungsstandort. Als Teil des Prozesses stellt Veeam Backup & Replication die VM-Replik am erforderlichen Wiederherstellungspunkt wieder her und überträgt alle E/A-Aktivitäten von der Quell-VM auf ihre Replik. Replikate dienen nicht nur für tatsächliche Katastrophen, sondern auch zur Simulation von DR-Übungen. Bei der Failover-Simulation läuft die Quell-VM weiter. Nach Abschluss der erforderlichen Tests kann das Failover rückgängig gemacht und der Betrieb wieder normalisiert werden.

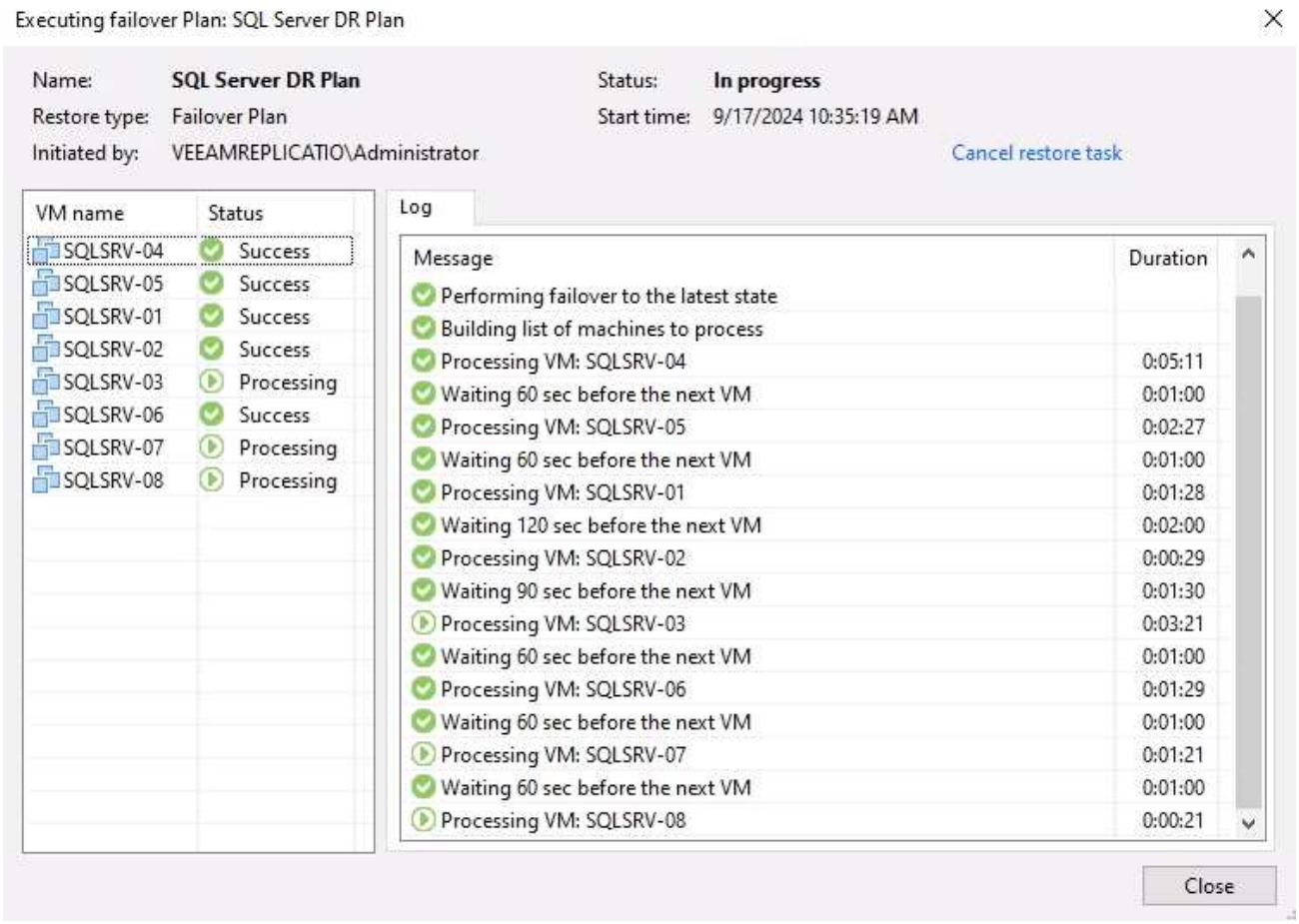
Stellen Sie sicher, dass eine Netzwerksegmentierung vorhanden ist, um IP-Konflikte während des Failovers zu vermeiden.

Führen Sie die folgenden Schritte aus, um den Failover-Plan zu starten:

1. Um zu beginnen, klicken Sie in der **Startseite**-Ansicht im linken Menü auf **Replikate > Failover-Pläne** und dann auf die Schaltfläche **Start**. Alternativ kann die Schaltfläche **Starten mit…** verwendet werden, um ein Failover zu einem vorherigen Wiederherstellungspunkt durchzuführen.



2. Überwachen Sie den Fortschritt des Failovers im Fenster **Failover-Plan wird ausgeführt**.



Veeam Backup & Replication stoppt alle Replikationsaktivitäten für die Quell-VM, bis deren Replikat wieder in den Zustand „Bereit“ versetzt wird.

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

▼ **Failback zum Produktionsstandort**

Die Durchführung eines Failovers wird als Zwischenschritt betrachtet und muss je nach Bedarf abgeschlossen werden. Zu den Optionen gehören die folgenden:

- **Failback zur Produktion** – Kehren Sie zur ursprünglichen VM zurück und synchronisieren Sie alle während der aktiven Phase der Replik vorgenommenen Änderungen zurück zur Quell-VM.

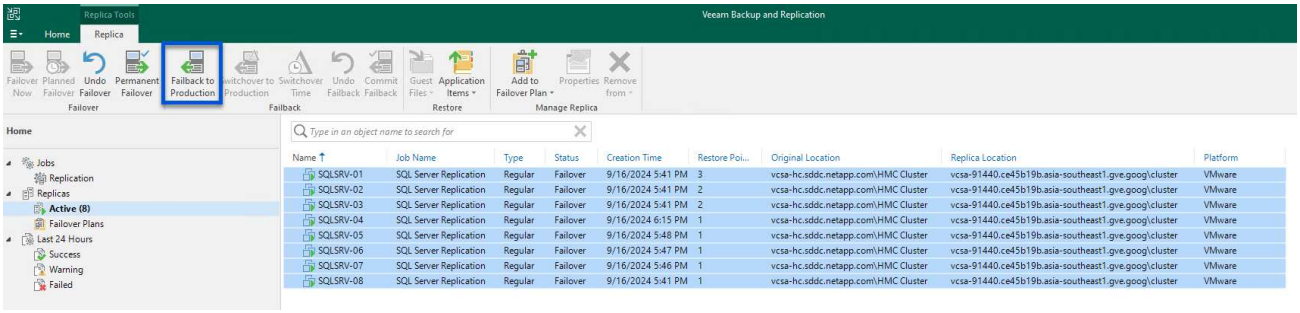
Beim Failback werden Änderungen übertragen, aber nicht sofort angewendet. Wählen Sie **Failback festschreiben**, sobald die Funktionalität der ursprünglichen VM überprüft wurde. Alternativ können Sie **Failback rückgängig machen** wählen, um zur VM-Replik zurückzukehren, wenn die ursprüngliche VM ein unerwartetes Verhalten zeigt.

- **Failover rückgängig machen** – Kehren Sie zur ursprünglichen VM zurück und verwerfen Sie alle während der Betriebszeit an der VM-Replik vorgenommenen Änderungen.
- **Permanentes Failover** – Wechseln Sie dauerhaft von der ursprünglichen VM zu ihrer Replik und richten Sie die Replik als neue primäre VM für laufende Vorgänge ein.

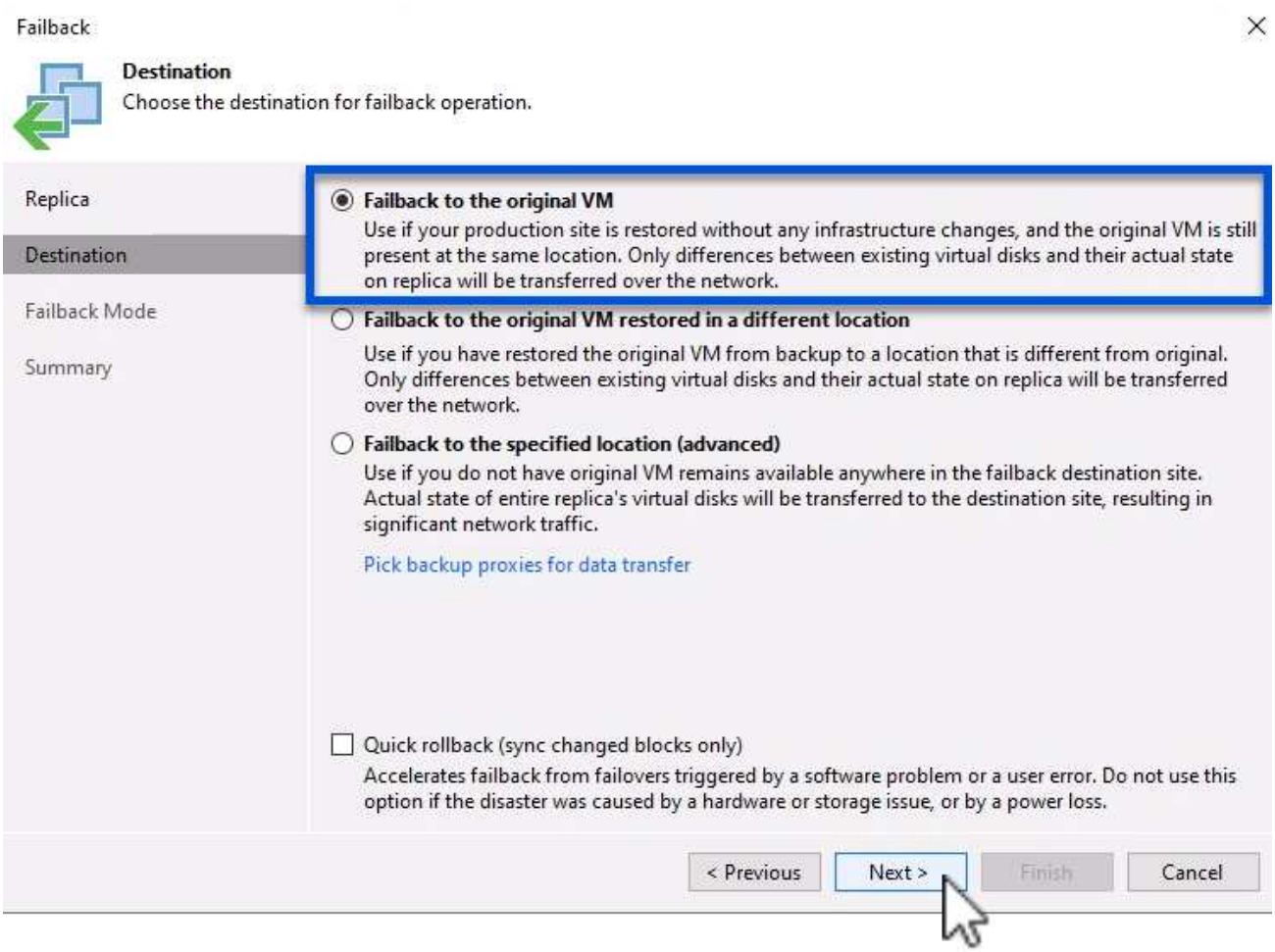
In diesem Szenario wurde die Option „Failback zur Produktion“ ausgewählt.

Führen Sie die folgenden Schritte aus, um ein Failback zur Produktionssite durchzuführen:

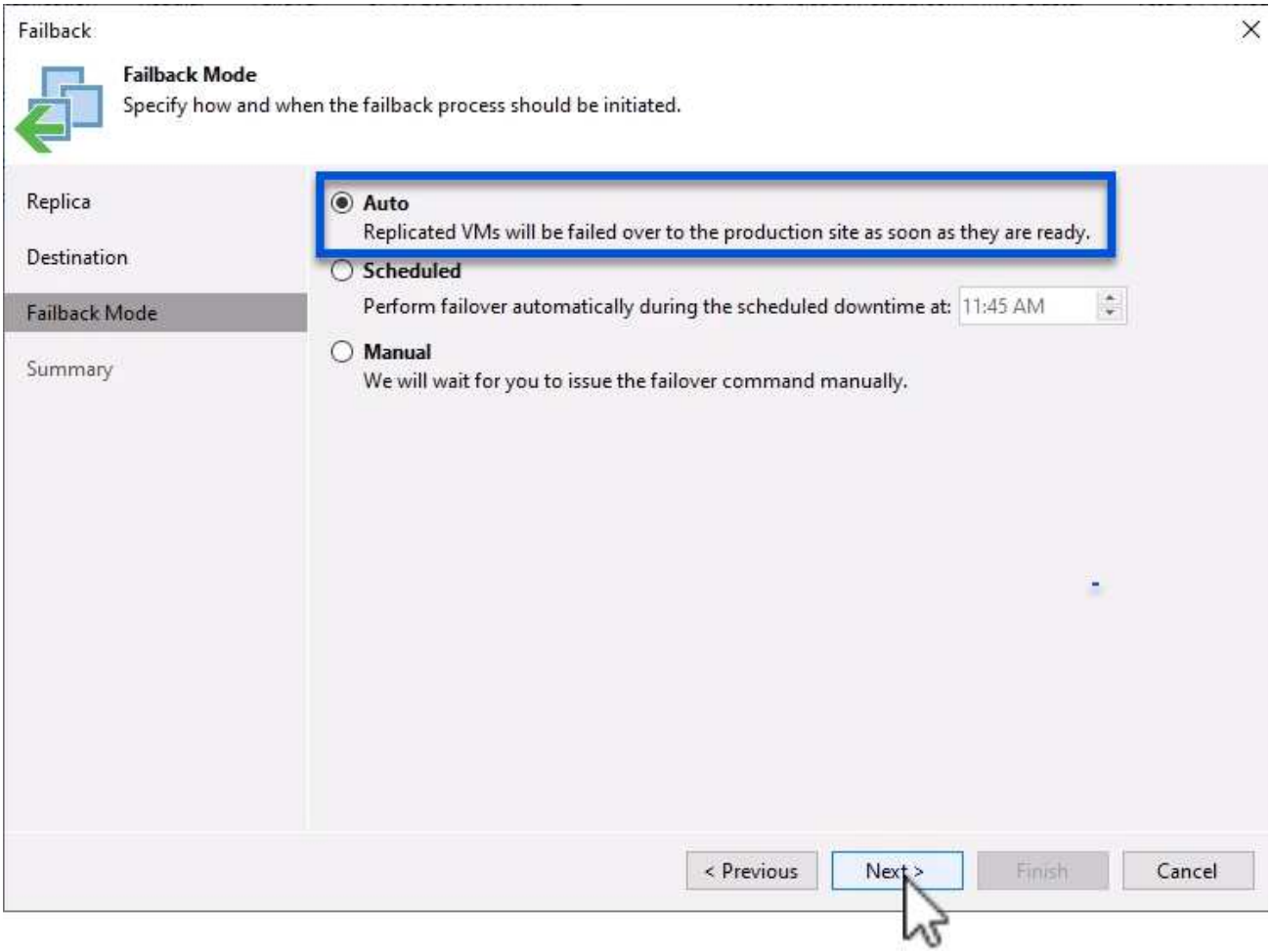
1. Klicken Sie in der **Startseite**-Ansicht im linken Menü auf **Replikate > Aktiv**. Wählen Sie die einzubindenden VMs aus und klicken Sie im oberen Menü auf die Schaltfläche **Failback zur Produktion**.



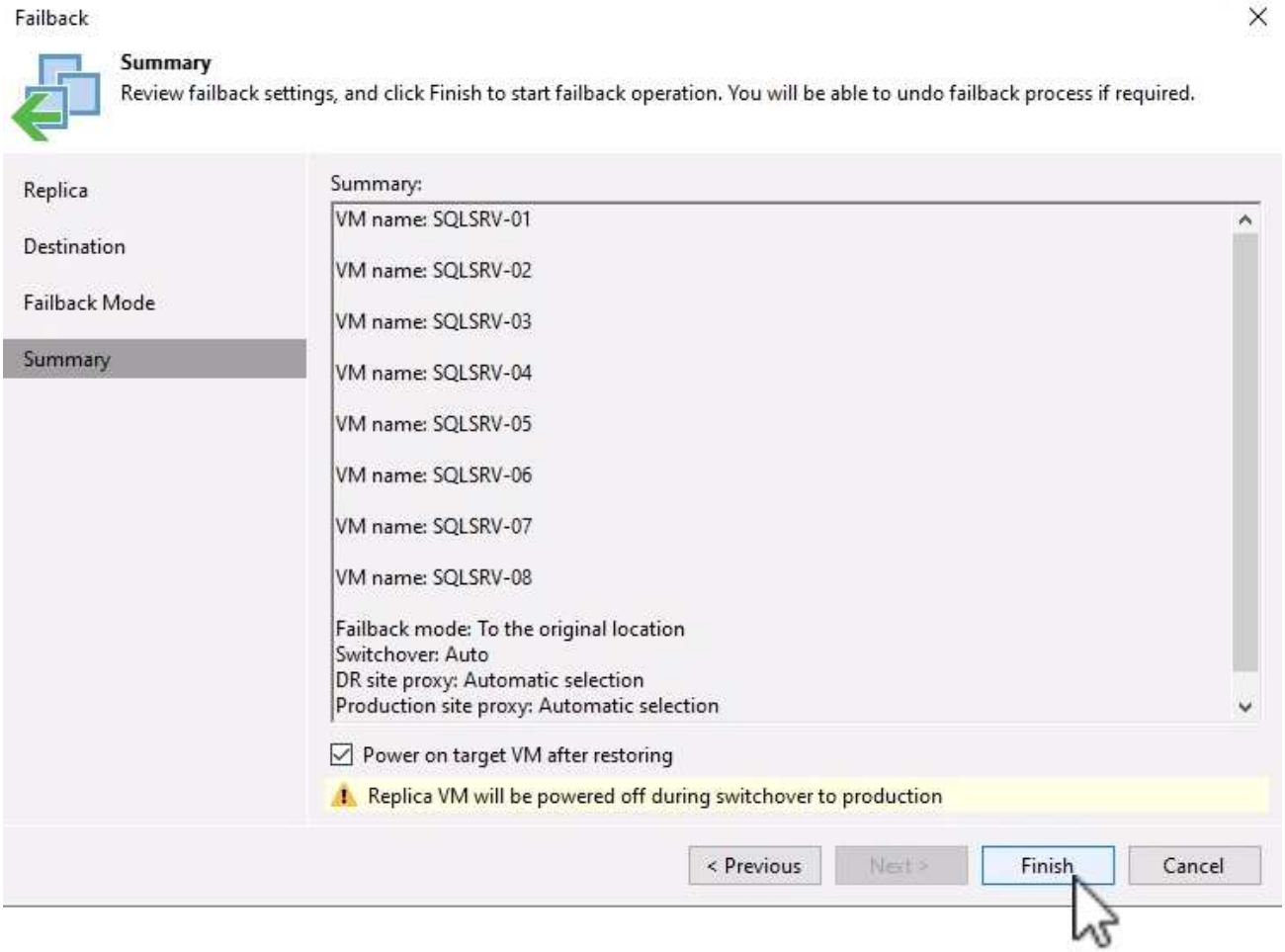
2. Wählen Sie auf der Seite **Replikat** des **Failback**-Assistenten die Replikate aus, die in den Failback-Job einbezogen werden sollen.
3. Wählen Sie auf der Seite **Ziel** die Option **Failback zur ursprünglichen VM** und klicken Sie auf **Weiter**, um fortzufahren.



4. Wählen Sie auf der Seite **Failback-Modus Auto** aus, um das Failback so schnell wie möglich zu starten.

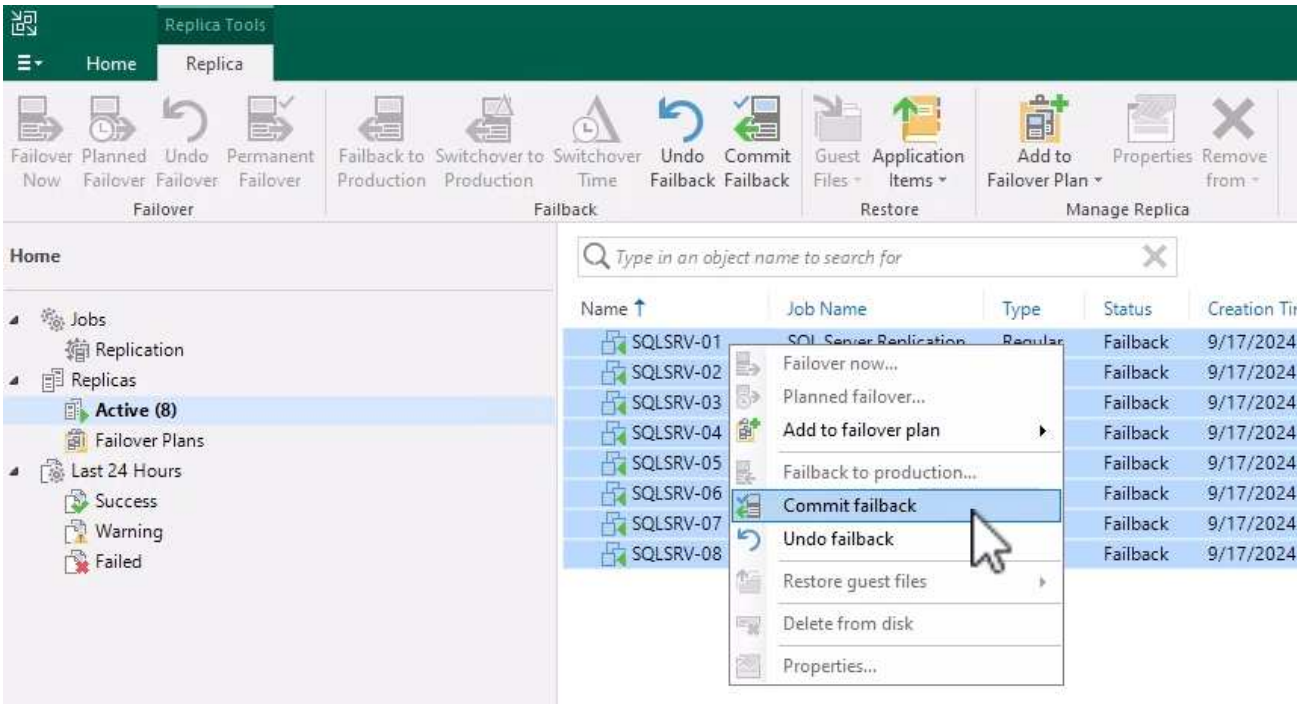


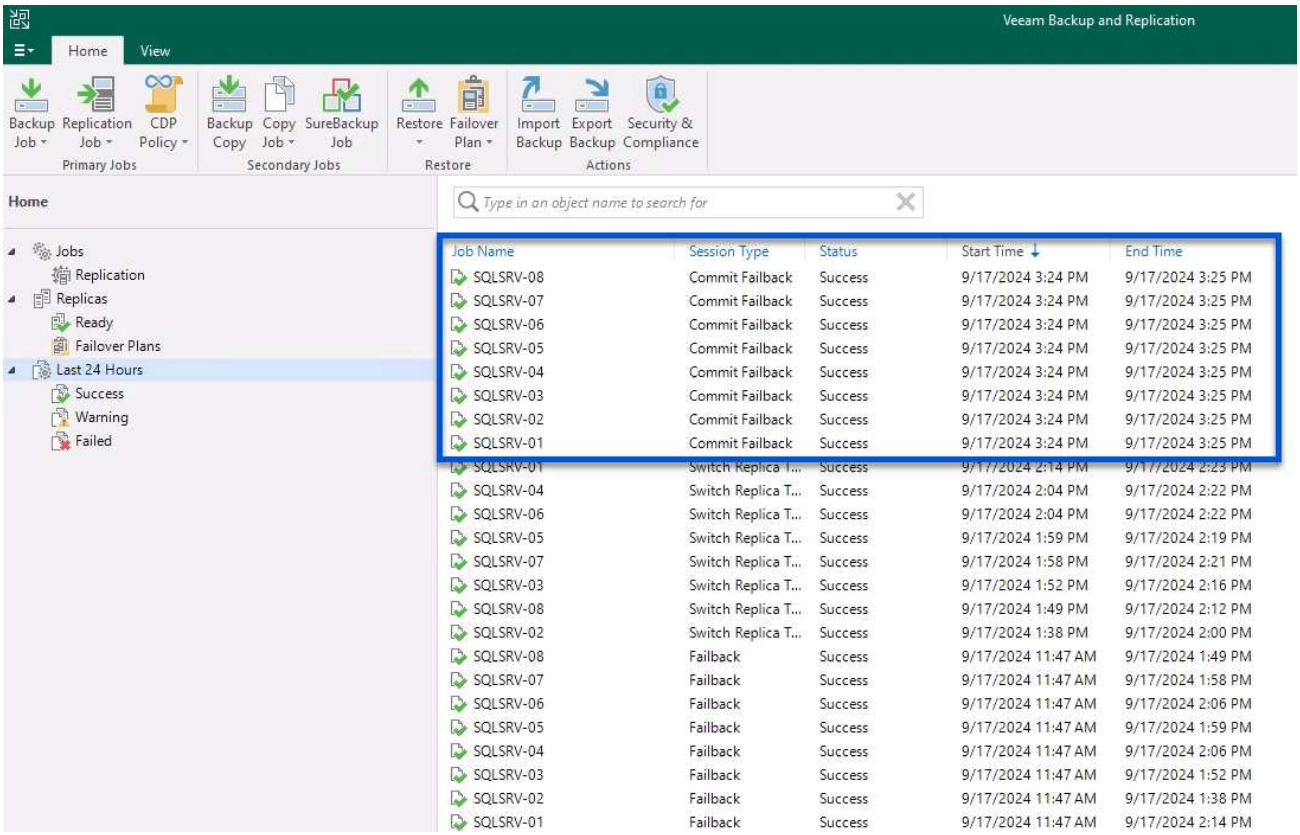
5. Wählen Sie auf der Seite **Zusammenfassung** aus, ob die **Ziel-VM nach der Wiederherstellung eingeschaltet** werden soll, und klicken Sie dann auf „Fertig stellen“, um den Failback-Job zu starten.



Das Failback-Commit schließt den Failback-Vorgang ab und bestätigt die erfolgreiche Integration der Änderungen in die Produktions-VM. Nach dem Commit nimmt Veeam Backup & Replication die regulären Replikationsaktivitäten für die wiederhergestellte Produktions-VM wieder auf. Dadurch ändert sich der Status der wiederhergestellten Replik von *Failback* in *Bereit*.

1. Um ein Failback durchzuführen, navigieren Sie zu **Replikate > Aktiv**, wählen Sie die VMs aus, für die ein Failback durchgeführt werden soll, klicken Sie mit der rechten Maustaste und wählen Sie **Failback durchführen**.





Nach einem erfolgreichen Failback zur Produktion werden alle VMs wieder am ursprünglichen Produktionsstandort wiederhergestellt.

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

Abschluss

Die Datenspeicherfunktionalität von Google Cloud NetApp Volumes ermöglicht Veeam und anderen validierten Tools von Drittanbietern die Bereitstellung kostengünstiger Disaster Recovery-Lösungen (DR). Durch die Verwendung von Pilot Light-Clustern anstelle großer, dedizierter Cluster für VM-Replikate können Unternehmen ihre Kosten erheblich senken. Dieser Ansatz ermöglicht maßgeschneiderte DR-Strategien, die vorhandene interne Backup-Lösungen für die Cloud-basierte Notfallwiederherstellung nutzen und so den Bedarf an zusätzlichen Rechenzentren vor Ort überflüssig machen. Im Katastrophenfall kann das Failover mit einem einzigen Klick eingeleitet oder so konfiguriert werden, dass es automatisch erfolgt, wodurch die Geschäftskontinuität mit minimalen Ausfallzeiten gewährleistet wird.

Um mehr über diesen Vorgang zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

Migrieren Sie Workloads auf GCP/GCVE

Migrieren Sie Workloads mit VMware HCX zum Google Cloud NetApp Volumes -Datenspeicher auf Google Cloud VMware Engine – Kurzanleitung

Einer der häufigsten Anwendungsfälle für den Google Cloud VMware Engine- und Cloud Volume Service-Datenspeicher ist die Migration von VMware-Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmechanismen zum Verschieben lokaler virtueller Maschinen (VMs) und ihrer Daten in NFS-Datenspeicher des Cloud Volume Service.

Übersicht: Migrieren virtueller Maschinen mit VMware HCX, Google Cloud NetApp Volumes Datenspeichern und Google Cloud VMware Engine (GCVE)

VMware HCX ist in erster Linie eine Migrationsplattform, die die Anwendungsmigration, die Neuverteilung der Arbeitslast und sogar die Geschäftskontinuität über Clouds hinweg vereinfachen soll. Es ist Teil der Google Cloud VMware Engine Private Cloud und bietet zahlreiche Möglichkeiten zur Migration von Workloads und kann für Disaster Recovery (DR)-Vorgänge verwendet werden.

Dieses Dokument enthält eine Schritt-für-Schritt-Anleitung zum Bereitstellen des Cloud Volume Service-Datenspeichers, gefolgt vom Herunterladen, Bereitstellen und Konfigurieren von VMware HCX, einschließlich aller Hauptkomponenten vor Ort und auf der Google Cloud VMware Engine-Seite, einschließlich Interconnect, Netzwerkerweiterung und WAN-Optimierung zum Aktivieren verschiedener VM-Migrationsmechanismen.

> ⓘ VMware HCX funktioniert mit jedem Datenspeichertyp, da die Migration auf VM-Ebene erfolgt. Daher ist dieses Dokument für bestehende NetApp -Kunden und Nicht- NetApp -Kunden relevant, die Cloud Volume Service mit Google Cloud VMware Engine für eine kostengünstige VMware-Cloud-Bereitstellung bereitstellen möchten.

▼ **Schritte auf hoher Ebene**

Diese Liste enthält die wichtigsten Schritte, die zum Koppeln und Migrieren der VMs vom lokalen HCX Connector zum HCX Cloud Manager auf der Google Cloud VMware Engine-Seite erforderlich sind:

1. Bereiten Sie HCX über das Google VMware Engine-Portal vor.
2. Laden Sie das HCX Connector Open Virtualization Appliance (OVA)-Installationsprogramm herunter und stellen Sie es auf dem lokalen VMware vCenter Server bereit.

3. Aktivieren Sie HCX mit dem Lizenzschlüssel.
4. Koppeln Sie den lokalen VMware HCX Connector mit Google Cloud VMware Engine HCX Cloud Manager.
5. Konfigurieren Sie das Netzwerkprofil, das Computeprofil und das Service Mesh.
6. (Optional) Führen Sie eine Netzwerkerweiterung durch, um eine erneute IP-Zuweisung während der Migration zu vermeiden.
7. Überprüfen Sie den Gerätestatus und stellen Sie sicher, dass eine Migration möglich ist.
8. Migrieren Sie die VM-Workloads.

▼ Voraussetzungen

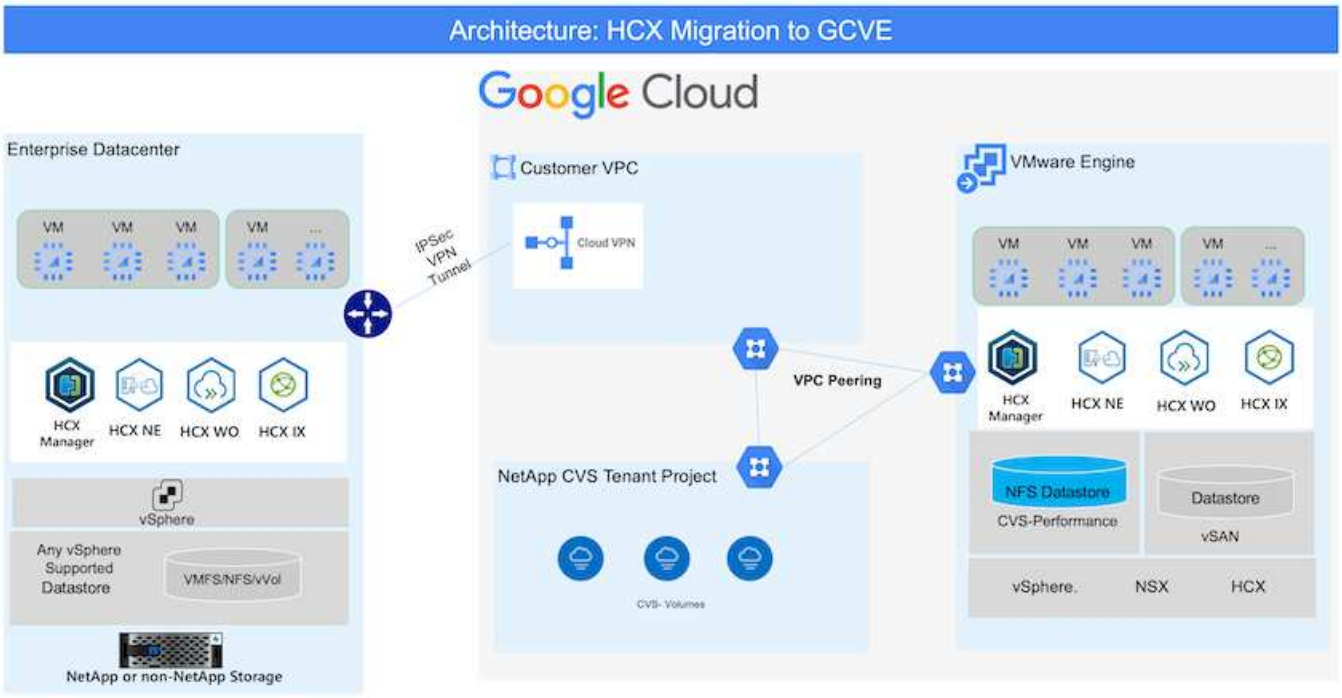
Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie hier "Link" . Nachdem die Voraussetzungen, einschließlich der Konnektivität, erfüllt sind, laden Sie den HCX-Lizenzschlüssel vom Google Cloud VMware Engine-Portal herunter. Nachdem das OVA-Installationsprogramm heruntergeladen wurde, fahren Sie mit dem Installationsvorgang wie unten beschrieben fort.

> ⓘ HCX Advanced ist die Standardoption und die VMware HCX Enterprise Edition ist auch über ein Support-Ticket verfügbar und wird ohne zusätzliche Kosten unterstützt. Verweisen "dieser Link"

- Verwenden Sie ein vorhandenes Google Cloud VMware Engine softwaredefiniertes Rechenzentrum (SDDC) oder erstellen Sie eine private Cloud, indem Sie dies verwenden"NetApp Link" oder das "Google-Link" .
- Die Migration von VMs und zugehörigen Daten aus dem lokalen VMware vSphere-fähigen Rechenzentrum erfordert eine Netzwerkkonnektivität vom Rechenzentrum zur SDDC-Umgebung. Bevor Sie Workloads migrieren, "Richten Sie eine Cloud VPN- oder Cloud Interconnect-Verbindung ein" zwischen der On-Premises-Umgebung und der jeweiligen privaten Cloud.
- Der Netzwerkpfad von der lokalen VMware vCenter Server-Umgebung zur privaten Cloud von 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-Datenverkehr zwischen dem lokalen vCenter Server und SDDC vCenter zulässig.
- Das NFS-Volume des Cloud Volume Service sollte als Datenspeicher in Google Cloud VMware Engine bereitgestellt werden. Befolgen Sie die in diesem Dokument beschriebenen Schritte "Link" um Cloud Volume Service-Datenspeicher an Google Cloud VMware Engines-Hosts anzuhängen.

▼ High-Level-Architektur

Zu Testzwecken wurde die für diese Validierung verwendete Laborumgebung vor Ort über ein Cloud-VPN verbunden, das eine lokale Verbindung zu Google Cloud VPC ermöglicht.



Weitere Informationen zur Verwendung von VMware HCX mit Google finden Sie unter "VMware-Link"

Lösungsbereitstellung

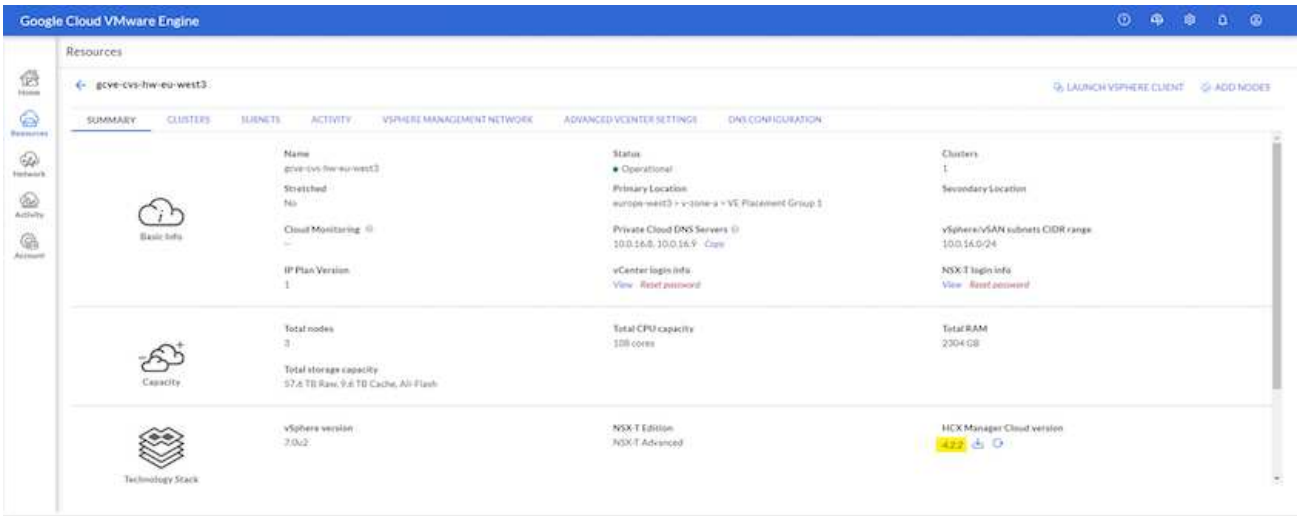
Befolgen Sie die Schritte, um die Bereitstellung dieser Lösung abzuschließen:

▼ **Schritt 1: HCX über das Google VMware Engine Portal vorbereiten**

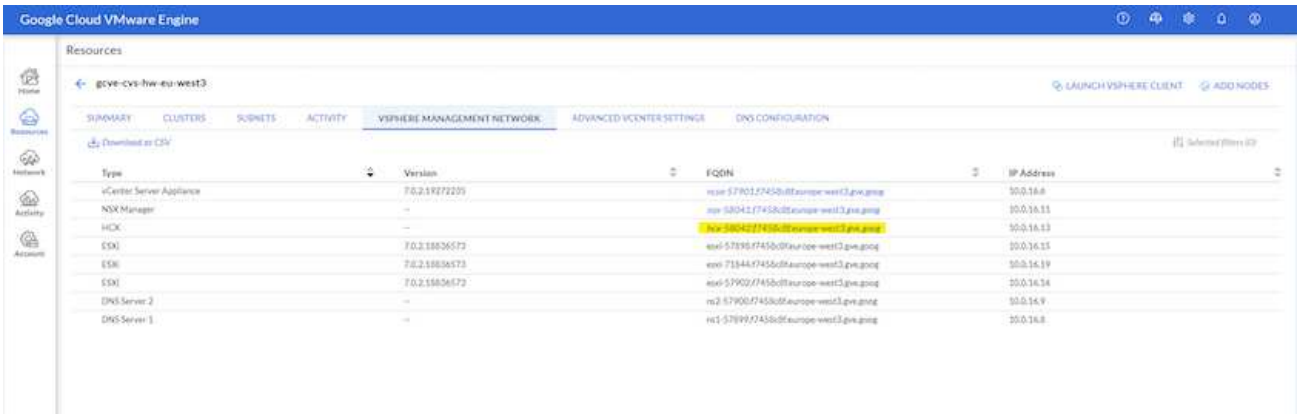
Die HCX Cloud Manager-Komponente wird automatisch installiert, wenn Sie eine private Cloud mit VMware Engine bereitstellen. Führen Sie zur Vorbereitung der Site-Kopplung die folgenden Schritte aus:

1. Melden Sie sich beim Google VMware Engine Portal an und melden Sie sich beim HCX Cloud Manager an.

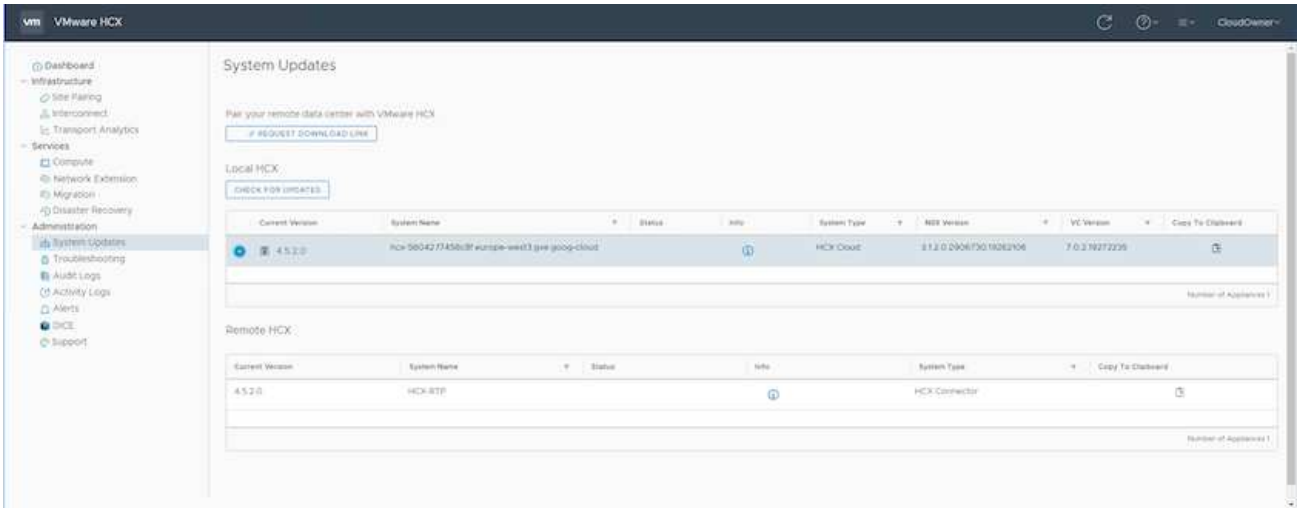
   Sie können sich bei der HCX-Konsole anmelden, indem Sie entweder auf den Link zur HCX-Version klicken



   oder klicken Sie auf der Registerkarte „vSphere Management Network“ auf HCX FQDN.



2. Gehen Sie im HCX Cloud Manager zu **Administration > Systemupdates**.
3. Klicken Sie auf **Download-Link anfordern** und laden Sie die OVA-Datei herunter.



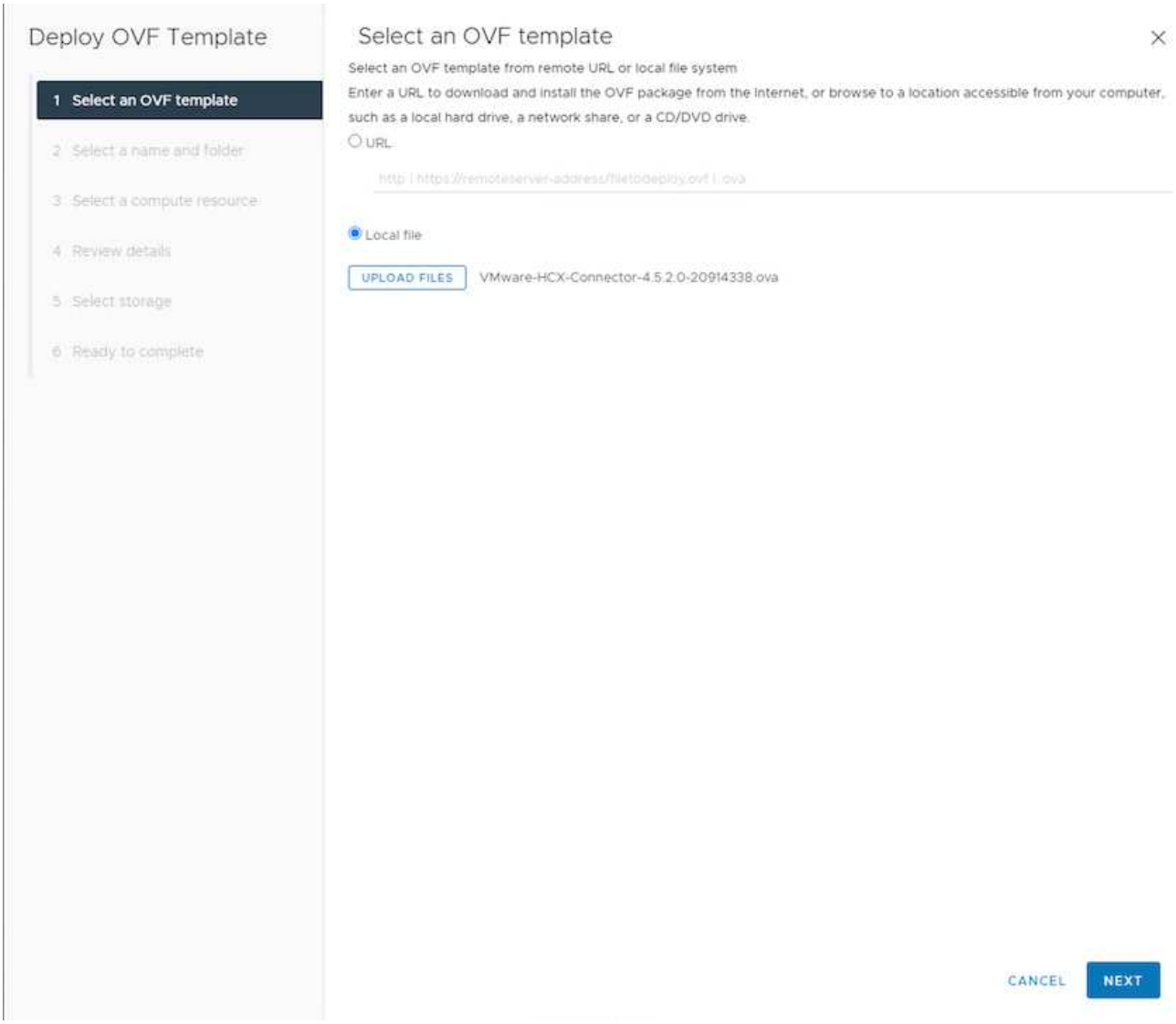
4. Aktualisieren Sie HCX Cloud Manager auf die neueste verfügbare Version über die HCX Cloud Manager-Benutzeroberfläche.

▼ **Schritt 2: Bereitstellen der OVA-Installationsdatei im lokalen vCenter Server**

Damit der lokale Connector eine Verbindung zum HCX Manager in Google Cloud VMware Engine herstellen kann, stellen Sie sicher, dass die entsprechenden Firewall-Ports in der lokalen Umgebung geöffnet sind.

Führen Sie die folgenden Schritte aus, um HCX Connector herunterzuladen und auf dem lokalen vCenter Server zu installieren:

1. Laden Sie die OVAs wie im vorherigen Schritt beschrieben von der HCX-Konsole auf Google Cloud VMware Engine herunter.
2. Nachdem die OVA heruntergeladen wurde, stellen Sie sie mithilfe der Option **OVF-Vorlage bereitstellen** in der lokalen VMware vSphere-Umgebung bereit.



3. Geben Sie alle erforderlichen Informationen für die OVA-Bereitstellung ein, klicken Sie auf **Weiter** und dann auf **Fertig**, um die OVA des VMware HCX-Connectors bereitzustellen.

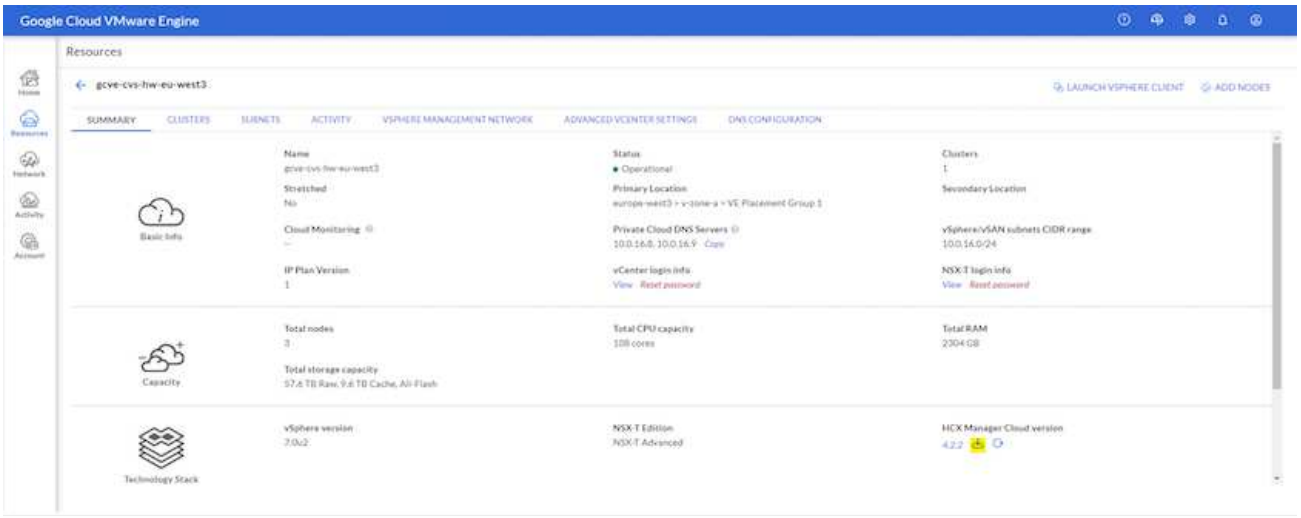
   Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "Google HCX-Dokumentation" .

▼ **Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren**

Nachdem Sie die VMware HCX Connector OVA vor Ort bereitgestellt und die Appliance gestartet haben, führen Sie die folgenden Schritte aus, um 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 aus und **klicken Sie unter HCX Manager Cloud-Version** auf das Download-Symbol.



Öffnen Sie die heruntergeladene Datei und kopieren Sie die Lizenzschlüsselzeichenfolge.

2. Melden Sie sich beim lokalen VMware HCX Manager an unter "`https://hcxmanagerIP:9443`" mit Administratoranmeldeinformationen.

> Verwenden Sie die hcxmanagerIP und das Kennwort, die während der OVA-Bereitstellung definiert wurden.

3. Geben Sie in der Lizenzierung den aus Schritt 3 kopierten Schlüssel ein und klicken Sie auf **Aktivieren**.

> Der lokale HCX-Connector sollte über Internetzugang verfügen.

4. Geben Sie unter **Rechenzentrumsstandort** den nächstgelegenen Standort für die lokale Installation des VMware HCX Manager an. Klicken Sie auf **Weiter**.
5. Aktualisieren Sie unter **Systemname** den Namen und klicken Sie auf **Weiter**.
6. Klicken Sie auf **Ja, fortfahren**.
7. Geben Sie unter **Verbinden Sie Ihr vCenter** den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des vCenter-Servers und die entsprechenden Anmeldeinformationen ein und klicken Sie auf **Weiter**.

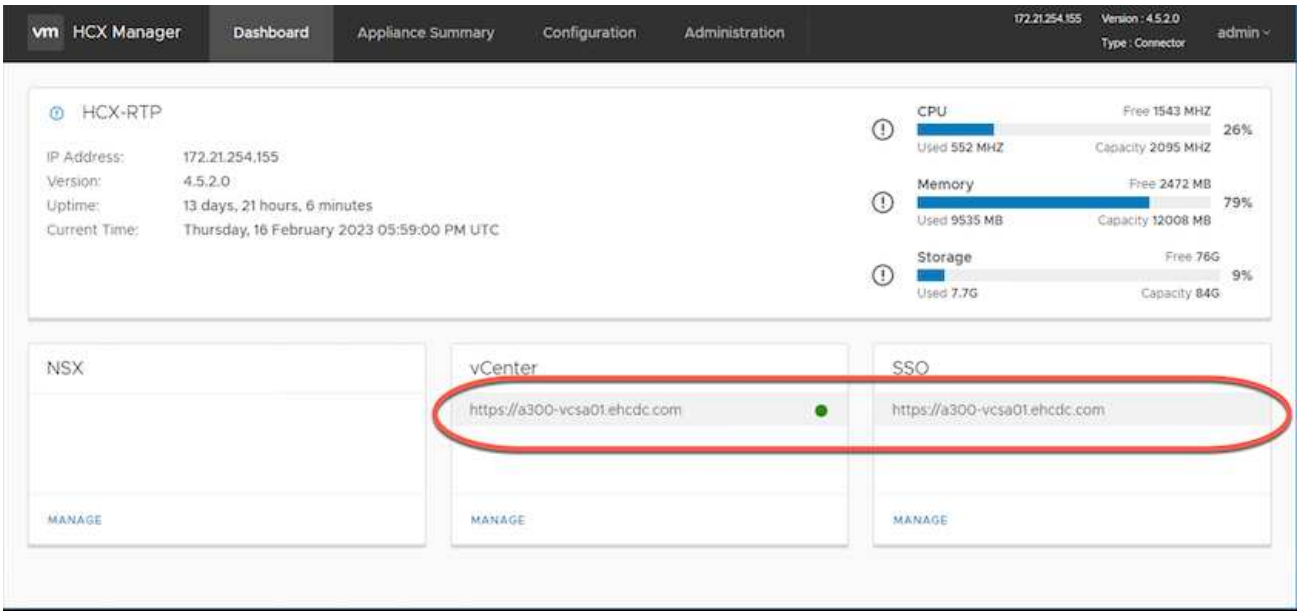
> Verwenden Sie den FQDN, um spätere Verbindungsprobleme zu vermeiden.

8. Geben Sie unter **SSO/PSC konfigurieren** den FQDN oder die IP-Adresse des Platform Services Controllers (PSC) ein und klicken Sie auf **Weiter**.

> Geben Sie für Embedded PSC den FQDN oder die IP-Adresse des VMware vCenter-Servers 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 denen auf der vorherigen Seite übereinstimmen sollten.

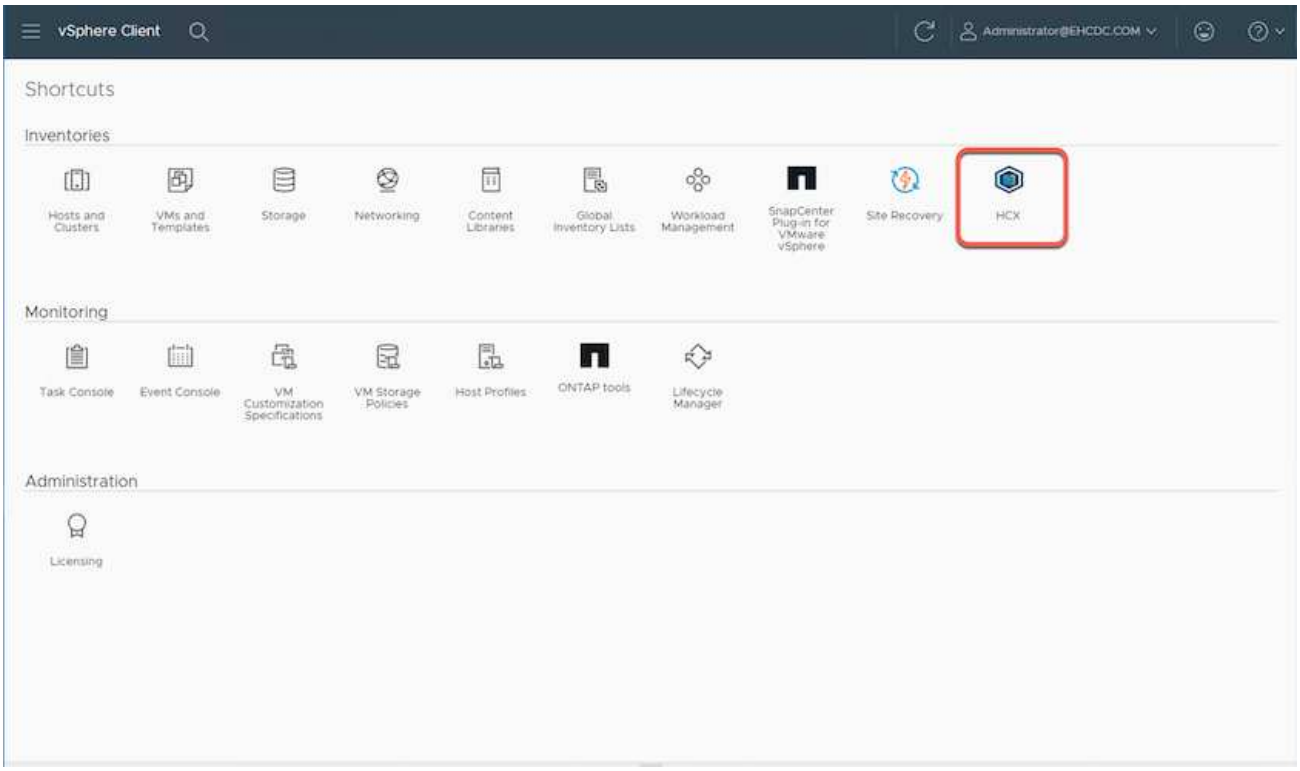
> Dieser Vorgang sollte etwa 10 bis 20 Minuten dauern und das Plug-In sollte dem vCenter Server hinzugefügt werden.



▼ Schritt 4: Koppeln Sie den lokalen VMware HCX Connector mit Google Cloud VMware Engine HCX Cloud Manager

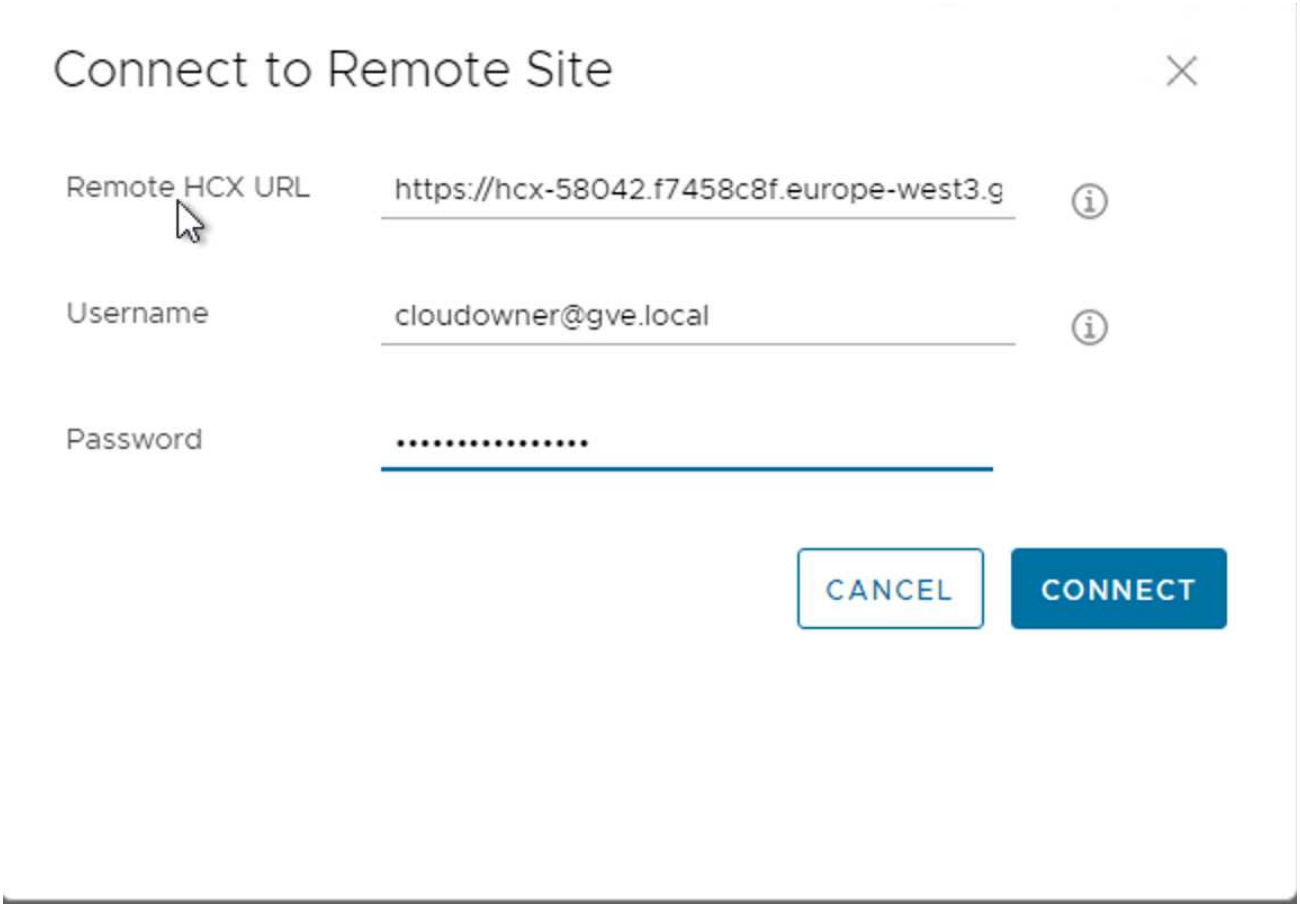
Nachdem HCX Connector im lokalen vCenter bereitgestellt und konfiguriert wurde, stellen Sie durch Hinzufügen der Kopplung eine Verbindung zu Cloud Manager her. Führen Sie die folgenden Schritte aus, um die Site-Kopplung zu konfigurieren:

1. Um ein Site-Paar zwischen der lokalen vCenter-Umgebung und 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-Paarung hinzufügen“*.

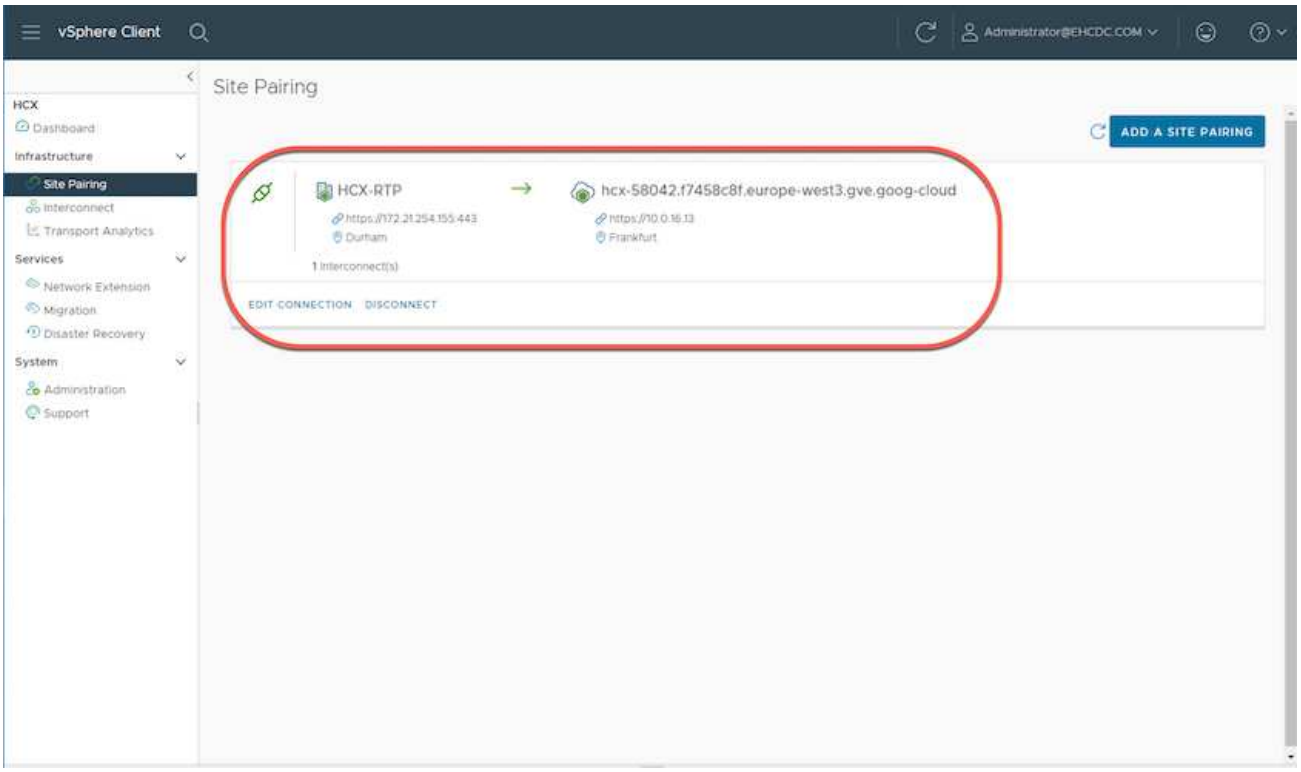
Geben Sie die URL oder IP-Adresse des Google Cloud VMware Engine HCX Cloud Managers und die Anmeldeinformationen für den Benutzer mit Cloud-Owner-Role-Berechtigungen für den Zugriff auf die private Cloud ein.



3. Klicken Sie auf **Verbinden**.

VMware HCX Connector muss in der Lage sein, über Port 443 an die IP-Adresse des HCX Cloud Managers weiterzuleiten.

4. Nachdem die Kopplung erstellt wurde, ist die neu konfigurierte Site-Kopplung auf dem HCX-Dashboard verfügbar.

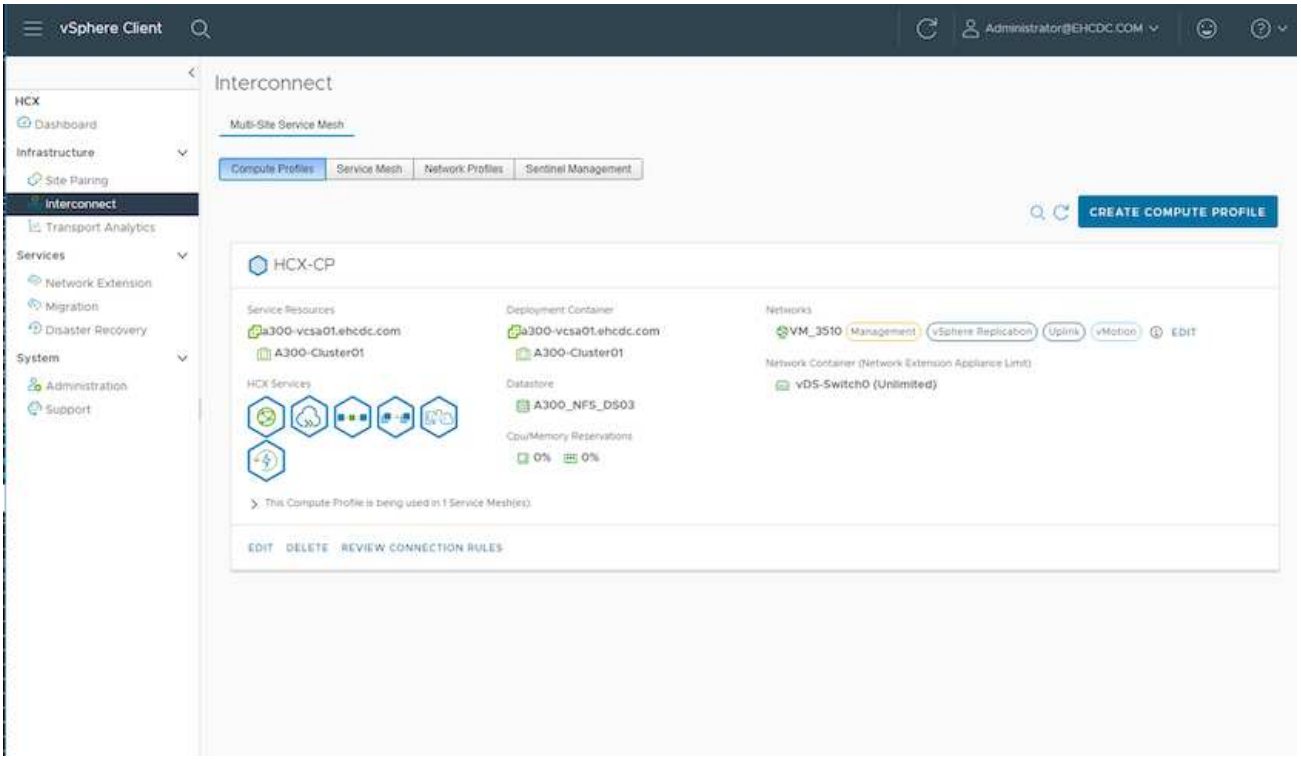


▼ **Schritt 5: Konfigurieren Sie das Netzwerkprofil, das Compute-Profil und das Service Mesh**

Die VMware HCX Interconnect Service Appliance bietet Replikations- und vMotion-basierte Migrationsfunktionen über das Internet und private Verbindungen zum Zielstandort. Die Verbindung bietet Verschlüsselung, Verkehrstechnik und VM-Mobilität. Führen Sie die folgenden Schritte aus, um eine Interconnect-Dienst-Appliance zu erstellen:

1. Wählen Sie unter „Infrastruktur“ die Option „Interconnect > Multi-Site Service Mesh > Compute-Profile > Compute-Profil erstellen“ aus.

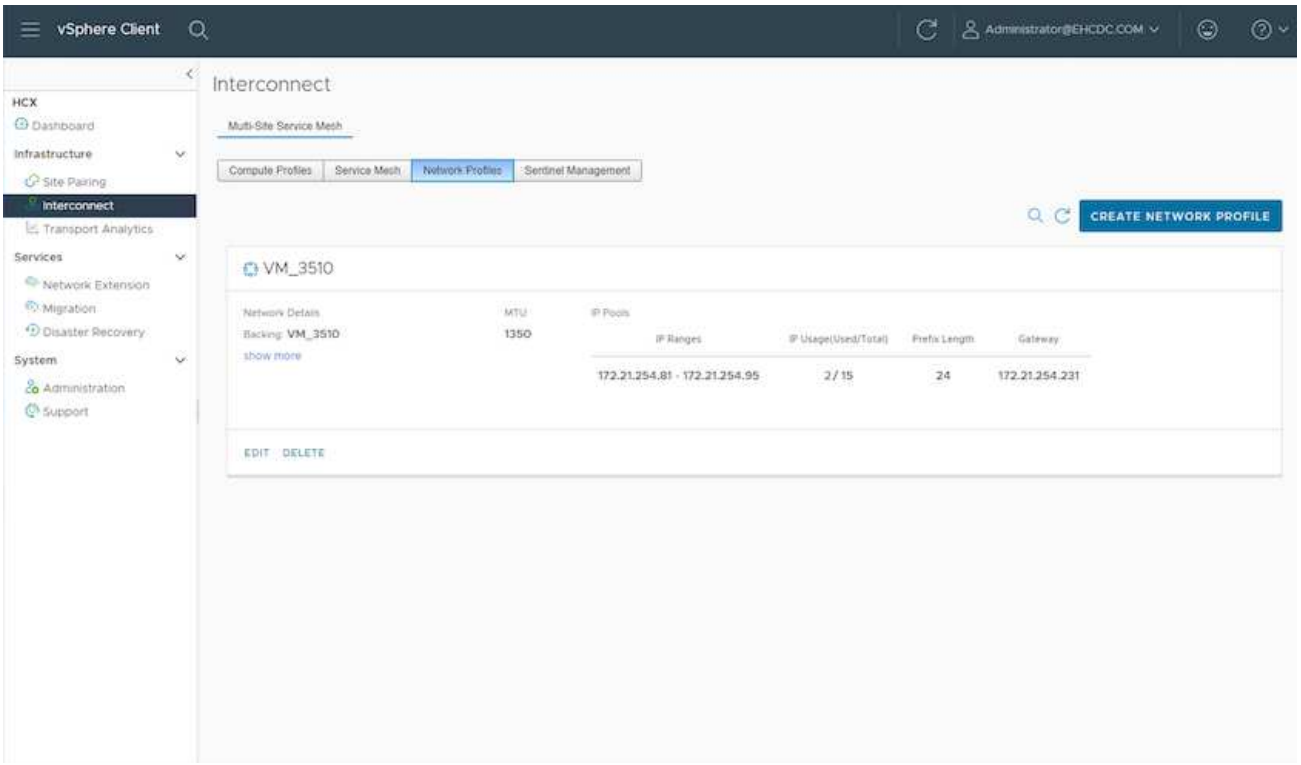
Die Rechenprofile definieren die Bereitstellungsparameter, einschließlich der bereitgestellten Appliances und der Teile des VMware-Rechenzentrums, auf die der HCX-Dienst zugreifen kann.



2. Nachdem das Compute-Profil erstellt wurde, erstellen Sie die Netzwerkprofile, indem Sie **Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen** auswählen.

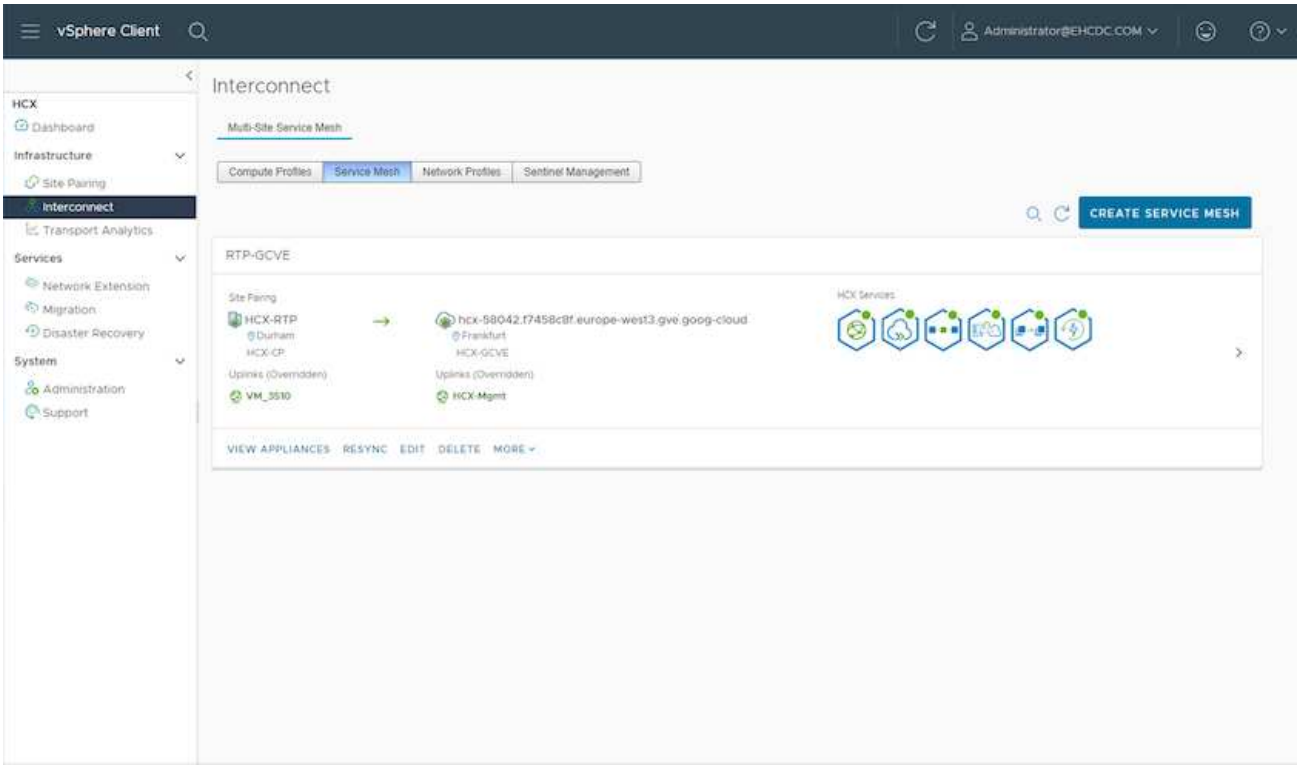
   Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

   Für diesen Schritt sind zwei oder mehr IP-Adressen erforderlich. Diese IP-Adressen werden vom Verwaltungsnetzwerk den Interconnect Appliances zugewiesen.

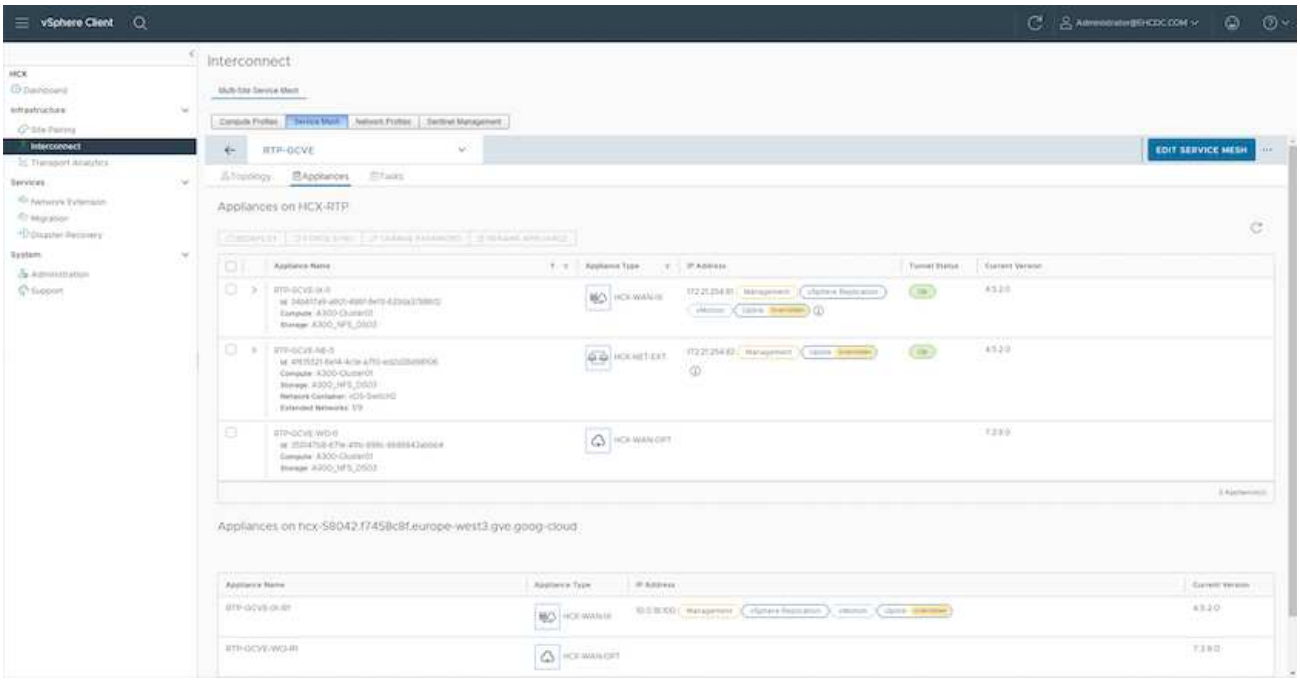


3. Zu diesem Zeitpunkt wurden die Computer- und Netzwerkprofile erfolgreich erstellt.
4. Erstellen Sie das Service Mesh, indem Sie die Registerkarte **Service Mesh** innerhalb der Option **Interconnect** auswählen und die lokalen und GCVE SDDC-Sites auswählen.
5. Das Service Mesh gibt ein lokales und ein Remote-Compute- und Netzwerkprofilpaar an.

> Im Rahmen dieses Prozesses werden die HCX-Geräte sowohl am Quell- als auch am Zielstandort bereitgestellt und automatisch konfiguriert, um ein sicheres Transport-Fabric zu erstellen.



6. Dies ist der letzte Schritt der Konfiguration. Die Bereitstellung sollte etwa 30 Minuten dauern. Nachdem das Service-Mesh konfiguriert wurde, ist die Umgebung mit den erfolgreich erstellten IPsec-Tunneln bereit, um die Workload-VMs zu migrieren.



▼ Schritt 6: Migrieren von Workloads

Workloads können mithilfe verschiedener VMware HCX-Migrationstechnologien bidirektional zwischen lokalen und GCVE-SDDCs migriert werden. VMs können mithilfe mehrerer Migrationstechnologien wie HCX-Massenmigration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (verfügbar mit der HCX Enterprise Edition) und HCX OS Assisted Migration (verfügbar mit der HCX Enterprise Edition) zu und von VMware HCX-aktivierten Einheiten verschoben werden.

Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter "Migrieren von VMware-VMs mithilfe der VMware HCX-Dokumentation" .

Das HCX-IX-Gerät verwendet den Mobility Agent-Dienst, um vMotion-, Cold- und Replication Assisted vMotion (RAV)-Migrationen durchzuführen.

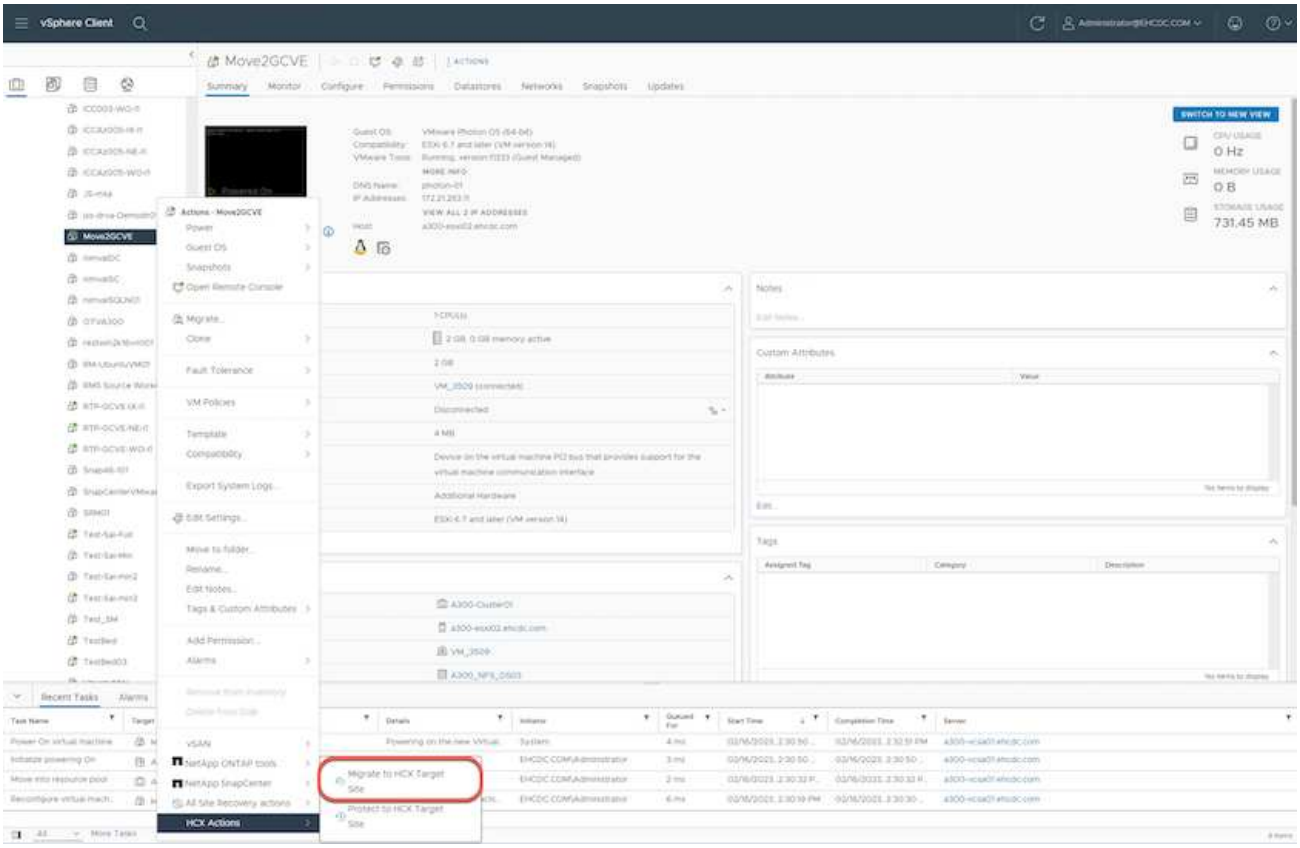
> ⓘ Die HCX-IX-Appliance fügt den Mobility Agent-Dienst als Hostobjekt im vCenter Server hinzu. Die in diesem Objekt angezeigten Prozessor-, Speicher-, Speicher- und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch auf dem physischen Hypervisor dar, auf dem die IX-Appliance gehostet wird.

HCX vMotion

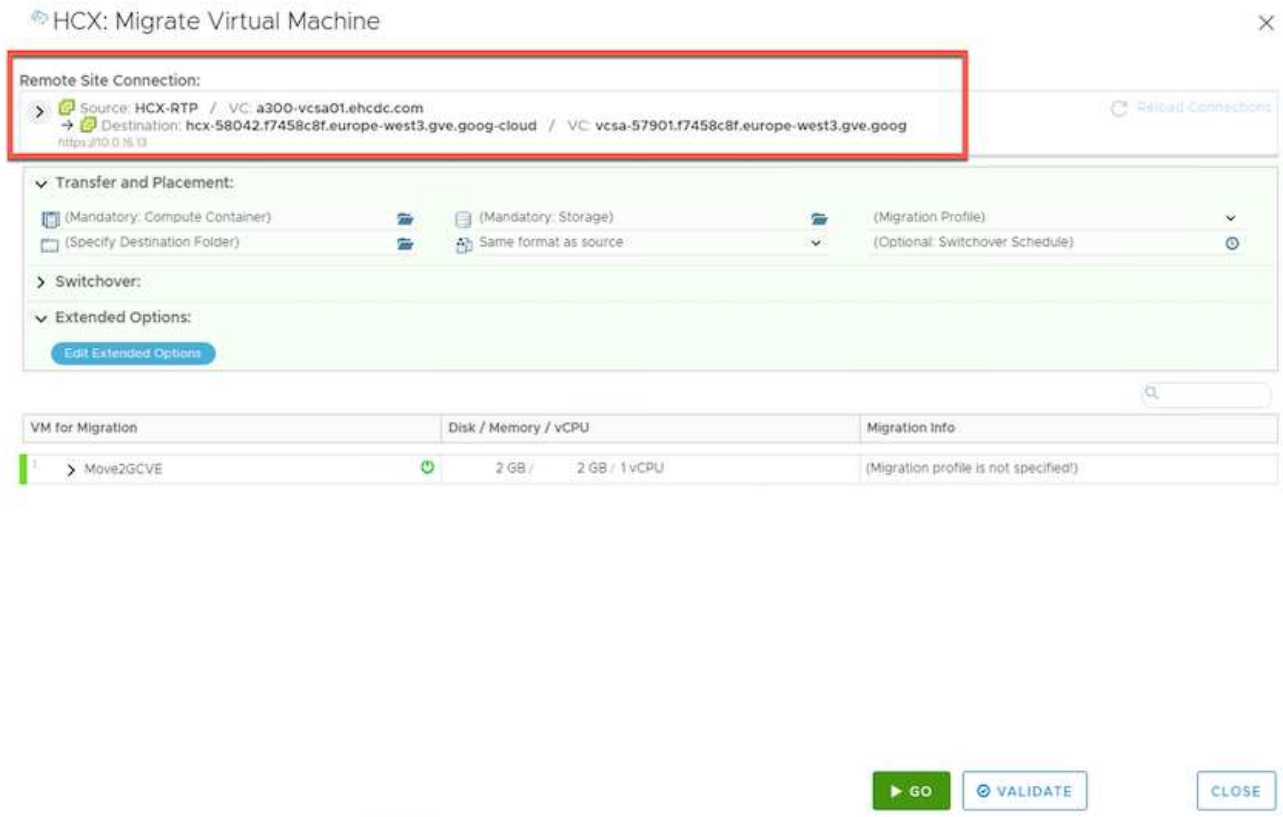
In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie verwendet das VMware vMotion-Protokoll, um eine VM zu GCVE zu migrieren. Die Migrationsoption vMotion wird zum Migrieren des VM-Status jeweils einer einzelnen VM verwendet. Bei dieser Migrationsmethode kommt es zu keiner Dienstunterbrechung.

> ⓘ Die Netzwerkerweiterung sollte vorhanden sein (für die Portgruppe, an die die VM angeschlossen ist), um die VM zu migrieren, ohne dass eine Änderung der IP-Adresse erforderlich ist.

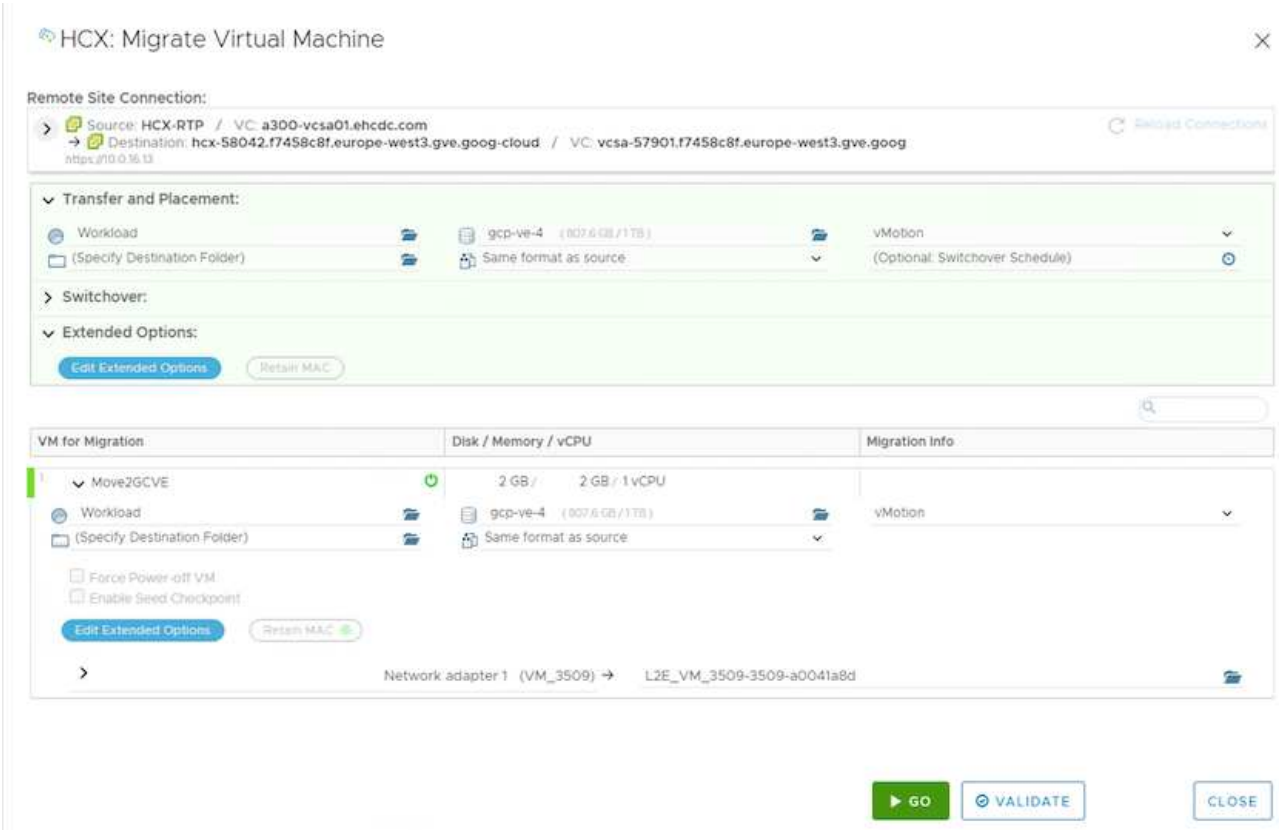
1. Gehen Sie im lokalen vSphere-Client zu „Inventar“, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie „HCX-Aktionen“ > „Zu HCX-Zielsite migrieren“.



2. Wählen Sie im Assistenten „Virtuelle Maschine migrieren“ die Remote-Site-Verbindung (Ziel-GCVE) aus.



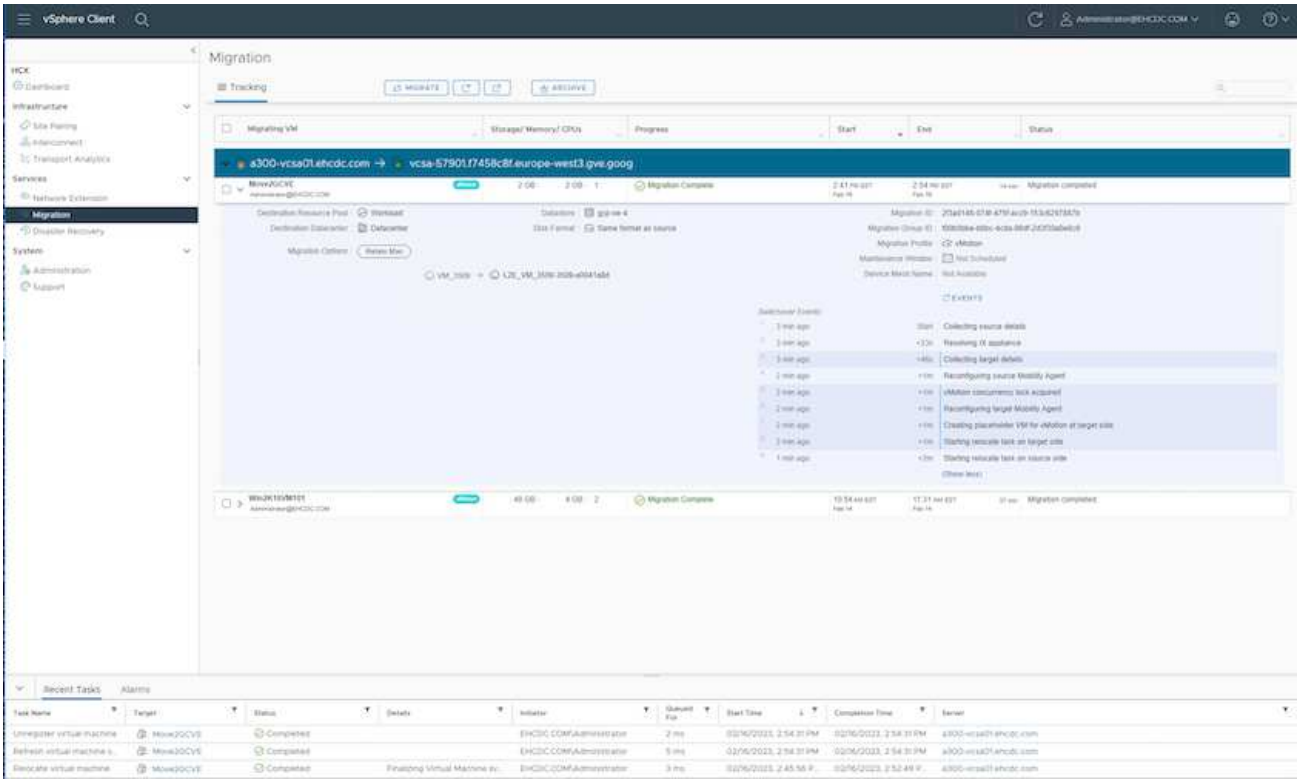
3. Aktualisieren Sie die Pflichtfelder (Cluster, Speicher und Zielnetzwerk) und klicken Sie auf „Validieren“.



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

> Die vMotion-Übertragung erfasst den aktiven Speicher der VM, ihren Ausführungsstatus, ihre IP-Adresse und ihre MAC-Adresse. Weitere Informationen zu den Anforderungen und Einschränkungen von HCX vMotion finden Sie unter "VMware HCX vMotion und Cold Migration verstehen" .

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



Der NFS-Zieldatenspeicher Google Cloud NetApp Volumes (NetApp Volumes) sollte über ausreichend Speicherplatz verfügen, um die Migration durchzuführen.

Abschluss

Unabhängig davon, ob Sie eine reine Cloud oder eine Hybrid-Cloud anstreben und Ihre Daten auf Speichersystemen beliebiger Art/Anbieter vor Ort gespeichert sind, bieten Cloud Volume Service und HCX hervorragende Optionen zum Bereitstellen und Migrieren der Anwendungs-Workloads bei gleichzeitiger Reduzierung der Gesamtbetriebskosten, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden. Wählen Sie für jeden Anwendungsfall Google Cloud VMware Engine zusammen mit Cloud Volume Service, um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und Vorgänge vor Ort und in mehreren Clouds zu nutzen, Workloads in beide Richtungen zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen. Es handelt sich um denselben bekannten Prozess und dieselben bekannten Verfahren, die zum Verbinden des Speichers und Migrieren von VMs mithilfe von VMware vSphere Replication, VMware vMotion oder sogar Network File Copy (NFC) verwendet werden.

Imbiss

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können Cloud Volume Service jetzt als Datenspeicher auf Google Cloud VMware Engine SDDC verwenden.
- Sie können Daten problemlos von lokalen Standorten in den Cloud Volume Service-Datenspeicher migrieren.
- Sie können den Cloud Volume Service-Datenspeicher problemlos vergrößern und verkleinern, um die Kapazitäts- und Leistungsanforderungen während der Migrationsaktivität zu erfüllen.

Videos von Google und VMware als Referenz

▼ **Von Google**

- "HCX Connector mit GCVE bereitstellen"
- "Konfigurieren Sie HCX ServiceMesh mit GCVE"
- "Migrieren Sie VM mit HCX zu GCVE"

▼ **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 Informationen finden Sie unter den folgenden Website-Links:

- Dokumentation zu Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Cloud Volume Service-Dokumentation

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- VMware HCX-Benutzerhandbuch

  "https://docs.vmware.com/en/VMware-HCX/index.html"

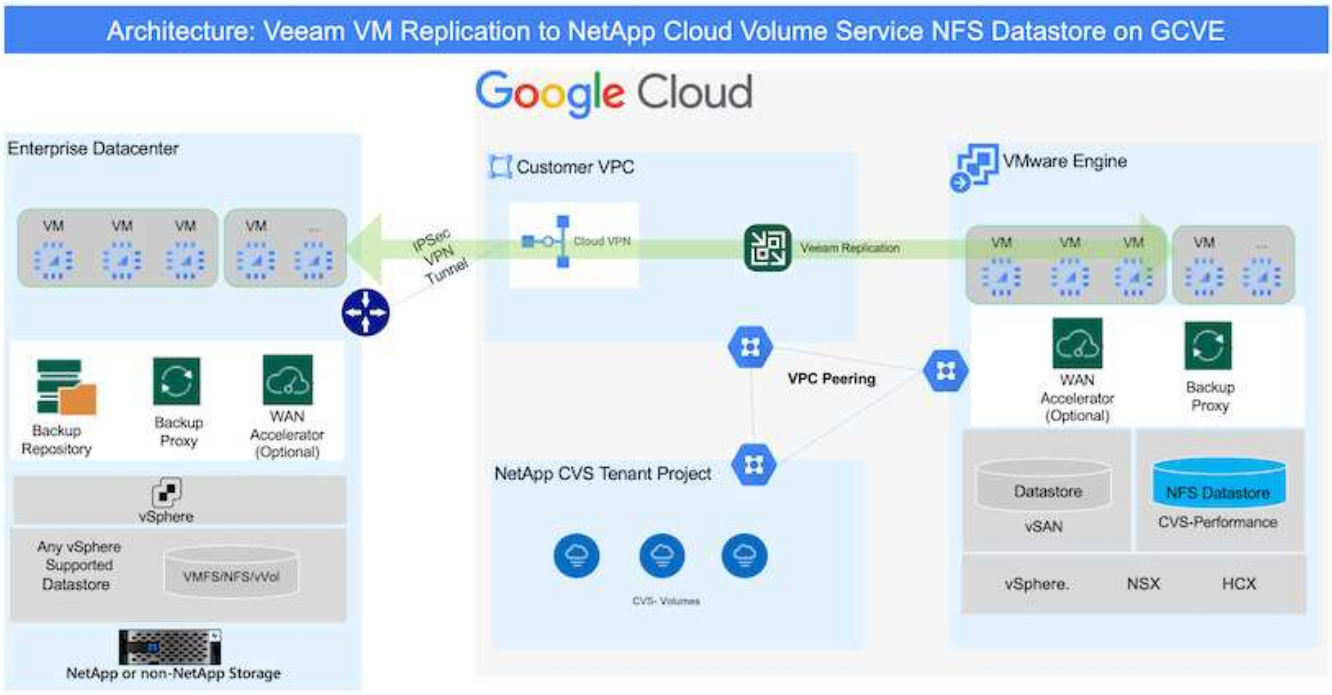
VM-Migration zum Google Cloud NetApp Volumes NFS-Datenspeicher auf Google Cloud VMware Engine mithilfe der Veeam-Replikationsfunktion

Kunden, die derzeit Veeam für ihre Datenschutzanforderungen verwenden, nutzen diese Lösung weiterhin, um die Workloads zu GCVE zu migrieren und die Vorteile der NFS-Datenspeicher von Google Cloud NetApp Volumes zu nutzen.

Überblick

Auf VMware vSphere ausgeführte VM-Workloads können mithilfe der Veeam-Replikationsfunktion auf die Google Cloud VMware Engine (GCVE) migriert werden.

Dieses Dokument bietet eine schrittweise Anleitung zum Einrichten und Durchführen einer VM-Migration unter Verwendung von Google Cloud NetApp Volumes, Veeam und der Google Cloud VMware Engine (GCVE).



Annahmen

In diesem Dokument wird davon ausgegangen, dass Sie entweder über Google Cloud VPN oder Cloud Interconnect oder eine andere Netzwerkoption verfügen, um eine Netzwerkkonnektivität von vorhandenen vSphere-Servern zu Google Cloud VMware Engine herzustellen.

> Es gibt mehrere Optionen zum Verbinden lokaler Rechenzentren mit Google Cloud, weshalb wir in diesem Dokument keinen bestimmten Arbeitsablauf beschreiben können. Weitere Informationen finden Sie im"Google Cloud-Dokumentation" für die geeignete Methode zur Konnektivität vor Ort zu Google.

Bereitstellen der Migrationslösung

Übersicht über die Lösungsbereitstellung

1. Stellen Sie sicher, dass der NFS-Datenspeicher von Google Cloud NetApp Volumes auf GCVE vCenter gemountet ist.
2. Stellen Sie sicher, dass Veeam Backup Recovery in einer vorhandenen VMware vSphere-Umgebung bereitgestellt wird
3. Erstellen Sie einen Replikationsauftrag, um mit der Replikation virtueller Maschinen auf die Google Cloud VMware Engine-Instanz zu beginnen.
4. Führen Sie ein Failover des Veeam-Replikationsjobs durch.
5. Führen Sie ein permanentes Failover auf Veeam durch.

Bereitstellungsdetails

Stellen Sie sicher, dass der NFS-Datenspeicher von Google Cloud NetApp Volumes auf GCVE vCenter gemountet ist

Melden Sie sich bei GCVE vCenter an und stellen Sie sicher, dass ein NFS-Datenspeicher mit ausreichend

Speicherplatz verfügbar ist. Wenn nicht, lesen Sie bitte"Mounten Sie NetApp Volumes als NFS-Datenspeicher auf GCVE"

Stellen Sie sicher, dass Veeam Backup Recovery in einer vorhandenen VMware vSphere-Umgebung bereitgestellt wird

Bitte beachten Sie"Veeam-Replikationskomponenten" Dokumentation zur Installation der erforderlichen Komponenten.

Erstellen Sie einen Replikationsauftrag, um mit der Replikation virtueller Maschinen auf die Google Cloud VMware Engine-Instanz zu beginnen.

Sowohl das lokale vCenter als auch das GCVE vCenter müssen bei Veeam registriert werden. "Einrichten des vSphere VM-Replikationsjobs" Hier ist ein Video, das erklärt, wie man"Replikationsauftrag konfigurieren" .

Die Replikat-VM kann eine andere IP als die Quell-VM haben und auch mit einer anderen Portgruppe verbunden sein. Weitere Einzelheiten finden Sie im obigen Video.

Failover des Veeam-Replikationsjobs durchführen

Um VMs zu migrieren, führen Sie"Failover durchführen"

Führen Sie ein permanentes Failover auf Veeam durch.

Um GCVE als Ihre neue Quellumgebung zu behandeln, führen Sie"Permanentes Failover"

Vorteile dieser Lösung

- Für die Migration kann die vorhandene Veeam-Backup-Infrastruktur genutzt werden.
- Die Veeam-Replikation ermöglicht das Ändern von VM-IP-Adressen auf der Zielsite.
- Kann vorhandene Daten neu zuordnen, die außerhalb von Veeam repliziert wurden (z. B. replizierte Daten aus dem NetApp System)
- Kann auf der Zielsite unterschiedliche Netzwerk-Portgruppen angeben.
- Kann die Reihenfolge der einzuschaltenden VMs angeben.
- Nutzt VMware Change Block Tracking, um die über das WAN zu sendende Datenmenge zu minimieren.
- Möglichkeit zum Ausführen von Pre- und Post-Skripten für die Replikation.
- Möglichkeit zum Ausführen von Pre- und Post-Skripten für Snapshots.

Sichern Sie Daten mit Google Cloud NetApp Volumes in Google Cloud

TR-4918: Sicherheitsübersicht – Google Cloud NetApp Volumes in Google Cloud

Oliver Krause, Justin Parisi, NetApp

Sicherheit, insbesondere in der Cloud, wo sich die Infrastruktur außerhalb der Kontrolle von Storage-Administratoren befindet, ist von größter Bedeutung, wenn Sie Ihre Daten den von Cloud-Anbietern bereitgestellten Services anvertrauen. Dieses Dokument bietet einen Überblick über die Sicherheitsangebote, die "Google Cloud NetApp Volumes bietet in Google Cloud".

Zielgruppe

Dieses Dokument richtet sich unter anderem an die folgenden Rollen:

- Cloud-Anbieter
- Speicheradministratoren
- Speicherarchitekten
- Feldressourcen
- Entscheidungsträger in Unternehmen

Wenn Sie Fragen zum Inhalt dieses technischen Berichts haben, lesen Sie den Abschnitt"Kontaktieren Sie uns."

Abkürzung	Definition
NetApp Volumes-SW	Google Cloud NetApp Volumes, Servicetyp NetApp Volumes
NetApp Volumes – Leistung	Cloud Volume Service, Servicetyp NetApp Volumes-Performance
PSA	

So sichert Google Cloud NetApp Volumes in Google Cloud Ihre Daten

Google Cloud NetApp Volumes in Google Cloud bietet eine Vielzahl von Möglichkeiten, Ihre Daten nativ zu sichern.

Sichere Architektur und Mietmodell

Google Cloud NetApp Volumes bietet eine sichere Architektur in Google Cloud, indem es das Servicemanagement (Steuerungsebene) und den Datenzugriff (Datenebene) über verschiedene Endpunkte segmentiert, sodass sich keiner von beiden gegenseitig beeinflussen kann (siehe Abschnitt"Google Cloud NetApp Volumes Architektur"). Es verwendet Googles "Zugang zu privaten Diensten" (PSA)-Framework zur Bereitstellung des Dienstes. Dieses Framework unterscheidet zwischen dem Service-Produzenten, der von NetApp bereitgestellt und betrieben wird, und dem Service-Consumer, bei dem es sich um eine Virtual Private Cloud (VPC) in einem Kundenprojekt handelt, die die Clients hostet, die auf die Dateifreigaben von Google Cloud NetApp Volumes zugreifen möchten.

In dieser Architektur sind Mandanten (siehe Abschnitt"Mietmodell") sind als Google Cloud-Projekte definiert, die vollständig voneinander isoliert sind, sofern sie nicht ausdrücklich vom Benutzer verbunden werden. Mandanten ermöglichen die vollständige Isolierung von Datenvolumes, externen Namensdiensten und anderen wichtigen Teilen der Lösung von anderen Mandanten mithilfe der Google Cloud NetApp Volumes -Volume-Plattform. Da die Google Cloud NetApp Volumes -Plattform über VPC-Peering verbunden ist, gilt diese Isolation auch für sie. Sie können die gemeinsame Nutzung von Google Cloud NetApp Volumes -Volumes zwischen mehreren Projekten ermöglichen, indem Sie eine Shared-VPC verwenden (siehe Abschnitt"Gemeinsam genutzte VPCs"). Sie können Zugriffskontrollen auf SMB-Freigaben und NFS-Exporte anwenden, um einzuschränken, wer oder was Datensätze anzeigen oder ändern kann.

Starkes Identitätsmanagement für die Steuerebene

In der Kontrollebene, in der die Konfiguration von Google Cloud NetApp Volumes stattfindet, wird das Identitätsmanagement mithilfe von verwaltet "Identitäts- und Zugriffsverwaltung (IAM)" . IAM ist ein Standarddienst, mit dem Sie die Authentifizierung (Anmeldungen) und Autorisierung (Berechtigungen) für

Google Cloud-Projektinstanzen steuern können. Die gesamte Konfiguration wird mit Google Cloud NetApp Volumes -APIs über einen sicheren HTTPS-Transport mit TLS 1.2-Verschlüsselung durchgeführt und die Authentifizierung erfolgt für zusätzliche Sicherheit mithilfe von JWT-Token. Die Google-Konsolen-Benutzeroberfläche für Google Cloud NetApp Volumes übersetzt Benutzereingaben in API-Aufrufe von Google Cloud NetApp Volumes .

Sicherheitshärtung – Angriffsflächen begrenzen

Zu einer effektiven Sicherheit gehört es, die Anzahl der in einem Dienst verfügbaren Angriffsflächen zu begrenzen. Angriffsflächen können eine Vielzahl von Dingen umfassen, darunter ruhende Daten, laufende Übertragungen, Anmeldungen und die Datensätze selbst.

Ein verwalteter Dienst beseitigt einige der Angriffsflächen, die seinem Design innewohnen. Infrastrukturmanagement, wie im Abschnitt beschrieben"Servicebetrieb," wird von einem engagierten Team verwaltet und ist automatisiert, um die Anzahl der Male zu reduzieren, die ein Mensch tatsächlich Konfigurationen berührt, was dazu beiträgt, die Anzahl absichtlicher und unabsichtlicher Fehler zu verringern. Die Vernetzung ist so abgeschottet, dass nur die notwendigen Dienste aufeinander zugreifen können. Die Verschlüsselung ist in den Datenspeicher integriert und nur die Datenebene erfordert Sicherheitsaufmerksamkeit von den Administratoren von Google Cloud NetApp Volumes . Indem der Großteil der Verwaltung hinter einer API-Schnittstelle verborgen wird, wird Sicherheit durch die Begrenzung der Angriffsflächen erreicht.

Zero-Trust-Modell

Historisch gesehen bestand die IT-Sicherheitsphilosophie darin, zu vertrauen, aber zu überprüfen, und manifestierte sich darin, dass man sich zur Eindämmung von Bedrohungen ausschließlich auf externe Mechanismen (wie Firewalls und Intrusion Detection Systems) verließ. Es gibt jedoch immer mehr Angriffe und Sicherheitsverletzungen, die die Verifizierung in Umgebungen durch Phishing, Social Engineering, Insider-Bedrohungen und andere Methoden umgehen, die die Verifizierung ermöglichen, um in Netzwerke einzudringen und Chaos anzurichten.

Zero Trust ist zu einer neuen Methode in der Sicherheit geworden, wobei das aktuelle Mantra lautet: „Vertraue nichts und überprüfe trotzdem alles.“ Daher ist standardmäßig kein Zugriff gestattet. Dieses Mantra wird auf verschiedene Weise durchgesetzt, unter anderem durch Standard-Firewalls und Intrusion Detection Systems (IDS) sowie mit den folgenden Methoden:

- Starke Authentifizierungsmethoden (wie AES-verschlüsselte Kerberos- oder JWT-Token)
- Einzelne starke Identitätsquellen (wie Windows Active Directory, Lightweight Directory Access Protocol (LDAP) und Google IAM)
- Netzwerksegmentierung und sichere Mandantenfähigkeit (standardmäßig ist nur Mandanten der Zugriff gestattet)
- Granulare Zugriffskontrollen mit Least Privileged Access-Richtlinien
- Kleine, exklusive Listen engagierter, vertrauenswürdiger Administratoren mit digitalen Prüf- und Papierprotokollen

Google Cloud NetApp Volumes, die in Google Cloud ausgeführt werden, folgen dem Zero Trust-Modell, indem sie die Haltung „Vertraue nichts, überprüfe alles“ umsetzen.

Verschlüsselung

Verschlüsseln Sie ruhende Daten (siehe Abschnitt"Datenverschlüsselung im Ruhezustand") durch die Verwendung von XTS-AES-256-Chiffren mit NetApp Volume Encryption (NVE) und während der Übertragung mit"SMB-Verschlüsselung" oder NFS Kerberos 5p-Unterstützung. Sie können beruhigt sein, denn

regionsübergreifende Replikationsübertragungen sind durch die TLS 1.2-Verschlüsselung geschützt (siehe Abschnitt "Regionenübergreifende Replikation"). Darüber hinaus bietet das Google-Netzwerk auch verschlüsselte Kommunikation (siehe Abschnitt"Datenverschlüsselung während der Übertragung") für eine zusätzliche Schutzebene gegen Angriffe. Weitere Informationen zur Transportverschlüsselung finden Sie im Abschnitt"Google Cloud-Netzwerk" .

Datenschutz und Backups

Bei der Sicherheit geht es nicht nur um die Verhinderung von Angriffen. Es geht auch darum, wie wir uns von Angriffen erholen, falls oder wenn sie auftreten. Diese Strategie umfasst Datenschutz und Backups. Google Cloud NetApp Volumes bietet Methoden zur Replikation in andere Regionen im Falle von Ausfällen (siehe Abschnitt"Regionsübergreifende Replikation") oder wenn ein Datensatz von einem Ransomware-Angriff betroffen ist. Es kann auch asynchrone Datensicherungen an Standorten außerhalb der Google Cloud NetApp Volumes Instanz durchführen, indem"Google Cloud NetApp Volumes Backup" . Durch regelmäßige Backups kann die Behebung von Sicherheitsvorfällen weniger Zeit in Anspruch nehmen und den Administratoren Geld und Nerven sparen.

Schnelle Abwehr von Ransomware mit branchenführenden Snapshot-Kopien

Zusätzlich zu Datenschutz und Backups bietet Google Cloud NetApp Volumes Unterstützung für unveränderliche Snapshot-Kopien (siehe Abschnitt"Unveränderliche Snapshot-Kopien") von Volumes, die eine Wiederherstellung nach Ransomware-Angriffen ermöglichen (siehe Abschnitt"Servicebetrieb") innerhalb von Sekunden nach Entdeckung des Problems und mit minimaler Unterbrechung. Wiederherstellungszeit und -effekte hängen vom Snapshot-Zeitplan ab, Sie können jedoch Snapshot-Kopien erstellen, die bei Ransomware-Angriffen nur eine Stunde Deltas aufweisen. Snapshot-Kopien haben einen vernachlässigbaren Einfluss auf die Leistung und Kapazitätsauslastung und stellen eine risikoarme, aber lohnende Methode zum Schutz Ihrer Datensätze dar.

Sicherheitsüberlegungen und Angriffsflächen

Der erste Schritt zum Verständnis der Sicherung Ihrer Daten besteht darin, die Risiken und potenziellen Angriffsflächen zu identifizieren.

Hierzu gehören (ohne darauf beschränkt zu sein) die folgenden:

- Administration und Logins
- Ruhende Daten
- Daten im Flug
- Netzwerk und Firewalls
- Ransomware, Malware und Viren

Wenn Sie die Angriffsflächen verstehen, können Sie Ihre Umgebungen besser schützen. Google Cloud NetApp Volumes in Google Cloud berücksichtigt bereits viele dieser Themen und implementiert Sicherheitsfunktionen standardmäßig, ohne dass ein administrativer Eingriff erforderlich ist.

Sichere Anmeldungen gewährleisten

Beim Sichern Ihrer kritischen Infrastrukturkomponenten müssen Sie unbedingt sicherstellen, dass sich nur autorisierte Benutzer anmelden und Ihre Umgebungen verwalten können. Wenn böswillige Akteure Ihre Administratoranmeldeinformationen verletzen, haben sie die Schlüssel zum Schloss und können alles tun, was sie wollen – Konfigurationen ändern, Volumes und Backups löschen, Hintertüren erstellen oder Snapshot-Zeitpläne deaktivieren.

Google Cloud NetApp Volumes für Google Cloud bietet Schutz vor nicht autorisierten Administratoranmeldungen durch die Verschleierung von Storage as a Service (StaaS). Google Cloud NetApp Volumes wird vollständig vom Cloud-Anbieter verwaltet und es besteht keine Möglichkeit, sich extern anzumelden. Alle Einrichtungs- und Konfigurationsvorgänge sind vollständig automatisiert, sodass ein menschlicher Administrator außer in sehr seltenen Fällen nie mit den Systemen interagieren muss.

Wenn eine Anmeldung erforderlich ist, sichert Google Cloud NetApp Volumes in Google Cloud die Anmeldungen, indem es eine sehr kurze Liste vertrauenswürdiger Administratoren verwaltet, die Zugriff auf die Anmeldung bei den Systemen haben. Dieses Gatekeeping trägt dazu bei, die Anzahl potenzieller böswilliger Akteure mit Zugriff zu reduzieren. Darüber hinaus verbirgt das Google Cloud-Netzwerk die Systeme hinter mehreren Netzwerksicherheitsebenen und gibt nur das Nötige an die Außenwelt weiter. Informationen zur Google Cloud, Google Cloud NetApp Volumes Architektur finden Sie im Abschnitt"Google Cloud NetApp Volumes Architektur."

Clusterverwaltung und Upgrades

Zwei Bereiche mit potenziellen Sicherheitsrisiken sind die Clusterverwaltung (was passiert, wenn ein böswilliger Akteur Administratorzugriff hat) und Upgrades (was passiert, wenn ein Software-Image kompromittiert wird).

Schutz der Speicherverwaltung

Durch die Bereitstellung von Speicher als Service wird das zusätzliche Risiko einer Gefährdung der Administratoren beseitigt, indem Endbenutzern außerhalb des Cloud-Rechenzentrums der Zugriff entzogen wird. Stattdessen wird von den Kunden nur die Konfiguration für die Datenzugriffsebene vorgenommen. Jeder Mandant verwaltet seine eigenen Volumes und kein Mandant kann auf andere Google Cloud NetApp Volumes -Instanzen zugreifen. Der Dienst wird automatisiert verwaltet, wobei einer sehr kleinen Liste vertrauenswürdiger Administratoren über die im Abschnitt beschriebenen Prozesse Zugriff auf die Systeme gewährt wird."Servicebetrieb."

Der Servicetyp „NetApp Volumes-Performance“ bietet die Möglichkeit einer regionsübergreifenden Replikation, um im Falle eines Regionsausfalls den Datenschutz in einer anderen Region zu gewährleisten. In diesen Fällen kann ein Failover der Google Cloud NetApp Volumes in die nicht betroffene Region durchgeführt werden, um den Datenzugriff aufrechtzuerhalten.

Service-Upgrades

Updates helfen, anfällige Systeme zu schützen. Jedes Update bietet Sicherheitsverbesserungen und Fehlerbehebungen, die Angriffsflächen minimieren. Software-Updates werden aus zentralen Repositories heruntergeladen und vor der Freigabe der Updates validiert, um sicherzustellen, dass offizielle Images verwendet werden und die Upgrades nicht durch böswillige Akteure kompromittiert wurden.

Bei Google Cloud NetApp Volumes werden Updates von den Teams des Cloud-Anbieters durchgeführt. Dadurch wird das Risiko für Administratorteams verringert, da Experten mit umfassenden Kenntnissen in Konfiguration und Upgrades zur Verfügung stehen, die den Prozess automatisiert und vollständig getestet haben. Upgrades erfolgen unterbrechungsfrei und Google Cloud NetApp Volumes hält die neuesten Updates bereit, um optimale Gesamtergebnisse zu erzielen.

Informationen zum Administratorteam, das diese Service-Upgrades durchführt, finden Sie im Abschnitt"Servicebetrieb."

Sicherung ruhender Daten

Die Verschlüsselung ruhender Daten ist wichtig, um vertrauliche Daten zu schützen, falls eine Festplatte gestohlen, zurückgegeben oder zweckentfremdet wird. Daten in Google Cloud NetApp Volumes werden im

Ruhezustand durch softwarebasierte Verschlüsselung geschützt.

- Für NetApp Volumes-SW werden von Google generierte Schlüssel verwendet.
- Für NetApp Volumes-Performance werden die Schlüssel pro Volume in einem in Google Cloud NetApp Volumes integrierten Schlüsselmanager gespeichert, der NetApp ONTAP CryptoMod zum Generieren von AES-256-Verschlüsselungsschlüsseln verwendet. CryptoMod ist in der Liste der validierten CMVP FIPS 140-2-Module aufgeführt. Sehen "FIPS 140-2-Zertifikat Nr. 4144" .

Ab November 2021 wurde die Vorschaufunktion „Customer-Managed Encryption“ (CMEK) für NetApp Volumes-Performance verfügbar gemacht. Mit dieser Funktion können Sie die Schlüssel pro Volume mit Hauptschlüsseln pro Projekt und pro Region verschlüsseln, die im Google Key Management Service (KMS) gehostet werden. KMS ermöglicht Ihnen das Anschließen externer Schlüsselmanager.

Einzelheiten zur Konfiguration von KMS für NetApp Volumes Performance, "siehe die Google Cloud NetApp Volumes -Dokumentation".

Weitere Informationen zur Architektur finden Sie im Abschnitt"Google Cloud NetApp Volumes Architektur."

Datensicherung während der Übertragung

Zusätzlich zur Sicherung ruhender Daten müssen Sie auch in der Lage sein, Daten zu sichern, wenn diese zwischen der Google Cloud NetApp Volumes -Instanz und einem Client oder Replikationsziel übertragen werden. Google Cloud NetApp Volumes bietet Verschlüsselung für In-Flight-Daten über NAS-Protokolle durch den Einsatz von Verschlüsselungsmethoden wie SMB-Verschlüsselung mit Kerberos, Signieren/Versiegeln von Paketen und NFS Kerberos 5p für die End-to-End-Verschlüsselung von Datenübertragungen.

Die Replikation von Google Cloud NetApp Volumes Volumes verwendet TLS 1.2, das die Vorteile der AES-GCM-Verschlüsselungsmethoden nutzt.

Die meisten unsicheren In-Flight-Protokolle wie Telnet, NDMP usw. sind standardmäßig deaktiviert. DNS wird jedoch nicht von Google Cloud NetApp Volumes verschlüsselt (keine DNS Sec-Unterstützung) und sollte nach Möglichkeit mithilfe einer externen Netzwerkverschlüsselung verschlüsselt werden. Siehe den Abschnitt"Datenverschlüsselung während der Übertragung" Weitere Informationen zum Sichern von Daten während der Übertragung.

Informationen zur NAS-Protokollverschlüsselung finden Sie im Abschnitt"NAS-Protokolle."

Benutzer und Gruppen für NAS-Berechtigungen

Zur Sicherung Ihrer Daten in der Cloud gehört unter anderem eine ordnungsgemäße Benutzer- und Gruppenauthentifizierung, bei der die Benutzer, die auf die Daten zugreifen, als echte Benutzer in der Umgebung verifiziert werden und die Gruppen gültige Benutzer enthalten. Diese Benutzer und Gruppen bieten anfänglichen Freigabe- und Exportzugriff sowie eine Berechtigungsüberprüfung für Dateien und Ordner im Speichersystem.

Google Cloud NetApp Volumes verwendet die standardmäßige Active Directory-basierte Windows-Benutzer- und Gruppenauthentifizierung für SMB-Freigaben und Berechtigungen im Windows-Stil. Der Dienst 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 für die LDAP-Funktionalität nur Active Directory LDAP mit Google Cloud NetApp Volumes unterstützt.

Erkennung, Prävention und Eindämmung von Ransomware, Malware und Viren

Ransomware, Malware und Viren stellen eine ständige Bedrohung für Administratoren dar und die Erkennung, Prävention und Eindämmung dieser Bedrohungen hat für Unternehmen stets oberste Priorität. Ein einziger Ransomware-Angriff auf einen kritischen Datensatz kann potenziell Millionen von Dollar kosten. Daher ist es sinnvoll, alles zu tun, um das Risiko zu minimieren.

Obwohl Google Cloud NetApp Volumes derzeit keine nativen Erkennungs- oder Präventionsmaßnahmen wie Virenschutz oder "automatische Ransomware-Erkennung" umfasst, gibt es Möglichkeiten, sich nach einem Ransomware-Angriff durch die Aktivierung regelmäßiger Snapshot-Zeitpläne schnell zu erholen. Snapshot Kopien sind unveränderliche, schreibgeschützte Zeiger auf geänderte Blöcke im Dateisystem, werden nahezu sofort erstellt, beeinträchtigen die Leistung nur minimal und belegen nur dann Speicherplatz, wenn Daten geändert oder gelöscht werden. Es ist möglich, Zeitpläne für Snapshot Kopien so festzulegen, dass sie dem gewünschten Recovery Point Objective (RPO) beziehungsweise Recovery Time Objective (RTO) entsprechen, und pro Volume können bis zu 1.024 Snapshot Kopien beibehalten werden.

Snapshot-Support ist ohne zusätzliche Kosten (über die Datenspeichergebühren für geänderte Blöcke/Daten hinaus, die in Snapshot-Kopien gespeichert sind) in Google Cloud NetApp Volumes enthalten und kann im Falle eines Ransomware-Angriffs verwendet werden, um zu einer Snapshot-Kopie vor dem Angriff zurückzukehren. Die Wiederherstellung von Snapshots dauert nur wenige Sekunden und Sie können anschließend wieder wie gewohnt mit der Datenbereitstellung fortfahren. Weitere Informationen finden Sie unter "Die NetApp Lösung für Ransomware" .

Um zu verhindern, dass Ihr Unternehmen von Ransomware betroffen ist, ist ein mehrschichtiger Ansatz erforderlich, der mindestens eines der folgenden Elemente umfasst:

- Endpunktschutz
- Schutz vor externen Bedrohungen durch Netzwerk-Firewalls
- Erkennung von Datenanomalien
- Mehrere Backups (vor Ort und außerhalb) kritischer Datensätze
- Regelmäßige Wiederherstellungstests von Backups
- Unveränderliche, schreibgeschützte NetApp Snapshot-Kopien
- Multifaktor-Authentifizierung für kritische Infrastrukturen
- Sicherheitsüberprüfungen von Systemanmeldungen

Diese Liste ist bei weitem nicht vollständig, stellt jedoch eine gute Vorlage für den Umgang mit potenziellen Ransomware-Angriffen dar. Google Cloud NetApp Volumes in Google Cloud bietet mehrere Möglichkeiten, sich vor Ransomware-Vorfällen zu schützen und deren Auswirkungen zu reduzieren.

Unveränderliche Snapshot-Kopien

Google Cloud NetApp Volumes bietet nativ unveränderliche, schreibgeschützte Snapshot-Kopien, die nach einem anpassbaren Zeitplan erstellt werden, um im Falle einer Datenlöschung oder wenn ein ganzes Volume Opfer eines Ransomware-Angriffs wurde, eine schnelle Wiederherstellung zu einem bestimmten Zeitpunkt zu ermöglichen. Snapshot-Wiederherstellungen auf vorherige, fehlerfreie Snapshot-Kopien erfolgen schnell und minimieren den Datenverlust basierend auf der Aufbewahrungsdauer Ihrer Snapshot-Zeitpläne und RTO/RPO. Der Leistungseffekt der Snapshot-Technologie ist vernachlässigbar.

Da Snapshot-Kopien in Google Cloud NetApp Volumes schreibgeschützt sind, können sie nicht mit Ransomware infiziert werden, es sei denn, die Ransomware hat sich unbemerkt im Datensatz ausgebreitet und es wurden Snapshot-Kopien der mit Ransomware infizierten Daten erstellt. Aus diesem Grund müssen Sie auch die Ransomware-Erkennung anhand von Datenanomalien in Betracht ziehen. Google Cloud NetApp

Volumes bietet derzeit keine native Erkennung, Sie können jedoch externe Überwachungssoftware verwenden.

Sicherungen und Wiederherstellungen

Google Cloud NetApp Volumes bietet standardmäßige NAS-Client-Backup-Funktionen (z. B. Backups über NFS oder SMB).

- NetApp Volumes-Performance bietet regionsübergreifende Volume-Replikation zu anderen NetApp Volumes-Performance Volumes. Weitere Informationen bietet "Volumereplikation" die Dokumentation zu Google Cloud NetApp Volumes.
- NetApp Volumes-SW bietet service-native Funktionen zum Sichern und Wiederherstellen von Volumes. Weitere Informationen enthält "Cloud-Backup" die Dokumentation zu Google Cloud NetApp Volumes.

Die Volume-Replikation bietet eine exakte Kopie des Quellvolumes für ein schnelles Failover im Katastrophenfall, einschließlich Ransomware-Vorfällen.

Regionsübergreifende Replikation

Mit NetApp Volumes-Performance können Sie Volumes für Datenschutz- und Archivierungsanwendungsfälle sicher über Google Cloud-Regionen hinweg replizieren, indem Sie die TLS1.2 AES 256 GCM-Verschlüsselung in einem von NetApp gesteuerten Back-End-Servicenetzwerk mithilfe spezifischer Schnittstellen verwenden, die für die Replikation im Google-Netzwerk verwendet werden. Ein primäres (Quell-)Volume enthält die aktiven Produktionsdaten und wird auf ein sekundäres (Ziel-)Volume repliziert, um eine exakte Replik des primären Datensatzes bereitzustellen.

Bei der ersten Replikation werden alle Blöcke übertragen, bei Updates werden jedoch nur die geänderten Blöcke in einem primären Volume übertragen. Wenn beispielsweise eine 1 TB große Datenbank, die sich auf einem primären Volume befindet, auf das sekundäre Volume repliziert wird, wird bei der ersten Replikation 1 TB Speicherplatz übertragen. Wenn diese Datenbank einige hundert Zeilen (hypothetisch einige MB) enthält, die sich zwischen der Initialisierung und der nächsten Aktualisierung ändern, werden nur die Blöcke mit den geänderten Zeilen auf die sekundäre Datenbank repliziert (einige MB). Dadurch werden die Übertragungszeiten gering gehalten und die Replikationskosten niedrig gehalten.

Alle Berechtigungen für Dateien und Ordner werden auf das sekundäre Volume repliziert, Freigabezugriffsberechtigungen (wie Exportrichtlinien und -regeln oder SMB-Freigaben und Freigabe-ACLs) müssen jedoch separat behandelt werden. Im Falle eines Site-Failovers sollte die Zielsite dieselben Namensdienste und Active Directory-Domänenverbindungen nutzen, um eine konsistente Handhabung der Benutzer- und Gruppenidentitäten und -berechtigungen zu gewährleisten. Sie können ein sekundäres Volume im Katastrophenfall als Failover-Ziel verwenden, indem Sie die Replikationsbeziehung unterbrechen, wodurch das sekundäre Volume in einen Lese-/Schreibzugriff umgewandelt wird.

Volume-Replikate sind schreibgeschützt und bieten eine unveränderliche Kopie der Daten außerhalb des Standorts für eine schnelle Wiederherstellung der Daten in Fällen, in denen ein Virus die Daten infiziert hat oder Ransomware den primären Datensatz verschlüsselt hat. Schreibgeschützte Daten werden nicht verschlüsselt, aber wenn das primäre Volume betroffen ist und eine Replikation stattfindet, werden auch die infizierten Blöcke repliziert. Sie können ältere, nicht betroffene Snapshot-Kopien zur Wiederherstellung verwenden, aber die SLAs können je nachdem, wie schnell ein Angriff erkannt wird, außerhalb des Bereichs des versprochenen RTO/RPO liegen.

Darüber hinaus können Sie böswillige administrative Aktionen wie das Löschen von Volumes, das Löschen von Snapshots oder Änderungen an Snapshot-Zeitplänen durch das Management der regionsübergreifenden Replikation (CRR) in Google Cloud verhindern. Dies erfolgt durch die Erstellung benutzerdefinierter Rollen, die Volume-Administratoren, die Quell-Volumes löschen können, aber keine Mirror-Beziehungen aufheben und

daher keine Ziel-Volumes löschen können, von CRR-Administratoren trennen, die keine Volume-Operationen durchführen können. Informationen zu den für die einzelnen Administratorgruppen zulässigen Berechtigungen finden Sie "Sicherheitsüberlegungen" in der Dokumentation zu Google Cloud NetApp Volumes.

Google Cloud NetApp Volumes Backup

Obwohl Google Cloud NetApp Volumes eine hohe Datenbeständigkeit bietet, können externe Ereignisse zu Datenverlust führen. Im Falle eines Sicherheitsvorfalls wie einem Virus oder Ransomware sind Sicherungen und Wiederherstellungen für die zeitnahe Wiederherstellung des Datenzugriffs von entscheidender Bedeutung. Ein Administrator könnte versehentlich ein Google Cloud NetApp Volumes -Volume löschen. Oder Benutzer möchten einfach Sicherungsversionen ihrer Daten viele Monate lang aufbewahren und die Beibehaltung des zusätzlichen Speicherplatzes für Snapshot-Kopien innerhalb des Volumes wird zu einer Kostenherausforderung. Obwohl Snapshot-Kopien die bevorzugte Methode sein sollten, um Sicherungsversionen der letzten Wochen aufzubewahren und verlorene Daten daraus wiederherzustellen, bleiben sie auf dem Datenträger und gehen verloren, wenn dieser gelöscht wird.

Aus all diesen Gründen bietet Google Cloud NetApp Volumes Backup Services über "Google Cloud NetApp Volumes Backup" an.

Beim Google Cloud NetApp Volumes -Backup wird eine Kopie des Volumes auf Google Cloud Storage (GCS) erstellt. Es werden nur die tatsächlich auf dem Datenträger gespeicherten Daten gesichert, nicht der freie Speicherplatz. Es funktioniert dauerhaft inkrementell, d. h., es überträgt den Volume-Inhalt einmal und sichert von da an nur die geänderten Daten. Im Vergleich zu klassischen Backup-Konzepten mit mehreren Voll-Backups werden große Mengen an Backup-Speicherplatz gespart und so die Kosten gesenkt. Da der monatliche Preis für Backup-Speicherplatz im Vergleich zu einem Volume niedriger ist, ist er ein idealer Ort, um Backup-Versionen länger aufzubewahren.

Benutzer können eine Google Cloud NetApp Volumes -Sicherung verwenden, um jede Sicherungsversion auf demselben oder einem anderen Volume innerhalb derselben Region wiederherzustellen. Wenn das Quellvolume gelöscht wird, bleiben die Sicherungsdaten erhalten und müssen separat verwaltet (z. B. gelöscht) werden.

Google Cloud NetApp Volumes Backup ist optional in Google Cloud NetApp Volumes integriert. Benutzer können entscheiden, welche Volumes geschützt werden sollen, indem sie Google Cloud NetApp Volumes Backup auf Volume-Basis aktivieren. Informationen zu Backups, den "Dokumentation zur Sicherung von Google Cloud NetApp Volumes", der Zeitplanung und "Anzahl der maximal unterstützten Sicherungsversionen" finden Sie in der "Preisgestaltung".

Alle Sicherungsdaten eines Projekts werden in einem GCS-Bucket gespeichert, der vom Dienst verwaltet wird und für den Benutzer nicht sichtbar ist. Jedes Projekt verwendet einen anderen Bucket. Derzeit befinden sich die Buckets in derselben Region wie die Google Cloud NetApp Volumes -Volumes, es werden jedoch weitere Optionen diskutiert. Den aktuellen Stand finden Sie in der Dokumentation.

Der Datentransport von einem Google Cloud NetApp Volumes Bucket zu GCS erfolgt über dienstinterne Google-Netzwerke mit HTTPS und TLS1.2. Daten werden im Ruhezustand mit von Google verwalteten Schlüsseln verschlüsselt.

Für das Managen von Google Cloud NetApp Volumes Backups (Erstellen, Löschen und Wiederherstellen von Backups) muss ein Benutzer über die "roles/netapp.admin"Rolle verfügen.

Überblick

Um einer Cloud-Lösung vertrauen zu können, muss man die Architektur und ihre Sicherung verstehen. In diesem Abschnitt werden verschiedene Aspekte der Google

Cloud NetApp Volumes -Architektur in Google erläutert, um mögliche Bedenken hinsichtlich der Datensicherung auszuräumen und Bereiche aufzuzeigen, in denen möglicherweise zusätzliche Konfigurationsschritte erforderlich sind, um eine möglichst sichere Bereitstellung zu erreichen.

Die allgemeine Architektur von Google Cloud NetApp Volumes kann in zwei Hauptkomponenten unterteilt werden: die Steuerebene und die Datenebene.

Steuerebene

Die Steuerebene in Google Cloud NetApp Volumes ist die Backend-Infrastruktur, die von Google Cloud NetApp Volumes Administratoren und der nativen Automatisierungssoftware von NetApp verwaltet wird. Diese Ebene ist für Endbenutzer völlig transparent und umfasst Netzwerk-, Speicherhardware- und Softwareupdates usw., um den Mehrwert einer Cloud-basierten Lösung wie Google Cloud NetApp Volumes zu steigern.

Datenebene

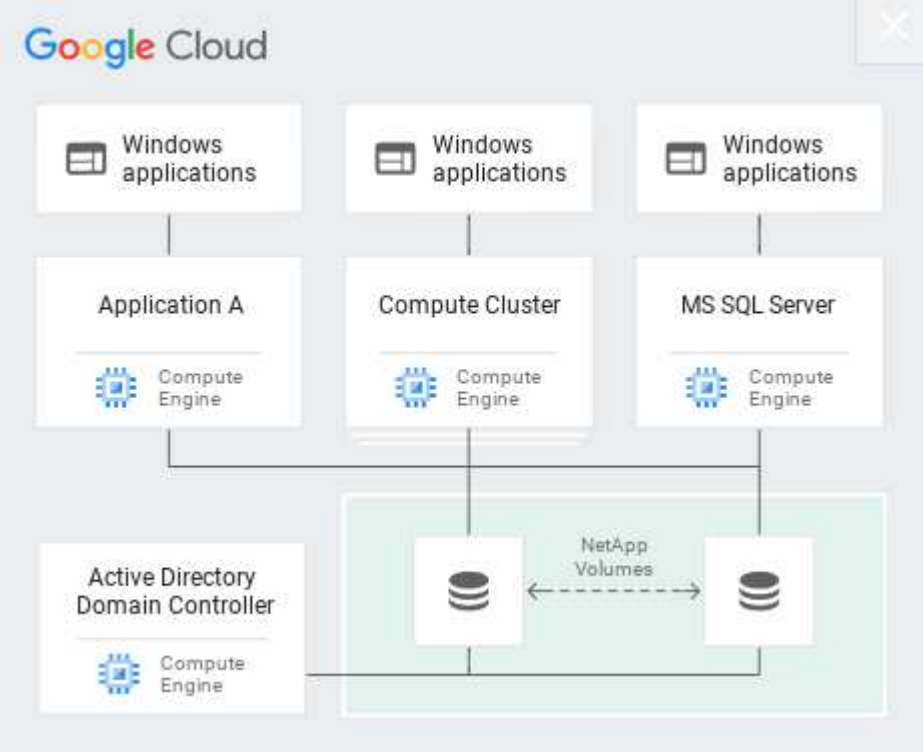
Die Datenebene in Google Cloud NetApp Volumes umfasst die eigentlichen Datenvolumes und die gesamte Google Cloud NetApp Volumes -Konfiguration (wie Zugriffskontrolle, Kerberos-Authentifizierung usw.). Die Datenebene unterliegt vollständig der Kontrolle der Endbenutzer und Verbraucher der Google Cloud NetApp Volumes -Plattform.

Es gibt deutliche Unterschiede in der Art und Weise, wie die einzelnen Flugzeuge gesichert und verwaltet werden. Die folgenden Abschnitte behandeln diese Unterschiede und beginnen mit einer Übersicht über die Architektur von Google Cloud NetApp Volumes .

Google Cloud NetApp Volumes Architektur

Ähnlich wie andere native Google Cloud-Dienste wie CloudSQL, Google Cloud VMware Engine (GCVE) und FileStore verwendet Google Cloud NetApp Volumes "Google PSA" um den Dienst zu erbringen. In PSA werden Dienste innerhalb eines Service-Producer-Projekts erstellt, das "VPC-Netzwerk-Peering" um eine Verbindung zum Service-Consumer herzustellen. Der Service-Produzent wird von NetApp bereitgestellt und betrieben, und der Service-Consumer ist ein VPC in einem Kundenprojekt, das die Clients hostet, die auf die Dateifreigaben von Google Cloud NetApp Volumes zugreifen möchten.

Die folgende Abbildung, entnommen aus der "Google Cloud NetApp Volumes-Dokumentation", zeigt eine Übersicht auf hoher Ebene.



Der Teil über der gepunkteten Linie zeigt die Steuerebene des Dienstes, die den Lebenszyklus des Volumes steuert. Der Teil unterhalb der gepunkteten Linie zeigt die Datenebene. Das linke blaue Kästchen stellt den Benutzer VPC (Service Consumer) dar, das rechte blaue Kästchen ist der von NetApp bereitgestellte Service Producer. Beide sind über VPC-Peering verbunden.

Mietmodell

In Google Cloud NetApp Volumes werden einzelne Projekte als eindeutige Mandanten betrachtet. Dies bedeutet, dass die Manipulation von Volumes, Snapshot-Kopien usw. auf Projektbasis erfolgt. Mit anderen Worten: Alle Volumes gehören dem Projekt, in dem sie erstellt wurden, und nur dieses Projekt kann standardmäßig die darin enthaltenen Daten verwalten und darauf zugreifen. Dies wird als die Steuerungsebenenansicht des Dienstes betrachtet.

Gemeinsam genutzte VPCs

In der Datenebenenansicht können Google Cloud NetApp Volumes eine Verbindung zu einem gemeinsam genutzten VPC herstellen. Sie können Volumes im Hosting-Projekt oder in einem der mit der gemeinsam genutzten VPC verbundenen Serviceprojekte erstellen. Alle mit diesem gemeinsam genutzten VPC verbundenen Projekte (Host oder Dienst) können die Volumes auf der Netzwerkebene (TCP/IP) erreichen. Da alle Clients mit Netzwerkkonnektivität auf der gemeinsam genutzten VPC potenziell über NAS-Protokolle auf die Daten zugreifen können, muss die Zugriffskontrolle auf dem einzelnen Volume (z. B. Benutzer-/Gruppen-Zugriffskontrolllisten (ACLs) und Hostnamen/IP-Adressen für NFS-Exporte) verwendet werden, um zu steuern, wer auf die Daten zugreifen kann.

Sie können Google Cloud NetApp Volumes mit bis zu fünf VPCs pro Kundenprojekt verbinden. Auf der Steuerebene ermöglicht Ihnen das Projekt die Verwaltung aller erstellten Volumes, unabhängig davon, mit welchem VPC sie verbunden sind. Auf der Datenebene sind VPCs voneinander isoliert und jedes Volume kann nur mit einer VPC verbunden werden.

Der Zugriff auf die einzelnen Volumes wird durch protokollspezifische (NFS/SMB) Zugriffskontrollmechanismen gesteuert.

Mit anderen Worten: Auf der Netzwerkebene können alle mit der gemeinsam genutzten VPC verbundenen Projekte das Volume sehen, während auf der Verwaltungsseite die Steuerebene nur dem Eigentümerprojekt die Anzeige des Volumes ermöglicht.

VPC-Dienststeuerungen

VPC Service Controls richten einen Zugriffskontrollbereich um Google Cloud-Dienste ein, die mit dem Internet verbunden und weltweit zugänglich sind. Diese Dienste ermöglichen eine Zugriffskontrolle über Benutzeridentitäten, können jedoch nicht einschränken, von welchem Netzwerkstandort die Anfragen stammen. VPC Service Controls schließt diese Lücke, indem es die Möglichkeit einführt, den Zugriff auf definierte Netzwerke einzuschränken.

Die Datenebene von Google Cloud NetApp Volumes ist nicht mit dem externen Internet verbunden, sondern mit privaten VPCs mit klar definierten Netzwerkgrenzen (Perimetern). Innerhalb dieses Netzwerks verwendet jedes Volume eine protokollspezifische Zugriffskontrolle. Jede externe Netzwerkkonnektivität wird ausdrücklich von den Google Cloud-Projektadministratoren erstellt. Die Kontrollebene bietet jedoch nicht den gleichen Schutz wie die Datenebene und kann von jedem von überall mit gültigen Anmeldeinformationen aufgerufen werden ("JWT-Token").

Kurz gesagt: Die Datenebene von Google Cloud NetApp Volumes bietet die Möglichkeit der Netzwerkzugriffskontrolle, ohne dass VPC Service Controls unterstützt werden müssen, und verwendet VPC Service Controls nicht explizit.

Überlegungen zum Packet Sniffing/Trace

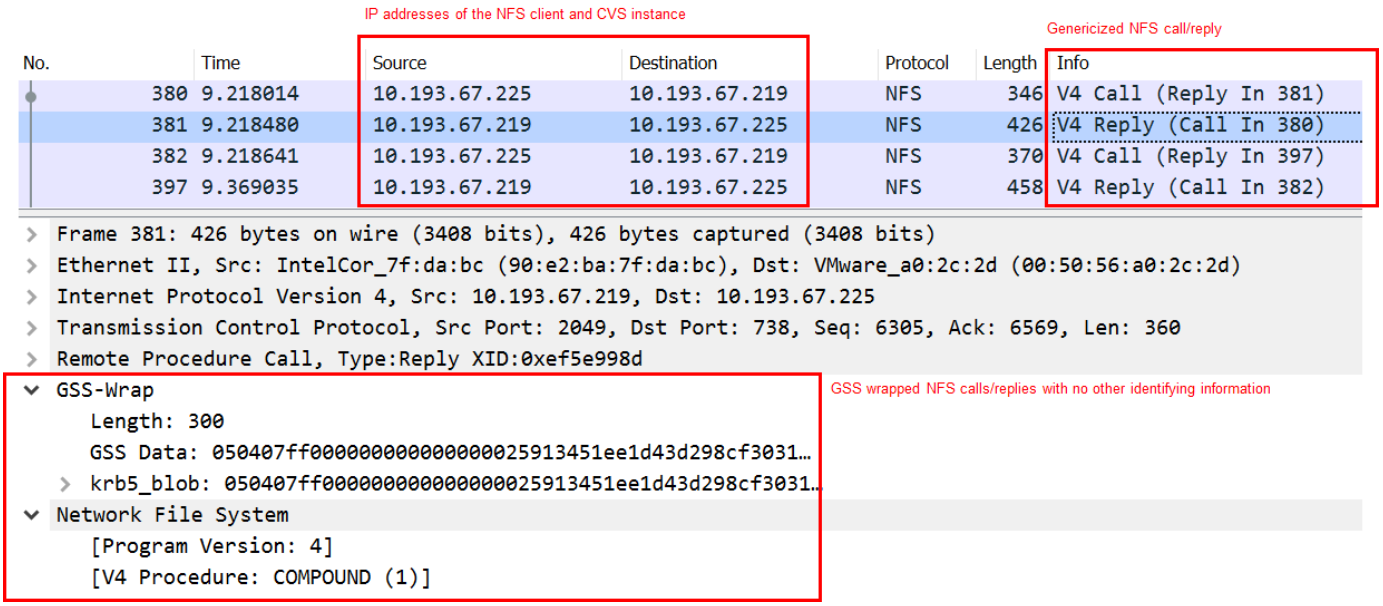
Paketerfassungen können bei der Behebung von Netzwerkproblemen oder anderen Problemen (wie NAS-Berechtigungen, LDAP-Konnektivität usw.) hilfreich sein, können aber auch böswillig missbraucht werden, um Informationen über Netzwerk-IP-Adressen, MAC-Adressen, Benutzer- und Gruppennamen und die auf den Endpunkten verwendete Sicherheitsstufe zu erhalten. Aufgrund der Art und Weise, wie Google Cloud-Netzwerke, VPCs und Firewall-Regeln konfiguriert sind, sollte es ohne Benutzeranmeldeinformationen schwierig sein, unerwünschten Zugriff auf Netzwerkpakete zu erhalten oder"JWT-Token" in die Cloud-Instanzen. Paketerfassungen sind nur auf Endpunkten (wie virtuellen Maschinen (VMs)) und nur auf Endpunkten innerhalb der VPC möglich, es sei denn, es wird eine gemeinsam genutzte VPC und/oder ein externer Netzwerktunnel/eine IP-Weiterleitung verwendet, um externen Datenverkehr zu Endpunkten ausdrücklich zuzulassen. Es gibt keine Möglichkeit, den Datenverkehr außerhalb der Clients abzuhören.

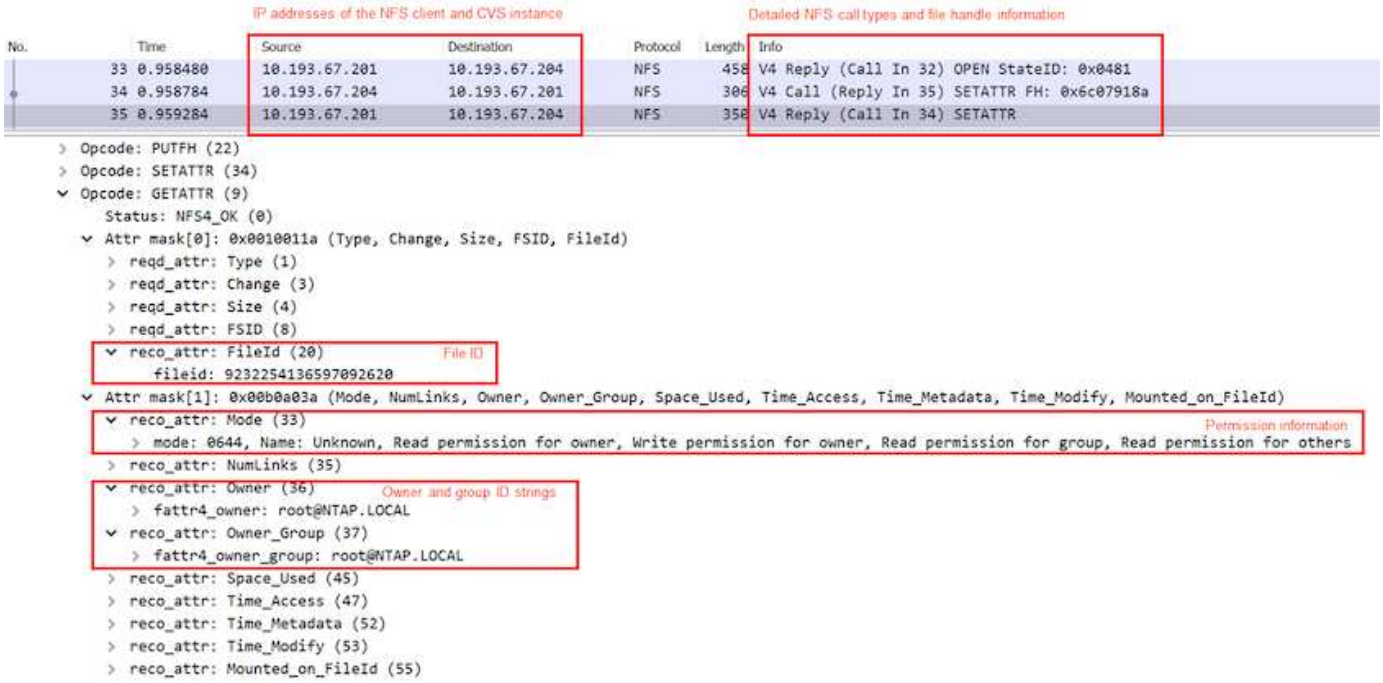
Bei der Verwendung von Shared VPCs ist eine In-Flight-Verschlüsselung mit NFS Kerberos und/oder"SMB-Verschlüsselung" kann viele der aus Spuren gewonnenen Informationen verschleiern. Ein Teil des Datenverkehrs wird jedoch weiterhin im Klartext gesendet, beispielsweise"DNS" Und"LDAP-Abfragen" . Die folgende Abbildung zeigt eine Paketerfassung aus einer Klartext-LDAP-Abfrage, die von Google Cloud NetApp Volumes stammt, und die potenziell offengelegten Identifizierungsinformationen. LDAP-Abfragen in Google Cloud NetApp Volumes unterstützen derzeit keine Verschlüsselung oder LDAP über SSL. NetApp Volumes-Performance unterstützt LDAP-Signierung, wenn dies von Active Directory angefordert wird. NetApp Volumes-SW unterstützt keine LDAP-Signierung.



unixUserPassword wird von LDAP abgefragt und nicht im Klartext, sondern in einem gesalzenen 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 bei Clients nutzen müssen. Google Cloud NetApp Volumes unterstützt keine interaktiven LDAP-Anmeldungen bei den Instanzen.

Die folgende Abbildung zeigt eine Paketerfassung aus einer NFS-Kerberos-Konversation neben einer Erfassung von NFS über AUTH_SYS. Beachten Sie, dass sich die in einer Ablaufverfolgung verfügbaren Informationen bei beiden unterscheiden und dass die Aktivierung der In-Flight-Verschlüsselung eine höhere Gesamtsicherheit für den NAS-Verkehr bietet.





VM-Netzwerkschnittstellen

Ein Trick, den Angreifer versuchen könnten, besteht darin, einer VM eine neue Netzwerkkarte (NIC) hinzuzufügen in "Promiscuous-Modus" (Portspiegelung) oder aktivieren Sie den Promiscuous-Modus auf einer vorhandenen Netzwerkkarte, um den gesamten Datenverkehr abzuhören. In Google Cloud erfordert das Hinzufügen einer neuen Netzwerkkarte das vollständige Herunterfahren einer VM, wodurch Warnungen ausgelöst werden, sodass Angreifer dies nicht unbemerkt tun können.

Darüber hinaus können NICs überhaupt nicht auf den Promiscuous-Modus eingestellt werden und lösen Warnungen in Google Cloud aus.

Architektur der Steuerebene

Alle Verwaltungsaktionen für Google Cloud NetApp Volumes werden über die API durchgeführt. Die in die GCP Cloud Console integrierte Verwaltung von Google Cloud NetApp Volumes verwendet auch die API von Google Cloud NetApp Volumes .

Identitäts- und Zugriffsverwaltung

Identitäts- und Zugriffsverwaltung("ICH BIN") ist ein Standarddienst, mit dem Sie die Authentifizierung (Anmeldungen) und Autorisierung (Berechtigungen) für Google Cloud-Projektinstanzen steuern können. Google IAM bietet einen vollständigen Prüfpfad für die Autorisierung und Entfernung von Berechtigungen. Derzeit bietet Google Cloud NetApp Volumes keine Überwachung der Steuerungsebene.

Übersicht über Autorisierungen/Berechtigungen

IAM bietet integrierte, granulare Berechtigungen für Google Cloud NetApp Volumes. Sie finden eine "vollständige Liste der detaillierten Berechtigungen hier".

IAM bietet außerdem zwei vordefinierte Rollen namens `netappcloudvolumes.admin` Und `netappcloudvolumes.viewer` . Diese Rollen können bestimmten Benutzern oder Dienstkonten zugewiesen werden.

Weisen Sie entsprechende Rollen und Berechtigungen zu, damit IAM-Benutzer Google Cloud NetApp Volumes verwalten können.

Beispiele für die Verwendung granularer Berechtigungen sind:

- Erstellen Sie eine benutzerdefinierte Rolle mit ausschließlich den Berechtigungen „Abrufen/Auflisten/Erstellen/Aktualisieren“, sodass Benutzer keine Volumes löschen können.
- Verwenden Sie eine benutzerdefinierte Rolle mit nur `snapshot.*` Berechtigungen zum Erstellen eines Dienstkontos, das zum Erstellen einer anwendungskonsistenten Snapshot-Integration verwendet wird.
- Erstellen Sie eine benutzerdefinierte Rolle zum Delegieren `volumereplication.*` für bestimmte Benutzer.

Dienstkonten

Um Google Cloud NetApp Volumes API-Aufrufe über Skripte oder "Terraform" müssen Sie ein Dienstkonto mit dem `roles/netappcloudvolumes.admin` Rolle. Sie können dieses Dienstkonto verwenden, um die JWT-Token zu generieren, die zur Authentifizierung von Google Cloud NetApp Volumes API-Anfragen auf zwei verschiedene Arten erforderlich sind:

- Generieren Sie einen JSON-Schlüssel und verwenden Sie Google APIs, um daraus ein JWT-Token abzuleiten. Dies ist der einfachste Ansatz, erfordert jedoch die manuelle Verwaltung der Geheimnisse (des JSON-Schlüssels).
- Verwenden "Identitätswechsel beim Dienstkonto" mit `roles/iam.serviceAccountTokenCreator` . Der Code (Skript, Terraform usw.) wird ausgeführt mit "Standardanmeldeinformationen für Anwendungen" und gibt sich als Dienstkonto aus, um dessen Berechtigungen zu erhalten. Dieser Ansatz spiegelt die bewährten Sicherheitspraktiken von Google wider.

Weitere Informationen sind "Erstellen Ihres Dienstkontos und Ihres privaten Schlüssels" in der Google Cloud-Dokumentation verfügbar.

Google Cloud NetApp Volumes API

Die Google Cloud NetApp Volumes API verwendet eine REST-basierte API und nutzt HTTPS (TLSv1.2) als zugrunde liegendes Netzwerkprotokoll. Die aktuelle API-Definition und Informationen zur Verwendung der API sind unter "Cloud Volumes-APIs in der Google Cloud-Dokumentation" zu finden.

Der API-Endpunkt wird von NetApp mithilfe der Standard-HTTPS-Funktionalität (TLSv1.2) betrieben und gesichert.

JWT-Token

Die Authentifizierung gegenüber der API erfolgt mit JWT-Bearer-Token("RFC-7519"). Gültige JWT-Token müssen mithilfe der Google Cloud IAM-Authentifizierung abgerufen werden. Dies muss durch Abrufen eines Tokens von IAM durch Bereitstellung eines JSON-Schlüssels für das Dienstkonto erfolgen.

Überwachungsprotokollierung

Derzeit sind keine für den Benutzer zugänglichen Prüfprotokolle der Steuerungsebene verfügbar.

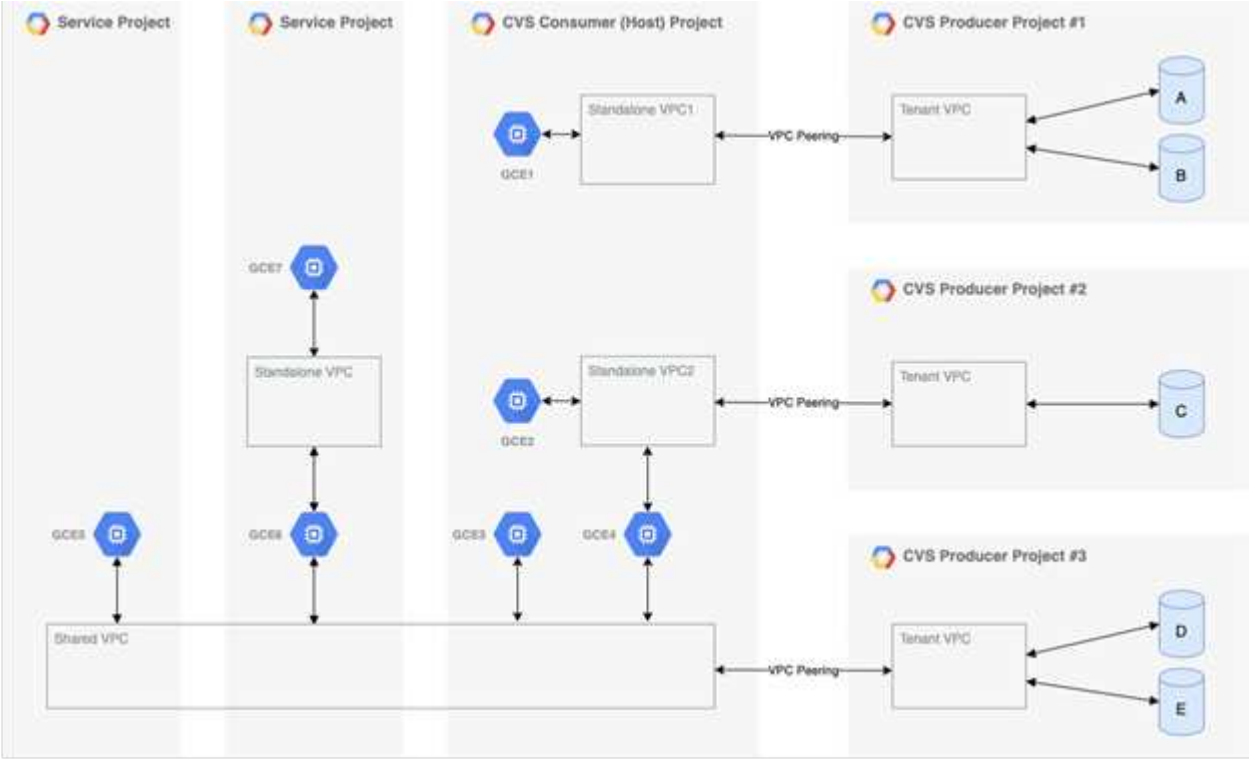
Datenebenenarchitektur

Google Cloud NetApp Volumes für Google Cloud nutzt die Google Cloud "Zugang zu privaten Diensten" Rahmen. In diesem Rahmen können Benutzer eine Verbindung zu

den Google Cloud NetApp Volumes herstellen. Dieses Framework verwendet Service Networking- und VPC-Peering-Konstrukte wie andere Google Cloud-Dienste und gewährleistet so eine vollständige Isolierung zwischen den Mandanten.

Eine Architekturübersicht von Google Cloud NetApp Volumes für Google Cloud ist unter "Architektur für Google Cloud NetApp Volumes" verfügbar.

Benutzer-VPCs (eigenständig oder gemeinsam genutzt) sind mit VPCs innerhalb von von Google Cloud NetApp Volumes verwalteten Mandantenprojekten verbunden, die die Volumes hosten.



Die obige Abbildung zeigt ein Projekt (das NetApp Volumes-Consumer-Projekt in der Mitte) mit drei VPC-Netzwerken, die mit Google Cloud NetApp Volumes verbunden sind, und mehreren Compute Engine-VMs (GCE1-7), die Volumes gemeinsam nutzen:

- VPC1 ermöglicht GCE1 den Zugriff auf die Volumes A und B.
- VPC2 ermöglicht GCE2 und GCE4 den Zugriff auf Volume C.
- Das dritte VPC-Netzwerk ist ein gemeinsam genutztes VPC, das von zwei Serviceprojekten gemeinsam genutzt wird. Es ermöglicht GCE3, GCE4, GCE5 und GCE6 den Zugriff auf die Volumes D und E. Gemeinsam genutzte VPC-Netzwerke werden nur für Volumes des Diensttyps „NetApp Volumes-Performance“ unterstützt.

GCE7 kann auf kein Volume zugreifen.

Daten können sowohl während der Übertragung (mithilfe von Kerberos- und/oder SMB-Verschlüsselung) als auch im Ruhezustand in Google Cloud NetApp Volumes verschlüsselt werden.

Datenverschlüsselung während der Übertragung

Während der Übertragung übertragene Daten können auf der NAS-Protokollebene

verschlüsselt werden, und das Google Cloud-Netzwerk selbst ist verschlüsselt, wie in den folgenden Abschnitten beschrieben.

Google Cloud-Netzwerk

Google Cloud verschlüsselt den Datenverkehr auf Netzwerkebene wie in "Verschlüsselung während der Übertragung" in der Google-Dokumentation. Wie im Abschnitt „Architektur von Google Cloud NetApp Volumes “ erwähnt, wird Google Cloud NetApp Volumes aus einem von NetApp gesteuerten PSA-Produzentenprojekt bereitgestellt.

Im Fall von NetApp Volumes-SW führt der Producer-Tenant Google-VMs aus, um den Dienst bereitzustellen. Der Datenverkehr zwischen Benutzer-VMs und Google Cloud NetApp Volumes -VMs wird automatisch von Google verschlüsselt.

Obwohl der Datenpfad für NetApp Volumes-Performance auf der Netzwerkebene nicht vollständig verschlüsselt ist, verwenden NetApp und Google eine Kombination "der IEEE 802.1AE-Verschlüsselung (MACSec)" , "Verkapselung" (Datenverschlüsselung) und physisch eingeschränkte Netzwerke zum Schutz von Daten während der Übertragung zwischen dem Diensttyp „NetApp Google Cloud NetApp Volumes und Google Cloud.

NAS-Protokolle

NFS- und SMB-NAS-Protokolle bieten optionale Transportverschlüsselung auf Protokollebene.

SMB-Verschlüsselung

"SMB-Verschlüsselung"bietet eine End-to-End-Verschlüsselung von SMB-Daten und schützt Daten vor Abhörmaßnahmen 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-/Domänencontroller-Authentifizierung aktivieren.

Wenn die SMB-Verschlüsselung aktiviert ist, können Clients, die keine Verschlüsselung unterstützen, nicht auf die Freigabe zugreifen.

Google Cloud NetApp Volumes unterstützt die Sicherheitschiffren RC4-HMAC, AES-128-CTS-HMAC-SHA1 und AES-256-CTS-HMAC-SHA1 für die SMB-Verschlüsselung. SMB handelt den höchsten vom Server unterstützten Verschlüsselungstyp aus.

NFSv4.1 Kerberos

Für NFSv4.1 bietet NetApp Volumes-Performance Kerberos-Authentifizierung wie in "RFC7530" Sie können Kerberos auf Volume-Basis aktivieren.

Der derzeit stärkste verfügbare Verschlüsselungstyp für Kerberos ist AES-256-CTS-HMAC-SHA1. Google Cloud NetApp Volumes 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-Verkehr, aber nicht für NFS.

Kerberos bietet drei verschiedene Sicherheitsstufen für NFS-Mounts, die Auswahlmöglichkeiten für die Stärke der Kerberos-Sicherheit bieten.

Laut RedHat "Gängige Montageoptionen" 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.
```

Als allgemeine Regel gilt: Je mehr die Kerberos-Sicherheitsebene leisten muss, desto schlechter ist die Leistung, da Client und Server Zeit mit dem Ver- und Entschlüsseln von NFS-Operationen für jedes gesendete Paket verbringen. Viele Clients und NFS-Server unterstützen die Auslagerung von AES-NI auf die CPUs, um ein besseres Gesamterlebnis zu erzielen. Allerdings sind die Auswirkungen von Kerberos 5p (vollständige End-to-End-Verschlüsselung) auf die Leistung deutlich größer als die Auswirkungen von Kerberos 5 (Benutzerauthentifizierung).

Die folgende Tabelle zeigt die Unterschiede zwischen den einzelnen Ebenen in Bezug auf Sicherheit und Leistung.

Sicherheitsstufe	Sicherheit	Performance
NFSv3 – sys	• Am wenigsten sicher; Klartext mit numerischen Benutzer-IDs/Gruppen-IDs • Kann UID, GID, Client-IP-Adressen, Exportpfade, Dateinamen und Berechtigungen in Paketerfassungen anzeigen	• Am besten für die meisten Fälle
NFSv4.x – sys	• Sicherer als NFSv3 (Client-IDs, Übereinstimmung von Namenszeichenfolge und Domänenzeichenfolge), aber immer noch Klartext • Kann UID, GID, Client-IP-Adressen, Namenszeichenfolgen, Domänen-IDs, Exportpfade, Dateinamen und Berechtigungen in Paketerfassungen anzeigen	• Gut für sequenzielle Workloads (wie VMs, Datenbanken, große Dateien) • Schlecht bei hoher Dateianzahl/hohen Metadaten (30–50 % schlechter)

Sicherheitsstufe	Sicherheit	Performance
NFS – krb5	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – verpackt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Der Benutzer, der Zugriff auf die Bereitstellung anfordert, benötigt ein gültiges Kerberos-Ticket (entweder über Benutzername/Passwort oder manuellen Schlüssel-Tab-Austausch). Das Ticket läuft nach einer bestimmten Zeit ab und der Benutzer muss sich für den Zugriff erneut authentifizieren. • Keine Verschlüsselung für NFS-Operationen oder Zusatzprotokolle wie Mount/Portmapper/NLM (kann Exportpfade, IP-Adressen, Dateihandles, Berechtigungen, Dateinamen, Atime/Mtime in Paketerfassungen sehen)	• In den meisten Fällen am besten für Kerberos; schlechter als AUTH_SYS

Sicherheitsstufe	Sicherheit	Performance
NFS – krb5i	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – verpackt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Der Benutzer, der Zugriff auf die Bereitstellung anfordert, benötigt ein gültiges Kerberos-Ticket (entweder über Benutzername/Passwort oder manuellen Schlüssel-Tab-Austausch). Das Ticket läuft nach einer bestimmten Zeit ab und der Benutzer muss sich für den Zugriff erneut authentifizieren. • Keine Verschlüsselung für NFS-Operationen oder Zusatzprotokolle wie Mount/Portmapper/NLM (kann Exportpfade, IP-Adressen, Dateihandles, Berechtigungen, Dateinamen, Atime/Mtime in Paketerfassungen sehen) • Um sicherzustellen, dass die Pakete nicht abgefangen werden, wird jedem Paket eine Kerberos-GSS-Prüfsumme hinzugefügt. Wenn die Prüfsummen übereinstimmen, ist die Konversation zulässig.	• Besser als krb5p, da die NFS-Nutzlast nicht verschlüsselt ist; der einzige zusätzliche Aufwand im Vergleich zu krb5 ist die Integritätsprüfsumme. Die Leistung von krb5i wird nicht viel schlechter sein als die von krb5, es wird jedoch zu einer gewissen Verschlechterung kommen.

Sicherheitsstufe	Sicherheit	Performance
NFS – krb5p	• Kerberos-Verschlüsselung für Anmeldeinformationen in jedem NFS-Paket – verpackt UID/GID von Benutzern/Gruppen in RPC-Aufrufen in GSS-Wrapper • Der Benutzer, der Zugriff auf die Bereitstellung anfordert, benötigt ein gültiges Kerberos-Ticket (entweder über Benutzername/Passwort oder manuellen Keytab-Austausch). Das Ticket läuft nach einer bestimmten Zeitspanne ab und der Benutzer muss sich für den Zugriff erneut authentifizieren. • Alle Nutzdaten der NFS-Pakete werden mit dem GSS-Wrapper verschlüsselt (Dateihandles, Berechtigungen, Dateinamen, Atime/Mtime können in Paketerfassungen nicht angezeigt werden). • Beinhaltet eine Integritätsprüfung. • Der NFS-Operationstyp ist sichtbar (FSINFO, ACCESS, GETATTR usw.). • Zusatzprotokolle (Mount, Portmap, NLM usw.) sind nicht verschlüsselt – (Exportpfade und IP-Adressen sind sichtbar)	• Schlechteste Leistung der Sicherheitsstufen; krb5p muss mehr verschlüsseln/entschlüsseln. • Bessere Leistung als krb5p mit NFSv4.x bei Workloads mit hoher Dateianzahl.

In Google Cloud NetApp Volumes wird ein konfigurierter Active Directory-Server als Kerberos-Server und LDAP-Server verwendet (um Benutzeridentitäten aus einem RFC2307-kompatiblen Schema nachzuschlagen). Es werden keine anderen Kerberos- oder LDAP-Server unterstützt. NetApp empfiehlt dringend, LDAP für die Identitätsverwaltung in Google Cloud NetApp Volumes zu verwenden. Informationen dazu, wie NFS Kerberos in Paketerfassungen angezeigt wird, finden Sie im Abschnitt "Packet sniffing/trace considerations."

Datenverschlüsselung im Ruhezustand

Alle Volumes in Google Cloud NetApp Volumes werden im Ruhezustand mit AES-256-Verschlüsselung verschlüsselt. Dies bedeutet, dass alle auf Medien geschriebenen Benutzerdaten verschlüsselt sind und nur mit einem Schlüssel pro Volume entschlüsselt werden können.

- Für NetApp Volumes-SW werden von Google generierte Schlüssel verwendet.
- Für NetApp Volumes-Performance werden die Schlüssel pro Volume in einem in die Google Cloud NetApp Volumes integrierten Schlüsselmanager gespeichert.

Ab November 2021 wurde die Vorschaufunktion für kundenverwaltete Verschlüsselungsschlüssel (CMEK) verfügbar gemacht. Dadurch können Sie die Schlüssel pro Volume mit einem pro Projekt und pro Region gültigen Hauptschlüssel verschlüsseln, der in "Google Schlüsselverwaltungsdienst (KMS)." KMS ermöglicht Ihnen das Anschließen externer Schlüsselmanager.

Informationen zur Konfiguration von KMS für NetApp Volumes-Performance finden sich unter "Einrichten von kundenverwalteten Verschlüsselungsschlüsseln".

Firewall

Google Cloud NetApp Volumes stellt mehrere TCP-Ports bereit, um NFS- und SMB-Freigaben bereitzustellen:

- "Für den NFS-Zugriff erforderliche Ports"
- "Für den SMB-Zugriff erforderliche Ports"

Zusätzlich erfordern SMB, NFS mit LDAP einschließlich Kerberos und Dual-Protokoll-Konfigurationen Zugriff auf eine Windows Active Directory-Domäne. Active Directory-Verbindungen müssen "konfiguriert" pro Region eingerichtet werden. Active Directory-Domänencontroller (DCs) werden mithilfe von "DNS-basierte DC-Erkennung" unter Verwendung der angegebenen DNS-Server identifiziert. Alle zurückgegebenen DCs werden verwendet. Die Liste der infrage kommenden DCs kann durch die Angabe eines Active Directory-Standorts eingeschränkt werden.

Google Cloud NetApp Volumes greift mit IP-Adressen aus dem CIDR-Bereich zu, der mit dem `gcloud compute address` Befehl zugewiesen wurde, während "Onboarding der Google Cloud NetApp Volumes". Sie können diesen CIDR-Bereich als Quelladressen verwenden, um eingehende Firewalls für Ihre Active Directory-Domänencontroller zu konfigurieren.

Active Directory Domain Controllers müssen "Ports für die Google Cloud NetApp Volumes CIDRs verfügbar machen, wie hier erwähnt".

Übersicht über NAS-Protokolle

Zu den NAS-Protokollen gehören NFS (v3 und v4.1) und SMB/CIFS (2.x und 3.x). Mit diesen Protokollen ermöglicht NetApp Volumes den gemeinsamen Zugriff auf Daten über mehrere NAS-Clients hinweg. Darüber hinaus können Google Cloud NetApp Volumes gleichzeitig Zugriff auf NFS- und SMB/CIFS-Clients gewähren (Dual-Protokoll) und dabei alle Identitäts- und Berechtigungseinstellungen für Dateien und Ordner in den NAS-Freigaben berücksichtigen. Um die höchstmögliche Sicherheit bei der Datenübertragung zu gewährleisten, unterstützt Google Cloud NetApp Volumes die Protokollverschlüsselung während der Übertragung mithilfe von SMB-Verschlüsselung und NFS Kerberos 5p.

Dual-Protokoll ist nur mit NetApp Volumes-Performance verfügbar.

Grundlagen der NAS-Protokolle

NAS-Protokolle bieten mehreren Clients in einem Netzwerk die Möglichkeit, auf dieselben Daten auf einem Speichersystem zuzugreifen, beispielsweise Google Cloud NetApp Volumes auf GCP. NFS und SMB sind die definierten NAS-Protokolle und arbeiten auf

Client/Server-Basis, wobei Google Cloud NetApp Volumes als Server fungiert. Clients senden Zugriffs-, Lese- und Schreibanforderungen 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 verantwortlich.

Wenn ein NAS-Client beispielsweise eine neue Datei in einem Ordner erstellen möchte, wird der folgende allgemeine Prozess befolgt.

1. Der Client fordert vom Server Informationen zum Verzeichnis an (Berechtigungen, Eigentümer, Gruppe, Datei-ID, verfügbarer Speicherplatz usw.). Der Server antwortet mit den Informationen, wenn der anfordernde Client und der Benutzer über die erforderlichen Berechtigungen für den übergeordneten Ordner verfügen.
2. Wenn die Berechtigungen für das Verzeichnis den Zugriff erlauben, fragt der Client den Server, ob der zu erstellende Dateiname bereits im Dateisystem vorhanden ist. Wenn der Dateiname bereits verwendet wird, schlägt die Erstellung fehl. Wenn der Dateiname nicht vorhanden ist, teilt der Server dem Client mit, dass er fortfahren kann.
3. Der Client sendet einen Aufruf an den Server, um die Datei mit dem Verzeichnis-Handle und dem Dateinamen zu erstellen und legt die Zugriffs- und Änderungszeiten fest. Der Server weist der Datei eine eindeutige Datei-ID zu, um sicherzustellen, dass keine anderen Dateien mit derselben Datei-ID erstellt werden.
4. Der Client sendet einen Aufruf, um vor dem Schreibvorgang die Dateiattribute zu überprüfen. Wenn die Berechtigungen es zulassen, schreibt der Client dann die neue Datei. Wenn das Protokoll/die Anwendung eine Sperre verwendet, fordert der Client vom Server eine Sperre an, um zu verhindern, dass andere Clients auf die Datei zugreifen, während sie gesperrt ist, und um so eine Datenbeschädigung zu vermeiden.

NFS

NFS ist ein verteiltes Dateisystemprotokoll, das ein offener IETF-Standard ist, der in Request for Comments (RFC) definiert ist und es jedem ermöglicht, das Protokoll zu implementieren.

Volumes in Google Cloud NetApp Volumes werden an NFS-Clients weitergegeben, indem ein Pfad exportiert wird, auf den ein Client oder eine Gruppe von Clients zugreifen kann. Die Berechtigungen zum Mounten dieser Exporte werden durch Exportrichtlinien und -regeln definiert, die von den Administratoren von Google Cloud NetApp Volumes konfiguriert werden können.

Die NetApp NFS-Implementierung gilt als Goldstandard für das Protokoll und wird in zahllosen Enterprise-NAS-Umgebungen verwendet. In den folgenden Abschnitten werden NFS und bestimmte Sicherheitsfunktionen behandelt, die in Google Cloud NetApp Volumes verfügbar sind, und wie diese implementiert werden.

Standardmäßige lokale UNIX-Benutzer und -Gruppen

Google Cloud NetApp Volumes enthält mehrere standardmäßige UNIX-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 Google Cloud NetApp Volumes 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 und ihre entsprechenden numerischen IDs.

NetApp empfiehlt, keine neuen Benutzer oder Gruppen in LDAP oder auf den lokalen Clients zu erstellen, die diese numerischen IDs wiederverwenden.

Standardbenutzer: numerische IDs	Standardgruppen: numerische IDs
• Wurzel:0 • PC-Benutzer:65534 • niemand:65535	• Wurzel:0 • Dämon:1 • PC-Benutzer:65534 • niemand:65535

Bei Verwendung von NFSv4.1 wird der Root-Benutzer beim Ausführen von Verzeichnislistenbefehlen auf NFS-Clients möglicherweise als „Niemand“ angezeigt. Dies liegt an der ID-Domänenzuordnungskonfiguration des Clients. Siehe den Abschnitt mit dem TitelNFSv4.1 und der/die Niemand-Benutzer/Gruppe Weitere Informationen zu diesem Problem und seiner Lösung finden Sie unter.

Der Root-Benutzer

Unter Linux hat das Root-Konto Zugriff auf alle Befehle, Dateien und Ordner in einem Linux-basierten Dateisystem. Aufgrund der Macht dieses Kontos erfordern bewährte Sicherheitspraktiken häufig, dass der Root-Benutzer deaktiviert oder auf andere Weise eingeschränkt wird. Bei NFS-Exporten kann die Macht eines Root-Benutzers über die Dateien und Ordner in Google Cloud NetApp Volumes durch Exportrichtlinien und -regeln sowie ein als Root-Squash bekanntes Konzept gesteuert werden.

Durch Root-Squashing wird sichergestellt, dass der Root-Benutzer, der auf einen NFS-Mount zugreift, auf den anonymen numerischen Benutzer 65534 reduziert wird (siehe Abschnitt "Der anonyme Benutzer ") und ist derzeit nur verfügbar, wenn Sie NetApp Volumes-Performance verwenden und beim Erstellen der Exportrichtlinienregel „Aus“ für den Root-Zugriff auswählen. Wenn der Root-Benutzer zum anonymen Benutzer gequetscht wird, hat er keinen Zugriff mehr auf die Ausführung von chown oder "setuid/setgid-Befehle (der Sticky-Bit)" bei Dateien oder Ordnern im NFS-Mount und bei Dateien oder Ordnern, die vom Root-Benutzer erstellt wurden, wird die anonyme UID als Eigentümer/Gruppe angezeigt. 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 hat. Wenn Sie den Zugriff auf die Datei- und Ordnerberechtigungen eines Root-Benutzers einschränken möchten, sollten Sie ein Volume mit NTFS-ACLs verwenden und einen Windows-Benutzer mit dem Namen `root` und wenden Sie die gewünschten Berechtigungen auf die Dateien oder Ordner an.

Der anonyme Benutzer

Die anonyme (anon) Benutzer-ID gibt eine UNIX-Benutzer-ID oder einen Benutzernamen an, der Clientanforderungen zugeordnet wird, die ohne gültige NFS-Anmeldeinformationen eingehen. Dies kann den Root-Benutzer einschließen, wenn Root-Squashing verwendet wird. Der anonyme Benutzer in Google Cloud NetApp Volumes ist 65534.

Diese UID ist normalerweise mit dem Benutzernamen verknüpft `nobody` oder `nfsnobody` in Linux-Umgebungen. Google Cloud NetApp Volumes verwendet auch 65534 als lokalen UNIX-Benutzer `pcuser` (siehe Abschnitt "Standardmäßige lokale UNIX-Benutzer und -Gruppen "), der auch der standardmäßige Fallback-Benutzer für die Zuordnung von Windows-zu-UNIX-Namen ist, wenn in LDAP kein gültiger passender UNIX-Benutzer gefunden werden kann.

Aufgrund der Unterschiede bei den Benutzernamen zwischen Linux und Google Cloud NetApp Volumes für UID 65534 stimmt die Namenszeichenfolge für Benutzer, die 65534 zugeordnet sind, bei Verwendung von NFSv4.1 möglicherweise nicht überein. Als Ergebnis sehen Sie möglicherweise `nobody` als Benutzer auf

einigen Dateien und Ordnern. Siehe Abschnitt "NFSv4.1 und der/die Niemand-Benutzer/Gruppe " für Informationen zu diesem Problem und seiner Lösung.

Zugriffskontrolle/Exporte

Der anfängliche Export-/Freigabezugriff für NFS-Mounts wird durch hostbasierte Exportrichtlinienregeln gesteuert, die in einer Exportrichtlinie enthalten sind. Um den Zugriff zum Mounten der NFS-Freigabe zu ermöglichen, wird eine Host-IP, ein Hostname, ein Subnetz, eine Netzgruppe oder eine Domäne sowie die für den Host zulässige Zugriffsebene definiert. Die Konfigurationsoptionen für Exportrichtlinienregeln hängen von der Google Cloud NetApp Volumes -Ebene ab.

Für NetApp Volumes-SW stehen die folgenden Optionen für die Exportrichtlinienkonfiguration zur Verfügung:

- **Client-Übereinstimmung.** Durch Kommas getrennte Liste von IP-Adressen, durch Kommas getrennte Liste von Hostnamen, Subnetzen, Netzgruppen, Domänennamen.
- **RO/RW-Zugriffsregeln.** Wählen Sie „Lesen/Schreiben“ oder „Nur Lesen“, um die Zugriffsebene für den Export zu steuern. NetApp Volumes-Performance bietet die folgenden Optionen:
- **Client-Übereinstimmung.** Durch Kommas getrennte Liste von IP-Adressen, durch Kommas getrennte Liste von Hostnamen, Subnetzen, Netzgruppen, Domänennamen.
- **RO/RW-Zugriffsregeln.** Wählen Sie „Lesen/Schreiben“ oder „Nur Lesen“, um die Zugriffsebene für den Export zu steuern.
- **Root-Zugriff (ein/aus).** Konfiguriert Root Squash (siehe Abschnitt "Der Root-Benutzer " für Details).
- **Protokolltyp.** Dadurch wird der Zugriff auf die NFS-Einbindung auf eine bestimmte Protokollversion beschränkt. 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 krb5, krb5i und/oder krb5p für schreibgeschützten oder Lese-/Schreibzugriff.

Eigentümerschaft ändern (chown) und Gruppe ändern (chgrp)

NFS auf Google Cloud NetApp Volumes erlaubt dem Root-Benutzer nur, chown/chgrp auf Dateien und Ordnern auszuführen. Andere Benutzer sehen eine `Operation not permitted` Fehler – sogar bei Dateien, die ihnen gehören. Wenn Sie Wurzelkürbis verwenden (wie im Abschnitt "Der Root-Benutzer "), wird der Root zu einem Nicht-Root-Benutzer reduziert und erhält keinen Zugriff auf chown und chgrp. Derzeit gibt es in Google Cloud NetApp Volumes keine Problemumgehungen, um chown und chgrp für Nicht-Root-Benutzer zuzulassen. Wenn Eigentümerwechsel erforderlich sind, sollten Sie die Verwendung von Dualprotokoll-Volumes in Betracht ziehen und den Sicherheitsstil auf NTFS festlegen, um die Berechtigungen von der Windows-Seite aus zu steuern.

Berechtigungsverwaltung

Google Cloud NetApp Volumes unterstützt sowohl Modusbits (wie 644, 777 usw. für rwx) als auch NFSv4.1-ACLs, um Berechtigungen auf NFS-Clients für Volumes zu steuern, die den UNIX-Sicherheitsstil verwenden. Hierfür wird die Standardberechtigungsverwaltung verwendet (z. B. chmod, chown oder nfs4_setfacl) und sie funktionieren mit jedem Linux-Client, der sie unterstützt.

Darüber hinaus können NFS-Clients bei der Verwendung von auf NTFS eingestellten Dual-Protocol-Volumes die Namenszuordnung von Google Cloud NetApp Volumes zu Windows-Benutzern nutzen, die dann zum Auflösen der NTFS-Berechtigungen verwendet werden. Dies erfordert eine LDAP-Verbindung zu Google Cloud NetApp Volumes, um die Übersetzung von numerischen IDs in Benutzernamen zu ermöglichen, da Google Cloud NetApp Volumes einen gültigen UNIX-Benutzernamen benötigt, um eine korrekte Zuordnung zu einem Windows-Benutzernamen zu ermöglichen.

Bereitstellung granularer ACLs für NFSv3

Modusbitberechtigungen decken in der Semantik nur den Besitzer, die Gruppe und alle anderen ab. Das bedeutet, dass für das grundlegende NFSv3 keine granularen Benutzerzugriffskontrollen vorhanden sind. Google Cloud NetApp Volumes unterstützt weder POSIX-ACLs noch erweiterte Attribute (wie etwa chattr), daher sind granulare ACLs nur in den folgenden Szenarien mit NFSv3 möglich:

- Volumes im NTFS-Sicherheitsstil (CIFS-Server erforderlich) mit gültigen UNIX-zu-Windows-Benutzerzuordnungen.
- NFSv4.1-ACLs wurden mithilfe eines Admin-Clients angewendet, der NFSv4.1 mountet, um ACLs anzuwenden.

Beide Methoden erfordern eine LDAP-Verbindung für die UNIX-Identitätsverwaltung und gültige UNIX-Benutzer- und Gruppeninformationen (siehe Abschnitt"LDAP") und sind nur mit NetApp Volumes-Performance-Instanzen verfügbar. Um Volumes im NTFS-Sicherheitsstil mit NFS zu verwenden, müssen Sie ein Dualprotokoll (SMB und NFSv3) oder ein Dualprotokoll (SMB und NFSv4.1) verwenden, auch wenn keine SMB-Verbindungen hergestellt werden. Um NFSv4.1-ACLs mit NFSv3-Mounts zu verwenden, müssen Sie `Both (NFSv3/NFSv4.1)` als Protokolltyp.

Reguläre UNIX-Modusbits bieten nicht die gleiche Granularität bei den Berechtigungen wie NTFS- oder NFSv4.x-ACLs. Die folgende Tabelle vergleicht die Berechtigungsgranularität zwischen NFSv3-Modusbits und NFSv4.1-ACLs. Informationen zu NFSv4.1-ACLs finden Sie unter "nfs4_acl – NFSv4-Zugriffskontrolllisten" .

NFSv3-Modusbits	NFSv4.1-ACLs
• Benutzer-ID bei Ausführung festlegen • Gruppen-ID bei Ausführung festlegen • Ausgetauschten Text speichern (nicht in POSIX definiert) • Leseberechtigung für Besitzer • Schreibberechtigung für Eigentümer • Ausführen der Berechtigung für den Eigentümer einer Datei; oder Suchen der Berechtigung für den Eigentümer im Verzeichnis • Leseberechtigung für die Gruppe • Schreibberechtigung für die Gruppe • Ausführen der Berechtigung für eine Gruppe auf einer Datei; oder Suchen der Berechtigung für eine Gruppe im Verzeichnis • Leseberechtigung für andere • Schreibberechtigung für andere • Ausführen von Berechtigungen für andere auf einer Datei; oder Suchen nach Berechtigungen für andere im Verzeichnis	Typen von Zugriffskontrolleinträgen (ACE) (Zulassen/Verweigern/Überwachen) * Vererbungsflags * Verzeichnis-vererben * Datei-vererben * Keine-Propagierung-vererben * Nur-vererben Berechtigungen * Daten lesen (Dateien) / Verzeichnis auflisten (Verzeichnisse) * Daten schreiben (Dateien) / Datei erstellen (Verzeichnisse) * Daten anhängen (Dateien) / Unterverzeichnis erstellen (Verzeichnisse) * Ausführen (Dateien) / Verzeichnis ändern (Verzeichnisse) * Löschen * Untergeordnetes Element löschen * Attribute lesen * Attribute schreiben * Benannte Attribute lesen * Benannte Attribute schreiben * ACL lesen * ACL schreiben * Besitzer schreiben * Synchronisieren

Schließlich ist die NFS-Gruppenmitgliedschaft (sowohl in NFSv3 als auch in NFSV4.x) gemäß den RPC-Paketlimits auf ein Standardmaximum von 16 für AUTH_SYS begrenzt. NFS Kerberos bietet bis zu 32 Gruppen und NFSv4-ACLs heben die Einschränkung durch granulare Benutzer- und Gruppen-ACLs auf (bis zu 1024 Einträge pro ACE).

Zusätzlich bietet Google Cloud NetApp Volumes erweiterte Gruppenunterstützung, um die maximal unterstützte Anzahl von Gruppen auf 32 zu erhöhen. Dies erfordert eine LDAP-Verbindung zu einem LDAP-Server, der gültige UNIX-Benutzer- und Gruppenidentitäten enthält. Weitere Informationen zur Konfiguration sind "Erstellen und Verwalten von NFS-Volumes" in der Google-Dokumentation verfügbar.

NFSv3-Benutzer- und Gruppen-IDs

NFSv3-Benutzer- und Gruppen-IDs werden als numerische IDs und nicht als Namen über die Leitung übertragen. Google Cloud NetApp Volumes führt für diese numerischen IDs mit NFSv3 keine Benutzernamenauflösung durch, wobei Volumes im UNIX-Sicherheitsstil nur Modusbits verwenden. Wenn NFSv4.1-ACLs vorhanden sind, ist eine numerische ID-Suche und/oder eine Namenszeichenfolgensuche erforderlich, um die ACL ordnungsgemäß aufzulösen – auch bei Verwendung von NFSv3. Bei Volumes im NTFS-Sicherheitsstil müssen Google Cloud NetApp Volumes eine numerische ID in einen gültigen UNIX-Benutzer auflösen und dann einem gültigen Windows-Benutzer zuordnen, um Zugriffsrechte auszuhandeln.

Sicherheitsbeschränkungen von NFSv3-Benutzer- und Gruppen-IDs

Bei NFSv3 müssen Client und Server nie bestätigen, dass der Benutzer, der mit einer numerischen ID einen Lese- oder Schreibvorgang versucht, ein gültiger Benutzer ist; ihm wird einfach implizit vertraut. Dadurch wird das Dateisystem durch das einfache Fälschen einer beliebigen numerischen ID für potenzielle Sicherheitsverletzungen anfällig. Um Sicherheitslücken wie diese zu vermeiden, stehen Google Cloud NetApp Volumes einige Optionen zur Verfügung.

- Durch die Implementierung von Kerberos für NFS werden Benutzer gezwungen, sich mit einem Benutzernamen und Kennwort oder einer Keytab-Datei zu authentifizieren, um ein Kerberos-Ticket zu erhalten, das den Zugriff auf einen Mount ermöglicht. Kerberos ist mit NetApp Volumes-Performance-Instanzen und nur mit NFSv4.1 verfügbar.
- Durch die Einschränkung der Hostliste in Ihren Exportrichtlinienregeln wird eingeschränkt, welche NFSv3-Clients Zugriff auf das Google Cloud NetApp Volumes -Volume haben.
- Durch die Verwendung von Dual-Protokoll-Volumes und die Anwendung von NTFS-ACLs auf das Volume werden NFSv3-Clients gezwungen, numerische IDs in gültige UNIX-Benutzernamen aufzulösen, um sich für den Zugriff auf Mounts ordnungsgemäß zu authentifizieren. Dazu müssen LDAP aktiviert und UNIX-Benutzer- und Gruppenidentitäten konfiguriert werden.
- Durch das Unterdrücken des Root-Benutzers wird der Schaden begrenzt, den ein Root-Benutzer an einer NFS-Einbindung anrichten kann, das Risiko wird jedoch nicht vollständig beseitigt. Weitere Informationen finden Sie im Abschnitt "Der Root-Benutzer ."

Letztendlich ist die NFS-Sicherheit auf das beschränkt, was die von Ihnen verwendete Protokollversion bietet. NFSv3 ist zwar im Allgemeinen leistungsfähiger als NFSv4.1, bietet jedoch nicht das gleiche Maß an Sicherheit.

NFSv4.1

NFSv4.1 bietet im Vergleich zu NFSv3 aus folgenden Gründen mehr Sicherheit und Zuverlässigkeit:

- Integrierte Sperrung durch einen leasingbasierten Mechanismus
- Zustandsbehaftete Sitzungen
- Alle NFS-Funktionen über einen einzigen Port (2049)
- Nur TCP
- ID-Domänenzuordnung
- Kerberos-Integration (NFSv3 kann Kerberos verwenden, aber nur für NFS, nicht für Zusatzprotokolle wie

NLM)

NFSv4.1-Abhängigkeiten

Aufgrund der zusätzlichen Sicherheitsfunktionen in NFSv4.1 sind einige externe Abhängigkeiten beteiligt, die für die Verwendung von NFSv3 nicht erforderlich waren (ähnlich wie SMB Abhängigkeiten wie Active Directory erfordert).

NFSv4.1-ACLs

Google Cloud NetApp Volumes bietet Unterstützung für NFSv4.x-ACLs, die gegenüber normalen Berechtigungen im POSIX-Stil deutliche Vorteile bieten, beispielsweise die folgenden:

- Granulare Kontrolle des Benutzerzugriffs auf Dateien und Verzeichnisse
- Bessere NFS-Sicherheit
- Verbesserte Interoperabilität mit CIFS/SMB
- Aufhebung der NFS-Beschränkung von 16 Gruppen pro Benutzer mit AUTH_SYS-Sicherheit
- ACLs umgehen die Notwendigkeit der Gruppen-ID-Auflösung (GID), wodurch die GID-Beschränkung effektiv aufgehoben wird. ACLs von NFSv4.1 werden von NFS-Clients gesteuert, nicht von Google Cloud NetApp Volumes. Um NFSv4.1-ACLs zu verwenden, stellen Sie sicher, dass die Softwareversion Ihres Clients diese 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), verfügen jedoch über ähnliche Funktionen. Wenn in Multiprotokoll-NAS-Umgebungen jedoch NFSv4.1-ACLs vorhanden sind und Sie einen Dualprotokoll-Zugriff (NFS und SMB auf denselben Datensätzen) verwenden, können Clients, die SMB2.0 und höher verwenden, ACLs nicht über die Windows-Sicherheitsregisterkarten anzeigen oder verwalten.

Funktionsweise von NFSv4.1-ACLs

Zur Referenz werden die folgenden Begriffe definiert:

- **Zugriffskontrollliste (ACL).** Eine Liste mit Berechtigungseinträgen.
- **Zugangskontrolle (ACE).** Ein Berechtigungseintrag in der Liste.

Wenn ein Client während eines SETATTR-Vorgangs eine NFSv4.1-ACL für eine Datei festlegt, legt Google Cloud NetApp Volumes diese ACL für das Objekt fest und ersetzt dabei alle vorhandenen ACLs. Wenn für eine Datei keine ACL vorhanden ist, werden die Modusberechtigungen für die Datei aus OWNER@, GROUP@ und EVERYONE@ berechnet. Wenn in der Datei bereits SUID/SGID/STICKY-Bits vorhanden sind, sind diese nicht betroffen.

Wenn ein Client im Verlauf eines GETATTR-Vorgangs eine NFSv4.1-ACL für eine Datei erhält, liest Google Cloud NetApp Volumes 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 Modusbits verfügt, wird aus den Modusbits eine ACL erstellt und an den Client zurückgegeben.

Der Zugriff wird verweigert, wenn in der ACL ein DENY ACE vorhanden ist; der Zugriff wird gewährt, wenn ein ALLOW ACE vorhanden ist. Der Zugriff wird jedoch auch verweigert, wenn keiner der ACEs in der ACL vorhanden ist.

Ein Sicherheitsdeskriptor besteht aus einer Sicherheits-ACL (SACL) und einer diskretionären ACL (DACL). Wenn NFSv4.1 mit CIFS/SMB interoperiert, wird die DACL eins zu eins mit NFSv4 und CIFS abgebildet. Die DACL besteht aus den ACEs ALLOW und DENY.

Wenn eine grundlegende `chmod` wird auf einer Datei oder einem Ordner mit festgelegten NFSv4.1-ACLs ausgeführt. Vorhandene Benutzer- und Gruppen-ACLs bleiben erhalten, die Standard-ACLs OWNER@, GROUP@ und EVERYONE@ werden jedoch 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 neues Unterverzeichnis in einem Verzeichnis mit einer ACL erstellt wird, erbt dieses Objekt alle ACEs in der ACL, die mit dem entsprechenden Tag versehen wurden. "Vererbungsflags" .

Wenn eine Datei oder ein Verzeichnis über eine NFSv4.1-ACL verfügt, wird diese ACL zur Zugriffskontrolle verwendet, unabhängig davon, welches Protokoll für den Zugriff auf die Datei oder das Verzeichnis verwendet wird.

Dateien und Verzeichnisse erben ACEs von NFSv4-ACLs auf übergeordneten Verzeichnissen (möglicherweise mit entsprechenden Änderungen), solange die ACEs mit den richtigen Vererbungsflags markiert wurden.

Wenn eine Datei oder ein Verzeichnis als Ergebnis einer NFSv4-Anforderung erstellt wird, hängt die ACL für die resultierende Datei oder das resultierende Verzeichnis davon ab, ob die Anforderung zur Dateierstellung 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 hat, wird der Client-Dateimodus verwendet, um standardmäßige UNIX-Dateizugriffsberechtigungen festzulegen.
- Wenn die Anforderung nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält und das übergeordnete Verzeichnis über eine nicht vererbbare ACL verfügt, wird für das neue Objekt eine Standard-ACL basierend auf den in der Anforderung übergebenen Modusbits festgelegt.
- Wenn die Anforderung nur standardmäßige UNIX-Dateizugriffsberechtigungen enthält, das übergeordnete Verzeichnis jedoch über eine ACL verfügt, werden die ACEs in der ACL des übergeordneten Verzeichnisses von der neuen Datei oder dem neuen Verzeichnis übernommen, sofern die ACEs mit den entsprechenden Vererbungsflags gekennzeichnet wurden.

ACE-Berechtigungen

NFSv4.1 ACLs-Berechtigungen verwenden eine Reihe von Groß- und Kleinbuchstaben (wie z. B. `rxtncy`), um den Zugriff zu steuern. Weitere Informationen zu diesen Buchstabenwerten finden Sie unter "SO WIRD'S GEMACHT: Verwenden der NFSv4-ACL" .

NFSv4.1 ACL-Verhalten mit umask und ACL-Vererbung

"NFSv4-ACLs bieten die Möglichkeit, ACL-Vererbung anzubieten" . ACL-Vererbung bedeutet, dass Dateien oder Ordner, die unter Objekten mit festgelegten NFSv4.1-ACLs erstellt wurden, die ACLs basierend auf der Konfiguration des "ACL-Vererbungsflag" .

"Umask"wird verwendet, um die Berechtigungsstufe zu steuern, auf der Dateien und Ordner in einem Verzeichnis ohne Administratorinteraktion erstellt werden. Standardmäßig erlaubt Google Cloud NetApp Volumes umask, geerbte ACLs zu überschreiben, was gemäß "RFC 5661" .

ACL-Formatierung

NFSv4.1-ACLs haben eine bestimmte Formatierung. Das folgende Beispiel ist ein ACE-Satz für eine Datei:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

Das obige Beispiel folgt den folgenden ACL-Formatrichtlinien:

```
type:flags:principal:permissions
```

Eine Art von `A` bedeutet „erlauben“. Die Vererbungsflags werden in diesem Fall nicht gesetzt, da der Auftraggeber keine Gruppe ist und keine Vererbung beinhaltet. Da es sich bei dem ACE nicht um einen AUDIT-Eintrag handelt, ist es auch nicht erforderlich, die Audit-Flags festzulegen. 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 vom Client und Server nicht aufgelöst werden kann), verhält sich die ACL möglicherweise nicht wie erwartet oder die ACL-Änderung kann nicht angewendet werden und es tritt ein Fehler auf.

Zu den Beispielfehlern gehören:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

Explizites VERWEIGERN

NFSv4.1-Berechtigungen können explizite DENY-Attribute für OWNER, GROUP und EVERYONE enthalten. Dies liegt daran, dass NFSv4.1-ACLs standardmäßig verweigert werden. Dies bedeutet, dass eine ACL verweigert wird, wenn sie nicht explizit durch einen ACE gewährt wird. Explizite DENY-Attribute überschreiben alle ACCESS ACEs, ob explizit oder nicht.

DENY ACEs werden mit einem Attribut-Tag von `D` .

Im folgenden Beispiel werden GROUP@ alle Lese- und Ausführungsberechtigungen gewährt, jedoch jeglicher Schreibzugriff 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 nach Möglichkeit vermieden werden, da sie verwirrend und kompliziert sein können;

ALLOW-ACLs, die nicht explizit definiert sind, werden implizit abgelehnt. Wenn DENY ACEs festgelegt sind, kann Benutzern der Zugriff verweigert werden, obwohl sie damit rechnen, dass ihnen der Zugriff gewährt wird.

Der vorhergehende Satz von ACEs entspricht 755 Modusbits, was bedeutet:

- Der Eigentümer hat alle Rechte.
- Gruppen haben nur Lesezugriff.
- Andere haben nur gelesen.

Selbst wenn die Berechtigungen auf das Äquivalent von 775 angepasst werden, kann der Zugriff jedoch aufgrund der expliziten Einstellung DENY für EVERYONE verweigert werden.

NFSv4.1 ID-Domänenzuordnungsabhängigkeiten

NFSv4.1 nutzt die ID-Domänenzuordnungslogik als Sicherheitsebene, um zu überprüfen, ob ein Benutzer, der versucht, auf eine NFSv4.1-Einbindung zuzugreifen, tatsächlich derjenige ist, der er vorgibt zu sein. In diesen Fällen wird dem Benutzernamen und Gruppennamen vom NFSv4.1-Client eine Namenszeichenfolge angehängt und diese an die Google Cloud NetApp Volumes Instanz gesendet. Wenn die Kombination aus Benutzername/Gruppenname und ID-Zeichenfolge nicht übereinstimmt, wird der Benutzer und/oder die Gruppe auf den Standardbenutzer „nobody“ reduziert, der in der `/etc/idmapd.conf` Datei auf dem Client.

Diese ID-Zeichenfolge ist eine Voraussetzung für die ordnungsgemäße Einhaltung der Berechtigungen, insbesondere wenn NFSv4.1-ACLs und/oder Kerberos verwendet werden. Daher sind Abhängigkeiten von Nameservice-Servern wie LDAP-Servern erforderlich, um die Konsistenz zwischen Clients und Google Cloud NetApp Volumes für eine ordnungsgemäße Identitätsauflösung von Benutzer- und Gruppennamen sicherzustellen.

Google Cloud NetApp Volumes verwendet einen statischen Standard-ID-Domänennamenwert von `defaultv4iddomain.com` . NFS-Clients verwenden standardmäßig den DNS-Domänennamen für ihre ID-Domänennameneinstellungen, Sie können den ID-Domänennamen jedoch manuell anpassen in `/etc/idmapd.conf` .

Wenn LDAP in Google Cloud NetApp Volumes aktiviert ist, automatisiert Google Cloud NetApp Volumes die Änderung der NFS-ID-Domäne zu der für die Suchdomäne in DNS konfigurierten Domäne. Clients müssen nicht geändert werden, es sei denn, sie verwenden andere DNS-Domänensuchnamen.

Wenn Google Cloud NetApp Volumes einen Benutzernamen oder Gruppennamen in lokalen Dateien oder LDAP auflösen kann, wird die Domänenzeichenfolge verwendet und nicht übereinstimmende Domänen-IDs werden auf „Niemand“ gequetscht. Wenn Google Cloud NetApp Volumes 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 ordnungsgemäß auf (dies ähnelt dem Verhalten von NFSv3).

Ohne die NFSv4.1-ID-Domäne des Clients so zu ändern, dass sie mit der vom Google Cloud NetApp Volumes Volume verwendeten übereinstimmt, sehen Sie das folgende Verhalten:

- UNIX-Benutzer und -Gruppen mit lokalen Einträgen in Google Cloud NetApp Volumes (z. B. Root, wie in lokalen UNIX-Benutzern und -Gruppen definiert) werden auf den Wert „Nobody“ reduziert.
- UNIX-Benutzer und -Gruppen mit Einträgen in LDAP (wenn Google Cloud NetApp Volumes für die Verwendung von LDAP konfiguriert ist) werden auf „niemand“ zusammengefasst, wenn sich die DNS-Domänen zwischen NFS-Clients und Google Cloud NetApp Volumes unterscheiden.
- UNIX-Benutzer und -Gruppen ohne lokale Einträge oder LDAP-Einträge verwenden den numerischen ID-Wert und lösen ihn in den auf dem NFS-Client angegebenen Namen auf. Wenn auf dem Client kein Name vorhanden ist, wird nur die numerische ID angezeigt.

Im Folgenden sind die Ergebnisse des vorhergehenden Szenarios dargestellt:

```
# 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, sieht die gleiche Dateiliste folgendermaßen aus:

```
# 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 Problem und seiner Lösung finden Sie im Abschnitt „NFSv4.1 und der/die Niemand-Benutzer/Gruppe ."

Kerberos-Abhängigkeiten

Wenn Sie Kerberos mit NFS verwenden möchten, müssen Sie bei Google Cloud NetApp Volumes über Folgendes verfügen:

- Active Directory-Domäne für Kerberos Distribution Center-Dienste (KDC)
- Active Directory-Domäne mit Benutzer- und Gruppenattributen, die mit UNIX-Informationen für die LDAP-Funktionalität gefüllt sind (NFS Kerberos in Google Cloud NetApp Volumes erfordert für die ordnungsgemäße Funktionalität eine Zuordnung von Benutzer-SPN zu UNIX-Benutzer.)
- LDAP auf der Google Cloud NetApp Volumes Instanz aktiviert
- Active Directory-Domäne für DNS-Dienste

NFSv4.1 und der/die Niemand-Benutzer/Gruppe

Eines der häufigsten Probleme bei einer NFSv4.1-Konfiguration ist, wenn eine Datei oder ein Ordner in einer Liste mit `ls` als Eigentum der `user:group` Kombination aus `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 ist `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 zeigt die Datei zwar den richtigen Besitzer an, `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 `nfsnobody` Benutzer. Sie können sehen, wie ein NFS-Client jeden Benutzer sieht, indem Sie den `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 wird die `nobody` Benutzer ist der Standardbenutzer, der vom `idmapd.conf` Datei und kann als jeder beliebige Benutzer definiert werden.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Warum passiert das?

Da Sicherheit durch Namenszeichenfolgenzuordnung ein zentraler Grundsatz von NFSv4.1-Vorgängen ist, besteht das Standardverhalten bei einer nicht korrekten Übereinstimmung einer Namenszeichenfolge darin, den Benutzer auf einen Namen zu beschränken, der normalerweise keinen Zugriff auf Dateien und Ordner hat, die Benutzern 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 Groß- und Kleinschreibung eine Rolle spielen.

Wenn beispielsweise user1@CVSDEMO.LOCAL (uid 1234, gid 1234) auf einen Export zugreift, muss Google Cloud NetApp Volumes in der Lage sein, user1@CVSDEMO.LOCAL (uid 1234, gid 1234) zu finden. Wenn der Benutzer in Google Cloud NetApp Volumes USER1@CVSDEMO.LOCAL ist, stimmt dies nicht überein (USER1 in Großbuchstaben gegenüber user1 in Kleinbuchstaben). In vielen Fällen können Sie in der Nachrichtendatei auf dem Client Folgendes 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'
```

Client und Server müssen sich darüber einig sein, dass ein Benutzer tatsächlich der ist, der er vorgibt zu sein. Daher müssen Sie Folgendes überprüfen, um sicherzustellen, dass der Benutzer, den der Client sieht, über dieselben Informationen verfügt wie der Benutzer, den Google Cloud NetApp Volumes sieht.

- **NFSv4.x-ID-Domäne.** Kunde: `idmapd.conf` Datei; Google Cloud NetApp Volumes verwendet `defaultv4iddomain.com` und kann nicht manuell geändert werden. Bei Verwendung von LDAP mit NFSv4.1 ändert Google Cloud NetApp Volumes die ID-Domäne in die von der DNS-Suchdomäne verwendete Domäne, die mit der AD-Domäne identisch ist.
- **Benutzername und numerische IDs.** Dadurch wird bestimmt, wo der Client nach Benutzernamen sucht, und die Konfiguration des Name Service Switches wird genutzt – Client: `nsswitch.conf` und/oder lokale Passwd- und Gruppendateien; Google Cloud NetApp Volumes lässt hier keine Änderungen zu, fügt LDAP jedoch automatisch zur Konfiguration hinzu, wenn es aktiviert ist.
- **Gruppenname und numerische IDs.** Dadurch wird bestimmt, wo der Client nach Gruppennamen sucht, und die Konfiguration des Name Service Switches wird genutzt – Client: `nsswitch.conf` und/oder lokale Passwd- und Gruppendateien; Google Cloud NetApp Volumes lässt hier keine Änderungen zu, fügt LDAP jedoch automatisch zur Konfiguration hinzu, wenn es aktiviert ist.

In fast allen Fällen, wenn Sie sehen `nobody` In Benutzer- und Gruppenlisten von Clients liegt das Problem in der Übersetzung der Domänen-ID des Benutzer- oder Gruppennamens zwischen Google Cloud NetApp Volumes und dem NFS-Client. Um dieses Szenario zu vermeiden, verwenden Sie LDAP, um Benutzer- und Gruppeninformationen zwischen Clients und Google Cloud NetApp Volumes aufzulösen.

Anzeigen von Namens-ID-Zeichenfolgen für NFSv4.1 auf Clients

Wenn Sie NFSv4.1 verwenden, findet während NFS-Vorgängen eine Name-String-Zuordnung statt, wie zuvor beschrieben.

Neben der Verwendung `/var/log/messages` Um ein Problem mit NFSv4-IDs zu finden, können Sie die "nfsidmap -l" auf dem NFS-Client, um anzuzeigen, welche Benutzernamen der NFSv4-Domäne ordnungsgemäß zugeordnet wurden.

Dies ist beispielsweise die Ausgabe des Befehls, nachdem ein Benutzer, der vom Client und Google Cloud NetApp Volumes gefunden werden kann, auf ein 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 nicht richtig in die NFSv4.1-ID-Domäne abgebildet wird (in diesem Fall `netapp-user`) versucht, auf denselben Mount zuzugreifen und eine Datei berührt, werden sie 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` Die Ausgabe zeigt den Benutzer `pcuser` im Display, aber nicht `netapp-user` ; dies ist der anonyme Benutzer in unserer Exportrichtlinienregel(`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
```

KMU

"KMU" ist ein von Microsoft entwickeltes Netzwerkdateifreigabeprotokoll, das eine zentrale Benutzer-/Gruppenauthentifizierung, Berechtigungen, Sperren und Dateifreigabe für mehrere SMB Clients über ein Ethernet-Netzwerk bereitstellt. Dateien und Ordner werden Clients über Freigaben präsentiert, die mit verschiedenen Freigabeeigenschaften konfiguriert werden können und eine Zugriffskontrolle über Berechtigungen auf Freigabeebene bieten. SMB kann jedem Client bereitgestellt werden, der das Protokoll unterstützt, darunter Windows-, Apple- und Linux-Clients.

Google Cloud NetApp Volumes bietet Unterstützung für die SMB-Versionen 2.1 und 3.x des Protokolls.

Zugriffskontrolle/SMB-Freigaben

- Wenn ein Windows-Benutzername Zugriff auf das Google Cloud NetApp Volumes -Volume anfordert, sucht Google Cloud NetApp Volumes mithilfe der von den Google Cloud NetApp Volumes Administratoren konfigurierten Methoden nach einem UNIX-Benutzernamen.
- Wenn ein externer UNIX-Identitätsanbieter (LDAP) konfiguriert ist und die Windows-/UNIX-Benutzernamen identisch sind, werden die Windows-Benutzernamen 1:1 den UNIX-Benutzernamen zugeordnet, ohne dass

eine zusätzliche Konfiguration erforderlich ist. Wenn LDAP aktiviert ist, wird Active Directory zum Hosten dieser UNIX-Attribute für Benutzer- und Gruppenobjekte verwendet.

- Wenn Windows-Namen und UNIX-Namen nicht identisch sind, muss LDAP so konfiguriert werden, dass Google Cloud NetApp Volumes die LDAP-Namenszuordnungskonfiguration verwenden kann (siehe Abschnitt"Verwenden von LDAP für die asymmetrische Namenszuordnung").
- Wenn LDAP nicht verwendet wird, werden Windows SMB-Benutzer einem lokalen UNIX-Standardbenutzer namens `pcuser` in Google Cloud NetApp Volumes. Dies bedeutet, dass von Benutzern in Windows geschriebene Dateien, die auf `pcuser` UNIX-Besitz anzeigen als `pcuser` in Multiprotokoll-NAS-Umgebungen. `pcuser` hier ist effektiv die `nobody` Benutzer in Linux-Umgebungen (UID 65534).

Bei Bereitstellungen nur mit SMB ist die `pcuser` Die Zuordnung erfolgt zwar weiterhin, spielt jedoch keine Rolle, da die Windows-Benutzer- und Gruppeneigentümerschaft korrekt angezeigt wird und der NFS-Zugriff auf das Nur-SMB-Volume nicht zulässig ist. Darüber hinaus unterstützen reine SMB-Volumes nach ihrer Erstellung keine Konvertierung in NFS- oder Dualprotokoll-Volumes.

Windows nutzt Kerberos für die Benutzernamenauthentifizierung mit den Active Directory-Domänencontrollern, was einen Benutzernamen-/Passwortaustausch mit den AD-DCs erfordert, der sich außerhalb der Google Cloud NetApp Volumes -Instanz befindet. Die Kerberos-Authentifizierung wird verwendet, wenn `\\SERVERNAME` Der UNC-Pfad wird von den SMB-Clients verwendet und Folgendes gilt:

- DNS A/AAAA-Eintrag für SERVERNAME vorhanden
- Für SERVERNAME ist ein gültiger SPN für SMB/CIFS-Zugriff vorhanden

Wenn ein Google Cloud NetApp Volumes SMB-Volume erstellt wird, wird der Maschinenkontoname wie im Abschnitt definiert erstellt."So werden Google Cloud NetApp Volumes in Active Directory angezeigt." Dieser Computerkontoname wird auch zum SMB-Freigabezugriffspfad, da Google Cloud NetApp Volumes Dynamic DNS (DDNS) nutzt, um die erforderlichen A/AAAA- und PTR-Einträge in DNS und die erforderlichen SPN-Einträge auf dem Hauptkonto des Computers zu erstellen.

> Damit PTR-Einträge erstellt werden können, muss die Reverse-Lookup-Zone für die IP-Adresse der Google Cloud NetApp Volumes Instanz auf dem DNS-Server vorhanden sein.

Beispielsweise verwendet dieses Google Cloud NetApp Volumes Volume den folgenden UNC-Freigabepfad: `\\cvs-east- 433d.cvsdemo.local .`

In Active Directory sind dies die von Google Cloud NetApp Volumes 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 der DNS-Vorwärts-/Rückwärtssuche:

```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
```

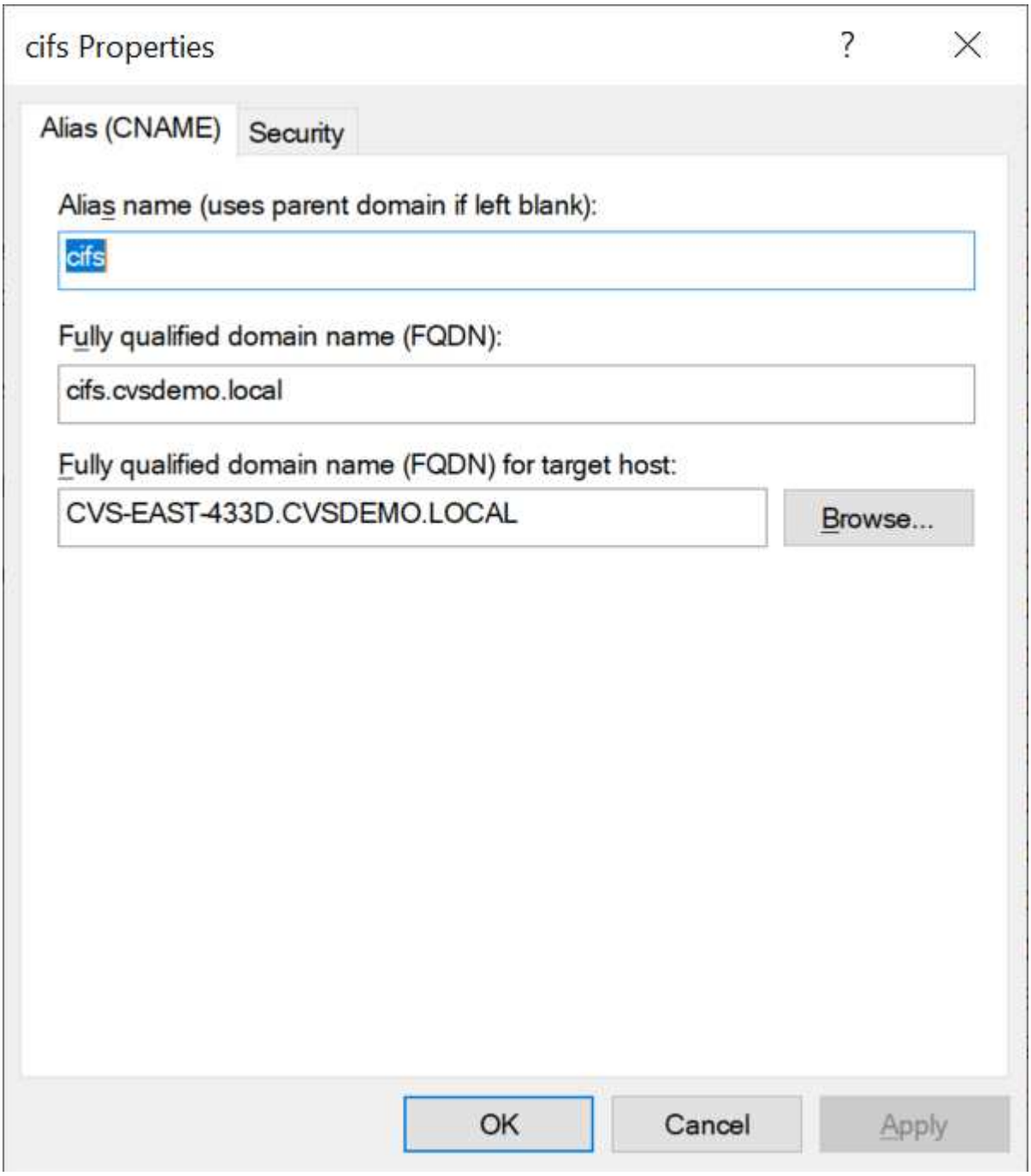
```
Address:  10.xx.0.xx
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Optional kann eine stärkere Zugriffskontrolle angewendet werden, indem die SMB-Verschlüsselung für SMB-Freigaben in Google Cloud NetApp Volumes aktiviert/erforderlich wird. Wenn die SMB-Verschlüsselung von einem der Endpunkte nicht unterstützt wird, ist der Zugriff nicht zulässig.

Verwenden von SMB-Namensaliasen

In einigen Fällen kann es für Endbenutzer ein Sicherheitsrisiko darstellen, den für Google Cloud NetApp Volumes verwendeten Computerkontonamen zu kennen. In anderen Fällen möchten Sie Ihren Endbenutzern möglicherweise einfach einen einfacheren Zugriffspfad bereitstellen. In diesen Fällen können Sie SMB-Aliase erstellen.

Wenn Sie Aliase für den SMB-Freigabepfad erstellen möchten, können Sie einen sogenannten CNAME-Eintrag im DNS nutzen. Wenn Sie beispielsweise den Namen `\\CIFS` um auf Freigaben zuzugreifen, anstatt `\\cvs-east- 433d.cvsdemo.local` , Sie möchten aber dennoch die Kerberos-Authentifizierung verwenden. Ein CNAME im DNS, der auf den vorhandenen A/AAAA-Eintrag verweist, und ein zusätzlicher SPN, der dem vorhandenen Computerkonto hinzugefügt wird, ermöglichen den Kerberos-Zugriff.



Dies ist das resultierende DNS-Forward-Lookup-Ergebnis 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:    NetApp Volumes-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
```

Bei einer Paketerfassung können wir die Sitzungseinrichtungsanforderung mithilfe des an den CNAME gebundenen SPN sehen.

```
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

Google Cloud NetApp Volumes unterstützt Folgendes "Dialekte" für die SMB-Authentifizierung:

- LM
- NTLM
- NTLMv2
- Kerberos

Die Kerberos-Authentifizierung für den SMB-Freigabezugriff ist die sicherste Authentifizierungsebene, die Sie verwenden können. Durch die aktivierte AES- und SMB-Verschlüsselung wird das Sicherheitsniveau weiter erhöht.

Google Cloud NetApp Volumes unterstützt auch die Abwärtskompatibilität für die LM- und NTLM-Authentifizierung. Wenn Kerberos falsch konfiguriert ist (z. B. beim Erstellen von SMB-Aliasen), wird beim Freigabezugriff auf schwächere Authentifizierungsmethoden (z. B. NTLMv2) zurückgegriffen. 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 Freigabezugriff fehl, da keine gültige Authentifizierungsmethode vorhanden ist, auf die zurückgegriffen werden kann.

Informationen zum Konfigurieren/Anzeigen Ihrer unterstützten Authentifizierungsebenen in Active Directory finden Sie unter "Netzwerksicherheit: LAN Manager-Authentifizierungsebene" .

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 `Basic` oder `Advanced` und kann eingestellt werden auf `Allow` oder `Deny` zur Zugangskontrolle.

Zu den grundlegenden Berechtigungen gehören die folgenden:

- Volle Kontrolle
- Ändern
- Lesen und Ausführen
- Lesen
- Schreiben

Wenn Sie Berechtigungen für einen Benutzer oder eine Gruppe festlegen (ein sogenannter ACE), befinden sich diese in einer ACL. NTFS-Berechtigungen verwenden dieselben Lese-/Schreib-/Ausführungsgrundlagen wie UNIX-Modusbits, können sich jedoch auch auf detailliertere und erweiterte Zugriffskontrollen (auch als Sonderberechtigungen bezeichnet) erstrecken, z. B. „Eigentümerschaft übernehmen“, „Ordner erstellen/Daten anhängen“, „Attribute schreiben“ und mehr.

Standardmäßige UNIX-Modusbits bieten nicht dieselbe Granularität wie NTFS-Berechtigungen (z. B. die Möglichkeit, Berechtigungen für einzelne Benutzer- und Gruppenobjekte in einer ACL festzulegen oder erweiterte Attribute festzulegen). NFSv4.1-ACLs bieten jedoch die gleiche Funktionalität wie NTFS-ACLs.

NTFS-Berechtigungen sind spezifischer als Freigabeberechtigungen und können in Verbindung mit Freigabeberechtigungen verwendet werden. Bei NTFS-Berechtigungsstrukturen gilt die restriktivste. Daher überschreibt die explizite Ablehnung eines Zugriffsrechts für einen Benutzer oder eine Gruppe sogar die Vollzugriffsberechtigung bei der Definition von Zugriffsrechten.

NTFS-Berechtigungen werden von Windows SMB-Clients gesteuert.

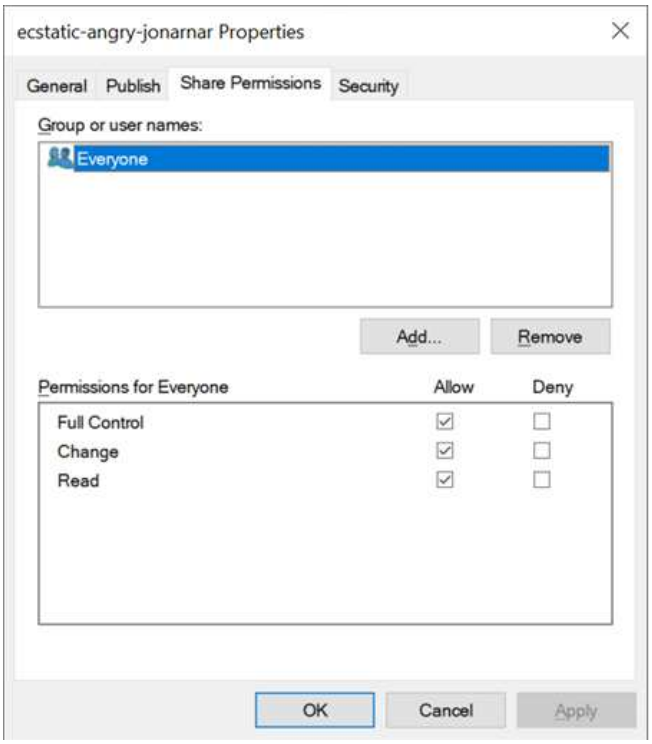
Freigabeberechtigungen

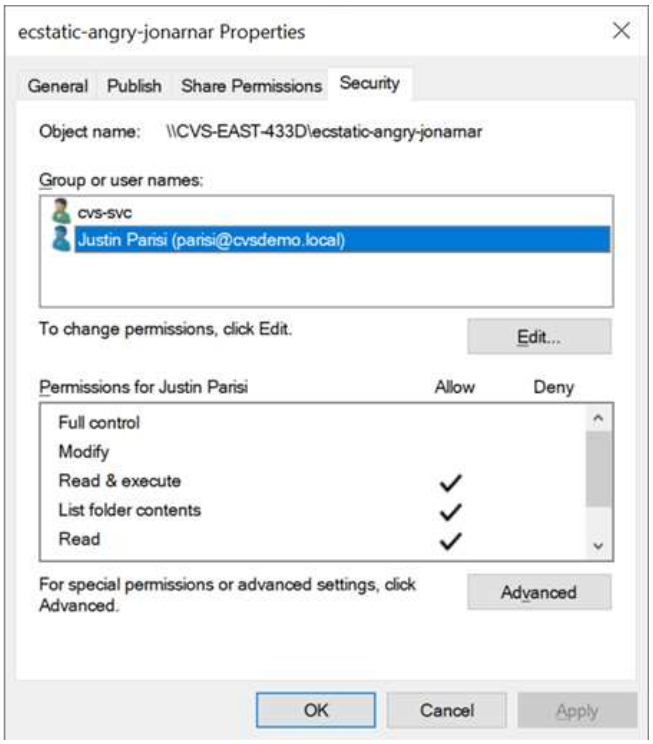
Freigabeberechtigungen sind allgemeiner als NTFS-Berechtigungen (nur Lesen/Ändern/Vollzugriff) und steuern den ersten Zugriff auf eine SMB-Freigabe – ähnlich wie NFS-Exportrichtlinienregeln funktionieren.

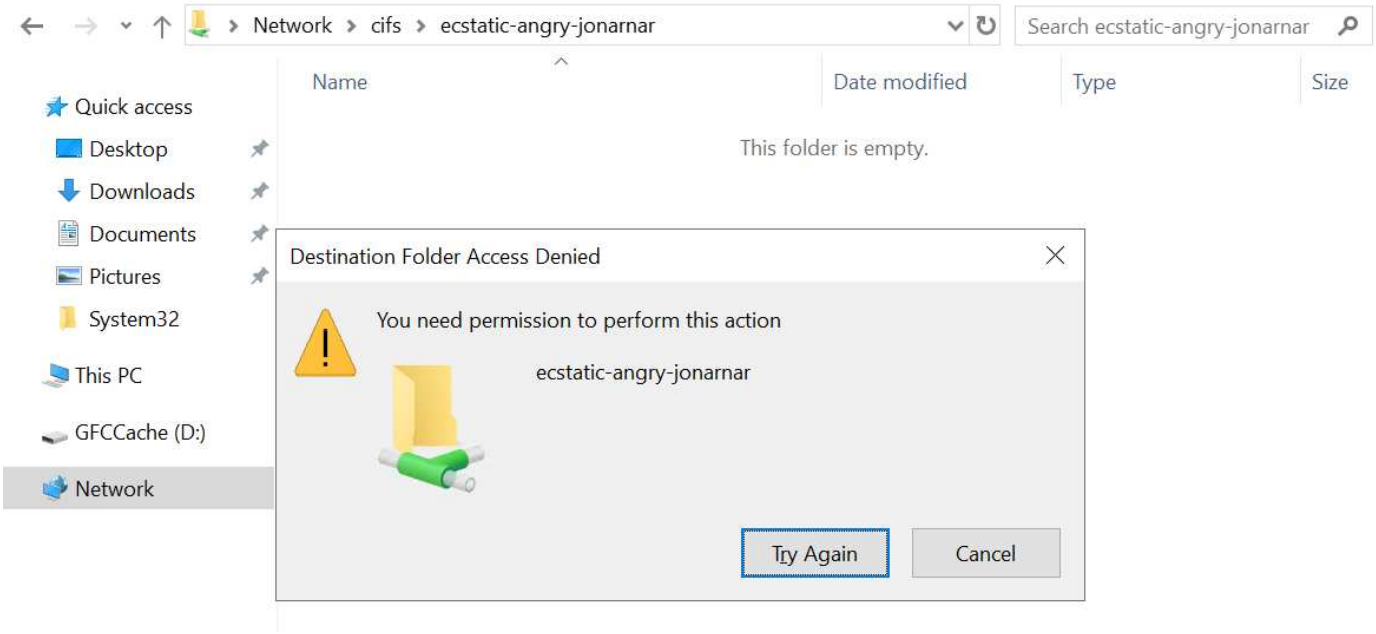
Obwohl NFS-Exportrichtlinienregeln den Zugriff über hostbasierte Informationen wie IP-Adressen oder Hostnamen steuern, können SMB-Freigabeberechtigungen den Zugriff mithilfe von Benutzer- und Gruppen-ACEs in einer Freigabe-ACL steuern. Sie können Freigabe-ACLs entweder über den Windows-Client oder über die Verwaltungsbenutzeroberfläche von Google Cloud NetApp Volumes festlegen.

Standardmäßig enthalten Freigabe-ACLs und anfängliche Volume-ACLs „Jeder mit Vollzugriff“. Die Datei-ACLs sollten geändert werden, aber die Freigabeberechtigungen werden durch die Dateiberechtigungen für Objekte in der Freigabe außer Kraft gesetzt.

Wenn einem Benutzer beispielsweise nur Lesezugriff auf die Datei-ACL des Google Cloud NetApp Volumes -Volumes gewährt wird, wird ihm der Zugriff zum Erstellen von Dateien und Ordnern verweigert, obwohl die Freigabe-ACL auf „Jeder mit Vollzugriff“ eingestellt ist, wie in der folgenden Abbildung dargestellt.







Um optimale Sicherheitsergebnisse zu erzielen, gehen Sie wie folgt vor:

- Entfernen Sie „Jeder“ aus den Freigabe- und Datei-ACLs und legen Sie stattdessen den Freigabezugriff für Benutzer oder Gruppen fest.
- Verwenden Sie zur Zugriffskontrolle Gruppen anstelle einzelner Benutzer, um die Verwaltung zu vereinfachen und Benutzer schneller zu entfernen/hinzuzufügen, um ACLs über die Gruppenverwaltung gemeinsam zu nutzen.
- Erlauben Sie weniger restriktiven, allgemeineren Freigabezugriff auf die ACEs der Freigabeberechtigungen und sperren Sie den Zugriff für Benutzer und Gruppen mit Dateiberechtigungen für eine detailliertere Zugriffskontrolle.
- Vermeiden Sie die allgemeine Verwendung expliziter Ablehnungs-ACLs, da diese Zulassungs-ACLs außer

Kraft setzen. Beschränken Sie die Verwendung expliziter Zugriffssteuerungslisten (ACLs) für Benutzer oder Gruppen, denen der Zugriff auf ein Dateisystem schnell verweigert werden muss.

- Achten Sie unbedingt auf die "ACL-Vererbung" Einstellungen beim Ändern von Berechtigungen; das Setzen des Vererbungsflags auf der obersten Ebene eines Verzeichnisses oder Datenträgers mit einer hohen Dateianzahl bedeutet, dass jeder Datei unterhalb dieses Verzeichnisses oder Datenträgers vererbte Berechtigungen hinzugefügt werden, was zu unerwünschtem Verhalten wie unbeabsichtigtem Zugriff/unbeabsichtigter Zugriffsverweigerung und einem langen Wechsel der Berechtigungsänderungen führen kann, während jede Datei angepasst wird.

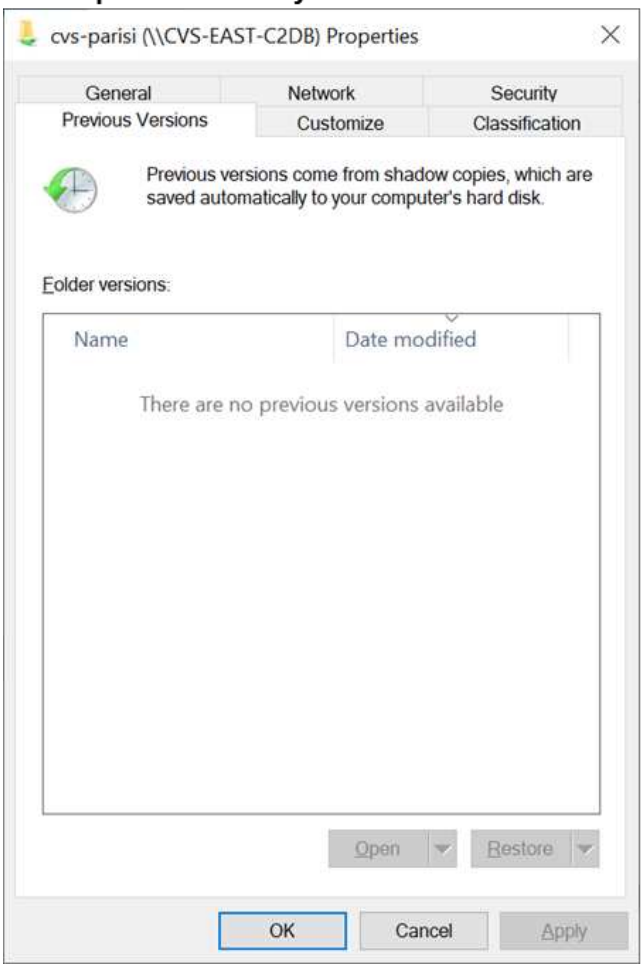
Sicherheitsfunktionen für SMB-Freigaben

Wenn Sie zum ersten Mal ein Volume mit SMB-Zugriff in Google Cloud NetApp Volumes erstellen, werden Ihnen eine Reihe von Auswahlmöglichkeiten zum Sichern dieses Volumes angezeigt.

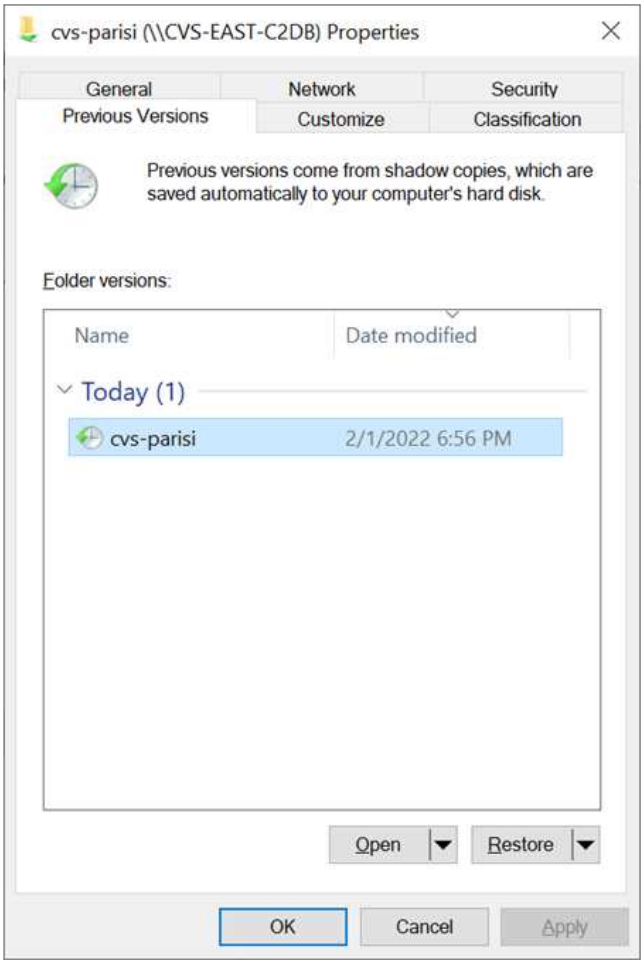
Einige dieser Auswahlmöglichkeiten hängen von der Google Cloud NetApp Volumes Ebene (Leistung oder Software) ab und umfassen folgende Auswahlmöglichkeiten:

- **Snapshot-Verzeichnis sichtbar machen (verfügbar für NetApp Volumes-Performance und NetApp Volumes-SW).** Diese Option steuert, ob SMB-Clients auf das Snapshot-Verzeichnis in einer SMB-Freigabe zugreifen können oder nicht.(`\\server\share\~snapshot` und/oder Registerkarte „Vorherige Versionen“). Die Standardeinstellung ist Nicht aktiviert, was bedeutet, dass das Volume standardmäßig ausgeblendet wird und den Zugriff auf die `~snapshot` Verzeichnis und auf der Registerkarte „Vorherige Versionen“ für das Volume werden keine Snapshot-Kopien angezeigt.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Das Verbergen von Snapshot-Kopien vor Endbenutzern kann aus Sicherheitsgründen, Leistungsgründen (Verbergen dieser Ordner vor AV-Scans) oder aufgrund persönlicher Vorlieben wünschenswert sein. Snapshots von Google Cloud NetApp Volumes sind schreibgeschützt. Selbst wenn diese Snapshots sichtbar sind, können Endbenutzer keine Dateien im Snapshot-Verzeichnis löschen oder ändern. Es gelten die Dateiberechtigungen für die Dateien oder Ordner zum Zeitpunkt der Erstellung 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 je nach Berechtigung auf diese Dateien oder Ordner zugreifen. Während das Löschen oder Ändern von Dateien im Snapshot-Verzeichnis nicht möglich ist, ist es möglich, Dateien oder Ordner aus dem Snapshot-Verzeichnis zu kopieren.

- **SMB-Verschlüsselung aktivieren (verfügbar für NetApp Volumes-Performance und NetApp Volumes-SW).** Die SMB-Verschlüsselung ist auf der SMB-Freigabe standardmäßig deaktiviert (nicht aktiviert). Durch Aktivieren des Kontrollkästchens wird die SMB-Verschlüsselung aktiviert. Dies bedeutet, dass der Datenverkehr zwischen dem SMB-Client und dem Server während der Übertragung mit den höchsten ausgehandelten unterstützten Verschlüsselungsstufen verschlüsselt wird. Google Cloud NetApp Volumes unterstützt bis zu AES-256-Verschlüsselung für SMB. Das Aktivieren der SMB-Verschlüsselung geht mit einer Leistungseinbuße einher, die für Ihre SMB-Clients möglicherweise spürbar ist, aber nicht muss – etwa im Bereich von 10–20 %. NetApp empfiehlt dringend Tests, um festzustellen, ob diese Leistungseinbußen akzeptabel sind.
- **SMB-Freigabe ausblenden (verfügbar für NetApp Volumes-Performance und NetApp Volumes-SW).** Durch Festlegen dieser Option wird der SMB-Freigabepfad beim normalen Durchsuchen ausgeblendet. Dies bedeutet, dass Clients, die den Freigabepfad nicht kennen, die Freigaben nicht sehen können, wenn sie auf den Standard-UNC-Pfad zugreifen (z. B. `\\NetApp Volumes-SMB`). Wenn das Kontrollkästchen aktiviert ist, können nur Clients darauf zugreifen, die den SMB-Freigabepfad explizit kennen oder für die der Freigabepfad durch ein Gruppenrichtlinienobjekt definiert ist (Sicherheit durch Verschleierung).
- **Aktivieren Sie die zugriffsbasierte Enumeration (ABE) (nur NetApp Volumes-SW).** Dies ähnelt dem Ausblenden der SMB-Freigabe, mit der Ausnahme, dass die Freigaben oder Dateien nur vor Benutzern oder Gruppen ausgeblendet werden, die keine Berechtigung zum Zugriff auf die Objekte haben. Wenn beispielsweise ein Windows-Benutzer `joe` ist der Lesezugriff durch die Berechtigungen nicht erlaubt, dann ist der Windows-Benutzer `joe` kann die SMB-Freigabe oder die Dateien überhaupt nicht sehen. Dies ist standardmäßig deaktiviert und Sie können es durch Aktivieren des Kontrollkästchens aktivieren. Weitere Informationen zu ABE finden Sie im NetApp Knowledge Base-Artikel "Wie funktioniert Access Based Enumeration (ABE)?"
- **Aktivieren Sie die Unterstützung für Continuously Available (CA)-Freigaben (nur NetApp Volumes-Performance).** "Ständig verfügbare SMB-Freigaben" bieten eine Möglichkeit, Anwendungsunterbrechungen während Failover-Ereignissen zu minimieren, indem Sperrzustände über Knoten im Google Cloud NetApp Volumes Backend-System repliziert werden. Dies ist keine Sicherheitsfunktion, bietet aber insgesamt eine bessere Ausfallsicherheit. Derzeit werden für diese Funktionalität nur SQL Server- und FSLogix-Anwendungen unterstützt.

Standardmäßig ausgeblendete Freigaben

Wenn ein SMB-Server in Google Cloud NetApp Volumes erstellt wird, gibt es "versteckte administrative Freigaben" (unter Verwendung der $-Namenskonvention), die zusätzlich zur SMB-Freigabe des Datenvolumes erstellt werden. Hierzu zählen C$ (Namespace-Zugriff) und IPC$ (gemeinsame Nutzung benannter Pipes für die Kommunikation zwischen Programmen, wie etwa die Remote Procedure Calls (RPC), die für den Zugriff auf die Microsoft Management Console (MMC) verwendet werden).

Die IPC$-Freigabe enthält keine Freigabe-ACLs und kann nicht geändert werden. Sie wird ausschließlich für RPC-Aufrufe verwendet und "Windows verbietet standardmäßig den anonymen Zugriff auf diese Freigaben" .

Die C$-Freigabe ermöglicht BUILTIN/Administratoren standardmäßig den Zugriff, aber die Automatisierung von

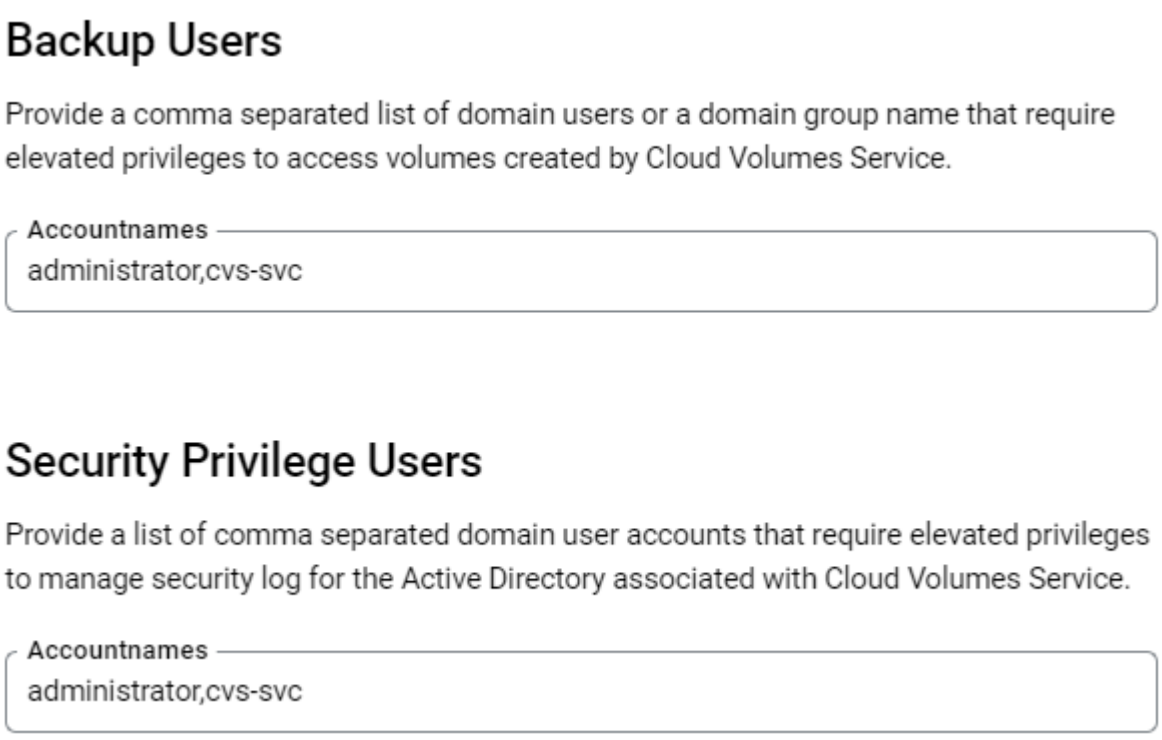
Google Cloud NetApp Volumes entfernt die Freigabe-ACL und gewährt niemandem Zugriff, da der Zugriff auf die C$-Freigabe Einblick in alle bereitgestellten Volumes in den Dateisystemen von Google Cloud NetApp Volumes ermöglicht. Infolgedessen werden Versuche, zu navigieren `\\SERVER\C$` scheitern.

Konten mit lokalen/integrierten Administrator-/Backup-Rechten

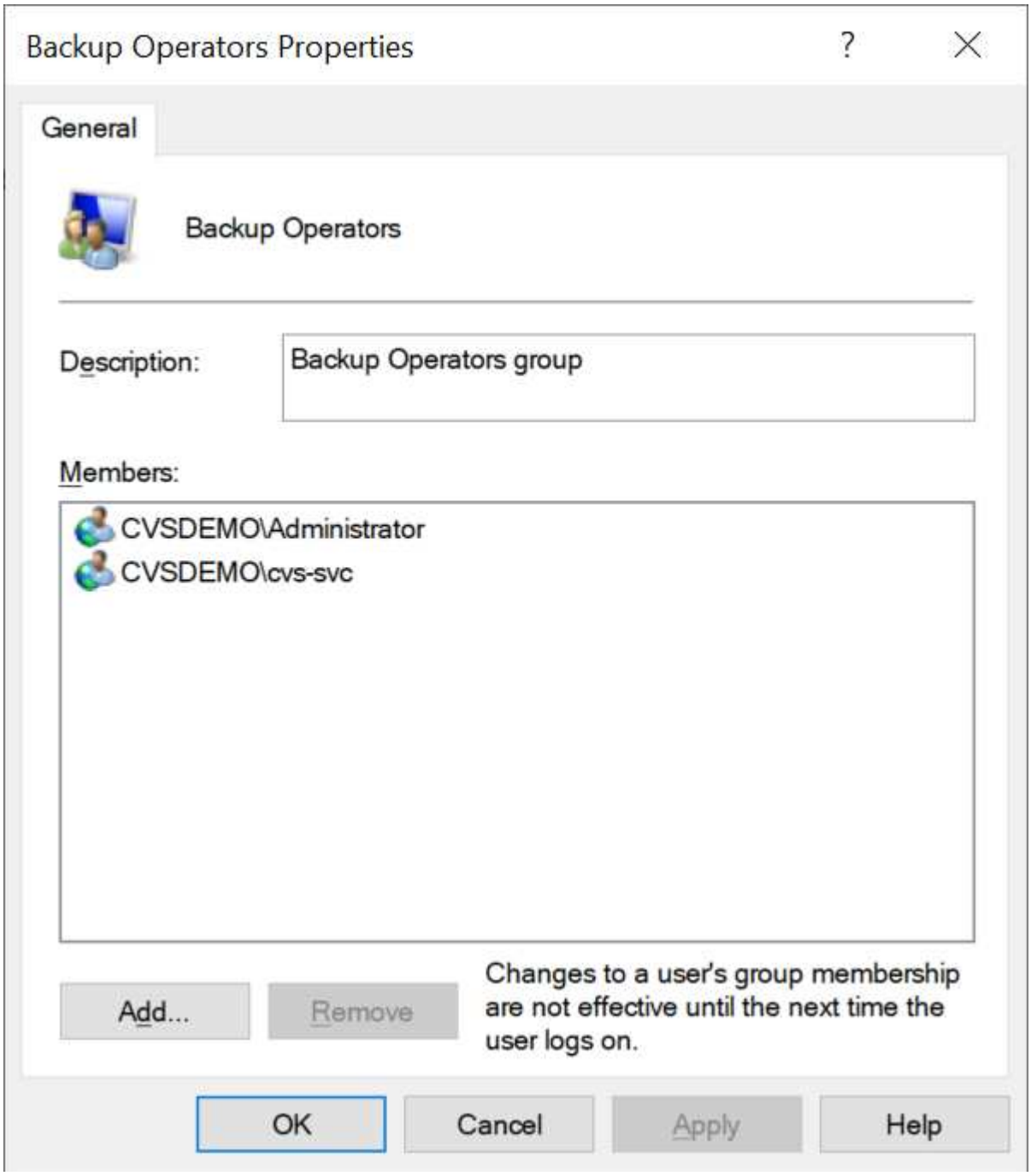
Google Cloud NetApp Volumes SMB-Server verfügen über eine ähnliche Funktionalität wie normale Windows SMB-Server, da es lokale Gruppen (wie z. B. BUILTIN\Administrators) gibt, die Zugriffsrechte auf ausgewählte Domänenbenutzer und -gruppen anwenden.

Wenn Sie einen Benutzer angeben, der zu Backup-Benutzern hinzugefügt werden soll, wird der Benutzer der Gruppe BUILTIN\Backup Operators in der Google Cloud NetApp Volumes Instanz hinzugefügt, die diese Active Directory-Verbindung verwendet. Diese erhält dann die "SeBackupPrivilege und SeRestorePrivilege" .

Wenn Sie einen Benutzer zu den Sicherheitsprivilegbenutzern hinzufügen, erhält der Benutzer das SeSecurityPrivilege, das in einigen Anwendungsfällen nützlich ist, wie zum Beispiel "SQL Server auf SMB-Freigaben" .



Sie können die lokalen Gruppenmitgliedschaften von Google Cloud NetApp Volumes mit den entsprechenden Berechtigungen über die MMC anzeigen. Die folgende Abbildung zeigt Benutzer, die mithilfe der Google Cloud NetApp Volumes Konsole hinzugefügt wurden.

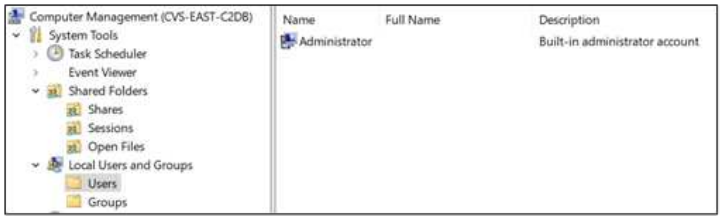


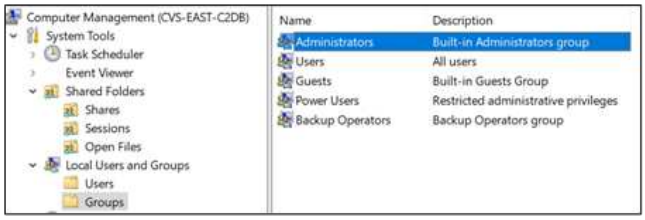
Die folgende Tabelle zeigt die Liste der standardmäßigen BUILTIN-Gruppen und welche Benutzer/Gruppen standardmäßig hinzugefügt werden.

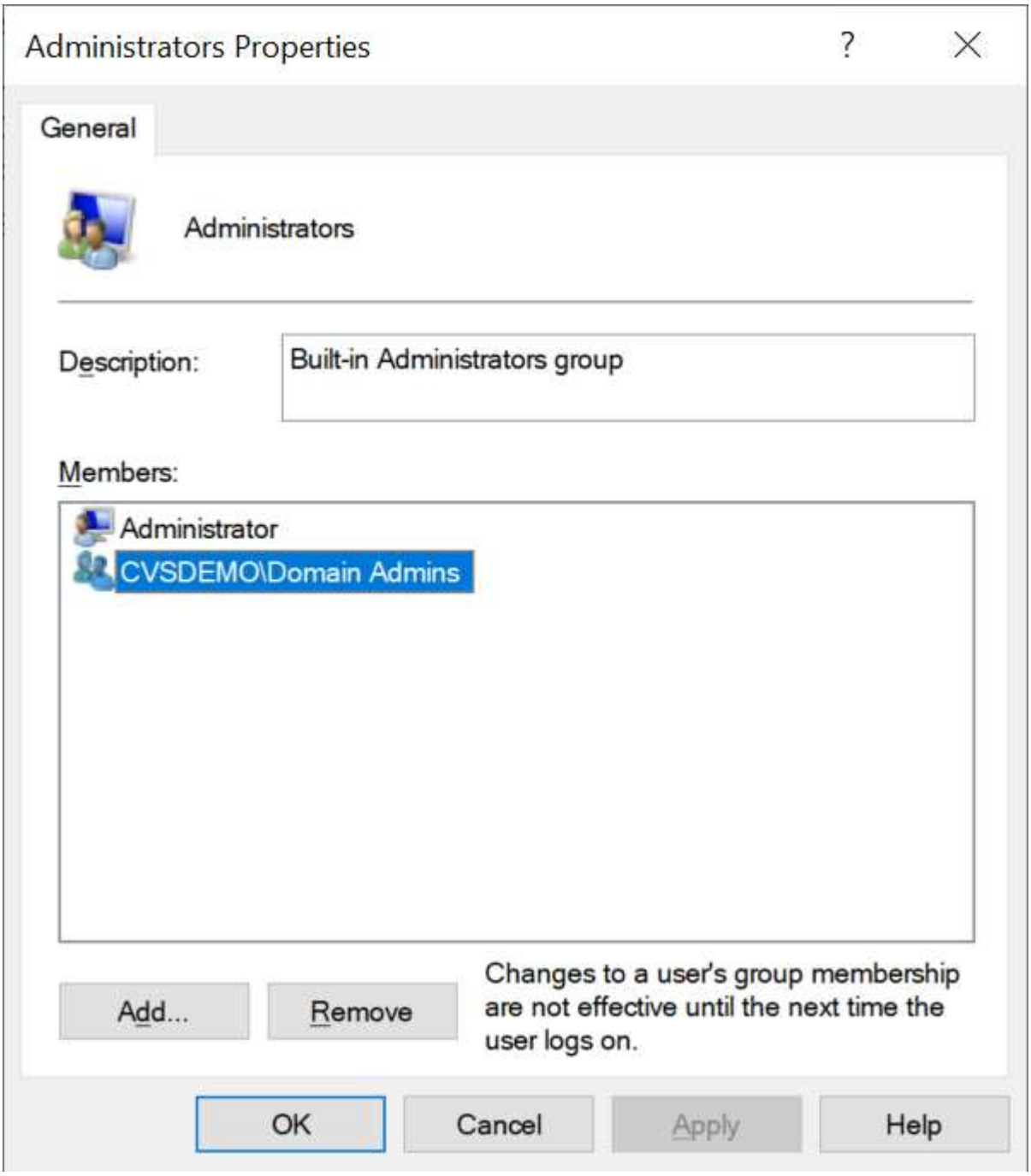
Lokale/BUILTIN-Gruppe	Standardmitglieder
BUILTIN\Administratoren*	DOMAIN\Domänenadministratoren
BUILTIN\Backup-Operatoren*	Keine
GEBAUT\Gäste	DOMAIN\Domänengäste
BUILTIN\Power-User	Keine
BUILTIN\Domänenbenutzer	DOMÄNE\Domänenbenutzer

*Gruppenmitgliedschaft wird in der Active Directory-Verbindungskonfiguration von Google Cloud NetApp Volumes gesteuert.

Sie können lokale Benutzer und Gruppen (und Gruppenmitglieder) im MMC-Fenster anzeigen, Sie können von dieser Konsole aus jedoch keine Objekte hinzufügen oder löschen oder Gruppenmitgliedschaften ändern. Standardmäßig werden nur die Domänenadministratorgruppen und der Administrator zur Gruppe BUILTIN\Administrators in Google Cloud NetApp Volumes hinzugefügt. Derzeit können Sie dies nicht ändern.







MMC/Computerverwaltungszugriff

Der SMB-Zugriff in Google Cloud NetApp Volumes bietet Konnektivität zur Computerverwaltungs-MMC, mit der Sie Freigaben anzeigen, Freigabe-ACLs verwalten und SMB-Sitzungen anzeigen/verwalten und Dateien öffnen können.

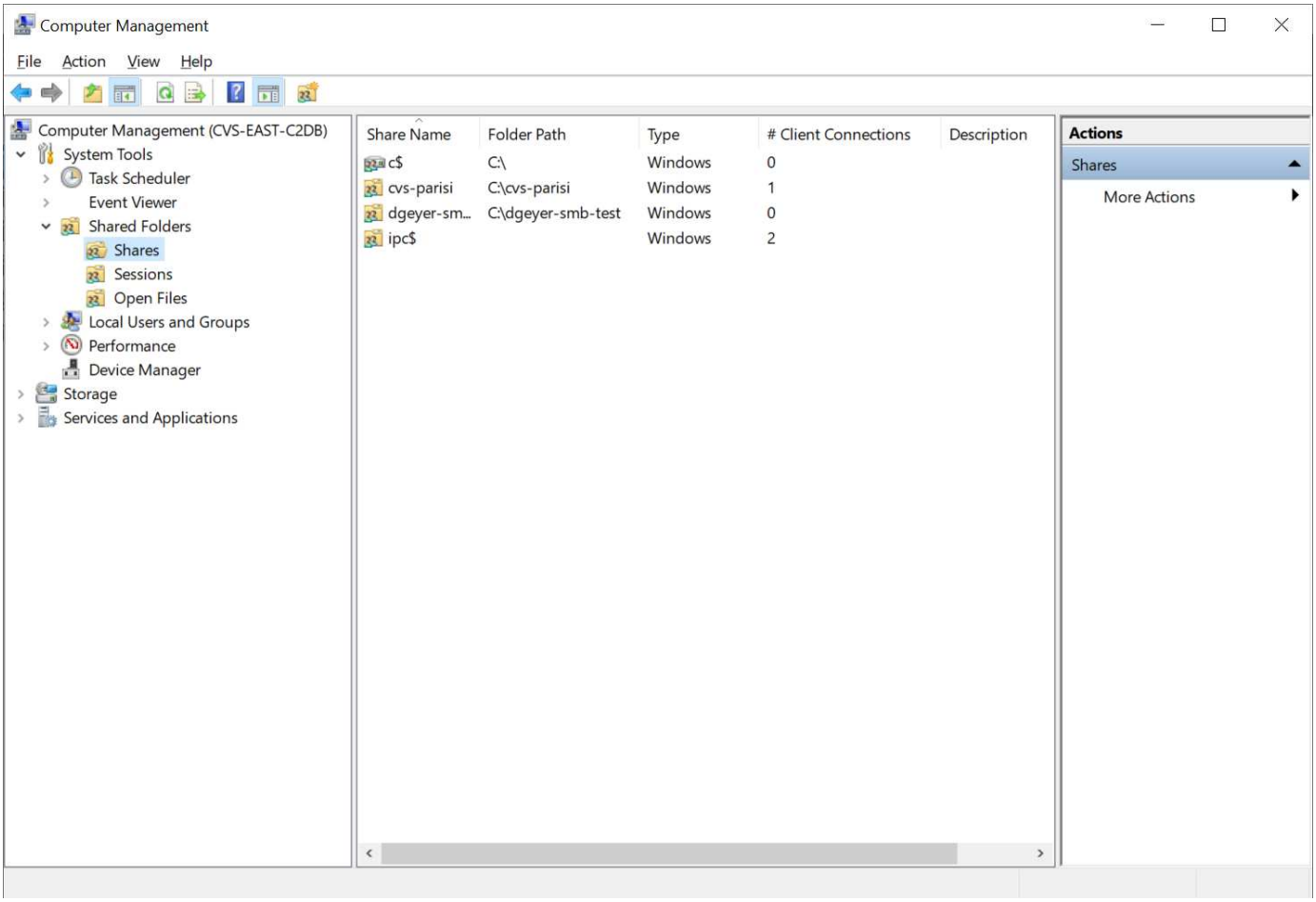
Um die MMC zum Anzeigen von SMB-Freigaben und -Sitzungen in Google Cloud NetApp Volumes zu verwenden, muss der aktuell angemeldete Benutzer ein Domänenadministrator sein. Andere Benutzer dürfen über MMC auf den SMB-Server zugreifen und ihn anzeigen oder verwalten. Beim Versuch, Freigaben oder Sitzungen auf der SMB-Instanz von Google Cloud NetApp Volumes anzuzeigen, wird ihnen das Dialogfeld „Sie verfügen nicht über die erforderlichen Berechtigungen“ angezeigt.

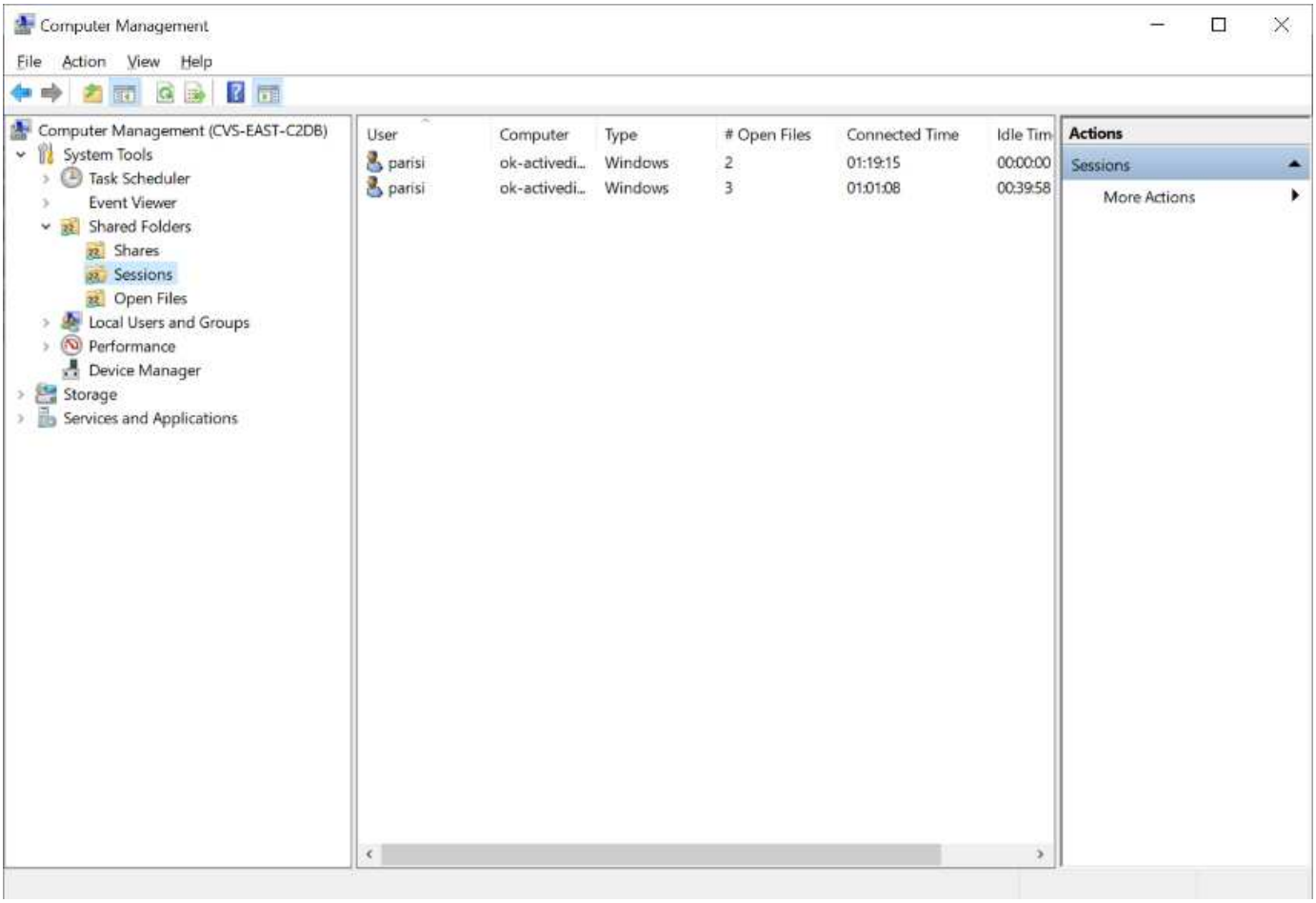
Um eine Verbindung zum SMB-Server herzustellen, öffnen Sie die Computerverwaltung, klicken Sie mit der rechten Maustaste auf Computerverwaltung und wählen Sie dann „Mit einem anderen Computer verbinden“.

Dadurch wird das Dialogfeld „Computer auswählen“ geöffnet, in dem Sie den SMB-Servernamen eingeben können (zu finden in den Volumeinformationen von Google Cloud NetApp Volumes).

Wenn Sie SMB-Freigaben mit den entsprechenden Berechtigungen anzeigen, sehen Sie alle verfügbaren Freigaben in der Google Cloud NetApp Volumes Instanz, die die Active Directory-Verbindung gemeinsam nutzen. Um dieses Verhalten zu steuern, aktivieren Sie die Option „SMB-Freigaben ausblenden“ auf der Google Cloud NetApp Volumes -Volume-Instanz.

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 die MMC.

Unterstützte Funktionen	Nicht unterstützte Funktionen
• Freigaben anzeigen • Aktive SMB-Sitzungen anzeigen • Geöffnete Dateien anzeigen • Anzeigen lokaler Benutzer und Gruppen • Lokale Gruppenmitgliedschaften anzeigen • Auflisten der Sitzungen, Dateien und Baumverbindungen im System • Schließen Sie geöffnete Dateien im System • Offene Sitzungen schließen • Freigaben erstellen/verwalten	• Erstellen neuer lokaler Benutzer/Gruppen • Verwalten/Anzeigen vorhandener lokaler Benutzer/Gruppen • Anzeigen von Ereignissen oder Leistungsprotokollen • Speicherverwaltung • Verwalten von Diensten und Anwendungen

Sicherheitsinformationen für SMB-Server

Der SMB-Server in Google Cloud NetApp Volumes verwendet eine Reihe von Optionen, die Sicherheitsrichtlinien für SMB-Verbindungen definieren, darunter Dinge wie Kerberos-Taktabweichung, Ticketalter, Verschlüsselung und mehr.

Die folgende Tabelle enthält eine Liste dieser Optionen, ihre Funktion, die Standardkonfigurationen und ob sie

mit Google Cloud NetApp Volumes geändert werden können. Einige Optionen gelten nicht für Google Cloud NetApp Volumes.

Sicherheitsoption	Was es bewirkt	Standardwert	Kann sich ändern?
Maximale Kerberos-Uhrabweichung (Minuten)	Maximale Zeitabweichung zwischen Google Cloud NetApp Volumes und Domänencontrollern. Wenn die Zeitabweichung 5 Minuten überschreitet, schlägt die Kerberos-Authentifizierung fehl. Dies ist auf den Active Directory-Standardwert eingestellt.	5	Nein
Lebensdauer des Kerberos-Tickets (Stunden)	Maximale Gültigkeitsdauer eines Kerberos-Tickets, bevor eine Erneuerung erforderlich ist. Erfolgt innerhalb der 10 Stunden keine Verlängerung, müssen Sie sich ein neues Ticket besorgen. Google Cloud NetApp Volumes führt diese Erneuerungen automatisch durch. 10 Stunden ist der Active Directory-Standardwert.	10	Nein
Maximale Kerberos-Ticket-Erneuerung (Tage)	Maximale Anzahl von Tagen, die ein Kerberos-Ticket erneuert werden kann, bevor eine neue Autorisierungsanforderung erforderlich ist. Google Cloud NetApp Volumes erneuert Tickets für SMB-Verbindungen automatisch. Sieben Tage ist der Active Directory-Standardwert.	7	Nein
Kerberos KDC-Verbindungs-Timeout (Sek.)	Die Anzahl der Sekunden, bevor eine KDC-Verbindung abläuft.	3	Nein

Sicherheitsoption	Was es bewirkt	Standardwert	Kann sich ändern?
Signierung für eingehenden SMB-Verkehr erforderlich	Einstellung, um eine Signierung für SMB-Verkehr zu erfordern. Wenn dieser Wert auf „true“ gesetzt ist, schlägt die Konnektivität für Clients fehl, die die Signierung nicht unterstützen.	FALSCH	
Kennwortkomplexität für lokale Benutzerkonten erforderlich	Wird für Passwörter lokaler SMB-Benutzer verwendet. Google Cloud NetApp Volumes unterstützt keine lokale Benutzererstellung, daher gilt diese Option nicht für Google Cloud NetApp Volumes.	WAHR	Nein
Verwenden Sie start_tls für Active Directory-LDAP-Verbindungen	Wird verwendet, um den Start von TLS-Verbindungen für Active Directory LDAP zu ermöglichen. Google Cloud NetApp Volumes unterstützt diese Aktivierung derzeit nicht.	FALSCH	Nein
Ist die AES-128- und AES-256-Verschlüsselung für Kerberos aktiviert?	Dadurch wird gesteuert, ob AES-Verschlüsselung für Active Directory-Verbindungen verwendet wird. Dies wird mit der Option „AES-Verschlüsselung für Active Directory-Authentifizierung aktivieren“ beim Erstellen/Ändern der Active Directory-Verbindung gesteuert.	FALSCH	Ja
LM-Kompatibilitätsstufe	Ebene der unterstützten Authentifizierungsdialekte für Active Directory-Verbindungen. Siehe Abschnitt "SMB-Authentifizierungsdialekte " für weitere Informationen.	ntlmv2-krb	Nein

Sicherheitsoption	Was es bewirkt	Standardwert	Kann sich ändern?
SMB-Verschlüsselung für eingehenden CIFS-Verkehr erforderlich	Erfordert SMB-Verschlüsselung für alle Freigaben. Dies wird von Google Cloud NetApp Volumes nicht verwendet. Legen Sie stattdessen die Verschlüsselung pro Volume fest (siehe Abschnitt „Sicherheitsfunktionen für SMB-Freigaben ").	FALSCH	Nein
Client-Sitzungssicherheit	Legt die Signatur und/oder Versiegelung für die LDAP-Kommunikation fest. Dies ist derzeit in Google Cloud NetApp Volumes nicht festgelegt, könnte aber in zukünftigen Versionen zur Behebung dieses Problems erforderlich sein. Die Behebung von LDAP-Authentifizierungsproblemen aufgrund des Windows-Patches wird im Abschnitt"LDAP-Kanalbindung." .	Keine	Nein
SMB2-Aktivierung für DC-Verbindungen	Verwendet SMB2 für DC-Verbindungen. Standardmäßig aktiviert.	Systemstandard	Nein
LDAP-Referral-Jagd	Bei der Verwendung mehrerer LDAP-Server ermöglicht die Verweisverfolgung dem Client, auf andere LDAP-Server in der Liste zu verweisen, wenn auf dem ersten Server kein Eintrag gefunden wird. Dies wird derzeit von Google Cloud NetApp Volumes nicht unterstützt.	FALSCH	Nein
Verwenden Sie LDAPS für sichere Active Directory-Verbindungen	Ermöglicht die Verwendung von LDAP über SSL. Wird derzeit von Google Cloud NetApp Volumes nicht unterstützt.	FALSCH	Nein

Sicherheitsoption	Was es bewirkt	Standardwert	Kann sich ändern?
Für die DC-Verbindung ist eine Verschlüsselung erforderlich	Erfordert Verschlüsselung für erfolgreiche DC-Verbindungen. In Google Cloud NetApp Volumes standardmäßig deaktiviert.	FALSCH	Nein

Dualprotokoll/Multiprotokoll

Google Cloud NetApp Volumes ermöglicht die gemeinsame Nutzung derselben Datensätze für SMB- und NFS-Clients unter Beibehaltung der korrekten Zugriffsberechtigungen ("Dual-Protokoll"). Dies wird durch die Koordination der Identitätszuordnung zwischen den Protokollen und die Verwendung eines zentralen LDAP-Servers im Backend erreicht, der Google Cloud NetApp Volumes die UNIX-Identitäten bereitstellt. Windows Active Directory kann verwendet werden, um sowohl Windows- als auch UNIX-Benutzer für eine höhere Anwenderfreundlichkeit bereitzustellen.

Zugriffskontrolle

- **Zugriffskontrollen teilen.** Bestimmen Sie, welche Clients und/oder Benutzer und Gruppen auf eine NAS-Freigabe zugreifen können. Bei NFS steuern Exportrichtlinien und -regeln den Clientzugriff auf Exporte. NFS-Exporte werden von der Google Cloud NetApp Volumes Instanz verwaltet. SMB nutzt CIFS/SMB-Freigaben und Freigabe-ACLs, um eine detailliertere Kontrolle auf Benutzer- und Gruppenebene zu ermöglichen. Sie können ACLs auf Freigabeebene von SMB-Clients nur konfigurieren, indem Sie MMC/Computerverwaltung mit einem Konto verwenden, das über Administratorrechte für die Google Cloud NetApp Volumes Instanz verfügt (siehe Abschnitt "Konten mit lokalen/INTEGRIERTEN Administrator-/Sicherungsrechten.").
- **Dateizugriffskontrollen.** Steuern Sie Berechtigungen auf Datei- oder Ordnerebene und verwalten Sie diese immer vom NAS-Client aus. NFS-Clients können traditionelle Modusbits (rwx) oder NFSv4-ACLs verwenden. SMB-Clients nutzen NTFS-Berechtigungen.

Die Zugriffskontrolle für Volumes, die Daten sowohl an NFS als auch an 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 Google Cloud NetApp Volumes, den eingehenden Benutzer einem gültigen Benutzer in die entgegengesetzte Richtung zuzuordnen. Dies ist notwendig, damit der ordnungsgemäße Zugriff über alle Protokolle hinweg sichergestellt werden kann und um sicherzustellen, dass der Benutzer, der den Zugriff anfordert, tatsächlich derjenige ist, für den er sich ausgibt.

Wenn beispielsweise ein Windows-Benutzer mit dem Namen `joe` versucht, über SMB auf ein Volume mit UNIX-Berechtigungen zuzugreifen, dann führt Google Cloud NetApp Volumes eine Suche durch, um einen entsprechenden UNIX-Benutzer mit dem Namen zu finden `joe` . Falls vorhanden, werden Dateien, die als Windows-Benutzer in eine SMB-Freigabe geschrieben werden, `joe` erscheint als UNIX-Benutzer `joe` von NFS-Clients.

Alternativ, wenn ein UNIX-Benutzer mit dem Namen `joe` versucht, mit Windows-Berechtigungen auf ein Google Cloud NetApp Volumes -Volume zuzugreifen, muss der UNIX-Benutzer einem gültigen Windows-

Benutzer zugeordnet werden können. Andernfalls wird der Zugriff auf das Volume verweigert.

Aktuell wird für die externe UNIX-Identitätsverwaltung mit LDAP nur Active Directory unterstützt. Weitere Informationen zur Konfiguration des Zugriffs auf diesen Dienst sind unter "Erstellen einer AD-Verbindung" verfügbar.

Berechtigungsmodell

Bei der Verwendung von Dual-Protokoll-Setups verwendet Google Cloud NetApp Volumes Sicherheitsstile für Volumes, um den ACL-Typ zu bestimmen. Diese Sicherheitsstile werden basierend auf dem angegebenen NAS-Protokoll festgelegt. Im Fall eines dualen Protokolls wird die Auswahl zum Zeitpunkt der Erstellung des Google Cloud NetApp Volumes -Volumes getroffen.

- Wenn Sie nur NFS verwenden, verwenden Google Cloud NetApp Volumes -Volumes UNIX-Berechtigungen.
- Wenn Sie nur SMB verwenden, verwenden Google Cloud NetApp Volumes -Volumes NTFS-Berechtigungen.

Wenn Sie ein Dualprotokoll-Volume erstellen, können Sie den ACL-Stil bei der Volume-Erstellung auswählen. Diese Entscheidung sollte auf Basis der gewünschten Berechtigungsverwaltung getroffen werden. Wenn Ihre Benutzer Berechtigungen von Windows-/SMB-Clients verwalten, wählen Sie NTFS. Wenn Ihre Benutzer die Verwendung von NFS-Clients und chmod/chown bevorzugen, verwenden Sie UNIX-Sicherheitsstile.

Überlegungen zum Erstellen von Active Directory-Verbindungen

Google Cloud NetApp Volumes bietet die Möglichkeit, Ihre Google Cloud NetApp Volumes Instanz mit einem externen Active Directory-Server zu verbinden, um die Identitätsverwaltung sowohl für SMB- als auch für UNIX-Benutzer zu ermöglichen. Zur Verwendung von SMB in Google Cloud NetApp Volumes ist das Erstellen einer Active Directory-Verbindung erforderlich.

Die Konfiguration hierfür bietet mehrere Optionen, die einige Überlegungen zur Sicherheit erfordern. Der externe Active Directory-Server kann eine lokale Instanz oder eine Cloud-native Instanz sein. Wenn Sie einen lokalen Active Directory-Server verwenden, stellen Sie die Domäne nicht dem externen Netzwerk zur Verfügung (z. B. mit einer DMZ oder einer externen IP-Adresse). Verwenden Sie stattdessen sichere private Tunnel oder VPNs, unidirektionale Gesamtstrukturvertrauensstellungen oder dedizierte Netzwerkverbindungen zu den lokalen Netzwerken mit "Privater Google-Zugriff" . Weitere Informationen zu "Best Practices für die Verwendung von Active Directory in Google Cloud" .

> NetApp Volumes-SW erfordert, dass sich Active Directory-Server in derselben Region befinden. Wenn in NetApp Volumes-SW eine DC-Verbindung zu einer anderen Region versucht wird, schlägt der Versuch fehl. Achten Sie bei der Verwendung von NetApp Volumes-SW darauf, Active Directory-Sites zu erstellen, die die Active Directory-DCs enthalten, und geben Sie dann Sites in Google Cloud NetApp Volumes an, um regionsübergreifende DC-Verbindungsversuche zu vermeiden.

Active Directory-Anmeldeinformationen

Wenn SMB oder LDAP für NFS aktiviert ist, interagiert Google Cloud NetApp Volumes mit den Active Directory-Controllern, um ein Maschinenkontoobjekt zu erstellen, das zur Authentifizierung verwendet werden kann. Dies unterscheidet sich nicht davon, wie ein Windows SMB-Client einer Domäne beitritt und erfordert dieselben Zugriffsrechte auf Organisationseinheiten (OUs) in Active Directory.

In vielen Fällen erlauben Sicherheitsgruppen nicht die Verwendung eines Windows-Administratorkontos auf externen Servern wie Google Cloud NetApp Volumes. In einigen Fällen wird der Windows-Administratorbenutzer aus Sicherheitsgründen vollständig deaktiviert.

Zum Erstellen von SMB-Computerkonten erforderliche Berechtigungen

Um Google Cloud NetApp Volumes -Maschinenobjekte zu einem Active Directory hinzuzufügen, ist ein Konto erforderlich, das entweder über Administratorrechte für die Domäne verfügt oder "delegierte Berechtigungen zum Erstellen und Ändern von Maschinenkontoobjekten" zu einer angegebenen OU ist erforderlich. Sie können dies mit dem Assistenten zur Delegation der Kontrolle in Active Directory tun, indem Sie eine benutzerdefinierte Aufgabe erstellen, die einem Benutzer Zugriff auf das Erstellen/Löschen von Computerobjekten mit den folgenden Zugriffsberechtigungen gewährt:

- Lesen/Schreiben
- Alle untergeordneten Objekte erstellen/löschen
- Alle Eigenschaften lesen/schreiben
- 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 minimiert. Nachdem ein Benutzer delegiert wurde, können dieser Benutzername und das Kennwort in diesem Fenster als Active Directory-Anmeldeinformationen angegeben werden.

> Der Benutzername und das Kennwort, die an die Active Directory-Domäne übergeben werden, nutzen während der Abfrage und Erstellung des Computerkontoobjekts die Kerberos-Verschlüsselung für zusätzliche Sicherheit.

Active Directory-Verbindungsdetails

Die "Details zur Active Directory-Verbindung" bieten Administratoren Anleitungen, um spezifische Active Directory-Schemainformationen für die Platzierung von Computerkonten anzugeben, wie zum Beispiel die folgenden:

- **Active Directory-Verbindungstyp.** Wird verwendet, um anzugeben, ob die Active Directory-Verbindung in einer Region für Volumes des Diensttyps „Google Cloud NetApp Volumes“ oder „NetApp Volumes-Performance“ verwendet wird. Wenn dies bei einer bestehenden Verbindung falsch eingestellt ist, funktioniert es bei Verwendung oder Bearbeitung möglicherweise nicht richtig.
- **Domain.** Der Active Directory-Domänenname.
- **Standort.** Beschränkt Active Directory-Server aus Sicherheits- und Leistungsgründen auf einen bestimmten Standort "Überlegungen". Dies ist erforderlich, wenn sich mehrere Active Directory-Server über verschiedene Regionen erstrecken, da Google Cloud NetApp Volumes derzeit keine Active Directory Authentifizierungsanfragen an Active Directory-Server in einer anderen Region als der Google Cloud NetApp Volumes-Instanz unterstützt. (Beispielsweise befindet sich der Active Directory-Domänencontroller in einer Region, die nur NetApp Volumes-Performance unterstützt, Sie benötigen jedoch eine SMB-Freigabe in einer NetApp Volumes-SW-Instanz.)
- **DNS-Server.** DNS-Server zur Verwendung bei Namenssuchen.
- **NetBIOS-Name (optional).** Falls gewünscht, der NetBIOS-Name für den Server. Dies wird verwendet, wenn neue Computerkonten mithilfe der Active Directory-Verbindung erstellt werden. Wenn der NetBIOS-Name beispielsweise auf „NetApp Volumes-EAST“ eingestellt ist, lauten die Computerkontonamen „NetApp Volumes-EAST-{1234}“. Siehe den Abschnitt"So werden Google Cloud NetApp Volumes im Active Directory angezeigt" für weitere Informationen.

- **Organisationseinheit (OU).** Die spezifische Organisationseinheit zum Erstellen des Computerkontos. Dies ist nützlich, wenn Sie die Kontrolle über Computerkonten an eine bestimmte Organisationseinheit an einen Benutzer delegieren.
- **AES-Verschlüsselung.** Sie können auch das Kontrollkästchen „AES-Verschlüsselung für AD-Authentifizierung aktivieren“ aktivieren oder deaktivieren. Durch Aktivieren der AES-Verschlüsselung für die Active Directory-Authentifizierung wird die Kommunikation zwischen Google Cloud NetApp Volumes und Active Directory bei Benutzer- und Gruppensuchen zusätzlich geschützt. Bevor Sie diese Option aktivieren, wenden Sie sich an Ihren Domänenadministrator, um zu bestätigen, dass die Active Directory-Domänencontroller die AES-Authentifizierung unterstützen.

> Standardmäßig deaktivieren die meisten Windows-Server schwächere Verschlüsselungsverfahren (wie DES oder RC4-HMAC) nicht. Wenn Sie sich jedoch für die Deaktivierung schwächerer Verschlüsselungsverfahren entscheiden, vergewissern Sie sich, dass die Active Directory-Verbindung von Google Cloud NetApp Volumes so konfiguriert wurde, dass AES aktiviert wird. Andernfalls kommt es zu Authentifizierungsfehlern. Durch die Aktivierung der AES-Verschlüsselung werden schwächere Chiffren nicht deaktiviert, sondern dem SMB-Computerkonto von Google Cloud NetApp Volumes wird stattdessen Unterstützung für AES-Chiffren hinzugefügt.

Kerberos-Realmdetails

Diese Option gilt nicht für SMB-Server. Es wird vielmehr bei der Konfiguration von NFS Kerberos für das Google Cloud NetApp Volumes -System verwendet. Wenn diese Details ausgefüllt sind, wird der NFS-Kerberos-Bereich konfiguriert (ähnlich einer krb5.conf-Datei unter Linux) und verwendet, wenn NFS Kerberos bei der Erstellung des Google Cloud NetApp Volumes Volumes angegeben wird, da die Active Directory-Verbindung als NFS Kerberos Distribution Center (KDC) fungiert.

> Die Verwendung von Nicht-Windows-KDCs mit Google Cloud NetApp Volumes wird derzeit nicht unterstützt.

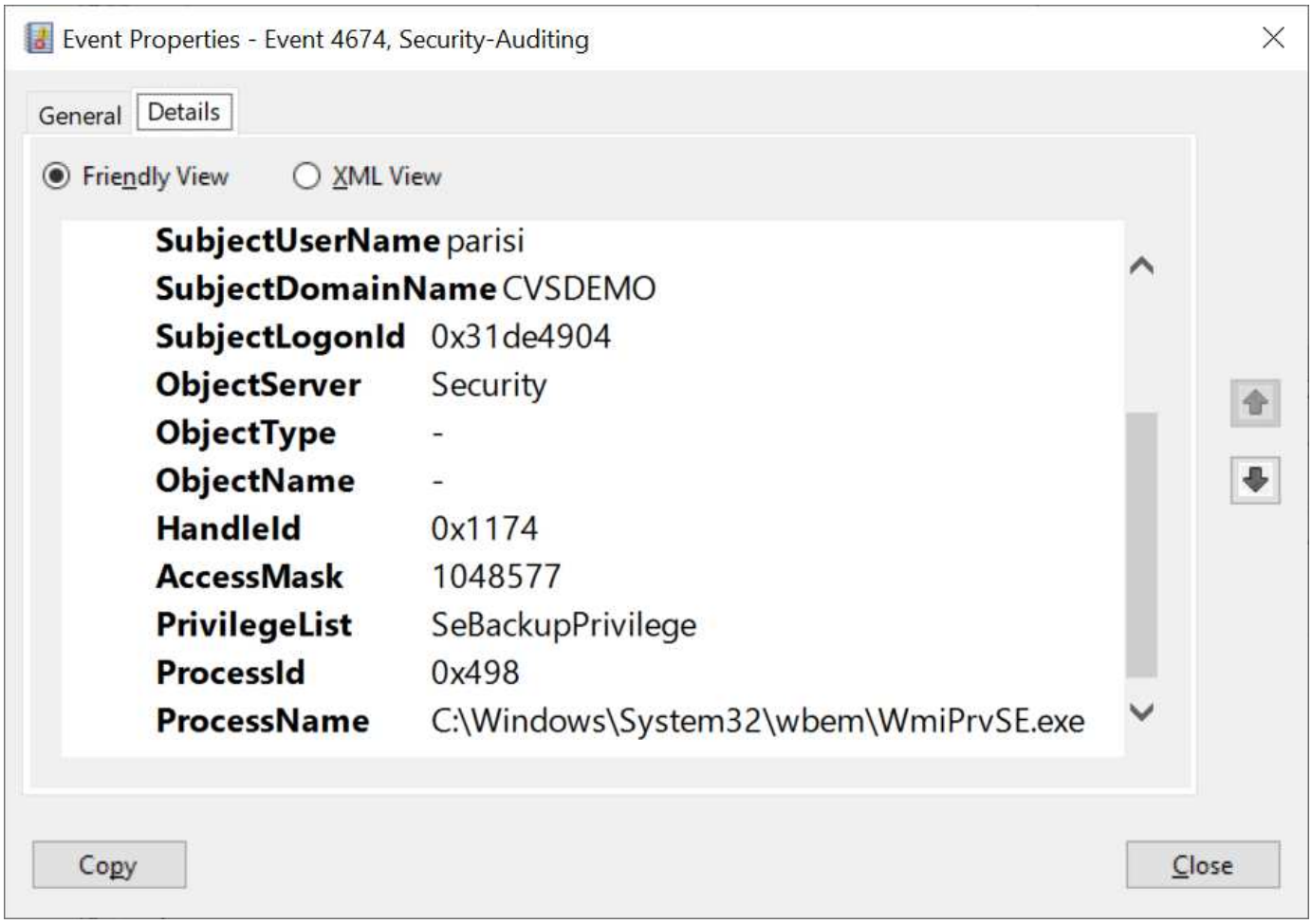
Region

Mithilfe einer Region können Sie den Standort angeben, an dem sich die Active Directory-Verbindung befindet. Diese Region muss dieselbe Region sein wie das Google Cloud NetApp Volumes -Volume.

- **Lokale NFS-Benutzer mit LDAP.** In diesem Abschnitt gibt es auch eine Option zum Zulassen lokaler NFS-Benutzer mit LDAP. Diese Option muss deaktiviert bleiben, wenn Sie die Unterstützung Ihrer UNIX-Benutzergruppenmitgliedschaft über die 16-Gruppen-Beschränkung von NFS (erweiterte Gruppen) hinaus erweitern möchten. Die Verwendung erweiterter Gruppen erfordert jedoch einen konfigurierten LDAP-Server für UNIX-Identitäten. Wenn Sie keinen LDAP-Server haben, lassen Sie diese Option deaktiviert. Wenn Sie über einen LDAP-Server verfügen und auch lokale UNIX-Benutzer (z. B. root) verwenden möchten, wählen Sie diese Option.

Backup-Benutzer

Mit dieser Option können Sie Windows-Benutzer angeben, die über Sicherungsberechtigungen für das Google Cloud NetApp Volumes -Volume verfügen. Für einige Anwendungen sind Sicherungsberechtigungen (SeBackupPrivilege) erforderlich, um Daten in NAS-Volumes ordnungsgemäß zu sichern und wiederherzustellen. Dieser Benutzer hat einen hohen Zugriff auf die Daten im Volume. Sie sollten daher Folgendes berücksichtigen: "Aktivieren der Überwachung dieses Benutzerzugriffs" . Nach der Aktivierung werden Überwachungsereignisse in der Ereignisanzeige > Windows-Protokolle > Sicherheit angezeigt.



Benutzer mit Sicherheitsberechtigung

Mit dieser Option können Sie Windows-Benutzer angeben, die über Berechtigungen zur Sicherheitsänderung für das Google Cloud NetApp Volumes -Volume verfügen. Sicherheitsberechtigungen (SeSecurityPrivilege) sind für einige Anwendungen erforderlich("wie SQL Server"), um die Berechtigungen während der Installation richtig festzulegen. Dieses Privileg ist zum Verwalten des Sicherheitsprotokolls erforderlich. Obwohl dieses Privileg nicht so leistungsfähig ist wie SeBackupPrivilege, empfiehlt NetApp "Überwachung des Benutzerzugriffs von Benutzern" mit dieser Berechtigungsstufe, falls erforderlich.

Weitere Informationen finden Sie unter "Der Neuanmeldung werden besondere Berechtigungen zugewiesen" .

So werden Google Cloud NetApp Volumes im Active Directory angezeigt

Google Cloud NetApp Volumes wird in Active Directory als normales Maschinenkontoobjekt angezeigt. Die Namenskonventionen lauten wie folgt.

- CIFS/SMB und NFS Kerberos erstellen separate Maschinenkontoobjekte.
- NFS mit aktiviertem LDAP erstellt ein Computerkonto in Active Directory für Kerberos-LDAP-Bindungen.
- Dualprotokoll-Volumes mit LDAP teilen sich das CIFS/SMB-Maschinenkonto für LDAP und SMB.
- CIFS/SMB-Maschinenkonten verwenden für das Maschinenkonto die Namenskonvention NAME-1234 (zufällige vierstellige ID mit Bindestrich an den Namen mit <10 Zeichen). Sie können NAME über die NetBIOS-Namenseinstellung der Active Directory-Verbindung definieren (siehe Abschnitt "Active Directory-Verbindungsdetails ").

- NFS Kerberos verwendet NFS-NAME-1234 als Namenskonvention (bis zu 15 Zeichen). Wenn mehr als 15 Zeichen verwendet werden, lautet der Name NFS-TRUNCATED-NAME-1234.
- Nur-NFS- NetApp Volumes-Performance-Instanzen mit aktiviertem LDAP erstellen ein SMB-Maschinenkonto für die Bindung an den LDAP-Server mit derselben Namenskonvention wie CIFS/SMB-Instanzen.
- Wenn ein SMB-Computerkonto erstellt wird, werden standardmäßig ausgeblendete Administratorfreigaben (siehe Abschnitt"Standardmäßig ausgeblendete Freigaben") werden ebenfalls erstellt (c$, admin$, ipc$), aber diesen Freigaben sind keine ACLs zugewiesen und sie sind nicht zugänglich.
- Die Computerkontoobjekte werden standardmäßig in CN=Computers platziert, Sie können jedoch bei Bedarf eine andere OU angeben. Siehe Abschnitt "Zum Erstellen von SMB-Computerkonten erforderliche Berechtigungen " für Informationen darüber, welche Zugriffsrechte zum Hinzufügen/Entfernen von Maschinenkontoobjekten für Google Cloud NetApp Volumes erforderlich sind.

Wenn Google Cloud NetApp Volumes das SMB-Maschinenkonto zu Active Directory hinzufügt, werden die folgenden Felder ausgefüllt:

- cn (mit dem angegebenen SMB-Servernamen)
- dNSHostName (mit SMBserver.domain.com)
- msDS-SupportedEncryptionTypes (Erlaubt 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-Ticketaustausch mit dem Computerkonto für SMB zulässig)
- Name (mit dem SMB-Servernamen)
- sAMAccountName (mit SMBserver$)
- servicePrincipalName (mit host/smbserver.domain.com und host/smbserver SPNs für Kerberos)

Wenn Sie schwächere Kerberos-Verschlüsselungstypen (enctype) auf dem Computerkonto deaktivieren möchten, können Sie den Wert msDS-SupportedEncryptionTypes auf dem Computerkonto in einen der Werte in der folgenden Tabelle ändern, um nur AES zuzulassen.

msDS-SupportedEncryptionTypes-Wert	Enctype 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, "siehe die Google Cloud NetApp Volumes -Dokumentation".

Andere Dienstabhängigkeiten der NAS-Infrastruktur (KDC, LDAP und DNS)

Bei der Verwendung von Google Cloud NetApp Volumes für NAS-Freigaben sind möglicherweise externe Abhängigkeiten für die ordnungsgemäße Funktionalität erforderlich. Diese Abhängigkeiten kommen unter bestimmten Umständen zum Tragen. Die folgende Tabelle zeigt verschiedene Konfigurationsoptionen und welche Abhängigkeiten ggf. erforderlich sind.

Konfiguration	Erforderliche Abhängigkeiten
Nur NFSv3	Keine
Nur NFSv3 Kerberos	Windows Active Directory: * KDC * DNS * LDAP
Nur NFSv4.1	Client-ID-Mapping-Konfiguration (/etc/idmap.conf)
Nur NFSv4.1 Kerberos	• Client-ID-Mapping-Konfiguration (/etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP
Nur SMB	Active Directory: * KDC * DNS
Multiprotokoll-NAS (NFS und SMB)	• Client-ID-Mapping-Konfiguration (nur NFSv4.1; /etc/idmap.conf) • Windows Active Directory: KDC DNS LDAP

Kerberos-Keytab-Rotation/Kennwortrücksetzung für Maschinenkontoobjekte

Bei SMB-Maschinenkonten plant Google Cloud NetApp Volumes regelmäßige Kennwortzurücksetzungen für das SMB-Maschinenkonto. Diese Kennwortzurücksetzungen erfolgen mithilfe der Kerberos-Verschlüsselung und werden jeden vierten Sonntag zu einer zufälligen Uhrzeit zwischen 23:00 und 01:00 Uhr durchgeführt. Diese Kennwortzurücksetzungen ändern die Kerberos-Schlüsselversionen, rotieren die auf dem Google Cloud NetApp Volumes System gespeicherten Keytabs und tragen dazu bei, ein höheres Maß an Sicherheit für SMB-Server aufrechtzuerhalten, die in Google Cloud NetApp Volumes ausgeführt werden. Die Passwörter der Computerkonten werden nach dem Zufallsprinzip erstellt und sind den Administratoren nicht bekannt.

Bei NFS-Kerberos-Maschinenkonten werden Passwörter nur zurückgesetzt, wenn ein neuer Keytab erstellt bzw. mit dem KDC ausgetauscht wird. Derzeit ist dies in Google Cloud NetApp Volumes nicht möglich.

Netzwerkports zur Verwendung mit LDAP und Kerberos

Bei der Verwendung von LDAP und Kerberos sollten Sie die von diesen Services verwendeten Netzwerk-Ports ermitteln. Eine vollständige Liste der von Google Cloud NetApp Volumes verwendeten Ports finden Sie in der "Google Cloud NetApp Volumes -Dokumentation zu Sicherheitsaspekten".

LDAP

Google Cloud NetApp Volumes fungiert als LDAP-Client und verwendet standardmäßige LDAP-Suchabfragen für Benutzer- und Gruppensuchen nach UNIX-Identitäten. LDAP ist erforderlich, wenn Sie Benutzer und Gruppen außerhalb der von Google Cloud NetApp Volumes bereitgestellten Standardbenutzer verwenden möchten. LDAP ist auch erforderlich, wenn Sie NFS Kerberos mit Benutzerprinzipalen (z. B. user1@domain.com) verwenden möchten. Derzeit wird nur LDAP mit Microsoft Active Directory unterstützt.

Um Active Directory als UNIX-LDAP-Server zu verwenden, müssen Sie die erforderlichen UNIX-Attribute für Benutzer und Gruppen angeben, die Sie für UNIX-Identitäten verwenden möchten. Google Cloud NetApp Volumes verwendet eine Standard-LDAP-Schemavorlage, die Attribute basierend auf "RFC-2307-bis" . Daher

zeigt die folgende Tabelle die unbedingt erforderlichen Active Directory-Attribute zum Ausfüllen für Benutzer und Gruppen und wofür jedes Attribut verwendet wird.

Weitere Informationen zum Festlegen von LDAP-Attributen in Active Directory finden Sie unter "Verwalten des Dualprotokollzugriffs."

Attribut	Was es bewirkt
UID*	Gibt den UNIX-Benutzernamen an
uidNummer*	Gibt die numerische ID des UNIX-Benutzers an
gidNummer*	Gibt die numerische ID der primären Gruppe des UNIX-Benutzers an
Objektklasse*	Gibt an, welcher Objekttyp verwendet wird. Google Cloud NetApp Volumes erfordert, dass „Benutzer“ in der Liste der Objektklassen enthalten ist (ist in den meisten Active Directory-Bereitstellungen standardmäßig enthalten).
Name	Allgemeine Informationen zum Konto (richtiger Name, Telefonnummer usw. – auch bekannt als Gecos)
unixUserPassword	Dies muss nicht festgelegt werden; wird bei UNIX-Identitätssuchen für die NAS-Authentifizierung nicht verwendet. Durch diese Einstellung wird der konfigurierte Wert von „unixUserPassword“ im Klartext ausgegeben.
UnixHomeDirectory	Definiert den Pfad zu UNIX-Home-Verzeichnissen, wenn sich ein Benutzer von einem Linux-Client aus gegenüber LDAP authentifiziert. Legen Sie dies fest, wenn Sie LDAP für die UNIX-Home-Verzeichnisfunktion verwenden möchten.
loginShell	Definiert den Pfad zur Bash-/Profil-Shell für Linux-Clients, wenn sich ein Benutzer gegenüber LDAP authentifiziert.

*Bezeichnet, dass das Attribut für die ordnungsgemäße Funktionalität mit Google Cloud NetApp Volumes erforderlich ist. Die verbleibenden Attribute sind nur für die Verwendung auf der Clientseite bestimmt.

Attribut	Was es bewirkt
cn*	Gibt den UNIX-Gruppennamen an. Bei Verwendung von Active Directory für LDAP wird dies beim ersten Erstellen des Objekts festgelegt, kann aber später geändert werden. Dieser Name darf nicht mit dem anderer Objekte identisch sein. Wenn Ihr UNIX-Benutzer mit dem Namen „user1“ beispielsweise zu einer Gruppe mit dem Namen „user1“ auf Ihrem Linux-Client gehört, lässt Windows nicht zwei Objekte mit demselben cn-Attribut zu. Um dies zu umgehen, benennen Sie den Windows-Benutzer in einen eindeutigen Namen um (z. B. „user1-UNIX“). LDAP in Google Cloud NetApp Volumes verwendet das Attribut „uid“ für UNIX-Benutzernamen.
gidNummer*	Gibt die numerische ID der UNIX-Gruppe an.
Objektklasse*	Gibt an, welcher Objekttyp verwendet wird. Google Cloud NetApp Volumes erfordert, dass die Gruppe in der Liste der Objektklassen enthalten ist (dieses Attribut ist in den meisten Active Directory-Bereitstellungen standardmäßig enthalten).
Mitglieds-ID	Gibt an, welche UNIX-Benutzer Mitglieder der UNIX-Gruppe sind. Mit Active Directory LDAP in Google Cloud NetApp Volumes ist dieses Feld nicht erforderlich. Das LDAP-Schema von Google Cloud NetApp Volumes verwendet das Feld „Mitglied“ für Gruppenmitgliedschaften.
Mitglied*	Erforderlich für Gruppenmitgliedschaften/sekundäre UNIX-Gruppen. Dieses Feld wird ausgefüllt, indem Windows-Benutzer zu Windows-Gruppen hinzugefügt werden. Wenn die UNIX-Attribute der Windows-Gruppen jedoch nicht ausgefüllt sind, werden sie nicht in die Gruppenmitgliedschaftslisten der UNIX-Benutzer aufgenommen. Alle Gruppen, die in NFS verfügbar sein müssen, müssen die in dieser Tabelle aufgeführten erforderlichen UNIX-Gruppenattribute ausfüllen.

*Bezeichnet, dass das Attribut für die ordnungsgemäße Funktionalität mit Google Cloud NetApp Volumes erforderlich ist. Die verbleibenden Attribute sind nur für die Verwendung auf der Clientseite bestimmt.

LDAP-Bindungsinformationen

Um Benutzer in LDAP abzufragen, muss Google Cloud NetApp Volumes eine Bindung (Anmeldung) zum LDAP-Dienst herstellen. Diese Anmeldung verfügt über schreibgeschützte Berechtigungen und wird zum Abfragen von LDAP-UNIX-Attributen für Verzeichnissuchen verwendet. Derzeit sind LDAP-Bindungen nur über ein SMB-Computerkonto möglich.

Sie können LDAP nur aktivieren für `NetApp Volumes-Performance` Instanzen und verwenden Sie es für NFSv3-, NFSv4.1- oder Dualprotokoll-Volumes. Für die erfolgreiche Bereitstellung des LDAP-fähigen Volumes muss eine Active Directory-Verbindung in derselben Region wie das Google Cloud NetApp Volumes -Volume hergestellt werden.

Wenn LDAP aktiviert ist, geschieht in bestimmten Szenarien Folgendes.

- Wenn für das Google Cloud NetApp Volumes -Projekt nur NFSv3 oder NFSv4.1 verwendet wird, wird im Active Directory-Domänencontroller ein neues Computerkonto erstellt und der LDAP-Client in Google Cloud NetApp Volumes stellt mithilfe der Anmeldeinformationen des Computerkontos eine Bindung zu Active Directory her. Für das NFS-Volume und die standardmäßigen versteckten administrativen Freigaben werden keine SMB-Freigaben erstellt (siehe Abschnitt"Standardmäßig ausgeblendete Freigaben") wurden Freigabe-ACLs entfernt.
- Wenn für das Google Cloud NetApp Volumes Projekt Dual-Protokoll-Volumes verwendet werden, wird nur das für den SMB-Zugriff erstellte Einzelmaschinenkonto verwendet, um den LDAP-Client in Google Cloud NetApp Volumes an Active Directory zu binden. Es werden keine zusätzlichen Maschinenkonten erstellt.
- Wenn dedizierte SMB-Volumes separat erstellt werden (entweder vor oder nach der Aktivierung von NFS-Volumes mit LDAP), wird das Computerkonto für LDAP-Bindungen mit dem SMB-Computerkonto geteilt.
- Wenn auch NFS Kerberos aktiviert ist, werden zwei Computerkonten erstellt – eines für SMB-Freigaben und/oder LDAP-Bindungen und eines für die NFS Kerberos-Authentifizierung.

LDAP-Abfragen

Obwohl LDAP-Bindungen verschlüsselt sind, werden LDAP-Abfragen im Klartext über den gemeinsamen LDAP-Port 389 übertragen. Dieser bekannte Port kann derzeit in Google Cloud NetApp Volumes nicht geändert werden. Dies hat zur Folge, dass jemand mit Zugriff auf die Paketüberwachung im Netzwerk Benutzer- und Gruppennamen, numerische IDs und Gruppenmitgliedschaften sehen kann.

Google Cloud-VMs können jedoch den Unicast-Verkehr anderer VMs nicht abhören. Nur VMs, die aktiv am LDAP-Verkehr teilnehmen (d. h. eine Bindung herstellen können), können den Verkehr vom LDAP-Server sehen. Weitere Informationen zum Packet Sniffing in Google Cloud NetApp Volumes finden Sie im Abschnitt"Überlegungen zum Paket-Sniffing/Trace."

LDAP-Client-Konfigurationsvorgaben

Wenn LDAP in einer Google Cloud NetApp Volumes Instanz aktiviert ist, wird standardmäßig eine LDAP-Clientkonfiguration mit bestimmten Konfigurationsdetails erstellt. In einigen Fällen gelten Optionen entweder nicht für Google Cloud NetApp Volumes (werden nicht unterstützt) oder sind nicht konfigurierbar.

LDAP-Client-Option	Was es bewirkt	Standardwert	Kann sich ändern?
LDAP-Serverliste	Legt die für Abfragen zu verwendenden LDAP-Servernamen oder IP-Adressen fest. Dies wird nicht für Google Cloud NetApp Volumes verwendet. Stattdessen wird die Active Directory-Domäne zum Definieren von LDAP-Servern verwendet.	Nicht festgelegt	Nein

LDAP-Client-Option	Was es bewirkt	Standardwert	Kann sich ändern?
Active Directory-Domäne	Legt die Active Directory-Domäne fest, die für LDAP-Abfragen verwendet werden soll. Google Cloud NetApp Volumes nutzt SRV-Einträge für LDAP in DNS, um LDAP-Server in der Domäne zu finden.	Auf die in der Active Directory-Verbindung angegebene Active Directory-Domäne einstellen.	Nein
Bevorzugte Active Directory-Server	Legt die bevorzugten Active Directory-Server für die Verwendung von LDAP fest. Wird von Google Cloud NetApp Volumes nicht unterstützt. Verwenden Sie stattdessen Active Directory-Sites, um die LDAP-Serverauswahl zu steuern.	Nicht festgelegt.	Nein
Binden mit SMB-Server-Anmeldeinformationen	Bindet an LDAP unter Verwendung des SMB-Computerkontos. Derzeit ist dies die einzige unterstützte LDAP-Bindungsmethode in Google Cloud NetApp Volumes.	WAHR	Nein
Schemavorlage	Die für LDAP-Abfragen verwendete Schemavorlage.	MS-AD-BIS	Nein
LDAP-Server-Port	Die für LDAP-Abfragen verwendete Portnummer. Google Cloud NetApp Volumes verwendet derzeit nur den Standard-LDAP-Port 389. LDAPS/Port 636 wird derzeit nicht unterstützt.	389	Nein
Ist LDAPS aktiviert?	Steuert, ob LDAP über Secure Sockets Layer (SSL) für Abfragen und Bindungen verwendet wird. Wird derzeit von Google Cloud NetApp Volumes nicht unterstützt.	FALSCH	Nein

LDAP-Client-Option	Was es bewirkt	Standardwert	Kann sich ändern?
Abfrage-Timeout (Sek.)	Zeitüberschreitung für Abfragen. Wenn Abfragen länger als der angegebene Wert dauern, schlagen die Abfragen fehl.	3	Nein
Minimale Bind-Authentifizierungsebene	Die minimal unterstützte Bindungsebene. Da Google Cloud NetApp Volumes Maschinenkonten für LDAP-Bindungen verwendet und Active Directory anonyme Bindungen standardmäßig nicht unterstützt, spielt diese Option aus Sicherheitsgründen keine Rolle.	Anonym	Nein
Bind-DN	Der Benutzername/Distinguished Name (DN), der für Bindungen verwendet wird, wenn eine einfache Bindung verwendet wird. Google Cloud NetApp Volumes verwendet Maschinenkonten für LDAP-Bindungen und unterstützt derzeit keine einfache Bindungsauthentifizierung.	Nicht festgelegt	Nein
Basis-DN	Der für LDAP-Suchen verwendete Basis-DN.	Die für die Active Directory-Verbindung verwendete Windows-Domäne im DN-Format (d. h. DC=Domäne, DC=Lokal).	Nein
Basissuchbereich	Der Suchbereich für Basis-DN-Suchen. Zu den Werten können „Basis“, „Eine Ebene“ oder „Unterbaum“ gehören. Google Cloud NetApp Volumes unterstützt nur Unterbaumsuchen.	Teilbaum	Nein

LDAP-Client-Option	Was es bewirkt	Standardwert	Kann sich ändern?
Benutzer-DN	Definiert den DN, bei dem Benutzersuchen für LDAP-Abfragen beginnen. Wird derzeit für Google Cloud NetApp Volumes nicht unterstützt, daher beginnen alle Benutzersuchen beim Basis-DN.	Nicht festgelegt	Nein
Benutzersuchbereich	Der Suchbereich für Benutzer-DN-Suchen. Zu den Werten können „Basis“, „Eine Ebene“ oder „Unterbaum“ gehören. Google Cloud NetApp Volumes unterstützt das Festlegen des Benutzersuchbereichs nicht.	Teilbaum	Nein
Gruppen-DN	Definiert den DN, bei dem Gruppensuchen für LDAP-Abfragen beginnen. Wird derzeit für Google Cloud NetApp Volumes nicht unterstützt, daher beginnen alle Gruppensuchen beim Basis-DN.	Nicht festgelegt	Nein
Gruppensuchbereich	Der Suchbereich für Gruppen-DN-Suchen. Zu den Werten können „Basis“, „Eine Ebene“ oder „Unterbaum“ gehören. Google Cloud NetApp Volumes unterstützt das Festlegen des Gruppensuchbereichs nicht.	Teilbaum	Nein
Netzgruppen-DN	Definiert den DN, bei dem die Netzgruppensuche für LDAP-Abfragen beginnt. Wird derzeit für Google Cloud NetApp Volumes nicht unterstützt, daher beginnen alle Netgroup-Suchen beim Basis-DN.	Nicht festgelegt	Nein

LDAP-Client-Option	Was es bewirkt	Standardwert	Kann sich ändern?
Netgroup-Suchbereich	Der Suchbereich für Netgroup-DN-Suchen. Zu den Werten können „Basis“, „Eine Ebene“ oder „Unterbaum“ gehören. Google Cloud NetApp Volumes unterstützt das Festlegen des Netgroup-Suchbereichs nicht.	Teilbaum	Nein
Verwenden Sie start_tls über LDAP	Nutzt Start TLS für zertifikatsbasierte LDAP-Verbindungen über Port 389. Wird derzeit von Google Cloud NetApp Volumes nicht unterstützt.	FALSCH	Nein
Aktivieren Sie die Netgroup-by-Host-Suche	Ermöglicht die Suche nach Netzgruppen nach Hostnamen, anstatt die Netzgruppen zu erweitern, um alle Mitglieder aufzulisten. Wird derzeit von Google Cloud NetApp Volumes nicht unterstützt.	FALSCH	Nein
Netgroup-by-Host-DN	Definiert den DN, bei dem Netgroup-by-Host-Suchen für LDAP-Abfragen beginnen. Netgroup-by-Host wird derzeit für Google Cloud NetApp Volumes nicht unterstützt.	Nicht festgelegt	Nein
Netgroup-by-Host-Suchbereich	Der Suchbereich für Netgroup-by-Host-DN-Suchen. Die Werte können „Basis“, „Eine Ebene“ oder „Unterbaum“ umfassen. Netgroup-by-Host wird derzeit für Google Cloud NetApp Volumes nicht unterstützt.	Teilbaum	Nein

LDAP-Client-Option	Was es bewirkt	Standardwert	Kann sich ändern?
Sicherheit der Clientsitzung	Definiert, welche Ebene der Sitzungssicherheit von LDAP verwendet wird (Signieren, Siegel oder keine). Die LDAP-Signierung wird von NetApp Volumes-Performance unterstützt, sofern dies von Active Directory angefordert wird. NetApp Volumes-SW unterstützt keine LDAP-Signierung. Für beide Diensttypen wird die Versiegelung derzeit nicht unterstützt.	Keine	Nein
LDAP-Verweise verfolgen	Bei der Verwendung mehrerer LDAP-Server ermöglicht die Verweisverfolgung dem Client, auf andere LDAP-Server in der Liste zu verweisen, wenn auf dem ersten Server kein Eintrag gefunden wird. Dies wird derzeit von Google Cloud NetApp Volumes nicht unterstützt.	FALSCH	Nein
Gruppenmitgliedschaftsfilter	Bietet einen benutzerdefinierten LDAP-Suchfilter, der beim Suchen der Gruppenmitgliedschaft von einem LDAP-Server verwendet werden kann. Wird derzeit nicht mit Google Cloud NetApp Volumes unterstützt.	Nicht festgelegt	Nein

Verwenden von LDAP für die asymmetrische Namenszuordnung

Google Cloud NetApp Volumes ordnet standardmäßig Windows-Benutzer und UNIX-Benutzer mit identischen Benutzernamen bidirektional zu, ohne dass eine spezielle Konfiguration erforderlich ist. Solange Google Cloud NetApp Volumes einen gültigen UNIX-Benutzer (mit LDAP) finden kann, erfolgt eine 1:1-Namenszuordnung. Wenn beispielsweise ein Windows-Benutzer `johnsmith` verwendet wird, dann, wenn Google Cloud NetApp Volumes einen UNIX-Benutzer namens finden kann `johnsmith` in LDAP, die Namenszuordnung für diesen Benutzer erfolgreich ist, alle Dateien/Ordner, die von `johnsmith` zeigen die korrekte Benutzereigentümerschaft und alle ACLs an, die `johnsmith` werden unabhängig vom verwendeten NAS-Protokoll berücksichtigt. Dies wird als symmetrische Namenszuordnung bezeichnet.

Eine asymmetrische Namenszuordnung liegt vor, wenn die Identität des Windows-Benutzers und des UNIX-

Benutzers nicht übereinstimmt. Wenn beispielsweise ein Windows-Benutzer `johnsmith` hat eine UNIX-Identität von `jsmith` , Google Cloud NetApp Volumes benötigt eine Möglichkeit, über die Abweichung informiert zu werden. Da Google Cloud NetApp Volumes derzeit die Erstellung statischer Namenszuordnungsregeln nicht unterstützt, muss LDAP verwendet werden, um die Identität der Benutzer sowohl für Windows- als auch für UNIX-Identitäten nachzuschlagen und so den ordnungsgemäßen Besitz von Dateien und Ordnern sowie die erwarteten Berechtigungen sicherzustellen.

Standardmäßig umfasst Google Cloud NetApp Volumes `LDAP` im NS-Switch der Instanz für die Namenszuordnungsdatenbank, sodass Sie zur Bereitstellung der Namenszuordnungsfunktionalität durch Verwendung von LDAP für asymmetrische Namen nur einige der Benutzer-/Gruppenattribute ändern müssen, um widerzuspiegeln, wonach Google Cloud NetApp Volumes sucht.

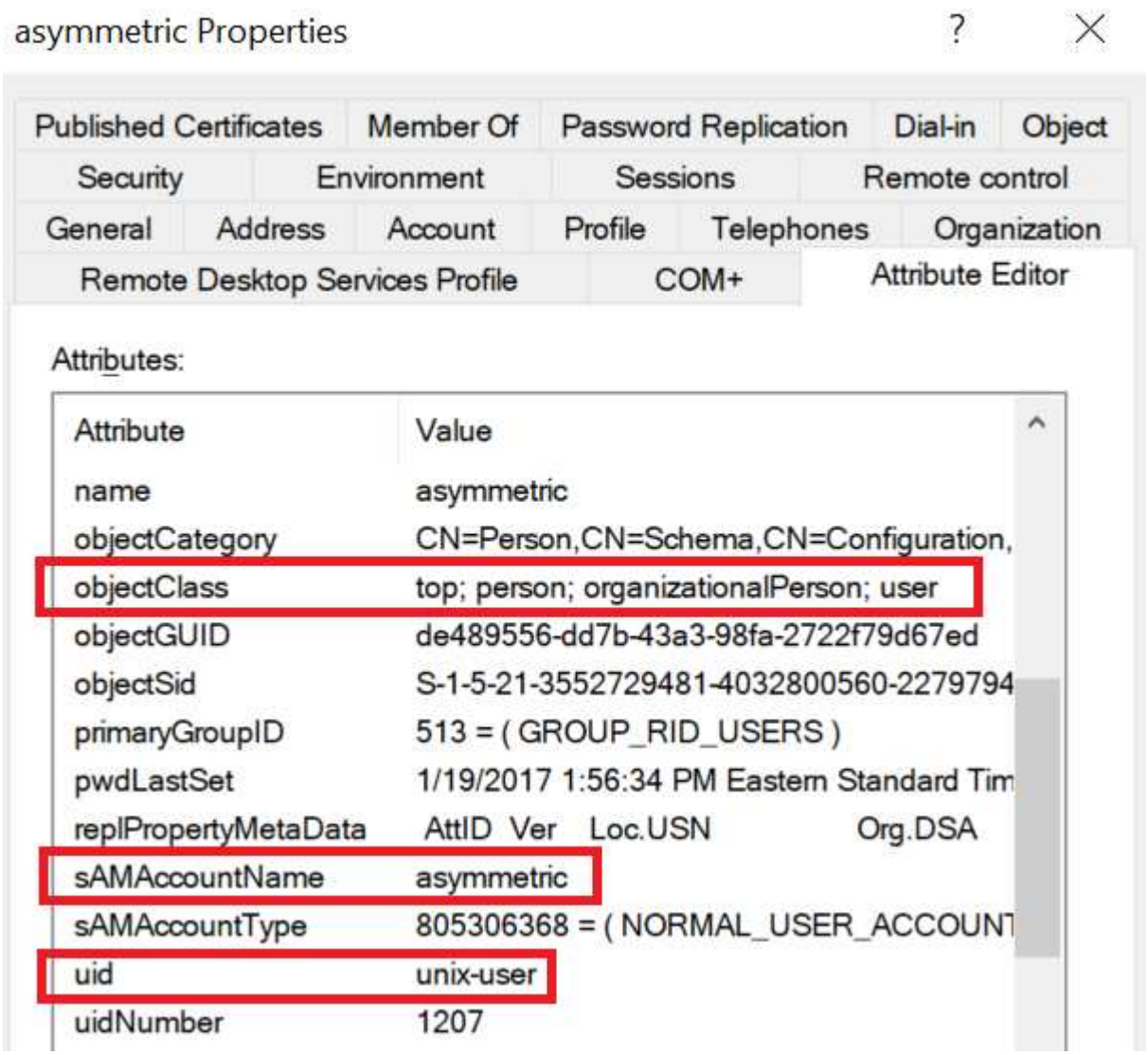
Die folgende Tabelle zeigt, welche Attribute in LDAP für die asymmetrische Namenszuordnungsfunktion ausgefüllt werden müssen. In den meisten Fällen ist Active Directory bereits entsprechend konfiguriert.

Google Cloud NetApp Volumes Attribut	**Was es bewirkt**	**Von Google Cloud NetApp Volumes für die Namenszuordnung verwendeter Wert**
Windows zu UNIX Objektklasse	Gibt den Typ des verwendeten Objekts an. (Das heißt, Benutzer, Gruppe, POSIX-Konto usw.)	Muss den Benutzer enthalten (kann bei Bedarf mehrere andere Werte enthalten).
Windows-zu-UNIX-Attribut	das den Windows-Benutzernamen bei der Erstellung definiert. Google Cloud NetApp Volumes verwendet dies für Windows-zu-UNIX-Lookups.	Hier ist keine Änderung erforderlich; sAMAccountName ist derselbe wie der Windows-Anmeldename.
UID	Definiert den UNIX-Benutzernamen.	Gewünschter UNIX-Benutzername.

Google Cloud NetApp Volumes verwendet derzeit keine Domänenpräfixe in LDAP-Lookups, sodass LDAP-Umgebungen mit mehreren Domänen bei LDAP-Namemap-Lookups nicht ordnungsgemäß funktionieren.

Das folgende Beispiel zeigt einen Benutzer mit dem Windows-Namen `asymmetric` , der UNIX-Name `unix-user` und das Verhalten beim Schreiben von Dateien sowohl von SMB als auch von NFS.

Die folgende Abbildung zeigt, wie LDAP-Attribute vom Windows-Server aussehen.



Von einem NFS-Client aus können Sie den UNIX-Namen, aber nicht 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 von NFS als `unix-user` , das Folgende ist das Ergebnis des NFS-Clients:

```
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)
```

Auf einem Windows-Client können Sie sehen, 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 können Dateien, die vom Windows-Benutzer erstellt wurden, `asymmetric` von einem SMB-Client den richtigen UNIX-Besitzer anzeigen, wie im folgenden Text gezeigt.

KMU:

```
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 Sicherheitslücke in Windows Active Directory-Domänencontrollern "Microsoft-Sicherheitsempfehlung ADV190023" ändert, wie DCs LDAP-Bindungen zulassen.

Die Auswirkungen auf Google Cloud NetApp Volumes sind dieselben wie für jeden LDAP-Client. Google Cloud NetApp Volumes unterstützt derzeit keine Kanalbindung. Da Google Cloud NetApp Volumes standardmäßig die LDAP-Signierung durch Aushandlung unterstützt, sollte die LDAP-Kanalbindung kein Problem darstellen. Wenn bei der Bindung an LDAP bei aktivierter Kanalbindung Probleme auftreten, befolgen Sie die Abhilfeschritte in ADV190023, damit LDAP-Bindungen von Google Cloud NetApp Volumes erfolgreich sind.

DNS

Sowohl Active Directory als auch Kerberos sind für die Auflösung von Hostnamen zu IP bzw. von IP zu Hostnamen von DNS abhängig. DNS erfordert, dass Port 53 geöffnet ist. Google Cloud NetApp Volumes nimmt keine Änderungen an DNS-Einträgen vor und unterstützt derzeit auch nicht die Verwendung von "dynamisches DNS" auf Netzwerkschnittstellen.

Sie können Active Directory DNS konfigurieren, um einzuschränken, welche Server DNS-Einträge aktualisieren können. Weitere Informationen finden Sie unter "Sicheres Windows DNS" .

Beachten Sie, dass Ressourcen innerhalb eines Google-Projekts standardmäßig Google Cloud DNS verwenden, das nicht mit Active Directory DNS verbunden ist. Clients, die Cloud DNS verwenden, können die von Google Cloud NetApp Volumes zurückgegebenen UNC-Pfade nicht auflösen. Windows-Clients, die der Active Directory-Domäne beigetreten sind, sind für die Verwendung von Active Directory DNS konfiguriert und

können solche UNC-Pfade auflösen.

Um einen Client in Active Directory einzubinden, müssen Sie dessen DNS-Konfiguration so anpassen, dass er Active Directory DNS verwendet. Optional können Sie Cloud DNS so konfigurieren, dass Anfragen an Active Directory DNS weitergeleitet werden. Weitere Informationen finden Sie unter "Warum kann mein Client den SMB-NetBIOS-Namen nicht auflösen?".



Google Cloud NetApp Volumes unterstützt derzeit kein DNSSEC und DNS-Abfragen werden im Klartext durchgeführt.

Dateizugriffsüberwachung

Wird derzeit für Google Cloud NetApp Volumes nicht unterstützt.

Virenschutz

Sie müssen auf dem Client einer NAS-Freigabe einen Virenscan in Google Cloud NetApp Volumes durchführen. Derzeit gibt es keine native Antivirenintegration mit Google Cloud NetApp Volumes.

Servicebetrieb

Das Google Cloud NetApp Volumes -Team verwaltet die Backend-Dienste in Google Cloud und verwendet mehrere Strategien, um die Plattform zu sichern und unerwünschten Zugriff zu verhindern.

Jeder Kunde erhält sein eigenes, einzigartiges Subnetz, dessen Zugriff standardmäßig von anderen Kunden abgeschottet ist, und jeder Mandant in Google Cloud NetApp Volumes erhält seinen eigenen Namespace und sein eigenes VLAN zur vollständigen Datenisolierung. Nachdem ein Benutzer authentifiziert wurde, kann die Service Delivery Engine (SDE) nur die für diesen Mandanten spezifischen Konfigurationsdaten lesen.

Physische Sicherheit

Mit der entsprechenden Vorabgenehmigung haben nur Techniker vor Ort und Field Support Engineers (FSEs) mit NetApp Ausweis Zugriff auf den Käfig und die Racks für physische Arbeiten. Speicher- und Netzwerkverwaltung ist nicht zulässig. Nur diese Ressourcen vor Ort können Hardware-Wartungsaufgaben durchführen.

Für Techniker vor Ort wird ein Ticket für die Leistungsbeschreibung (SOW) erstellt, das die Rack-ID und den Gerätestandort (RU) sowie alle anderen Details enthält. Für NetApp FSEs muss beim COLO ein Site-Besuchsticket erstellt werden, das zu Prüfzwecken die Details, das Datum und die Uhrzeit des Besuchers enthält. Die Leistungsbeschreibung für den FSE wird NetApp intern mitgeteilt.

Betriebsteam

Das Betriebsteam für Google Cloud NetApp Volumes besteht aus einem Produktionsingenieur und einem Site Reliability Engineer (SRE) für Google Cloud NetApp Volumes sowie NetApp Field Support Engineers und Partnern für die Hardware. Alle Mitglieder des Betriebsteams sind für die Arbeit in Google Cloud akkreditiert und für jedes erstellte Ticket werden detaillierte Arbeitsaufzeichnungen geführt. Darüber hinaus gibt es einen strengen Änderungskontroll- und Genehmigungsprozess, um sicherzustellen, dass jede Entscheidung angemessen geprüft wird.

Das SRE-Team verwaltet die Steuerebene und die Art und Weise, wie die Daten von UI-Anfragen an die Backend-Hardware und -Software in Google Cloud NetApp Volumes weitergeleitet werden. Das SRE-Team verwaltet auch Systemressourcen wie Volume- und Inode-Maxima. SREs dürfen nicht mit Kundendaten

interagieren oder auf diese zugreifen. SREs übernehmen außerdem die Koordination von RMAs (Return Material Authorizations), beispielsweise bei Anfragen zum Austausch neuer Festplatten oder Arbeitsspeicher für die Backend-Hardware.

Kundenpflichten

Kunden von Google Cloud NetApp Volumes verwalten das Active Directory und die Benutzerrollenverwaltung ihres Unternehmens sowie die Volume- und Datenvorgänge. Kunden können über Administratorrollen verfügen und Berechtigungen an andere Endbenutzer innerhalb desselben Google Cloud-Projekts delegieren, indem sie die beiden vordefinierten Rollen verwenden, die NetApp und Google Cloud bereitstellen (Administrator und Viewer).

Der Administrator kann jedes VPC innerhalb des Kundenprojekts mit Google Cloud NetApp Volumes verbinden, das der Kunde für geeignet hält. Es liegt in der Verantwortung des Kunden, den Zugriff auf sein Google Cloud Marketplace-Abonnement zu verwalten und die VPCs zu verwalten, die Zugriff auf die Datenebene haben.

Schutz vor bösartigen SREs

Eine mögliche Frage ist, wie Google Cloud NetApp Volumes vor Szenarien schützt, in denen ein bösartiger SRE vorhanden ist oder SRE-Anmeldeinformationen kompromittiert wurden.

Der Zugriff auf die Produktionsumgebung ist nur einer begrenzten Anzahl von SRE-Mitarbeitern gestattet. Darüber hinaus sind die Administratorrechte auf eine Handvoll erfahrener Administratoren beschränkt. Alle von Personen in der Google Cloud NetApp Volumes -Produktionsumgebung ausgeführten Aktionen werden protokolliert und alle Anomalien der Basislinie oder verdächtigen Aktivitäten werden von unserer Threat Intelligence-Plattform für Security Information and Event Management (SIEM) erkannt. Dadurch können böswillige Aktionen verfolgt und abgemildert werden, bevor dem Backend von Google Cloud NetApp Volumes zu großer Schaden zugefügt wird.

Volume-Lebenszyklus

Google Cloud NetApp Volumes verwaltet nur die Objekte innerhalb des Dienstes, nicht die Daten innerhalb der Volumes. Nur Clients, die auf die Volumes zugreifen, können die Daten, die ACLs, Dateieigentümer usw. verwalten. Die Daten in diesen Volumes werden im Ruhezustand verschlüsselt und der Zugriff ist auf Mandanten der Google Cloud NetApp Volumes Instanz beschränkt.

Der Volume-Lebenszyklus für Google Cloud NetApp Volumes ist Erstellen-Aktualisieren-Löschen. Volumes behalten Snapshot-Kopien von Volumes bei, bis die Volumes gelöscht werden, und nur validierte Google Cloud NetApp Volumes Administratoren können Volumes in Google Cloud NetApp Volumes löschen. Wenn ein Administrator die Löschung eines Volumes anfordert, ist zur Bestätigung der Löschung ein zusätzlicher Schritt zur Eingabe des Volumenamens erforderlich. Nachdem ein Volume gelöscht wurde, ist es verloren und kann nicht wiederhergestellt werden.

In Fällen, in denen ein Google Cloud NetApp Volumes -Vertrag gekündigt wird, markiert NetApp Volumes nach einem bestimmten Zeitraum zum Löschen. Vor Ablauf dieser Frist können Sie auf Kundenwunsch Volumes wiederherstellen.

Zertifizierungen

Google Cloud NetApp Volumes für Google Cloud ist derzeit nach den Standards ISO/IEC 27001:2013 und ISO/IEC 27018:2019 zertifiziert. Der Dienst hat außerdem vor Kurzem seinen SOC2 Typ I-Bescheinigungsbericht erhalten. Informationen zum Engagement von NetApp für Datensicherheit und Datenschutz finden Sie unter "Compliance: Datensicherheit und Datenschutz" .

DSGVO

Unsere Verpflichtungen in Bezug auf Datenschutz und Compliance mit der GDPR sind in mehreren unserer "Kundenverträge" verfügbar, beispielsweise in unserer "Nachtrag zur Data Processing", die die "Standardvertragsklauseln" der Europäischen Kommission enthält. Diese Verpflichtungen sind außerdem in unserer Privacy Policy enthalten und werden durch die in unserem unternehmensweiten Code of Conduct festgelegten Kernwerte untermauert.

Weitere Informationen und Kontaktinformationen

Weitere Informationen zu den in diesem Dokument beschriebenen Informationen finden Sie in den folgenden Dokumenten und/oder auf den folgenden Websites:

- Google Cloud-Dokumentation für Google Cloud NetApp Volumes

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Zugriff auf private Google-Dienste

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- NetApp Produktdokumentation

  "https://www.netapp.com/support-and-training/documentation/"

- Programm für kryptografisches Validierungsmodul – NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- Die NetApp Lösung für Ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: NFS Kerberos in 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. Geben Sie in der Betreffzeile „TECHNISCHER BERICHT 4918“ an.

NetApp Disaster Recovery

3-2-1-Datenschutz für VMware mit SnapCenter Plug-in sowie NetApp Backup und Recovery zum Schutz von VMware-Workloads

Die 3-2-1-Backup-Strategie ist eine branchenweit anerkannte Methode zum Datenschutz und bietet einen umfassenden Ansatz zum Schutz wertvoller Daten. Diese Strategie ist zuverlässig und stellt sicher, dass auch im Falle eines unerwarteten Notfalls immer noch eine Kopie der Daten verfügbar ist.

Überblick

Die Strategie besteht aus drei Grundregeln:

1. Bewahren Sie mindestens drei Kopien Ihrer Daten auf. Dadurch wird sichergestellt, dass Sie auch dann noch über mindestens zwei verbleibende Kopien verfügen, wenn eine Kopie verloren geht oder beschädigt wird.
2. Speichern Sie zwei Sicherungskopien auf unterschiedlichen Speichermedien oder Geräten. Durch die Diversifizierung der Speichermedien können Sie sich vor geräte- oder medienspezifischen Ausfällen schützen. Wenn ein Gerät beschädigt wird oder ein Medientyp ausfällt, bleibt die andere Sicherungskopie davon unberührt.
3. Stellen Sie abschließend sicher, dass mindestens eine Sicherungskopie außerhalb des Standorts gespeichert ist. Die externe Speicherung dient als Ausfallsicherung gegen lokale Katastrophen wie Brände oder Überschwemmungen, die die Kopien vor Ort unbrauchbar machen könnten.

Dieses Lösungsdokument behandelt eine 3-2-1-Backup-Lösung, bei der mit SnapCenter Plug-in for VMware vSphere (SCV) primäre und sekundäre Backups unserer lokalen virtuellen Maschinen erstellt werden und NetApp Backup and Recovery für virtuelle Maschinen eine Kopie unserer Daten in Cloud Storage oder StorageGRID sichert.

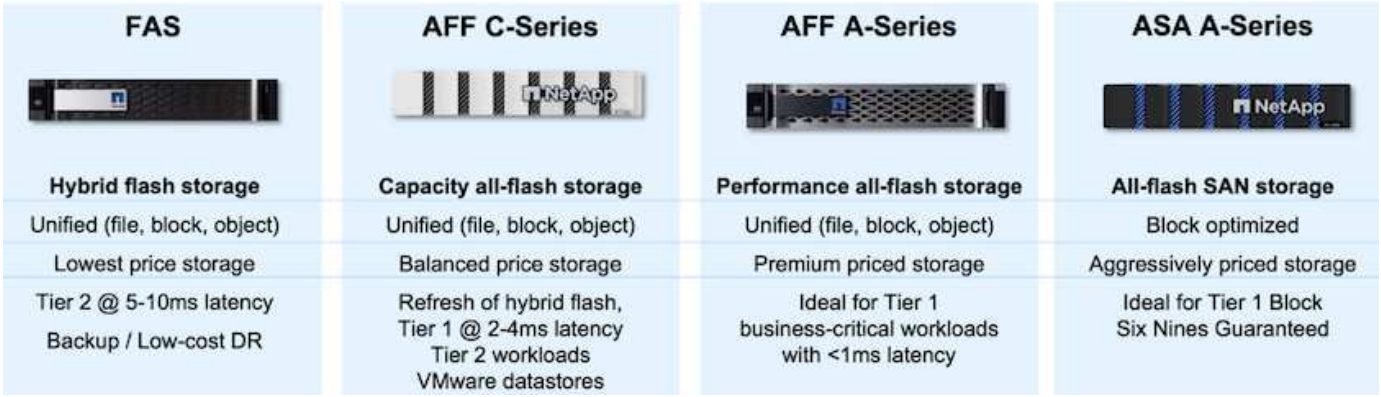
Anwendungsfälle

Diese Lösung ist für die folgenden Anwendungsfälle geeignet:

- Sicherung und Wiederherstellung von virtuellen Maschinen und Datenspeichern vor Ort mithilfe des SnapCenter Plug-in for VMware vSphere.
- Backup und Wiederherstellung von lokalen virtuellen Maschinen und Datastores, die auf ONTAP Clustern gehostet und mithilfe von NetApp Backup and Recovery for virtual machines in Objektspeicher gesichert werden.

NetApp ONTAP Datenspeicher

ONTAP ist die branchenführende Speicherlösung von NetApp, die einheitlichen Speicher bietet, unabhängig davon, ob Sie über SAN- oder NAS-Protokolle zugreifen. Die 3-2-1-Backup-Strategie stellt sicher, dass lokale Daten auf mehr als einem Medientyp geschützt sind, und NetApp bietet Plattformen von Hochgeschwindigkeits-Flash bis hin zu kostengünstigeren Medien.



Weitere Informationen zu allen Hardware-Plattformen von NetApp finden Sie unter "NetApp Datenspeicher" .

SnapCenter Plug-in for VMware vSphere

Das SnapCenter -Plugin für VMware vSphere ist ein Datenschutzangebot, das eng in VMware vSphere integriert ist und eine einfache Verwaltung von Backups und Wiederherstellungen für virtuelle Maschinen ermöglicht. Als Teil dieser Lösung bietet SnapMirror eine schnelle und zuverlässige Methode zum Erstellen einer zweiten unveränderlichen Sicherungskopie der Daten virtueller Maschinen auf einem sekundären ONTAP Speichercluster. Mit dieser Architektur können Wiederherstellungsvorgänge für virtuelle Maschinen problemlos von den primären oder sekundären Sicherungsstandorten aus gestartet werden.

SCV wird als virtuelle Linux-Appliance mithilfe einer OVA-Datei bereitgestellt. Das Plug-in verwendet jetzt eine Remote-Plug-in-Architektur. Das Remote-Plug-In wird außerhalb des vCenter-Servers ausgeführt und auf der virtuellen SCV-Appliance gehostet.

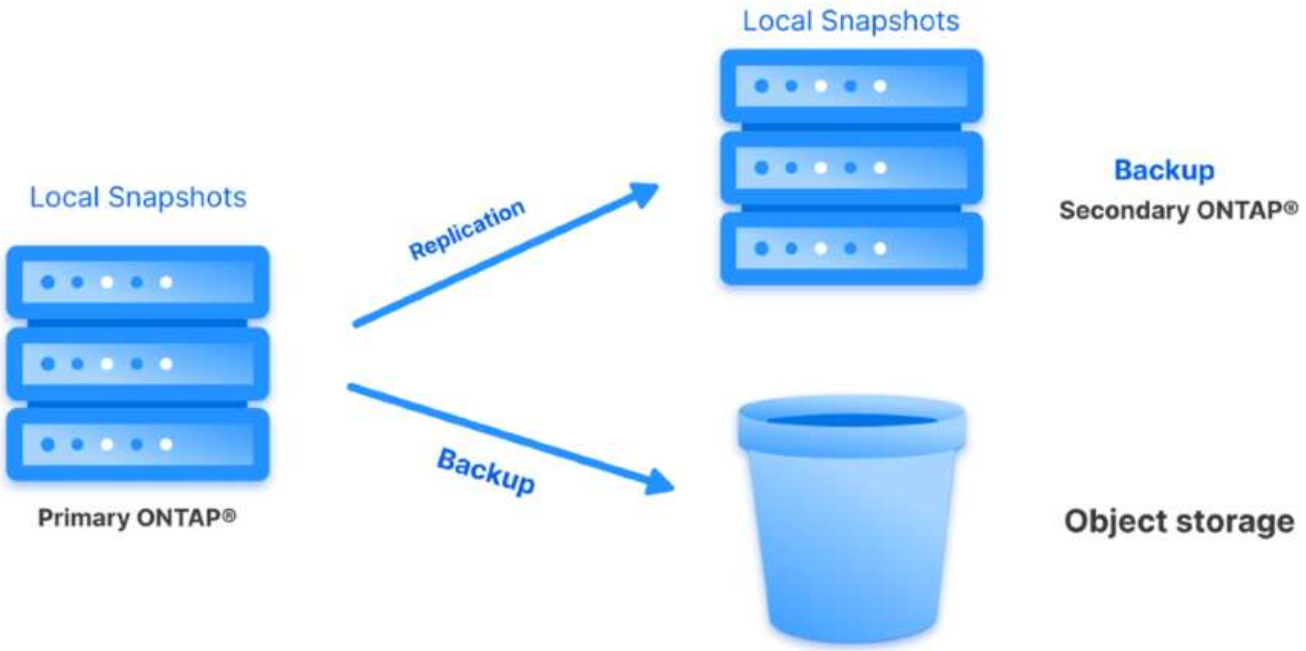
Ausführliche Informationen zu SCV finden Sie unter "SnapCenter Plug-in for VMware vSphere Dokumentation" .

NetApp Backup and Recovery zum Schutz von VMware Workloads

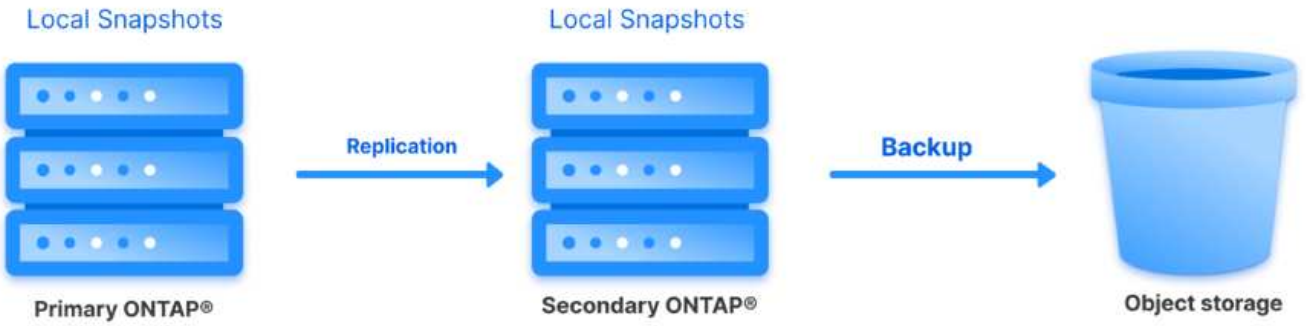
NetApp Backup and Recovery ist ein cloudbasiertes Tool für Datenmanagement, das eine zentrale Kontrollebene für ein breites Spektrum an Backup und Recovery Vorgängen in lokalen und Cloud-Umgebungen bietet. Teil der NetApp Backup and Recovery for VM Suite ist eine Funktion, die in das SnapCenter Plug-in for VMware vSphere (lokal) integriert ist, um eine Kopie der Daten auf Objektspeicher in der Cloud zu erweitern. Dadurch wird eine dritte externe Kopie der Daten an einem externen Standort erstellt, die aus den Backups des primären oder sekundären Storage-Systems stammt. NetApp Backup and Recovery for VMs ermöglicht die einfache Einrichtung von Storage-Richtlinien, die Kopien Ihrer Daten von einem dieser beiden lokalen Standorte übertragen.

Die Wahl zwischen primären und sekundären Backups als Quelle in NetApp Backup and Recovery führt zur Implementierung einer von zwei Topologien:

Fan-out-Topologie - Wenn ein Backup durch das SnapCenter Plug-in for VMware vSphere initiiert wird, wird sofort ein lokaler Snapshot erstellt. SCV initiiert dann einen SnapMirror Vorgang, der den neuesten Snapshot auf den sekundären ONTAP Cluster repliziert. In NetApp Backup and Recovery legt eine Richtlinie den primären ONTAP Cluster als Quelle für eine Snapshot-Kopie der Daten fest, die in den Objektspeicher bei dem Cloud-Anbieter Ihrer Wahl übertragen werden soll.



Kaskadierende Topologie – Das Erstellen der primären und sekundären Datenkopien mithilfe von SCV entspricht der oben beschriebenen Fan-out-Topologie. Allerdings wird diesmal in NetApp Backup and Recovery eine Richtlinie erstellt, die festlegt, dass das Backup in Objekt-Storage vom sekundären ONTAP Cluster ausgeht.



NetApp Backup and Recovery kann Sicherungskopien von lokalen ONTAP Snapshots in AWS Glacier, Azure Blob und GCP Archive Storage erstellen.







AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

Darüber hinaus können Sie NetApp StorageGRID als Sicherungsziel für den Objektspeicher verwenden. Weitere Informationen zu StorageGRID finden Sie im "StorageGRID -Landingpage" .

▼ **Übersicht über die Lösungsbereitstellung**

Diese Liste enthält die übergeordneten Schritte, die zur Konfiguration dieser Lösung und zur Durchführung von Backup- und Restore-Vorgängen über SCV und NetApp Console erforderlich sind:

1. Konfigurieren Sie die SnapMirror -Beziehung zwischen den ONTAP Clustern, die für primäre und sekundäre Datenkopien verwendet werden sollen.
2. Konfigurieren Sie das SnapCenter Plug-In für VMware vSphere.
   a. Speichersysteme hinzufügen
   b. Erstellen von Sicherungsrichtlinien
   c. Erstellen von Ressourcengruppen
   d. Führen Sie die ersten Sicherungsaufträge aus
3. Konfiguration von NetApp Backup and Recovery für virtuelle Maschinen
   a. Arbeitsumgebung hinzufügen
   b. Entdecken Sie SCV- und vCenter-Geräte
   c. Erstellen von Sicherungsrichtlinien
   d. Backups aktivieren
4. Stellen Sie virtuelle Maschinen mithilfe von SCV vom primären und sekundären Speicher wieder her.
5. Wiederherstellung virtueller Maschinen aus Objekt-Storage mit NetApp Console.

▼ **Voraussetzungen**

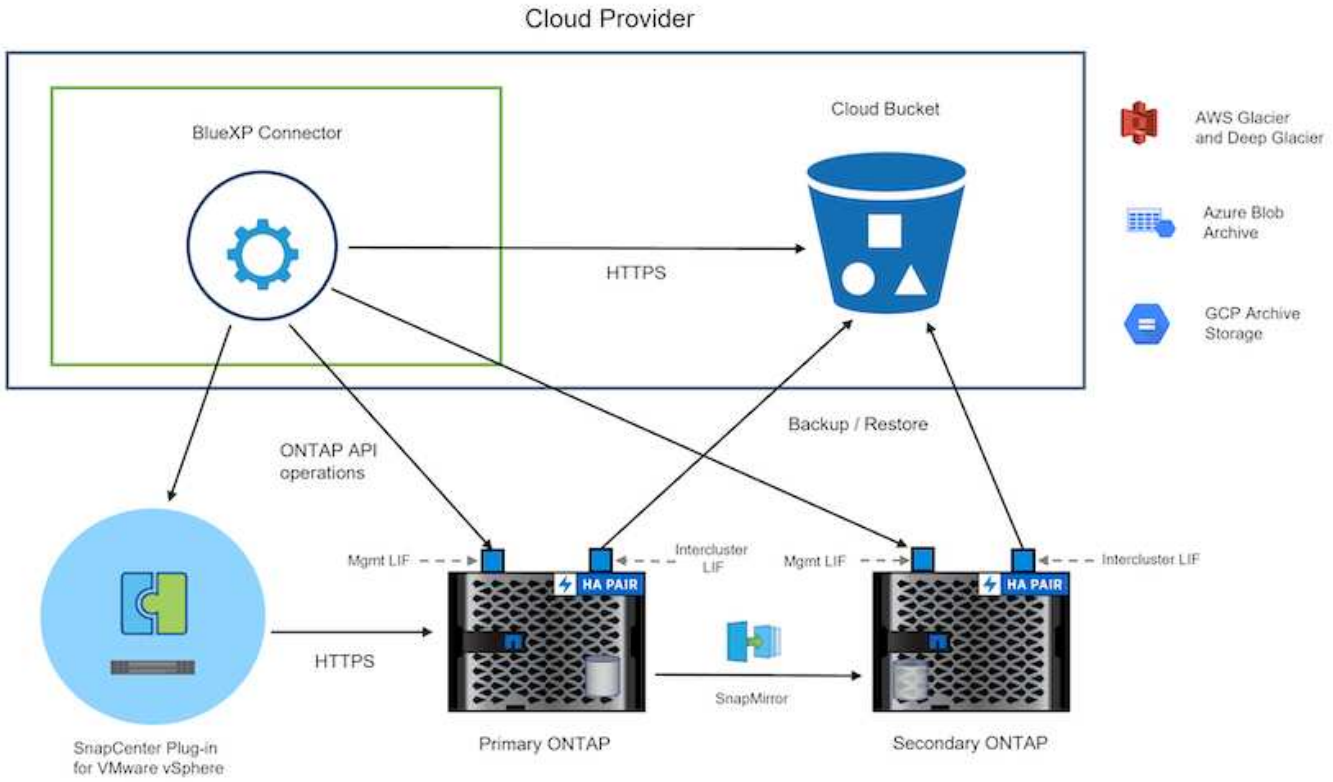
Der Zweck dieser Lösung besteht darin, den Datenschutz virtueller Maschinen zu demonstrieren, die in VMware vSphere ausgeführt werden und sich auf von NetApp ONTAP gehosteten NFS-Datenspeichern befinden. Diese Lösung setzt voraus, dass die folgenden Komponenten konfiguriert und einsatzbereit sind:

1. ONTAP -Speichercluster mit NFS- oder VMFS-Datenspeichern, verbunden mit VMware vSphere. Es werden sowohl NFS- als auch VMFS-Datenspeicher unterstützt. Für diese Lösung wurden NFS-Datenspeicher verwendet.
2. Sekundärer ONTAP Speichercluster mit SnapMirror -Beziehungen, die für Volumes eingerichtet wurden, die für NFS-Datenspeicher verwendet werden.
3. Console Agent für den Cloud-Anbieter installiert, der für Backups von Objektspeicher verwendet wird.

4. Zu sichernde virtuelle Maschinen befinden sich auf NFS-Datenspeichern, die sich auf dem primären ONTAP Speichercluster befinden.
5. Netzwerkverbindung zwischen dem Console Agent und den Management-Schnittstellen des lokalen ONTAP Storage-Clusters.
6. Netzwerkverbindung zwischen dem Console Agenten und der lokalen SCV Appliance VM sowie zwischen dem Console Agenten und vCenter.
7. Netzwerkkonnektivität zwischen den lokalen ONTAP Intercluster-LIFs und dem Objektspeicherdienst.
8. DNS für Management-SVM auf primären und sekundären ONTAP Speicherclustern konfiguriert. Weitere Informationen finden Sie unter "Konfigurieren Sie DNS für die Hostnamenauflösung" .

High-Level-Architektur

Die Prüfung/Validierung dieser Lösung wurde in einem Labor durchgeführt, das möglicherweise nicht der endgültigen Bereitstellungsumgebung entspricht.



Lösungsbereitstellung

In dieser Lösung werden detaillierte Anweisungen für das Deployment und die Validierung einer Lösung bereitgestellt, die das SnapCenter Plug-in for VMware vSphere zusammen mit Backup und Recovery nutzt, um das Backup und Recovery von Windows- und Linux-virtuellen Maschinen innerhalb eines VMware vSphere Clusters in einem lokalen Datacenter durchzuführen. Die virtuellen Maschinen in diesem Setup sind auf NFS-Datastores gespeichert, die von einem ONTAP A300 Storage-Cluster gehostet werden. Zusätzlich dient ein separates ONTAP A300 Storage-Cluster als sekundäres Ziel für Volumes, die mit SnapMirror repliziert werden. Darüber hinaus wurden Objektspeicher, die auf Amazon Web Services und Azure Blob gehostet werden, als Ziele für eine dritte Kopie der Daten eingesetzt.

Es folgt ein Überblick über die Erstellung von SnapMirror Beziehungen für sekundäre Kopien unserer von SCV verwalteten Backups sowie über die Konfiguration von Backup-Aufträgen sowohl in SCV als auch in NetApp

Console.

Ausführliche Informationen zum SnapCenter Plug-in for VMware vSphere finden Sie im "SnapCenter Plug-in for VMware vSphere Dokumentation" .

Detaillierte Informationen zu Backup und Recovery finden Sie in der "Dokumentation zu Datensicherung und Wiederherstellung".

Herstellen von SnapMirror -Beziehungen zwischen ONTAP Clustern

Das SnapCenter Plug-in for VMware vSphere verwendet die ONTAP SnapMirror -Technologie, um den Transport sekundärer SnapMirror und/oder SnapVault -Kopien zu einem sekundären ONTAP Cluster zu verwalten.

SCV-Sicherungsrichtlinien bieten die Möglichkeit, SnapMirror oder SnapVault -Beziehungen zu verwenden. Der Hauptunterschied besteht darin, dass bei Verwendung der SnapMirror -Option der in der Richtlinie für Backups konfigurierte Aufbewahrungsplan am primären und sekundären Standort derselbe ist. SnapVault ist für die Archivierung konzipiert und bei Verwendung dieser Option kann mit der SnapMirror -Beziehung ein separater Aufbewahrungsplan für die Snapshot-Kopien auf dem sekundären ONTAP Speichercluster erstellt werden.

Das Einrichten von SnapMirror Beziehungen kann in NetApp Console erfolgen, wo viele der Schritte automatisiert sind, oder mit System Manager und der ONTAP CLI. Alle diese Methoden werden im Folgenden erläutert.

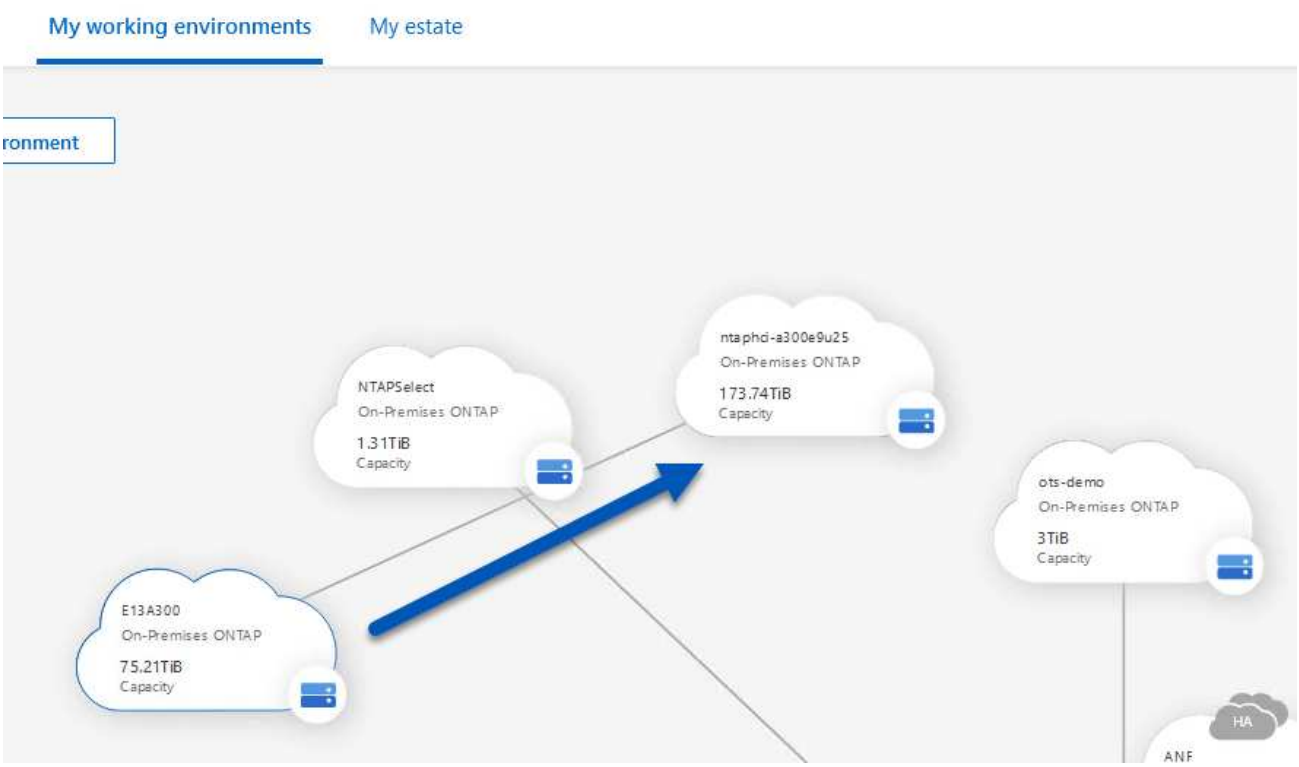
Einrichten von SnapMirror Beziehungen mit NetApp Console

Die folgenden Schritte sind in der NetApp Console auszuführen:

▼ **Replikations-Setup für primäre und sekundäre ONTAP Speichersysteme**

Zunächst erfolgt die Anmeldung bei der NetApp Console und die Navigation zu „Systeme“.

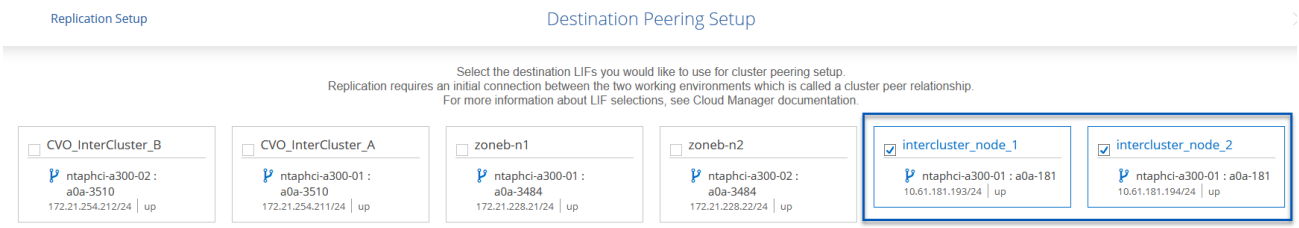
1. Ziehen Sie das Quell ONTAP -Speichersystem (primär) per Drag & Drop auf das Ziel ONTAP -Speichersystem (sekundär).



2. Wählen Sie im angezeigten Menü **Replikation** aus.

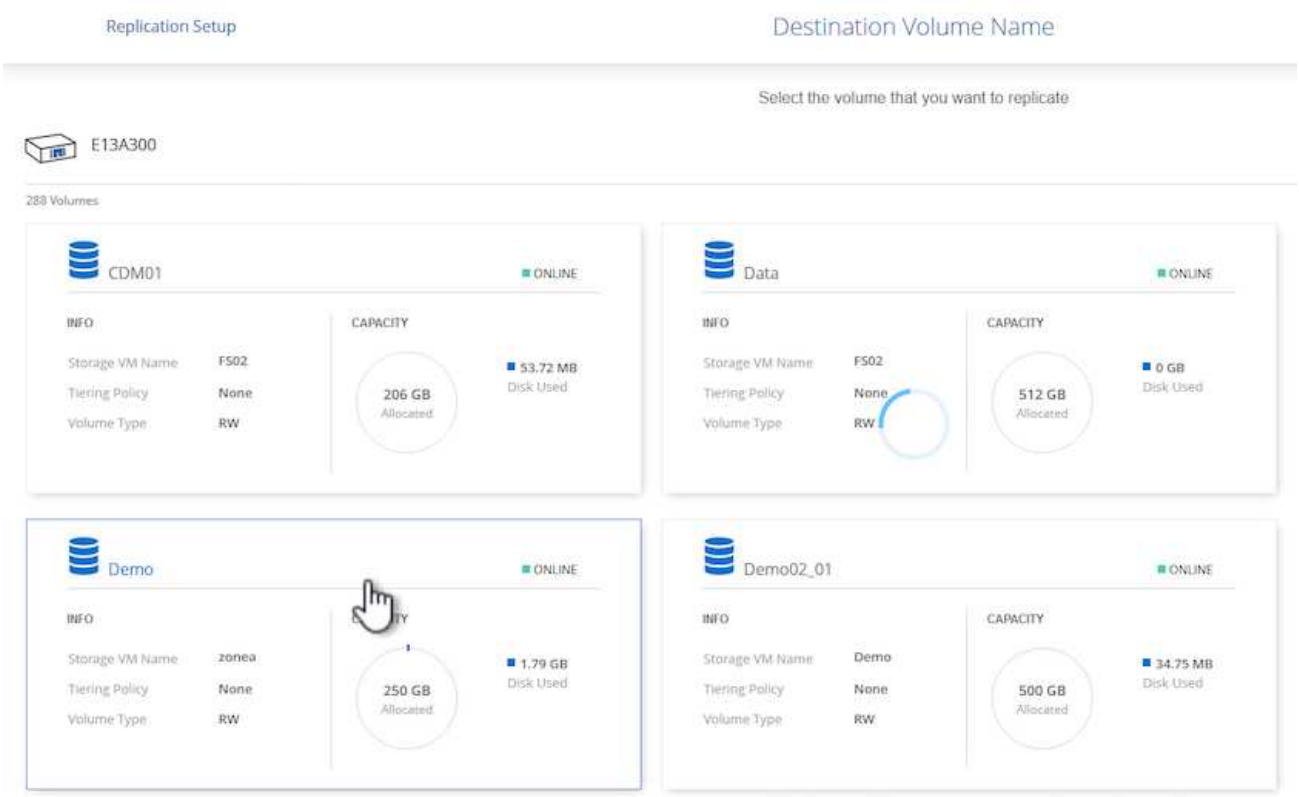


3. Wählen Sie auf der Seite **Destination Peering Setup** die Ziel-Intercluster-LIFs aus, die für die Verbindung zwischen Speichersystemen verwendet werden sollen.



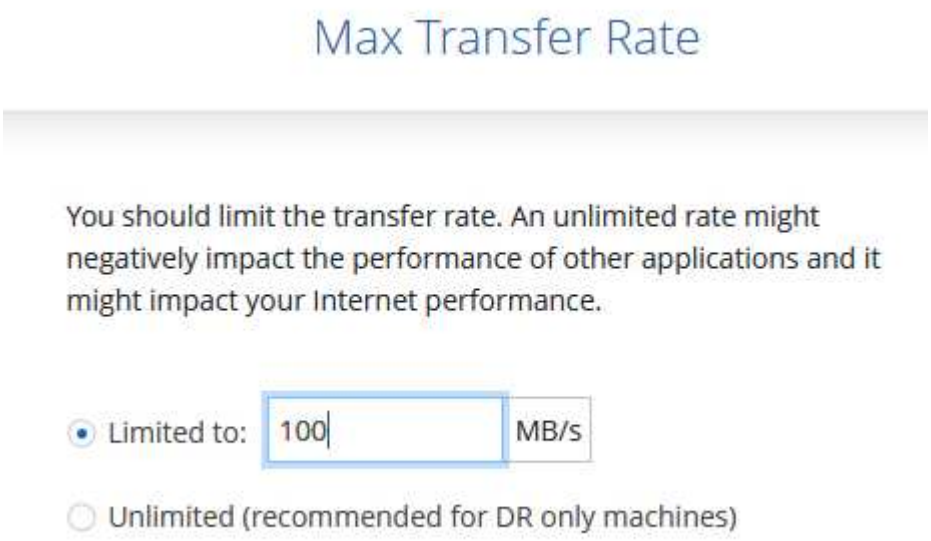
4. Wählen Sie auf der Seite **Zielvolumename** zuerst das Quellvolume aus, geben Sie dann den Zielvolumenamen ein und wählen Sie die Ziel-SVM und das Zielaggregat aus. Klicken Sie auf **Weiter**,

um fortzufahren.

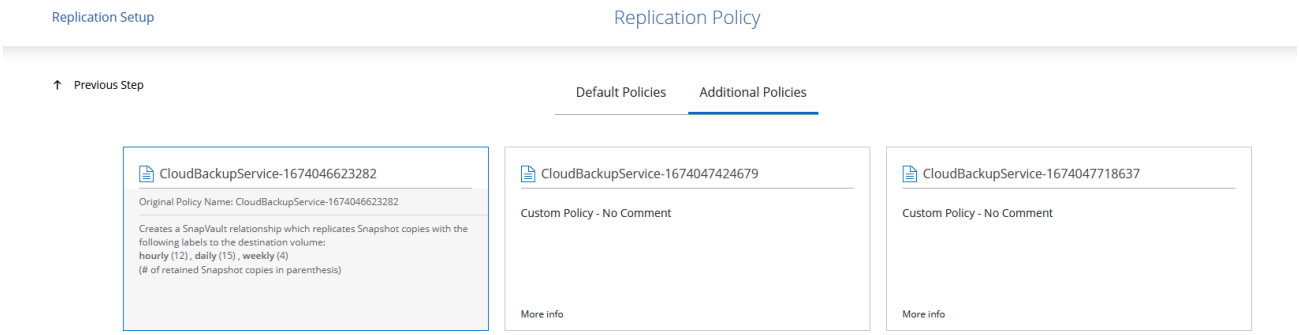




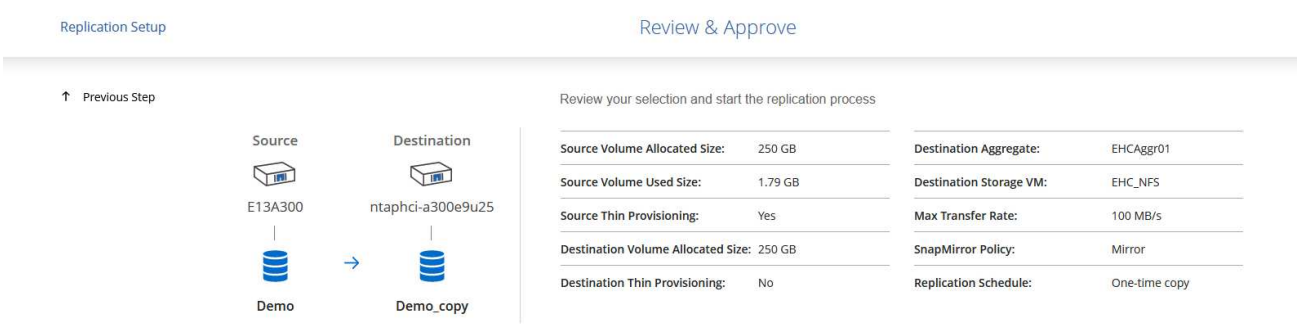
5. Wählen Sie die maximale Übertragungsrate für die Replikation.



6. Wählen Sie die Richtlinie aus, die den Aufbewahrungszeitplan für sekundäre Sicherungen bestimmt. Diese Richtlinie kann im Voraus erstellt werden (siehe den manuellen Prozess unten im Schritt **Erstellen einer Snapshot-Aufbewahrungsrichtlinie**) oder bei Bedarf nachträglich geändert werden.



7. Überprüfen Sie abschließend alle Informationen und klicken Sie auf die Schaltfläche **Los**, um den Replikationseinrichtungsprozess zu starten.



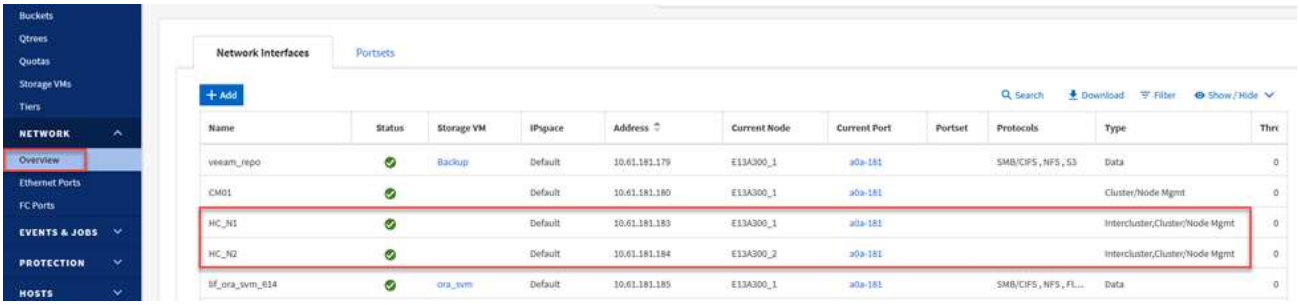
Stellen Sie SnapMirror -Beziehungen mit System Manager und ONTAP CLI her

Alle erforderlichen Schritte zum Herstellen von SnapMirror -Beziehungen können mit System Manager oder der ONTAP CLI durchgeführt werden. Der folgende Abschnitt enthält detaillierte Informationen zu beiden Methoden:

▼ **Notieren Sie die logischen Quell- und Zielschnittstellen zwischen Clustern.**

Für die Quell- und Ziel ONTAP Cluster können Sie die LIF-Informationen zwischen den Clustern vom System Manager oder von der CLI abrufen.

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



2. Um die Intercluster-IP-Adressen mithilfe der CLI abzurufen, führen Sie den folgenden Befehl aus:

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

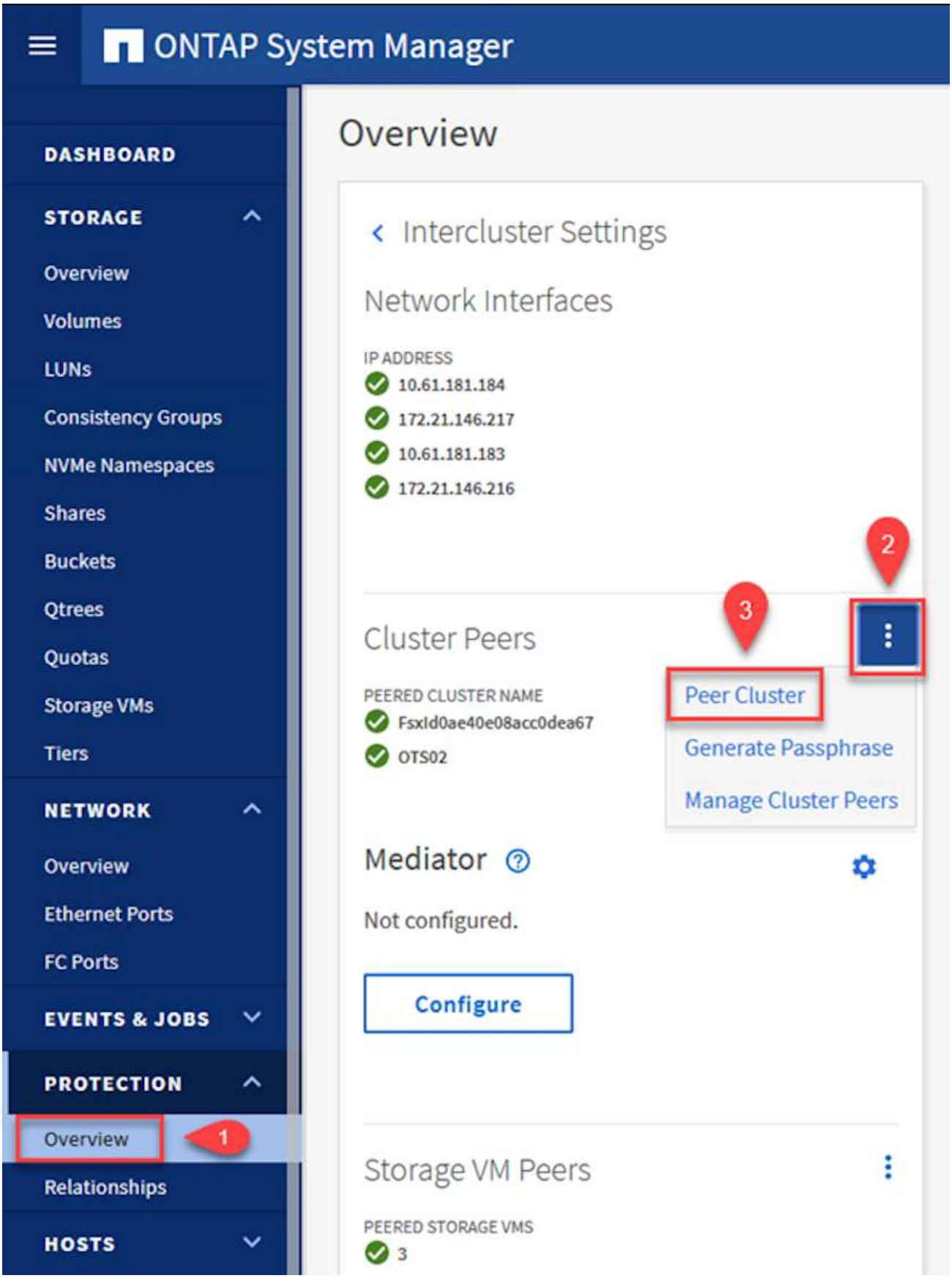
▼ **Cluster-Peering zwischen ONTAP -Clustern einrichten**

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

1. Richten Sie Peering auf dem Ziel ONTAP -Cluster ein, indem Sie `cluster peer create` Befehl. Geben Sie bei entsprechender Aufforderung 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 Quellcluster können Sie die Cluster-Peer-Beziehung entweder mit ONTAP System Manager oder der CLI herstellen. Navigieren Sie im ONTAP System Manager zu „Schutz > Übersicht“ und wählen Sie „Peer-Cluster“ aus.



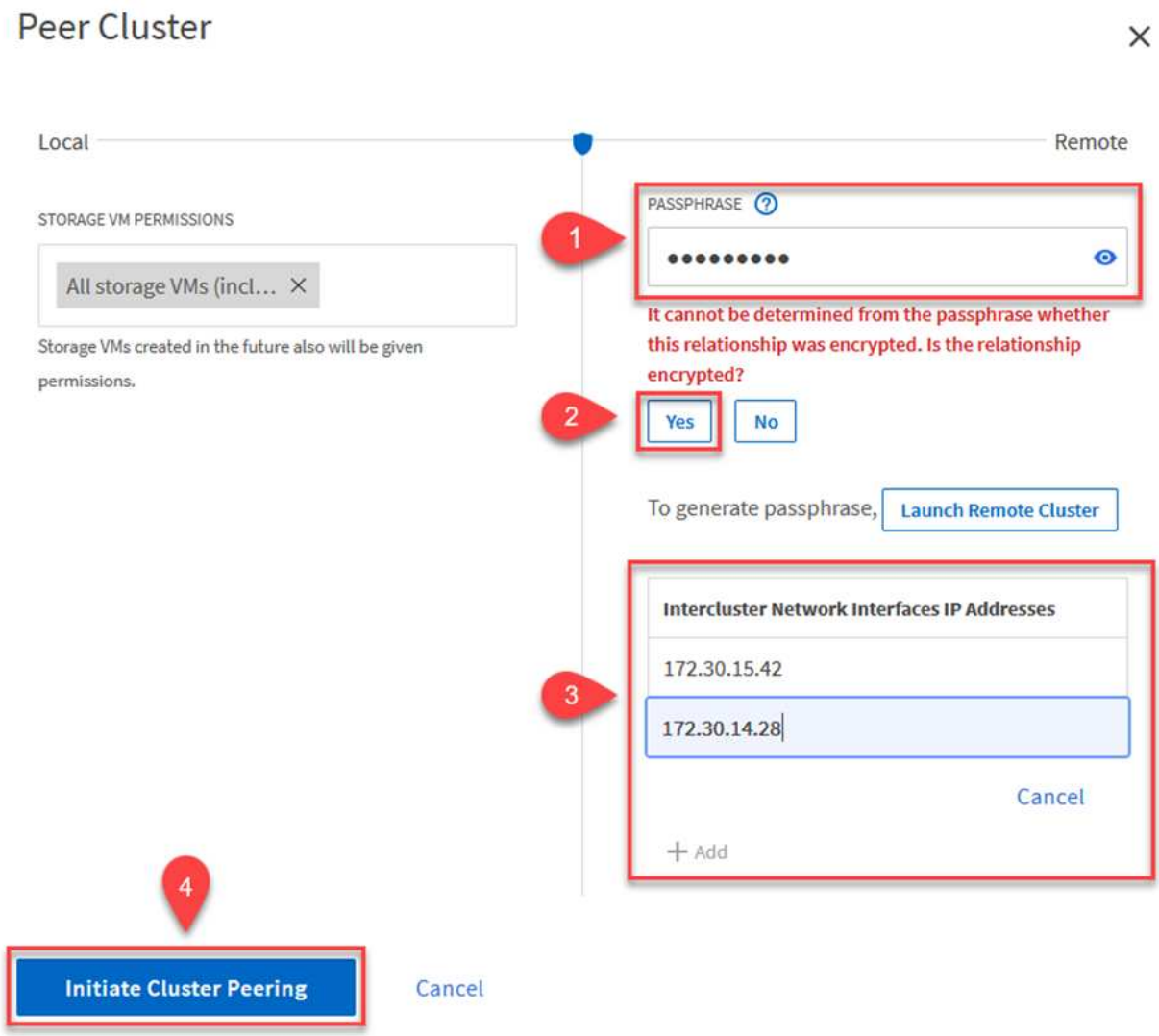
3. Geben Sie im Dialogfeld „Peer-Cluster“ die erforderlichen Informationen ein:
   a. Geben Sie die Passphrase ein, die zum Herstellen der Peer-Cluster-Beziehung auf dem Ziel ONTAP

Cluster verwendet wurde.

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

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

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



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

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

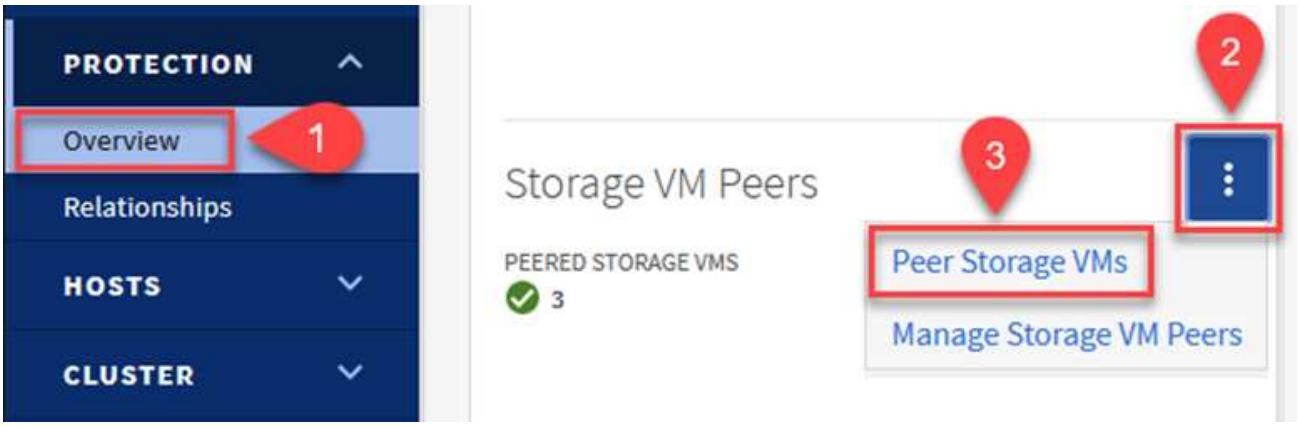
▼ **Herstellen einer SVM-Peering-Beziehung**

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

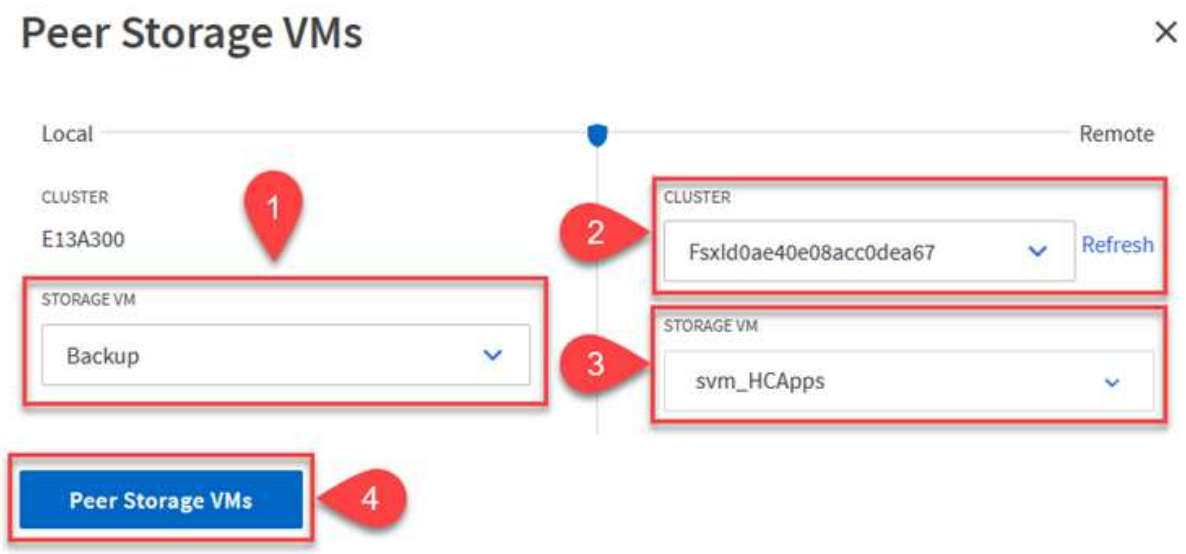
1. Verwenden Sie vom Ziel ONTAP Cluster aus den folgenden Befehl aus der CLI, um die SVM-Peer-Beziehung zu erstellen:

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

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



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



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

▼ **Erstellen einer Snapshot-Aufbewahrungsrichtlinie**

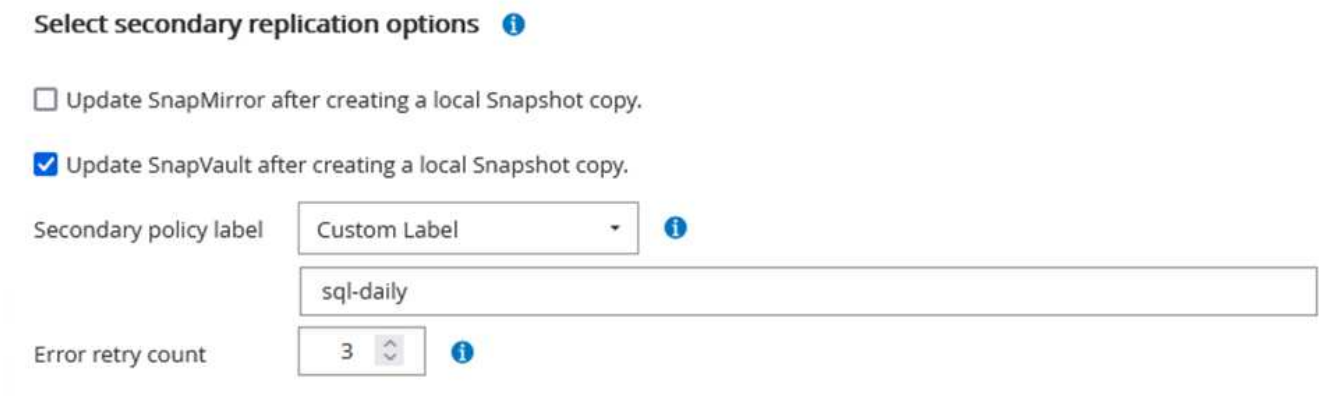
SnapCenter verwaltet Aufbewahrungspläne für Backups, die als Snapshot-Kopien auf dem primären Speichersystem vorhanden sind. Dies wird beim Erstellen einer Richtlinie in SnapCenter festgelegt. SnapCenter verwaltet keine Aufbewahrungsrichtlinien für Backups, die auf sekundären Speichersystemen

aufbewahrt werden. Diese Richtlinien werden separat über eine SnapMirror -Richtlinie verwaltet, die auf dem sekundären FSx-Cluster erstellt und den Zielvolumes zugeordnet wird, die in einer SnapMirror -Beziehung mit dem Quellvolume stehen.

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

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

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



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

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

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

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

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

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

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

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy
```

```
Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

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

▼ **Zielvolumes erstellen**

Um ein Zielvolume auf ONTAP zu erstellen, das Snapshot-Kopien von unseren Quellvolumes empfängt, 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
```

▼ **Erstellen Sie die SnapMirror -Beziehungen zwischen Quell- und Zielvolumes**

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

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

▼ **Initialisieren Sie die SnapMirror -Beziehungen**

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

Um ein Volume zu erstellen, führen Sie den folgenden Befehl auf dem Ziel ONTAP -Cluster aus:

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

Konfigurieren des SnapCenter Plug-in for VMware vSphere

Nach der Installation kann über die Verwaltungsschnittstelle der vCenter Server Appliance auf das SnapCenter Plug-in for VMware vSphere zugegriffen werden. SCV verwaltet Backups für die auf den ESXi-Hosts bereitgestellten NFS-Datenspeicher, die die Windows- und Linux-VMs enthalten.

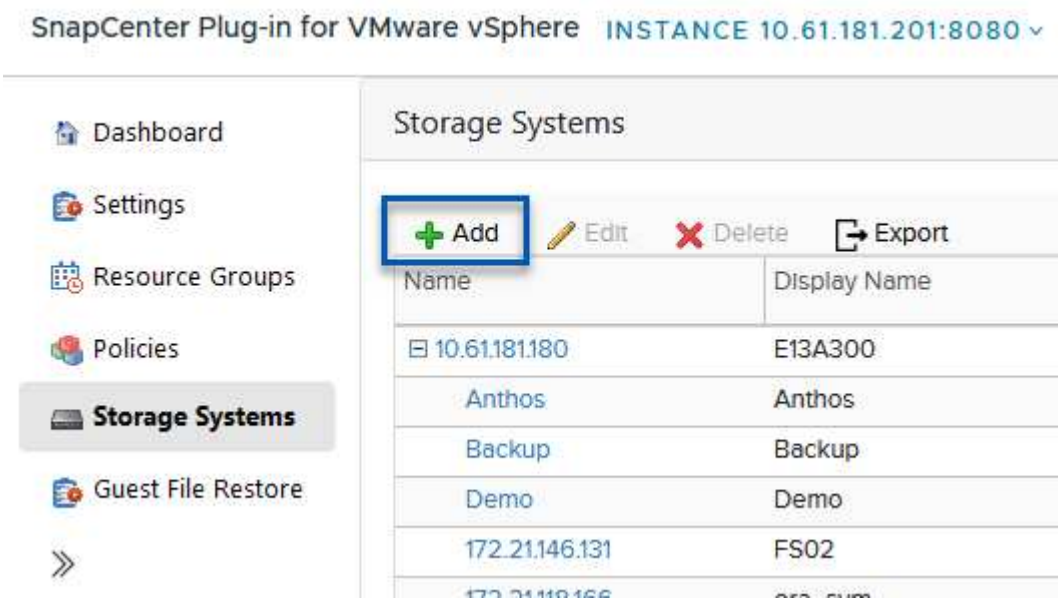
Überprüfen Sie die "Datenschutz-Workflow" Weitere Informationen zu den Schritten zum Konfigurieren von Sicherungen finden Sie im Abschnitt „Sicherungskonfiguration“ der SCV-Dokumentation.

Um Sicherungen Ihrer virtuellen Maschinen und Datenspeicher zu konfigurieren, müssen die folgenden Schritte über die Plug-In-Schnittstelle ausgeführt werden.

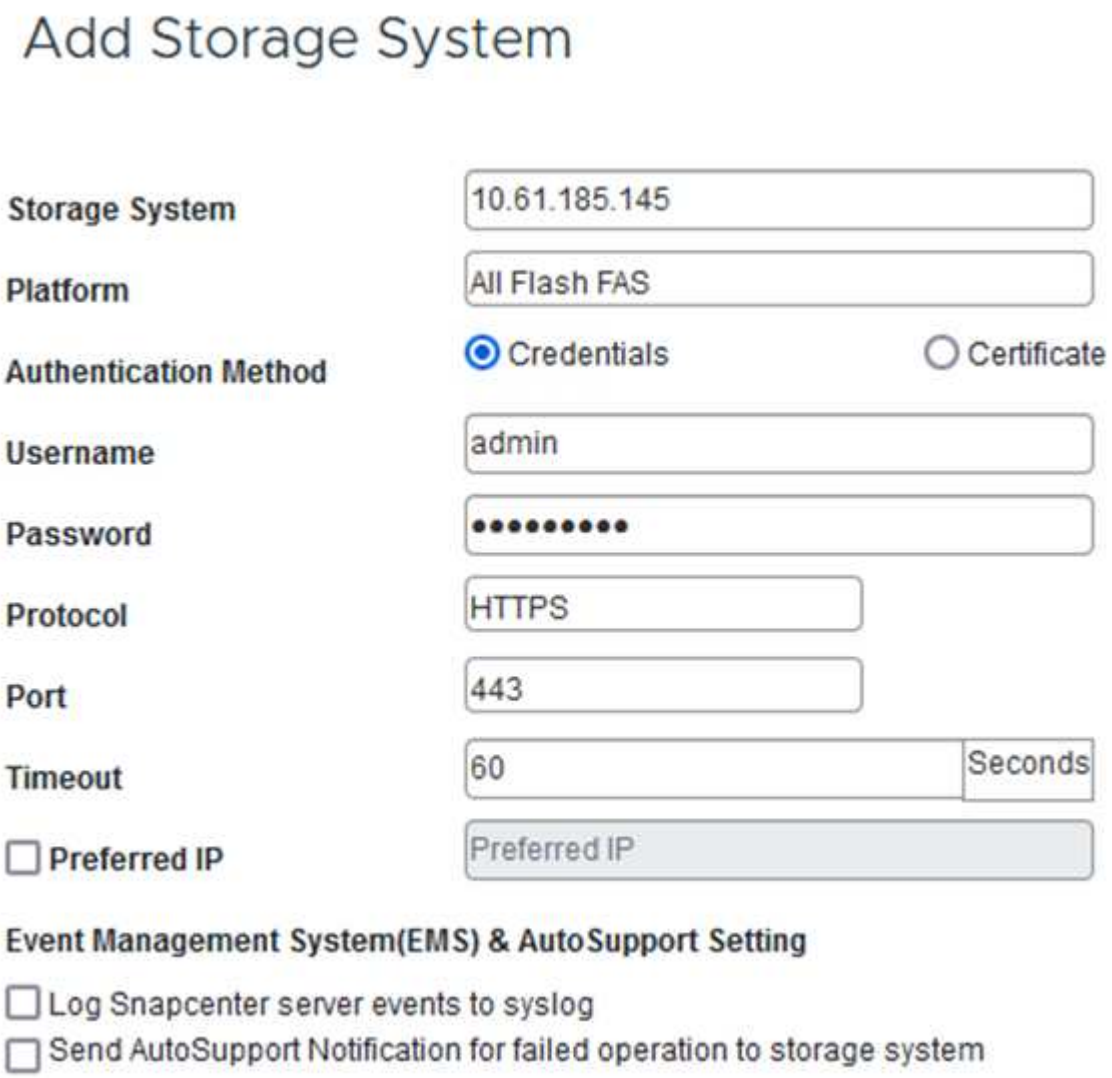
▼ **Discovery ONTAP -Speichersysteme**

Entdecken Sie die ONTAP Speichercluster, die sowohl für primäre als auch für sekundäre Backups verwendet werden sollen.

1. Navigieren Sie im SnapCenter Plug-in for VMware vSphere im linken Menü zu **Speichersysteme** und klicken Sie auf die Schaltfläche **Hinzufügen**.



2. Geben Sie die Anmeldeinformationen und den Plattformtyp für das primäre ONTAP Speichersystem ein und klicken Sie auf **Hinzufügen**.



3. Wiederholen Sie diesen Vorgang für das sekundäre ONTAP Speichersystem.

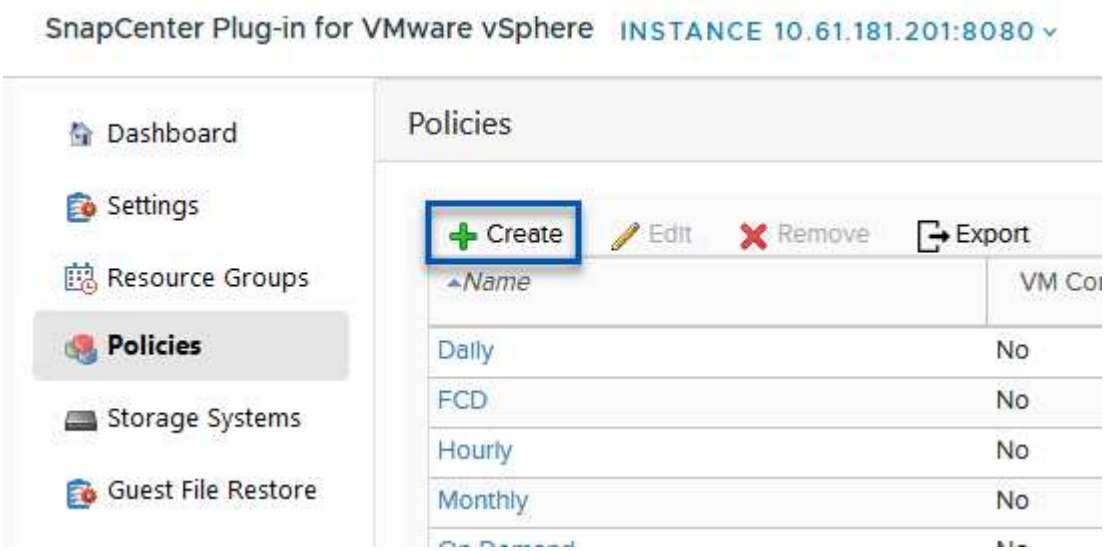
▼ **Erstellen von SCV-Sicherungsrichtlinien**

Richtlinien legen die Aufbewahrungsdauer, Häufigkeit und Replikationsoptionen für die von SCV verwalteten Backups fest.

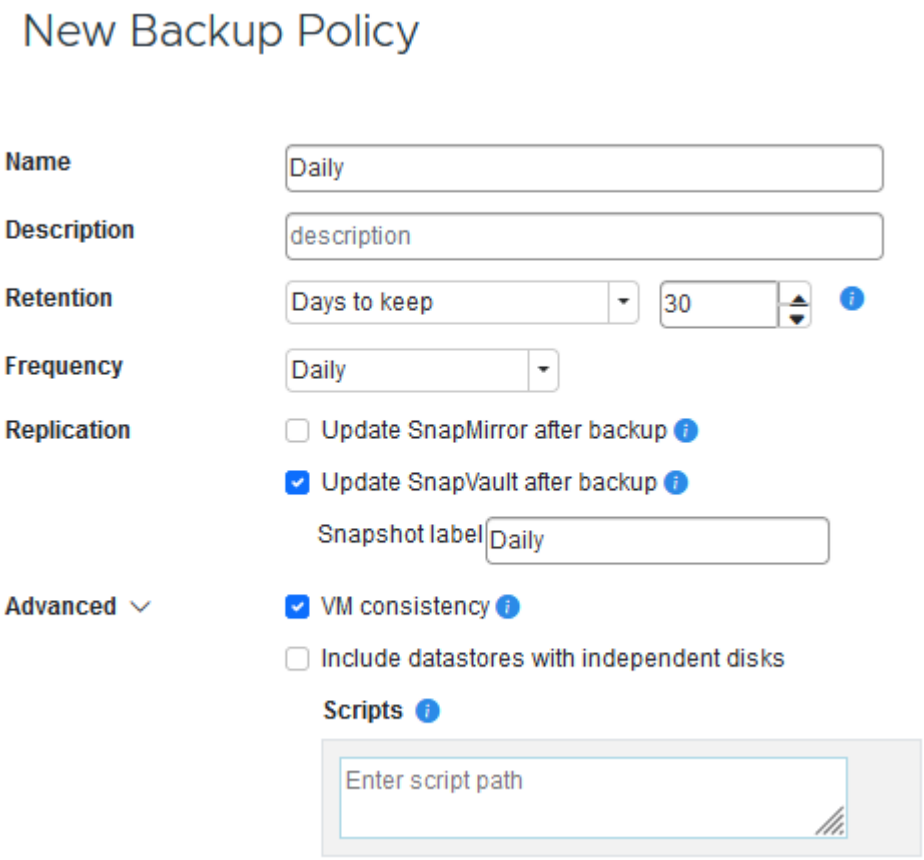
Überprüfen Sie die "Erstellen Sie Sicherungsrichtlinien für VMs und Datenspeicher" Weitere Informationen finden Sie im Abschnitt der Dokumentation.

Führen Sie zum Erstellen von Sicherungsrichtlinien die folgenden Schritte aus:

1. Navigieren Sie im SnapCenter Plug-in for 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 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 Aufbewahrungszeitplan für die primären und sekundären Snapshots derselbe. Wenn Sie SnapVault wählen, basiert der Aufbewahrungszeitplan für den sekundären Snapshot auf einem separaten Zeitplan, der mit der SnapMirror -Beziehung implementiert wird. Dies ist nützlich, wenn Sie längere Aufbewahrungszeiträume für sekundäre Sicherungen wünschen.

Snapshot-Bezeichnungen sind nützlich, da sie zur Festlegung von Richtlinien mit einer bestimmten Aufbewahrungsdauer für die auf den sekundären ONTAP Cluster replizierten SnapVault Kopien verwendet werden können. Bei Verwendung von SCV mit NetApp Data Services muss das Feld für die Snapshot-Bezeichnung entweder leer sein oder der in der Backup-Richtlinie angegebenen Bezeichnung entsprechen.

3. Wiederholen Sie den Vorgang für jede erforderliche Richtlinie. Beispielsweise separate Richtlinien für tägliche, wöchentliche und monatliche Backups.

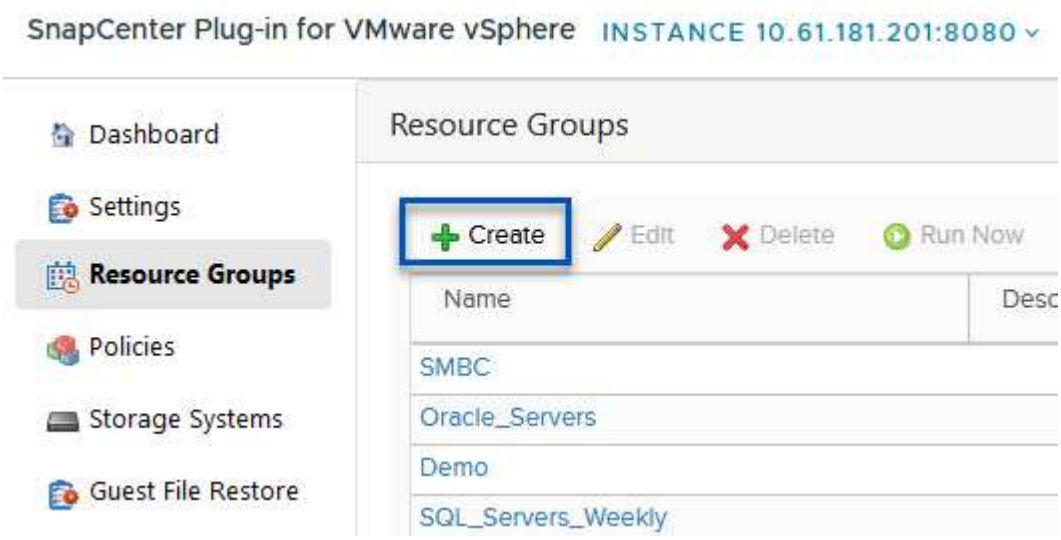
▼ **Erstellen von Ressourcengruppen**

Ressourcengruppen enthalten die Datenspeicher und virtuellen Maschinen, die in einen Sicherungsauftrag einbezogen werden sollen, zusammen mit der zugehörigen Richtlinie und dem Sicherungszeitplan.

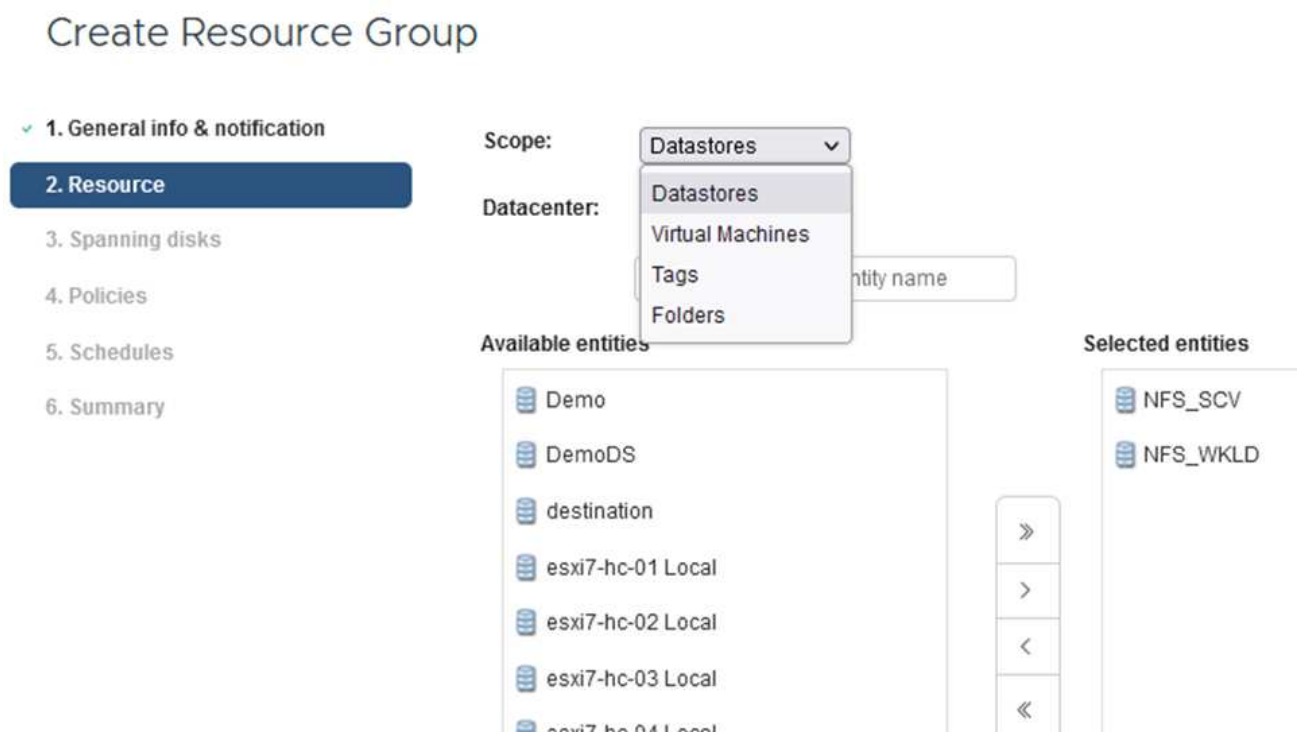
Überprüfen Sie die "Erstellen von Ressourcengruppen" Weitere Informationen finden Sie im Abschnitt der Dokumentation.

Führen Sie zum Erstellen von Ressourcengruppen die folgenden Schritte aus.

1. Navigieren Sie im SnapCenter Plug-in for VMware vSphere im linken Menü zu **Ressourcengruppen** und klicken Sie auf die Schaltfläche **Erstellen**.



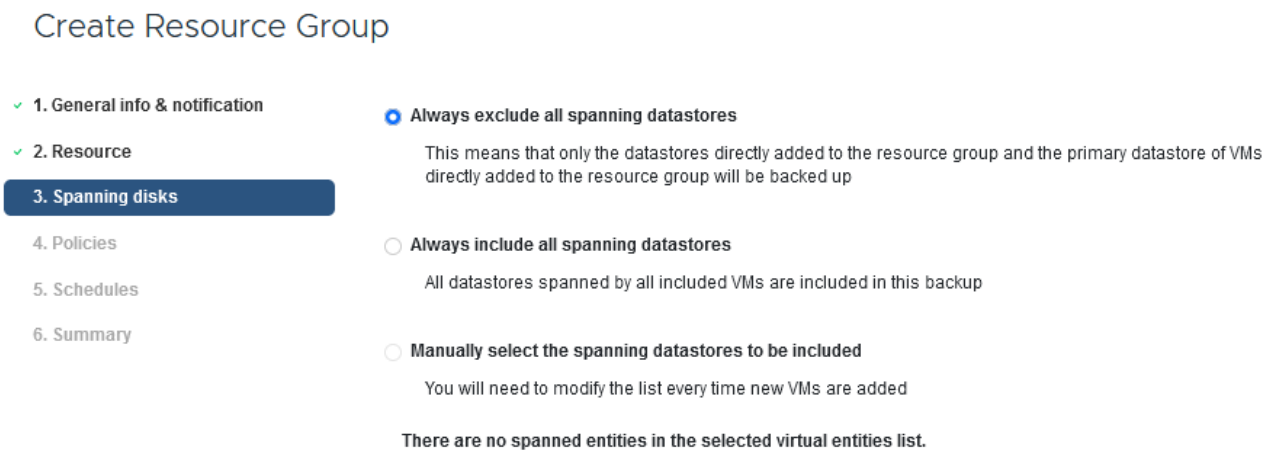
2. Geben Sie im Assistenten „Ressourcengruppe erstellen“ einen Namen und eine Beschreibung für die Gruppe sowie die zum Empfangen von Benachrichtigungen erforderlichen Informationen ein. Klicken Sie auf **Weiter**
3. Wählen Sie auf der nächsten Seite die Datenspeicher und virtuellen Maschinen aus, die in den Sicherungsauftrag einbezogen werden sollen, und klicken Sie dann auf **Weiter**.



Sie haben die Möglichkeit, bestimmte VMs oder ganze Datenspeicher auszuwählen. Unabhängig davon, welche Option Sie auswählen, wird das gesamte Volume (und der Datenspeicher) gesichert, da die Sicherung das Ergebnis der Erstellung eines Snapshots des zugrunde liegenden Volumes ist. In den meisten Fällen ist es am einfachsten, den gesamten Datenspeicher auszuwählen. Wenn Sie jedoch die Liste der verfügbaren VMs beim Wiederherstellen einschränken möchten, können Sie nur eine Teilmenge der VMs

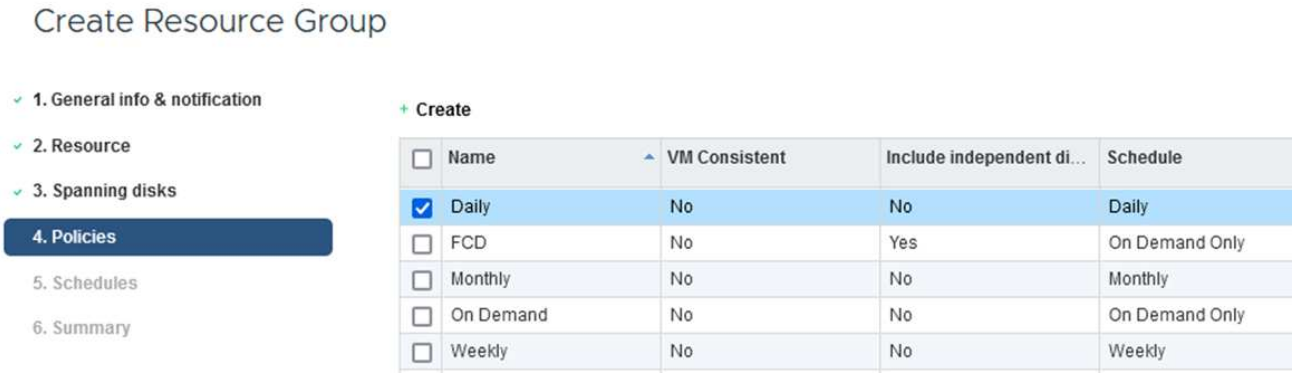
für die Sicherung auswählen.

4. Wählen Sie Optionen zum Überspannen von Datenspeichern für VMs mit VMDKs, die sich auf mehreren Datenspeichern befinden, und klicken Sie dann auf **Weiter**.



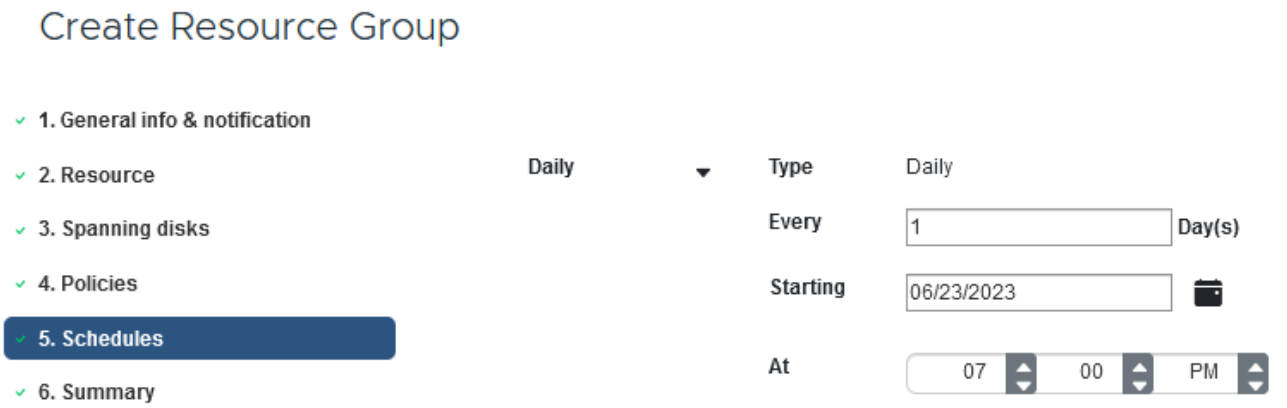
Backup und Recovery zum Schutz von VMware Workloads unterstützt derzeit keine Sicherung von VMs mit VMDKs, die sich über mehrere Datastores erstrecken.

5. Wählen Sie auf der nächsten Seite die Richtlinien aus, die der Ressourcengruppe zugeordnet werden sollen, und klicken Sie auf **Weiter**.



Beim Sichern von SCV-verwalteten Snapshots in Objekt-Storage mithilfe von Backup and Recovery kann jede Ressourcengruppe nur einer einzigen Richtlinie zugeordnet werden.

6. Wählen Sie einen Zeitplan aus, der bestimmt, zu welchen Zeiten die Sicherungen ausgeführt werden. Klicken Sie auf **Weiter**.

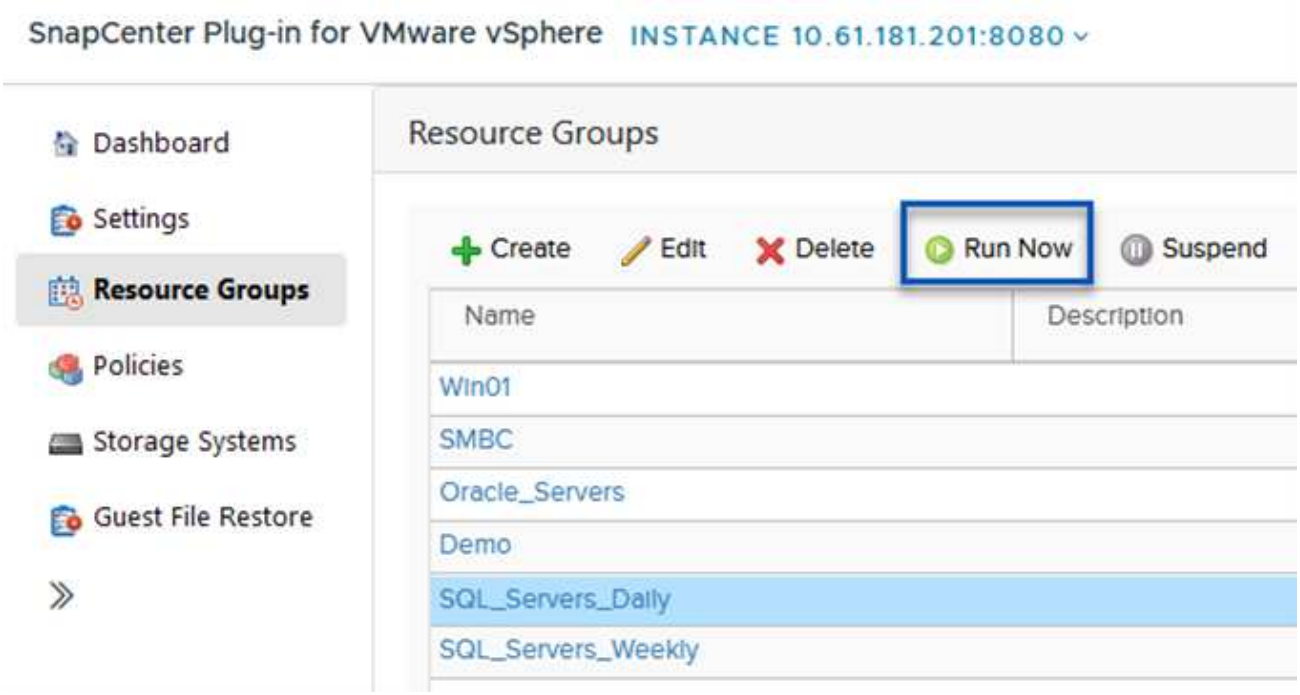


7. Überprüfen Sie abschließend die Übersichtsseite und klicken Sie dann auf **Fertig**, um die Erstellung der Ressourcengruppe abzuschließen.

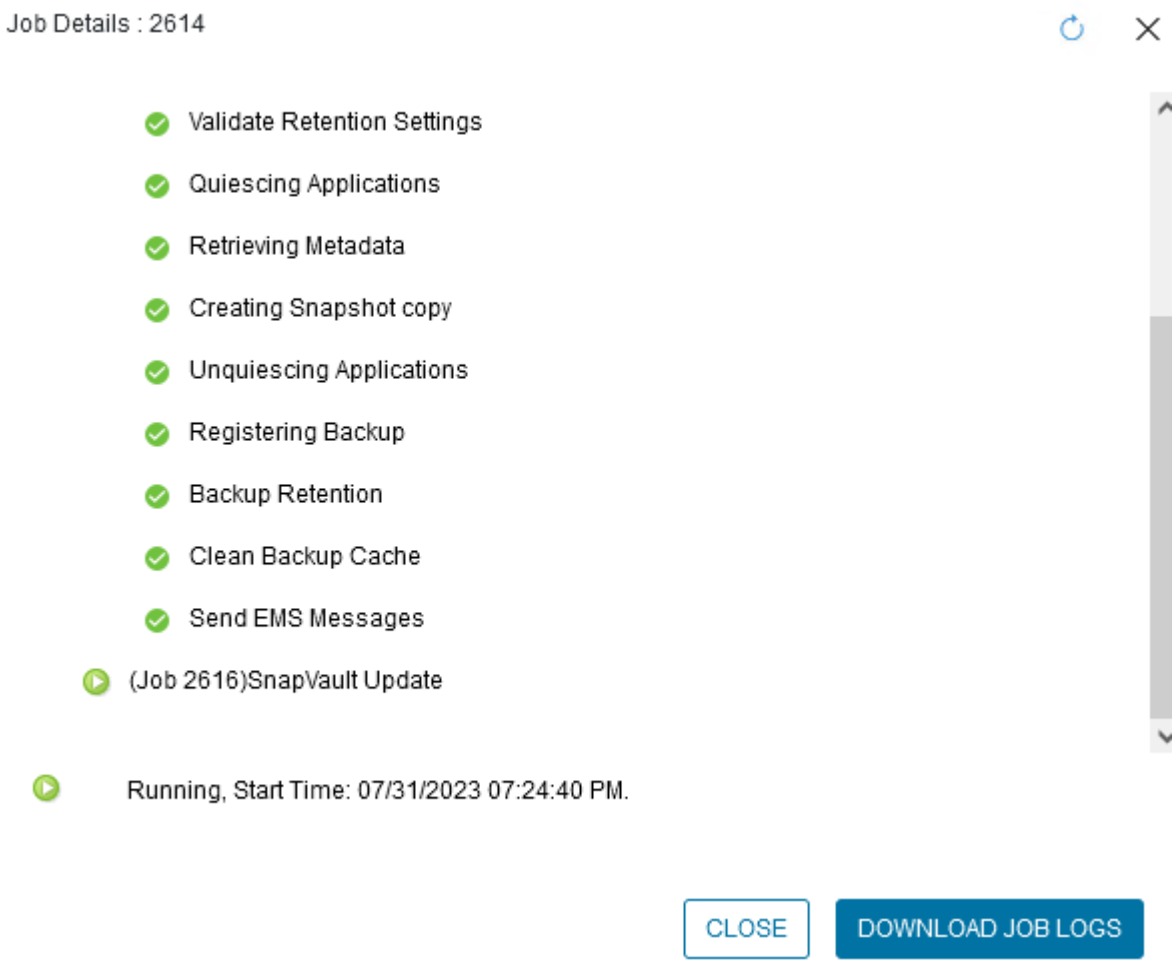
▼ **Ausführen eines Sicherungsauftrags**

In diesem letzten Schritt wird ein Sicherungsauftrag ausgeführt und sein Fortschritt überwacht. Mindestens ein Sicherungsauftrag muss in SCV erfolgreich abgeschlossen sein, bevor Ressourcen in der NetApp Console identifiziert werden können.

1. Navigieren Sie im SnapCenter Plug-in for VMware vSphere im linken Menü zu **Ressourcengruppen**.
2. Um einen Sicherungsauftrag 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 **Letzte Jobaktivitäten** auf die Job-ID-Nummer, um den Jobfortschritt zu überwachen.



Konfigurieren von Backups in Objektspeicher in NetApp Console

Damit NetApp Console die Dateninfrastruktur effektiv managen kann, ist die vorherige Installation eines Console Agenten erforderlich. Der Console Agent führt die Aktionen zur Identifizierung von Ressourcen und zum Managen von Datenvorgängen aus.

Weitere Informationen zum Console Agenten finden Sie "Informationen zu Console Agents" in der NetApp Console Dokumentation.

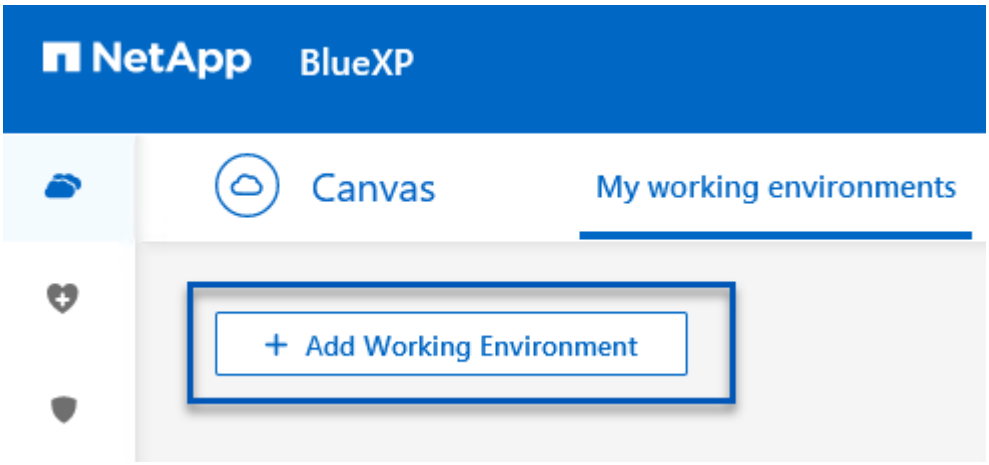
Sobald der Agent für den verwendeten Cloud-Anbieter installiert ist, ist in den Systemen eine grafische Darstellung des Objektspeichers sichtbar.

Um Backup und Recovery so zu konfigurieren, dass die von SCV lokal verwalteten Daten gesichert werden, sind die folgenden Schritte erforderlich:

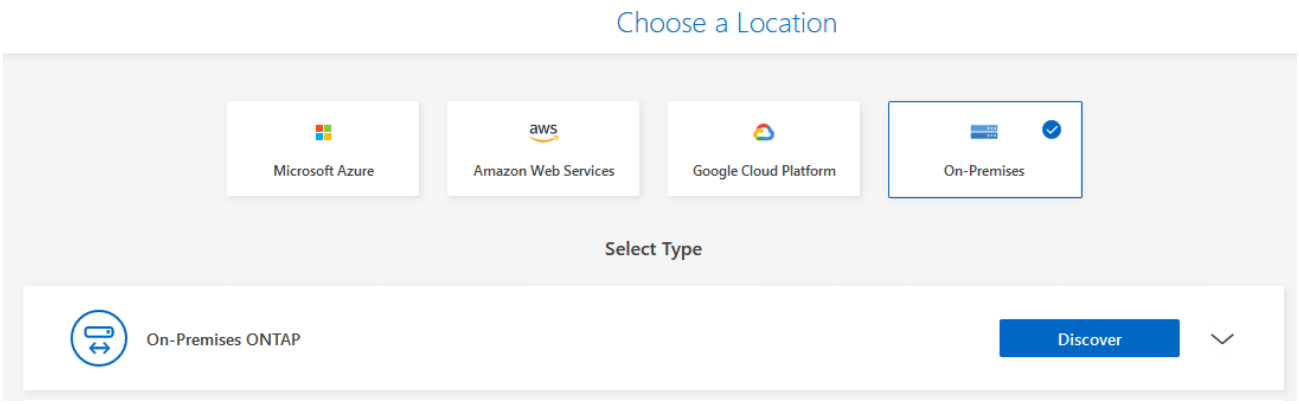
▼ **ONTAP Storage-System zu Systems hinzufügen**

Der erste Schritt besteht darin, die lokalen ONTAP Storage-Systeme zu NetApp Console hinzuzufügen.

1. Unter „Systems“ beginnt der Vorgang mit **+ Add**.



2. Wählen Sie aus der Standortauswahl **On-Premises** aus und klicken Sie dann auf die Schaltfläche **Discover**.



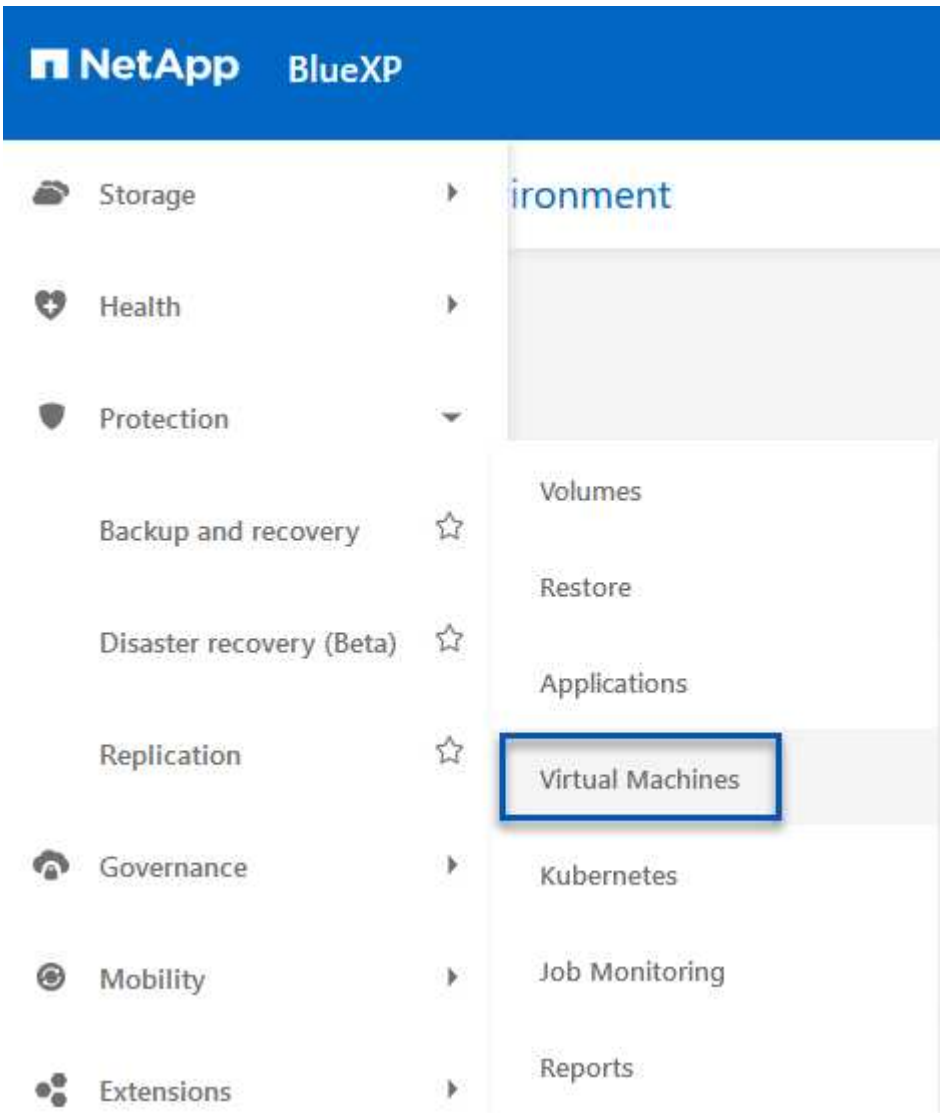
3. Geben Sie die Anmeldeinformationen für das ONTAP Speichersystem ein und klicken Sie auf die Schaltfläche **Erkennen**, um die Arbeitsumgebung hinzuzufügen.



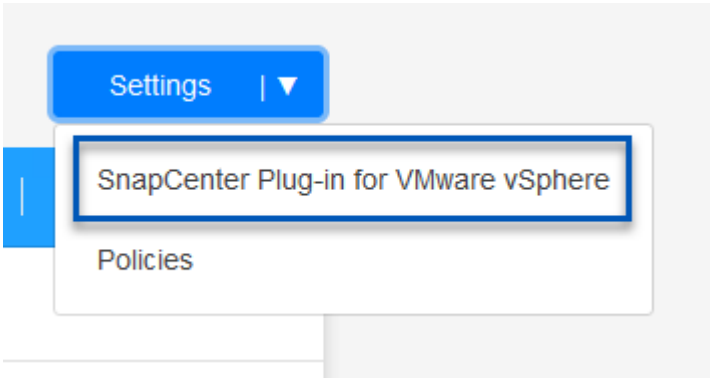
▼ **Entdecken Sie lokale SCV-Geräte und vCenter**

Um den lokalen Datenspeicher und die virtuellen Maschinenressourcen zu ermitteln, fügen Sie Informationen für den SCV-Datenbroker und Anmeldeinformationen für die vCenter-Verwaltungs-Appliance hinzu.

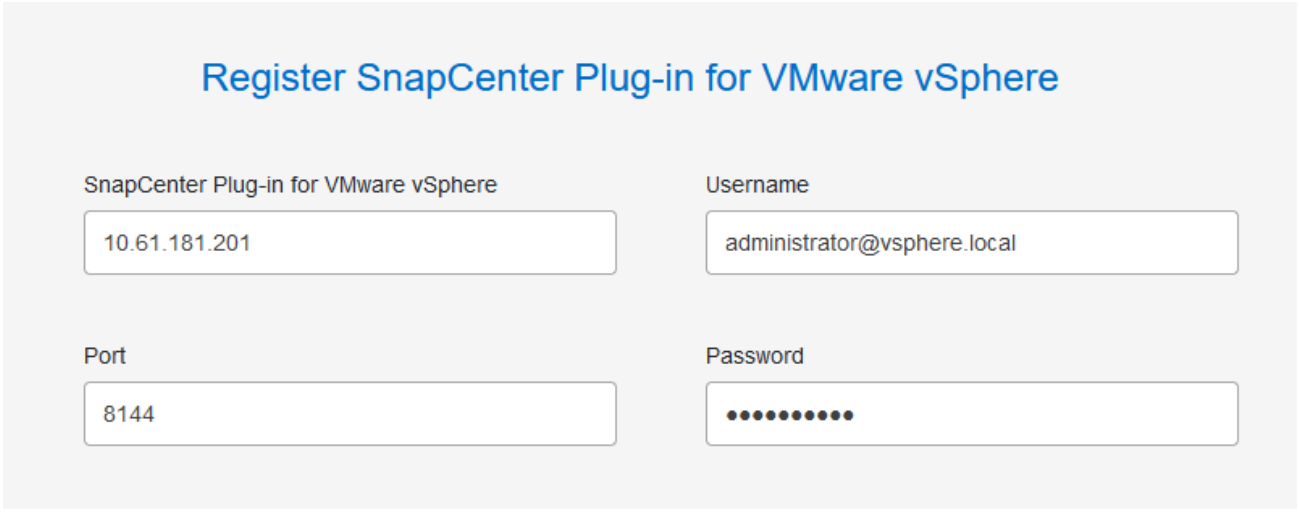
1. Über die Auswahl **Protection > Backup und Recovery > Workloads > VMware** im linken Menü der NetApp Console



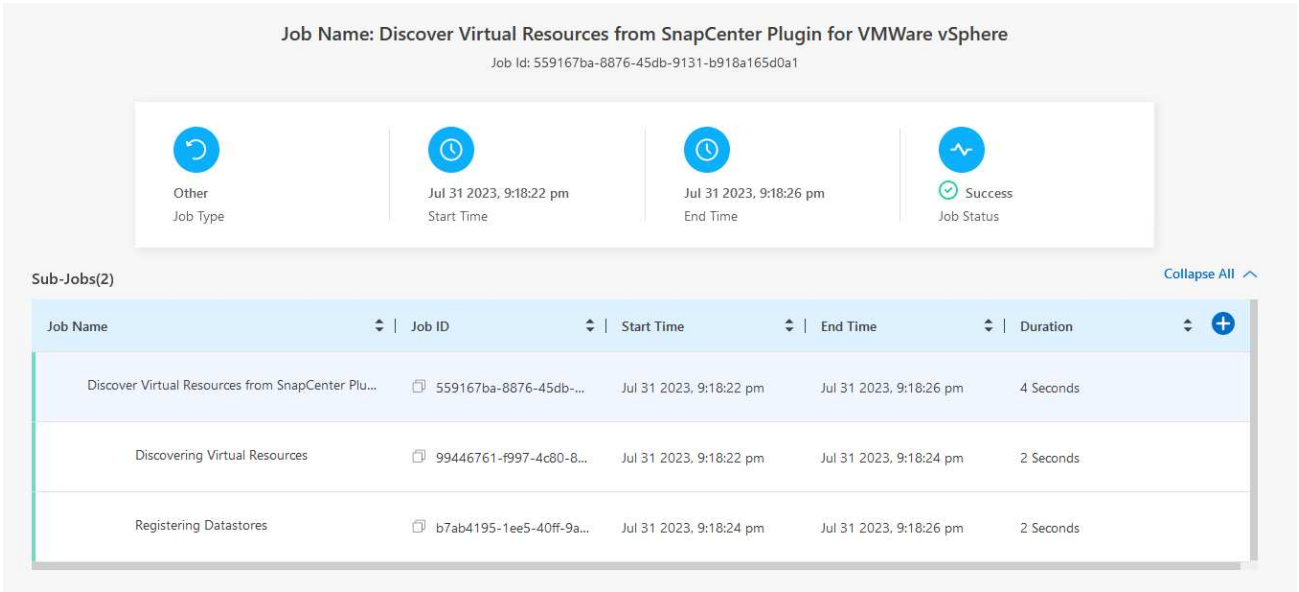
2. Rufen Sie vom Hauptbildschirm der virtuellen Maschinen aus das Dropdown-Menü **Einstellungen** auf und wählen Sie * SnapCenter Plug-in for VMware vSphere* aus.



3. Klicken Sie auf die Schaltfläche **Registrieren** und geben Sie dann die IP-Adresse und Portnummer für das SnapCenter Plug-in-Gerät sowie den Benutzernamen und das Kennwort für das vCenter-Verwaltungsgerät ein. Klicken Sie auf die Schaltfläche **Registrieren**, um den Erkennungsprozess zu starten.

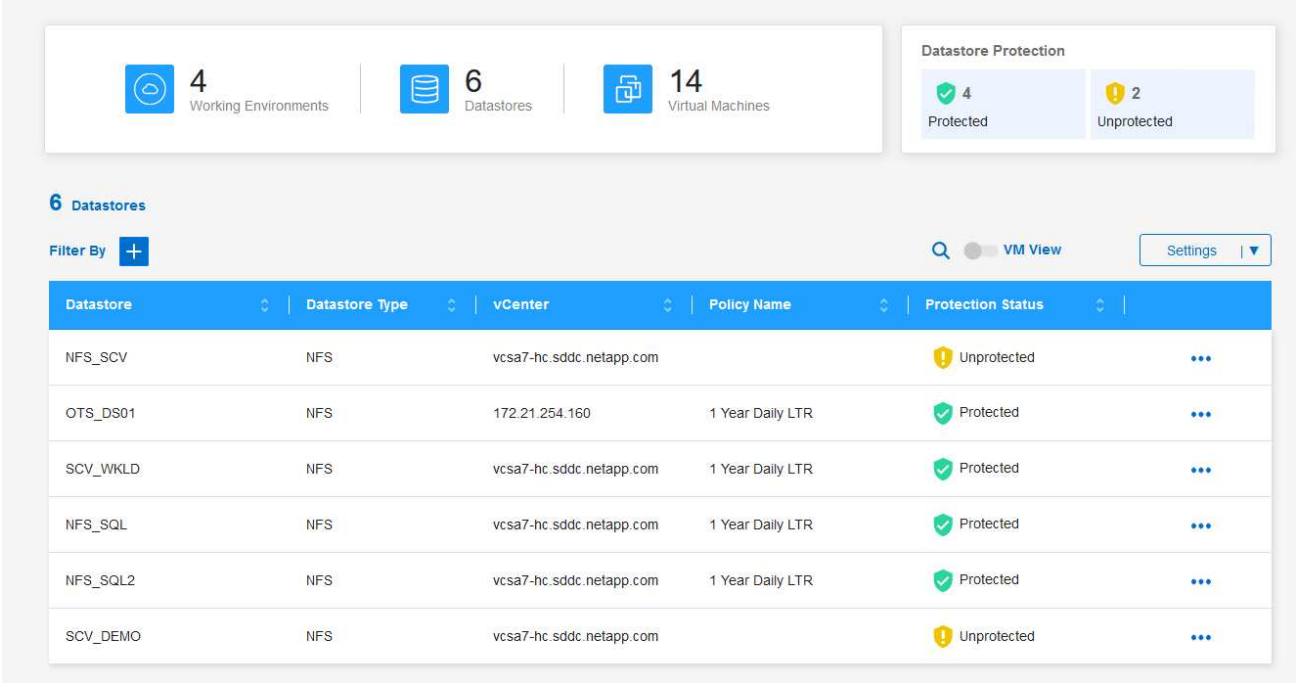


4. Der Fortschritt von Jobs kann auf der Registerkarte „Jobüberwachung“ überwacht werden.



5. Sobald die Erkennung abgeschlossen ist, können Sie die Datenspeicher und virtuellen Maschinen auf

allen erkannten SCV-Geräten anzeigen.

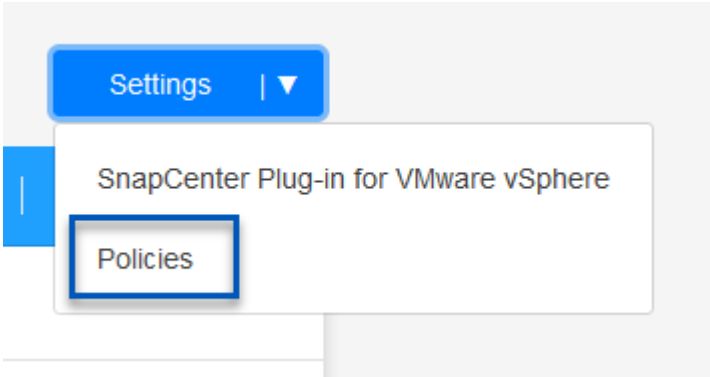


▼ Erstellen von Sicherungsrichtlinien

In NetApp Backup and Recovery for Virtual Machines lassen sich Richtlinien erstellen, mit denen die Aufbewahrungsfrist, die Backup-Quelle und die Archivierungsrichtlinie festgelegt werden.

Weitere Informationen zur Erstellung von Schutzgruppen finden Sie unter "Erstellen Sie eine Schutzgruppe".

1. Auf der Hauptseite von NetApp Backup and Recovery for Virtual Machines kann über das Dropdown-Menü **Settings** auf **Policies** zugegriffen werden.



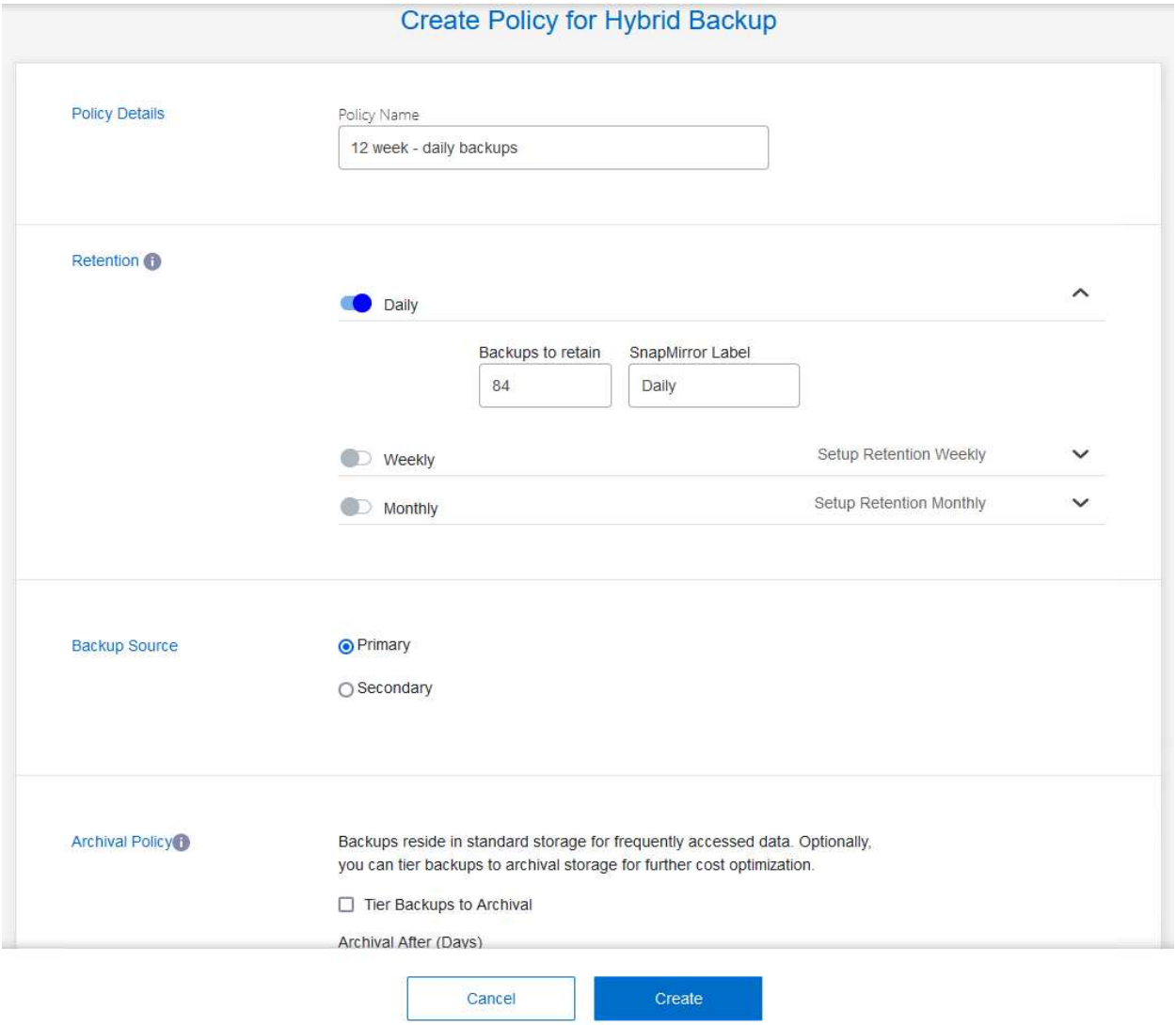
2. Klicken Sie auf **Richtlinie erstellen**, um auf das Fenster **Richtlinie für Hybrid-Backup erstellen** zuzugreifen.

   a. Fügen Sie einen Namen für die Richtlinie hinzu

   b. Wählen Sie die gewünschte Aufbewahrungsdauer

   c. Wählen Sie aus, ob die Backups vom primären oder sekundären lokalen ONTAP Speichersystem stammen sollen

   d. Geben Sie optional an, nach welchem Zeitraum die Sicherungen in den Archivspeicher verschoben werden, um zusätzliche Kosten zu sparen.



Das hier eingegebene SnapMirror -Label wird verwendet, um zu identifizieren, auf welche Backups die Richtlinie angewendet werden soll. Der Bezeichnungsname muss mit dem Bezeichnungsnamen in der entsprechenden lokalen SCV-Richtlinie übereinstimmen.

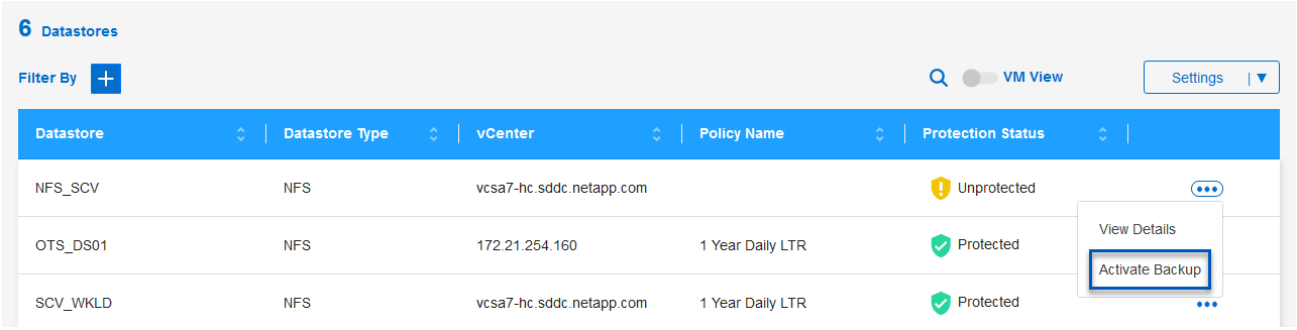
3. Klicken Sie auf **Erstellen**, um die Richtlinienerstellung abzuschließen.

▼ **Datenspeicher auf Amazon Web Services sichern**

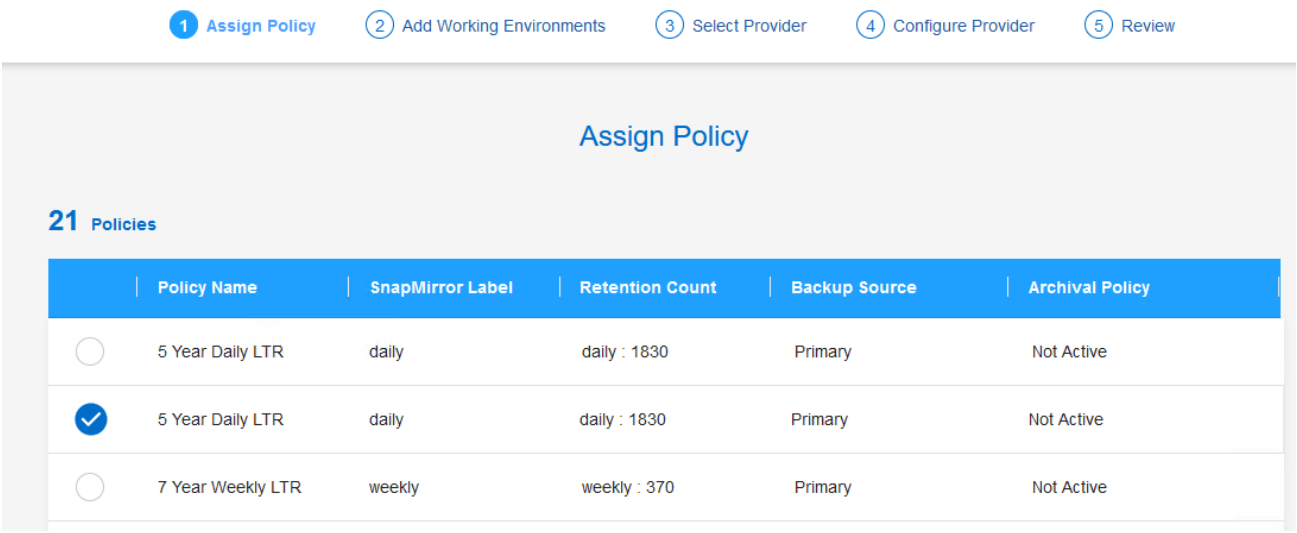
Der letzte Schritt besteht darin, den Datenschutz für die einzelnen Datenspeicher und virtuellen Maschinen zu aktivieren. Die folgenden Schritte beschreiben, wie Sie Backups in AWS aktivieren.

Weitere Informationen finden Sie unter "VMware Workloads sichern".

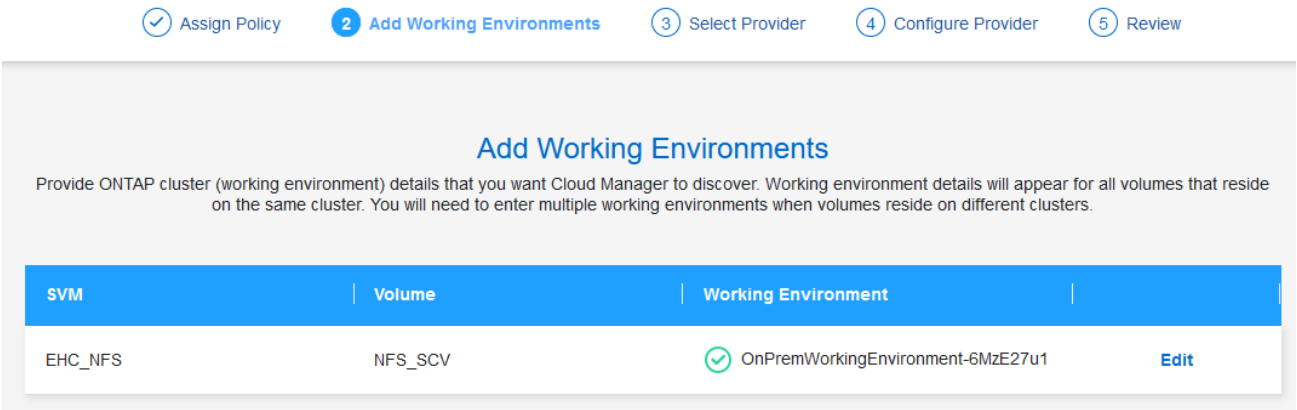
1. Auf der Hauptseite von NetApp Backup and Recovery for Virtual Machines können Sie das Dropdown-Menü „Einstellungen“ für den zu sichernden Datenspeicher öffnen und **Activate Backup** auswählen.



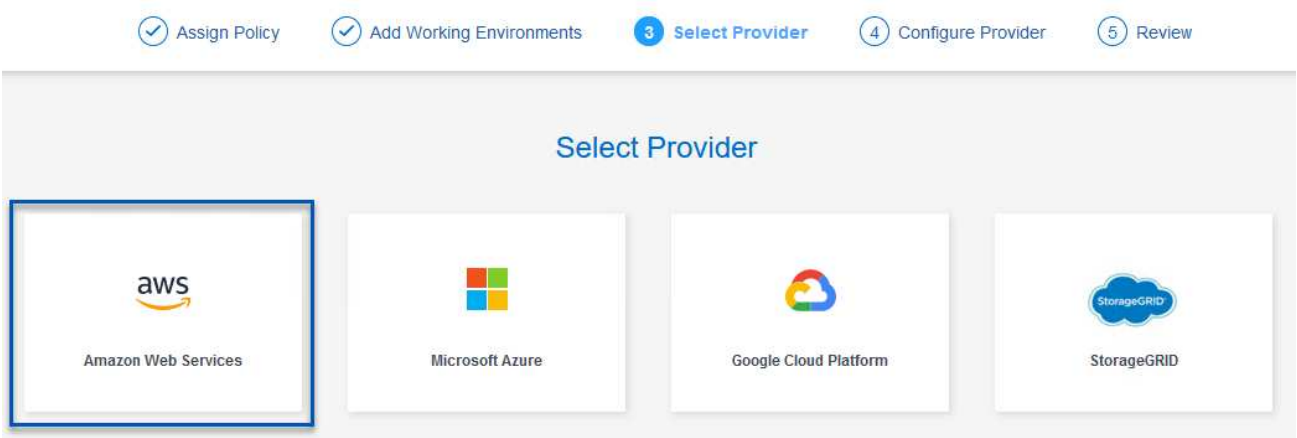
2. Weisen Sie die für den Datenschutzvorgang zu verwendende Richtlinie zu und klicken Sie auf **Weiter**.



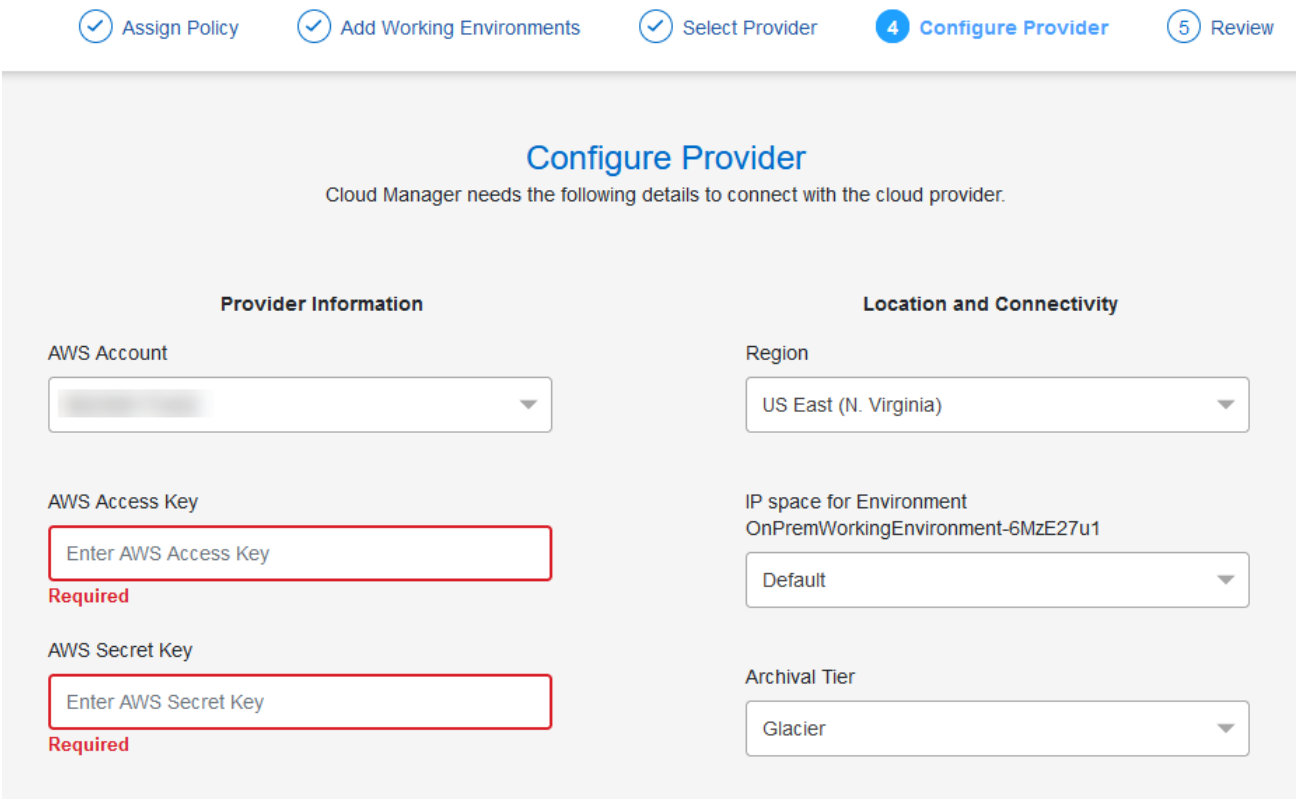
3. Auf der Seite **Arbeitsumgebungen hinzufügen** sollten der Datenspeicher und die Arbeitsumgebung mit einem Häkchen angezeigt werden, wenn die Arbeitsumgebung zuvor erkannt wurde. Wenn die Arbeitsumgebung noch nicht erkannt wurde, können Sie sie hier hinzufügen. Klicken Sie auf **Weiter**, um fortzufahren.



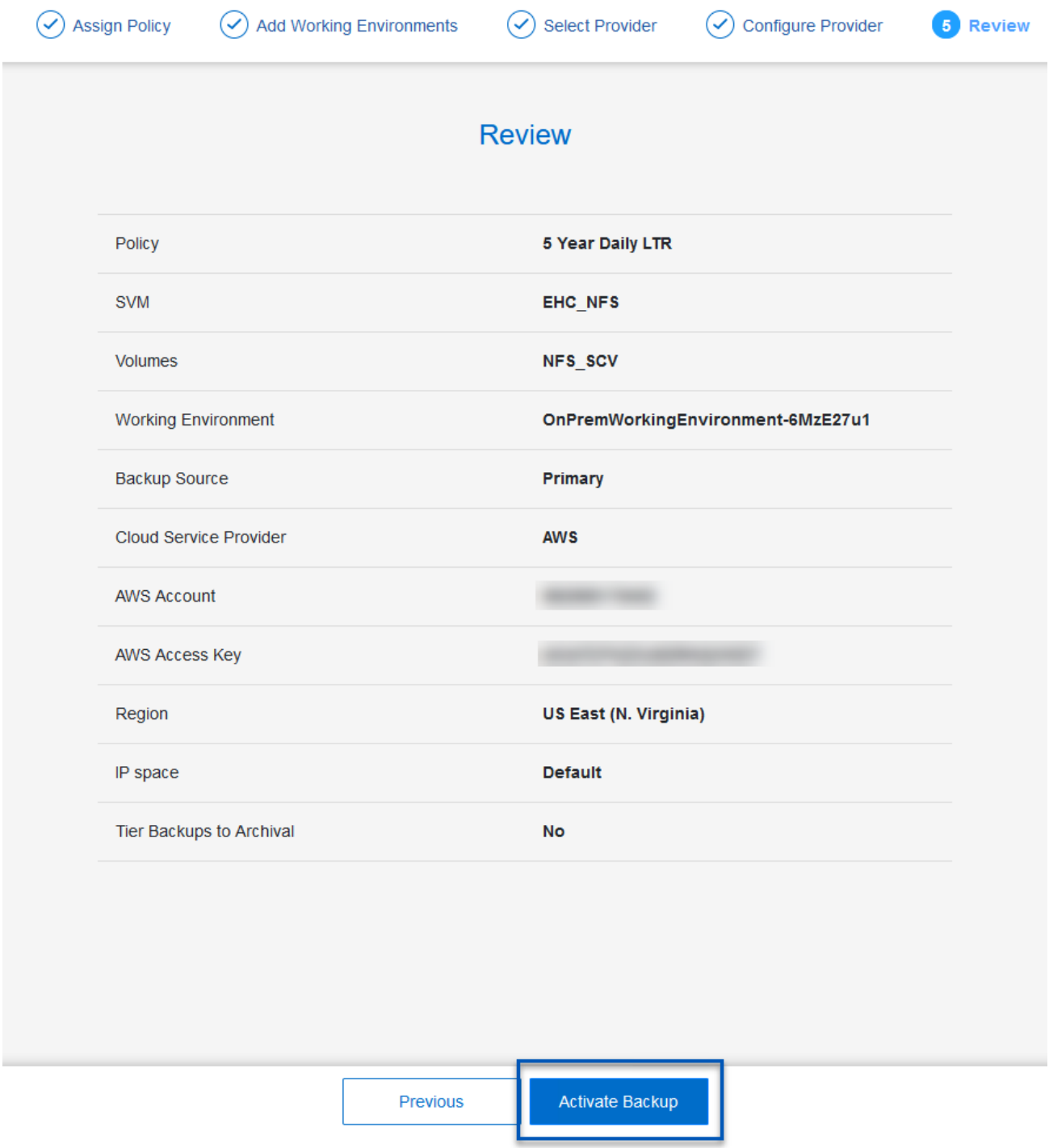
4. Klicken Sie auf der Seite **Anbieter auswählen** auf AWS und dann auf die Schaltfläche **Weiter**, um fortzufahren.



5. Füllen Sie die anbieterspezifischen Anmeldeinformationen für AWS aus, einschließlich des AWS-Zugriffsschlüssels und des geheimen Schlüssels, der Region und der zu verwendenden Archivierungsebene. Wählen Sie außerdem den ONTAP -IP-Bereich für das lokale ONTAP Speichersystem aus. Klicken Sie auf **Weiter**.



6. Überprüfen Sie abschließend die Details des Sicherungsauftrags und klicken Sie auf die Schaltfläche **Sicherung aktivieren**, um den Datenschutz des Datenspeichers zu starten.



Zu diesem Zeitpunkt beginnt der Datentransfer möglicherweise nicht sofort. NetApp Backup and Recovery sucht stündlich nach ausstehenden Snapshots und überträgt sie anschließend in den Objektspeicher.

Wiederherstellung virtueller Maschinen im Falle eines Datenverlusts

Die Gewährleistung der Sicherheit Ihrer Daten ist nur ein Aspekt eines umfassenden Datenschutzes. Ebenso wichtig ist die Möglichkeit, Daten im Falle eines Datenverlusts oder eines Ransomware-Angriffs umgehend von jedem beliebigen Ort aus wiederherzustellen. Diese Fähigkeit ist für die Aufrechterhaltung eines reibungslosen Geschäftsbetriebs und das Erreichen der Wiederherstellungspunktziele von entscheidender Bedeutung.

NetApp bietet eine äußerst anpassungsfähige 3-2-1-Strategie, die eine individuelle Kontrolle über Aufbewahrungspläne an den primären, sekundären und Objektspeicherstandorten ermöglicht. Diese Strategie bietet die Flexibilität, Datenschutzansätze an spezifische Anforderungen anzupassen.

Dieser Abschnitt bietet einen Überblick über den Datenwiederherstellungsprozess sowohl aus dem SnapCenter Plug-in for VMware vSphere als auch aus NetApp Backup and Recovery für virtuelle Maschinen.

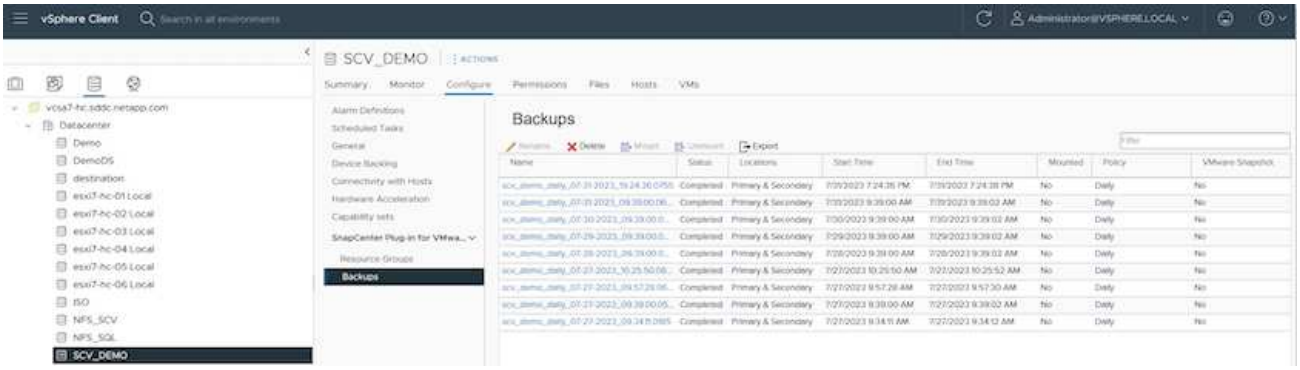
Wiederherstellen virtueller Maschinen vom SnapCenter Plug-in for VMware vSphere

Für diese Lösung wurden virtuelle Maschinen an ursprünglichen und alternativen Standorten wiederhergestellt. Diese Lösung deckt nicht alle Aspekte der Datenwiederherstellungsfunktionen von SCV ab. Ausführliche Informationen zu allen Angeboten von SCV finden Sie im "Wiederherstellen von VMs aus Backups" in der Produktdokumentation.

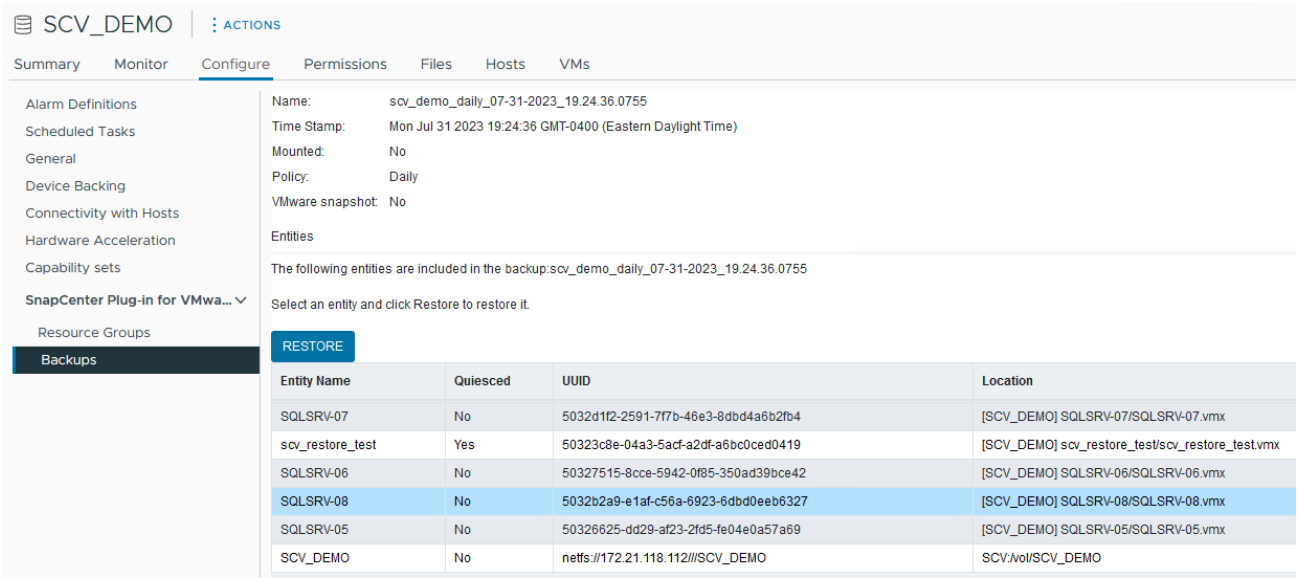
▼ **Wiederherstellen virtueller Maschinen aus SCV**

Führen Sie die folgenden Schritte aus, um eine virtuelle Maschine vom primären oder sekundären Speicher wiederherzustellen.

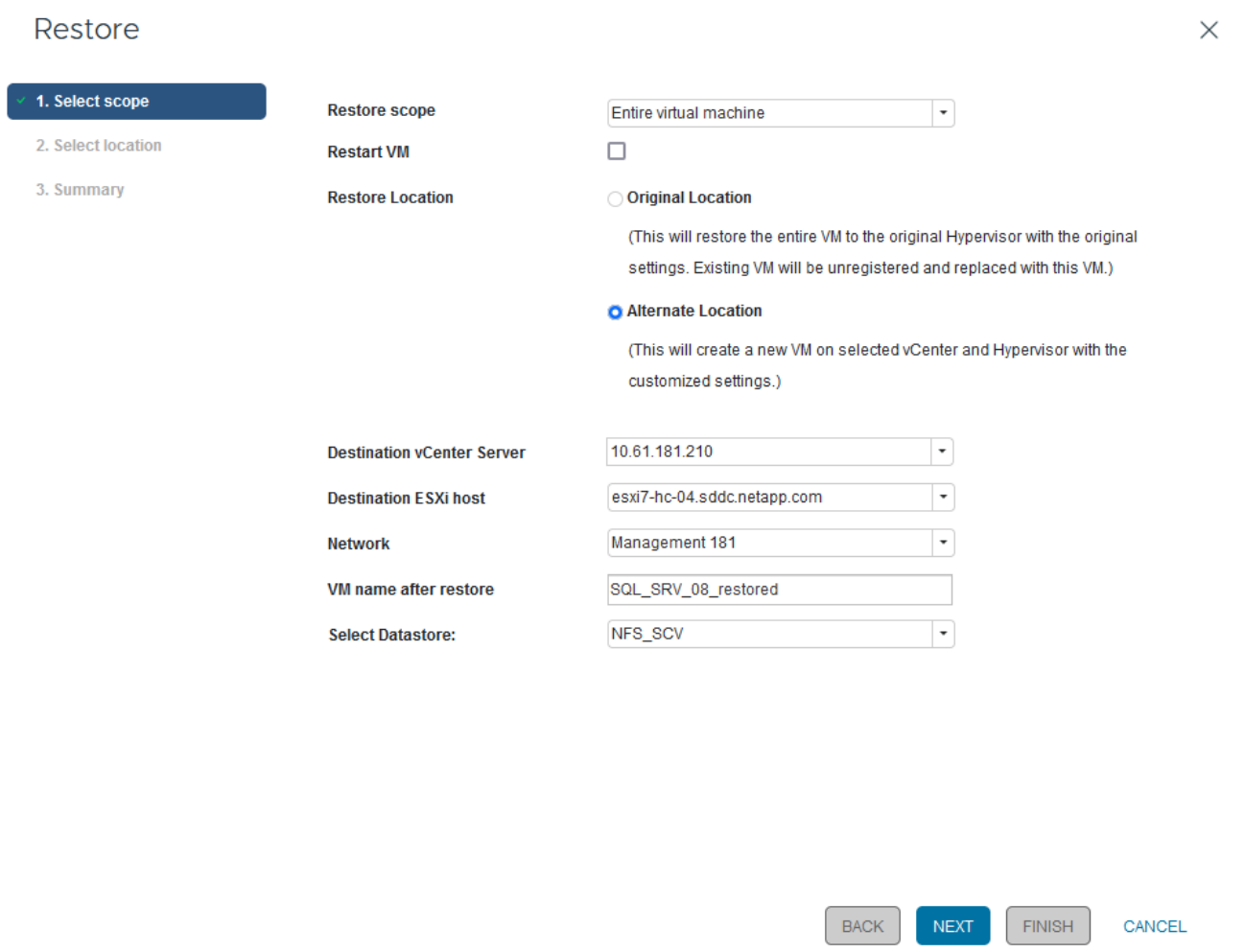
1. Navigieren Sie im vCenter-Client zu **Inventar > Speicher** und klicken Sie auf den Datenspeicher, der die virtuellen Maschinen enthält, die Sie wiederherstellen möchten.
2. Klicken Sie auf der Registerkarte **Konfigurieren** auf **Backups**, um auf die Liste der verfügbaren Backups zuzugreifen.



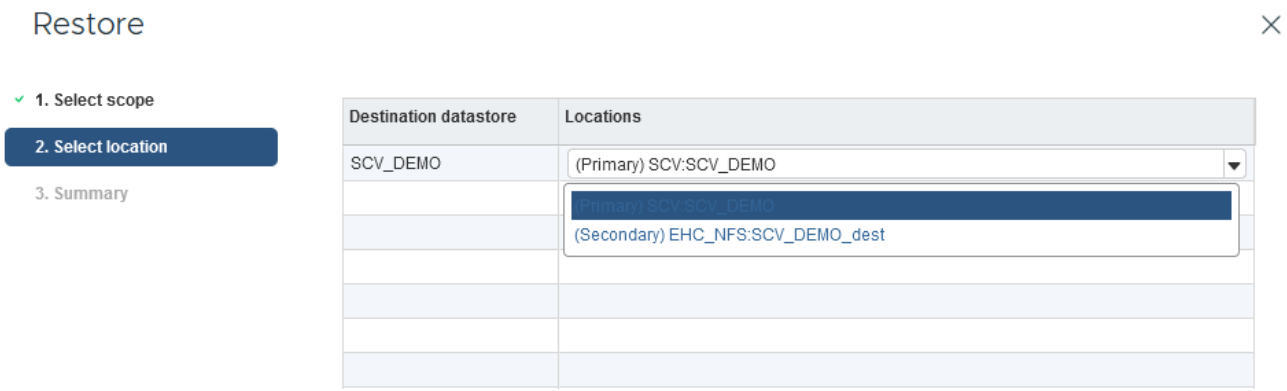
3. Klicken Sie auf eine Sicherung, um auf die Liste der VMs zuzugreifen, und wählen Sie dann eine VM zur Wiederherstellung aus. Klicken Sie auf **Wiederherstellen**.



4. Wählen Sie im Wiederherstellungsassistenten aus, ob die gesamte virtuelle Maschine oder ein bestimmtes VMDK wiederhergestellt werden soll. Wählen Sie die Installation am ursprünglichen oder alternativen Speicherort aus, geben Sie den VM-Namen nach der Wiederherstellung und den Zieldatenspeicher an. Klicken Sie auf **Weiter**.



5. Wählen Sie, ob Sie vom primären oder sekundären Speicherort sichern möchten.



6. Überprüfen Sie abschließend eine Zusammenfassung des Sicherungsauftrags und klicken Sie auf „Fertig stellen“, um den Wiederherstellungsvorgang zu starten.

Wiederherstellung virtueller Maschinen aus NetApp Backup and Recovery for Virtual Machines

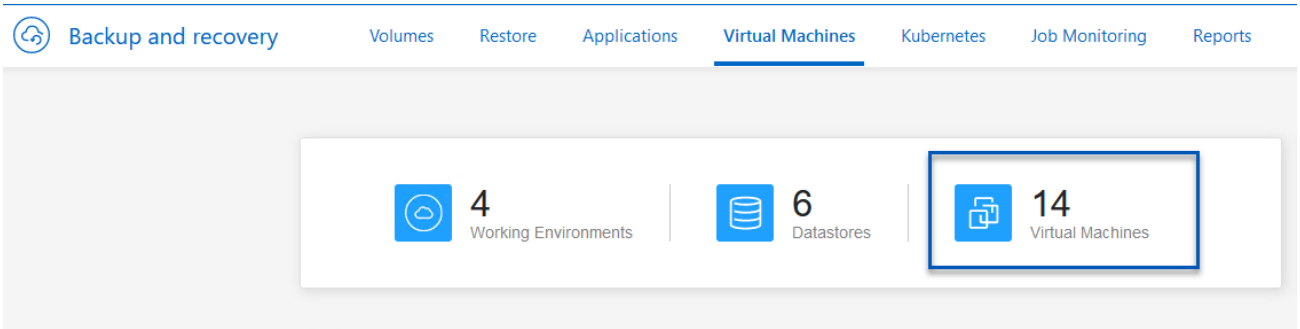
NetApp Backup and Recovery for Virtual Machines ermöglicht die Wiederherstellung virtueller Maschinen an ihrem ursprünglichen Speicherort. Auf die Wiederherstellungsfunktionen wird über die NetApp Backup and Recovery Web-Managementplattform zugegriffen.

Weitere Informationen finden Sie unter "Wiederherstellen von Daten virtueller Maschinen aus der Cloud".

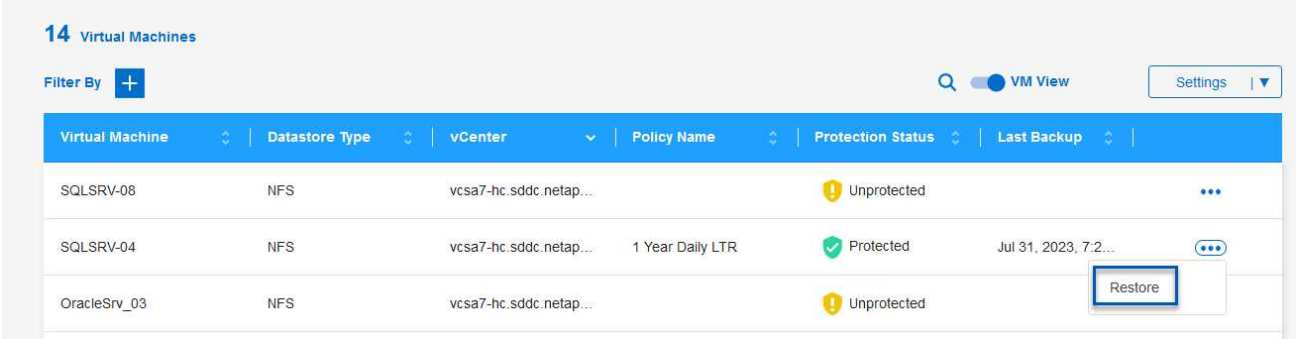
▼ **Virtuelle Maschinen aus NetApp Backup and Recovery wiederherstellen**

Zum Wiederherstellen einer virtuellen Maschine aus NetApp Backup and Recovery sind die folgenden Schritte erforderlich.

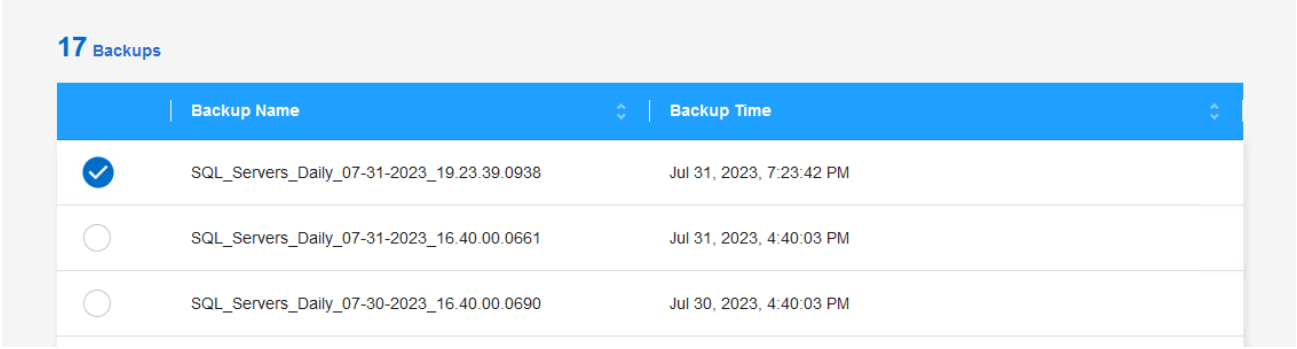
1. Navigieren Sie zu **Schutz > Sicherung und Wiederherstellung > Virtuelle Maschinen** und klicken Sie auf Virtuelle Maschinen, um die Liste der für die Wiederherstellung verfügbaren virtuellen Maschinen anzuzeigen.



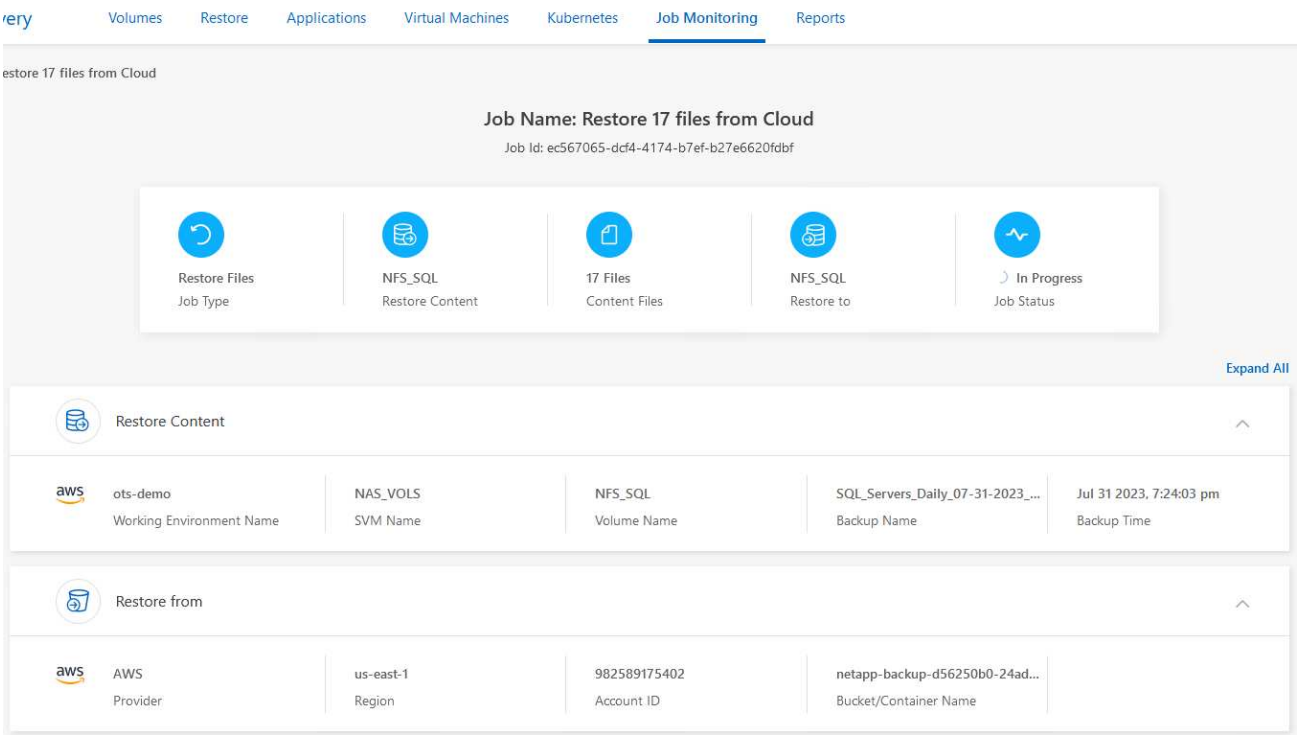
2. Rufen Sie das Dropdown-Menü „Einstellungen“ für die wiederherzustellende VM auf und wählen Sie



3. Wählen Sie das Backup aus, aus dem die Wiederherstellung erfolgen soll, und klicken Sie auf **Weiter**.



4. Überprüfen Sie eine Zusammenfassung des Sicherungsauftrags und klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.
5. Überwachen Sie den Fortschritt des Wiederherstellungsauftrags auf der Registerkarte **Auftragsüberwachung**.



Abschluss

Die 3-2-1-Backup-Strategie bietet bei der Implementierung mit SnapCenter Plug-in for VMware vSphere und NetApp Backup and Recovery für virtuelle Maschinen eine robuste, zuverlässige und kostengünstige Lösung für den Datenschutz. Diese Strategie gewährleistet nicht nur Datenredundanz und Zugänglichkeit, sondern bietet auch die Flexibilität, Daten von jedem beliebigen Standort sowie sowohl aus lokalen ONTAP Storage-Systemen als auch aus cloudbasiertem Objektspeicher wiederherzustellen.

Der in dieser Dokumentation vorgestellte Anwendungsfall konzentriert sich auf bewährte Datenschutztechnologien und hebt die Integration zwischen NetApp, VMware und den führenden Cloud-Anbietern hervor. Das SnapCenter Plug-in für VMware vSphere ermöglicht die nahtlose Integration mit VMware vSphere und damit das effiziente und zentrale Management von Datenschutzvorgängen. Diese Integration optimiert die Backup und Recovery Prozesse für virtuelle Maschinen und ermöglicht eine einfache

Planung, Überwachung und flexible Restore-Vorgänge innerhalb des VMware-Ökosystems. NetApp Backup and Recovery für virtuelle Maschinen bietet die Eins (1) in 3-2-1 durch sichere, physisch bzw. logisch isolierte Backups von Daten virtueller Maschinen in cloudbasierten Objekt-Storage. Die intuitive Benutzeroberfläche und der logische Workflow bieten eine sichere Plattform für die langfristige Archivierung kritischer Daten.

Weitere Informationen

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

- "SnapCenter Plug-in for VMware vSphere Dokumentation"
- "NetApp Console-Dokumentation"

NetApp Disaster Recovery

Überblick

Disaster Recovery steht bei jedem VMware-Administrator an erster Stelle. Da VMware ganze Server in eine Reihe von Dateien kapselt, aus denen die virtuelle Maschine besteht, nutzen Administratoren block-Storage-basierte Techniken wie Klone, Snapshots und Replikate, um diese VMs zu schützen. ONTAP Arrays bieten integrierte Replizierung, um Volume-Daten und damit die virtuellen Maschinen auf den vorgesehenen Datastore-LUNs von einem Standort zum anderen zu übertragen. NetApp Disaster Recovery integriert sich in vSphere und automatisiert den gesamten Workflow für nahtloses Failover und Failback im Katastrophenfall. Durch die Kombination von Storage-Replizierung mit intelligenter Automatisierung verfügen Administratoren nun über eine praktikable Möglichkeit, Disaster-Recovery-Pläne nicht nur zu konfigurieren, zu automatisieren und zu testen, sondern sie im Katastrophenfall auch einfach auszuführen.

Der zeitaufwändigste Teil eines DR-Failovers in einer VMware vSphere-Umgebung ist die Ausführung der Schritte, die zum Inventarisieren, Registrieren, Neukonfigurieren und Einschalten der VMs am DR-Standort erforderlich sind. Eine ideale Lösung hat sowohl einen niedrigen RPO (gemessen in Minuten) als auch einen niedrigen RTO (gemessen in Minuten bis Stunden). Ein Faktor, der bei einer DR-Lösung oft übersehen wird, ist die Möglichkeit, die DR-Lösung in regelmäßigen Abständen effizient zu testen.

Berücksichtigen Sie beim Entwerfen einer DR-Lösung die folgenden Faktoren:

- Das Wiederherstellungszeitziel (RTO). Die RTO gibt an, wie schnell sich ein Unternehmen von einem Desaster erholen kann, oder genauer gesagt, wie lange es dauert, den Wiederherstellungsprozess auszuführen, um die Geschäftsdienste wieder verfügbar zu machen.
- Das Wiederherstellungspunktziel (RPO). Das RPO gibt an, wie alt die wiederhergestellten Daten nach ihrer Bereitstellung im Verhältnis zum Zeitpunkt des Katastrophenfalls sind.
- Skalierbarkeit und Anpassungsfähigkeit. Zu diesem Faktor gehört die Möglichkeit, die Speicherressourcen bei steigender Nachfrage schrittweise zu erweitern.

Weitere technische Informationen zu den verfügbaren Lösungen finden Sie unter:

- "NetApp Disaster Recovery für NFS Datastores"
- "NetApp Disaster Recovery für VMFS-Datastores"

NetApp Disaster Recovery für NFS Datastores

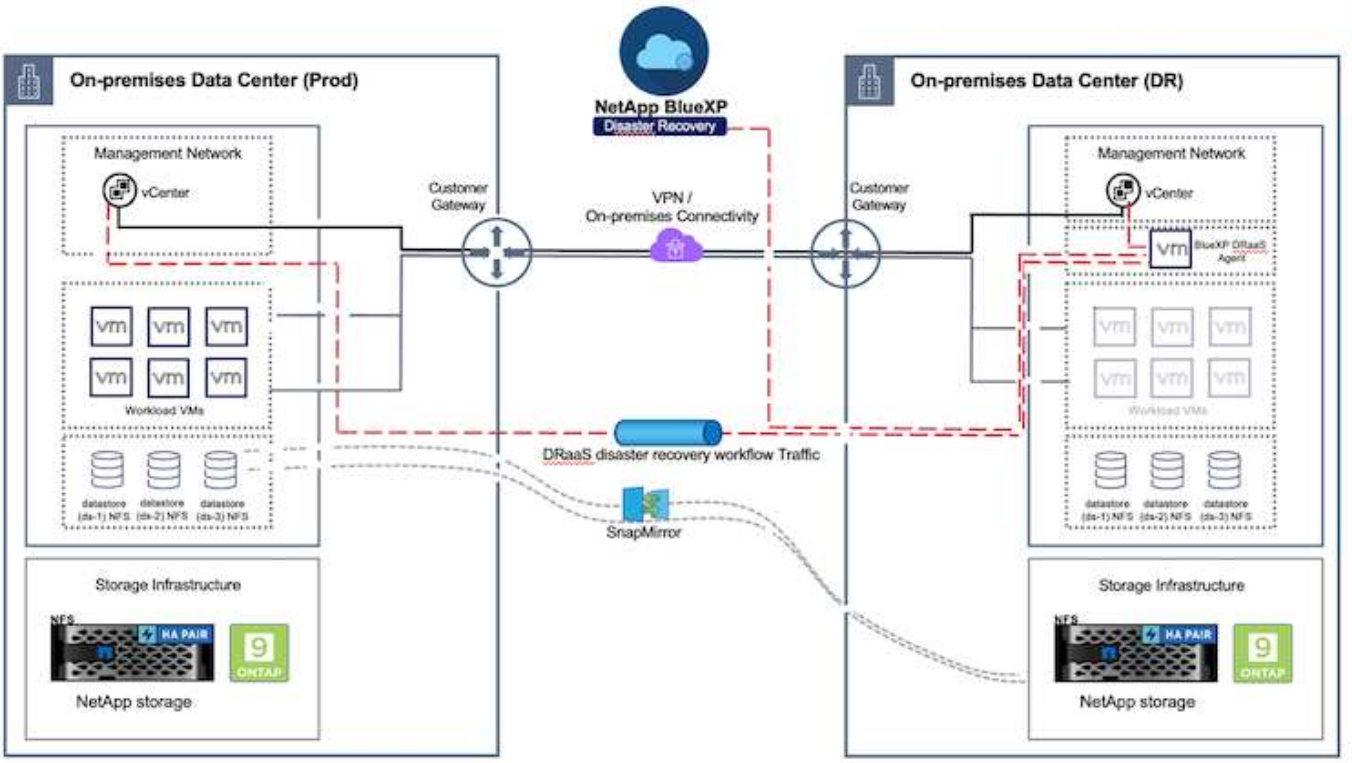
NetApp Disaster Recovery für NFS Datastores

Die Implementierung einer Notfallwiederherstellung durch Blockreplikation vom Produktionsstandort zum Notfallwiederherstellungsstandort ist eine robuste und kostengünstige Methode zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen, wie beispielsweise Ransomware-Angriffen. Mithilfe der NetApp SnapMirror Replikation können VMware-Workloads, die auf lokalen ONTAP -Systemen mit NFS-Datenspeicher ausgeführt werden, auf ein anderes ONTAP Speichersystem repliziert werden, das sich in einem dafür vorgesehenen Wiederherstellungs-Rechenzentrum befindet, in dem auch VMware bereitgestellt wird.

Dieser Abschnitt des Dokuments beschreibt die Konfiguration von NetApp Disaster Recovery, um die Disaster Recovery für lokale VMware VMs an einem anderen vorgesehenen Standort einzurichten. Zu diesem Setup gehören Console agent, das Onboarding der ONTAP Arrays, Defining Sites und das Zuordnen von VMware vCenter. Außerdem wird in diesem Dokument detailliert beschrieben, wie die Replikation zwischen Standorten konfiguriert wird und wie ein Wiederherstellungsplan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Failover des Standorts und zum Failback, sobald der primäre Standort wiederhergestellt ist und wieder online ist.

Mithilfe von Disaster Recovery, Teil von NetApp Data Services, können Unternehmen ihre lokalen VMware vCenters und ONTAP Storage identifizieren. Anschließend können Unternehmen Ressourcengruppen erstellen, einen Disaster Recovery Plan erstellen, ihn mit Ressourcengruppen verknüpfen und Failover und Failback testen oder ausführen. SnapMirror bietet Blockreplikation auf Storage-Ebene, um die beiden Standorte mit inkrementellen Änderungen auf dem neuesten Stand zu halten, was zu einem Recovery Point Objective (RPO) von bis zu 5 Minuten führt. Darüber hinaus ist es möglich, Disaster-Recovery-Verfahren zu simulieren, ohne die Produktion zu beeinträchtigen oder zusätzliche Storage-Kosten zu verursachen.

Disaster Recovery nutzt die ONTAP FlexClone Technologie, um aus dem zuletzt replizierten Snapshot am Disaster Recovery Standort eine platzsparende Kopie des NFS Datastore zu erstellen. Nach Abschluss des Disaster Recovery Tests können Kunden die Testumgebung einfach löschen, ohne die tatsächlich replizierten Produktionsressourcen zu beeinträchtigen. Im Fall eines tatsächlichen Failover orchestriert Disaster Recovery alle erforderlichen Schritte, um die geschützten virtuellen Maschinen mit nur wenigen Klicks automatisch am vorgesehenen Disaster Recovery Standort zu starten. Der Service kehrt außerdem die SnapMirror Beziehung zum primären Standort um und repliziert bei Bedarf alle Änderungen vom sekundären zum primären Standort für einen Failback-Vorgang. All diese Funktionen sind im Vergleich zu anderen bekannten Alternativen zu einem Bruchteil der Kosten verfügbar.

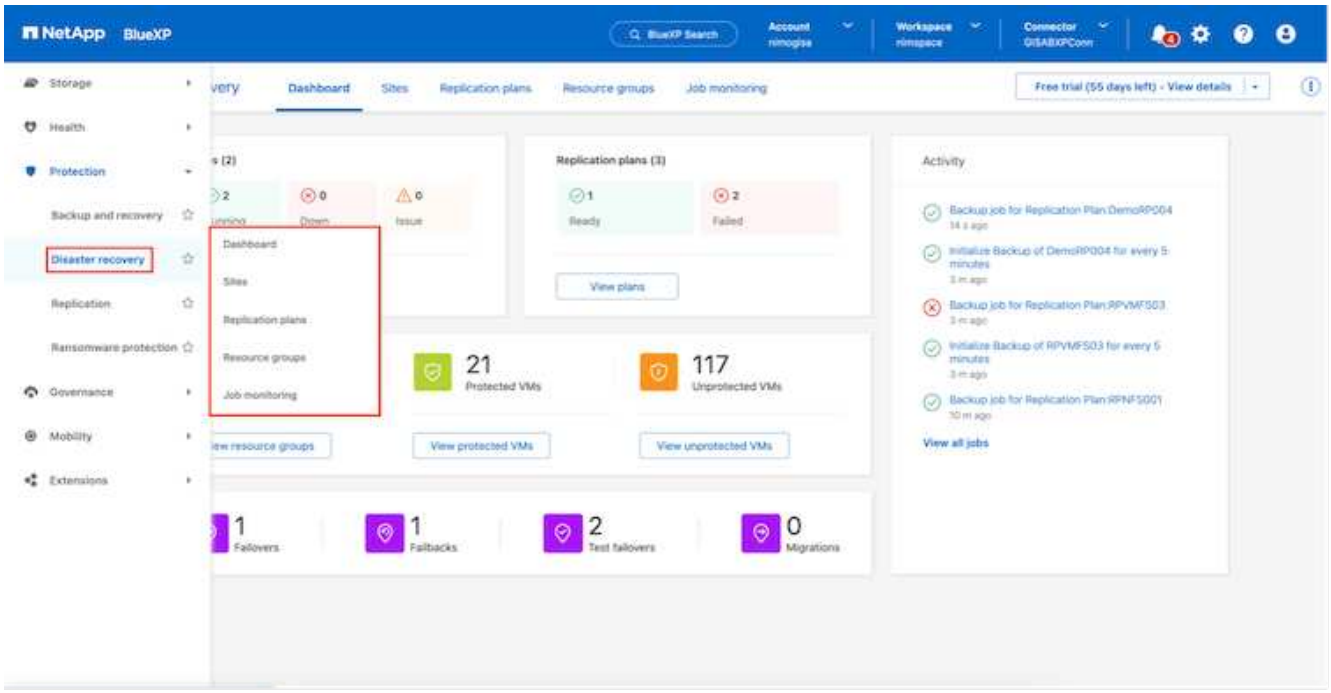


Aktuelle Informationen und unterstützte Versionen von vCenter Server, ESXi und ONTAP for Disaster Recovery finden Sie in der "Unterstützte Konfigurationen für die Notfallwiederherstellung".

Erste Schritte

Für den Einstieg in NetApp Disaster Recovery wird die NetApp Managementplattform verwendet, anschließend erfolgt der Zugriff auf den Service.

1. Anmeldung bei Console.
2. In der linken Navigation der Console erfolgt die Auswahl von „Schutz“ > „Disaster Recovery“.
3. Das Dashboard für die Notfallwiederherstellung erscheint.

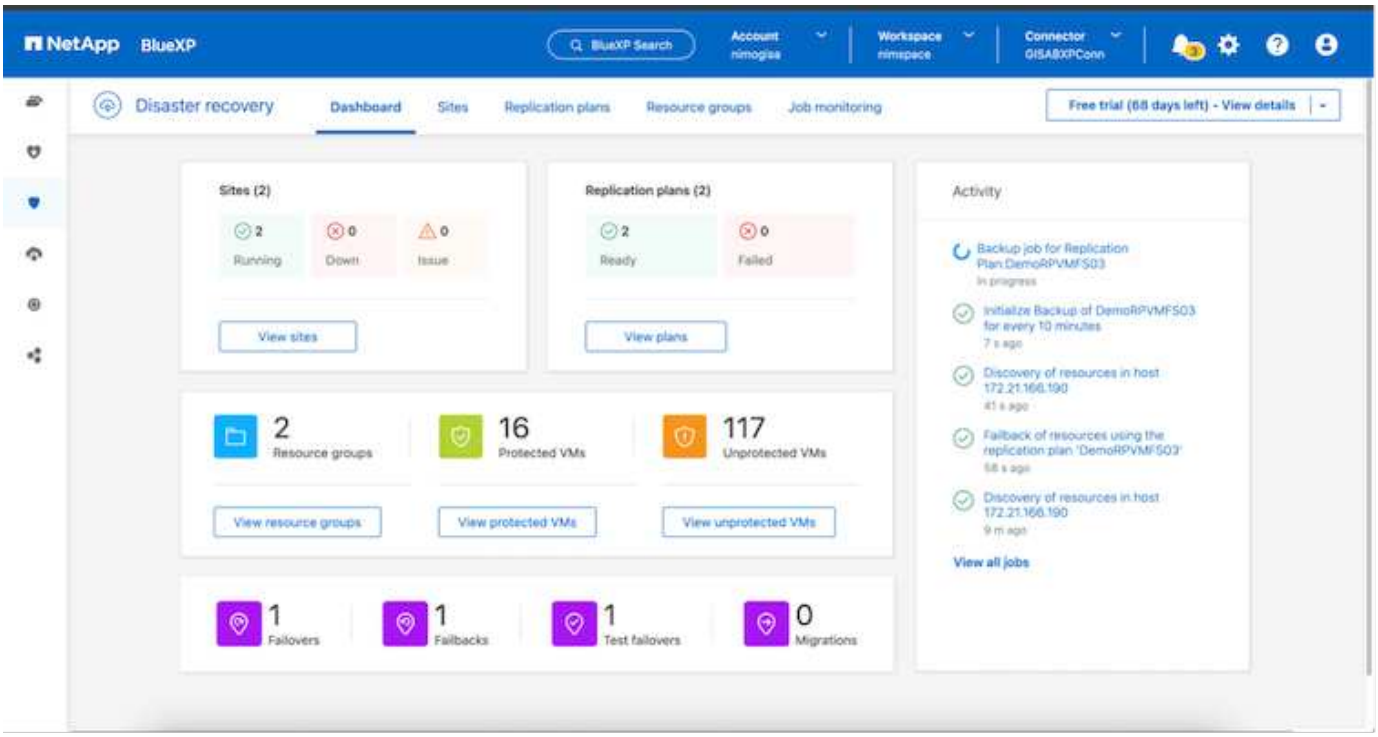


Vor der Konfiguration des Disaster Recovery-Plans müssen die folgenden Voraussetzungen erfüllt sein:

- Console Agent wurde eingesetzt.
- Der Agent verfügt über Konnektivität zum Quell- und Ziel-vCenter sowie zu den Storage-Systemen.
- Ein ONTAP Cluster mit einer SVM mit aktiviertem NFS-Service ist verfügbar.
- Lokale NetApp Storage-Systeme, die NFS-Datastores für VMware hosten, werden in Console hinzugefügt.
- Bei der Verwendung von DNS-Namen sollte eine DNS-Auflösung vorhanden sein. Andernfalls verwenden Sie IP-Adressen für das vCenter.
- Die SnapMirror Replikation ist für die angegebenen NFS-basierten Datenspeichervolumes konfiguriert.
- Stellen Sie sicher, dass die Umgebung über unterstützte Versionen von vCenter Server und ESXi-Servern verfügt.

Sobald die Verbindung zwischen Quell- und Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Dies sollte einige Klicks dauern und etwa 3 bis 5 Minuten dauern.

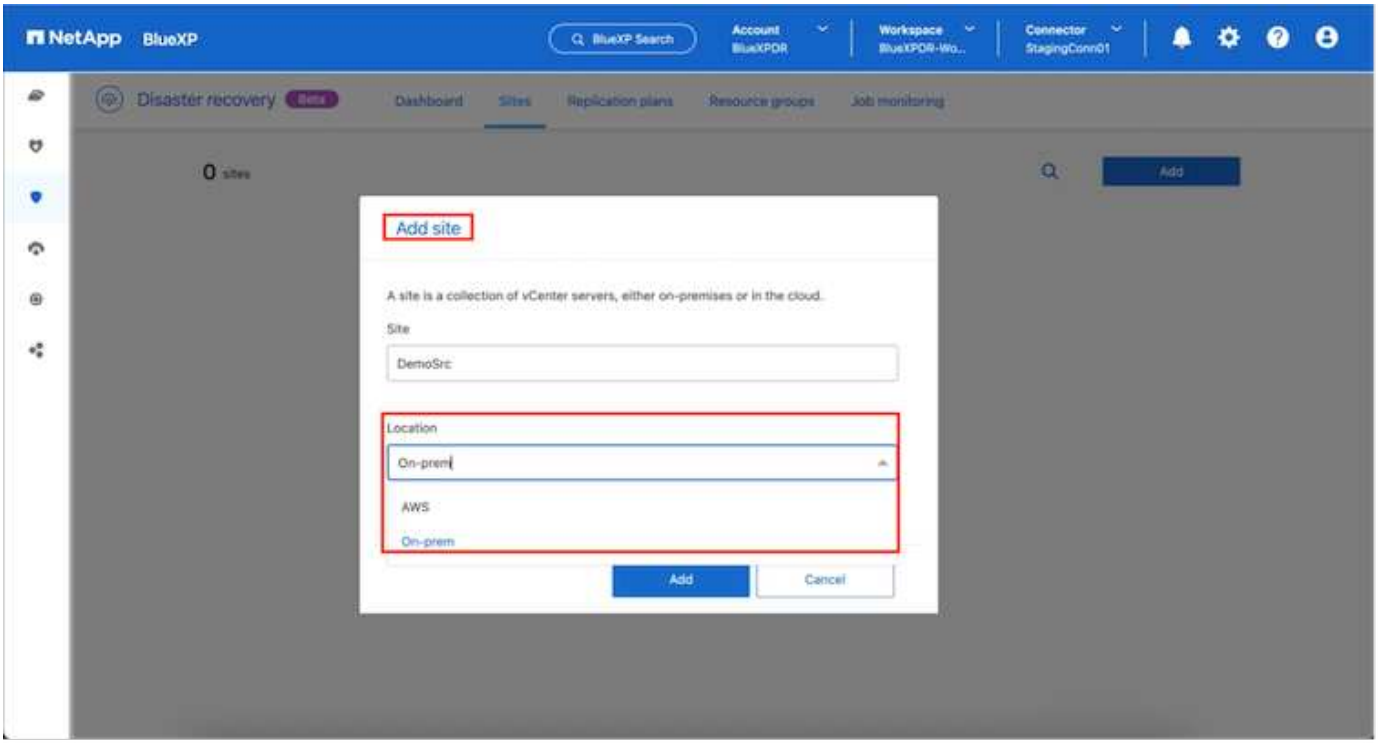
NetApp empfiehlt die Bereitstellung des Console Agenten am Zielstandort oder an einem dritten Standort, sodass der Console Agent über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.



NetApp Disaster Recovery Konfiguration

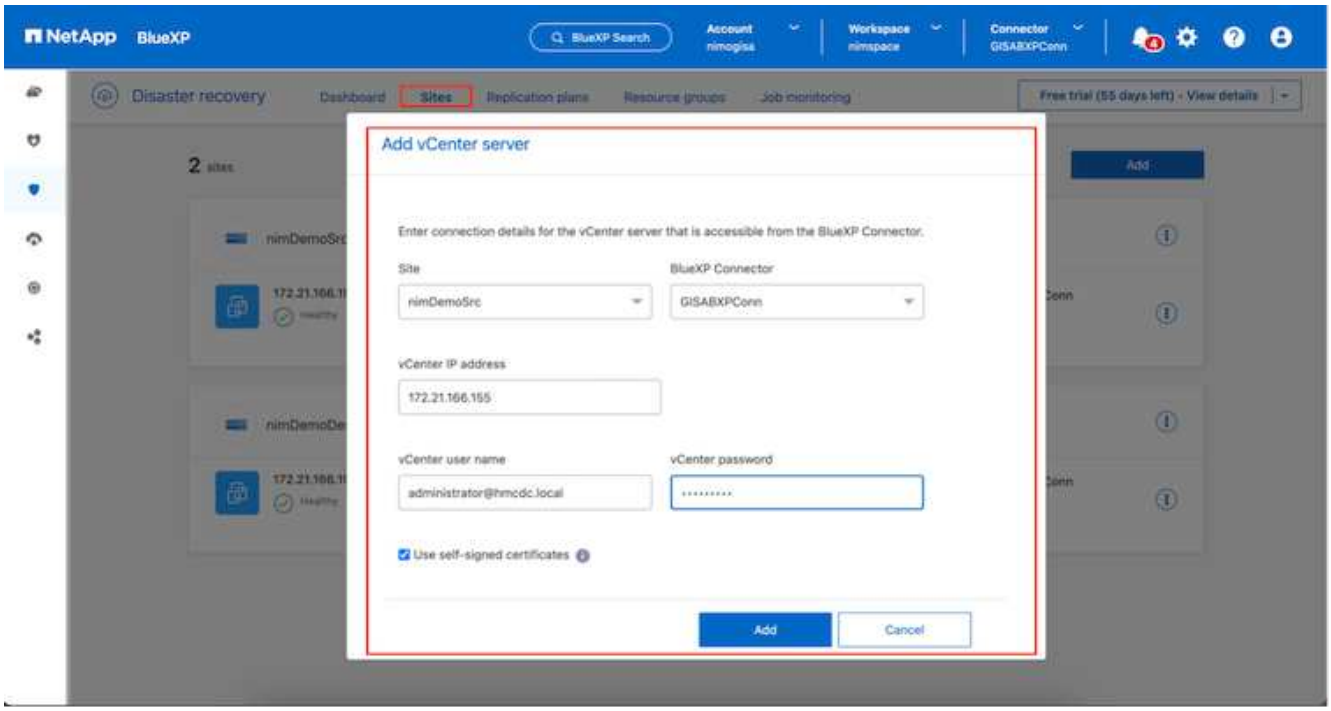
Der erste Schritt bei der Vorbereitung auf die Notfallwiederherstellung besteht darin, die lokalen vCenter- und Storage-Ressourcen zu NetApp Disaster Recovery zu identifizieren und hinzuzufügen.

Console öffnen und in der linken Navigation **Protection > Disaster Recovery** auswählen. Auf **Sites** klicken, einen Namen angeben und den Standorttyp auswählen. Anschließend auf die Schaltfläche **Add vCenter** klicken.

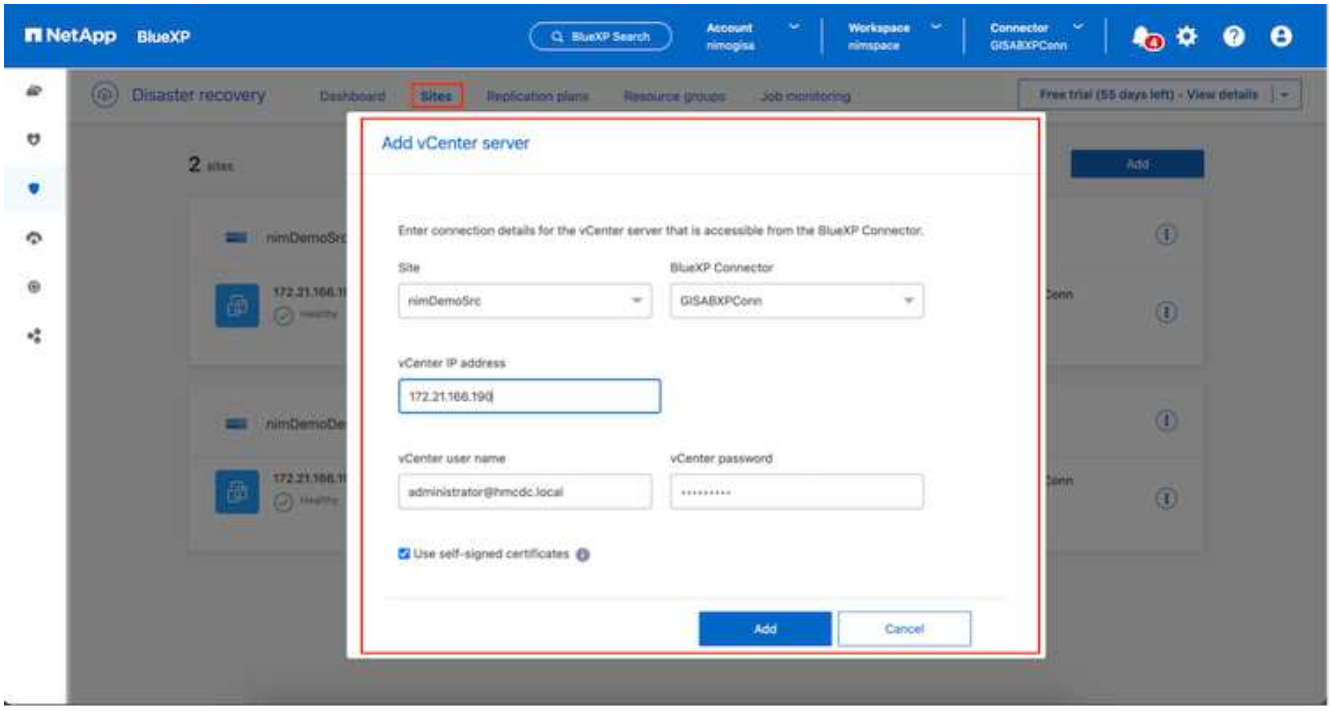


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle**. Lokales vCenter.



- **Ziel**. VMC SDDC vCenter.



Sobald die vCenter hinzugefügt wurden, wird die automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen Quellstandort-Array und Zielstandort-Array

SnapMirror bietet Datenreplizierung in einer NetApp Umgebung. Basierend auf der NetApp Snapshot

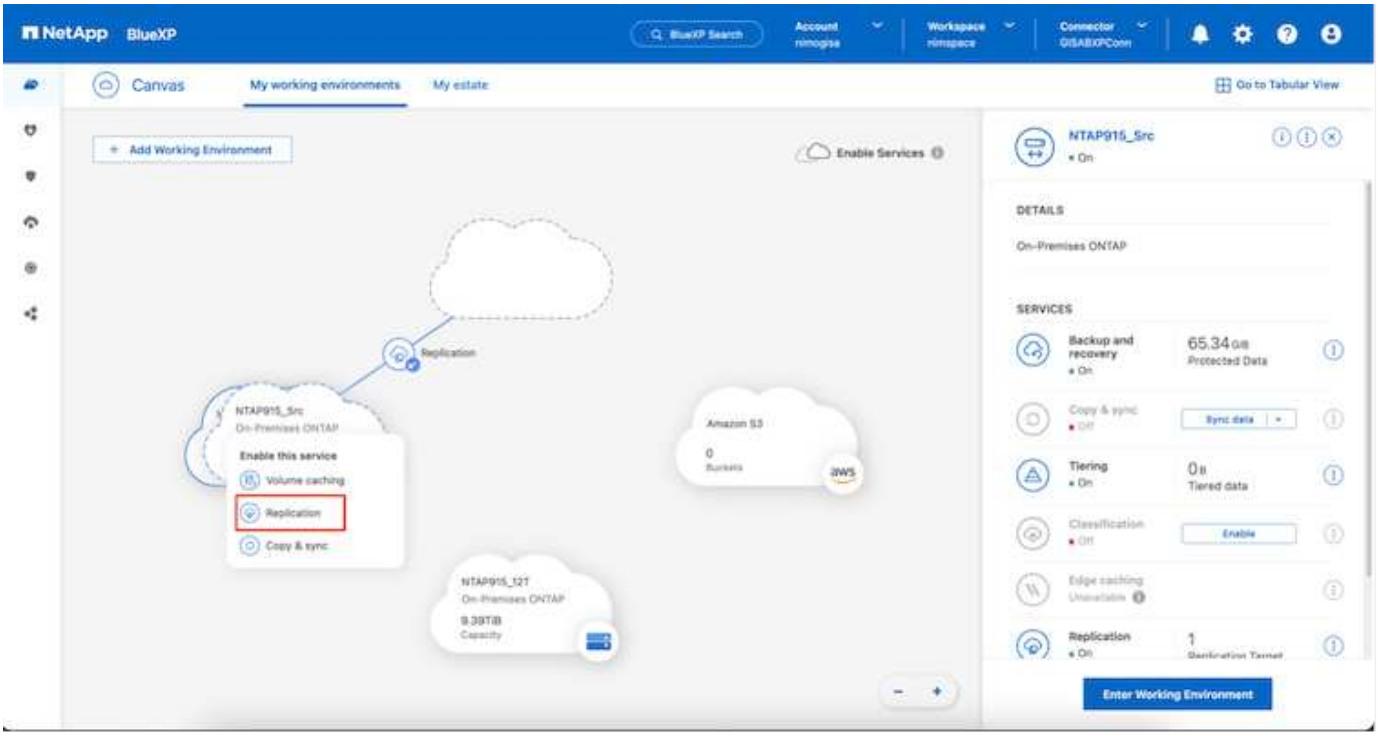
Technologie ist die SnapMirror Replizierung äußerst effizient, da nur die Blöcke repliziert werden, die seit dem vorherigen Update geändert oder hinzugefügt wurden. SnapMirror lässt sich einfach mit NetApp OnCommand System Manager oder der ONTAP CLI konfigurieren. NetApp Data Services erstellt außerdem die SnapMirror Beziehung, sofern Cluster- und SVM-Peering zuvor konfiguriert sind.

In Fällen, in denen der primäre Storage nicht vollständig verloren ist, bietet SnapMirror eine effiziente Möglichkeit, den primären Standort und den DR-Standort zu resynchronisieren. SnapMirror kann die beiden Standorte resynchronisieren, wobei durch einfaches Umkehren der SnapMirror Beziehungen nur geänderte oder neue Daten vom DR-Standort zurück an den primären Standort übertragen werden. Das bedeutet, dass Replikationspläne in Disaster Recovery nach einem Failover in beide Richtungen resynchronisiert werden können, ohne das gesamte Volume neu zu kopieren. Wenn eine Beziehung in umgekehrter Richtung resynchronisiert wird, werden nur neue Daten, die seit der letzten erfolgreichen Synchronisierung der Snapshot Kopie geschrieben wurden, an das Ziel zurückgesendet.

Wenn die SnapMirror Beziehung für das Volume bereits über die CLI oder den System Manager konfiguriert ist, übernimmt NetApp Data Services diese Beziehung und setzt die übrigen Workflow-Operationen fort.

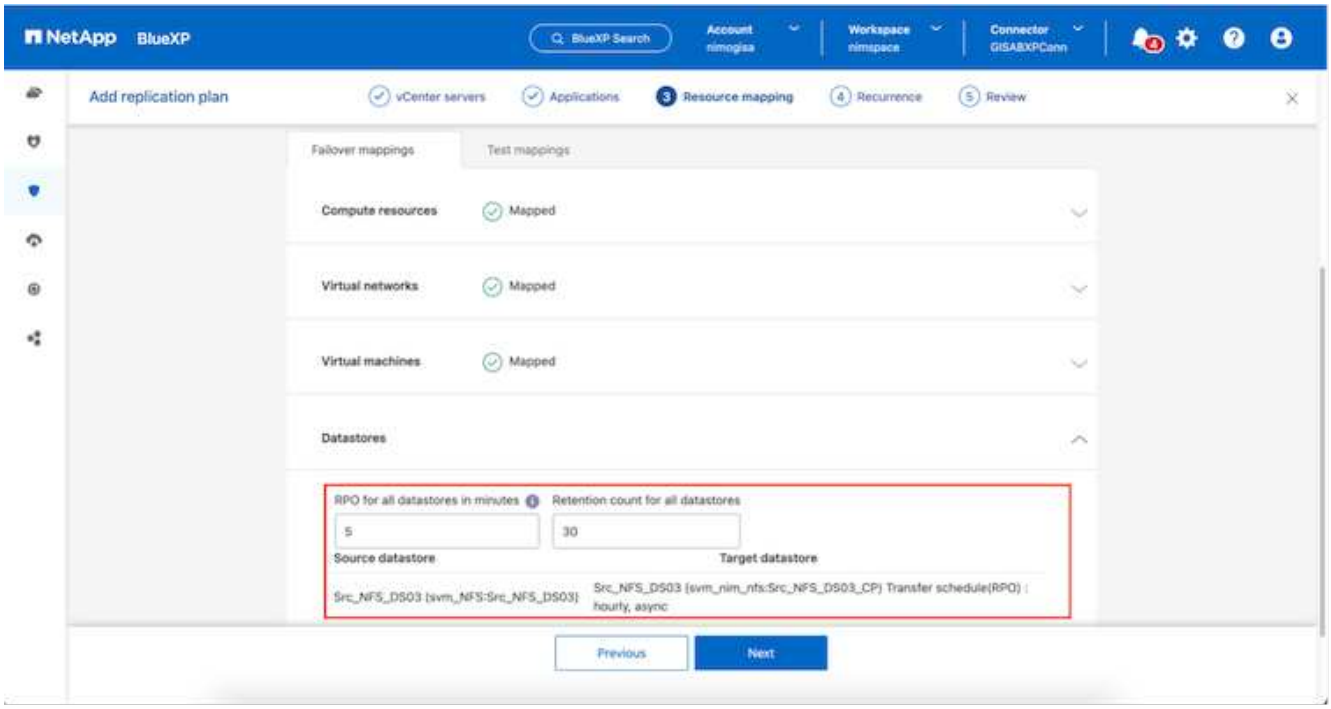
So richten Sie es für VMware Disaster Recovery ein

Der Prozess zur Erstellung einer SnapMirror Replikation bleibt für jede gegebene Applikation gleich. Der Prozess kann manuell oder automatisiert sein. Der einfachste Weg ist die Nutzung der NetApp Console zur Konfiguration der SnapMirror Replikation mittels einfachem Drag-and-Drop des Quell-ONTAP-Systems in der Umgebung auf das Ziel, um den Assistenten zu starten, der durch den weiteren Prozess führt.



Die Notfallwiederherstellung kann denselben Prozess auch automatisieren, sofern die folgenden beiden Kriterien erfüllt sind:

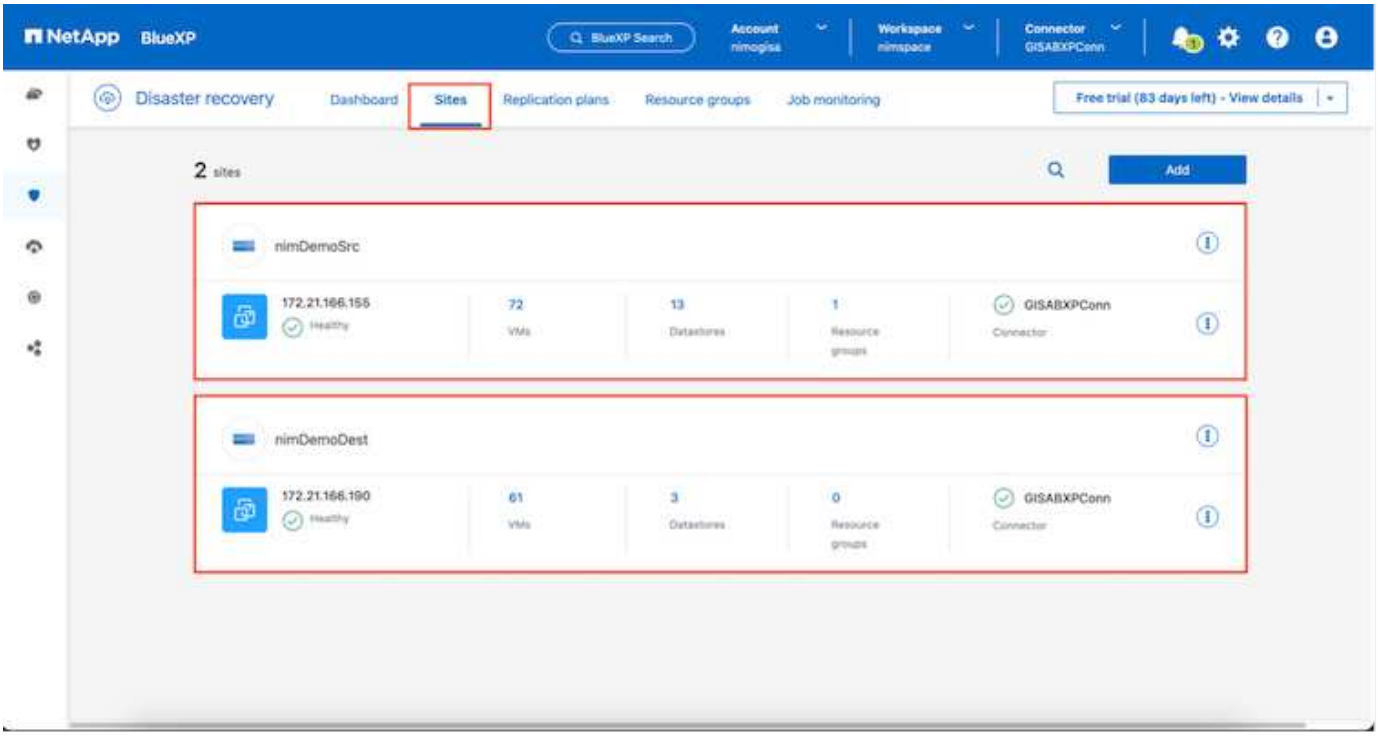
- Quell- und Zielcluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.



Wenn die SnapMirror Beziehung für das Volume bereits über die CLI konfiguriert ist, erkennt Disaster Recovery die Beziehung und fährt mit den übrigen Workflow-Operationen fort.

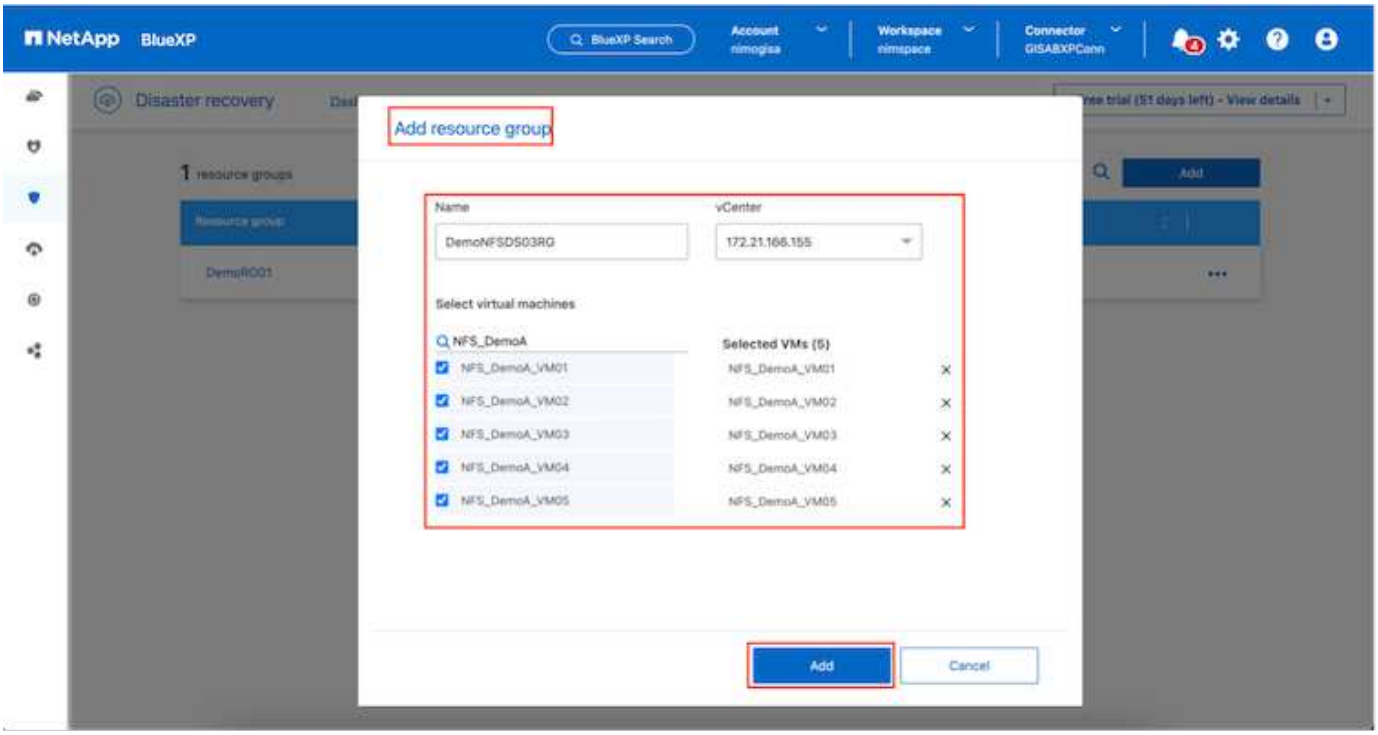
Was kann Disaster Recovery für Sie tun?

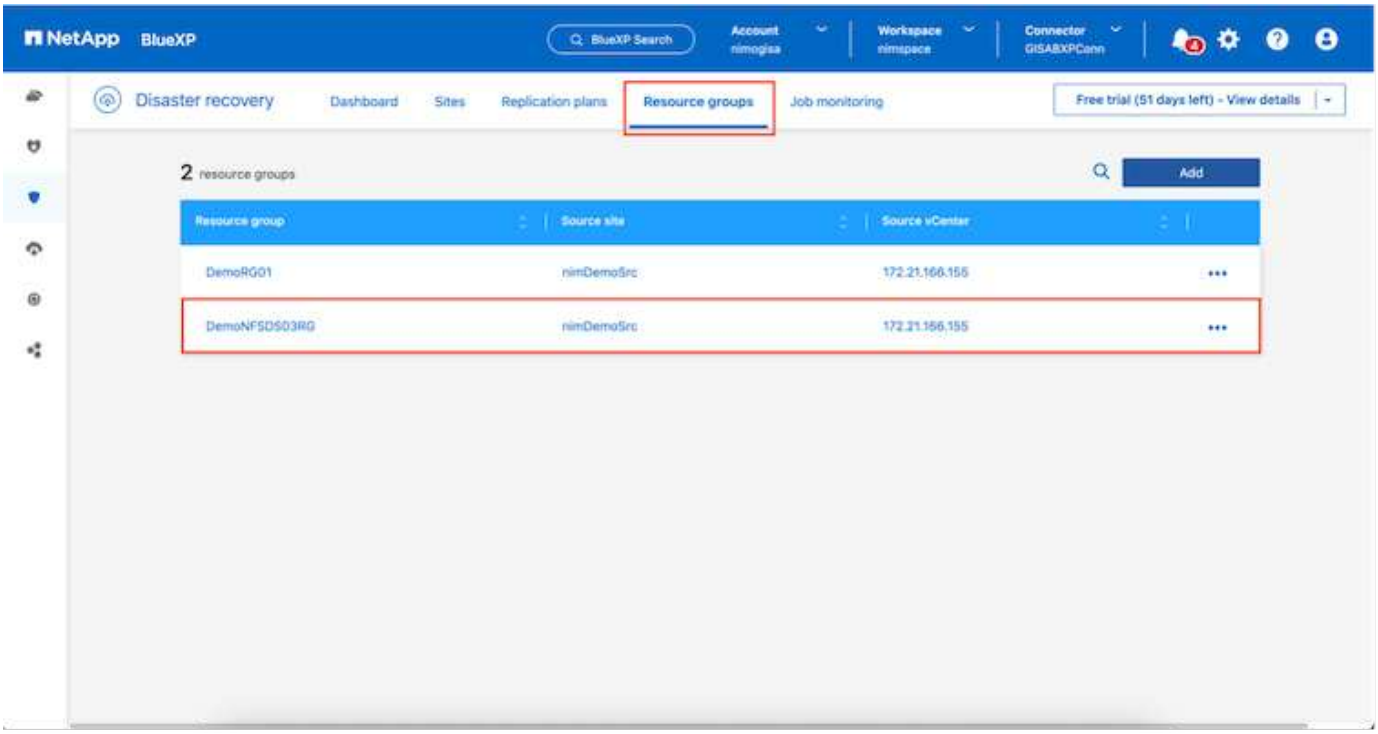
Nach dem Hinzufügen der Quell- und Zielstandorte führt Disaster Recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Disaster Recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und trägt diese ein.



Nachdem die Standorte hinzugefügt wurden, können VMs in Ressourcengruppen zusammengefasst werden.

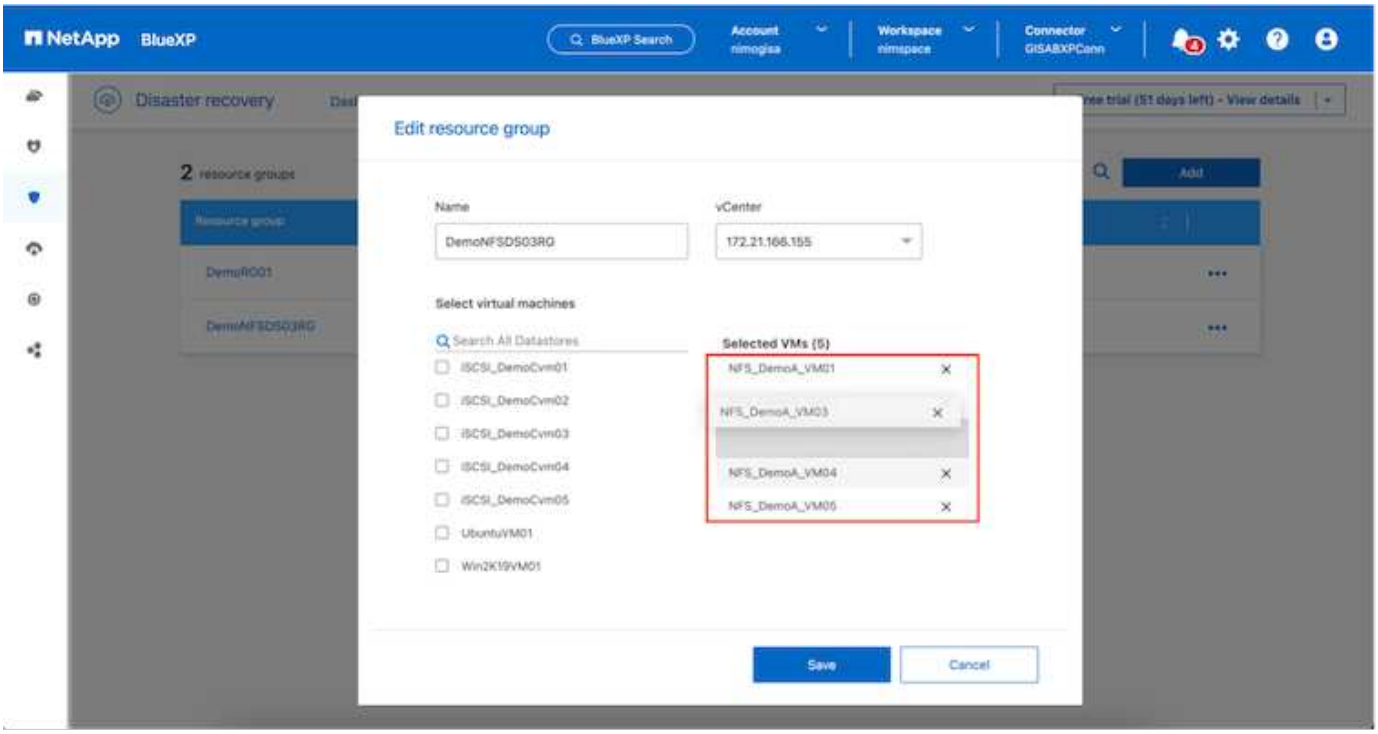
Disaster Recovery Ressourcengruppen ermöglichen die Gruppierung abhängiger VMs in logische Gruppen, die deren Startreihenfolgen und Startverzögerungen enthalten und bei der Wiederherstellung ausgeführt werden können. Die Erstellung von Ressourcengruppen beginnt unter **Resource Groups** mit einem Klick auf **Create New Resource Group**.



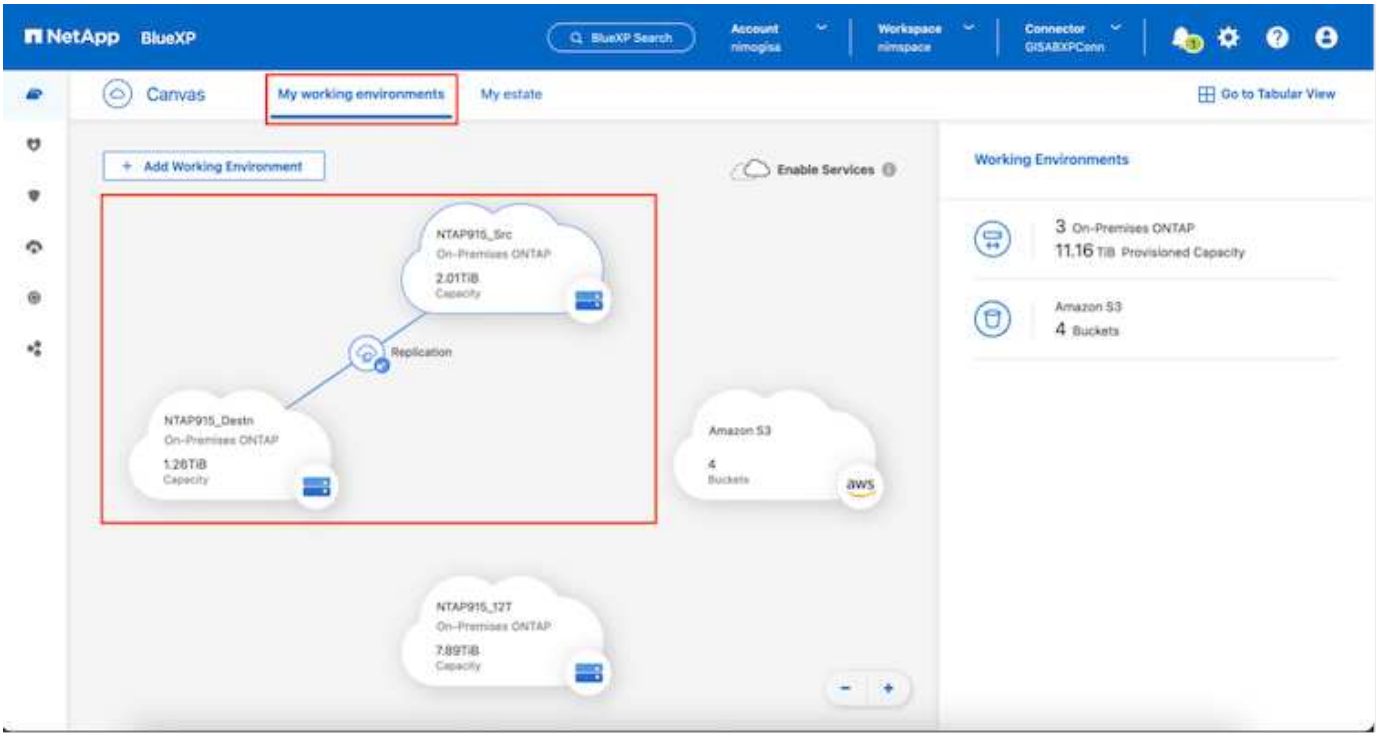


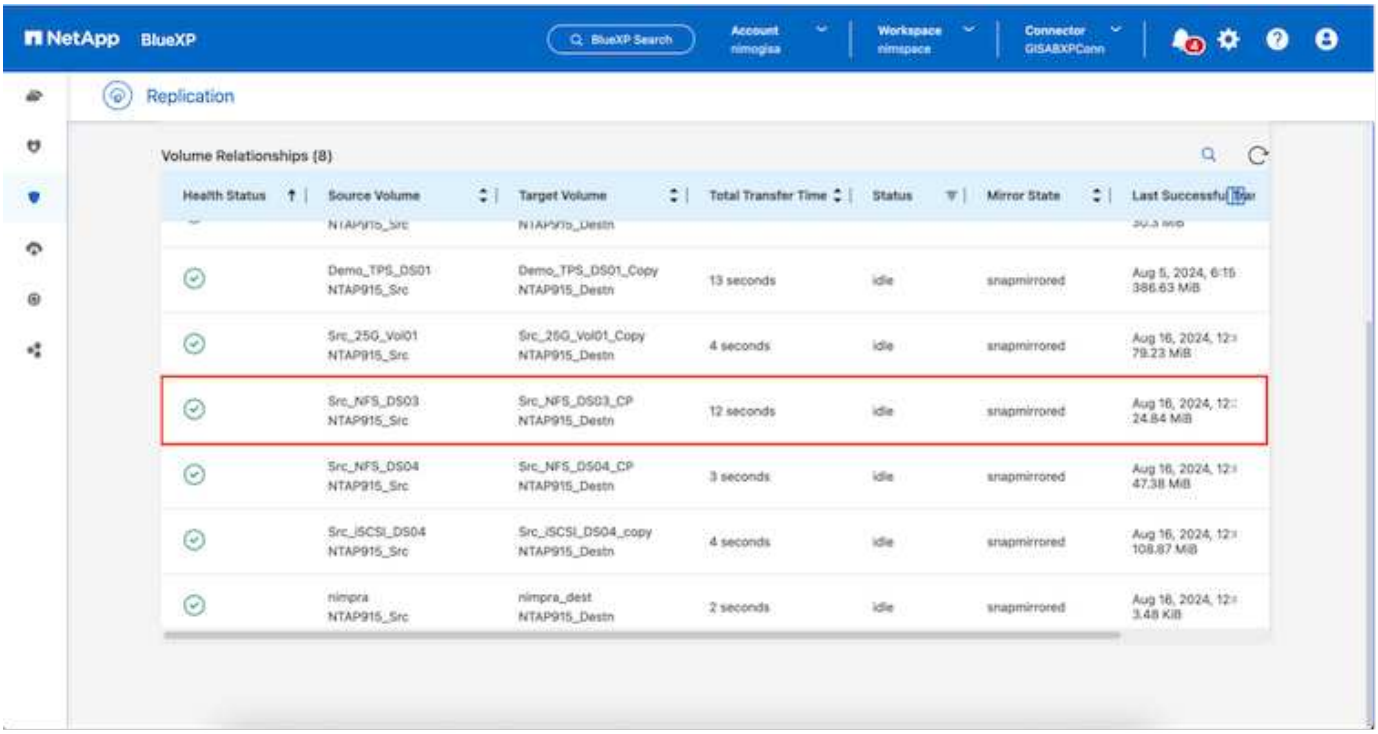
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

Die Startreihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen Drag-and-Drop-Mechanismus definiert oder geändert werden.



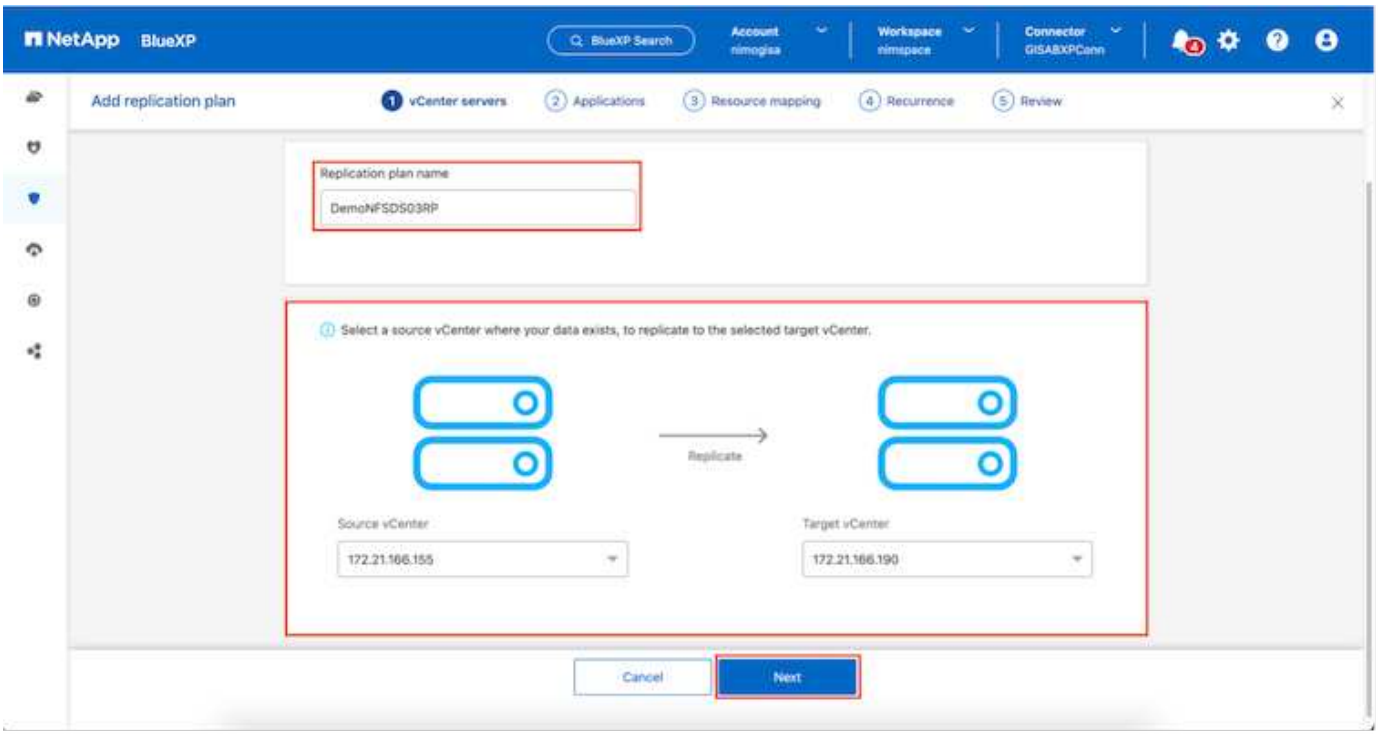
Sobald die Ressourcengruppen erstellt sind, besteht der nächste Schritt darin, den Ausführungsentwurf oder einen Plan zur Wiederherstellung virtueller Maschinen und Anwendungen im Katastrophenfall zu erstellen. Wie in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie mithilfe des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des Replikationsplans angegeben wurden.





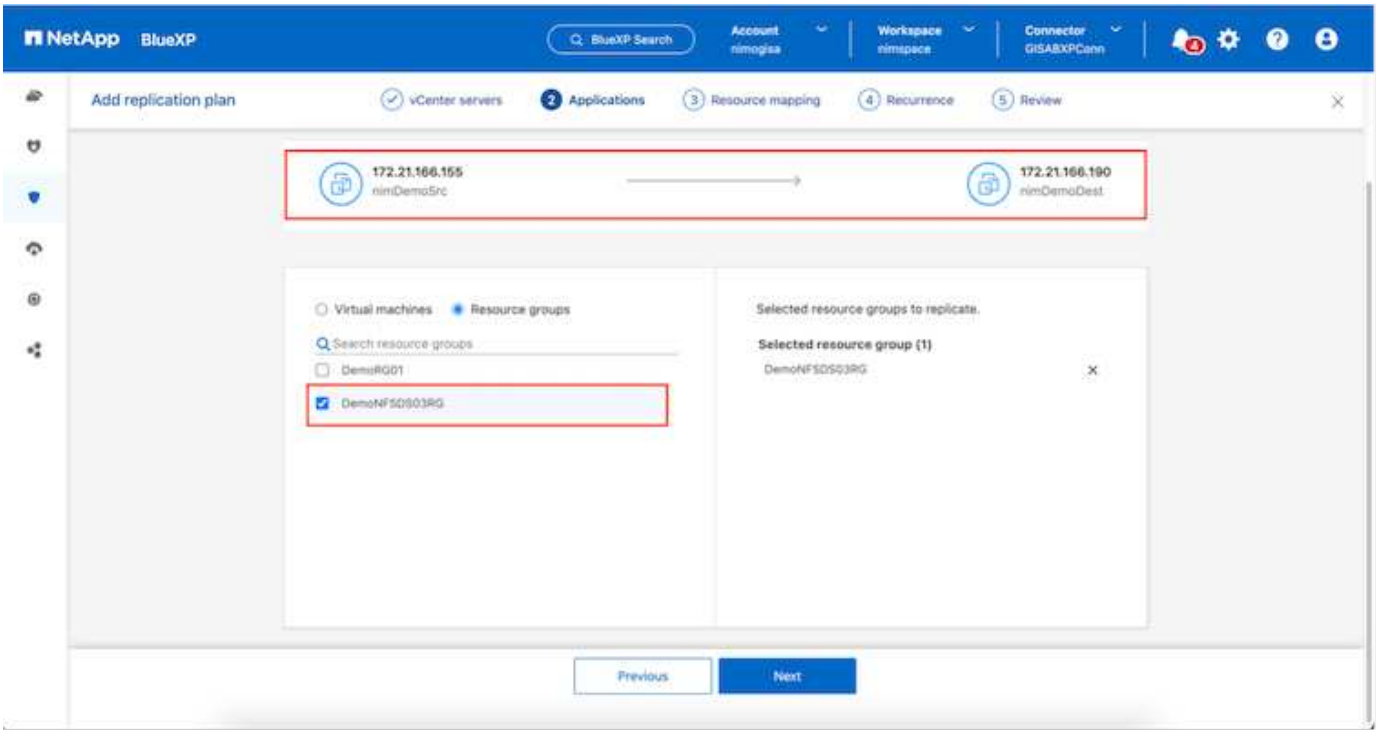
Konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und der Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

Wählen Sie zuerst das Quell-vCenter und dann das Ziel-vCenter aus.



Der nächste Schritt besteht darin, vorhandene Ressourcengruppen auszuwählen. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent dabei, die erforderlichen virtuellen Maschinen basierend

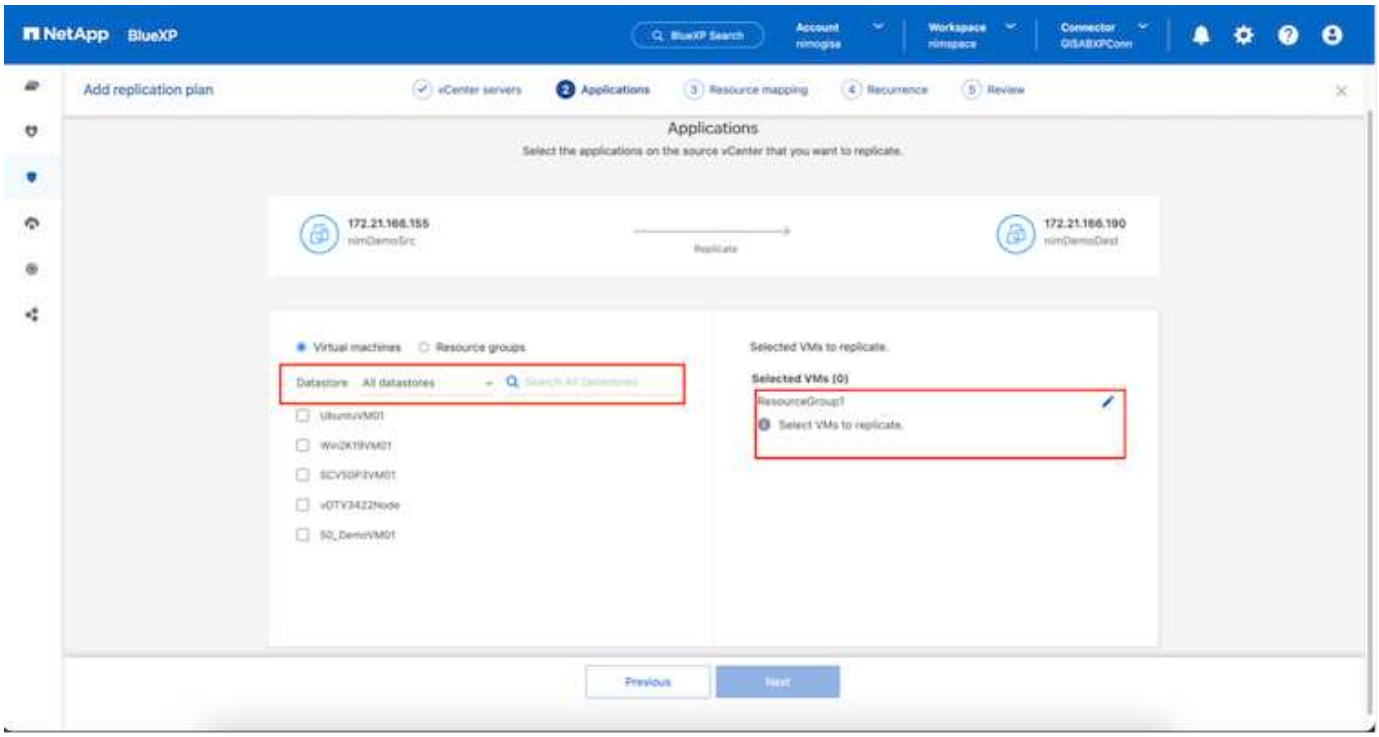
auf den Wiederherstellungszielen zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Vorgangsreihenfolge für die Wiederherstellung virtueller Anwendungsmaschinen zu definieren.



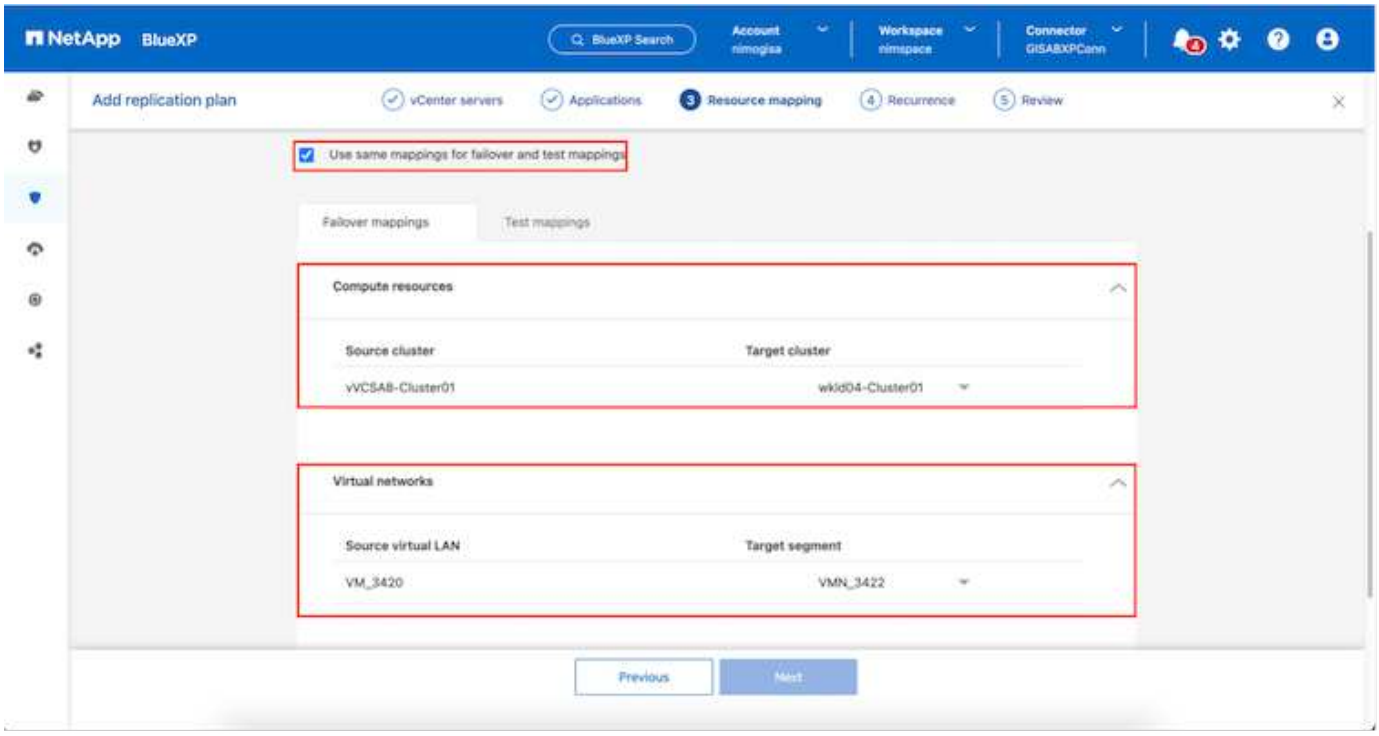
Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.

Jede virtuelle Maschine innerhalb einer Ressourcengruppe wird der Reihe nach basierend auf der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

Der folgende Screenshot zeigt die Option zum Filtern virtueller Maschinen oder bestimmter Datenspeicher basierend auf organisatorischen Anforderungen, wenn nicht zuvor Ressourcengruppen erstellt wurden.

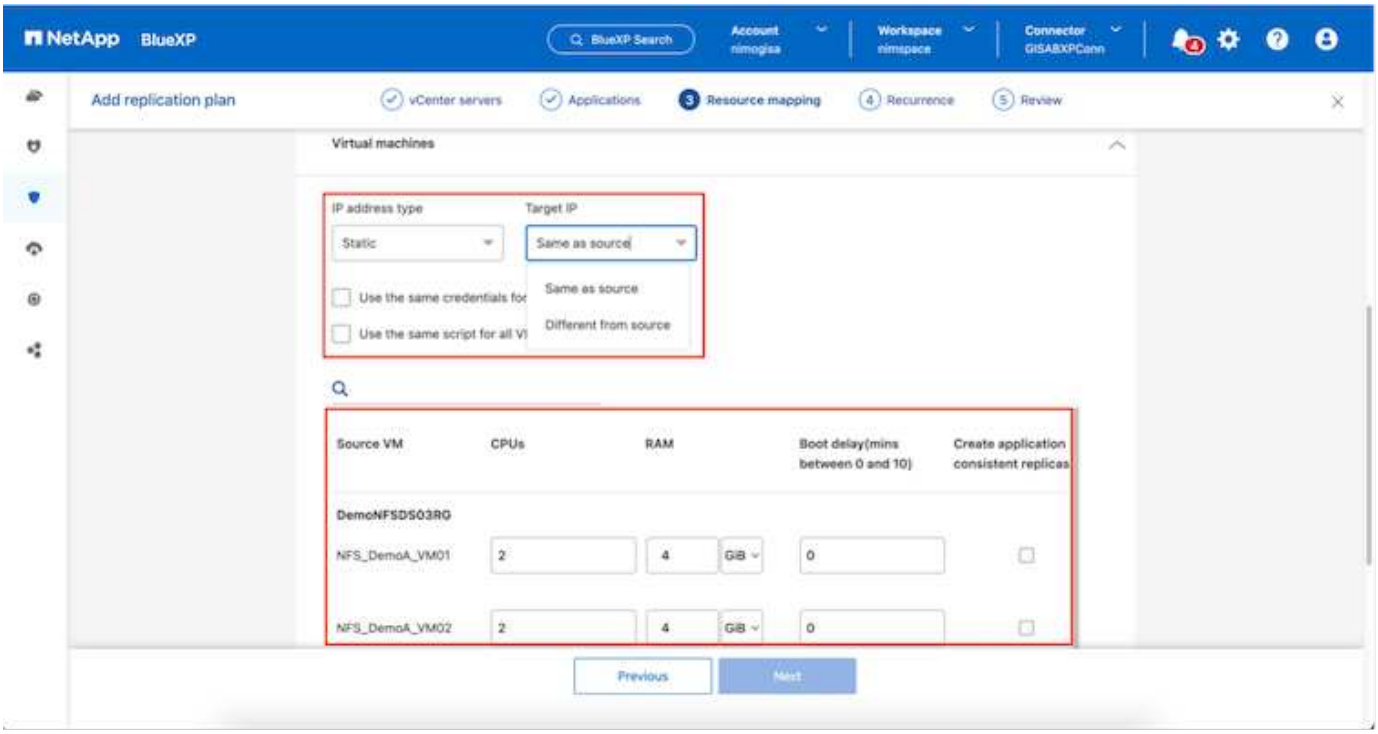


Sobald die Ressourcengruppen ausgewählt sind, werden die Failover-Zuordnungen erstellt. In diesem Schritt wird festgelegt, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dies umfasst Rechenressourcen und virtuelle Netzwerke. Dazu gehören IP-Anpassung, Vor- und Nachskripte, Startverzögerungen, Applikationskonsistenz usw. Ausführliche Informationen finden Sie in "Erstellen eines Replikationsplans".

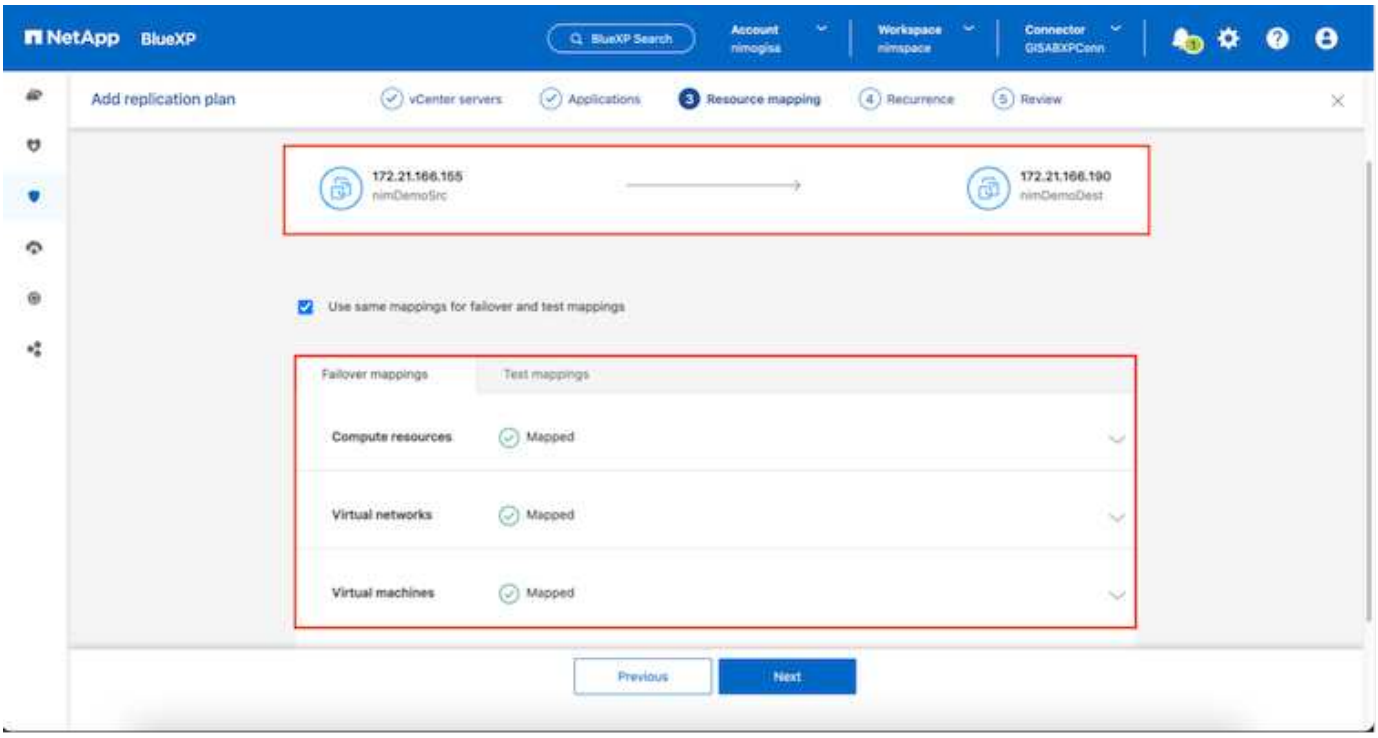


Standardmäßig werden für Test- und Failovervorgänge dieselben Zuordnungsparameter verwendet. Um verschiedene Zuordnungen für die Testumgebung festzulegen, wählen Sie die Option „Testzuordnung“ aus, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert

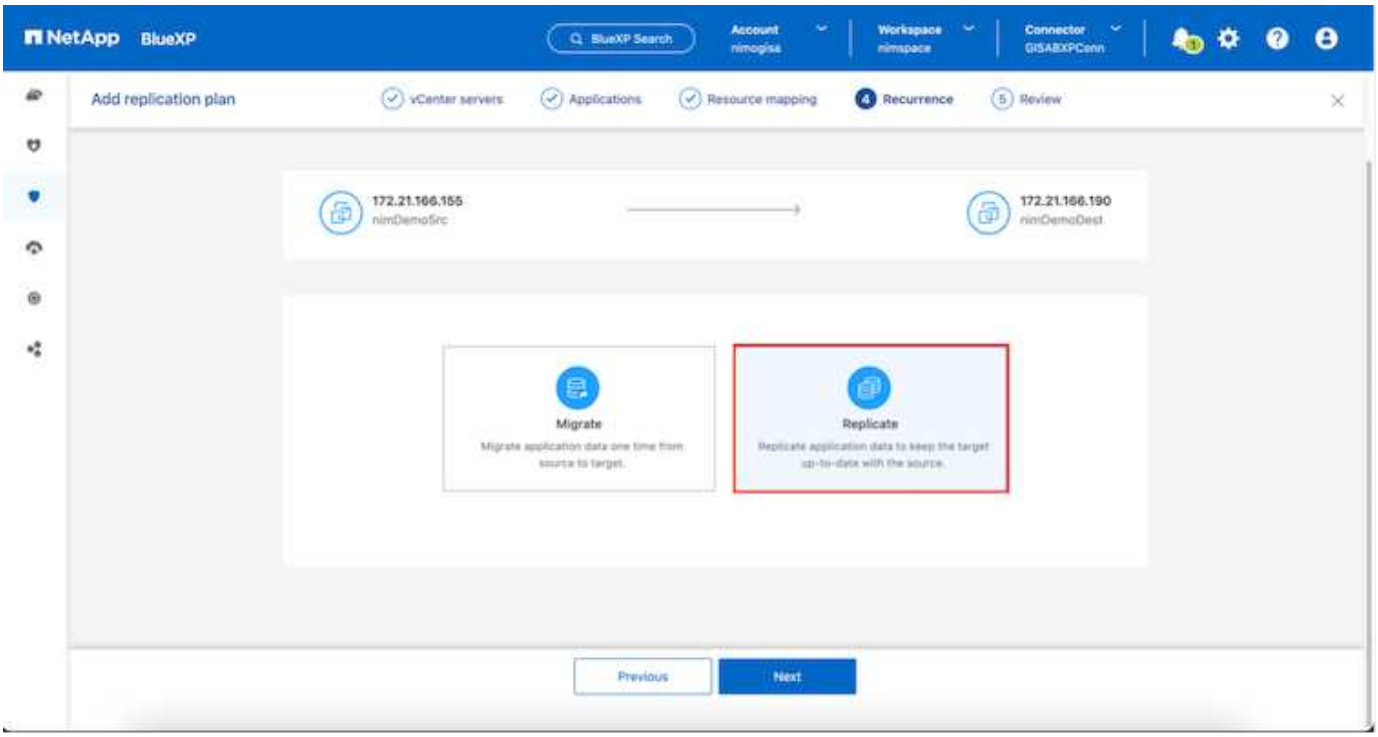
haben:



Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.

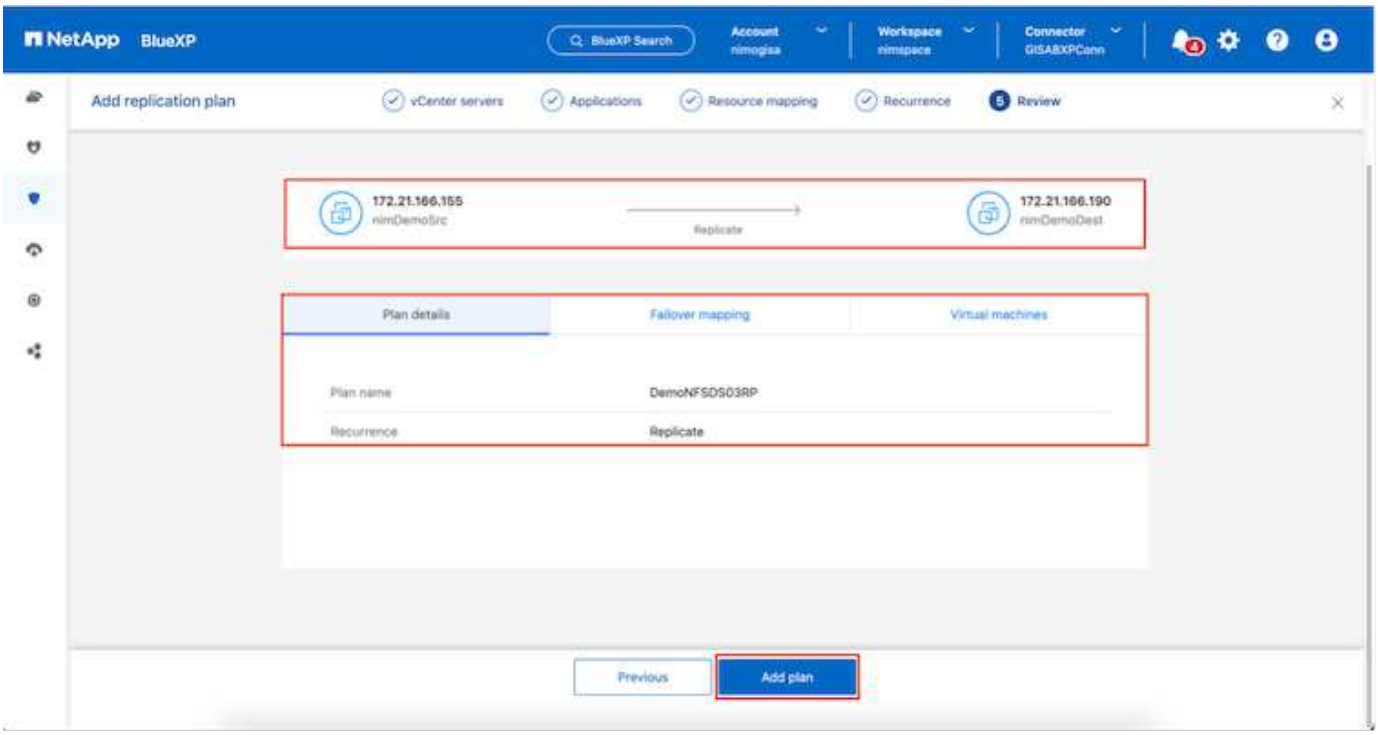


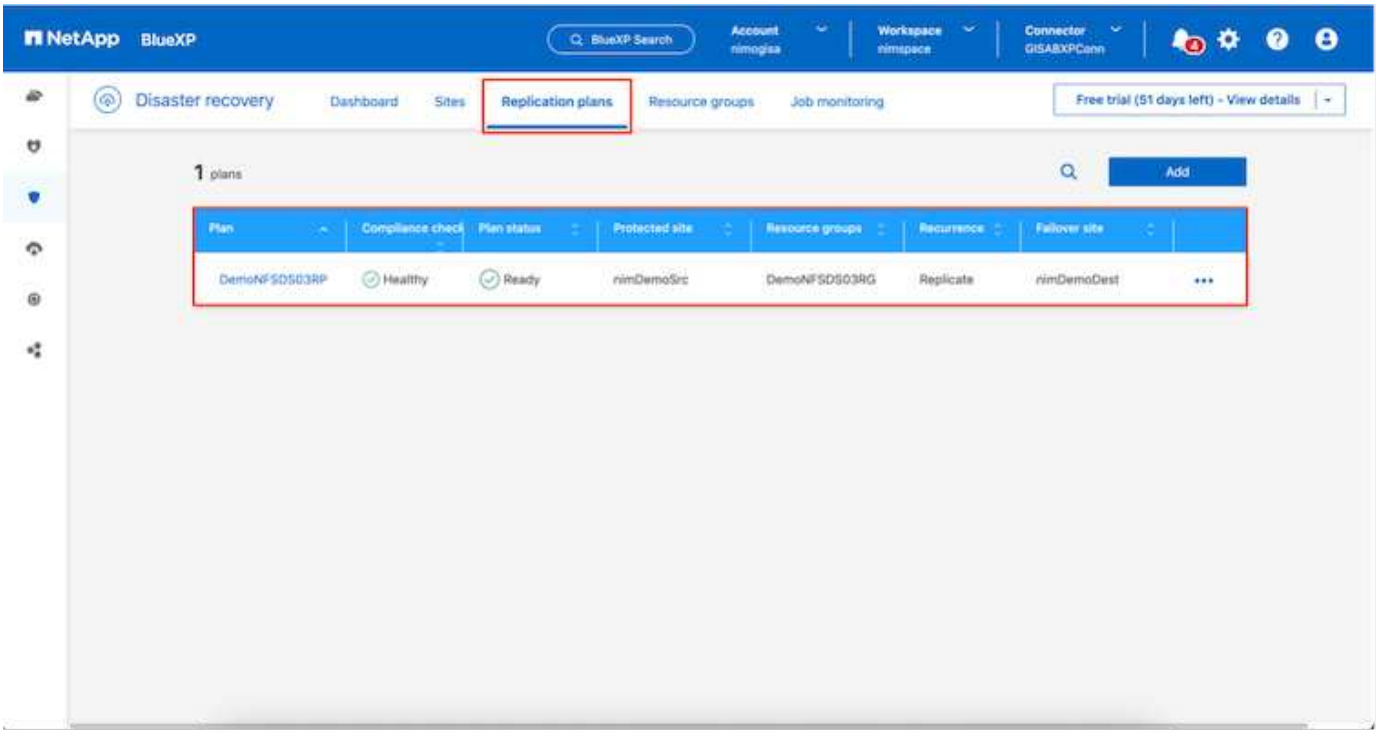
Wählen Sie den Wiederholungstyp aus. Einfach ausgedrückt: Wählen Sie „Migrieren“ (einmalige Migration mit Failover) oder die Option „Wiederkehrende kontinuierliche Replikation“. In dieser exemplarischen Vorgehensweise ist die Option „Replizieren“ ausgewählt.



Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf **Plan hinzufügen**.

VMs von verschiedenen Volumes und SVMs können in einen Replikationsplan einbezogen werden. Abhängig von der VM-Platzierung (ob auf demselben Volume oder auf einem separaten Volume innerhalb derselben SVM oder auf separaten Volumes auf verschiedenen SVMs) erstellt Disaster Recovery einen Konsistenzgruppen-Snapshot.



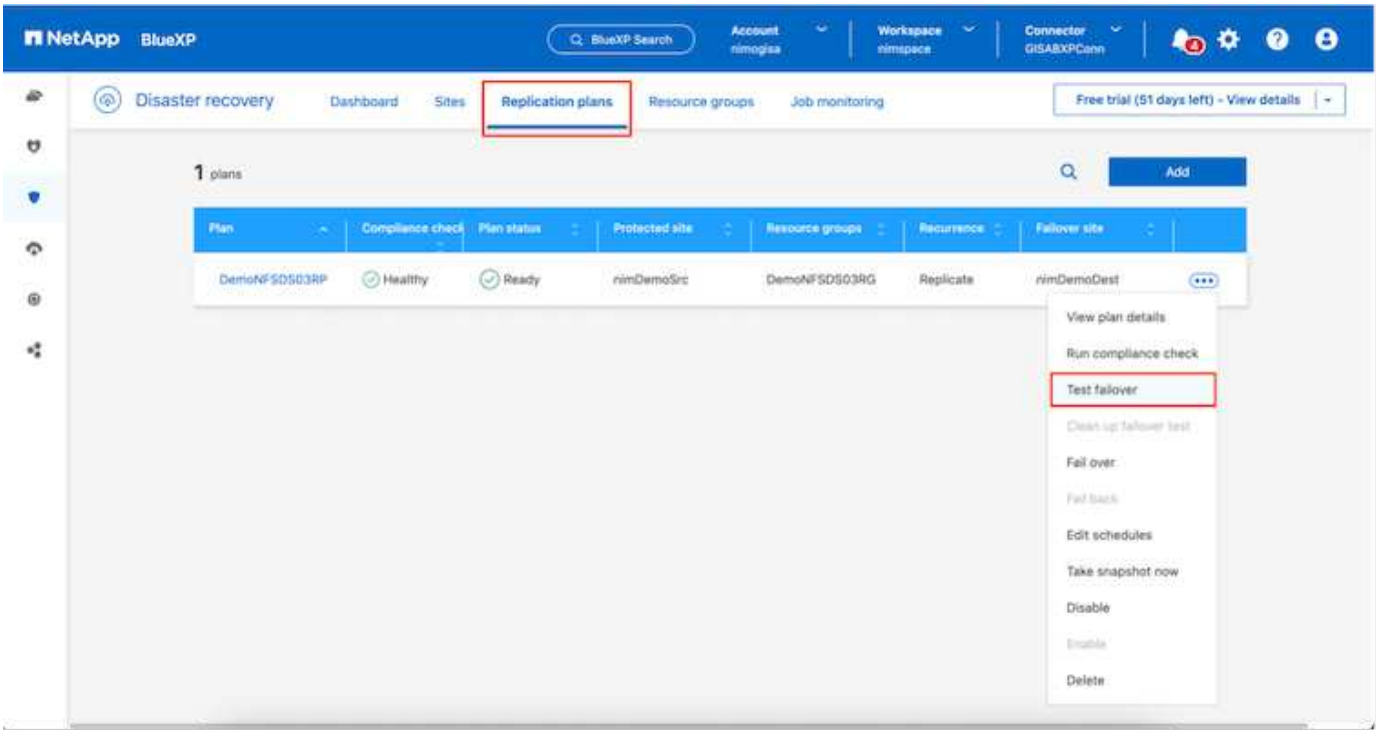


Disaster Recovery umfasst die folgenden Workflows:

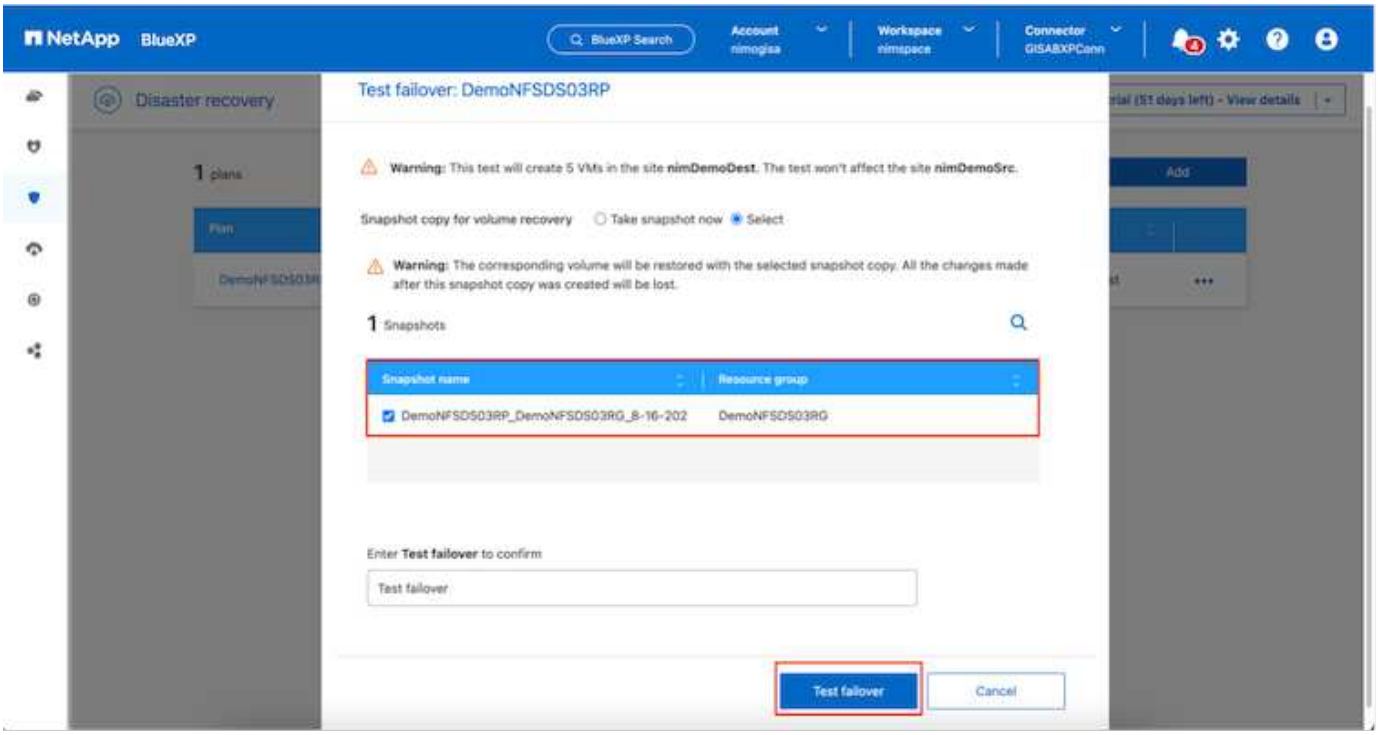
- Test-Failover (einschließlich regelmäßiger automatisierter Simulationen)
- Failovertest bereinigen
- Ausfallsicherung
- Failback

Testen des Failovers

Der Test Failover in Disaster Recovery ist ein operatives Verfahren, das VMware-Administratoren die vollständige Validierung ihrer Wiederherstellungspläne ermöglicht, ohne ihre Produktionsumgebungen zu beeinträchtigen. Während eines Test Failover erstellt Disaster Recovery platzsparende NetApp FlexClone Kopien der replizierten NFS-Datastore-Volumes auf dem DR Storage-System. Diese FlexClone Volumes werden dann auf den ESXi-Hosts am DR-Standort eingebunden, und die VMs werden in einem isolierten Testnetzwerk gestartet. Dieser Prozess ermöglicht Administratoren die Überprüfung, ob ihre Disaster Recovery Pläne im Falle einer tatsächlichen Katastrophe wie vorgesehen funktionieren.



Disaster Recovery umfasst die Möglichkeit, den Snapshot als optionale Funktion im Test Failover-Vorgang auszuwählen. Diese Funktion ermöglicht es dem VMware-Administrator, zu überprüfen, ob kürzlich in der Umgebung vorgenommene Änderungen an den Zielstandort repliziert wurden und somit während des Tests verfügbar sind. Zu diesen Änderungen gehören beispielsweise Patches für das Gastbetriebssystem der virtuellen Maschine.

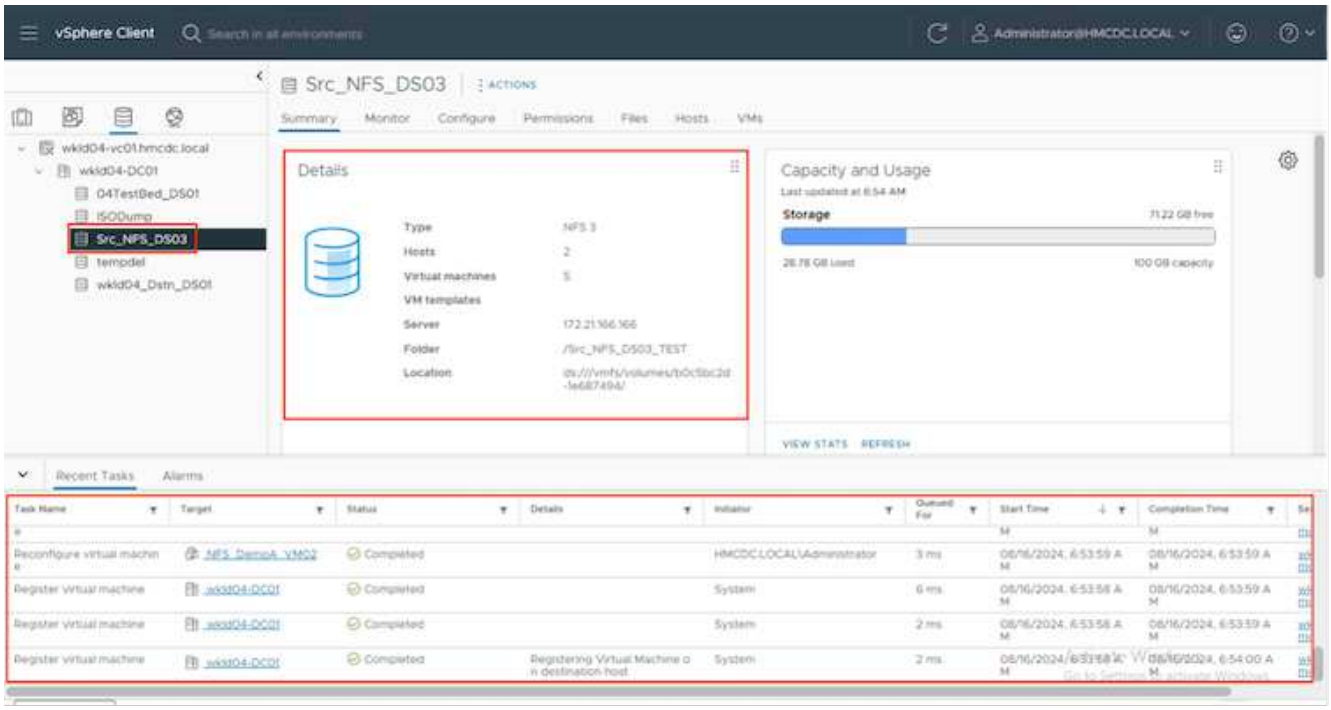


Wenn der VMware-Administrator einen Test-Failover ausführt, automatisiert Disaster Recovery die folgenden Aufgaben:

- Auslösen von SnapMirror -Beziehungen, um den Speicher am Zielstandort mit allen kürzlich am

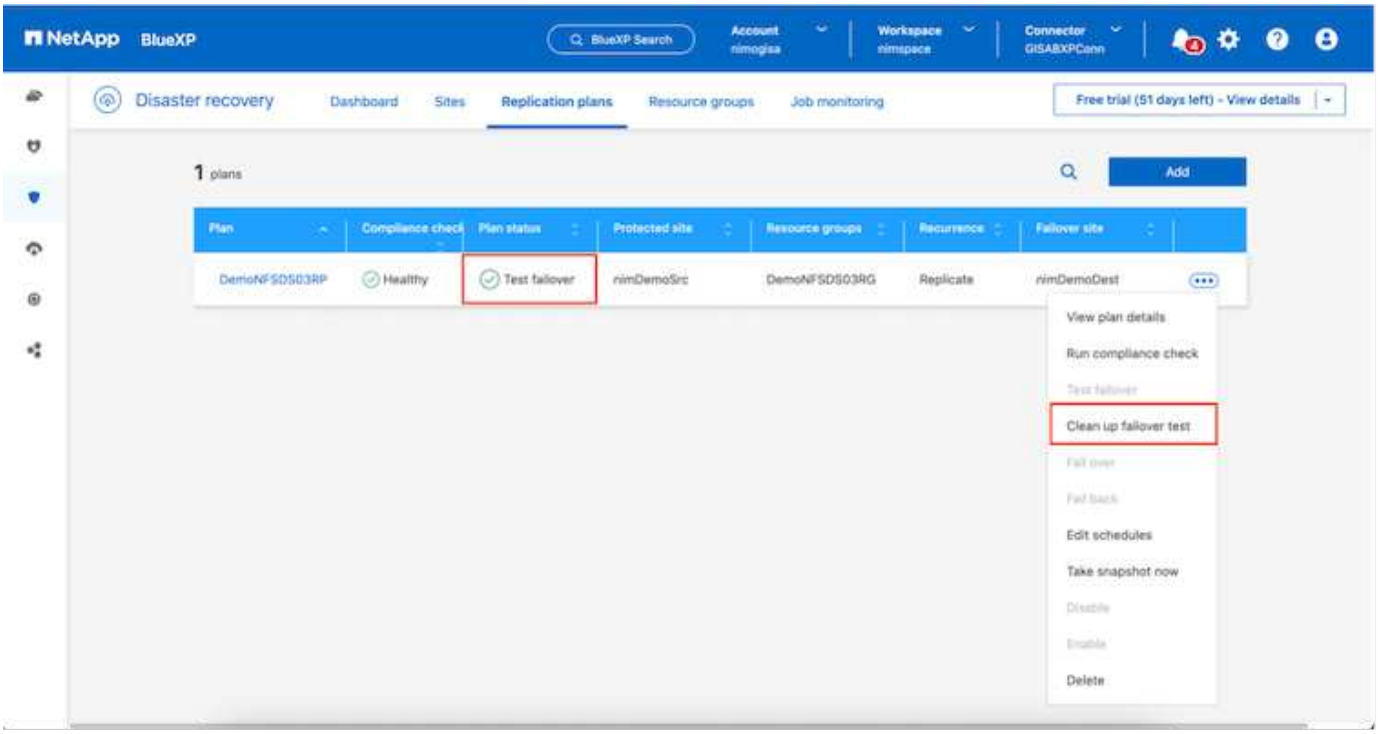
Produktionsstandort vorgenommenen Änderungen zu aktualisieren.

- Erstellen von NetApp FlexClone -Volumes der FlexVol -Volumes auf dem DR-Speicherarray.
- Verbinden der NFS-Datenspeicher in den FlexClone -Volumes mit den ESXi-Hosts am DR-Standort.
- Verbinden der VM-Netzwerkadapter mit dem während der Zuordnung angegebenen Testnetzwerk.
- Neukonfigurieren der Netzwerkeinstellungen des VM-Gastbetriebssystems wie für das Netzwerk am DR-Standort definiert.
- Ausführen aller benutzerdefinierten Befehle, die im Replikationsplan gespeichert wurden.
- Einschalten der VMs in der im Replikationsplan festgelegten Reihenfolge.



Bereinigungs-Failover-Testvorgang

Der Bereinigungs-Failover-Testvorgang wird ausgeführt, nachdem der Replikationsplantest abgeschlossen wurde und der VMware-Administrator auf die Bereinigungsaufforderung reagiert.



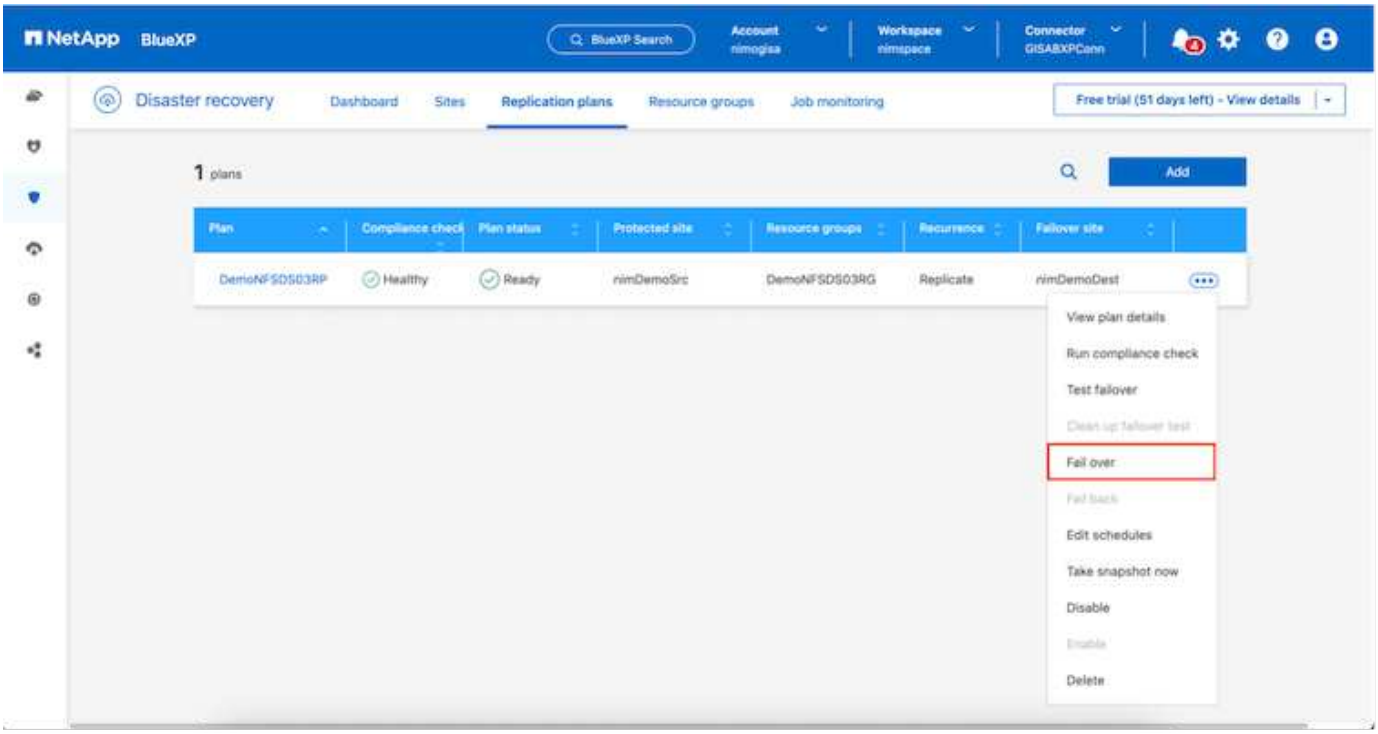
Durch diese Aktion werden die virtuellen Maschinen (VMs) und der Status des Replikationsplans auf den Bereitschaftszustand zurückgesetzt.

Wenn der VMware-Administrator einen Wiederherstellungsvorgang durchführt, schließt Disaster Recovery den folgenden Prozess ab:

1. Es schaltet jede wiederhergestellte VM in der FlexClone -Kopie aus, die zum Testen verwendet wurde.
2. Es löscht das FlexClone Volume, das während des Tests zum Präsentieren der wiederhergestellten VMs verwendet wurde.

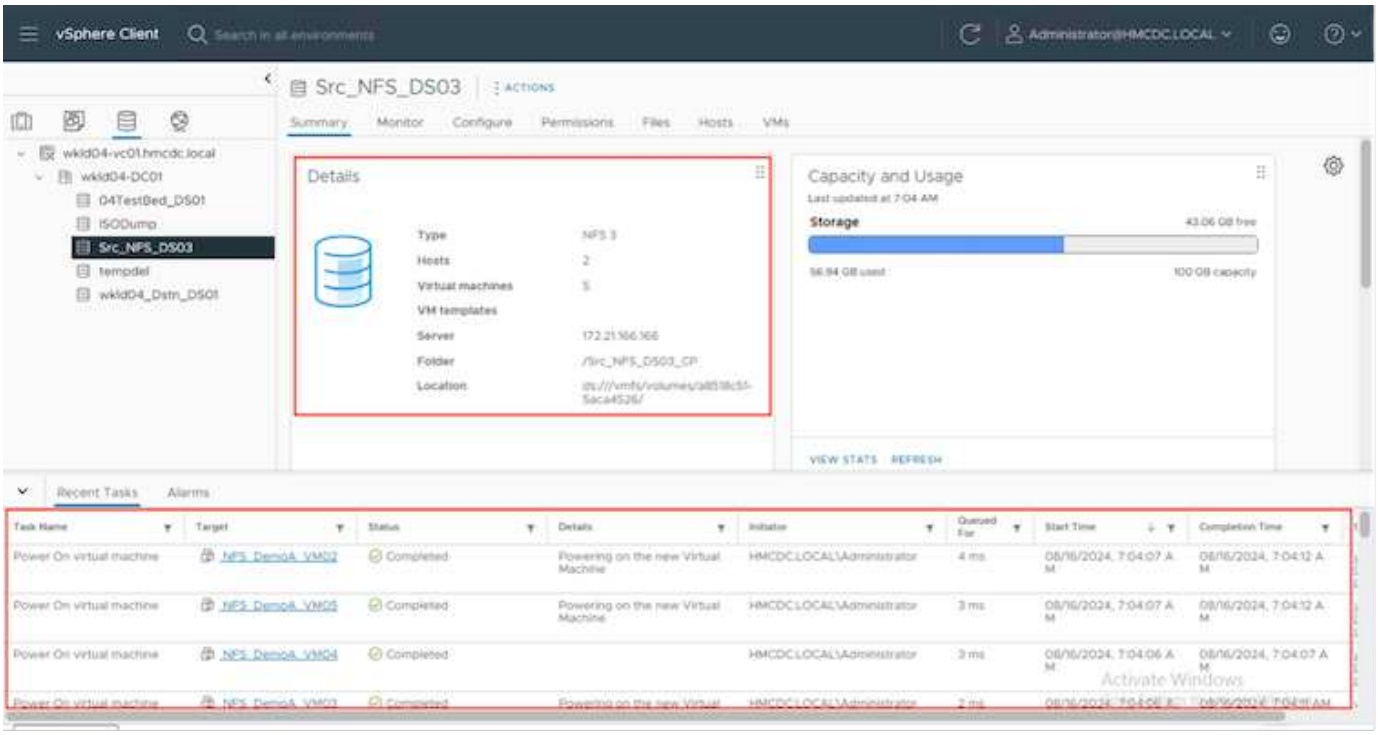
Geplante Migration und Failover

Disaster Recovery bietet zwei Methoden zur Durchführung eines tatsächlichen Failover: geplante Migration und Failover. Die erste Methode, die geplante Migration, integriert das Herunterfahren der virtuellen Maschinen (VMs) und die Synchronisierung der Storage-Replizierung in den Prozess, um die VMs am Zielstandort wiederherzustellen oder effektiv dorthin zu verschieben. Für die geplante Migration ist Zugriff auf den Quellstandort erforderlich. Die zweite Methode, das Failover, ist ein geplantes oder ungeplantes Failover, bei dem die VMs am Zielstandort auf Grundlage des letzten abgeschlossenen Intervalls der Storage-Replizierung wiederhergestellt werden. Abhängig vom RPO, das in die Lösung eingeplant wurde, ist im DR-Szenario mit einem gewissen Datenverlust zu rechnen.



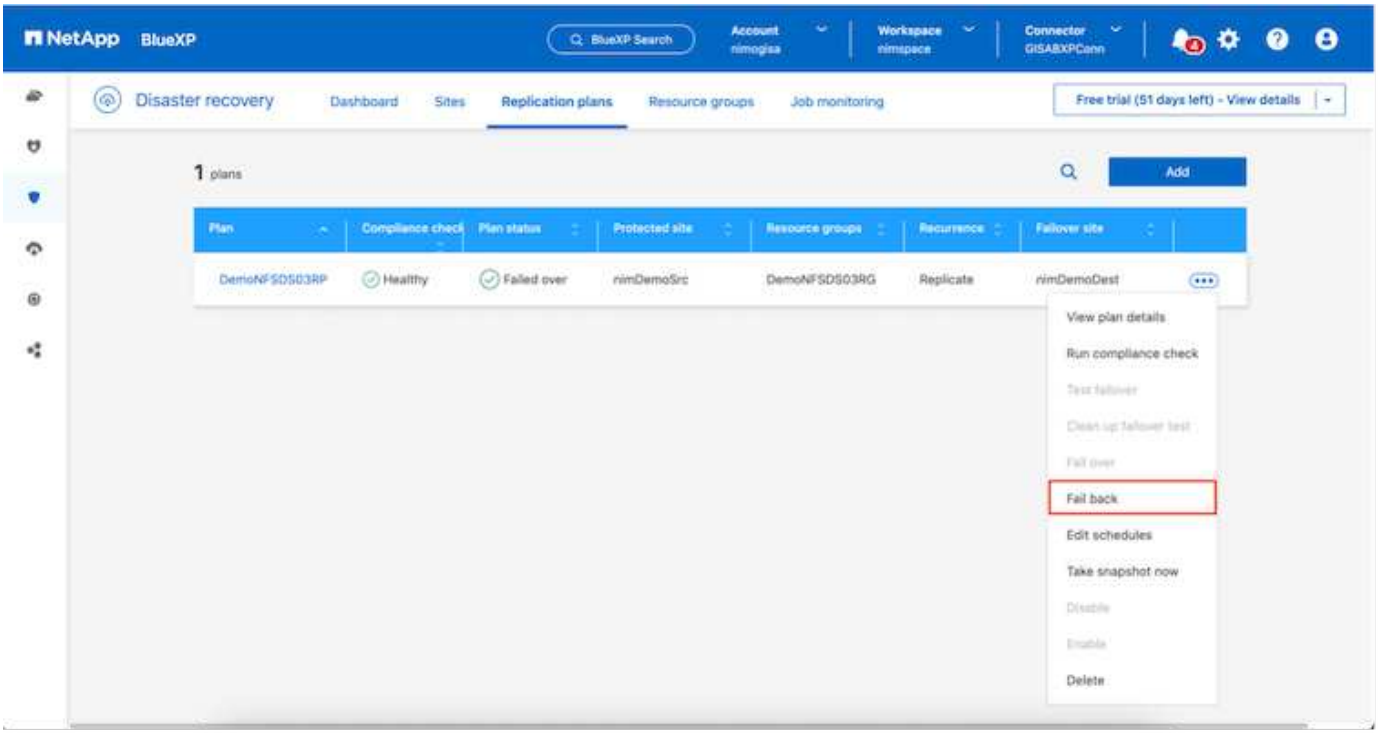
Wenn der VMware-Administrator einen Failover-Vorgang durchführt, automatisiert Disaster Recovery die folgenden Aufgaben:

- Unterbrechen und Failover der NetApp SnapMirror -Beziehungen.
- Verbinden Sie die replizierten NFS-Datenspeicher mit den ESXi-Hosts am DR-Standort.
- Verbinden Sie die VM-Netzwerkadapter mit dem entsprechenden Zielstandortnetzwerk.
- Konfigurieren Sie die Netzwerkeinstellungen des VM-Gastbetriebssystems neu, wie für das Netzwerk am Zielstandort definiert.
- Führen Sie alle benutzerdefinierten Befehle (sofern vorhanden) aus, die im Replikationsplan gespeichert wurden.
- Schalten Sie die VMs in der im Replikationsplan festgelegten Reihenfolge ein.



Failback

Ein Failback ist ein optionales Verfahren, das nach einer Wiederherstellung die ursprüngliche Konfiguration der Quell- und Zielsites wiederherstellt.



VMware-Administratoren können ein Failback-Verfahren konfigurieren und ausführen, wenn sie bereit sind, die Dienste auf der ursprünglichen Quellsite wiederherzustellen.

HINWEIS: Disaster Recovery repliziert (resynchronisiert) alle Änderungen zurück auf die ursprüngliche Quell-VM, bevor die Replikationsrichtung umgekehrt wird. Dieser Prozess beginnt mit einer Beziehung, für die ein

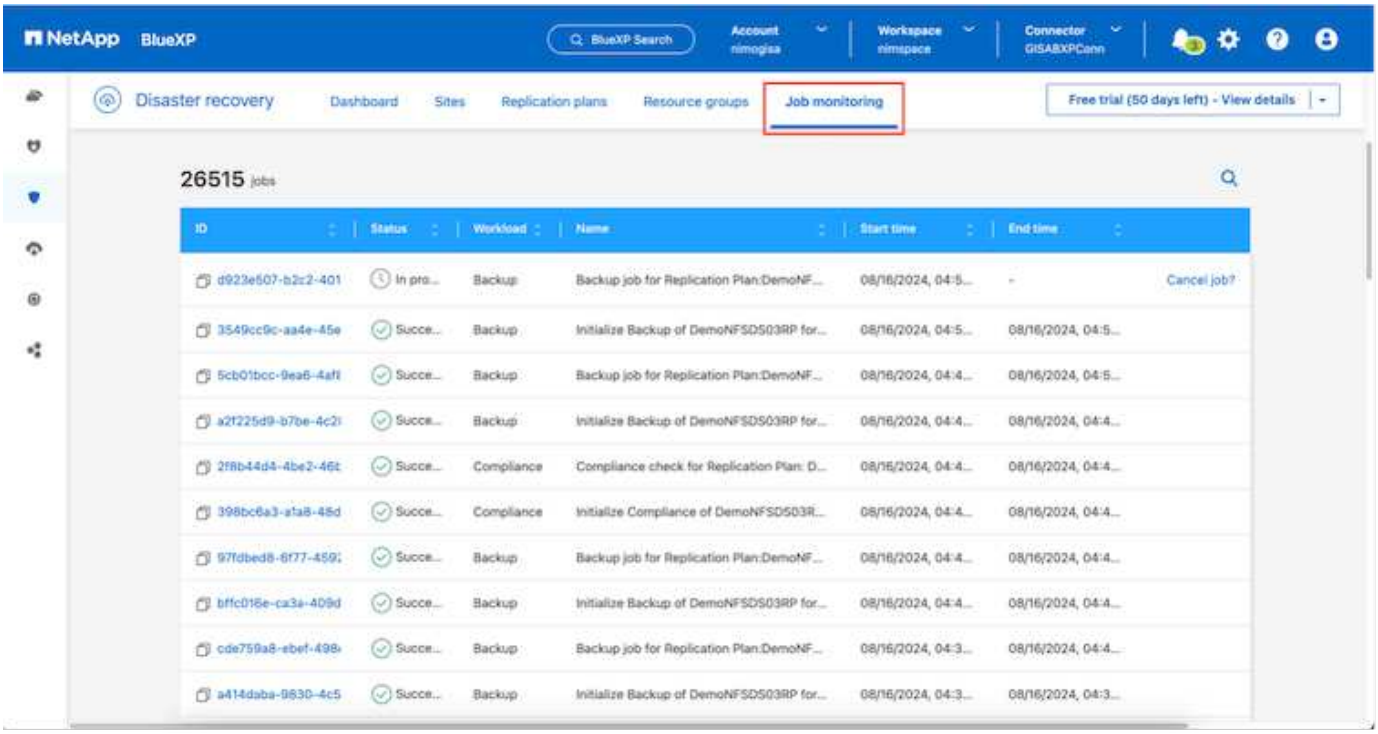
Failover zu einem Ziel abgeschlossen wurde, und umfasst die folgenden Schritte:

- Schalten Sie die virtuellen Maschinen aus und heben Sie die Registrierung auf. Die Volumes auf der Zielsite werden ausgehängt.
- Unterbrechen Sie die SnapMirror -Beziehung zur Originalquelle, um Lese-/Schreibzugriff zu ermöglichen.
- Synchronisieren Sie die SnapMirror -Beziehung erneut, um die Replikation umzukehren.
- Mounten Sie das Volume auf der Quelle, schalten Sie die virtuellen Quellmaschinen ein und registrieren Sie sie.

Weitere Informationen zum Zugriff auf und zur Konfiguration von Disaster Recovery sind in "Informationen zu NetApp Disaster Recovery for VMware" enthalten.

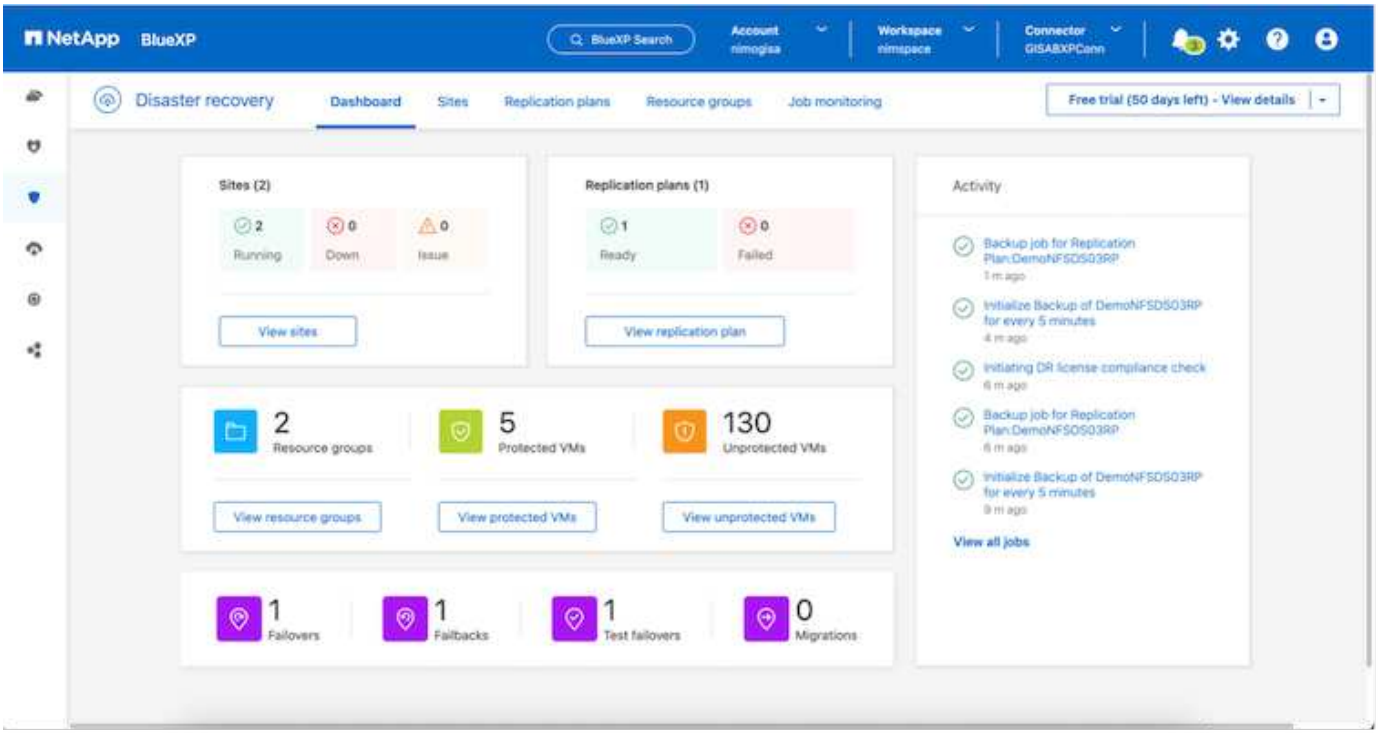
Überwachung und Dashboard

Über Console oder die ONTAP CLI können Sie den Systemstatus der entsprechenden Datastore-Volumes überwachen, und der Status eines Failover oder Test-Failover lässt sich über Job Monitoring verfolgen.



Wenn ein Auftrag gerade ausgeführt wird oder sich in der Warteschlange befindet und Sie ihn stoppen möchten, können Sie ihn mit der Option „Abbrechen“ abbrechen.

Mit dem Dashboard für Disaster Recovery lässt sich der Status von Disaster-Recovery-Standorten und Replikationsplänen zuverlässig bewerten. Dadurch lassen sich funktionsfähige, getrennte oder beeinträchtigte Standorte und Pläne durch Administratoren schnell identifizieren.



Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten und individuellen Notfallwiederherstellungsplans. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Um mehr über diesen Prozess zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen oder die"Lösungssimulator" .

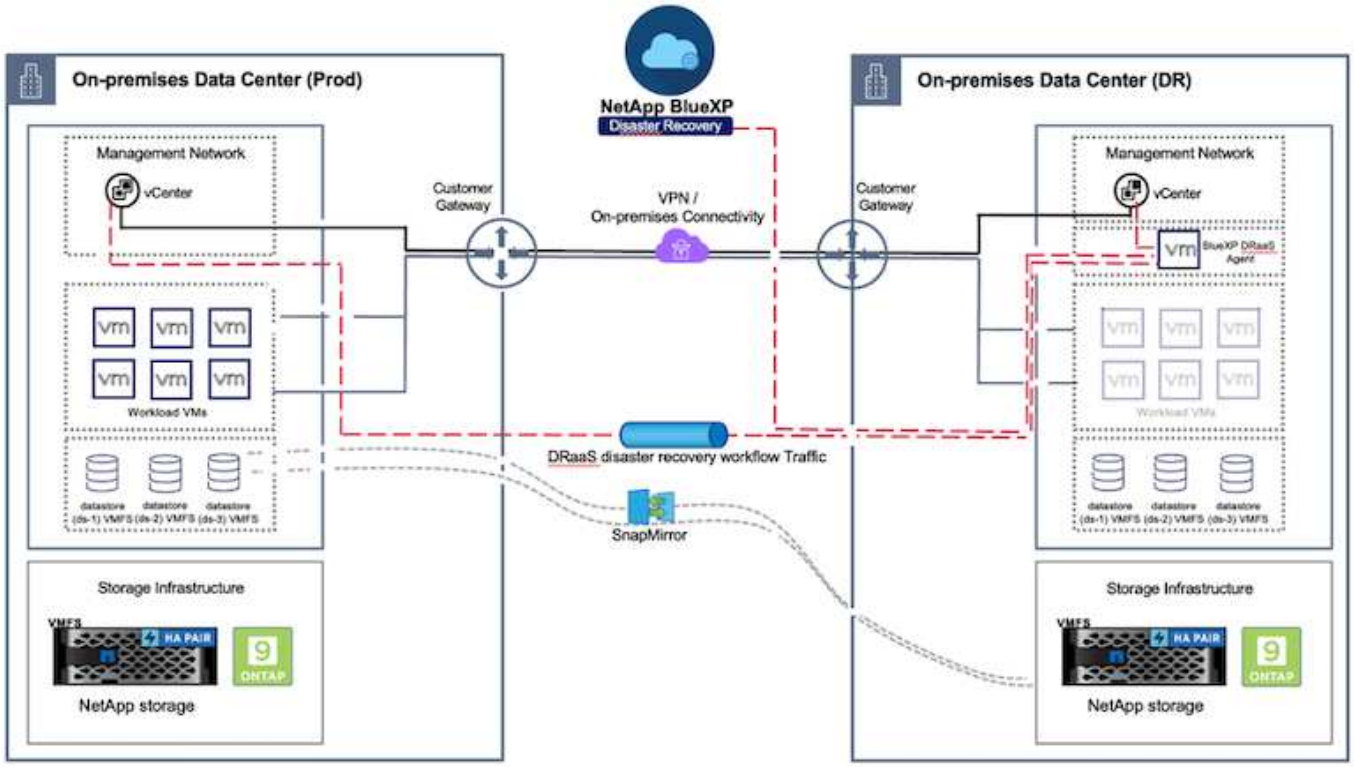
NetApp Disaster Recovery für VMFS-Datastores

Die Notfallwiederherstellung mithilfe der Blockebenenreplikation vom Produktionsstandort zum Notfallwiederherstellungsstandort ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware-Angriffen zu schützen. Mit der NetApp SnapMirror Replikation können VMware-Workloads, die auf lokalen ONTAP -Systemen mit VMFS-Datenspeicher ausgeführt werden, auf ein anderes ONTAP Speichersystem in einem dafür vorgesehenen Wiederherstellungs-Rechenzentrum repliziert werden, in dem sich VMware befindet.

Dieser Abschnitt des Dokuments beschreibt die Konfiguration von NetApp Diaster Recovery, um die Disaster Recovery für lokale VMware-VMs an einem anderen festgelegten Standort einzurichten. Zu dieser Einrichtung gehören Console agent, das Onboarding der ONTAP-Arrays, die Definition von Standorten und die Zuordnung von VMware vCenter. Darüber hinaus wird in diesem Dokument подробно beschrieben, wie die Replikation zwischen Standorten konfiguriert wird und wie ein Wiederherstellungsplan eingerichtet und getestet wird. Im letzten Abschnitt wird beschrieben, wie ein vollständiges Standort-Failover durchgeführt wird und wie ein Failback erfolgt, wenn der primäre Standort wiederhergestellt und wieder online gebracht wurde.

Mithilfe von Disaster Recovery, einem Teil von NetApp Data Services, können Kunden ihre lokalen VMware vCenters zusammen mit ONTAP Storage identifizieren, Ressourcengruppen erstellen, einen Disaster Recovery Plan erstellen, ihn mit Ressourcengruppen verknüpfen und Failover sowie Failback testen oder ausführen. SnapMirror bietet Storage-seitige Blockreplizierung, um die beiden Standorte mit inkrementellen Änderungen auf dem neuesten Stand zu halten, was zu einem RPO von bis zu 5 Minuten führt. Außerdem können DR-Prozeduren als regelmäßige Übung simuliert werden, ohne die Produktionsumgebung und die

replizierten Datastores zu beeinträchtigen oder zusätzliche Storage-Kosten zu verursachen. NetApp Data Services nutzt die FlexClone Technologie von ONTAP, um eine platzsparende Kopie des VMFS-Datastores aus dem zuletzt replizierten Snapshot am DR-Standort zu erstellen. Nach Abschluss des DR-Tests können Kunden die Testumgebung einfach löschen, wiederum ohne Auswirkungen auf die tatsächlich replizierten Produktionsressourcen. Wenn ein tatsächliches Failover erforderlich ist, ob geplant oder ungeplant, orchestriert Disaster Recovery mit wenigen Klicks alle erforderlichen Schritte, um die geschützten virtuellen Maschinen am vorgesehenen Disaster Recovery Standort automatisch hochzufahren. Der Service kehrt bei Bedarf auch die SnapMirror Beziehung zum primären Standort um und repliziert alle Änderungen vom sekundären zum primären Standort für einen Failback-Vorgang. All dies lässt sich im Vergleich zu anderen bekannten Alternativen zu einem Bruchteil der Kosten erreichen.

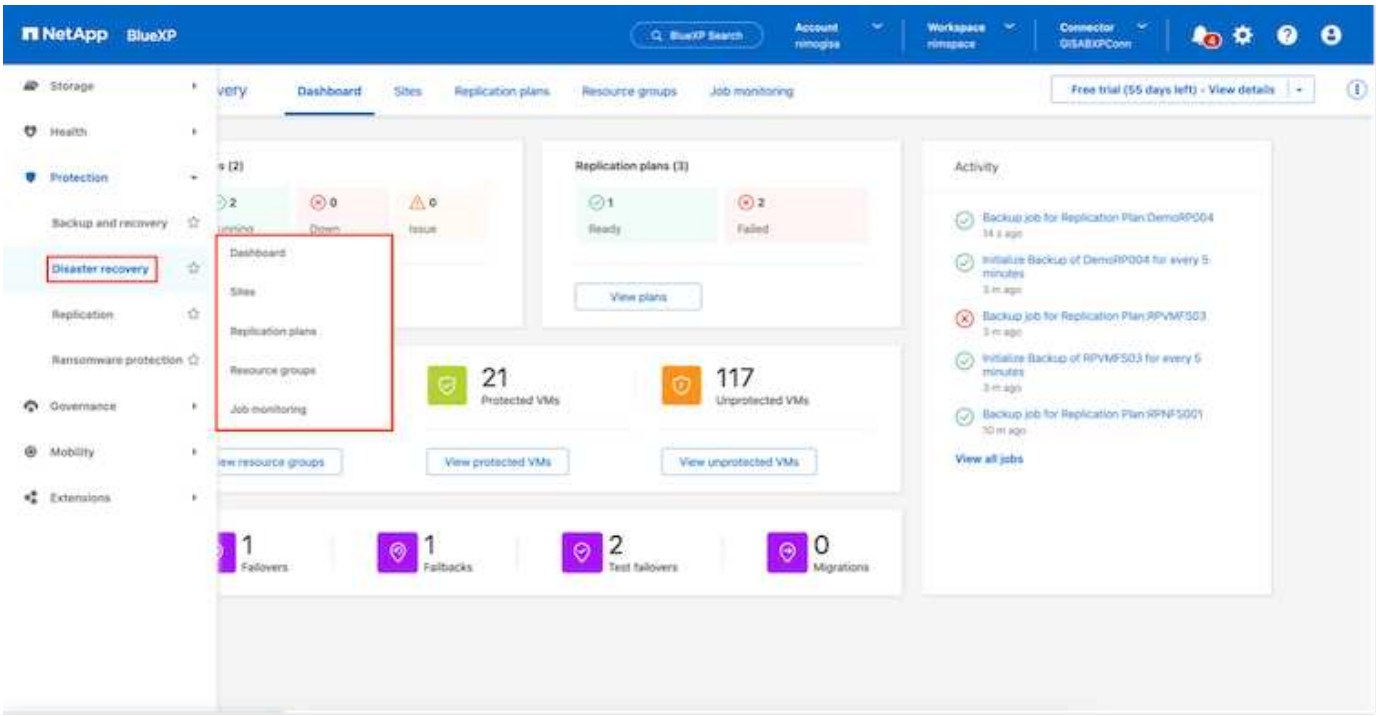


Aktuelle Informationen und unterstützte Versionen von vCenter Server, ESXi und ONTAP for Disaster Recovery finden Sie in der "Unterstützte Konfigurationen für die Notfallwiederherstellung".

Erste Schritte

Für den Einstieg in Disaster Recovery verwenden Sie die NetApp Console; anschließend greifen Sie auf den Dienst zu.

1. Anmeldung bei Console.
2. Die Auswahl erfolgt in der linken Navigationsleiste der Console über Protection > Disaster recovery.
3. Das Dashboard für die Notfallwiederherstellung erscheint.

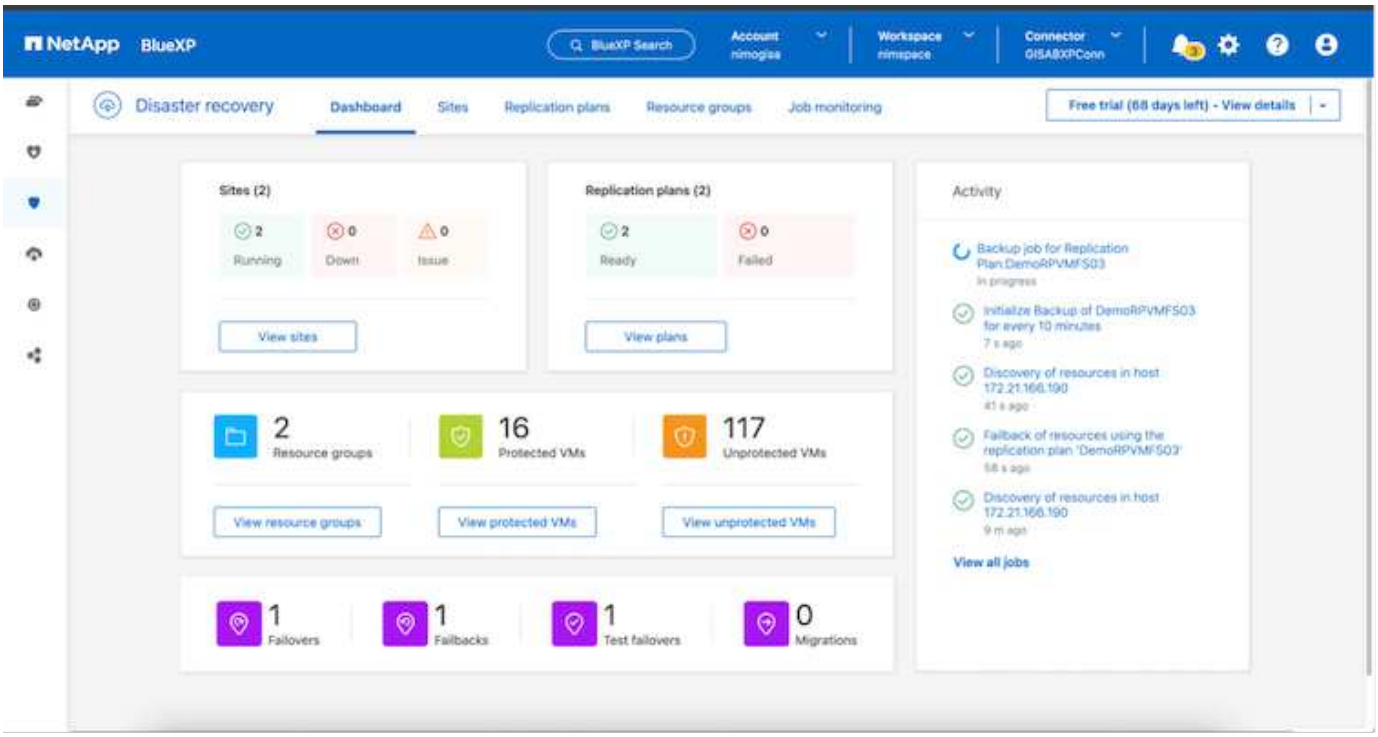


Stellen Sie vor der Konfiguration des Notfallwiederherstellungsplans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der Console Agent wird in einer AWS VPC bereitgestellt.
- Die Console Agent-Instanz verfügt über Verbindungen zu den Quell- und Ziel-vCenter- sowie zu den Storage-Systemen.
- In Console werden lokale NetApp Storage-Systeme hinzugefügt, die VMFS-Datenspeicher für VMware hosten.
- Bei der Verwendung von DNS-Namen sollte eine DNS-Auflösung vorhanden sein. Andernfalls verwenden Sie IP-Adressen für das vCenter.
- Die SnapMirror Replikation ist für die angegebenen VMFS-basierten Datenspeichervolumes konfiguriert.

Sobald die Verbindung zwischen Quell- und Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Dies sollte etwa 3 bis 5 Minuten dauern.

NetApp empfiehlt die Bereitstellung des Console Agenten am Disaster-Recovery-Standort oder an einem dritten Standort, damit der Console Agent während tatsächlicher Ausfälle oder Naturkatastrophen über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.

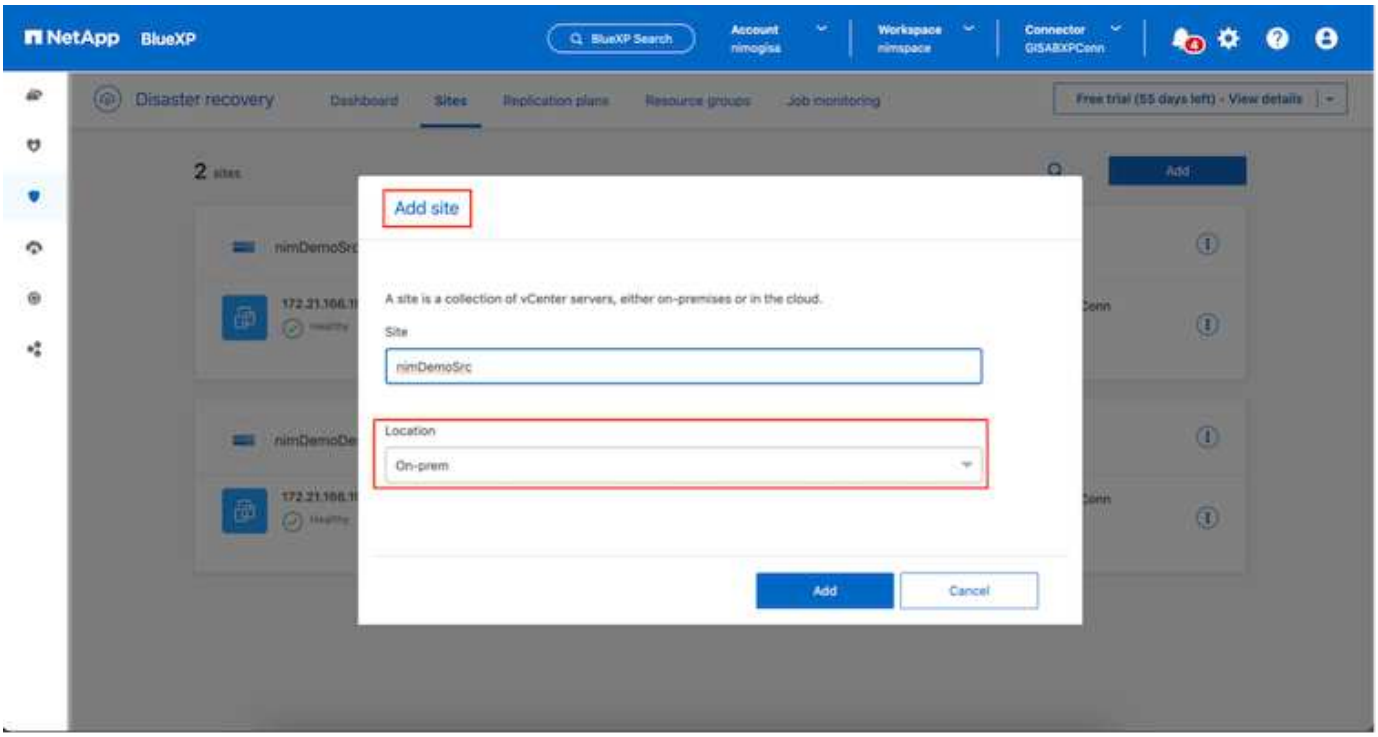


Die Unterstützung für lokale VMFS-Datenspeicher befindet sich beim Schreiben dieses Dokuments in der Technologievorschau. Die Funktion wird sowohl mit FC- als auch mit ISCSI-Protokoll-basierten VMFS-Datenspeichern unterstützt.

Konfiguration für die Notfallwiederherstellung

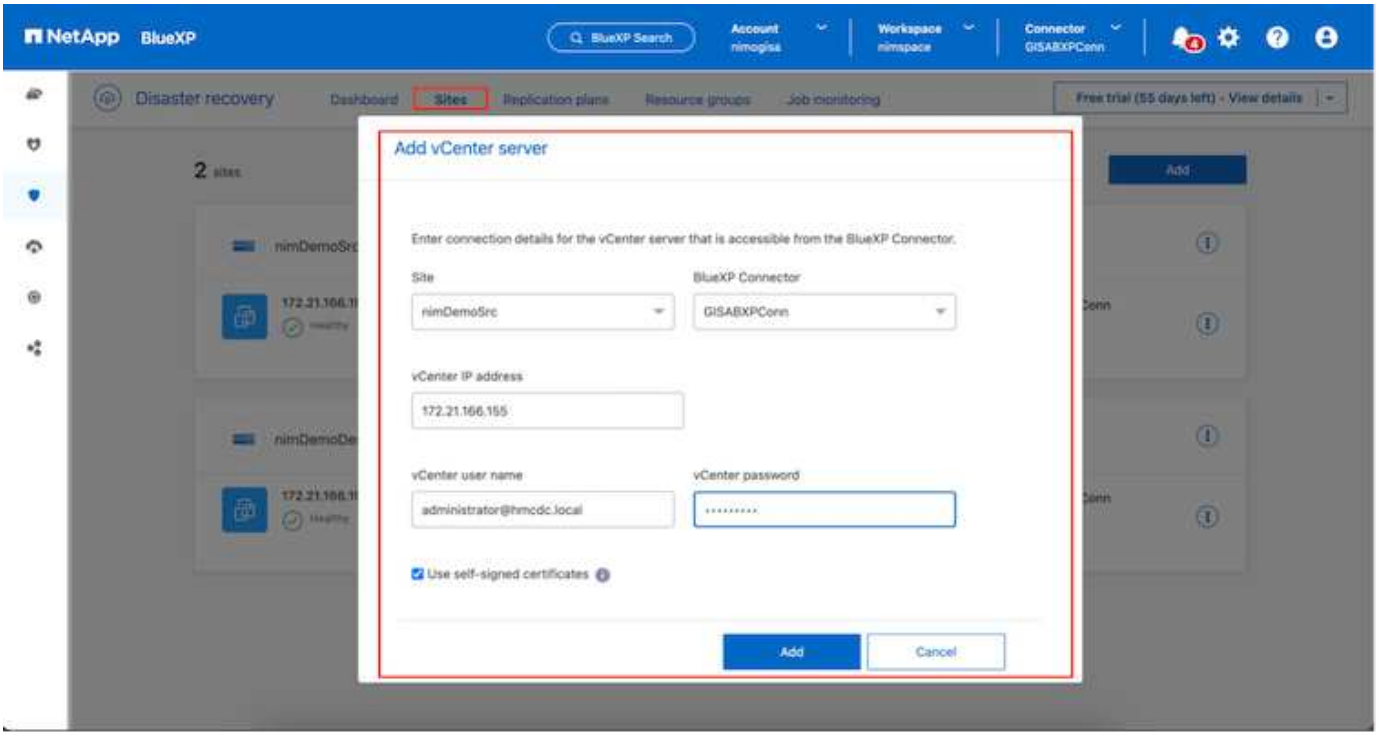
Der erste Schritt bei der Vorbereitung auf Disaster Recovery besteht darin, die lokalen Ressourcen für vCenter und Storage zu identifizieren und zu Disaster Recovery hinzuzufügen.

Voraussetzung ist, dass die ONTAP Storage-Systeme in der Arbeitsumgebung innerhalb des Canvas hinzugefügt wurden. In Console erfolgt in der linken Navigation die Auswahl von **Protection > Disaster Recovery**. Anschließend steht **Discover vCenter servers** zur Auswahl, alternativ über das obere Menü **Sites > Add > Add vCenter**.

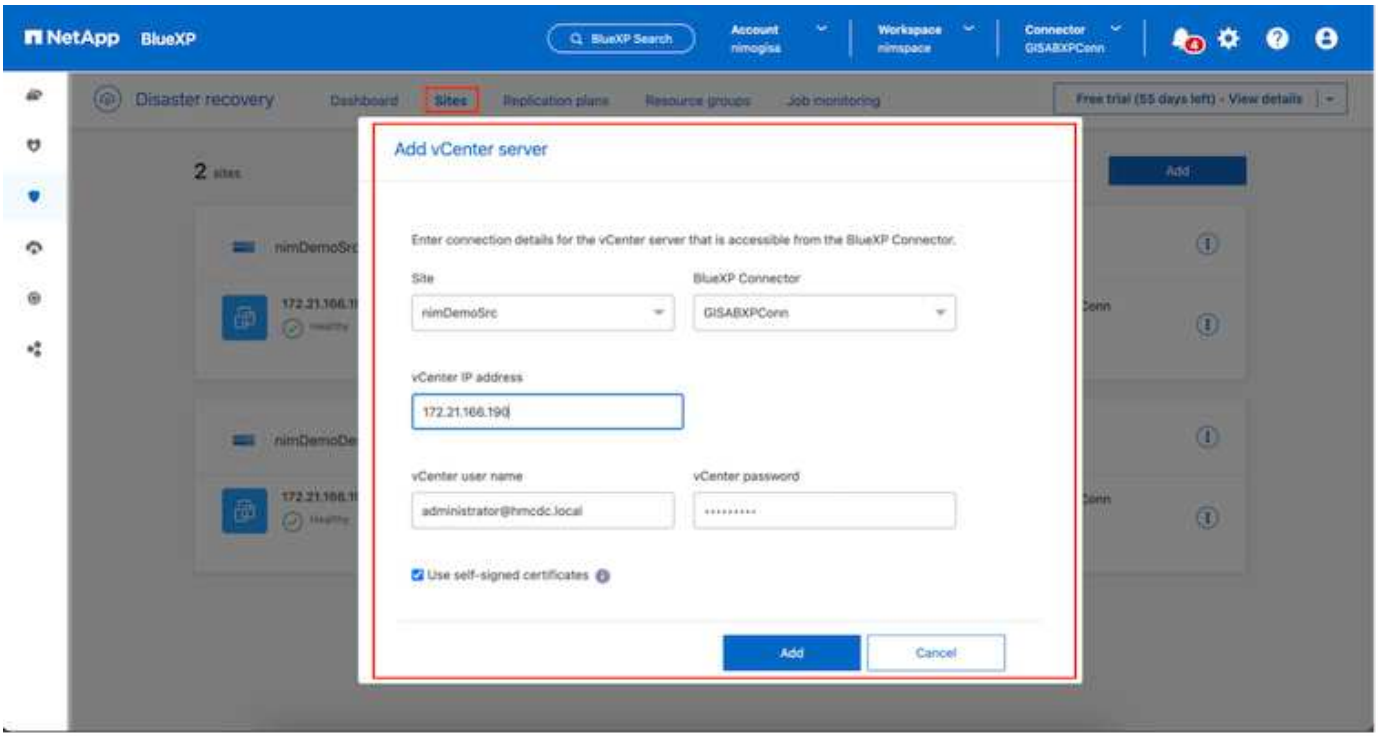


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle**. Lokales vCenter.



- **Ziel**. VMC SDDC vCenter.



Sobald die vCenter hinzugefügt wurden, wird die automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen Quell- und Zielstandort

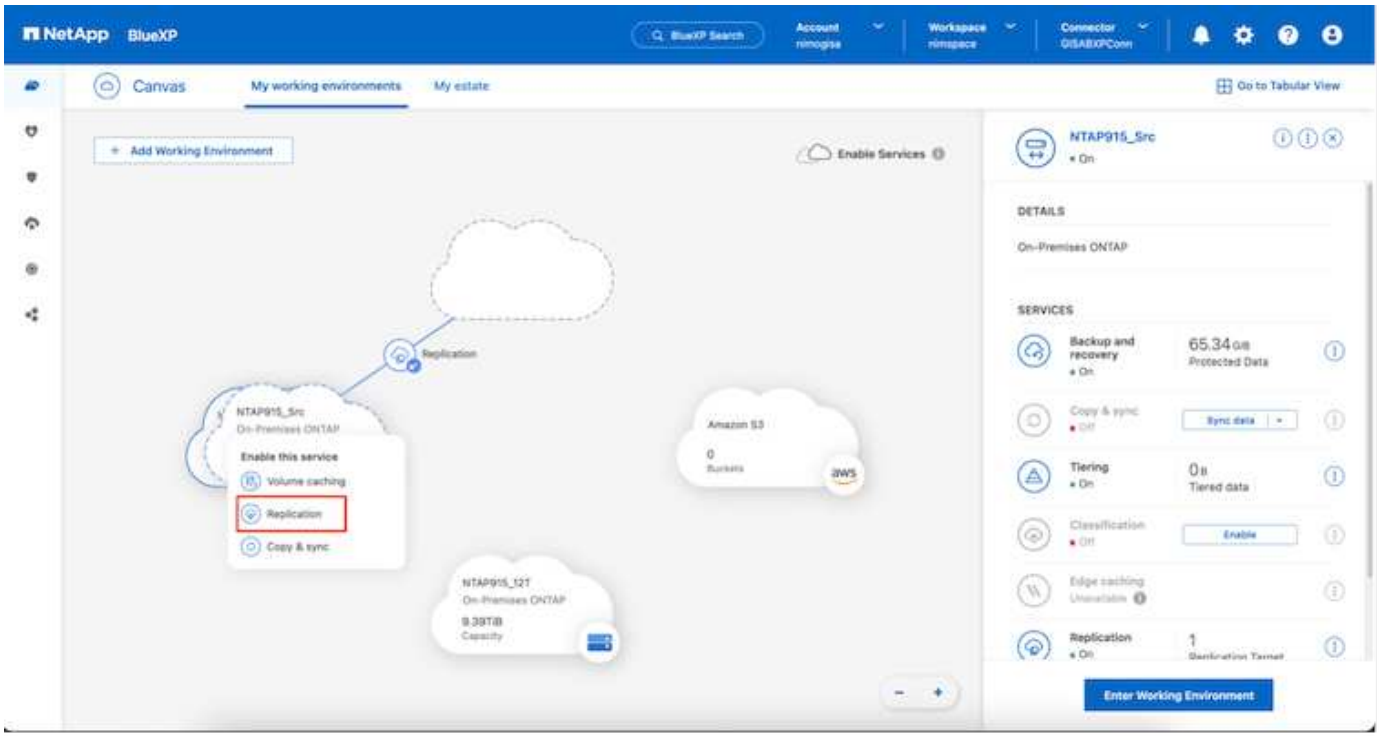
SnapMirror nutzt ONTAP -Snapshots, um die Datenübertragung von einem Ort zum anderen zu verwalten. Zunächst wird eine vollständige Kopie basierend auf einem Snapshot des Quellvolumes auf das Ziel kopiert, um eine Basissynchronisierung durchzuführen. Wenn an der Quelle Datenänderungen auftreten, wird ein neuer Snapshot erstellt und mit dem Basis-Snapshot verglichen. Die Blöcke, bei denen Änderungen festgestellt wurden, werden dann zum Ziel repliziert, wobei der neuere Snapshot zur aktuellen Basislinie oder zum neuesten gemeinsamen Snapshot wird. Dadurch kann der Vorgang wiederholt und inkrementelle Updates an das Ziel gesendet werden.

Wenn eine SnapMirror -Beziehung hergestellt wurde, befindet sich das Zielvolume in einem schreibgeschützten Online-Zustand und ist daher weiterhin zugänglich. SnapMirror arbeitet mit physischen Speicherblöcken und nicht auf Datei- oder anderer logischer Ebene. Dies bedeutet, dass das Zielvolume eine identische Replik des Quellvolumes ist, einschließlich Snapshots, Volumeeinstellungen usw. Wenn ONTAP Speicherplatzeffizienzfunktionen wie Datenkomprimierung und Datendeduplizierung vom Quellvolume verwendet werden, behält das replizierte Volume diese Optimierungen bei.

Durch das Aufheben der SnapMirror Beziehung wird das Zielvolume beschreibbar und wird normalerweise zum Durchführen eines Failovers verwendet, wenn SnapMirror zum Synchronisieren von Daten mit einer DR-Umgebung verwendet wird. SnapMirror ist so ausgereift, dass die am Failover-Standort geänderten Daten effizient mit dem primären System resynchronisiert werden können, falls dieses später wieder online geht. Anschließend kann die ursprüngliche SnapMirror Beziehung wiederhergestellt werden.

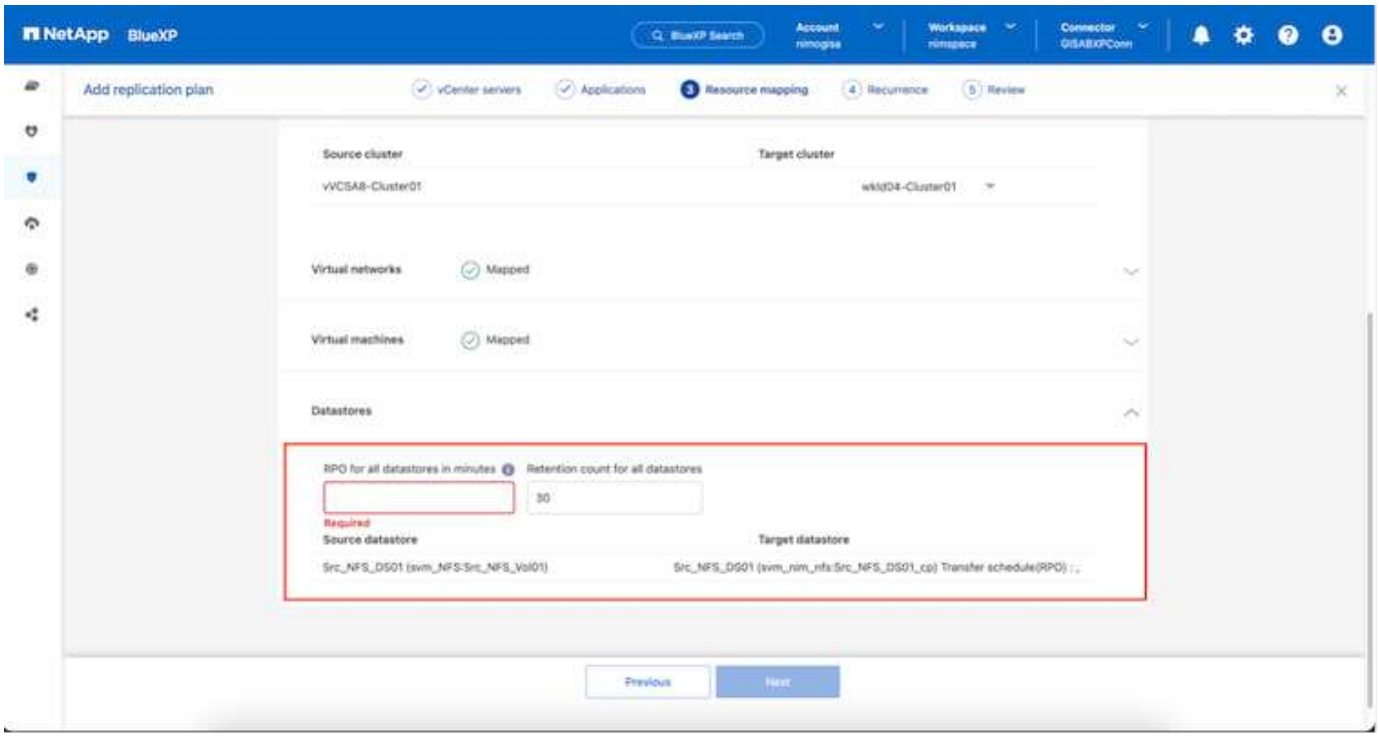
So richten Sie es für VMware Disaster Recovery ein

Der Prozess zur Erstellung der SnapMirror Replikation bleibt für jede beliebige Applikation gleich. Der Prozess kann manuell oder automatisiert sein. Am einfachsten lässt sich die SnapMirror Replikation mit Console konfigurieren, indem das Quell-ONTAP-System in der Umgebung per Drag & Drop auf das Ziel gezogen wird, um den Assistenten zu starten, der durch den restlichen Prozess führt.



NetApp Data Services kann denselben Vorgang auch automatisieren, sofern die folgenden beiden Kriterien erfüllt sind:

- Quell- und Zielcluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.

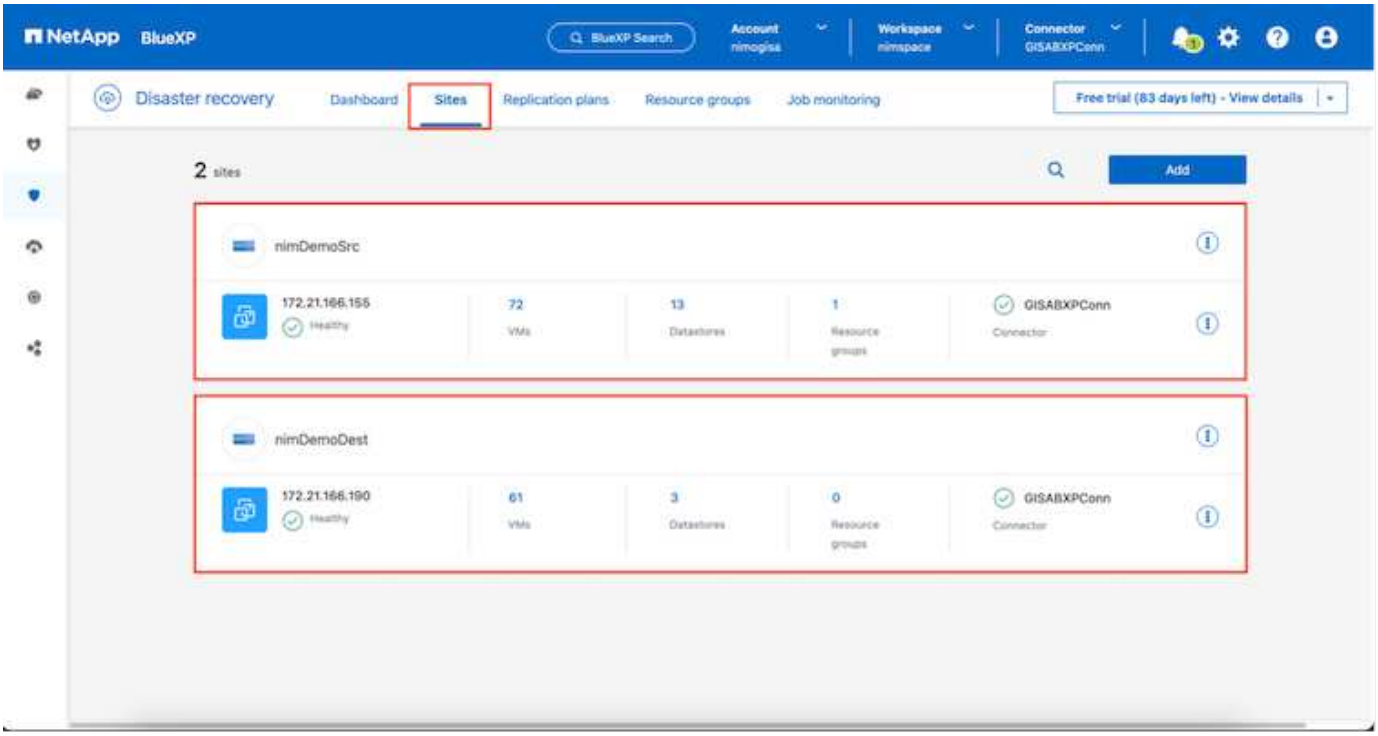


Wenn die SnapMirror Beziehung für das Volume bereits über die CLI konfiguriert ist, erkennt Console die Beziehung und fährt mit den übrigen Workflow-Operationen fort.

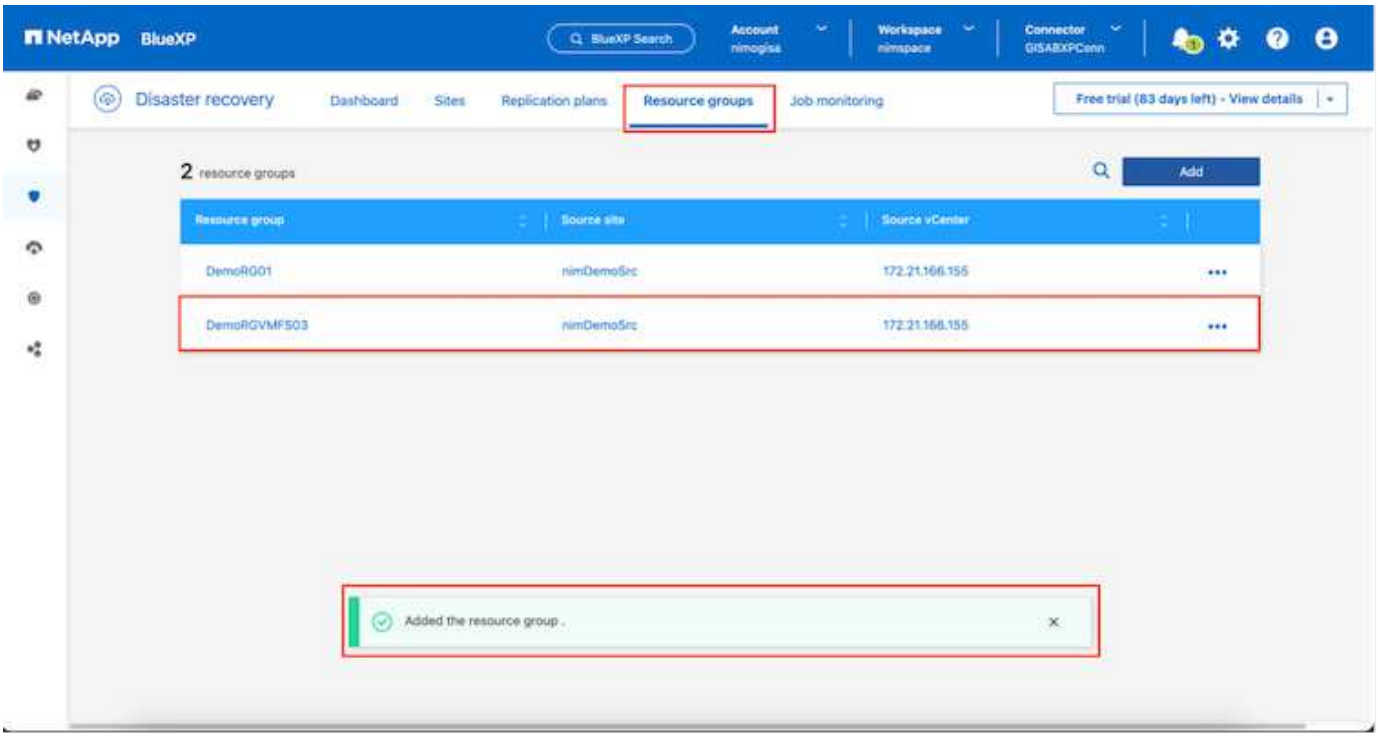
Neben den oben genannten Ansätzen kann die SnapMirror Replikation auch über ONTAP CLI oder System Manager erstellt werden. Unabhängig vom Ansatz zur Synchronisierung der Daten mit SnapMirror orchestriert Disaster Recovery den Workflow für nahtlose und effiziente Disaster-Recovery-Abläufe.

Was kann Disaster Recovery für Sie tun?

Nach dem Hinzufügen der Quell- und Zielstandorte führt Disaster Recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Disaster Recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und trägt diese ein.

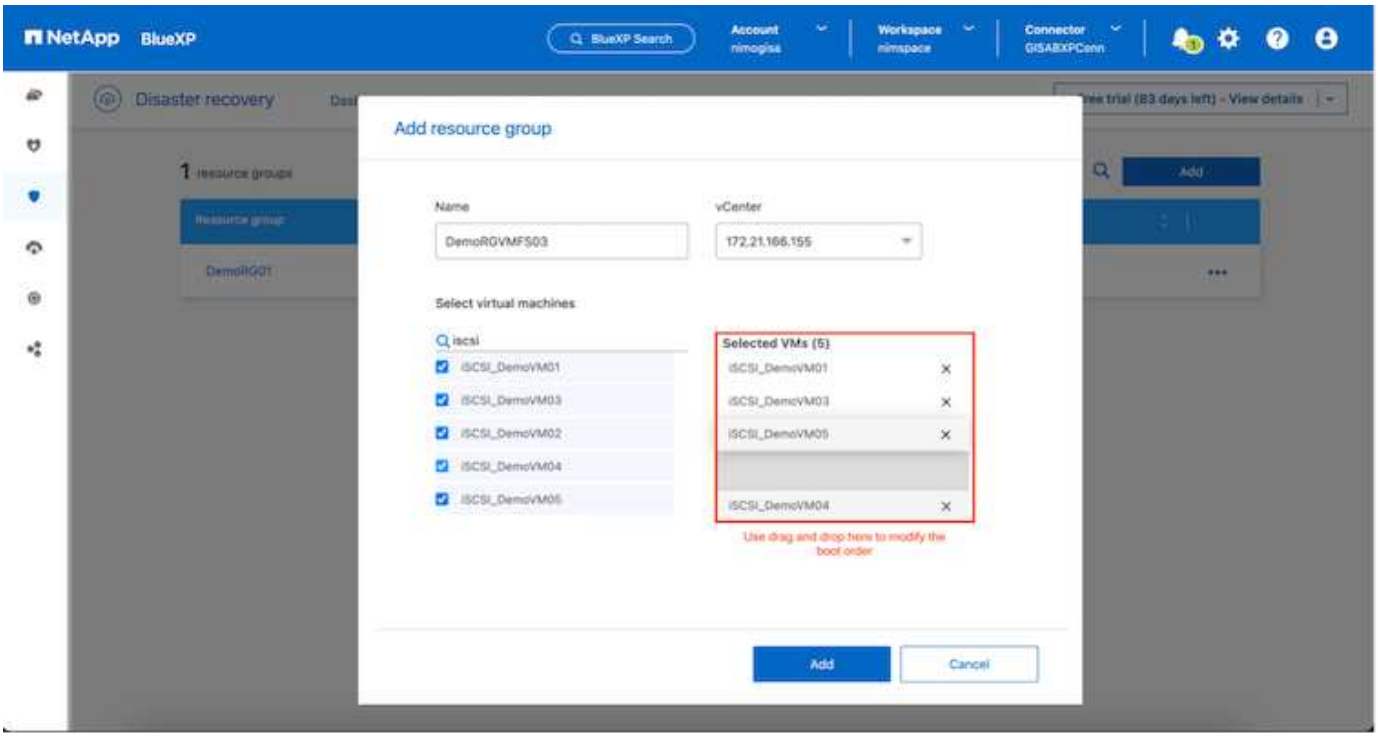


Nachdem die Standorte hinzugefügt wurden, können VMs in Ressourcengruppen zusammengefasst werden. Disaster Recovery Ressourcengruppen ermöglichen die Gruppierung abhängiger VMs in logische Gruppen, die deren Startreihenfolgen und Startverzögerungen enthalten und bei der Wiederherstellung ausgeführt werden können. Die Erstellung von Ressourcengruppen beginnt unter **Resource Groups** mit einem Klick auf **Create New Resource Group**.



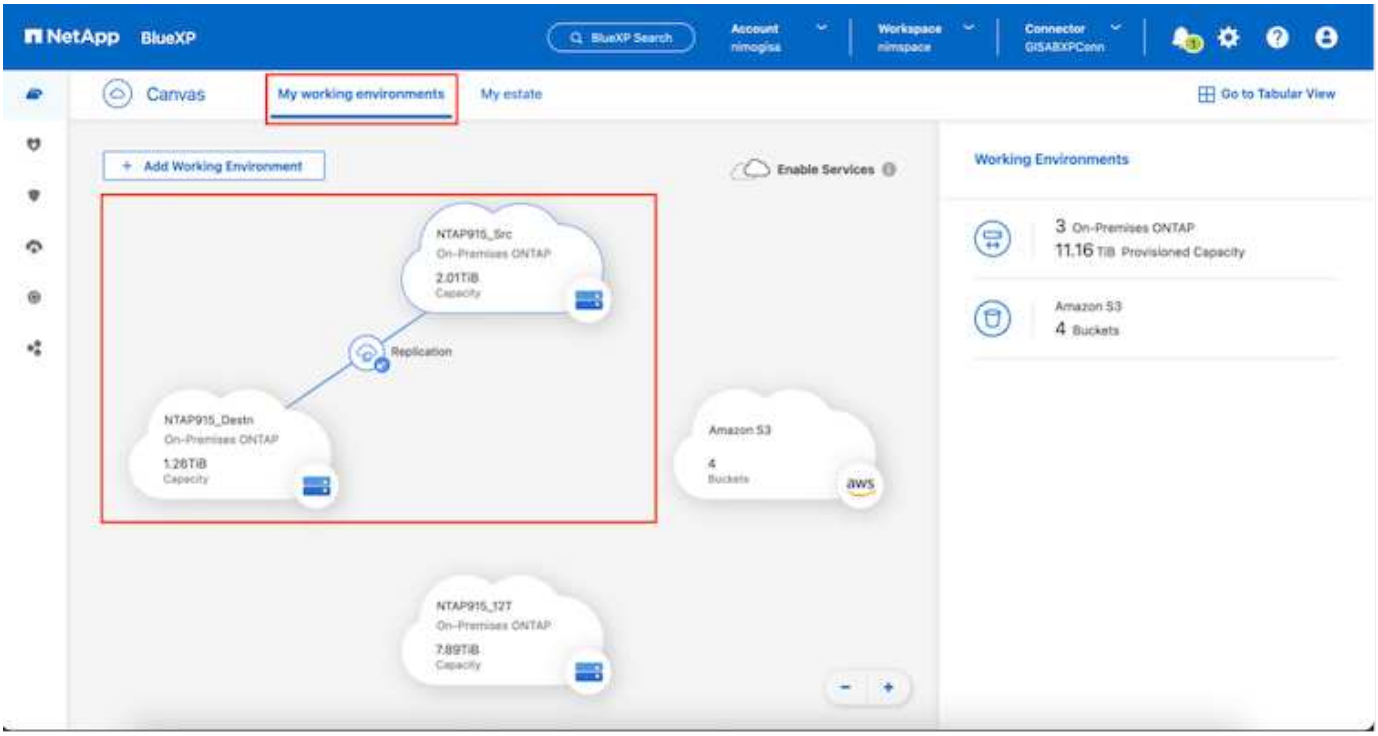
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

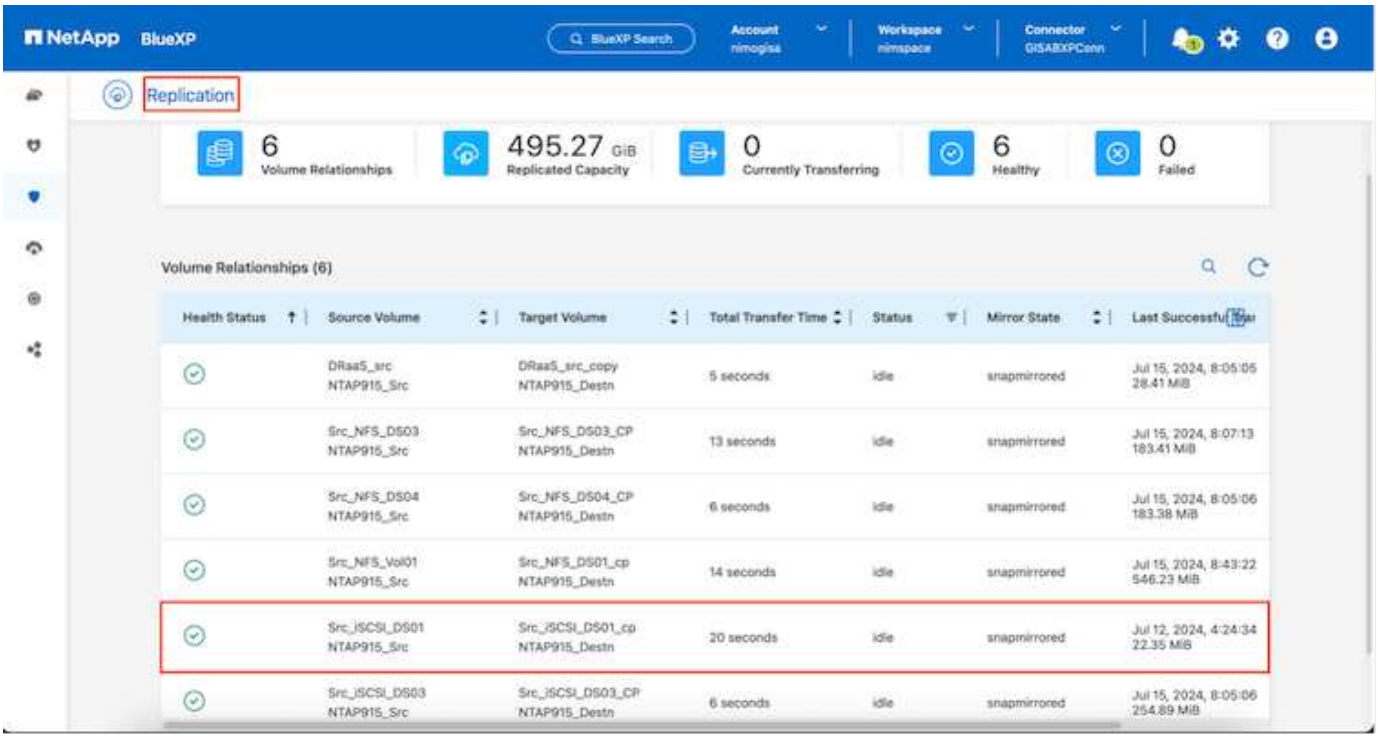
Die Startreihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen Drag-and-Drop-Mechanismus definiert oder geändert werden.



Sobald die Ressourcengruppen erstellt sind, besteht der nächste Schritt darin, den Ausführungsentwurf oder einen Plan zur Wiederherstellung virtueller Maschinen und Anwendungen im Katastrophenfall zu erstellen. Wie in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie mithilfe des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des

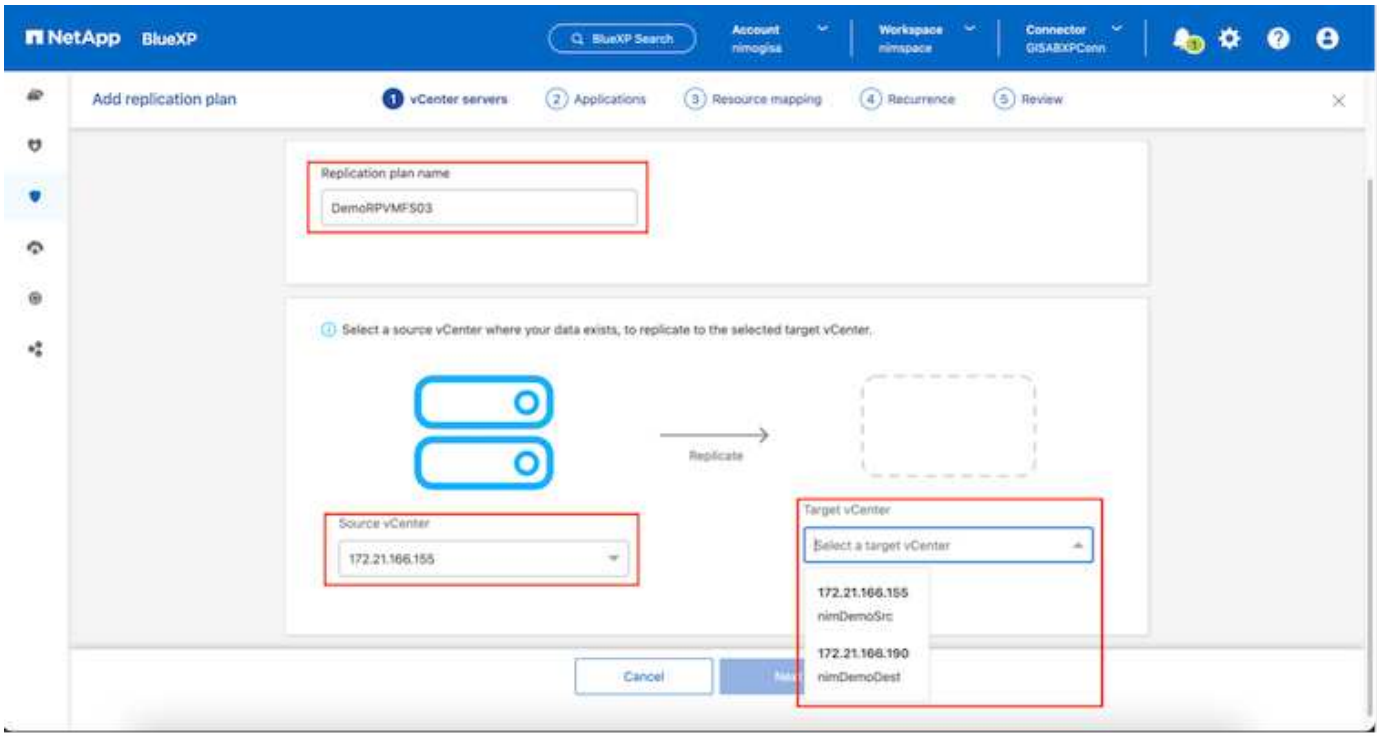
Replikationsplans angegeben wurden.



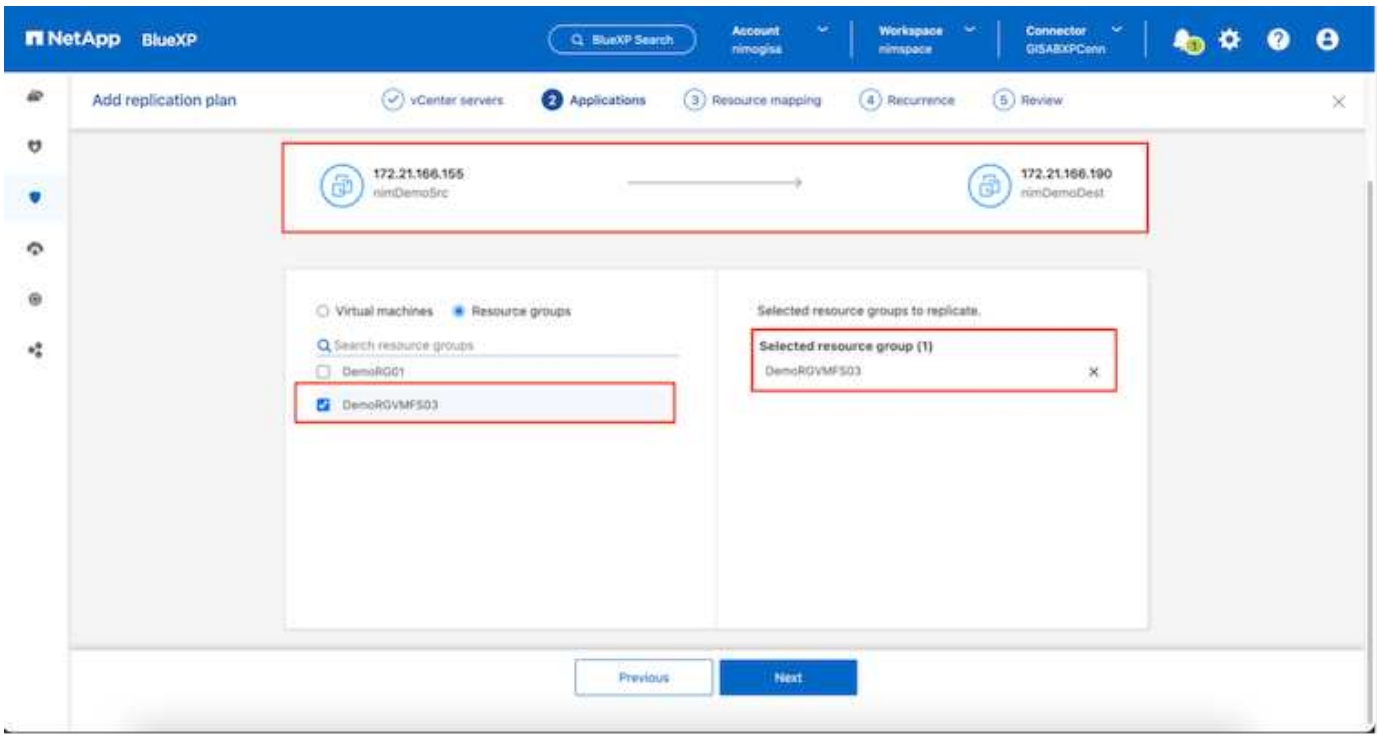


Konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und der Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

Wählen Sie zuerst das Quell-vCenter und dann das Ziel-vCenter aus.



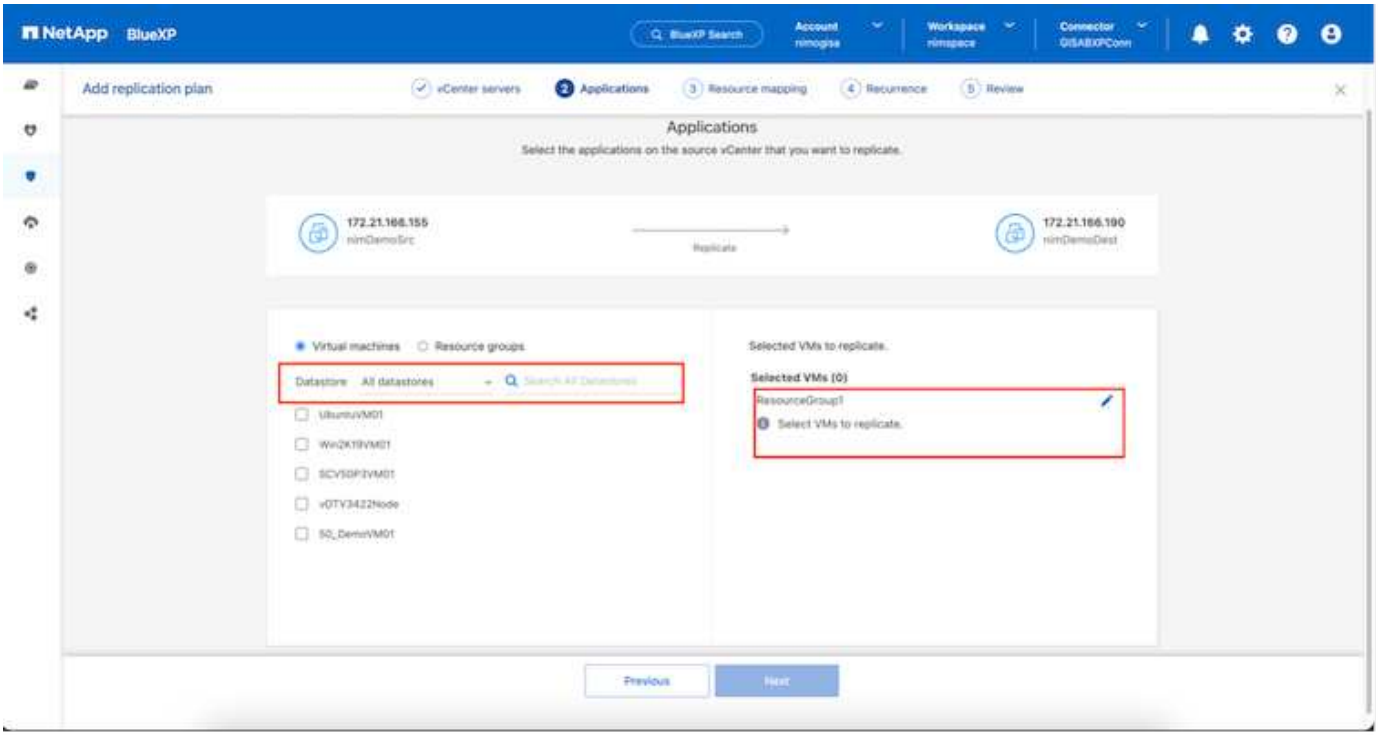
Der nächste Schritt besteht darin, vorhandene Ressourcengruppen auszuwählen. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent dabei, die erforderlichen virtuellen Maschinen basierend auf den Wiederherstellungszielen zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Vorgangsreihenfolge für die Wiederherstellung virtueller Anwendungsmaschinen zu definieren.



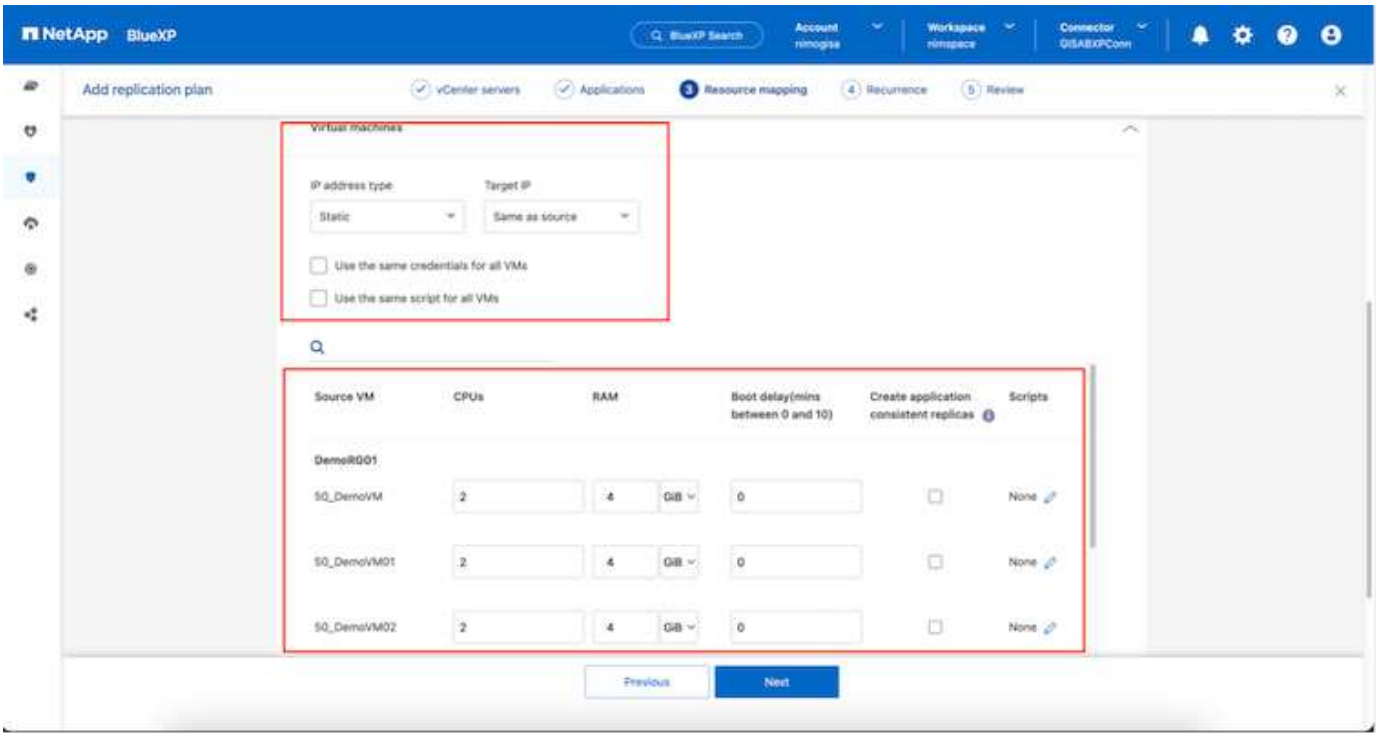
Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.

Jede virtuelle Maschine innerhalb einer Ressourcengruppe wird der Reihe nach basierend auf der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

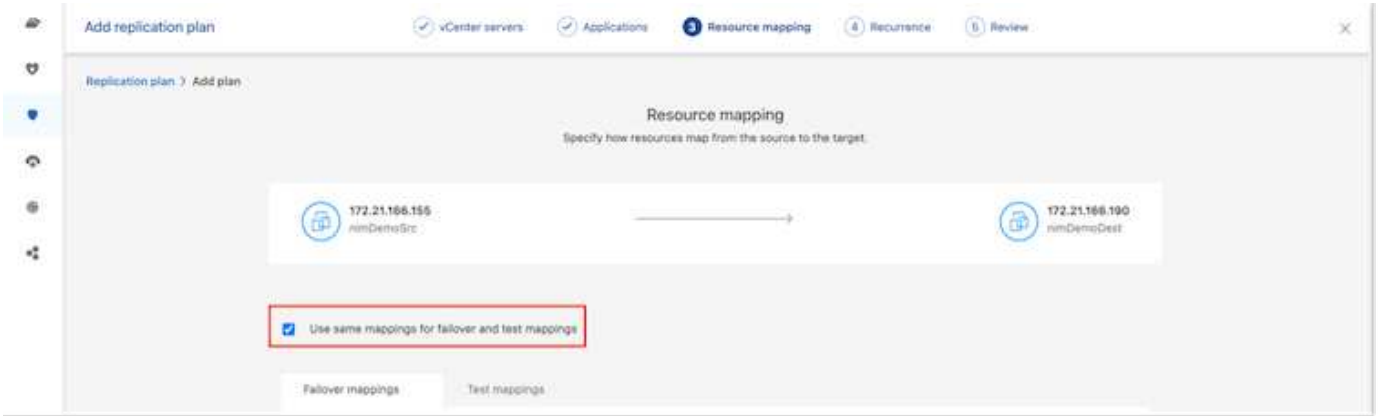
Der folgende Screenshot zeigt die Option zum Filtern virtueller Maschinen oder bestimmter Datenspeicher basierend auf organisatorischen Anforderungen, wenn nicht zuvor Ressourcengruppen erstellt wurden.



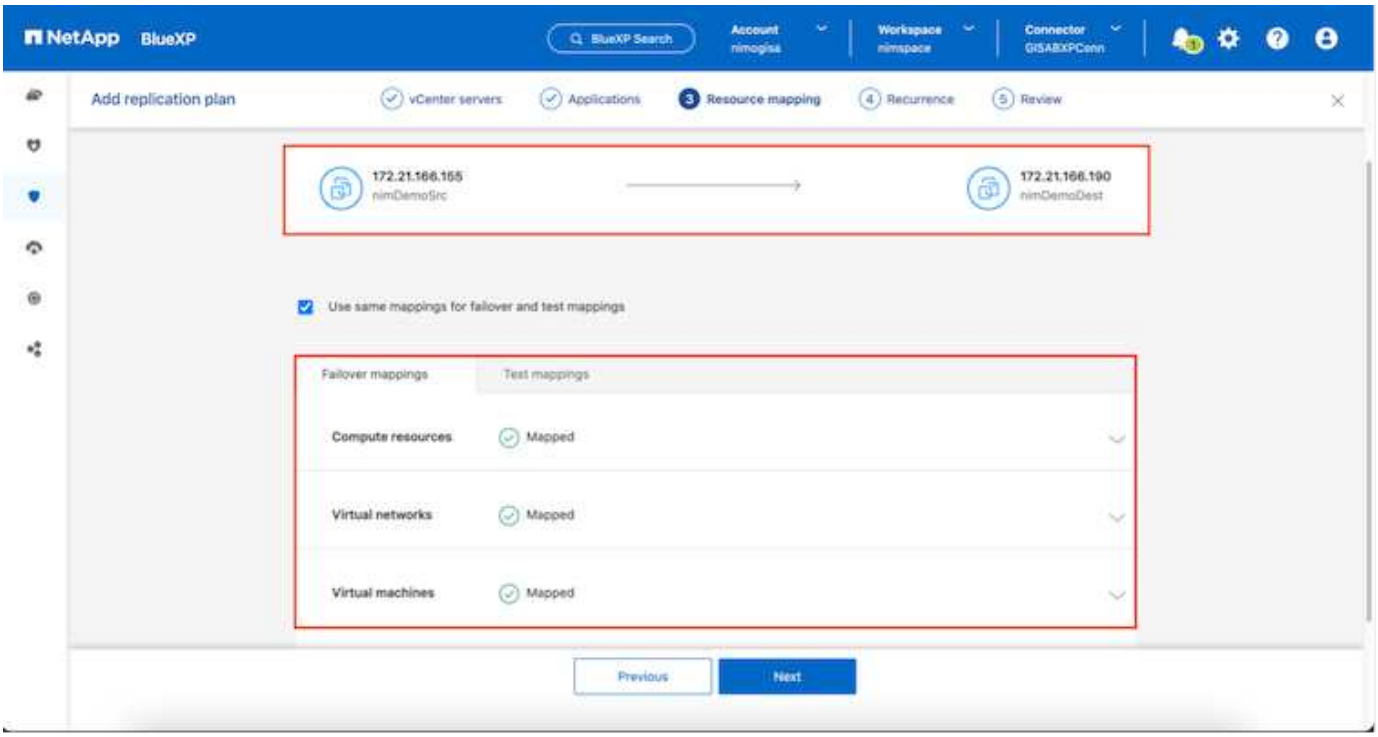
Nach der Auswahl der Ressourcengruppen folgt die Erstellung der Failover-Zuordnungen. In diesem Schritt wird festgelegt, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen und virtuelle Netzwerke. Auch IP-Anpassungen, Vor- und Nachskripte, Startverzögerungen, Applikationskonsistenz usw. sind darin enthalten. Ausführliche Informationen enthält "Erstellen eines Replikationsplans".



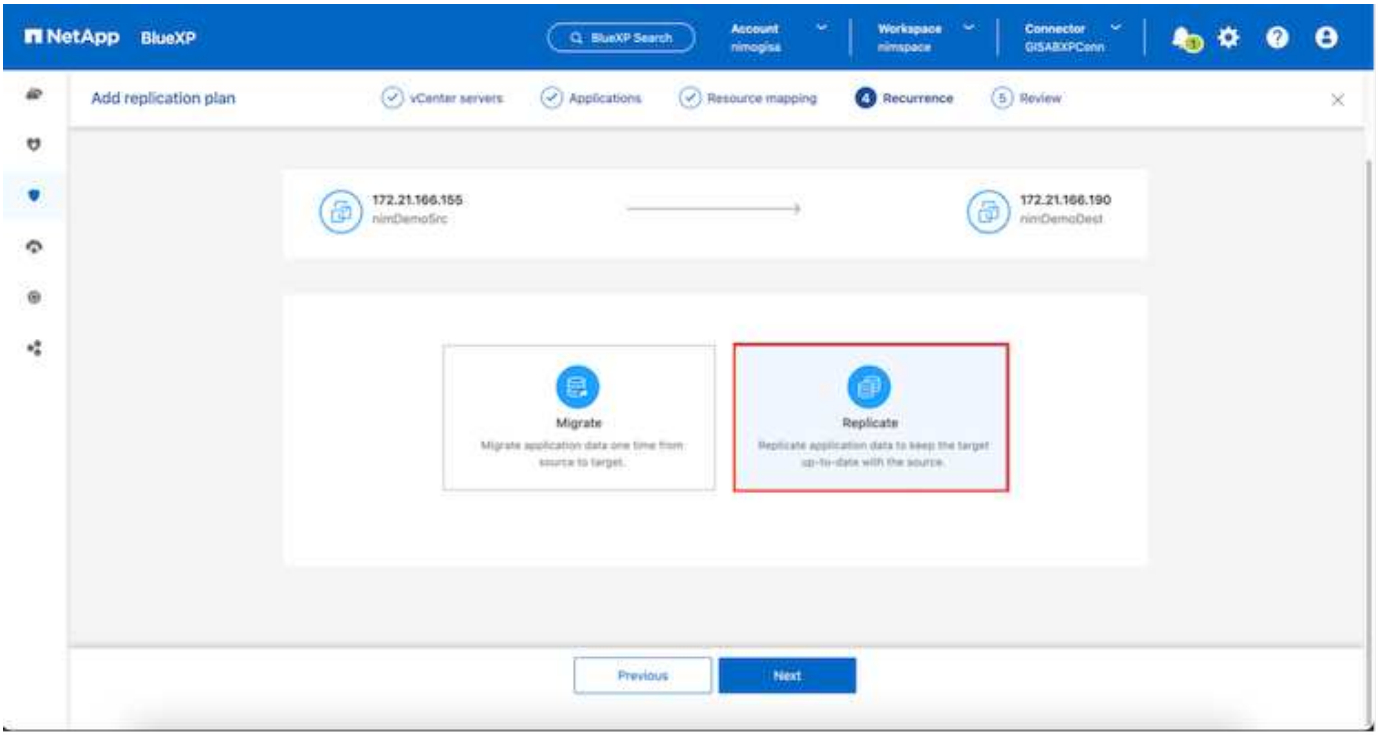
Standardmäßig werden für Test- und Failovervorgänge dieselben Zuordnungsparameter verwendet. Um verschiedene Zuordnungen für die Testumgebung anzuwenden, wählen Sie die Option „Testzuordnung“ aus, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:



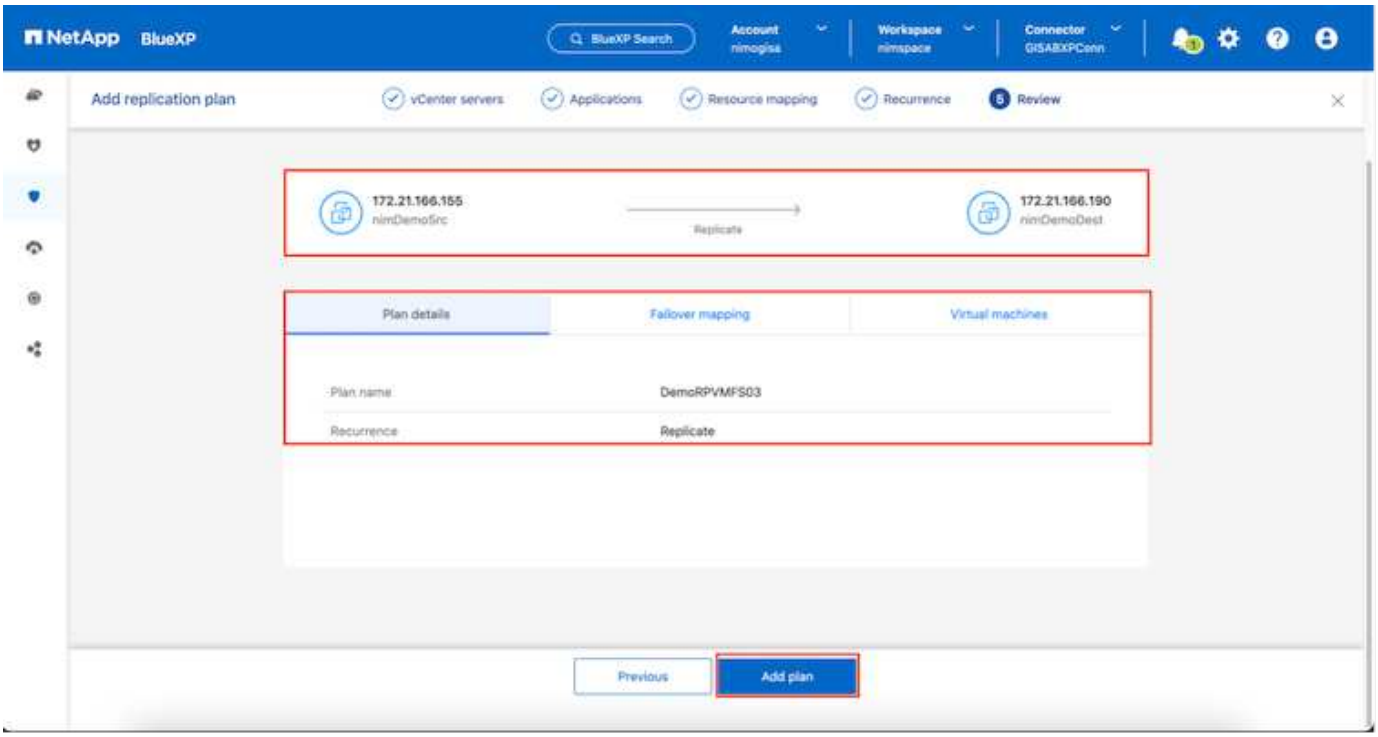
Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.

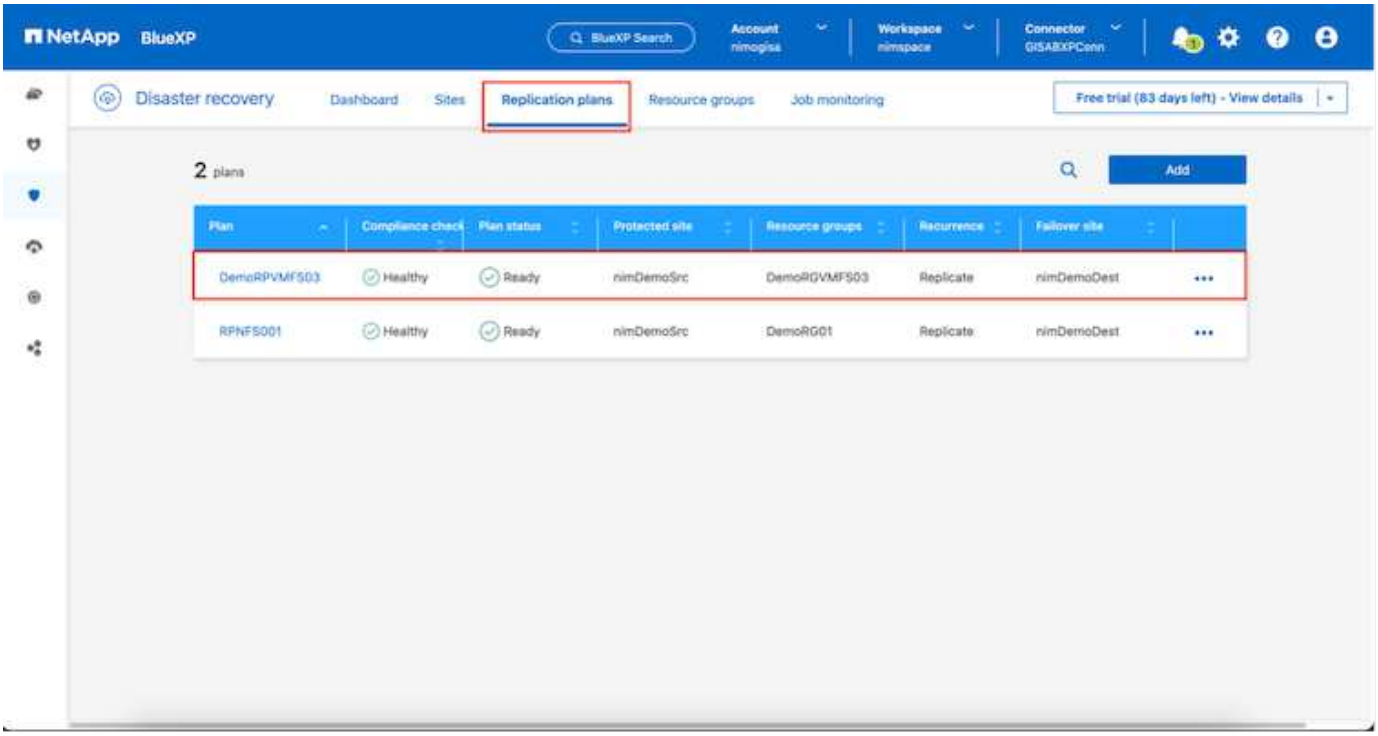


Wählen Sie den Wiederholungstyp aus. Einfach ausgedrückt: Wählen Sie „Migrieren“ (einmalige Migration mit Failover) oder die Option „Wiederkehrende kontinuierliche Replikation“. In dieser exemplarischen Vorgehensweise ist die Option „Replizieren“ ausgewählt.

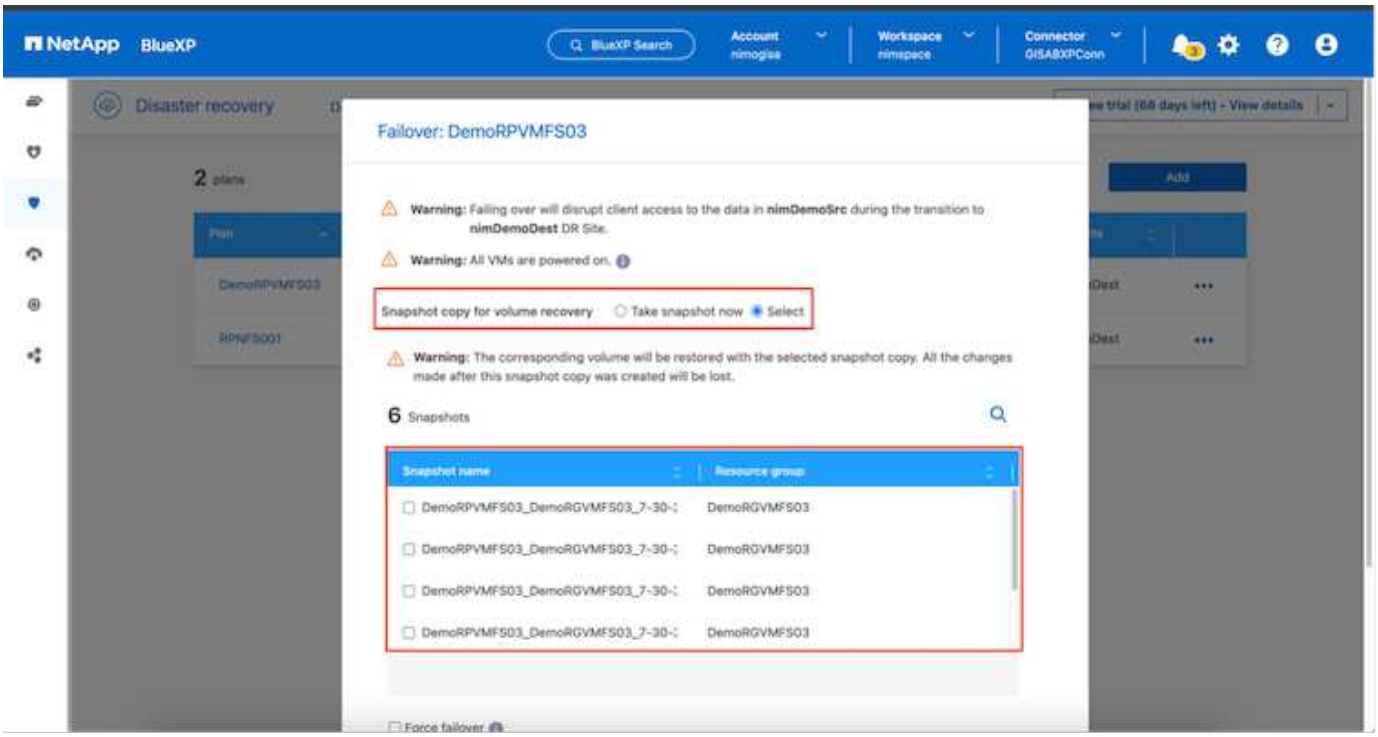


Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf „Plan hinzufügen“.

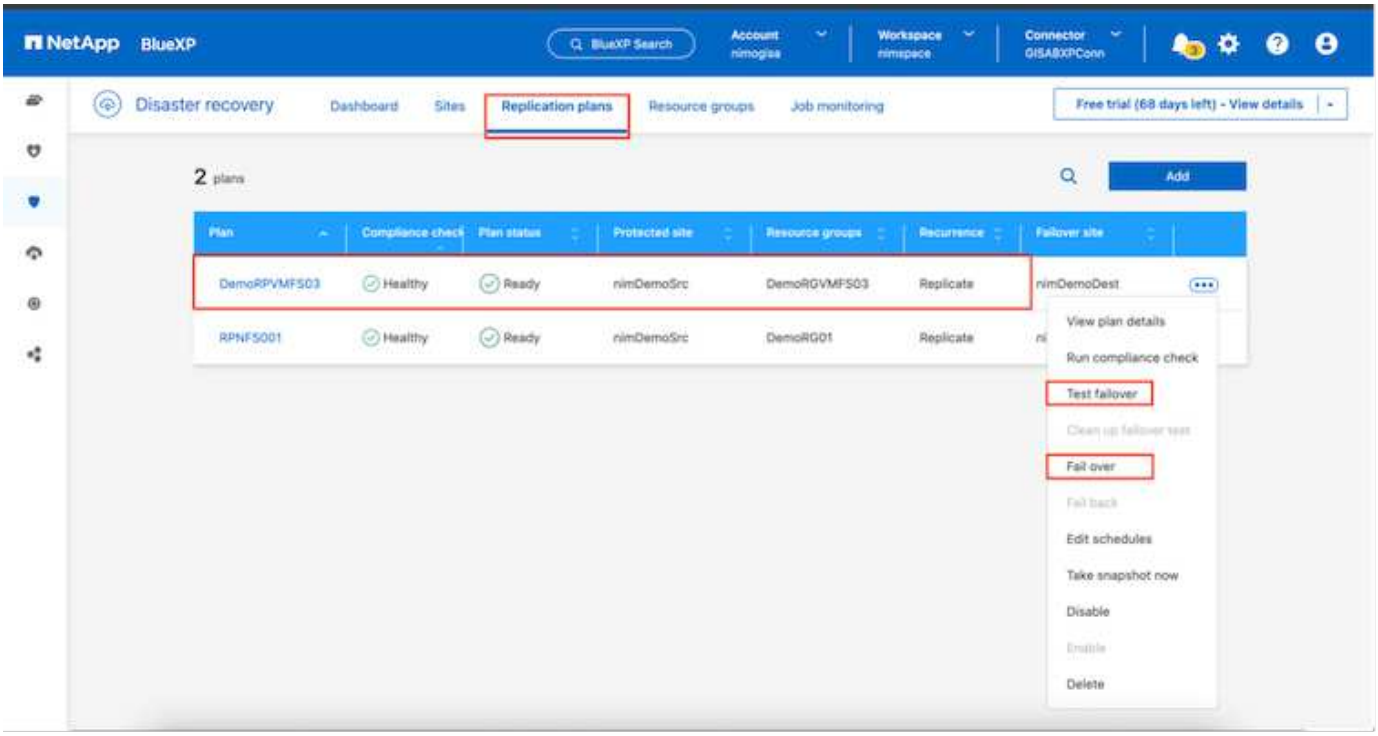




Sobald der Replikationsplan erstellt wurde, kann je nach Anforderungen ein Failover durchgeführt werden, indem die Option für Failover, Test-Failover oder Migration ausgewählt wird. Disaster Recovery stellt sicher, dass der Replikationsprozess alle 30 Minuten gemäß dem Plan ausgeführt wird. Bei den Optionen Failover und Test-Failover können Sie die neueste SnapMirror Snapshot Kopie verwenden, oder Sie können eine bestimmte Snapshot Kopie aus einer zeitpunktgenauen Snapshot Kopie auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die zeitpunktgenaue Option kann bei einem Beschädigungsereignis wie Ransomware sehr hilfreich sein, wenn die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. Disaster Recovery zeigt alle verfügbaren Wiederherstellungspunkte an.



Um ein Failover oder ein Test-Failover mit der im Replikationsplan angegebenen Konfiguration auszulösen, klicken Sie auf **Failover** oder **Test-Failover**.

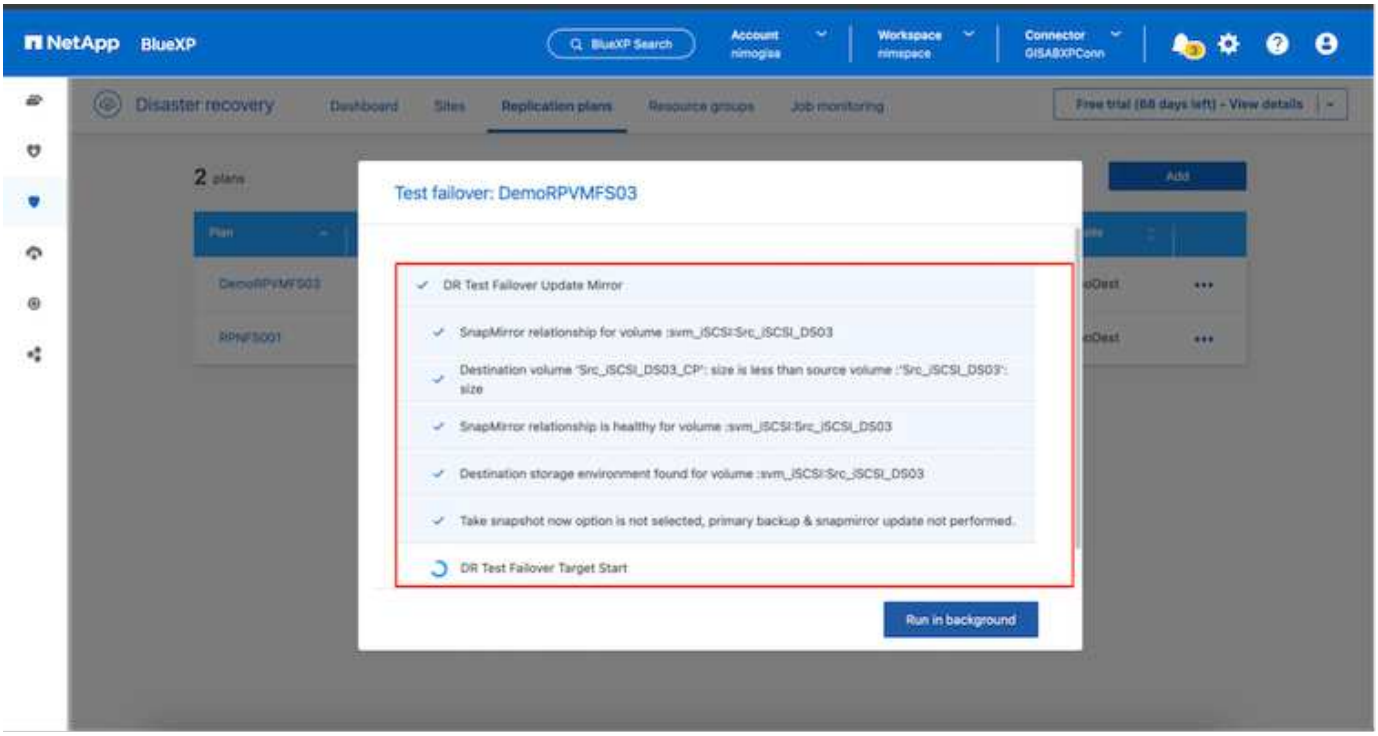


Was passiert während eines Failovers oder Test-Failover-Vorgangs?

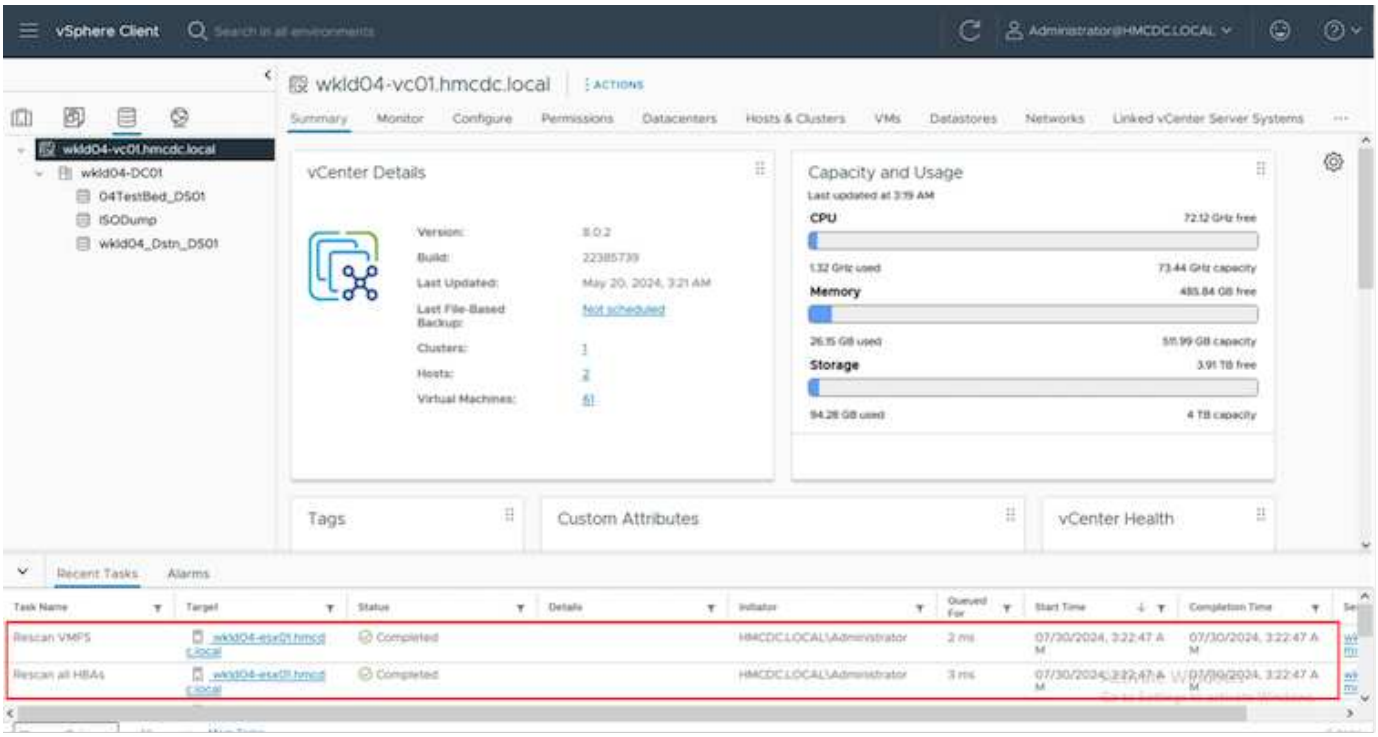
Während eines Test-Failover-Vorgangs erstellt Disaster Recovery ein FlexClone Volume auf dem ONTAP Storage-System am Ziel unter Verwendung der neuesten Snapshot-Kopie oder eines ausgewählten Snapshots des Ziel-Volumes.

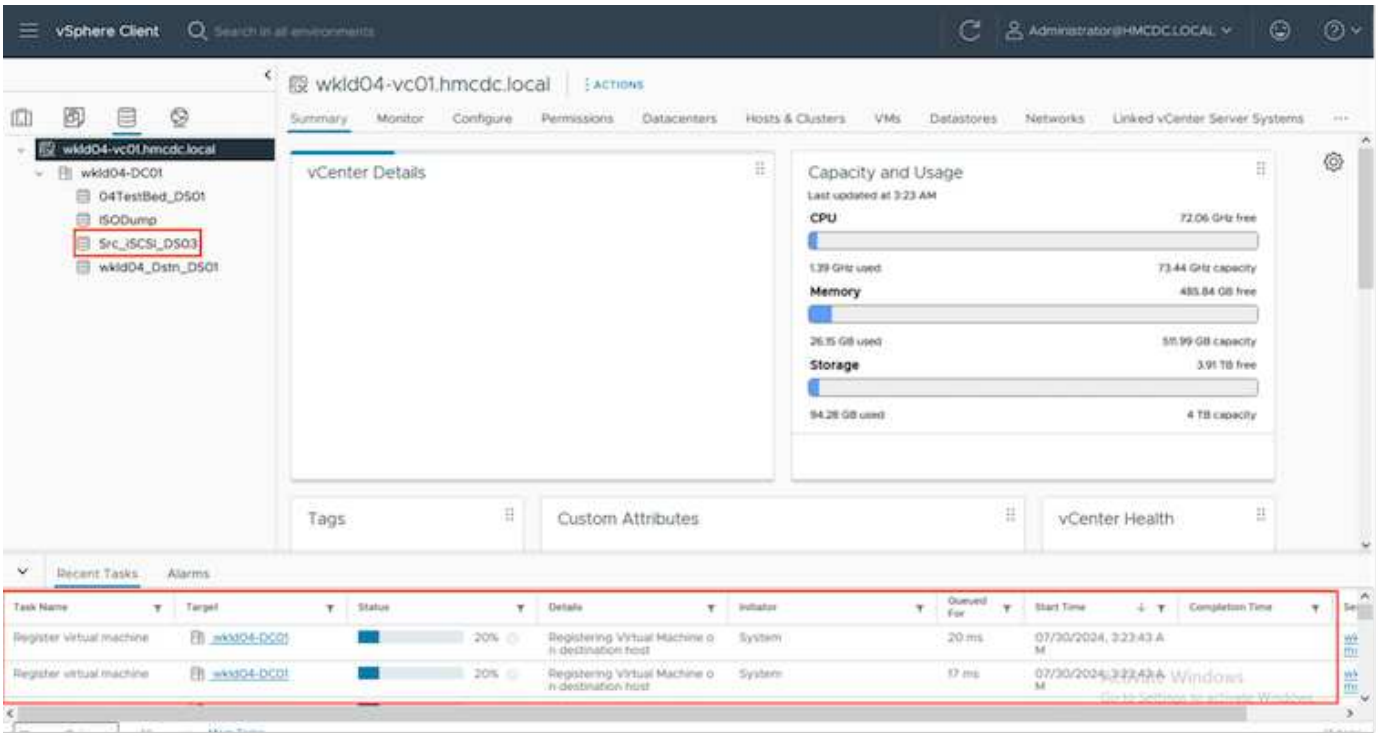
Ein Test-Failover-Vorgang erstellt ein geklontes Volume auf dem Ziel ONTAP -Speichersystem.

Das Ausführen eines Testwiederherstellungsvorgangs hat keine Auswirkungen auf die SnapMirror Replikation.



Während des Prozesses ordnet Disaster Recovery das ursprüngliche Ziel-Volume nicht zu. Stattdessen erstellt Disaster Recovery aus dem ausgewählten Snapshot ein neues FlexClone Volume, und ein temporärer Datenspeicher, der das FlexClone Volume unterstützt, wird den ESXi Hosts zugeordnet.

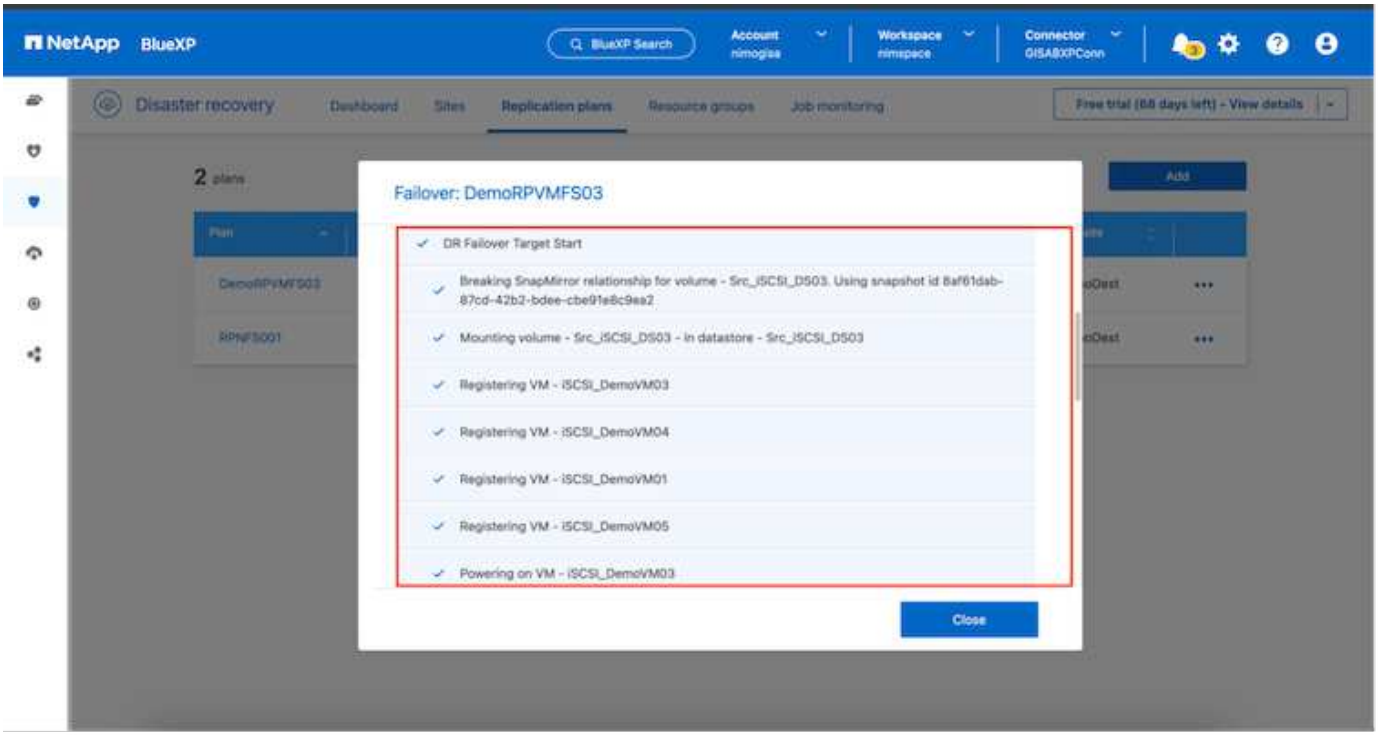




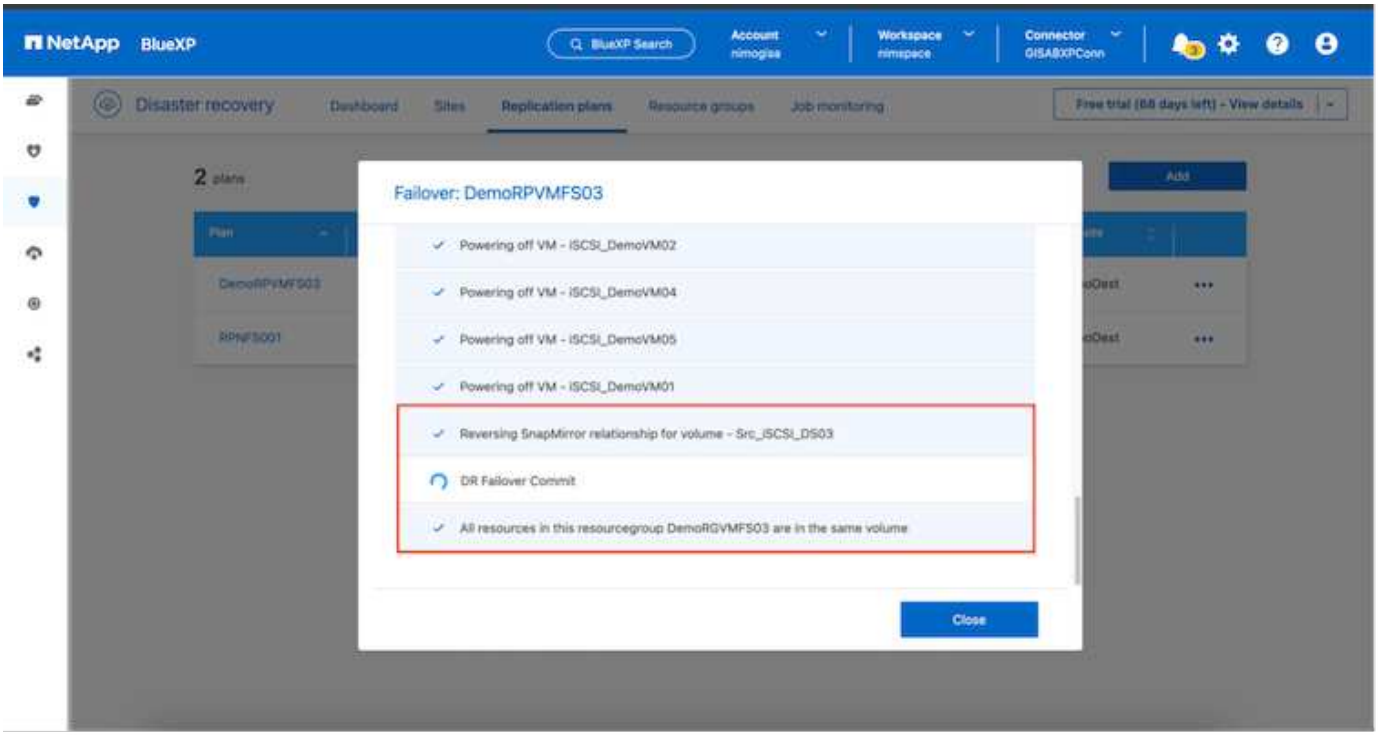
Wenn der Test-Failover-Vorgang abgeschlossen ist, kann die Bereinigungsoperation mit **"Clean Up failover test"** ausgelöst werden. Während dieses Vorgangs löscht Disaster Recovery das FlexClone Volume, das im Vorgang verwendet wurde.

Im Falle eines tatsächlichen Katastrophenereignisses führt Disaster Recovery die folgenden Schritte durch:

1. Bricht die SnapMirror -Beziehung zwischen den Sites ab.
2. Mountet das VMFS-Datenspeichervolume nach der Neusignierung zur sofortigen Verwendung.
3. Registrieren der VMs
4. VMs einschalten

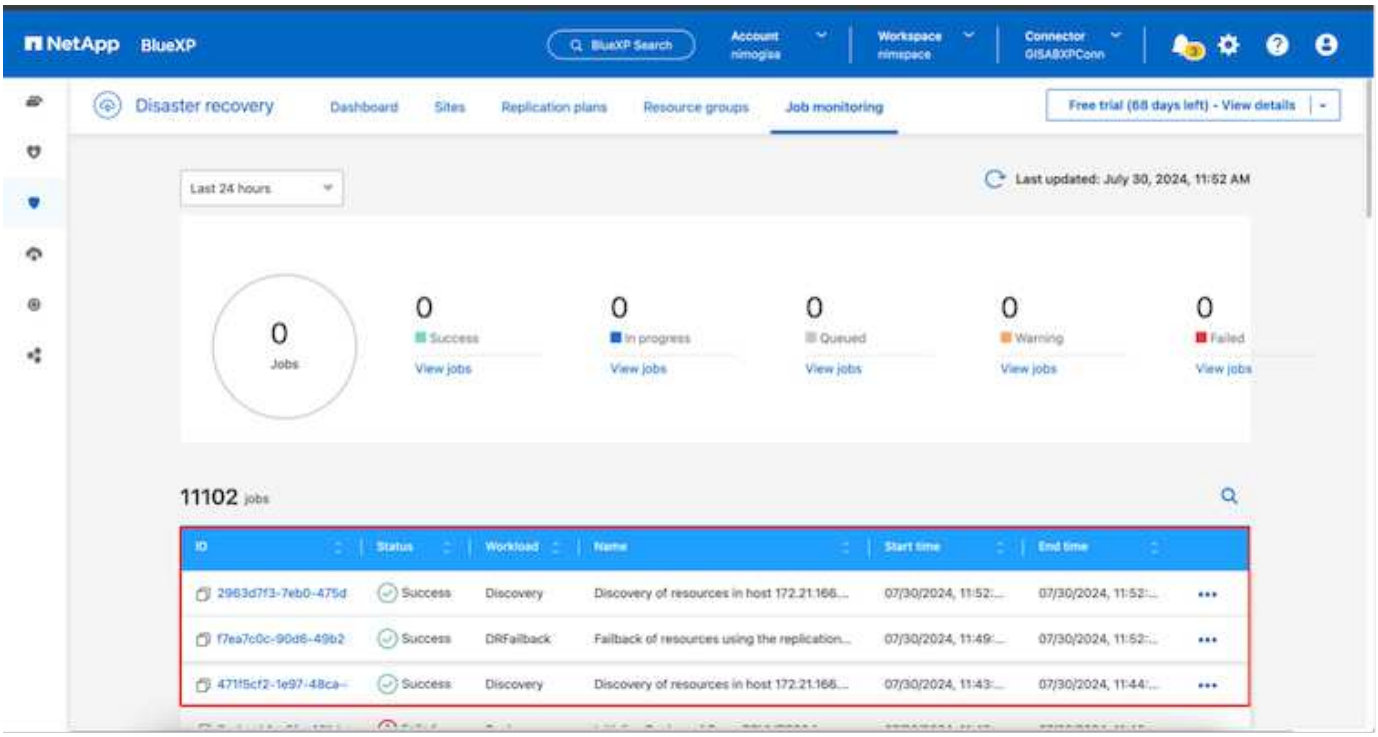


Sobald der primäre Standort betriebsbereit ist, ermöglicht Disaster Recovery die umgekehrte Resynchronisierung für SnapMirror und das Failback, was wiederum mit einem Klick auf eine Schaltfläche durchgeführt werden kann.



Und wenn die Migrationsoption gewählt wird, wird dies als geplantes Failover-Ereignis betrachtet. In diesem Fall wird ein zusätzlicher Schritt ausgelöst, der darin besteht, die virtuellen Maschinen am Quellstandort herunterzufahren. Die restlichen Schritte bleiben dieselben wie beim Failover-Ereignis.

Über Console oder die ONTAP CLI können Sie den Systemstatus der entsprechenden Datastore-Volumes überwachen, und der Status eines Failover oder Test-Failover lässt sich über Job Monitoring verfolgen.



Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten und individuellen Notfallwiederherstellungsplans. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Um mehr über diesen Prozess zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen oder die"Lösungssimulator" .

NetApp Hybrid Multicloud mit Red Hat OpenShift Container-Workloads

Erste Schritte

NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads

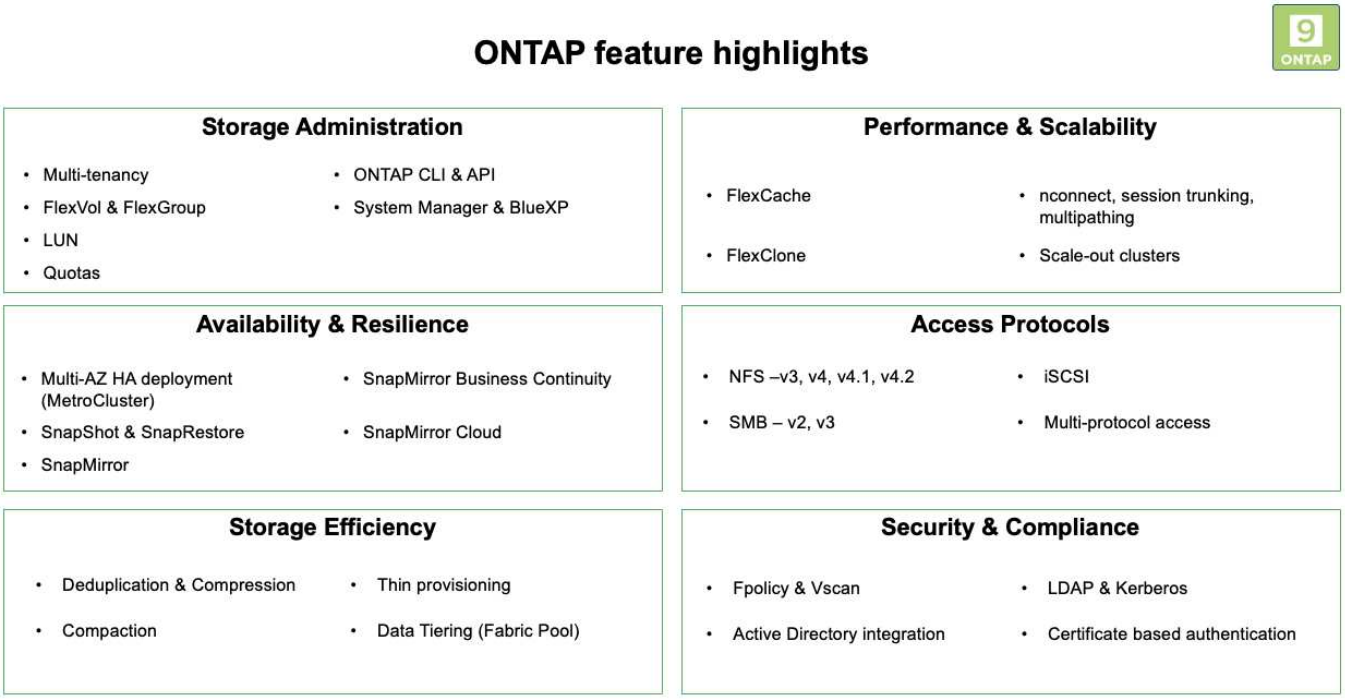
NetApp verzeichnet einen deutlichen Anstieg der Zahl der Kunden, die ihre alten Unternehmensanwendungen modernisieren und mithilfe von Containern und Orchestrierungsplattformen, die auf Kubernetes basieren, neue Anwendungen erstellen. Die Red Hat OpenShift Container Platform ist ein Beispiel, das unserer Erfahrung nach von vielen unserer Kunden übernommen wird.

Überblick

Da immer mehr Kunden Container in ihren Unternehmen einsetzen, ist NetApp optimal aufgestellt, um die persistenten Speicheranforderungen ihrer Stateful-Anwendungen und die klassischen Datenverwaltungsanforderungen wie Datenschutz, Datensicherheit und Datenmigration zu erfüllen. Diese Anforderungen werden jedoch mithilfe unterschiedlicher Strategien, Tools und Methoden erfüllt.

Die unten aufgeführten Speicheroptionen auf Basis von **NetApp ONTAP** bieten Sicherheit, Datenschutz, Zuverlässigkeit und Flexibilität für Container- und Kubernetes-Bereitstellungen.

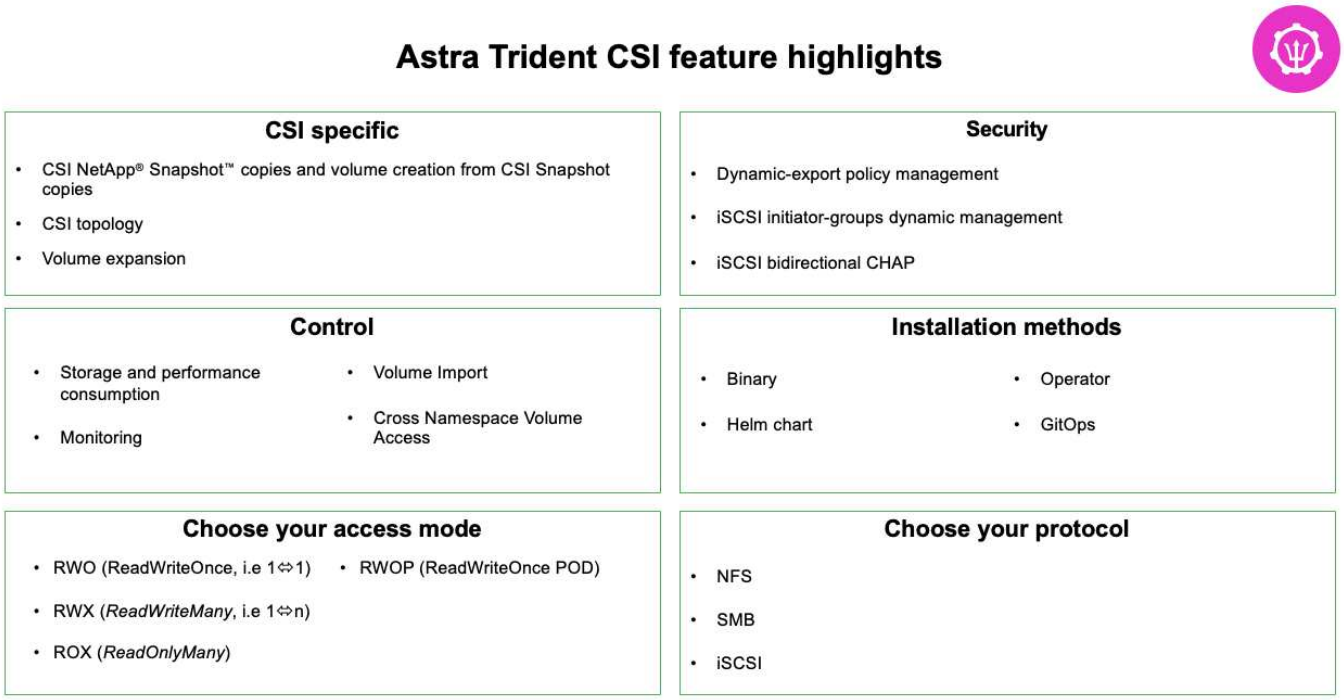
- Selbstverwalteter Speicher vor Ort:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Arrays (AFF), NetApp All SAN Array (ASA) und ONTAP Select
- Vom Anbieter verwalteter Speicher vor Ort:
  - NetApp Keystone bietet Storage as a Service (STaaS)
- Selbstverwalteter Speicher in der Cloud:
  - NetApp Cloud Volumes ONTAP(CVO) bietet selbstverwalteten Speicher in den Hyperscalern
- Vom Anbieter verwalteter Speicher in der Cloud:
  - Amazon FSx for NetApp ONTAP, Azure NetApp Files und Google Cloud NetApp Volumes bieten dateibasierten Speicher in der Cloud.



NetApp Console ermöglicht Ihnen das Managen all Ihrer Storage- und Datenressourcen über eine einzige Kontrollebene/Schnittstelle.

NetApp Console kann zum Erstellen und Verwalten von Cloud Storage (z. B. Cloud Volumes ONTAP und Azure NetApp Files), zum Verschieben, Schützen und Analysieren von Daten sowie zum Steuern zahlreicher lokaler und Edge-Storage-Systeme verwendet werden.

- NetApp Trident** ist ein CSI-konformer Speicher-Orchestrator, der eine schnelle und einfache Nutzung von persistentem Speicher ermöglicht, der durch eine Vielzahl der oben genannten NetApp -Speicheroptionen unterstützt wird. Es handelt sich um eine Open-Source-Software, die von NetApp gepflegt und unterstützt wird.



Geschäftskritische Container-Workloads erfordern mehr als nur persistente Volumes. Ihre Datenverwaltungsanforderungen erfordern auch den Schutz und die Migration der Kubernetes-Anwendungsobjekte.

> Anwendungsdaten umfassen neben den Benutzerdaten auch Kubernetes-Objekte: Einige Beispiele sind: - Kubernetes-Objekte wie Pods-Spezifikationen, PVCs, Bereitstellungen, Dienste - benutzerdefinierte Konfigurationsobjekte wie Konfigurationszuordnungen und Geheimnisse - persistente Daten wie Snapshot-Kopien, Backups, Klone - benutzerdefinierte Ressourcen wie CRs und CRDs

NetApp Trident Protect, als kostenloses Add-on zu NetApp Trident, bietet erweiterte Funktionen für das Anwendungsdatenmanagement, die die Funktionalität und Verfügbarkeit zustandsbehafteter Kubernetes-Anwendungen verbessern, die von NetApp ONTAP-Speichersystemen unterstützt werden. Trident Protect vereinfacht die Verwaltung, den Schutz und die Bewegung containerisierter Workloads sowohl in öffentlichen Clouds als auch in On-Premises-Umgebungen. Es bietet außerdem robuste Automatisierungsfunktionen über seine API und CLI.

Diese Referenzdokumentation bietet eine Validierung des Datenschutzes von containerbasierten Anwendungen, die auf der RedHat OpenShift-Plattform mit Trident Protect bereitgestellt werden. Darüber hinaus bietet die Lösung detaillierte Informationen zur Bereitstellung und Verwendung von Red Hat Advanced Cluster Management (ACM) zur Verwaltung der Containerplattformen. Das Dokument hebt auch die Details zur Integration von NetApp -Speicher mit Red Hat OpenShift-Containerplattformen mithilfe des Trident CSI Provisioner hervor.

Wertversprechen der NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift Container-Workloads

Die meisten Kunden beginnen nicht einfach mit dem Aufbau von Kubernetes-basierten Umgebungen ohne vorhandene Infrastruktur. Vielleicht handelt es sich um einen traditionellen IT-Shop, der die meisten seiner Unternehmensanwendungen auf virtuellen

Maschinen ausführt (beispielsweise in großen VMware-Umgebungen). Dann beginnen sie mit dem Aufbau kleiner containerbasierter Umgebungen, um die Anforderungen ihrer modernen Anwendungsentwicklungsteams zu erfüllen. Diese Initiativen beginnen normalerweise im Kleinen und breiten sich immer weiter aus, wenn die Teams diese neuen Technologien und Fähigkeiten erlernen und die vielen Vorteile erkennen, die sich aus ihrer Einführung ergeben. Die gute Nachricht für Kunden ist, dass NetApp die Anforderungen beider Umgebungen erfüllen kann. Dieses Lösungspaket für Hybrid-Multicloud mit Red Hat OpenShift ermöglicht es NetApp -Kunden, moderne Cloud-Technologien und -Dienste zu übernehmen, ohne ihre gesamte Infrastruktur und Organisation umbauen zu müssen. Unabhängig davon, ob Kundenanwendungen und -daten vor Ort, in der Cloud, auf virtuellen Maschinen oder in Containern gehostet werden, kann NetApp konsistentes Datenmanagement, Schutz, Sicherheit und Portabilität bieten. Mit diesen neuen Lösungen steht derselbe Mehrwert, den NetApp seit Jahrzehnten in lokalen Rechenzentrumsumgebungen bietet, für den gesamten Datenhorizont des Unternehmens zur Verfügung, ohne dass erhebliche Investitionen in die Umrüstung, den Erwerb neuer Fähigkeiten oder den Aufbau neuer Teams erforderlich sind. NetApp ist gut aufgestellt, um Kunden bei der Lösung dieser geschäftlichen Herausforderungen zu unterstützen, unabhängig davon, in welcher Phase ihrer Cloud-Reise sie sich befinden.

NetApp Hybrid Multi-Cloud mit Red Hat Openshift:

- Bietet Kunden validierte Designs und Vorgehensweisen, die ihnen die besten Möglichkeiten zum Verwalten, Schützen, Sichern und Migrieren ihrer Daten und Anwendungen bei der Verwendung von Red Hat OpenShift mit NetApp basierten Speicherlösungen aufzeigen.
- Präsentieren Sie Best Practices für Kunden, die Red Hat OpenShift mit NetApp -Speicher in VMware-Umgebungen, Bare-Metal-Infrastruktur oder einer Kombination aus beidem ausführen.
- Demonstrieren Sie Strategien und Optionen sowohl für lokale als auch für Cloud-Umgebungen sowie für Hybridumgebungen, in denen beide verwendet werden.

Unterstützte Lösungen von NetApp Hybrid Multicloud für Red Hat OpenShift Container-Workloads

Die Lösung testet und validiert Migration und zentralisierten Datenschutz mit OpenShift Container Platform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp Console und NetApp Trident Protect.

Für diese Lösung wurden die folgenden Szenarien von NetApp getestet und validiert. Die Lösung ist basierend auf den folgenden Merkmalen in mehrere Szenarien unterteilt:

- vor Ort
- Wolke
  - selbstverwaltete OpenShift-Cluster und selbstverwalteter NetApp Speicher
  - Vom Anbieter verwaltete OpenShift-Cluster und vom Anbieter verwalteter NetApp Speicher

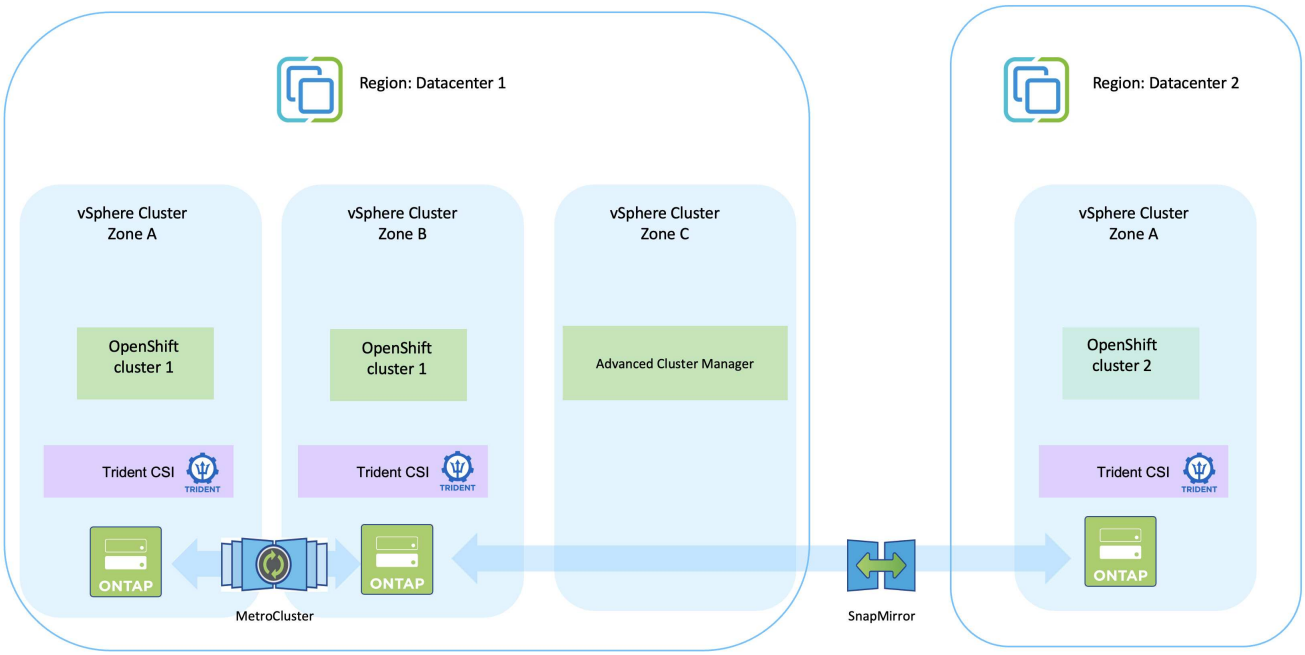
Wir werden in Zukunft weitere Lösungen und Anwendungsfälle entwickeln.

Szenario 1: Datenschutz und Migration innerhalb der lokalen Umgebung mit Trident Protect

Vor Ort: selbstverwaltete OpenShift-Cluster und selbstverwalteter NetApp Speicher

- Verwenden Sie Trident Protect, um Anwendungen zu schützen und die Migration zwischen den On-Premises-Clustern zu unterstützen.

Szenario 1

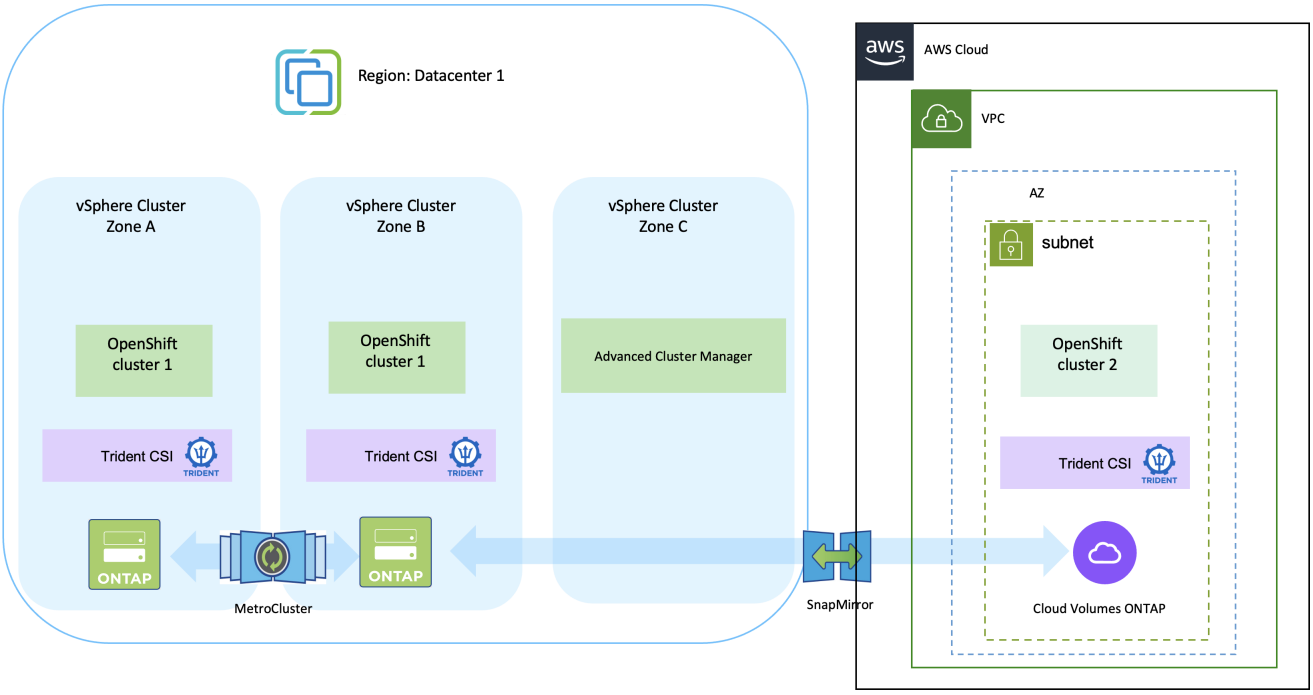


Szenario 2: Datenschutz und Migration von der lokalen Umgebung in die AWS-Umgebung mit Trident Protect

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher AWS Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher

- Nutzen Sie Trident Protect, um Anwendungen zu schützen und die Migration zwischen den lokalen Clustern und den selbstverwalteten OpenShift Clustern in AWS zu unterstützen.

Szenario 2

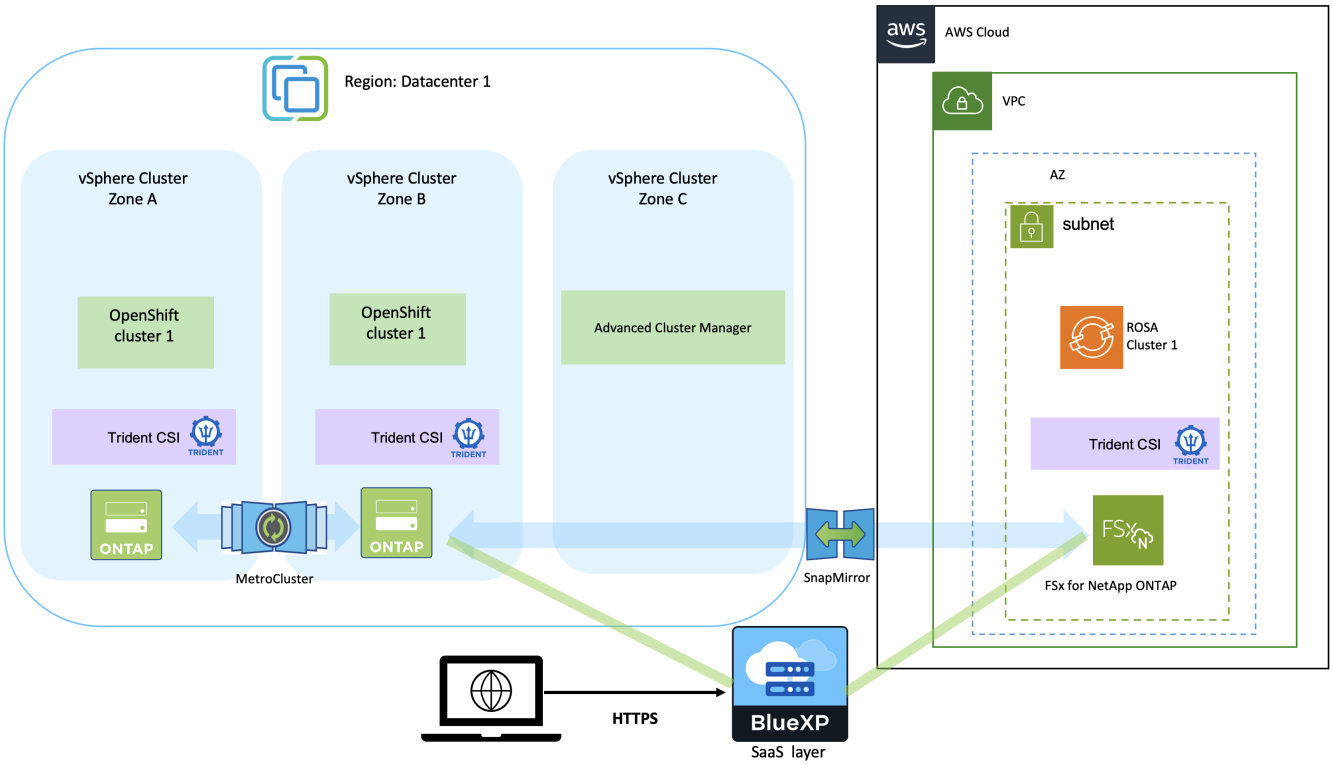


Szenario 3: Datenschutz und Migration von der lokalen Umgebung in die AWS-Umgebung

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher AWS Cloud: Vom Anbieter verwalteter OpenShift-Cluster (ROSA) und vom Anbieter verwalteter Speicher (FSx ONTAP)

- Die Replikation persistenter Volumes (FSx ONTAP) erfolgt in der NetApp Console.
- Erstellen Sie mithilfe von OpenShift GitOps Anwendungsmetadaten neu.

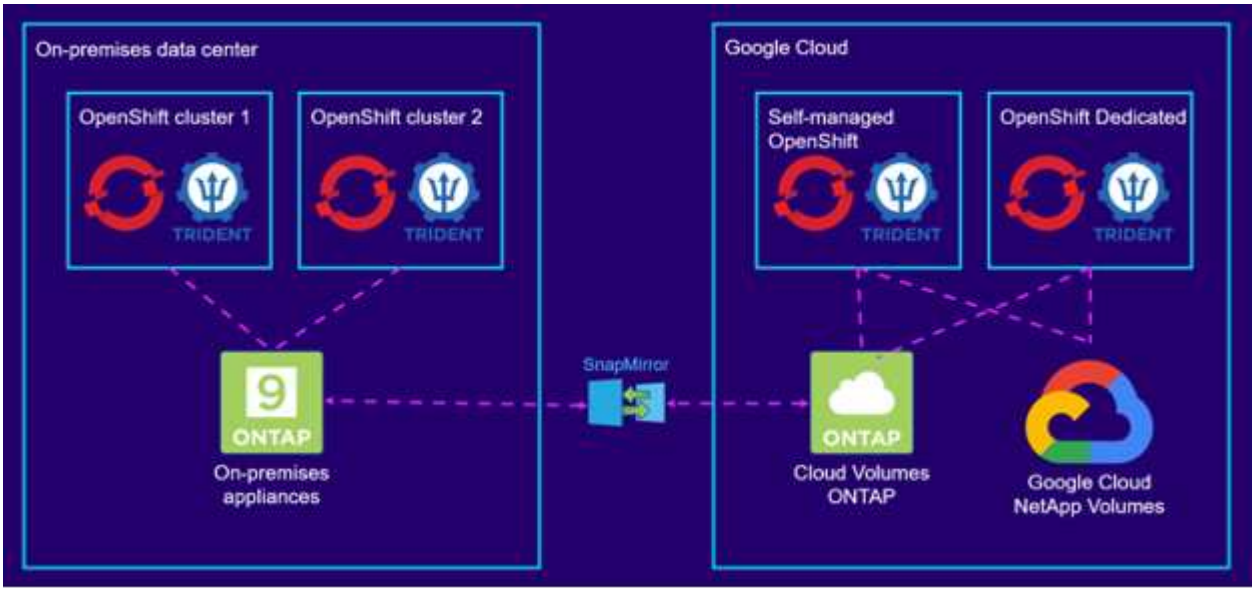
Szenario 3



Szenario 4: Datenschutz und Migration von der lokalen Umgebung zur GCP-Umgebung mit Trident Protect

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher Google Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher

- Nutzen Sie Trident Protect, um Anwendungen zu schützen und die Migration zwischen lokalen und Google Cloud OpenShift Clustern zu unterstützen.

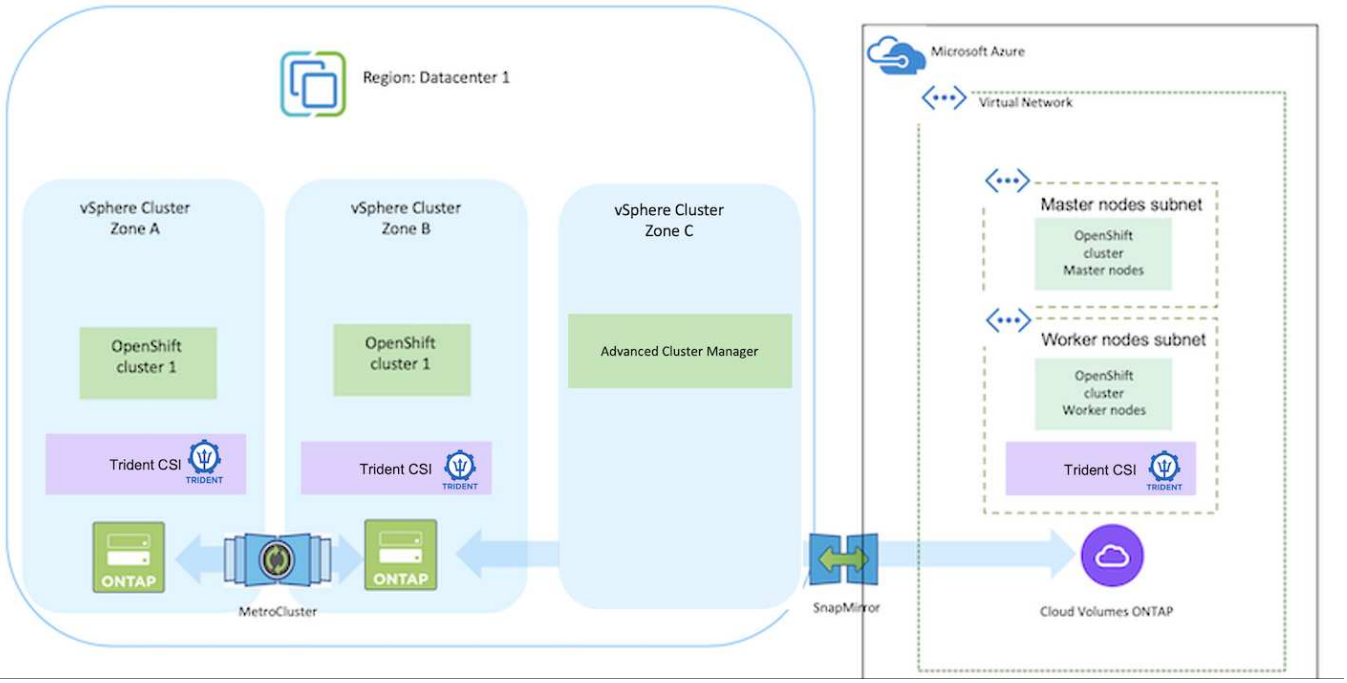


Hinweise zur Verwendung von ONTAP in einer MetroCluster -Konfiguration finden Sie unter"hier," .

Szenario 5: Datenschutz und Migration von der lokalen Umgebung in die Azure-Umgebung mit Trident Protect

Vor Ort: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher Azure Cloud: Selbstverwalteter OpenShift-Cluster und selbstverwalteter Speicher

- Nutzen Sie Trident Protect, um Anwendungen zu schützen und die Migration zwischen lokalen Systemen und OpenShift Clustern in Azure zu unterstützen.



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 Migration und zentralisierten Datenschutz mit der OpenShift-Containerplattform, OpenShift Advanced Cluster Manager, NetApp ONTAP und NetApp Trident Protect.

Die Szenarien 1, 2 und 3 der Lösung wurden mit den in der folgenden Tabelle gezeigten Versionen validiert:

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 vor Ort und in AWS
* NetApp Trident*	Trident Server und Client 23.04.0
* NetApp Trident Protect*	Trident Protect 22.11.0-82
* NetApp ONTAP*	ONTAP 9.12.1
AWS FSx ONTAP	Einzel-AZ

Szenario 4 der Lösung wurde mit den in der folgenden Tabelle gezeigten Versionen validiert:

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 vor Ort und in Google Cloud
* NetApp Trident*	Trident Server und Client 23.07.0
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Einzelne AZ, einzelner Knoten, 9.14.0

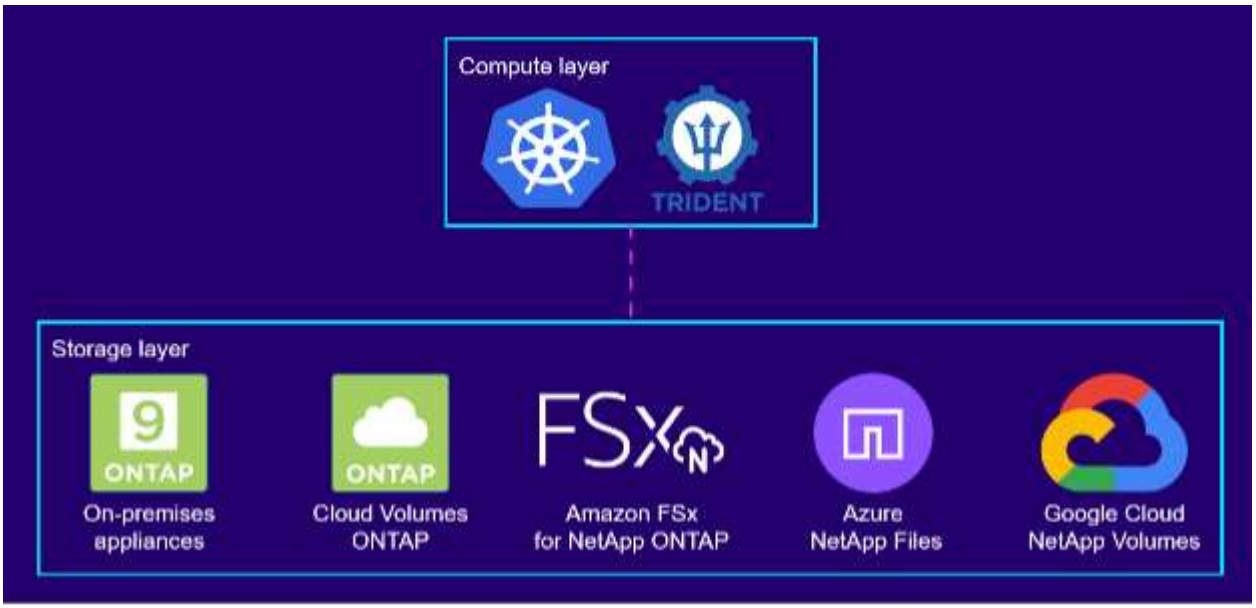
Szenario 5 der Lösung wurde mit den in der folgenden Tabelle gezeigten Versionen validiert:

Komponente	Version
VMware	vSphere-Client-Version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Quell- und Zielcluster	OpenShift 4.13.25 vor Ort und in Azure
* NetApp Trident*	Trident Server und Client 23.10.0
* NetApp Trident Protect*	Trident Protect 23.10
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Einzelne AZ, einzelner Knoten, 9.14.0

Unterstützte NetApp Storage-Integrationen mit Red Hat OpenShift Containers

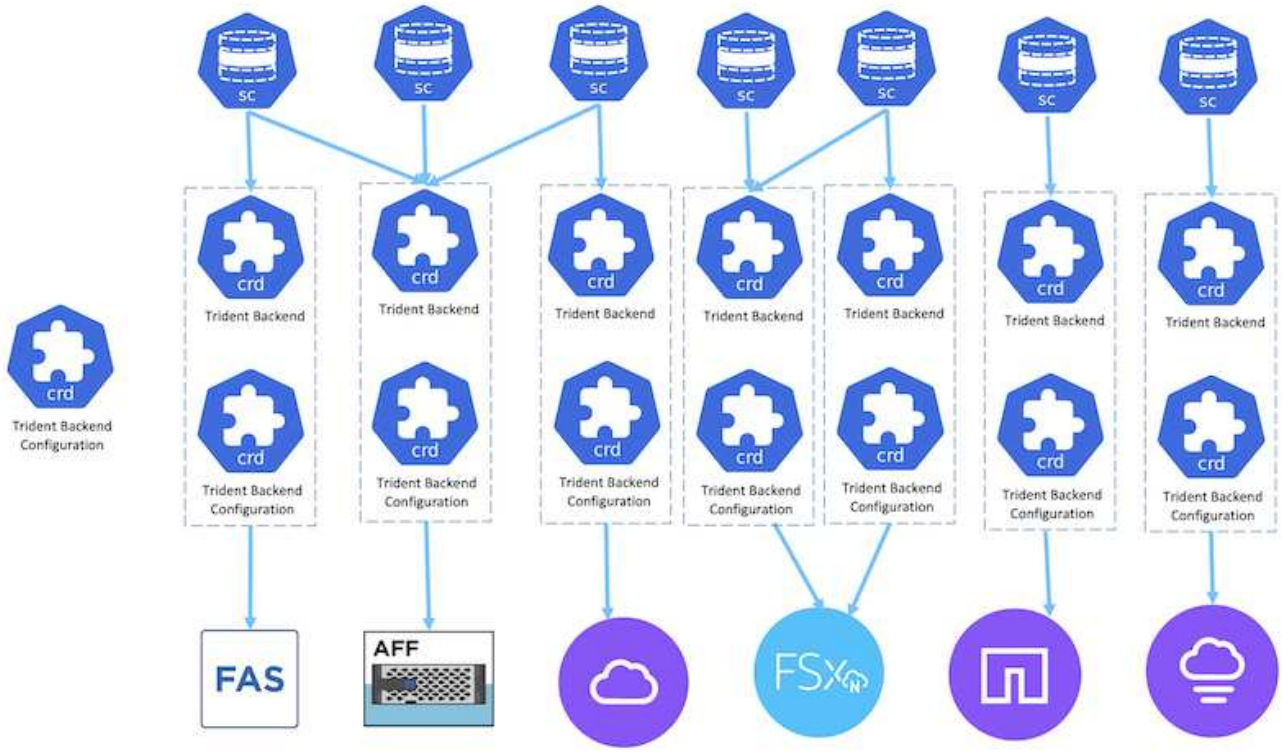
Unabhängig davon, ob die Red Hat OpenShift-Container auf VMware oder in den Hyperscalern ausgeführt werden, kann NetApp Trident als CSI-Provisioner für die verschiedenen Arten von Backend NetApp -Speicher verwendet werden, die es unterstützt.

Das folgende Diagramm zeigt die verschiedenen Backend NetApp -Speicher, die mithilfe von NetApp Trident in OpenShift-Cluster integriert werden können.



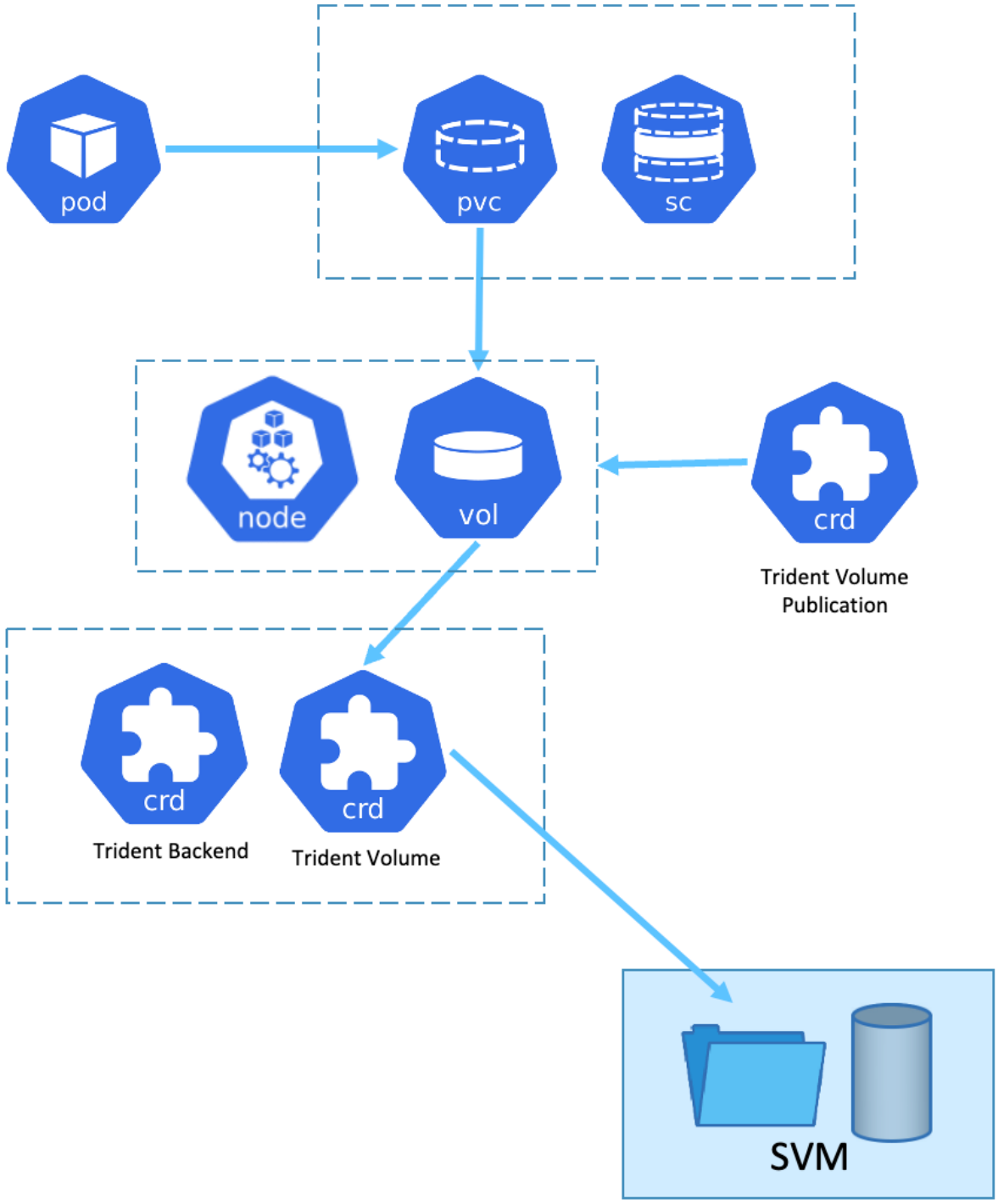
ONTAP Storage Virtual Machine (SVM) bietet sichere Mandantenfähigkeit. Ein einzelner OpenShift-Cluster kann eine Verbindung zu einem oder mehreren SVMs oder sogar zu mehreren ONTAP Clustern herstellen. Die Speicherklasse filtert den Backend-Speicher basierend auf Parametern oder Bezeichnungen. Speicheradministratoren definieren die Parameter für die Verbindung mit dem Speichersystem mithilfe der Trident-Backend-Konfiguration. Bei erfolgreichem Verbindungsaufbau erstellt es das Trident-Backend und füllt die Informationen, die die Speicherklasse filtern kann.

Die Beziehung zwischen der Speicherklasse und dem Backend wird unten dargestellt.



Der Anwendungsbesitzer fordert ein dauerhaftes Volume unter Verwendung der Speicherklasse an. Die Speicherklasse filtert den Backend-Speicher.

Die Beziehung zwischen dem Pod und dem Backend-Speicher wird unten dargestellt.



Optionen für die Container Storage Interface (CSI)

In vSphere-Umgebungen können Kunden den VMware CSI-Treiber und/oder Trident CSI zur Integration mit ONTAP auswählen. Bei VMware CSI werden die persistenten Volumes als lokale SCSI-Festplatten verwendet, während sie bei Trident über das Netzwerk verwendet werden.

Da VMware CSI keine RWX-Zugriffsmodi mit ONTAP unterstützt, müssen Anwendungen Trident CSI verwenden, wenn der RWX-Modus erforderlich ist. Bei FC-basierten Bereitstellungen wird VMware CSI

bevorzugt und SnapMirror Business Continuity (SMBC) bietet Hochverfügbarkeit auf Zonenebene.

VMware CSI unterstützt

- Core Block-basierte Datenspeicher (FC, FCoE, iSCSI, NVMeoF)
- Core File-basierte Datenspeicher (NFS v3, v4)
- vVol-Datenspeicher (Block und Datei)

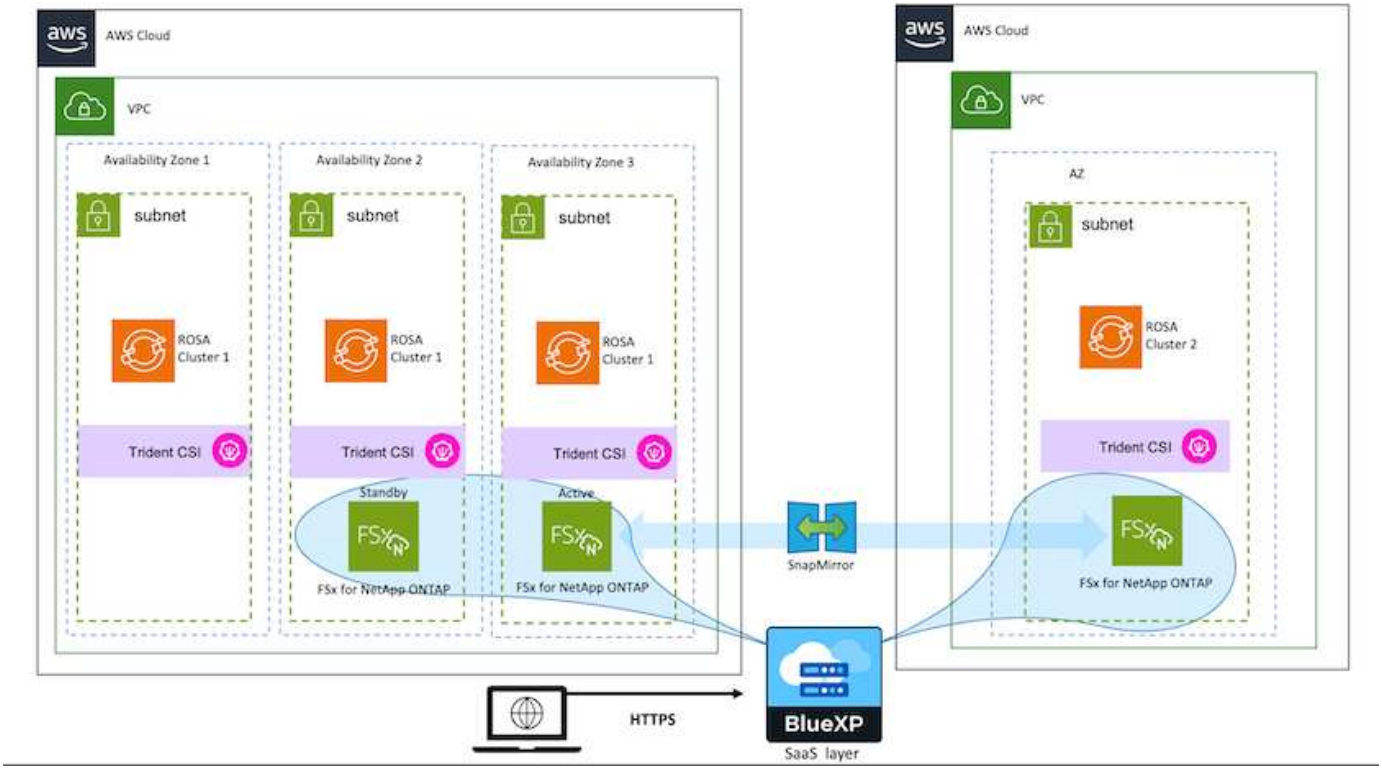
Trident verfügt über folgende Treiber zur Unterstützung von ONTAP

- ontap-san (dediziertes Volume)
- ontap-san-economy (gemeinsam genutztes Volume)
- ontap-nas (dediziertes Volume)
- ontap-nas-economy (gemeinsam genutztes Volume)
- ontap-nas-flexgroup (dediziertes Großvolume)

Sowohl für VMware CSI als auch für Trident CSI unterstützt ONTAP Nconnect, Session Trunking, Kerberos usw. für NFS und Multipathing, Chap-Authentifizierung usw. für Blockprotokolle.

In AWS kann Amazon FSx for NetApp ONTAP (FSx ONTAP) in einer einzelnen Availability Zone (AZ) oder in mehreren AZs bereitgestellt werden. Für Produktions-Workloads, die eine hohe Verfügbarkeit erfordern, bietet Multi-AZ Fehlertoleranz auf Zonenebene und verfügt im Vergleich zu Single-AZ über einen besseren NVMe-Lesecache. Weitere Informationen finden Sie unter"AWS-Leistungsrichtlinien" .

Um Kosten für die Notfallwiederherstellungssite zu sparen, kann ein einzelner AZ FSx ONTAP verwendet werden.



Informationen zur Anzahl der von FSx ONTAP unterstützten SVMs finden Sie unter"Verwalten der virtuellen FSx ONTAP -Speichermaschine"

Zusätzliche Dokumentation

Hier finden Sie einige zusätzliche Dokumentationen als Referenz:

1. "VMware vSphere"
2. "Produktdokumentation zur OpenShift Container-Plattform"
3. "Installieren von OpenShift-Containerplattformclustern"
4. "Produktdokumentation zur erweiterten Clusterverwaltung"
5. "Erstellen eines Clusters mit ACM"
6. "Bereitstellen von Red Hat Quay auf OpenShift"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda" - Verda (Open source) bietet eine Sammlung von Referenz-Execution-Hooks für gängige Cloud nativ datenintensive Anwendungen
10. "NetApp Datenservices"
11. "Red Hat OpenShift Service auf AWS klassische Architektur"
12. "Amazon FSx ONTAP"
13. "Installieren von OpenShift-Clustern auf GCP"
14. "Installieren von OpenShift-Clustern auf Azure"

Openshift für lokale Anwendungen

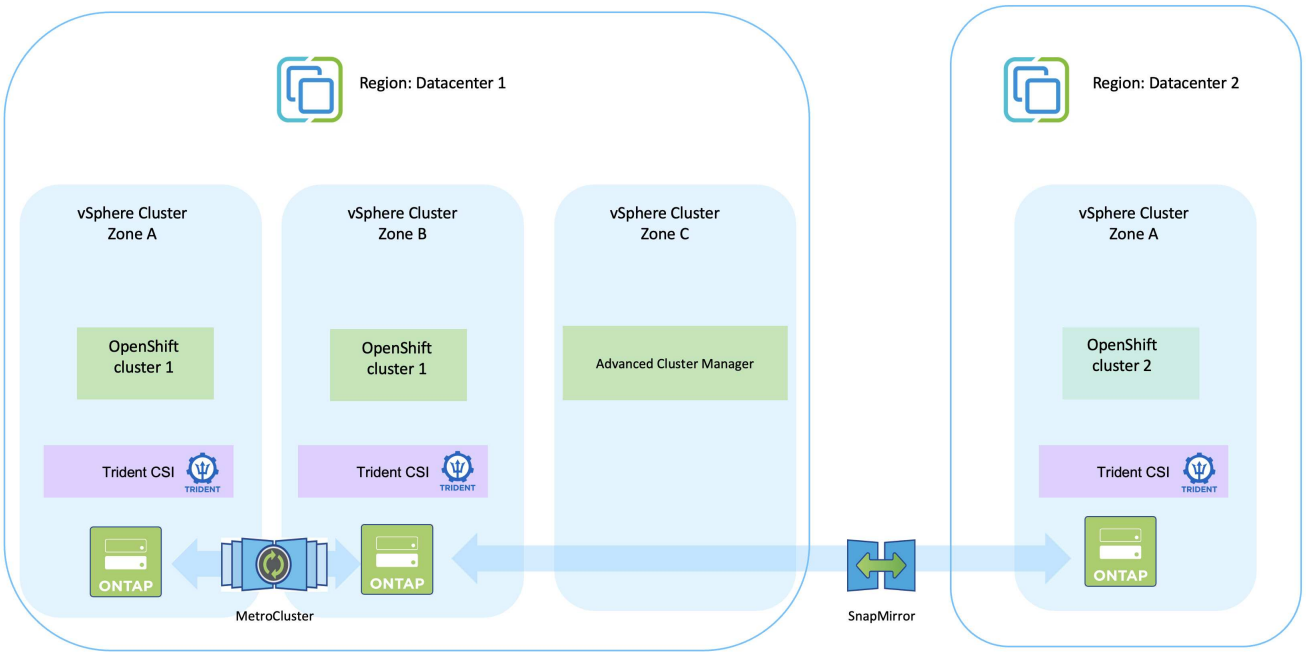
NetApp -Lösung mit Red Hat OpenShift Container-Plattform-Workloads auf VMware

Wenn Kunden ihre modernen containerisierten Anwendungen auf der Infrastruktur ihrer privaten Rechenzentren ausführen müssen, können sie dies tun. Sie sollten die Red Hat OpenShift-Containerplattform (OCP) für eine erfolgreiche produktionsbereite Umgebung zur Bereitstellung ihrer Container-Workloads planen und bereitstellen. Ihre OCP-Cluster können auf VMware oder Bare Metal bereitgestellt werden.

NetApp ONTAP Speicher bietet Datenschutz, Zuverlässigkeit und Flexibilität für Containerbereitstellungen. Trident dient als dynamischer Speicherbereitsteller, um persistenten ONTAP Speicher für zustandsbehaftete Anwendungen der Kunden zu nutzen. NetApp Trident Protect kann für die zahlreichen Datenverwaltungsanforderungen von Stateful-Anwendungen wie Datenschutz, Migration und Geschäftskontinuität verwendet werden.

Mit VMware vSphere bieten NetApp ONTAP -Tools ein vCenter-Plugin, das zum Bereitstellen von Datenspeichern verwendet werden kann. Wenden Sie Tags an und verwenden Sie sie mit OpenShift zum Speichern der Knotenkonfiguration und -daten. NVMe-basierter Speicher bietet geringere Latenz und hohe Leistung.

Datenschutz- und Migrationslösung für OpenShift-Container-Workloads mit Trident Protect

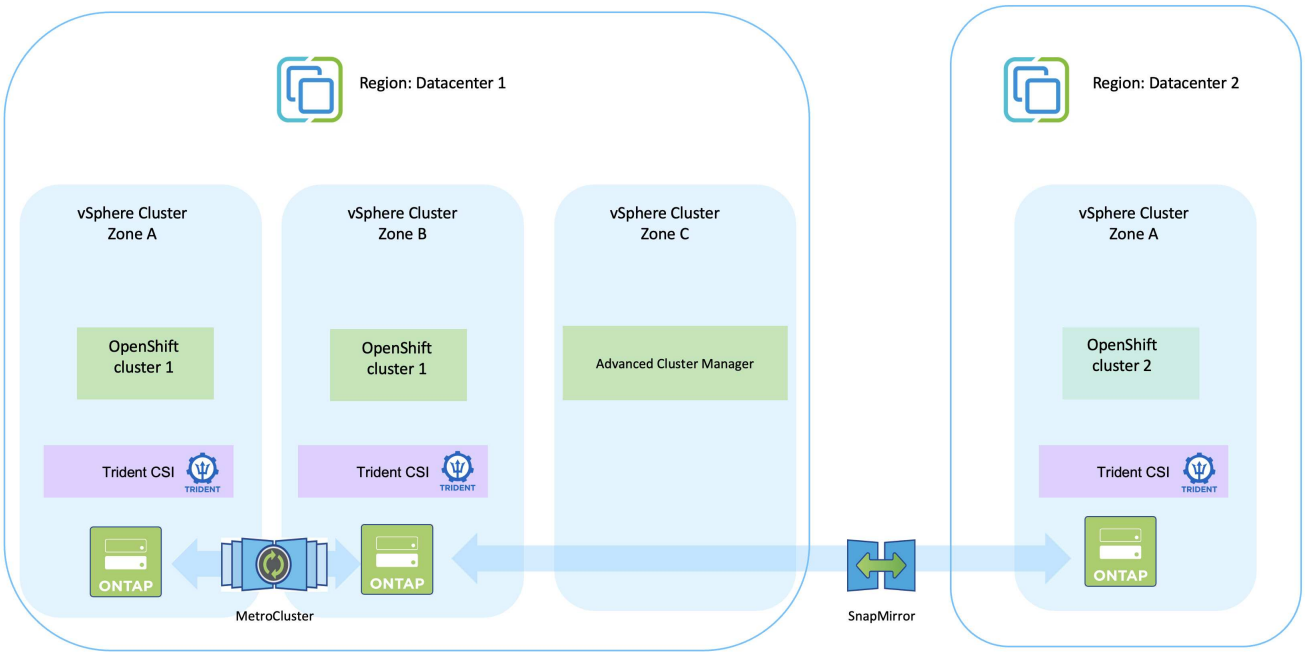


Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf VMware

In diesem Abschnitt wird ein allgemeiner Workflow zum Einrichten und Verwalten von OpenShift-Clustern und zum Verwalten von statusbehafteten Anwendungen darauf beschrieben. Es zeigt die Verwendung von NetApp ONTAP Speicherarrays mit Hilfe von Trident zur Bereitstellung persistenter Volumes.

Es gibt mehrere Möglichkeiten, Red Hat OpenShift Container-Plattformcluster bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentationslinks für die jeweils verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im"Ressourcenbereich" .

Hier ist ein Diagramm, das die auf VMware in einem Rechenzentrum bereitgestellten Cluster darstellt.



Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

▼ Bereitstellen und Konfigurieren einer CentOS-VM

- Es wird in der VMware vSphere-Umgebung bereitgestellt.
- Diese VM wird zum Bereitstellen einiger Komponenten wie NetApp Trident und NetApp Trident Protect für die Lösung verwendet.
- Während der Installation wird auf dieser VM ein Root-Benutzer konfiguriert.

▼ Bereitstellen und Konfigurieren eines OpenShift Container Platform-Clusters auf VMware vSphere (Hub-Cluster)

Es gelten die Anweisungen für die "Unterstützte Bereitstellung"Methode zum Einsetzen eines OCP Clusters.

Denken Sie an Folgendes: – Erstellen Sie einen öffentlichen und privaten SSH-Schlüssel, um ihn dem Installationsprogramm bereitzustellen. Diese Schlüssel werden bei Bedarf zum Anmelden bei den Master- und Worker-Knoten verwendet. - Laden Sie das Installationsprogramm vom unterstützten Installationsprogramm 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 Mindestanforderungen an CPU, Speicher und Festplatte erfüllen. (Siehe die VM-Erstellungsbefehle auf"Das" Seite für den Master und die Worker-Knoten, die diese Informationen bereitstellen) – Die DiskUUID sollte auf allen VMs aktiviert sein. – Erstellen Sie mindestens 3 Knoten für den Master und 3 Knoten für den Worker. – Sobald sie vom Installationsprogramm erkannt wurden, aktivieren Sie den Umschaltknopf für die VMware vSphere-Integration.

▼ Installieren Sie Advanced Cluster Management auf dem Hub-Cluster

Dies wird mithilfe des Advanced Cluster Management Operator auf dem Hub-Cluster installiert. Beachten Sie die Anweisungen"hier," .

▼ Installieren Sie zwei zusätzliche OCP-Cluster (Quelle und Ziel).

- Die zusätzlichen Cluster können mithilfe des ACM auf dem Hub-Cluster bereitgestellt werden.
- Siehe die Anweisungen "hier,".

▼ **Konfigurieren des NetApp ONTAP -Speichers**

- Installieren Sie einen ONTAP Cluster mit Konnektivität zu den OCP-VMs in der VMWare-Umgebung.
- Erstellen Sie eine SVM.
- Konfigurieren Sie NAS-Datenlebensdauer, um auf den Speicher in SVM zuzugreifen.

▼ **Installieren Sie NetApp Trident auf den OCP-Clustern**

- Installieren Sie NetApp Trident auf allen drei Clustern: Hub-, Quell- und Zielcluster
- Siehe die Anweisungen "hier,".
- Erstellen Sie ein Speicher-Backend für ontap-nas.
- Erstellen Sie eine Speicherklasse für ontap-nas.
- Siehe Anweisungen"hier," .

▼ **Bereitstellen einer Anwendung auf dem Quellcluster**

Verwenden Sie OpenShift GitOps, um eine Anwendung bereitzustellen. (z. B. Postgres, Ghost)

Der nächste Schritt besteht darin, Trident Protect für den Datenschutz und die Datenmigration vom Quell- zum Zielcluster zu verwenden. Verweisen"hier," Anweisungen hierzu finden Sie unter.

Datenschutz mit Trident Protect

Diese Seite zeigt die Datenschutzoptionen für Red Hat OpenShift Container-basierte Anwendungen, die auf VMware vSphere mit Trident Protect ausgeführt werden.

Im Zuge der Modernisierung ihrer Anwendungen mit Red Hat OpenShift sollte eine Datenschutzstrategie vorhanden sein, um sie vor versehentlichem Löschen oder anderen menschlichen Fehlern zu schützen. Oft ist auch eine Schutzstrategie aus regulatorischen oder Compliance-Gründen erforderlich, um ihre Daten vor einer Katastrophe zu schützen.

Die Anforderungen an den Datenschutz variieren von der Rückkehr zu einer Point-in-Time-Kopie bis hin zum automatischen Failover auf eine andere Fehlerdomäne ohne menschliches Eingreifen. Viele Kunden wählen ONTAP als bevorzugte Speicherplattform für ihre Kubernetes-Anwendungen aufgrund der umfangreichen Funktionen wie Mandantenfähigkeit, Multiprotokoll, hohe Leistung und Kapazitätsangebote, Replikation und Caching für mehrere Standorte, Sicherheit und Flexibilität.

Für Details zum Schutz und zur Migration von Container-Workloads mit Trident Protect lesen Sie bitte den folgenden Abschnitt: - "Schützen und migrieren Sie Container-Apps mit Trident Protect"

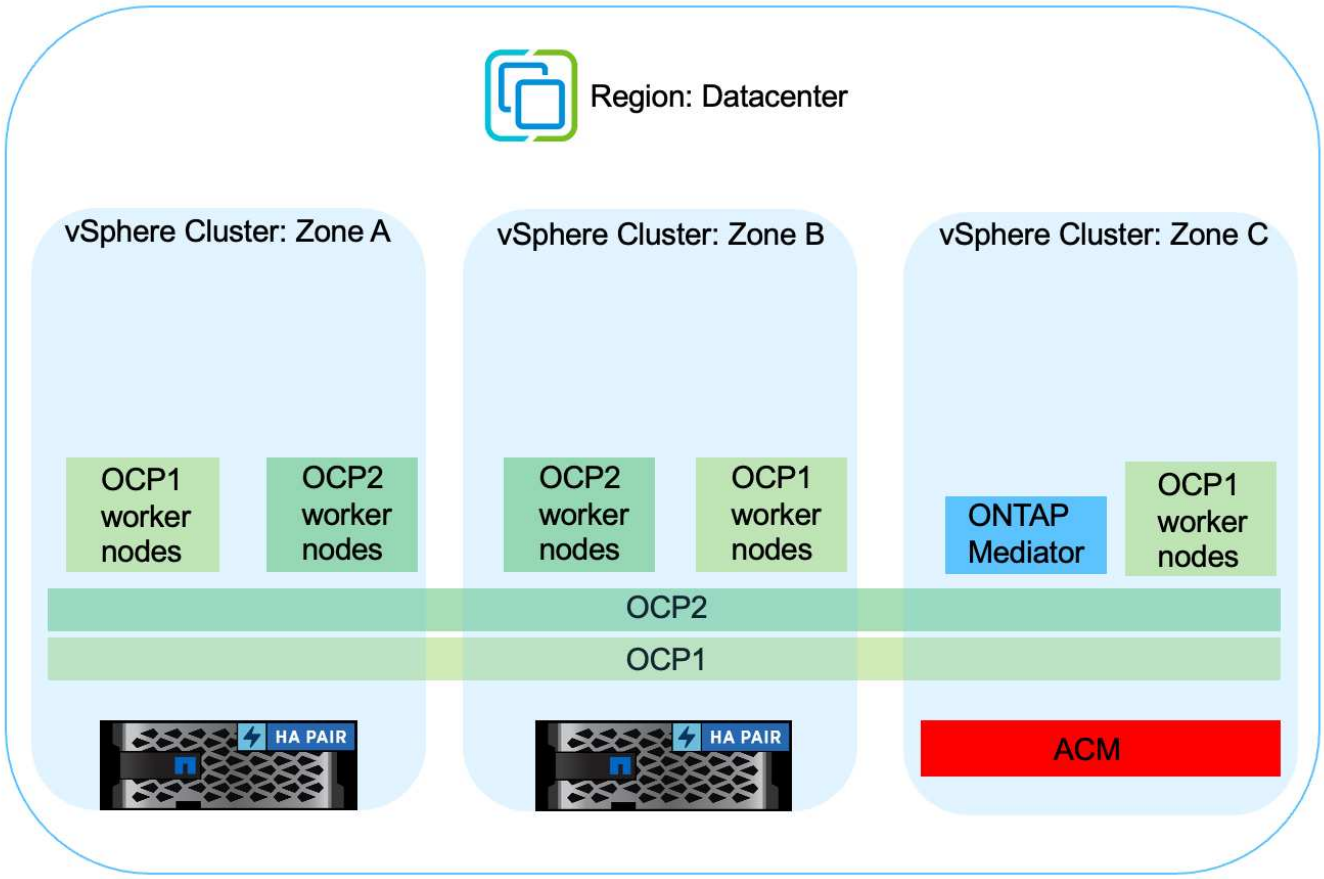
Geschäftskontinuität mit MetroCluster

Die meisten unserer Hardwareplattformen für ONTAP verfügen über Hochverfügbarkeitsfunktionen zum Schutz vor Geräteausfällen, sodass keine Notfallwiederherstellung erforderlich ist. Zum Schutz vor Feuer oder anderen Katastrophen und um das Geschäft mit Null-RPO und niedrigem RTO fortzuführen, wird jedoch häufig eine MetroCluster Lösung verwendet.

Kunden, die derzeit über ein ONTAP -System verfügen, können es auf MetroCluster erweitern, indem sie unterstützte ONTAP -Systeme innerhalb der Entfernungsbeschränkungen hinzufügen, um eine Notfallwiederherstellung auf Zonenebene bereitzustellen. Trident, das CSI (Container Storage Interface),

unterstützt NetApp ONTAP einschließlich MetroCluster -Konfiguration sowie andere Optionen wie Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP usw. Trident bietet fünf Speichertreiberoptionen für ONTAP und alle werden für die MetroCluster Konfiguration unterstützt. Verweisen"hier," Weitere Informationen zu den von Trident unterstützten ONTAP Speichertreibern finden Sie unter.

Die MetroCluster -Lösung erfordert eine Layer-2-Netzwerkerweiterung oder die Fähigkeit, von beiden Fehlerdomänen aus auf dieselbe Netzwerkadresse zuzugreifen. Sobald die MetroCluster Konfiguration eingerichtet ist, ist die Lösung für Anwendungsbesitzer transparent, da alle Volumes im MetroCluster -SVM geschützt sind und die Vorteile von SyncMirror (Null-RPO) nutzen.



Geben Sie für die Trident -Backend-Konfiguration (TBC) bei Verwendung der MetroCluster -Konfiguration nicht dataLIF und SVM an. Geben Sie die SVM-Verwaltungs-IP für managementLIF an und verwenden Sie die Anmeldeinformationen der Rolle vsadmin.

Details zu den Datenschutzfunktionen von Trident Protect sind verfügbar "hier,".

Hybrid Cloud mit selbstverwalteten Komponenten

NetApp -Lösung mit Red Hat OpenShift Container-Plattform-Workloads in der Hybrid Cloud

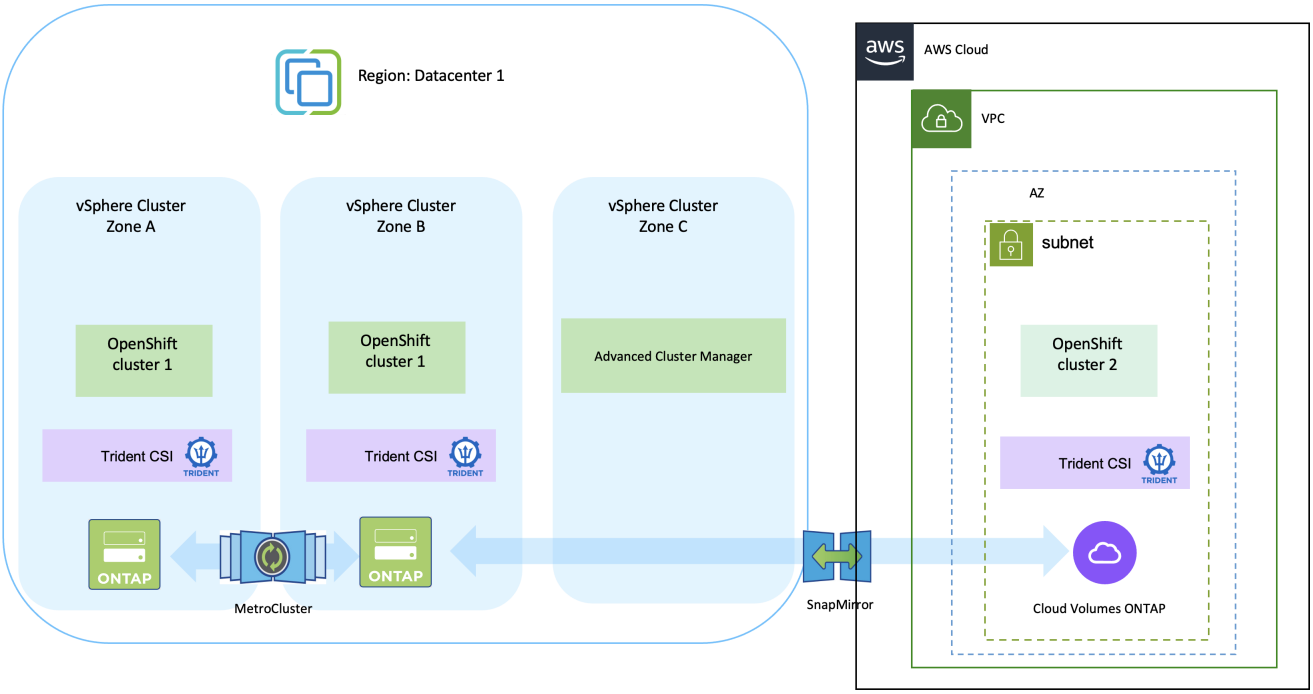
Kunden sind möglicherweise an einem Punkt ihrer Modernisierungsreise, an dem sie bereit sind, einige ausgewählte oder alle Workloads aus ihren Rechenzentren in die Cloud zu verschieben. Sie können sich aus verschiedenen Gründen für die Verwendung selbstverwalteter OpenShift-Container und selbstverwalteter NetApp Speicher in der

Cloud entscheiden. Sie sollten die Red Hat OpenShift-Containerplattform (OCP) in der Cloud planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für die Migration ihrer Container-Workloads aus ihren Rechenzentren zu schaffen. Ihre OCP-Cluster können in ihren Rechenzentren auf VMware oder Bare Metal und in der Cloud-Umgebung auf AWS, Azure oder Google Cloud bereitgestellt werden.

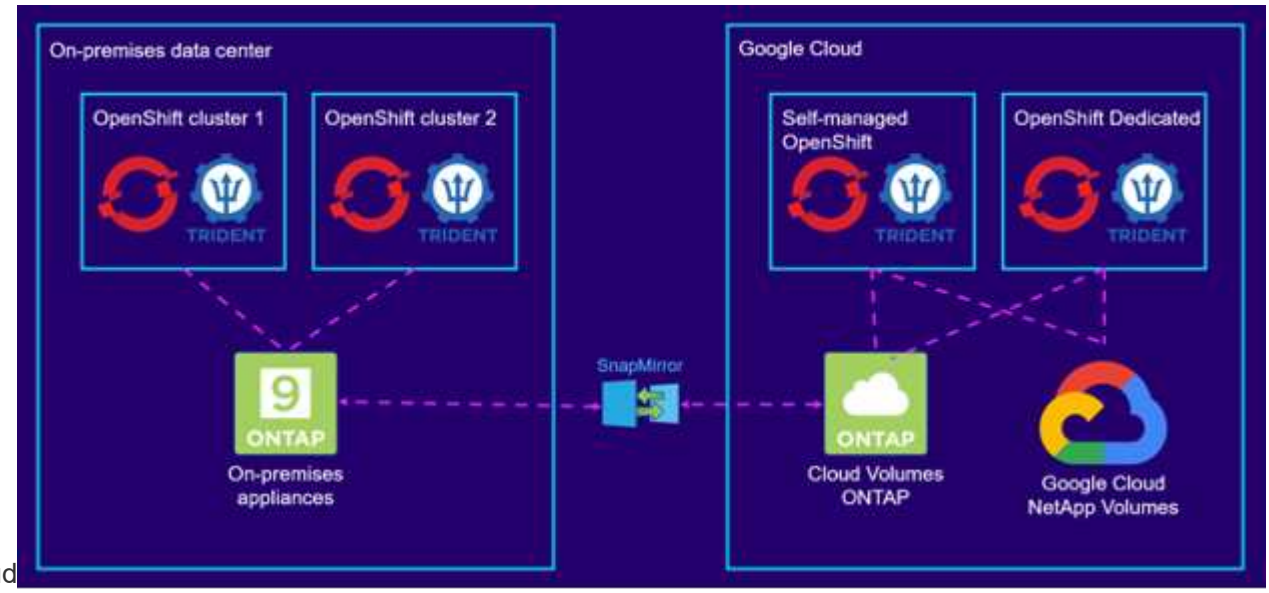
NetApp Cloud Volumes ONTAP storage bietet Datenschutz, Zuverlässigkeit und Flexibilität für Container-Bereitstellungen in AWS, Azure und Google Cloud. Trident dient als der dynamische Speicherbereitsteller, um den persistenten Cloud Volumes ONTAP storage für zustandsbehaftete Anwendungen der Kunden zu nutzen. Trident Protect kann für die Datenverwaltungsanforderungen zustandsbehafteter Anwendungen wie Datenschutz, Migration und Geschäftskontinuität verwendet werden.

Datenschutz- und Migrationslösung für OpenShift-Container-Workloads in einer Hybrid Cloud mit Trident Protect

Vor Ort und
AWS

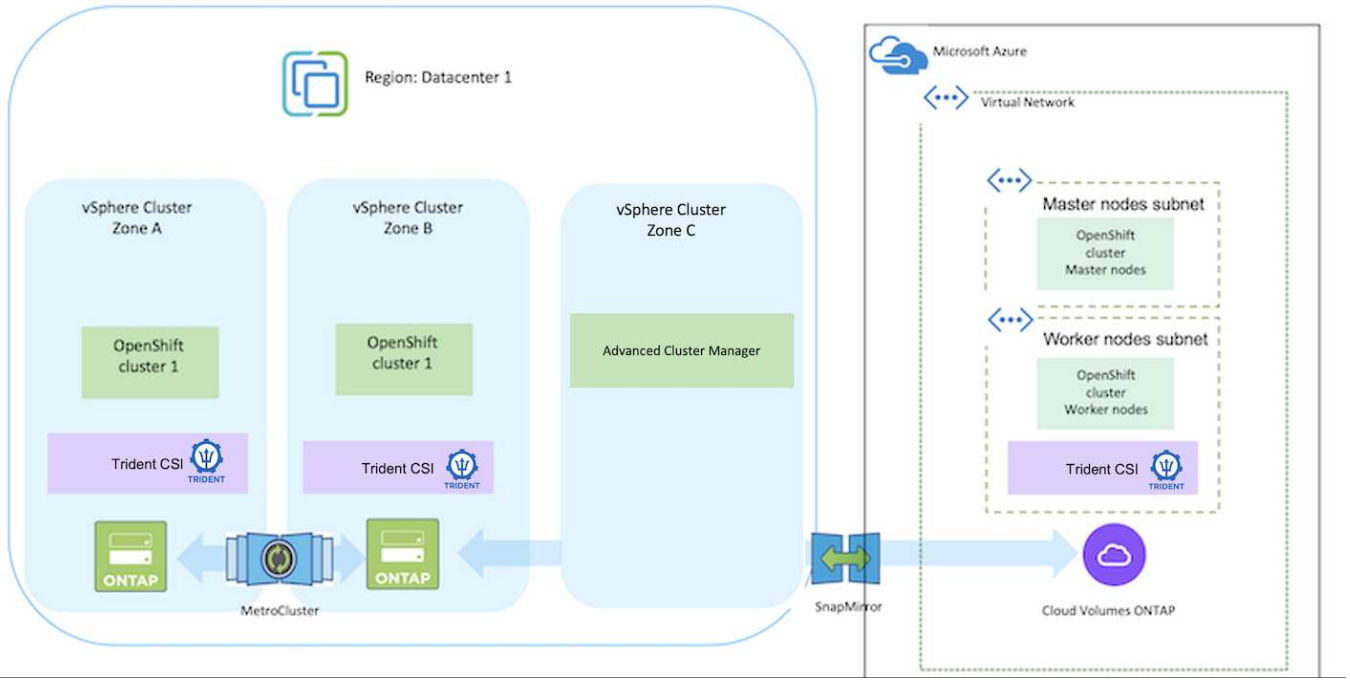


Vor Ort und in der Google



Cloud

Vor Ort und in der Azure Cloud

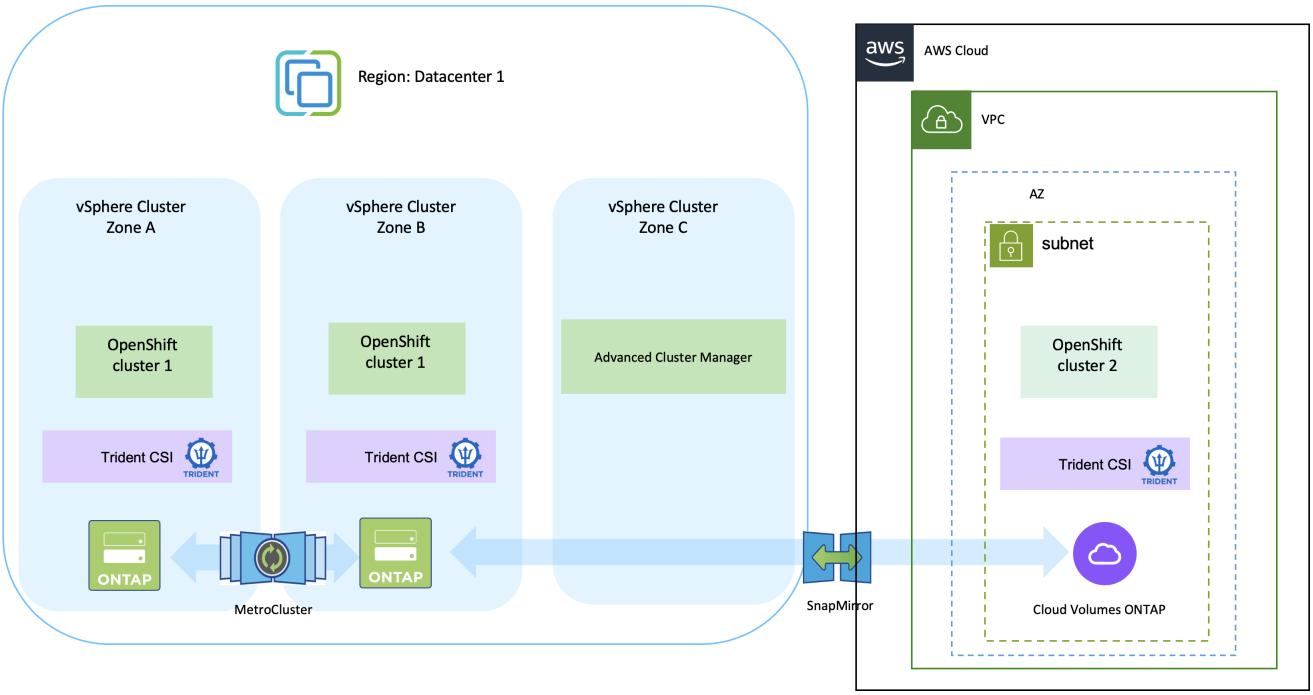


Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf AWS

In diesem Abschnitt wird ein allgemeiner Workflow zum Einrichten und Verwalten von OpenShift-Clustern in AWS und zum Bereitstellen von zustandsbehafteten Anwendungen darauf beschrieben. Es zeigt die Verwendung von NetApp Cloud Volumes ONTAP Speicher mit Hilfe von Trident zur Bereitstellung persistenter Volumes. Es werden Details zur Verwendung von Trident Protect zur Durchführung von Datenschutz- und Migrationsaktivitäten für die Stateful-Anwendungen bereitgestellt.

Es gibt mehrere Möglichkeiten, Red Hat OpenShift Container-Plattformcluster auf AWS bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentationslinks für die jeweils verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im"Ressourcenbereich" .

Hier ist ein Diagramm, das die auf AWS bereitgestellten und über ein VPN mit dem Rechenzentrum verbundenen Cluster darstellt.



Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

▼ **Installieren Sie einen OCP-Cluster auf AWS über die erweiterte Clusterverwaltung.**

- Erstellen Sie eine VPC mit einer Site-to-Site-VPN-Verbindung (mit pfsense), um eine Verbindung zum lokalen Netzwerk herzustellen.
- Das lokale Netzwerk verfügt über eine Internetverbindung.
- Erstellen Sie 3 private Subnetze in 3 verschiedenen AZs.
- Erstellen Sie eine privat gehostete Route 53-Zone und einen DNS-Resolver für die VPC.

Erstellung eines OpenShift Clusters auf AWS mit dem Assistenten Advanced Cluster Management (ACM). Weitere Informationen enthalten die Anweisungen "hier,".

Sie können den Cluster auch in AWS über die OpenShift Hybrid Cloud Konsole erstellen. Anweisungen finden sich "hier,".

Wenn Sie den Cluster mit ACM erstellen, können Sie die Installation anpassen, indem Sie die YAML-Datei bearbeiten, nachdem Sie die Details in der Formularansicht eingegeben haben. Nachdem der Cluster erstellt wurde, können Sie sich zur Fehlerbehebung oder für zusätzliche manuelle Konfigurationen per SSH bei den Knoten des Clusters anmelden. Verwenden Sie zur Anmeldung den SSH-Schlüssel, den Sie während der Installation

angegeben haben, und den Benutzernamen „core“.

▼ **Deployment von Cloud Volumes ONTAP in AWS mit NetApp Console.**

- Installieren Sie den Connector in einer lokalen VMware-Umgebung. Siehe Anweisungen"hier," .
- Stellen Sie mithilfe des Connectors eine CVO-Instanz in AWS bereit. Siehe Anweisungen"hier," .

Der Connector kann auch in der Cloud-Umgebung installiert werden. Verweisen"hier," für weitere Informationen.

▼ **Installieren Sie Trident im OCP-Cluster**

- Bereitstellung von Trident Operator mit Helm. Anweisungen "hier," finden Sie unter.
- Erstellen Sie ein Backend und eine Speicherklasse. Siehe Anweisungen"hier," .

Verwenden der CSI-Topologiefunktion von Trident für Mehrzonenarchitekturen

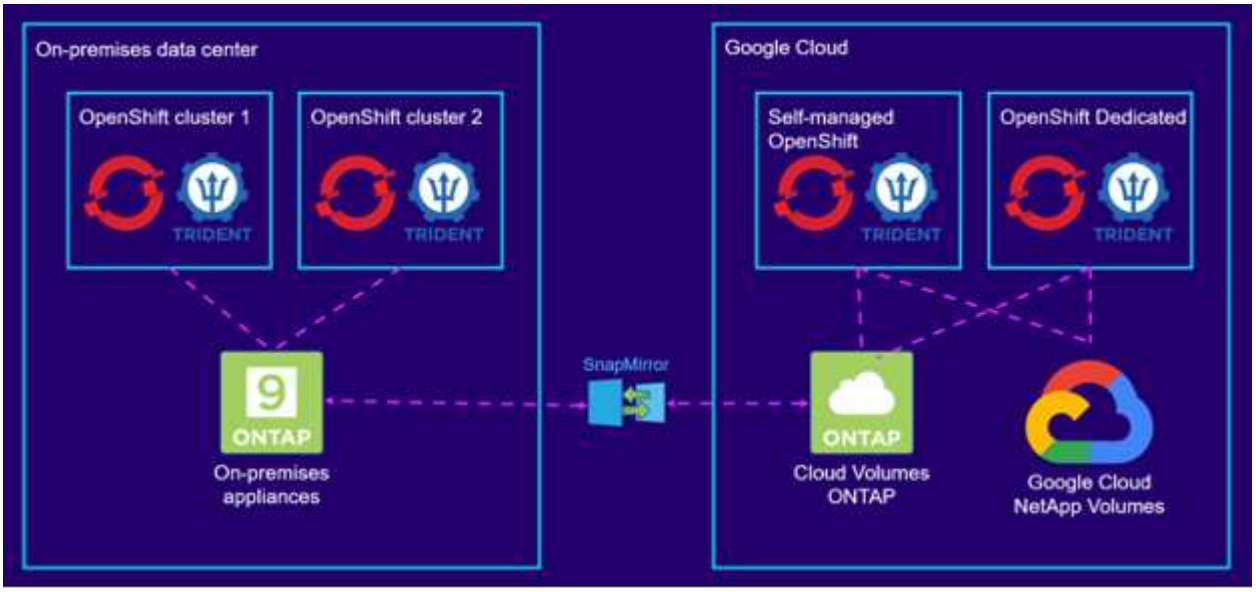
Cloud-Anbieter ermöglichen es Kubernetes/OpenShift-Clusteradministratoren heute, Knoten der Cluster zu erstellen, die zonenbasiert sind. Knoten können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über mehrere Regionen verteilt befinden. Um die Bereitstellung von Volumes für Workloads in einer Multizonenarchitektur zu erleichtern, verwendet Trident die CSI-Topologie. Mithilfe der CSI-Topologiefunktion kann der Zugriff auf Volumes basierend auf Regionen und Verfügbarkeitszonen auf eine Teilmenge von Knoten beschränkt werden. Verweisen"hier," für weitere Einzelheiten.

Kubernetes unterstützt zwei Volume-Bindungsmodi: – Wenn ***VolumeBindingMode*** **auf** ***Immediate*** (Standard) gesetzt ist, erstellt Trident das Volume ohne jegliche Topologieerkennung. Persistente Volumes werden ohne Abhängigkeit von den Planungsanforderungen des anfordernden Pods erstellt. – Wenn ***VolumeBindingMode*** **auf** ***WaitForFirstConsumer*** gesetzt ist, wird die Erstellung und Bindung eines persistenten Volumes für ein PVC verzögert, bis ein Pod, der das PVC verwendet, geplant und erstellt wurde. Auf diese Weise werden Volumes erstellt, die den Planungsbeschränkungen entsprechen, die durch die Topologieanforderungen erzwungen werden. Trident -Speicher-Backends können so konzipiert werden, dass Volumes basierend auf Verfügbarkeitszonen selektiv bereitgestellt werden (topologiebewusstes Backend). Für StorageClasses, die ein solches Backend verwenden, wird ein Volume nur erstellt, wenn es von einer Anwendung angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologiebewusste Speicherklasse) Siehe"hier," für weitere Einzelheiten.

Bereitstellen und Konfigurieren der Red Hat OpenShift Container Platform in Google Cloud

In diesem Abschnitt wird ein allgemeiner Workflow zum Einrichten und Verwalten von OpenShift-Clustern in GCP und zum Bereitstellen von zustandsbehafteten Anwendungen darauf beschrieben. Es zeigt die Verwendung von Google Cloud NetApp Volumes und NetApp Cloud Volumes ONTAP Speicher mit Hilfe von Trident zur Bereitstellung persistenter Volumes.

Hier ist ein Diagramm, das die auf GCP bereitgestellten und über ein VPN mit dem Rechenzentrum verbundenen Cluster zeigt.



Es gibt mehrere Möglichkeiten, Red Hat OpenShift Container-Plattformcluster in GCP bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentationslinks für die jeweils verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im"Ressourcenbereich" .

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

Installieren Sie einen OCP-Cluster auf GCP über die CLI

- Es ist sicherzustellen, dass Sie alle genannten Voraussetzungen erfüllt haben "hier,".
- Für die VPN-Konnektivität zwischen lokalen Standorten 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 Google Cloud Platform erstellt haben.
  - Die Remote-Netzwerk-IP-Adressen für Phase 2 können erst konfiguriert werden, nachdem das OpenShift-Cluster-Installationsprogramm ausgeführt wurde und die Infrastrukturkomponenten für den Cluster erstellt hat.
  - Das VPN in Google Cloud kann erst konfiguriert werden, nachdem die Infrastrukturkomponenten für den Cluster vom Installationsprogramm erstellt wurden.
- Installieren Sie jetzt den OpenShift-Cluster auf GCP.
  - Das Installationsprogramm und das Pull-Secret abrufen und den Cluster gemäß den in der Dokumentation beschriebenen Schritten einsetzen "hier,".
  - Die Installation erstellt ein VPC-Netzwerk in der Google Cloud Platform. Außerdem wird eine private Zone in Cloud DNS erstellt und A-Einträge hinzugefügt.
    - Verwenden Sie die CIDR-Blockadresse des VPC-Netzwerks, um pfsense zu konfigurieren und die VPN-Verbindung herzustellen. Stellen Sie sicher, dass die Firewalls richtig eingerichtet sind.
    - Fügen Sie A-Einträge im DNS der lokalen Umgebung hinzu, indem Sie die IP-Adresse in den A-Einträgen des Google Cloud DNS verwenden.
  - Die Installation des Clusters ist abgeschlossen und stellt eine Kubeconfig-Datei sowie einen Benutzernamen und ein Kennwort für die Anmeldung bei der Konsole des Clusters bereit.

Bereitstellen von Google Cloud NetApp Volumes

- Google Cloud NetApp Volumes können wie beschrieben zu Ihren Projekten hinzugefügt werden"hier," .

Deployment von Cloud Volumes ONTAP in GCP mit NetApp Console

- Installation eines Console Agenten in Google Cloud. Die Anweisungen finden Sie "hier,".
- Eine CVO-Instanz in Google Cloud kann mithilfe des Agenten eingesetzt werden. Die entsprechenden Anweisungen "hier," sind verfügbar.

Installieren Sie Trident im OCP-Cluster in GCP

- Es gibt viele Methoden, Trident wie gezeigt bereitzustellen "hier,".
- Für dieses Projekt wurde Trident durch die manuelle Bereitstellung von Trident Operator anhand der Anleitung "hier," installiert.
- Erstellen Sie ein Backend und Speicherklassen. Siehe Anweisungen"hier," .

Verwenden der CSI-Topologiefunktion von Trident für Mehrzonenarchitekturen

Cloud-Anbieter ermöglichen es Kubernetes/OpenShift-Clusteradministratoren heute, Knoten der Cluster zu erstellen, die zonenbasiert sind. Knoten können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über mehrere Regionen verteilt befinden. Um die Bereitstellung von Volumes für Workloads in einer Multizonenarchitektur zu erleichtern, verwendet Trident die CSI-Topologie. Mithilfe der CSI-Topologiefunktion kann der Zugriff auf Volumes basierend auf Regionen und Verfügbarkeitszonen auf eine Teilmenge von Knoten beschränkt werden. Verweisen"hier," für weitere Einzelheiten.

> Kubernetes unterstützt zwei Volume-Bindungsmodi: – Wenn ***VolumeBindingMode*** **auf** ***Immediate*** (Standard) gesetzt ist, erstellt Trident das Volume ohne jegliche Topologieerkennung. Persistente Volumes werden ohne Abhängigkeit von den Planungsanforderungen des anfordernden Pods erstellt. – Wenn ***VolumeBindingMode*** **auf** ***WaitForFirstConsumer*** gesetzt ist, wird die Erstellung und Bindung eines persistenten Volumes für ein PVC verzögert, bis ein Pod, der das PVC verwendet, geplant und erstellt wurde. Auf diese Weise werden Volumes erstellt, die den Planungsbeschränkungen entsprechen, die durch die Topologieanforderungen erzwungen werden. Trident -Speicher-Backends können so konzipiert werden, dass Volumes basierend auf Verfügbarkeitszonen selektiv bereitgestellt werden (topologiebewusstes Backend). Für StorageClasses, die ein solches Backend verwenden, wird ein Volume nur erstellt, wenn es von einer Anwendung angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologiebewusste Speicherklasse) Siehe"hier," für weitere Einzelheiten.

Demonstrationsvideo

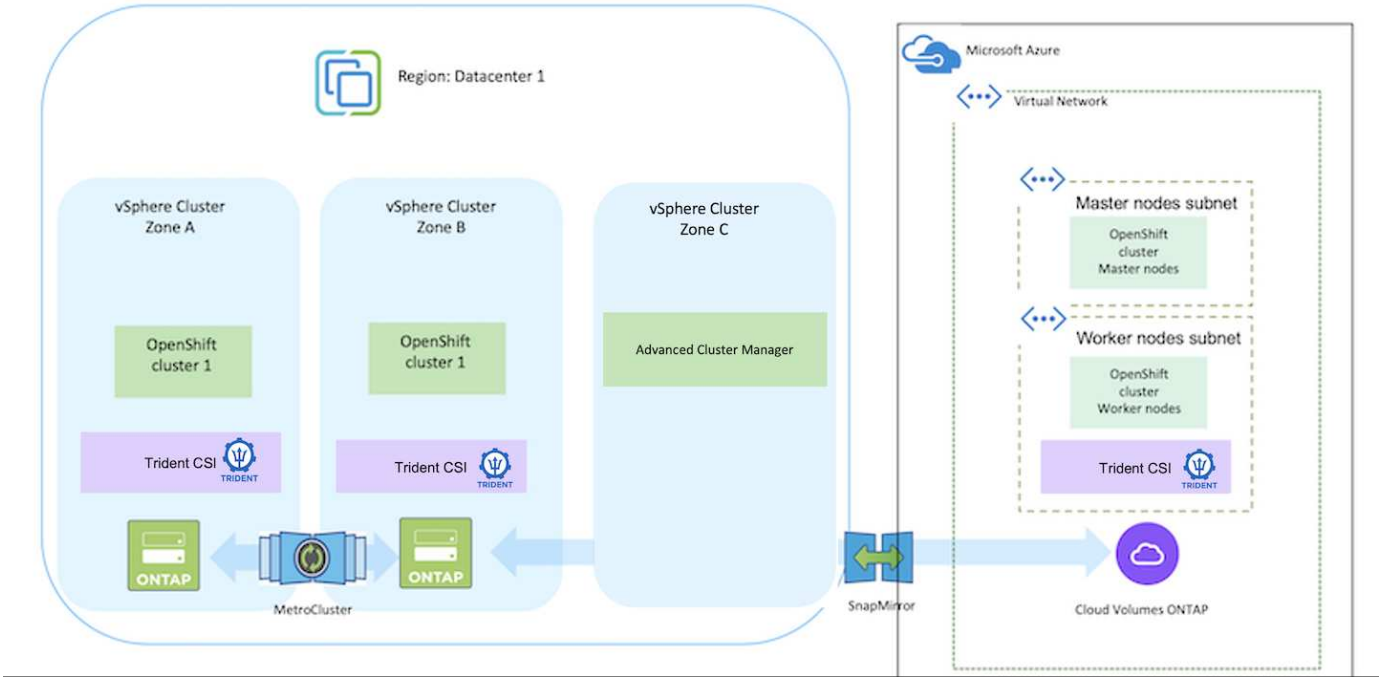
OpenShift-Clusterinstallation auf der Google Cloud Platform

Importieren von OpenShift-Clustern in Trident Protect

Bereitstellen und Konfigurieren der Red Hat OpenShift Container-Plattform auf Azure

In diesem Abschnitt wird ein allgemeiner Workflow zum Einrichten und Verwalten von OpenShift-Clustern in Azure und zum Bereitstellen zustandsbehafteter Anwendungen darauf beschrieben. Es zeigt die Verwendung von NetApp Cloud Volumes ONTAP Speicher mit Hilfe von Trident zur Bereitstellung persistenter Volumes. Es werden Details zur Verwendung von Trident Protect zur Durchführung von Datenschutz- und Migrationsaktivitäten für die Stateful-Anwendungen bereitgestellt.

Hier ist ein Diagramm, das die auf Azure bereitgestellten und über ein VPN mit dem Rechenzentrum verbundenen Cluster zeigt.



Es gibt mehrere Möglichkeiten, Red Hat OpenShift Container-Plattformcluster in Azure bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentationslinks für die jeweils verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im"Ressourcenbereich" .

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

▼ **Installieren Sie über die CLI einen OCP-Cluster auf Azure.**

- Es ist sicherzustellen, dass Sie alle genannten 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-Konnektivität zwischen dem lokalen Standort und Azure wurde eine pfsense-VM erstellt und konfiguriert. Anweisungen hierzu finden Sie unter"hier," .
- Die Beschaffung des Installationsprogramms und des Pull Secret sowie das Einsetzen des Clusters erfolgen gemäß den in der Dokumentation beschriebenen Schritten "hier,".
- Die Installation des Clusters ist abgeschlossen und stellt eine Kubeconfig-Datei sowie einen Benutzernamen und ein Kennwort für die Anmeldung bei der Konsole des Clusters bereit.

Unten finden Sie ein Beispiel für eine install-config.yaml-Datei.

```
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:
```

▼ **Deployment von Cloud Volumes ONTAP in Azure mit NetApp Console.**

- Installation eines NetApp Console Agent in Azure. Die entsprechenden Anweisungen "hier," finden Sie hier.
- Das Einsetzen einer CVO-Instanz in Azure erfolgt mithilfe des Agenten. Die Anweisungen finden Sie "hier,".

Verwenden der CSI-Topologiefunktion von Trident für Mehrzonenarchitekturen

Cloud-Anbieter ermöglichen es Kubernetes/OpenShift-Clusteradministratoren heute, Knoten der Cluster zu erstellen, die zonenbasiert sind. Knoten können sich in verschiedenen Verfügbarkeitszonen innerhalb einer Region oder über mehrere Regionen verteilt befinden. Um die Bereitstellung von Volumes für Workloads in einer Multizonenarchitektur zu erleichtern, verwendet Trident die CSI-Topologie. Mithilfe der CSI-Topologiefunktion kann der Zugriff auf Volumes basierend auf Regionen und Verfügbarkeitszonen auf eine Teilmenge von Knoten beschränkt werden. Verweisen"hier," für weitere Einzelheiten.

> Kubernetes unterstützt zwei Volume-Bindungsmodi: – Wenn ***VolumeBindingMode*** **auf** ***Immediate*** (Standard) gesetzt ist, erstellt Trident das Volume ohne jegliche Topologieerkennung. Persistente Volumes werden ohne Abhängigkeit von den Planungsanforderungen des anfordernden Pods erstellt. – Wenn ***VolumeBindingMode*** **auf** ***WaitForFirstConsumer*** gesetzt ist, wird die Erstellung und Bindung eines persistenten Volumes für ein PVC verzögert, bis ein Pod, der das PVC verwendet, geplant und erstellt wurde. Auf diese Weise werden Volumes erstellt, die den Planungsbeschränkungen entsprechen, die durch die Topologieanforderungen erzwungen werden. Trident -Speicher-Backends können so konzipiert werden, dass Volumes basierend auf Verfügbarkeitszonen selektiv bereitgestellt werden (topologiebewusstes Backend). Für StorageClasses, die ein solches Backend verwenden, wird ein Volume nur erstellt, wenn es von einer Anwendung angefordert wird, die in einer unterstützten Region/Zone geplant ist. (Topologiebewusste Speicherklasse) Siehe"hier," für weitere Einzelheiten.

Datenschutz mit Trident Protect

Für Details zum Schutz und zur Migration von Container-Workloads mit Trident Protect lesen Sie bitte den folgenden Abschnitt: - "Schützen und migrieren Sie Container-Apps mit Trident Protect"

Hybrid Cloud mit vom Anbieter verwalteten Komponenten

NetApp -Lösung mit verwalteten Red Hat OpenShift Container-Plattform-Workloads

Kunden sind möglicherweise „in der Cloud geboren“ oder befinden sich an einem Punkt ihrer Modernisierung, an dem sie bereit sind, einige ausgewählte oder alle Workloads aus ihren Rechenzentren in die Cloud zu verschieben. Sie können sich für die Ausführung ihrer Workloads für die Verwendung von vom Anbieter verwalteten OpenShift-Containern und vom Anbieter verwaltetem NetApp -Speicher in der Cloud entscheiden. Sie sollten die verwalteten Red Hat OpenShift-Containercluster in der Cloud planen und bereitstellen, um eine erfolgreiche produktionsbereite Umgebung für ihre Container-Workloads zu schaffen. NetApp bietet vollständig verwaltete Speicherangebote für Managed Red Hat-Lösungen in allen drei führenden öffentlichen Clouds.

- Amazon FSx for NetApp ONTAP (FSx ONTAP)*

FSx ONTAP bietet Datenschutz, Zuverlässigkeit und Flexibilität für Containerbereitstellungen in AWS. Trident dient als dynamischer Speicherbereitsteller, um den persistenten FSx ONTAP -Speicher für die zustandsbehafteten Anwendungen der Kunden zu nutzen.

Da ROSA im HA-Modus mit über mehrere Verfügbarkeitszonen verteilten Control Plane-Knoten bereitgestellt werden kann, kann FSx ONTAP auch mit der Multi-AZ-Option bereitgestellt werden, die hohe Verfügbarkeit bietet und vor AZ-Ausfällen schützt.

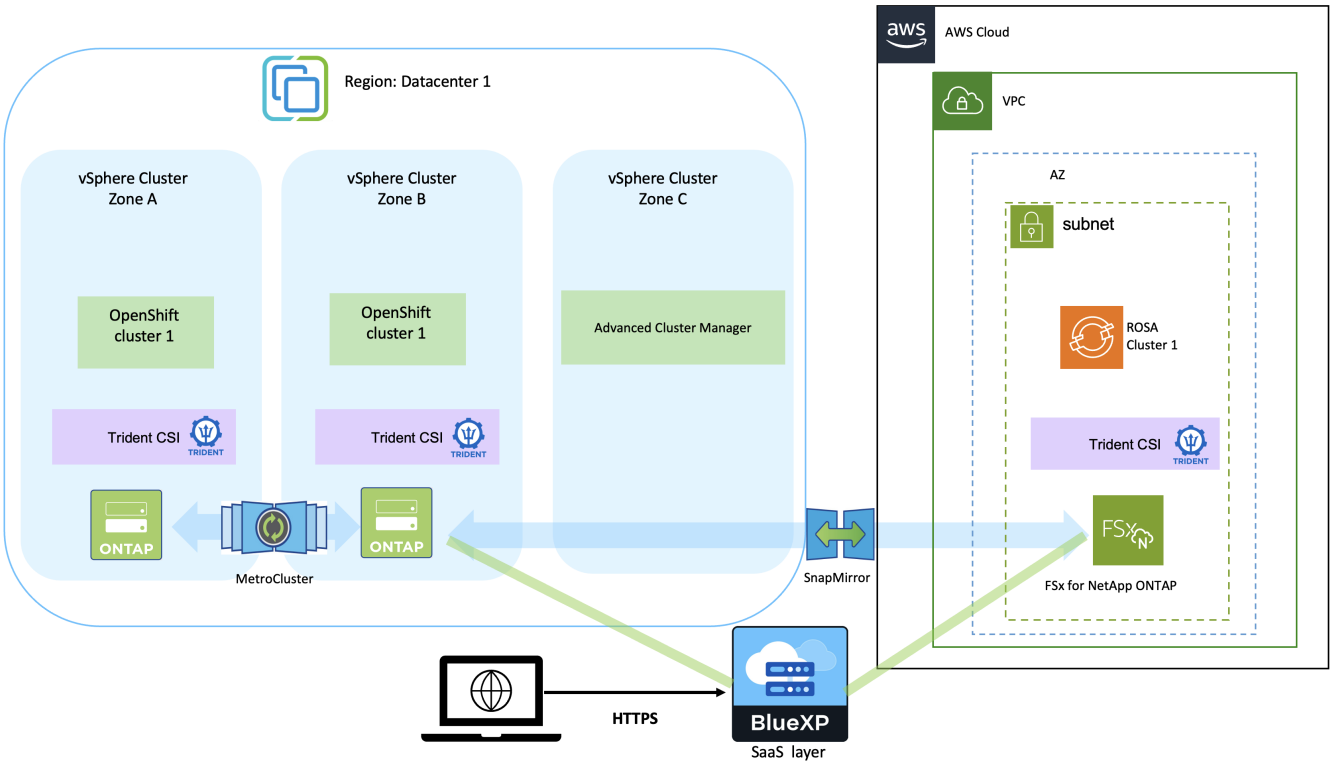
- Google Cloud NetApp Volumes*

Red Hat OpenShift Dedicated ist eine vollständig verwaltete Anwendungsplattform, mit der Sie Anwendungen in der gesamten Hybrid Cloud schnell erstellen, bereitstellen und skalieren können. Google Cloud NetApp Volumes bietet persistente Volumes und bringt die gesamte Palette der Enterprise-Datenverwaltungsfunktionen von ONTAP in OpenShift-Bereitstellungen in Google Cloud.

Bereitstellen und Konfigurieren der Managed Red Hat OpenShift Container-Plattform auf AWS

Dieser Abschnitt beschreibt einen allgemeinen Workflow für die Einrichtung der Managed Red Hat OpenShift Cluster auf AWS(ROSA). Er zeigt die Verwendung von Managed Amazon FSx for NetApp ONTAP (FSx ONTAP) als Storage-Backend durch Trident zur Bereitstellung persistenter Volumes. Es werden Details zum Deployment von FSx ONTAP auf AWS mithilfe von NetApp Console bereitgestellt. Außerdem werden Details zur Verwendung von NetApp Console und OpenShift GitOps (Argo CD) zur Durchführung von Datensicherungs- und Migrationsaktivitäten für die zustandsbehafteten Anwendungen auf ROSA Clustern bereitgestellt.

Hier ist ein Diagramm, das die auf AWS bereitgestellten ROSA-Cluster darstellt, die FSx ONTAP als Backend-Speicher verwenden.



Diese Lösung wurde durch die Verwendung von zwei ROSA-Clustern in zwei VPCs in AWS verifiziert. Jeder ROSA-Cluster wurde mithilfe von Trident in FSx ONTAP integriert. Es gibt mehrere Möglichkeiten, ROSA-Cluster und FSx ONTAP in AWS bereitzustellen. Diese allgemeine Beschreibung des Setups enthält Dokumentationslinks für die jeweils verwendete Methode. Weitere Methoden finden Sie in den entsprechenden Links im"Ressourcenbereich" .

Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

Installieren Sie ROSA-Cluster

- Erstellen Sie zwei VPCs und richten Sie eine VPC-Peering-Konnektivität zwischen den VPCs ein.
- Anweisungen zur Installation von ROSA Clustern finden Sie unter "hier,".

Installieren Sie FSx ONTAP

- Die Installation von FSx ONTAP auf den VPCs erfolgt über die NetApp Console. Informationen "hier," zur Erstellung eines NetApp Console Kontos und zu den ersten Schritten finden Sie in der Dokumentation. Informationen "hier," zur Installation von FSx ONTAP finden Sie in der Dokumentation. Informationen "hier," zum Erstellen eines Connectors in AWS zum Managen von FSx ONTAP finden Sie in der Dokumentation.
- Stellen Sie FSx ONTAP mit AWS bereit. Verweisen"hier," zur Bereitstellung mithilfe der AWS-Konsole.

Installieren Sie Trident auf ROSA-Clustern (mithilfe des Helm-Diagramms).

- Für die Installation von Trident auf ROSA Clustern wird das Helm Chart verwendet. Der Link zur Dokumentation befindet sich hier.

Integration von FSx ONTAP mit Trident für ROSA-Cluster

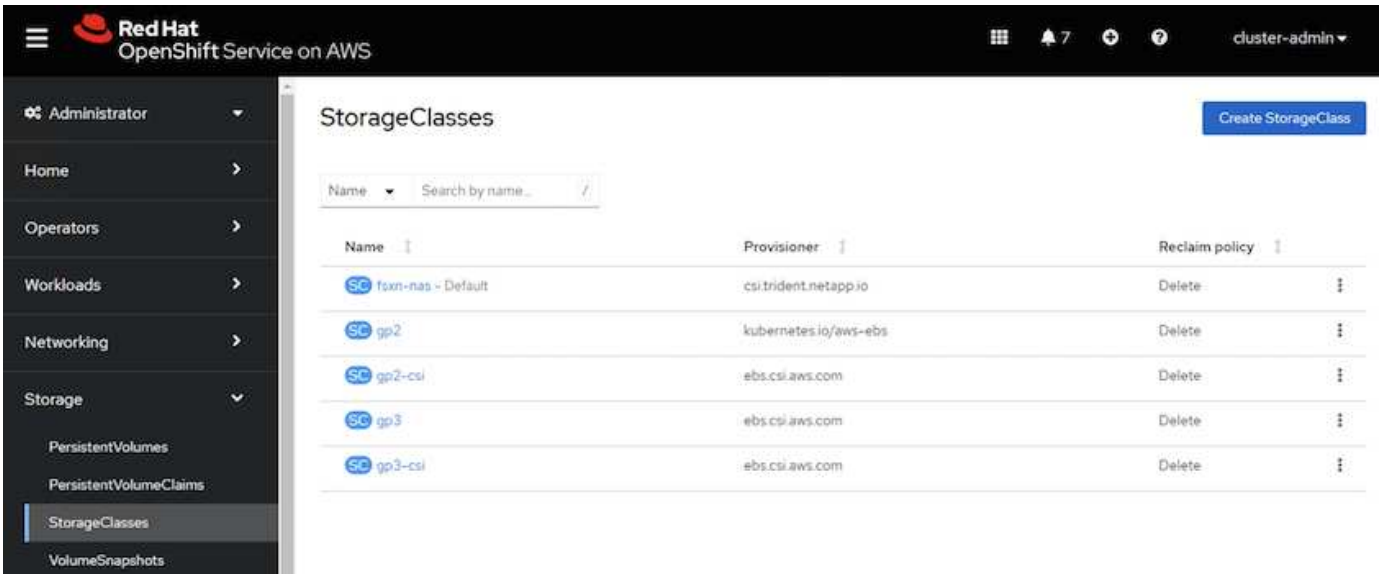
OpenShift GitOps kann verwendet werden, um Trident CSI auf allen verwalteten Clustern bereitzustellen, da diese mithilfe von ApplicationSet bei ArgoCD registriert werden.

```yaml
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
```



Erstellen Sie Backend- und Speicherklassen mit Trident (für FSx ONTAP)

- Verweisen"hier," für Details zum Erstellen von Backend- und Speicherklassen.
- Legen Sie die für FsxN mit Trident CSI erstellte Speicherklasse als Standard aus der OpenShift-Konsole fest. Siehe Screenshot unten:



Bereitstellen einer Anwendung mit OpenShift GitOps (Argo CD)

- Installation des OpenShift GitOps Operators auf dem Cluster. Verweis auf die Anweisungen "hier,".
- SetUp einer neuen Argo CD Instanz für den Cluster. Verweis auf die Anweisungen "hier,".

Die Konsole von Argo CD wird geöffnet und eine App wird bereitgestellt. Als Beispiel kann eine Jenkins App mit Argo CD unter Verwendung eines Helm Chart bereitgestellt werden. Beim Erstellen der Anwendung

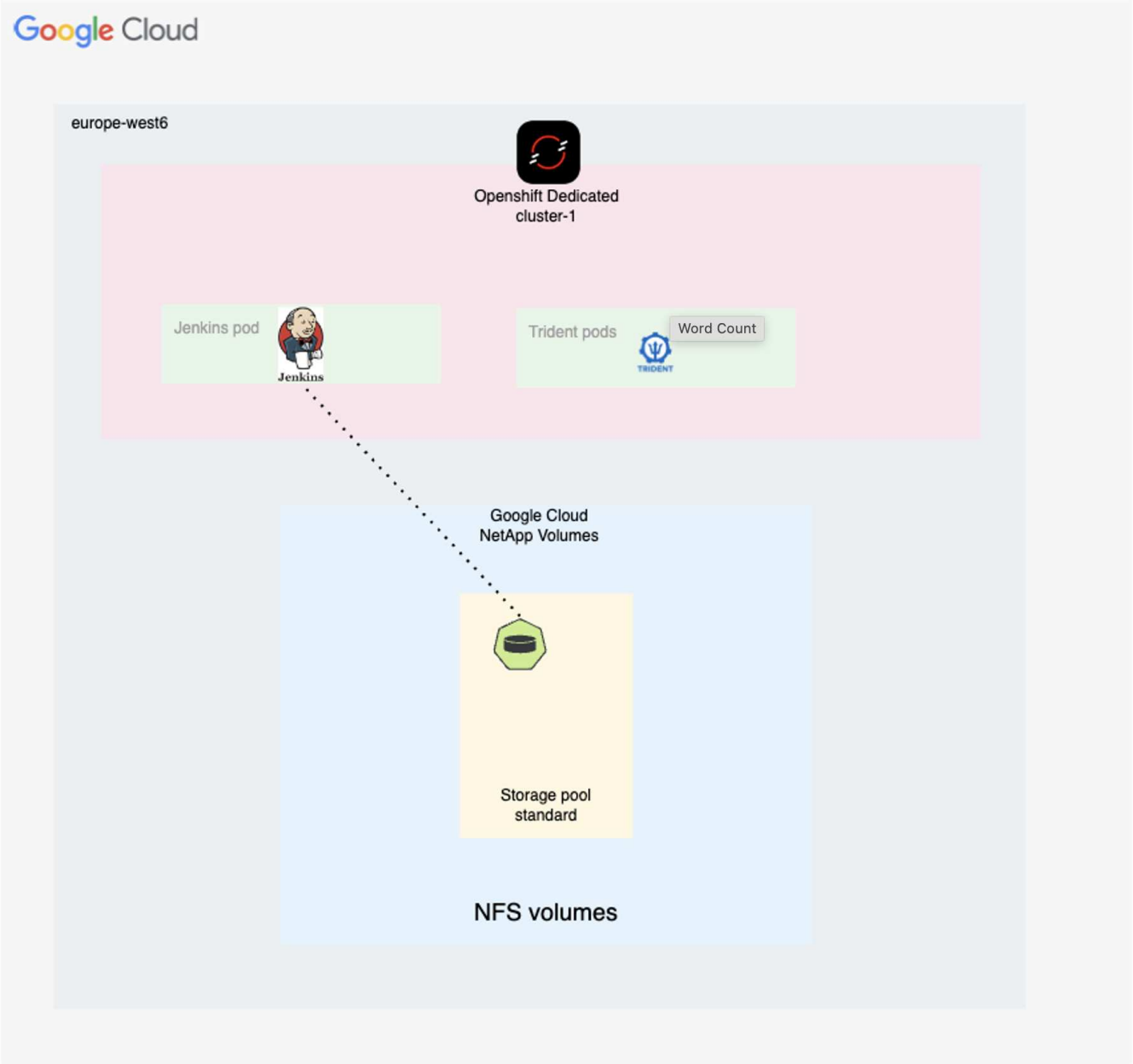
wurden die folgenden Details angegeben: Project: default cluster: 'https://kubernetes.default.svc'[] (without the quotes) Namespace: Jenkins The url for the Helm Chart: 'https://charts.bitnami.com/bitnami'[] (without the quotes)

Helm-Parameter: global.storageClass: fsxn-nas

Bereitstellen und Konfigurieren von OpenShift Dedicated auf Google Cloud mit Google Cloud NetApp Volumes

In diesem Abschnitt wird ein allgemeiner Workflow zum Einrichten von OpenShift Dedicated (OSD)-Clustern auf der Google Cloud-Plattform beschrieben. Es zeigt, wie NetApp Trident Google Cloud NetApp Volumes als Speicher-Backend verwendet, um persistente Volumes für zustandsbehaftete Anwendungen bereitzustellen, die mit Kubernetes ausgeführt werden.

Hier ist ein Diagramm, das einen OSD-Cluster darstellt, der in Google Cloud bereitgestellt wird und NetApp Volumes als Backend-Speicher verwendet.



Der Einrichtungsprozess kann in die folgenden Schritte unterteilt werden:

Installieren Sie OSD-Cluster in Google Cloud

- Wenn Sie eine vorhandene VPC für den Cluster verwenden möchten, müssen Sie die VPC, zwei Subnetze, einen Cloud-Router und zwei GCP-Cloud-NATs für den OSD-Cluster erstellen. Verweisen"hier," Anweisungen hierzu finden Sie unter.
- Anleitungen zur Installation von OSD Clustern auf GCP mit dem Abrechnungsmodell Customer Cloud Subscription (CCS) finden Sie "hier,". OSD ist auch im Google Cloud Marketplace verfügbar. Ein Video zur Installation von OSD mit der Google Cloud Marketplace-Lösung befindet sich "hier,".

Google Cloud NetApp Volumes aktivieren

- Verweisen"hier," Informationen zum Einrichten des Zugriffs auf Google Cloud NetApp Volumes. Befolgen Sie alle Schritte bis einschließlich
- Erstellen Sie einen Speicherpool. Verweisen"hier," Informationen zum Einrichten eines Speicherpools auf Google Cloud NetApp Volumes. Innerhalb des Speicherpools werden Volumes für die zustandsbehafteten

Kubernetes-Anwendungen erstellt, die auf OSD ausgeführt werden.

Installieren Sie Trident auf OSD-Clustern (mithilfe des Helm-Diagramms).

- Verwenden Sie ein Helm-Chart, um Trident auf OSD-Clustern zu installieren. Siehe "hier," für Anweisungen zur Installation des Helm-Charts.

Integration von NetApp Volumes mit NetApp Trident für OSD-Cluster

Erstellen Sie Backend- und Speicherklassen mit Trident (für Google Cloud NetApp Volumes)

- Weitere Informationen zum Erstellen des Backends finden Sie hier.
- Wenn eine der aktuellen Speicherklassen in Kubernetes als Standard markiert ist, entfernen Sie diese Anmerkung, indem Sie die Speicherklasse bearbeiten.
- Erstellen Sie mit dem Trident CSI Provisioner mindestens eine Speicherklasse für NetApp -Volumes. Machen Sie mithilfe einer Anmerkung genau eine der Speicherklassen zum Standard. Dadurch kann ein PVC diese Speicherklasse verwenden, wenn sie im PVC-Manifest nicht explizit aufgerufen wird. Ein Beispiel mit der Anmerkung wird unten angezeigt.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

Bereitstellen einer Anwendung mit OpenShift GitOps (Argo CD)

- Installation des OpenShift GitOps Operators auf dem Cluster. Die Anweisungen "hier," stehen zur Verfügung.
- SetUp einer neuen Argo CD Instanz für den Cluster. Verweis auf die Anweisungen "hier,".

Die Konsole von Argo CD wird geöffnet und eine App wird bereitgestellt. Als Beispiel kann eine Jenkins App mit Argo CD unter Verwendung eines Helm Chart bereitgestellt werden. Beim Erstellen der Anwendung wurden die folgenden Details angegeben: Project: default cluster: 'https://kubernetes.default.svc'[] (without the quotes) Namespace: Jenkins The url for the Helm Chart: 'https://charts.bitnami.com/bitnami'[] (without the quotes)

Datenschutz

Für Details zum Schutz und zur Migration von Container-Workloads mit Trident Protect lesen Sie bitte den folgenden Abschnitt: - "Schützen und migrieren Sie Container-Apps mit Trident Protect"

Zusätzliche NetApp Hybrid Multicloud-Lösungen für Red Hat OpenShift-Workloads

Die folgenden zusätzlichen Lösungen sind verfügbar:

- "Red Hat OpenShift Container-Lösung vor Ort"
- "Red Hat OpenShift Service auf AWS Containerlösung"
- "Red Hat OpenShift Virtualisierungslösung vor Ort"
- "Red Hat OpenShift Service auf AWS Virtualisierungslösung"

Schützen Sie Daten mit Trident Protect

Datenschutz für Container-Apps in OpenShift Container Platform mit Trident Protect

Dieser Abschnitt des Referenzdokuments bietet Details zur Erstellung von Snapshots und Backups von Container Apps mit Trident Protect. NetApp Trident Protect bietet erweiterte Funktionen für das Management von Anwendungsdaten, die die Funktionalität und Verfügbarkeit zustandsbehafteter Kubernetes-Anwendungen verbessern, die durch NetApp ONTAP-Speichersysteme und den NetApp Trident CSI Storage Provisioner unterstützt werden. Trident Protect erstellt Anwendungssnapshots und Backups. Das bedeutet, dass Snapshots und Backups nicht nur für Anwendungsdaten in persistenten Volumes, sondern auch für Anwendungsmetadaten erstellt werden. Die von Trident Protect erstellten Snapshots und Backups können in einem der folgenden Objektspeicher gespeichert und zu einem späteren Zeitpunkt daraus wiederhergestellt werden.

- AWS S3
- Azure Blob-Speicher
- Google Cloud-Speicher
- ONTAP S3
- StorageGrid
- Jeder andere S3-kompatible Speicher

Trident Protect nutzt das Kubernetes-Modell der rollenbasierten Zugriffssteuerung (RBAC). Standardmäßig stellt Trident Protect einen einzelnen System-Namespace namens trident-protect und das zugehörige Standard-Dienstkonto bereit. Wenn Sie eine Organisation mit vielen Benutzern oder spezifischen Sicherheitsanforderungen haben, können Sie die RBAC-Funktionen von Trident Protect nutzen, um den Zugriff auf Ressourcen und Namespaces detaillierter zu steuern.

Weitere Informationen zu RBAC in Trident Protect finden Sie im "Trident Protect Dokumentation"

> Der Clusteradministrator hat Zugriff auf Ressourcen im Standard-Trident-Protect-Namespace und kann auch auf Ressourcen in allen anderen Namespaces zugreifen. Benutzer können im Trident-Protect-Namespace keine benutzerdefinierten Ressourcen (CRs) für die Anwendungsdatenverwaltung wie Snapshot- und Backup-CRs erstellen. Als bewährte Methode müssen Benutzer diese CRs im Anwendungsnamespace erstellen.

Trident Protect kann mithilfe der in der Dokumentation bereitgestellten Anweisungen installiert werden "hier,".

In diesem Abschnitt wird der Workflow für den Datenschutz von Containeranwendungen und die Wiederherstellung der Anwendungen mit Trident Protect gezeigt. 1. Snapshot-Erstellung (auf Anforderung oder geplant) 2. Wiederherstellung aus Snapshot (Wiederherstellung im selben oder in einem anderen Namespace) 3. Backup-Erstellung 4. Wiederherstellung aus Backup

▼ **Voraussetzung**

Vor dem Erstellen der Snapshots und Backups für eine Anwendung muss der Objektspeicher in Trident Protect konfiguriert werden, um die Snapshots und Backups zu speichern. Dies geschieht mithilfe des Bucket-CR. Nur Administratoren können einen Bucket-CR erstellen und konfigurieren. Der Bucket-CR ist in Trident Protect als AppVault bekannt. AppVault-Objekte sind die deklarative Kubernetes-Workflow-Repräsentation eines Speicher-Buckets. Ein AppVault-CR enthält die Konfigurationen, die erforderlich sind, damit ein Bucket in Schutzvorgängen wie Backups, Snapshots, Wiederherstellungsvorgängen und SnapMirror-Replikation verwendet werden kann.

In diesem Beispiel zeigen wir die Verwendung von ONTAP S3 als Objektspeicher. Hier ist der Workflow zum Erstellen von AppVault CR für ONTAP S3: 1. Erstellen Sie einen S3-Objektspeicherserver in der SVM im ONTAP-Cluster. 2. Erstellen Sie einen Bucket im Objektspeicherserver. 3. Erstellen Sie einen S3-Benutzer in der SVM. Bewahren Sie den Zugriffsschlüssel und den geheimen Schlüssel an einem sicheren Ort auf. 4. Erstellen Sie in OpenShift ein Secret, um die ONTAP S3-Anmeldeinformationen zu speichern. 5. Erstellen Sie ein AppVault-Objekt für ONTAP S3

Trident Protect AppVault für ONTAP S3 konfigurieren

Beispiel-YAML-Datei zur Konfiguration von Trident Protect mit ONTAP S3 als AppVault

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
```

```
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+------------------+----------+-----------+------+-------+
|       NAME       | PROVIDER |   STATE   | AGE  | ERROR |
+------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

Beispiel-YAML-Datei zum Installieren der PostgreSQL-App

```
postgres.yaml
apiVersion: apps/v1
kind: Deployment
```

```
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 5Gi
```

```
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```

```
[root@localhost RedHat]# tp get app -n postgres
+--------------+------------+-------+-----+
|     NAME     | NAMESPACES | STATE | AGE |
+--------------+------------+-------+-----+
| postgres-app | postgres   | Ready | 24s |
+--------------+------------+-------+-----+
[root@localhost RedHat]#
```

▼ **Snapshots erstellen**

Erstellen eines On-Demand-Snapshots

```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-
s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+-----------------+--------------+-----------+-----+-------+
|      NAME       |   APP REF    |   STATE   | AGE | ERROR |
+-----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+-----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```

```
[root@localhost DataProtection]# oc get all,pvc,volumesnapshot -n postgres
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
Warning: kubevirt.io/v1 VirtualMachineInstancePresets is now deprecated and will be removed in v2.
NAME                            READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-jfx49     1/1     Running   0          3h47m

NAME               TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/postgres   ClusterIP   172.30.132.112   <none>        5432/TCP   3h47m

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/postgres   1/1     1            1           3h47m

NAME                                  DESIRED   CURRENT   READY   AGE
replicaset.apps/postgres-cd9d6ccb     1         1         1       3h47m

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAG
ECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   8Gi        RWO            sc-zon
ea-nas   <unset>                 4h40m
persistentvolumeclaim/postgres-pvc                  Bound    pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   5Gi        RWO            sc-zon
ea-nas   <unset>                 3h47m

NAME                                                                                                                                READYTO
USE   SOURCEPVC                  SOURCESNAPSHOTCONTENT   RESTORESIZE   SNAPSHOTCLASS           SNAPSHOTCONTENT
          CREATIONTIME   AGE
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true
      postgres-pvc                                      53676Ki       trident-snapshotclass   snapcontent-796ea7f8-59a0-493e-bbd8-3a
e76fe9036c   13m            13m
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true
      data-postgres-postgresql-0                        368Ki         trident-snapshotclass   snapcontent-86a464d4-ffd8-4279-9cf7-88
88a097c001   13m            13m
```

Erstellen eines Zeitplans Mit dem folgenden Befehl werden täglich um 15:33 Uhr Snapshots erstellt und zwei Snapshots und Backups aufbewahrt.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+-----+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE | ERROR |
+-----------+--------------+----------------------+---------+-------+-----+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 17s |       |
+-----------+--------------+----------------------+---------+-------+-----+-------+
[root@localhost DataProtection]#
```

Erstellen eines Zeitplans mit YAML

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+-------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP     |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+-------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+-------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

Sie können die nach diesem Zeitplan erstellten Snapshots sehen.

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

Außerdem werden Volume-Snapshots erstellt.

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                READYTOUSE   SOURCEPVC
                                CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ Löschen Sie die Anwendung, um den Verlust der Anwendung zu simulieren

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ Wiederherstellen aus Snapshot im selben Namespace

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

Die Anwendung und ihr PVC werden im selben Namespace wiederhergestellt.

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                     READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                 Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ **Wiederherstellen aus Snapshot in einem anderen Namespace**

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |     APPVAULT       |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

Sie können sehen, dass die Anwendung in einem neuen Namespace wiederhergestellt wurde.

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                          READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                 Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ **Backups erstellen**

Erstellen eines On-Demand-Backups

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+-----------------------------+-------------+-----------+--------+-------+
|            NAME             |   APP REF   |   STATE   |  AGE   | ERROR |
+-----------------------------+-------------+-----------+--------+-------+
| backup1                     | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300  | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300  | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1            | postgres-app | Completed | 6m19s  |       |
+-----------------------------+-------------+-----------+--------+-------+
```

Zeitplan für die Sicherung erstellen

Die täglichen und stündlichen Sicherungen in der obigen Liste werden anhand des zuvor eingerichteten Zeitplans erstellt.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ **Wiederherstellen aus einer Sicherung**

Löschen Sie die Anwendung und PVCs, um einen Datenverlust zu simulieren.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Im selben Namespace wiederherstellen #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore „postgres-bir“ erstellt.

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

Die Anwendung und die PVCs werden im selben Namespace wiederhergestellt.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w     1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                  Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

In einem anderen Namespace wiederherstellen Erstellen Sie einen neuen Namespace. Stellen Sie aus einer Sicherung im neuen Namespace wieder her.

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p     1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                  Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ **Migrieren von Anwendungen**

Um eine Anwendung auf einen anderen Cluster zu klonen oder zu migrieren (führen Sie einen clusterübergreifenden Klon durch), erstellen Sie eine Sicherung auf dem Quell-Cluster und stellen Sie die Sicherung anschließend auf einem anderen Cluster wieder her. Stellen Sie sicher, dass Trident Protect auf dem Ziel-Cluster installiert ist.

Führen Sie im Quellcluster die im folgenden Bild gezeigten Schritte aus:

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

Wechseln Sie vom Quellcluster zum Zielcluster. Stellen Sie dann sicher, dass vom Zielclusterkontext aus auf den AppVault zugegriffen werden kann, und rufen Sie den AppVault-Inhalt vom Zielcluster ab.

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+------------------+----------+-----------+------+-------+
|       NAME       | PROVIDER |   STATE   | AGE  | ERROR |
+------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+--------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-----------------------------------------------------------------------------+
|    CLUSTER   |     APP     |  TYPE  |            NAME             |        TIMESTAMP        |
                  PATH                                                       |
+--------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
-----------------------------------------------------------------------------+
| ocp-cluster11 | bbox        | backup | bboxbackup1                 | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                                                              |
| ocp-cluster11 | postgres-app | backup | backup1                     | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3                                                           |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300  | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd  |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300  | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d  |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031 |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1    | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3    |
```

Verwenden Sie den Sicherungspfad aus der Liste und erstellen Sie ein Backuprestore-CR-Objekt, wie im folgenden Befehl gezeigt.

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+---------+-------+
|           NAME           |      APPVAULT      |   STATE   |   AGE   | ERROR |
+--------------------------+--------------------+-----------+---------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+---------+-------+
```

Sie können jetzt sehen, dass die Anwendungspods und die PVCs im Zielcluster erstellt werden.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                     READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                       STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                 Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Schützen Sie VMs in Red Hat OpenShift Virtualization mit Trident Protect

Schützen Sie VMs in OpenShift Virtualization mithilfe von Snapshots und Backups. Dieses Verfahren umfasst die Erstellung eines AppVault mithilfe von ONTAP S3 Objektspeicher, die Konfiguration von Trident Protect zur Erfassung von VM-Daten, einschließlich Kubernetes-Ressourcenobjekten, persistenten Volumes und internen Images, sowie die Wiederherstellung der Daten bei Bedarf.

Virtuelle Maschinen in der OpenShift-Virtualisierungsumgebung sind containerisierte Anwendungen, die in den Worker-Knoten Ihrer OpenShift-Containerplattform ausgeführt werden. Es ist wichtig, die VM-Metadaten sowie die persistenten Datenträger der VMs zu schützen, damit Sie sie wiederherstellen können, wenn sie verloren gehen oder beschädigt werden.

Die persistenten Datenträger der OpenShift Virtualisierungs-VMs können durch ONTAP-Speicher, der in den OpenShift Cluster integriert ist, unterstützt werden "Trident CSI". In diesem Abschnitt verwenden wir "Trident Protect", um Snapshots und Backups von VMs einschließlich ihrer Datenvolumes im ONTAP Objektspeicher zu erstellen.

Bei Bedarf stellen wir dann eine Wiederherstellung aus einem Snapshot oder einem Backup her.

Trident Protect ermöglicht Snapshots, Backups, Wiederherstellungen und die Notfallwiederherstellung von Anwendungen und VMs auf einem OpenShift Cluster. Für OpenShift Virtualization VMs können mit Trident Protect Kubernetes-Ressourcenobjekte, persistente Volumes und interne Images geschützt werden.

Im Folgenden sind die Versionen der verschiedenen Komponenten aufgeführt, die für die Beispiele in diesem Abschnitt verwendet wurden.

- "OpenShift Cluster 4.17"
- "OpenShift-Virtualisierung installiert über OpenShift Virtualization Operator, bereitgestellt von Red Hat"
- "Trident 25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

Erstellen Sie AppVault für Objektspeicherung

▼ **AppVault erstellen**

Vor dem Erstellen von Snapshots und Backups für eine Anwendung oder eine VM muss der Objektspeicher in Trident Protect konfiguriert werden, um die Snapshots und Backups zu speichern. Dies geschieht mithilfe des Bucket-CR. Nur Administratoren können einen Bucket-CR erstellen und konfigurieren. Der Bucket-CR ist in Trident Protect als AppVault bekannt. AppVault-Objekte sind die deklarative Kubernetes-Workflow-Darstellung eines Speicher-Buckets. Ein AppVault-CR enthält die Konfigurationen, die erforderlich sind, damit ein Bucket in Schutzvorgängen wie Backups, Snapshots, Wiederherstellungsvorgängen und SnapMirror-Replikation verwendet werden kann.

In diesem Beispiel zeigen wir die Verwendung von ONTAP S3 als Objektspeicher. Hier ist der Workflow zum Erstellen eines AppVault CR für ONTAP S3: 1. Erstellen Sie einen S3-Objektspeicherserver in der SVM im ONTAP Cluster. 2. Erstellen Sie einen Bucket im Objektspeicherserver. 3. Erstellen Sie einen S3-Benutzer in der SVM. Bewahren Sie den Zugriffsschlüssel und den geheimen Schlüssel an einem sicheren Ort auf. 4. Erstellen Sie in OpenShift ein Secret, um die ONTAP S3-Anmeldeinformationen zu speichern. 5. Erstellen Sie ein AppVault Objekt für ONTAP S3

Trident Protect AppVault für ONTAP S3 konfigurieren

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
```

```
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+-------------------+----------+-----------+-------+---------+-------+
|       NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+-------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault | OntapS3  | Available |       |         | 8d17h |
+-------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

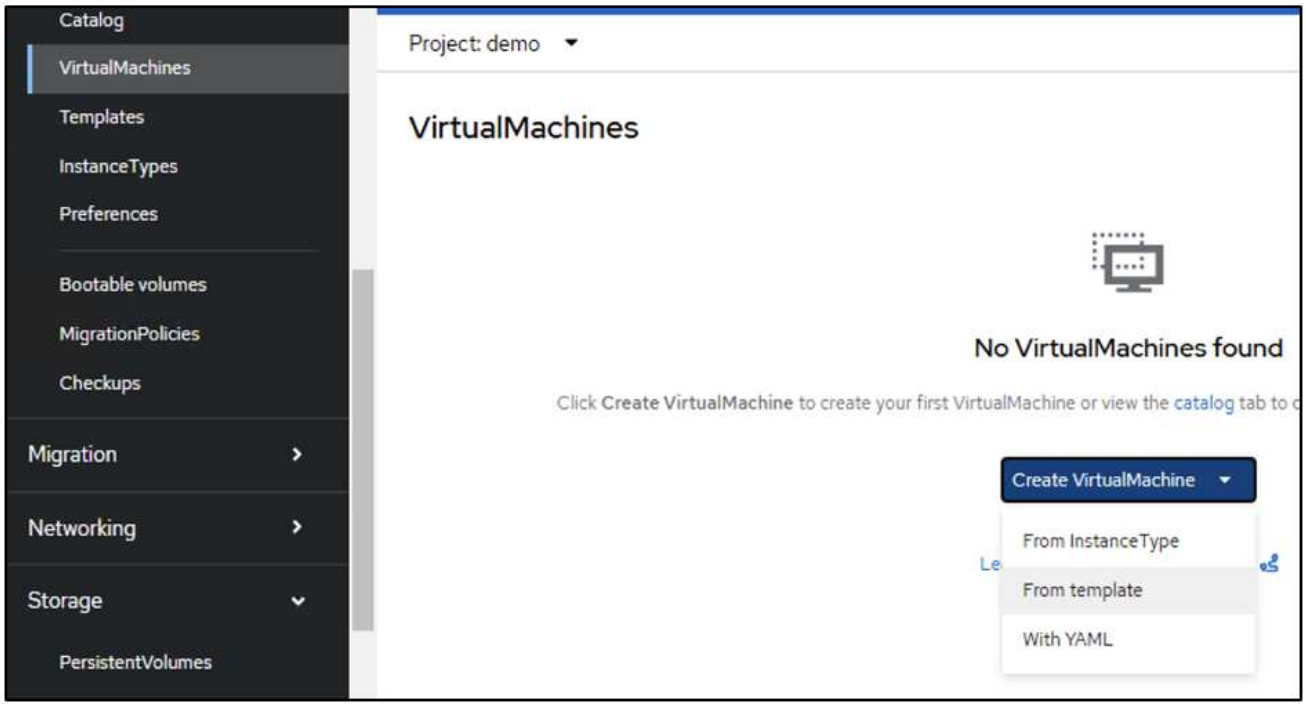
Erstellen einer VM in OpenShift Virtualization

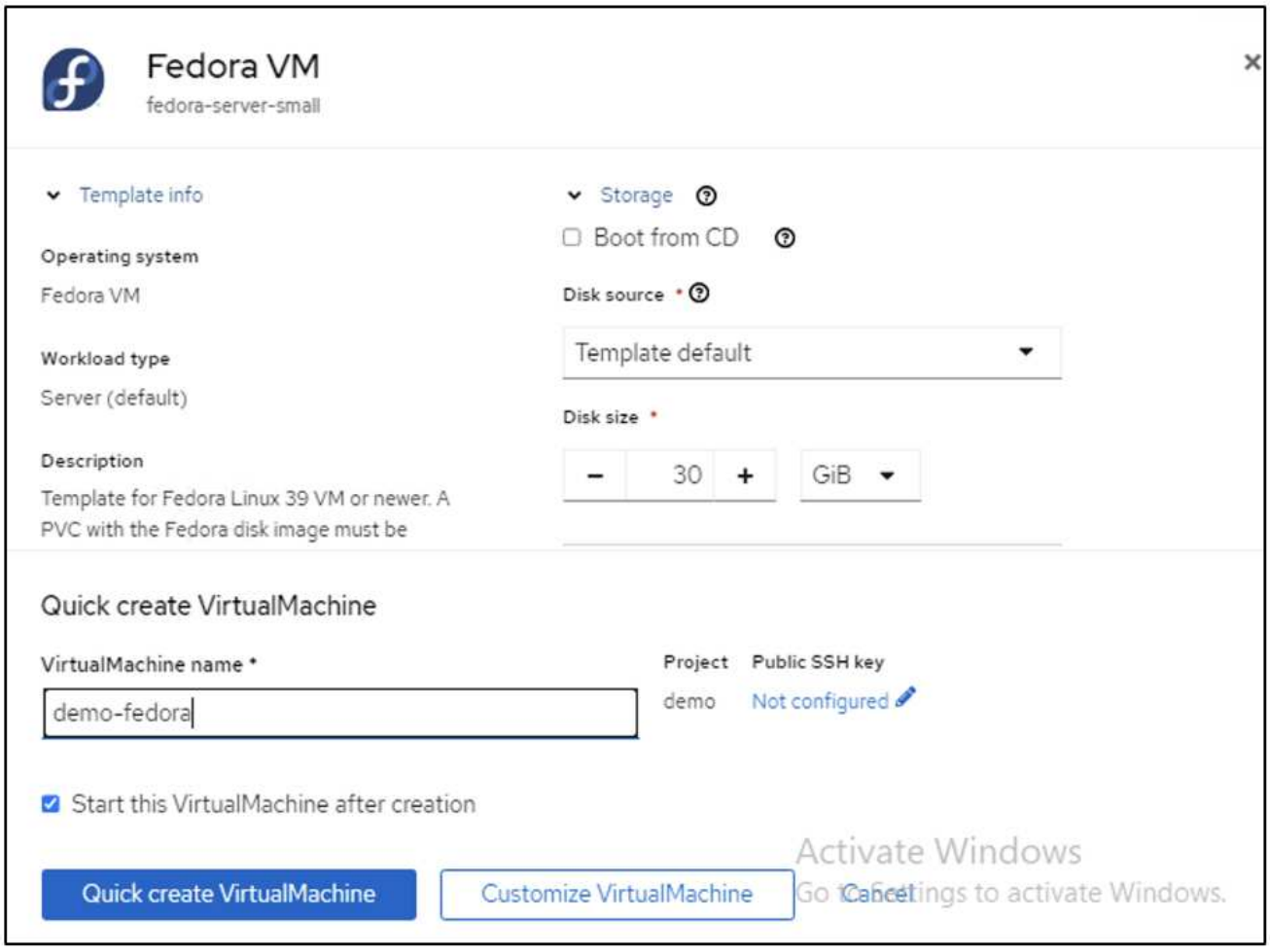
▼ **Erstellen einer VM in OpenShift Virtualization**

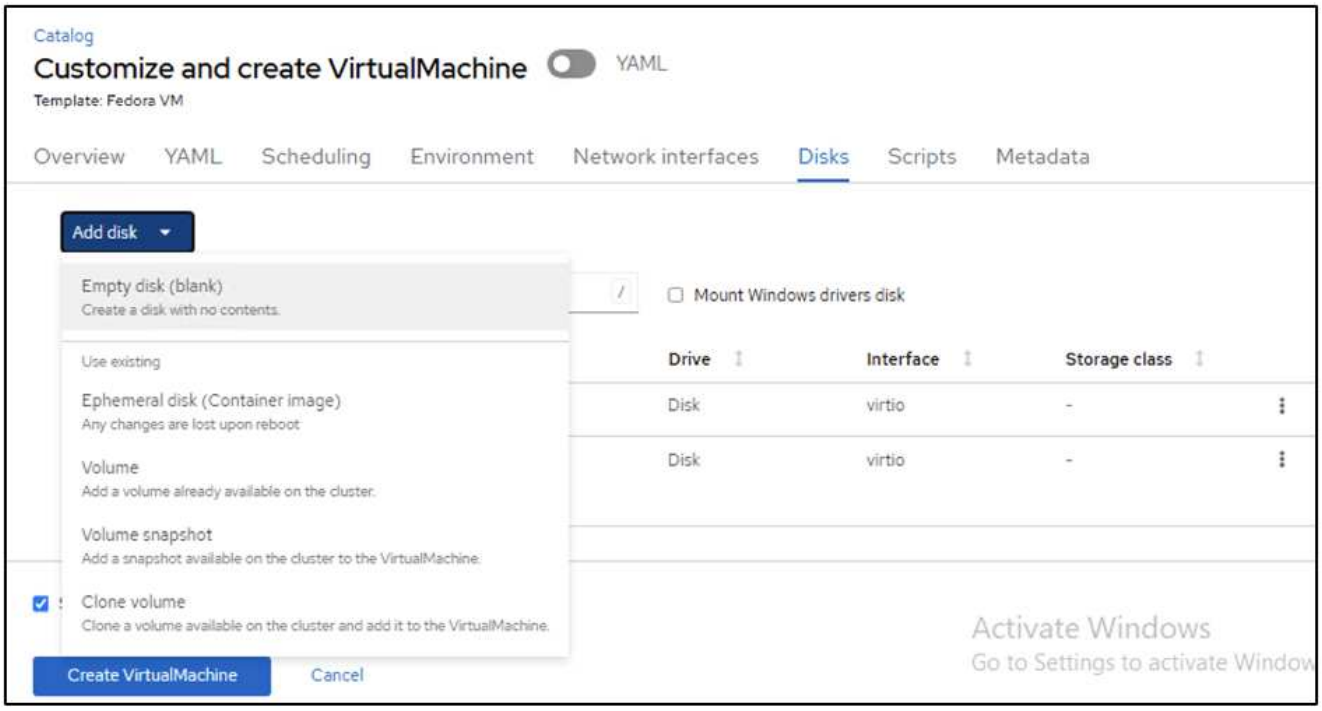
Die folgenden Screenshots zeigen die Erstellung der VM (Demo-Fedora im Namespace Demo) von der Konsole aus mithilfe der Vorlage. Die Root-Festplatte wählt die Standardspeicherklasse automatisch aus. Überprüfen Sie daher, ob die Standardspeicherklasse richtig eingestellt ist. In diesem Setup ist die Standardspeicherklasse **sc-zonea-san**. Stellen Sie sicher, dass Sie beim Erstellen der zusätzlichen Festplatte die Speicherklasse sc-zonea-san auswählen und das Kontrollkästchen „**Optimierte Speichereinstellungen anwenden**“ aktivieren. Dadurch werden die Zugriffsmodi auf RWX und der Volume-Modus auf Block gesetzt.

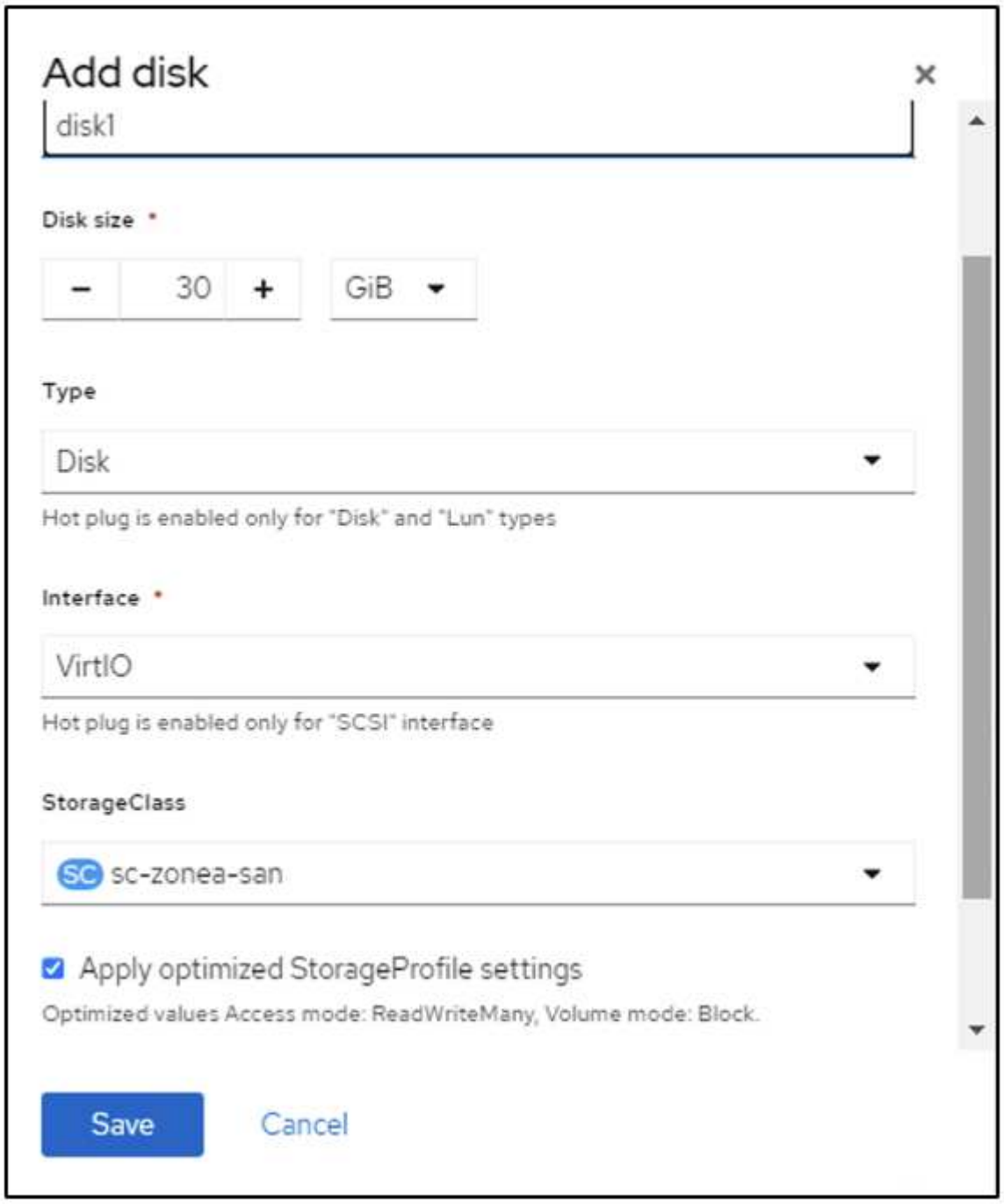
ⓘ Trident unterstützt den RWX-Zugriffsmodus im Block-Volume-Modus für SAN (iSCSI, NVMe/TCP und FC). (Dies ist der Standardzugriffsmodus für NAS). Der RWX-Zugriffsmodus ist erforderlich, wenn Sie zu einem späteren Zeitpunkt eine Livemigration der VMs durchführen müssen.

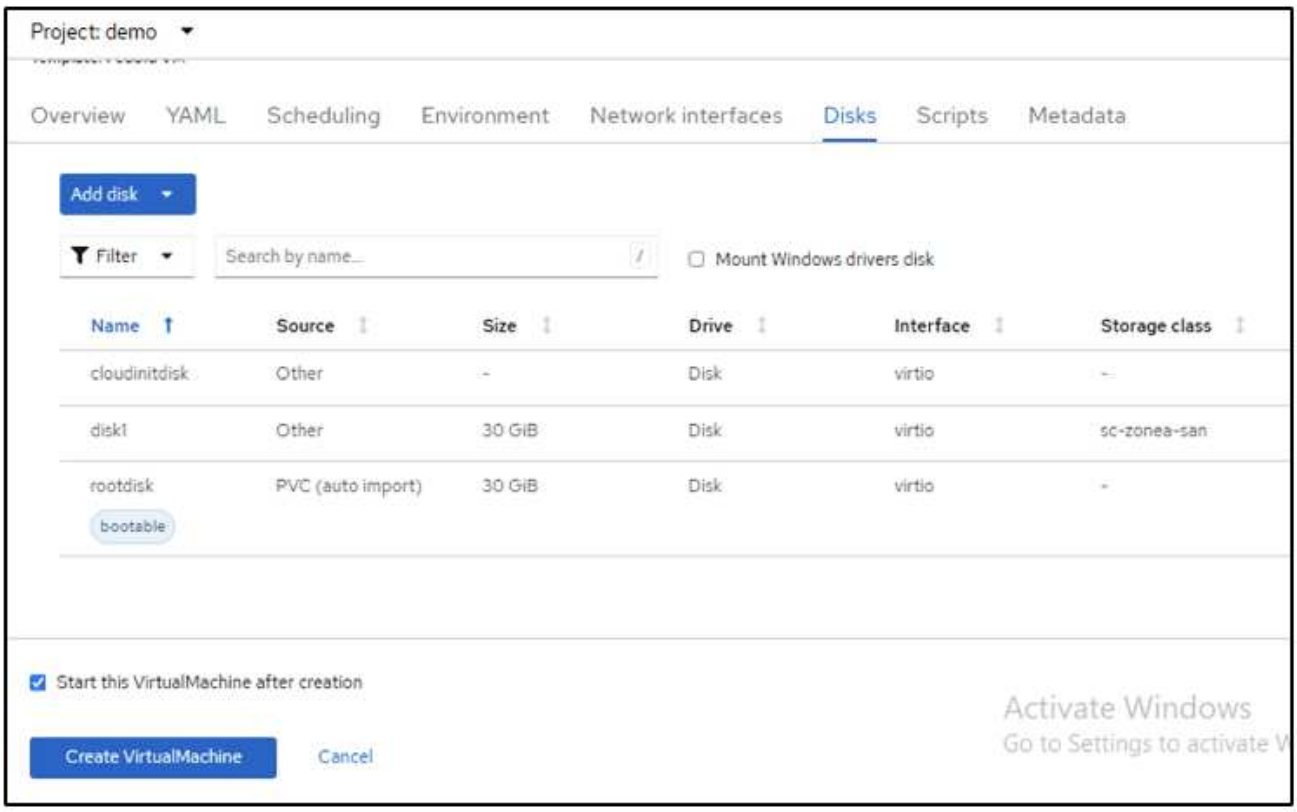



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Activate Windows
Go to Settings to activate Windows.
Quick create VirtualMachine
Customize VirtualMachine
Cancel


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Erstellen einer App

▼ App erstellen

Erstellen Sie eine Trident Protect App für die VM

Im Beispiel verfügt der demo namespace über eine VM und alle Ressourcen des namespace werden beim Erstellen der App einbezogen.

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
```

```
  namespace: demo
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

Schützen Sie die App, indem Sie ein Backup erstellen

▼ **Backups erstellen**

Erstellen Sie ein On-Demand-Backup

Erstellen Sie ein Backup für die zuvor erstellte App (Demo-VM), das alle Ressourcen im Demo-Namespace enthält. Geben Sie den Appvault-Namen an, in dem die Sicherungen gespeichert werden.

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+---------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |   AGE   |
+--------------------------+---------+----------------+-----------+-------+---------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+---------+
[root@localhost VM-DataProtection]#
```

Erstellen Sie Backups nach einem Zeitplan

Erstellen Sie einen Zeitplan für die Sicherungen und geben Sie dabei die Granularität und die Anzahl der aufzubewahrenden Sicherungen an.

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Wiederherstellen aus einer Sicherung

▼ **Wiederherstellen aus Backups**

Stellen Sie die VM im selben Namespace wieder her

Im Beispiel enthält das Backup demo-vm-backup-on-demand das Backup mit der Demo-App für die Fedora-VM.

Löschen Sie zunächst die VM und stellen Sie sicher, dass die PVCs, Pods und VM-Objekte aus dem Namespace „demo“ gelöscht werden.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                  STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

Erstellen Sie jetzt ein Backup-in-Place-Wiederherstellungsobjekt.

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Überprüfen Sie, ob die VM, Pods und PVCs wiederhergestellt sind

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Stellen Sie die VM in einem anderen Namespace wieder her

Erstellen Sie zunächst einen neuen Namespace, in dem Sie die App wiederherstellen möchten, in diesem Beispiel demo2. Erstellen Sie dann ein Backup-Wiederherstellungsobjekt

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
```

```
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

Überprüfen Sie, ob die VM, Pods und PVCs im neuen Namespace „Demo2“ erstellt werden.

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Schützen Sie die App mit Snapshots

▼ Snapshots erstellen

Erstellen Sie einen On-Demand-Snapshot Erstellen Sie einen Snapshot für die App und geben Sie den App-Tresor an, in dem er gespeichert werden soll.

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
```

```
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Erstellen Sie einen Zeitplan für Snapshots Erstellen Sie einen Zeitplan für die Snapshots. Geben Sie die Granularität und die Anzahl der aufzubewahrenden Snapshots an.

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-
s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n
demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-----------------------------------------+---------+----------------+-----------+-------+--------+
|                  NAME                   |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand               | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000             | demo-vm | Delete         | Completed |       | 1m29s  |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Wiederherstellen aus Snapshot

▼ **Wiederherstellen aus Snapshot**

Stellen Sie die VM aus dem Snapshot im selben Namespace wieder her. Löschen Sie die VM demo-fedora aus dem Namespace demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

Erstellen Sie aus dem Snapshot der VM ein Snapshot-in-Place-Restore-Objekt.

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
```

```
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+----------------------------------+-------------------+-----------+-------+--------+
|               NAME               |     APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Überprüfen Sie, ob die VM und ihre PVCs im Demo-Namespace erstellt werden.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                  STATUS   VOLUME
persistentvolumeclaim/demo-fedora                     Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

Stellen Sie die VM aus dem Snapshot in einem anderen Namespace wieder her

Löschen Sie die VM im Demo2-Namespace, die zuvor aus der Sicherung wiederhergestellt wurde.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                     Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                     Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

Erstellen Sie das Snapshot-Wiederherstellungsobjekt aus dem Snapshot und geben Sie die Namespace-Zuordnung an.

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-----------------------------------+------------------+-----------+-------+--------+
|                NAME               |     APPVAULT     |   STATE   | ERROR |  AGE   |
+-----------------------------------+------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-----------------------------------+------------------+-----------+-------+--------+
```

Überprüfen Sie, ob die VM und ihre PVCs im neuen Namespace „Demo2“ wiederhergestellt sind.

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                          STATUS   VOLUME
STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                             Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
sc-zonea-san   <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
sc-zonea-san   <unset>                 29h
[root@localhost RedHat]#
```

Wiederherstellen einer bestimmten VM

▼ Auswählen bestimmter VMs in einem Namespace zum Erstellen von Snapshots/Backups und Wiederherstellen

Im vorherigen Beispiel hatten wir eine einzelne VM innerhalb eines Namespace. Durch die Einbeziehung des gesamten Namespace in die Sicherung wurden alle mit dieser VM verknüpften Ressourcen erfasst. Im folgenden Beispiel fügen wir demselben Namespace eine weitere VM hinzu und erstellen mithilfe eines Label-Selektors eine App nur für diese neue VM.

Erstellen Sie eine neue VM (Demo-Centos-VM) im Demo-Namespace

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora   81m     Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g   1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh   1/1     Running   0          81m

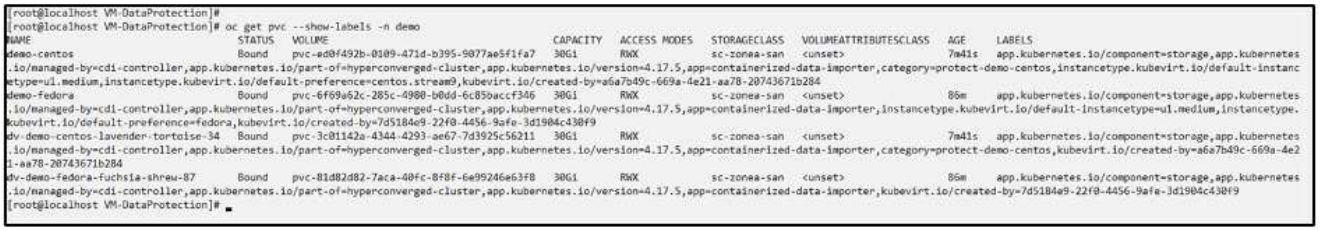
NAME                                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                             Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                             Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34     Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Beschriften Sie die Demo-Centos-VM und die zugehörigen Ressourcen

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

Überprüfen Sie, ob die Demo-CentOS-VM und die PVCs die Bezeichnungen erhalten haben.

```
[root@localhost VM-DataProtection]# oc get vm --show-labels -n demo
NAME          AGE     STATUS    READY   LABELS
demo-centos   6m31s   Running   True    app=demo-centos,category=protect-demo-centos,kubevirt.io/dynamic-credentials-support=true,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=centos-stream9-server-small
demo-fedora   85m     Running   True    app=demo-fedora,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=fedora-server-small
[root@localhost VM-DataProtection]#
```



Erstellen Sie mithilfe des Label-Selektors eine App nur für eine bestimmte VM (Demo-Centos)

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+-----------------+------------+-------+------+
|      NAME       | NAMESPACES | STATE | AGE  |
+-----------------+------------+-------+------+
| demo-centos-app | demo       | Ready | 56s  |
| demo-vm         | demo       | Ready | 4h6m |
+-----------------+------------+-------+------+
```

Die Methode zum Erstellen von Backups und Snapshots auf Abruf und nach Zeitplan ist dieselbe wie zuvor gezeigt. Da die zum Erstellen der Snapshots oder Backups verwendete Trident-Protect-App nur die spezifische VM aus dem Namespace enthält, wird bei der Wiederherstellung von dort nur eine bestimmte VM wiederhergestellt. Nachfolgend wird ein Beispiel für einen Sicherungs-/Wiederherstellungsvorgang

gezeigt.

Erstellen Sie ein Backup einer bestimmten VM in einem Namespace, indem Sie die entsprechende App verwenden

In den vorherigen Schritten wurde mithilfe von Label-Selektoren eine App erstellt, um nur die CentOS-VM in den Demo-Namespace aufzunehmen. Erstellen Sie ein Backup (in diesem Beispiel ein On-Demand-Backup) für diese App.

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+------------------------------+-----------------+----------------+-----------+-------+--------+
|             NAME             |       APP       | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+------------------------------+-----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand     | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500  | demo-vm         | Retain         | Completed |       | 56m17s |
+------------------------------+-----------------+----------------+-----------+-------+--------+
```

Eine bestimmte VM im selben Namespace wiederherstellen Das Backup einer bestimmten VM (CentOS) wurde mit der entsprechenden App erstellt. Wenn daraus ein Backup-in-Place-Restore oder ein Backup-Restore erstellt wird, wird nur diese spezielle VM wiederhergestellt. Löschen Sie die Centos-VM.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora   4m27s   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                    STATUS   VOLUME
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

Erstellen Sie eine direkte Sicherungswiederherstellung von „Demo-Centos-Backup-on-Demand“ und überprüfen Sie, ob die Centos-VM neu erstellt wurde.

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-
```

```
demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore | ontap-s3-appvault | Completed |       | 57m9s |
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos    29m   Running   True
virtualmachine.kubevirt.io/demo-fedora    85m   Running   True

NAME                                                          STATUS   VOLUME                                     C
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                             Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef   1
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                             Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc   1
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34     Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0   1
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c   1
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

Stellen Sie eine bestimmte VM in einem anderen Namespace wieder her. Erstellen Sie eine Sicherungswiederherstellung in einem anderen Namespace (Demo3) von Demo-Centos-Backup-on-Demand und überprüfen Sie, ob die Centos-VM neu erstellt wurde.

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-
demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

Videodemonstration

Das folgende Video zeigt eine Demonstration zum Schutz einer VM mit Snapshots

Schützen einer VM

Schützen Sie Container-Apps mit Tools von Drittanbietern

Datenschutz für Container-Apps in der OpenShift Container Platform mithilfe der OpenShift API for Data Protection (OADP)

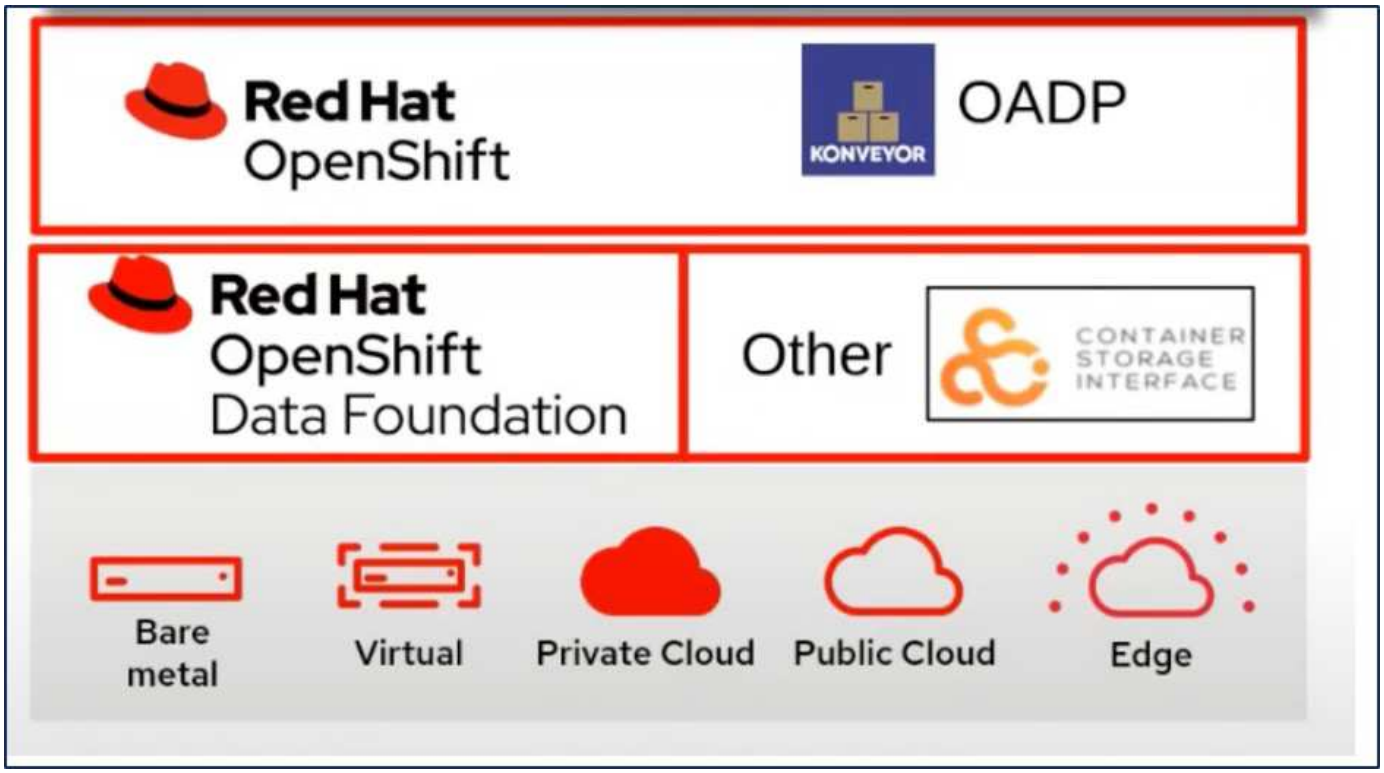
Dieser Abschnitt des Referenzdokuments enthält Details zum Erstellen von Backups von Container-Apps mithilfe der OpenShift API for Data Protection (OADP) mit Velero auf NetApp ONTAP S3 oder NetApp StorageGRID S3. Die Sicherungen der Ressourcen mit Namespace-Bereich, einschließlich der Persistent Volumes (PVs) der App, werden mithilfe von CSI Trident Snapshots erstellt.

Der persistente Storage für Container-Apps kann durch ONTAP Storage unterstützt werden, der mithilfe von "Trident CSI" in den OpenShift Cluster integriert ist. In diesem Abschnitt verwenden wir "OpenShift-API für Datenschutz (OADP)", um die Sicherung von Anwendungen einschließlich ihrer Daten-Volumes zu

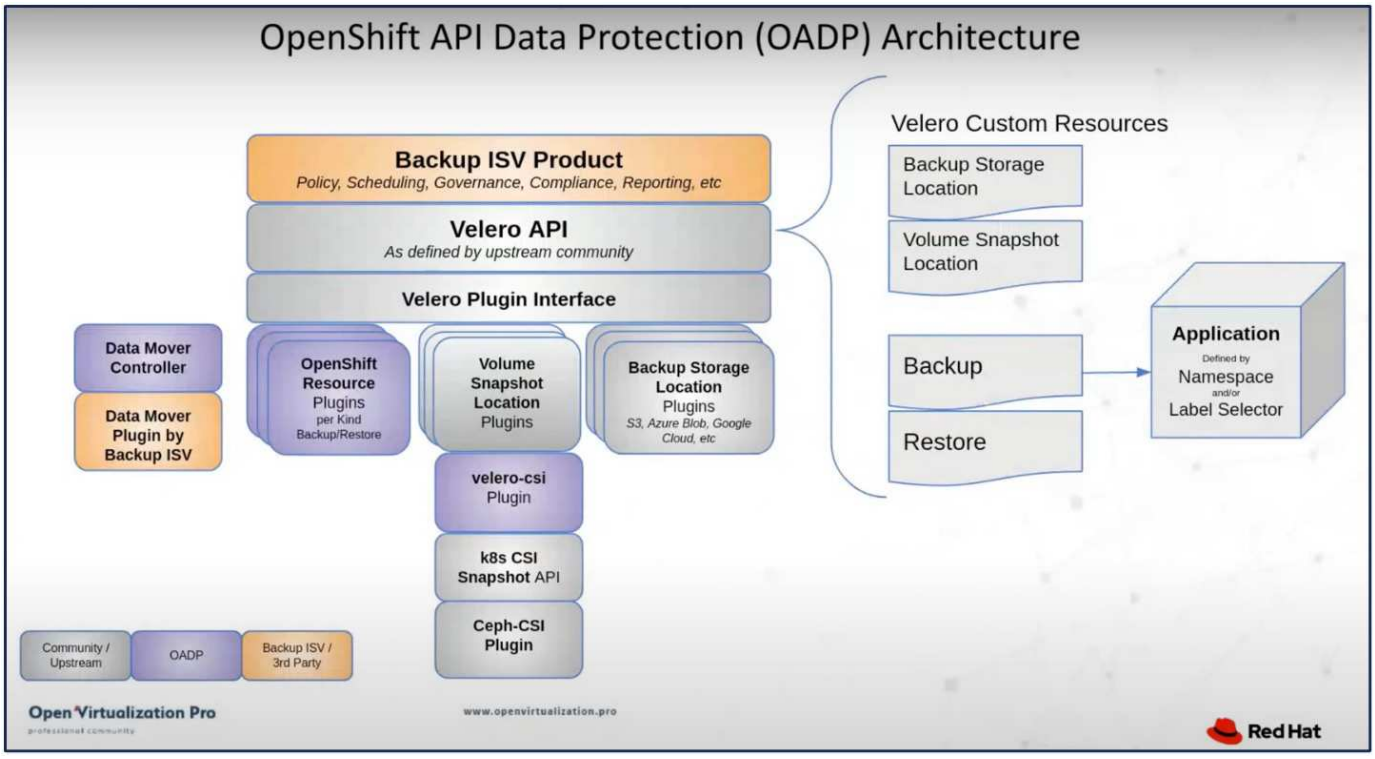
- ONTAP Objektspeicher
- StorageGrid

Bei Bedarf stellen wir dann eine Wiederherstellung aus dem Backup her. Bitte beachten Sie, dass die App nur in dem Cluster wiederhergestellt werden kann, von dem das Backup erstellt wurde.

OADP ermöglicht die Sicherung, Wiederherstellung und Notfallwiederherstellung von Anwendungen auf einem OpenShift-Cluster. Zu den Daten, die mit OADP geschützt werden können, gehören Kubernetes-Ressourcenobjekte, persistente Volumes und interne Images.



Red Hat OpenShift nutzt die von den OpenSource-Communitys entwickelten Lösungen zum Datenschutz. "Velero" ist ein Open-Source-Tool zum sicheren Sichern und Wiederherstellen, Durchführen einer Notfallwiederherstellung und Migrieren von Kubernetes-Clusterressourcen und persistenten Volumes. Um Velero einfach verwenden zu können, hat OpenShift den OADP-Operator und das Velero-Plugin zur Integration mit den CSI-Speichertreibern entwickelt. Der Kern der bereitgestellten OADP-APIs basiert auf den Velero-APIs. Nach der Installation und Konfiguration des OADP-Operators basieren die durchführbaren Sicherungs-/Wiederherstellungsvorgänge auf den von der Velero-API bereitgestellten Vorgängen.



OADP 1.3 ist im Operator Hub des OpenShift-Clusters 4.12 und höher verfügbar. Es verfügt über einen integrierten Data Mover, der CSI-Volume-Snapshots in einen Remote-Objektspeicher verschieben kann. Dies sorgt für Portabilität und Haltbarkeit, indem Snapshots während der Sicherung an einen Objektspeicherort verschoben werden. Die Snapshots stehen dann nach Katastrophen zur Wiederherstellung zur Verfügung.

Im Folgenden sind die Versionen der verschiedenen Komponenten aufgeführt, die für die Beispiele in diesem Abschnitt verwendet wurden.

- OpenShift Cluster 4.14
- OADP Operator 1.13 bereitgestellt von Red Hat
- Velero CLI 1.13 für Linux
- Trident 24.02
- ONTAP 9.12
- PostgreSQL mit Helm installiert.

"Trident CSI" "OpenShift-API für Datenschutz (OADP)" "Velero"

Installation des OpenShift API for Data Protection (OADP)-Operators

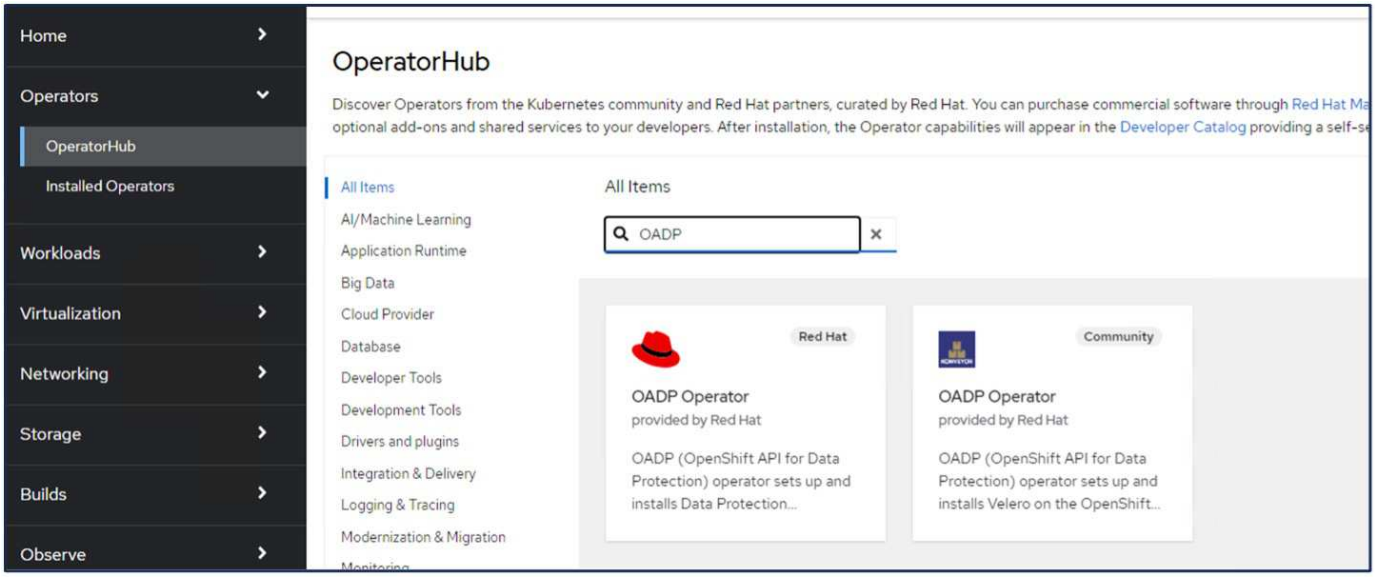
In diesem Abschnitt wird die Installation des OpenShift API for Data Protection (OADP) Operator beschrieben.

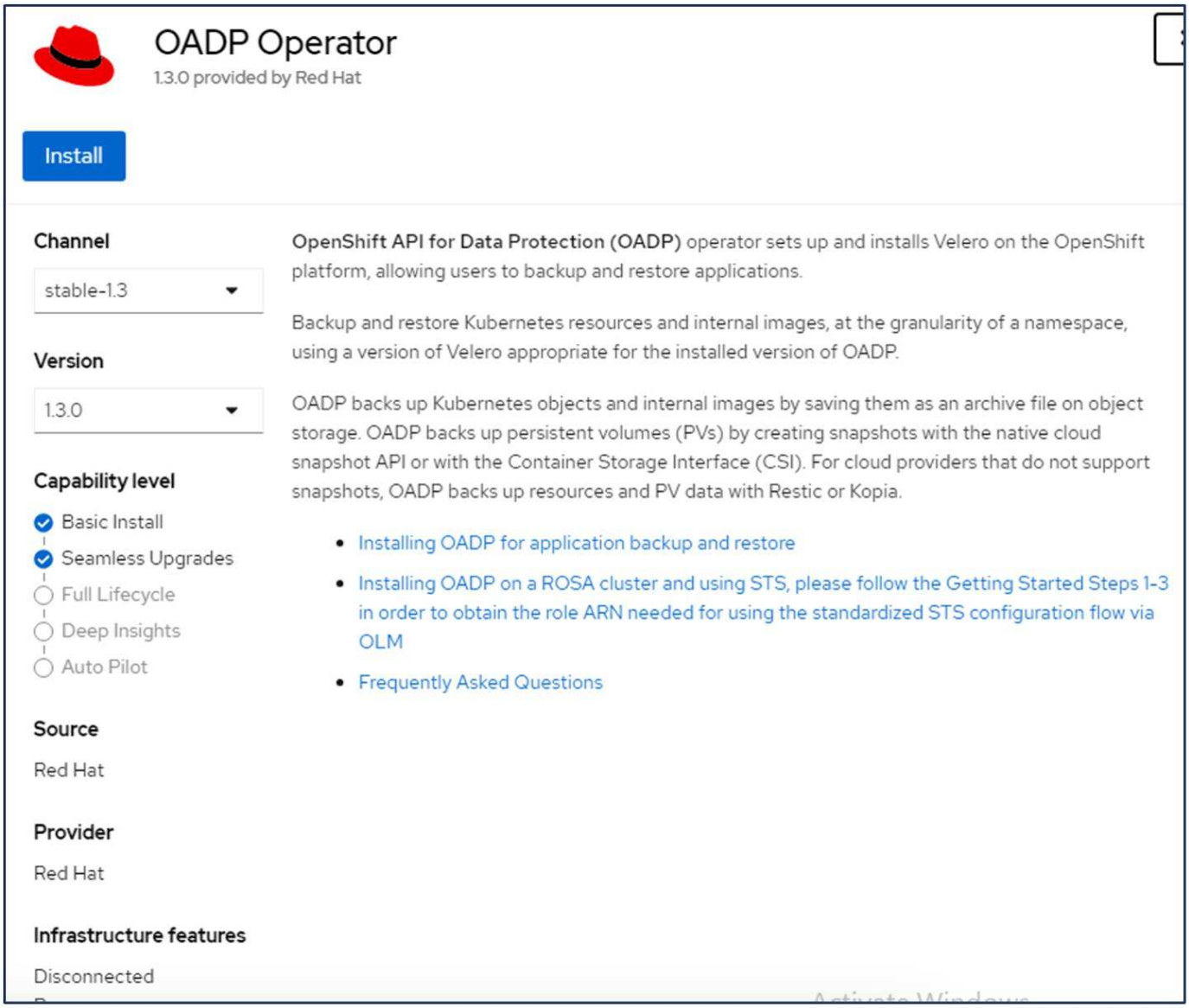
Voraussetzungen

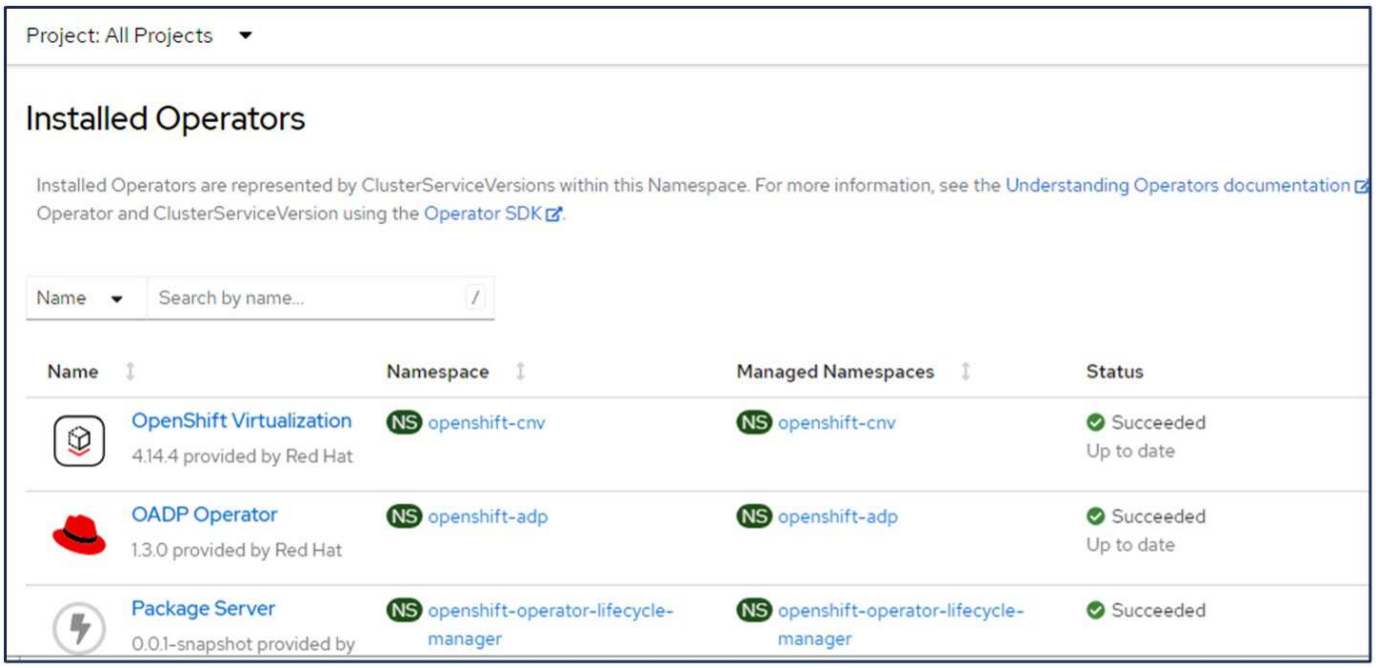
- Ein Red Hat OpenShift-Cluster (neuer als Version 4.12), installiert auf einer Bare-Metal-Infrastruktur mit RHCOS-Worker-Knoten
- Ein NetApp ONTAP -Cluster, der über Trident in den Cluster integriert ist
- Ein Trident -Backend, das mit einem SVM auf einem ONTAP -Cluster konfiguriert ist
- Eine auf dem OpenShift-Cluster konfigurierte StorageClass mit Trident als Provisioner
- Auf dem Cluster erstellte Trident Snapshot-Klasse
- Cluster-Admin-Zugriff auf den Red Hat OpenShift-Cluster
- Administratorzugriff auf NetApp ONTAP -Cluster
- Eine Anwendung, zB PostgreSQL, die auf dem Cluster bereitgestellt wird
- Eine Admin-Workstation mit installierten und zu $PATH hinzugefügten Tridentctl- und OC-Tools

Schritte zur Installation des OADP-Operators

1. Gehen Sie zum Operator Hub des Clusters und wählen Sie den Red Hat OADP-Operator aus. Verwenden Sie auf der Installationsseite alle Standardauswahlen und klicken Sie auf „Installieren“. Verwenden Sie auf der nächsten Seite erneut alle Standardeinstellungen und klicken Sie auf Installieren. Der OADP-Operator wird im Namespace openshift-adp installiert.


Home
Operators
OperatorHub
Installed Operators
Workloads
Virtualization
Networking
Storage
Builds
Observe
OperatorHub
Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Ma
optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the Developer Catalog providing a self-se
All Items
AI/Machine Learning
Application Runtime
Big Data
Cloud Provider
Database
Developer Tools
Development Tools
Drivers and plugins
Integration & Delivery
Logging & Tracing
Modernization & Migration
All Items
OADP
Red Hat
OADP Operator
provided by Red Hat
OADP (OpenShift API for Data Protection) operator sets up and installs Data Protection...
Community
OADP Operator
provided by Red Hat
OADP (OpenShift API for Data Protection) operator sets up and installs Velero on the OpenShift...


OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions



Voraussetzungen für die Velero-Konfiguration mit Ontap S3-Details

Nachdem die Installation des Operators erfolgreich war, konfigurieren Sie die Velero-Instanz. Velero kann für die Verwendung von S3-kompatiblem Object Storage konfiguriert werden. Konfigurieren Sie ONTAP S3 mit den Verfahren, die im"Abschnitt „Object Storage Management“ der ONTAP Dokumentation" . Für die Integration mit Velero benötigen Sie die folgenden Informationen aus Ihrer ONTAP S3-Konfiguration.

- Eine logische Schnittstelle (LIF), die für den Zugriff auf S3 verwendet werden kann
- Benutzeranmeldeinformationen für den Zugriff auf S3, einschließlich des Zugriffsschlüssels und des geheimen Zugriffsschlüssels
- Ein Bucket-Name in S3 für Backups mit Zugriffsberechtigungen für den Benutzer
- Für einen sicheren Zugriff auf den Objektspeicher sollte auf dem Objektspeicherserver ein TLS-Zertifikat installiert werden.

Voraussetzungen für die Velero-Konfiguration mit StorageGrid S3-Details

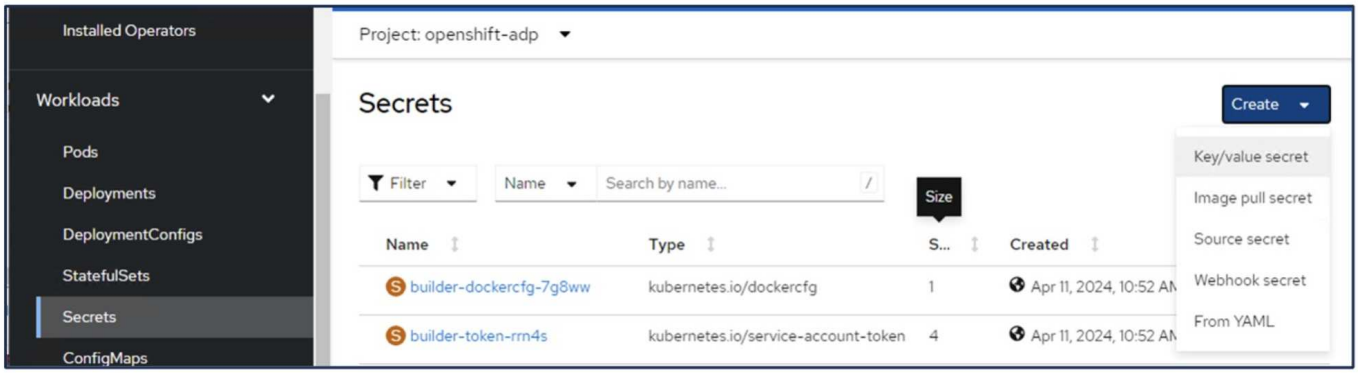
Velero kann für die Verwendung von S3-kompatiblem Object Storage konfiguriert werden. Sie können StorageGrid S3 mit den im folgenden Abschnitt beschriebenen Verfahren konfigurieren."StorageGrid-Dokumentation" . Für die Integration mit Velero benötigen Sie die folgenden Informationen aus Ihrer StorageGrid S3-Konfiguration.

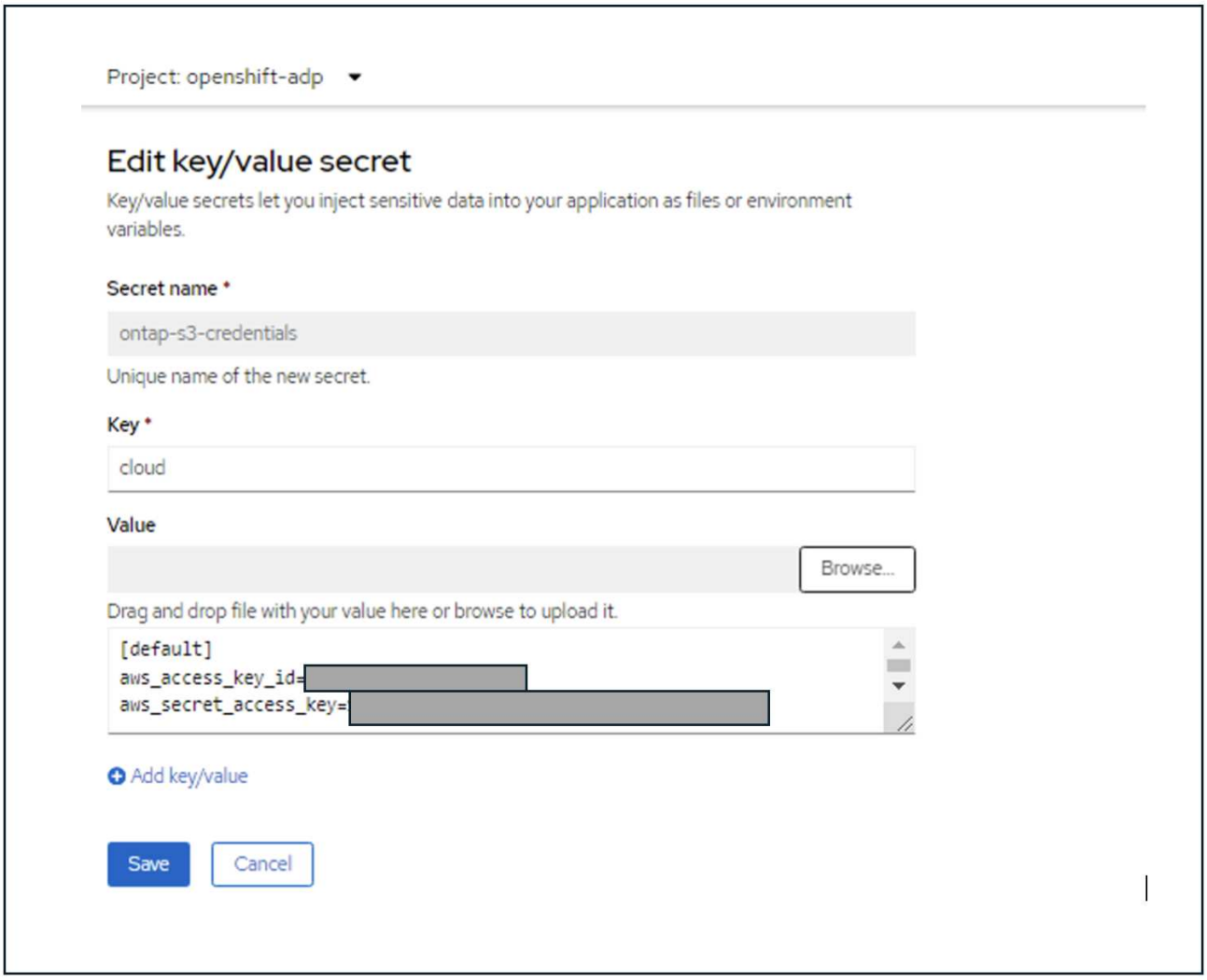
- Der Endpunkt, der für den Zugriff auf S3 verwendet werden kann
- Benutzeranmeldeinformationen für den Zugriff auf S3, einschließlich des Zugriffsschlüssels und des geheimen Zugriffsschlüssels
- Ein Bucket-Name in S3 für Backups mit Zugriffsberechtigungen für den Benutzer
- Für einen sicheren Zugriff auf den Objektspeicher sollte auf dem Objektspeicherserver ein TLS-Zertifikat installiert werden.

Schritte zum Konfigurieren von Velero

- Erstellen Sie zunächst ein Geheimnis für die Benutzeranmeldeinformationen eines ONTAP S3 oder eines StorageGrid Tenant. Dies wird später zur Konfiguration von Velero verwendet. Sie können ein Geheimnis

über die CLI oder die Webkonsole erstellen. Um ein Geheimnis über die Webkonsole zu erstellen, wählen Sie „Geheimnisse“ aus und klicken Sie dann auf „Schlüssel/Wert-Geheimnis“. Geben Sie die Werte für den Anmeldeinformationsnamen, den Schlüssel und den Wert wie angezeigt ein. Stellen Sie sicher, dass Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres S3-Benutzers verwenden. Geben Sie dem Geheimnis einen passenden Namen. Im folgenden Beispiel wird ein Geheimnis mit ONTAP S3-Benutzeranmeldeinformationen namens ontap-s3-credentials erstellt.





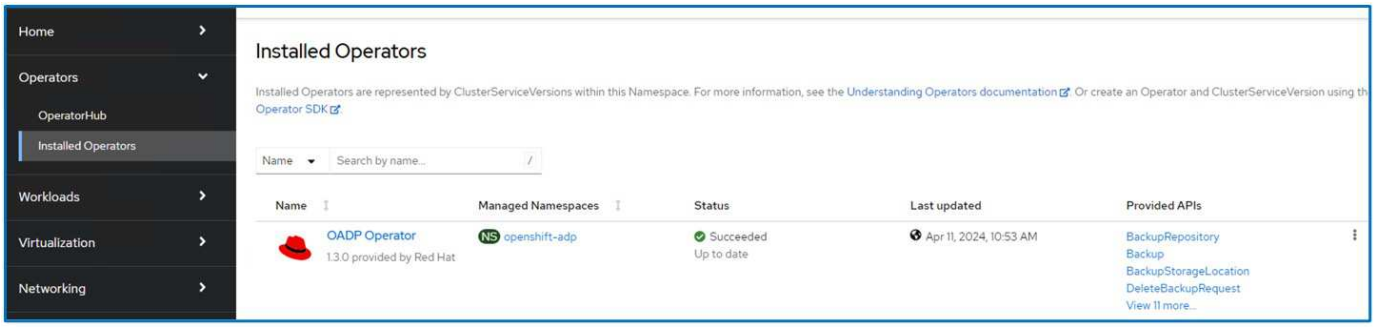
Um ein Geheimnis mit dem Namen sg-s3-credentials über die CLI zu erstellen, können Sie den folgenden Befehl verwenden.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

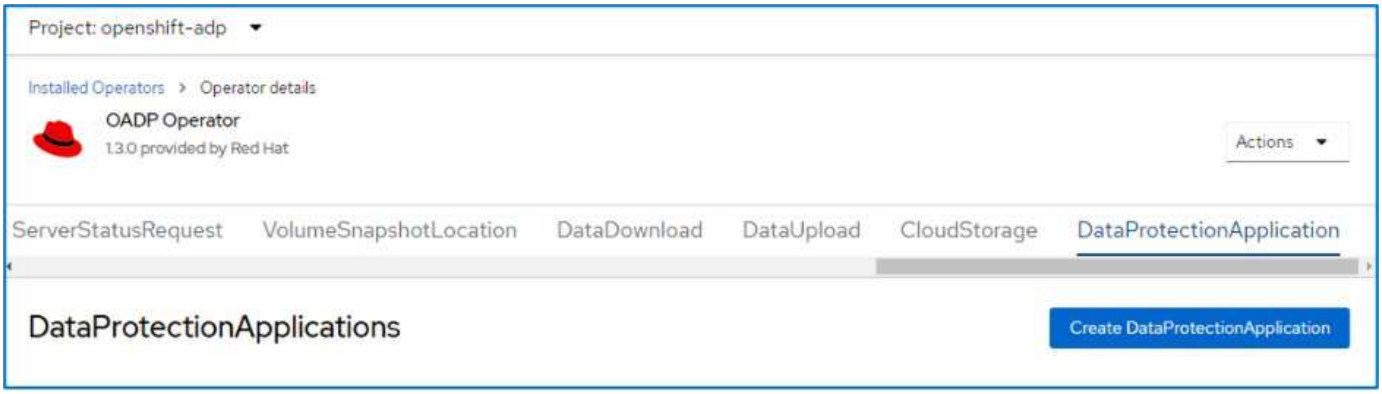
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- Um Velero zu konfigurieren, wählen Sie als Nächstes im Menüpunkt „Operatoren“ die Option „Installierte Operatoren“ aus, klicken Sie auf den OADP-Operator und wählen Sie dann die Registerkarte **DataProtectionApplication** aus.



Klicken Sie auf „DataProtectionApplication erstellen“. Geben Sie in der Formularansicht einen Namen für die DataProtection-Anwendung ein oder verwenden Sie den Standardnamen.



Gehen Sie nun zur YAML-Ansicht und ersetzen Sie die Spezifikationsinformationen wie in den folgenden YAML-Dateibeispielen gezeigt.

Beispiel-YAML-Datei zum Konfigurieren von Velero mit ONTAP S3 als Backup-Speicherort

```
spec:
  backupLocations:
    - velero:
```

```
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

Beispiel-YAML-Datei zum Konfigurieren von Velero mit StorageGrid S3 als Backup-Speicherort

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
```

```
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

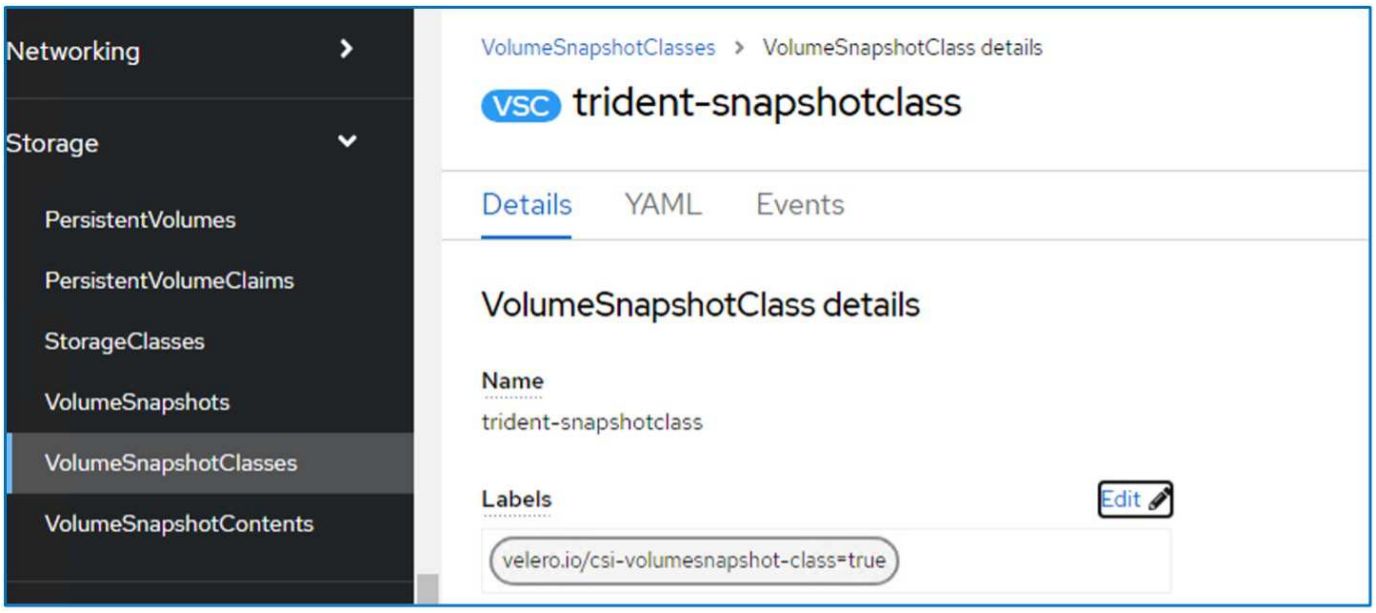
Der Abschnitt „Spec“ in der YAML-Datei sollte für die folgenden Parameter entsprechend dem obigen Beispiel konfiguriert werden.

backupLocations ONTAP S3 oder StorageGrid S3 (mit seinen Anmeldeinformationen und anderen Informationen, wie im YAML angezeigt) ist als Standard-BackupLocation für Velero konfiguriert.

snapshotLocations Wenn Sie Container Storage Interface (CSI)-Snapshots verwenden, müssen Sie keinen Snapshot-Speicherort angeben, da Sie ein VolumeSnapshotClass CR erstellen, um den CSI-Treiber zu registrieren. In unserem Beispiel verwenden Sie Trident CSI und haben zuvor VolumeSnapShotClass CR mit dem Trident CSI-Treiber erstellt.

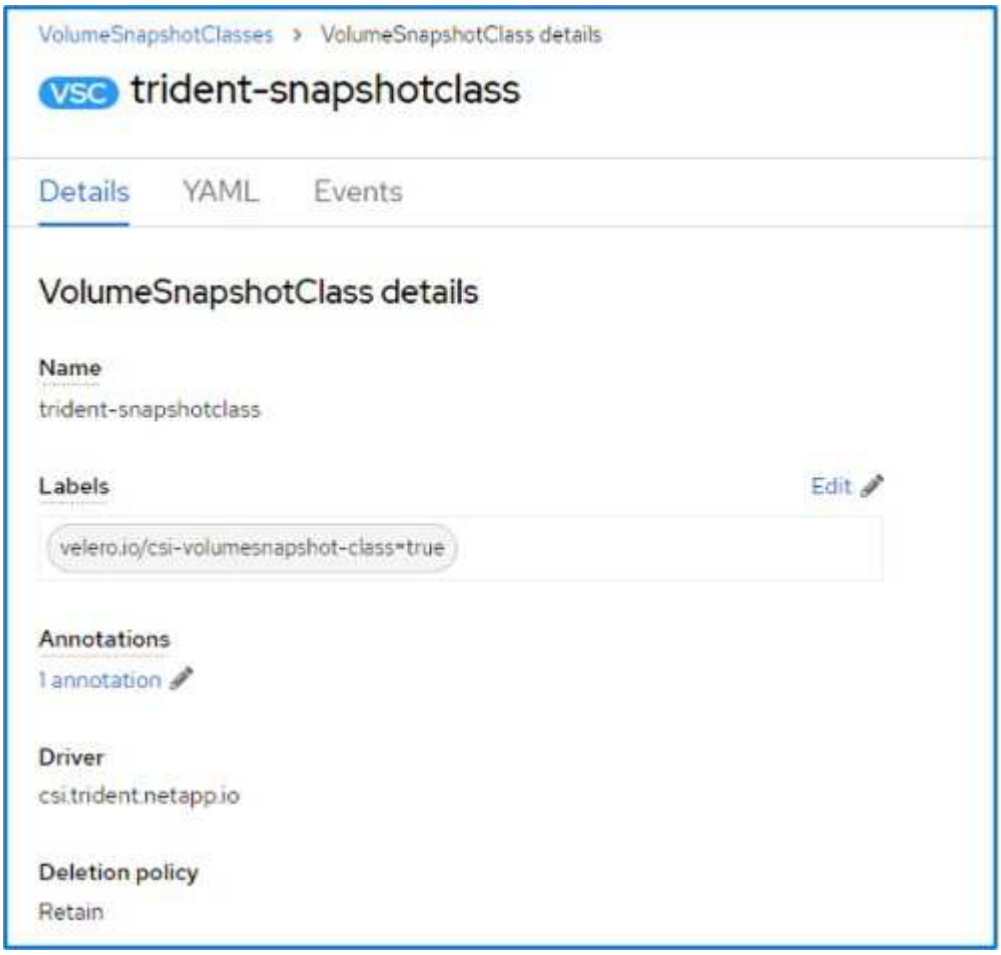
CSI-Plugin aktivieren Fügen Sie csi zu den Standard-Plugins für Velero hinzu, um persistente Volumes mit CSI-Snapshots zu sichern. Die Velero CSI-Plugins wählen zum Sichern von CSI-gestützten PVCs die VolumeSnapshotClass im Cluster aus, auf die das Label **velero.io/csi-volumesnapshot-class** gesetzt ist. Dafür

- Sie müssen die Trident VolumeSnapshotClass erstellt haben.
- Bearbeiten Sie die Bezeichnung der Trident-Snapshot-Klasse und setzen Sie sie wie unten gezeigt auf **velero.io/csi-volumesnapshot-class=true**.

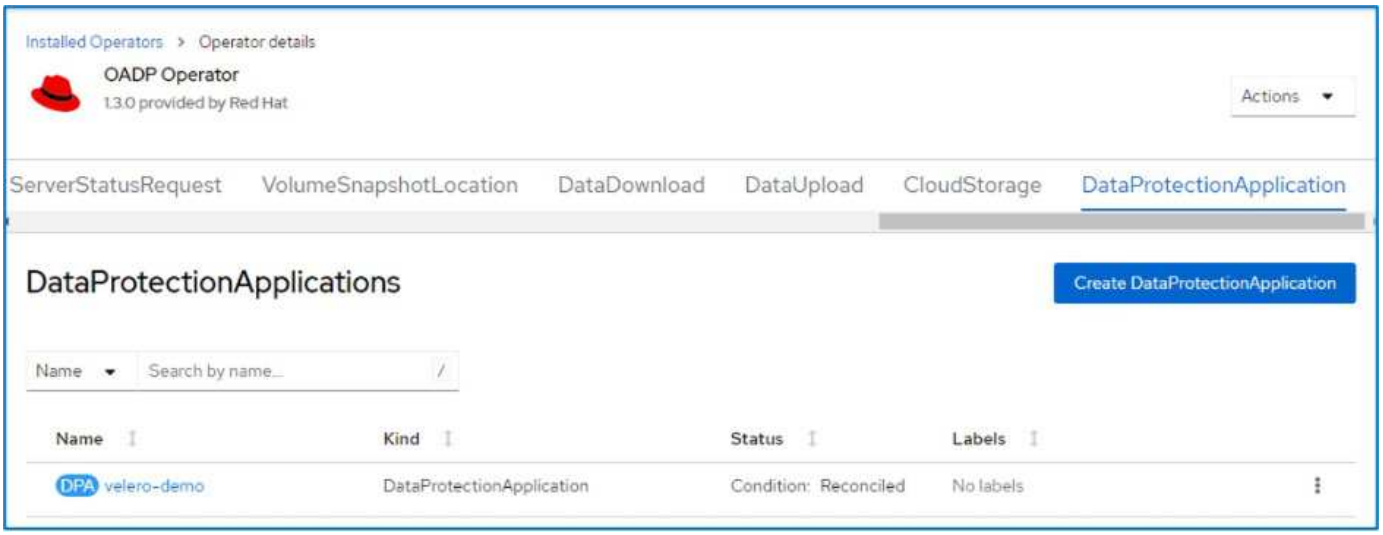


Stellen Sie sicher, dass die Snapshots auch dann bestehen bleiben, wenn die VolumeSnapshot-Objekte gelöscht werden. Dies kann durch Festlegen der **deletionPolicy** auf „Beibehalten“ erfolgen. Andernfalls gehen beim Löschen eines Namespace alle darin jemals gesicherten PVCs vollständig verloren.

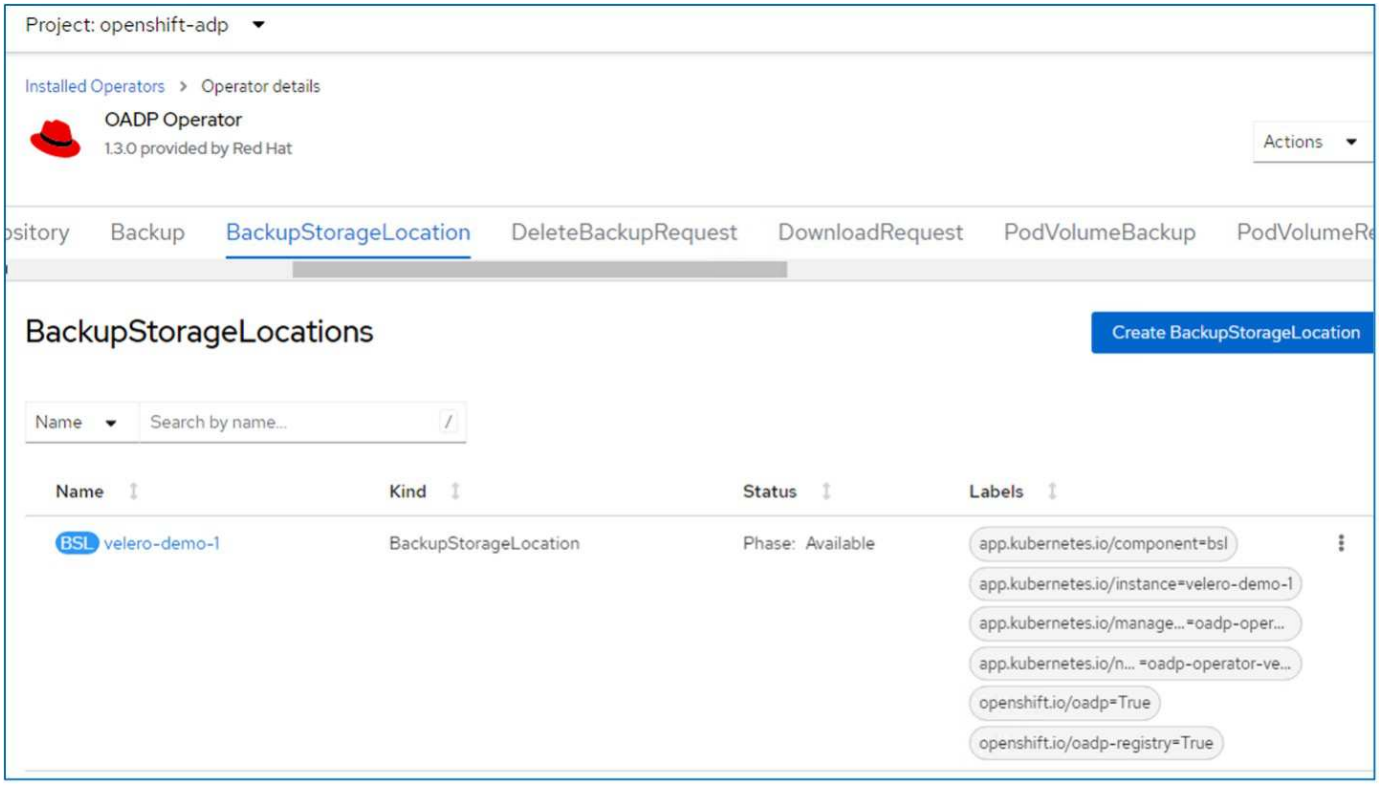
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Stellen Sie sicher, dass die DataProtectionApplication erstellt wurde und sich im Zustand „Abgestimmt“ befindet.



Der OADP-Operator erstellt einen entsprechenden BackupStorageLocation. Dieser wird beim Erstellen eines Backups verwendet.



Erstellen eines On-Demand-Backups für Apps in OpenShift Container Platform

In diesem Abschnitt wird beschrieben, wie Sie On-Demand-Backups für VMs in OpenShift Virtualization erstellen.

Schritte zum Erstellen einer Sicherungskopie einer App

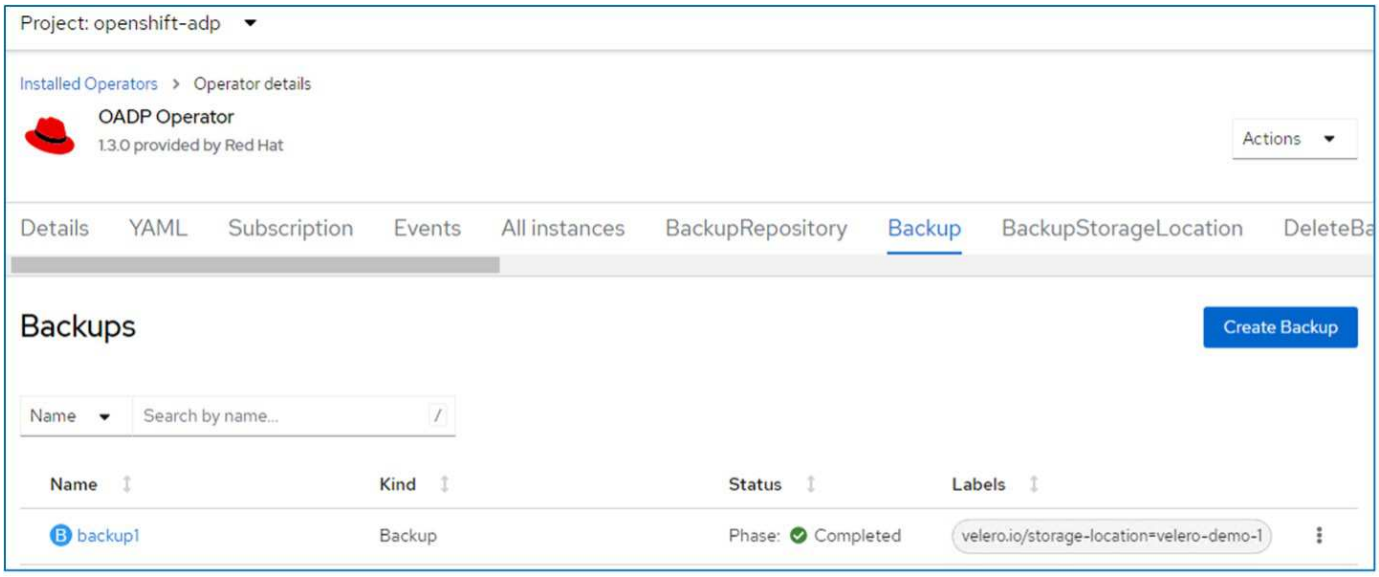
Zum Erstellen eines On-Demand-Backups einer App (App-Metadaten und persistente Volumes der App) wird über die Registerkarte **Backup** eine Backup Custom Resource (CR) erstellt. Zum Erstellen der Backup CR wird ein Beispiel-yaml bereitgestellt. Mit diesem yaml werden die App und ihr persistentes Storage im angegebenen Namespace gesichert. Zusätzliche Parameter können wie in "Dokumentation" gezeigt festgelegt werden.

Ein Snapshot der persistenten Volumes und der App-Ressourcen im angegebenen Namespace wird vom CSI erstellt. Dieser Snapshot wird am im YAML angegebenen Sicherungsspeicherort gespeichert. Das Backup bleibt gemäß TTL 30 Tage lang im System.

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
```

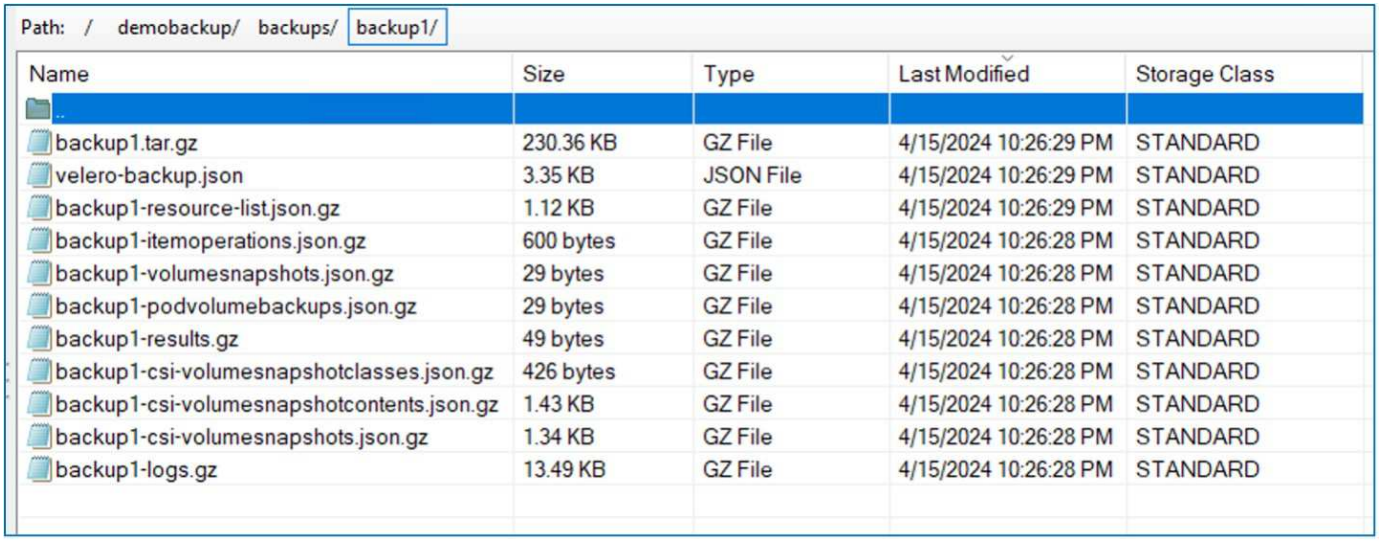
```
  ttl: 720h0m0s
```

Sobald die Sicherung abgeschlossen ist, wird ihre Phase als abgeschlossen angezeigt.



Sie können das Backup im Objektspeicher mithilfe einer S3-Browseranwendung überprüfen. Der Pfad des Backups wird im konfigurierten Bucket mit dem Präfixnamen (velero/container-demo-backup) angezeigt. Sie können sehen, dass der Inhalt der Sicherung die Volume-Snapshots, Protokolle und andere Metadaten der Anwendung umfasst.

In StorageGrid können Sie zum Anzeigen der Sicherungsobjekte auch die S3-Konsole verwenden, die über den Tenant Manager verfügbar ist.



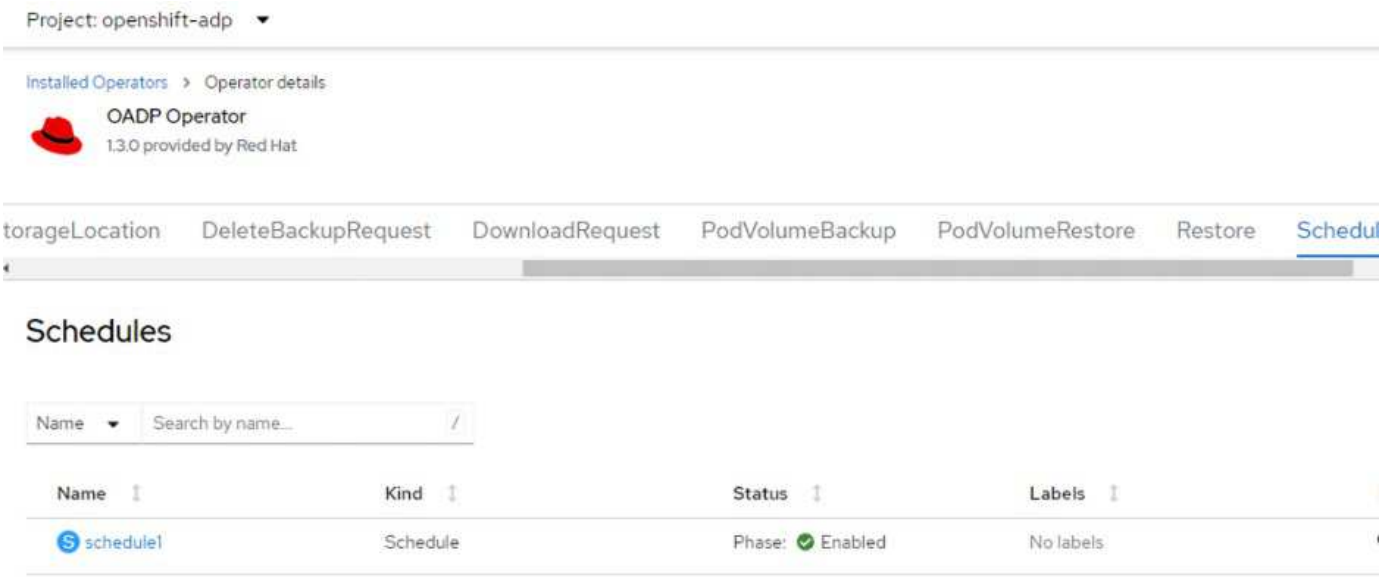
Erstellen geplanter Backups für Apps

Um Backups nach einem Zeitplan zu erstellen, müssen Sie einen Zeitplan-CR erstellen. Der Zeitplan ist einfach ein Cron-Ausdruck, mit dem Sie den Zeitpunkt angeben können, zu dem Sie das Backup erstellen möchten. Unten sehen Sie ein YAML-Beispiel zum Erstellen eines Schedule CR.

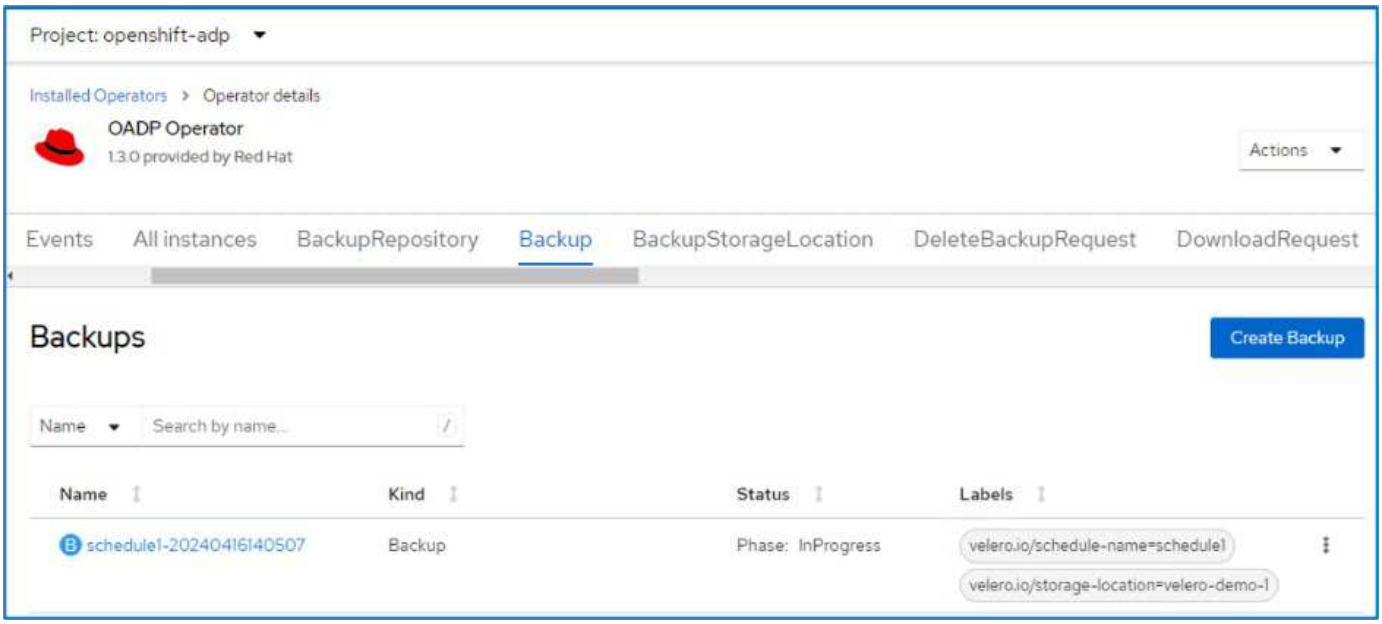
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

Der Cron-Ausdruck 0 7 * * * bedeutet, dass jeden Tag um 7:00 Uhr ein Backup erstellt wird. Außerdem werden die in die Sicherung einzubeziehenden Namespaces und der Speicherort für die Sicherung angegeben. Anstelle einer Backup-CR wird also eine geplante CR verwendet, um zum angegebenen Zeitpunkt und in der angegebenen Häufigkeit eine Sicherung zu erstellen.

Sobald der Zeitplan erstellt ist, wird er aktiviert.



Backups werden gemäß diesem Zeitplan erstellt und können auf der Registerkarte „Backup“ angezeigt werden.



Migrieren einer App von einem Cluster zu einem anderen

Die Sicherungs- und Wiederherstellungsfunktionen von Velero machen es zu einem wertvollen Tool für die Migration Ihrer Daten zwischen Clustern. In diesem Abschnitt wird beschrieben, wie Sie Apps von einem Cluster zu einem anderen migrieren, indem Sie eine Sicherungskopie der App im Objektspeicher eines Clusters erstellen und die App dann aus demselben Objektspeicher in einem anderen Cluster wiederherstellen. .

▼ **Sicherung vom ersten Cluster**

Voraussetzungen für Cluster 1

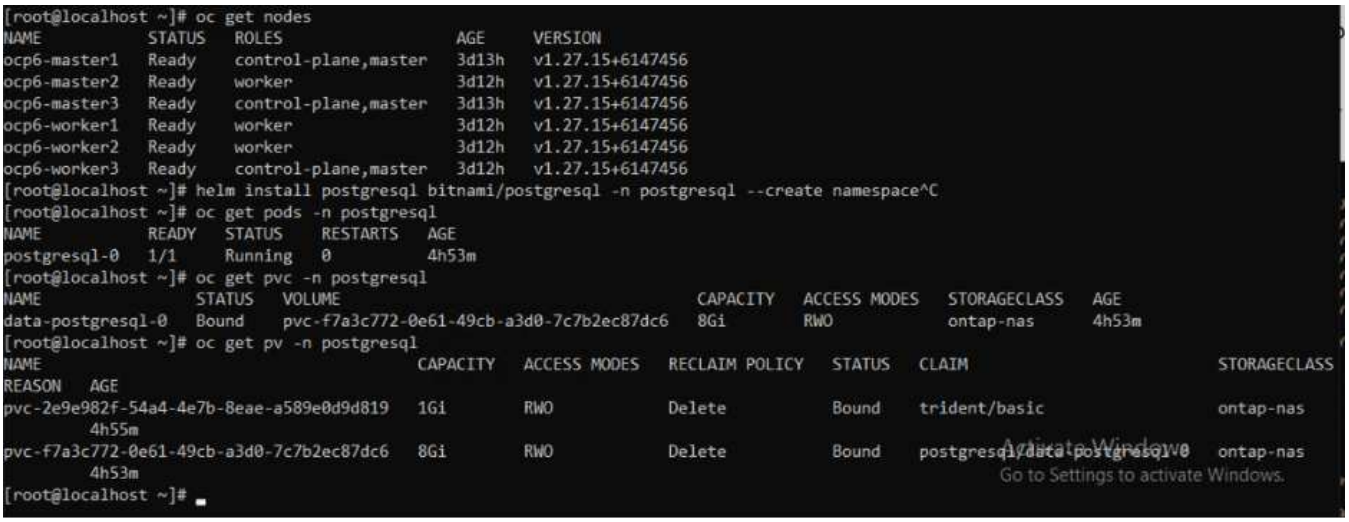
- Trident muss auf dem Cluster installiert sein.
- Es müssen ein Trident-Backend und eine Speicherklasse erstellt werden.
- Der OADP-Operator muss auf dem Cluster installiert sein.
- Die DataProtectionApplication sollte konfiguriert werden.

Verwenden Sie die folgende Spezifikation, um das DataProtectionApplication-Objekt zu konfigurieren.

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
```

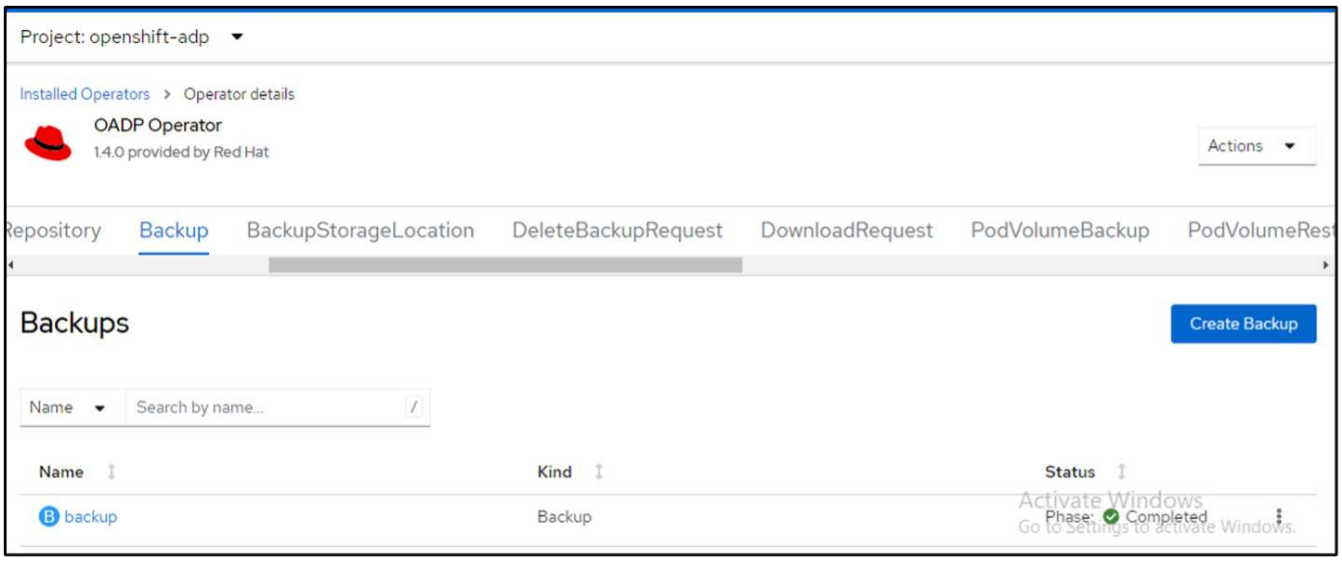
```
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

- Erstellen Sie eine Anwendung auf dem Cluster und erstellen Sie eine Sicherungskopie dieser Anwendung. Installieren Sie beispielsweise eine Postgres-Anwendung.



- Verwenden Sie die folgende Spezifikation für die Sicherungs-CR:

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



Sie können auf die Registerkarte **Alle Instanzen** klicken, um die verschiedenen Objekte anzuzeigen, die erstellt werden und verschiedene Phasen durchlaufen, bis sie schließlich zur Phase **abgeschlossen** der Sicherung gelangen.

Eine Sicherung der Ressourcen im Namespace „postgresql“ wird am Object Storage-Speicherort (ONTAP S3) gespeichert, der im „backupLocation“ in der OADP-Spezifikation angegeben ist.

▼ **Wiederherstellen auf einem zweiten Cluster**

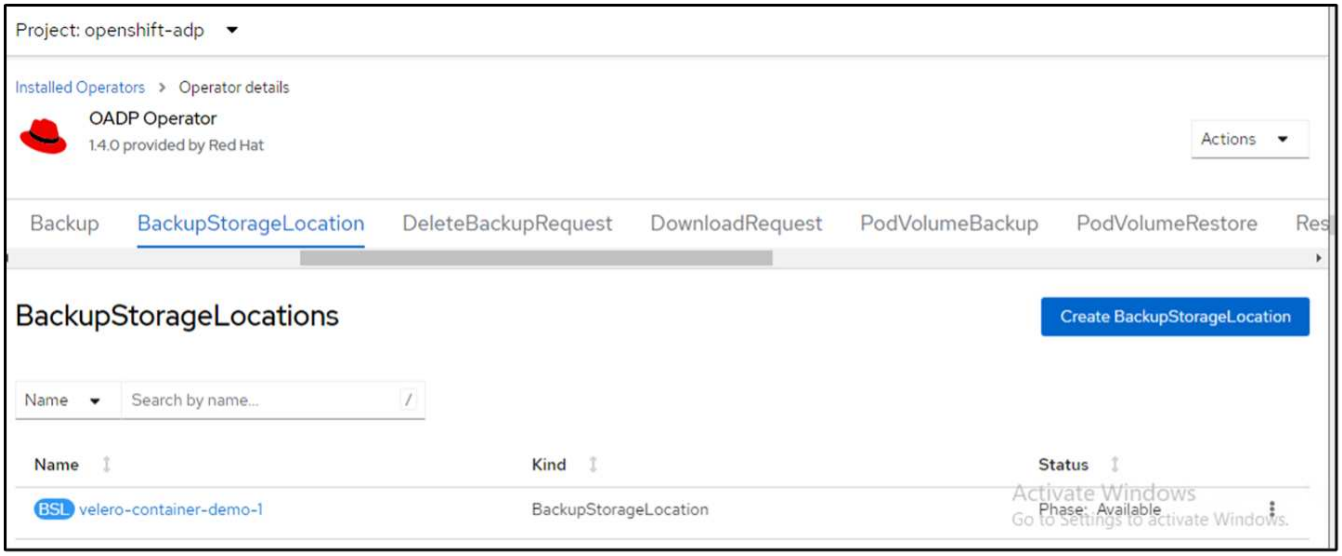
Voraussetzungen für Cluster 2

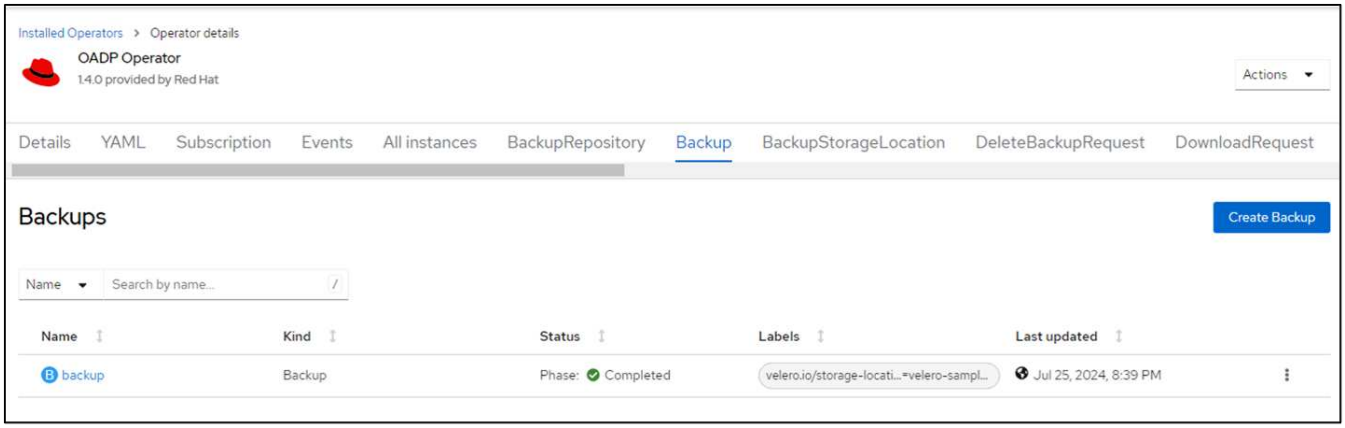
- Trident muss auf Cluster 2 installiert sein.
- Die PostgreSQL-App darf NICHT bereits im PostgreSQL-Namespace installiert sein.
- Der OADP-Operator muss auf Cluster 2 installiert sein und der BackupStorage-Speicherort muss auf denselben Objektspeicherort verweisen, an dem die Sicherung vom ersten Cluster gespeichert wurde.
- Der Backup-CR muss vom zweiten Cluster aus sichtbar sein.

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                 STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic         ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc      vsphere-sc              2d7
h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.



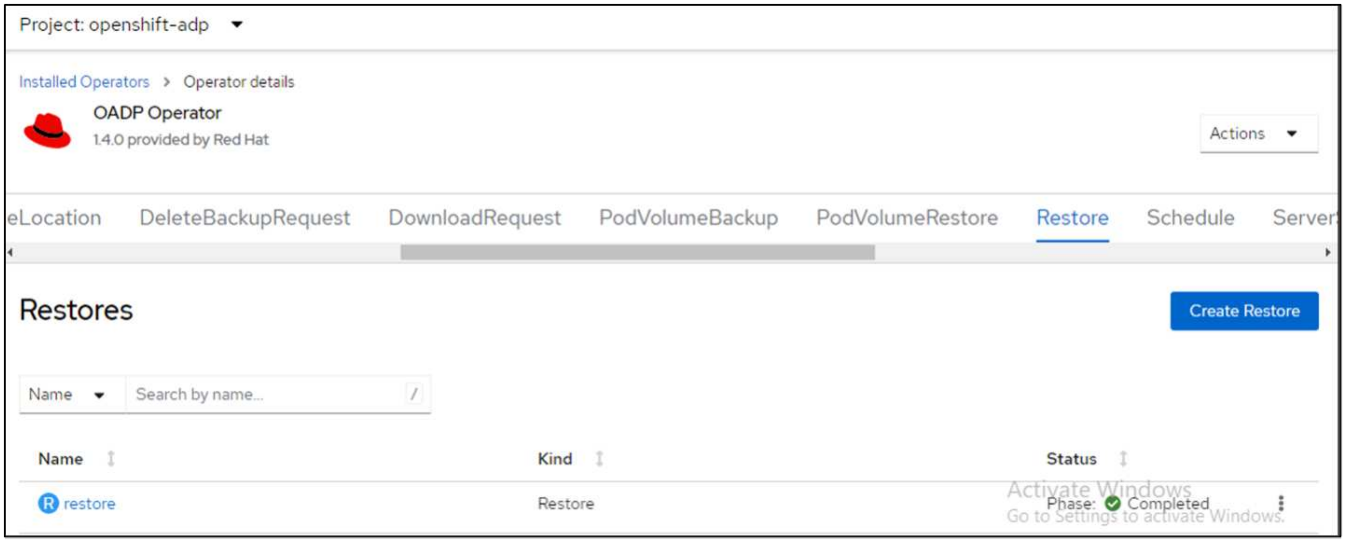


Stellen Sie die App auf diesem Cluster aus der Sicherung wieder her. Verwenden Sie das folgende YAML, um die Wiederherstellungs-CR zu erstellen.

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
```

```
spec:
  backupName: backup
  restorePVs: true
```

Wenn die Wiederherstellung abgeschlossen ist, sehen Sie, dass die PostgreSQL-App auf diesem Cluster ausgeführt wird und mit dem PVC und einem entsprechenden PV verknüpft ist. Der Zustand der App ist derselbe wie zum Zeitpunkt der Sicherung.




```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                  AGE    VERSION
ocp7-master1  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3  Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                           STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                   ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0    ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc                vsphere-sc
         2d10h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

Wiederherstellen einer App aus einem Backup

In diesem Abschnitt wird beschrieben, wie Sie Apps aus einer Sicherung wiederherstellen.

Voraussetzungen

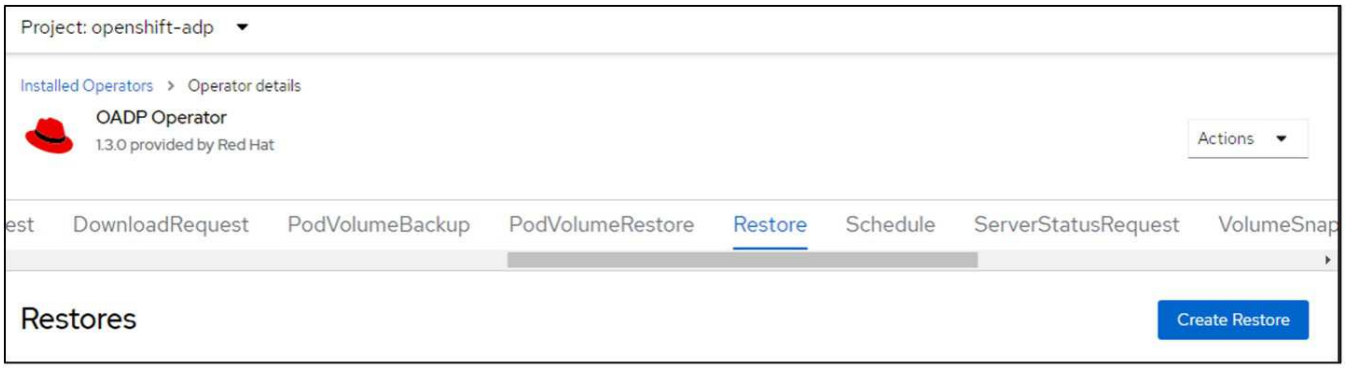
Um eine Wiederherstellung aus einer Sicherung durchzuführen, gehen wir davon aus, dass der Namespace, in dem die App vorhanden war, versehentlich gelöscht wurde.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

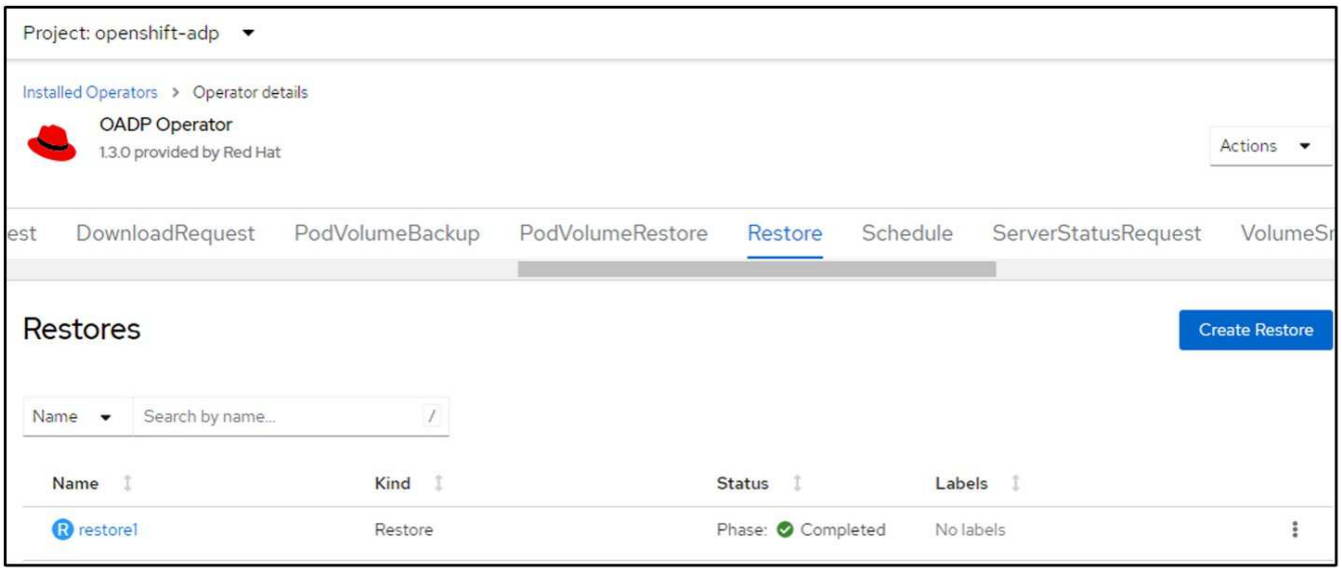
▼ **Wiederherstellen im selben Namespace**

Zum Wiederherstellen aus der Sicherung, die soeben erstellt wurde, muss eine benutzerdefinierte Restore Ressource (CR) erstellt werden. Dafür müssen ein Name, der Name der Sicherung, aus der wiederhergestellt werden soll, und restorePVs mit dem Wert true angegeben werden. Weitere Parameter können wie in der "Dokumentation" gezeigt festgelegt werden. Anschließend wird die Schaltfläche Create ausgewählt.




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

Wenn die Phase als abgeschlossen angezeigt wird, können Sie sehen, dass die App in den Zustand zurückversetzt wurde, in dem sie sich zum Zeitpunkt der Erstellung des Snapshots befand. Die App wird im selben Namespace wiederhergestellt.




```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

▼ **Wiederherstellen in einem anderen Namespace**

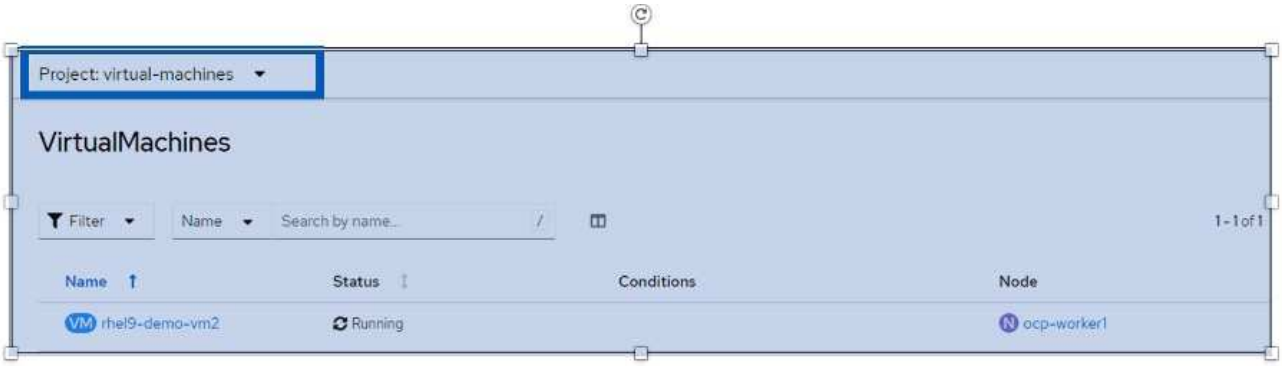
Um die App in einem anderen Namespace wiederherzustellen, können Sie in der YAML-Definition des Restore CR ein NamespaceMapping angeben.

Die folgende YAML-Beispieldatei erstellt eine Wiederherstellungs-CR, um eine App und ihren persistenten Speicher aus dem PostgreSQL-Namespace in den neuen Namespace „postgresql-restored“ wiederherzustellen.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
```

```
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

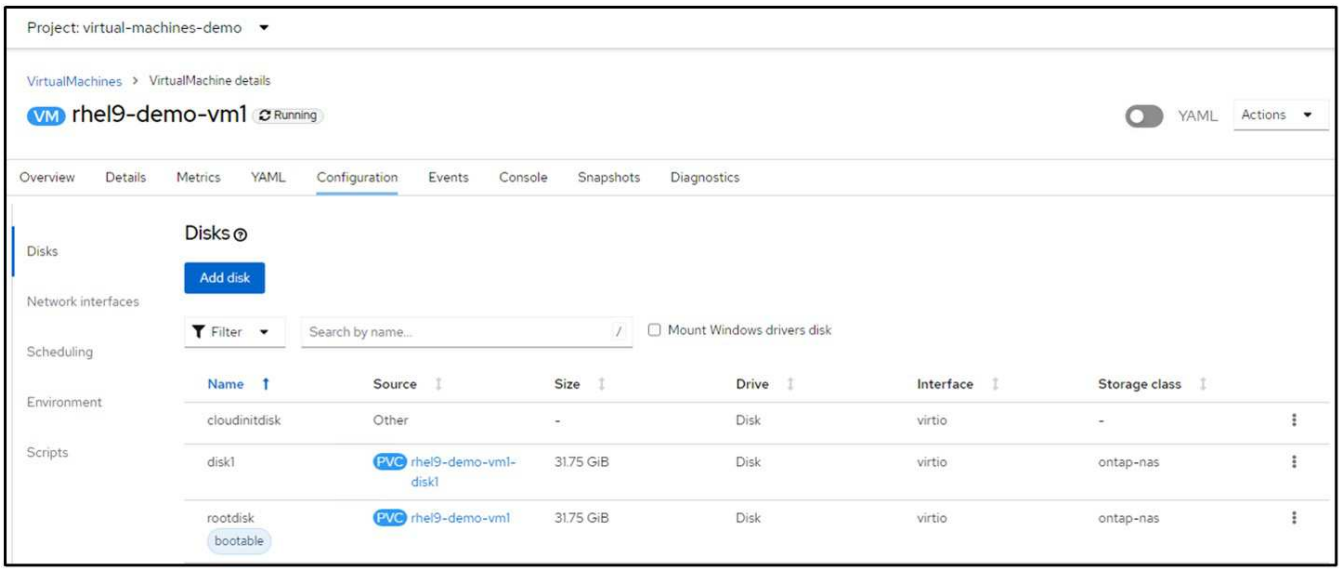
Wenn die Phase als abgeschlossen angezeigt wird, können Sie sehen, dass die App in den Zustand zurückversetzt wurde, in dem sie sich zum Zeitpunkt der Erstellung des Snapshots befand. Die App wird in einem anderen Namespace wiederhergestellt, wie im YAML angegeben.

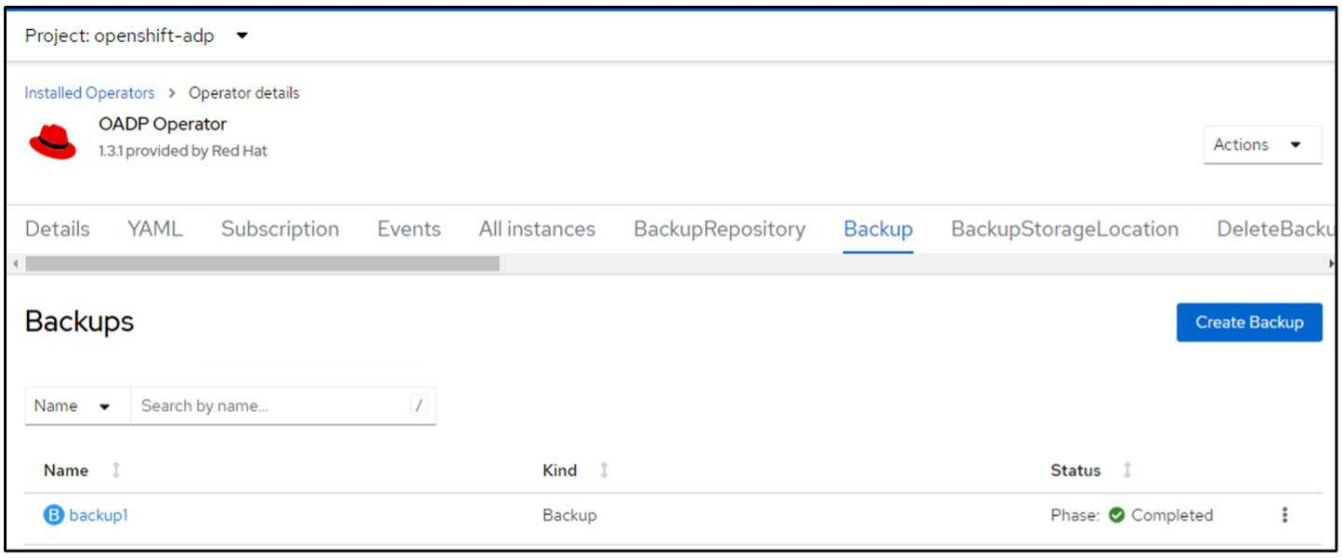


▼ **Wiederherstellen in einer anderen Speicherklasse**

Velero bietet eine allgemeine Möglichkeit, die Ressourcen während der Wiederherstellung durch Angabe von JSON-Patches zu ändern. Die JSON-Patches werden auf die Ressourcen angewendet, bevor sie wiederhergestellt werden. Die JSON-Patches werden in einer Konfigurationszuordnung angegeben und auf die Konfigurationszuordnung wird im Wiederherstellungsbefehl verwiesen. Mit dieser Funktion können Sie die Wiederherstellung mithilfe einer anderen Speicherklasse durchführen.

Im folgenden Beispiel verwendet die App während der Bereitstellung ontap-nas als Speicherklasse für ihre persistenten Volumes. Es wird ein Backup der App mit dem Namen backup-postgresql-ontaps3 erstellt.





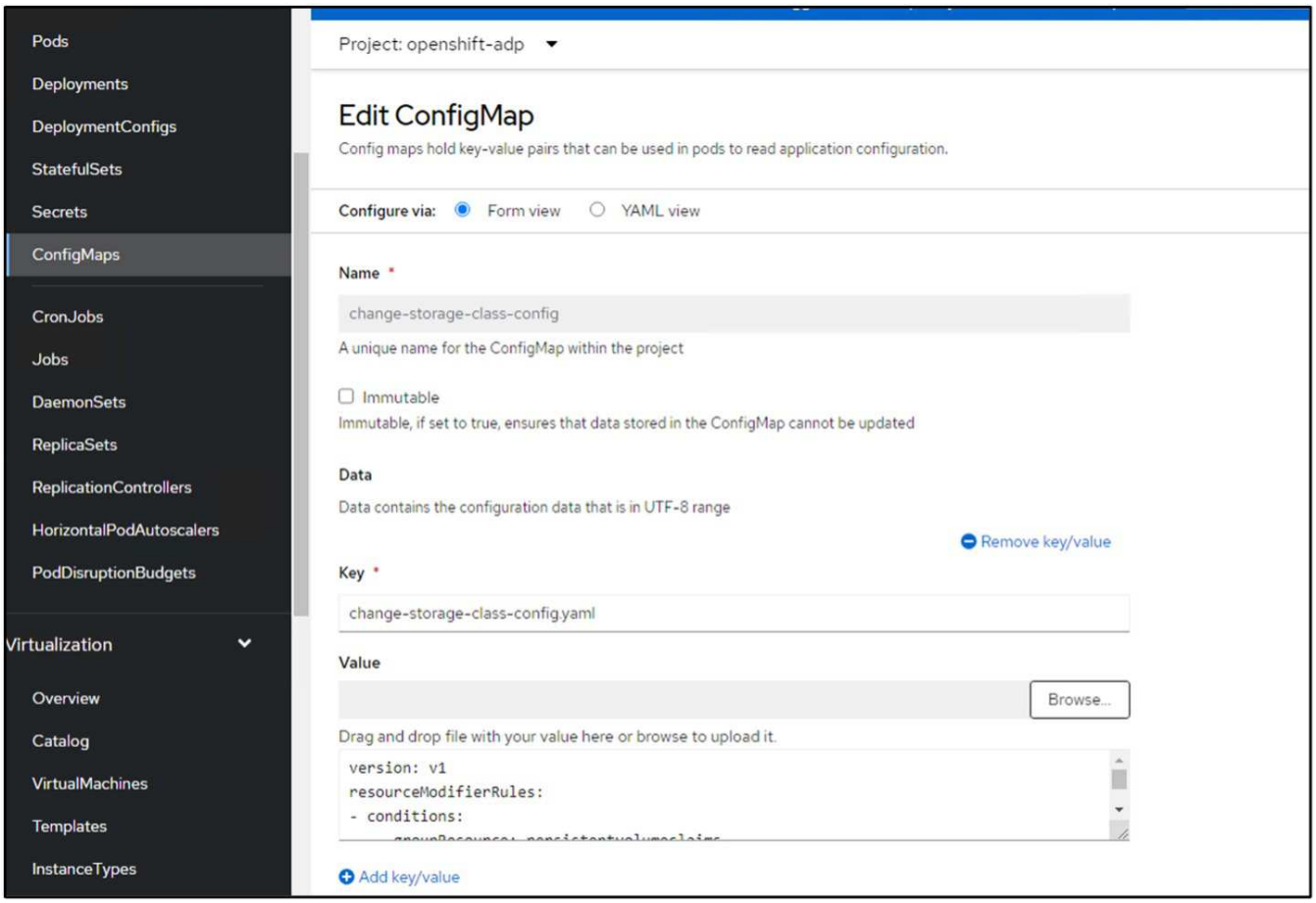
Simulieren Sie einen Verlust der App, indem Sie die App deinstallieren.

Um die VM mit einer anderen Speicherklasse wiederherzustellen, beispielsweise der Speicherklasse ontap-nas-eco, müssen Sie die folgenden zwei Schritte ausführen:

Schritt 1

Erstellen Sie wie folgt eine Konfigurationszuordnung (Konsole) im OpenShift-ADP-Namespace: Füllen Sie die Details wie im Screenshot gezeigt aus: Namespace auswählen: OpenShift-ADP Name: Change-Ontap-SC (kann ein beliebiger Name sein) Schlüssel: Change-Ontap-SC-Config.yaml: Wert:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



Das resultierende Konfigurationszuordnungsobjekt sollte folgendermaßen aussehen (CLI):

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"


BinaryData
====

Events:  <none>
```

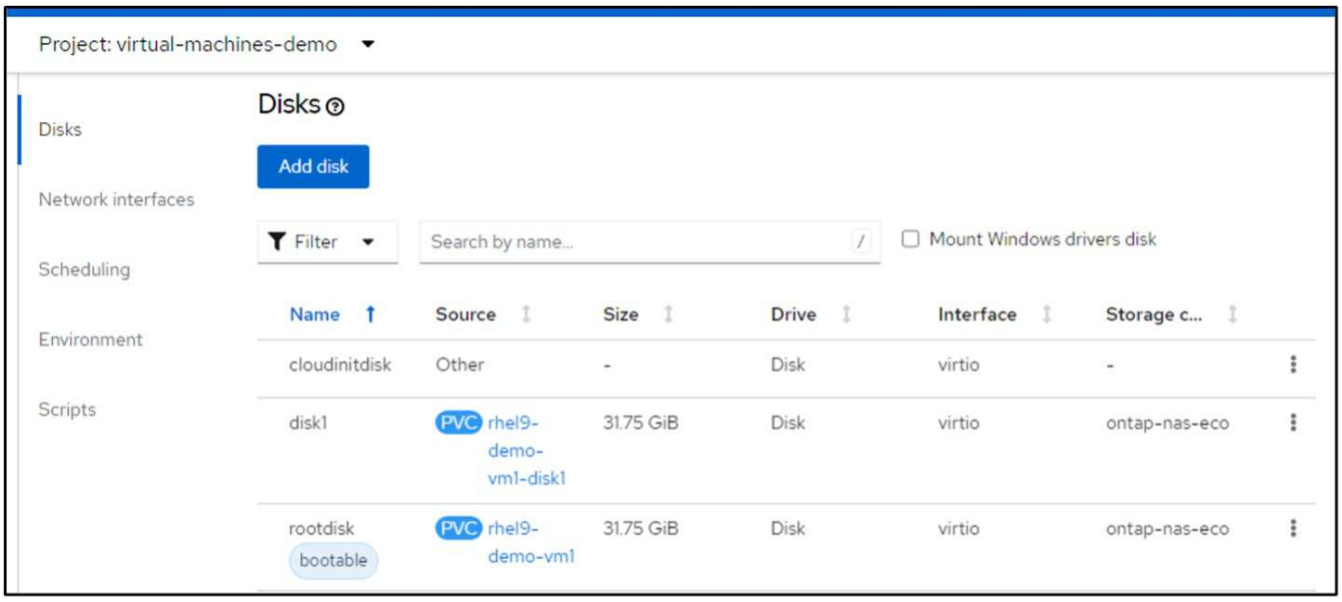
Diese Konfigurationszuordnung wendet die Ressourcenmodifikatorregel an, wenn die Wiederherstellung erstellt wird. Es wird ein Patch angewendet, um den Speicherklassennamen für alle persistenten Volume-Ansprüche, die mit rhel beginnen, durch ontap-nas-eco zu ersetzen.

Schritt 2

Um die VM wiederherzustellen, verwenden Sie den folgenden Befehl aus der Velero-CLI:

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

Die App wird im selben Namespace wiederhergestellt, in dem die persistenten Volume-Ansprüche mit der Speicherklasse ontap-nas-eco erstellt wurden.



Löschen von Backups und Wiederherstellungen mit Velero

In diesem Abschnitt wird beschrieben, wie Sie mithilfe von Velero Backups und Wiederherstellungen von Apps auf der OpenShift-Containerplattform löschen.

Alle Backups auflisten

Sie können alle Backup-CRs auflisten, indem Sie das OC CLI-Tool oder das Velero CLI-Tool verwenden. Laden Sie die Velero CLI gemäß den Anweisungen im"Velero-Dokumentation" .

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Löschen einer Sicherung

Sie können ein Backup-CR löschen, ohne die Object Storage-Daten zu löschen, indem Sie das OC CLI-Tool verwenden. Die Sicherung wird aus der CLI-/Konsolenausgabe entfernt. Da das entsprechende Backup jedoch nicht aus dem Objektspeicher entfernt wird, wird es erneut in der CLI-/Konsolenausgabe angezeigt.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

Wenn Sie das Backup CR UND die zugehörigen Objektspeicherdaten löschen möchten, können Sie dies mit dem Velero CLI-Tool tun.

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                       Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Löschen der Wiederherstellung

Sie können das Restore CR-Objekt entweder mit der OC CLI oder der Velero CLI löschen.

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

Sehen Sie sich Videos und Demos zu Hybrid-Multicloud-Lösungen mit NetApp an

Sehen Sie sich Videos zu Hybrid-Multicloud-Lösungen für Amazon Web Services mit NetApp an

Entdecken Sie die umfassende Videobibliothek von NetApp mit hybriden Multicloud-Lösungen für AWS mit NetApp. Sehen Sie sich Videos zu Gastspeicher, TCO-Einsparungen, zusätzlichen Datenspeichern und Migrations-Workflows für VMware Cloud auf AWS und Amazon FSx für ONTAP an, einschließlich Windows- und Linux-Szenarien.

Mit dem Gast verbundener Speicher

Windows Guest Connected Storage mit FSx ONTAP unter Verwendung von iSCSI

Linux Guest Connected Storage mit FSx ONTAP unter Verwendung von NFS

Gesamtbetriebskosten und zusätzliche Datenspeicher

VMware Cloud auf AWS TCO-Einsparungen mit Amazon FSx ONTAP

VMware Cloud auf AWS-Zusatzdatenspeicher mit Amazon FSx ONTAP

Migrations-Workflows (HCX)

VMware HCX-Bereitstellung und Konfigurations-Setup für VMC

vMotion-Migrationsdemonstration mit VMware HCX für VMC und FSx ONTAP

Demonstration der Kaltmigration mit VMware HCX für VMC und FSx ONTAP

Sehen Sie sich Videos zu Hybrid-Multicloud-Lösungen für Azure VMware Cloud mit NetApp an

Entdecken Sie die umfassende Videobibliothek von NetApp mit hybriden Multicloud-Lösungen für Azure VMware Solution (AVS) mit NetApp. Diese Sammlung enthält Videos zu zusätzlichen Datenspeichern, Notfallwiederherstellung und Migrations-Workflows.

Ergänzende Datenspeicher

Übersicht über den ergänzenden Datenspeicher der Azure VMware-Lösung mit Azure NetApp Files

Notfallwiederherstellung

Azure VMware Solution DR mit Cloud Volumes ONTAP, SnapCenter und JetStream

Migrations-Workflows (HCX)

Demonstration der Kaltmigration mit VMware HCX für AVS und ANF

vMotion-Demonstration mit VMware HCX für AVS und ANF

Demonstration der Massenmigration mit VMware HCX für AVS und ANF

Sehen Sie sich Videos zu Hybrid-Multicloud-Lösungen für Red Hat OpenShift mit NetApp an

Entdecken Sie die umfassende Videobibliothek von NetApp mit hybriden Multicloud-Lösungen für Red Hat OpenShift mit NetApp. Diese Sammlung enthält Demos zu Snapshots und Wiederherstellung für OpenShift auf AWS (ROSA) mit FSx ONTAP, Integration mit Trident, Failover und Failback für Apps sowie automatisierte Oracle RAC-Bereitstellung auf FlexPod mit Ansible.

Snapshots und Wiederherstellung

Snapshot/Wiederherstellung für Anwendungen auf Red Hat OpenShift Service auf AWS (ROSA)-Clustern mit Amazon FSx ONTAP -Speicher

Speicherintegration

Integration von FSx ONTAP mit Trident

Failover und Failback

Failover und Failback von Apps auf ROSA mit FSx ONTAP

Lösungsautomatisierung



Automatisierte Oracle 19c RAC-Bereitstellung auf FlexPod mit Ansible

Lesen Sie die Blogs zu Cloud-Lösungen von NetApp Experten

Lesen Sie die Blogs, die praktische Anleitungen und Best Practices zur Integration von ONTAP -Speicher in NetApp Cloud-Lösungen bieten.

VMware-Integration mit AWS und Amazon FSx für ONTAP

- "Migrieren Sie VMware-VMs mit Amazon EC2 und dem Amazon FSx ONTAP iSCSI-Protokoll zu AWS"
- "Amazon EVS ist jetzt in FSx für ONTAP integriert"
- "Amazon EVS kündigt Unterstützung für FSx für ONTAP an"
- "Konfigurieren Sie Hybrid Cloud mit FSx ONTAP und VMware Cloud on AWS SDDC mithilfe von VMware HCX"

Azure VMware-Lösung

- "Optimieren Sie speicher- und datenintensive VMware-Workloads in jeder Cloud"
- "VMware-Workloads zu Azure VMware Solution? Lesen Sie dies zuerst."

Google Cloud VMware Engine

- "Google Cloud NetApp Volumes Datenspeicherunterstützung für Google Cloud VMware Engine (NetApp)"
- "So verwenden Sie NetApp Volumes als Datenspeicher für Google Cloud VMware Engine (Google)"
- "NetApp Blog – Eine bessere Möglichkeit, Ihre speicherintensiven Apps in die Google Cloud zu migrieren"

Datenschutz und -verwaltung

- "3-2-1 Data Protection für VMware mit SnapCenter Plug-in und NetApp Backup and Recovery für VMs"
- "Observability für das moderne Rechenzentrum mit NetApp Cloud Insights"

NetApp für OpenShift-Container-Workloads

- "NetApp ONTAP dient gleichzeitig als Speicher für Protokolle in der Red Hat OpenShift-Containerplattform"

VMware Sovereign Cloud

- "Einführung der neuen Sovereign Cloud-Initiative"

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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