NetApp für GCP/GCVE

NetApp Solutions

NetApp
December 19, 2024

Inhalt

NetApp für GCP/GCVE

NetApp Funktionen für die Google Cloud Platform GSCVE

Weitere Informationen zu den Funktionen, die NetApp für die Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE) bietet – von NetApp als Storage-Gerät mit Gastverbindung oder als ergänzenden NFS-Datastore bis hin zur Migration von Workflows zur Erweiterung/Bursting in die Cloud, Backup/Restore und Disaster Recovery.

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

- "GCVE wird in GCP konfiguriert"
- "NetApp Storage-Optionen für GCVE"
- "NetApp/VMware Cloud-Lösungen"

GCVE wird in GCP konfiguriert

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

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

In-Guest-Storage ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP- und Google Cloud NetApp-Volumes mit GCVE.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

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

Details anzeigen "Konfigurationsschritte für GCVE".

NetApp Storage-Optionen für GCVE

NetApp Storage kann in GCP GCVE auf verschiedene Weise genutzt werden – entweder als „Raten“ verbunden oder als zusätzlicher NFS-Datenspeicher.

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

Google Cloud unterstützt NetApp Storage in den folgenden Konfigurationen:

- Cloud Volumes ONTAP (CVO) als Storage mit Gastzugriff
- Google Cloud NetApp Volumes (NetApp Volumes) als über das Gastsystem verbundenen Storage
- Google Cloud NetApp Volumes (NetApp Volumes) als ergänzender NFS-Datastore

Sehen Sie sich die detaillierten "Speicheroptionen für die Gastverbindung für GCVE". Sehen Sie sich die detaillierten "Zusätzliche NFS-Datastore-Optionen für GCVE".

Lesen Sie mehr über "Unterstützung von Google Cloud NetApp Volumes Datastore für Google Cloud VMware Engine (NetApp Blog)" oder "Verwenden von Google Cloud NetApp Volumes als Datastores für die Google Cloud VMware Engine (Google Blog)"

Anwendungsfälle Für Lösungen

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

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

"Informieren Sie sich über die NetApp Lösungen für Google Cloud GCVE"

Schutz von Workloads in GCP/GCVE

Applikationskonsistente Disaster Recovery mit NetApp SnapCenter und Veeam Replizierung

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die Storage mit Anbindung des Gastspeichers verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, die in Google Cloud ausgeführt werden.

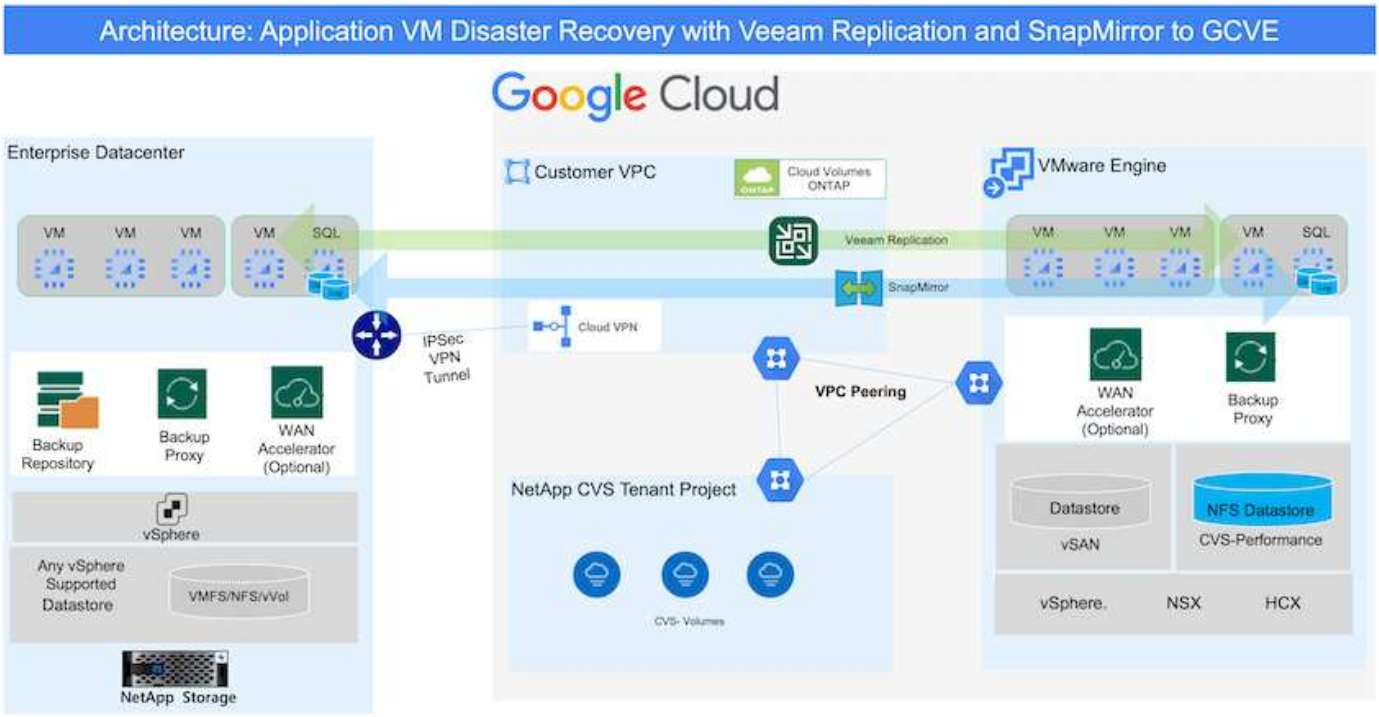
Autoren: Suresh ThopPay, NetApp

Überblick

Viele Kunden suchen nach einer effektiven Disaster Recovery-Lösung für ihre Applikations-VMs, die auf VMware vSphere gehostet werden. Viele von ihnen nutzen ihre bestehende Backup-Lösung, um im Diaster Recovery durchzuführen.
Oft erhöht diese Lösung die RTO und entspricht nicht ihren Erwartungen. Um RPO und RTO zu reduzieren, kann die Veeam VM-Replizierung sogar von On-Premises zu GCVE genutzt werden, sofern Netzwerkverbindungen und Umgebung mit entsprechenden Berechtigungen verfügbar sind.
HINWEIS: Veeam VM Replication schützt keine über VM-Gastsysteme verbundenen Storage-Geräte wie iSCSI- oder NFS-Mounts innerhalb der Gast-VM. Sie müssen sie separat schützen.

Für eine applikationskonsistente Replizierung für SQL VM und zur Reduzierung des RTO wurde SnapCenter zum Orchestrieren von snapmirror Vorgängen von SQL Datenbank- und Protokoll-Volumes eingesetzt.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

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

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

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

Übersicht Zur Lösungsimplementierung

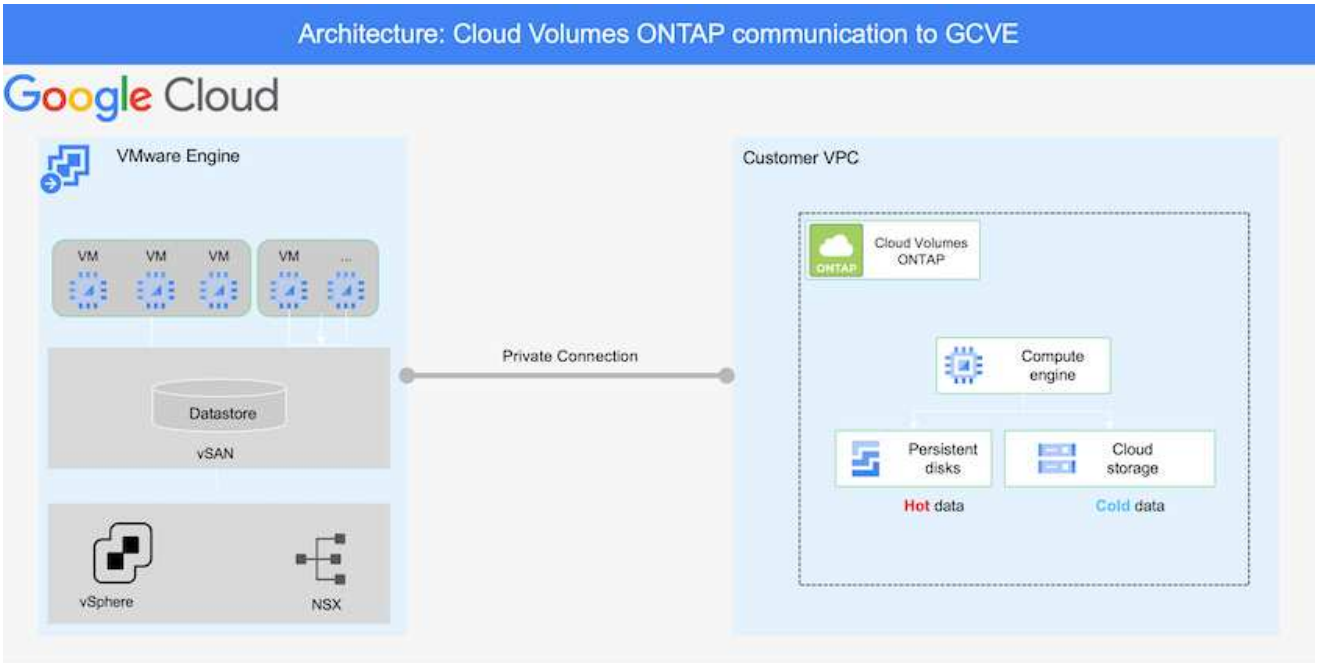
1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mit BlueXP innerhalb des entsprechenden Abonnements und virtuellen Netzwerks Cloud Volumes ONTAP mit der korrekten Instanzgröße bereit.
   a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
   b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.

3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Ausfalls die SnapMirror Beziehung mit BlueXP auf und lösen Sie Failover von Virtual Machines mit Veeam aus.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
   b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

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



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Überprüfen Sie den SQL VM-Schutz mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

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

Google Cloud NetApp Volumes für NFS Datastore und Cloud Volumes ONTAP für SQL Datenbanken und Protokoll können in jede VPC implementiert werden. GCVE sollte über eine private Verbindung zu diesem VPC verfügen, um den NFS-Datastore zu mounten und die VM mit den iSCSI-LUNs zu verbinden.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.
"Das Installationsverfahren finden Sie in der Veeam-Dokumentation"
Weitere Informationen finden Sie unter "Migration mit Veeam Replication"

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Failover von Microsoft SQL Server VM

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von

Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.

- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.

Disaster Recovery für Applikationen mit SnapCenter, Cloud Volumes ONTAP und Veeam Replication

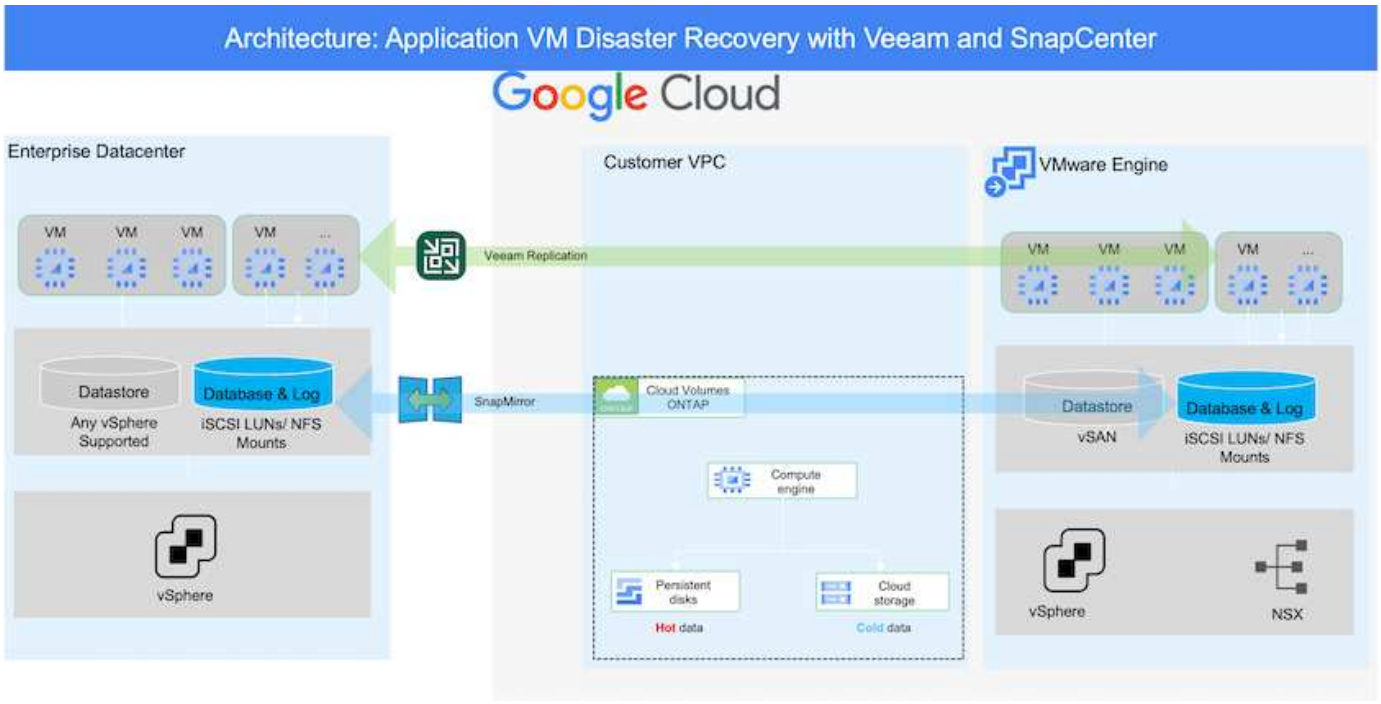
Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die Storage mit Anbindung des Gastspeichers verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, die in Google Cloud ausgeführt werden.

Autoren: Suresh ThopPay, NetApp

Überblick

Dies bezieht sich auf Applikationsdaten, doch was ist mit den eigentlichen VMs selbst. Disaster Recovery sollte alle abhängigen Komponenten, einschließlich Virtual Machines, VMDKs, Applikationsdaten und mehr, abdecken. Dazu kann SnapMirror zusammen mit Veeam verwendet werden, um Workloads, die von On-Premises zu Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen und gleichzeitig mit vSAN Storage für VM-VMDKs zu verwenden.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

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

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

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> ⓘ Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

Übersicht Zur Lösungsimplementierung

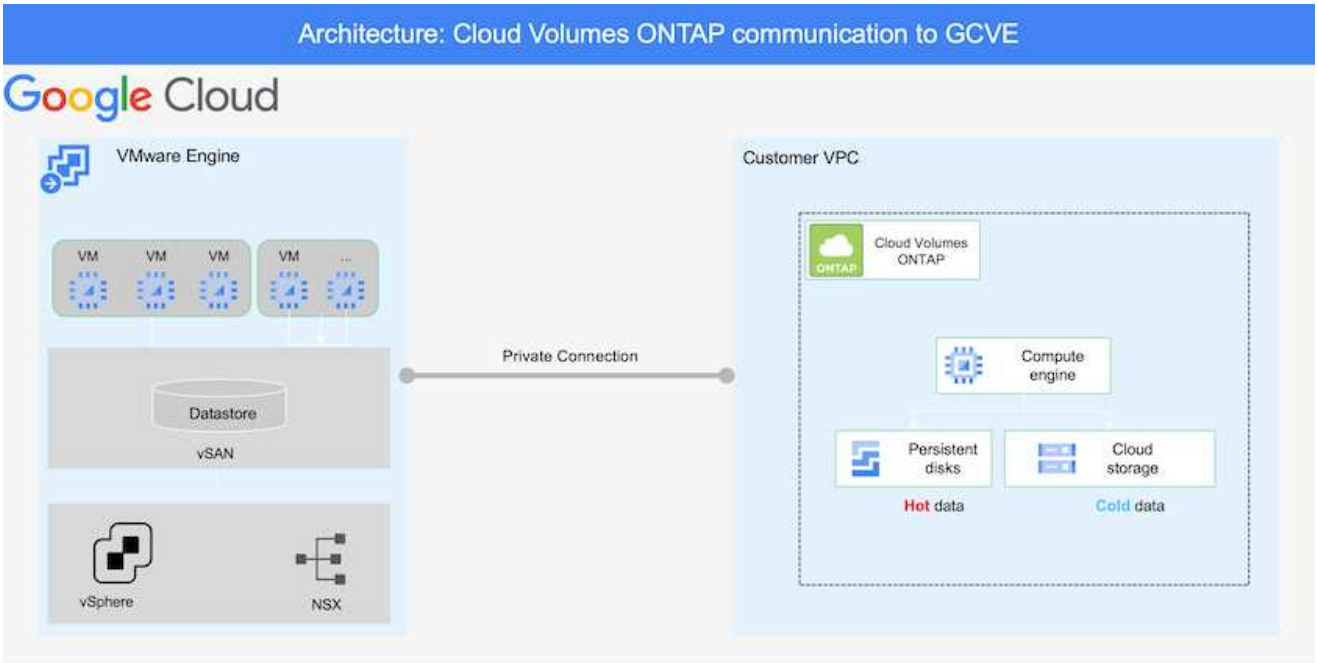
1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mithilfe von Cloud Manager Cloud Volumes ONTAP mit der richtigen Instanzgröße innerhalb des entsprechenden Abonnements und des virtuellen Netzwerks bereit.
   a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
   b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.

3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Notfallereignisses die SnapMirror Beziehung mithilfe von Cloud Manager auf und lösen Sie das Failover von Virtual Machines mit Veeam aus.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
   b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

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



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Einrichtung der Replikation mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

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

Cloud Volumes ONTAP kann in jede VPC implementiert werden und GCVE sollte über eine private Verbindung zu dieser VPC verfügen, damit VM-Verbindung mit iSCSI-LUNs hergestellt werden kann.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Das Installationsverfahren finden Sie in der Veeam-Dokumentation"]

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

VSphere VM Replication Job einrichten

Failover von Microsoft SQL Server VM

Failover von Microsoft SQL Server VM

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.

    - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
    - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
    - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.

Verwenden von Veeam Replication und Google Cloud NetApp Volumes Datastore für die Disaster Recovery in der Google Cloud VMware Engine

Für Unternehmen in Krisenzeiten ist ein umfassender Disaster Recovery-Plan unerlässlich. Viele Unternehmen nutzen das Cloud-Computing für ihren täglichen Betrieb und die Disaster Recovery. Dieser proaktive Ansatz kann teure Geschäftsunterbrechungen reduzieren oder beseitigen.

In diesem Artikel wird beschrieben, wie Sie mit Veeam Backup & Replication Disaster Recovery für lokale VMware VMs für die Google Cloud VMware Engine (GCVE) mit Google Cloud NetApp Volumes (NetApp Volumes) einrichten.

Überblick

Google Cloud NetApp Volumes ist ein Storage-Service von Google und NetApp, der für Google Cloud verfügbar ist. NetApp Volumes Service bietet hochperformanten NFS/SMB-Storage. Von VMware zertifizierter NetApp Volumes NFS-Storage kann als externer Datastore für ESXi-Hosts in GCVE verwendet werden. Die Benutzer müssen eine Peering-Verbindung zwischen ihrer GCVE Private Cloud und dem NetApp Volumes Projekt herstellen. Durch den Speicherzugriff innerhalb einer Region fallen keine Netzwerkgebühren an. Benutzer können NetApp Volumes in der Google Cloud Konsole erstellen und Löschschutz aktivieren, bevor sie Volumes als Datastores auf ihren ESXi Hosts mounten.

Mit NetApp Volumes basierten NFS-Datastores können Daten mithilfe einer validierten Drittanbieterlösung, die VM-Replizierungsfunktionen bietet, aus On-Premises-Systemen repliziert werden. Durch das Hinzufügen von NetApp-Volumes-Datastores wird die Bereitstellung kostenoptimiert, statt ein auf der Google Cloud VMware Engine (GCVE) basierendes SDDC mit einer großen Anzahl an ESXi-Hosts für den Storage 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 Datastore-Kapazität von NetApp-Volumes, um eine unabhängige Skalierung zur Erfüllung der Kapazitätsanforderungen zu ermöglichen.

Das Ziel besteht darin, eine kosteneffiziente Infrastruktur mit nur den Kernkomponenten für das Management eines Failovers zu erhalten. Ein Pilot-Light-Cluster kann im Falle eines Failovers weitere GCVE-Hosts erweitern und hinzufügen. Sobald der Failover behoben und der normale Betrieb wieder aufgenommen wurde, kann der Pilot-Light-Cluster seine Größe verringern und in einen kostengünstigen Betriebsmodus zurückkehren.

Zweck dieses Dokuments

In diesem Artikel wird beschrieben, wie Sie mithilfe der Veeam VM-Replikationssoftware eine Disaster Recovery für lokale VMware-VMs für GCVE mithilfe eines Google Cloud NetApp Volumes-Datenspeichers mit Veeam Backup & Replication einrichten.

Veeam Backup & Replication ist eine Backup- und Replizierungsapplikation 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 synchron. Die Replizierung bietet die beste Recovery Time Objective (RTO),

da am DR-Standort eine gemountete Kopie einer VM in einem startfähigen Zustand ist.

Dieser Replikationsmechanismus sorgt dafür, dass die Workloads im Falle eines Katastrophenfalls schnell in GCVE gestartet werden können. Die Veeam Backup & Replication Software optimiert darüber hinaus die Datenübertragung zur Replizierung über WAN und für langsame Verbindungen. Außerdem werden doppelte Datenblöcke, keine Datenblöcke, Swap-Dateien und „ausgeschlossene VM Gast-OS-Dateien“ herausgefiltert. Die Software komprimiert auch den Replikatverkehr. Um zu verhindern, dass Replikationsjobs die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Regeln zur Netzwerkdrosselung verwendet werden.

Der Replizierungsprozess in Veeam Backup & Replication ist auftraggesteuert, d. h. die Replizierung wird durch Konfiguration von Replizierungsjobs durchgeführt. Bei einem Ausfall kann ein Failover zur Wiederherstellung der VMs durch einen Failover auf die Replikatkopie ausgelöst werden. Wenn ein Failover durchgeführt wird, übernimmt eine replizierte VM die Rolle der ursprünglichen VM. Ein Failover kann auf den neuesten Status eines Replikats oder auf einen der bekanntermaßen fehlerfreien Wiederherstellungspunkte erfolgen. Dies ermöglicht bei Bedarf eine Wiederherstellung nach Ransomware-Angriffen oder isolierte Tests. Veeam Backup & Replication bietet mehrere Optionen für unterschiedliche Disaster-Recovery-Szenarien.

Lösungsüberblick

Diese Lösung deckt die folgenden grundlegenden Schritte ab:

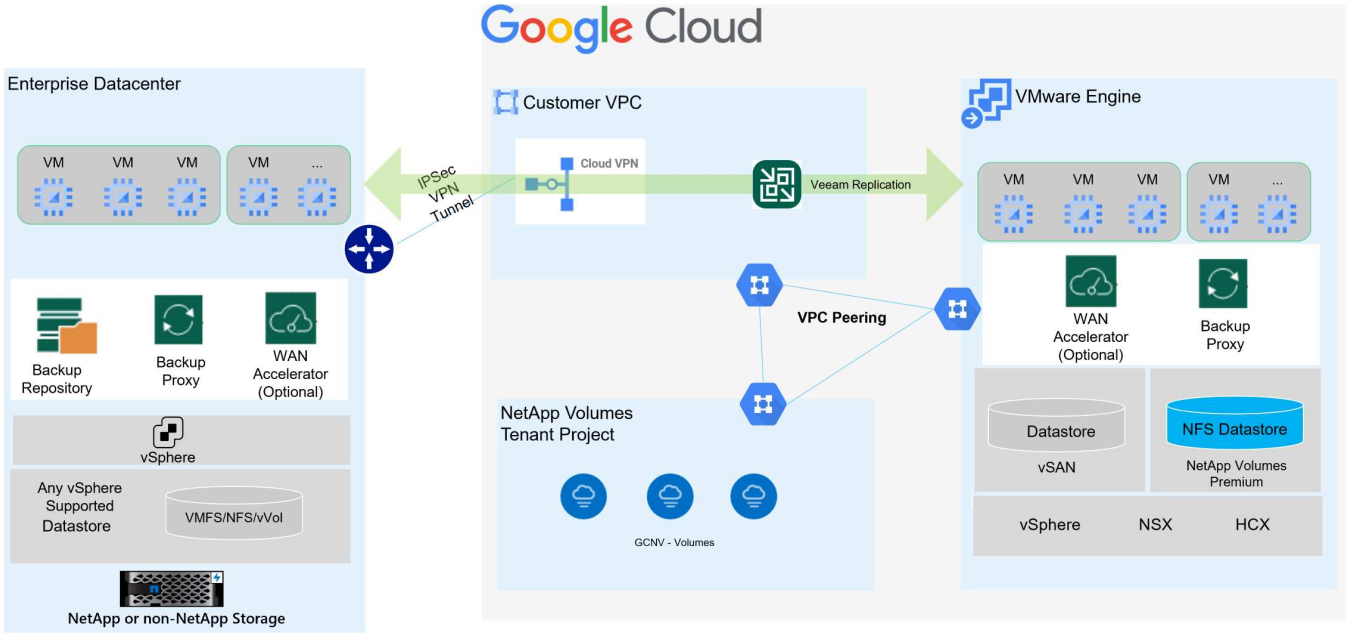
1. Erstellen Sie ein NFS-Volume mit Google Cloud NetApp Volumes
2. Mithilfe des GCP-Prozesses wird ein GCVE-Datastore aus dem NetApp Volumes NFS Volume erstellt.
3. Richten Sie einen Replikationsjob ein, um VM-Replikate mit Veeam Backup & Replication zu erstellen.
4. Erstellen Sie einen Failover-Plan und führen Sie ein Failover durch.
5. Wechseln Sie zurück zu den Produktions-VMs, sobald der Notfall abgeschlossen ist und der primäre Standort eingerichtet ist.

Bei der Erstellung eines Volumes in NetApp Volumes wird für die Verwendung als GCVE-Datastore nur NFS v3 unterstützt.

Weitere Informationen zur Verwendung von NetApp Volumes NFS-Volumes als Datastores für GCVE finden Sie im "Mit NFS-Volume als vSphere-Datastore, der von Google Cloud NetApp Volumes gehostet wird".

Der Netapp Architektur Sind

Das folgende Diagramm zeigt die Architektur der in dieser Dokumentation vorgestellten Lösung. Als Best Practice wird empfohlen, einen Veeam Backup & Replication Server sowohl am Standort als auch im GCVE SDDC zu verwenden. Backup und Recovery werden vor Ort vom Veeam Server durchgeführt und gemanagt, und die Replizierung wird vom Veeam Server im GCVE SDDC gemanagt. Diese Architektur bietet die höchste Verfügbarkeit bei einem Ausfall im primären Datacenter.



Voraussetzungen für die Veeam-Replikation zu GCVE- und NetApp-Volumes-Datastores

Diese Lösung erfordert die folgenden Komponenten und Konfigurationen:

1. NetApp Volumes bietet einen Speicherpool mit genügend freier Kapazität, um das zu erstellende NFS-Volume aufzunehmen.
2. Die Veeam Backup & Replication-Software wird in einer On-Premises-Umgebung mit entsprechender Netzwerkverbindung ausgeführt.
3. Stellen Sie sicher, dass die Backup-VM von Veeam Backup & Replication sowohl mit den Quell- als auch den Ziel-GCVE SDDC-Clustern verbunden ist.
4. Stellen Sie sicher, dass die Backup-VM von Veeam Backup & Replication sowohl auf den Quell- als auch auf den Ziel-GCVE-Clustern mit den VMs des Veeam Proxy-Servers verbunden ist.
5. Der Backup-Server muss in der Lage sein, Kurznamen aufzulösen und eine Verbindung zu Quell- und Ziel-vCenter herzustellen.

Die Benutzer müssen eine Peering-Verbindung zwischen ihrer GCVE Private Cloud und ihrem NetApp Volumes Projekt über das VPC-Netzwerk-Peering oder die privaten Verbindungsseiten innerhalb der VMware Engine Cloud-Konsolenbenutzeroberfläche herstellen.

> Veeam benötigt ein GCVE-Lösungs-Benutzerkonto mit erhöhten Privileges, wenn der GCVE vCenter-Server zum Veeam Backup and Replication-Inventar hinzugefügt wird. Weitere Informationen finden Sie in der Dokumentation zur Google Cloud Platform (GCP), "Erhöhung der VMware Engine Privileges".

Weitere Informationen finden Sie "Überlegungen und Einschränkungen" in der Dokumentation zu Veeam Backup & Replication.

Implementierungsschritte

In den folgenden Abschnitten werden die Implementierungsschritte beschrieben, um einen NFS-Datastore mithilfe von Google Cloud NetApp Volumes zu erstellen und zu mounten. Veeam Backup and Replication implementiert dann eine vollständige Disaster-Recovery-Lösung zwischen einem lokalen Datacenter und der

Google Cloud VMware Engine.

Erstellen Sie ein NetApp Volumes NFS-Volume und einen Datastore für GCVE

In "Mit NFS-Volume als vSphere-Datastore, der von Google Cloud NetApp Volumes gehostet wird" finden Sie eine Übersicht darüber, wie Sie Google Cloud NetApp Volumes als Datastore für GCVE verwenden.

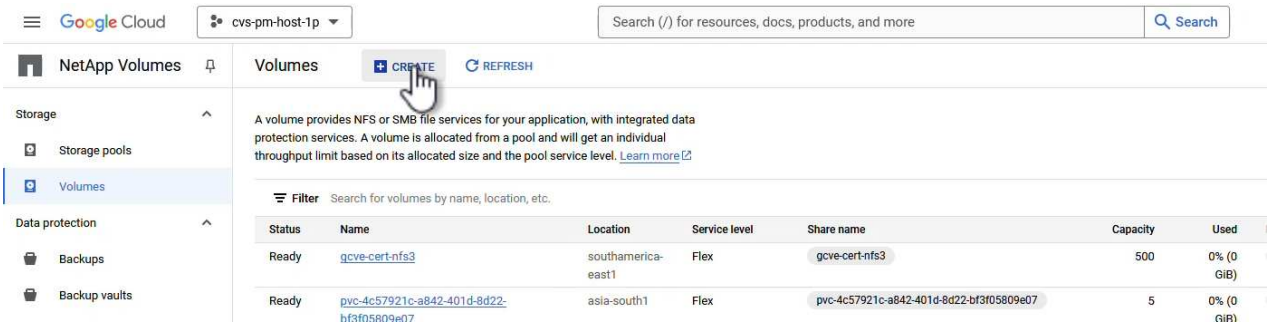
Führen Sie die folgenden Schritte aus, um einen NFS-Datastore für GCVE mit NetApp Volumes zu erstellen und zu verwenden:

Erstellen Sie ein NetApp Volumes NFS Volume

Auf Google Cloud NetApp Volumes wird über die GCP-Konsole (Google Cloud Platform) zugegriffen.

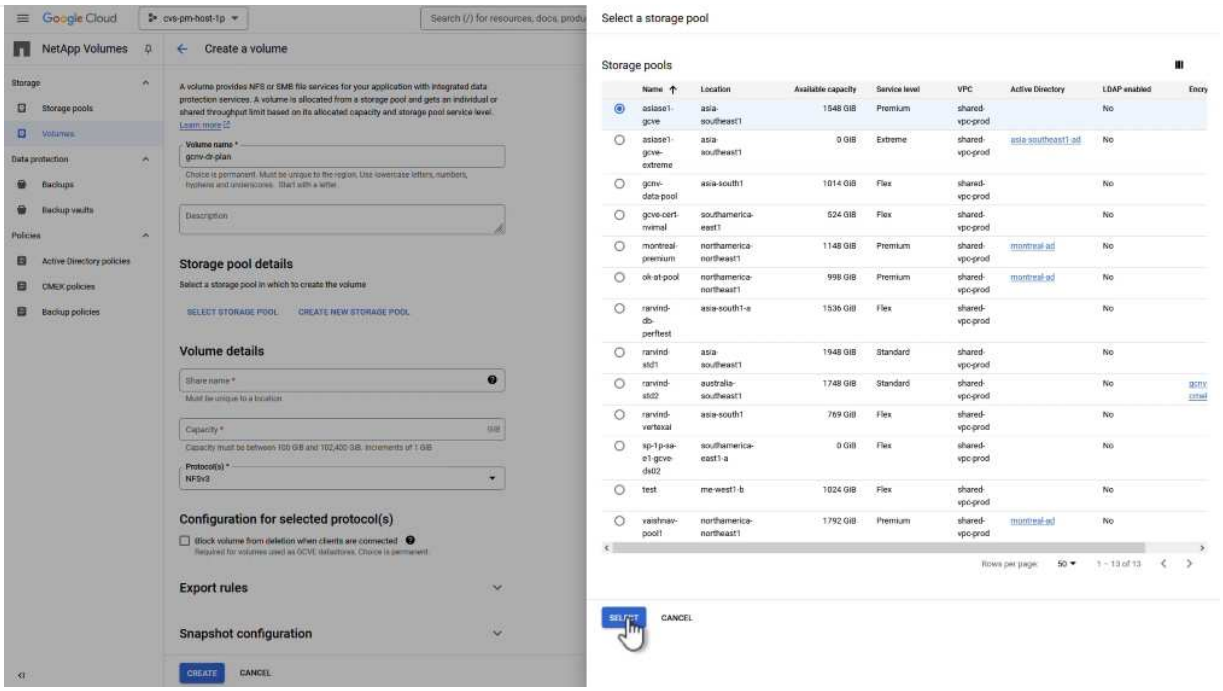
```
https://cloud.google.com/netapp/volumes/docs/configure-and-
use/volumes/create-volume["Erstellen eines Volumes"]In der
Dokumentation zu Google Cloud NetApp Volumes finden Sie detaillierte
Informationen zu diesem Schritt.
```

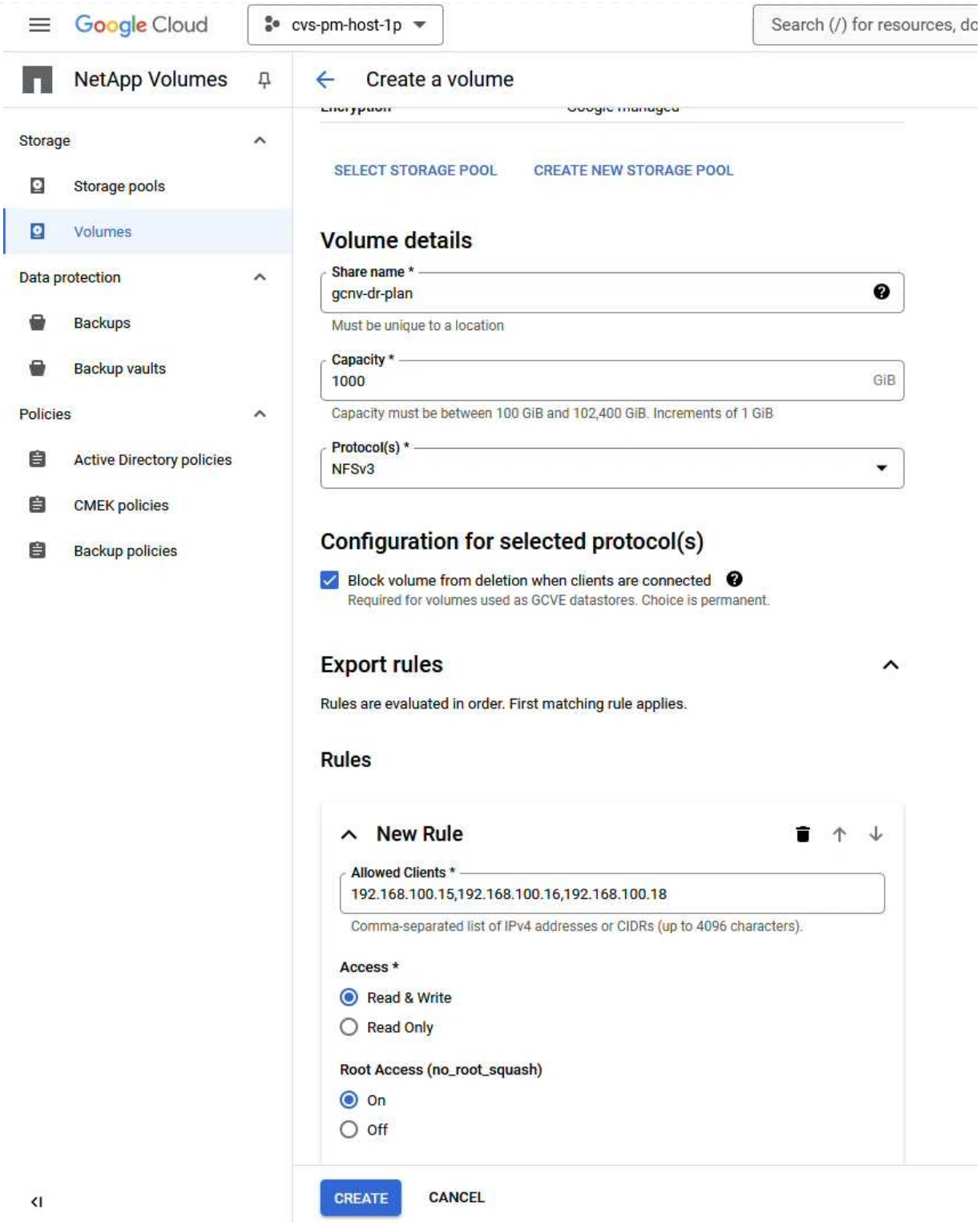
1. Navigieren Sie in einem Webbrowser zu https://console.cloud.google.com/ der GCP-Konsole, und melden Sie sich bei ihr an. Suchen Sie zunächst nach **NetApp Volumes**.
2. Klicken Sie in der Management-Oberfläche von **NetApp Volumes** auf **Erstellen**, um mit der Erstellung eines NFS-Volumes zu beginnen.



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 Volumes in gib.
   - Das zu verwendende Storage-Protokoll.
   - Aktivieren Sie das Kontrollkästchen zum Sperren des Volumes von der Löschung, wenn Clients verbunden sind* (wird von GCVE beim Einhängen als Datastore benötigt).
   - 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 Etiketten für das Volume erstellen.

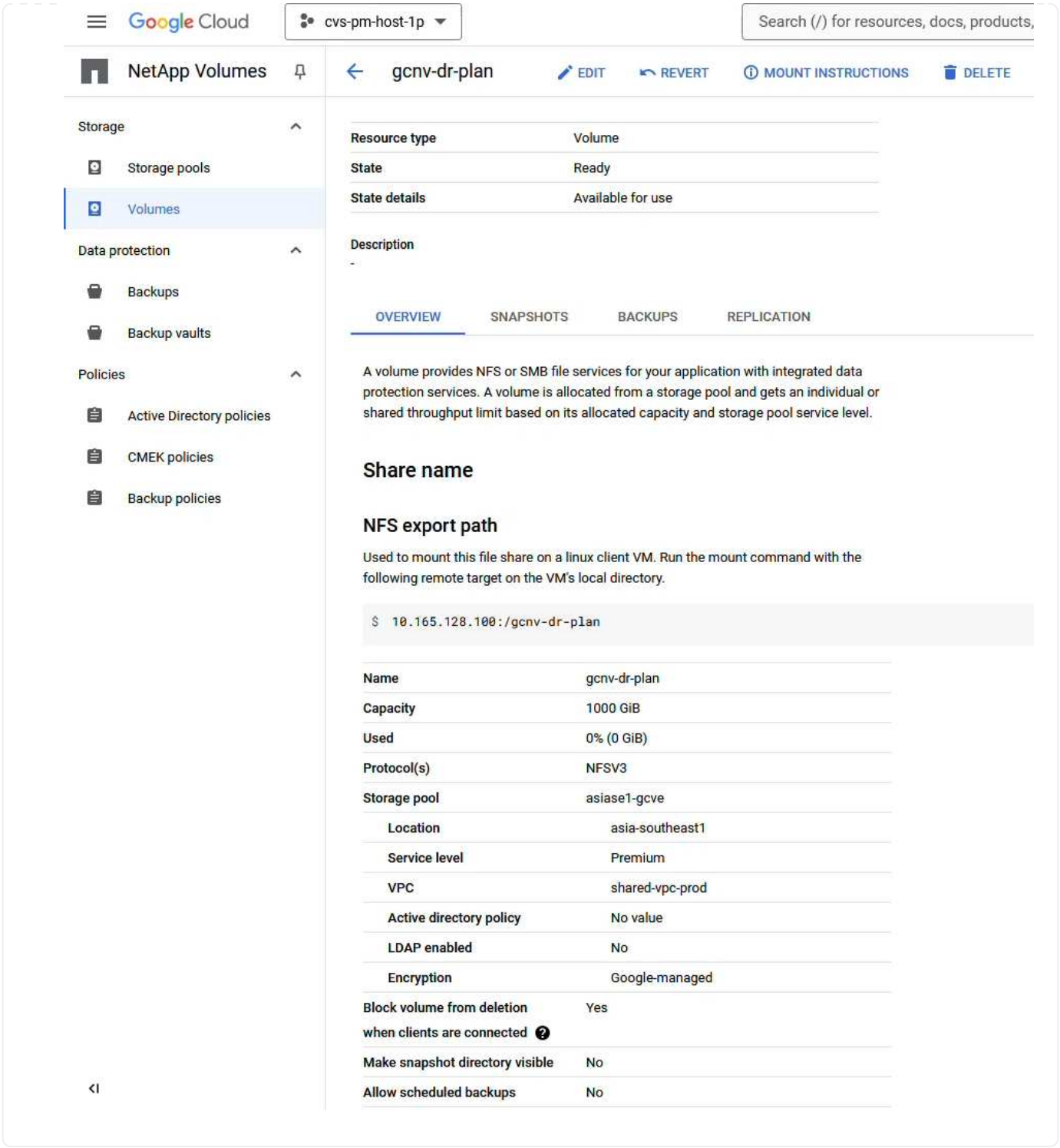
> Bei der Erstellung eines Volumes in NetApp Volumes wird für die Verwendung als GCVE-Datastore nur NFS v3 unterstützt.


Google Cloud
cvs-pm-host-1p
Search (/) for resources, docs, produ
NetApp Volumes
Create a volume
Storage
Storage pools
Volumes
Data protection
Backups
Backup vaults
Policies
Active Directory policies
CMEK policies
Backup policies
A volume provides NFS or SMB file services for your application with integrated data protection services. A volume is allocated from a storage pool and gets an individual or shared throughput limit based on its allocated capacity and storage pool service level.
Learn more
Volume name *
gcnv-dr-plan
Choice is permanent. Must be unique to the region. Use lowercase letters, numbers, hyphens and underscores. Start with a letter.
Description
Storage pool details
Select a storage pool in which to create the volume
SELECT STORAGE POOL
CREATE NEW STORAGE POOL
Volume details
Share name *
Must be unique to a location
Capacity *
GiB
Capacity must be between 100 GiB and 102,400 GiB. Increments of 1 GiB
Protocol(s) *
NFSv3
Configuration for selected protocol(s)
Block volume from deletion when clients are connected
Required for volumes used as OCVE datastores. Choice is permanent.
Export rules
Snapshot configuration
CREATE
CANCEL
Select a storage pool
Storage pools
Name
Location
Available capacity
Service level
VPC
Active Directory
LDAP enabled
Encry
asiase1-gcve
asia-southeast1
1548 GiB
Premium
shared-vpc-prod
No
asiase1-gcve-extreme
asia-southeast1
0 GiB
Extreme
shared-vpc-prod
asia-southeast1-ad
No
gcnv-data-pool
asia-south1
1014 GiB
Flex
shared-vpc-prod
No
gcve-cert-nvimal
southamerica-east1
524 GiB
Flex
shared-vpc-prod
No
montreal-premium
northamerica-northeast1
1148 GiB
Premium
shared-vpc-prod
montreal-ad
No
ok-at-pool
northamerica-northeast1
998 GiB
Premium
shared-vpc-prod
montreal-ad
No
ranvind-db-perftest
asia-south1-a
1536 GiB
Flex
shared-vpc-prod
No
ranvind-std1
asia-southeast1
1948 GiB
Standard
shared-vpc-prod
No
ranvind-std2
australia-southeast1
1748 GiB
Standard
shared-vpc-prod
No
gcnv cmek
ranvind-vertexai
asia-south1
769 GiB
Flex
shared-vpc-prod
No
sp-1p-sa-e1-gcve-ds02
southamerica-east1-a
0 GiB
Flex
shared-vpc-prod
No
test
me-west1-b
1024 GiB
Flex
shared-vpc-prod
No
vaishnav-pool1
northamerica-northeast1
1792 GiB
Premium
shared-vpc-prod
montreal-ad
No
Rows per page: 50
1 – 13 of 13
SELECT
CANCEL



Klicken Sie auf **Create**, um die Erstellung des Volumes abzuschließen.

4. Sobald das Volume erstellt wurde, kann der für das Mounten des Volume erforderliche NFS-Exportpfad auf der Eigenschaftenseite des Volume angezeigt werden.



Mounten Sie den NFS-Datastore in GCVE

Zum Zeitpunkt dieses Schreibens zum Mounten eines Datastore in GCVE muss ein GCP-Support-Ticket geöffnet werden, damit das Volume als NFS-Datastore gemountet werden kann.

Weitere Informationen finden Sie unter "Mit NFS-Volume als vSphere-Datastore, der von Google Cloud NetApp Volumes gehostet wird" .

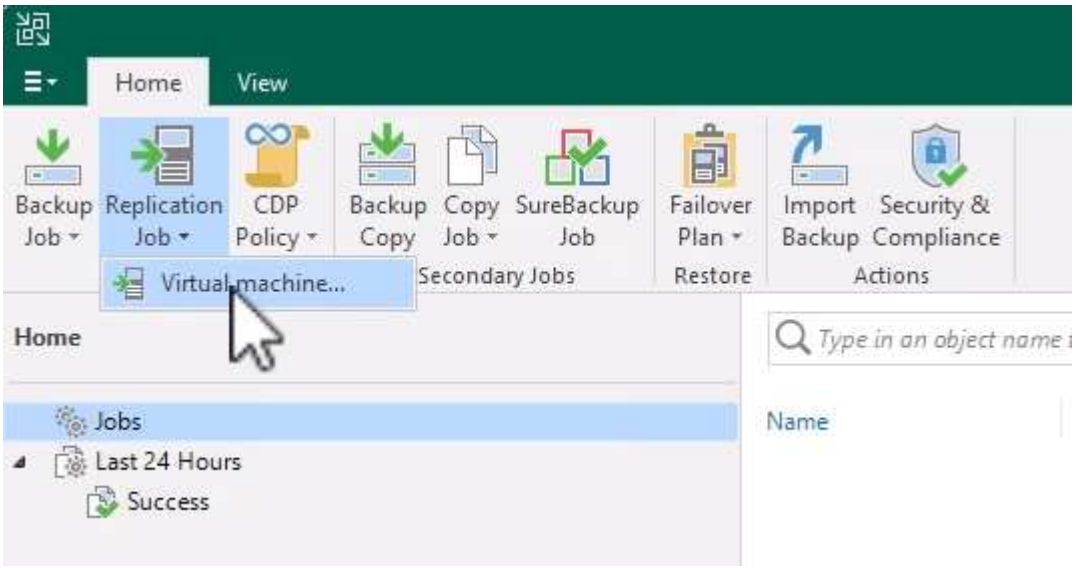
Replizieren von VMs zu GCVE und Ausführen von Failover-Plänen und Failback

Replizieren von VMs zum NFS-Datenspeicher in GCVE

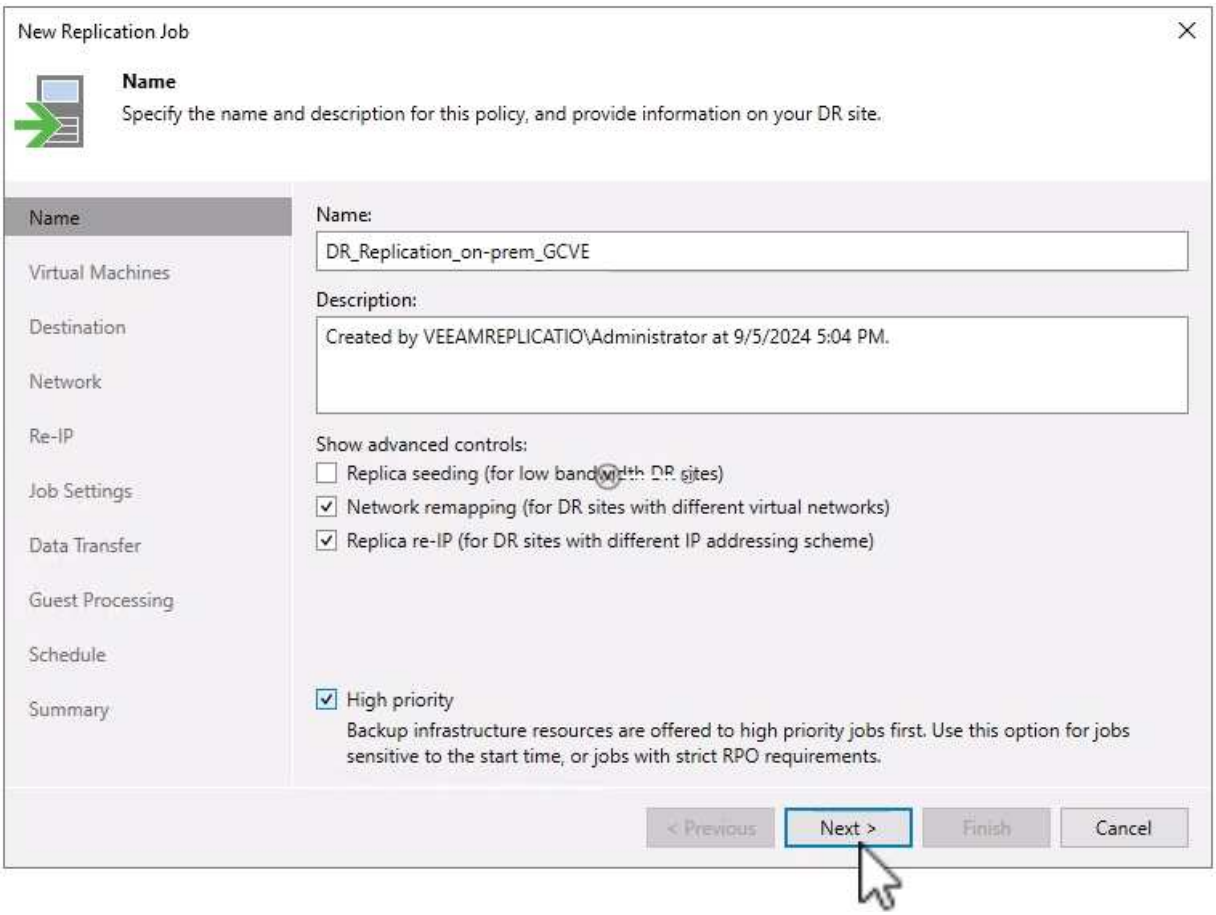
Veeam Backup & Replication nutzt VMware vSphere Snapshot-Funktionen während der Replikation, Veeam Backup & Replication fordert VMware vSphere auf, einen VM-Snapshot zu erstellen. Der VM-Snapshot ist die Point-in-Time-Kopie einer VM, die virtuelle Laufwerke, den Systemstatus, die Konfiguration und Metadaten umfasst. Veeam Backup & Replication verwendet den Snapshot als Datenquelle für die Replizierung.

Führen Sie zum Replizieren von VMs die folgenden Schritte aus:

1. Öffnen Sie die Veeam Backup & Replication Console.
2. Klicken Sie auf der Registerkarte **Home** auf **Replikationsjob > Virtuelle Maschine…**



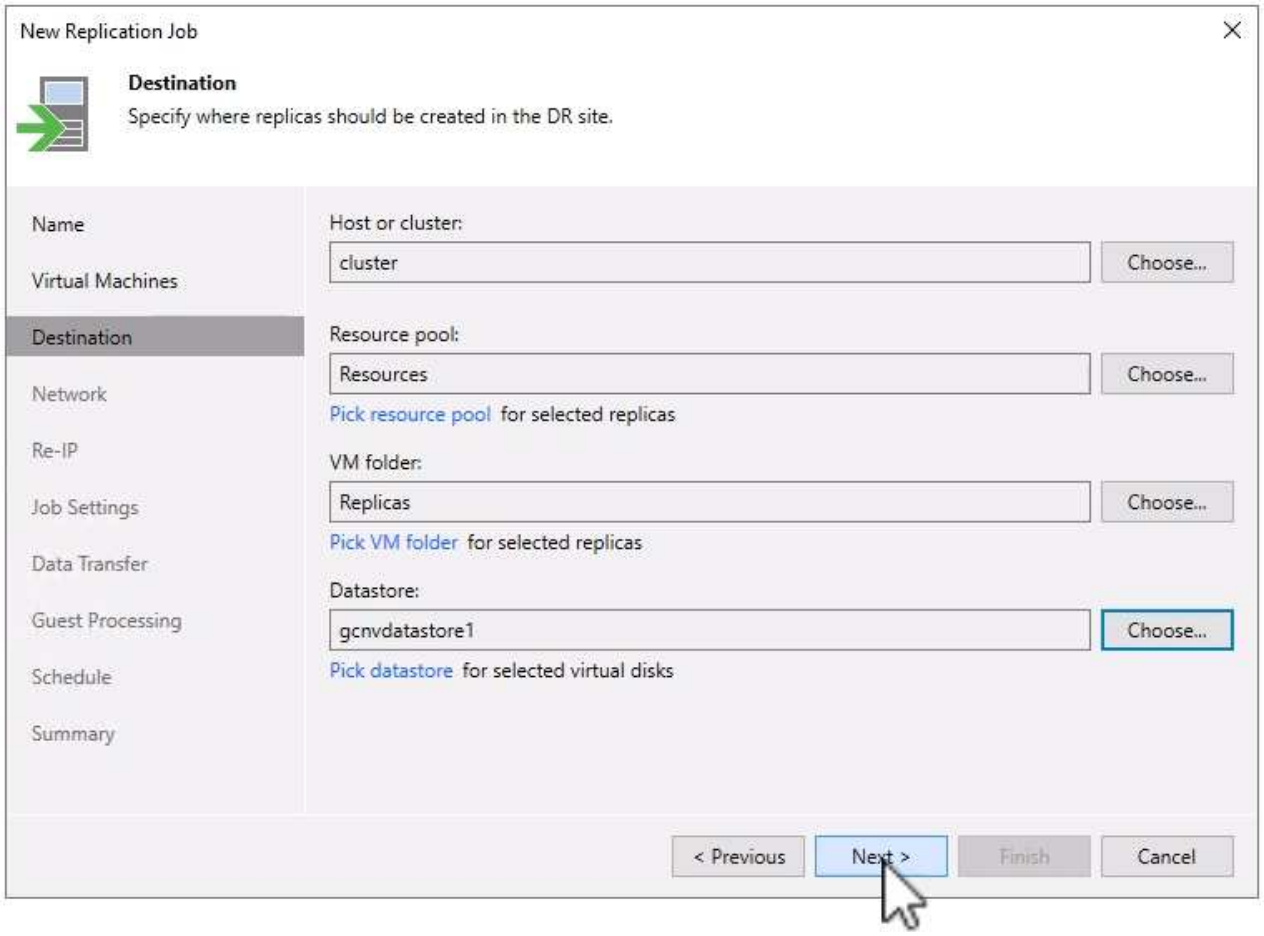
3. Geben Sie auf der Seite **Name** des Assistenten **New Replication Job** einen Jobnamen an und aktivieren Sie die entsprechenden Kontrollkästchen für die erweiterte Steuerung.
   - Aktivieren Sie das Kontrollkästchen Replikat-Seeding, wenn bei der Verbindung zwischen On-Premises und GCP eine eingeschränkte Bandbreite vorhanden ist.
   - Aktivieren Sie das Kontrollkästchen Netzwerkzuordnung (für GCVE SDDC-Standorte mit unterschiedlichen Netzwerken), wenn die Segmente im GCVE SDDC nicht mit denen der standortgebundenen Netzwerke übereinstimmen.
   - Aktivieren Sie das Kontrollkästchen Replikatre-IP (für DR-Standorte mit unterschiedlichem IP-Adressierungsschema), wenn sich das IP-Adressierungsschema am Produktionsstandort vor Ort vom Schema am GCVE-Zielstandort unterscheidet.



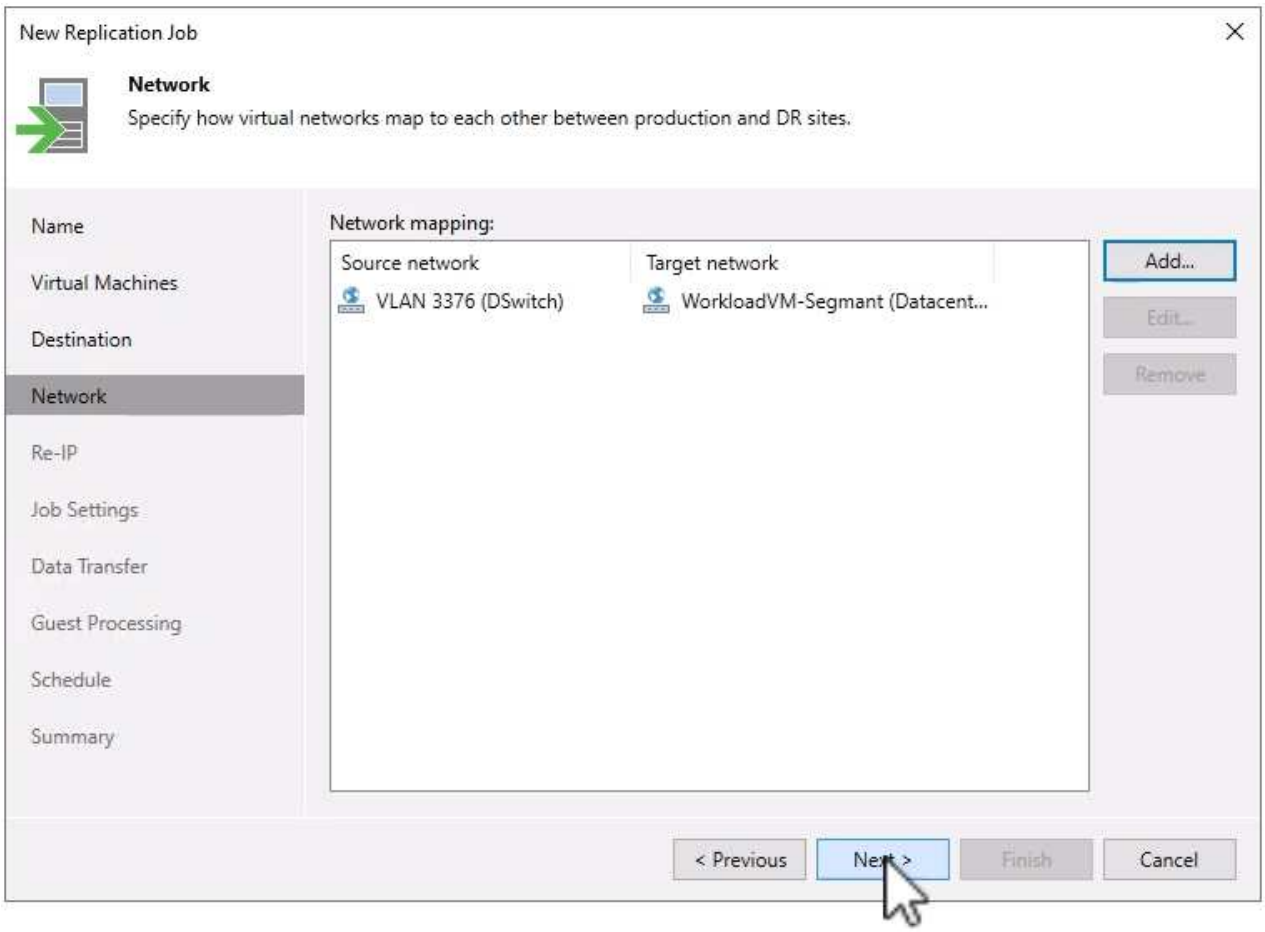
4. Wählen Sie auf der Seite **Virtuelle Maschinen** die VMs aus, die auf den NetApp-Volumes-Datastore repliziert werden sollen, der an ein GCVE SDDC angeschlossen ist. Klicken Sie auf **Hinzufügen**, wählen Sie dann im Fenster **Objekt hinzufügen** die erforderlichen VMs oder VM-Container aus und klicken Sie auf **Hinzufügen**. Klicken Sie Auf **Weiter**.

> Die Virtual Machines können auf vSAN platziert werden, um die verfügbare vSAN Datastore-Kapazität zu füllen. In einem Pilotcluster ist die nutzbare Kapazität eines vSAN-Clusters mit 3 Nodes begrenzt. Die restlichen Daten lassen sich problemlos auf Google Cloud NetApp Volumes Datastores platzieren, damit die VMs wiederhergestellt werden können. Darüber hinaus kann das Cluster später erweitert werden, um die CPU-/mem-Anforderungen zu erfüllen.

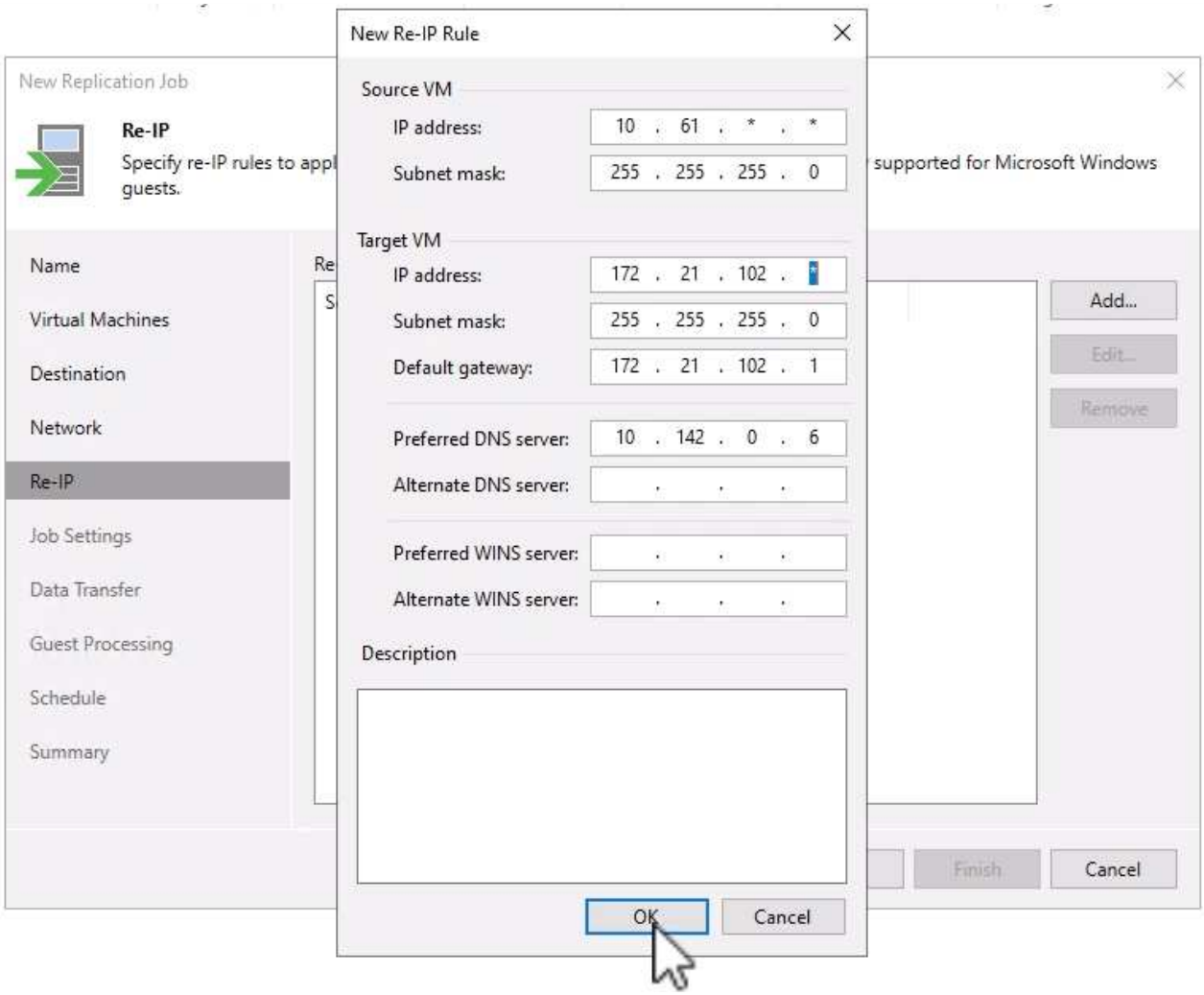
5. Wählen Sie auf der Seite **Ziel** das Ziel als GCVE SDDC-Cluster/Hosts und den entsprechenden Ressourcenpool, VM-Ordner und NetApp-Volumes-Datastore für die VM-Replikate aus. Klicken Sie auf **Weiter**, um fortzufahren.



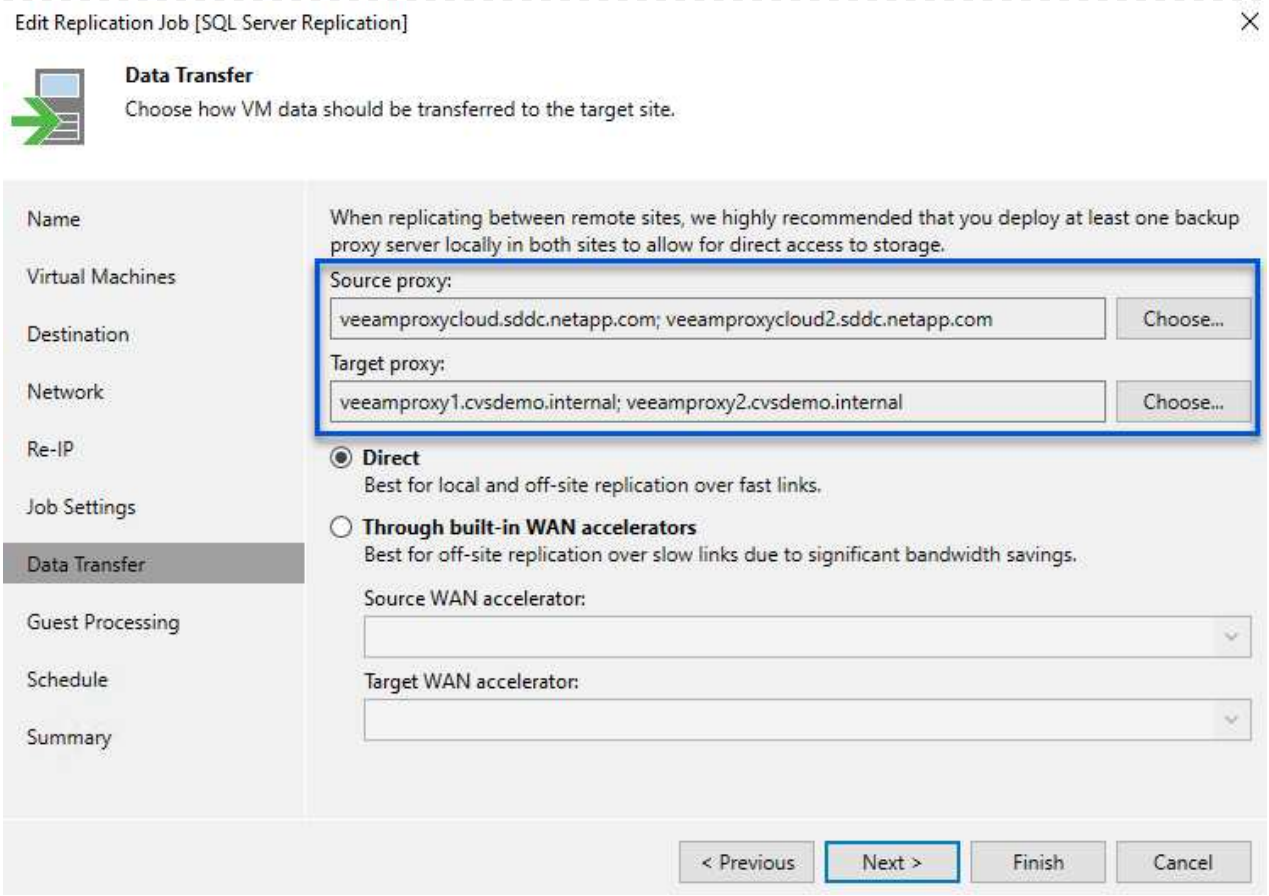
6. Erstellen Sie auf der Seite **Network** die Zuordnung zwischen Quell- und Ziel-virtuellen Netzwerken nach Bedarf. Klicken Sie auf **Weiter**, um fortzufahren.



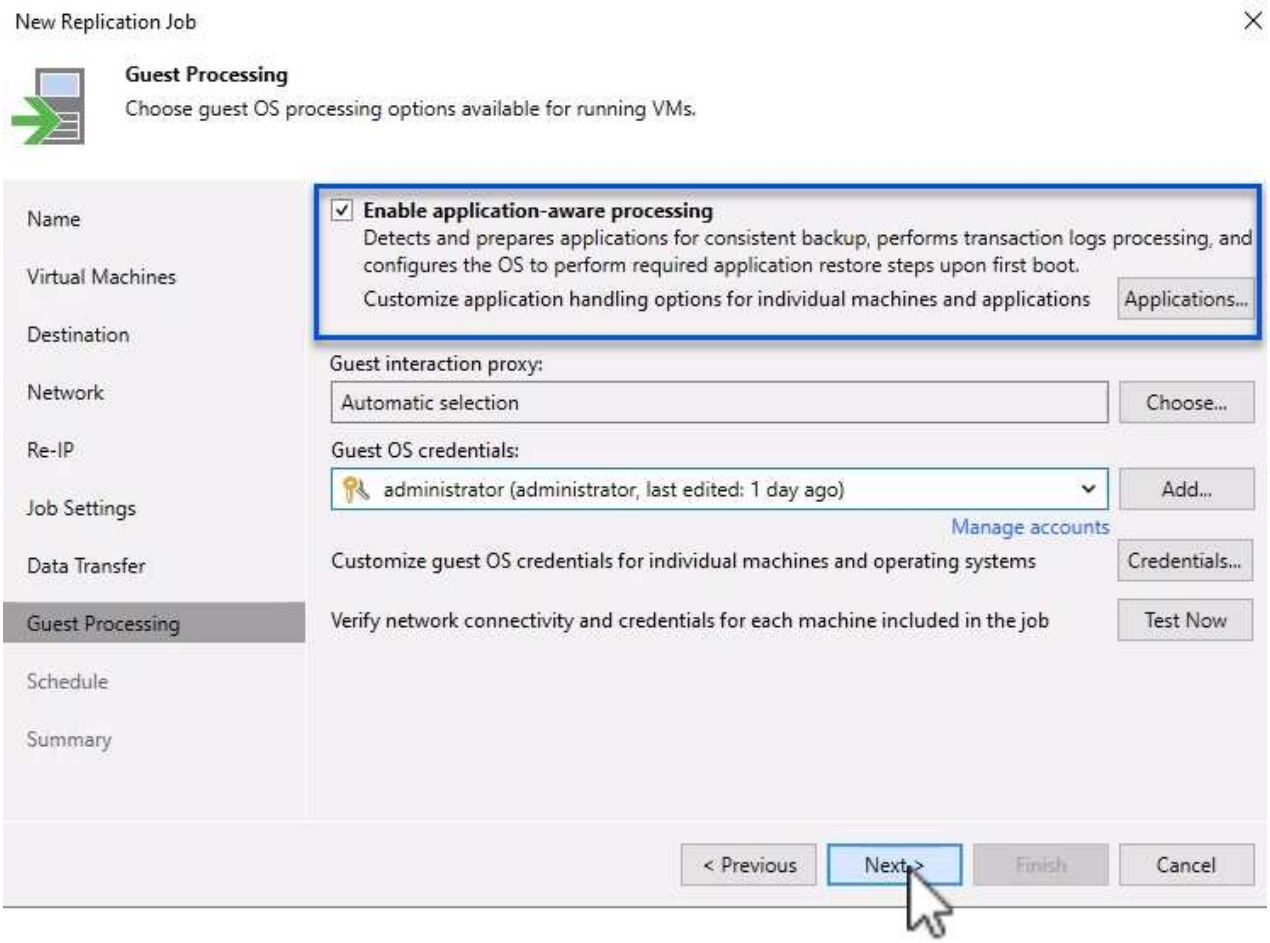
7. Klicken Sie auf der Seite **Re-IP** auf die Schaltfläche **Hinzufügen…**, um eine neue Re-ip-Regel hinzuzufügen. Geben Sie die ip-Bereiche der Quell- und Ziel-VM an, um das Netzwerk anzugeben, das im Falle eines Failovers auf die Quell-VMs angewendet wird. Verwenden Sie Sternchen, um einen Adressbereich anzugeben, der für dieses Oktett angegeben ist. Klicken Sie auf **Weiter**, um fortzufahren.



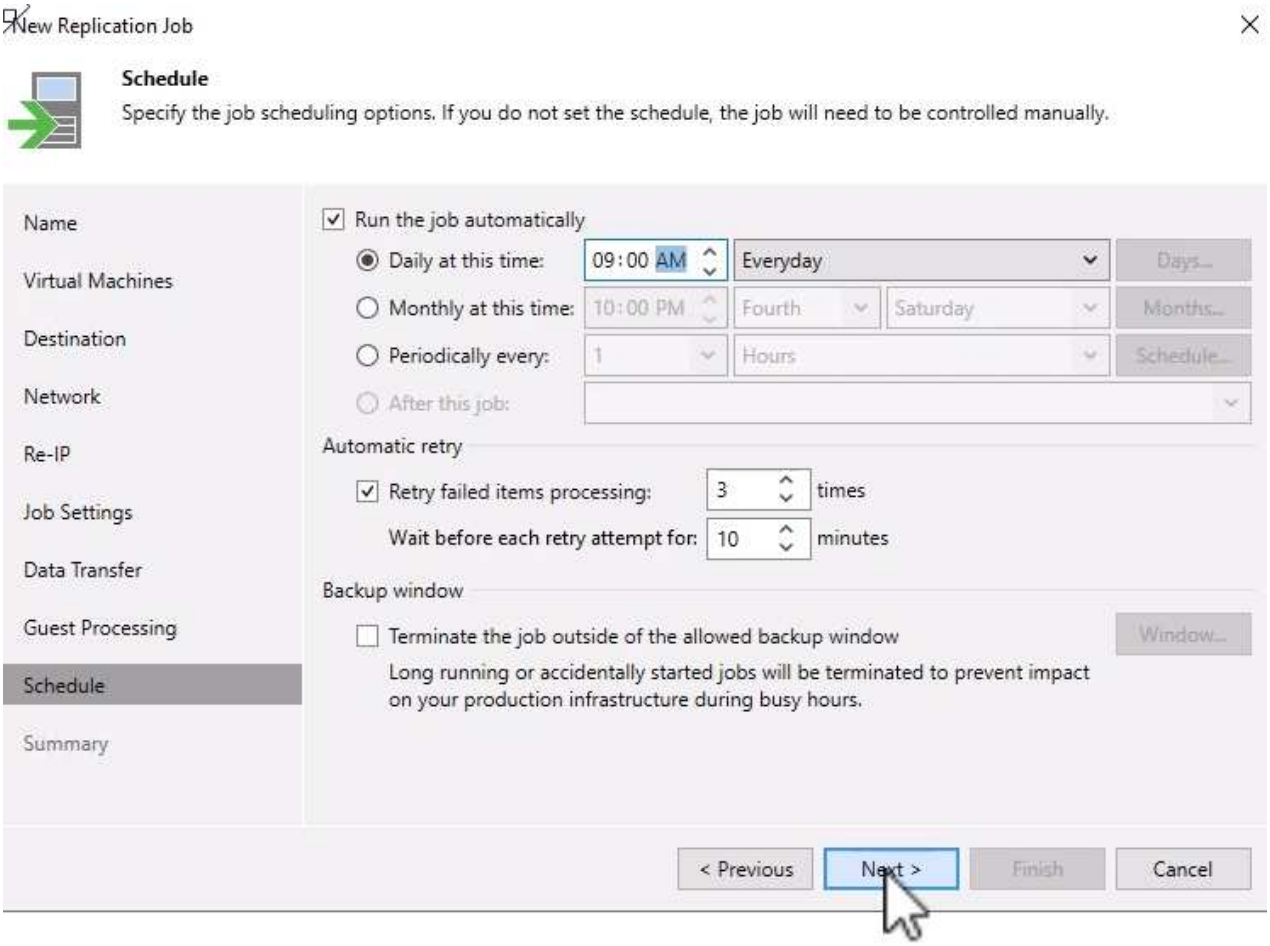
8. Geben Sie auf der Seite **Job-Einstellungen** das Backup-Repository an, das Metadaten für VM-Replikate speichert, die Aufbewahrungsrichtlinie und wählen Sie unten die Schaltfläche für **Advanced…** für zusätzliche Jobeinstellungen. Klicken Sie auf **Weiter**, um fortzufahren.
9. Wählen Sie unter **Datenübertragung** die Proxy-Server aus, die sich an den Quell- und Zielstandorten befinden, und lassen Sie die Option direkt ausgewählt. Bei entsprechender Konfiguration können auch WAN-Beschleuniger ausgewählt werden. Klicken Sie auf **Weiter**, um fortzufahren.



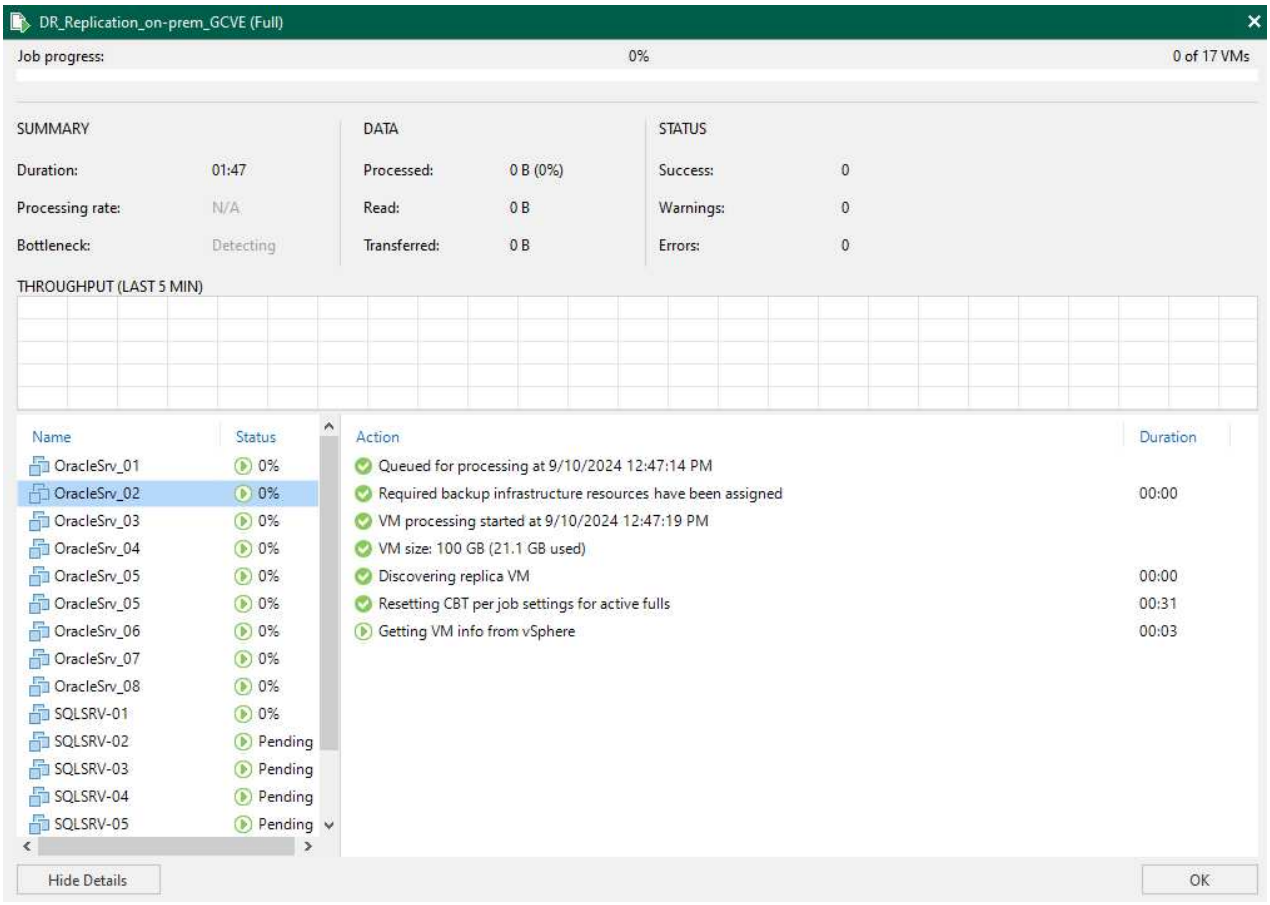
10. Aktivieren Sie auf der Seite **Guest Processing** das Kontrollkästchen für **enable Application-aware processing**, falls erforderlich, und wählen Sie die **Guest OS Credentials** aus. Klicken Sie auf **Weiter**, um fortzufahren.



11. Legen Sie auf der Seite **Schedule** die Zeiten und Häufigkeit fest, zu denen der Replikationsjob ausgeführt wird. Klicken Sie auf **Weiter**, um fortzufahren.



12. Überprüfen Sie abschließend die Jobeinstellungen auf der Seite **Zusammenfassung**. Aktivieren Sie das Kontrollkästchen, um den Job auszuführen, wenn ich auf Fertig stellen* klicke, und klicken Sie auf **Fertig stellen**, um die Erstellung des Replikationsjobs abzuschließen.
13. Nach der Ausführung kann der Replikationsjob im Fenster Job-Status angezeigt werden.



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

Erstellen eines Failover-Plans

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

Erstellen Sie nach Abschluss der ersten Replikation oder des Seeding einen Failover-Plan. Dieser Plan dient als strategisches Modell zur Orchestrierung des Failovers abhängiger VMs, entweder einzeln oder als Gruppe. Sie definiert die Verarbeitungsreihenfolge der VMs, integriert erforderliche Boot-Verzögerungen 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 der voneinander abhängigen Systeme bei einem Failover aufrechterhalten.

Beim Erstellen des Plans identifiziert Veeam Backup & Replication automatisch die aktuellsten Wiederherstellungspunkte und verwendet diese, um die VM-Replikate zu initiieren.

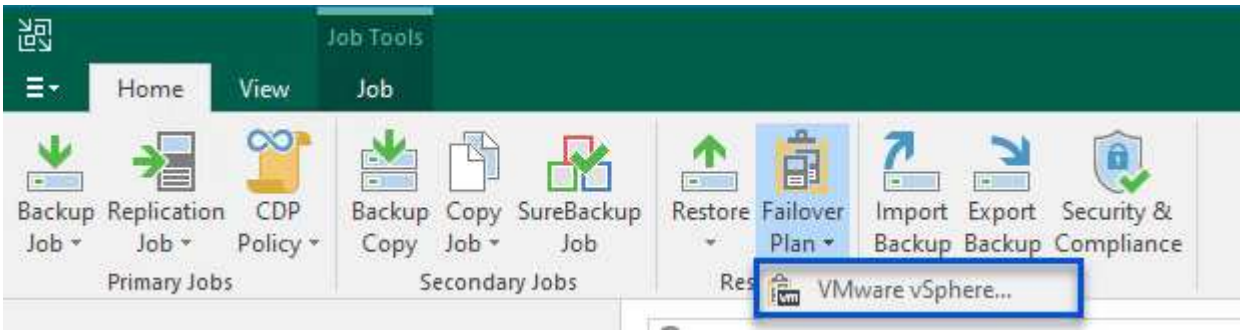
ⓘ Der Failover-Plan kann nur erstellt werden, wenn die erste Replikation abgeschlossen ist und sich die VM-Replikate im Bereitschaftszustand befinden.

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

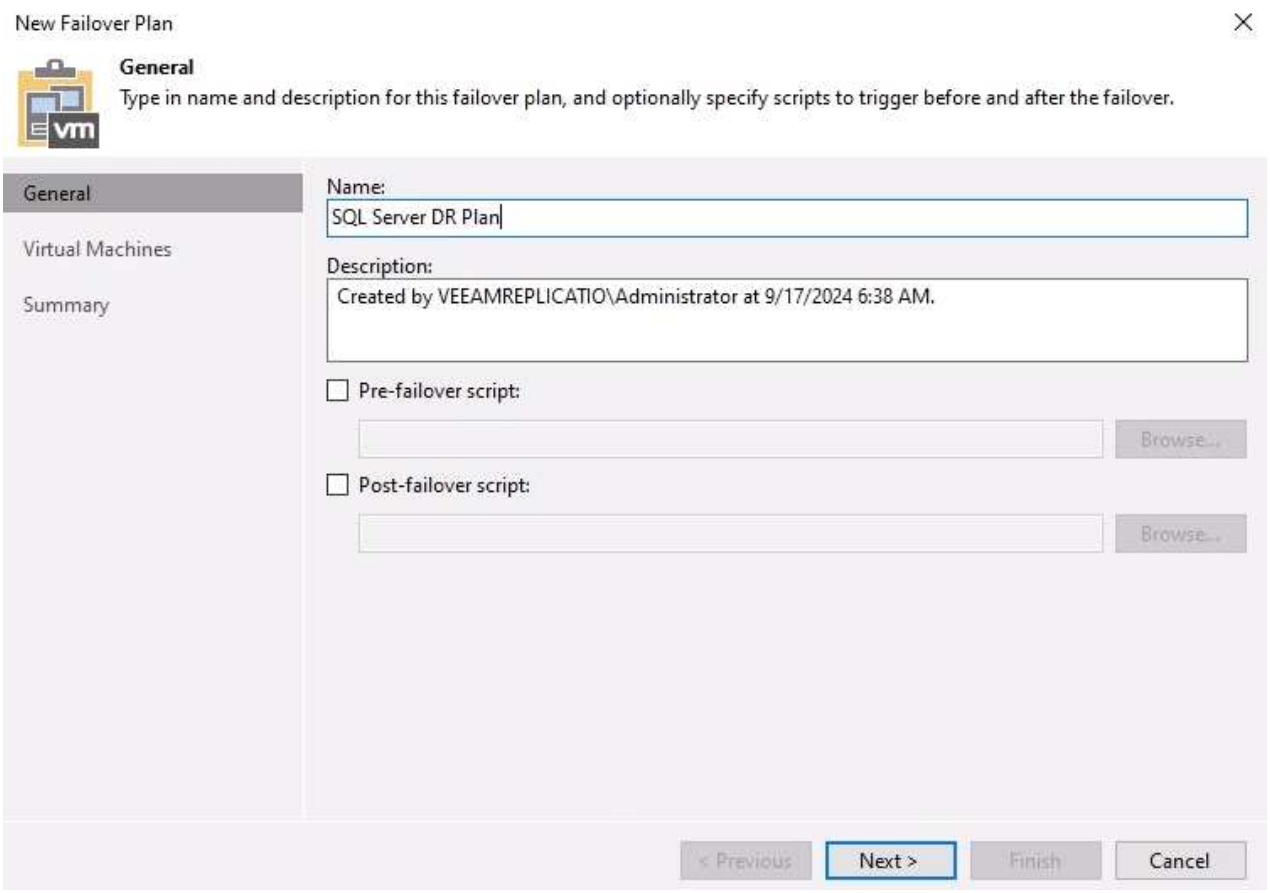
ⓘ Während des Failover-Prozesses werden die Quell-VMs nicht ausgeschaltet.

Führen Sie die folgenden Schritte aus, um den **Failover-Plan** zu erstellen:

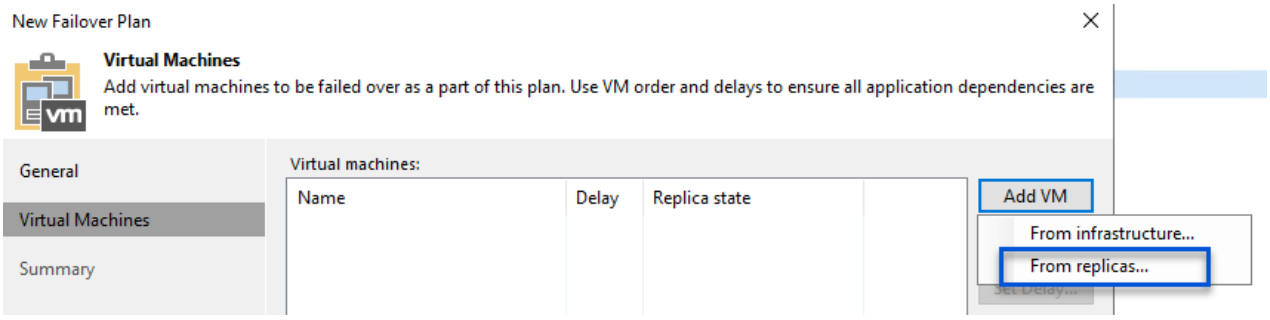
1. Klicken Sie in der Ansicht **Home** im Abschnitt **Wiederherstellen** auf die Schaltfläche **Failover-Plan**. Wählen Sie im Dropdown-Menü **VMware vSphere…** aus

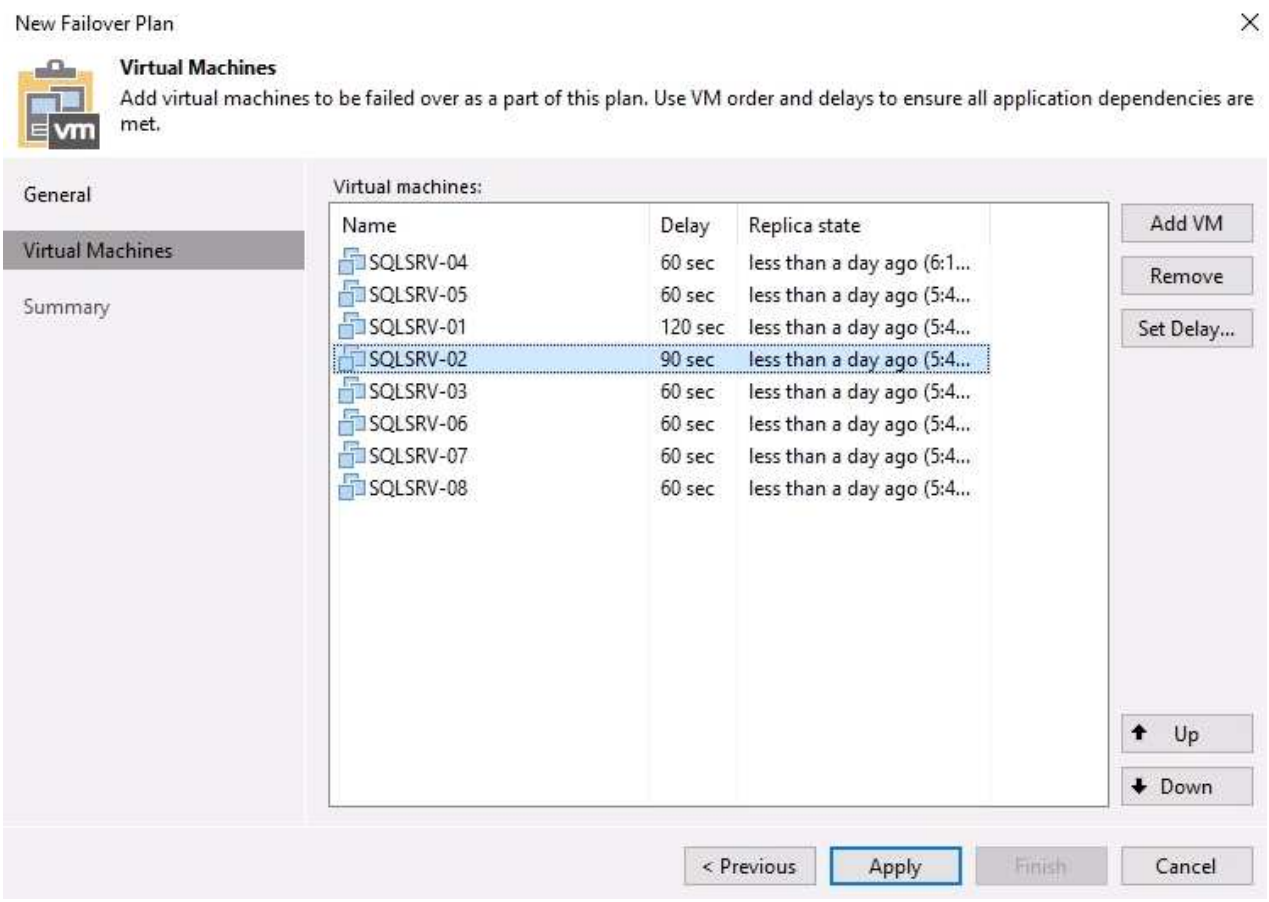


2. Geben Sie auf der Seite **General** des **New Failover Plan**-Assistenten einen Namen und eine Beschreibung für den Plan ein. Pre- und Post-Failover-Skripte können nach Bedarf hinzugefügt werden. Führen Sie beispielsweise ein Skript aus, um die VMs vor dem Starten der replizierten VMs herunterzufahren.



3. Klicken Sie auf der Seite **Virtuelle Maschinen** auf die Schaltfläche zu **VM hinzufügen** und wählen Sie **aus Replikaten…**. Wählen Sie die VMs aus, die Teil des Failover-Plans sind, und ändern Sie dann die VM-Boot-Reihenfolge sowie ggf. erforderliche Boot-Verzögerungen, um Applikationsabhängigkeiten zu erfüllen.





Klicken Sie auf **Apply**, um fortzufahren.

4. Überprüfen Sie schließlich alle Failover Plan-Einstellungen und klicken Sie auf **Fertig stellen**, um den Failover Plan zu erstellen.

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

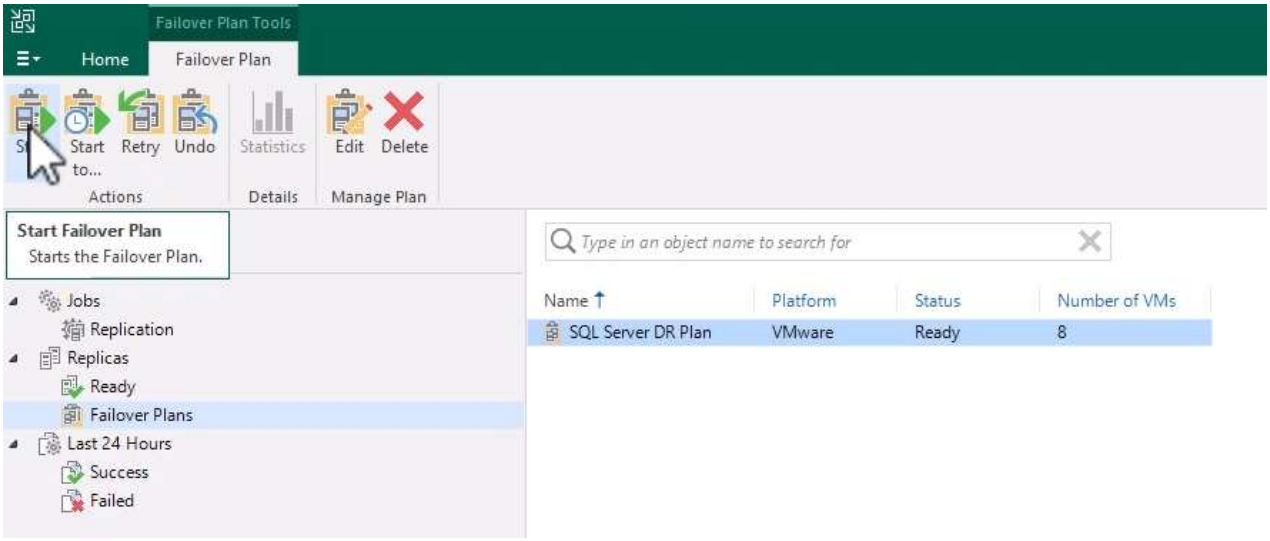
Ausführen des Failover-Plans

Bei einem Failover schaltet die Quell-VM am Produktionsstandort auf das Replikat am Disaster-Recovery-Standort um. Im Rahmen des Prozesses stellt Veeam Backup & Replication das VM-Replikat auf den erforderlichen Wiederherstellungspunkt wieder her und überträgt alle I/O-Aktivitäten von der Quell-VM auf sein Replikat. Replikate dienen nicht nur für tatsächliche Katastrophen, sondern auch zur Simulation von DR-Bohrern. In der Failover-Simulation wird die Quell-VM weiter ausgeführt. Nach Abschluss der erforderlichen Tests kann das Failover rückgängig gemacht werden, sodass der Betrieb wieder normal wird.

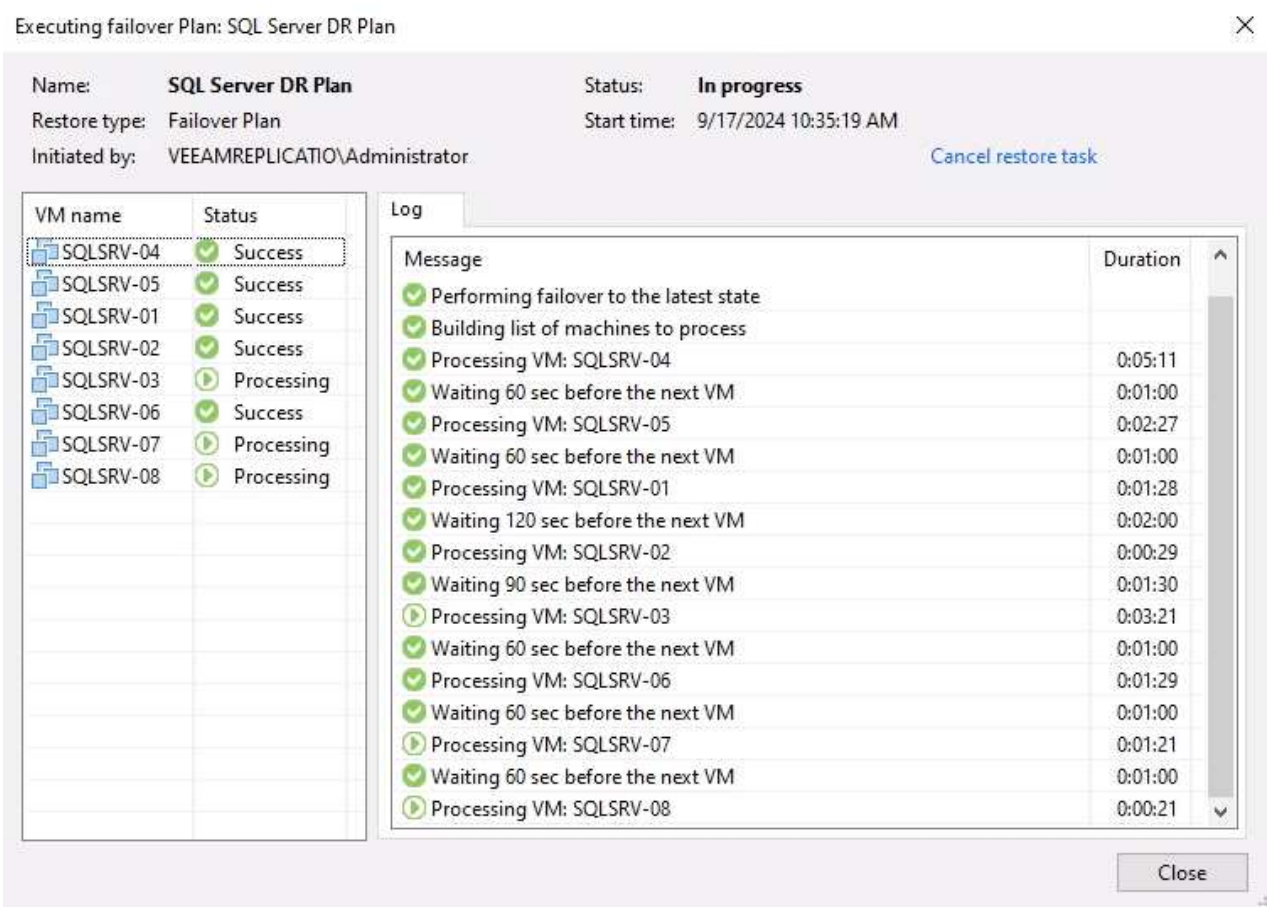
Stellen Sie sicher, dass die Netzwerksegmentierung vorhanden ist, um IP-Konflikte während des Failovers zu vermeiden.

Führen Sie die folgenden Schritte aus, um den Failover-Plan zu starten:

1. Um zu beginnen, klicken Sie in der **Home**-Ansicht im linken Menü auf **Replikate > Failover-Pläne** und dann auf den **Start**-Button. Alternativ kann die Schaltfläche **Start bis…** zum Failover auf einen früheren Wiederherstellungspunkt verwendet werden.



2. Überwachen Sie den Fortschritt des Failovers im Fenster **Executing Failover Plan**.



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

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

Failback auf den Produktionsstandort

Das Durchführen eines Failovers gilt als Zwischenschritt und muss auf Grundlage der Anforderung abgeschlossen werden. Folgende Optionen stehen zur Verfügung:

- **Failback zur Produktion** - kehrt zur ursprünglichen VM zurück und synchronisiert alle Änderungen, die während des aktiven Zeitraums des Replikats vorgenommen wurden, zurück zur Quell-VM.

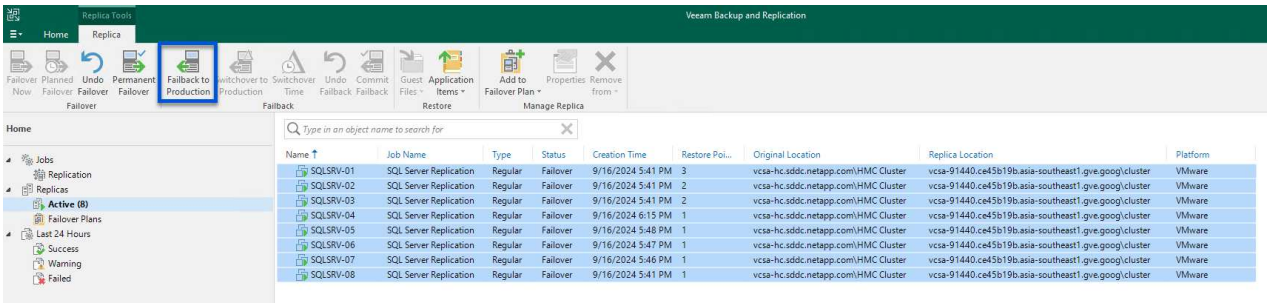
> ⓘ Während des Failback werden Änderungen übertragen, aber nicht sofort angewendet. Wählen Sie **commit Failback** aus, sobald die Funktionalität der ursprünglichen VM überprüft wurde. Alternativ können Sie **Rückgängig-Failback** wählen, um zum VM-Replikat zurückzukehren, wenn die ursprüngliche VM unerwartetes Verhalten aufweist.

- **Rückgängig-Failover** - Zurücksetzen auf die ursprüngliche VM, wobei alle Änderungen, die während des Betriebszeitraums am VM-Replikat vorgenommen wurden, verworfen werden.
- **Permanent Failover** - Wechseln Sie dauerhaft von der ursprünglichen VM auf das Replikat, indem Sie das Replikat als neue primäre VM für laufende Vorgänge einrichten.

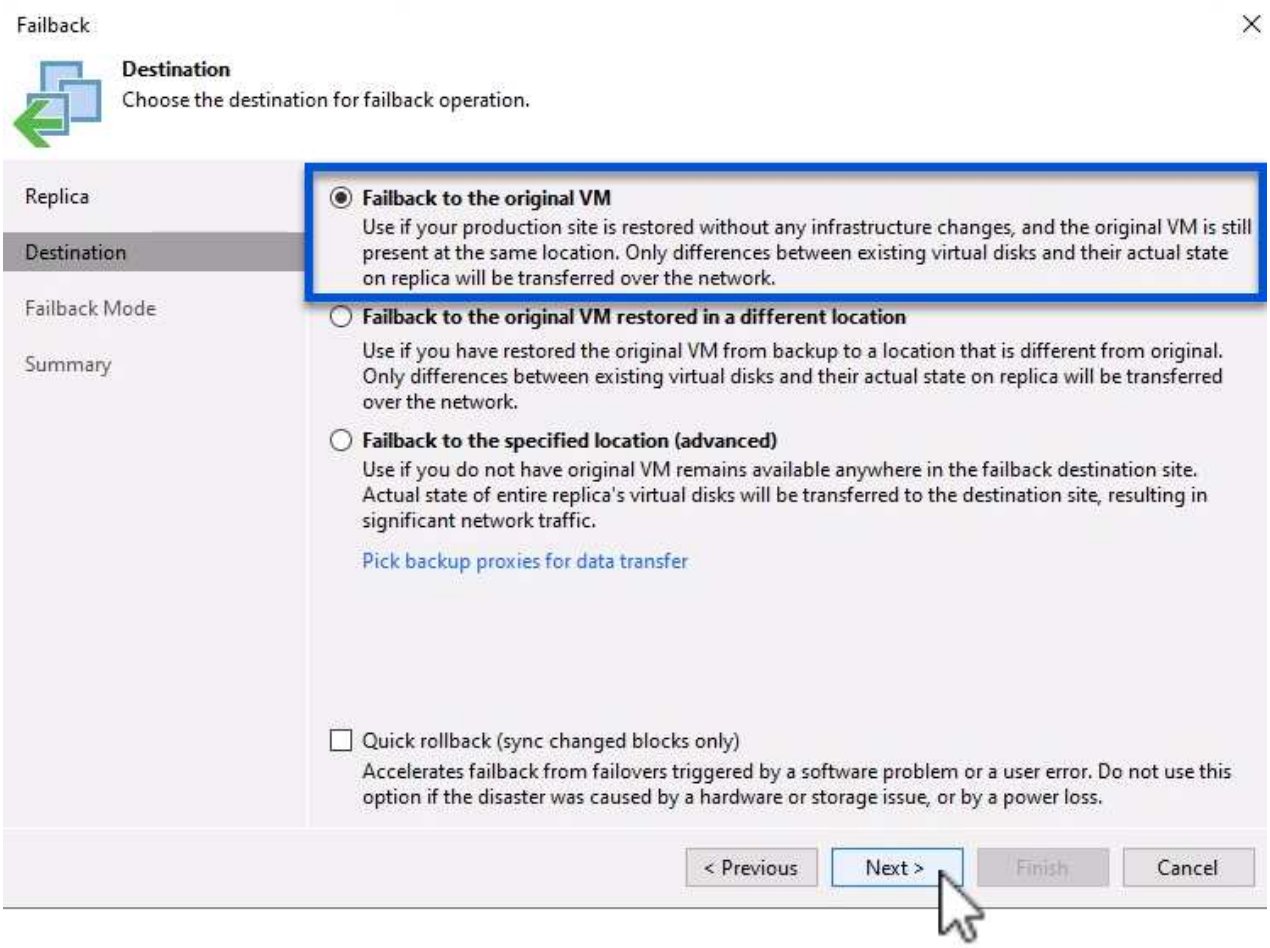
In diesem Szenario wurde die Option „Failback zur Produktion“ ausgewählt.

Führen Sie die folgenden Schritte durch, um ein Failback zum Produktionsstandort durchzuführen:

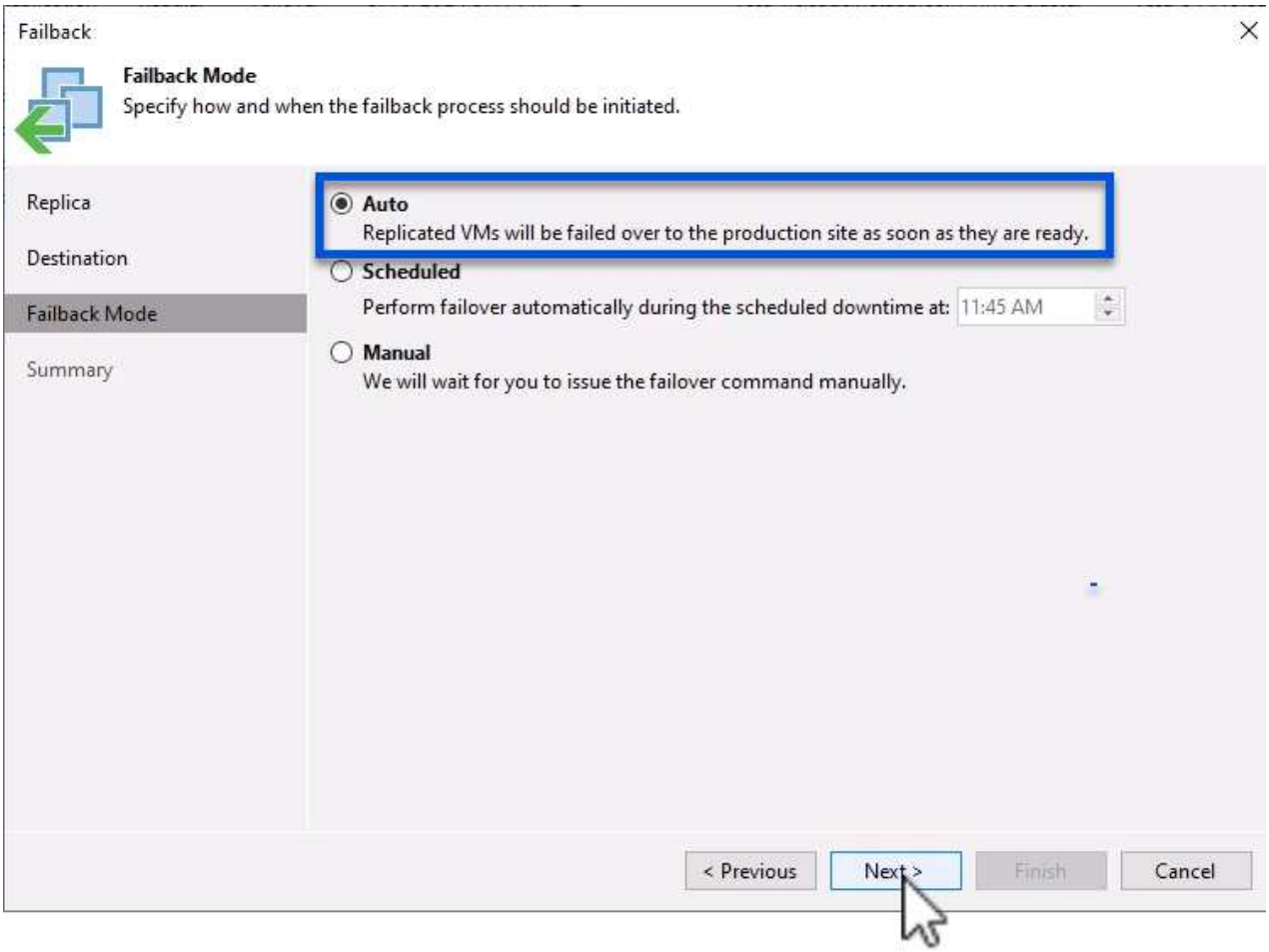
1. Klicken Sie in der Ansicht **Home** im linken Menü auf **Replikate > aktiv**. Wählen Sie die einzuschaltenden VMs aus und klicken Sie im oberen Menü auf die Schaltfläche **Failback zur Produktion**.



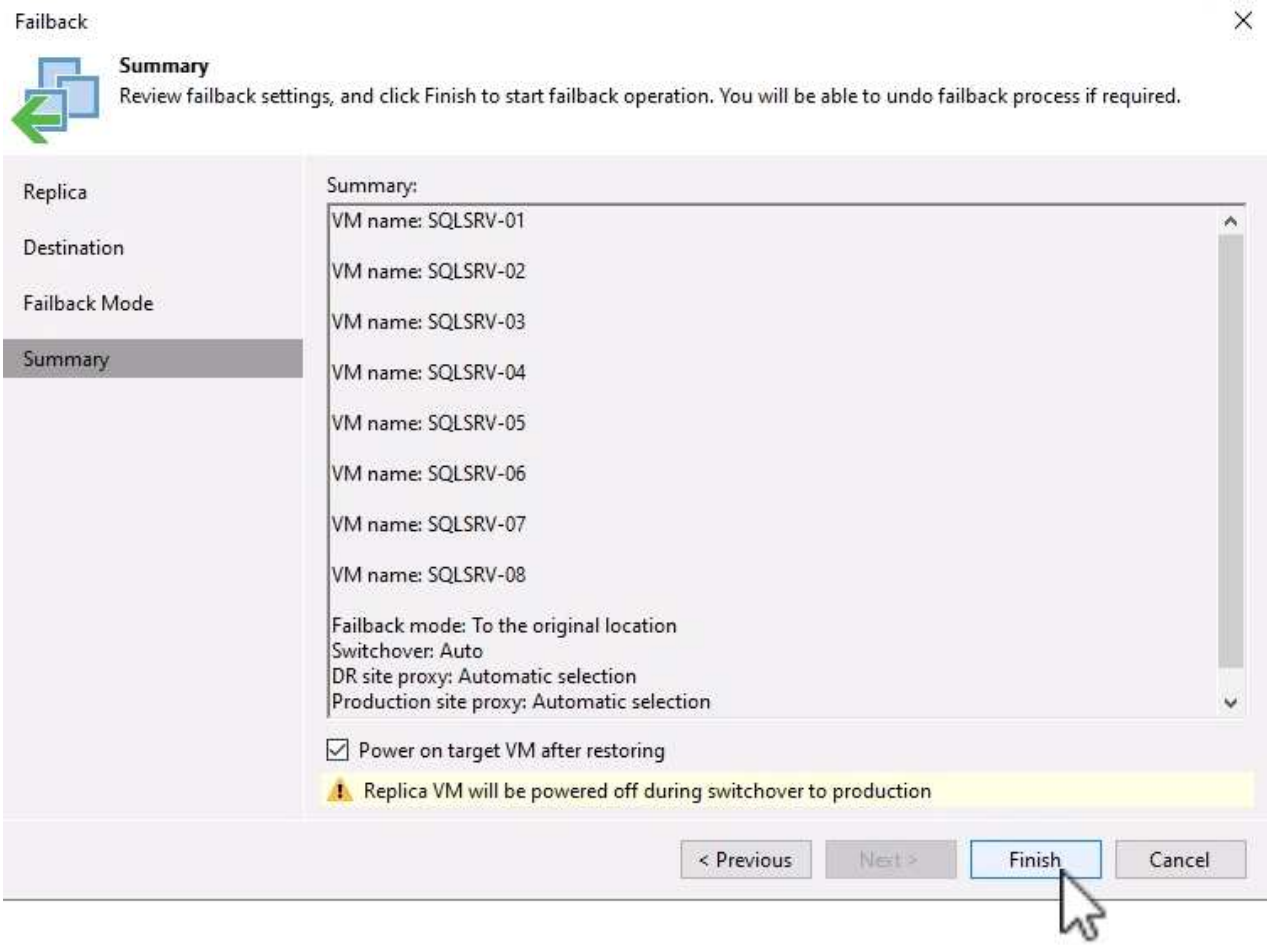
2. Wählen Sie auf der Seite **Replica** des **Failback**-Assistenten die Replikate aus, die in den Failback-Job aufgenommen werden sollen.
3. Wählen Sie auf der Seite **Destination Failback zur ursprünglichen VM** aus und klicken Sie auf **Next**, um fortzufahren.



4. Wählen Sie auf der Seite **Failback-Modus Auto** aus, um das Failback so schnell wie möglich zu starten.

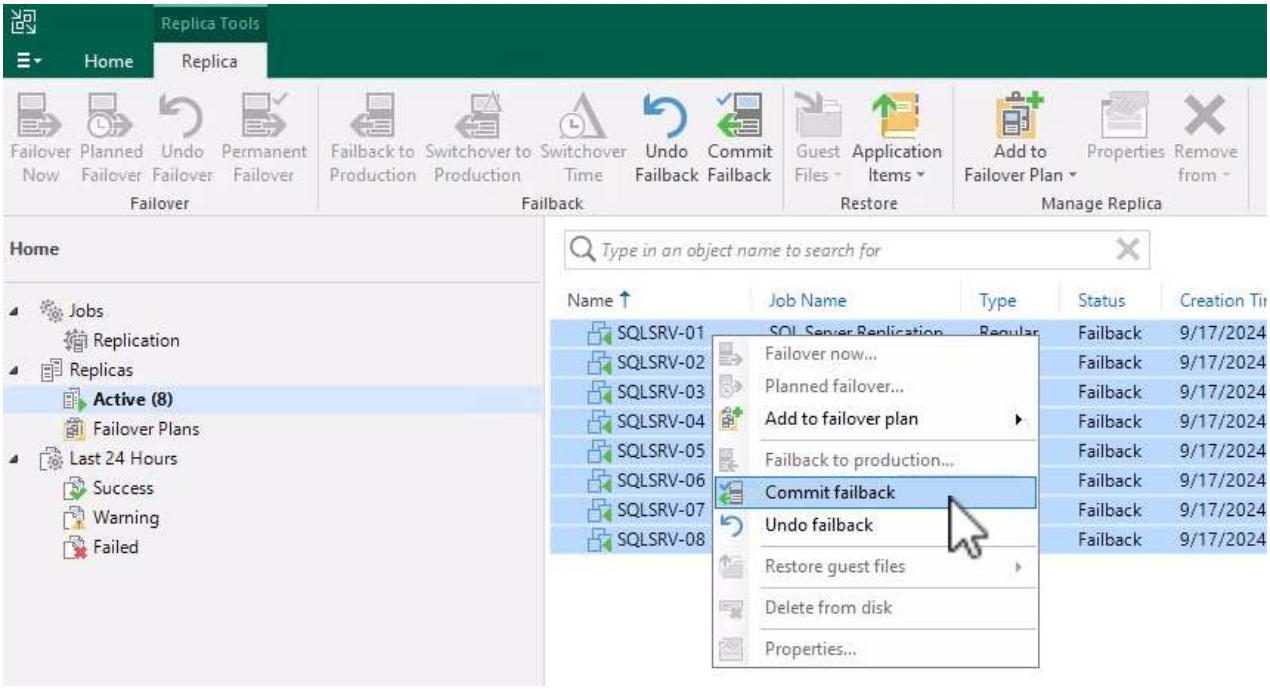


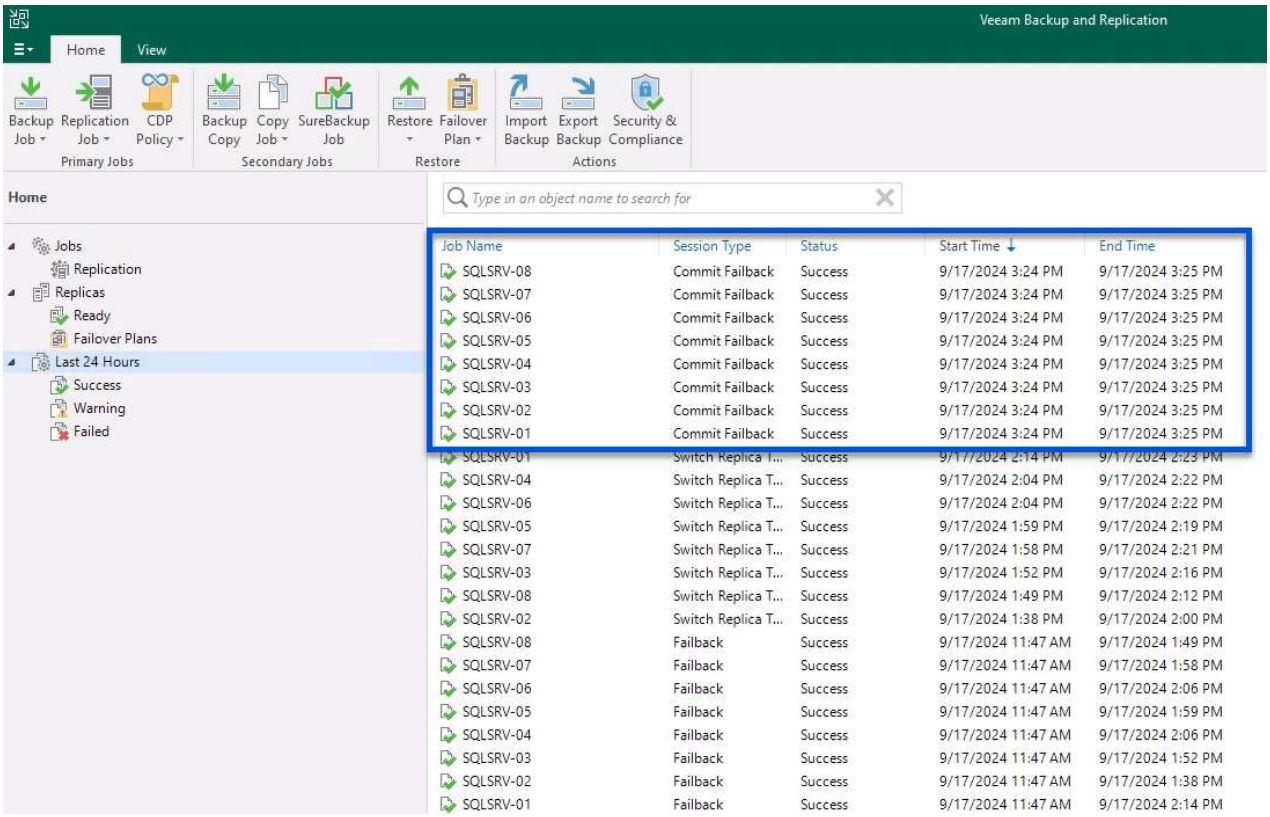
5. Wählen Sie auf der Seite **Zusammenfassung** aus, ob die Ziel-VM nach der Wiederherstellung eingeschaltet werden soll, und klicken Sie dann auf Fertig stellen, um den Failback-Job zu starten.



Failback Commit schließt den Failback-Vorgang ab und bestätigt damit die erfolgreiche Integration von Änderungen in die Produktions-VM. Nach dem Commit setzt Veeam Backup & Replication die regelmäßigen Replizierungsaktivitäten für die wiederhergestellte Produktions-VM fort. Dadurch wird der Status des wiederhergestellten Replikats von *Failback* in *Ready* geändert.

1. Um Failback zu aktivieren, navigieren Sie zu **Replikate > aktiv**, wählen Sie die zu besetzenden VMs aus, klicken Sie mit der rechten Maustaste und wählen Sie **Failback festschreiben** aus.





Nachdem das Failback zur Produktion erfolgreich war, werden alle VMs wieder auf den ursprünglichen Produktionsstandort zurückgesetzt.

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

Schlussfolgerung

Mit der Google Cloud NetApp Volumes-Datastore-Funktion können Veeam und andere validierte Tools von Drittanbietern kostengünstige Disaster-Recovery-Lösungen (DR) bereitstellen. Durch den Einsatz von Pilot Light-Clustern anstelle großer, dedizierter Cluster für VM-Replikate können Unternehmen die Kosten erheblich senken. Dieser Ansatz ermöglicht maßgeschneiderte DR-Strategien, die vorhandene interne Backup-Lösungen für Cloud-basierte Disaster Recovery nutzen und damit keine zusätzlichen Datacenter vor Ort mehr benötigen. Bei einem Ausfall kann der Failover mit einem einzigen Klick initiiert oder für die automatische Ausführung konfiguriert werden, um die Business Continuity mit minimalen Ausfallzeiten zu gewährleisten.

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

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

Migration von Workloads auf GCP/GCVE

Migrieren Sie Workloads mithilfe des VMware HCX – QuickStart Guide zu Google Cloud NetApp Volumes Datastore in der Google Cloud VMware Engine

Eine der gängigsten Anwendungsfälle für die Google Cloud VMware Engine und einen Cloud Volume Service-Datastore ist die Migration von VMware Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmechanismen zum Verschieben von On-Premises-Virtual Machines (VMs) und deren Daten in NFS-Datastores des Cloud Volume Service.

Autor(en): NetApp Solutions Engineering

Übersicht: Migration virtueller Maschinen mit VMware HCX, Google Cloud NetApp Volumes Datastores und Google Cloud VMware Engine (GCVE)

VMware HCX ist primär eine Migrationsplattform, die entwickelt wurde, um die Migration von Applikationen, die Ausbalancierung von Workloads und sogar Business Continuity Cloud-übergreifend zu vereinfachen. Dies ist Teil von Google Cloud VMware Engine Private Cloud und bietet zahlreiche Möglichkeiten zur Migration von Workloads und kann für Disaster-Recovery-Vorgänge (DR) genutzt werden.

Dieses Dokument enthält eine Schritt-für-Schritt-Anleitung für die Bereitstellung von Cloud Volume Service Datastore. Anschließend werden alle wichtigen Komponenten von VMware HCX heruntergeladen, implementiert und konfiguriert, einschließlich aller wichtigen Komponenten vor Ort und der Google Cloud VMware Engine Seite mit Interconnect, Netzwerkerweiterung und WAN-Optimierung für die Aktivierung verschiedener VM-Migrationsmechanismen.

> VMware HCX arbeitet mit jedem Datenspeichertyp zusammen, da die Migration auf VM-Ebene erfolgt. Daher eignet sich dieses Dokument für bestehende NetApp Kunden und andere Kunden, die den Cloud Volume Service mit der Google Cloud VMware Engine als kostengünstige VMware Cloud-Implementierung planen.

Allgemeine Schritte

Diese Liste enthält die grundlegenden Schritte, die zum Pairing und Migrieren der VMs zu HCX Cloud Manager auf der Google Cloud VMware Engine Seite von HCX Connector vor Ort erforderlich sind:

1. Bereiten Sie HCX über das Google VMware Engine Portal vor.
2. Laden Sie das Installationsprogramm für die HCX Connector Open Virtualization Appliance (OVA) im lokalen VMware vCenter Server herunter und implementieren Sie es.
3. HCX mit dem Lizenzschlüssel aktivieren.
4. Verbinden Sie den lokalen VMware HCX Connector mit der Google Cloud VMware Engine HCX Cloud Manager.
5. Sie konfigurieren das Netzwerkprofil, das Computing-Profil und das Service-Mesh.
6. (Optional) Sie können eine Netzwerkerweiterung vornehmen, um bei Migrationen eine erneute IP-Adresse zu vermeiden.
7. Validieren des Appliance-Status und Sicherstellen der Möglichkeit der Migration
8. Migration der VM-Workloads

Voraussetzungen

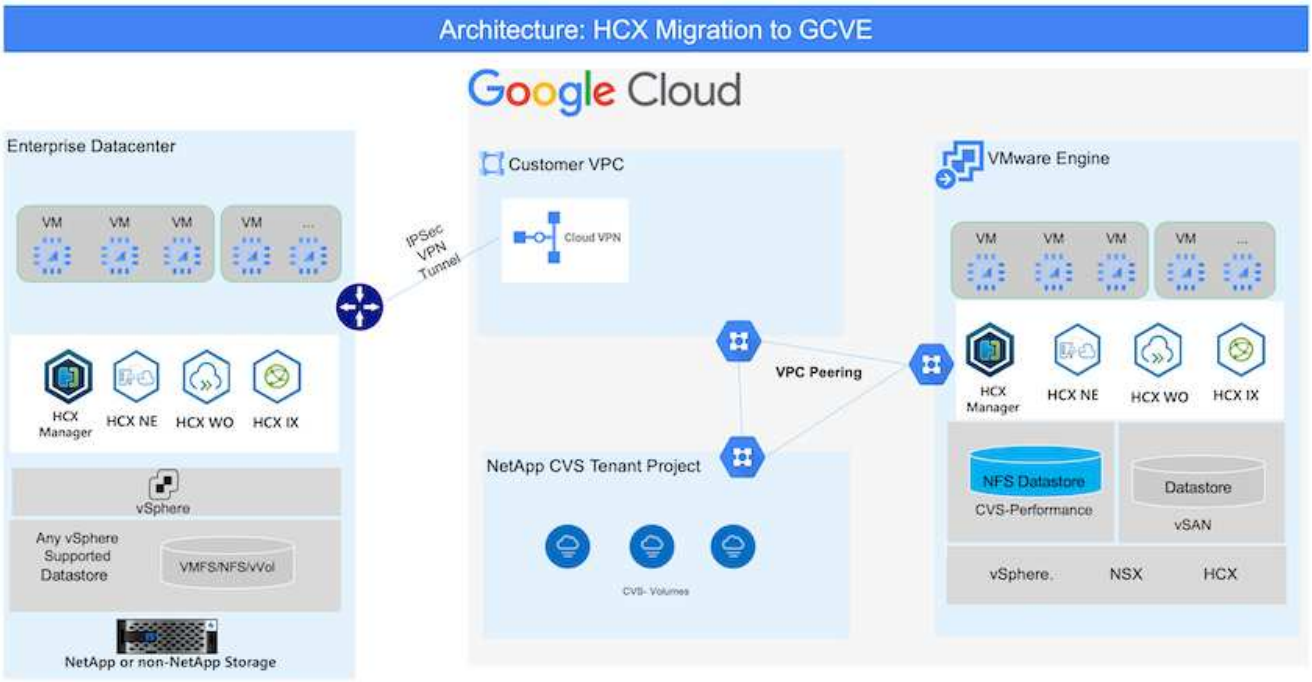
Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "Verlinken". Nachdem die Voraussetzungen, einschließlich Konnektivität, vorhanden sind, laden Sie den HCX-Lizenzschlüssel aus dem Google Cloud VMware Engine-Portal herunter. Nach dem Herunterladen des OVA-Installationsprogramms gehen Sie wie unten beschrieben mit der Installation vor.

> ⓘ HCX Advanced ist die Standardoption und die VMware HCX Enterprise Edition ist auch über ein Support-Ticket erhältlich und wird ohne zusätzliche Kosten unterstützt. Siehe "Dieser Link"

- Verwenden Sie ein vorhandenes softwaredefiniertes Google Cloud VMware Engine Datacenter (SDDC) oder erstellen Sie mithilfe dieses Modells eine Private Cloud "Link von NetApp" Oder hier "Google-Link".
- Die Migration von VMs und zugehörigen Daten vom lokalen Datacenter mit VMware vSphere erfordert Netzwerkkonnektivität vom Datacenter zur SDDC-Umgebung. Vor der Migration von Workloads "Einrichten eines Cloud-VPN oder einer Cloud Interconnect-Verbindung" Zwischen der lokalen Umgebung und der jeweiligen Private Cloud verschieben.
- Der Netzwerkpfad von der lokalen VMware vCenter Server Umgebung zur privaten Cloud der Google Cloud VMware Engine muss die Migration von VMs mithilfe von vMotion unterstützen.
- Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und -Ports" Sind für vMotion Traffic zwischen dem lokalen vCenter Server und SDDC vCenter zulässig.
- Cloud Volume Service NFS-Volume sollte als Datastore in der Google Cloud VMware Engine gemountet werden. Befolgen Sie die in diesem Schritt beschriebenen Schritte "Verlinken" Cloud Volume Service-Datenspeicher an Google Cloud VMware Engines Hosts anhängen.

Übergeordnete Architektur

Die Lab-Umgebung vor Ort für diese Validierung wurde zu Testzwecken über ein Cloud-VPN verbunden, das On-Premises-Konnektivität mit Google Cloud VPC ermöglicht.



Weitere Informationen zur Verwendung von VMware HCX mit Google finden Sie unter "Link zu VMware"

Lösungsimplementierung

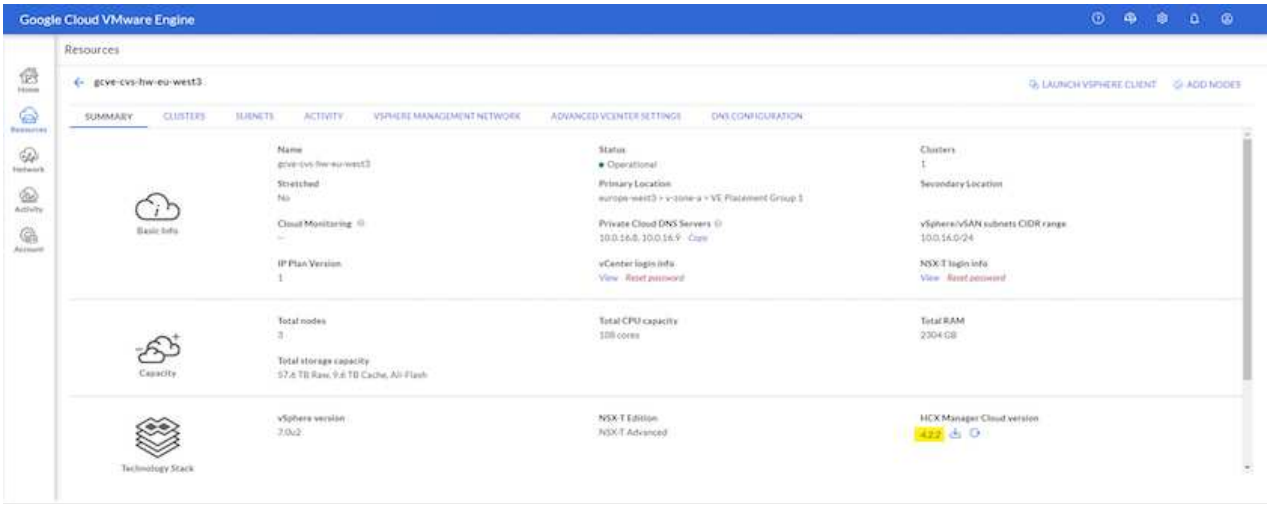
Führen Sie die folgenden Schritte aus, um die Implementierung dieser Lösung abzuschließen:

Schritt 1: HCX über das Google VMware Engine Portal vorbereiten

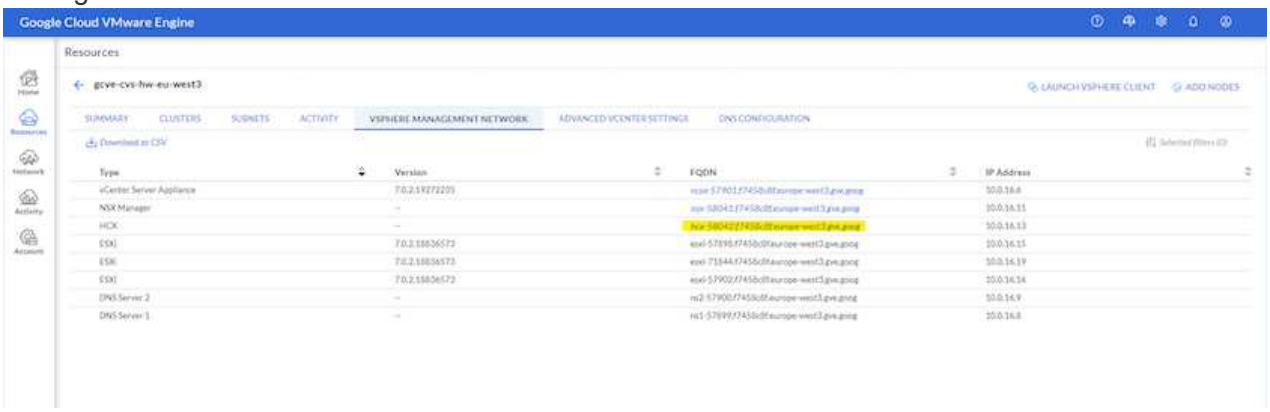
HCX Cloud Manager wird automatisch installiert, wenn Sie eine Private Cloud mit VMware Engine bereitstellen. Gehen Sie wie folgt vor, um die Standortpaarung vorzubereiten:

1. Melden Sie sich beim Google VMware Engine Portal an und melden Sie sich beim HCX Cloud Manager an.

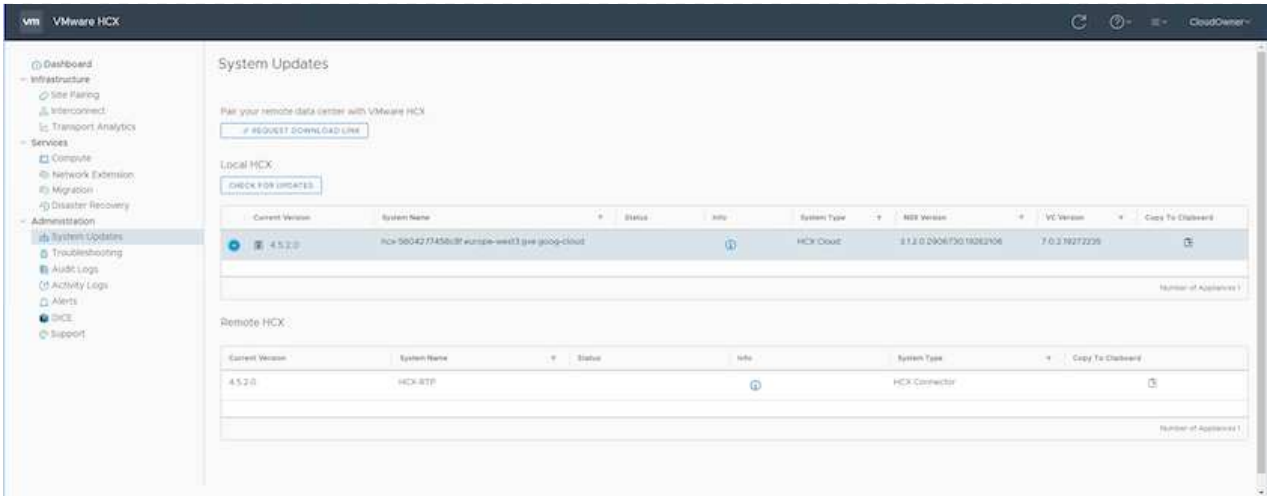
   Sie können sich bei der HCX-Konsole anmelden



   , indem Sie auf den Link HCX-Version klicken oder auf HCX FQDN unter der Registerkarte vSphere Management Network klicken.



2. Gehen Sie in HCX Cloud Manager zu **Administration > System Updates**.
3. Klicken Sie auf **Download-Link anfordern** und laden Sie die OVA-Datei herunter.



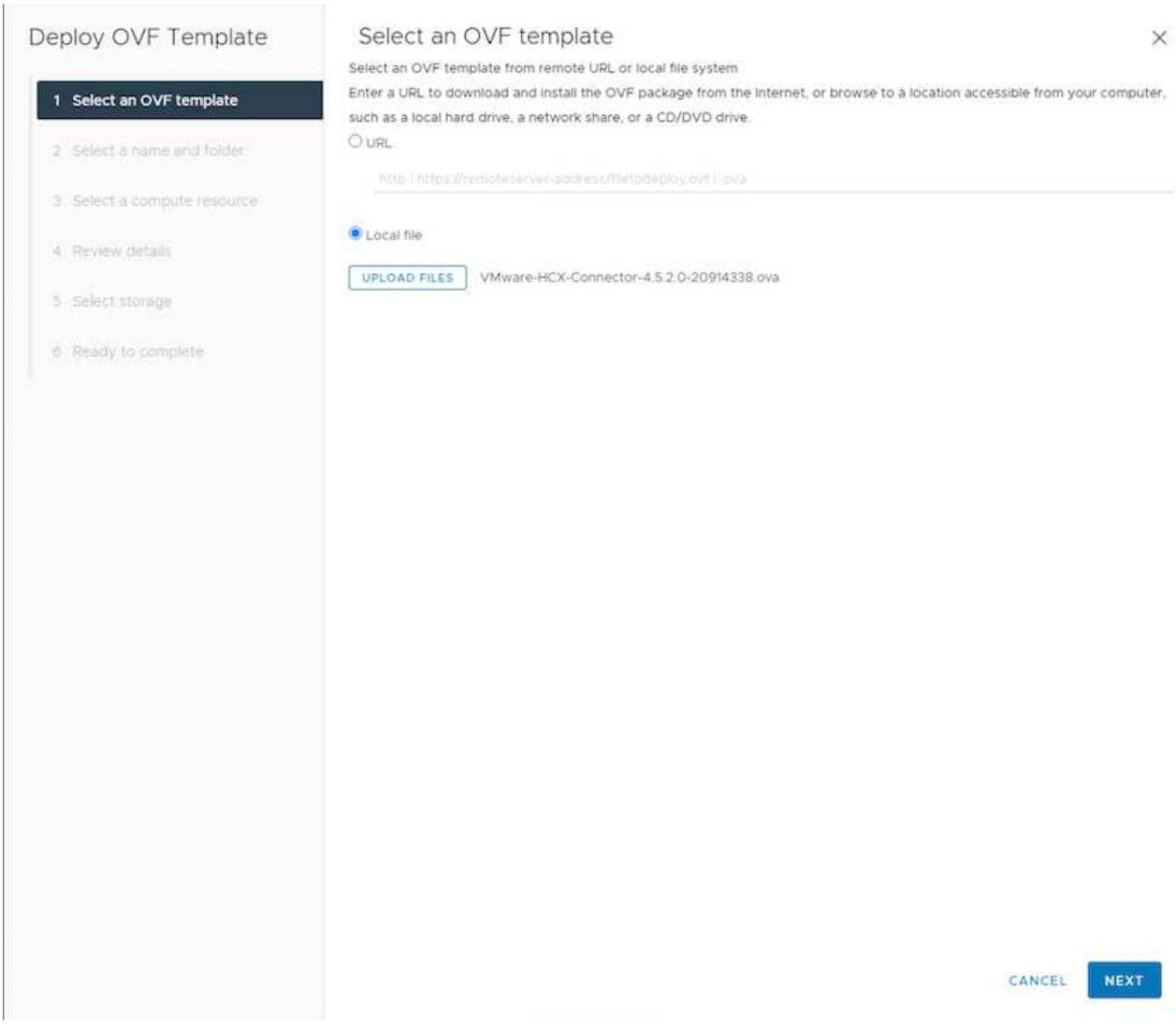
4. Aktualisieren Sie HCX Cloud Manager auf die neueste Version, die über die Benutzeroberfläche von HCX Cloud Manager verfügbar ist.

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

Damit der On-Premises Connector eine Verbindung zum HCX Manager in der Google Cloud VMware Engine herstellen kann, müssen die entsprechenden Firewall-Ports in der On-Premises-Umgebung geöffnet sein.

So laden Sie den HCX Connector auf dem lokalen vCenter Server herunter und installieren ihn:

1. Laden Sie die ova von der HCX-Konsole auf Google Cloud VMware Engine wie im vorherigen Schritt angegeben herunter.
2. Nachdem die OVA heruntergeladen wurde, stellen Sie sie in der lokalen VMware vSphere Umgebung mithilfe der Option **Deploy OVF Template** bereit.



3. Geben Sie alle erforderlichen Informationen für die OVA-Bereitstellung ein, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um die OVA des VMware HCX-Connectors bereitzustellen.

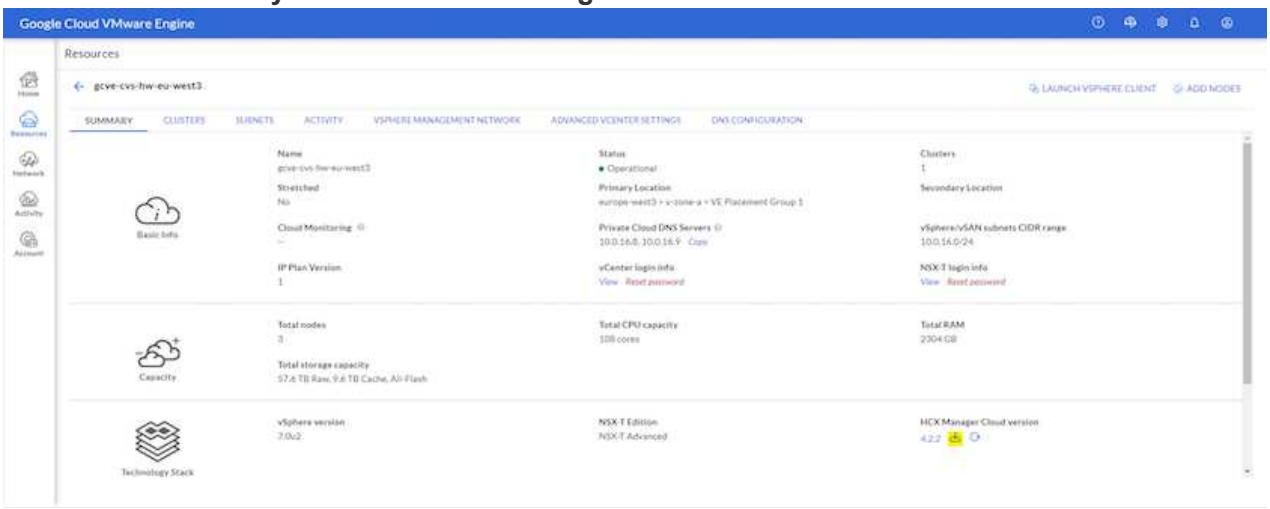
Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "Google HCX-Dokumentation".

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie den VMware HCX Connector OVA vor Ort bereitgestellt und das Gerät gestartet haben, führen Sie die folgenden Schritte aus, um den HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel aus dem Google Cloud VMware Engine Portal und aktivieren Sie ihn im VMware HCX Manager.

1. Klicken Sie im VMware Engine-Portal auf Ressourcen, wählen Sie die Private Cloud und **Klicken Sie auf das Download-Symbol unter HCX Manager Cloud Version**.



   Öffnen Sie die heruntergeladene Datei, und kopieren Sie die Lizenzschlüsselzeichenfolge.

2. Melden Sie sich beim lokalen VMware HCX Manager unter an `"https://hcxmanagerIP:9443"` Administratordaten werden verwendet.

   Verwenden Sie die hcxmanagerIP und das Passwort, das während der OVA-Bereitstellung definiert wurde.

3. Geben Sie in der Lizenzierung den aus Schritt 3 kopierten Schlüssel ein und klicken Sie auf **Aktivieren**.

   Der HCX-Connector sollte über einen Internetzugang verfügen.

4. Geben Sie unter **Datacenter Location** den nächstgelegenen Standort für die Installation des VMware HCX Managers vor Ort an. Klicken Sie Auf **Weiter**.
5. Aktualisieren Sie unter **Systemname** den Namen und klicken Sie auf **Weiter**.
6. Klicken Sie Auf **Ja, Weiter**.
7. Geben Sie unter **Connect Your vCenter** den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des vCenter Servers und die entsprechenden Anmeldeinformationen an und klicken Sie auf **Continue**.

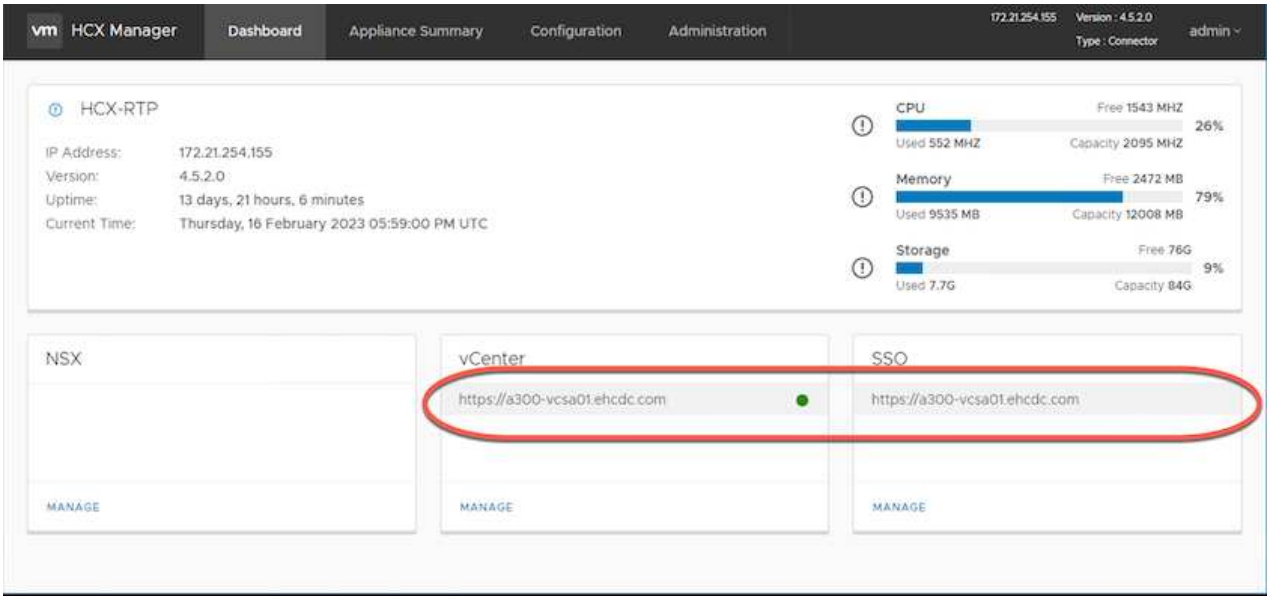
   Verwenden Sie den FQDN, um Verbindungsprobleme später zu vermeiden.

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

Geben Sie für Embedded PSC den VMware vCenter Server FQDN oder die IP-Adresse ein.

9. Überprüfen Sie, ob die eingegebenen Informationen korrekt sind, und klicken Sie auf **Neustart**.
10. Nach dem Neustart der Dienste wird vCenter Server auf der angezeigten Seite grün angezeigt. Sowohl vCenter Server als auch SSO müssen über die entsprechenden Konfigurationsparameter verfügen, die mit der vorherigen Seite übereinstimmen sollten.

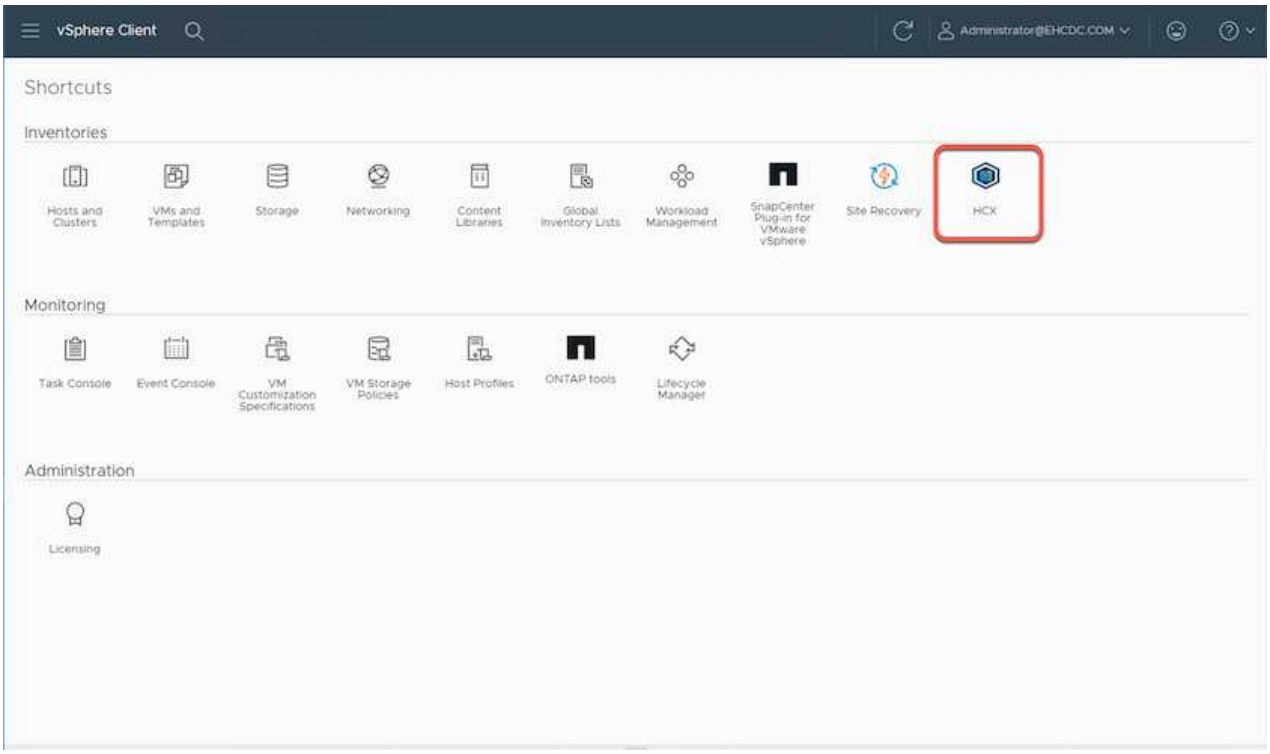
Dieser Vorgang dauert etwa 10 bis 20 Minuten, und das Plug-in wird dem vCenter Server hinzugefügt.



Schritt 4: Verbinden Sie den VMware HCX Connector vor Ort mit der Google Cloud VMware Engine HCX Cloud Manager

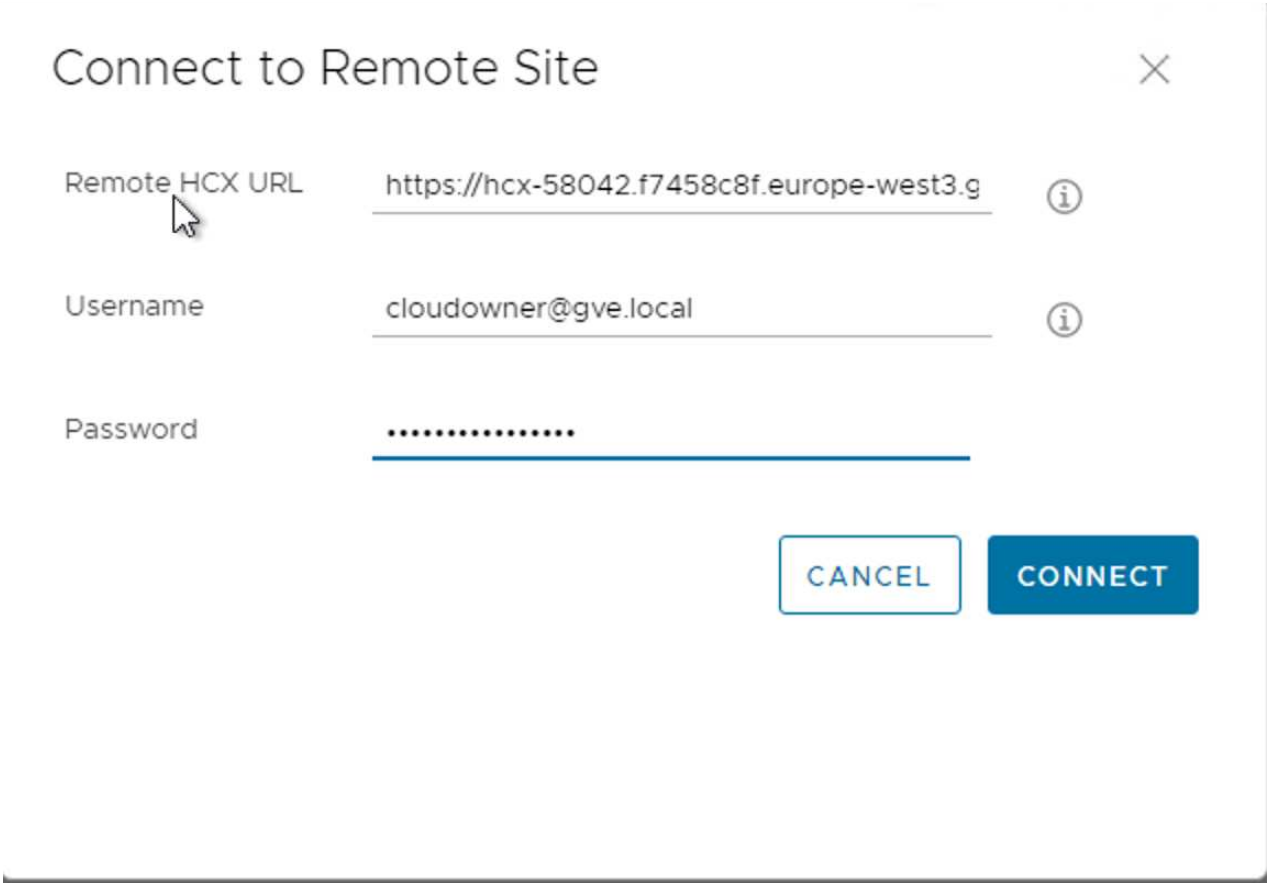
Nachdem HCX Connector im lokalen vCenter bereitgestellt und konfiguriert wurde, stellen Sie eine Verbindung zum Cloud Manager her, indem Sie die Paarung hinzufügen. Gehen Sie wie folgt vor, um die Standortpaarung zu konfigurieren:

1. Um ein Standortpaar zwischen der lokalen vCenter Umgebung und der Google Cloud VMware Engine SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das neue HCX vSphere Web Client Plug-in zu.



2. Klicken Sie unter Infrastruktur auf **Site Pairing hinzufügen**.

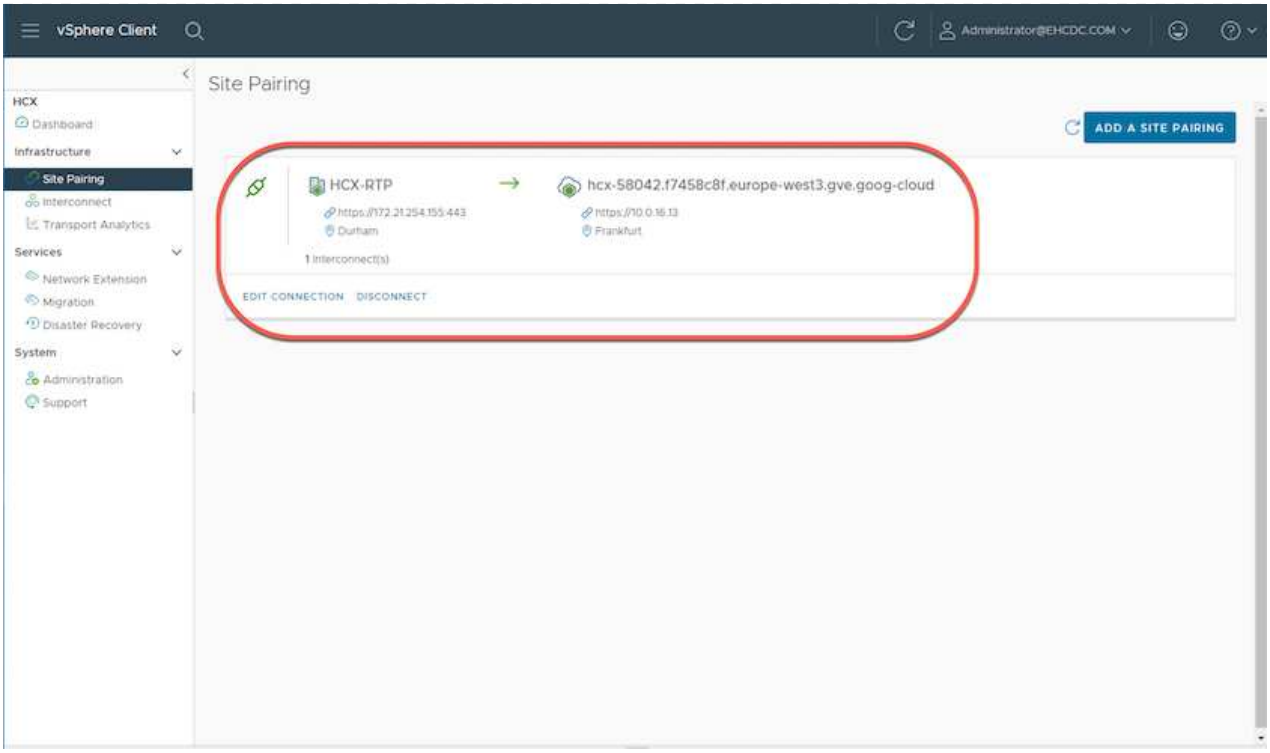
> Geben Sie die URL oder IP-Adresse des Google Cloud VMware Engine HCX Cloud Manager und die Anmeldedaten für Benutzer mit Cloud-Owner-Rollenberechtigungen für den Zugriff auf die private Cloud ein.



3. Klicken Sie Auf **Verbinden**.

   VMware HCX Connector muss über Port 443 zu HCX Cloud Manager IP weiterleiten können.

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

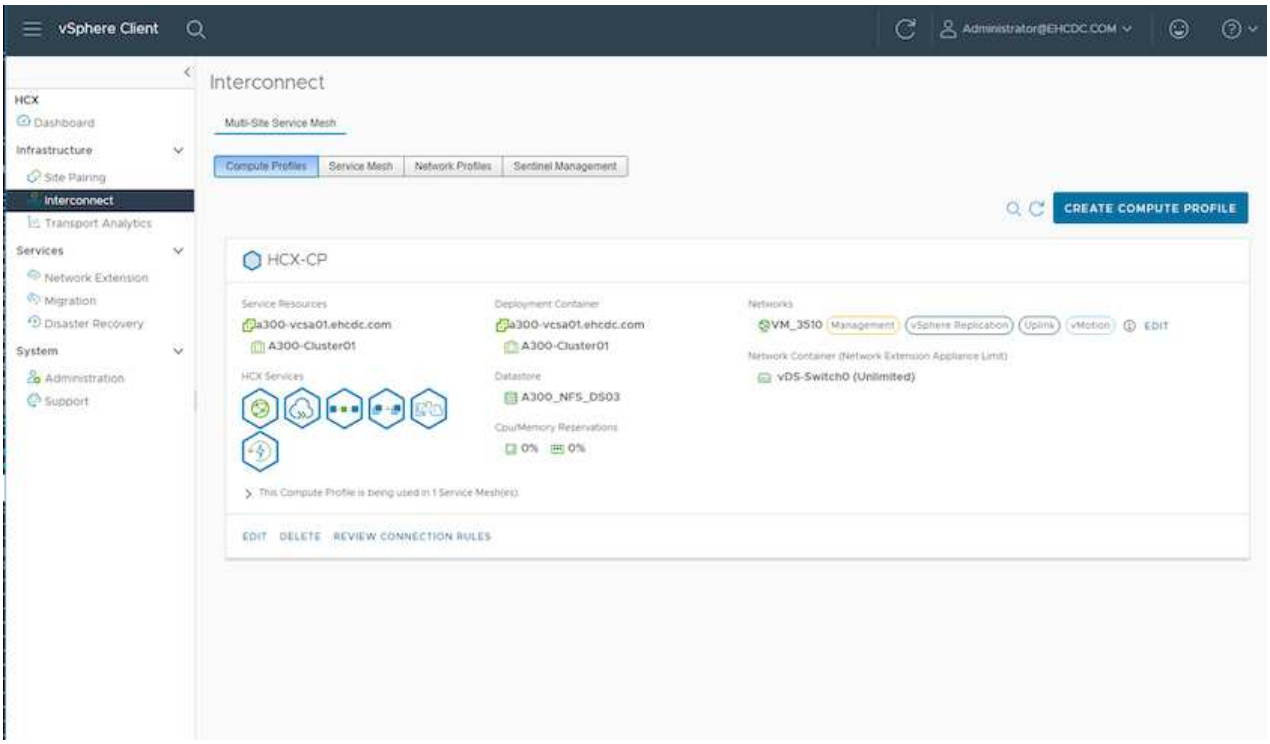

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud
https://10.0.16.13
Frankfurt
1 Interconnect(s)
EDIT CONNECTION
DISCONNECT

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

Die VMware HCX Interconnect Service Appliance bietet Replizierungs- und vMotion-basierte Migrationsfunktionen über das Internet und private Verbindungen zum Zielstandort. Das Interconnect bietet Verschlüsselung, Traffic Engineering und VM-Mobilität. Um eine Interconnect Service Appliance zu erstellen, gehen Sie wie folgt vor:

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

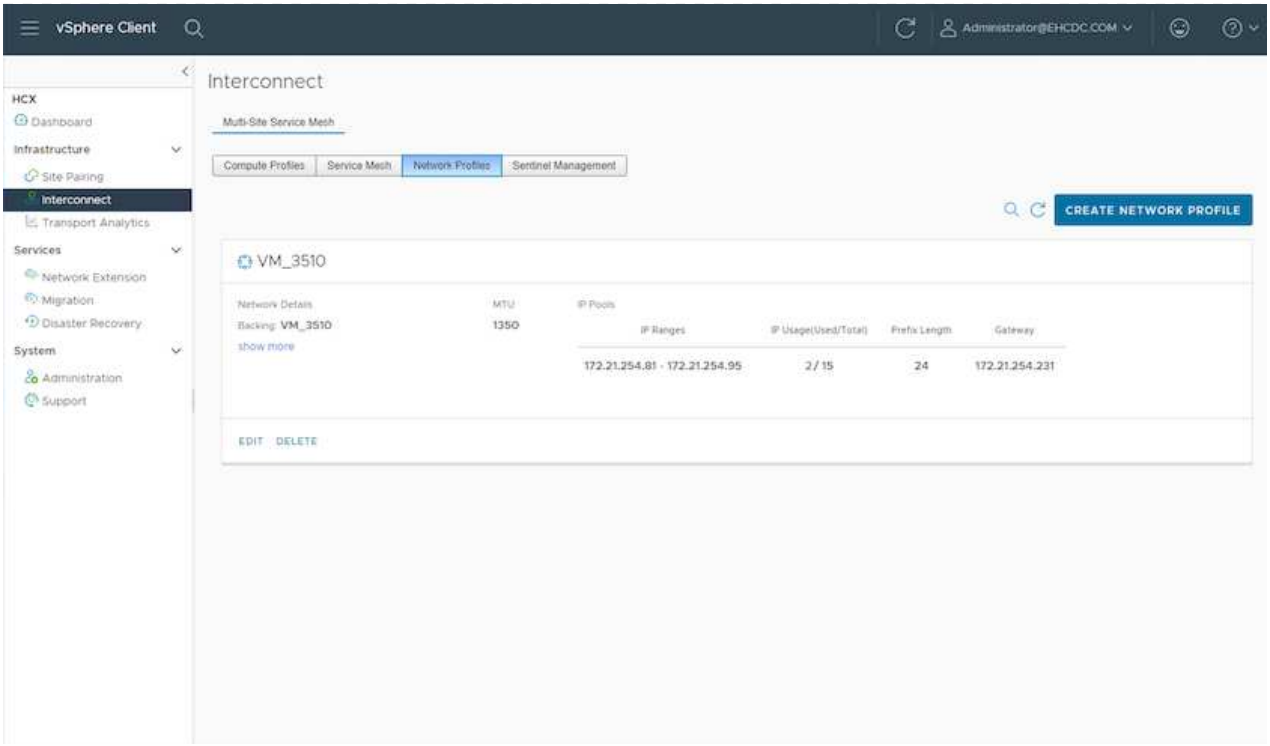
   Die Computing-Profile definieren die Implementierungsparameter einschließlich der Appliances, die bereitgestellt werden und welche Teile des VMware Datacenters für den HCX-Service verfügbar sind.



2. Erstellen Sie nach dem Erstellen des Rechenprofils die Netzwerkprofile, indem Sie **Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen** auswählen.

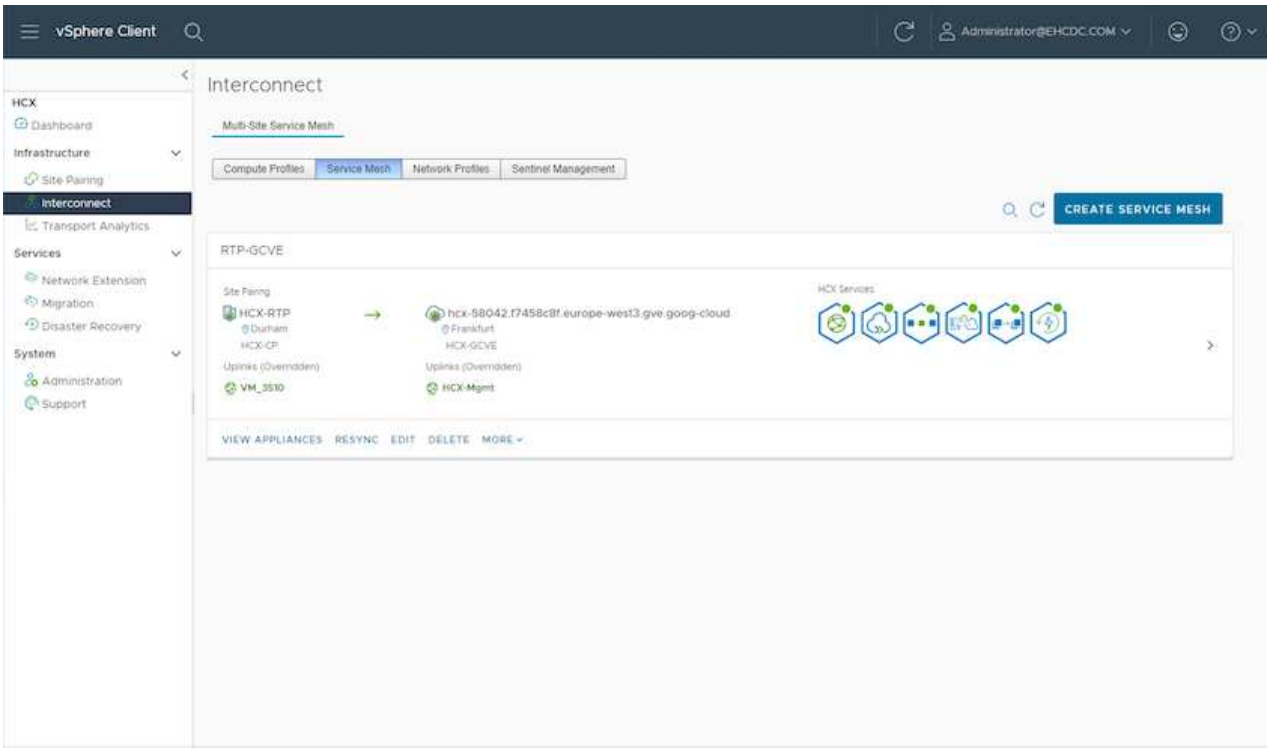
   Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

   Für diesen Schritt werden mindestens zwei IP-Adressen benötigt. Diese IP-Adressen werden den Interconnect Appliances vom Managementnetzwerk zugewiesen.

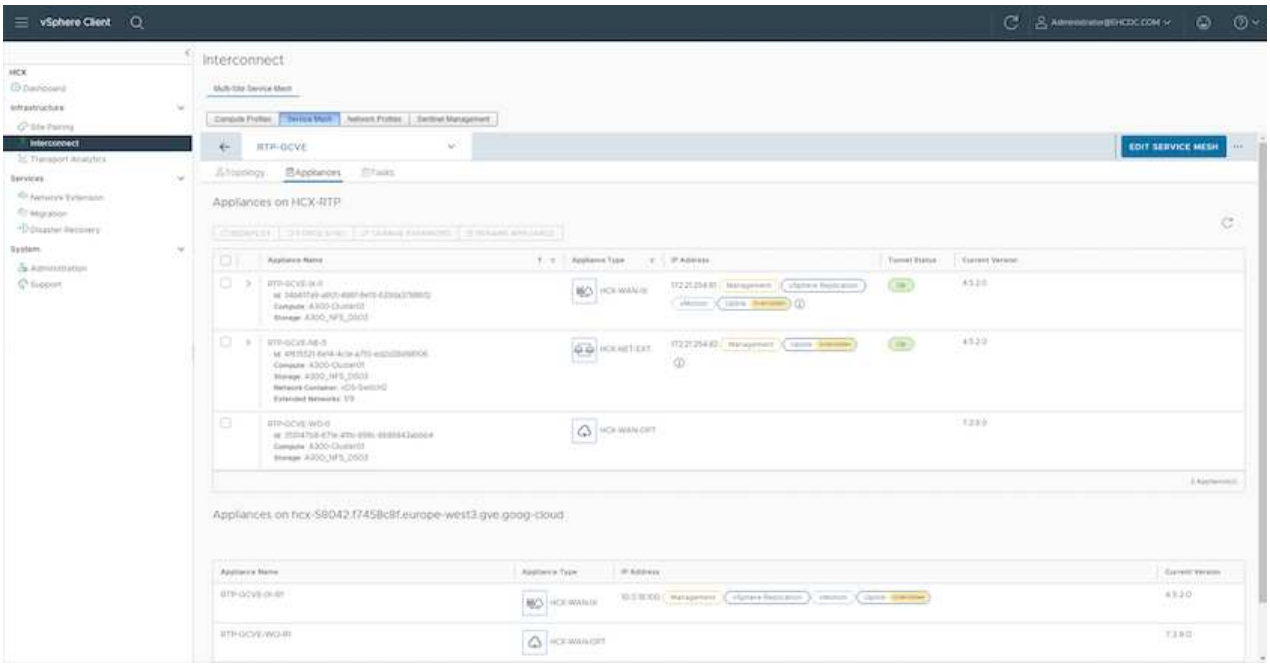


3. Derzeit wurden die Computing- und Netzwerkprofile erfolgreich erstellt.
4. Erstellen Sie das Service Mesh, indem Sie in der Option **Interconnect** die Registerkarte **Service Mesh** auswählen und die On-Premises- und GCVE SDDC-Sites auswählen.
5. Das Service Mesh gibt ein lokales und entferntes Compute- und Netzwerkprofilpaar an.

Im Rahmen dieses Prozesses werden die HCX-Appliances sowohl an den Quell- als auch an den Zielstandorten bereitgestellt und automatisch konfiguriert, um eine sichere Transportstruktur zu erstellen.



6. Dies ist der letzte Konfigurationsschritt. Die Implementierung sollte also fast 30 Minuten dauern. Nach der Konfiguration des Service-Mesh ist die Umgebung bereit, wobei die IPsec-Tunnel erfolgreich erstellt wurden, um die Workload-VMs zu migrieren.



Schritt 6: Migration von Workloads

Workloads können mithilfe verschiedener VMware HCX Migrationstechnologien bidirektional zwischen lokalen und GCVE SDDCs migriert werden. VMs können mithilfe von mehreren Migrationstechnologien wie HCX Bulk Migration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (erhältlich mit HCX Enterprise Edition) und HCX OS Assisted Migration (erhältlich mit der HCX Enterprise Edition) in und von VMware HCX Enterprise Edition verschoben werden.

Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter "Migration von VMware-VMs mithilfe der VMware HCX-Dokumentation".

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

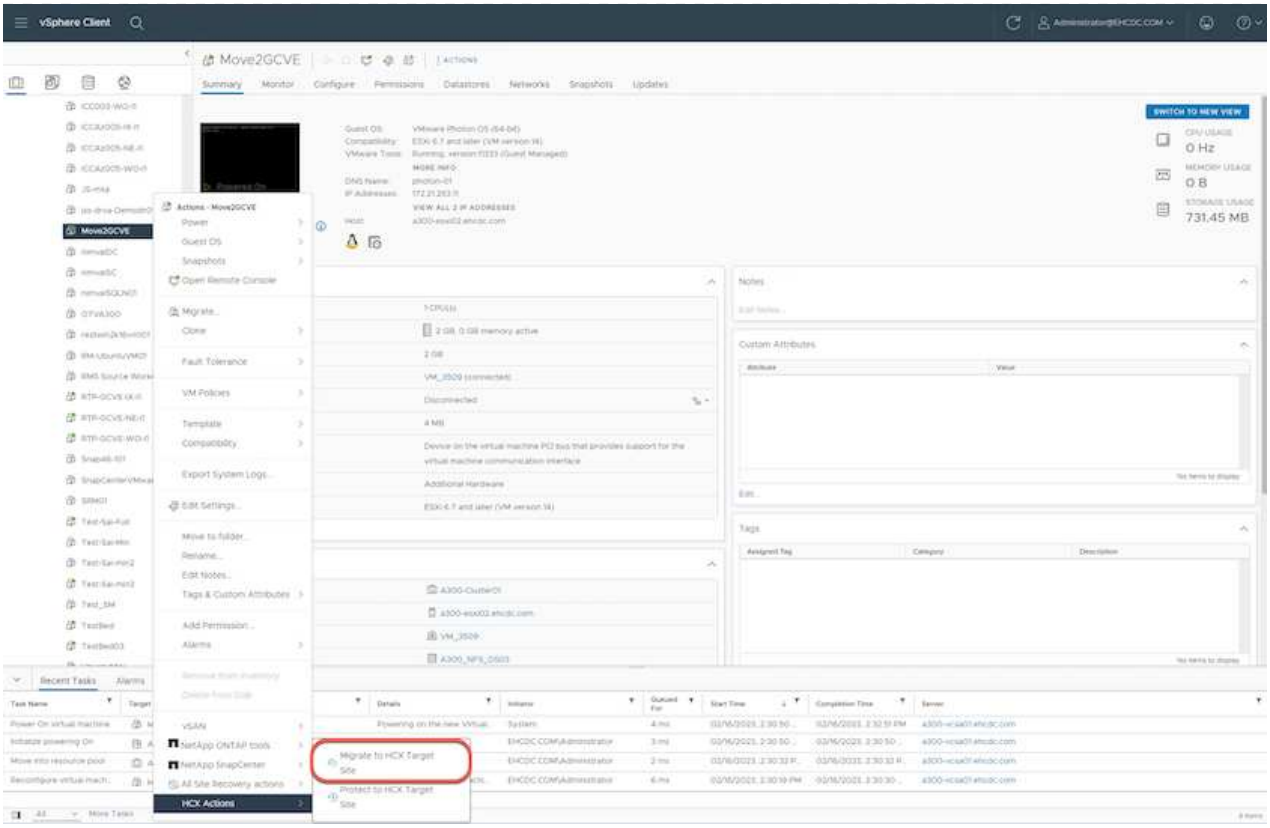
> ⓘ Die HCX-IX Appliance fügt den Mobility Agent-Service als Hostobjekt im vCenter Server hinzu. Der auf diesem Objekt angezeigte Prozessor, Arbeitsspeicher, Speicher und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch des physischen Hypervisors dar, der die IX-Appliance hostet.

HCX vMotion

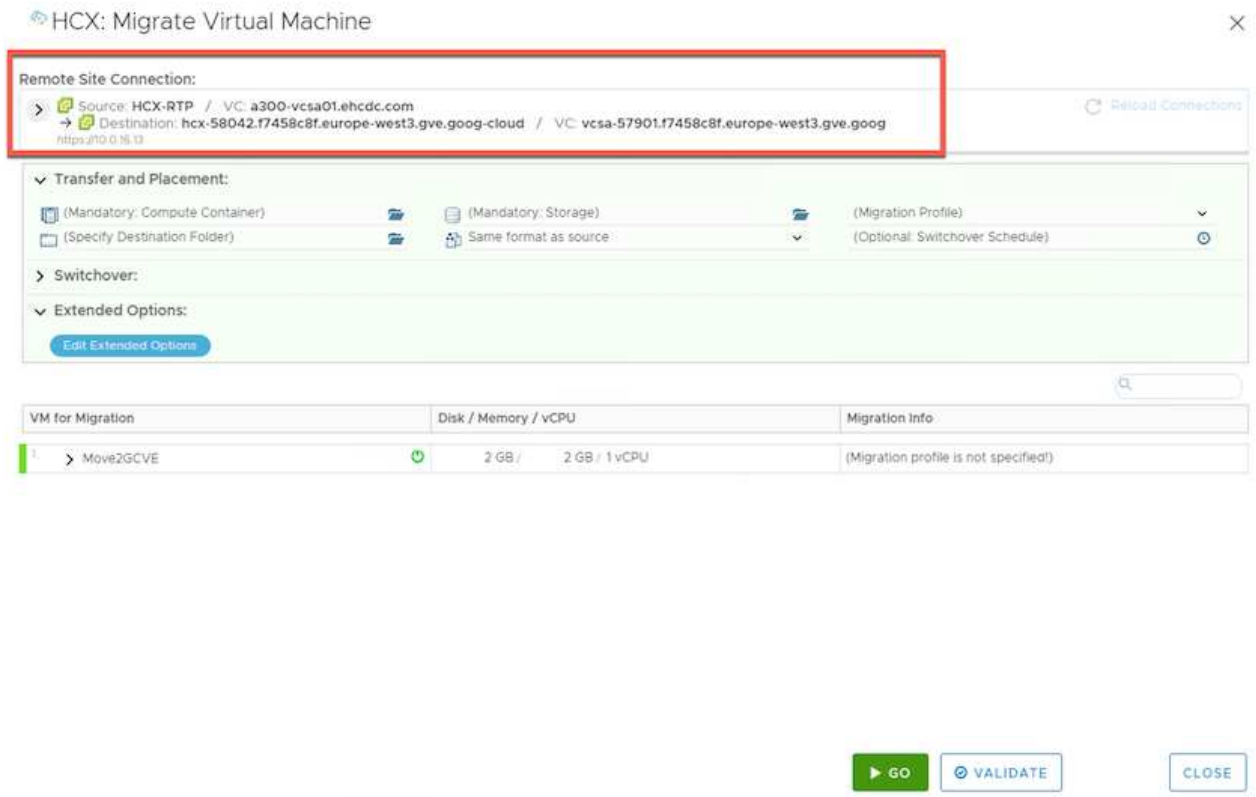
In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie verwendet das VMware vMotion Protokoll für die Migration einer VM zu GCVE. Die vMotion Migrationsoption wird verwendet, um den VM-Status einer einzelnen VM gleichzeitig zu migrieren. Während dieser Migrationsmethode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

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

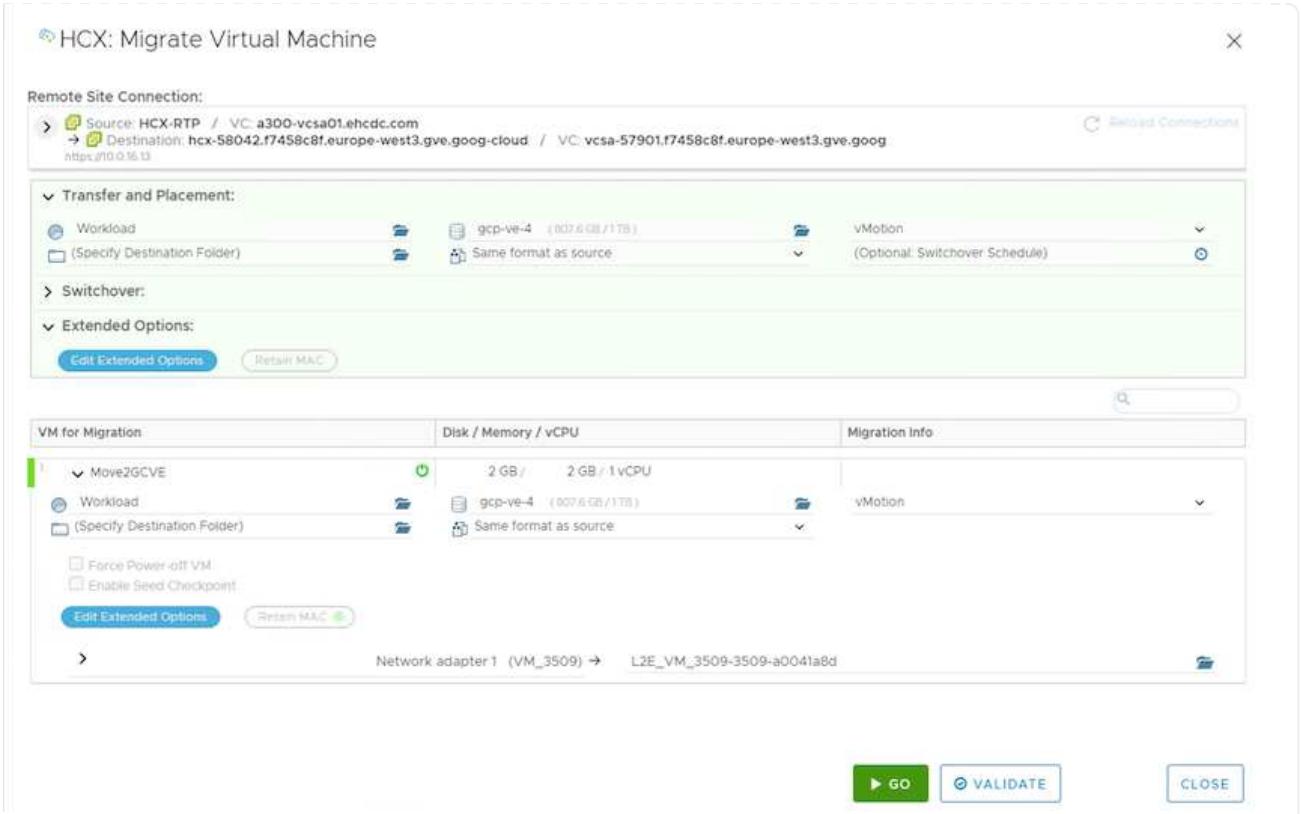
1. Wechseln Sie vom lokalen vSphere-Client zum Inventory, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie HCX Actions > Migrate to HCX Target Site aus.



2. Wählen Sie im Assistenten zum Migrieren von Virtual Machine die Remote-Standortverbindung (Ziel-GCVE) aus.



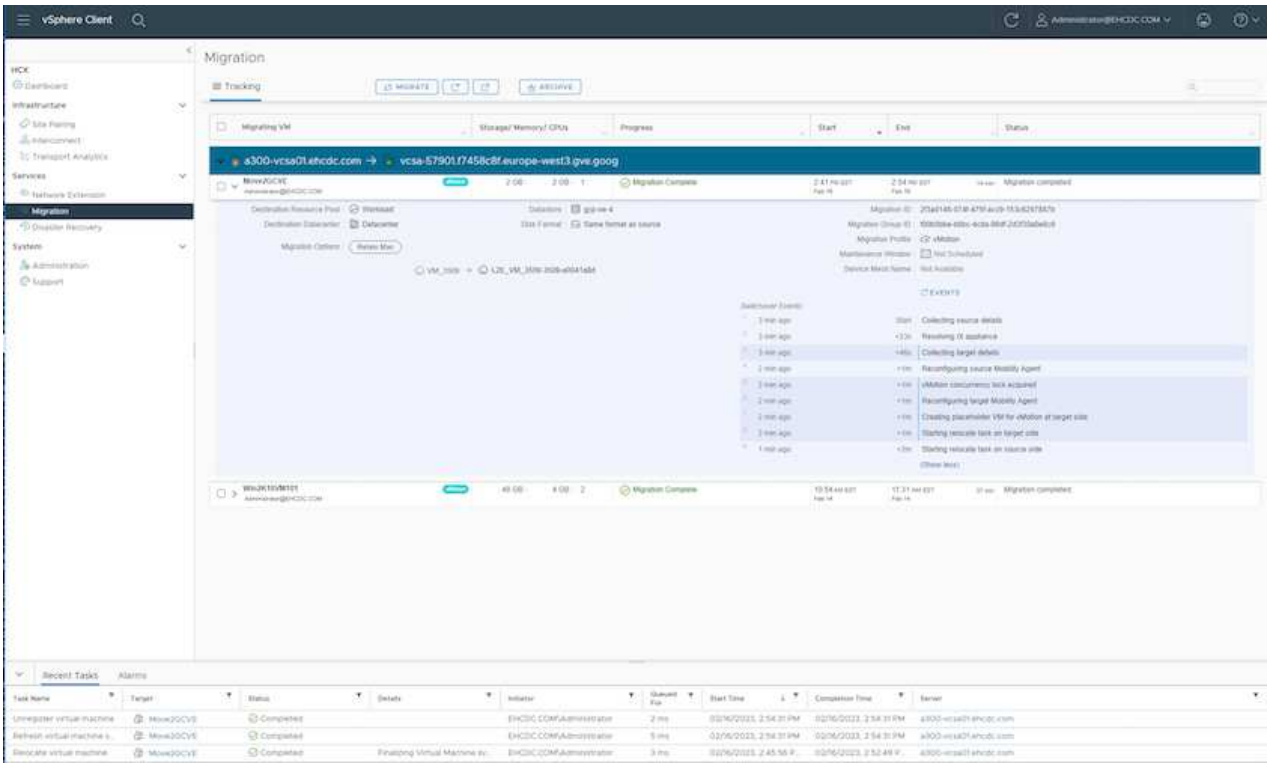
3. Aktualisieren Sie die Pflichtfelder (Cluster, Speicher und Zielnetzwerk), und klicken Sie auf Validieren.



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

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

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



Der Ziel-NFS-Datastore von Google Cloud NetApp Volumes (NetApp Volumes) sollte über ausreichend Speicherplatz für die Migration verfügen.

Schlussfolgerung

Egal, ob Sie auf All-Cloud- oder Hybrid-Cloud-Umgebungen oder Daten auf Storage eines beliebigen Typs oder Anbieters vor Ort abzielen – Cloud Volume Service und HCX bieten hervorragende Optionen für die Implementierung und Migration der Applikations-Workloads und senken gleichzeitig die TCO, indem die Datenanforderungen nahtlos auf die Applikationsebene reduziert werden. Wie auch immer der Anwendungsfall aussieht: Die Google Cloud VMware Engine und Cloud Volume Service sorgen für die schnelle Realisierung der Cloud-Vorteile, eine konsistente Infrastruktur und Abläufe vor Ort und in mehreren Clouds, bidirektionale Workload-Portabilität und Kapazität und Performance der Enterprise-Klasse. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, die zum Verbinden des Storage und zur Migration von VMs mithilfe von VMware vSphere Replication, VMware vMotion oder sogar NFS (Network File Copy) verwendet werden.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können Cloud Volume Service jetzt als Datastore auf dem Google Cloud VMware Engine SDDC nutzen.
- Daten lassen sich problemlos von On-Premises- zu Cloud Volume Service-Datastores migrieren.
- Erweitern und verkleinern Sie den Cloud Volume Service-Datastore einfach, um die Kapazitäts- und Performance-Anforderungen während der Migration zu erfüllen.

Videos von Google und VMware als Referenz

Von Google

- "HCX Connector mit GCVE bereitstellen"
- "Konfigurieren Sie HCX ServiceMesh mit GCVE"
- "VM mit HCX auf GCVE migrieren"

Von VMware

- "HCX Connector-Bereitstellung für GCVE"
- "HCX ServiceMesh-Konfiguration für GCVE"
- "HCX-Workload-Migration zu GCVE"

Wo Sie weitere Informationen finden

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

- Dokumentation der Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Dokumentation des Cloud Volume Service

  "https://cloud.google.com/architecture/partners/netapp-cloud-volumes"

- VMware HCX-Benutzerhandbuch

  "https://docs.vmware.com/en/VMware-HCX/index.html"

VM-Migration zu Google Cloud NetApp Volumes NFS-Datastore auf Google Cloud VMware Engine mithilfe der Veeam Replizierungsfunktion

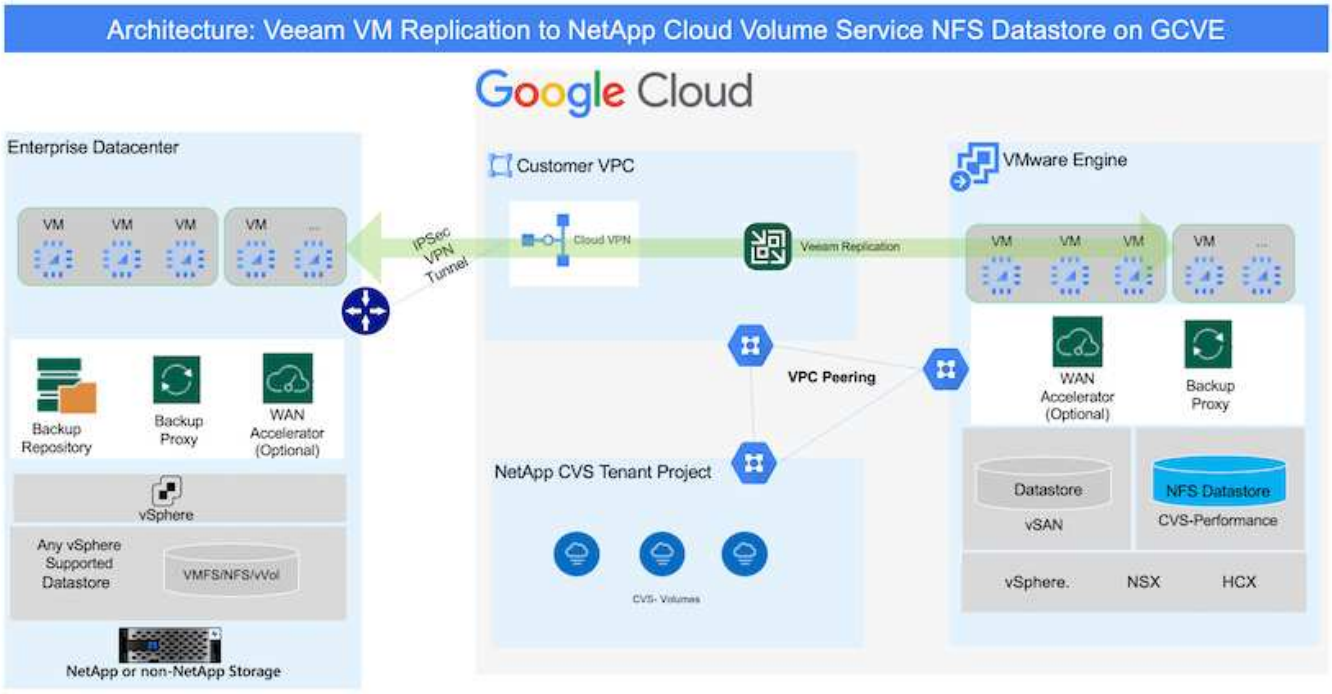
Kunden, die derzeit Veeam für ihre Datensicherungsanforderungen verwenden, verwenden die Lösung weiterhin, um die Workloads zu GCVE zu migrieren und von den Vorteilen der Google Cloud NetApp Volumes NFS-Datastores zu profitieren.

Überblick

Autoren: Suresh ThopPay, NetApp

VM-Workloads, die auf VMware vSphere ausgeführt werden, können mithilfe der Veeam Replication-Funktion in die Google Cloud VMware Engine (GCVE) migriert werden.

Dieses Dokument bietet einen Schritt-für-Schritt-Ansatz für die Einrichtung und Durchführung einer VM-Migration mit Google Cloud NetApp Volumes, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

In diesem Dokument wird vorausgesetzt, dass Sie entweder Google Cloud VPN oder Cloud Interconnect oder eine andere Netzwerkoption einsetzen, um die Netzwerkverbindung von bestehenden vSphere Servern zur Google Cloud VMware Engine herzustellen.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Siehe "Google Cloud-Dokumentation" Für die geeignete On-Premises-zu-Google-Verbindungsmethode.

Bereitstellen der Migrationslösung

Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass der NFS-Datastore aus den Google Cloud NetApp Volumes in GCVE vCenter gemountet ist.
2. Sicherstellen, dass Veeam Backup Recovery in vorhandener VMware vSphere-Umgebung implementiert wird
3. Erstellen Sie einen Replikationsjob, um die Replikation virtueller Maschinen auf die Instanz der Google Cloud VMware Engine zu starten.
4. Führen Sie ein Failover des Veeam Replication Job durch.
5. Führen Sie ein Permanent Failover auf Veeam durch.

Einzelheiten Zur Bereitstellung

Stellen Sie sicher, dass der NFS-Datastore aus den Google Cloud NetApp Volumes in GCVE vCenter gemountet ist

Melden Sie sich bei GCVE vCenter an, und stellen Sie sicher, dass ein NFS-Datastore mit ausreichend

Speicherplatz verfügbar ist. Falls nicht, wenden Sie sich bitte an "Mounten Sie NetApp Volumes als NFS-Datastore in GCVE"

Sicherstellen, dass Veeam Backup Recovery in vorhandener VMware vSphere-Umgebung implementiert wird

Weitere Informationen finden Sie unter "Veeam Replizierungskomponenten" Dokumentation zur Installation der erforderlichen Komponenten.

Erstellen Sie einen Replikationsjob, um die Replikation virtueller Maschinen auf die Instanz der Google Cloud VMware Engine zu starten.

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten"
Hier ist ein Video, in dem erklärt wird, wie
"Konfigurieren Sie Den Replikationsjob".

Die ReplikatVM kann eine andere IP-Adresse als die Quell-VM haben und kann auch mit einer anderen Portgruppe verbunden werden. Weitere Informationen finden Sie im Video oben.

Führen Sie ein Failover des Veeam Replication Job durch

Führen Sie zum Migrieren von VMs aus "Führen Sie Ein Failover Durch"

Führen Sie ein Permanent Failover auf Veeam durch.

Um GCVE als Ihre neue Quellumgebung zu behandeln, führen Sie aus "Permanenter Failover"

Vorteile dieser Lösung

- Die vorhandene Veeam Backup-Infrastruktur kann für die Migration genutzt werden.
- Veeam Replication ermöglicht das Ändern von VM-IP-Adressen am Zielstandort.
- Vorhandene Daten, die außerhalb von Veeam repliziert wurden (wie replizierte Daten von BlueXP), können neu zugeordnet werden.
- Kann unterschiedliche Netzwerk-Portgruppen am Zielstandort angeben.
- Kann die Reihenfolge der VMs angeben, die eingeschaltet werden sollen.
- Verwendet VMware Change Block Tracking, um die Datenmenge zu minimieren, die über WAN gesendet werden soll.
- Möglichkeit zum Ausführen von Pre- und Post-Skripten für die Replizierung.
- Möglichkeit zur Ausführung von Pre-und Post-Skripten für Snapshots.

Regionale Verfügbarkeit – ergänzender NFS-Datastore für Google Cloud Platform (GCP)

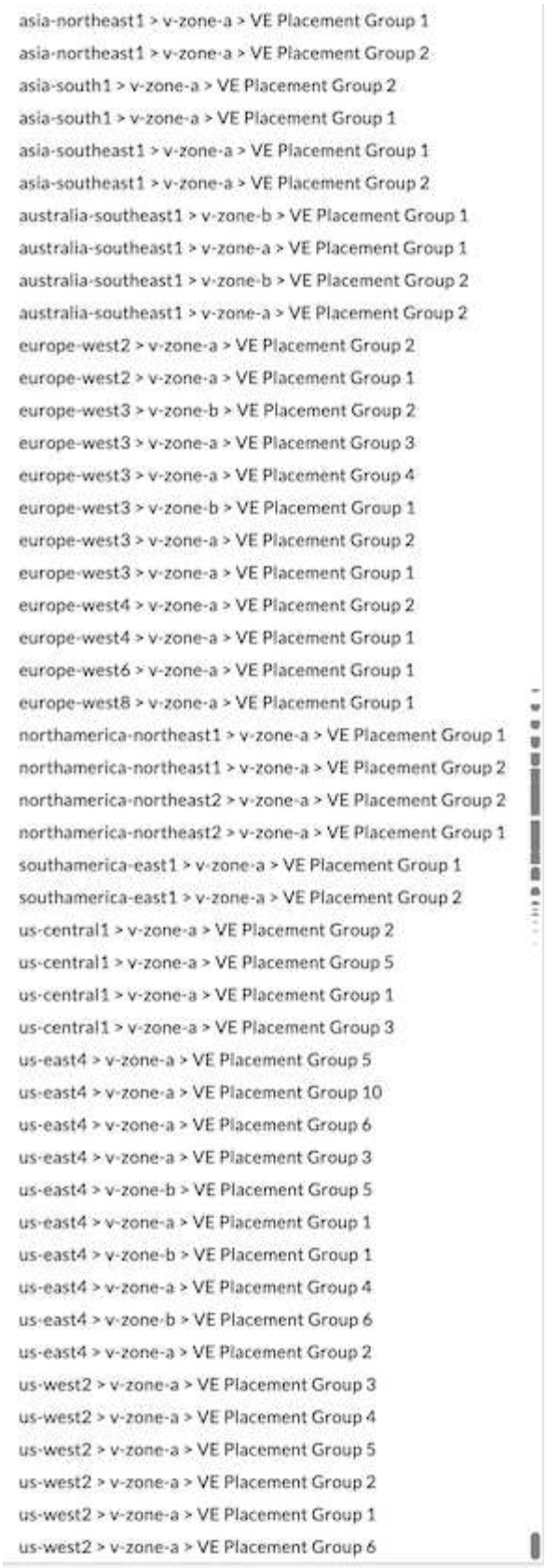
Weitere Informationen: Support für GCP, GCVE und NetApp Volumes in der globalen Region

Der NFS-Datastore ist in Regionen verfügbar, in denen beide Services (GCVE und NetApp Volumes Performance) verfügbar sind.

Der zusätzliche NFS-Datastore für GCVE wird von Google Cloud NetApp Volumes unterstützt.

> Für den GCVE NFS-Datastore können nur NetApp Volumes mit Performance Volume-Performance verwendet werden. Informationen zum verfügbaren Speicherort finden Sie unter "Globale Regionalkarte"

Google Cloud VMware Engine ist an folgenden Orten verfügbar:



Um die Latenz zu minimieren, sollten sich NetApp NetApp Volumes (NetApp Volumes) und GCVE, wo Sie das Volume mounten möchten, in derselben Verfügbarkeitszone befinden. Arbeiten Sie mit Google und NetApp Solution Architects zusammen, um Verfügbarkeit und TCO-Optimierung zu optimieren.