Migration von Workloads auf GCP/GCVE

NetApp Solutions

NetApp
April 26, 2024

Inhalt

Migration von Workloads auf GCP/GCVE

Workloads mit VMware HCX - QuickStart Guide auf den NetApp Cloud Volume Service Datastore auf der Google Cloud VMware Engine migrieren

Autor(en): NetApp Solutions Engineering

Übersicht: Migration von Virtual Machines mit VMware HCX, NetApp Cloud Volume Service Datastores und Google Cloud VMware Engine (GCVE)

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

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

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

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

Allgemeine Schritte

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

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

Voraussetzungen

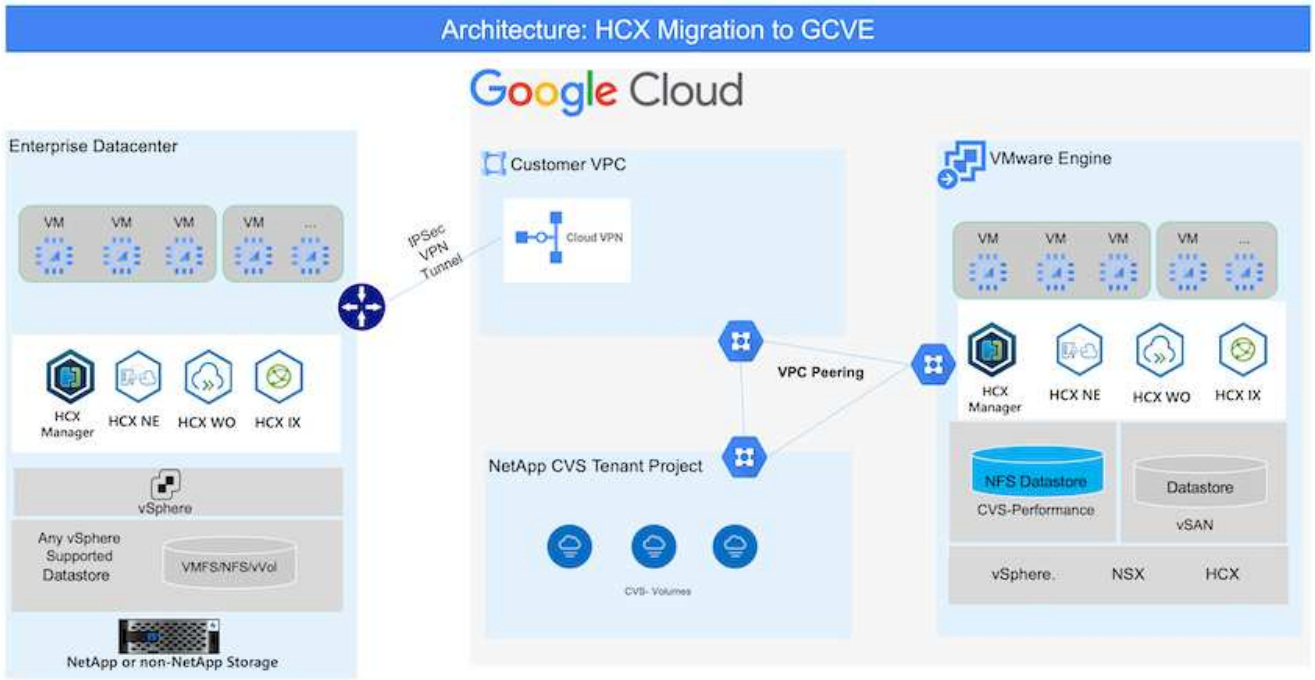
Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "Verlinken". Nachdem die Voraussetzungen, einschließlich Konnektivität, vorhanden sind, laden Sie den HCX-Lizenzschlüssel aus dem Google Cloud VMware Engine-Portal herunter.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

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

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

Übergeordnete Architektur

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



Nähere Informationen zu HCX finden Sie unter "Link zu VMware"

Lösungsimplementierung

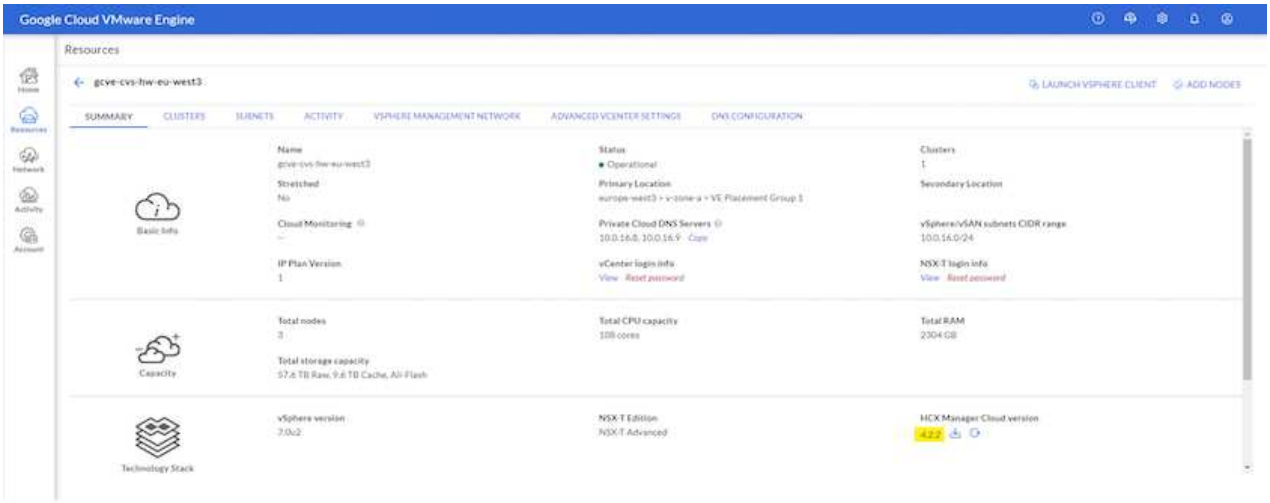
Führen Sie die folgenden Schritte aus, um die Implementierung dieser Lösung abzuschließen:

Schritt 1: HCX über das Google VMware Engine Portal vorbereiten

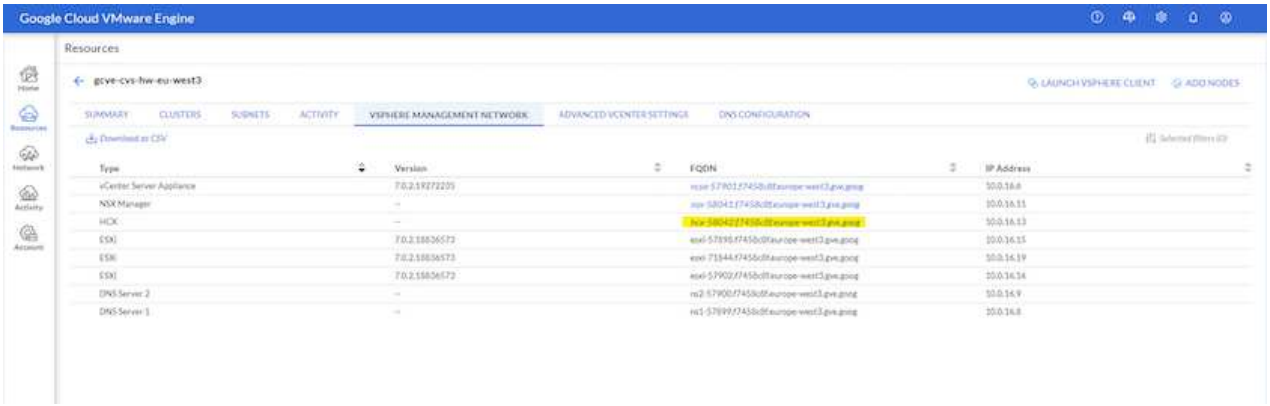
HCX Cloud Manager wird automatisch installiert, wenn Sie eine Private Cloud mit VMware Engine bereitstellen. Gehen Sie wie folgt vor, um die Standortpaarung vorzubereiten:

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

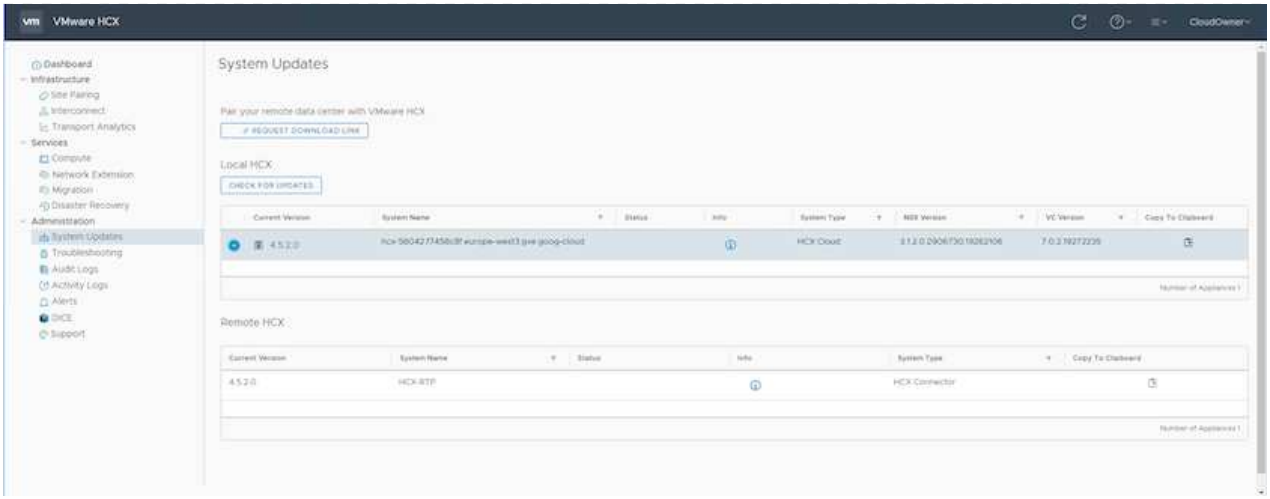
   Sie können sich bei der HCX Console anmelden, indem Sie auf den Link zur HCX-Version klicken

   Oder klicken Sie unter der Registerkarte vSphere Management Network auf HCX FQDN.

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



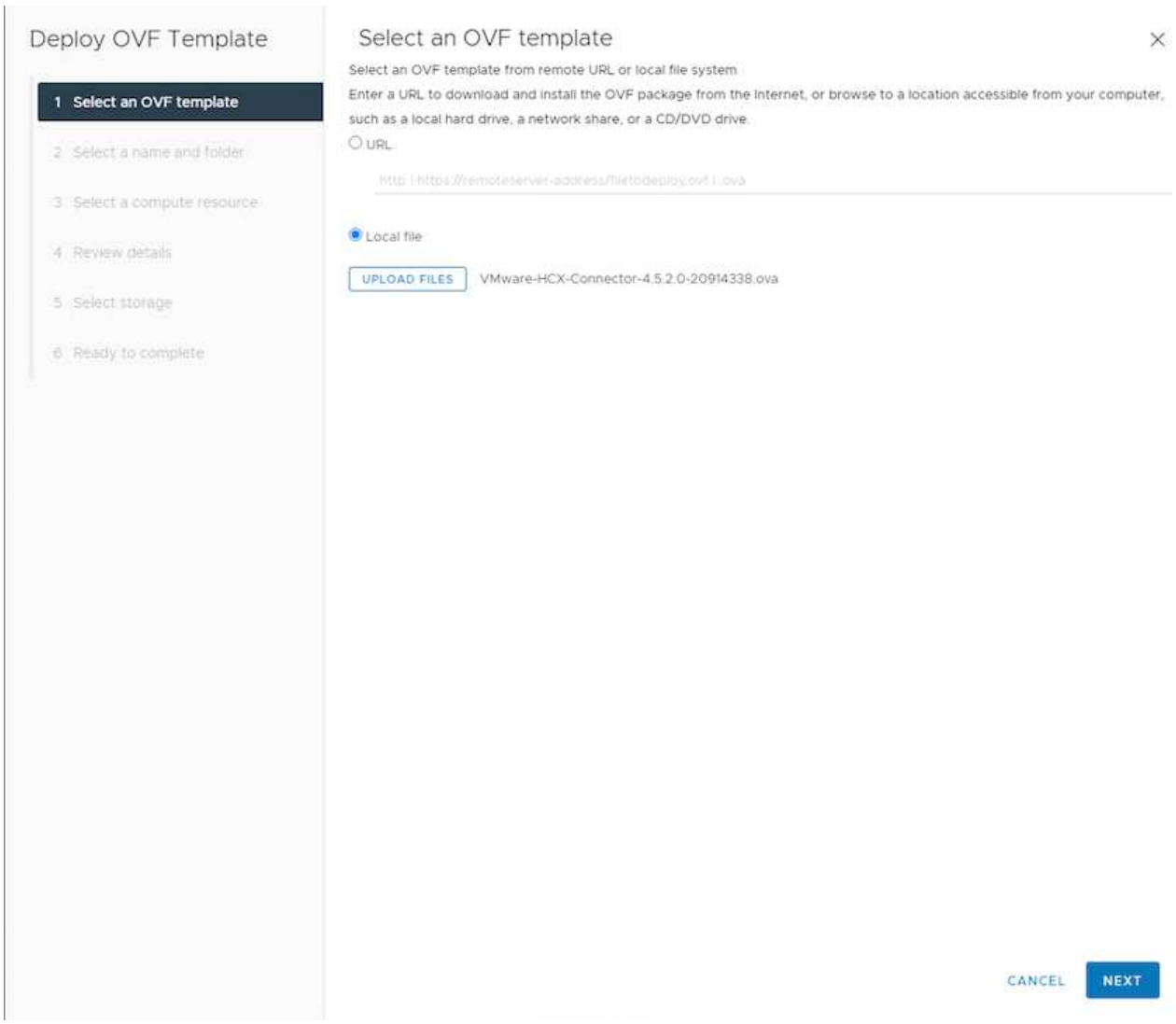
4. Aktualisieren Sie HCX Cloud Manager auf die neueste Version, die über die Benutzeroberfläche von HCX Cloud Manager verfügbar ist.

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

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

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

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



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

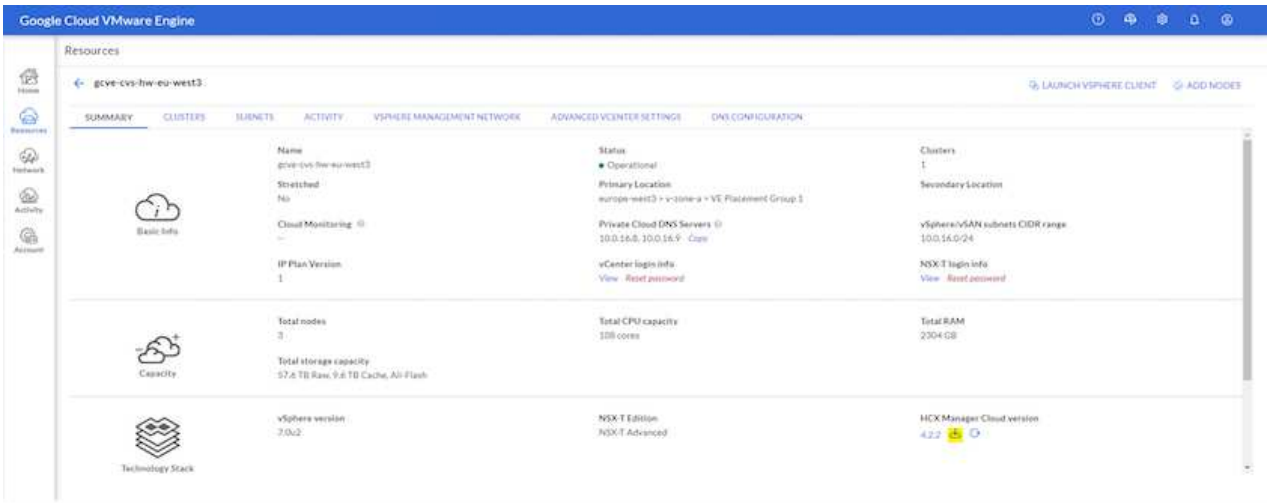
   Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "VMware HCX-Benutzerhandbuch".

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

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

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



   Öffnen Sie die heruntergeladene Datei und kopieren Sie die Zeichenfolge für den Lizenzschlüssel.

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

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

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

   > Der HCX-Connector sollte über einen Internetzugang verfügen.

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

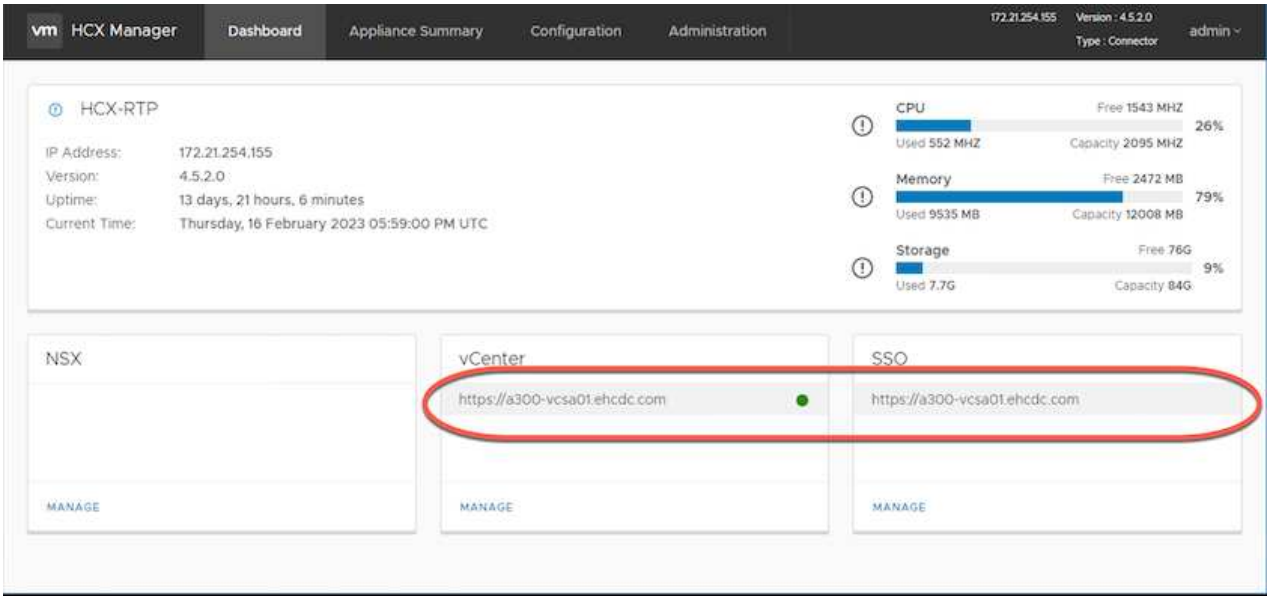
   > Verwenden Sie den FQDN, um Verbindungsprobleme später zu vermeiden.

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

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

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

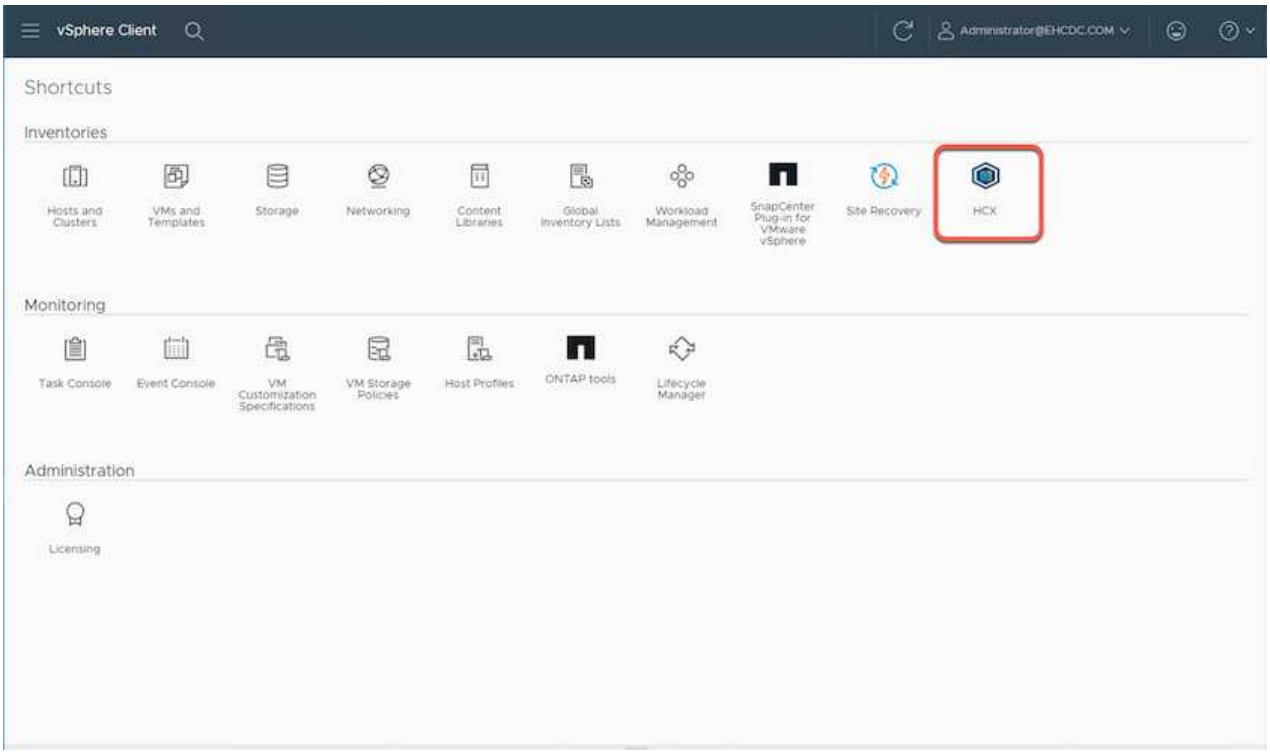
Dieser Vorgang dauert etwa 10 bis 20 Minuten, und das Plug-in wird dem vCenter Server hinzugefügt.



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

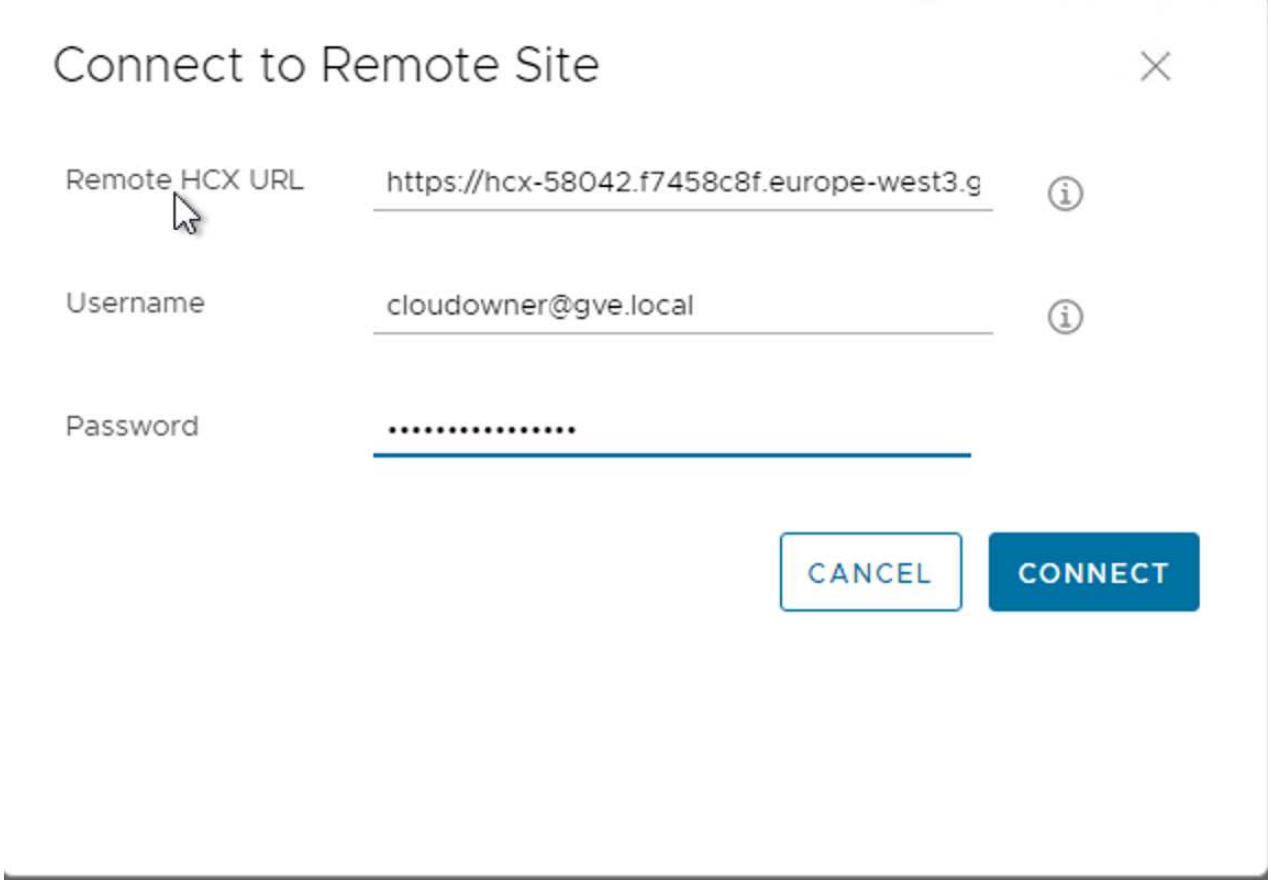
Nachdem HCX Connector im lokalen vCenter bereitgestellt und konfiguriert wurde, stellen Sie eine Verbindung zum Cloud Manager her, indem Sie die Paarung hinzufügen. Gehen Sie wie folgt vor, um die Standortpaarung zu konfigurieren:

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



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

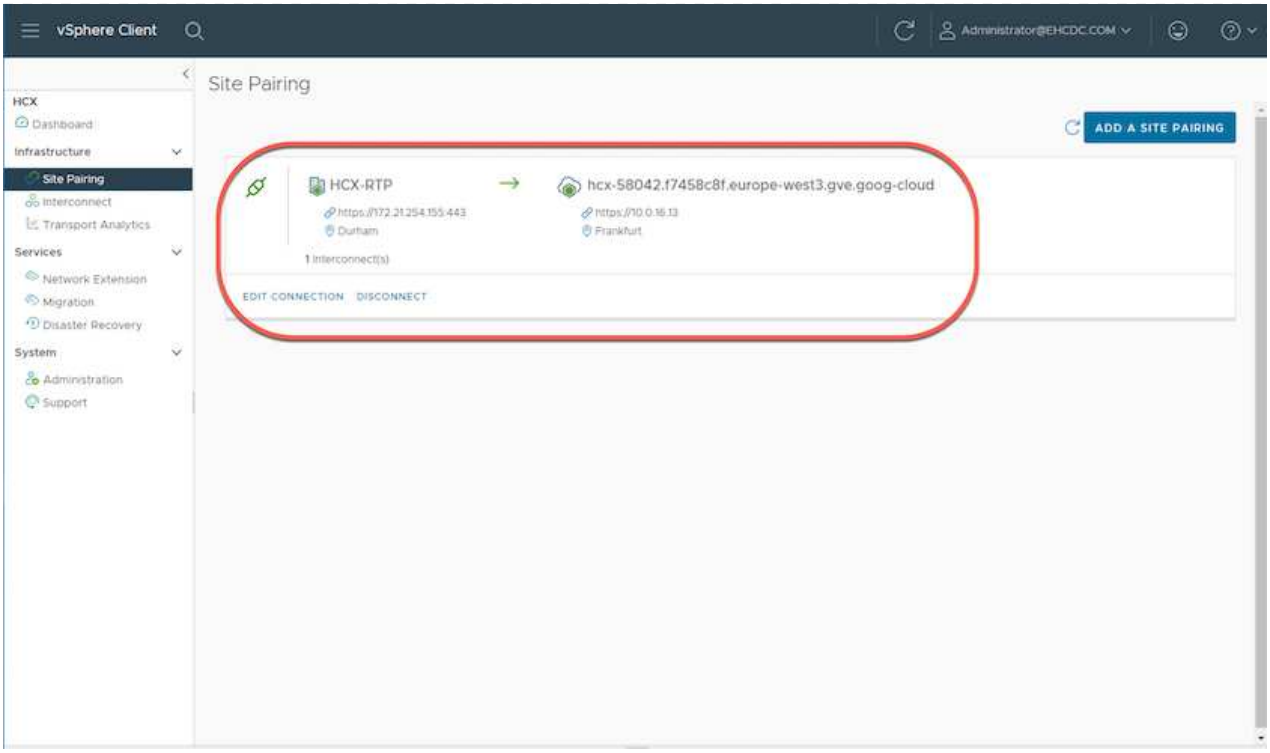
> Geben Sie die URL oder IP-Adresse des Google Cloud VMware Engine HCX Cloud Manager und die Anmeldedaten für Benutzer mit Cloud-Owner-Rollenberechtigungen für den Zugriff auf die private Cloud ein.



3. Klicken Sie Auf **Verbinden**.

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

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

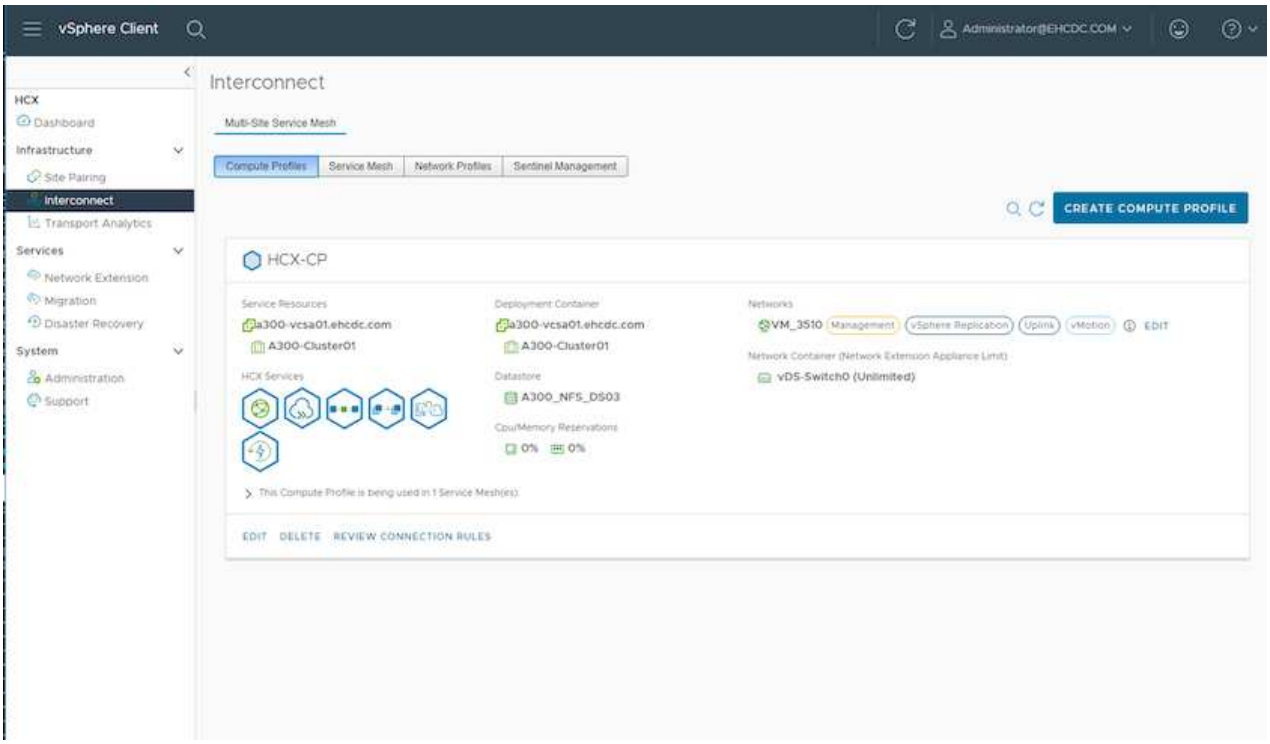

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
1 Interconnect(s)
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud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

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

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

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

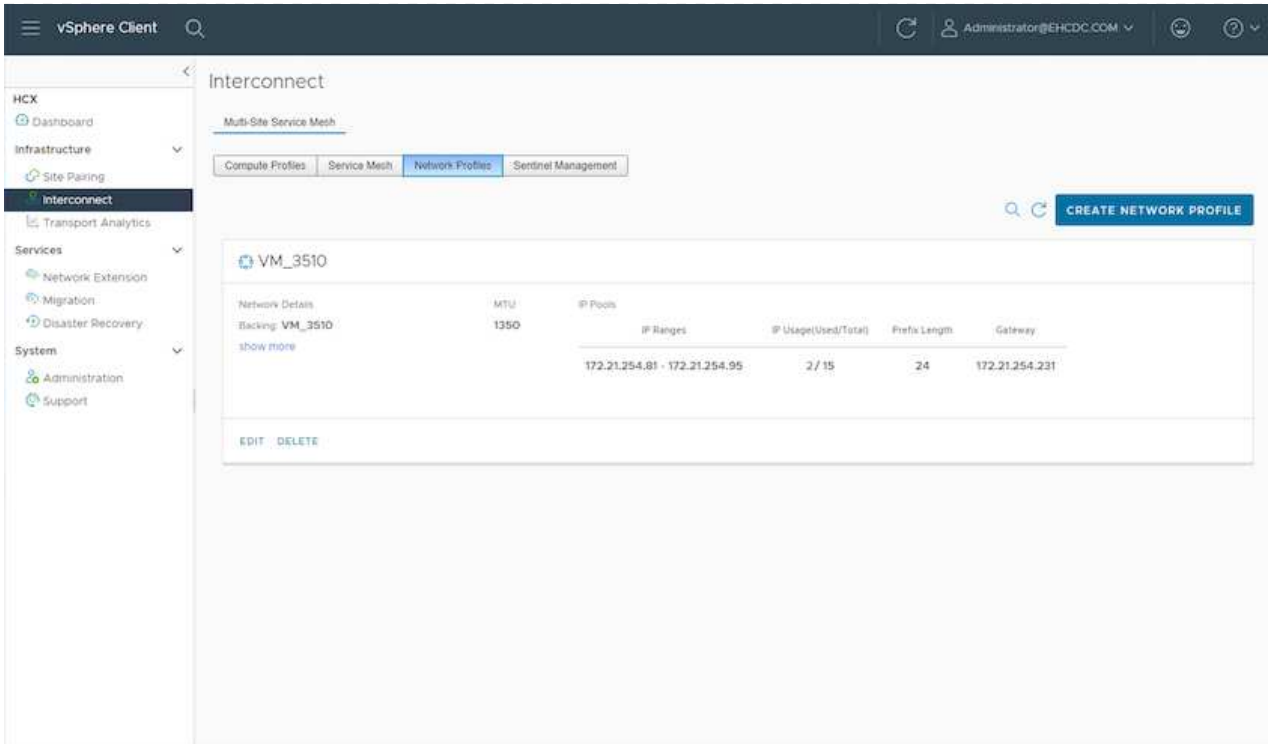
   Die Computing-Profile definieren die Implementierungsparameter einschließlich der Appliances, die bereitgestellt werden und welche Teile des VMware Datacenters für den HCX-Service verfügbar sind.



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

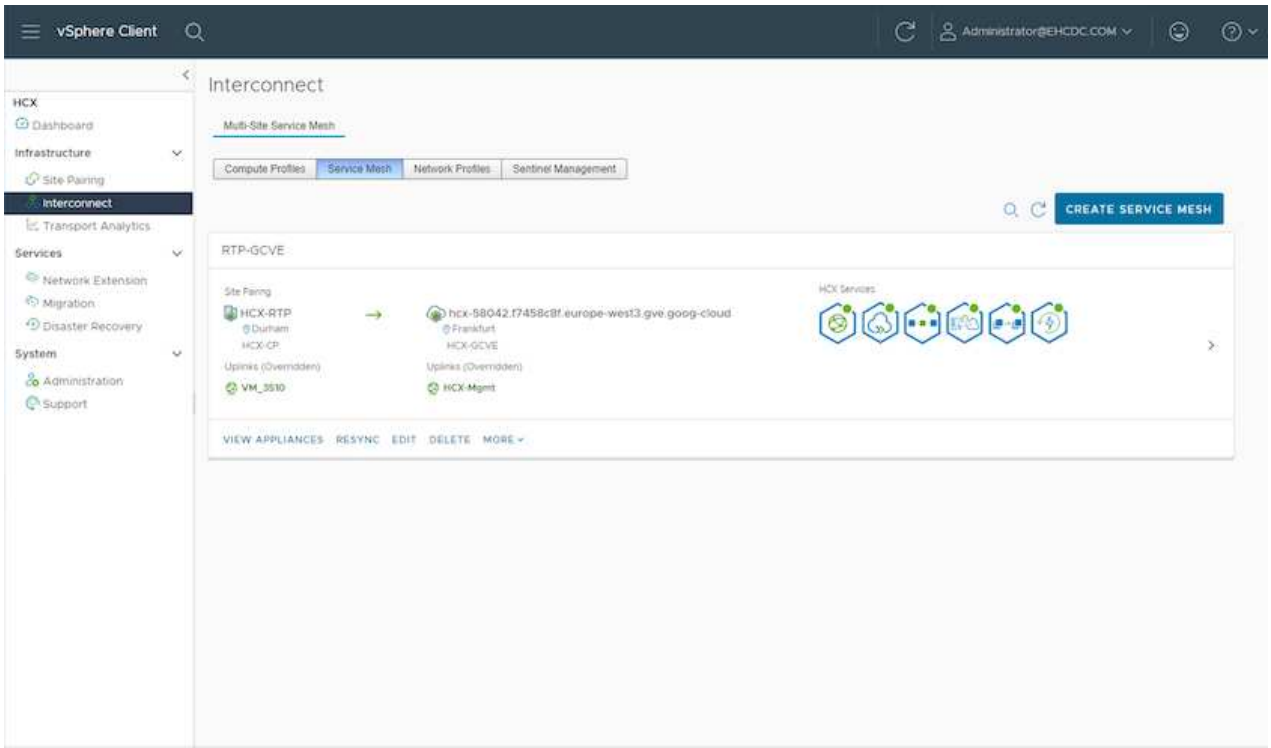
   Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

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

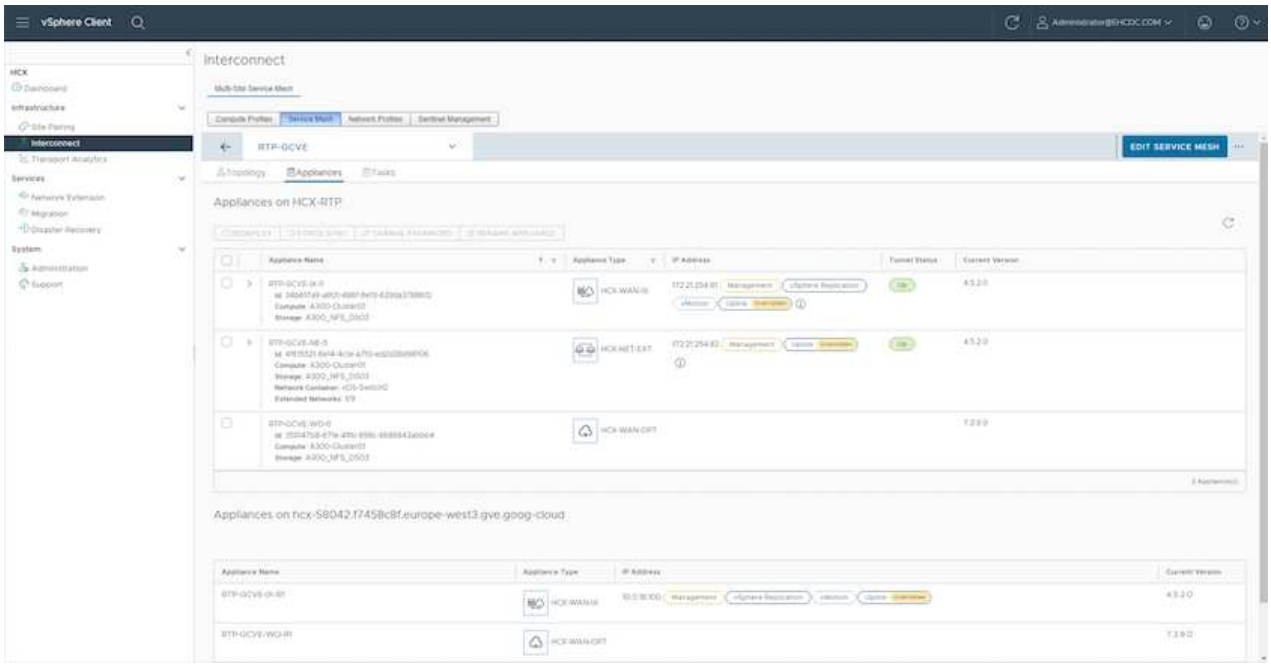


3. Derzeit wurden die Computing- und Netzwerkprofile erfolgreich erstellt.
4. Erstellen Sie das Service Mesh, indem Sie in der Option **Interconnect** die Registerkarte **Service Mesh** auswählen und die On-Premises- und GCVE SDDC-Sites auswählen.
5. Das Service Mesh gibt ein lokales und entferntes Compute-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

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



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



Schritt 6: Migration von Workloads

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

Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter "Migrationstypen von VMware HCX".

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

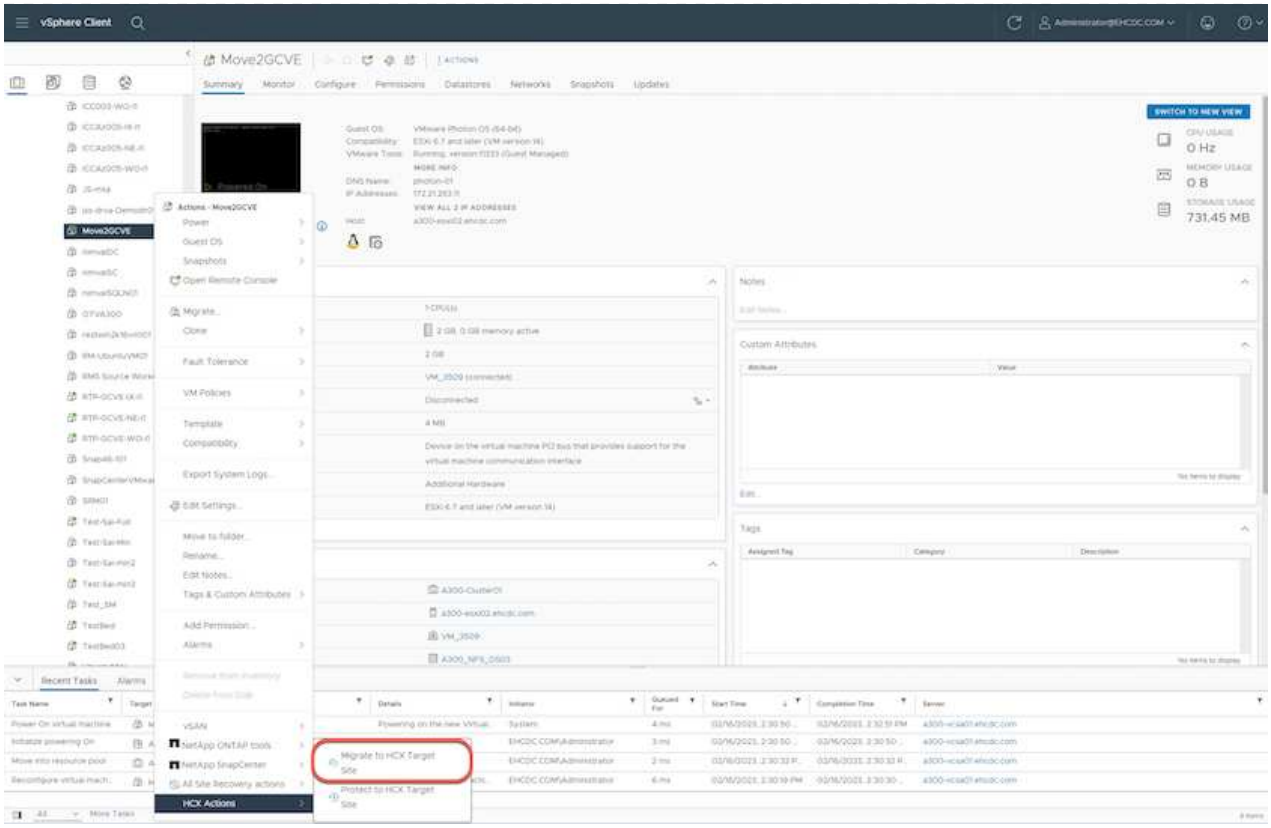
> Die HCX-IX Appliance fügt den Mobility Agent-Service als Hostobjekt im vCenter Server hinzu. Der auf diesem Objekt angezeigte Prozessor, Arbeitsspeicher, Speicher und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch des physischen Hypervisors dar, der die IX-Appliance hostet.

HCX vMotion

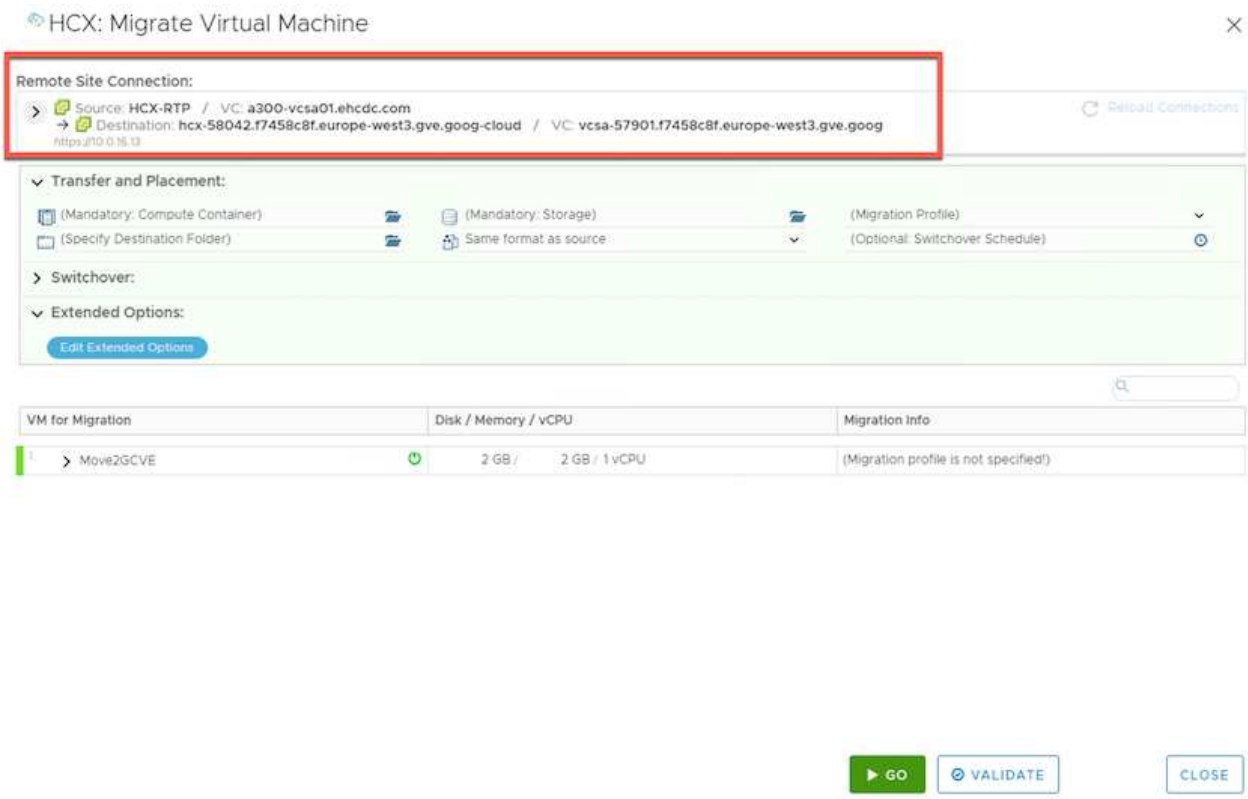
In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie verwendet das VMware vMotion Protokoll für die Migration einer VM zu GCVE. Die vMotion Migrationsoption wird verwendet, um den VM-Status einer einzelnen VM gleichzeitig zu migrieren. Während dieser Migrationsmethode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

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

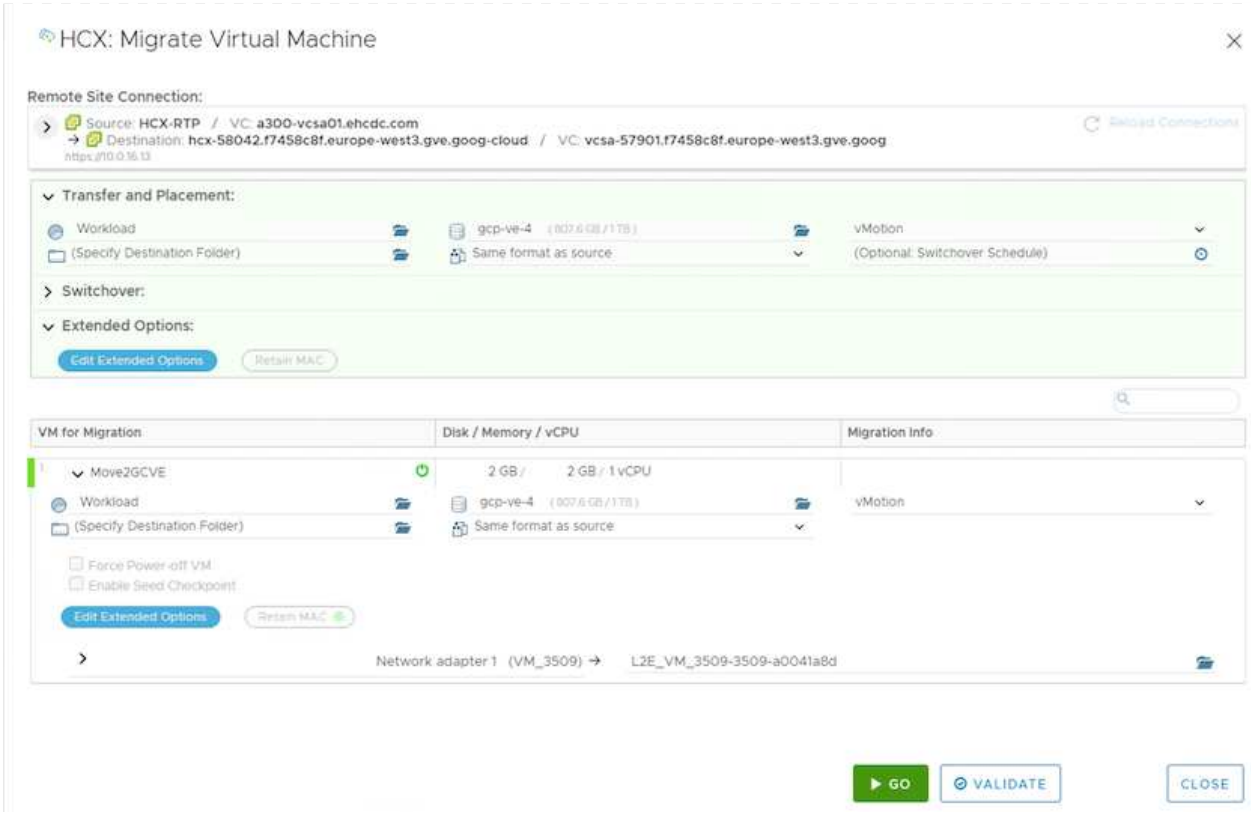
1. Wechseln Sie vom lokalen vSphere-Client zum Inventory, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie HCX Actions > Migrate to HCX Target Site aus.



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



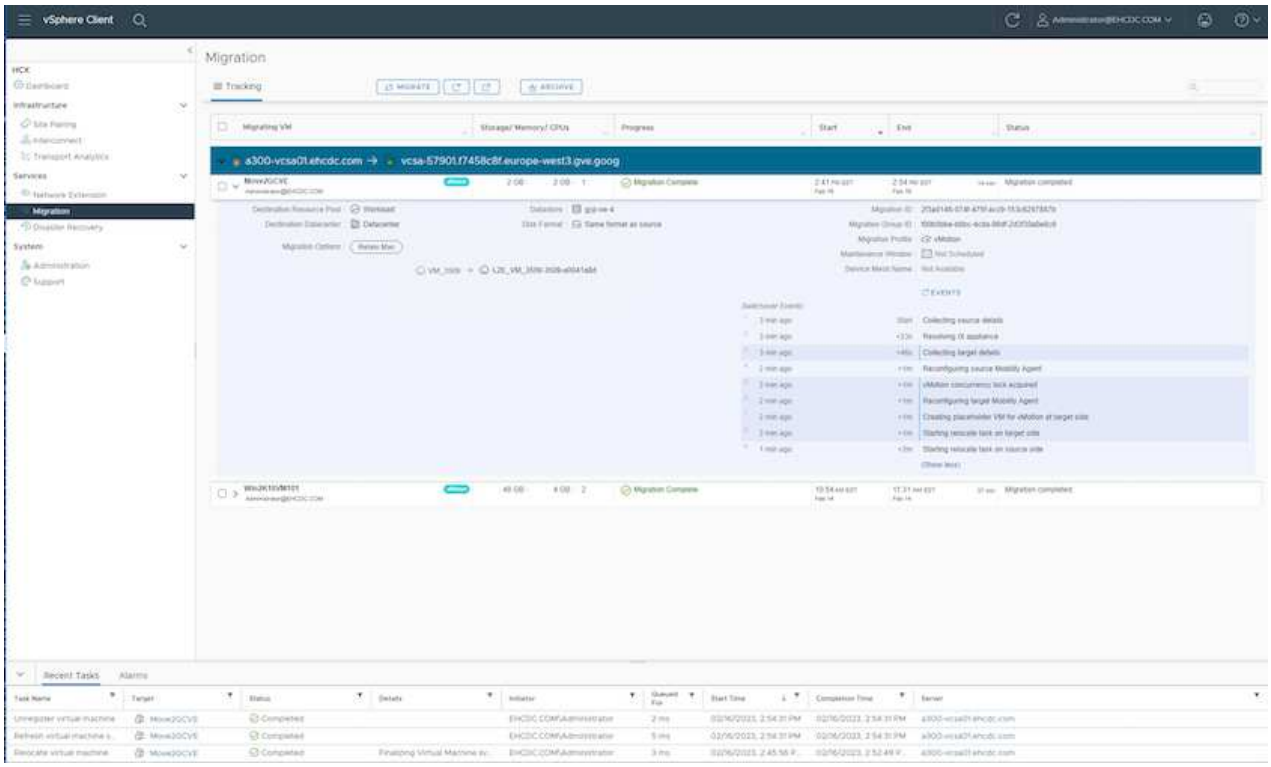
3. Aktualisieren Sie die Pflichtfelder (Cluster, Speicher und Zielnetzwerk), und klicken Sie auf Validieren.



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

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

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



Der CVS Ziel-NFS-Datastore sollte über ausreichend Speicherplatz für die Migration verfügen.

Schlussfolgerung

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

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

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

Videos von Google und VMware als Referenz

Von Google

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

Von VMware

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

Wo Sie weitere Informationen finden

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

- Dokumentation der Google Cloud VMware Engine

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

- Dokumentation des Cloud Volume Service

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

- VMware HCX-Benutzerhandbuch

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

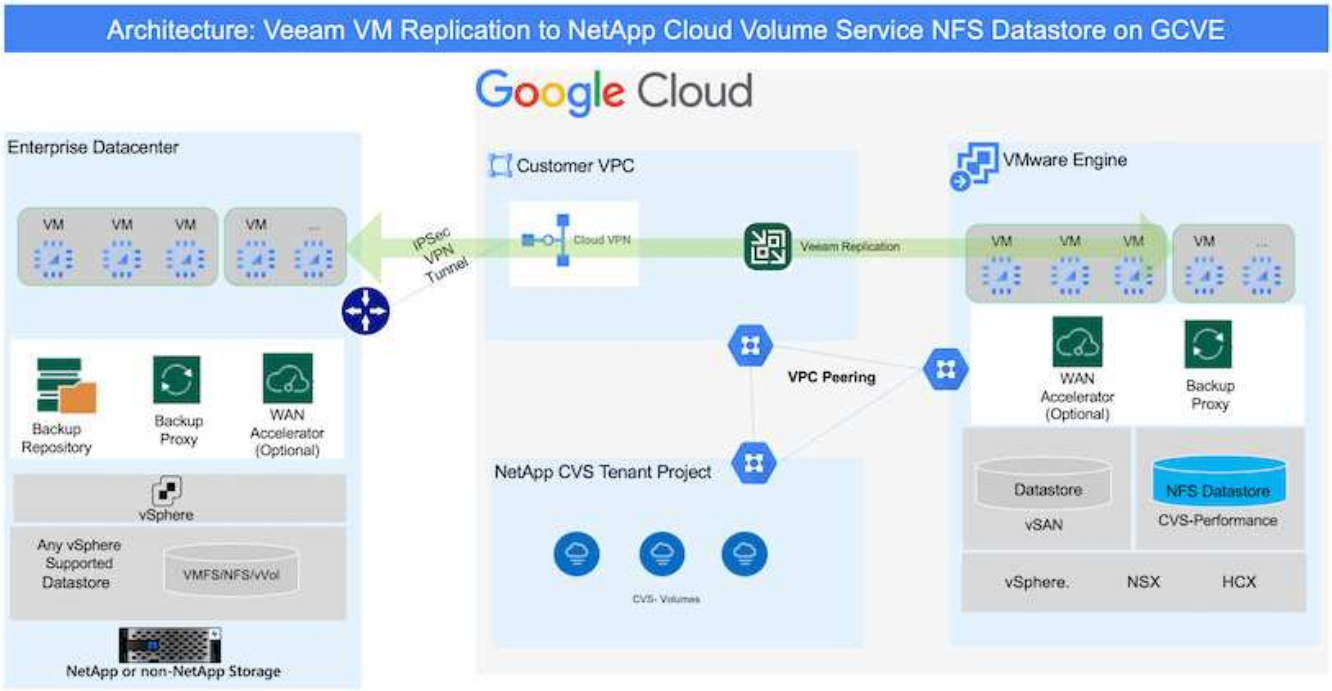
VM-Migration zu NetApp Cloud Volume Service NFS-Datastore auf Google Cloud VMware Engine mithilfe der Veeam Replizierungsfunktion

Überblick

Autoren: Suresh ThopPay, NetApp

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

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



Voraussetzungen

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

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

Bereitstellen der Migrationslösung

Übersicht Zur Lösungsimplementierung

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

Einzelheiten Zur Bereitstellung

Stellen Sie sicher, dass der NFS-Datastore aus dem NetApp-Cloud-Volume-Service in GCVE vCenter gemountet ist

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

Falls nicht, wenden Sie sich bitte an "Mounten Sie NetApp CVS als NFS-Datastore in GCVE"

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

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

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

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

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

Führen Sie ein Failover des Veeam Replication Job durch

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

Führen Sie ein Permanent Failover auf Veeam durch.

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

Vorteile dieser Lösung

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