



Migrazione dei carichi di lavoro su GCP/GCVE

NetApp Solutions

NetApp
April 26, 2024

Sommario

- Migrazione dei carichi di lavoro su GCP/GCVE 1
 - Migrazione dei carichi di lavoro nel datastore NetApp Cloud Volume Service su Google Cloud VMware Engine con VMware HCX - Guida rapida 1
 - Migrazione delle macchine virtuali al servizio volumi cloud NetApp Datastore NFS su Google Cloud VMware Engine con la funzione di replica Veeam 19

Migrazione dei carichi di lavoro su GCP/GCVE

Migrazione dei carichi di lavoro nel datastore NetApp Cloud Volume Service su Google Cloud VMware Engine con VMware HCX - Guida rapida

Autore: NetApp Solutions Engineering

Panoramica: Migrazione di macchine virtuali con VMware HCX, datastore NetApp Cloud Volume Service e Google Cloud VMware Engine (GCVE)

Uno dei casi di utilizzo più comuni per il datastore Google Cloud VMware Engine e Cloud Volume Service è la migrazione dei carichi di lavoro VMware. VMware HCX è un'opzione preferita e offre vari meccanismi di migrazione per spostare macchine virtuali (VM) on-premise e i relativi dati negli archivi dati NFS Cloud Volume Service.

VMware HCX è principalmente una piattaforma di migrazione progettata per semplificare la migrazione delle applicazioni, il ribilanciamento dei carichi di lavoro e persino la business continuity tra i cloud. È incluso come parte di Google Cloud VMware Engine Private Cloud e offre diversi modi per migrare i workload e può essere utilizzato per le operazioni di disaster recovery (DR).

Il presente documento fornisce istruzioni dettagliate per il provisioning del datastore Cloud Volume Service, seguito dal download, dall'implementazione e dalla configurazione di VMware HCX, inclusi tutti i componenti principali on-premise e dal lato motore VMware di Google Cloud, tra cui Interconnect, Network Extension e ottimizzazione WAN per l'abilitazione di vari meccanismi di migrazione delle macchine virtuali.



VMware HCX funziona con qualsiasi tipo di datastore poiché la migrazione è a livello di VM. Pertanto, questo documento è valido per i clienti NetApp esistenti e non NetApp che intendono implementare Cloud Volume Service con Google Cloud VMware Engine per un'implementazione cloud VMware conveniente.

Passaggi di alto livello

Questo elenco fornisce i passaggi di alto livello necessari per associare e migrare le macchine virtuali a HCX Cloud Manager sul lato Google Cloud VMware Engine da HCX Connector on-premise:

1. Preparare HCX attraverso il portale Google VMware Engine.
2. Scaricare e implementare IL programma di installazione DI HCX Connector Open Virtualization Appliance (OVA) nel server VMware vCenter on-premise.
3. Attivare HCX con la chiave di licenza.
4. Associare il connettore VMware HCX on-premise con Google Cloud VMware Engine HCX Cloud Manager.
5. Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio.
6. (Facoltativo) eseguire l'estensione di rete per evitare il re-IP durante le migrazioni.
7. Verificare lo stato dell'appliance e assicurarsi che sia possibile eseguire la migrazione.
8. Migrare i carichi di lavoro delle macchine virtuali.

Prerequisiti

Prima di iniziare, assicurarsi che siano soddisfatti i seguenti prerequisiti. Per ulteriori informazioni, consulta questa sezione ["collegamento"](#). Una volta soddisfatti i prerequisiti, inclusa la connettività, scaricare la chiave di licenza HCX dal portale VMware Engine di Google Cloud. Una volta scaricato il programma di installazione di OVA, procedere con la procedura di installazione come descritto di seguito.

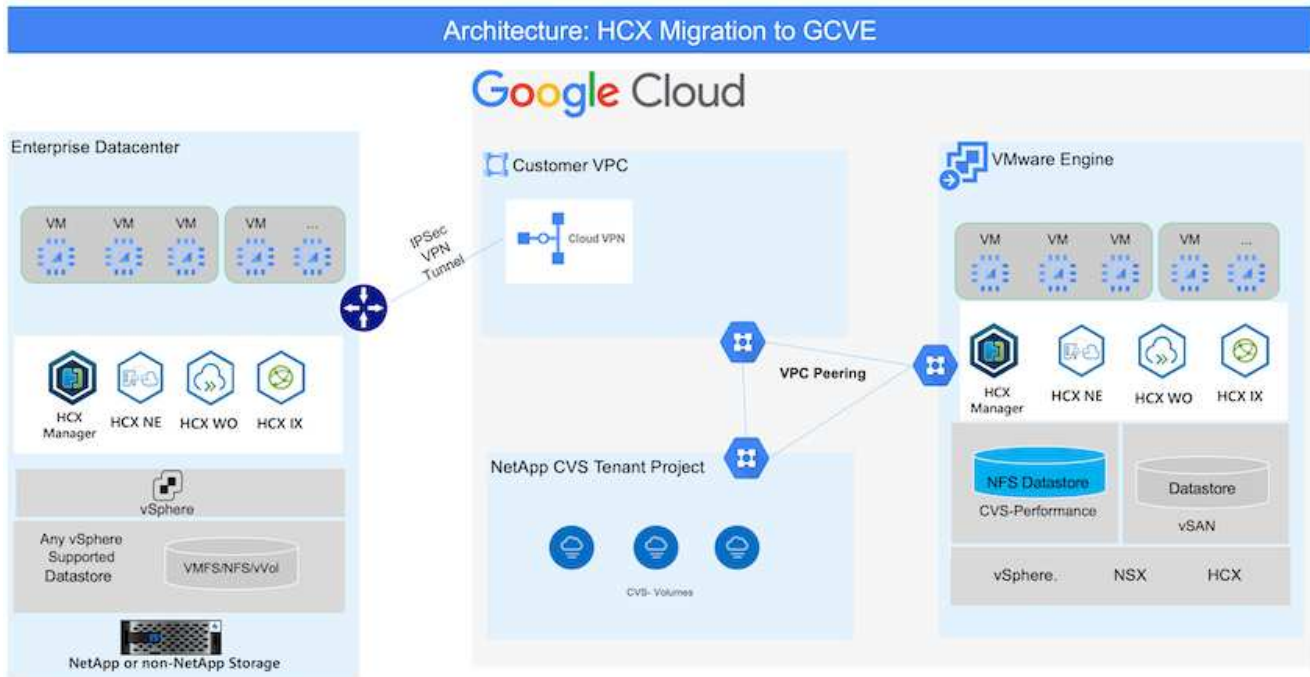


HCX Advanced è l'opzione predefinita e VMware HCX Enterprise Edition è disponibile anche attraverso un ticket di supporto e supportato senza costi aggiuntivi. Fare riferimento a. ["questo link"](#)

- Utilizza un data center software-defined (SDDC) Google Cloud VMware Engine esistente o crea un cloud privato utilizzando questo ["Link NetApp"](#) o questo ["Link di Google"](#).
- La migrazione delle macchine virtuali e dei dati associati dal data center abilitato VMware vSphere on-premise richiede la connettività di rete dal data center all'ambiente SDDC. Prima di migrare i carichi di lavoro, ["Configurare una connessione Cloud VPN o Cloud Interconnect"](#) tra l'ambiente on-premise e il rispettivo cloud privato.
- Il percorso di rete dall'ambiente VMware vCenter Server on-premise al cloud privato VMware Engine di Google Cloud deve supportare la migrazione delle macchine virtuali utilizzando vMotion.
- Assicurarsi di aver selezionato il necessario ["porte e regole del firewall"](#) Sono consentiti per il traffico vMotion tra vCenter Server on-premise e vCenter SDDC.
- Il volume NFS Cloud Volume Service deve essere montato come datastore in Google Cloud VMware Engine. Seguire i passaggi descritti in questa sezione ["collegamento"](#) Per collegare gli archivi dati Cloud Volume Service agli host Google Cloud VMware Engines.

Architettura di alto livello

A scopo di test, l'ambiente di laboratorio on-premise utilizzato per questa convalida è stato connesso tramite una VPN cloud, che consente la connettività on-premise con Google Cloud VPC.



Per uno schema più dettagliato su HCX, fare riferimento a. "[Link VMware](#)"

Implementazione della soluzione

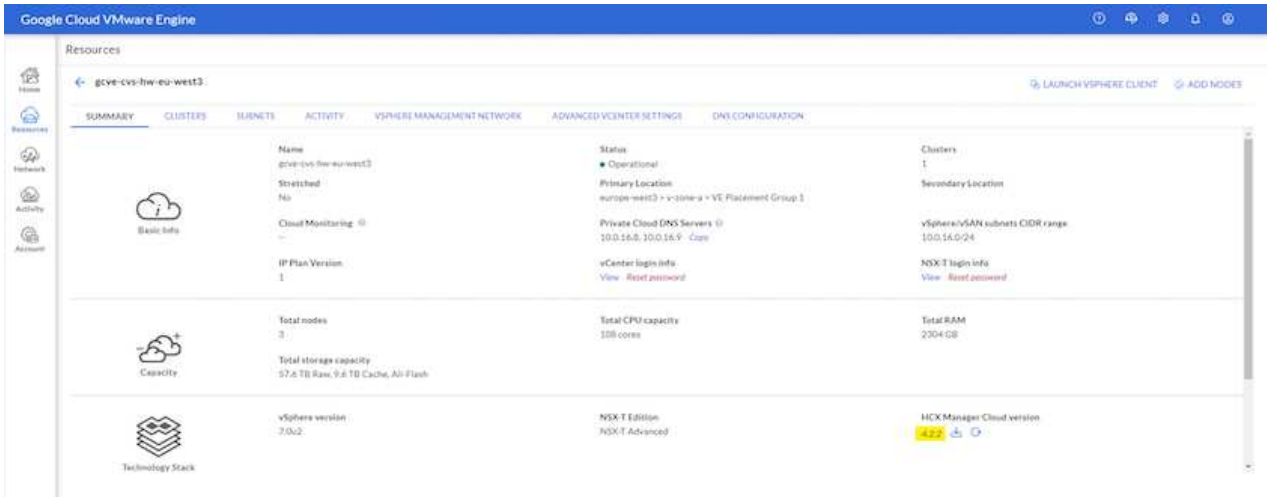
Seguire la serie di passaggi per completare l'implementazione di questa soluzione:

Fase 1: Preparazione DI HCX attraverso il portale Google VMware Engine

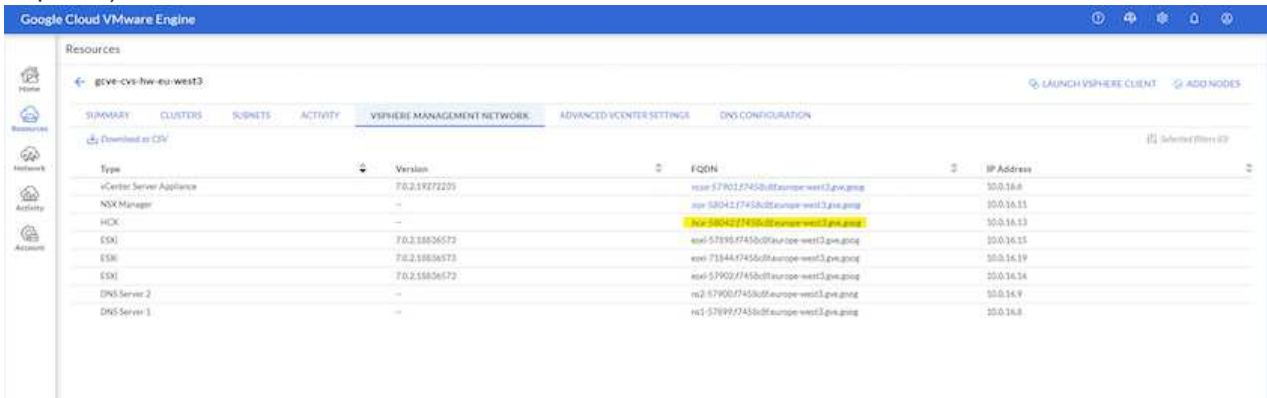
Il componente HCX Cloud Manager viene installato automaticamente durante il provisioning del cloud privato con VMware Engine. Per prepararsi all'associazione del sito, attenersi alla seguente procedura:

1. Accedi al portale Google VMware Engine e accedi A HCX Cloud Manager.

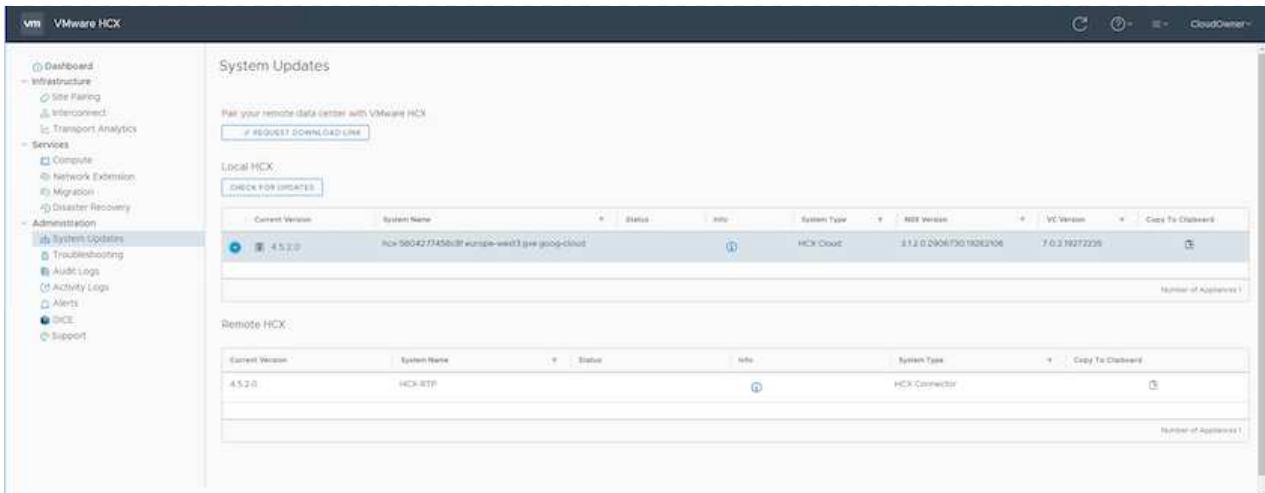
È possibile accedere ALLA console HCX facendo clic sul collegamento alla versione HCX



In alternativa, fare clic su HCX FQDN nella scheda vSphere Management Network (rete di gestione di vSphere).



2. In HCX Cloud Manager, accedere a **Administration > System Updates** (Amministrazione > aggiornamenti del sistema).
3. Fare clic su **Richiedi il download** e scaricare il file OVA.



4. Aggiornare HCX Cloud Manager alla versione più recente disponibile dall'interfaccia utente DI HCX Cloud Manager.

Fase 2: Implementazione dell'OVA del programma di installazione nel server vCenter on-premise

Affinché il connettore on-premise si connetta a HCX Manager in Google Cloud VMware Engine, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente on-premise.

Per scaricare e installare HCX Connector nel server vCenter on-premise, attenersi alla seguente procedura:

1. Fare scaricare la OVA dalla console HCX su Google Cloud VMware Engine come indicato nella fase precedente.
2. Una volta scaricato l'OVA, implementarlo nell'ambiente VMware vSphere on-premise utilizzando l'opzione **Deploy OVF Template**.

The screenshot shows the 'Deploy OVF Template' wizard in vSphere. The wizard is at step 1: 'Select an OVF template'. The left sidebar shows the steps: 1. Select an OVF template, 2. Select a name and folder, 3. Select a compute resource, 4. Review details, 5. Select storage, 6. Ready to complete. The main area shows the 'Select an OVF template' section. It says 'Select an OVF template from remote URL or local file system'. Below that, it says 'Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.' There are two radio buttons: 'URL' and 'Local file'. The 'Local file' option is selected. Below the radio buttons, there is a text input field with the URL 'http://remoteserver-address/filetoinstall.ova'. Below the text input field, there is a button labeled 'UPLOAD FILES'. Below the button, there is a text input field with the file name 'VMware-HCX-Connector-4.5.2.0-20914338.ova'. At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'.

3. Inserire tutte le informazioni richieste per l'implementazione di OVA, fare clic su **Avanti**, quindi fare clic su **fine** per implementare l'OVA di VMware HCX Connector.



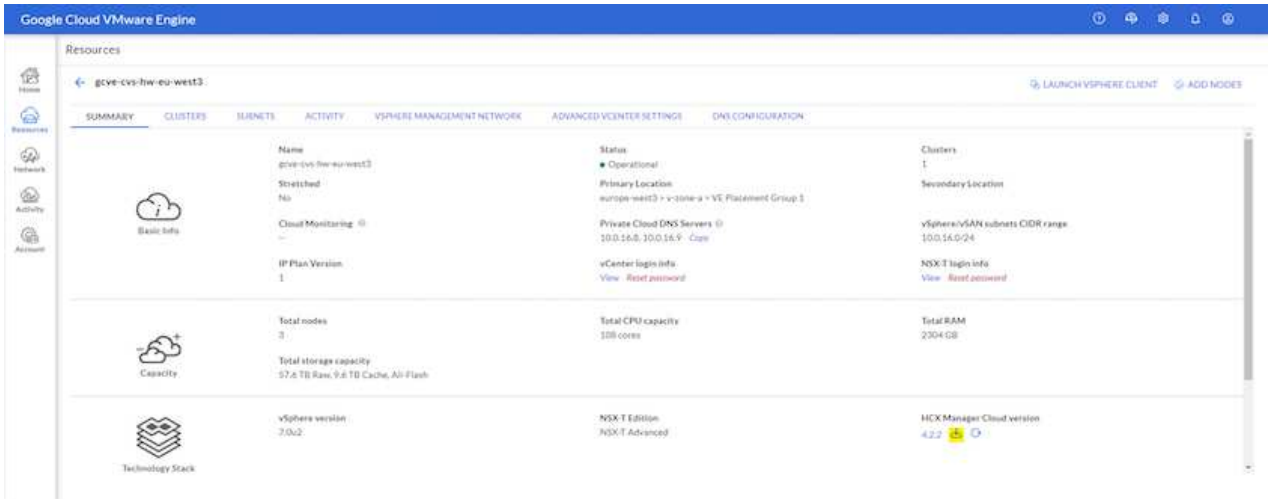
Accendere l'appliance virtuale manualmente.

Per istruzioni dettagliate, consultare ["Guida utente di VMware HCX"](#).

Fase 3: Attivare HCX Connector con la chiave di licenza

Dopo aver implementato VMware HCX Connector OVA on-premise e avviato l'appliance, completare la seguente procedura per attivare HCX Connector. Generare la chiave di licenza dal portale Google Cloud VMware Engine e attivarla in VMware HCX Manager.

1. Dal portale VMware Engine, fare clic su Resources (risorse), selezionare il cloud privato e **fare clic sull'icona di download sotto HCX Manager Cloud Version**



Aprire il file scaricato e copiare la stringa della chiave di licenza.

2. Accedere a VMware HCX Manager on-premise all'indirizzo "<https://hcxmanagerIP:9443>" utilizzando le credenziali di amministratore.



Utilizzare l'IP hcxmanagerIP e la password definiti durante l'implementazione di OVA.

3. Nella licenza, inserire la chiave copiata dal passaggio 3 e fare clic su **Activate** (attiva).



Il connettore HCX on-premise deve disporre di accesso a Internet.

4. In **posizione del data center**, fornire la posizione più vicina per l'installazione di VMware HCX Manager on-premise. Fare clic su **continua**.
5. In **Nome sistema**, aggiornare il nome e fare clic su **continua**.
6. Fare clic su **Sì, continua**.
7. In **Connect your vCenter**, fornire il nome di dominio completo (FQDN) o l'indirizzo IP di vCenter Server e le credenziali appropriate, quindi fare clic su **Continue** (continua).



Utilizzare l'FQDN per evitare problemi di connettività in un secondo momento.

8. In **Configure SSO/PSC** (Configura SSO/PSC), fornire l'indirizzo IP o il nome FQDN del Platform Services Controller (PSC) e fare clic su **Continue** (continua).



Per Embedded PSC, immettere l'indirizzo FQDN o IP di VMware vCenter Server.

9. Verificare che le informazioni immesse siano corrette e fare clic su **Restart** (Riavvia).
10. Dopo il riavvio dei servizi, vCenter Server viene visualizzato in verde nella pagina visualizzata.

VCenter Server e SSO devono disporre dei parametri di configurazione appropriati, che devono essere gli stessi della pagina precedente.



Questo processo richiede circa 10 - 20 minuti e l'aggiunta del plug-in al server vCenter.

The screenshot displays the HCX Manager interface. At the top, there's a navigation bar with tabs: vm, HCX Manager, Dashboard, Appliance Summary, Configuration, and Administration. The top right shows the IP address 172.21.254.155, Version 4.5.2.0, Type: Connector, and a user dropdown for admin.

The main content area is titled "HCX-RTP" and includes the following details:

- IP Address: 172.21.254.155
- Version: 4.5.2.0
- Uptime: 13 days, 21 hours, 6 minutes
- Current Time: Thursday, 16 February 2023 05:59:00 PM UTC

On the right side, there are three resource usage bars:

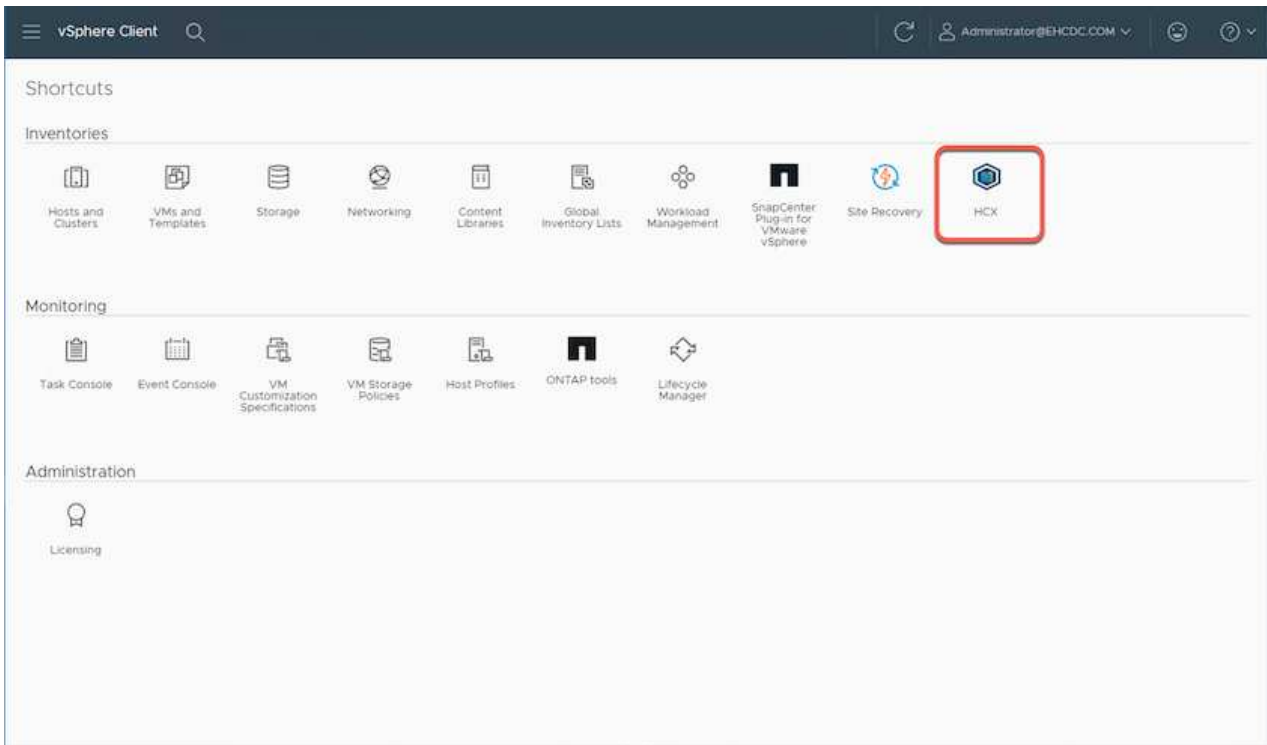
- CPU:** Free 1543 MHZ, Used 552 MHZ, Capacity 2095 MHZ, 26% used.
- Memory:** Free 2472 MB, Used 9535 MB, Capacity 12008 MB, 79% used.
- Storage:** Free 76G, Used 7.7G, Capacity 84G, 9% used.

Below these, there are three configuration cards for NSX, vCenter, and SSO, each with a "MANAGE" button. The vCenter and SSO cards show the URL `https://a300-vcso01.ehcdc.com`, which is circled in red in the original image. The vCenter card also features a green status indicator.

Fase 4: Associazione on-premise di VMware HCX Connector con Google Cloud VMware Engine HCX Cloud Manager

Una volta implementato E configurato IL connettore HCX on-premise vCenter, stabilire la connessione a Cloud Manager aggiungendo l'accoppiamento. Per configurare l'associazione del sito, attenersi alla seguente procedura:

1. Per creare una coppia di siti tra l'ambiente vCenter on-premise e Google Cloud VMware Engine SDDC, accedere a vCenter Server on-premise e al nuovo plug-in HCX vSphere Web Client.



2. In Infrastructure (infrastruttura), fare clic su **Add a Site Pairing** (Aggiungi associazione sito).



Inserire l'indirizzo IP o l'URL di Google Cloud VMware Engine HCX Cloud Manager e le credenziali per l'utente con privilegi di ruolo Cloud Owner per l'accesso al cloud privato.

Connect to Remote Site



Remote HCX URL

https://hcx-58042.f7458c8f.europe-west3.g



Username

cloudowner@gve.local



Password

.....

CANCEL

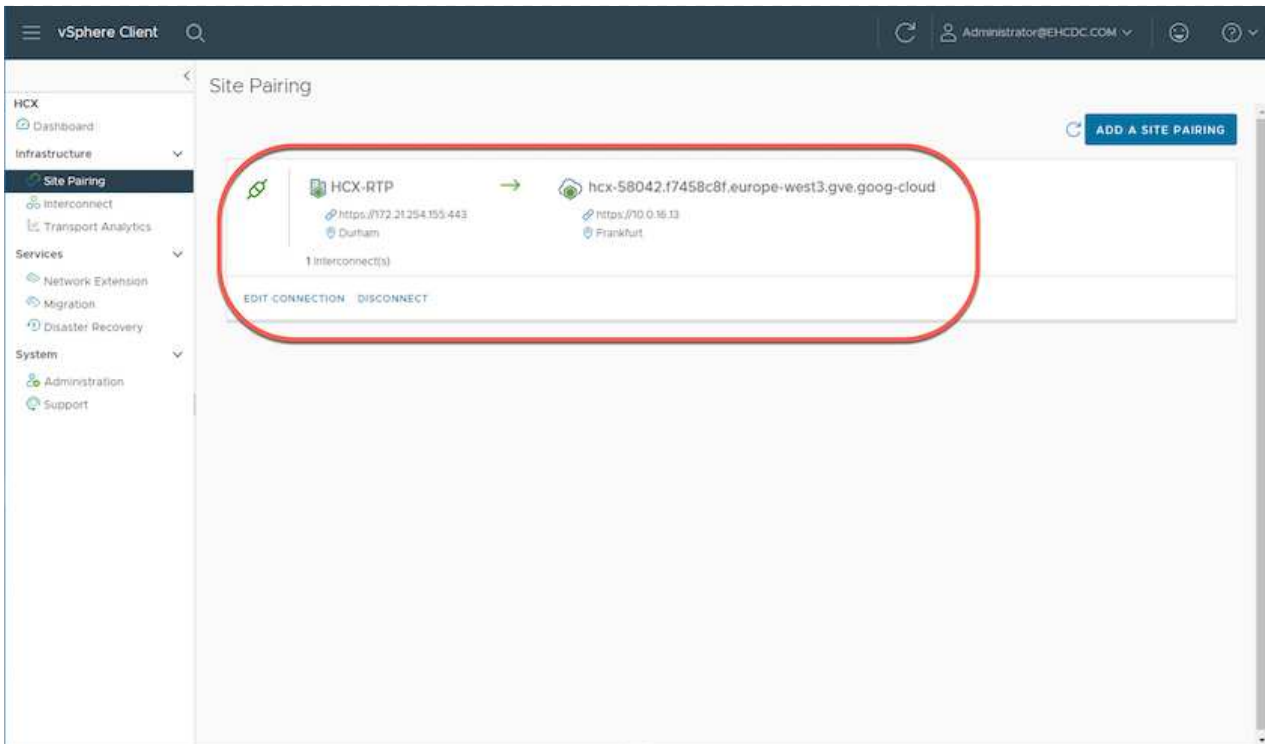
CONNECT

3. Fare clic su **Connect** (Connetti).



Il connettore VMware HCX deve essere in grado di instradare all'indirizzo IP DI HCX Cloud Manager tramite la porta 443.

4. Una volta creata l'associazione, l'associazione del sito appena configurata è disponibile nella dashboard HCX.



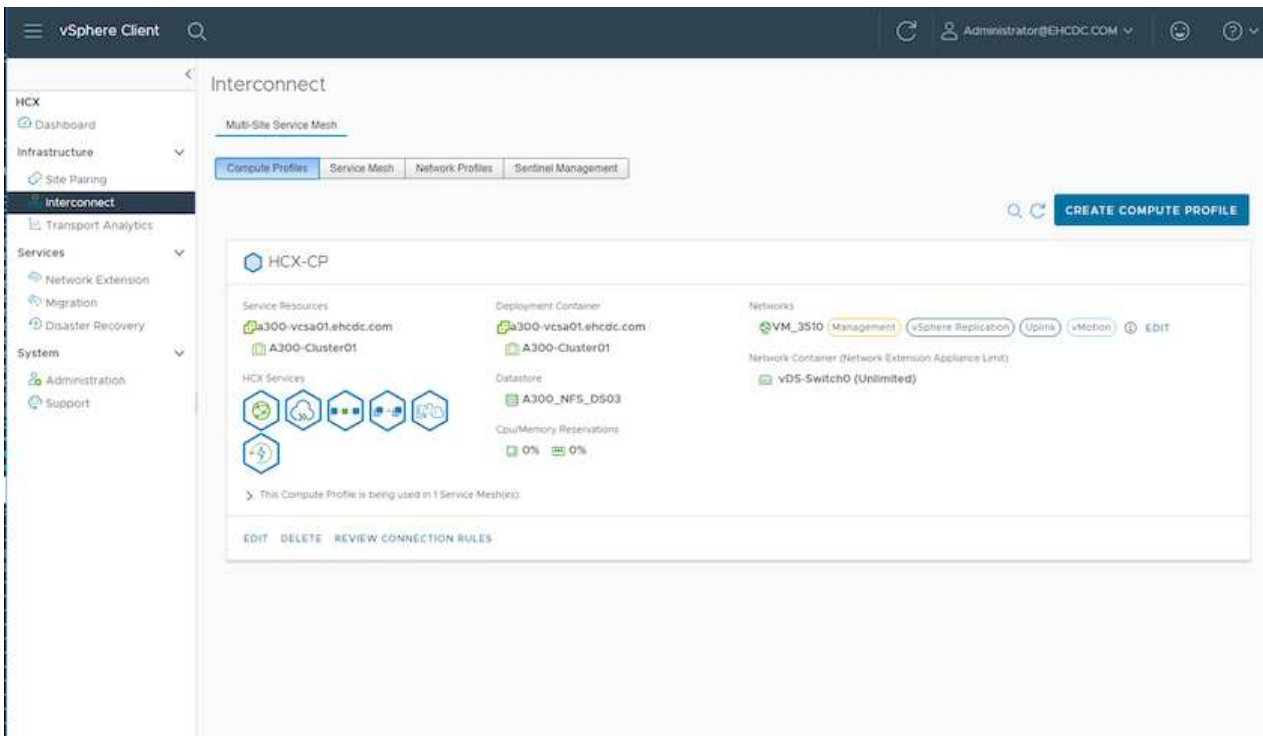
Fase 5: Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio

L'appliance di servizio VMware HCX Interconnect offre funzionalità di replica e migrazione basata su vMotion su Internet e connessioni private al sito di destinazione. L'interconnessione offre crittografia, progettazione del traffico e mobilità delle macchine virtuali. Per creare un'appliance di servizio Interconnect, attenersi alla seguente procedura:

1. In Infrastructure (infrastruttura), selezionare **Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile** (interconnessione > Mesh servizio multi-sito > profili di calcolo > Crea profilo di calcolo)



I profili di calcolo definiscono i parametri di implementazione, incluse le appliance implementate e la parte del data center VMware accessibile al servizio HCX.

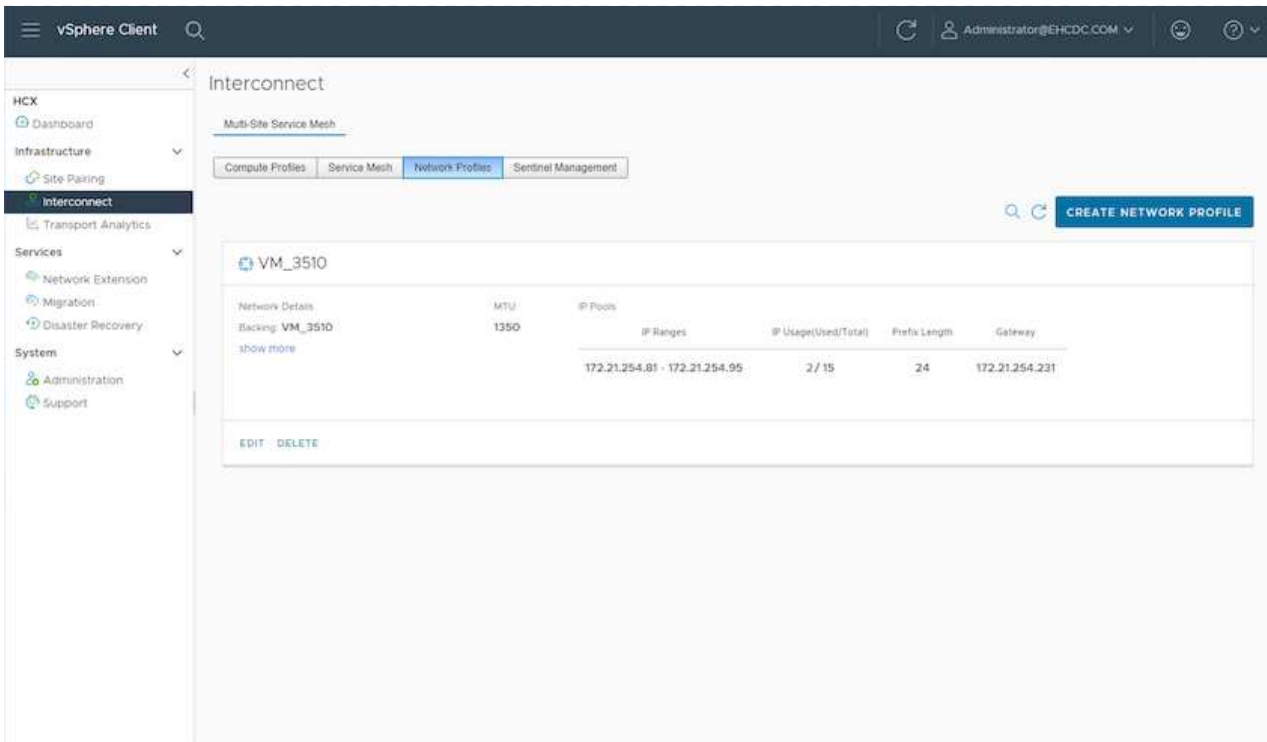


2. Una volta creato il profilo di calcolo, creare i profili di rete selezionando **Multi-Site Service Mesh > Network Profiles > Create Network Profile** (Mesh servizio multi-sito > profili di rete > Crea profilo di rete).

Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati DA HCX per le proprie appliance virtuali.



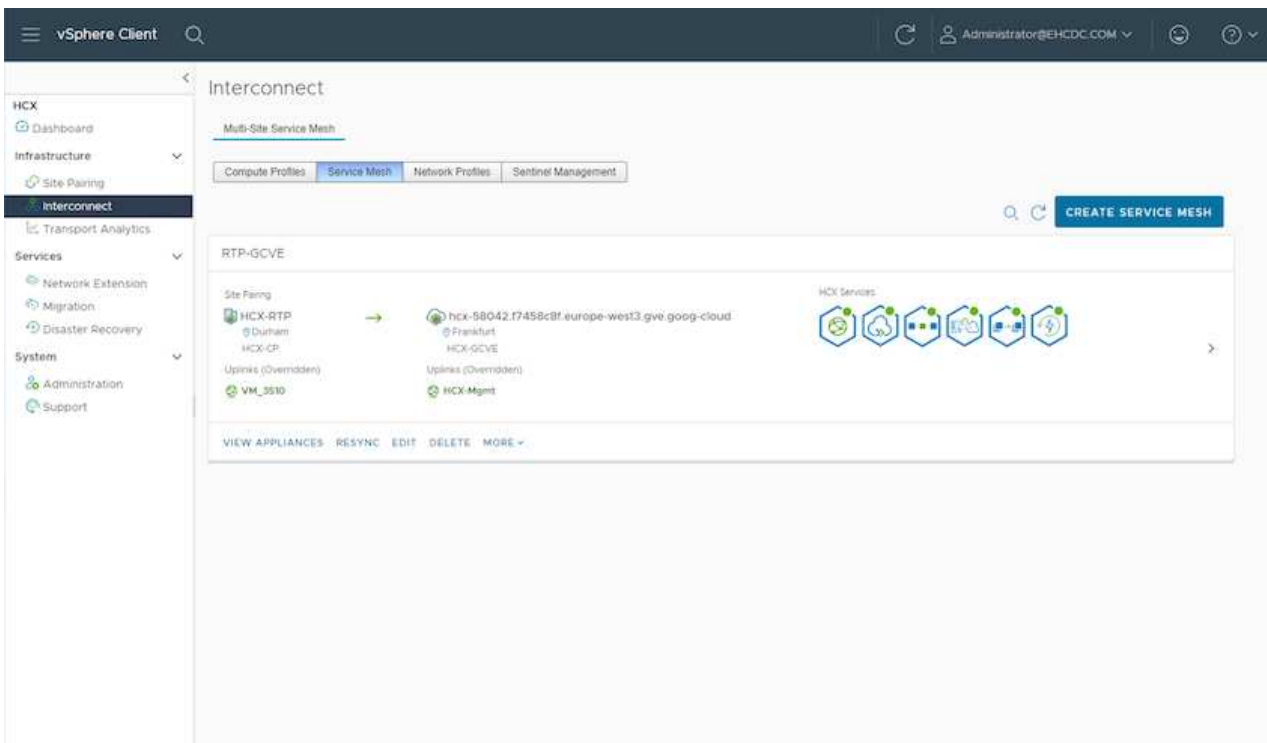
Questa operazione richiede due o più indirizzi IP. Questi indirizzi IP vengono assegnati dalla rete di gestione alle appliance di interconnessione.



3. A questo punto, i profili di calcolo e di rete sono stati creati correttamente.
4. Creare la Service Mesh selezionando la scheda **Service Mesh** all'interno dell'opzione **Interconnect** e selezionando i siti SDDC on-premise e GCVE.
5. Service Mesh specifica una coppia di profili di rete e di calcolo locale e remoto.



Nell'ambito di questo processo, le appliance HCX vengono implementate e configurate automaticamente sui siti di origine e di destinazione per creare un fabric di trasporto sicuro.



- Questa è la fase finale della configurazione. Il completamento dell'implementazione richiede circa 30 minuti. Una volta configurata la mesh del servizio, l'ambiente è pronto con i tunnel IPsec creati correttamente per migrare le macchine virtuali del carico di lavoro.

Fase 6: Migrazione dei carichi di lavoro

I carichi di lavoro possono essere migrati bidirezionalmente tra gli SDDC on-premise e GCVE utilizzando varie tecnologie di migrazione VMware HCX. Le VM possono essere spostate da e verso le entità attivate da VMware HCX utilizzando diverse tecnologie di migrazione, come LA migrazione in blocco HCX, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (disponibile con HCX Enterprise Edition) e HCX OS Assisted Migration (disponibile con HCX Enterprise Edition).

Per ulteriori informazioni sui vari meccanismi di migrazione HCX, vedere ["Tipi di migrazione VMware HCX"](#).

L'appliance HCX-IX utilizza il servizio Mobility Agent per eseguire migrazioni vMotion, Cold e Replication Assisted vMotion (RAV).



L'appliance HCX-IX aggiunge il servizio Mobility Agent come oggetto host in vCenter Server. Il processore, la memoria, lo storage e le risorse di rete visualizzati su questo oggetto non rappresentano il consumo effettivo dell'hypervisor fisico che ospita l'appliance IX.

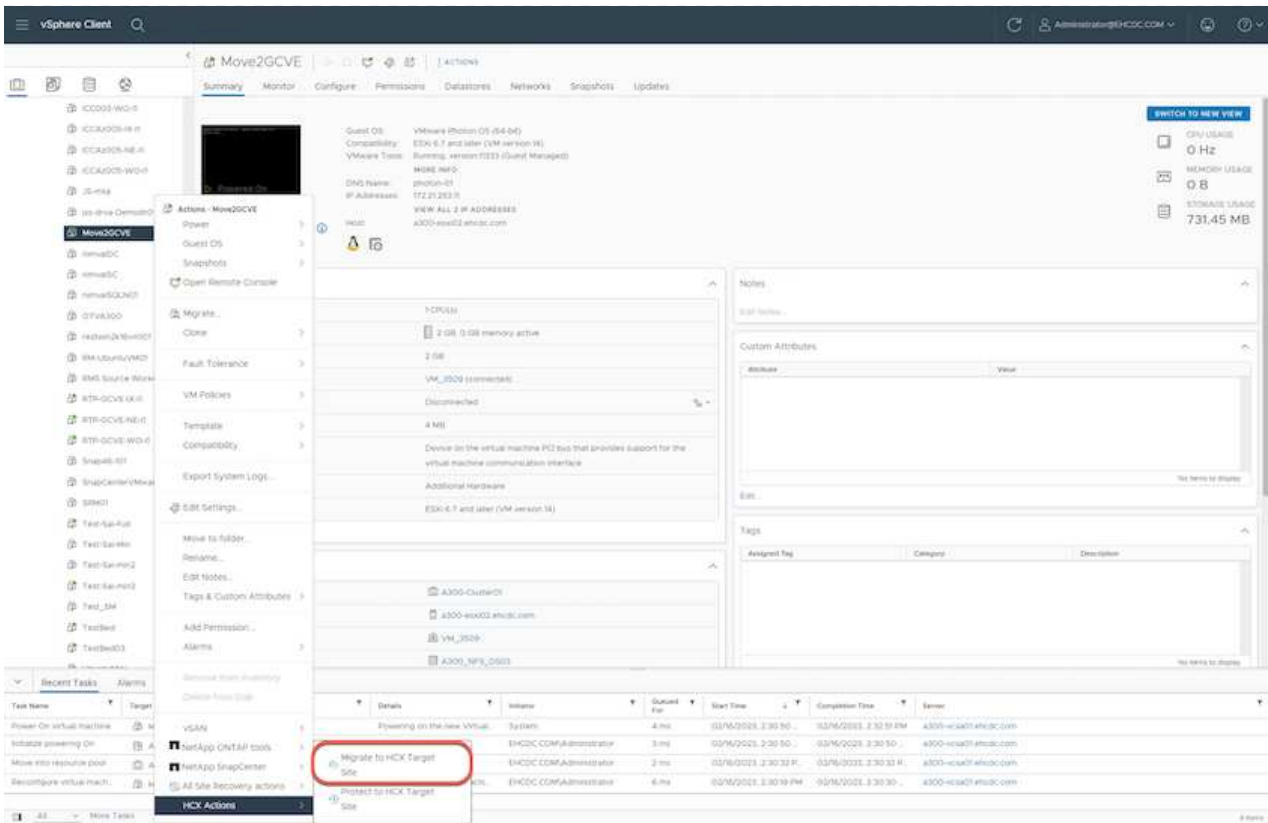
HCX vMotion

In questa sezione viene descritto il meccanismo vMotion DI HCX. Questa tecnologia di migrazione utilizza il protocollo VMware vMotion per migrare una macchina virtuale in GCVE. L'opzione di migrazione vMotion viene utilizzata per la migrazione dello stato della macchina virtuale di una singola macchina virtuale alla volta. Durante questo metodo di migrazione non si verifica alcuna interruzione del servizio.

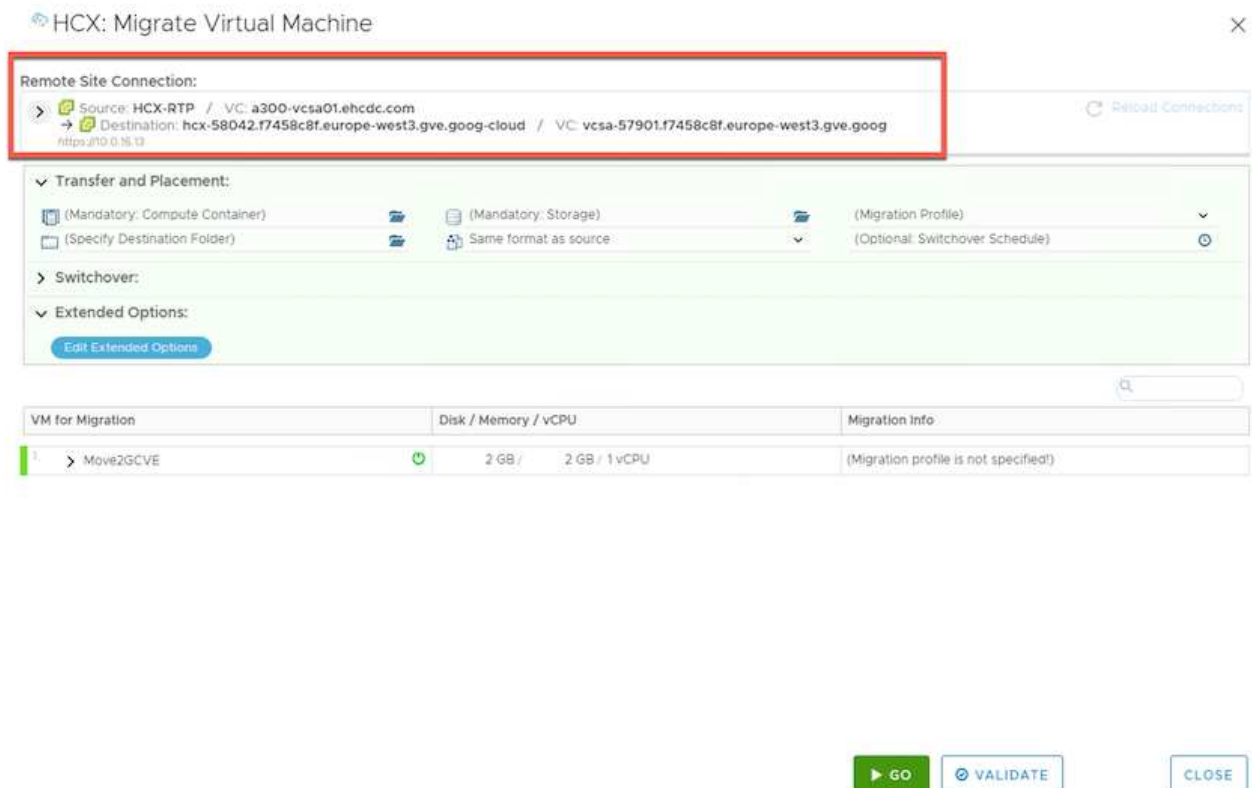


Network Extension deve essere installato (per il gruppo di porte a cui è collegata la macchina virtuale) per migrare la macchina virtuale senza dover modificare l'indirizzo IP.

1. Dal client vSphere on-premise, accedere a Inventory (inventario), fare clic con il pulsante destro del mouse sulla macchina virtuale da migrare e selezionare HCX Actions (azioni HCX) > Migrate to HCX Target Site (Migra al sito di destinazione HCX).



2. Nella procedura guidata Migrate Virtual Machine, selezionare Remote Site Connection (GCVE di destinazione).



3. Aggiornare i campi obbligatori (Cluster, Storage e Destination Network), quindi fare clic su Validate (convalida).

HCX: Migrate Virtual Machine

Remote Site Connection:

Source: HCX-RTP / VC: a300-vcsa01.ehcdc.com
 Destination: hcx-58042.f7458c8f.europe-west3.gcp.goog-cloud / VC: vcsa-57901.f7458c8f.europe-west3.gcp.goog
<https://10.0.16.13>

Transfer and Placement:

Workload: gcp-ve-4 (807.6 GB / 1 TB)
 (Specify Destination Folder): Same format as source
 vMotion (Optional: Switchover Schedule)

Switchover:

Extended Options:

Edit Extended Options

Retain MAC

VM for Migration	Disk / Memory / vCPU	Migration Info
1. Move2GCVE Workload: gcp-ve-4 (807.6 GB / 1 TB) (Specify Destination Folder): Same format as source <input type="checkbox"/> Force Power-off VM <input type="checkbox"/> Enable Seed Checkpoint Edit Extended Options Retain MAC	2 GB / 2 GB / 1 vCPU gcp-ve-4 (807.6 GB / 1 TB) Same format as source	vMotion
Network adapter 1 (VM_3509) → L2E_VM_3509-3509-a0041a8d		

GO

VALIDATE

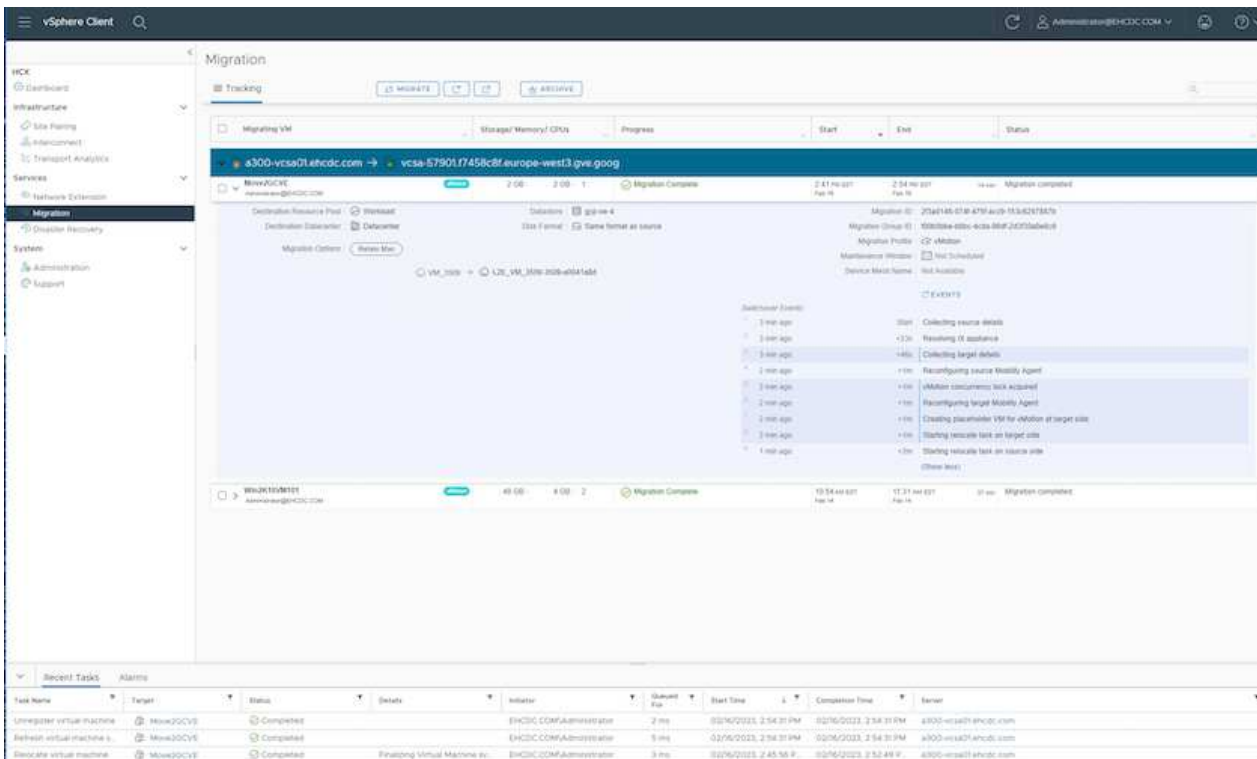
CLOSE

- Al termine dei controlli di convalida, fare clic su Go (Vai) per avviare la migrazione.



Il trasferimento vMotion acquisisce la memoria attiva della macchina virtuale, il suo stato di esecuzione, il suo indirizzo IP e il suo indirizzo MAC. Per ulteriori informazioni sui requisiti e sulle limitazioni di HCX vMotion, vedere ["Informazioni su VMware HCX vMotion e Cold Migration"](#).

- È possibile monitorare l'avanzamento e il completamento di vMotion dalla dashboard HCX > Migration (HCX > migrazione).



Il datastore NFS CVS di destinazione deve disporre di spazio sufficiente per gestire la migrazione.

Conclusione

Sia che tu stia prendendo di mira il cloud all-cloud o ibrido e i dati che risiedono su storage di qualsiasi tipo/vendor in on-premise, Cloud Volume Service e HCX offrono eccellenti opzioni per implementare e migrare i carichi di lavoro delle applicazioni, riducendo al contempo il TCO rendendo i requisiti dei dati perfetti per il livello applicativo. Qualunque sia il caso d'utilizzo, scegli Google Cloud VMware Engine insieme a Cloud Volume Service per una rapida realizzazione dei vantaggi del cloud, un'infrastruttura coerente e operazioni su cloud multipli e on-premise, portabilità bidirezionale dei carichi di lavoro e capacità e performance di livello Enterprise. Si tratta degli stessi processi e procedure familiari utilizzati per connettere lo storage e migrare le macchine virtuali utilizzando VMware vSphere Replication, VMware vMotion o persino la copia del file di rete (NFC).

Punti da asporto

I punti chiave di questo documento includono:

- Ora puoi utilizzare Cloud Volume Service come datastore su Google Cloud VMware Engine SDDC.
- È possibile migrare facilmente i dati dall'archivio dati on-premise a Cloud Volume Service.
- È possibile espandere e ridurre facilmente il datastore Cloud Volume Service per soddisfare i requisiti di capacità e performance durante l'attività di migrazione.

Video di Google e VMware come riferimento

Da Google

- ["Implementare HCX Connector con GCVE"](#)
- ["Configurare HCX ServiceMesh con GCVE"](#)
- ["Migrare VM con HCX in GCVE"](#)

Di VMware

- ["Implementazione DI HCX Connector per GCVE"](#)
- ["Configurazione HCX ServiceMesh per GCVE"](#)
- ["Migrazione del carico di lavoro HCX in GCVE"](#)

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, fare riferimento ai seguenti collegamenti Web:

- Documentazione di Google Cloud VMware Engine
["https://cloud.google.com/vmware-engine/docs/overview"](https://cloud.google.com/vmware-engine/docs/overview)
- Documentazione Cloud Volume Service
["https://cloud.google.com/architecture/partners/netapp-cloud-volumes"](https://cloud.google.com/architecture/partners/netapp-cloud-volumes)
- Guida utente di VMware HCX
["https://docs.vmware.com/en/VMware-HCX/index.html"](https://docs.vmware.com/en/VMware-HCX/index.html)

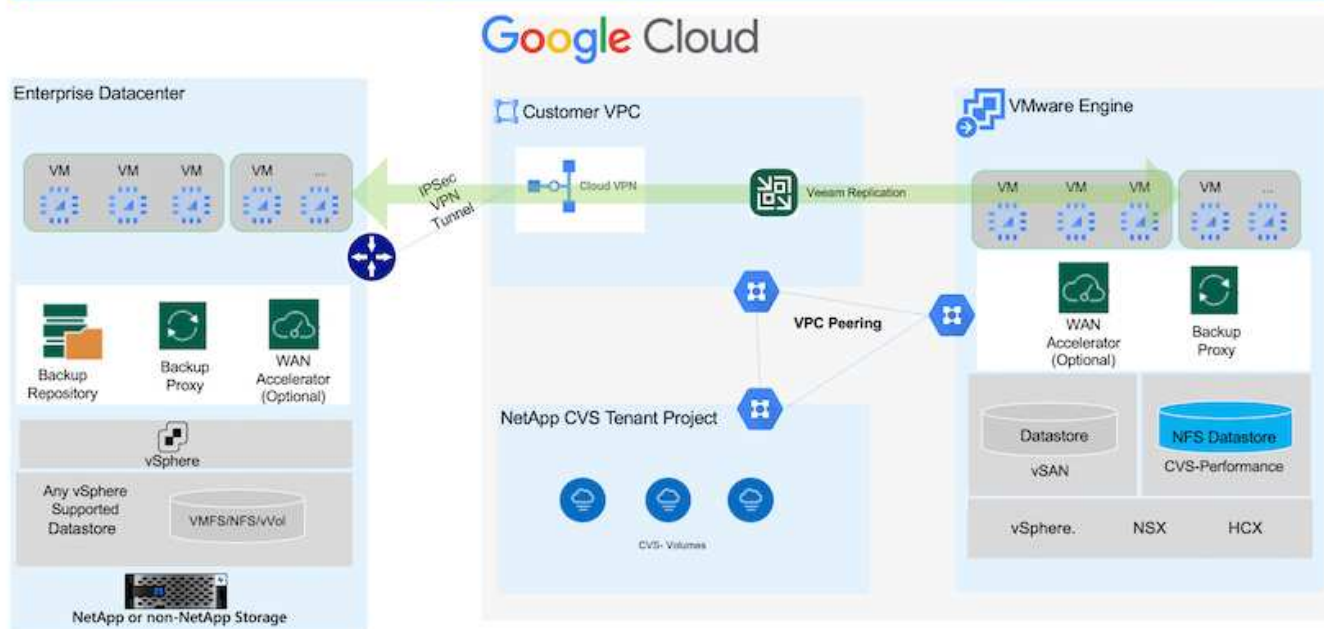
Migrazione delle macchine virtuali al servizio volumi cloud NetApp Datastore NFS su Google Cloud VMware Engine con la funzione di replica Veeam

Panoramica

Autori: Suresh Thoppay, NetApp

I carichi di lavoro delle macchine virtuali eseguiti su VMware vSphere possono essere migrati a Google Cloud VMware Engine (GCVE) utilizzando la funzione di replica Veeam.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione della migrazione delle macchine virtuali che utilizza il servizio volumi cloud di NetApp, Veeam e il motore VMware di Google Cloud (GCVE).



Presupposti

Il presente documento presuppone che l'utente disponga di Google Cloud VPN o Cloud Interconnect o di un'altra opzione di rete per stabilire la connettività di rete dai server vSphere esistenti a Google Cloud VMware Engine.



Esistono diverse opzioni per connettere i data center on-premise a Google Cloud, che ci impediscono di delineare un workflow specifico in questo documento. Fare riferimento a. ["Documentazione di Google Cloud"](#) Per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione di migrazione

Panoramica sull'implementazione della soluzione

1. Assicurarsi che il datastore NFS dal servizio volumi cloud di NetApp sia montato su GCVE vCenter.
2. Assicurarsi che Veeam Backup Recovery sia implementato nell'ambiente VMware vSphere esistente
3. Crea processo di replica per avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Eseguire il failover del processo di replica Veeam.
5. Eseguire il failover permanente su Veeam.

Dettagli sull'implementazione

Assicurarsi che il datastore NFS dal servizio volumi cloud di NetApp sia montato su GCVE vCenter

Accedere a GCVE vCenter e assicurarsi che sia disponibile un datastore NFS con spazio sufficiente. In caso contrario, fare riferimento a. ["Montare NetApp CVS come datastore NFS su GCVE"](#)

Assicurarsi che Veeam Backup Recovery sia implementato nell'ambiente VMware vSphere esistente

Fare riferimento a. ["Componenti di replica Veeam"](#) documentazione per l'installazione dei componenti richiesti.

Crea processo di replica per avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.

VCenter on-premise e gCVE vCenter devono essere registrati con Veeam. ["Processo di replica di vSphere VM"](#)

Ecco un video che spiega come
["Configurazione del processo di replica"](#).



La replica VM può avere un IP diverso dalla VM di origine e può anche essere collegata a un gruppo di porte diverso. Per ulteriori dettagli, consulta il video qui sopra.

Eseguire il failover del processo di replica Veeam

Per migrare le macchine virtuali, eseguire ["Eseguire il failover"](#)

Eseguire il failover permanente su Veeam.

Per trattare GCVE come nuovo ambiente di origine, eseguire ["Failover permanente"](#)

Vantaggi di questa soluzione

- L'infrastruttura di backup Veeam esistente può essere utilizzata per la migrazione.
- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito di destinazione.
- È in grado di rimappare i dati esistenti replicati al di fuori di Veeam (come i dati replicati da BlueXP)
- È in grado di specificare diversi portgroup di rete sul sito di destinazione.
- Può specificare l'ordine di accensione delle macchine virtuali.
- Utilizza VMware Change Block Tracking per ridurre al minimo la quantità di dati da inviare attraverso la WAN.
- Capacità di eseguire script pre e post per la replica.
- Capacità di eseguire script pre e post per le snapshot.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.