Cloud pubblico e ibrido

NetApp Solutions

NetApp
May 10, 2024

Sommario

Cloud pubblico e ibrido

Multicloud ibrido NetApp con soluzioni VMware

VMware per il cloud pubblico

Panoramica del multicloud ibrido NetApp con VMware

La maggior parte delle organizzazioni IT segue l'approccio ibrido cloud-first. Queste organizzazioni sono in fase di trasformazione e i clienti stanno valutando il loro attuale panorama IT e quindi migrando i workload nel cloud in base all'esercizio di valutazione e scoperta.

I fattori per i clienti che migrano al cloud possono includere flessibilità e burst, uscita dal data center, consolidamento del data center, scenari di fine ciclo di vita, fusioni, acquisizioni e così via. Il motivo di questa migrazione può variare in base a ciascuna organizzazione e alle rispettive priorità di business. Durante il passaggio al cloud ibrido, la scelta dello storage giusto nel cloud è molto importante per liberare la potenza dell'implementazione e dell'elasticità del cloud.

Opzioni di VMware Cloud nel cloud pubblico

In questa sezione viene descritto il modo in cui ciascun provider cloud supporta uno stack VMware Software Defined Data Center (SDDC) e/o VMware Cloud Foundation (VCF) all'interno delle rispettive offerte di cloud pubblico.

Soluzione VMware Azure

Azure VMware Solution è un servizio di cloud ibrido che consente il funzionamento completo degli SDDC VMware nel cloud pubblico Microsoft Azure. Azure VMware Solution è una soluzione di prima parte completamente gestita e supportata da Microsoft, verificata da VMware sfruttando l'infrastruttura Azure. Ciò significa che quando Azure VMware Solution viene implementata, i clienti ottengono VMware ESXi per la virtualizzazione del calcolo, vSAN per lo storage iperconvergente, E NSX per il networking e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture di data center leader di settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure native.

VMware Cloud su AWS

VMware Cloud su AWS porta il software SDDC di livello Enterprise di VMware su AWS Cloud con accesso ottimizzato ai servizi AWS nativi. Basato su VMware Cloud Foundation, VMware Cloud su AWS integra i prodotti di calcolo, storage e virtualizzazione di rete di VMware (VMware vSphere, VMware vSAN e VMware NSX) insieme alla gestione di VMware vCenter Server, ottimizzata per l'esecuzione su un'infrastruttura AWS bare-metal flessibile e dedicata.

Motore VMware Google Cloud

Google Cloud VMware Engine è un'offerta Infrastructure-as-a-service (IaaS) basata sull'infrastruttura scalabile e dalle performance elevate di Google Cloud e sullo stack VMware Cloud Foundation: VMware vSphere, vCenter, vSAN e NSX-T. Questo servizio consente un percorso rapido verso il cloud, migrando o estendendo senza problemi i workload VMware esistenti dagli ambienti on-premise alla piattaforma Google Cloud senza i costi, gli sforzi o il rischio di riprogettare le applicazioni o di riorganizzare le operazioni. Si tratta di un servizio venduto e supportato da Google, che lavora a stretto contatto con VMware.

Il cloud privato SDDC e la co-locazione dei volumi cloud NetApp offrono le migliori performance con una latenza di rete minima.

Lo sapevi?

Indipendentemente dal cloud utilizzato, quando viene implementato un VMware SDDC, il cluster iniziale include i seguenti prodotti:

- VMware ESXi ospita la virtualizzazione di calcolo con un'appliance vCenter Server per la gestione
- Storage iperconvergente VMware vSAN che incorpora le risorse di storage fisico di ciascun host ESXi
- VMware NSX per reti virtuali e sicurezza con cluster NSX Manager per la gestione

Configurazione dello storage

Per i clienti che intendono ospitare carichi di lavoro a uso intensivo di storage e scalare su qualsiasi soluzione VMware ospitata nel cloud, l'infrastruttura iperconvergente predefinita impone che l'espansione debba essere sulle risorse di calcolo e storage.

Grazie all'integrazione con NetApp Cloud Volumes, come Azure NetApp Files, Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP (disponibile in tutti e tre gli hyperscaler principali) e Cloud Volumes Service per Google Cloud, i clienti ora hanno la possibilità di scalare in modo indipendente lo storage separatamente, E aggiungere nodi di calcolo al cluster SDDC solo se necessario.

Note:

- VMware non consiglia configurazioni di cluster sbilanciate, pertanto l'espansione dello storage implica l'aggiunta di più host, il che implica un TCO maggiore.
- È possibile utilizzare un solo ambiente vSAN. Pertanto, tutto il traffico dello storage sarà direttamente in concorrenza con i carichi di lavoro di produzione.
- Non è possibile fornire più livelli di performance per allineare requisiti, performance e costi delle applicazioni.
- È molto semplice raggiungere i limiti di capacità dello storage di vSAN costruito sugli host del cluster. Utilizza NetApp Cloud Volumes per scalare lo storage in modo da ospitare set di dati attivi o dati Tier-cooler in storage persistente.

Azure NetApp Files, Amazon FSX per NetApp ONTAP, Cloud Volumes ONTAP (disponibile in tutti e tre i principali hyperscaler) e Cloud Volumes Service per Google Cloud possono essere utilizzati insieme alle macchine virtuali guest. Questa architettura di storage ibrido è costituita da un datastore vSAN che contiene i dati binari del sistema operativo guest e dell'applicazione. I dati dell'applicazione vengono collegati alla

macchina virtuale tramite un iniziatore iSCSI basato su guest o i supporti NFS/SMB che comunicano direttamente con Amazon FSX per NetApp ONTAP, Cloud Volume ONTAP, Azure NetApp Files e Cloud Volumes Service per Google Cloud rispettivamente. Questa configurazione consente di superare facilmente le sfide con la capacità dello storage, come con vSAN, lo spazio libero disponibile dipende dallo spazio a vuoto e dalle policy di storage utilizzate.

Prendiamo in considerazione un cluster SDDC a tre nodi su VMware Cloud su AWS:

- Capacità raw totale per un SDDC a tre nodi = 31,1 TB (circa 10 TB per ogni nodo).
- Lo spazio a vuoto da mantenere prima dell'aggiunta di host aggiuntivi = 25% = (0,25 x 31,1 TB) = 7,7 TB.
- La capacità raw utilizzabile dopo la deduzione dello spazio a vuoto = 23,4 TB
- Lo spazio libero effettivo disponibile dipende dalla policy di storage applicata.

  Ad esempio:

  - RAID 0 = spazio libero effettivo = 23,4 TB (capacità raw utilizzabile/1)
  - RAID 1 = spazio libero effettivo = 11,7 TB (capacità raw utilizzabile/2)
  - RAID 5 = spazio libero effettivo = 17,5 TB (capacità raw utilizzabile/1.33)

Pertanto, l'utilizzo di NetApp Cloud Volumes come storage connesso agli ospiti contribuirebbe ad espandere lo storage e ottimizzare il TCO, soddisfacendo al contempo i requisiti di performance e protezione dei dati.

> Lo storage in-guest era l'unica opzione disponibile al momento della stesura del presente documento. Non appena sarà disponibile il supporto supplementare per datastore NFS, sarà disponibile ulteriore documentazione "qui".

Punti da ricordare

- Nei modelli di storage ibrido, posizionare i carichi di lavoro di livello 1 o ad alta priorità sul datastore vSAN per soddisfare qualsiasi requisito di latenza specifico, poiché fanno parte dell'host stesso e si trovano nelle vicinanze. Utilizzare meccanismi in-guest per qualsiasi workload VM per cui le latenze transazionali sono accettabili.
- Utilizza la tecnologia NetApp SnapMirror® per replicare i dati del carico di lavoro dal sistema ONTAP on-premise a Cloud Volumes ONTAP o Amazon FSX per NetApp ONTAP per semplificare la migrazione utilizzando meccanismi a livello di blocco. Ciò non si applica a Azure NetApp Files e ai servizi Cloud Volumes. Per la migrazione dei dati su Azure NetApp Files o Cloud Volumes Services, utilizza NetApp XCP, la copia e sincronizzazione di BlueXP, rysnc o robocopy, a seconda del protocollo del file utilizzato.
- I test mostrano una latenza aggiuntiva di 2-4 ms durante l'accesso allo storage dai rispettivi SDDC. Considerare questa latenza aggiuntiva nei requisiti dell'applicazione quando si esegue la mappatura dello storage.
- Per il montaggio dello storage connesso agli ospiti durante il failover di test e il failover effettivo, assicurarsi che gli iniziatori iSCSI siano riconfigurati, che il DNS sia aggiornato per le condivisioni SMB e che i punti di montaggio NFS siano aggiornati in fstab.
- Assicurarsi che le impostazioni del Registro di sistema di i/o multipath Microsoft (MPIO), firewall e timeout del disco in-guest siano configurate correttamente all'interno della macchina virtuale.

> Questo vale solo per lo storage connesso guest.

Vantaggi dello storage cloud NetApp

Lo storage cloud di NetApp offre i seguenti vantaggi:

- Migliora la densità di calcolo-storage scalando lo storage indipendentemente dal calcolo.
- Consente di ridurre il numero di host, riducendo così il TCO complessivo.
- Il guasto del nodo di calcolo non influisce sulle prestazioni dello storage.
- La risagomatura dei volumi e la funzionalità dinamica a livello di servizio di Azure NetApp Files consentono di ottimizzare i costi dimensionando i carichi di lavoro a stato stazionario e impedendo in tal modo l'over provisioning.
- Le efficienze dello storage, il tiering del cloud e le funzionalità di modifica del tipo di istanza di Cloud Volumes ONTAP consentono di aggiungere e scalare lo storage in modo ottimale.
- Impedisce l'overprovisioning delle risorse di storage vengono aggiunte solo quando necessario.
- Copie Snapshot e cloni efficienti consentono di creare rapidamente copie senza alcun impatto sulle performance.
- Aiuta a risolvere gli attacchi ransomware utilizzando il ripristino rapido dalle copie Snapshot.
- Offre un disaster recovery regionale basato su trasferimento incrementale dei blocchi efficiente e un livello di blocchi di backup integrato nelle varie regioni per offrire RPO e RTO migliori.

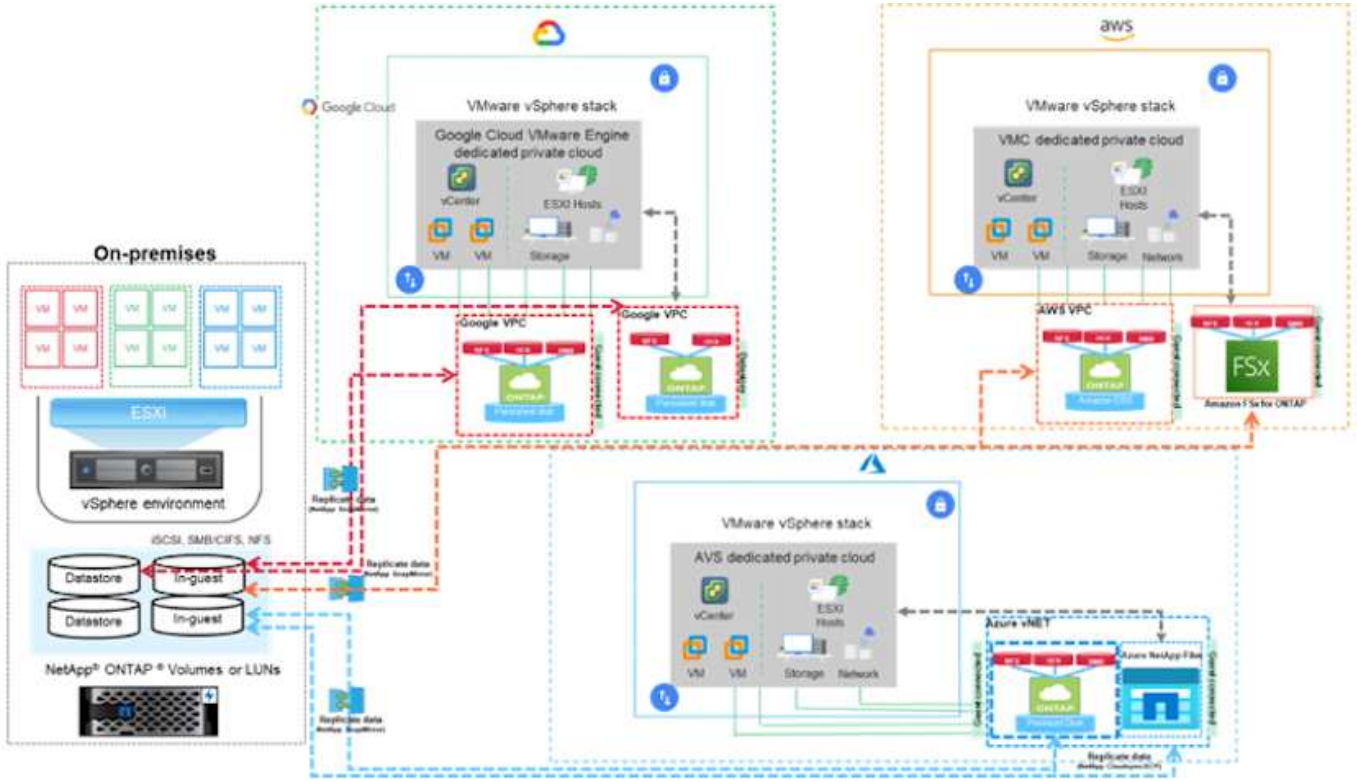
Presupposti

- La tecnologia SnapMirror o altri meccanismi di migrazione dei dati rilevanti sono abilitati. Esistono molte opzioni di connettività, da on-premise a qualsiasi cloud hyperscaler. Utilizzare il percorso appropriato e collaborare con i team di rete interessati.
- Lo storage in-guest era l'unica opzione disponibile al momento della stesura del presente documento. Non appena sarà disponibile il supporto supplementare per datastore NFS, sarà disponibile ulteriore documentazione "qui".

> Coinvolgi i Solution Architect di NetApp e i rispettivi cloud architect hyperscaler per la pianificazione e il dimensionamento dello storage e il numero richiesto di host. NetApp consiglia di identificare i requisiti di performance dello storage prima di utilizzare Cloud Volumes ONTAP Sizer per finalizzare il tipo di istanza dello storage o il livello di servizio appropriato con il throughput corretto.

Architettura dettagliata

Da un punto di vista di alto livello, questa architettura (illustrata nella figura seguente) illustra come ottenere connettività multicloud ibrida e portabilità delle applicazioni tra più cloud provider utilizzando NetApp Cloud Volumes ONTAP, Cloud Volumes Service per Google Cloud e Azure NetApp Files come opzione aggiuntiva di storage in-guest.



Soluzioni NetApp per VMware negli hyperscaler

Scopri di più sulle funzionalità offerte da NetApp ai tre (3) hyperscaler principali: Da NetApp come dispositivo di storage connesso come guest o come datastore NFS supplementare alla migrazione dei flussi di lavoro, all'estensione/diffusione nel cloud, al backup/ripristino e al disaster recovery.

Scegli il tuo cloud e lascia che NetApp faccia il resto!

Per visualizzare le funzionalità di un hyperscaler specifico, fare clic sulla scheda appropriata per tale hyperscaler.

Passare alla sezione relativa al contenuto desiderato selezionando una delle seguenti opzioni:

- "VMware nella configurazione degli hyperscaler"

- "Opzioni di storage NetApp"
- "Soluzioni cloud NetApp/VMware"

VMware nella configurazione degli hyperscaler

Come per i sistemi on-premise, la pianificazione di un ambiente di virtualizzazione basato sul cloud è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

AWS/VMC

Questa sezione descrive come configurare e gestire VMware Cloud su AWS SDDC e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad AWS VMC.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementazione e configurazione di VMware Cloud per AWS
- Connetti VMware Cloud a FSX ONTAP

Visualizza i dettagli "Procedura di configurazione per VMC".

Azure/AVS

Questa sezione descrive come configurare e gestire Azure VMware Solution e utilizzarla in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP alla soluzione VMware Azure.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Registrare il provider di risorse e creare un cloud privato
- Connettersi a un gateway di rete virtuale ExpressRoute nuovo o esistente
- Convalidare la connettività di rete e accedere al cloud privato

Visualizza i dettagli "Procedura di configurazione per AVS".

GCP/GCVE

Questa sezione descrive come configurare e gestire GCVE e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP e Cloud Volumes Services a GCVE.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementare e configurare GCVE
- Attiva accesso privato a GCVE

Visualizza i dettagli "Procedura di configurazione per GCVE".

Opzioni di storage NetApp

Lo storage NetApp può essere utilizzato in diversi modi, come guest connesso o come datastore NFS supplementare, all'interno di ciascuno dei 3 principali hyperscaler.

Visitare il sito "Opzioni di storage NetApp supportate" per ulteriori informazioni.

AWS/VMC

AWS supporta lo storage NetApp nelle seguenti configurazioni:

- FSX ONTAP come storage connesso guest
- Cloud Volumes ONTAP (CVO) come storage connesso guest
- FSX ONTAP come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per VMC". Visualizza i dettagli "Opzioni aggiuntive del datastore NFS per VMC".

Azure/AVS

Azure supporta lo storage NetApp nelle seguenti configurazioni:

- Azure NetApp Files (ANF) come storage connesso guest
- Cloud Volumes ONTAP (CVO) come storage connesso guest
- Azure NetApp Files (ANF) come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per AVS". Visualizza i dettagli "Opzioni aggiuntive del datastore NFS per AVS".

GCP/GCVE

Google Cloud supporta lo storage NetApp nelle seguenti configurazioni:

- Cloud Volumes ONTAP (CVO) come storage connesso guest
- Cloud Volumes Service (CVS) come storage connesso al guest
- Cloud Volumes Service (CVS) come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per GCVE".

Scopri di più "Supporto del datastore NetApp Cloud Volumes Service per il motore VMware di Google Cloud (blog NetApp)" oppure "Come utilizzare NetApp CVS come datastore per Google Cloud VMware Engine (Google blog)"

Soluzioni cloud NetApp/VMware

Con le soluzioni cloud NetApp e VMware, molti casi di utilizzo sono semplici da implementare nell'hyperscaler scelto. VMware definisce i casi di utilizzo del carico di lavoro del cloud primario come:

- Protect (include disaster recovery e backup/ripristino)
- Migrare
- Estendi

AWS/VMC

"Esplora le soluzioni NetApp per AWS/VMC"

Azure/AVS

"Esplora le soluzioni NetApp per Azure / AVS"

GCP/GCVE

"Esplora le soluzioni NetApp per Google Cloud Platform (GCP) / GCVE"

Configurazioni supportate per NetApp Hybrid Multibloud con VMware

Comprendere le combinazioni per il supporto dello storage NetApp nei principali hyperscaler.

	Guest connesso	Database NFS supplementare
AWS	ONTAP CVO FSX"Dettagli"	ONTAP FSX"Dettagli"
Azure	ANF. CVO"Dettagli"	AN"Dettagli"
GCP	CVO CVS"Dettagli"	CVS"Dettagli"

Configurazione dell'ambiente di virtualizzazione nel cloud provider

I dettagli su come configurare l'ambiente di virtualizzazione in ciascuno degli hyperscaler supportati sono illustrati qui.

AWS/VMC

Questa sezione descrive come configurare e gestire VMware Cloud su AWS SDDC e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad AWS VMC.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementazione e configurazione di VMware Cloud per AWS
- Connetti VMware Cloud a FSX ONTAP

Visualizza i dettagli "Procedura di configurazione per VMC".

Azure/AVS

Questa sezione descrive come configurare e gestire Azure VMware Solution e utilizzarla in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP alla soluzione VMware Azure.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Registrare il provider di risorse e creare un cloud privato
- Connettersi a un gateway di rete virtuale ExpressRoute nuovo o esistente
- Convalidare la connettività di rete e accedere al cloud privato

Visualizza i dettagli "Procedura di configurazione per AVS".

GCP/GCVE

Questa sezione descrive come configurare e gestire GCVE e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP e Cloud Volumes Services a GCVE.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementare e configurare GCVE
- Attiva accesso privato a GCVE

Visualizza i dettagli "Procedura di configurazione per GCVE".

Implementare e configurare l'ambiente di virtualizzazione su AWS

Come per i servizi on-premise, la pianificazione di VMware Cloud su AWS è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire VMware Cloud su AWS SDDC e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è attualmente l'unico metodo supportato per connettere Cloud Volumes ONTAP (CVO) ad AWS VMC.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Implementare e configurare VMware Cloud per AWS

"VMware Cloud su AWS" Offre un'esperienza nativa nel cloud per i carichi di lavoro basati su VMware nell'ecosistema AWS. Ogni VMware Software-Defined Data Center (SDDC) viene eseguito in un Amazon Virtual Private Cloud (VPC) e fornisce uno stack VMware completo (incluso vCenter Server), networking software-defined NSX-T, storage vSAN software-defined e uno o più host ESXi che forniscono risorse di calcolo e storage ai carichi di lavoro.

Questa sezione descrive come configurare e gestire VMware Cloud su AWS e utilizzarlo in combinazione con Amazon FSX per NetApp ONTAP e/o Cloud Volumes ONTAP su AWS con storage in-guest.

Lo storage in-guest è attualmente l'unico metodo supportato per connettere Cloud Volumes ONTAP (CVO) ad AWS VMC.

Il processo di configurazione può essere suddiviso in tre parti:

Registrati per un account AWS

Registratevi per un "Account Amazon Web Services".

Per iniziare, è necessario un account AWS, supponendo che non ne sia già stato creato uno. Nuovi o esistenti, per eseguire molte operazioni di questa procedura sono necessari privilegi amministrativi nell'account. Vedi questo "collegamento" Per ulteriori informazioni sulle credenziali AWS.

Registrati per un account My VMware

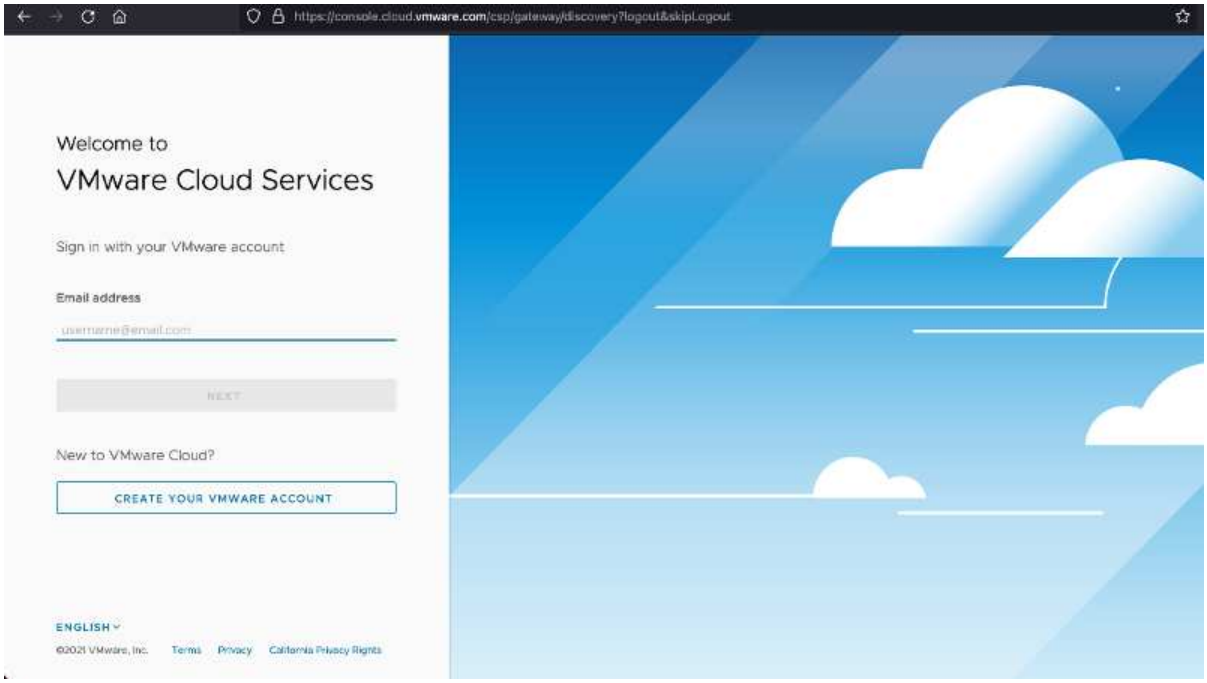
Registratevi per un "Il mio VMware" account.

Per accedere al portfolio cloud di VMware (incluso VMware Cloud su AWS), è necessario un account cliente VMware o un account My VMware. Se non lo si è già fatto, creare un account VMware "qui".

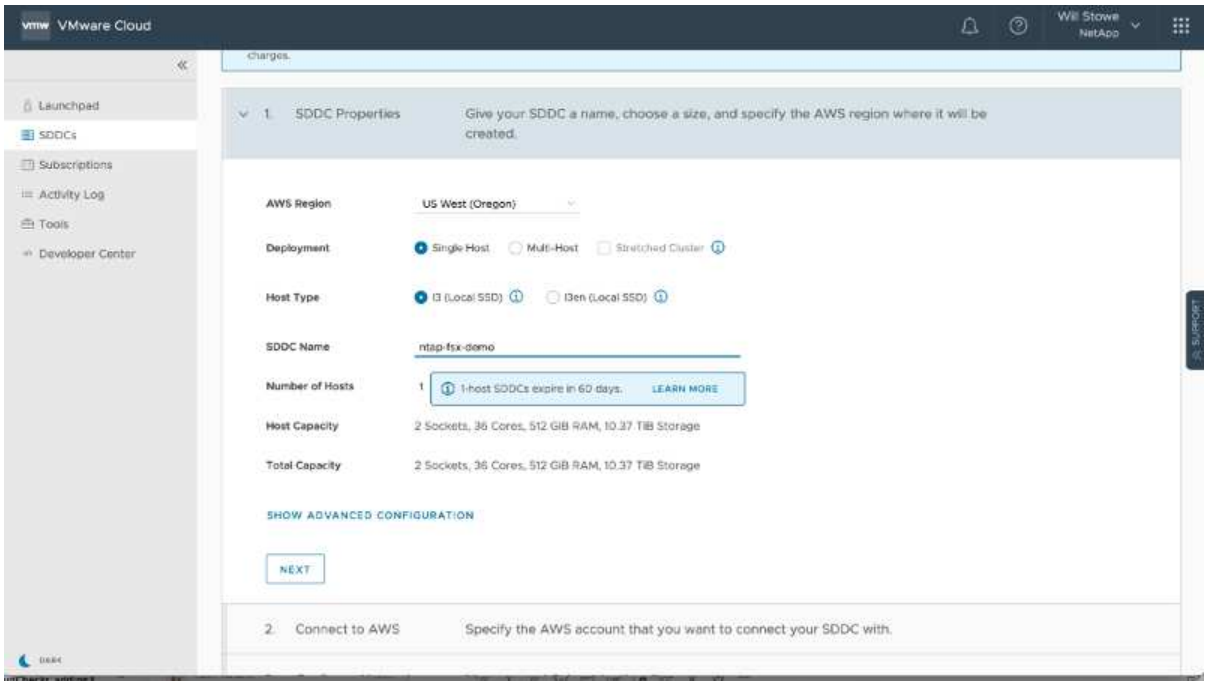
Provisioning di SDDC in VMware Cloud

Una volta configurato l'account VMware e eseguito il dimensionamento corretto, l'implementazione di un Software-Defined Data Center è il passaggio successivo più ovvio per l'utilizzo del servizio VMware Cloud su AWS. Per creare un SDDC, scegliere una regione AWS per ospitarla, assegnare un nome all'SDDC e specificare quanti host ESXi si desidera che l'SDDC contenga. Se non si dispone già di un account AWS, è comunque possibile creare un SDDC di configurazione iniziale contenente un singolo host ESXi.

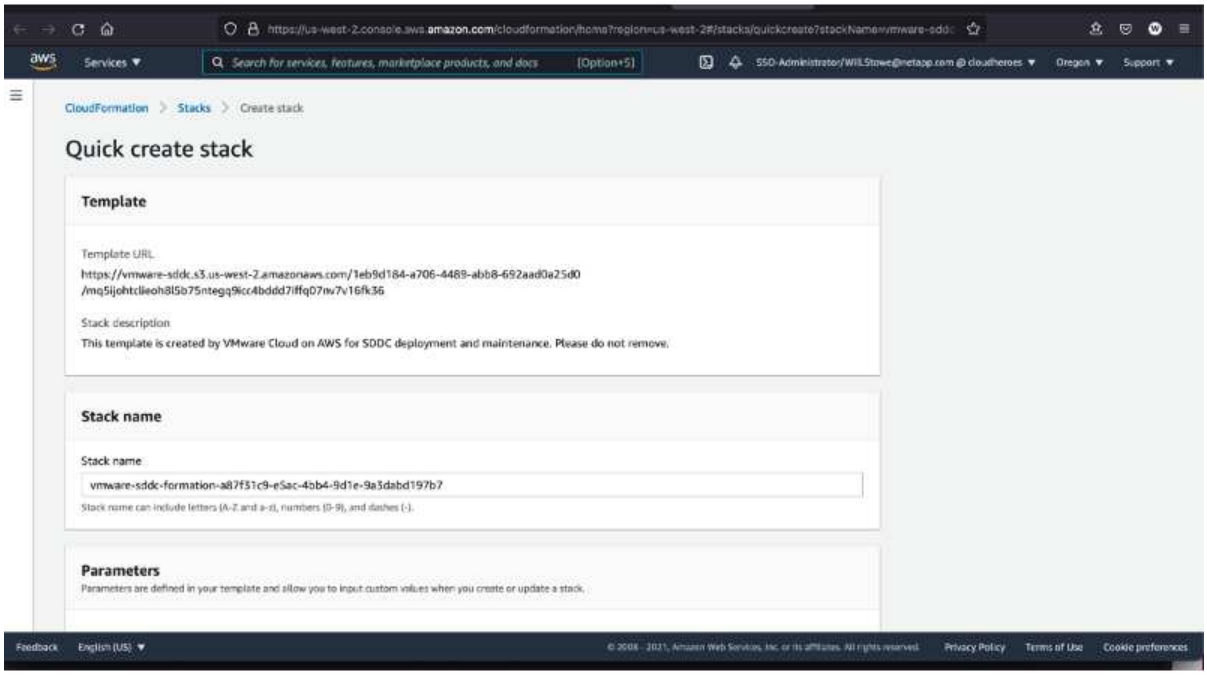
1. Accedere a VMware Cloud Console utilizzando le credenziali VMware esistenti o create di recente.

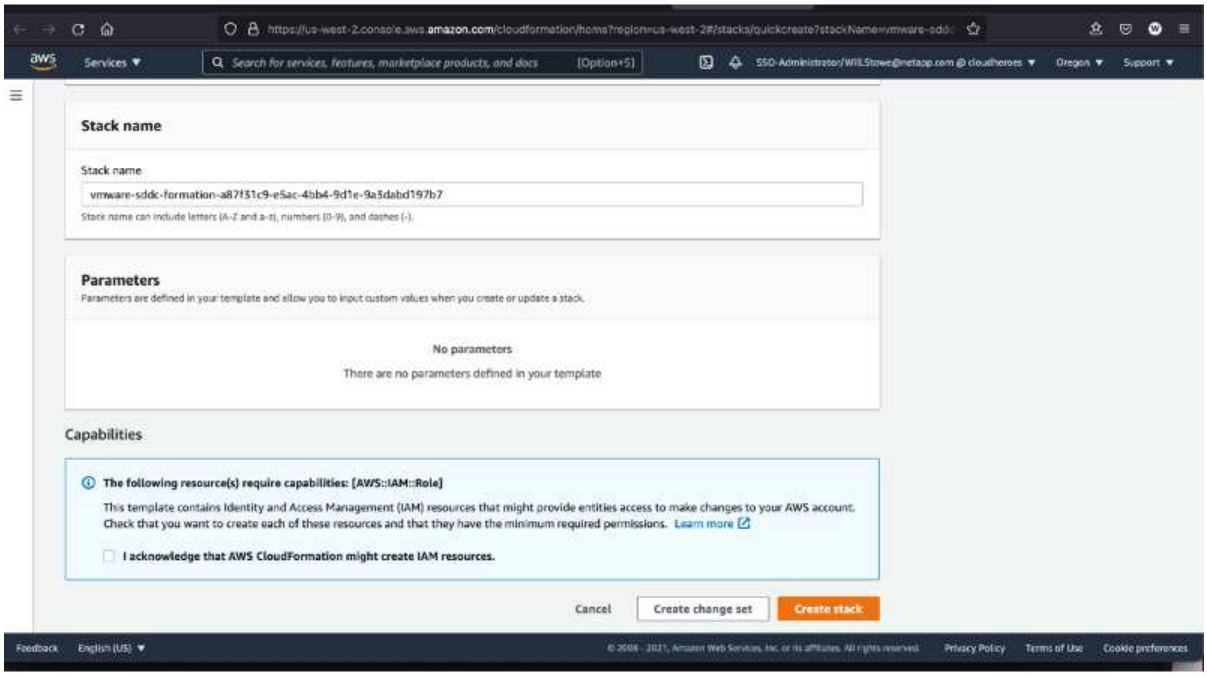


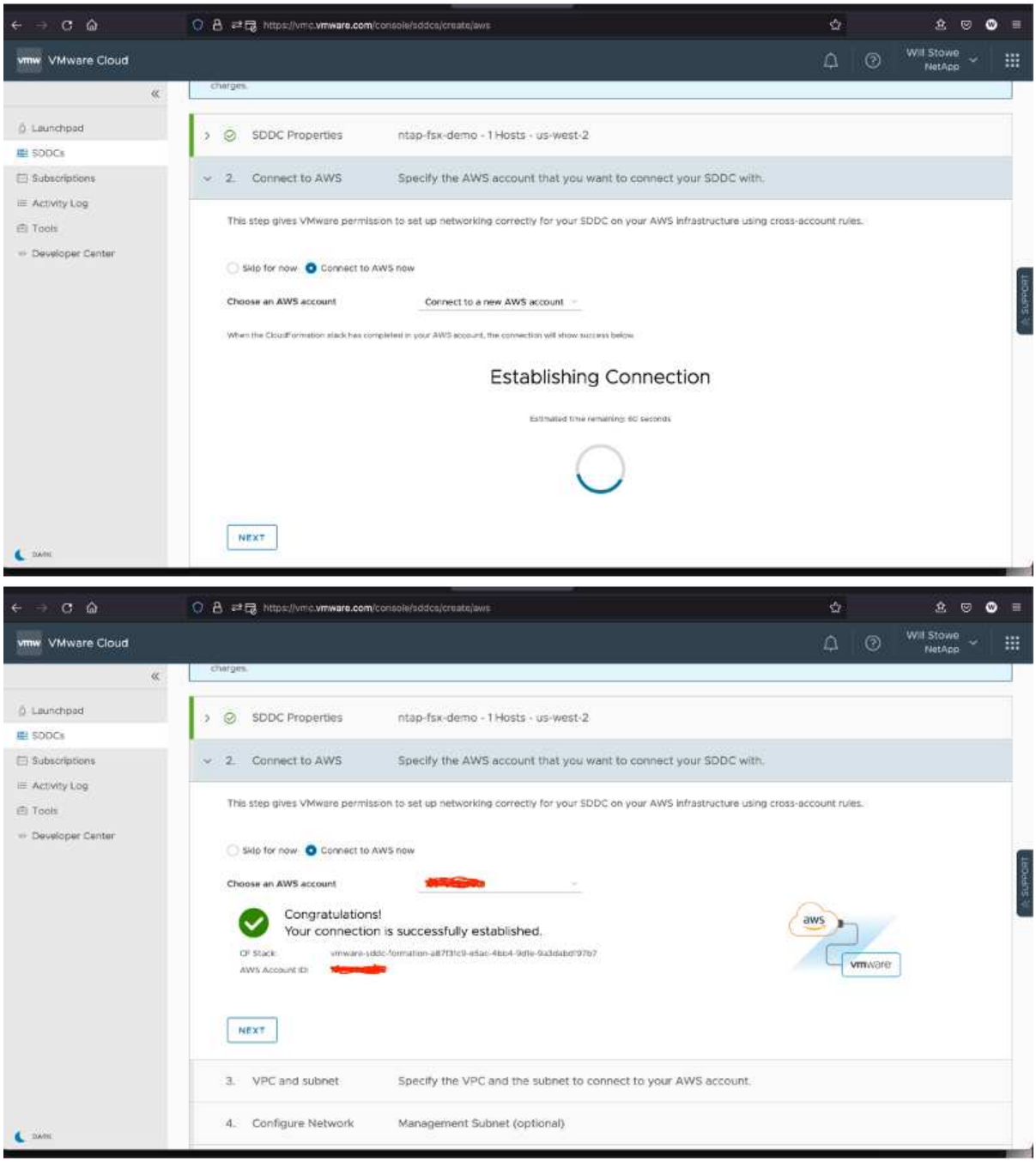
2. Configurare la regione AWS, l'implementazione, il tipo di host e il nome SDDC:



3. Connettersi all’account AWS desiderato ed eseguire lo stack di formazione cloud AWS.

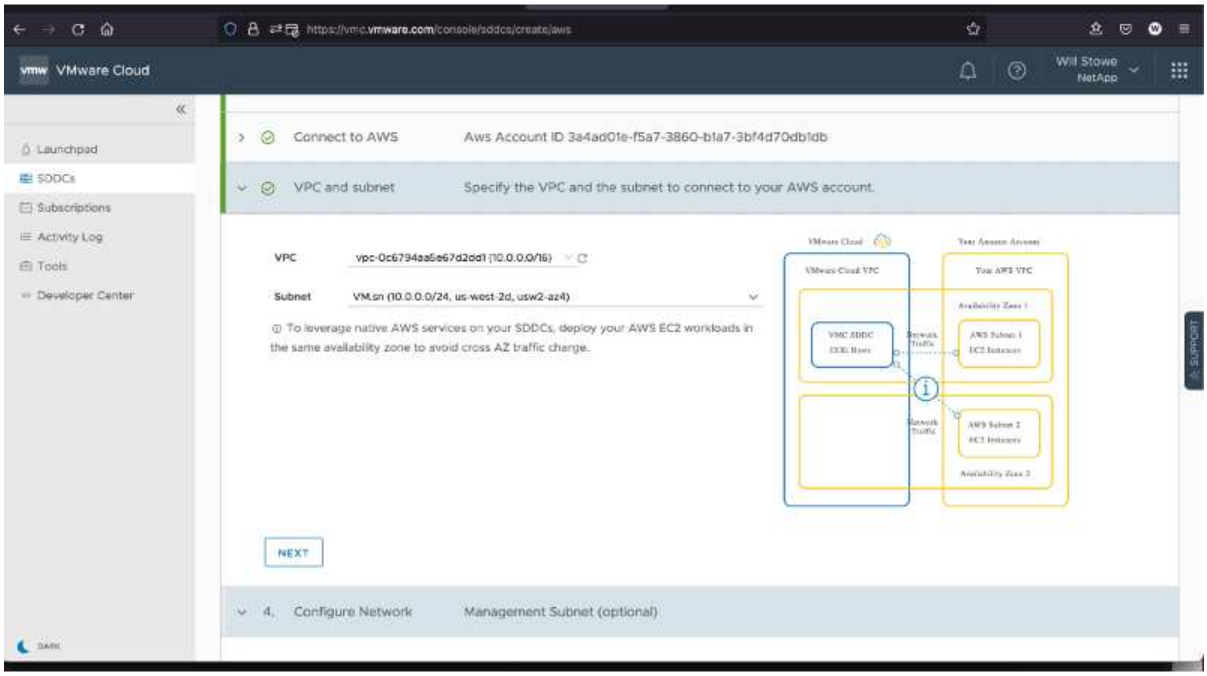




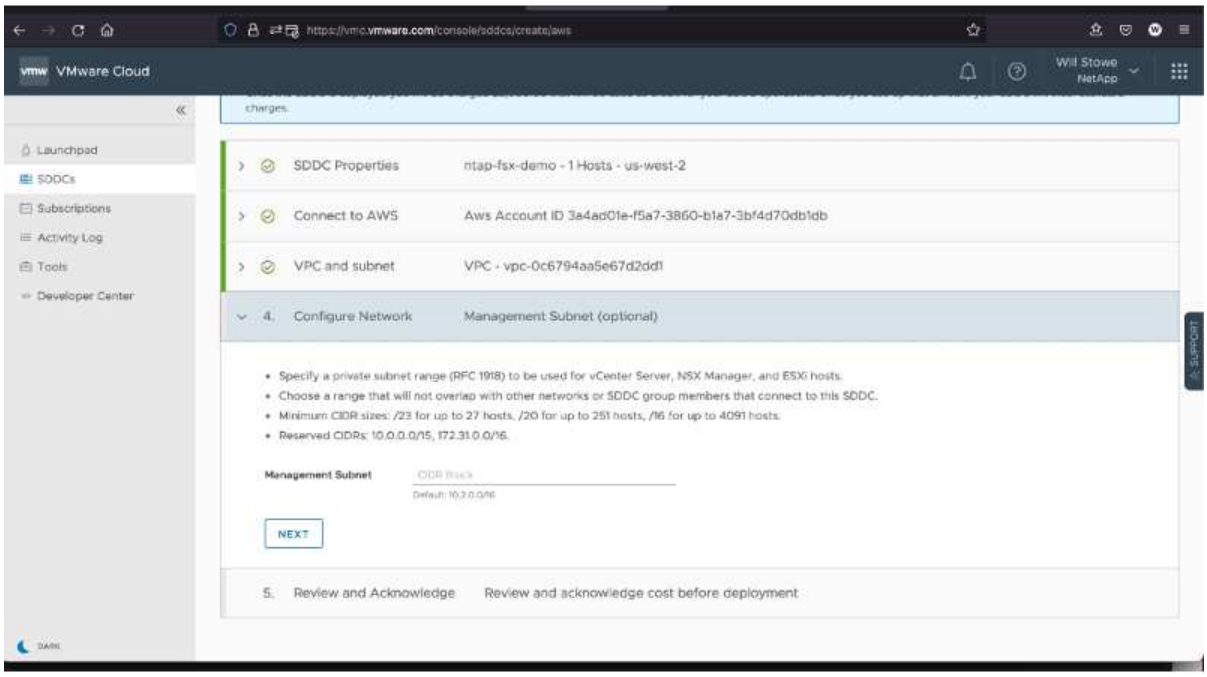


In questa convalida viene utilizzata la configurazione a host singolo.

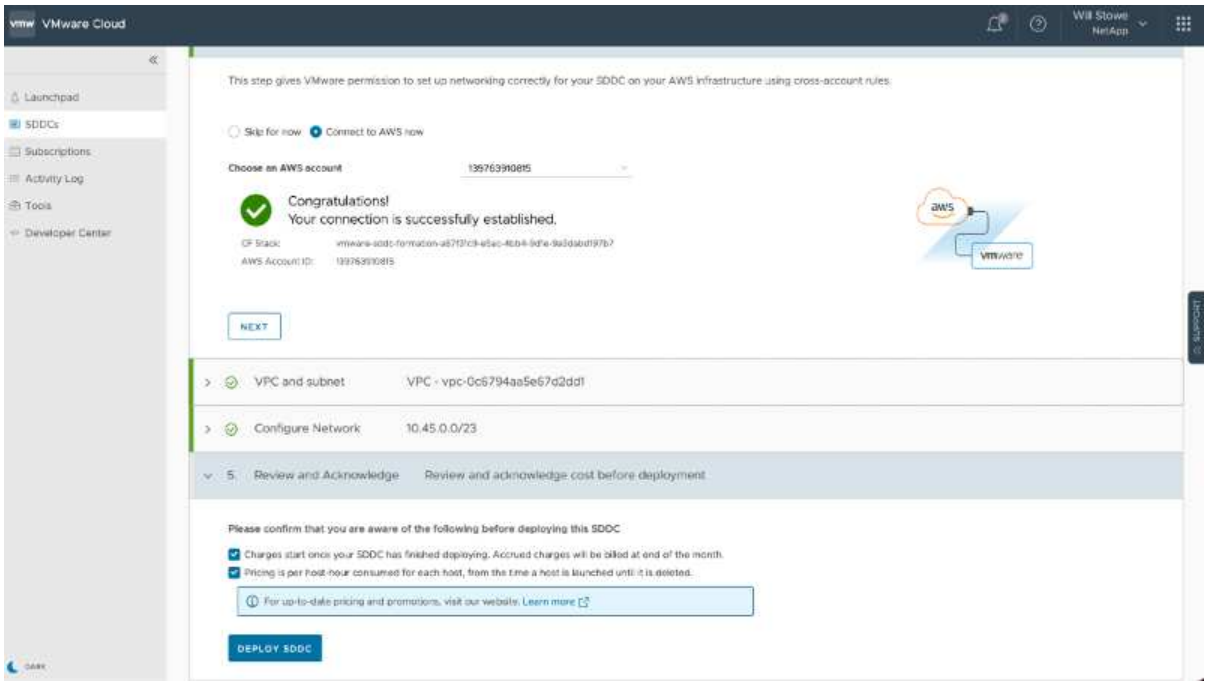
4. Selezionare il VPC AWS desiderato per la connessione dell'ambiente VMC.



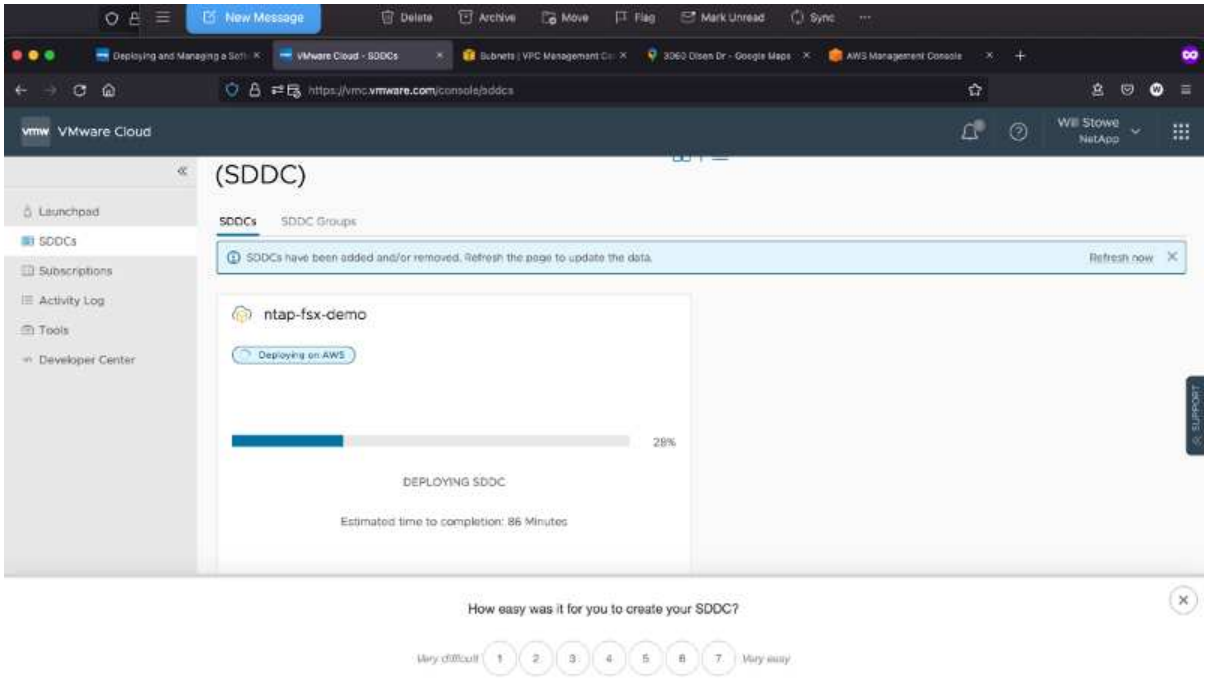
5. Configurare la subnet di gestione VMC; questa subnet contiene servizi gestiti da VMC come vCenter, NSX e così via. Non scegliere uno spazio di indirizzi sovrapposto con altre reti che necessitano di connettività all'ambiente SDDC. Infine, seguire le raccomandazioni per la dimensione CIDR indicate di seguito.



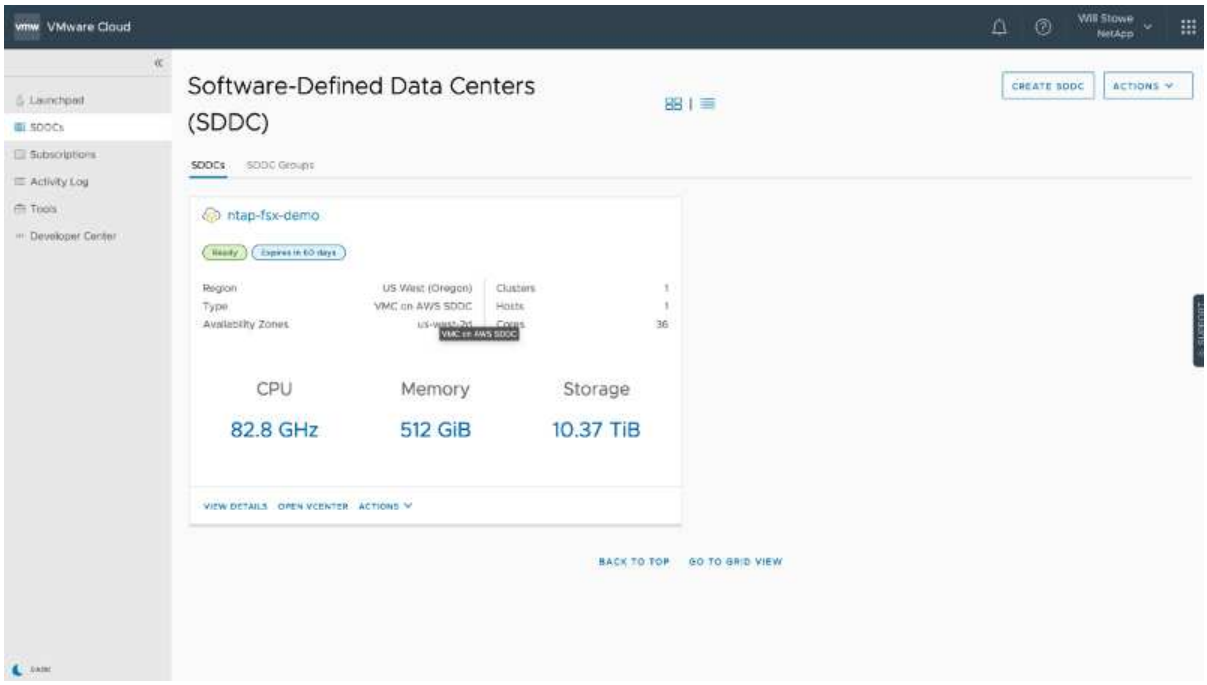
6. Esaminare e riconoscere la configurazione SDDC, quindi fare clic su Deploy the SDDC (implementa SDDC).



Il completamento del processo di implementazione richiede in genere circa due ore.



7. Al termine dell'operazione, SDDC è pronto per l'uso.

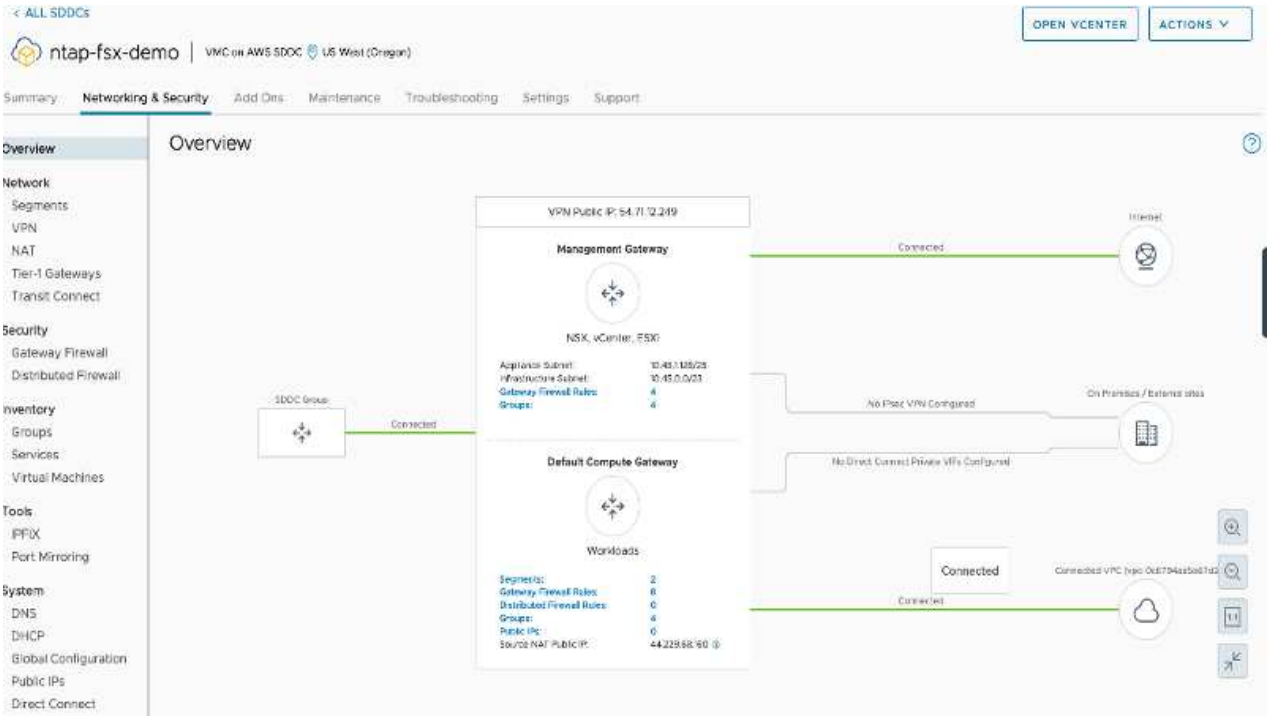


Per una guida dettagliata sull'implementazione di SDDC, vedere "Implementare un SDDC dalla console VMC".

Connetti VMware Cloud a FSX ONTAP

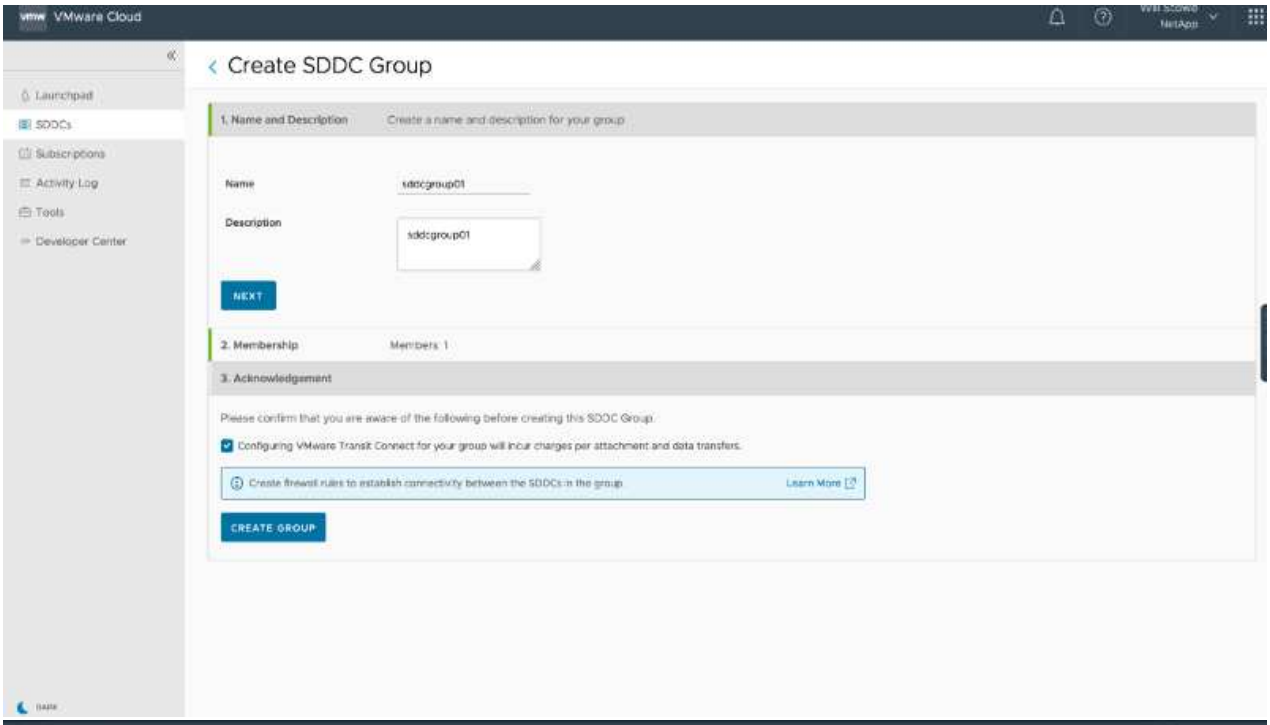
Per connettere VMware Cloud a FSX ONTAP, attenersi alla seguente procedura:

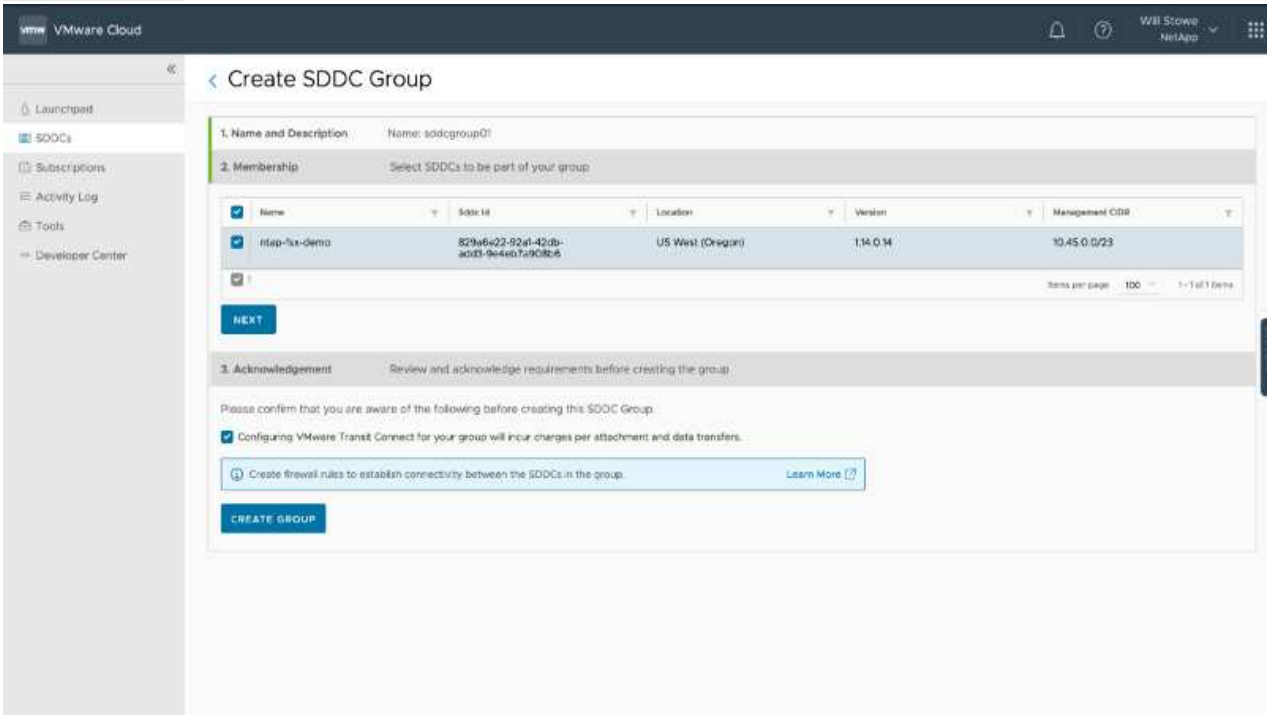
1. Una volta completata l'implementazione di VMware Cloud e connessa ad AWS VPC, è necessario implementare Amazon FSX per NetApp ONTAP in un nuovo VPC anziché nel VPC collegato originale (vedere la schermata riportata di seguito). FSX (IP mobili NFS e SMB) non è accessibile se viene implementato nel VPC connesso. Tenere presente che gli endpoint ISCSI come Cloud Volumes ONTAP funzionano correttamente dal VPC connesso.

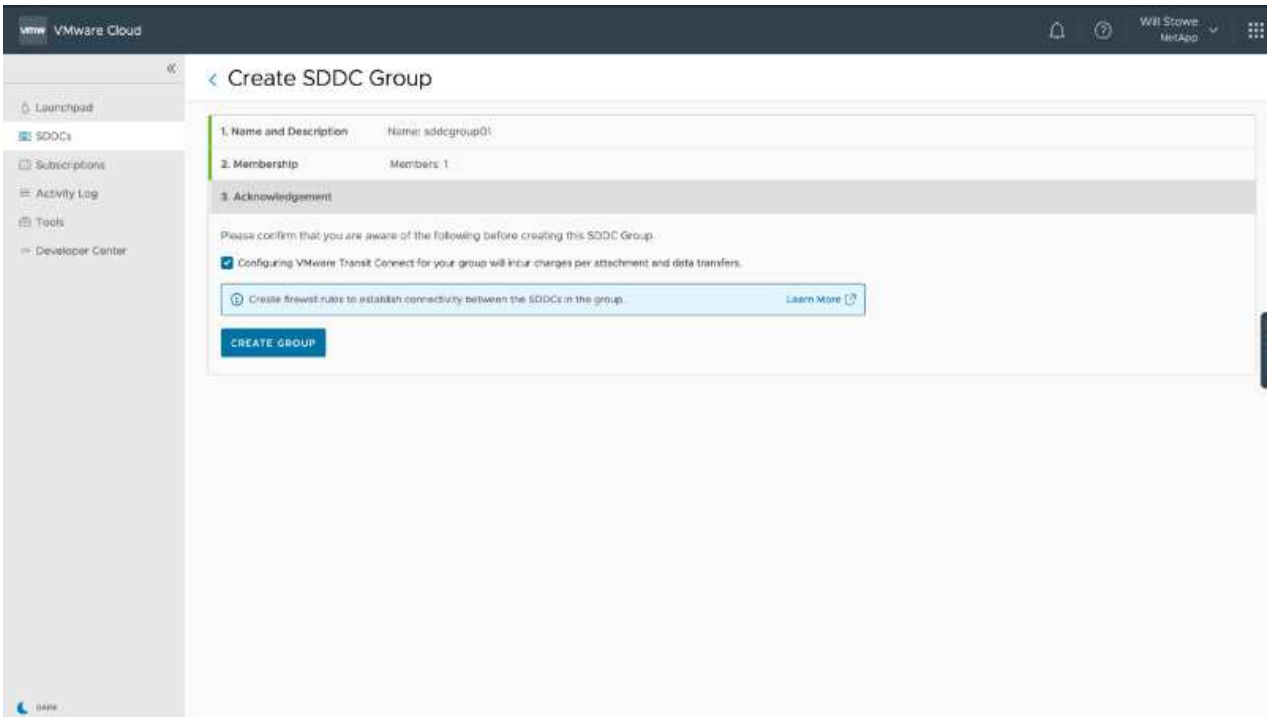


2. Implementare un VPC aggiuntivo nella stessa regione, quindi implementare Amazon FSX per NetApp ONTAP nel nuovo VPC.

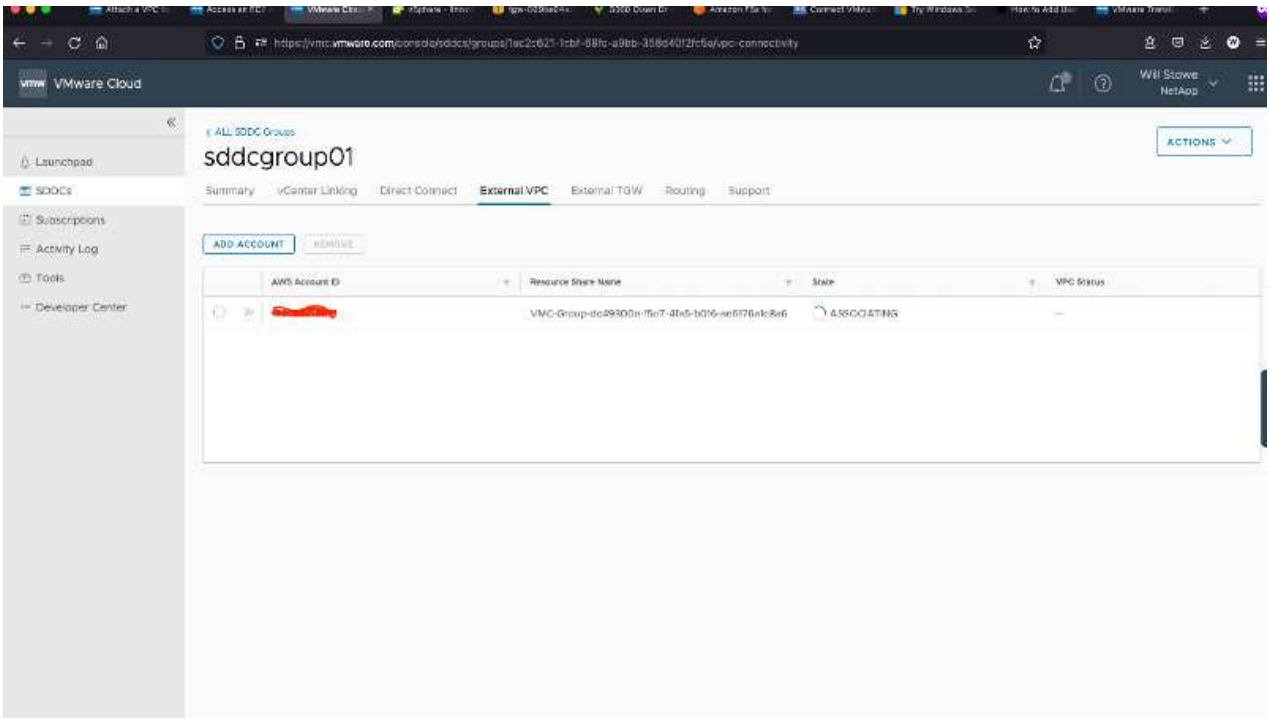
   La configurazione di un gruppo SDDC nella console VMware Cloud abilita le opzioni di configurazione di rete necessarie per connettersi al nuovo VPC in cui viene implementato FSX. Nella fase 3, verificare che l'opzione "Configurazione di VMware Transit Connect per il gruppo comporterà costi per allegato e trasferimento dati" sia selezionata, quindi scegliere Crea gruppo. Il completamento del processo può richiedere alcuni minuti.

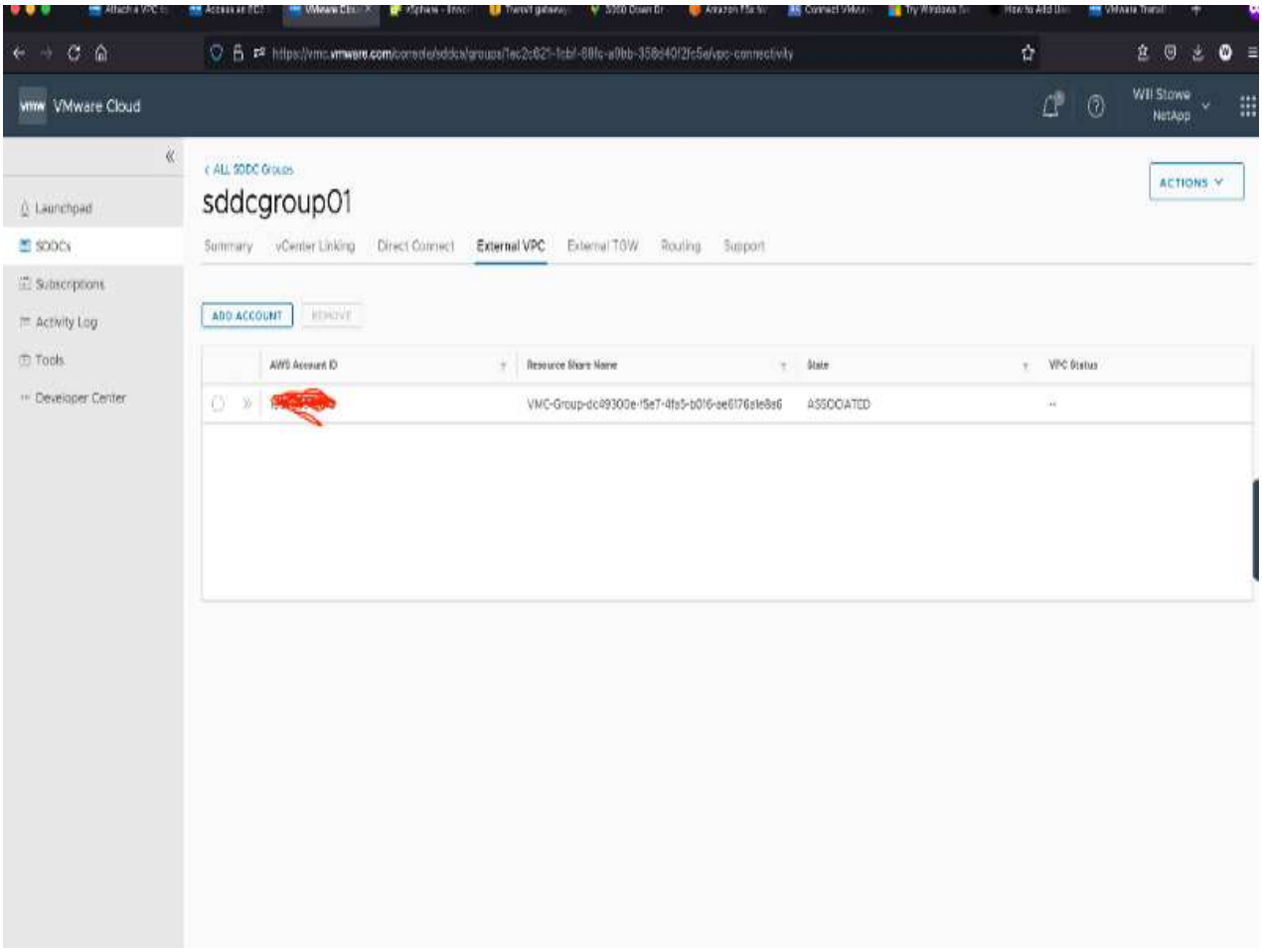

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are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


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

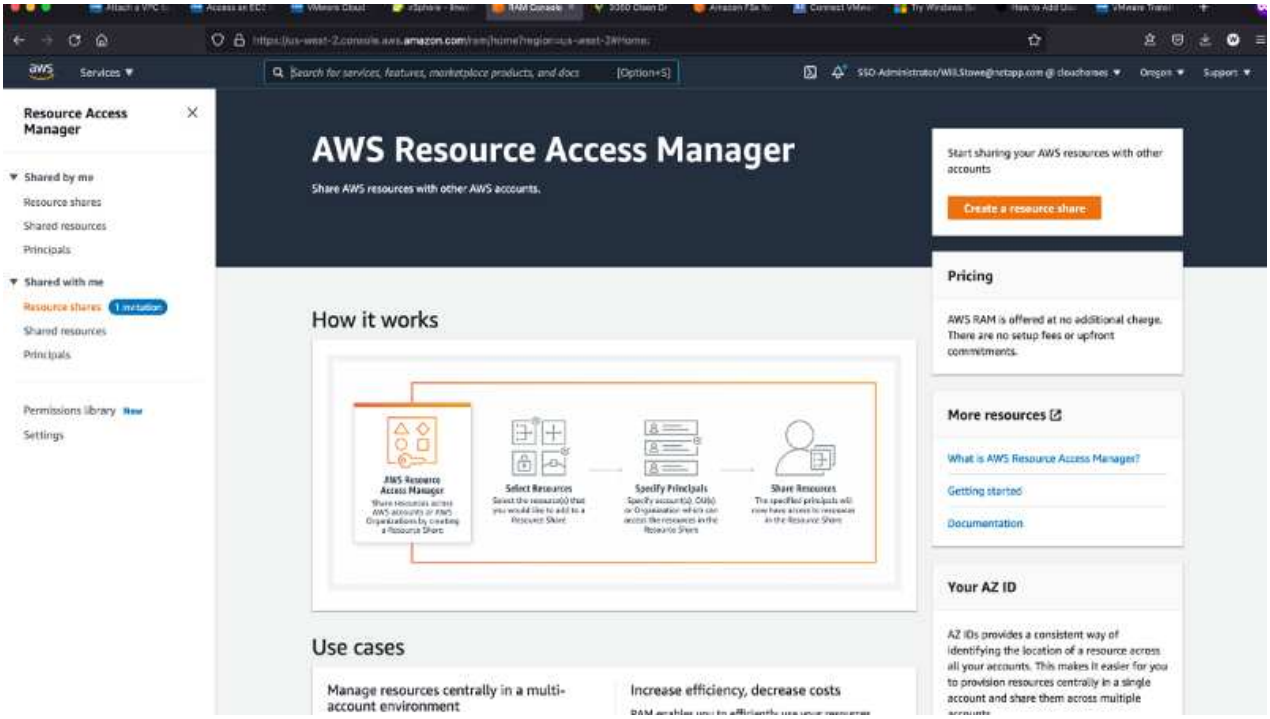


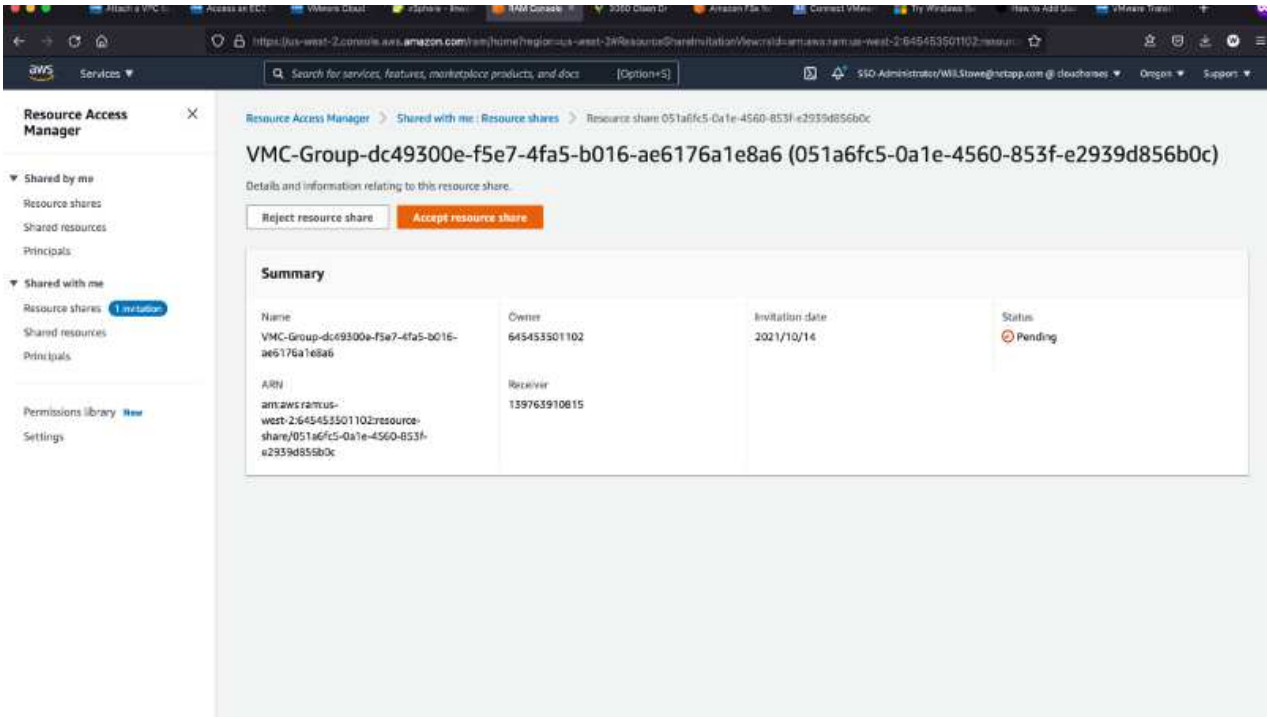
3. Collegare il VPC appena creato al gruppo SDDC appena creato. Selezionare la scheda External VPC (VPC esterno) e seguire le istruzioni "Istruzioni per il collegamento di un VPC esterno" al gruppo. Il completamento di questo processo può richiedere da 10 a 15 minuti.



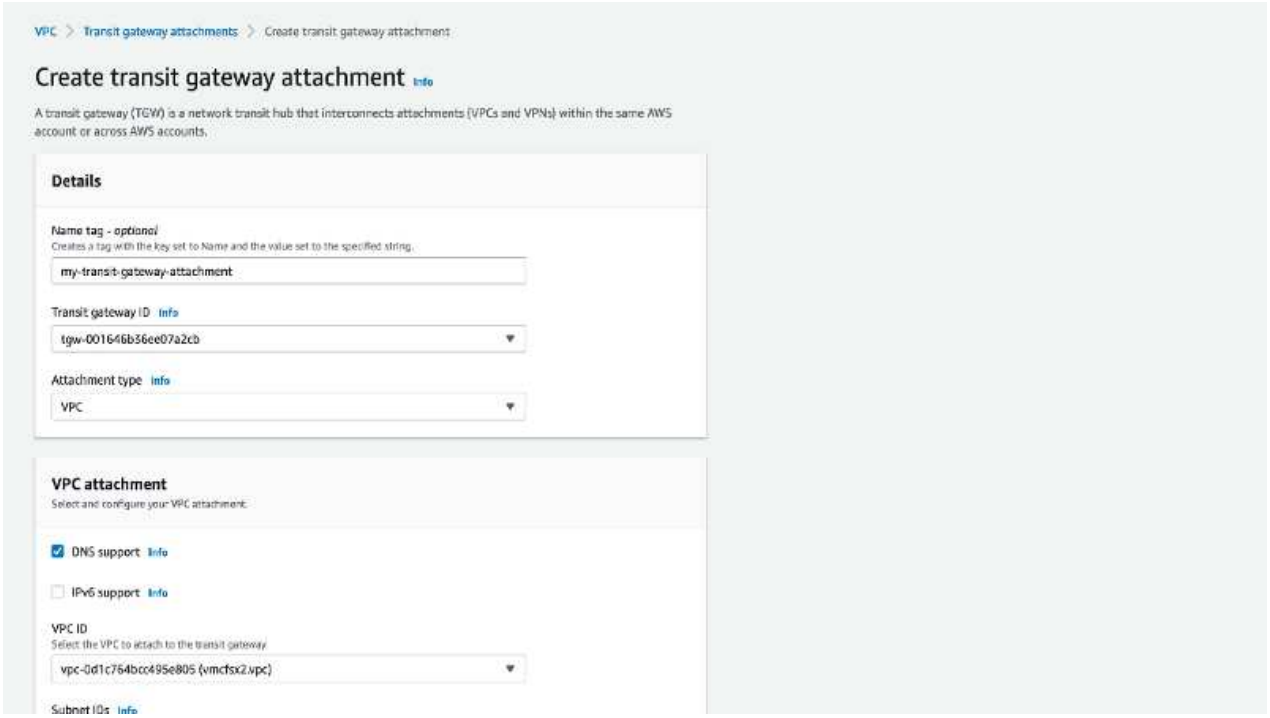


4. Nell'ambito del processo VPC esterno, viene richiesto tramite la console AWS di accedere a una nuova risorsa condivisa tramite Resource Access Manager. La risorsa condivisa è "AWS Transit Gateway" Gestito da VMware Transit Connect.

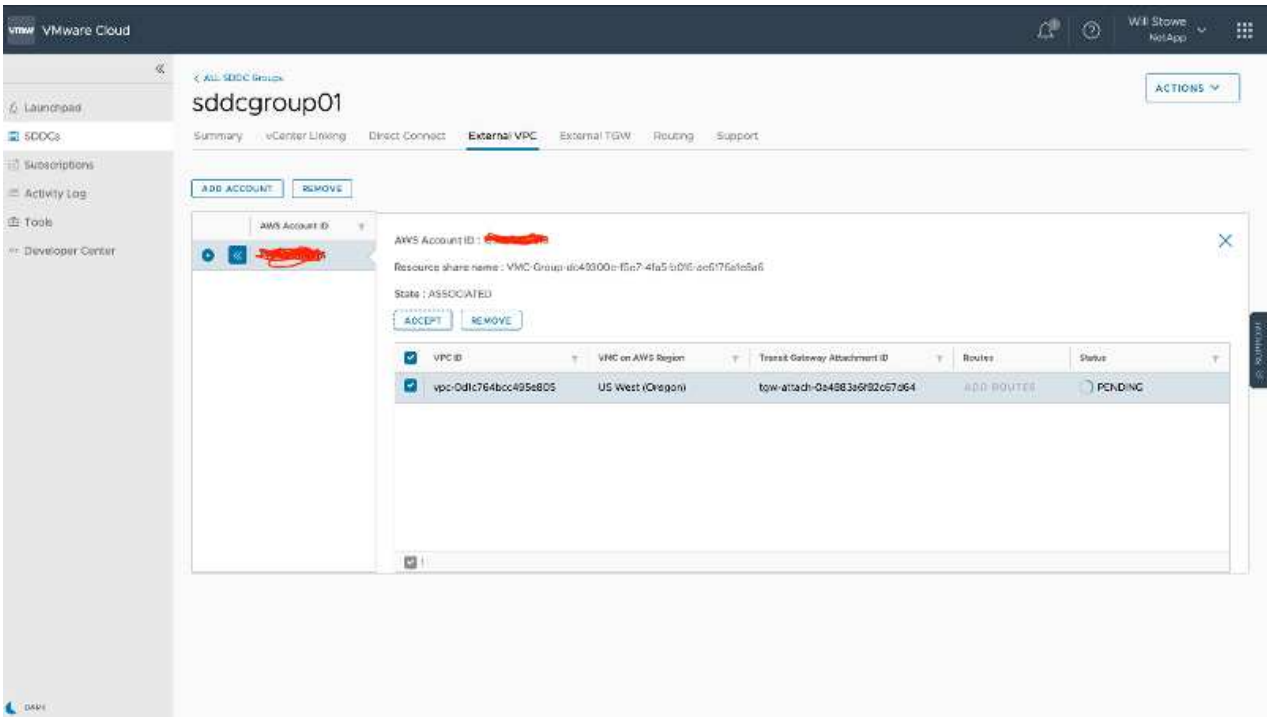




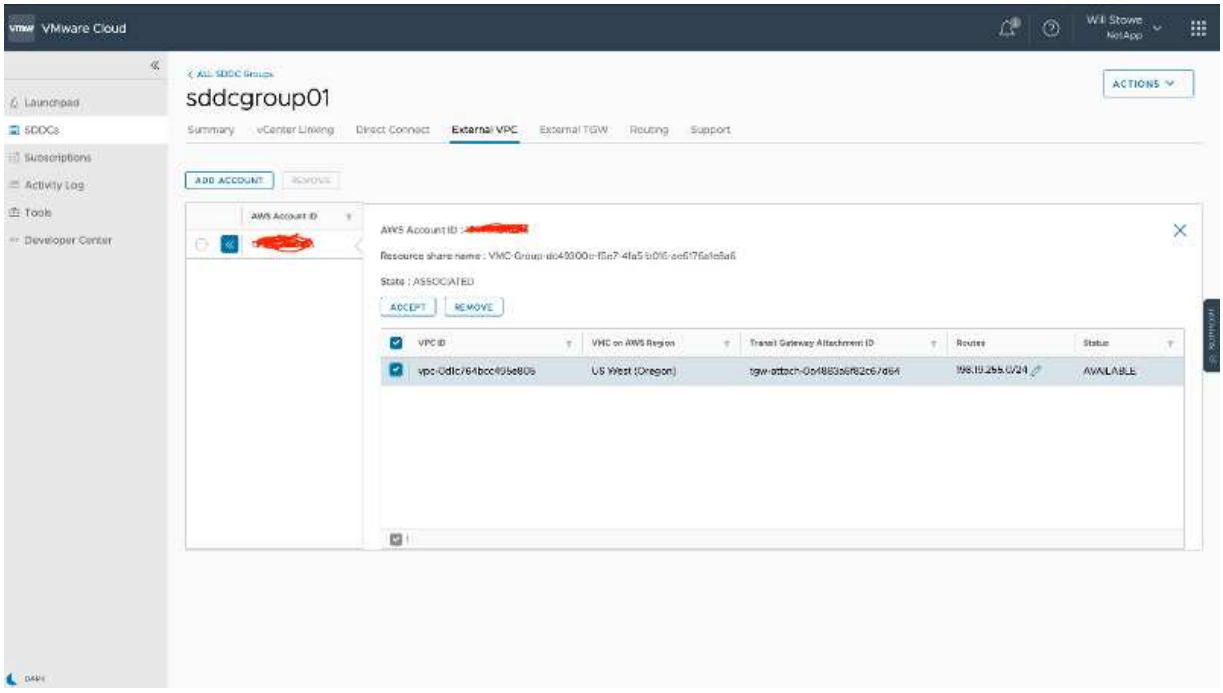
5. Creare l'allegato del gateway di transito.



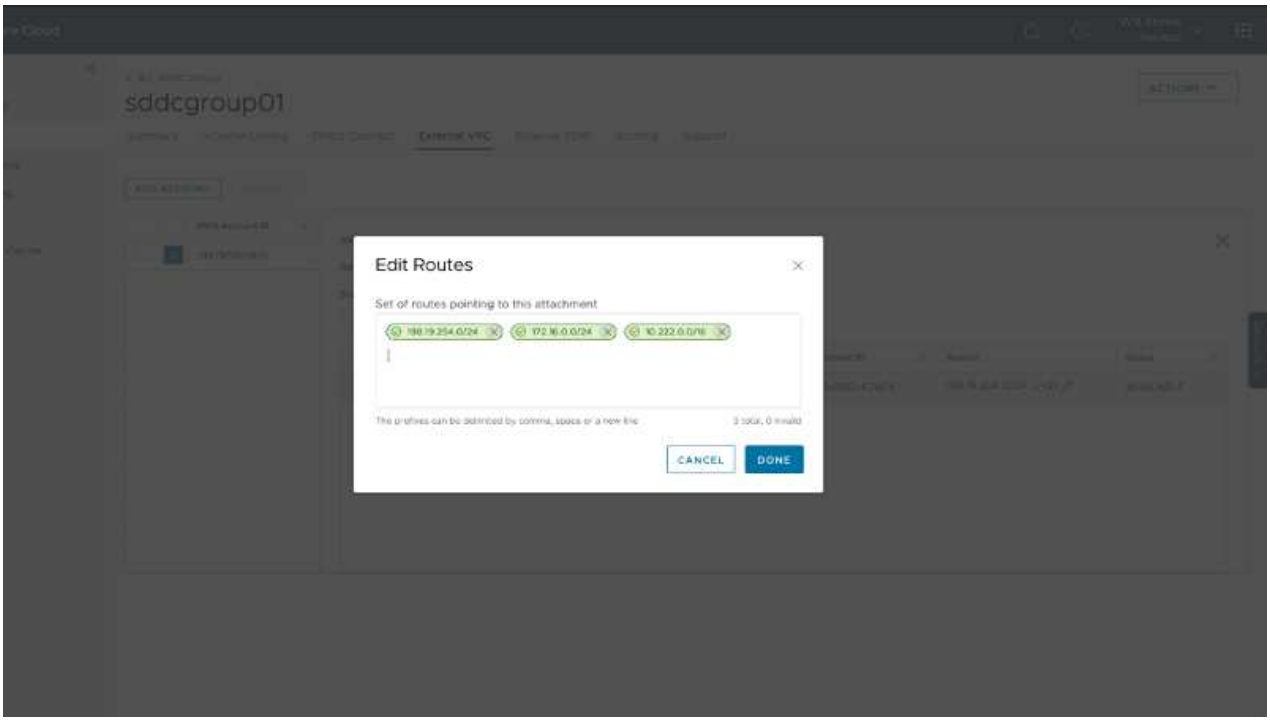
6. Sulla console VMC, accettare l'allegato VPC. Il completamento di questo processo può richiedere circa 10 minuti.



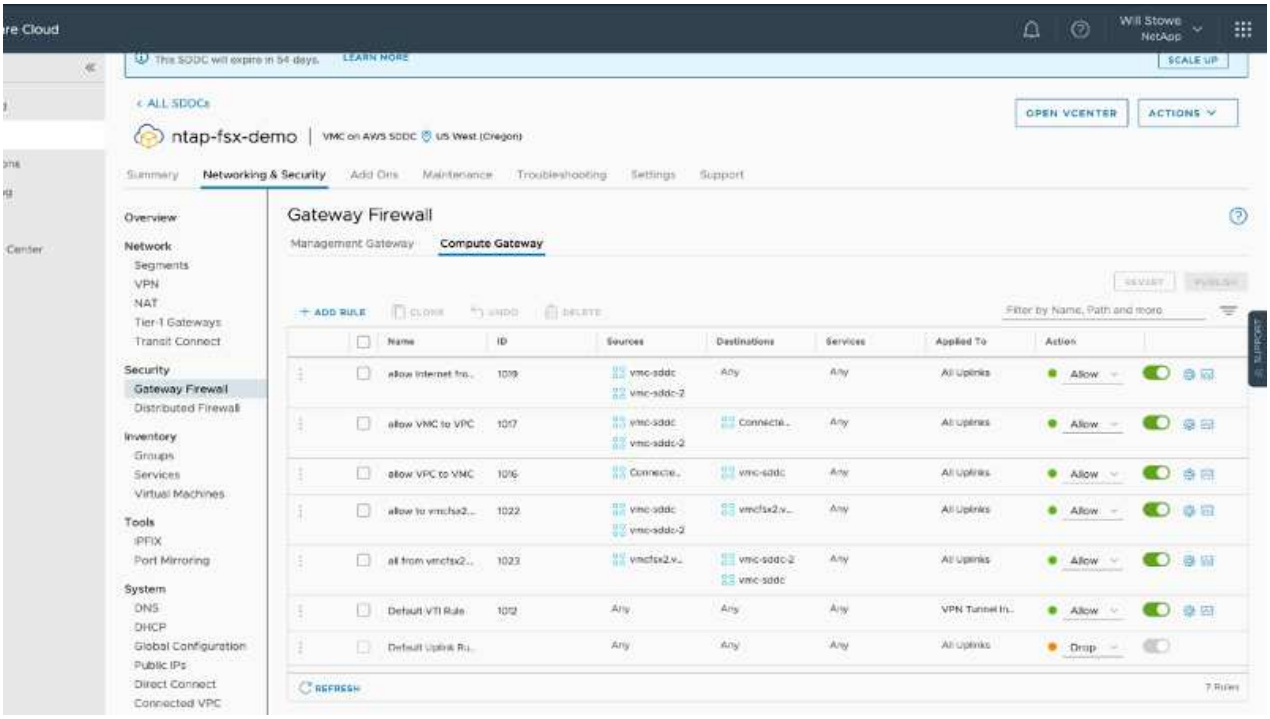
7. Nella scheda External VPC (VPC esterno), fare clic sull'icona di modifica nella colonna routes (percorsi) e aggiungere i seguenti percorsi richiesti:
   - Un percorso per l'intervallo IP mobile per Amazon FSX per NetApp ONTAP "IP mobili".
   - Route per l'intervallo IP mobile per Cloud Volumes ONTAP (se applicabile).
   - Un percorso per lo spazio di indirizzi VPC esterno appena creato.



8. Infine, consentire il traffico bidirezionale "regole del firewall" Per l'accesso a FSX/CVO. Seguire queste istruzioni "passaggi dettagliati" Per le regole firewall del gateway di calcolo per la connettività dei carichi di lavoro SDDC.



9. Una volta configurati i gruppi di firewall per il gateway di gestione e di calcolo, è possibile accedere a vCenter come segue:



Il passaggio successivo consiste nel verificare che Amazon FSX ONTAP o Cloud Volumes ONTAP sia configurato in base ai requisiti e che i volumi siano configurati per trasferire i componenti di storage da vSAN per ottimizzare l'implementazione.

Come per la soluzione VMware di Azure on-premise, la pianificazione è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

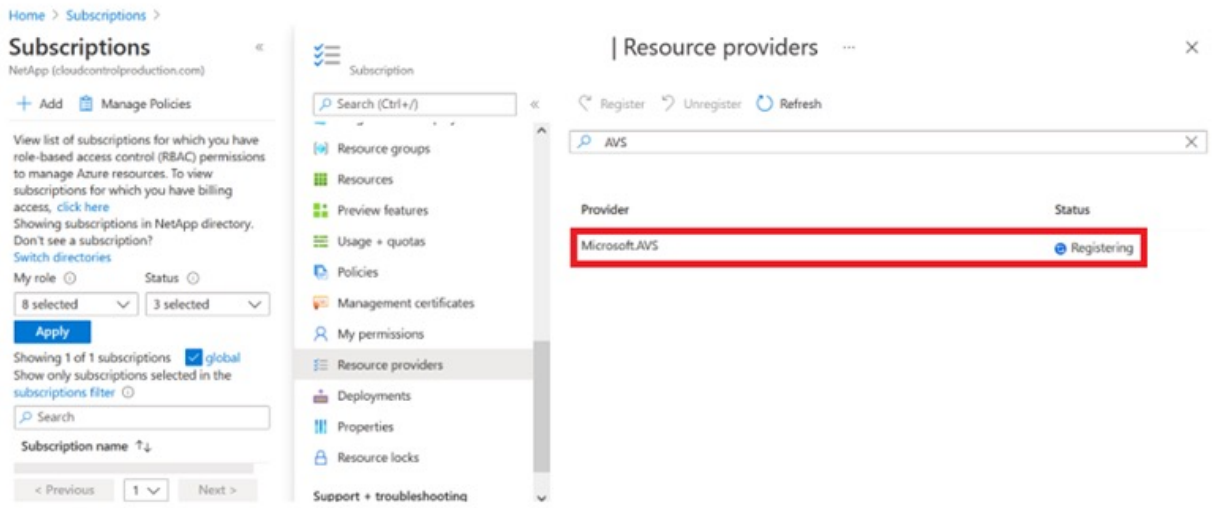
Questa sezione descrive come configurare e gestire Azure VMware Solution e utilizzarla in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Registrare il provider di risorse e creare un cloud privato

Per utilizzare Azure VMware Solution, registrare innanzitutto il provider di risorse nell'abbonamento identificato:

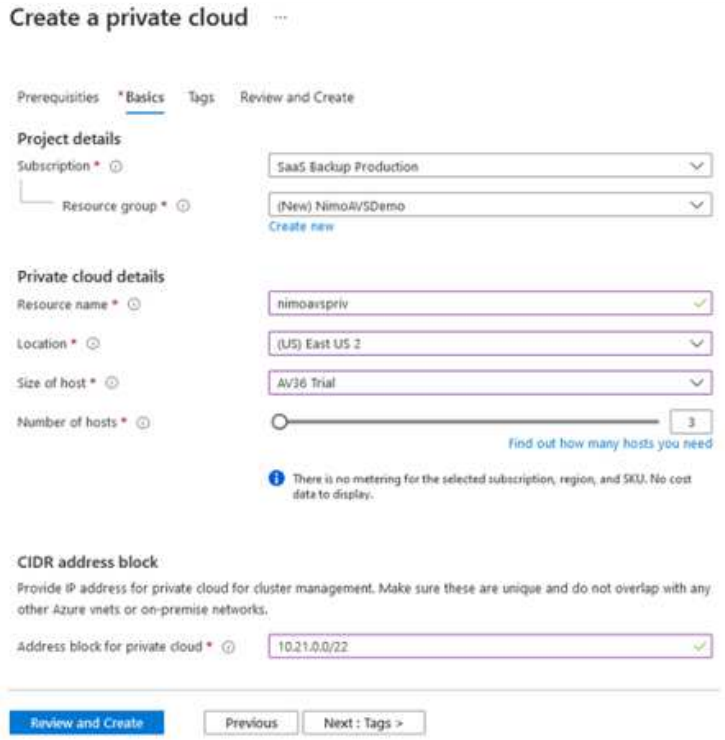
1. Accedi al portale Azure.
2. Nel menu del portale Azure, selezionare tutti i servizi.
3. Nella finestra di dialogo tutti i servizi, inserire l'abbonamento e selezionare Abbonamenti.
4. Per visualizzare, selezionare l'abbonamento dall'elenco.
5. Selezionare Resource Providers (Provider di risorse) e immettere Microsoft.AVS nella ricerca.
6. Se il provider di risorse non è registrato, selezionare Registra.



7. Una volta registrato il provider di risorse, creare un cloud privato Azure VMware Solution utilizzando il portale Azure.
8. Accedi al portale Azure.
9. Selezionare Crea una nuova risorsa.
10. Nella casella di testo Cerca nel marketplace, immettere Azure VMware Solution e selezionarla dai risultati.
11. Nella pagina Azure VMware Solution, selezionare Create (Crea).
12. Nella scheda Basics (informazioni di base), immettere i valori nei campi e selezionare Review (esamina) + Create (Crea).

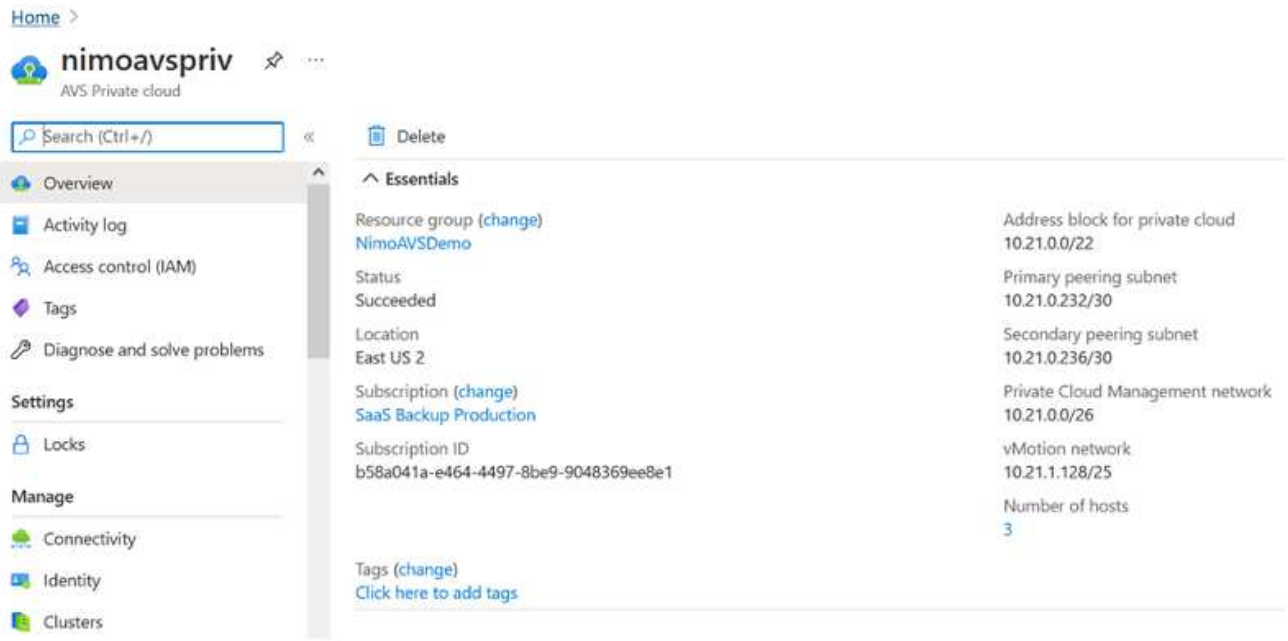
Note:

- Per un rapido avvio, raccogliere le informazioni necessarie durante la fase di pianificazione.
- Selezionare un gruppo di risorse esistente o creare un nuovo gruppo di risorse per il cloud privato. Un gruppo di risorse è un container logico in cui le risorse Azure vengono distribuite e gestite.
- Assicurarsi che l'indirizzo CIDR sia univoco e non si sovrapponga ad altre reti virtuali Azure o on-premise. Il CIDR rappresenta la rete di gestione del cloud privato e viene utilizzato per i servizi di gestione del cluster, come vCenter Server e NSX-T Manager. NetApp consiglia di utilizzare uno spazio di indirizzi /22. In questo esempio, viene utilizzato 10.21.0.0/22.



Il processo di provisioning richiede circa 4-5 ore. Una volta completato il processo, verificare che l'implementazione abbia avuto esito positivo accedendo al cloud privato dal portale Azure. Al termine dell'implementazione viene visualizzato lo stato riuscito.

Un cloud privato Azure VMware Solution richiede una rete virtuale Azure. Poiché Azure VMware Solution non supporta vCenter on-premise, sono necessari ulteriori passaggi per l'integrazione con un ambiente on-premise esistente. È inoltre necessaria la configurazione di un circuito ExpressRoute e di un gateway di rete virtuale. In attesa del completamento del provisioning del cluster, creare una nuova rete virtuale o utilizzarne una esistente per connettersi alla soluzione VMware Azure.



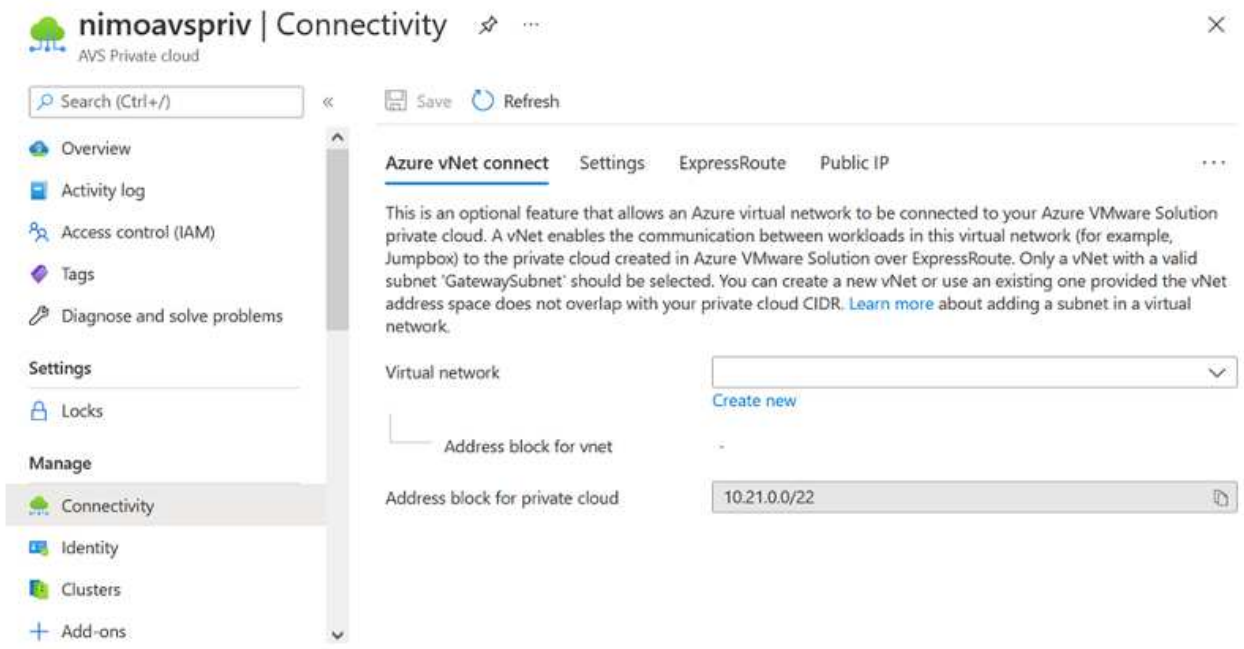
Connettersi a un gateway di rete virtuale ExpressRoute nuovo o esistente

Per creare una nuova rete virtuale Azure (VNET), selezionare la scheda Azure VNET Connect. In alternativa, è possibile crearne una manualmente dal portale Azure utilizzando la procedura guidata Create Virtual Network (Crea rete virtuale):

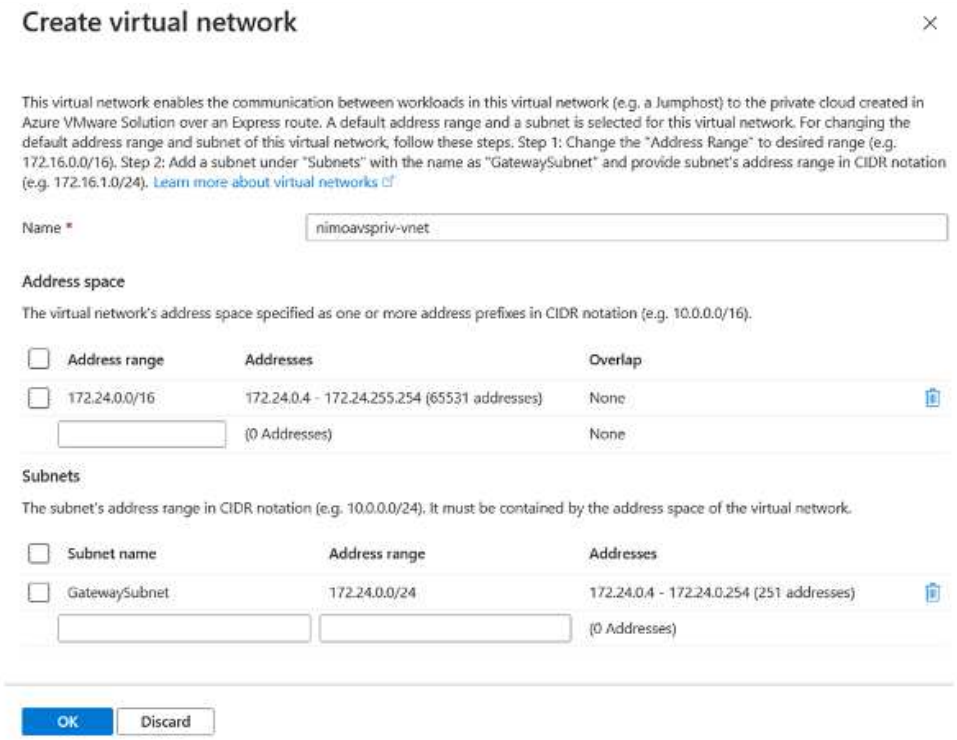
1. Accedere al cloud privato Azure VMware Solution e alla connettività sotto l'opzione Manage (Gestisci).
2. Selezionare Azure VNET Connect.
3. Per creare un nuovo VNET, selezionare l'opzione Create New (Crea nuovo).

   Questa funzione consente di connettere un VNET al cloud privato Azure VMware Solution. VNET consente la comunicazione tra i carichi di lavoro in questa rete virtuale creando automaticamente i componenti necessari (ad esempio, jump box, servizi condivisi come Azure NetApp Files e Cloud Volume ONTAP) al cloud privato creato in Azure VMware Solution su ExpressRoute.

   Nota: lo spazio degli indirizzi VNET non deve sovrapporsi al CIDR del cloud privato.



4. Fornire o aggiornare le informazioni per il nuovo VNET e selezionare OK.

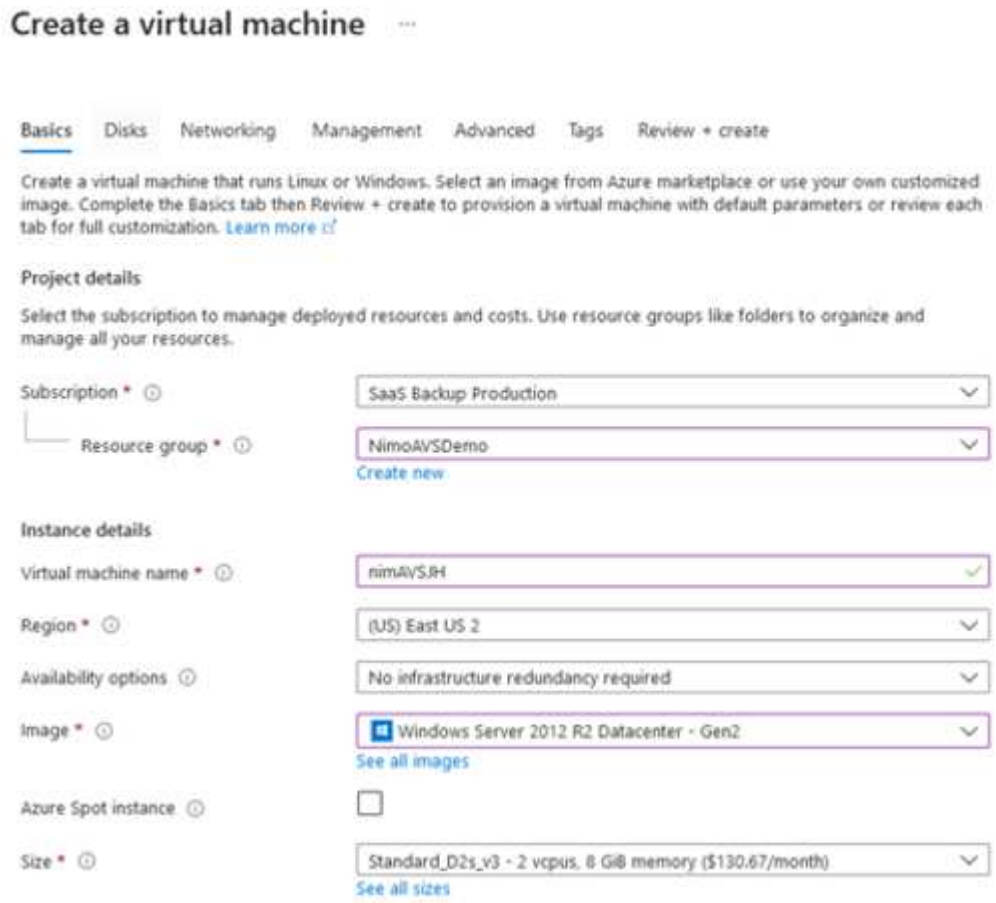


La rete VNET con l'intervallo di indirizzi e la subnet del gateway forniti viene creata nel gruppo di risorse e di abbonamento designato.

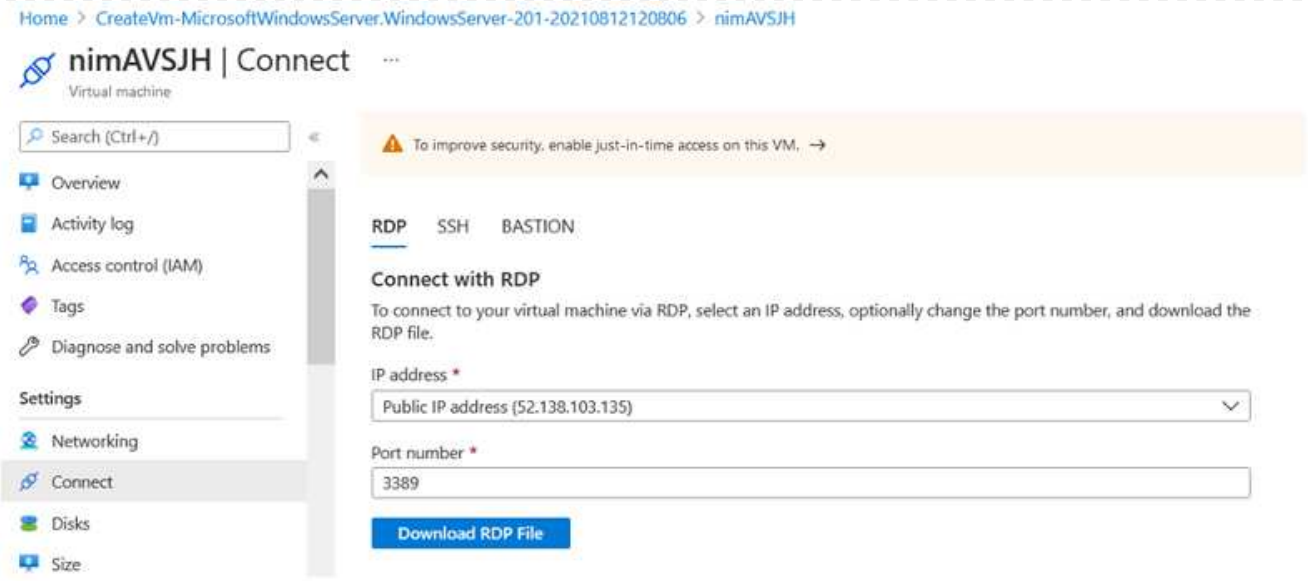
Se si crea un VNET manualmente, creare un gateway di rete virtuale con lo SKU appropriato e ExpressRoute come tipo di gateway. Una volta completata l'implementazione, collegare la connessione ExpressRoute al gateway di rete virtuale contenente il cloud privato Azure VMware Solution utilizzando la chiave di autorizzazione. Per ulteriori informazioni, vedere "Configura il networking per il tuo cloud privato VMware in Azure".

Convalidare la connessione di rete e l'accesso al cloud privato Azure VMware Solution

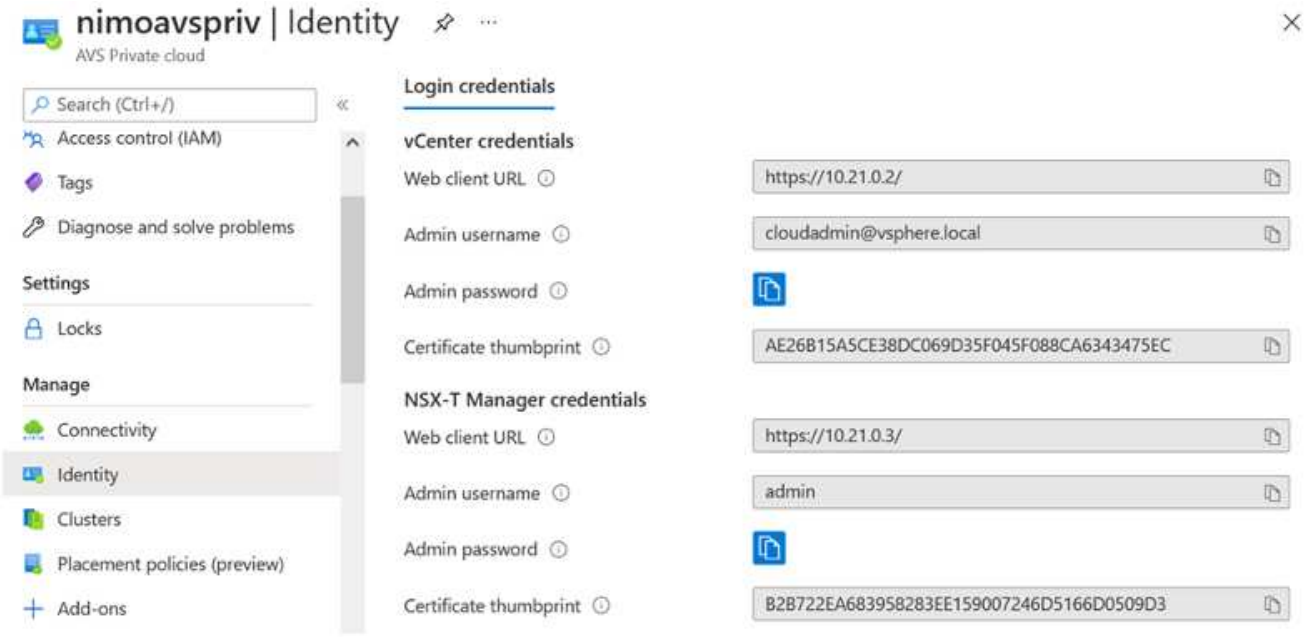
Azure VMware Solution non consente di gestire un cloud privato con VMware vCenter on-premise. Per connettersi all'istanza di Azure VMware Solution vCenter è invece necessario un host jump. Creare un host jump nel gruppo di risorse designato e accedere a Azure VMware Solution vCenter. Questo host jump dovrebbe essere una macchina virtuale Windows sulla stessa rete virtuale creata per la connettività e dovrebbe fornire l'accesso a vCenter e NSX Manager.



Una volta eseguito il provisioning della macchina virtuale, utilizzare l'opzione Connect (Connetti) per accedere a RDP.

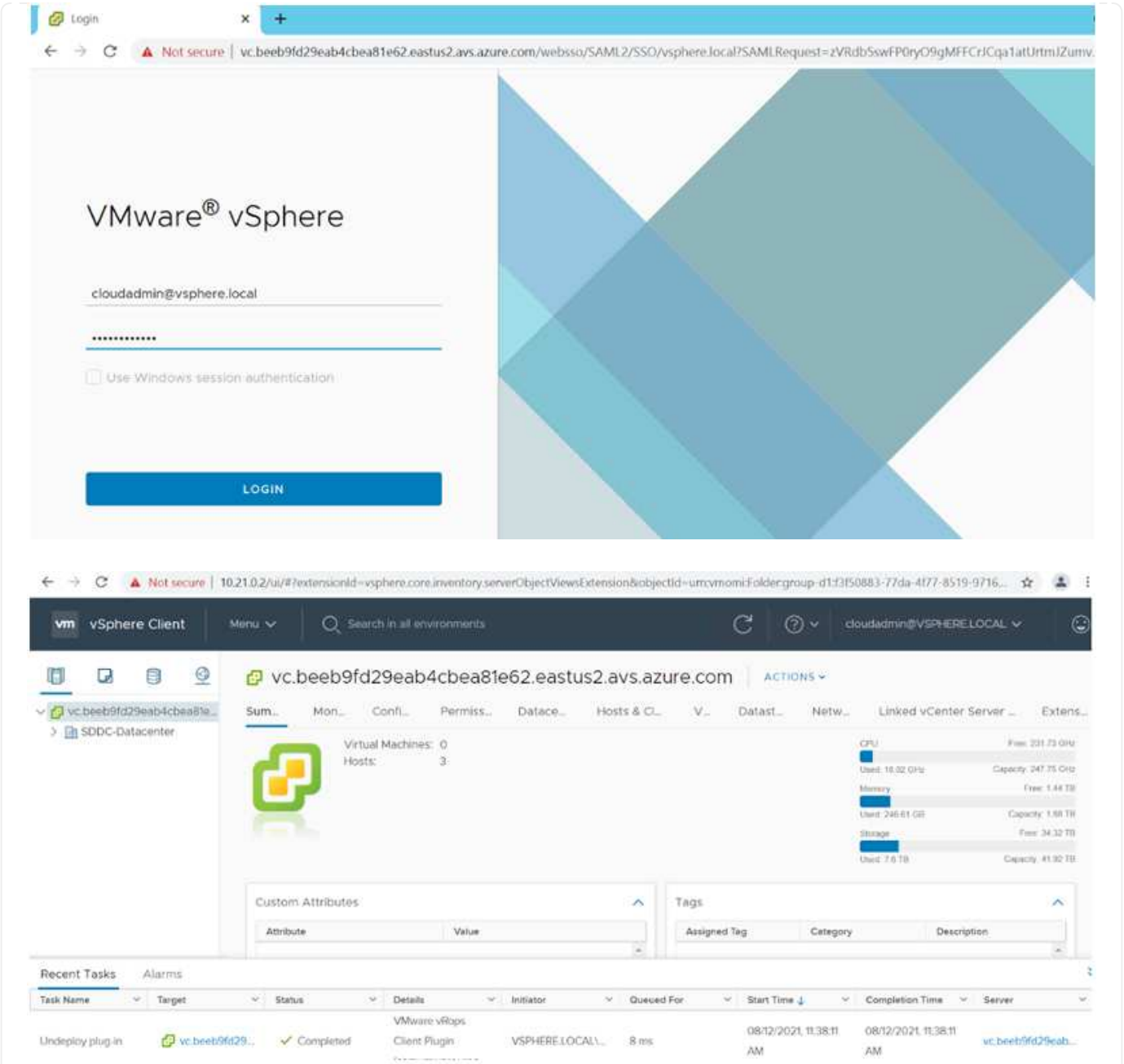


Accedere a vCenter da questa nuova macchina virtuale host jump utilizzando l'utente amministratore cloud . Per accedere alle credenziali, accedere al portale Azure e selezionare Identity (identità) (sotto l'opzione Manage (Gestisci) nel cloud privato). Da qui è possibile copiare gli URL e le credenziali utente per il cloud privato vCenter e NSX-T Manager.



Nella macchina virtuale Windows, aprire un browser e accedere all'URL del client Web vCenter e utilizzare il nome utente admin come **cloudadmin@vsphere.local** e incollare la password copiata. Allo stesso modo, è possibile accedere al gestore NSX-T anche utilizzando l'URL del client Web e utilizzare il nome utente admin e incollare la password copiata per creare nuovi segmenti o modificare i gateway tier esistenti.

Gli URL del client Web sono diversi per ogni SDDC fornito.



Azure VMware Solution SDDC è ora implementato e configurato. Sfrutta ExpressRoute Global Reach per connettere l'ambiente on-premise al cloud privato Azure VMware Solution. Per ulteriori informazioni, vedere "Ambienti on-premise peer per Azure VMware Solution".

Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform (GCP)

Come avviene per le applicazioni on-premise, la pianificazione di Google Cloud VMware Engine (GCVE) è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire GCVE e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Distribuire e configurare GCVE

Per configurare un ambiente GCVE su GCP, accedere alla console GCP e al portale VMware Engine.

Fare clic sul pulsante "New Private Cloud" (nuovo cloud privato) e immettere la configurazione desiderata per il cloud privato GCVE. In "posizione", assicurarsi di implementare il cloud privato nella stessa regione/zona in cui viene implementato CVS/CVO, per garantire le migliori performance e la latenza più bassa.

Prerequisiti:

- Configurare il ruolo IAM di VMware Engine Service Admin
- "Abilitare l'accesso API VMware Engine e la quota del nodo"
- Assicurati che la gamma CIDR non si sovrapponga a nessuna delle tue subnet on-premise o cloud. L'intervallo CIDR deve essere /27 o superiore.

Nota: La creazione di un cloud privato può richiedere da 30 minuti a 2 ore.

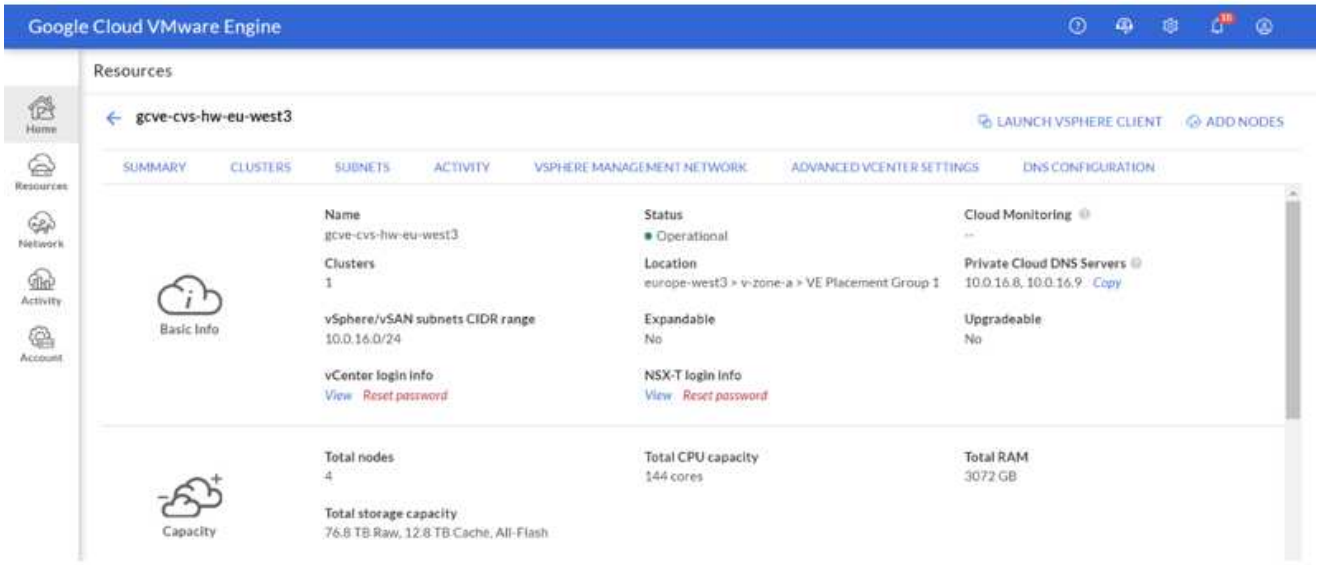
Attiva accesso privato a GCVE

Una volta eseguito il provisioning del cloud privato, configurare l'accesso privato al cloud privato per una connessione con percorso dati a bassa latenza e throughput elevato.

In questo modo, la rete VPC in cui sono in esecuzione le istanze di Cloud Volumes ONTAP sarà in grado di comunicare con il cloud privato GCVE. Per eseguire questa operazione, seguire la "Documentazione GCP". Per il servizio volume cloud, stabilire una connessione tra VMware Engine e Cloud Volumes Service eseguendo un peering una tantum tra i progetti host del tenant. Per informazioni dettagliate, seguire questa procedura "collegamento".

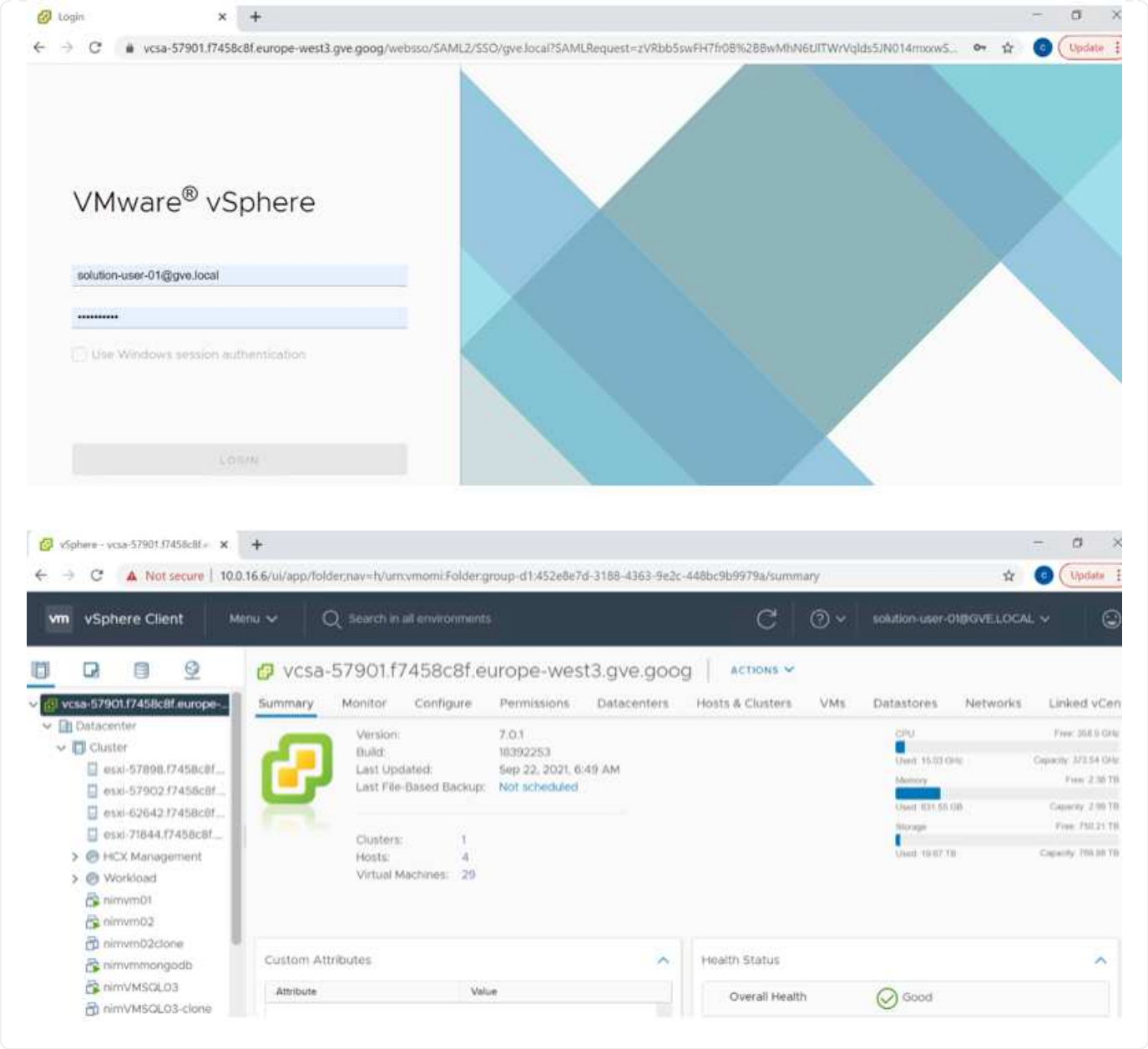
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

Accedere a vcenter utilizzando CloudOwner@gve.local utente. Per accedere alle credenziali, accedere al portale VMware Engine, andare a risorse e selezionare il cloud privato appropriato. Nella sezione Basic info (informazioni di base), fare clic sul collegamento View (Visualizza) per le informazioni di accesso vCenter (vCenter Server, HCX Manager) o NSX-T (NSX Manager).



In una macchina virtuale Windows, aprire un browser e accedere all'URL del client Web vCenter E utilizzare il nome utente admin come CloudOwner@gve.local e incollare la password copiata. Allo stesso modo, è possibile accedere al gestore NSX-T anche utilizzando l'URL del client Web e utilizzare il nome utente admin e incollare la password copiata per creare nuovi segmenti o modificare i gateway tier esistenti.

Per la connessione da una rete on-premise al cloud privato VMware Engine, sfrutta la VPN cloud o l'interconnessione cloud per una connettività appropriata e assicurati che le porte richieste siano aperte. Per informazioni dettagliate, seguire questa procedura "collegamento".



Implementare il datastore supplementare del servizio volume cloud di NetApp in GCVE

Fare riferimento a. "Procedura per implementare un datastore NFS supplementare con CVS NetApp in GCVE"

Opzioni di storage NetApp per i provider di cloud pubblico

Esplora le opzioni per NetApp come storage nei tre principali hyperscaler.

AWS/VMC

AWS supporta lo storage NetApp nelle seguenti configurazioni:

- FSX ONTAP come storage connesso guest
- Cloud Volumes ONTAP (CVO) come storage connesso guest
- FSX ONTAP come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per VMC". Visualizza i dettagli "Opzioni aggiuntive del datastore NFS per VMC".

Azure/AVS

Azure supporta lo storage NetApp nelle seguenti configurazioni:

- Azure NetApp Files (ANF) come storage connesso guest
- Cloud Volumes ONTAP (CVO) come storage connesso guest
- Azure NetApp Files (ANF) come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per AVS". Visualizza i dettagli "Opzioni aggiuntive del datastore NFS per AVS".

GCP/GCVE

Google Cloud supporta lo storage NetApp nelle seguenti configurazioni:

- Cloud Volumes ONTAP (CVO) come storage connesso guest
- Cloud Volumes Service (CVS) come storage connesso al guest
- Cloud Volumes Service (CVS) come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per GCVE".

Scopri di più "Supporto del datastore NetApp Cloud Volumes Service per il motore VMware di Google Cloud (blog NetApp)" oppure "Come utilizzare NetApp CVS come datastore per Google Cloud VMware Engine (Google blog)"

TR-4938: Montare Amazon FSX per ONTAP come datastore NFS con VMware Cloud su AWS

Niyaz Mohamed, NetApp

Introduzione

Ogni organizzazione di successo sta passando per la trasformazione e la modernizzazione. Nell'ambito di questo processo, le aziende utilizzano solitamente i propri investimenti VMware esistenti per sfruttare i vantaggi del cloud e scoprire come migrare, eseguire il burst, estendere e fornire il disaster recovery per i processi nel modo più semplice possibile. I clienti che migrano al cloud devono valutare i casi di utilizzo per flessibilità e burst, uscita dal data center, consolidamento del data center, scenari di fine ciclo di vita, fusioni, acquisizioni e così via.

Anche se VMware Cloud su AWS è l'opzione preferita dalla maggior parte dei clienti perché offre funzionalità ibride uniche a un cliente, opzioni di storage nativo limitate ne hanno limitato l'utilità per le organizzazioni con carichi di lavoro elevati in termini di storage. Poiché lo storage è direttamente legato agli host, l'unico modo per

scalare lo storage è aggiungere più host, che possono aumentare i costi del 35-40% o più per i carichi di lavoro a elevato utilizzo dello storage. Questi carichi di lavoro richiedono storage aggiuntivo e performance separate, non potenza aggiuntiva, ma ciò significa pagare per altri host. È qui che si trova "integrazione recente" Di FSX per ONTAP è utile per i carichi di lavoro con storage e performance intensive con VMware Cloud su AWS.

Consideriamo il seguente scenario: Un cliente richiede otto host per la potenza (vCPU/VMEM), ma ha anche un requisito sostanziale per lo storage. In base alla loro valutazione, sono necessari 16 host per soddisfare i requisiti di storage. Questo aumenta il TCO complessivo perché devono acquistare tutta la potenza aggiuntiva quando è necessario solo uno storage maggiore. Questo è valido per qualsiasi caso di utilizzo, inclusi migrazione, disaster recovery, bursting, sviluppo/test, e così via.

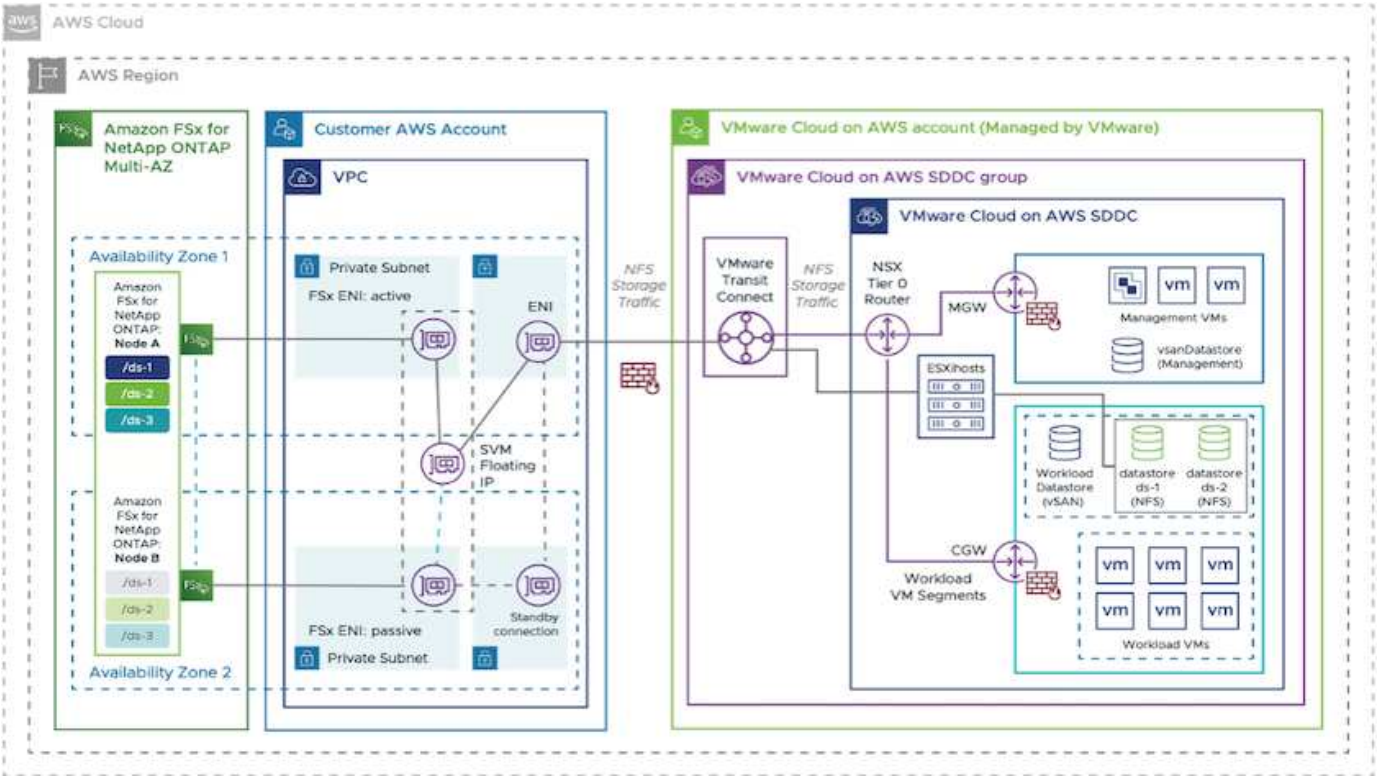
Questo documento illustra i passaggi necessari per il provisioning e l'aggiunta di FSX per ONTAP come datastore NFS per VMware Cloud su AWS.

Questa soluzione è disponibile anche da VMware. Visitare il "Tech zone di VMware Cloud" per ulteriori informazioni.

Opzioni di connettività

VMware Cloud su AWS supporta implementazioni multi-AZ e single-AZ di FSX per ONTAP.

In questa sezione viene descritta l'architettura di connettività di alto livello e le fasi necessarie per implementare la soluzione per espandere lo storage in un cluster SDDC senza la necessità di aggiungere altri host.



Le fasi di implementazione di alto livello sono le seguenti:

1. Creare Amazon FSX per ONTAP in un nuovo VPC designato.

2. Creare un gruppo SDDC.
3. Creare VMware Transit Connect e un allegato TGW.
4. Configurare il routing (AWS VPC e SDDC) e i gruppi di sicurezza.
5. Collegare un volume NFS come datastore al cluster SDDC.

Prima di eseguire il provisioning e collegare FSX per ONTAP come datastore NFS, è necessario configurare un ambiente VMware su cloud SDDC o aggiornare un SDDC esistente alla versione 1.20 o superiore. Per ulteriori informazioni, consultare "Introduzione a VMware Cloud su AWS".

FSX per ONTAP non è attualmente supportato con i cluster estesi.

Conclusione

Questo documento illustra i passaggi necessari per configurare Amazon FSX per ONTAP con VMware cloud su AWS. Amazon FSX per ONTAP offre opzioni eccellenti per implementare e gestire i carichi di lavoro delle applicazioni insieme ai file service, riducendo al contempo il TCO, rendendo i requisiti dei dati perfetti a livello applicativo. Qualunque sia il caso d'utilizzo, scegli VMware Cloud su AWS insieme ad Amazon FSX per ONTAP per ottenere una rapida realizzazione dei vantaggi del cloud, un'infrastruttura coerente e operazioni da on-premise ad AWS, portabilità bidirezionale dei carichi di lavoro e capacità e performance di livello Enterprise. Si tratta degli stessi processi e procedure familiari utilizzati per collegare lo storage. Ricorda che è solo la posizione dei dati che sono stati modificati insieme ai nuovi nomi; i tool e i processi rimangono tutti gli stessi e Amazon FSX per ONTAP aiuta a ottimizzare l'implementazione generale.

Per ulteriori informazioni su questo processo, segui il video dettagliato.

Amazon FSX per ONTAP e il cloud VMware

Opzioni di storage NetApp Guest Connected per AWS

AWS supporta lo storage NetApp connesso agli ospiti con il servizio FSX nativo (FSX ONTAP) o con Cloud Volumes ONTAP (CVO).

ONTAP FSX

Amazon FSX per NetApp ONTAP è un servizio completamente gestito che offre un file storage altamente affidabile, scalabile, dalle performance elevate e ricco di funzionalità, basato sul popolare file system ONTAP di NetApp. FSX per ONTAP combina le funzionalità, le performance, le funzionalità e le operazioni API dei file system NetApp con l'agilità, la scalabilità e la semplicità di un servizio AWS completamente gestito.

FSX per ONTAP offre uno storage di file condiviso ricco di funzionalità, rapido e flessibile, ampiamente accessibile dalle istanze di calcolo Linux, Windows e macOS eseguite in AWS o on-premise. FSX per ONTAP offre storage a stato solido (SSD) dalle performance elevate con latenze sotto al millisecondo. Con FSX per ONTAP, puoi ottenere livelli di performance SSD per il tuo carico di lavoro pagando allo stesso tempo lo storage SSD per una piccola frazione dei tuoi dati.

La gestione dei dati con FSX per ONTAP è più semplice perché puoi creare snapshot, clonare e replicare i file con un semplice clic. Inoltre, FSX per ONTAP esegue automaticamente il Tier dei dati per uno storage elastico e a basso costo, riducendo la necessità di eseguire il provisioning o la gestione della capacità.

FSX per ONTAP offre inoltre storage altamente disponibile e durevole con backup completamente gestiti e supporto per il disaster recovery multiregione. Per semplificare la protezione e la protezione dei dati, FSX per ONTAP supporta le applicazioni antivirus e di sicurezza dei dati più diffuse.

FSX ONTAP come storage connesso guest

Configurare Amazon FSX per NetApp ONTAP con VMware Cloud su AWS

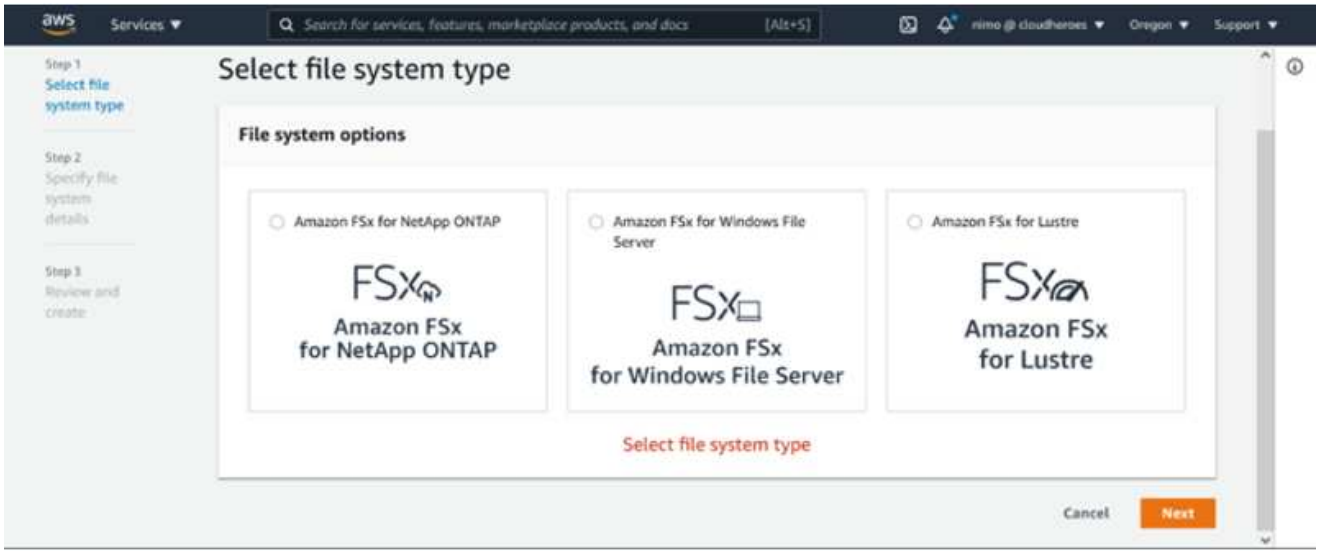
Le condivisioni e le LUN dei file ONTAP di Amazon FSX per NetApp possono essere montate da macchine virtuali create nell'ambiente SDDC di VMware presso AWS. I volumi possono anche essere montati sul client Linux e mappati sul client Windows utilizzando il protocollo NFS o SMB, mentre I LUN possono essere utilizzati sui client Linux o Windows come dispositivi a blocchi se montati su iSCSI. Amazon FSX per il file system NetApp ONTAP può essere configurato rapidamente con i seguenti passaggi.

Amazon FSX per NetApp ONTAP e VMware Cloud su AWS devono trovarsi nella stessa zona di disponibilità per ottenere performance migliori ed evitare i costi di trasferimento dei dati tra le zone di disponibilità.

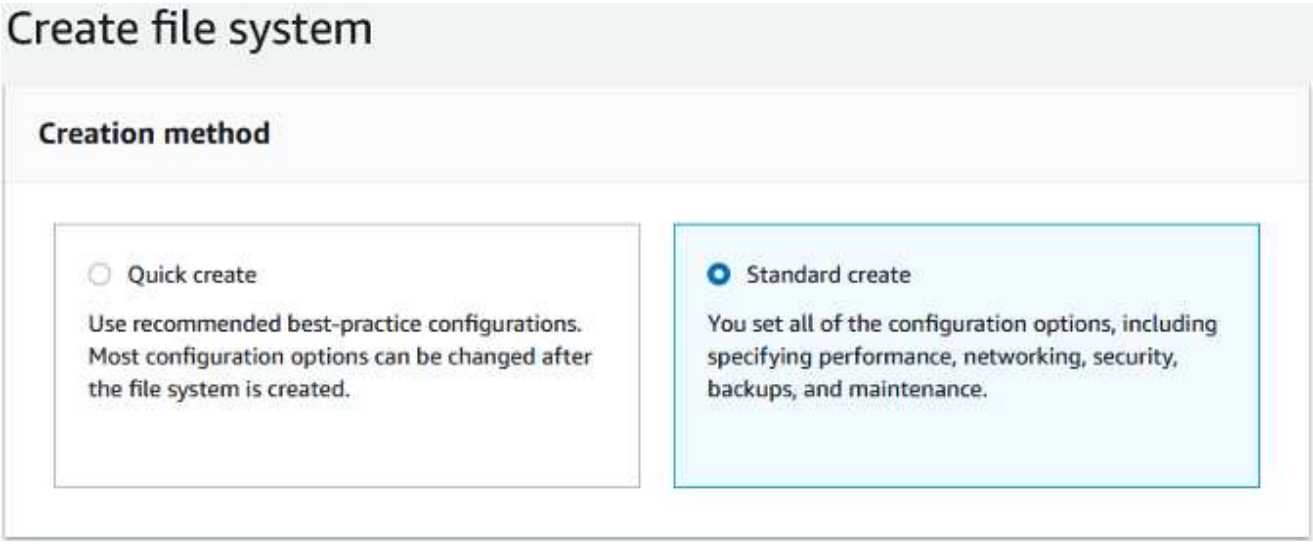
Creare e montare Amazon FSX per ONTAP Volumes

Per creare e montare il file system Amazon FSX per NetApp ONTAP, attenersi alla seguente procedura:

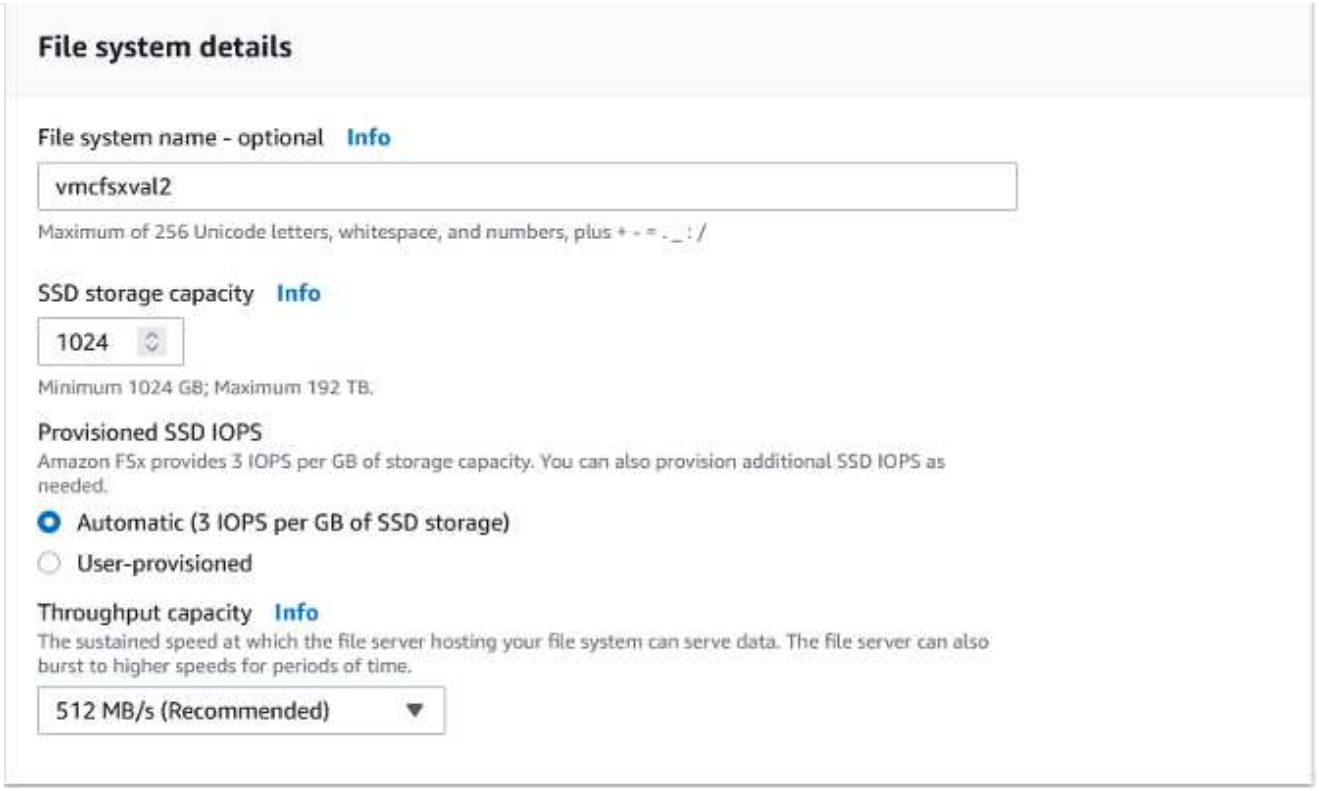
1. Aprire "Console Amazon FSX" E scegliere Create file system (Crea file system) per avviare la creazione guidata del file system.
2. Nella pagina Seleziona tipo di file system, scegliere Amazon FSX per NetApp ONTAP, quindi Avanti. Viene visualizzata la pagina Create file System (Crea file system).



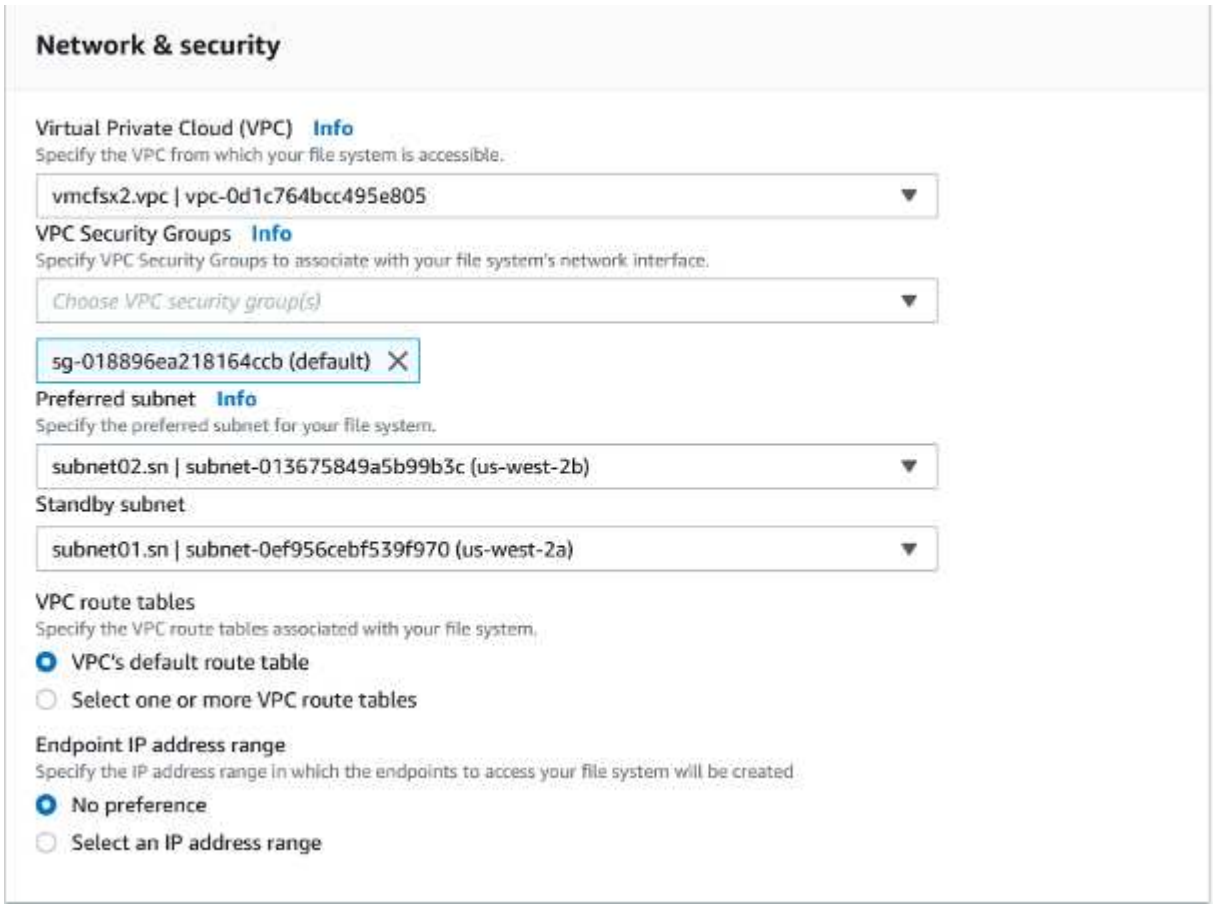
1. Nella sezione rete, per Virtual Private Cloud (VPC), scegliere le subnet VPC e preferite appropriate insieme alla tabella di routing. In questo caso, vmcfsx2.vpc viene selezionato dal menu a discesa.



1. Per il metodo di creazione, scegliere Standard Create (Crea standard). È anche possibile scegliere creazione rapida, ma questo documento utilizza l'opzione di creazione standard.

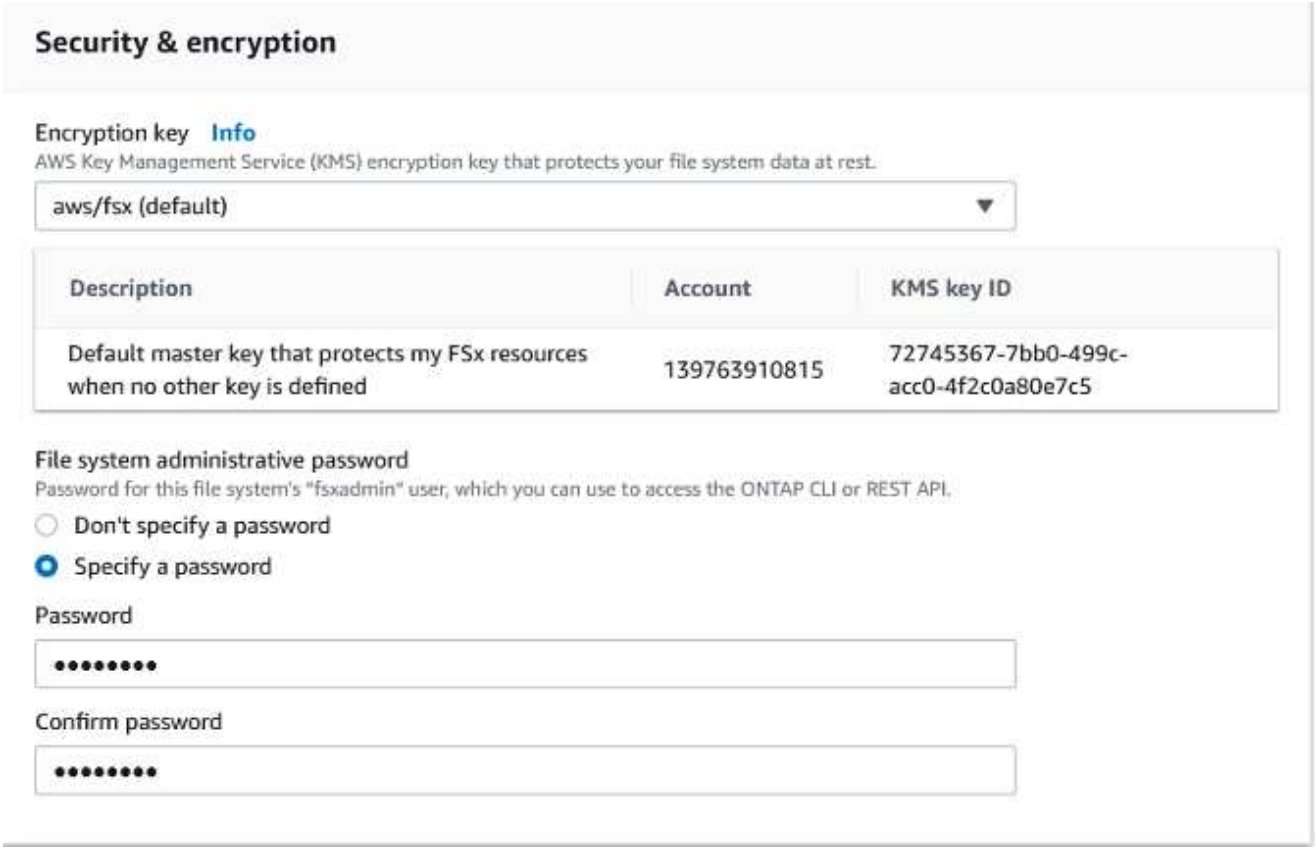


1. Nella sezione rete, per Virtual Private Cloud (VPC), scegliere le subnet VPC e preferite appropriate insieme alla tabella di routing. In questo caso, vmcfsx2.vpc viene selezionato dal menu a discesa.

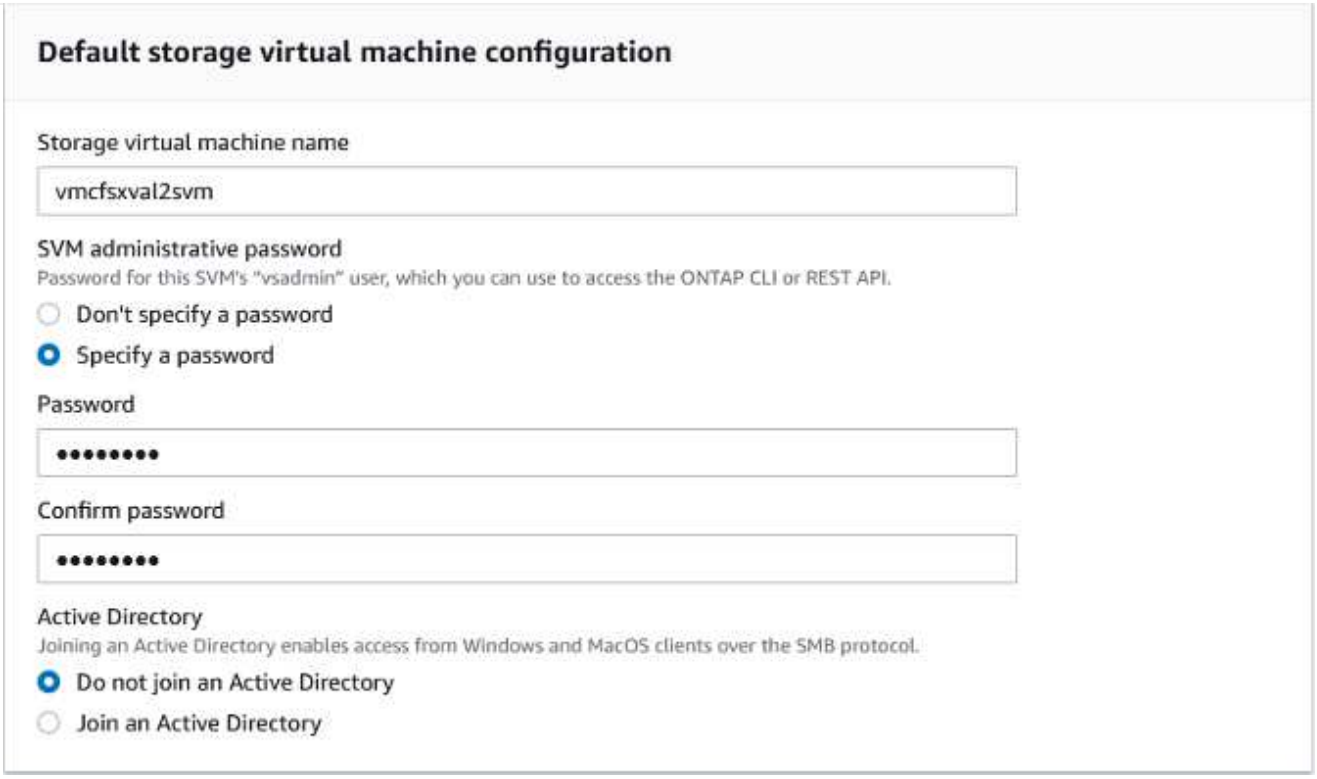


Nella sezione rete, per Virtual Private Cloud (VPC), scegliere le subnet VPC e preferite appropriate insieme alla tabella di routing. In questo caso, vmcfsx2.vpc viene selezionato dal menu a discesa.

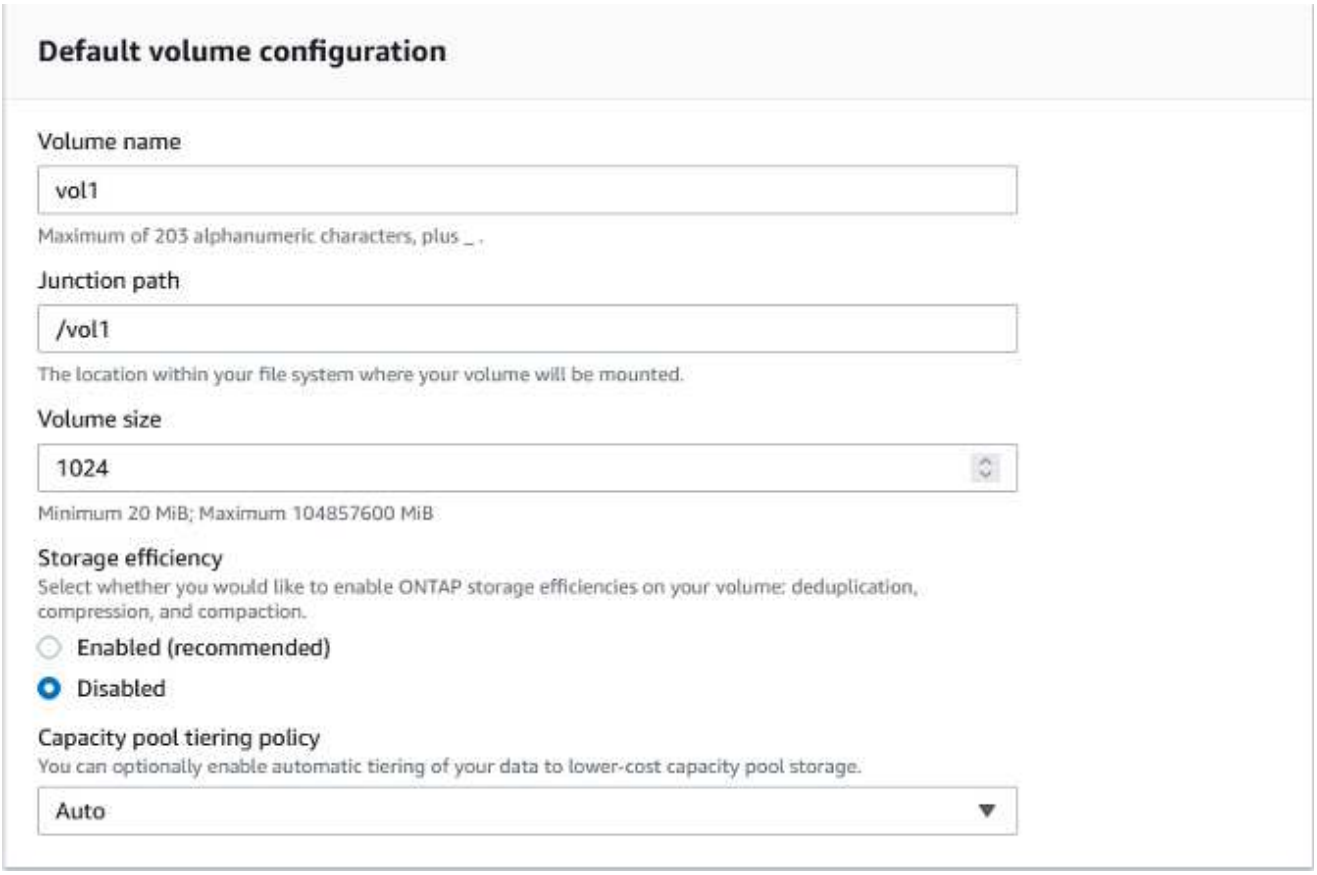
1. Nella sezione Security & Encryption (sicurezza e crittografia), per la chiave di crittografia, scegliere la chiave di crittografia AWS Key Management Service (AWS KMS) che protegge i dati del file system inattivi. Per la password amministrativa del file system, immettere una password sicura per l'utente fsxadmin.



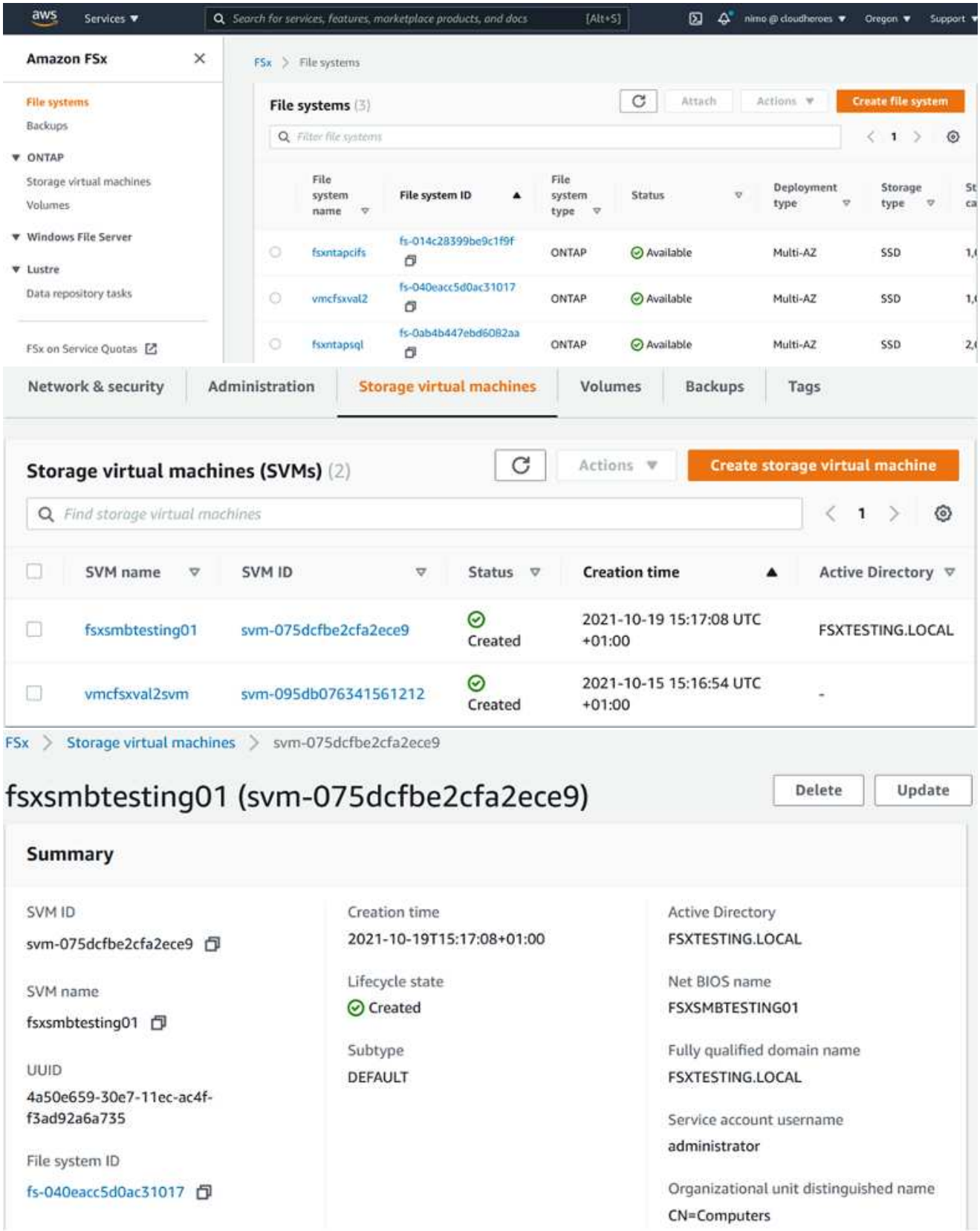
1. Nella macchina virtuale e specificare la password da utilizzare con vsadmin per l'amministrazione di ONTAP utilizzando API REST o CLI. Se non viene specificata alcuna password, è possibile utilizzare un utente fsxadmin per amministrare la SVM. Nella sezione Active Directory, assicurarsi di aggiungere Active Directory a SVM per il provisioning delle condivisioni SMB. Nella sezione Default Storage Virtual Machine Configuration (Configurazione macchina virtuale dello storage predefinita), specificare un nome per lo storage in questa convalida. Il provisioning delle condivisioni SMB viene eseguito utilizzando un dominio Active Directory autogestato.



1. Nella sezione Default Volume Configuration (Configurazione volume predefinita), specificare il nome e le dimensioni del volume. Si tratta di un volume NFS. Per l'efficienza dello storage, scegliere Enabled (attivato) per attivare le funzioni di efficienza dello storage ONTAP (compressione, deduplica e compattazione) o Disabled (Disattivato) per disattivarle.



1. Esaminare la configurazione del file system mostrata nella pagina Create file System (Crea file system).
2. Fare clic su Crea file system.



Per ulteriori informazioni, vedere "Introduzione a Amazon FSX per NetApp ONTAP".

Dopo aver creato il file system come sopra, creare il volume con le dimensioni e il protocollo richiesti.

1. Aprire "Console Amazon FSX".
2. Nel riquadro di spostamento di sinistra, scegliere file system, quindi scegliere il file system ONTAP per cui si desidera creare un volume.
3. Selezionare la scheda Volumes (volumi).
4. Selezionare la scheda Create Volume (Crea volume).
5. Viene visualizzata la finestra di dialogo Create Volume (Crea volume).

A scopo dimostrativo, in questa sezione viene creato un volume NFS che può essere facilmente montato sulle macchine virtuali in esecuzione sul cloud VMware su AWS. nfsdemovol01 viene creato come illustrato di seguito:

Montare il volume FSX ONTAP sul client Linux

Per montare il volume FSX ONTAP creato nel passaggio precedente. Dalle macchine virtuali Linux all'interno di VMC su AWS SDDC, completare i seguenti passaggi:

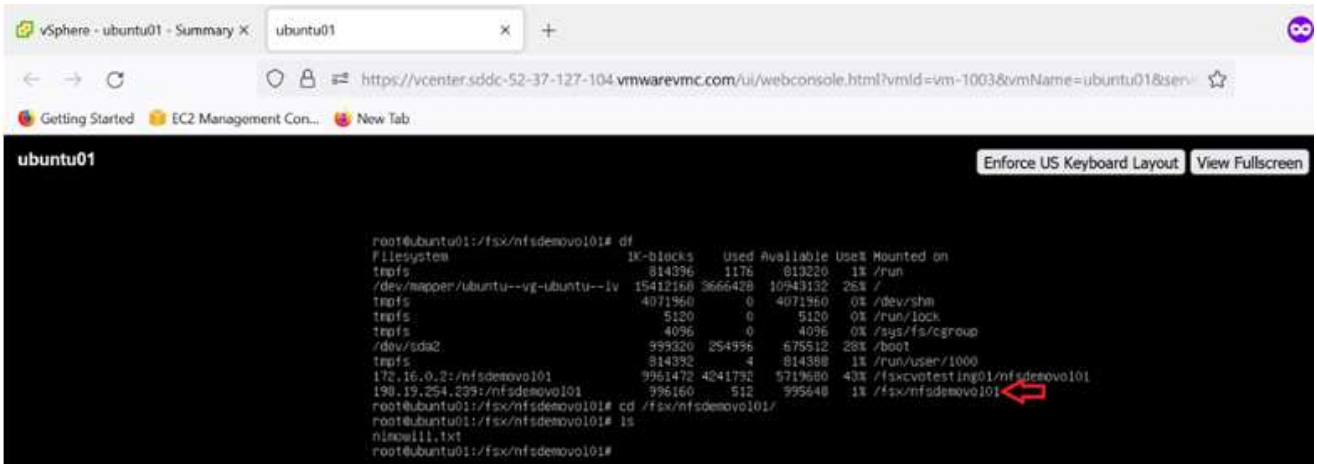
1. Connettersi all'istanza Linux designata.
2. Aprire un terminale sull'istanza utilizzando Secure Shell (SSH) e accedere con le credenziali appropriate.
3. Creare una directory per il punto di montaggio del volume con il seguente comando:

```
 $ sudo mkdir /fsx/nfsdemovol01
. Montare il volume NFS Amazon FSX per NetApp ONTAP nella directory
creata nel passaggio precedente.
```

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

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

1. Una volta eseguito, eseguire il comando df per convalidare il mount.



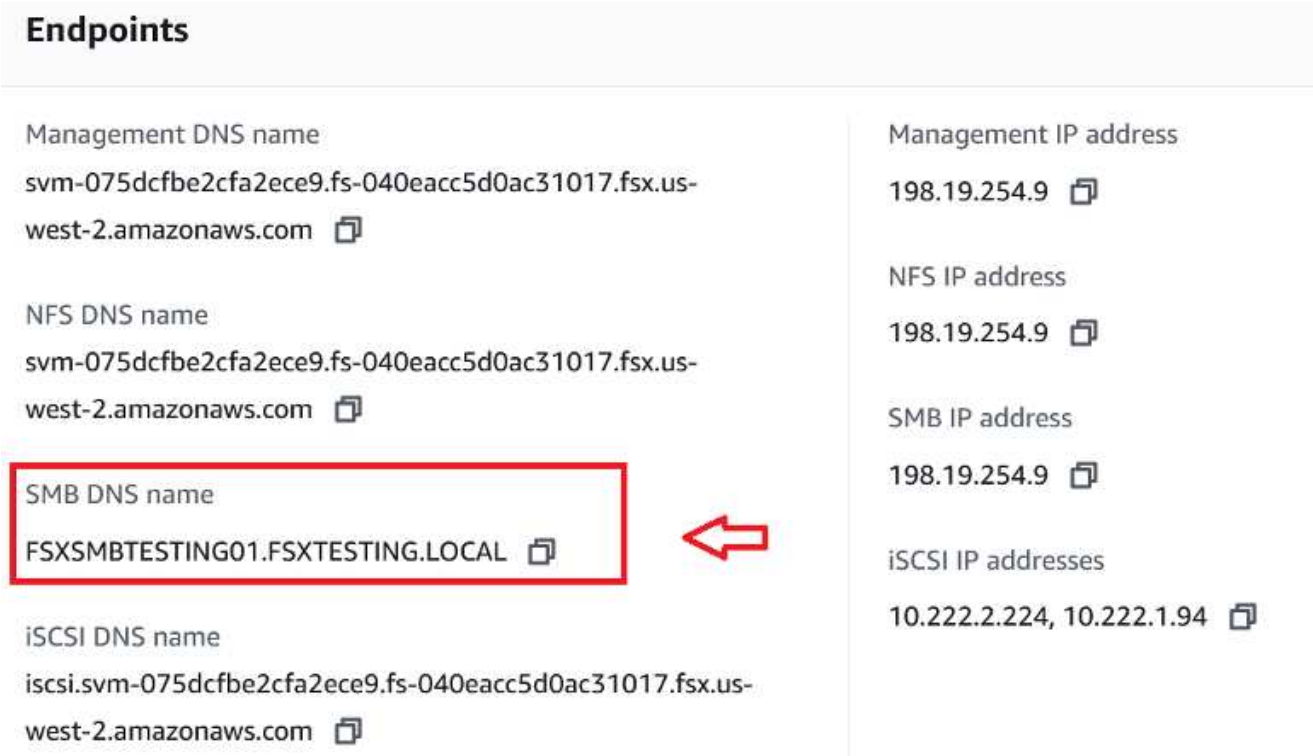
Montare il volume FSX ONTAP sul client Linux

Collegare i volumi FSX ONTAP ai client Microsoft Windows

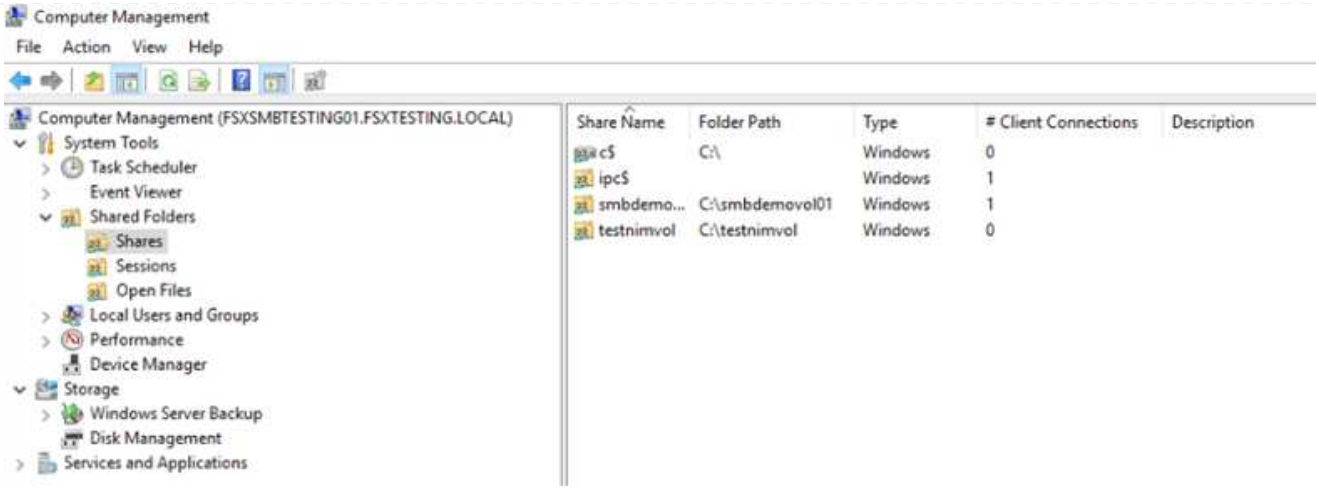
Per gestire e mappare le condivisioni di file su un file system Amazon FSX, è necessario utilizzare la GUI delle cartelle condivise.

1. Aprire il menu Start ed eseguire fsmgmt.msc utilizzando Esegui come amministratore. In questo modo si apre la GUI delle cartelle condivise.
2. Fare clic su azione > tutte le attività e scegliere Connetti a un altro computer.
3. Per un altro computer, immettere il nome DNS della macchina virtuale di storage (SVM). Ad esempio, in questo esempio viene utilizzato FSXSMBTESTING01.FSXTESTING.LOCAL.

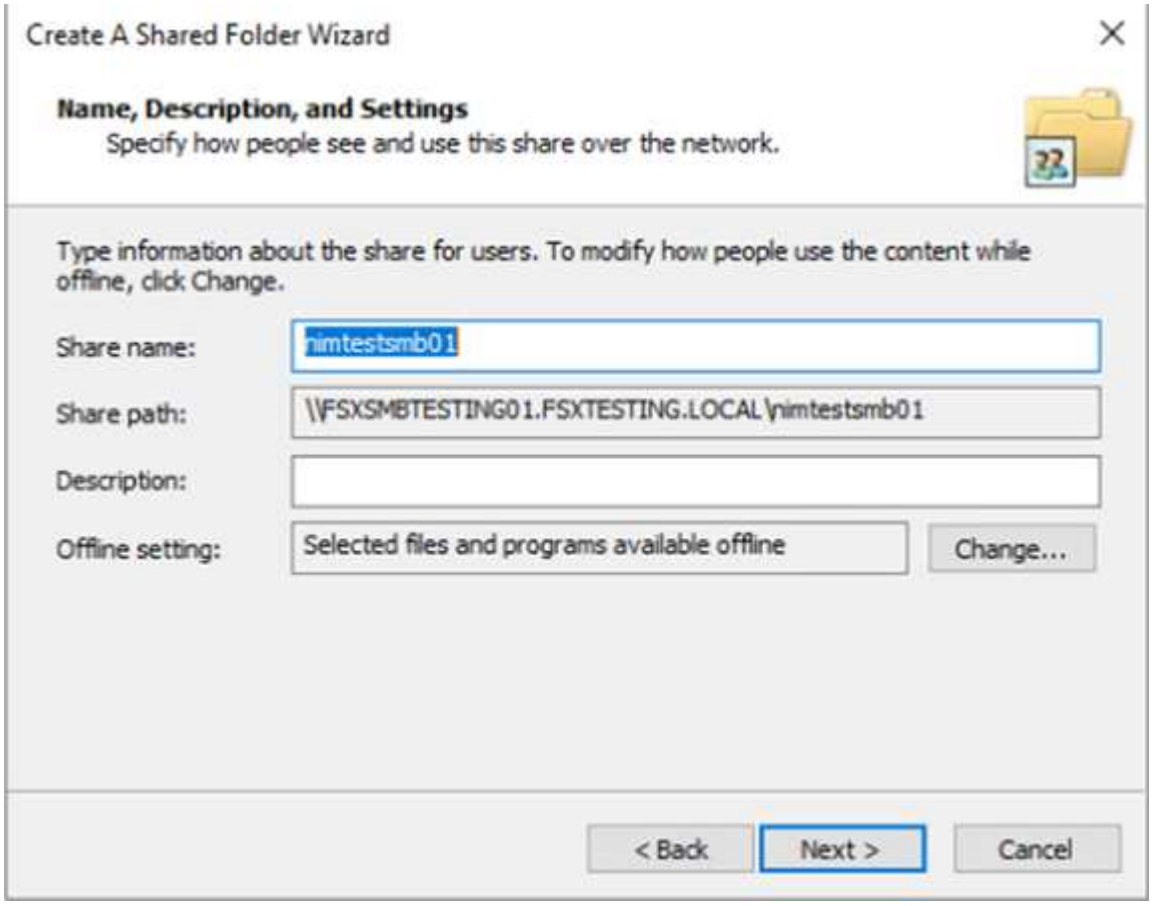
TP individuare il nome DNS della SVM sulla console Amazon FSX, scegliere Storage Virtual Machines, SVM, quindi scorrere verso il basso fino agli endpoint per trovare il nome DNS SMB. Fare clic su OK. Il file system Amazon FSX viene visualizzato nell'elenco delle cartelle condivise.



1. Nello strumento cartelle condivise, scegliere condivisioni nel riquadro sinistro per visualizzare le condivisioni attive per il file system Amazon FSX.

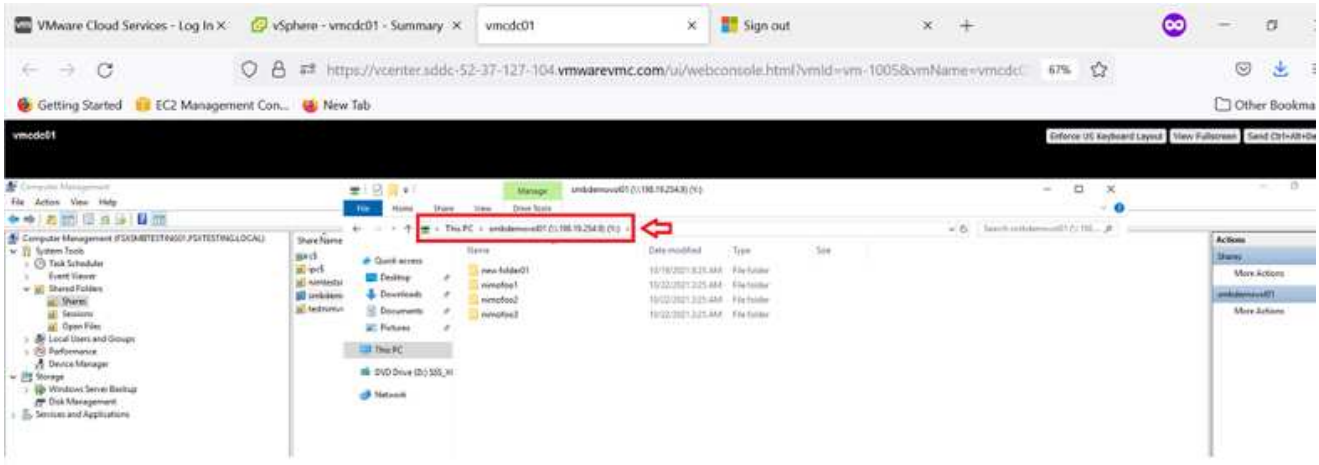


1. A questo punto, scegliere una nuova condivisione e completare la procedura guidata Crea una cartella condivisa.



Per ulteriori informazioni sulla creazione e la gestione delle condivisioni SMB su un file system Amazon FSX, consulta "Creazione di condivisioni SMB".

1. Dopo aver attivato la connettività, è possibile collegare e utilizzare la condivisione SMB per i dati delle applicazioni. A tale scopo, copiare il percorso di condivisione e utilizzare l'opzione Map Network Drive (Mappa unità di rete) per montare il volume sulla macchina virtuale in esecuzione su VMware Cloud su AWS SDDC.



Connessione di un LUN FSX per NetApp ONTAP a un host utilizzando iSCSI

Connessione di un LUN FSX per NetApp ONTAP a un host utilizzando iSCSI

Il traffico iSCSI per FSX attraversa VMware Transit Connect/AWS Transit Gateway attraverso i percorsi forniti nella sezione precedente. Per configurare un LUN in Amazon FSX per NetApp ONTAP, seguire la documentazione disponibile "qui".

Sui client Linux, assicurarsi che il daemon iSCSI sia in esecuzione. Una volta eseguito il provisioning dei LUN, consultare le istruzioni dettagliate sulla configurazione iSCSI con Ubuntu (come esempio) "qui".

In questo documento, viene illustrata la connessione del LUN iSCSI a un host Windows:

Provisioning di un LUN in FSX per NetApp ONTAP:

1. Accedere alla CLI di NetApp ONTAP utilizzando la porta di gestione di FSX per il file system ONTAP.
2. Creare le LUN con le dimensioni richieste, come indicato dall'output di dimensionamento.

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

In questo esempio, è stato creato un LUN di dimensioni 5g (5368709120).

1. Creare gli igroups necessari per controllare quali host hanno accesso a LUN specifiche.

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

FsxId040eacc5d0ac31017::> igroup show

Vserver   Igroup       Protocol OS Type  Initiators

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

vmcfsxval2svm

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

vmcfsxval2svm

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

Sono state visualizzate due voci.

1. Associare i LUN a igroups utilizzando il seguente comando:

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

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

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

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

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

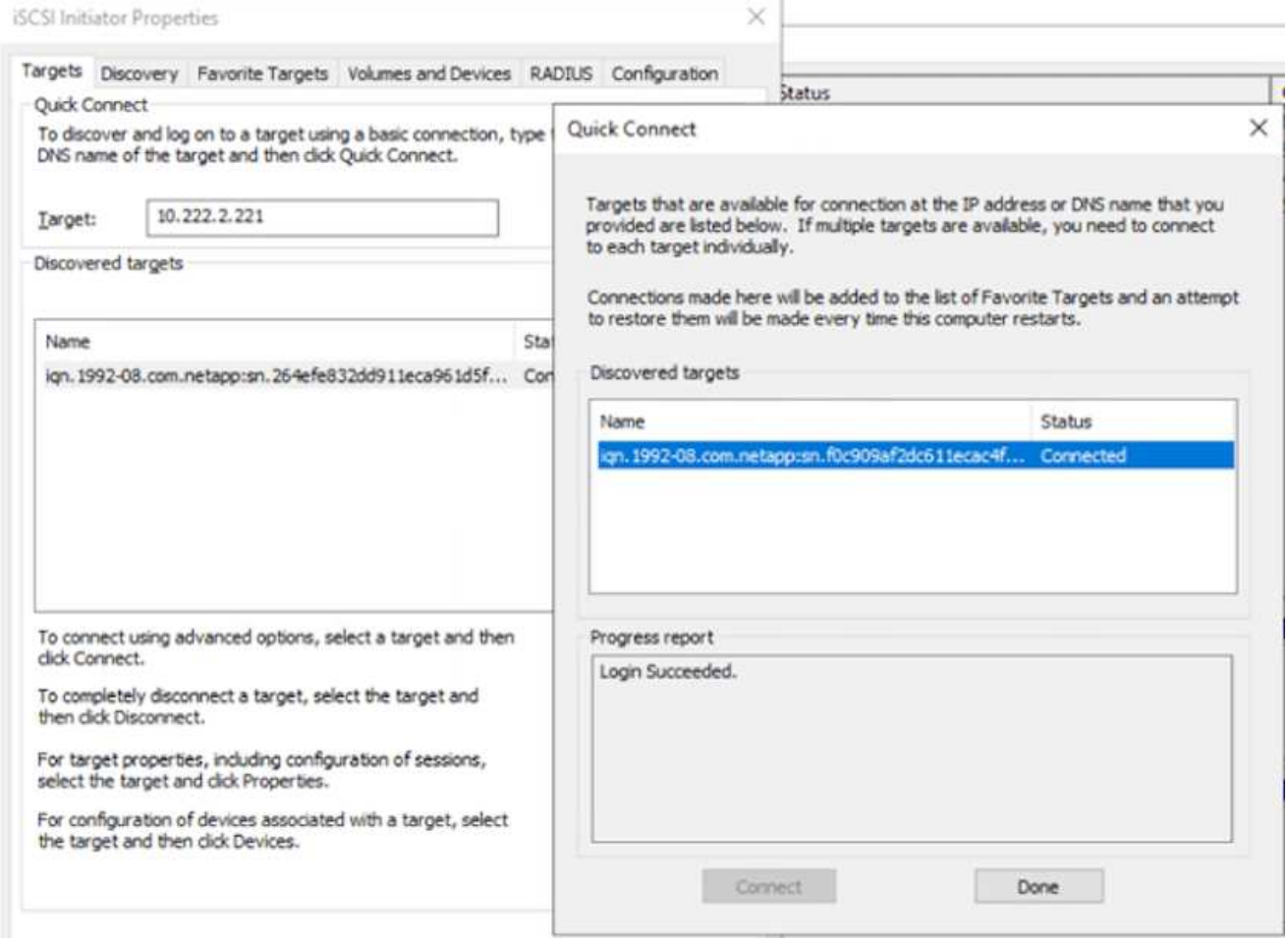
Sono state visualizzate due voci.

1. Connettere il LUN appena fornito a una macchina virtuale Windows:

Per collegare il nuovo LUN a un host Windows che risiede sul cloud VMware su AWS SDDC, attenersi alla seguente procedura:

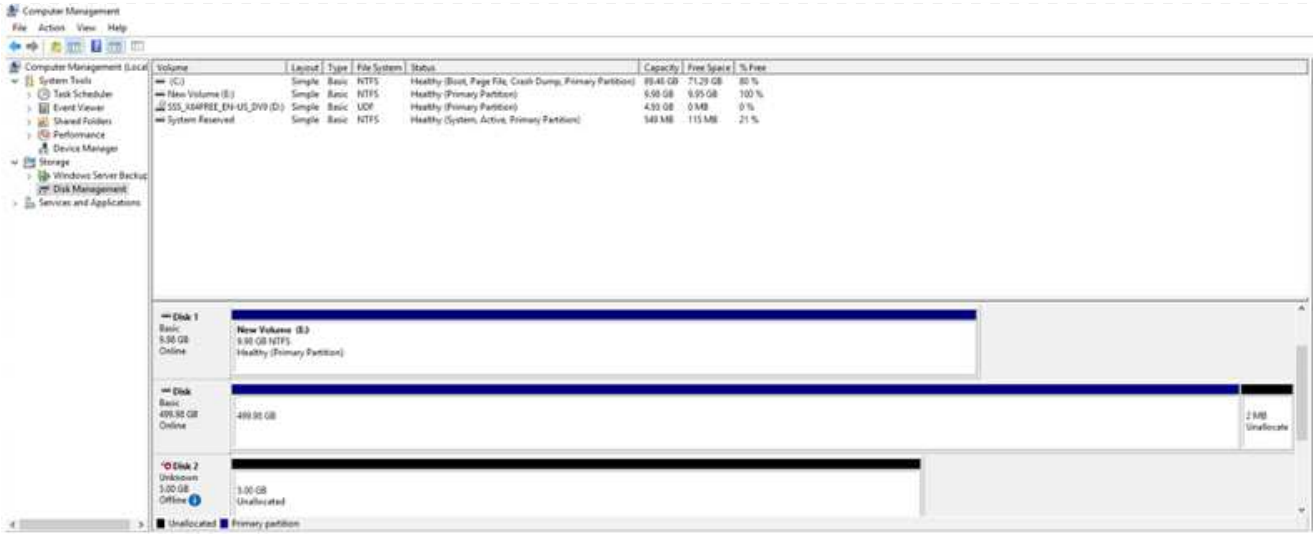
1. RDP sulla macchina virtuale Windows ospitata su VMware Cloud su AWS SDDC.
2. Accedere a Server Manager > Dashboard > Tools > iSCSI Initiator per aprire la finestra di dialogo iSCSI Initiator Properties (Proprietà iSCSI Initiator).
3. Dalla scheda Discovery (rilevamento), fare clic su Discover Portal (Scopri portale) o Add Portal (Aggiungi portale), quindi inserire l'indirizzo IP della porta di destinazione iSCSI.
4. Dalla scheda Target, selezionare la destinazione rilevata, quindi fare clic su Log on (Accedi) o Connect (Connetti).
5. Selezionare attiva multipath, quindi selezionare "Ripristina automaticamente la connessione all'avvio del computer" o "Aggiungi questa connessione all'elenco delle destinazioni preferite". Fare clic su Avanzate.

> L'host Windows deve disporre di una connessione iSCSI a ciascun nodo del cluster. Il DSM nativo seleziona i percorsi migliori da utilizzare.



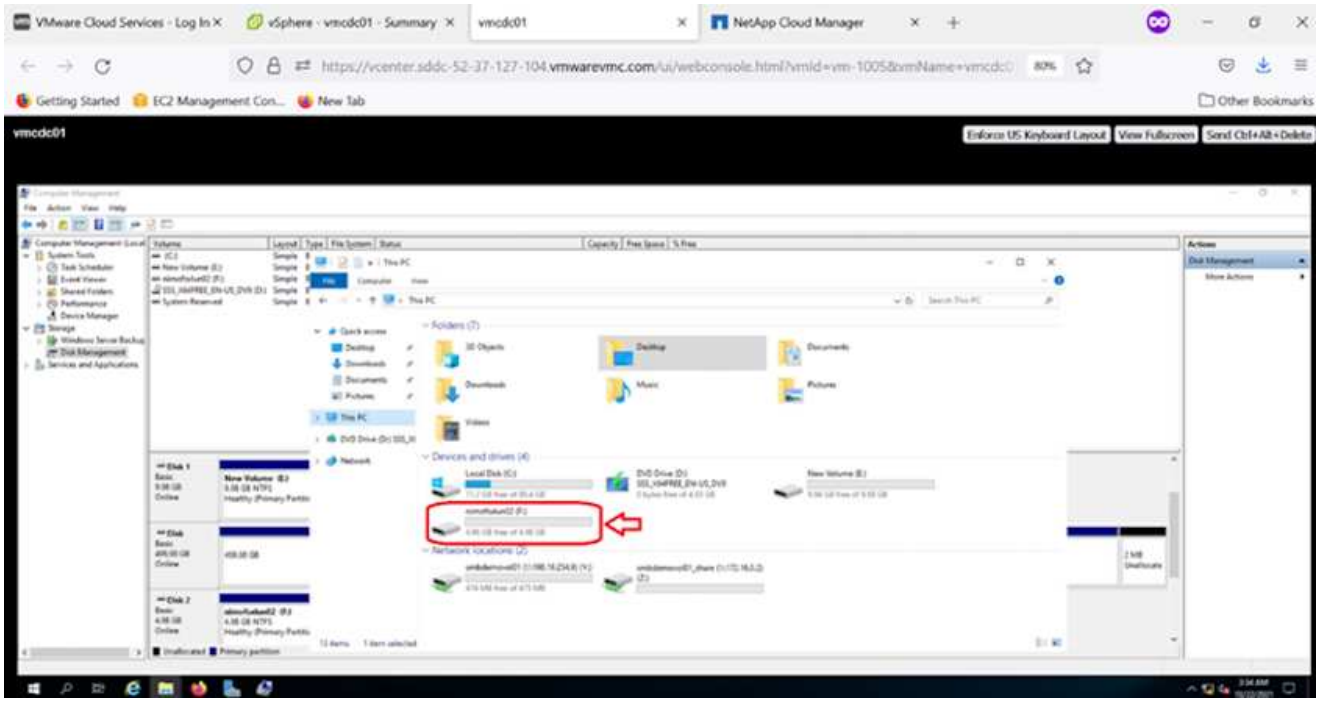
I LUN sulla macchina virtuale di storage (SVM) vengono visualizzati come dischi sull'host Windows. I nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Attivare una nuova scansione manuale per rilevare i dischi completando la seguente procedura:

1. Aprire l'utility Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
2. Espandere il nodo Storage nella struttura di navigazione.
3. Fare clic su Gestione disco.
4. Fare clic su Action (azione) > Rescan Disks (Nuova scansione



Quando l'host Windows accede per la prima volta a un nuovo LUN, non dispone di partizione o file system. Inizializzare il LUN e, facoltativamente, formattare il LUN con un file system attenendosi alla seguente procedura:

1. Avviare Gestione disco di Windows.
2. Fare clic con il pulsante destro del mouse sul LUN, quindi selezionare il tipo di disco o partizione richiesto.
3. Seguire le istruzioni della procedura guidata. In questo esempio, viene montato il disco F:.



Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, o CVO, è la soluzione per la gestione dei dati nel cloud leader del settore basata sul software di storage ONTAP, disponibile in modalità nativa su Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

Si tratta di una versione software-defined di ONTAP che utilizza lo storage nativo del cloud, consentendoti di avere lo stesso software di storage nel cloud e on-premise, riducendo la necessità di riorganizzare il tuo staff IT con metodi completamente nuovi per gestire i tuoi dati.

CVO offre ai clienti la possibilità di spostare senza problemi i dati dall'edge al data center, al cloud e viceversa, unendo il tuo cloud ibrido, il tutto gestito con una console di gestione a singolo pannello, NetApp Cloud Manager.

Per progettazione, CVO offre performance estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud

Cloud Volumes ONTAP (CVO) come storage connesso guest

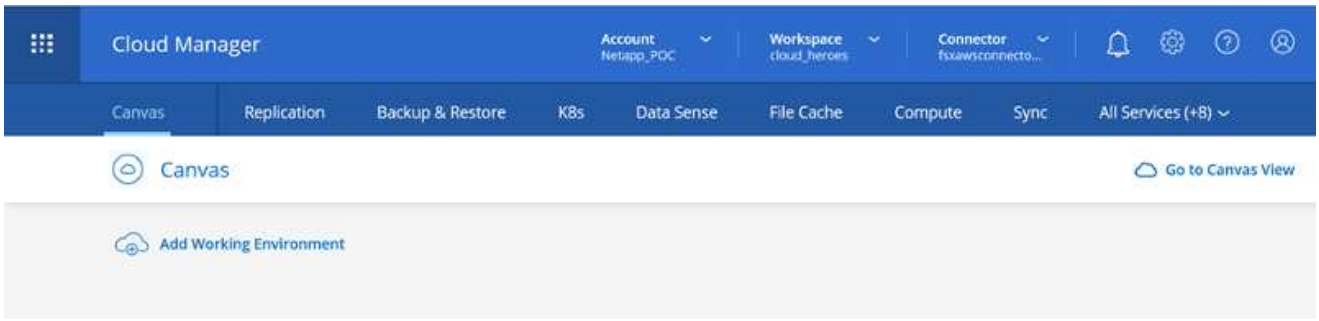
Implementare la nuova istanza di Cloud Volumes ONTAP in AWS (eseguire l'operazione autonomamente)

Le condivisioni e i LUN Cloud Volumes ONTAP possono essere montati dalle macchine virtuali create nell'ambiente SDDC di VMware Cloud su AWS. I volumi possono essere montati anche su client Windows nativi di AWS VM e I LUN possono essere utilizzati su client Linux o Windows come dispositivi a blocchi quando montati su iSCSI perché Cloud Volumes ONTAP supporta i protocolli iSCSI, SMB e NFS. I volumi Cloud Volumes ONTAP possono essere configurati in pochi semplici passaggi.

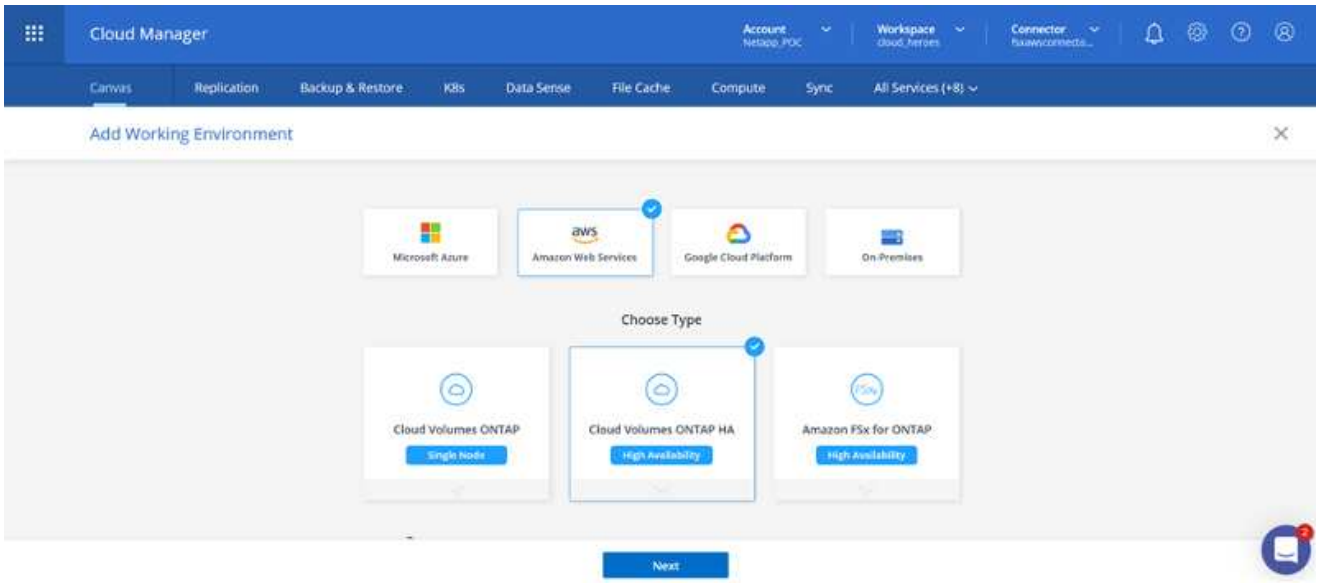
Per replicare i volumi da un ambiente on-premise al cloud per scopi di disaster recovery o migrazione, stabilire la connettività di rete ad AWS, utilizzando una VPN sito-sito o DirectConnect. La replica dei dati da on-premise a Cloud Volumes ONTAP non rientra nell'ambito di questo documento. Per replicare i dati tra sistemi on-premise e Cloud Volumes ONTAP, vedere "Configurazione della replica dei dati tra sistemi".

Utilizzare "Cloud Volumes ONTAP Sizer" Per dimensionare con precisione le istanze di Cloud Volumes ONTAP. Inoltre, è possibile monitorare le performance on-premise da utilizzare come input nel Cloud Volumes ONTAP Sizer.

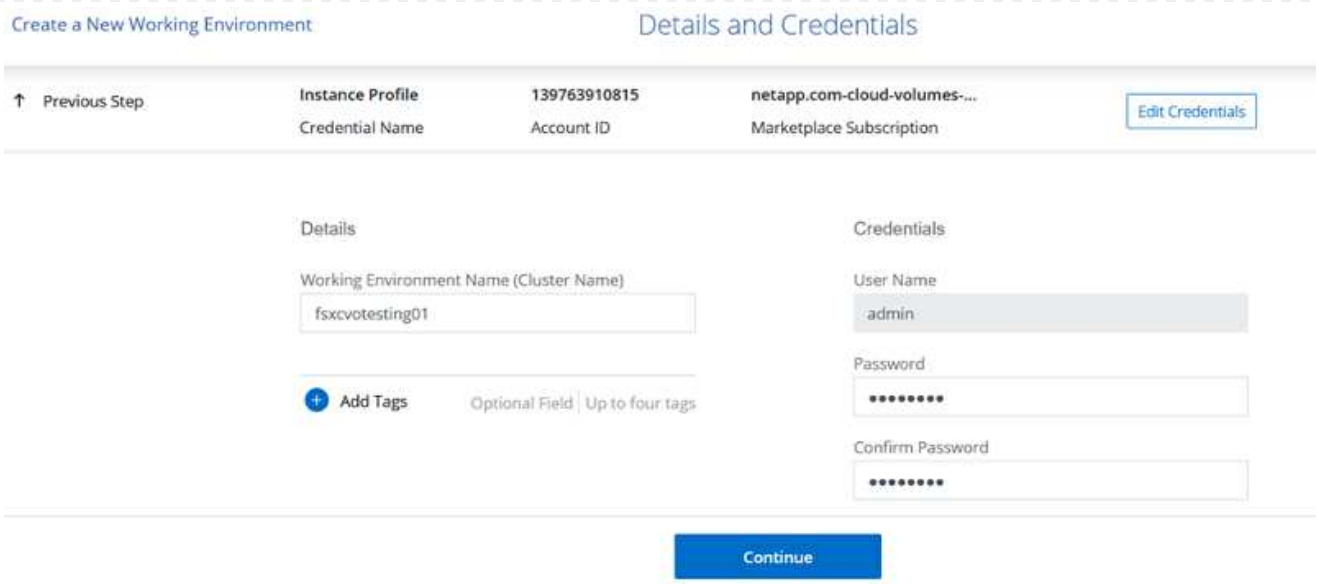
1. Accedere a NetApp Cloud Central; viene visualizzata la schermata Fabric View. Individuare la scheda Cloud Volumes ONTAP (Gestione cloud) e selezionare Go to Cloud Manager (Vai a Gestione cloud). Una volta effettuato l'accesso, viene visualizzata la schermata Canvas.



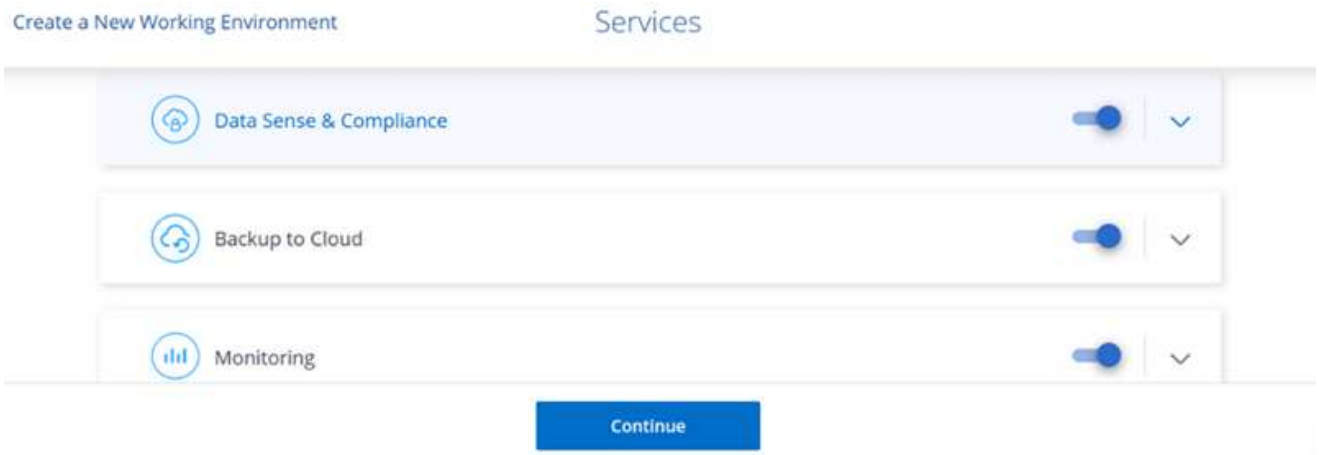
1. Nella home page di Cloud Manager, fare clic su Add a Working Environment (Aggiungi ambiente di lavoro), quindi selezionare AWS come cloud e il tipo di configurazione del sistema.



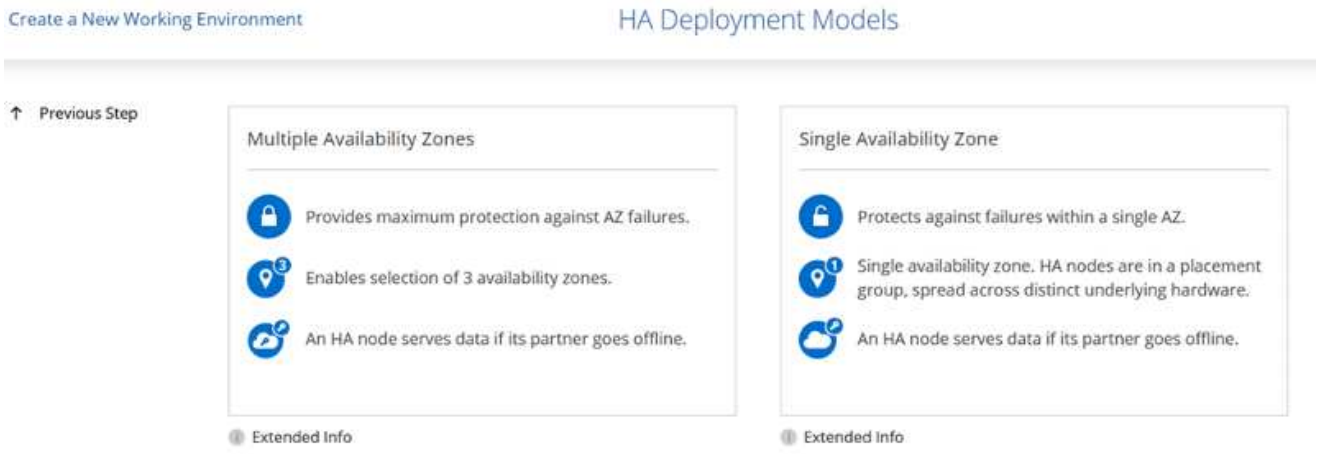
1. Fornire i dettagli dell'ambiente da creare, inclusi il nome dell'ambiente e le credenziali di amministratore. Fare clic su continua.



1. Seleziona i servizi add-on per l'implementazione di Cloud Volumes ONTAP, inclusi classificazione BlueXP, backup e recovery di BlueXP e Cloud Insights. Fare clic su continua.

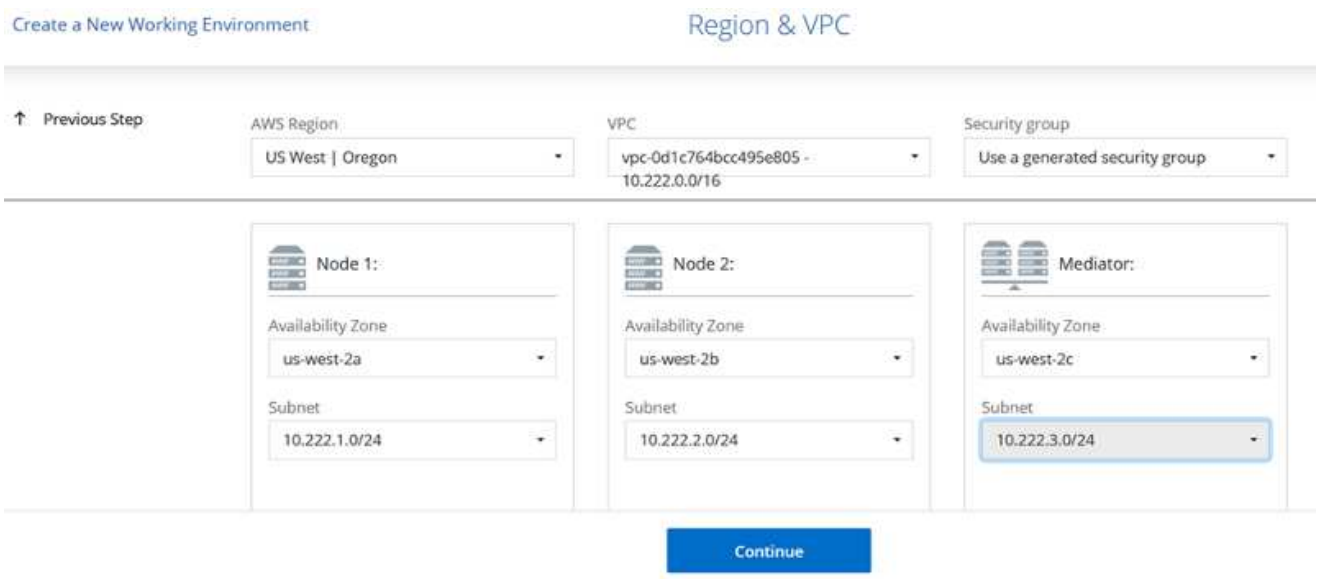


1. Nella pagina ha Deployment Models (modelli di implementazione ha), scegliere la configurazione di più zone di disponibilità.

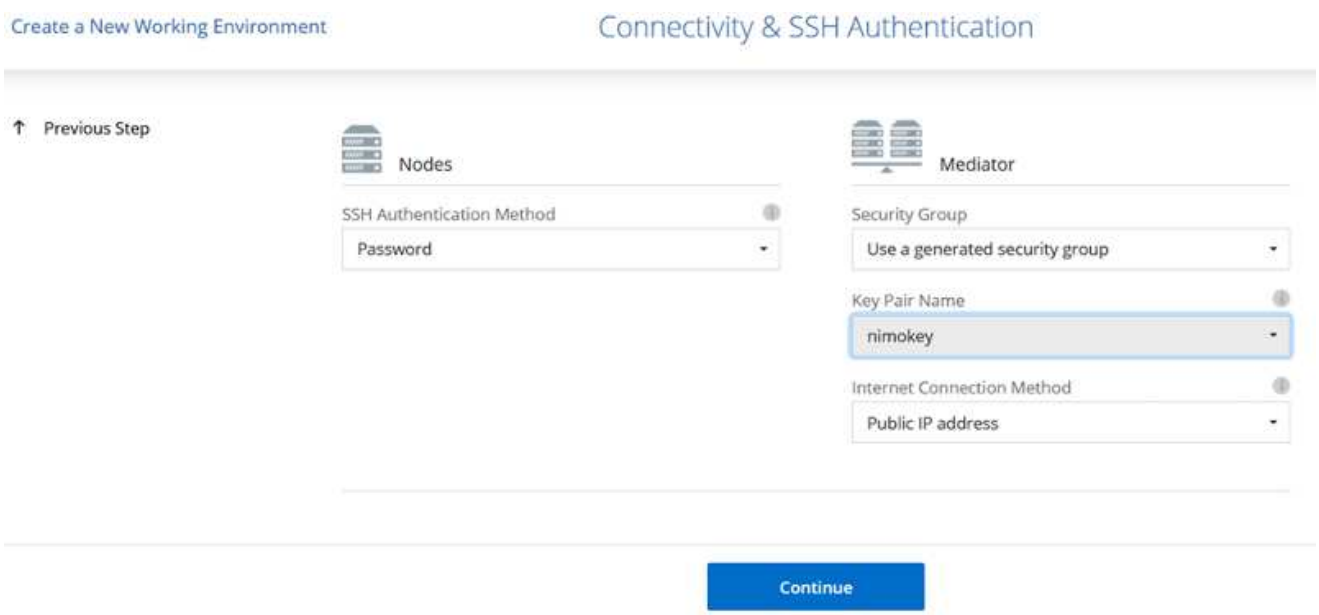


1. Nella pagina Region & VPC (Regione e VPC), immettere le informazioni di rete, quindi fare clic su

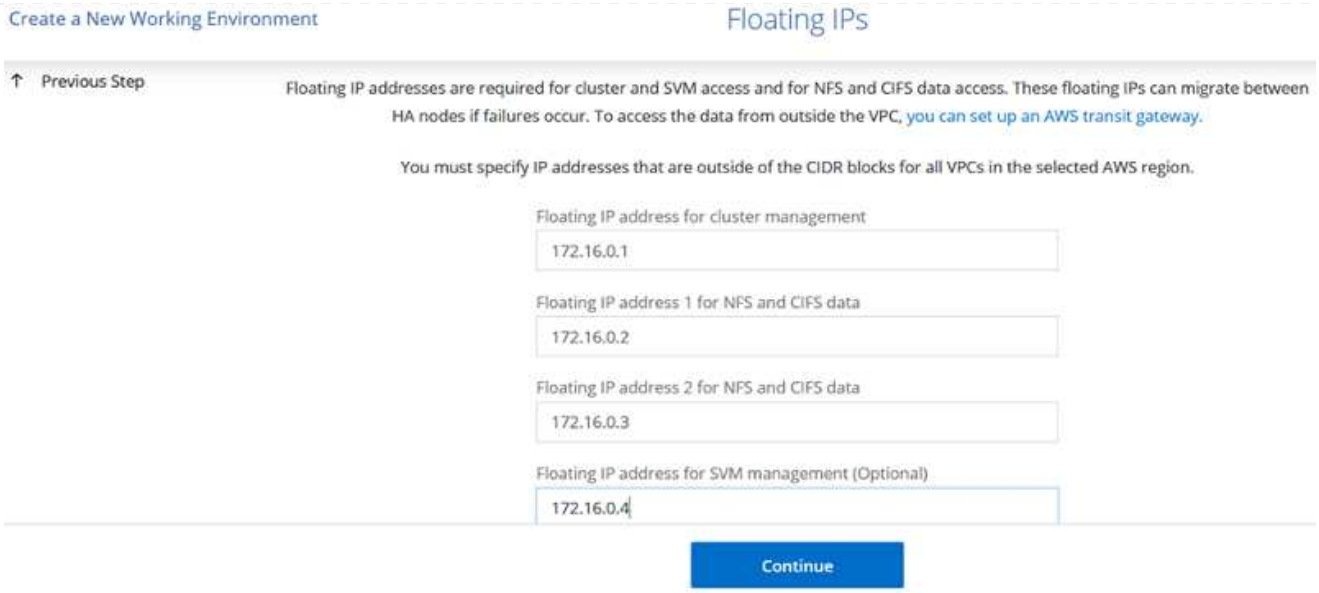
Continue (continua).



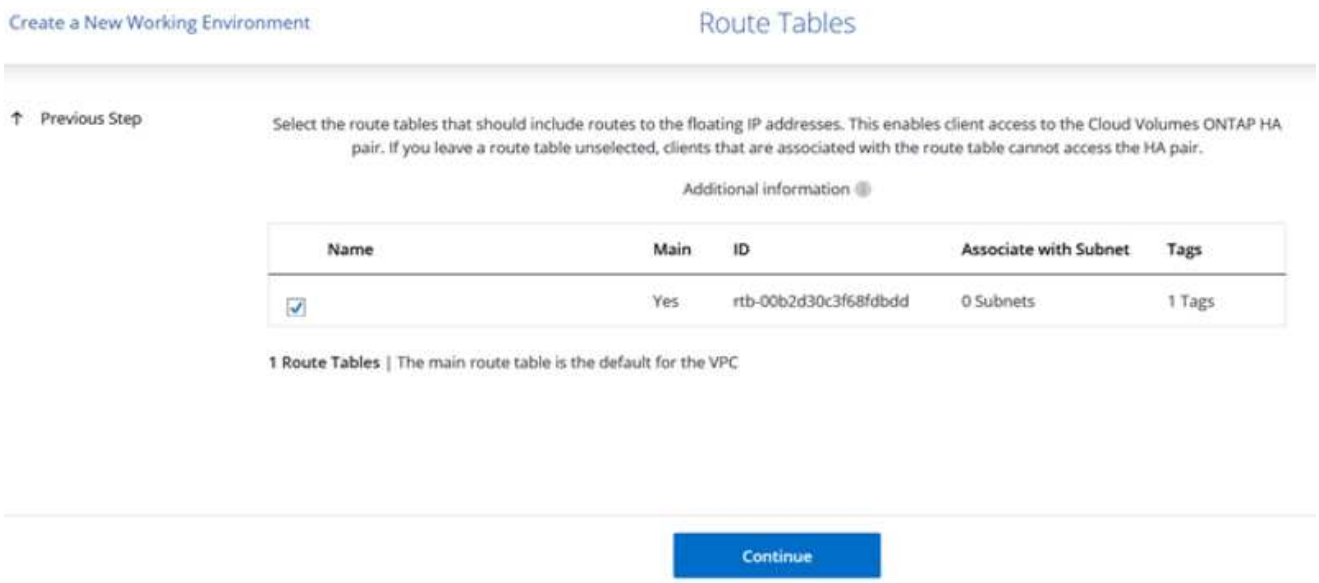
1. Nella pagina Connectivity and SSH Authentication (connettività e autenticazione SSH), scegliere i metodi di connessione per la coppia ha e il mediatore.



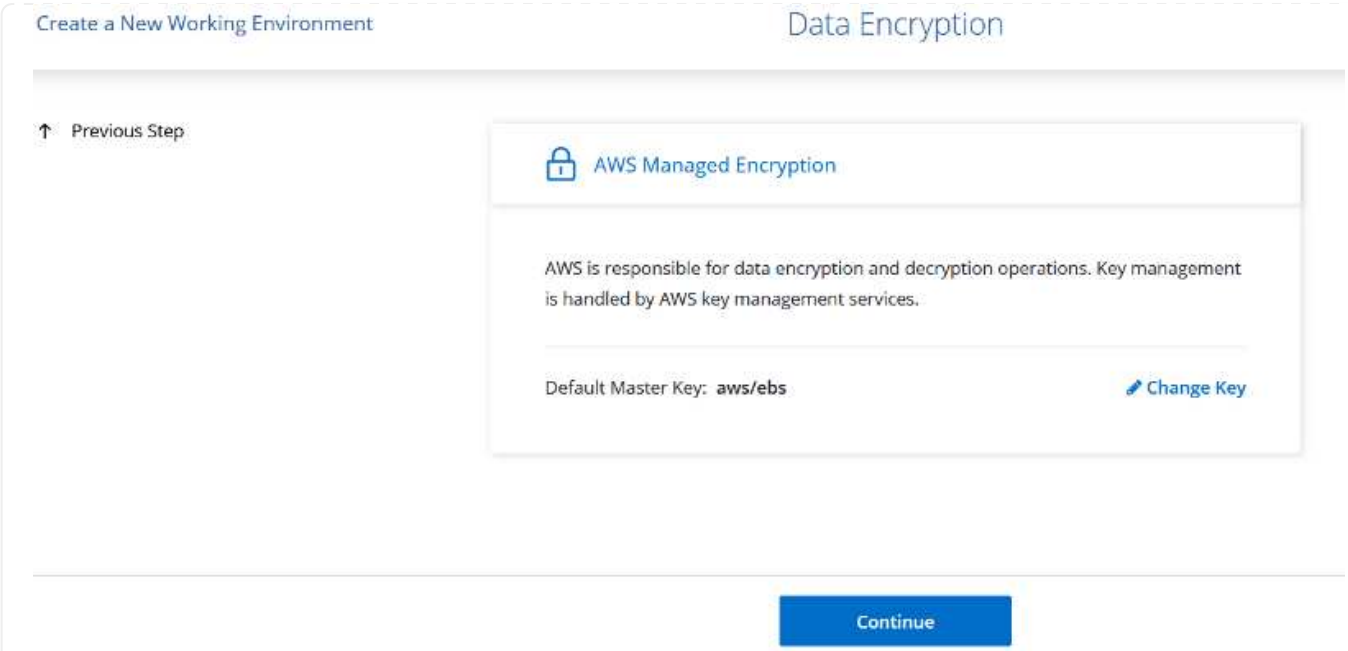
1. Specificare gli indirizzi IP mobili, quindi fare clic su Continue (continua).



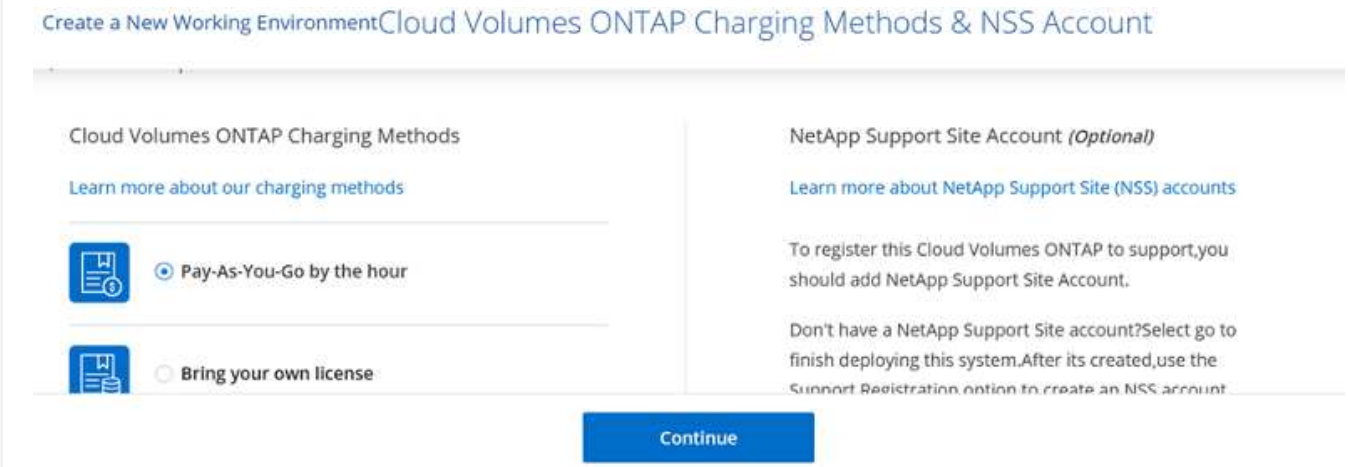
1. Selezionare le tabelle di routing appropriate per includere i percorsi verso gli indirizzi IP mobili, quindi fare clic su continua.



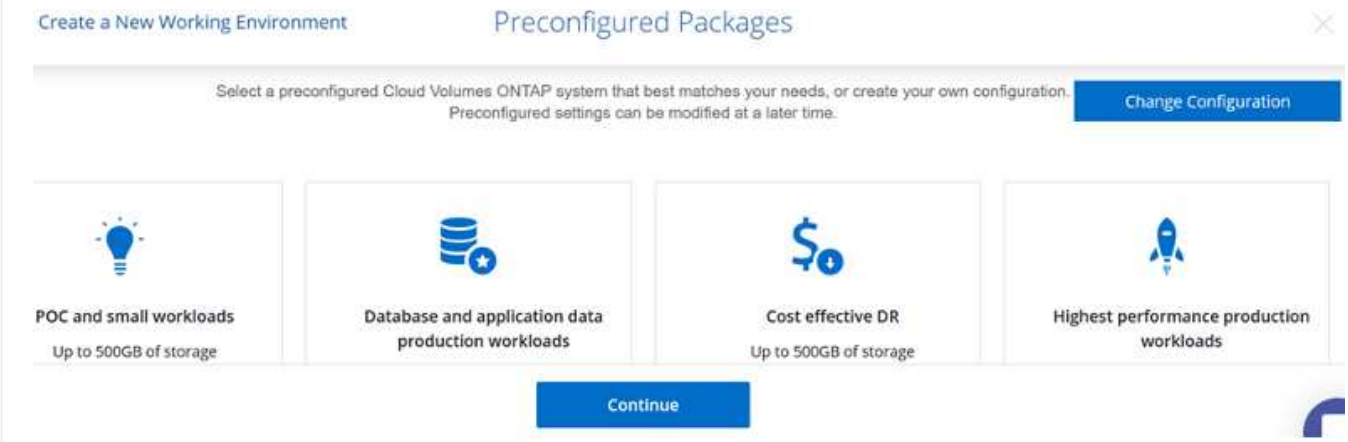
1. Nella pagina Data Encryption (crittografia dati), scegliere AWS-Managed Encryption (crittografia gestita da AWS).



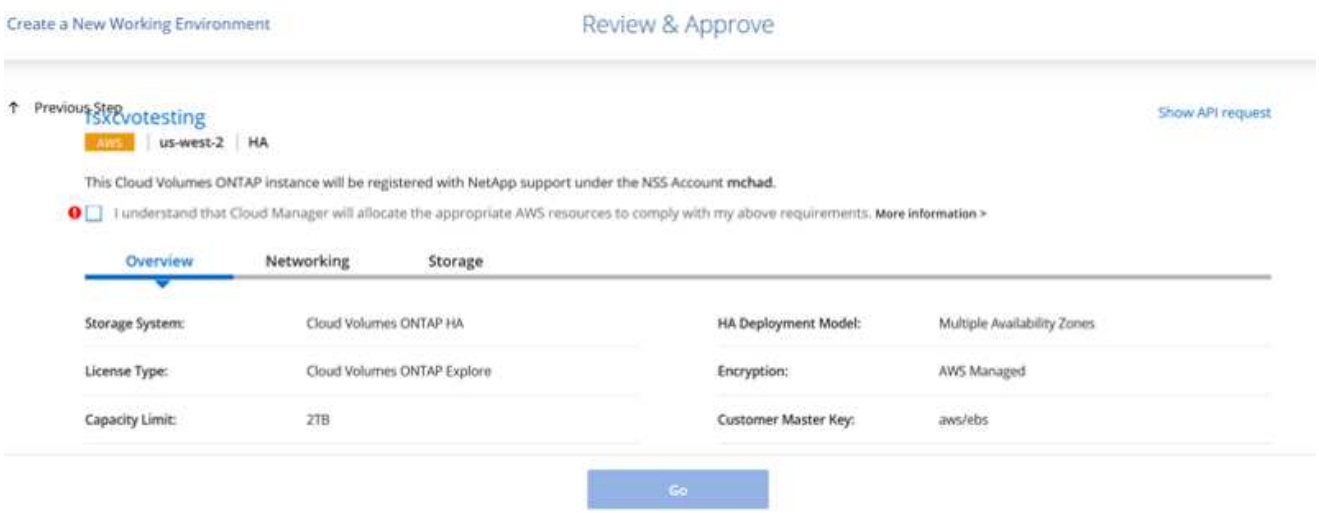
1. Selezionare l'opzione di licenza: Pay-as-you-Go o BYOL per utilizzare una licenza esistente. In questo esempio, viene utilizzata l'opzione Pay-as-You-Go.



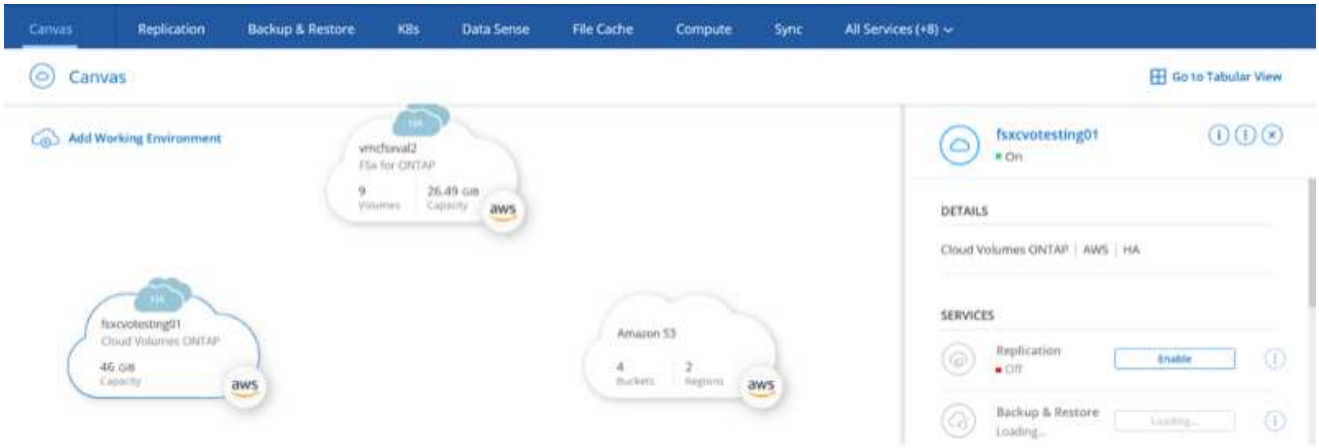
1. Scegliere tra diversi pacchetti preconfigurati disponibili in base al tipo di carico di lavoro da implementare sulle macchine virtuali in esecuzione sul cloud VMware su AWS SDDC.



1. Nella pagina Review & Approve (esamina e approva), rivedere e confermare le selezioni.per creare l'istanza di Cloud Volumes ONTAP, fare clic su Go (Vai).

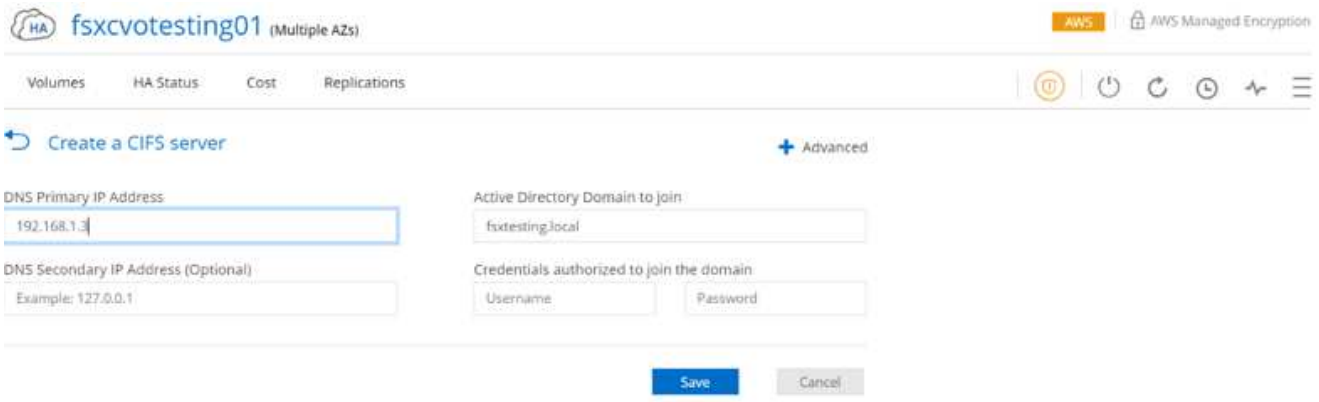


1. Una volta eseguito il provisioning, Cloud Volumes ONTAP viene elencato negli ambienti di lavoro nella pagina Canvas.

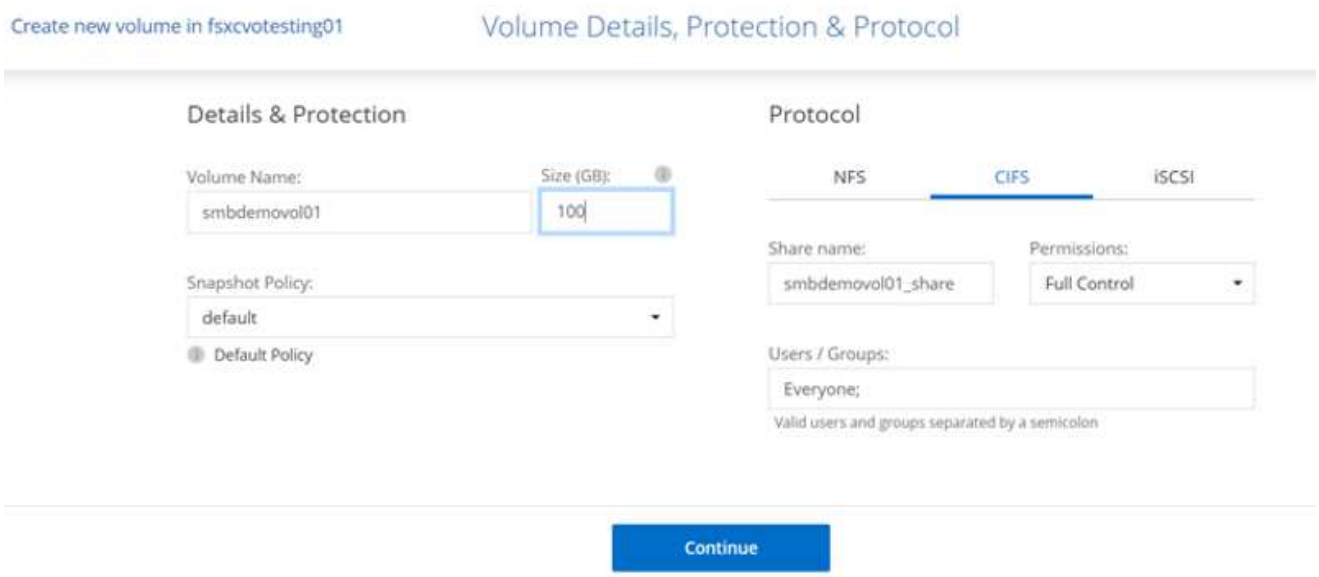


Configurazioni aggiuntive per volumi SMB

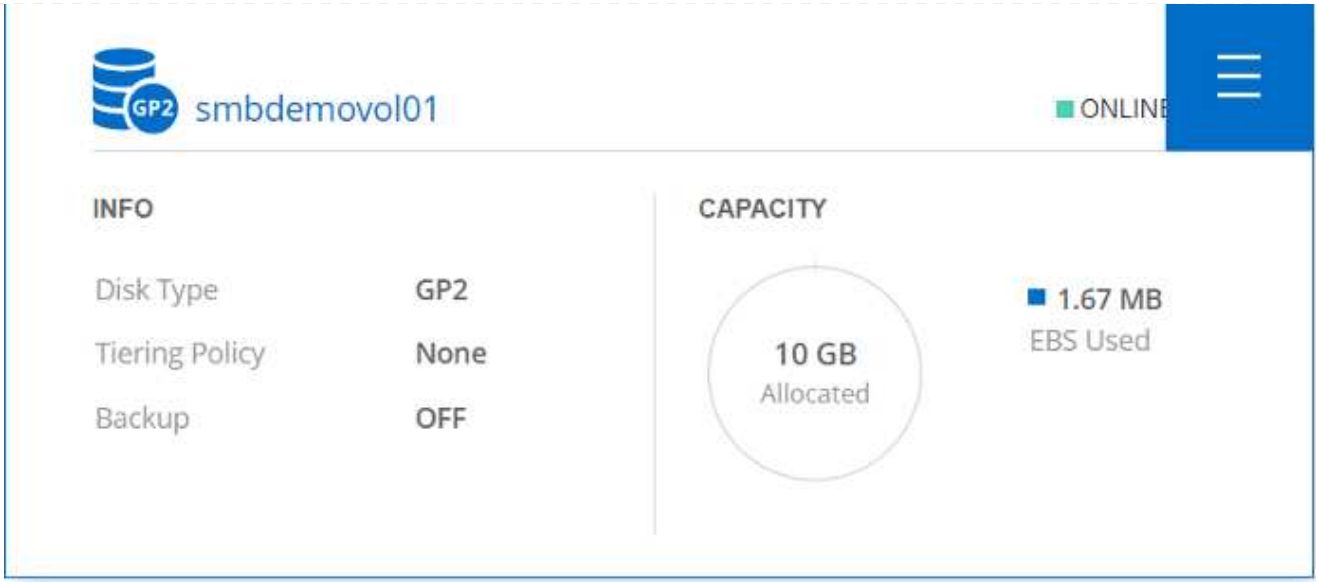
1. Una volta pronto l'ambiente di lavoro, assicurarsi che il server CIFS sia configurato con i parametri di configurazione DNS e Active Directory appropriati. Questo passaggio è necessario prima di poter creare il volume SMB.



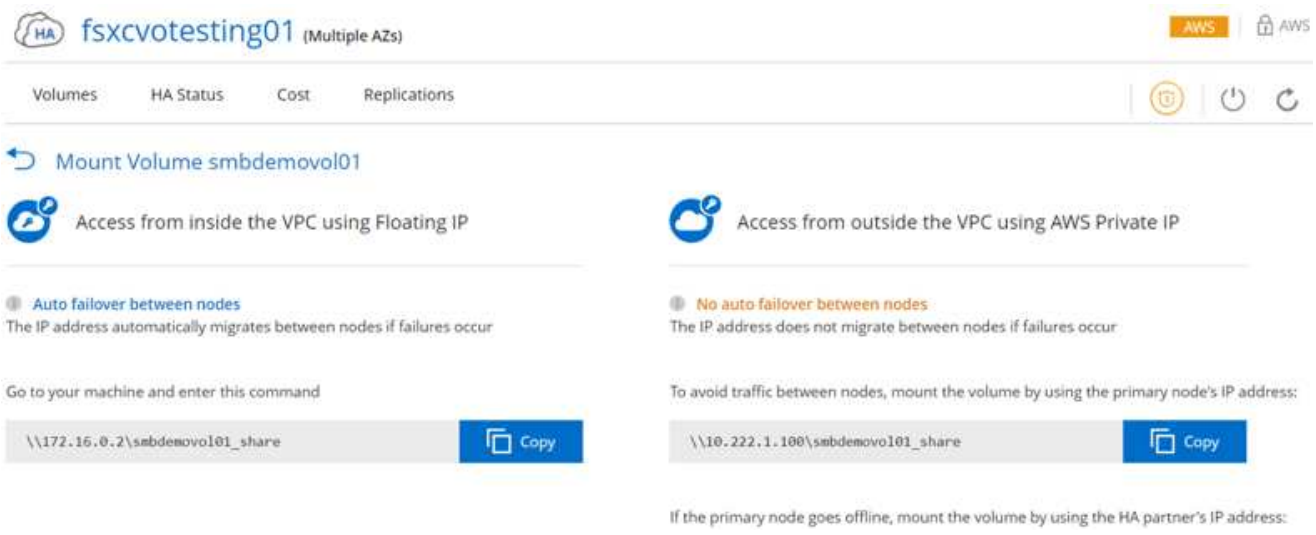
1. Selezionare l'istanza CVO per creare il volume e fare clic sull'opzione Create Volume (Crea volume). Scegli le dimensioni appropriate e il cloud manager sceglie l'aggregato contenente o utilizza un meccanismo di allocazione avanzato da collocare su un aggregato specifico. Per questa demo, SMB viene selezionato come protocollo.

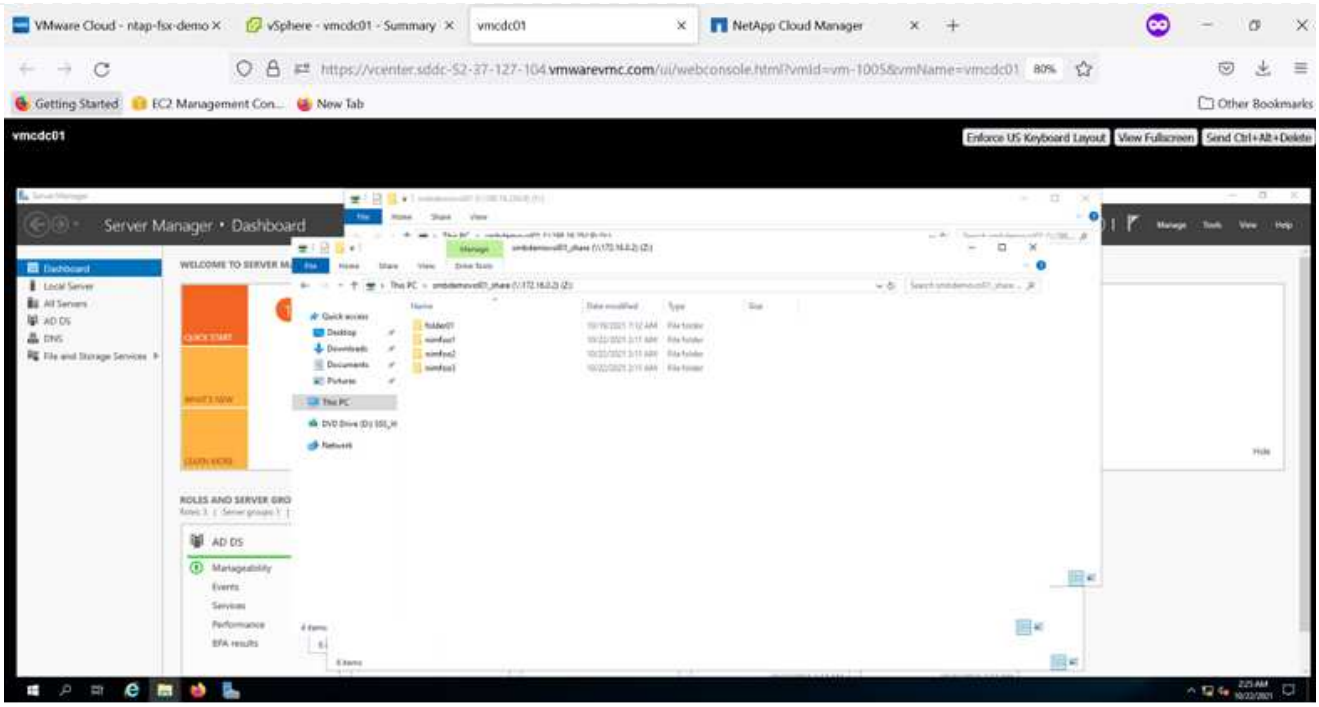


1. Una volta eseguito il provisioning, il volume è disponibile nel riquadro Volumes (volumi). Poiché viene fornita una condivisione CIFS, è necessario concedere agli utenti o ai gruppi l'autorizzazione per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file.



1. Una volta creato il volume, utilizzare il comando mount per connettersi alla condivisione dalla macchina virtuale in esecuzione su VMware Cloud negli host AWS SDDC.
2. Copiare il seguente percorso e utilizzare l'opzione Map Network Drive per montare il volume sulla macchina virtuale in esecuzione su VMware Cloud in AWS SDDC.

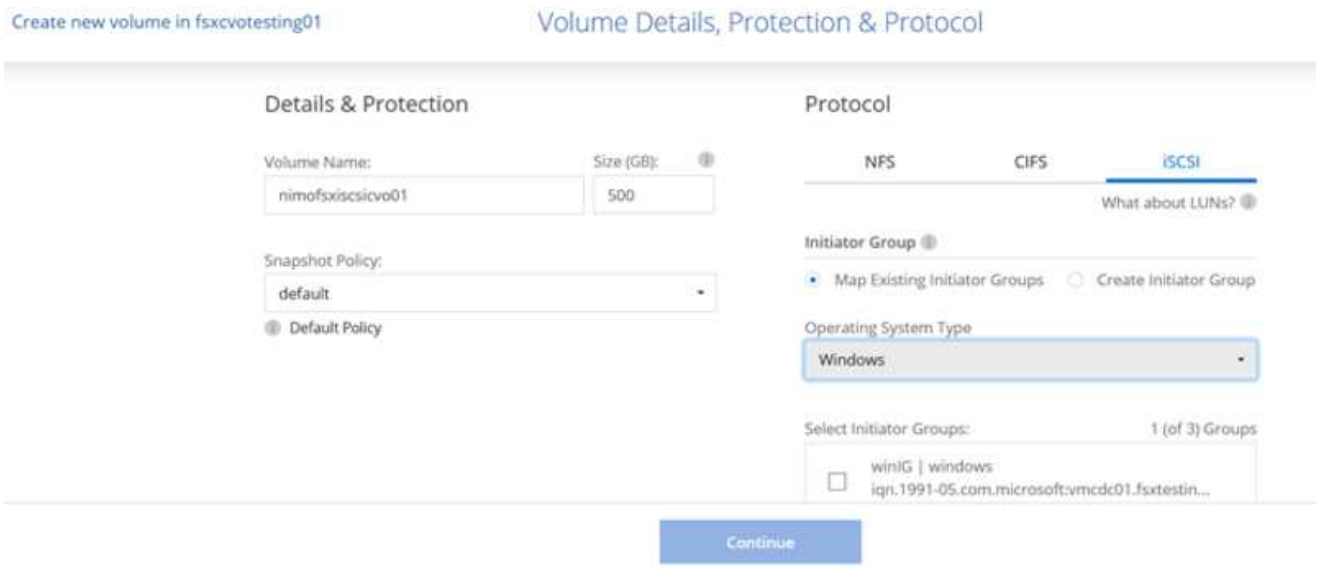


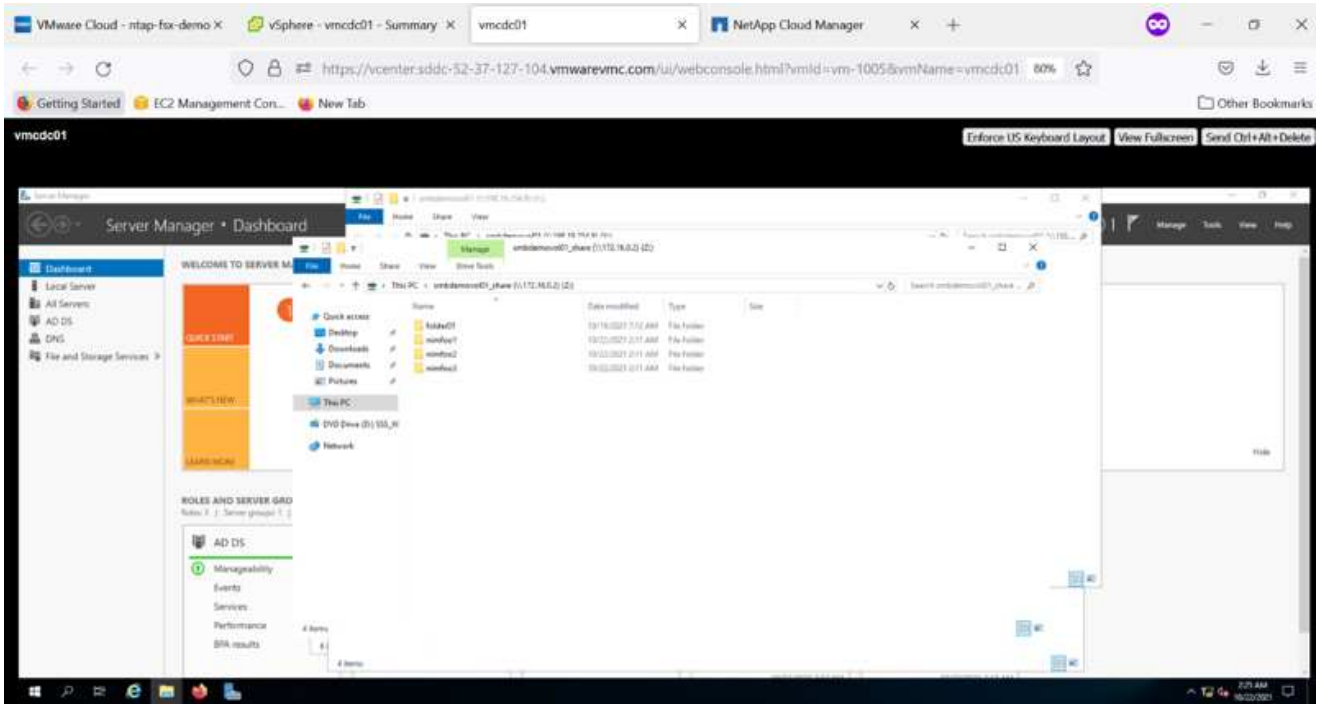

VMware Cloud - ntap-fsx-demo
vSphere - vmcdc01 - Summary
vmcdc01
NetApp Cloud Manager
https://vcenter.sddc-52-37-127-104.vmwarevmc.com/ui/webconsole.html?vmId=vm-1005&vmName=vmcdc01
Getting Started
EC2 Management Con...
New Tab
Other Bookmarks
vmcdc01
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete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

Collegare il LUN a un host

Per collegare il LUN Cloud Volumes ONTAP a un host, attenersi alla seguente procedura:

1. Nella pagina Canvas di Cloud Manager, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP per creare e gestire i volumi.
2. Fare clic su Add Volume (Aggiungi volume) > New Volume (nuovo volume), selezionare iSCSI, quindi fare clic su Create Initiator Group (Crea gruppo di Fare clic su continua.





1. Una volta eseguito il provisioning del volume, selezionare il volume, quindi fare clic su Target IQN (IQN di destinazione). Per copiare il nome qualificato iSCSI (IQN), fare clic su Copy (Copia). Impostare una connessione iSCSI dall'host al LUN.

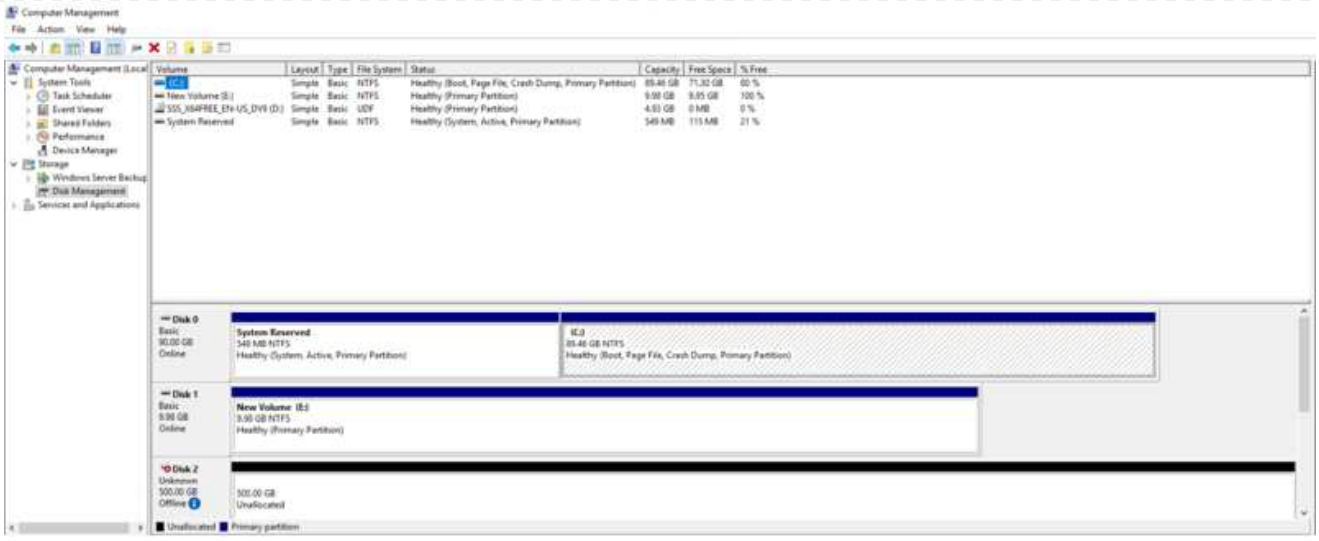
Per ottenere lo stesso risultato per l'host residente su VMware Cloud su AWS SDDC, attenersi alla seguente procedura:

1. RDP sulla macchina virtuale ospitata sul cloud VMware su AWS.
2. Aprire la finestra di dialogo iSCSI Initiator Properties (Proprietà iSCSI Initiator): Server Manager > Dashboard > Tools > iSCSI Initiator.
3. Dalla scheda Discovery (rilevamento), fare clic su Discover Portal (Scopri portale) o Add Portal (Aggiungi portale), quindi inserire l'indirizzo IP della porta di destinazione iSCSI.
4. Dalla scheda Target, selezionare la destinazione rilevata, quindi fare clic su Log on (Accedi) o Connect (Connetti).
5. Selezionare Enable multipath (attiva multipath), quindi selezionare Automatically Restore this Connection when the computer starts or Add this Connection to the List of Favorite targets (Ripristina automaticamente questa connessione all'avvio del computer). Fare clic su Avanzate.

L'host Windows deve disporre di una connessione iSCSI a ciascun nodo del cluster. Il DSM nativo seleziona i percorsi migliori da utilizzare.

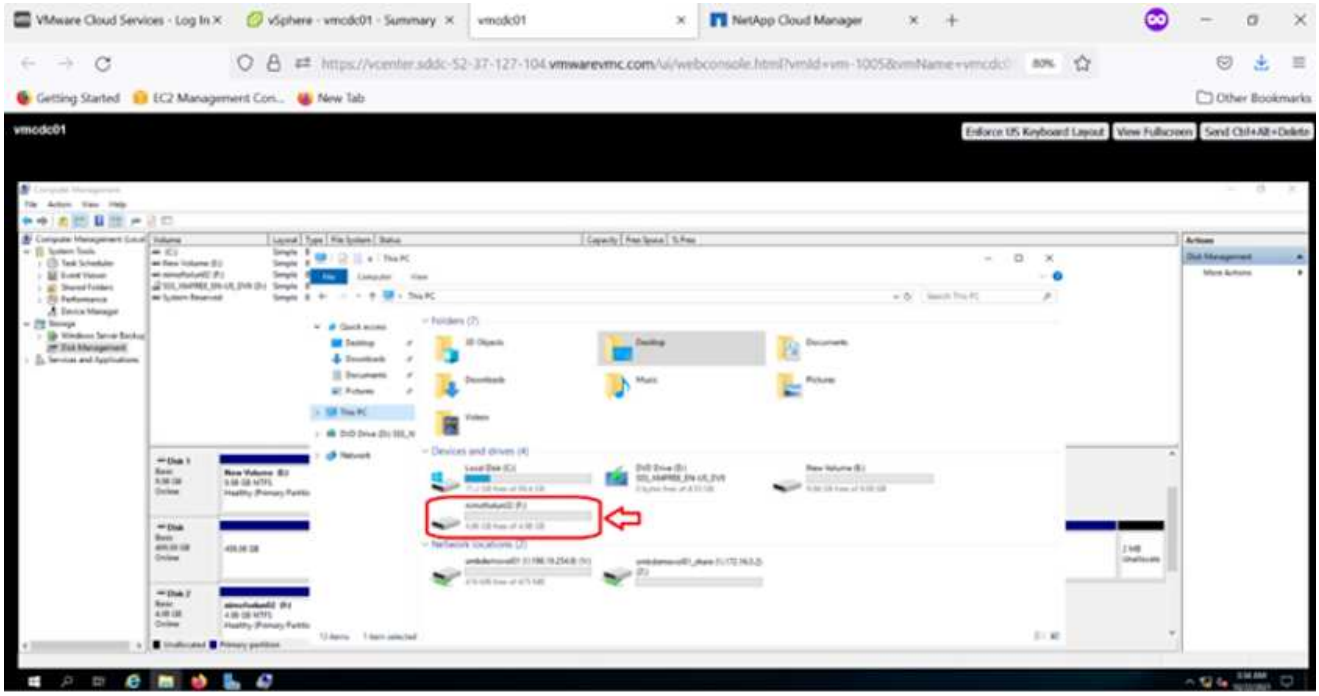
I LUN della SVM vengono visualizzati come dischi sull'host Windows. I nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Attivare una nuova scansione manuale per rilevare i dischi completando la seguente procedura:

1. Aprire l'utility Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
2. Espandere il nodo Storage nella struttura di navigazione.
3. Fare clic su Gestione disco.
4. Fare clic su Action (azione) > Rescan Disks (Nuova scansione



Quando l'host Windows accede per la prima volta a un nuovo LUN, non dispone di partizione o file system. Inizializzare il LUN e, facoltativamente, formattare il LUN con un file system completando la seguente procedura:

1. Avviare Gestione disco di Windows.
2. Fare clic con il pulsante destro del mouse sul LUN, quindi selezionare il tipo di disco o partizione richiesto.
3. Seguire le istruzioni della procedura guidata. In questo esempio, viene montato il disco F:.



Sui client Linux, assicurarsi che il daemon iSCSI sia in esecuzione. Dopo aver eseguito il provisioning dei LUN, consultare le istruzioni dettagliate sulla configurazione iSCSI per la distribuzione Linux. Ad esempio, è possibile trovare la configurazione iSCSI di Ubuntu "qui". Per verificare, eseguire lsblk cmd dalla shell.

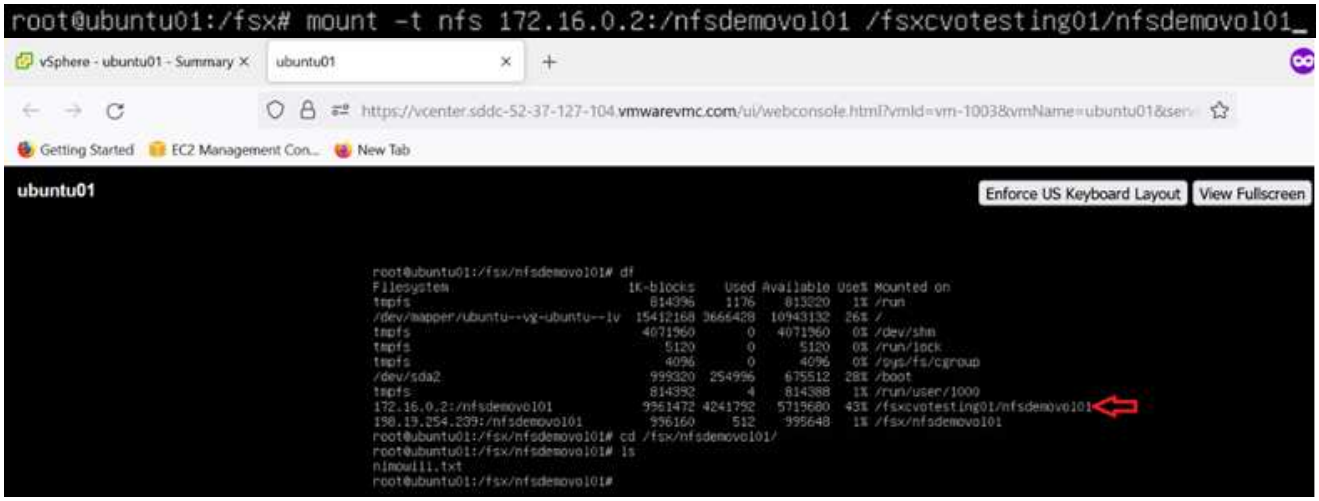
Montare il volume NFS Cloud Volumes ONTAP sul client Linux

Per montare il file system Cloud Volumes ONTAP (DIY) dalle macchine virtuali all'interno di VMC su AWS SDDC, attenersi alla seguente procedura:

1. Connettersi all'istanza Linux designata.
2. Aprire un terminale sull'istanza utilizzando la shell sicura (SSH) e accedere con le credenziali appropriate.
3. Creare una directory per il punto di montaggio del volume con il seguente comando.

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. Montare il volume NFS Amazon FSX per NetApp ONTAP nella directory
creata nel passaggio precedente.
```

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



Panoramica delle soluzioni ANF Datastore

Ogni organizzazione di successo sta passando per la trasformazione e la modernizzazione. Nell'ambito di questo processo, le aziende utilizzano solitamente i propri investimenti VMware esistenti, sfruttando al contempo i vantaggi del cloud e esplorando come rendere i processi di migrazione, burst, exteNd e disaster recovery il più possibile perfetti. I clienti che migrano al cloud devono valutare i problemi di flessibilità e burst, uscita dal data center, consolidamento del data center, scenari di fine vita, fusioni, acquisizioni e così via. L'approccio adottato da ciascuna organizzazione può variare in base alle rispettive priorità di business. Nella scelta delle operazioni basate sul cloud, la scelta di un modello a basso costo con performance appropriate e un minimo ostacolo è un obiettivo critico. Oltre a scegliere la piattaforma giusta, l'orchestrazione dello storage e del workflow è particolarmente importante per liberare la potenza

dell'implementazione e dell'elasticità del cloud.

Casi di utilizzo

Sebbene la soluzione Azure VMware offra funzionalità ibride uniche a un cliente, opzioni di storage nativo limitate ne hanno limitato l'utilità per le organizzazioni con carichi di lavoro elevati in termini di storage. Poiché lo storage è direttamente legato agli host, l'unico modo per scalare lo storage è aggiungere più host, che possono aumentare i costi del 35-40% o più per i carichi di lavoro a elevato utilizzo dello storage. Questi carichi di lavoro necessitano di storage aggiuntivo, non di potenza aggiuntiva, ma ciò significa pagare per host aggiuntivi.

Consideriamo il seguente scenario: Un cliente richiede sei host per la potenza (vCPU/VMEM), ma ha anche un requisito sostanziale per lo storage. In base alla loro valutazione, sono necessari 12 host per soddisfare i requisiti di storage. Questo aumenta il TCO complessivo perché devono acquistare tutta la potenza aggiuntiva quando è necessario solo uno storage maggiore. Questo è valido per qualsiasi caso di utilizzo, inclusi migrazione, disaster recovery, bursting, sviluppo/test, e così via.

Un altro caso di utilizzo comune per Azure VMware Solution è il disaster recovery (DR). La maggior parte delle organizzazioni non dispone di una strategia di disaster recovery a prova di fool o potrebbe avere difficoltà a giustificare l'esecuzione di un data center fantasma solo per il DR. Gli amministratori possono esplorare opzioni di disaster recovery a impatto zero con un cluster pilota o un cluster on-demand. Quindi, potevano scalare lo storage senza aggiungere host aggiuntivi, un'opzione potenzialmente interessante.

In sintesi, i casi di utilizzo possono essere classificati in due modi:

- Scalabilità della capacità di storage con datastore ANF
- Utilizzo di datastore ANF come destinazione di disaster recovery per un workflow di recovery ottimizzato in termini di costi da aree locali o interne ad Azure tra i data center software-defined (SDDC). Questa guida fornisce informazioni sull'utilizzo di Azure NetApp Files per fornire storage ottimizzato per i datastore (attualmente in anteprima pubblica) Oltre alla protezione dei dati e alle funzionalità di DR Best-in-class di una soluzione VMware Azure, che consente di trasferire la capacità dello storage dallo storage vSAN.

Per ulteriori informazioni sull'utilizzo dei datastore ANF, contattare NetApp o i Solution Architect Microsoft della propria regione.

Opzioni di VMware Cloud in Azure

Soluzione VMware Azure

Azure VMware Solution (AVS) è un servizio di cloud ibrido che offre SDDC VMware pienamente funzionanti all'interno di un cloud pubblico Microsoft Azure. AVS è una soluzione di prima parte completamente gestita e supportata da Microsoft e verificata da VMware che utilizza l'infrastruttura Azure. Pertanto, i clienti ottengono VMware ESXi per la virtualizzazione del calcolo, vSAN per lo storage iperconvergente e NSX per il networking e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture di data center leader di settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure native. Una combinazione di SDDC e Azure NetApp Files per la soluzione VMware Azure offre le migliori performance con una latenza di rete minima.

Indipendentemente dal cloud utilizzato, quando viene implementato un VMware SDDC, il cluster iniziale include i seguenti componenti:

- VMware ESXi ospita la virtualizzazione dell'elaborazione con un'appliance server vCenter per la gestione.
- Storage iperconvergente VMware vSAN che incorpora le risorse di storage fisico di ciascun host ESXi.

- VMware NSX per reti virtuali e sicurezza con cluster NSX Manager per la gestione.

Conclusione

Sia che tu stia prendendo come riferimento il cloud all-cloud o ibrido, Azure NetApp Files offre opzioni eccellenti per implementare e gestire i carichi di lavoro delle applicazioni insieme ai file service, riducendo al contempo il TCO rendendo i requisiti dei dati perfetti a livello applicativo. Qualunque sia il caso d'utilizzo, scegli Azure VMware Solution insieme a Azure NetApp Files per realizzare rapidamente i benefici 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 collegare lo storage. Ricorda che è solo la posizione dei dati che sono stati modificati insieme ai nuovi nomi; i tool e i processi rimangono tutti gli stessi e Azure NetApp Files aiuta a ottimizzare l'implementazione complessiva.

Punti da asporto

I punti chiave di questo documento includono:

- Ora puoi utilizzare Azure NetApp Files come datastore su AVS SDDC.
- Aumenta i tempi di risposta delle applicazioni e offri una maggiore disponibilità per fornire i dati del carico di lavoro di accesso quando e dove sono necessari.
- Semplifica la complessità generale dello storage vSAN con funzionalità di ridimensionamento semplici e istantanee.
- Performance garantite per carichi di lavoro mission-critical grazie a funzionalità di risagomatura dinamica.
- Se la destinazione è Azure VMware Solution Cloud, Azure NetApp Files è la soluzione di storage ideale per un'implementazione ottimizzata.

Dove trovare ulteriori informazioni

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

- Documentazione della soluzione VMware Azure

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

- Documentazione Azure NetApp Files

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

- Collegamento di datastore Azure NetApp Files agli host delle soluzioni VMware Azure (anteprima)

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

Opzioni di storage NetApp Guest Connected per Azure

Azure supporta lo storage NetApp connesso come guest con il servizio ANF (Azure NetApp Files) nativo o con Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

Azure NetApp Files porta la gestione dei dati e lo storage di livello Enterprise in Azure, in modo da poter gestire i carichi di lavoro e le applicazioni con facilità. Migrare i carichi di lavoro nel cloud ed eseguirli senza sacrificare le performance.

Azure NetApp Files elimina gli ostacoli, in modo da poter spostare tutte le applicazioni basate su file nel cloud. Per la prima volta, non è necessario riprogettare le applicazioni e ottenere uno storage persistente per le applicazioni senza complessità.

Poiché il servizio viene fornito tramite il portale Microsoft Azure, gli utenti sperimentano un servizio completamente gestito come parte del contratto aziendale Microsoft. Il supporto di livello mondiale, gestito da Microsoft, ti offre la massima tranquillità. Questa singola soluzione consente di aggiungere in modo rapido e semplice carichi di lavoro multiprotocollo. È possibile creare e implementare applicazioni basate su file Windows e Linux, anche per ambienti legacy.

Azure NetApp Files (ANF) come storage connesso guest

Configurazione di Azure NetApp Files con la soluzione VMware Azure (AVS)

Le condivisioni Azure NetApp Files possono essere montate da macchine virtuali create nell'ambiente SDDC della soluzione VMware Azure. I volumi possono anche essere montati sul client Linux e mappati sul client Windows perché Azure NetApp Files supporta i protocolli SMB e NFS. I volumi Azure NetApp Files possono essere configurati in cinque semplici passaggi.

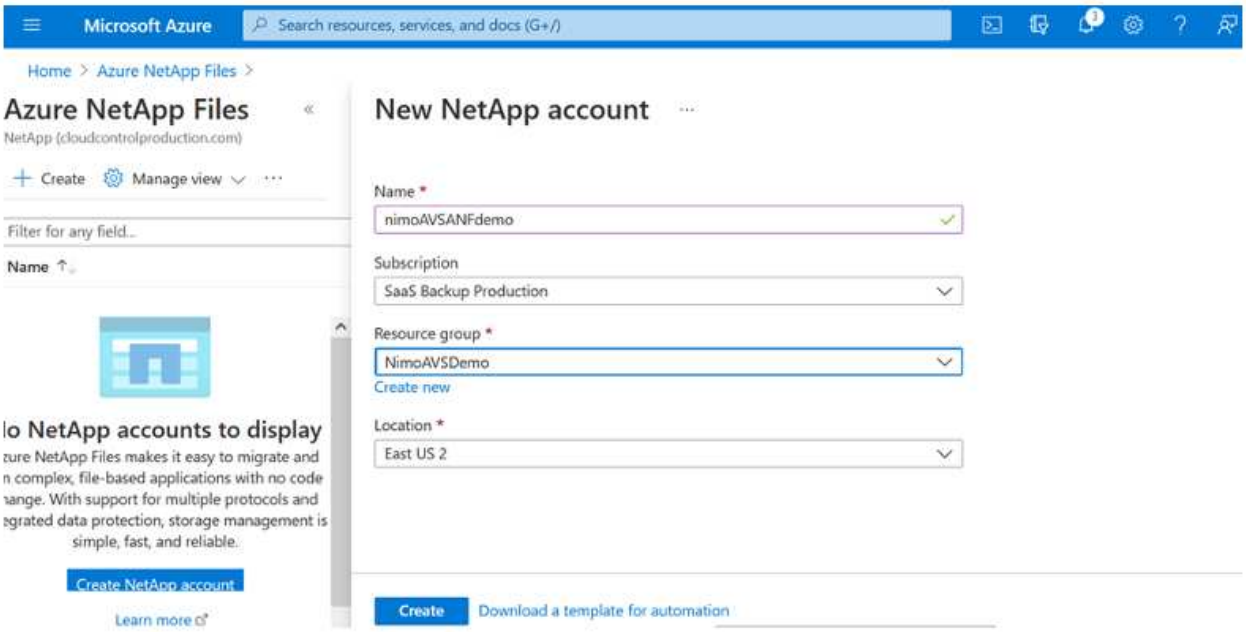
La soluzione Azure NetApp Files e Azure deve trovarsi nella stessa regione di Azure.

Creare e montare volumi Azure NetApp Files

Per creare e montare volumi Azure NetApp Files, attenersi alla seguente procedura:

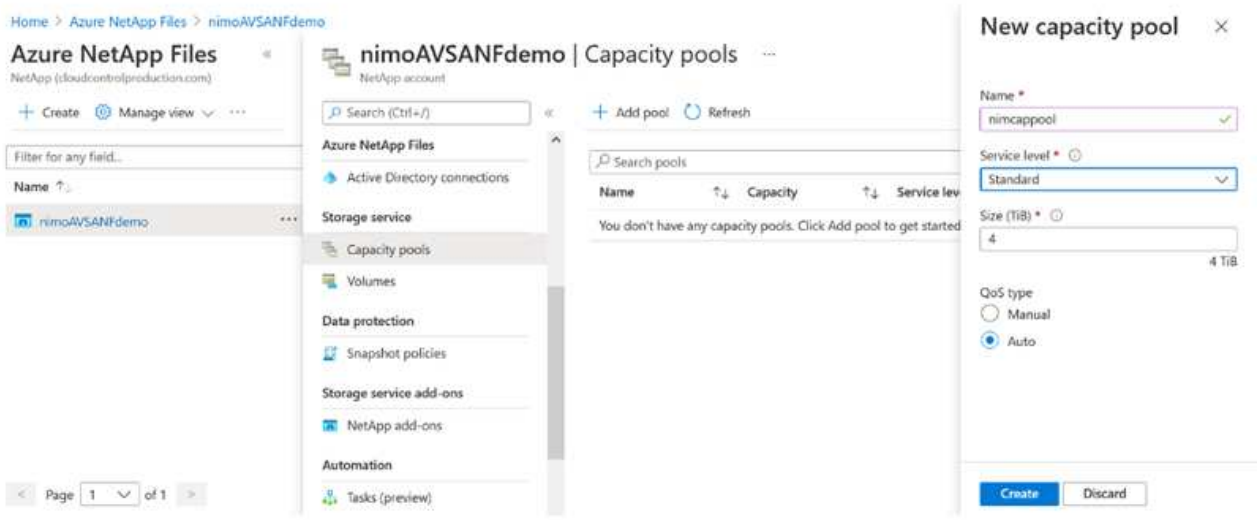
1. Accedi al portale Azure e accedi a Azure NetApp Files. Verificare l'accesso al servizio Azure NetApp Files e registrare il provider di risorse Azure NetApp Files utilizzando il comando *az provider register --namespace Microsoft.NetApp –wait*. Al termine della registrazione, creare un account NetApp.

   Per informazioni dettagliate, vedere "Condivisioni Azure NetApp Files". Questa pagina guida l'utente attraverso il processo passo-passo.

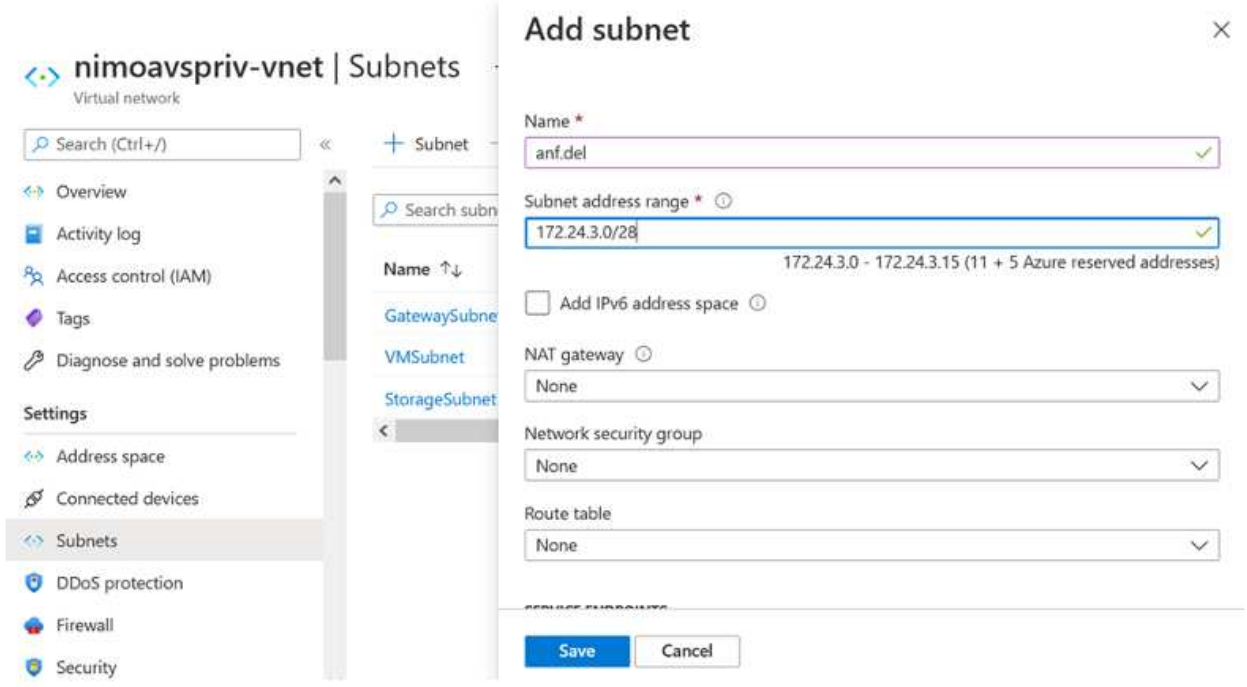


2. Una volta creato l'account NetApp, impostare i pool di capacità con il livello e le dimensioni di servizio richiesti.

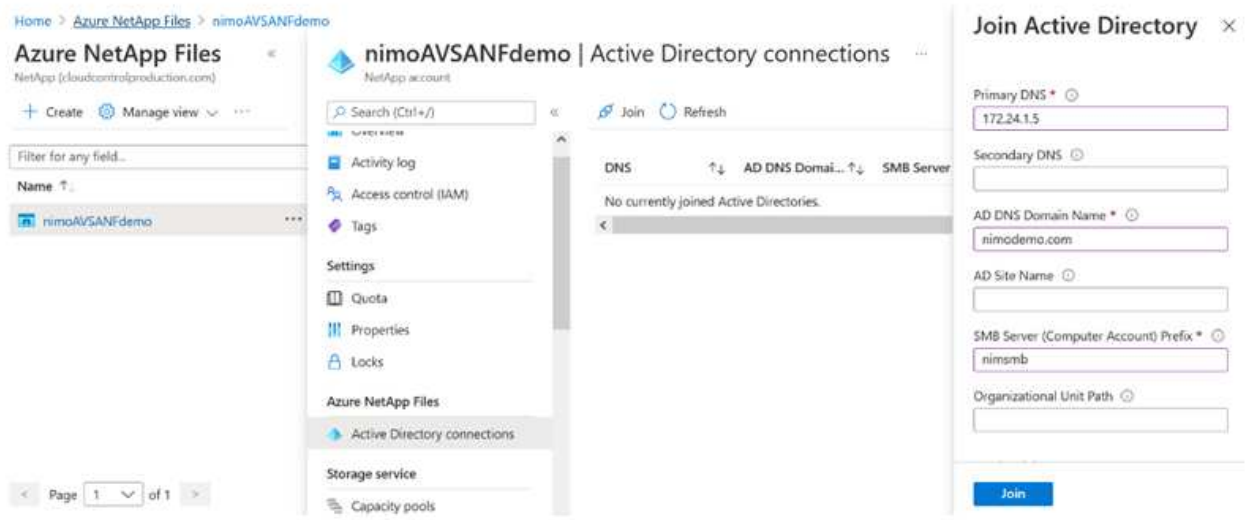
   Per ulteriori informazioni, vedere "Impostare un pool di capacità".



3. Configurare la subnet delegata per Azure NetApp Files e specificare questa subnet durante la creazione dei volumi. Per informazioni dettagliate sulla creazione di una subnet delegata, vedere "Delegare una subnet a Azure NetApp Files".

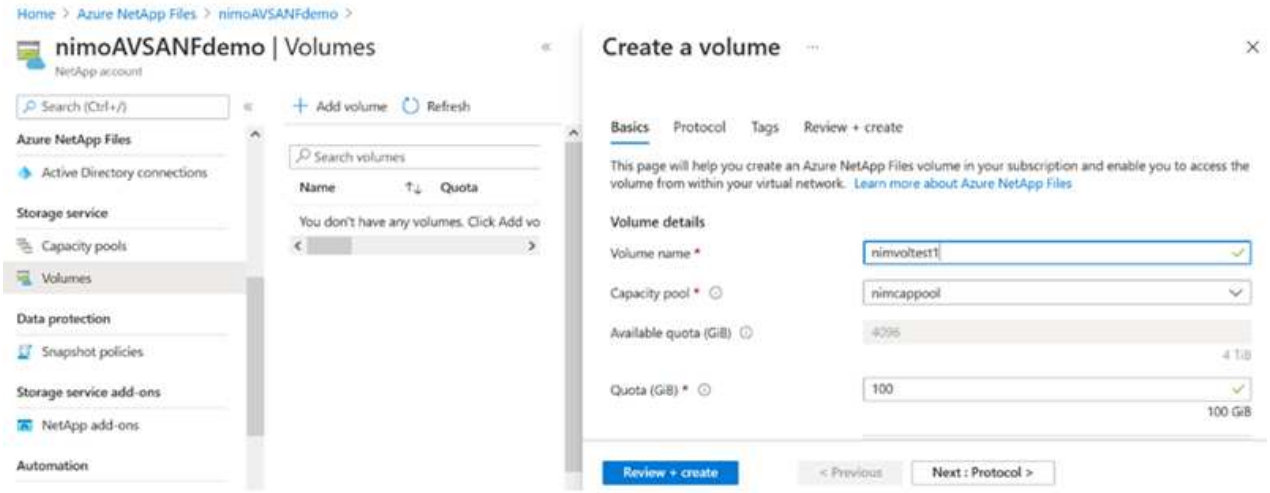


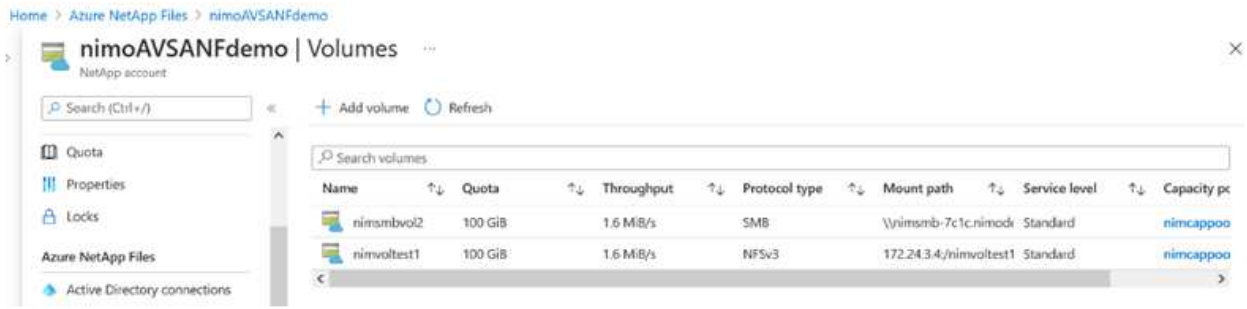
4. Aggiungere un volume SMB utilizzando il blade Volumes sotto il blade Capacity Pools. Assicurarsi che Active Directory Connector sia configurato prima di creare il volume SMB.



5. Fare clic su Review + Create (Rivedi + Crea) per creare il volume SMB.

   Se l'applicazione è SQL Server, attivare la disponibilità continua SMB.

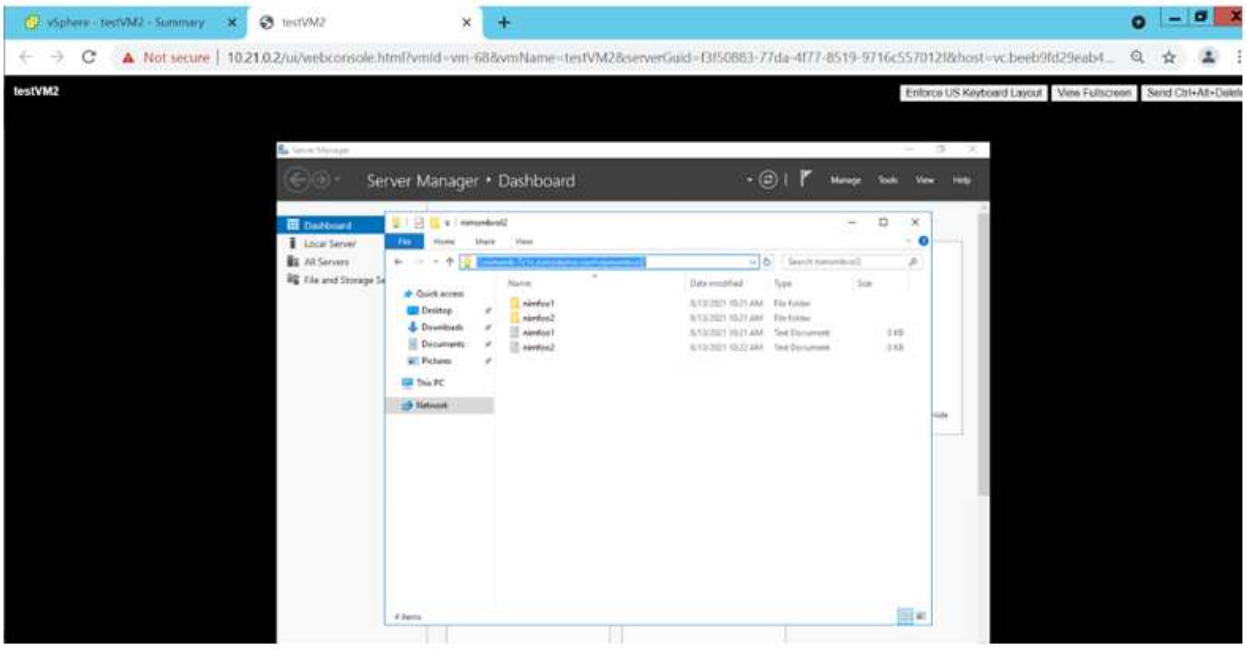


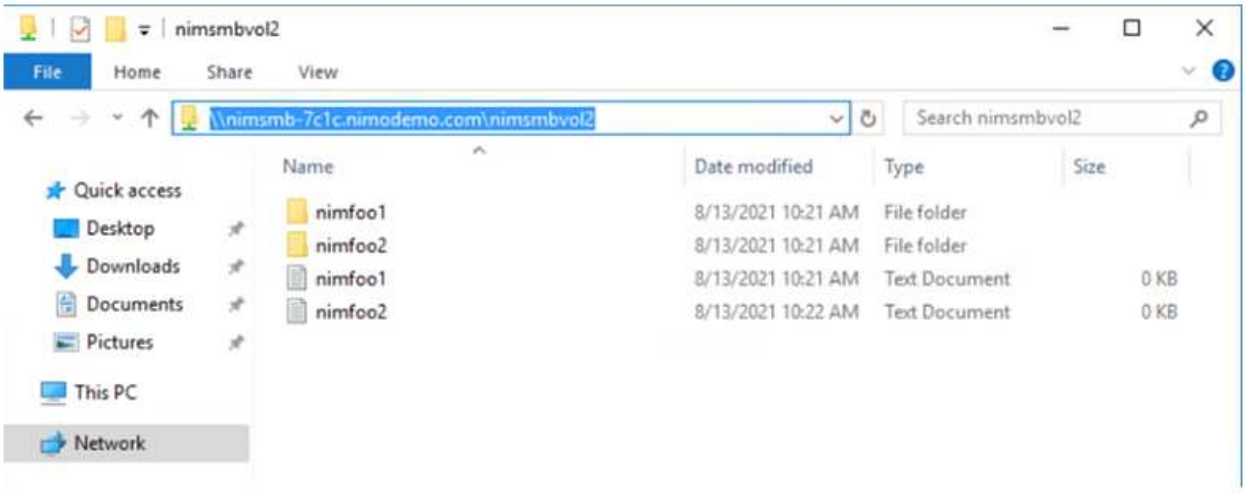


Per ulteriori informazioni sulle prestazioni dei volumi Azure NetApp Files in base alle dimensioni o alla quota, vedere "Considerazioni sulle performance per Azure NetApp Files".

6. Dopo aver attivato la connettività, è possibile montare e utilizzare il volume per i dati dell'applicazione.

   A tale scopo, dal portale Azure, fare clic sul blade Volumes, quindi selezionare il volume da montare e accedere alle istruzioni di montaggio. Copiare il percorso e utilizzare l'opzione Map Network Drive per montare il volume sulla macchina virtuale in esecuzione su Azure VMware Solution SDDC.





7. Per montare volumi NFS su macchine virtuali Linux eseguite su Azure VMware Solution SDDC, utilizzare questo stesso processo. Utilizza la riformizzazione dei volumi o la funzionalità del livello di servizio dinamico per soddisfare le esigenze dei carichi di lavoro.

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

Per ulteriori informazioni, vedere "Modificare dinamicamente il livello di servizio di un volume".

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, o CVO, è la soluzione per la gestione dei dati nel cloud leader del settore basata sul software di storage ONTAP, disponibile in modalità nativa su Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

Si tratta di una versione software-defined di ONTAP che utilizza lo storage nativo del cloud, consentendoti di avere lo stesso software di storage nel cloud e on-premise, riducendo la necessità di riorganizzare il tuo staff

IT con metodi completamente nuovi per gestire i tuoi dati.

CVO offre ai clienti la possibilità di spostare senza problemi i dati dall'edge al data center, al cloud e viceversa, unendo il tuo cloud ibrido, il tutto gestito con una console di gestione a singolo pannello, NetApp Cloud Manager.

Per progettazione, CVO offre performance estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud

Cloud Volumes ONTAP (CVO) come storage connesso guest

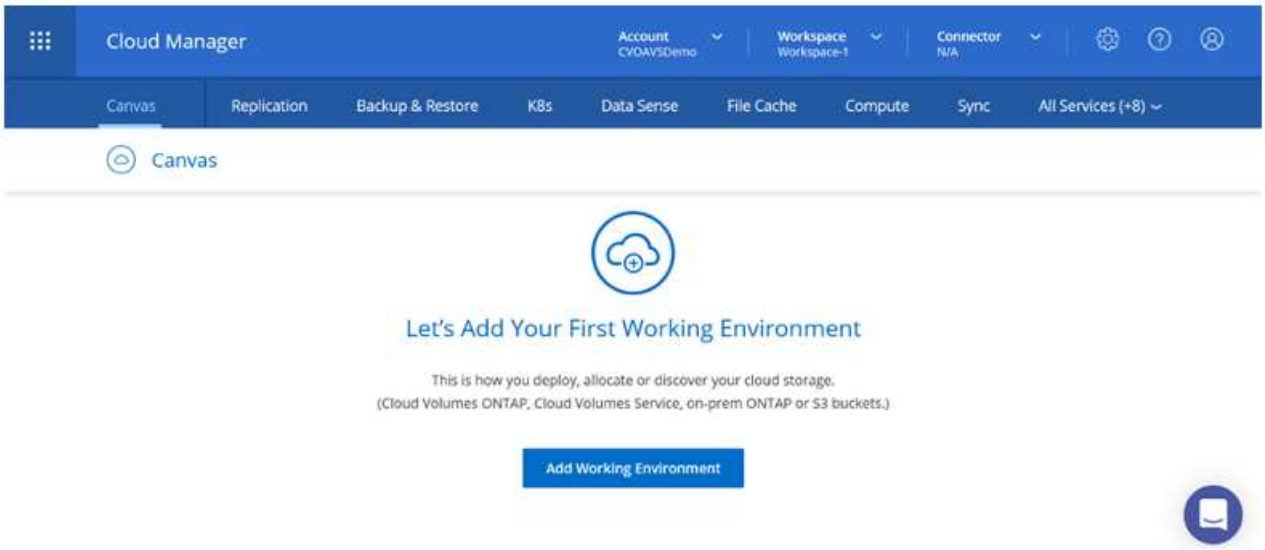
Implementa il nuovo Cloud Volumes ONTAP in Azure

Le condivisioni e i LUN Cloud Volumes ONTAP possono essere montati da macchine virtuali create nell'ambiente SDDC della soluzione VMware Azure. I volumi possono essere montati anche sul client Linux e sul client Windows, poiché Cloud Volumes ONTAP supporta i protocolli iSCSI, SMB e NFS. I volumi Cloud Volumes ONTAP possono essere configurati in pochi semplici passaggi.

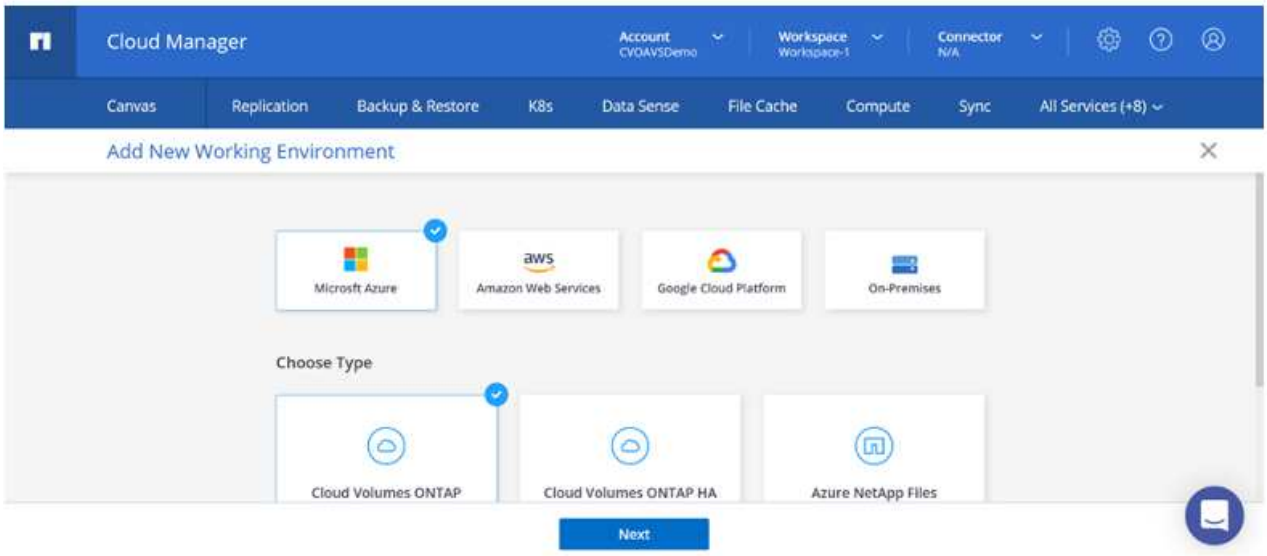
Per replicare i volumi da un ambiente on-premise al cloud per scopi di disaster recovery o migrazione, stabilire la connettività di rete con Azure, utilizzando una VPN site-to-site o ExpressRoute. La replica dei dati da on-premise a Cloud Volumes ONTAP non rientra nell'ambito di questo documento. Per replicare i dati tra sistemi on-premise e Cloud Volumes ONTAP, vedere "Configurazione della replica dei dati tra sistemi".

Utilizzare "Cloud Volumes ONTAP Sizer" Per dimensionare con precisione le istanze di Cloud Volumes ONTAP. Monitorare anche le performance on-premise da utilizzare come input nel Cloud Volumes ONTAP Sizer.

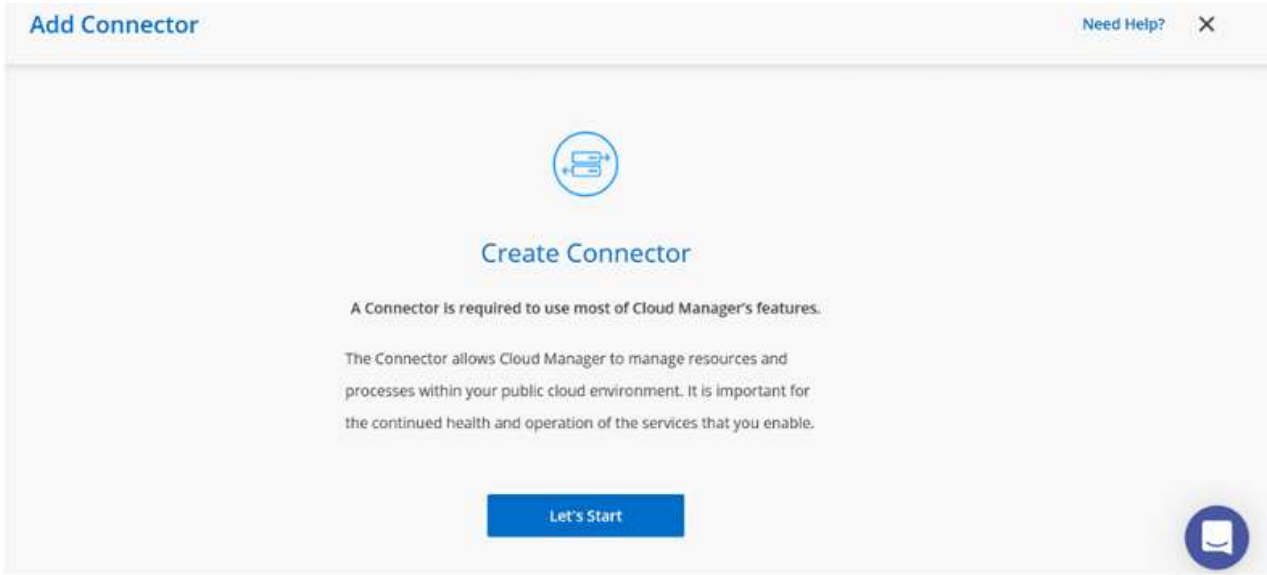
1. Accedi a NetApp Cloud Central: Viene visualizzata la schermata Fabric View. Individuare la scheda Cloud Volumes ONTAP (Gestione cloud) e selezionare Go to Cloud Manager (Vai a Gestione cloud). Una volta effettuato l'accesso, viene visualizzata la schermata Canvas.



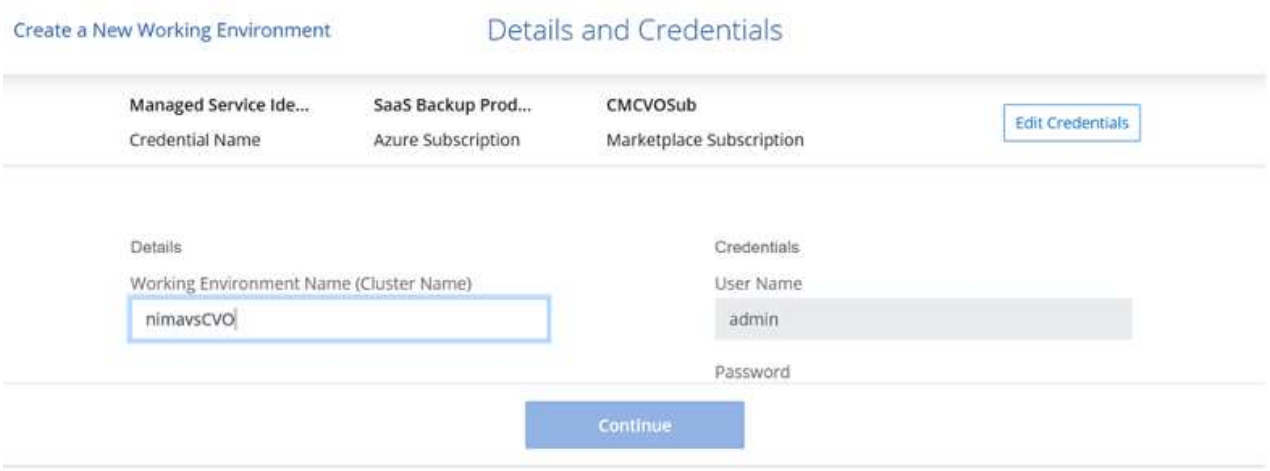
2. Nella home page di Cloud Manager, fare clic su Add a Working Environment (Aggiungi ambiente di lavoro), quindi selezionare Microsoft Azure come cloud e il tipo di configurazione del sistema.



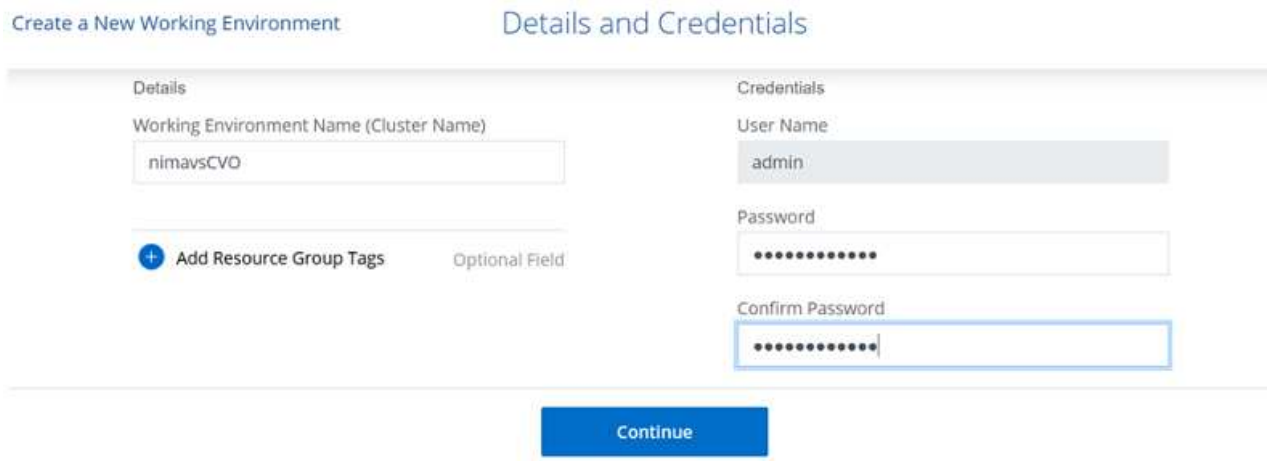
3. Quando si crea il primo ambiente di lavoro Cloud Volumes ONTAP, viene richiesto di implementare un connettore.



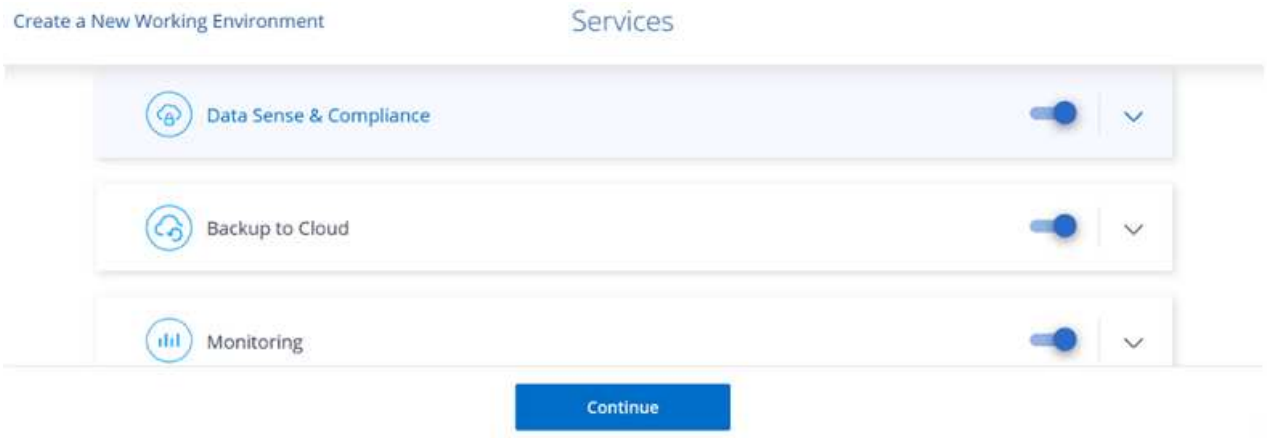
4. Una volta creato il connettore, aggiornare i campi Dettagli e credenziali.



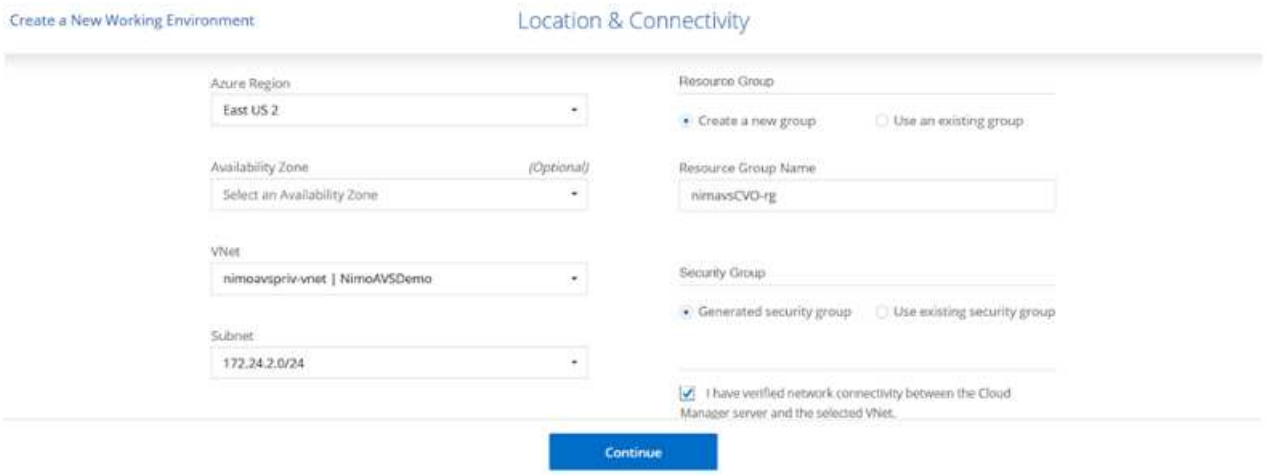
5. Fornire i dettagli dell'ambiente da creare, inclusi il nome dell'ambiente e le credenziali di amministratore. Aggiungere tag di gruppo di risorse per l'ambiente Azure come parametro facoltativo. Al termine, fare clic su Continue (continua).



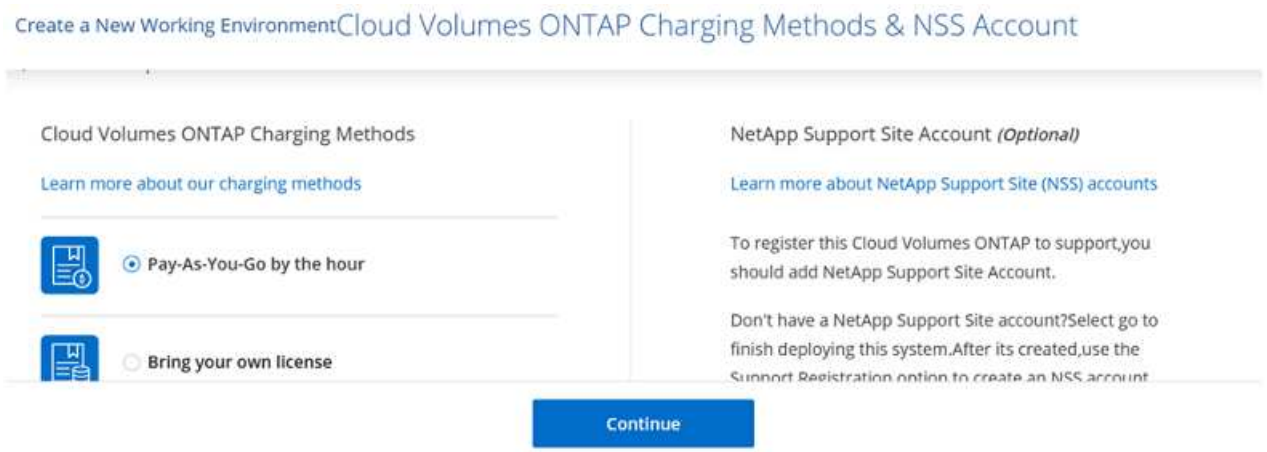
6. Seleziona i servizi add-on per l'implementazione di Cloud Volumes ONTAP, inclusi classificazione BlueXP, backup e recovery di BlueXP e Cloud Insights. Selezionare i servizi e fare clic su continua.



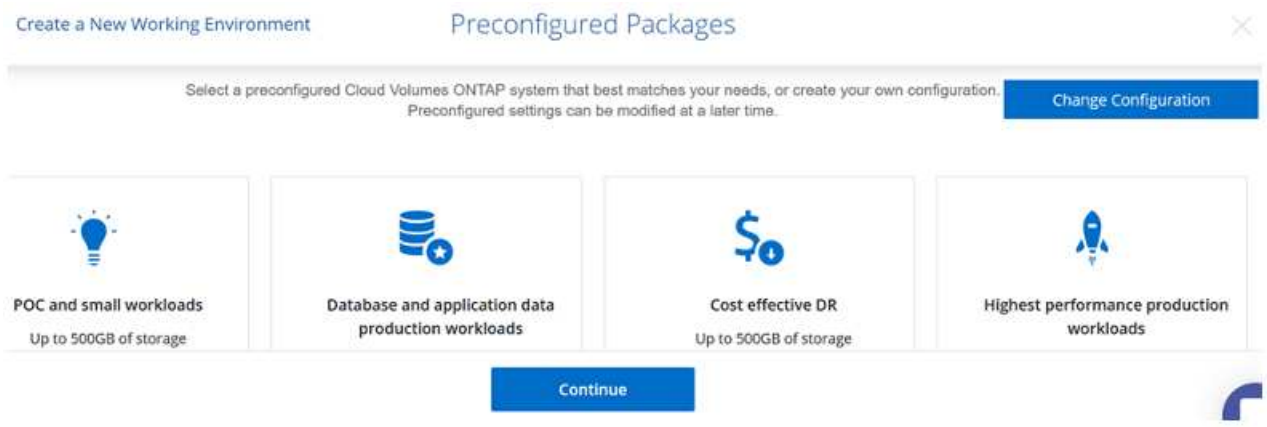
7. Configurare la posizione e la connettività di Azure. Selezionare la regione Azure, il gruppo di risorse, VNET e la subnet da utilizzare.



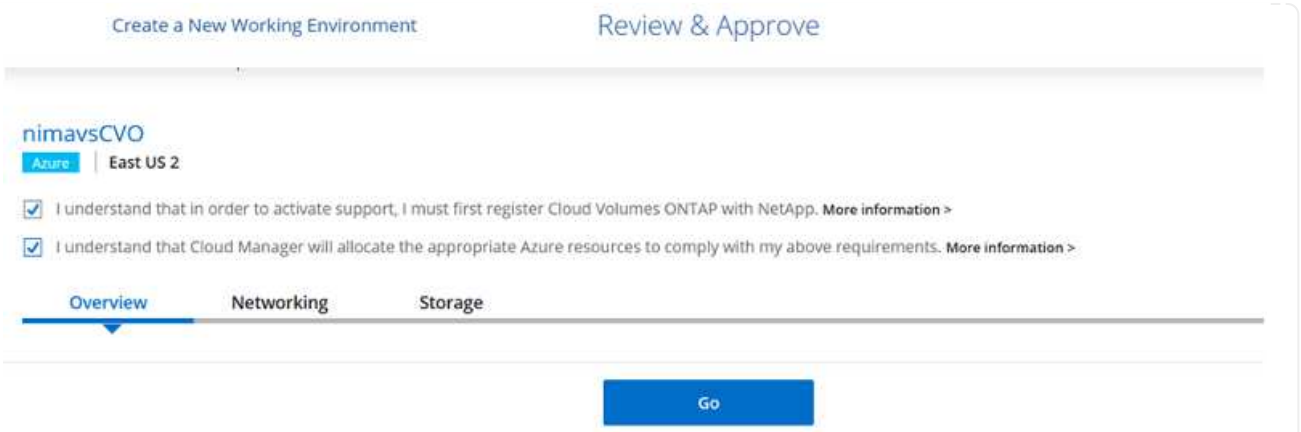
8. Selezionare l'opzione di licenza: Pay-as-you-Go o BYOL per utilizzare la licenza esistente. In questo esempio, viene utilizzata l'opzione Pay-as-You-Go.



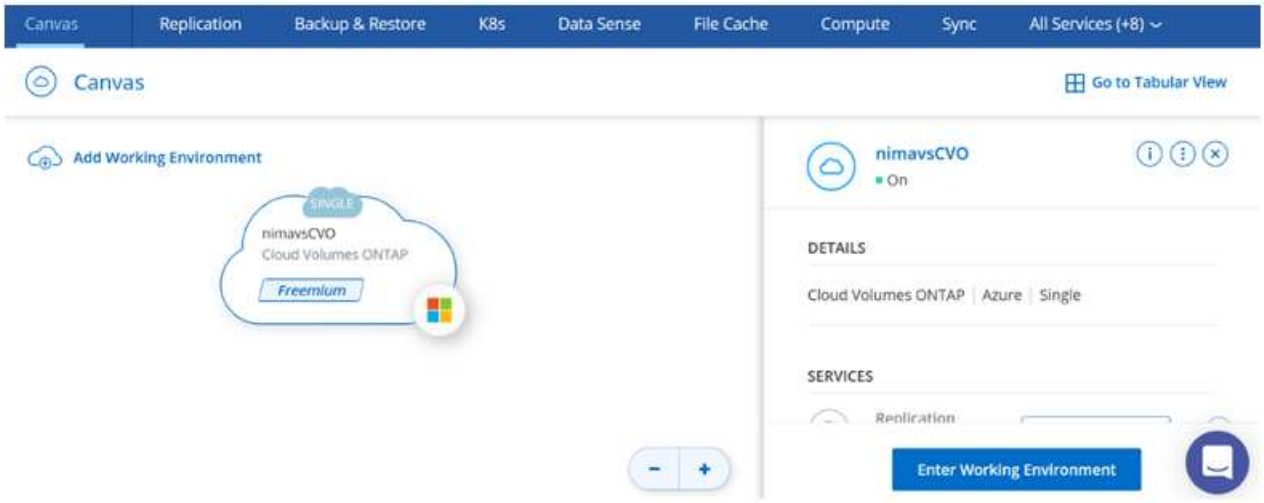
9. Scegli tra diversi pacchetti preconfigurati disponibili per i vari tipi di carichi di lavoro.



10. Accettare i due accordi relativi all'attivazione del supporto e all'allocazione delle risorse di Azure.per creare l'istanza di Cloud Volumes ONTAP, fare clic su Vai.

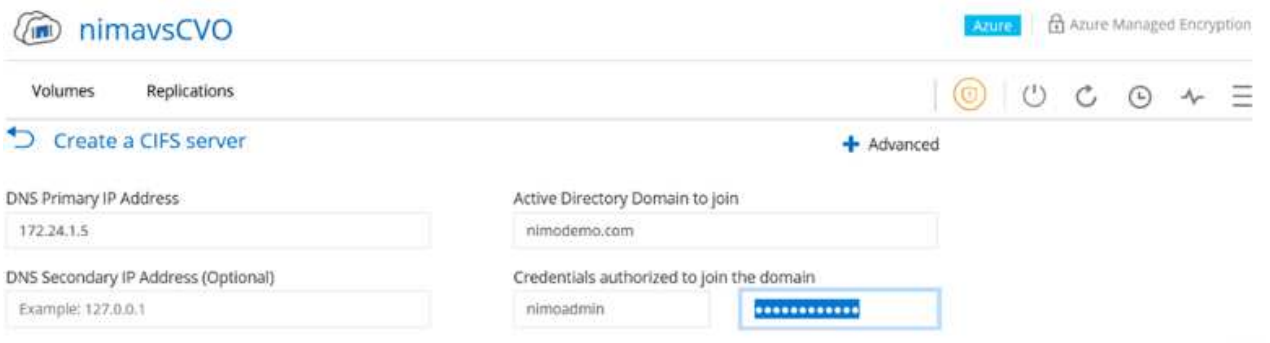


11. Una volta eseguito il provisioning, Cloud Volumes ONTAP viene elencato negli ambienti di lavoro nella pagina Canvas.

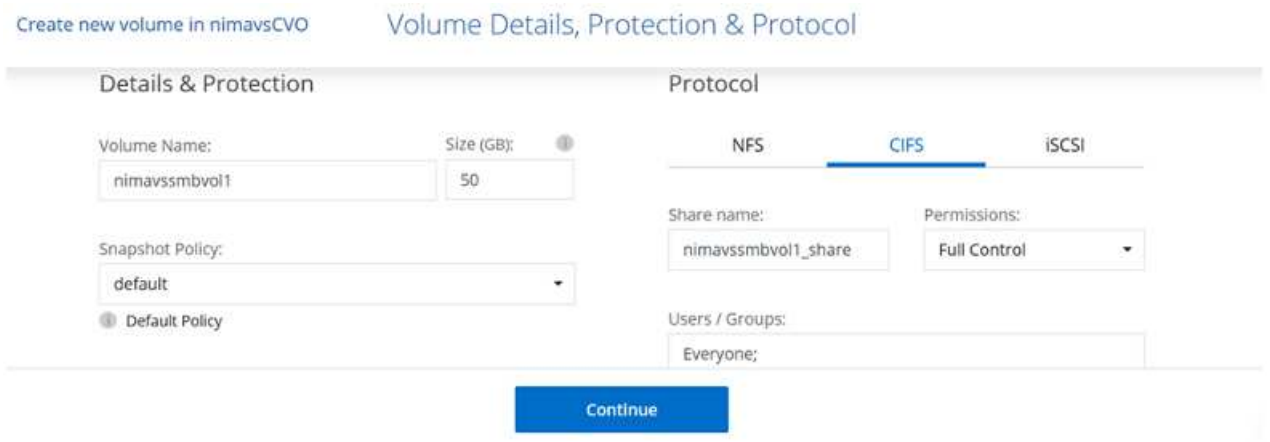


Configurazioni aggiuntive per volumi SMB

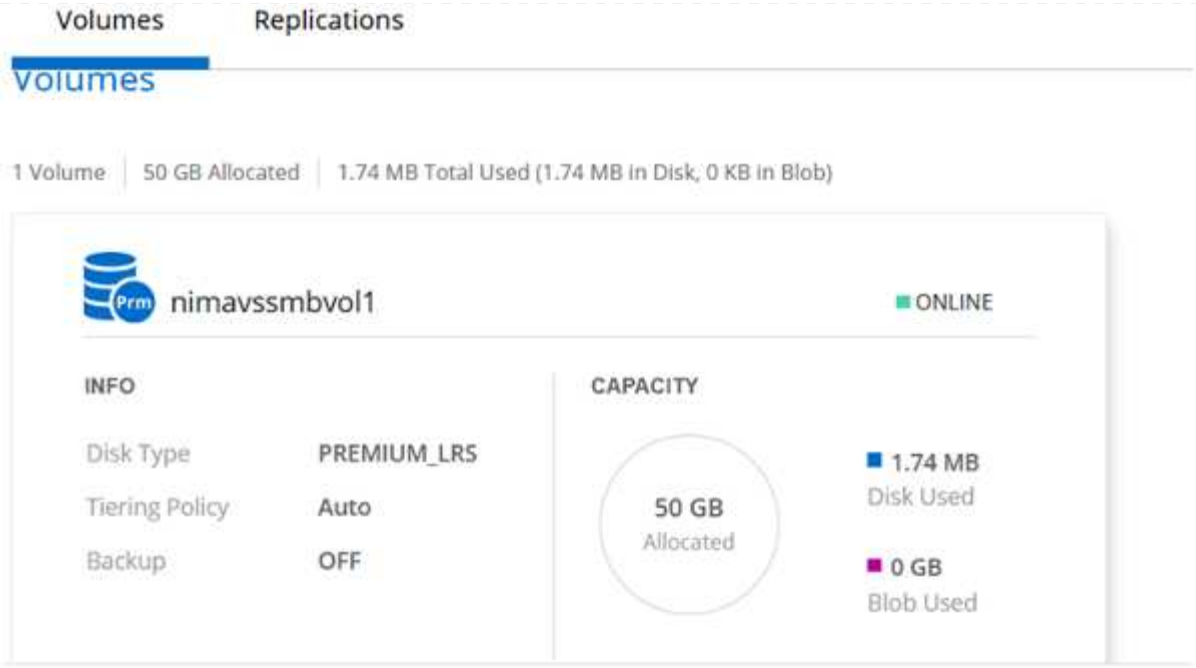
1. Una volta pronto l'ambiente di lavoro, assicurarsi che il server CIFS sia configurato con i parametri di configurazione DNS e Active Directory appropriati. Questo passaggio è necessario prima di poter creare il volume SMB.



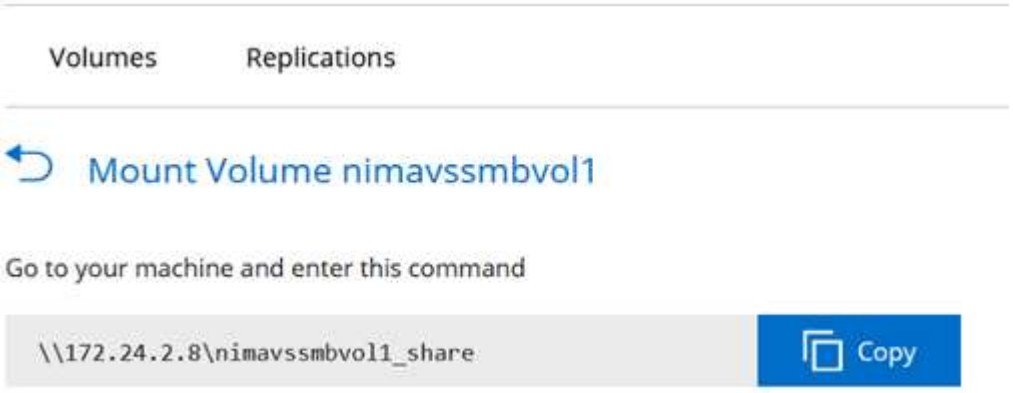
2. La creazione del volume SMB è un processo semplice. Selezionare l'istanza CVO per creare il volume e fare clic sull'opzione Create Volume (Crea volume). Scegli le dimensioni appropriate e il cloud manager sceglie l'aggregato contenente o utilizza un meccanismo di allocazione avanzato da collocare su un aggregato specifico. Per questa demo, SMB viene selezionato come protocollo.



3. Una volta eseguito il provisioning, il volume sarà disponibile nel riquadro Volumes (volumi). Poiché viene fornita una condivisione CIFS, assegnare agli utenti o ai gruppi l'autorizzazione per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file. Questo passaggio non è necessario se il volume viene replicato da un ambiente on-premise perché le autorizzazioni per file e cartelle vengono mantenute come parte della replica di SnapMirror.



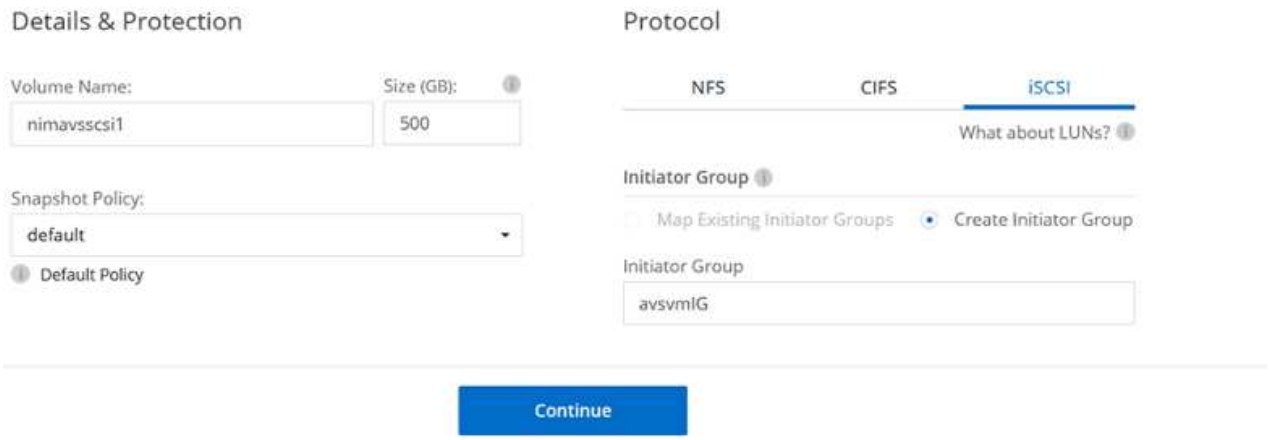
4. Una volta creato il volume, utilizzare il comando mount per connettersi alla condivisione dalla macchina virtuale in esecuzione sugli host Azure VMware Solution SDDC.
5. Copiare il seguente percorso e utilizzare l'opzione Map Network Drive per montare il volume sulla macchina virtuale in esecuzione su Azure VMware Solution SDDC.



Collegare il LUN a un host

Per collegare il LUN a un host, attenersi alla seguente procedura:

1. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP per creare e gestire i volumi.
2. Fare clic su Add Volume (Aggiungi volume) > New Volume (nuovo volume), quindi selezionare iSCSI e fare clic su Create Initiator Group (Crea Fare clic su continua.



3. Una volta eseguito il provisioning del volume, selezionare il volume, quindi fare clic su Target IQN (IQN di destinazione). Per copiare il nome qualificato iSCSI (IQN), fare clic su Copy (Copia). Impostare una connessione iSCSI dall'host al LUN.

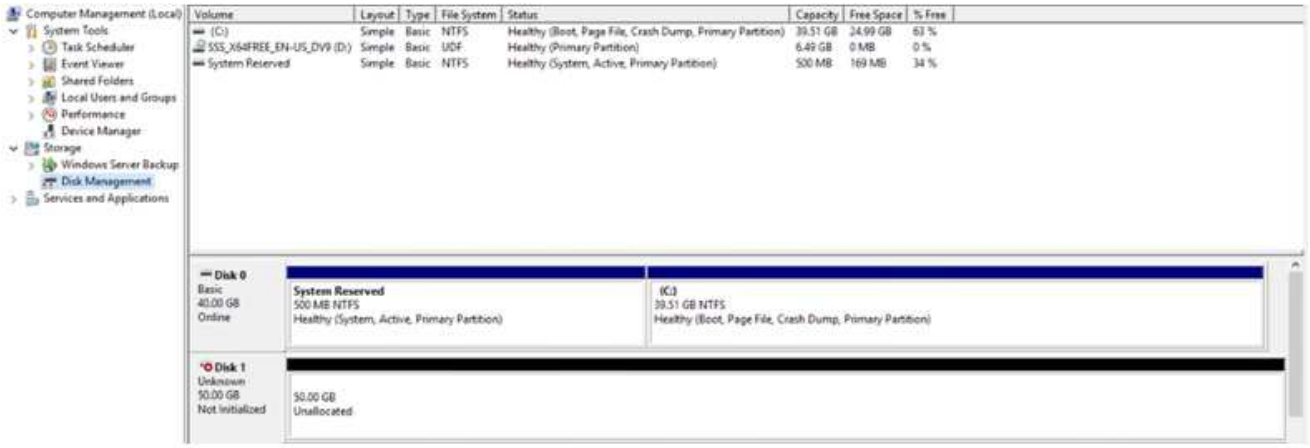
   Per ottenere lo stesso risultato per l'host residente su Azure VMware Solution SDDC:

   a. RDP sulla macchina virtuale ospitata su Azure VMware Solution SDDC.
   b. Aprire la finestra di dialogo iSCSI Initiator Properties (Proprietà iSCSI Initiator): Server Manager > Dashboard > Tools > iSCSI Initiator.
   c. Dalla scheda Discovery (rilevamento), fare clic su Discover Portal (Scopri portale) o Add Portal (Aggiungi portale), quindi inserire l'indirizzo IP della porta di destinazione iSCSI.
   d. Dalla scheda Target, selezionare la destinazione rilevata, quindi fare clic su Log on (Accedi) o Connect (Connetti).
   e. Selezionare Enable multipath (attiva multipath), quindi selezionare Automatically Restore this Connection when the computer starts or Add this Connection to the List of Favorite targets (Ripristina automaticamente questa connessione all'avvio del computer). Fare clic su Avanzate.

      Nota: l'host Windows deve disporre di una connessione iSCSI a ciascun nodo del cluster. Il DSM nativo seleziona i percorsi migliori da utilizzare.

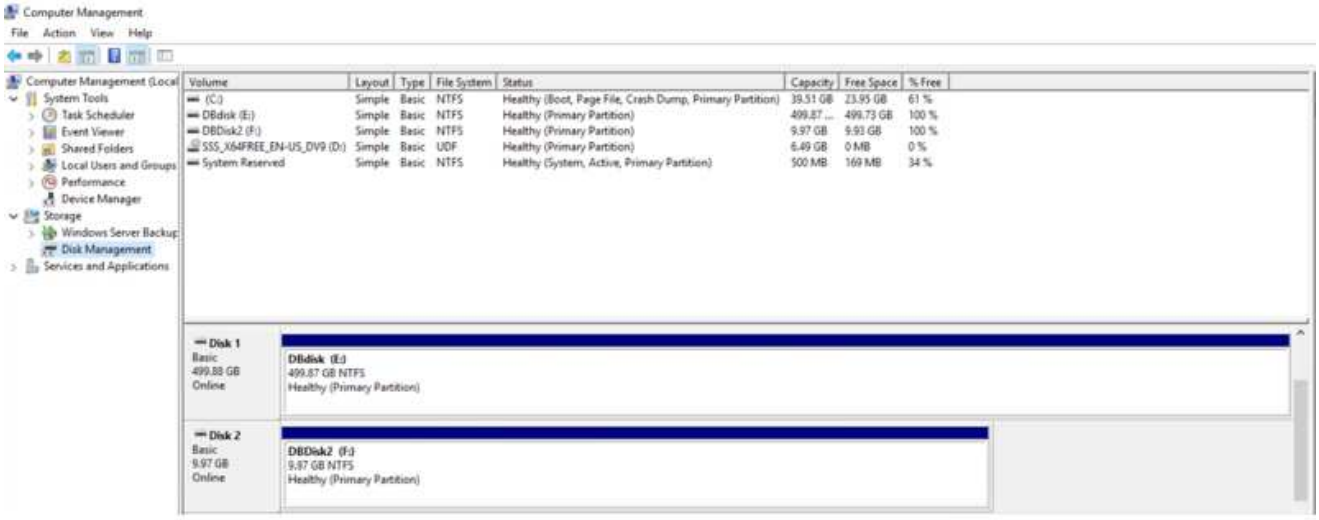
I LUN sulla macchina virtuale di storage (SVM) vengono visualizzati come dischi sull'host Windows. I nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Attivare una nuova scansione manuale per rilevare i dischi completando la seguente procedura:

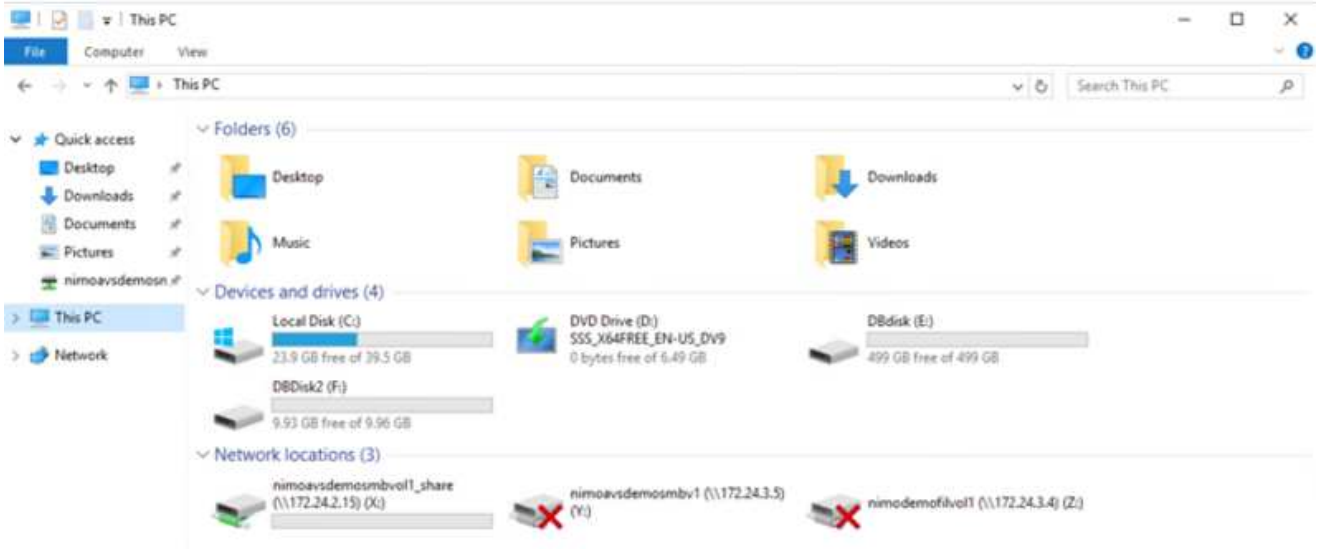
1. Aprire l'utility Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
2. Espandere il nodo Storage nella struttura di navigazione.
3. Fare clic su Gestione disco.
4. Fare clic su Action (azione) > Rescan Disks (Nuova scansione



Quando l'host Windows accede per la prima volta a un nuovo LUN, non dispone di partizione o file system. Inizializzare il LUN e, facoltativamente, formattare il LUN con un file system completando la seguente procedura:

1. Avviare Gestione disco di Windows.
2. Fare clic con il pulsante destro del mouse sul LUN, quindi selezionare il tipo di disco o partizione richiesto.
3. Seguire le istruzioni della procedura guidata. In questo esempio, viene montato il disco e:



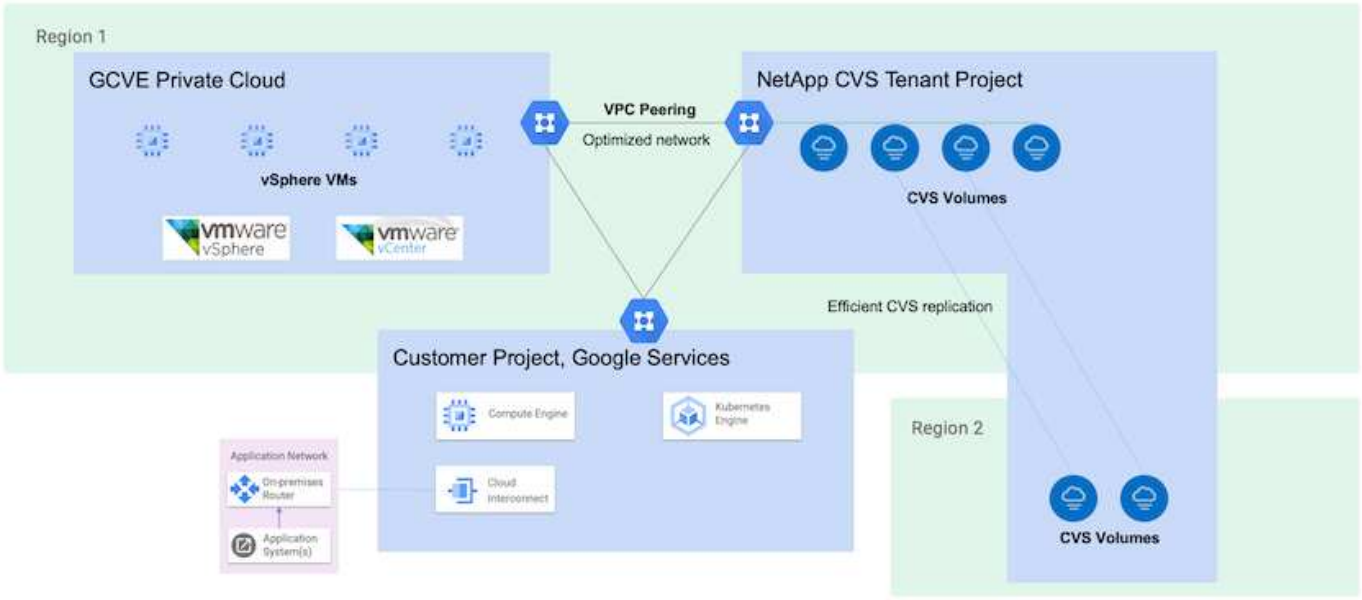


Datastore NFS supplementare di Google Cloud con il servizio volumi cloud di NetApp

Panoramica

Autori: Suresh Thoppay, NetApp

I clienti che richiedono capacità di storage aggiuntiva nell'ambiente Google Cloud VMware Engine (GCVE) possono utilizzare il servizio volumi cloud di NetApp per il montaggio come archivio dati NFS supplementare. L'archiviazione dei dati nel servizio volumi cloud di NetApp consente ai clienti di replicare tra regioni per proteggersi dal diaster.



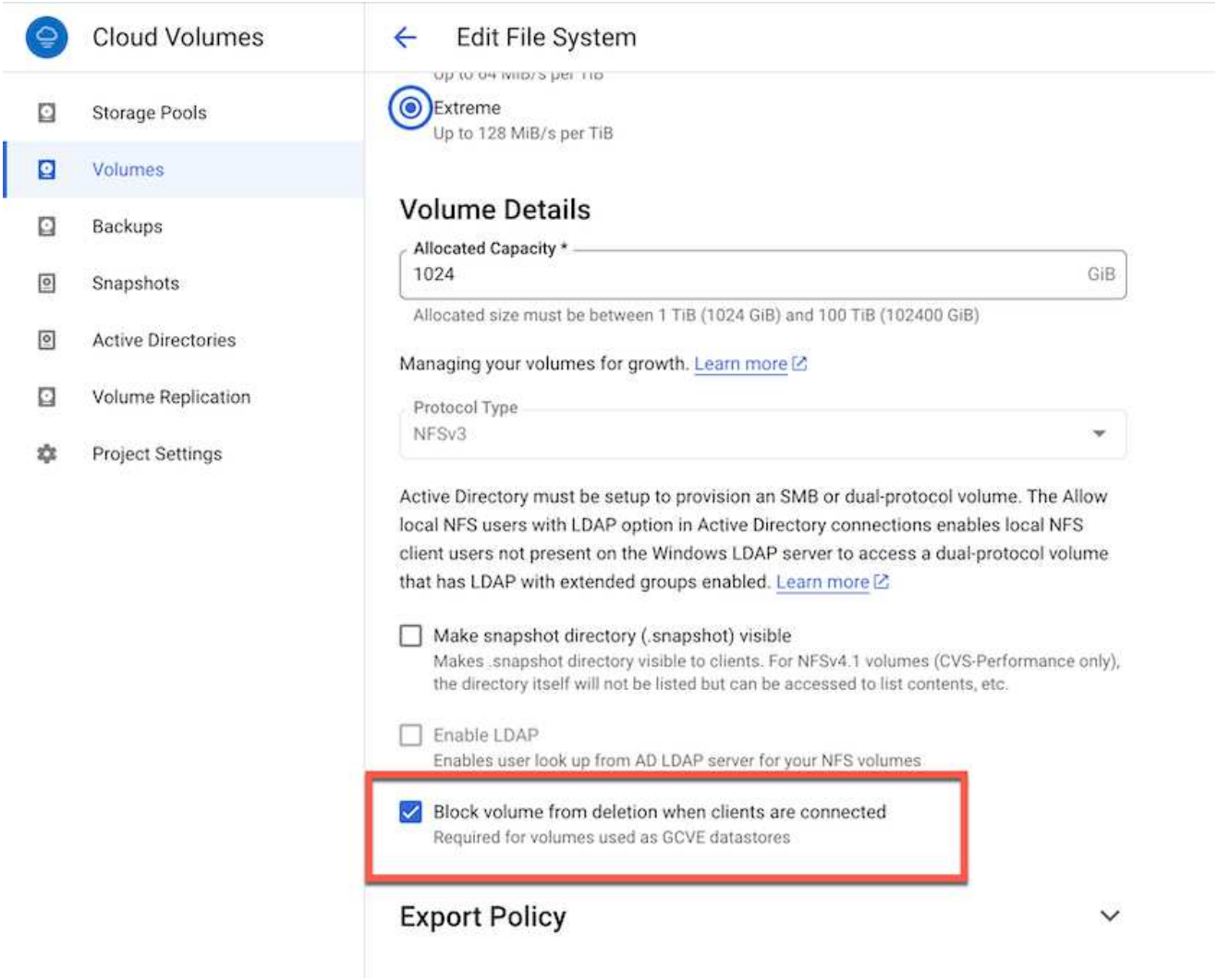
Fasi di implementazione per montare il datastore NFS da NetApp CVS su GCVE

Provisioning del volume CVS-Performance

Il provisioning del volume del servizio volume cloud NetApp può essere eseguito da
"Con Google Cloud Console"
"Utilizzando il portale o l'API BlueXP di NetApp"

Contrassegnare il volume CVS come non cancellabile

Per evitare l'eliminazione accidentale del volume mentre la macchina virtuale è in esecuzione, assicurarsi che il volume sia contrassegnato come non cancellabile, come mostrato nella seguente schermata.



Per ulteriori informazioni, fare riferimento a. "Creazione di un volume NFS" documentazione.

Assicurarsi che sia presente una connessione privata su GCVE per VPC tenant CVS NetApp.

Per montare NFS Datastore, dovrebbe esistere una connessione privata tra il progetto GCVE e il progetto CVS di NetApp.
Per ulteriori informazioni, fare riferimento a. "Come configurare l'accesso al servizio privato"

Montare il datastore NFS

Per istruzioni su come montare il datastore NFS su GCVE, fare riferimento "Come creare un datastore NFS con NetApp CVS"

> Poiché gli host vSphere sono gestiti da Google, non è possibile installare NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB).
> Se hai bisogno di supporto per i volumi virtuali (vVol), contattaci.
> Se si desidera utilizzare i frame jumbo, fare riferimento a. "Dimensioni MTU massime supportate su GCP"

Risparmi con il servizio volumi cloud di NetApp

Per ulteriori informazioni sul potenziale risparmio con il servizio volumi cloud di NetApp per le tue esigenze di storage su GCVE, consulta la sezione "Calcolatore del ROI di NetApp"

Link di riferimento

- "Blog di Google - come utilizzare NetApp CVS come datastore per Google Cloud VMware Engine"
- "Blog di NetApp: Un modo migliore per migrare le tue applicazioni ricche di storage su Google Cloud"

Opzioni di storage NetApp per GCP

GCP supporta lo storage NetApp connesso come guest con Cloud Volumes ONTAP (CVO) o Cloud Volumes Service (CVS).

Cloud Volumes ONTAP (CVO)

Cloud Volumes ONTAP, o CVO, è la soluzione per la gestione dei dati nel cloud leader del settore basata sul software di storage ONTAP, disponibile in modalità nativa su Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

Si tratta di una versione software-defined di ONTAP che utilizza lo storage nativo del cloud, consentendoti di avere lo stesso software di storage nel cloud e on-premise, riducendo la necessità di riorganizzare il tuo staff IT con metodi completamente nuovi per gestire i tuoi dati.

CVO offre ai clienti la possibilità di spostare senza problemi i dati dall'edge al data center, al cloud e viceversa, unendo il tuo cloud ibrido, il tutto gestito con una console di gestione a singolo pannello, NetApp Cloud Manager.

Per progettazione, CVO offre performance estreme e funzionalità avanzate di gestione dei dati per soddisfare anche le applicazioni più esigenti nel cloud

Cloud Volumes ONTAP (CVO) come storage connesso guest

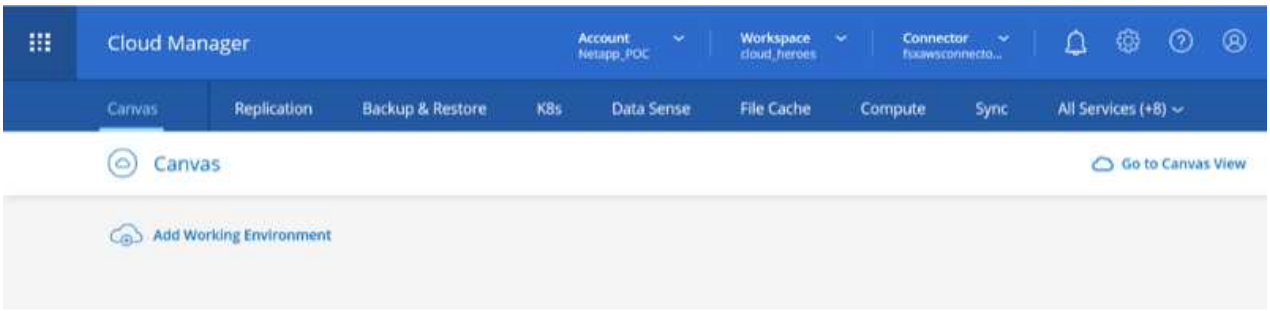
Implementare Cloud Volumes ONTAP in Google Cloud (fai da te)

Le condivisioni e le LUN Cloud Volumes ONTAP possono essere montate da macchine virtuali create nell'ambiente di cloud privato GCVE. I volumi possono essere montati anche sul client Linux e sul client Windows, mentre I LUN possono essere utilizzati su client Linux o Windows come dispositivi a blocchi quando montati su iSCSI, perché Cloud Volumes ONTAP supporta i protocolli iSCSI, SMB e NFS. I volumi Cloud Volumes ONTAP possono essere configurati in pochi semplici passaggi.

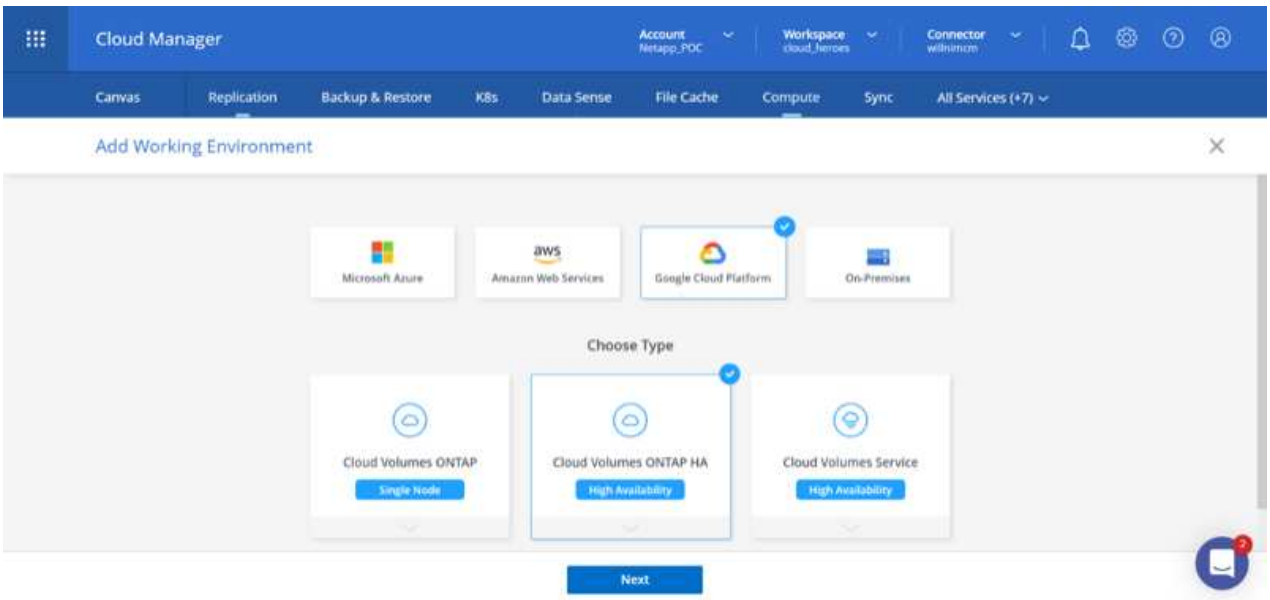
Per replicare i volumi da un ambiente on-premise al cloud per scopi di disaster recovery o migrazione, stabilire la connettività di rete a Google Cloud, utilizzando una VPN sito-sito o un'interconnessione cloud. La replica dei dati da on-premise a Cloud Volumes ONTAP non rientra nell'ambito di questo documento. Per replicare i dati tra sistemi on-premise e Cloud Volumes ONTAP, vedere xref:./ehc/"Configurazione della replica dei dati tra sistemi".

> Utilizzare "Cloud Volumes ONTAP Sizer" Per dimensionare con precisione le istanze di Cloud Volumes ONTAP. Monitorare anche le performance on-premise da utilizzare come input nel Cloud Volumes ONTAP Sizer.

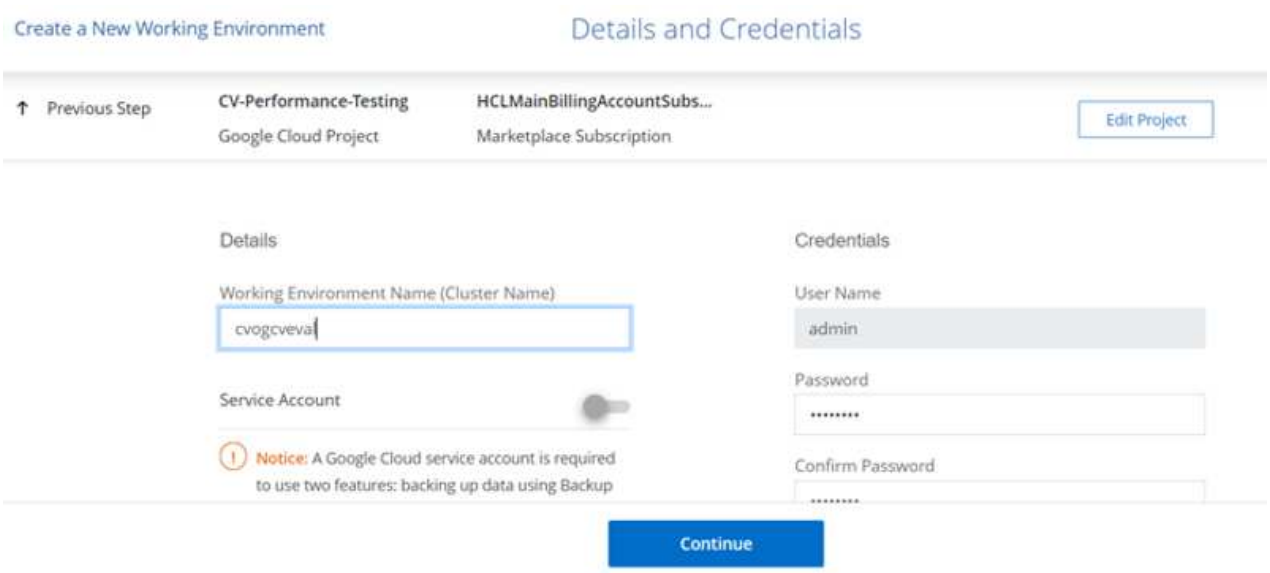
1. Accedi a NetApp Cloud Central: Viene visualizzata la schermata Fabric View. Individuare la scheda Cloud Volumes ONTAP (Gestione cloud) e selezionare Go to Cloud Manager (Vai a Gestione cloud). Una volta effettuato l'accesso, viene visualizzata la schermata Canvas.



2. Nella scheda Cloud Manager Canvas, fare clic su Add a Working Environment (Aggiungi ambiente di lavoro), quindi selezionare Google Cloud Platform come cloud e il tipo di configurazione del sistema. Quindi, fare clic su Next (Avanti).

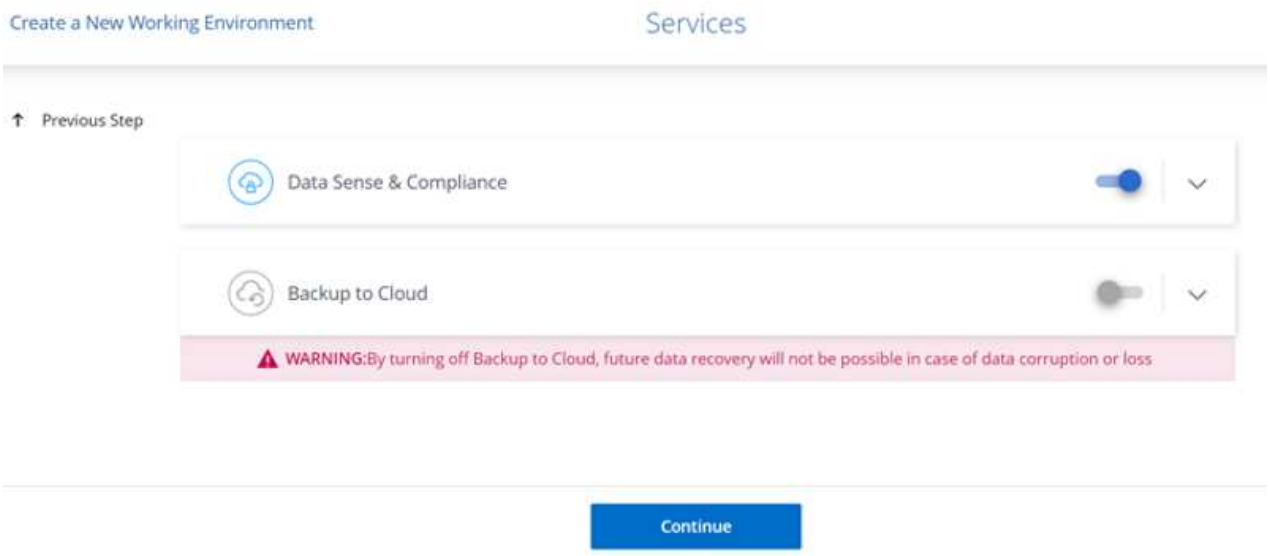


3. Fornire i dettagli dell'ambiente da creare, inclusi il nome dell'ambiente e le credenziali di amministratore. Al termine, fare clic su Continue (continua).

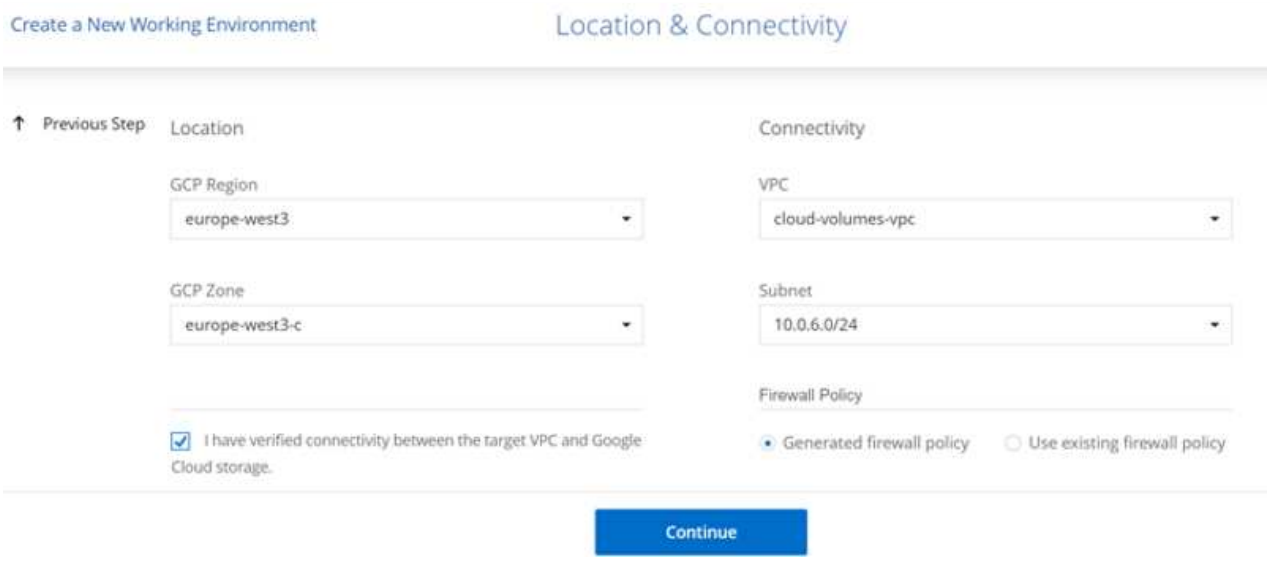


4. Seleziona o deseleziona i servizi aggiuntivi per l'implementazione di Cloud Volumes ONTAP, tra cui rilevamento e conformità dei dati o backup nel cloud. Quindi, fare clic su Continue (continua).

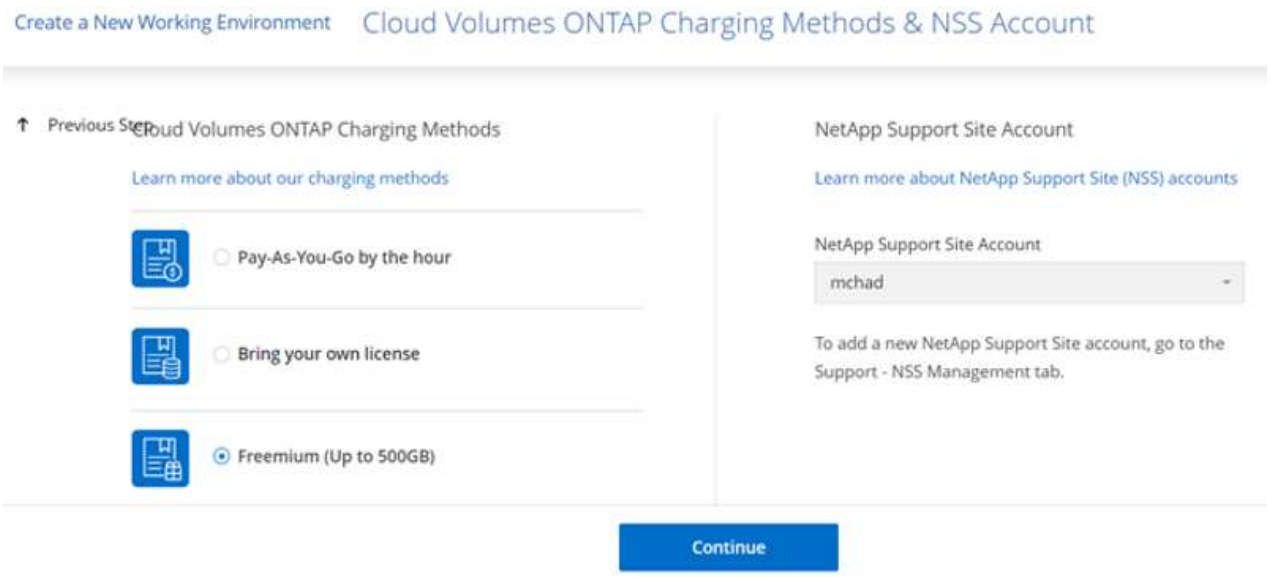
   SUGGERIMENTO: Quando si disattivano i servizi aggiuntivi, viene visualizzato un messaggio a comparsa di verifica. I servizi add-on possono essere aggiunti/rimossi dopo l'implementazione di CVO; se non necessari, è consigliabile deselezionarli dall'inizio per evitare i costi.



5. Selezionare una posizione, scegliere un criterio firewall e selezionare la casella di controllo per confermare la connettività di rete allo storage Google Cloud.

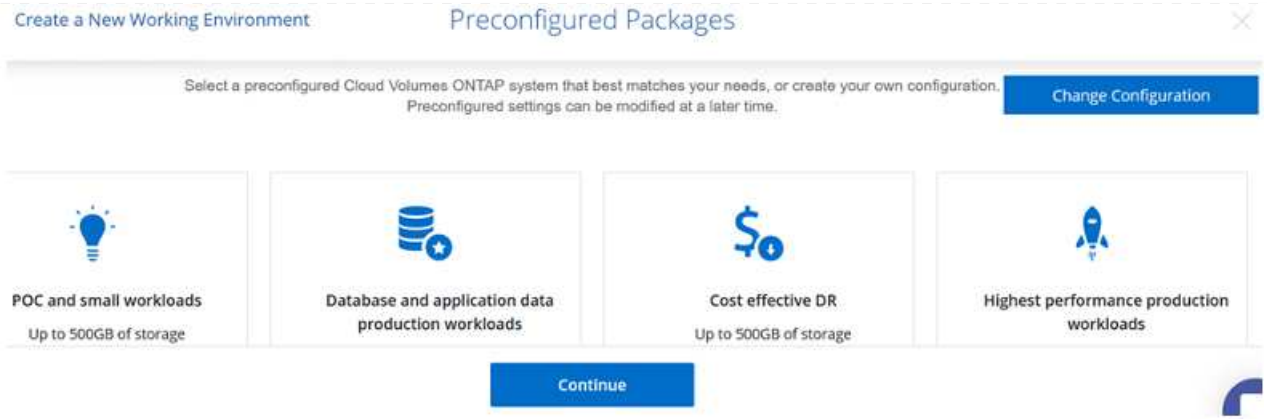


6. Selezionare l'opzione di licenza: Pay-as-you-Go o BYOL per utilizzare la licenza esistente. In questo esempio, viene utilizzata l'opzione Freemium. Quindi, fare clic su Continue (continua).

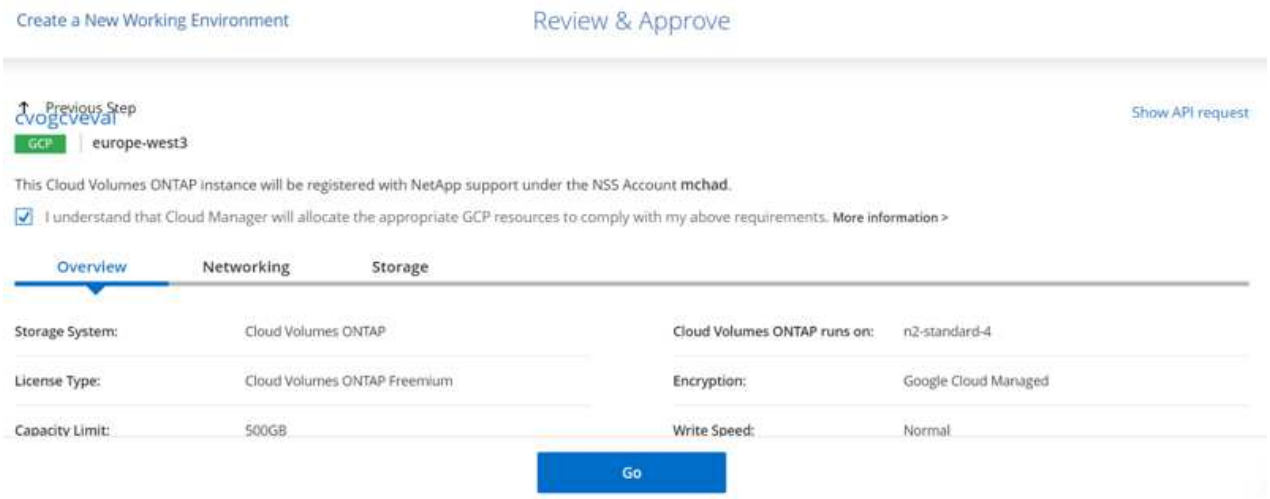


7. Scegliere tra diversi pacchetti preconfigurati disponibili in base al tipo di carico di lavoro che verrà implementato sulle macchine virtuali in esecuzione sul cloud VMware su AWS SDDC.

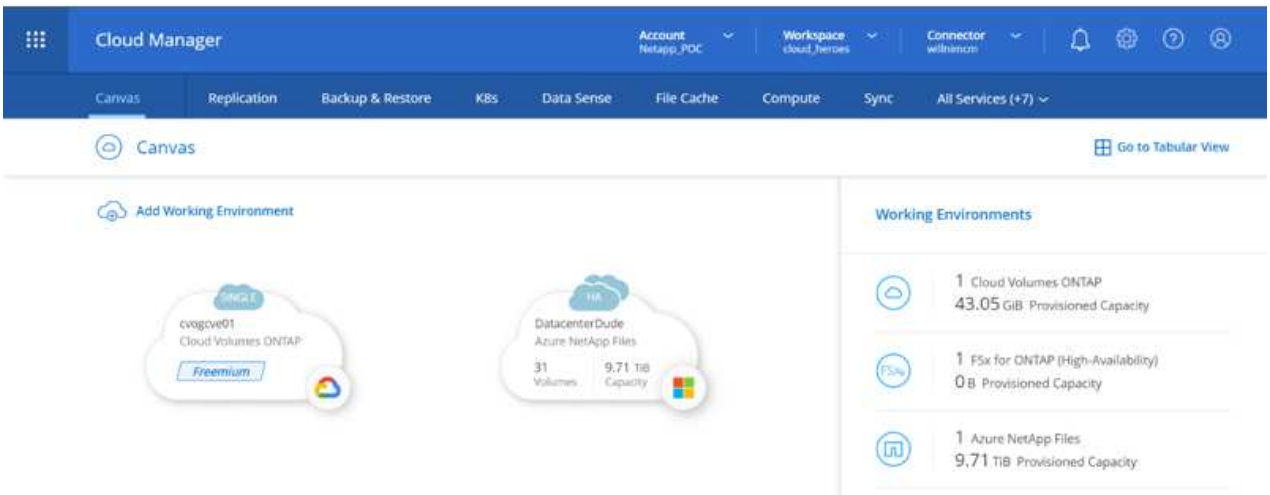
   SUGGERIMENTO: Passare il mouse sui riquadri per ulteriori dettagli o personalizzare i componenti CVO e la versione di ONTAP facendo clic su Modifica configurazione.



8. Nella pagina Review & Approve (esamina e approva), rivedere e confermare le selezioni.per creare l'istanza di Cloud Volumes ONTAP, fare clic su Go (Vai).



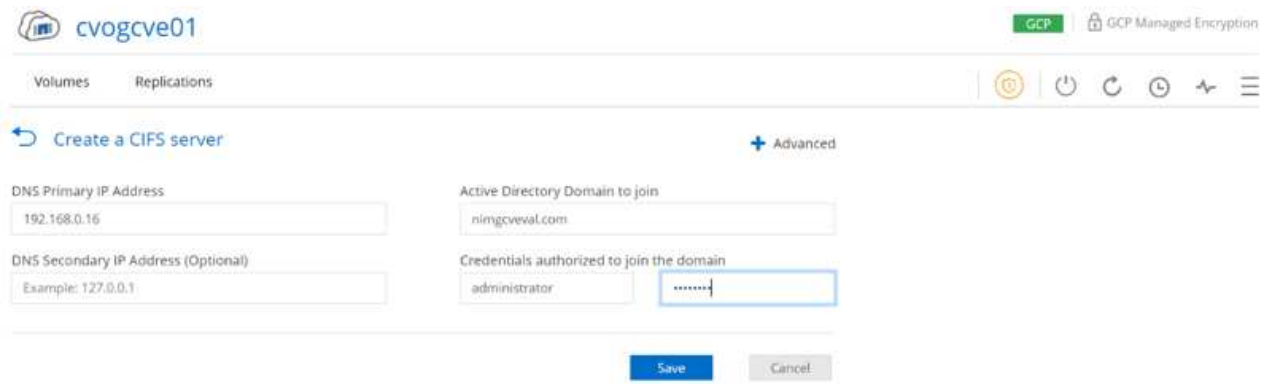
9. Una volta eseguito il provisioning, Cloud Volumes ONTAP viene elencato negli ambienti di lavoro nella pagina Canvas.



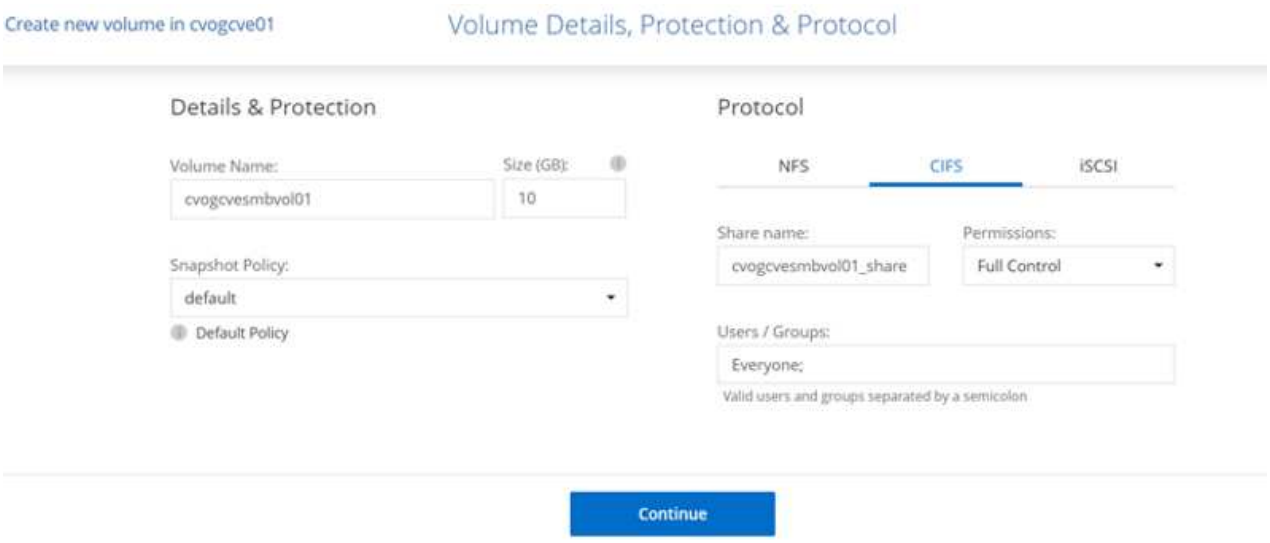
Configurazioni aggiuntive per volumi SMB

1. Una volta pronto l'ambiente di lavoro, assicurarsi che il server CIFS sia configurato con i parametri di configurazione DNS e Active Directory appropriati. Questo passaggio è necessario prima di poter creare il volume SMB.

   SUGGERIMENTO: Fare clic sull'icona Menu (º), selezionare Advanced (Avanzate) per visualizzare altre opzioni e selezionare CIFS setup (Configurazione CIFS).



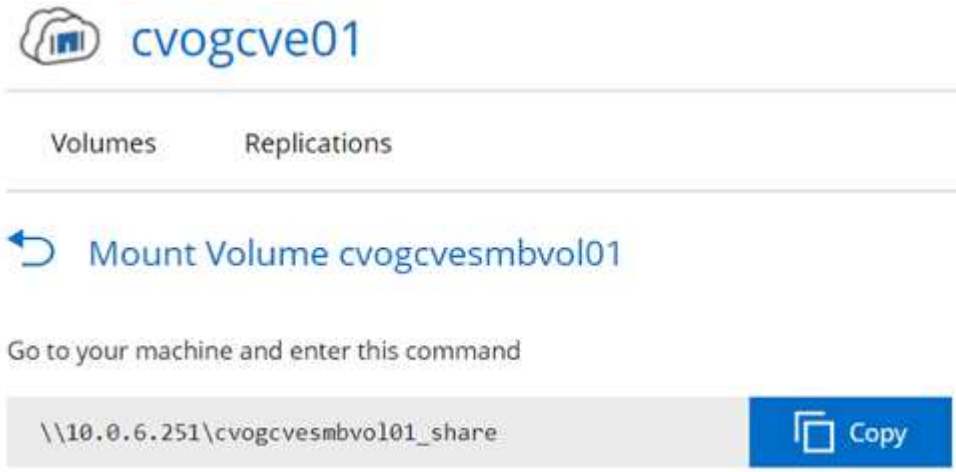
2. La creazione del volume SMB è un processo semplice. In Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP per creare e gestire i volumi e fare clic sull'opzione Crea volume. Scegli le dimensioni appropriate e il cloud manager sceglie l'aggregato contenente o utilizza un meccanismo di allocazione avanzato da collocare su un aggregato specifico. Per questa demo, CIFS/SMB è selezionato come protocollo.



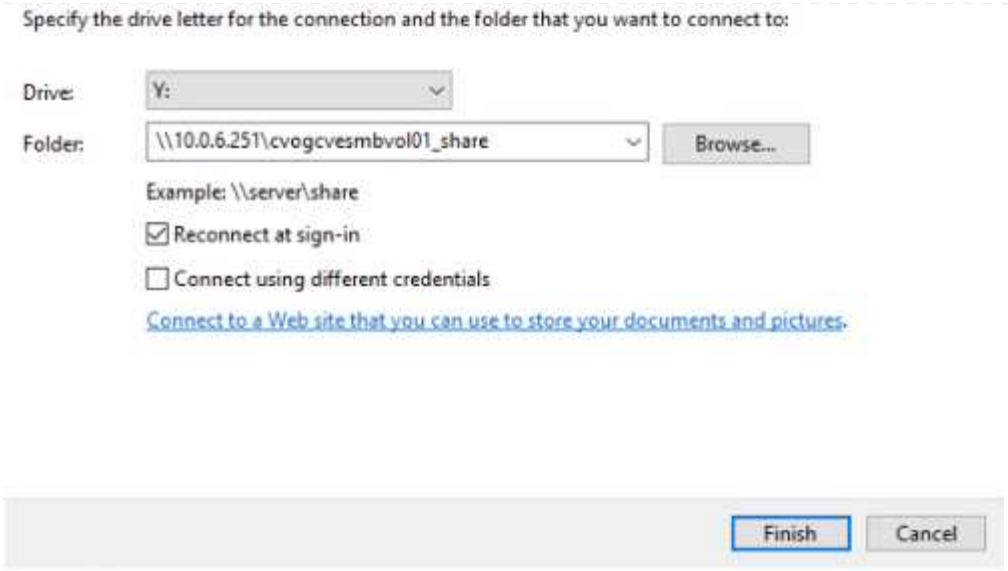
3. Una volta eseguito il provisioning, il volume sarà disponibile nel riquadro Volumes (volumi). Poiché viene fornita una condivisione CIFS, assegnare agli utenti o ai gruppi l'autorizzazione per i file e le cartelle e verificare che tali utenti possano accedere alla condivisione e creare un file. Questo passaggio non è necessario se il volume viene replicato da un ambiente on-premise perché le autorizzazioni per file e cartelle vengono mantenute come parte della replica di SnapMirror.

   SUGGERIMENTO: Fare clic sul menu del volume (º) per visualizzarne le opzioni.

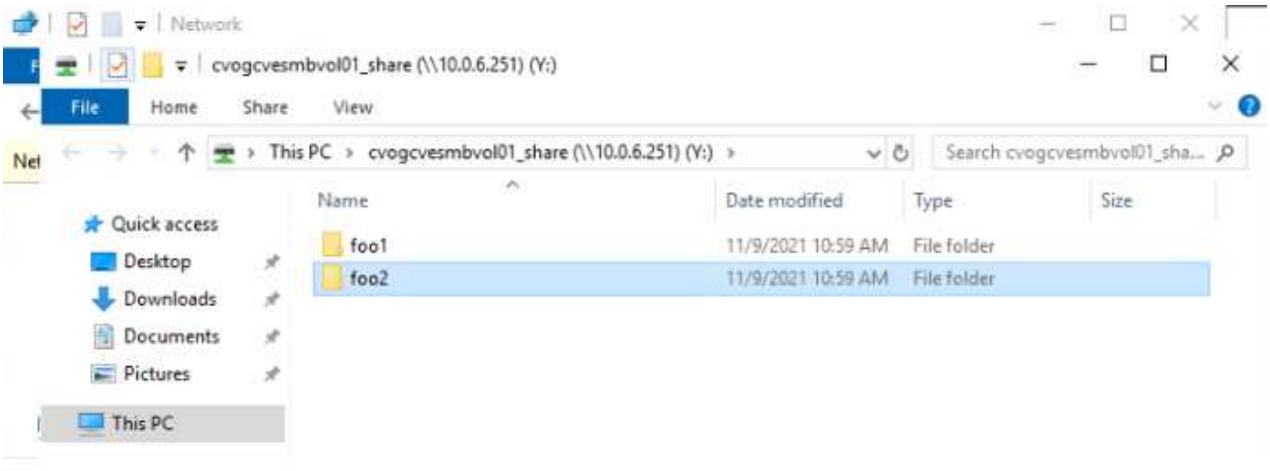
4. Una volta creato il volume, utilizzare il comando mount per visualizzare le istruzioni di connessione del volume, quindi connettersi alla condivisione dalle macchine virtuali su Google Cloud VMware Engine.



5. Copiare il seguente percorso e utilizzare l'opzione Map Network Drive per montare il volume sulla macchina virtuale in esecuzione su Google Cloud VMware Engine.



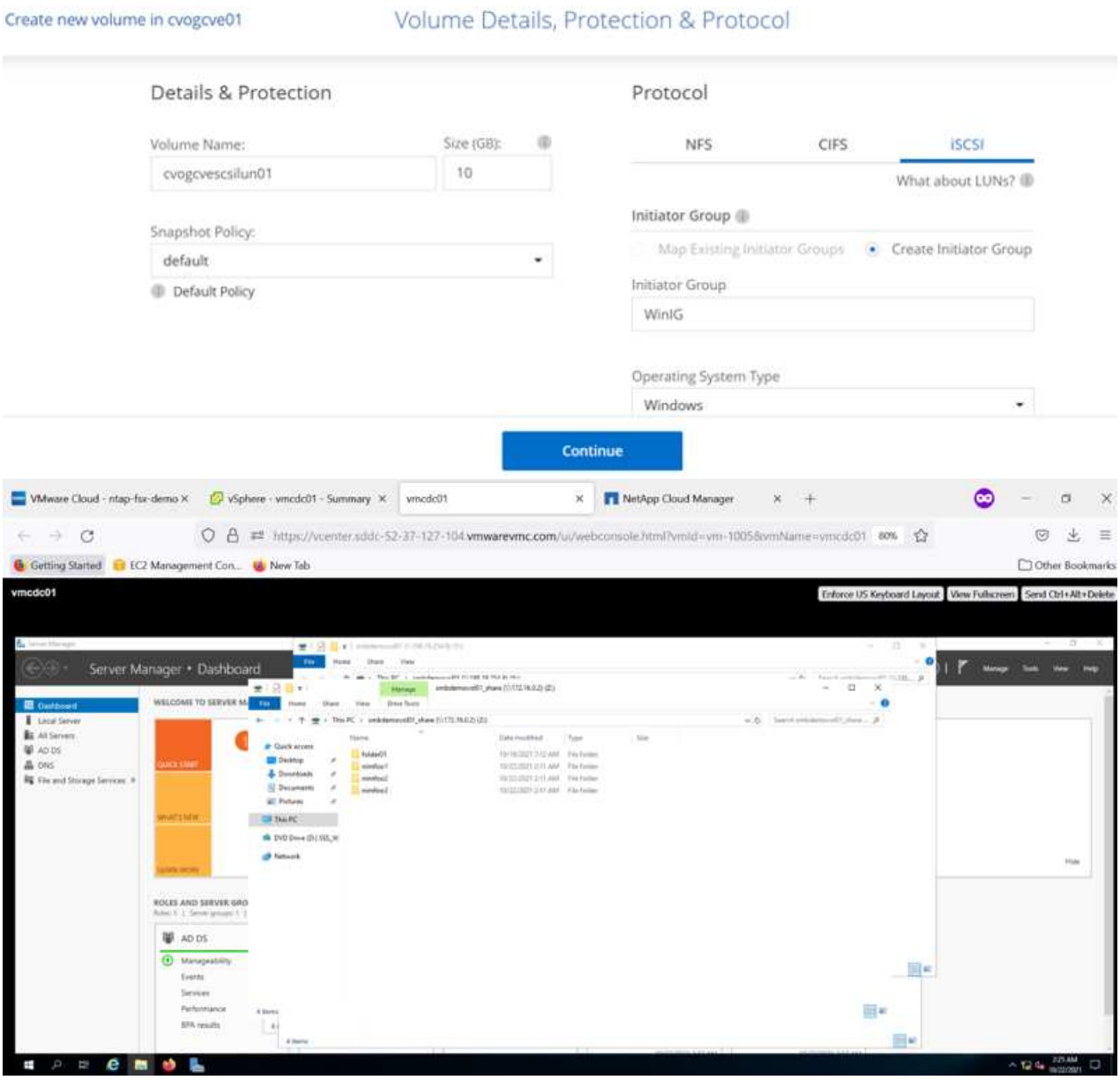
Una volta mappato, è possibile accedervi facilmente e impostare le autorizzazioni NTFS di conseguenza.



Collegare il LUN su Cloud Volumes ONTAP a un host

Per collegare il LUN Cloud Volumes ONTAP a un host, attenersi alla seguente procedura:

1. Nella pagina Canvas, fare doppio clic sull'ambiente di lavoro Cloud Volumes ONTAP per creare e gestire i volumi.
2. Fare clic su Add Volume (Aggiungi volume) > New Volume (nuovo volume), quindi selezionare iSCSI e fare clic su Create Initiator Group (Crea Fare clic su continua.



3. Una volta eseguito il provisioning del volume, selezionare il menu del volume (º), quindi fare clic su Target IQN (IQN di destinazione). Per copiare il nome qualificato iSCSI (IQN), fare clic su Copy (Copia). Impostare una connessione iSCSI dall'host al LUN.

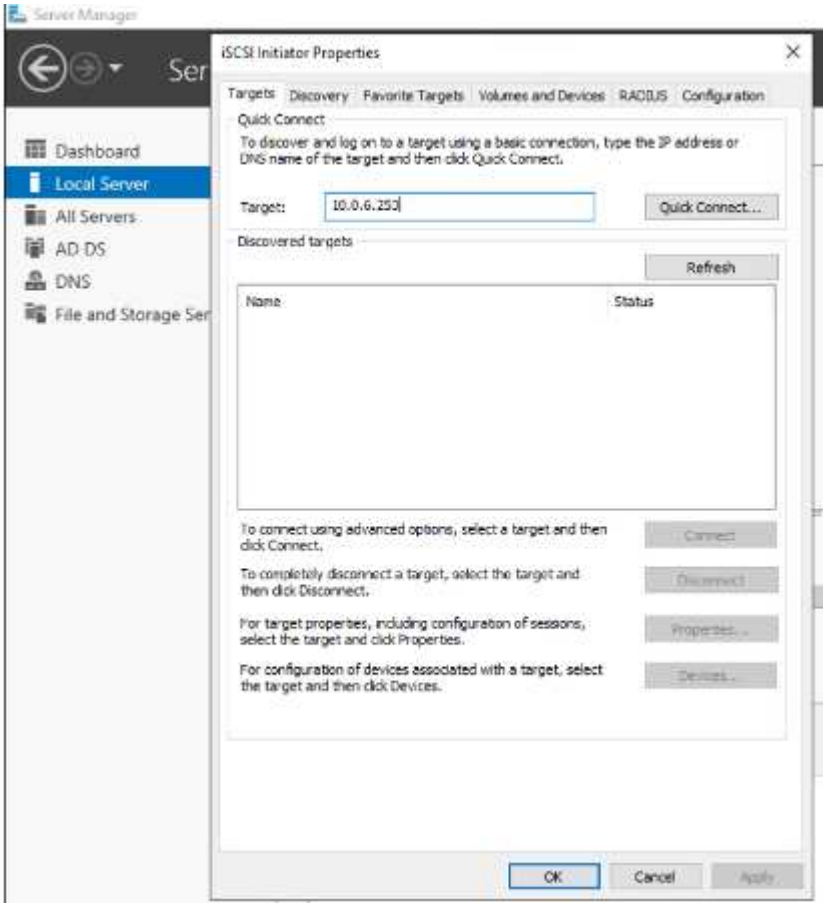
Per ottenere lo stesso risultato per l'host residente su Google Cloud VMware Engine:

1. RDP sulla macchina virtuale ospitata su Google Cloud VMware Engine.
2. Aprire la finestra di dialogo iSCSI Initiator Properties (Proprietà iSCSI Initiator): Server Manager >

Dashboard > Tools > iSCSI Initiator.

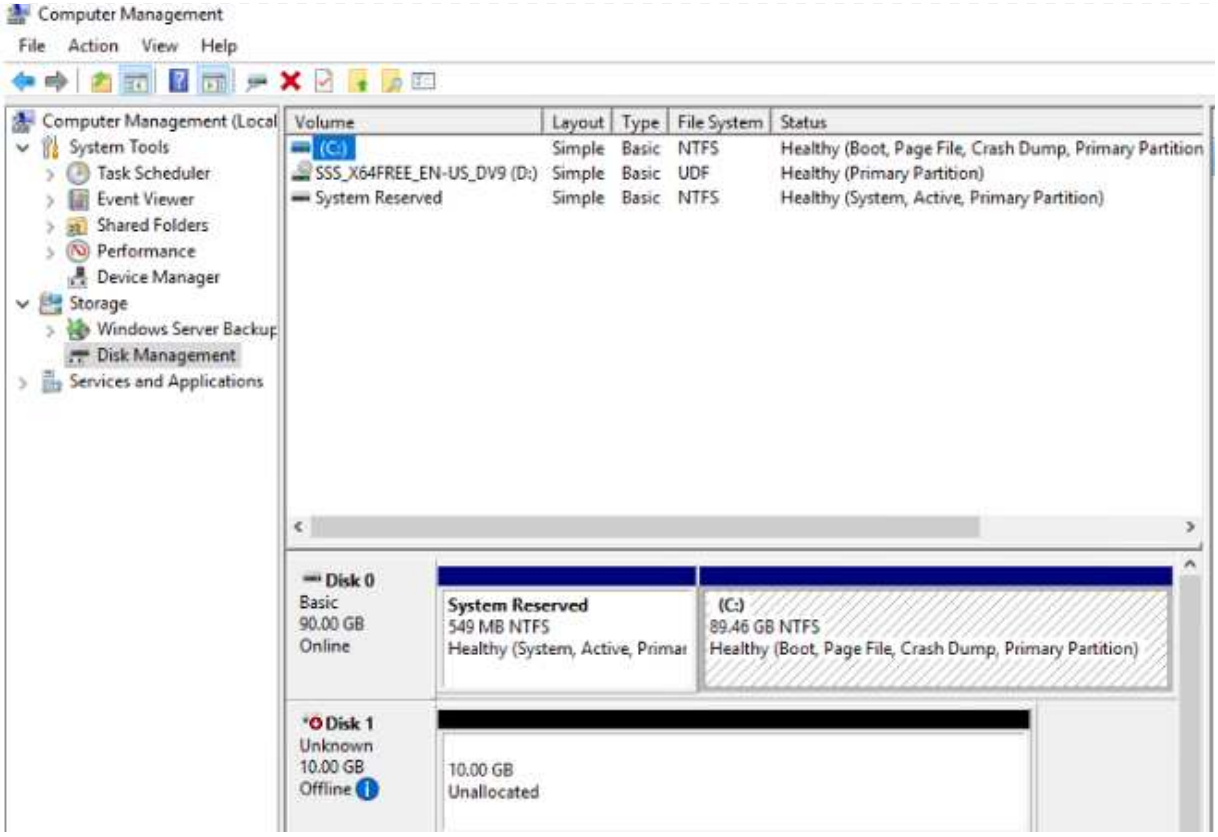
3. Dalla scheda Discovery (rilevamento), fare clic su Discover Portal (Scopri portale) o Add Portal (Aggiungi portale), quindi inserire l'indirizzo IP della porta di destinazione iSCSI.
4. Dalla scheda Target, selezionare la destinazione rilevata, quindi fare clic su Log on (Accedi) o Connect (Connetti).
5. Selezionare Enable multipath (attiva multipath), quindi selezionare Automatically Restore this Connection when the computer starts or Add this Connection to the List of Favorite targets (Ripristina automaticamente questa connessione all'avvio del computer). Fare clic su Avanzate.

> L'host Windows deve disporre di una connessione iSCSI a ciascun nodo del cluster. Il DSM nativo seleziona i percorsi migliori da utilizzare.



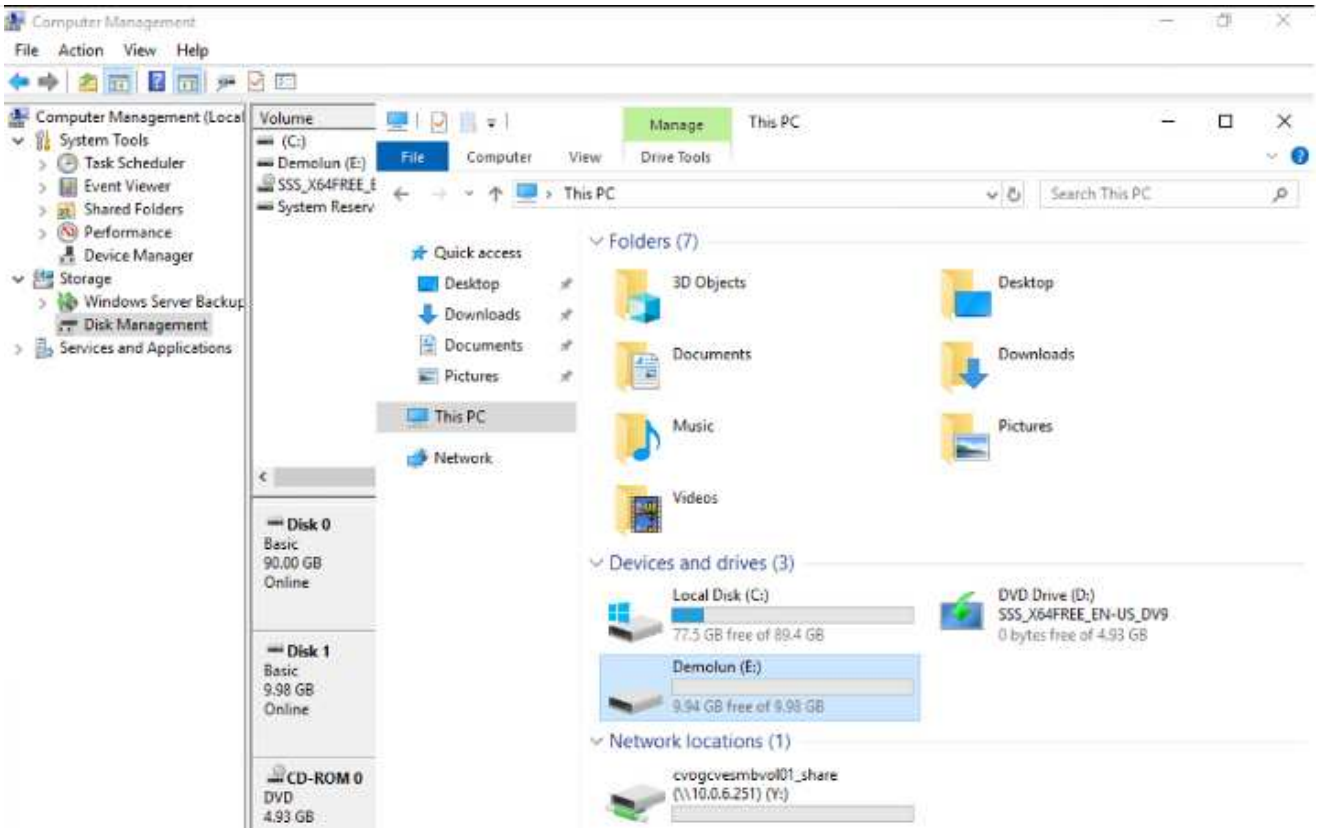
I LUN sulla macchina virtuale di storage (SVM) vengono visualizzati come dischi sull'host Windows. I nuovi dischi aggiunti non vengono rilevati automaticamente dall'host. Attivare una nuova scansione manuale per rilevare i dischi completando la seguente procedura:

a. Aprire l'utility Gestione computer di Windows: Start > Strumenti di amministrazione > Gestione computer.
b. Espandere il nodo Storage nella struttura di navigazione.
c. Fare clic su Gestione disco.
d. Fare clic su Action (azione) > Rescan Disks (Nuova scansione



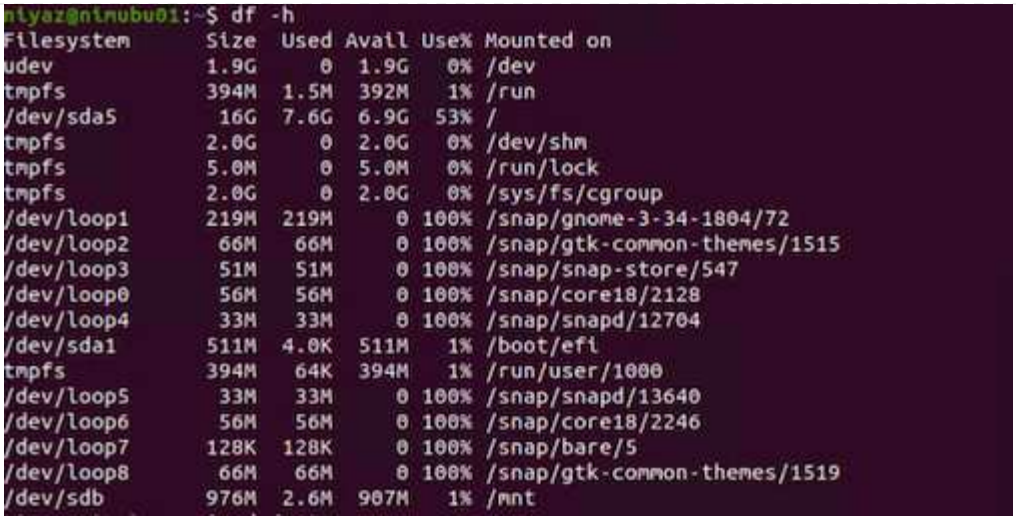
Quando l'host Windows accede per la prima volta a un nuovo LUN, non dispone di partizione o file system. Inizializzare il LUN e, facoltativamente, formattare il LUN con un file system completando la seguente procedura:

a. Avviare Gestione disco di Windows.
b. Fare clic con il pulsante destro del mouse sul LUN, quindi selezionare il tipo di disco o partizione richiesto.
c. Seguire le istruzioni della procedura guidata. In questo esempio, viene montato il disco F:.



Sui client Linux, assicurarsi che il daemon iSCSI sia in esecuzione. Una volta eseguito il provisioning dei LUN, fare riferimento alla guida dettagliata sulla configurazione iSCSI con Ubuntu come esempio qui. Per verificare, eseguire lsblk cmd dalla shell.

```
nlyaz@nlmubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

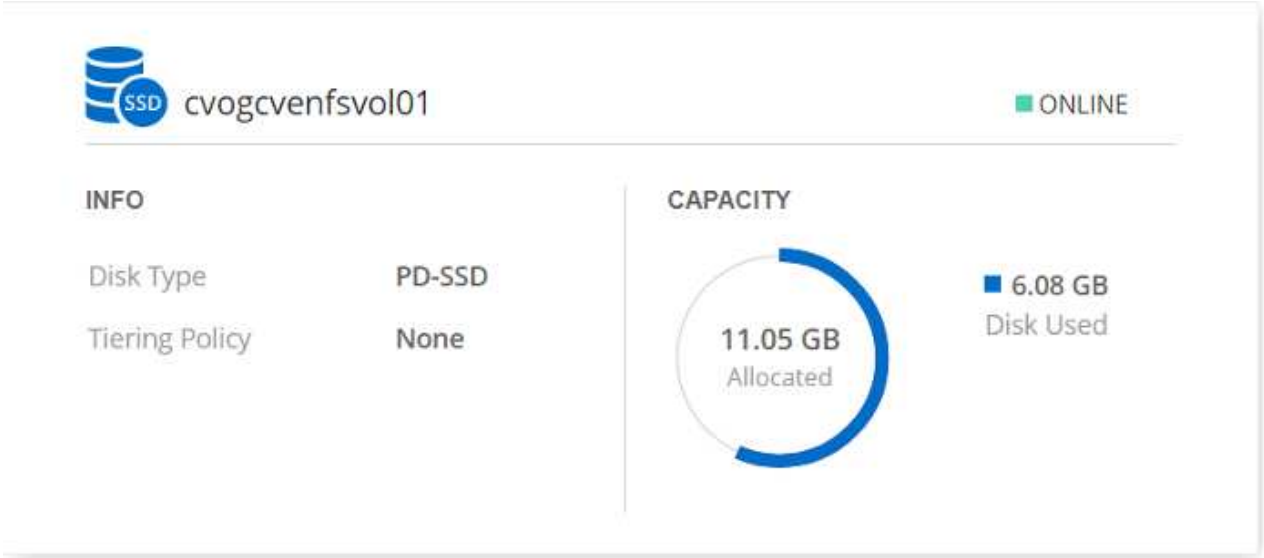

niyaz@ninubu01:~$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 1.9G 0 1.9G 0% /dev
tmpfs 394M 1.5M 392M 1% /run
/dev/sda5 16G 7.6G 6.9G 53% /
tmpfs 2.0G 0 2.0G 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup
/dev/loop1 219M 219M 0 100% /snap/gnome-3-34-1804/72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

Montare il volume NFS Cloud Volumes ONTAP sul client Linux

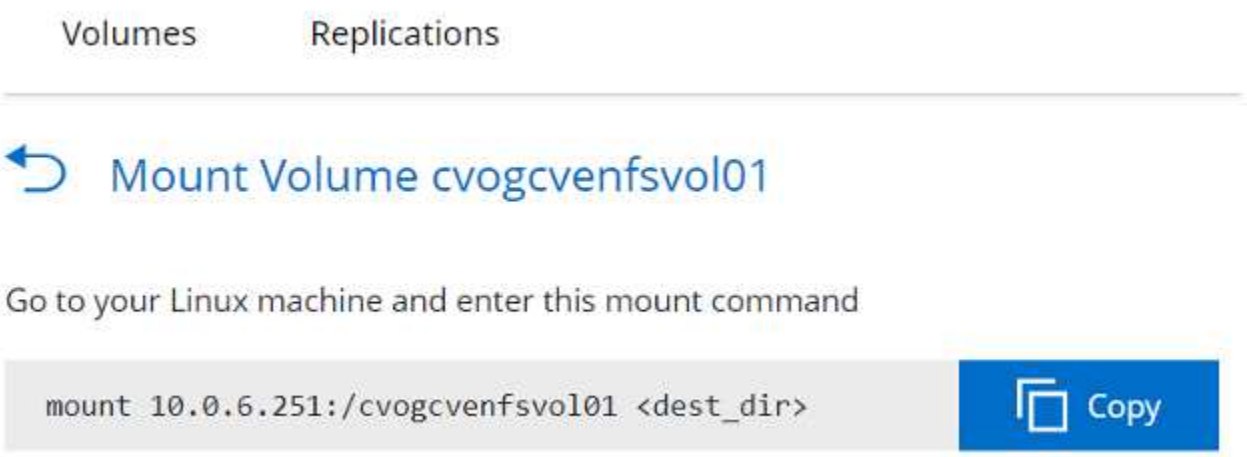
Per montare il file system Cloud Volumes ONTAP (DIY) dalle macchine virtuali all'interno del motore VMware di Google Cloud, attenersi alla seguente procedura:

Eseguire il provisioning del volume seguendo la procedura riportata di seguito

1. Nella scheda Volumes (volumi), fare clic su Create New Volume (Crea nuovo volume).
2. Nella pagina Create New Volume (Crea nuovo volume), selezionare un tipo di volume:



3. Nella scheda Volumes (volumi), posizionare il cursore del mouse sul volume, selezionare l'icona del menu (º), quindi fare clic su Mount Command.



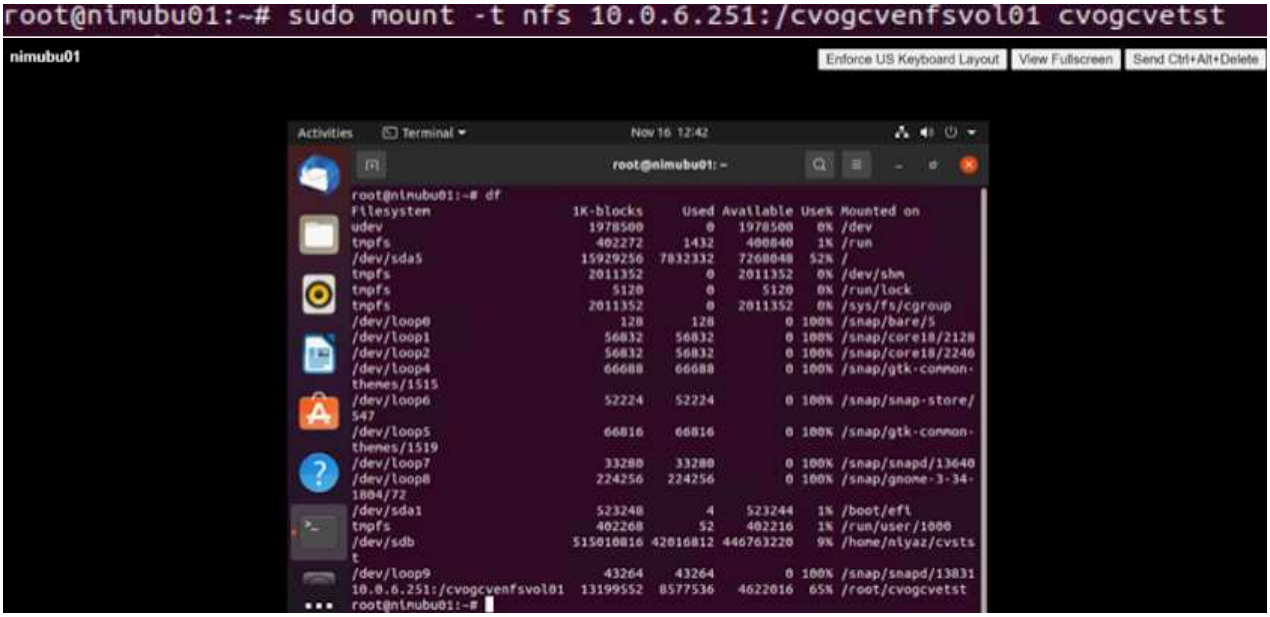
4. Fare clic su Copia.
5. Connettersi all'istanza Linux designata.
6. Aprire un terminale sull'istanza utilizzando la shell sicura (SSH) e accedere con le credenziali appropriate.
7. Creare una directory per il punto di montaggio del volume con il seguente comando.

```
$ sudo mkdir /cvogcvetst
```

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

8. Montare il volume NFS di Cloud Volumes ONTAP nella directory creata nel passaggio precedente.

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



Cloud Volumes Service (CVS)

Cloud Volumes Services (CVS) è un portfolio completo di servizi dati per offrire soluzioni cloud avanzate. Cloud Volumes Services supporta diversi protocolli di accesso ai file per i principali cloud provider (supporto NFS e SMB).

Altri vantaggi e funzionalità includono: Protezione e ripristino dei dati con Snapshot, funzionalità speciali per replicare, sincronizzare e migrare le destinazioni dei dati on-premise o nel cloud e performance costantemente elevate a livello di un sistema di storage flash dedicato.

Cloud Volumes Service (CVS) come storage connesso al guest

Configurare Cloud Volumes Service con VMware Engine

Le condivisioni Cloud Volumes Service possono essere montate da macchine virtuali create nell'ambiente VMware Engine. I volumi possono anche essere montati sul client Linux e mappati sul client Windows perché Cloud Volumes Service supporta i protocolli SMB e NFS. I volumi Cloud Volumes Service possono essere configurati in semplici passaggi.

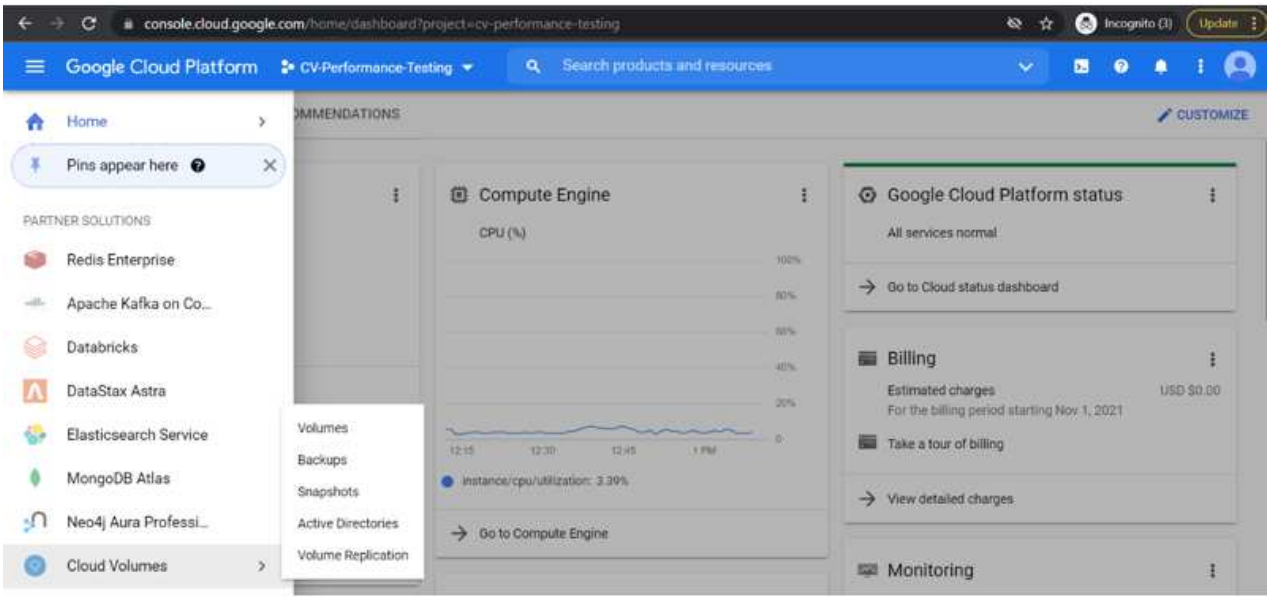
Cloud Volume Service e il cloud privato VMware Engine di Google Cloud devono trovarsi nella stessa regione.

Per acquistare, abilitare e configurare NetApp Cloud Volumes Service per Google Cloud da Google Cloud Marketplace, seguire questa procedura dettagliata "guida".

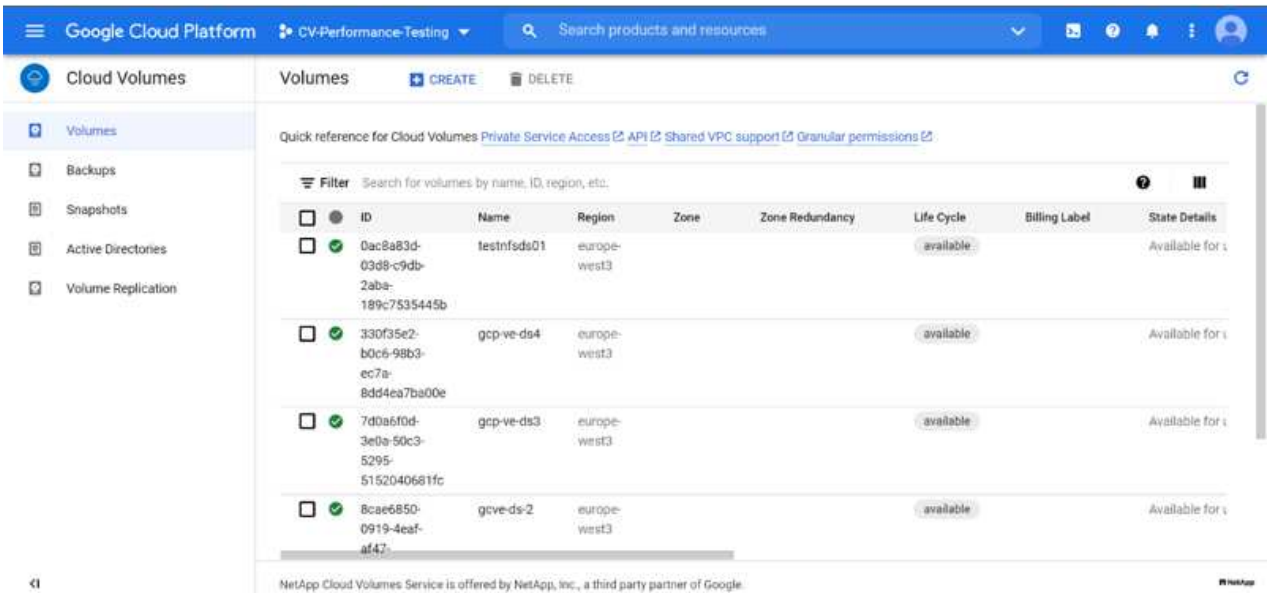
Creare un volume NFS CVS nel cloud privato GCVE

Per creare e montare volumi NFS, attenersi alla seguente procedura:

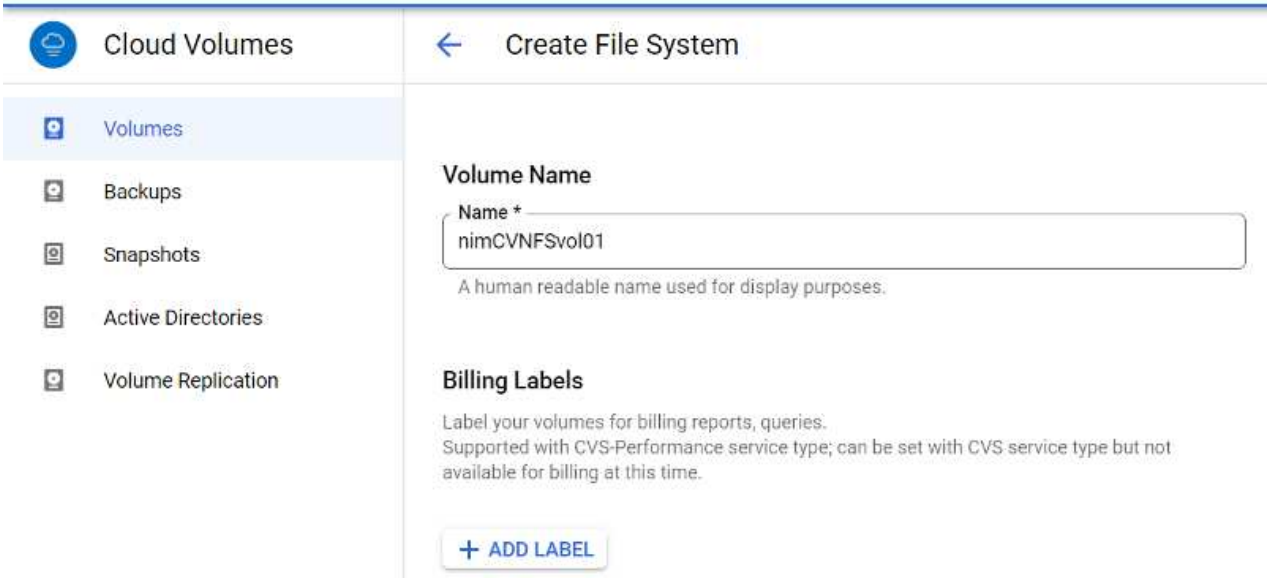
1. Accedi a Cloud Volumes da Partner Solutions all'interno della console cloud di Google.



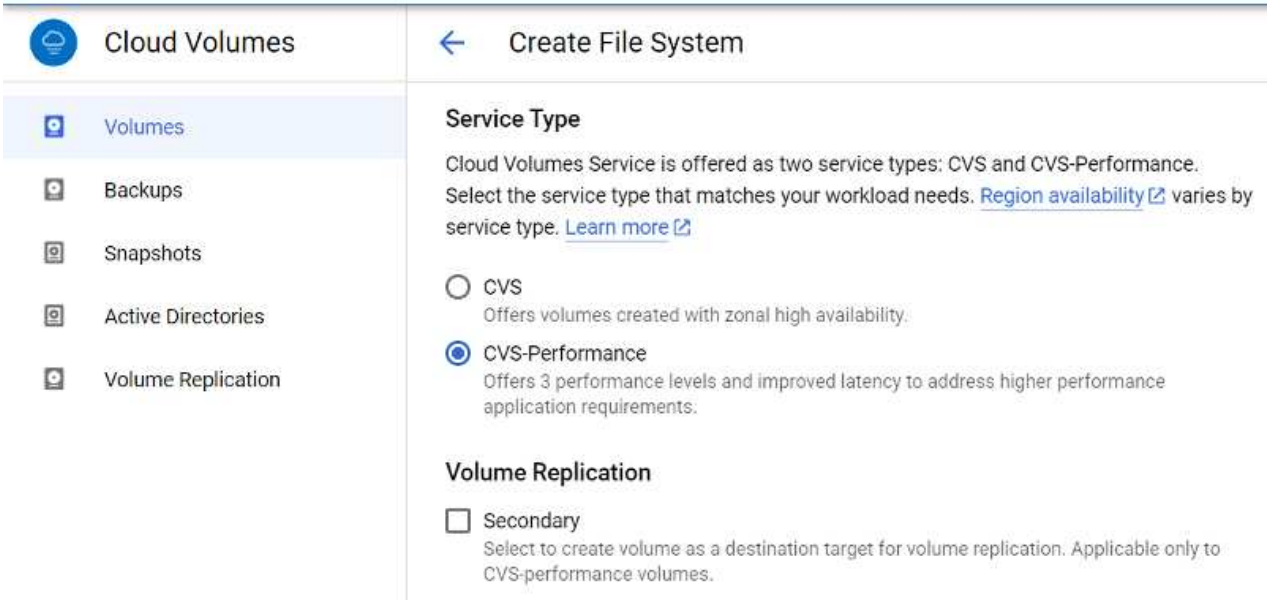
2. Nella Cloud Volumes Console, accedere alla pagina Volumes (volumi) e fare clic su Create (Crea).



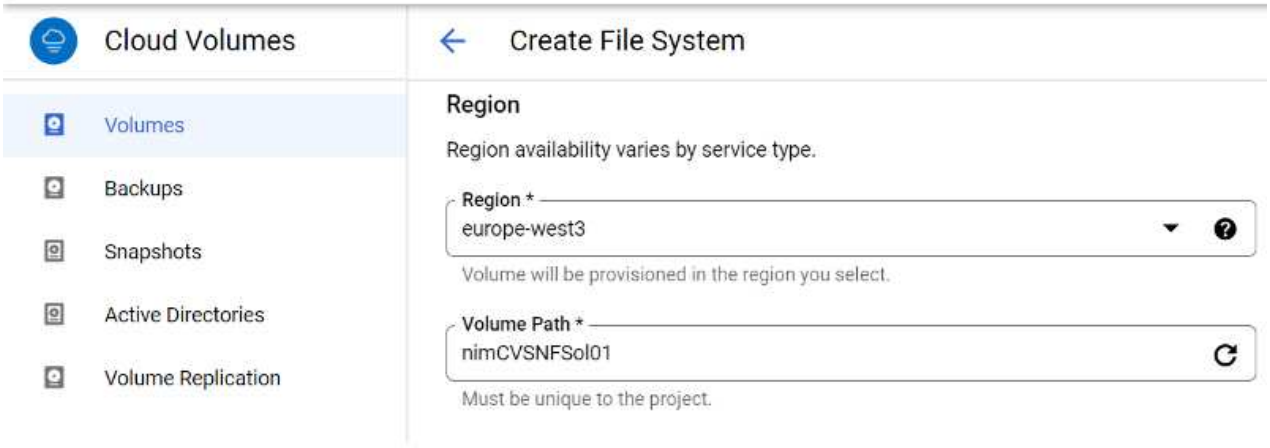
3. Nella pagina Create file System (Crea file system), specificare il nome del volume e le etichette di fatturazione necessari per i meccanismi di chargeback.



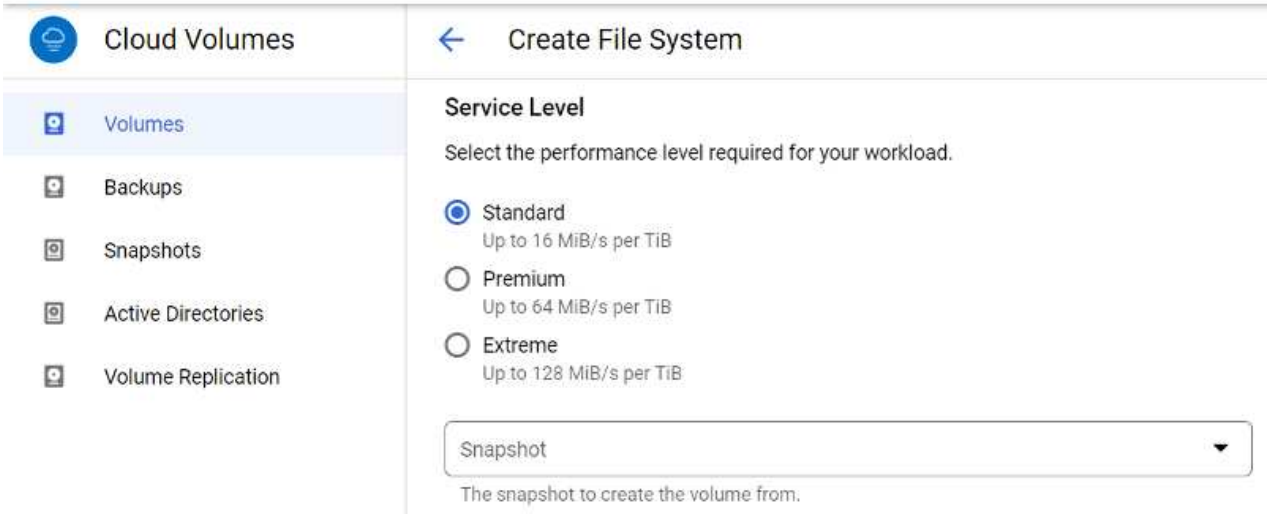
4. Selezionare il servizio appropriato. Per GCVE, scegliere CVS-Performance e il livello di servizio desiderato per una latenza migliorata e performance più elevate in base ai requisiti del carico di lavoro dell'applicazione.



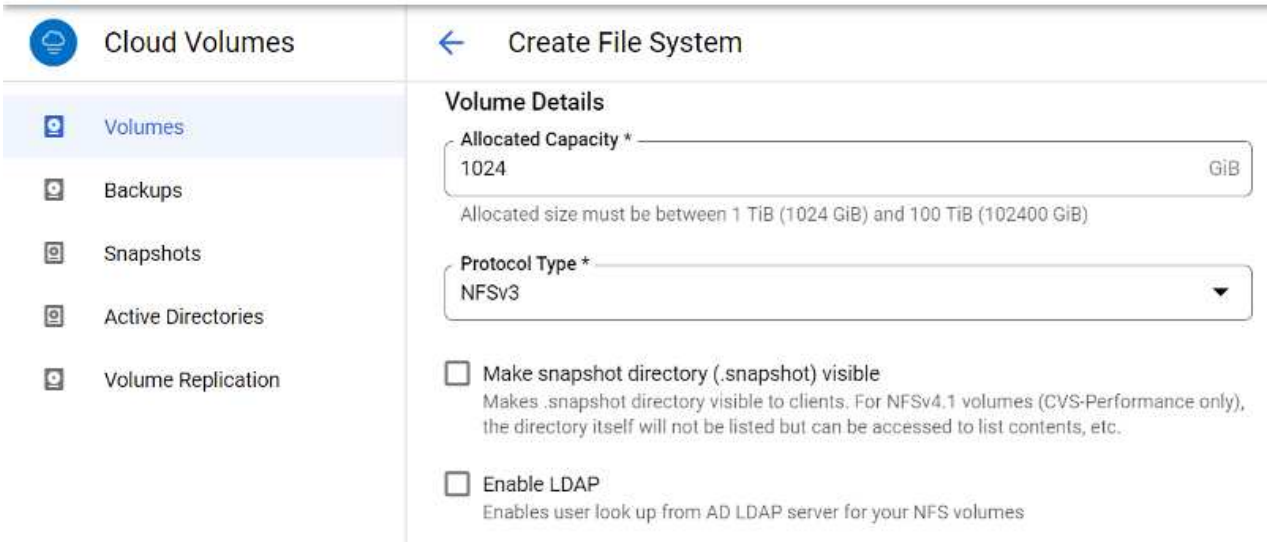
5. Specificare l'area di Google Cloud per il volume e il percorso del volume (il percorso del volume deve essere unico in tutti i volumi cloud del progetto)



6. Selezionare il livello di performance per il volume.

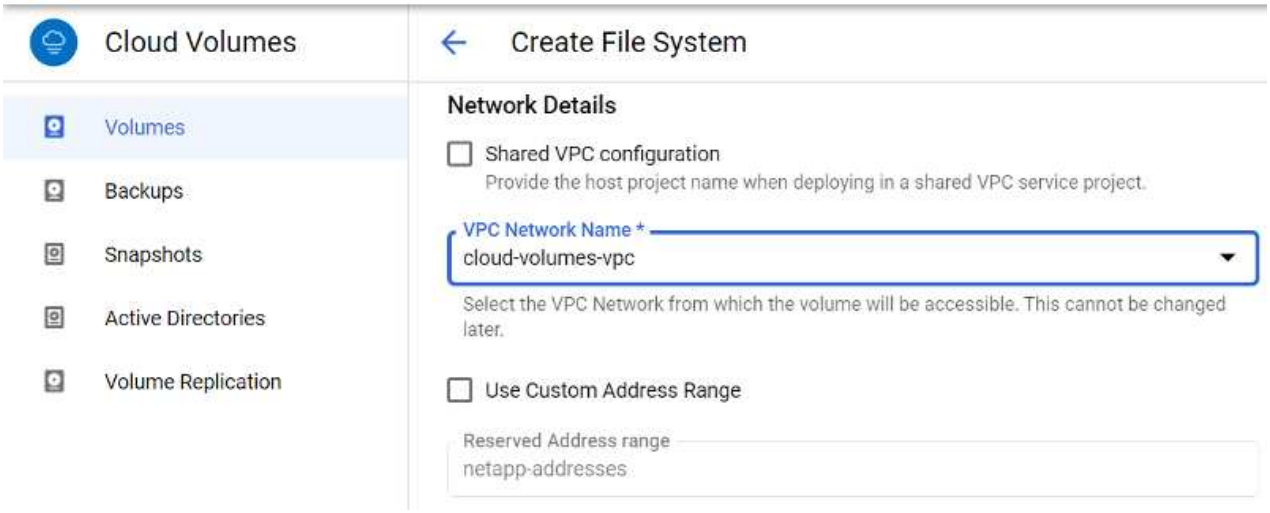


7. Specificare le dimensioni del volume e il tipo di protocollo. In questo test viene utilizzato NFSv3.



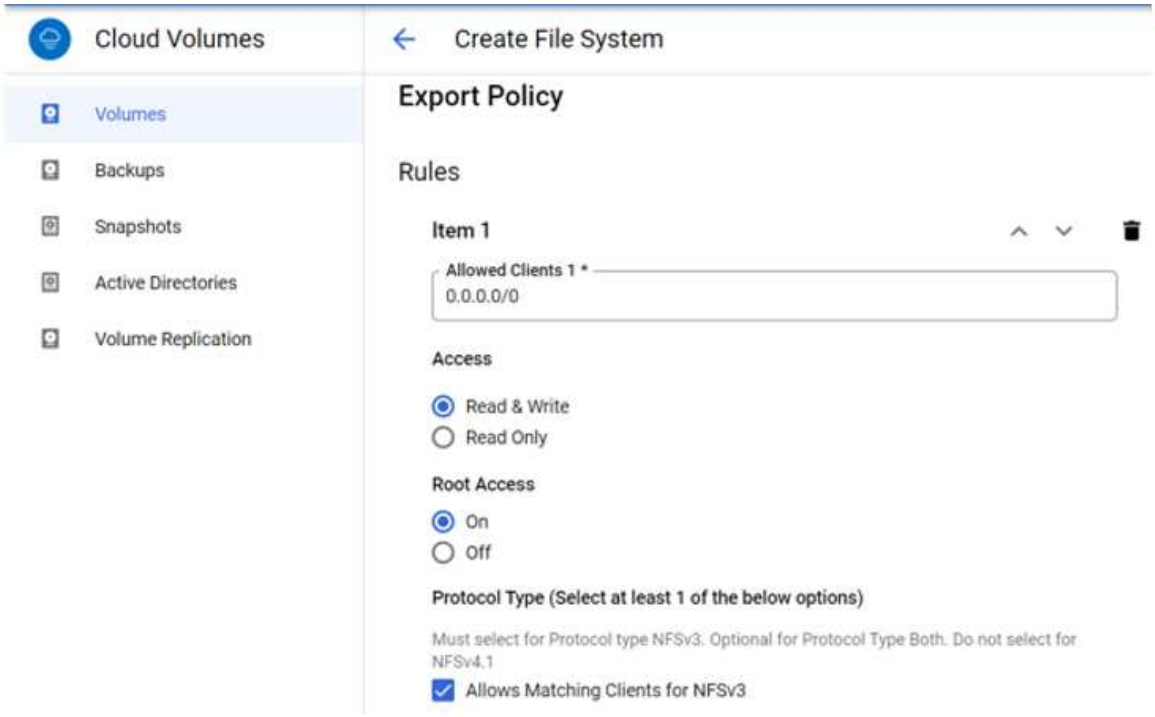
8. In questa fase, selezionare la rete VPC da cui sarà possibile accedere al volume. Assicurarsi che il peering VPC sia in posizione.

SUGGERIMENTO: Se il peering VPC non è stato eseguito, viene visualizzato un pulsante a comparsa che guida l'utente attraverso i comandi di peering. Aprire una sessione della shell cloud ed eseguire i comandi appropriati per mettere in relazione il VPC con il produttore Cloud Volumes Service. Nel caso in cui si decida di preparare il peering VPC in anticipo, fare riferimento a queste istruzioni.



9. Gestire le regole dei criteri di esportazione aggiungendo le regole appropriate e selezionare la casella di controllo per la versione NFS corrispondente.

   Nota: L'accesso ai volumi NFS non sarà possibile a meno che non venga aggiunta una policy di esportazione.



10. Fare clic su Save (Salva) per creare il volume.

Montare le esportazioni NFS sulle macchine virtuali in esecuzione su VMware Engine

Prima di prepararsi al montaggio del volume NFS, assicurarsi che lo stato di peering della connessione privata sia indicato come attivo. Una volta che lo stato è attivo, utilizzare il comando mount.

Per montare un volume NFS, procedere come segue:

1. Nella Cloud Console, andare a Cloud Volumes > Volumes (volumi cloud > volumi).
2. Accedere alla pagina Volumes (volumi)
3. Fare clic sul volume NFS per il quale si desidera montare le esportazioni NFS.
4. Scorrere verso destra, sotto Mostra altri, fare clic su istruzioni di montaggio.

Per eseguire il processo di montaggio dal sistema operativo guest della macchina virtuale VMware, attenersi alla procedura riportata di seguito:

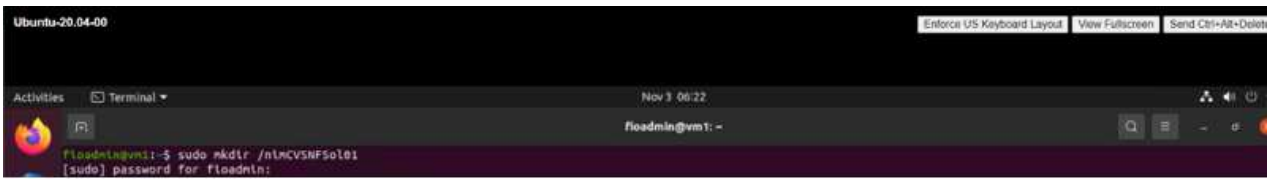
1. Utilizzare il client SSH e SSH per la macchina virtuale.
2. Installare il client nfs sull'istanza.
   a. Su Red Hat Enterprise Linux o istanza di SUSE Linux:

```
 sudo yum install -y nfs-utils
.. Su un'istanza di Ubuntu o Debian:
```

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

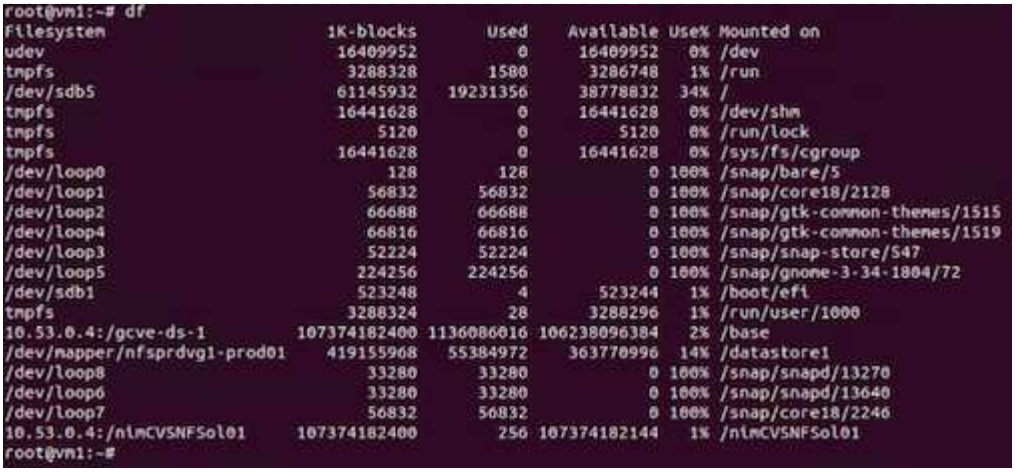
3. Creare una nuova directory sull'istanza, ad esempio "/nimCVSNFSol01":

```
sudo mkdir /nimCVSNFSol01
```



4. Montare il volume utilizzando il comando appropriato. Di seguito è riportato un esempio di comando del laboratorio:

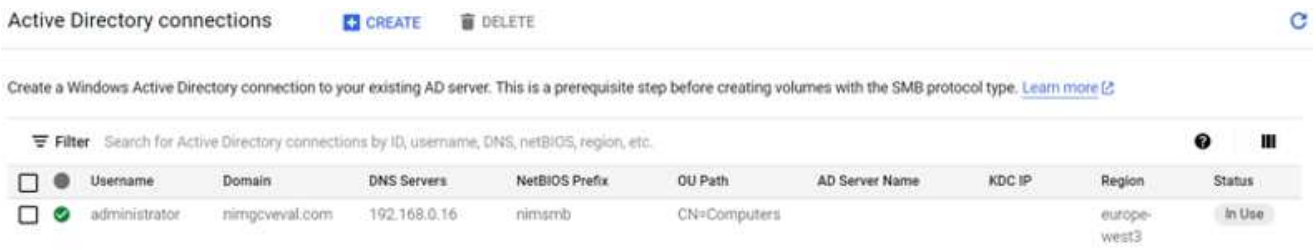
```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



```
root@vm1:~# df
Filesystem                     1K-blocks        Used    Available Use% Mounted on
udev                            16409952           0     16409952   0% /dev
tmpfs                            3288328        1580      3286748   1% /run
/dev/sdb5                       61145932    19231356     38778832  34% /
tmpfs                           16441628           0     16441628   0% /dev/shm
tmpfs                               5120           0         5120   0% /run/lock
tmpfs                           16441628           0     16441628   0% /sys/fs/cgroup
/dev/loop0                            128         128            0 100% /snap/bare/5
/dev/loop1                          56832       56832            0 100% /snap/core18/2128
/dev/loop2                          66688       66688            0 100% /snap/gtk-common-themes/1515
/dev/loop4                          66816       66816            0 100% /snap/gtk-common-themes/1519
/dev/loop3                          52224       52224            0 100% /snap/snap-store/547
/dev/loop5                         224256      224256            0 100% /snap/gnome-3-34-1804/72
/dev/sdb1                          523248           4       523244   1% /boot/efi
tmpfs                             3288324          28      3288296   1% /run/user/1000
10.53.0.4:/gcve-ds-1          107374182400  1136086016 106238096384   2% /base
/dev/mapper/nfsprdvg1-prod01    419155968    55384972    363770996  14% /datastore1
/dev/loop8                          33280       33280            0 100% /snap/snapd/13270
/dev/loop6                          33280       33280            0 100% /snap/snapd/13640
/dev/loop7                          56832       56832            0 100% /snap/core18/2246
10.53.0.4:/nimCVSNFSol01      107374182400         256 107374182144   1% /nimCVSNFSol01
root@vm1:~#
```

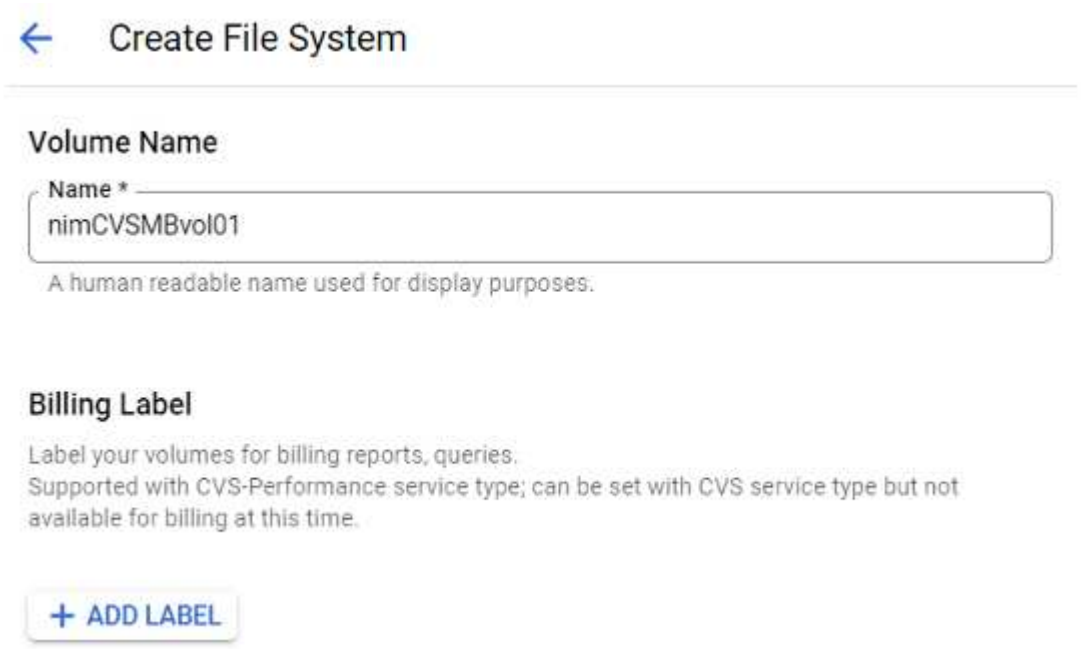
Creazione e montaggio di SMB Share sulle macchine virtuali in esecuzione su VMware Engine

Per i volumi SMB, assicurarsi che le connessioni Active Directory siano configurate prima di creare il volume SMB.

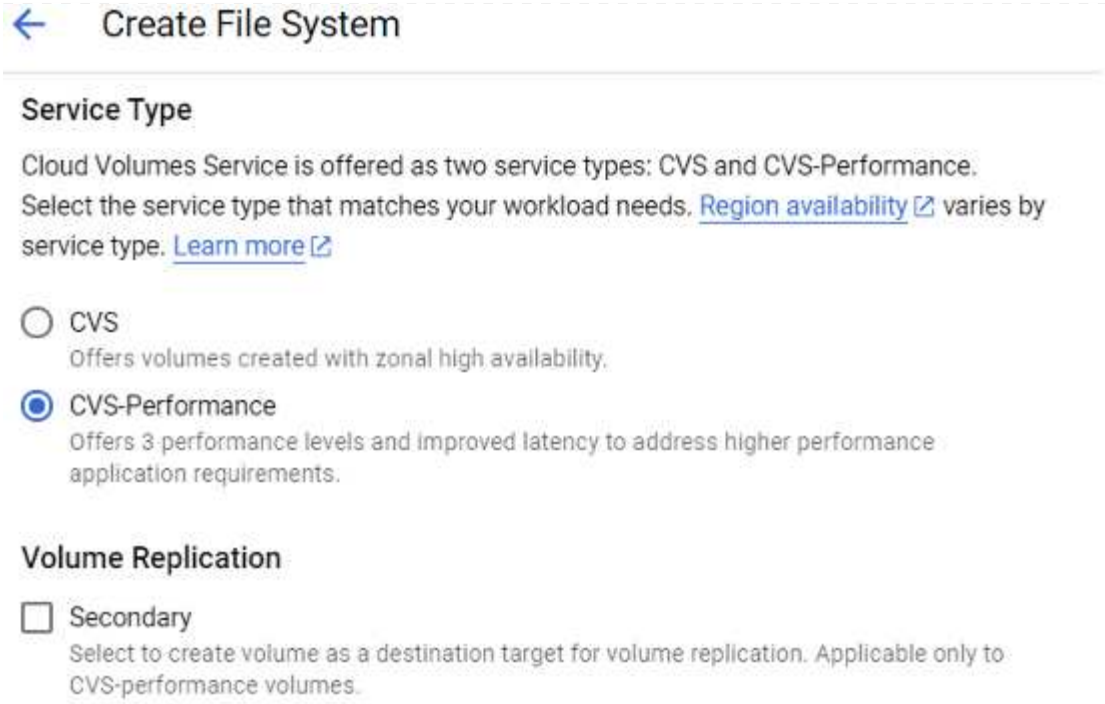


Una volta stabilita la connessione ad, creare il volume con il livello di servizio desiderato. I passaggi sono simili alla creazione di un volume NFS, ad eccezione della selezione del protocollo appropriato.

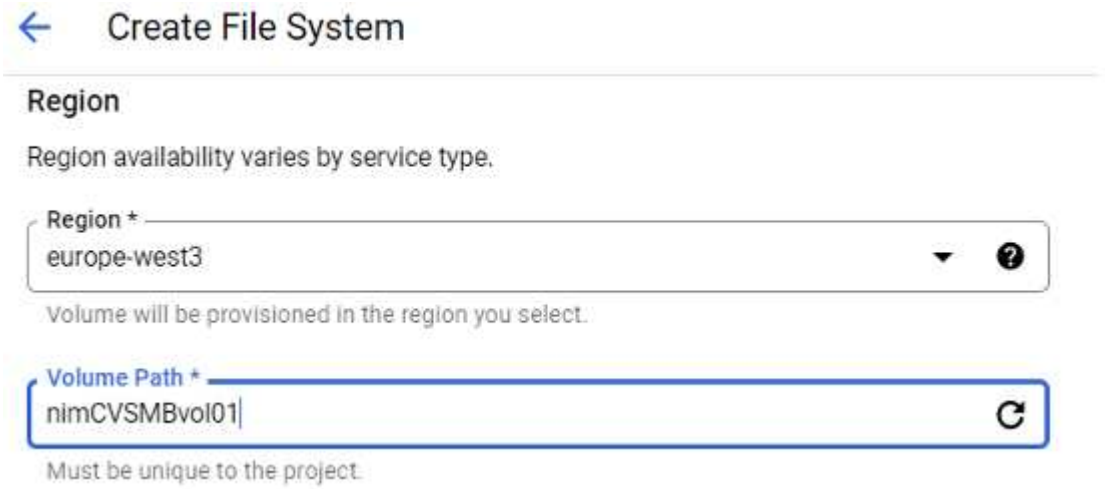
1. Nella Cloud Volumes Console, accedere alla pagina Volumes (volumi) e fare clic su Create (Crea).
2. Nella pagina Create file System (Crea file system), specificare il nome del volume e le etichette di fatturazione necessari per i meccanismi di chargeback.



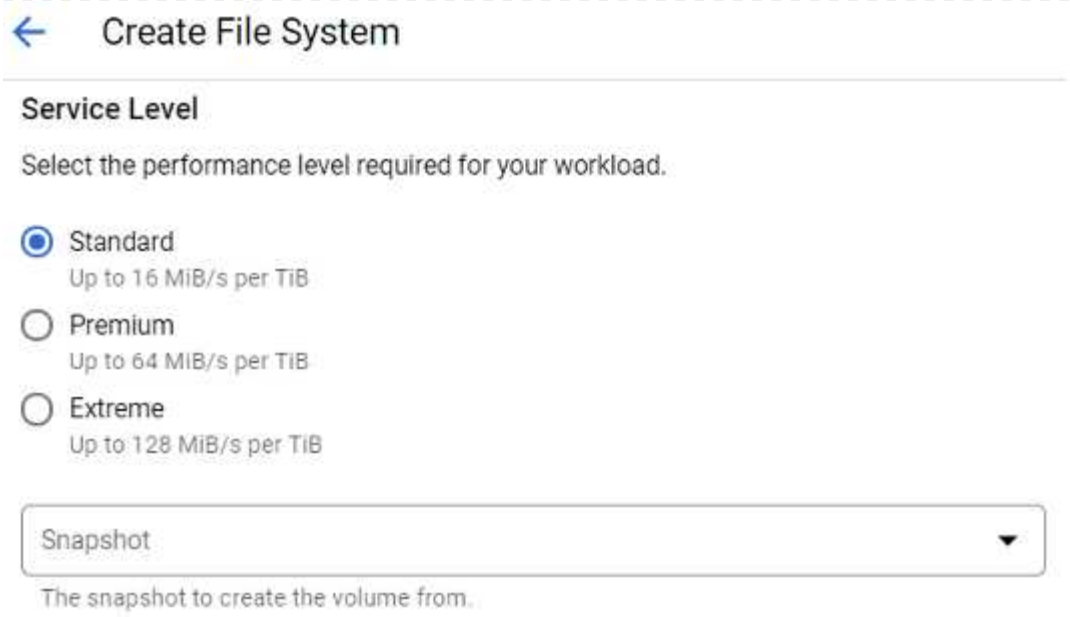
3. Selezionare il servizio appropriato. Per GCVE, scegliere CVS-Performance e il livello di servizio desiderato per una latenza migliorata e performance più elevate in base ai requisiti del carico di lavoro.



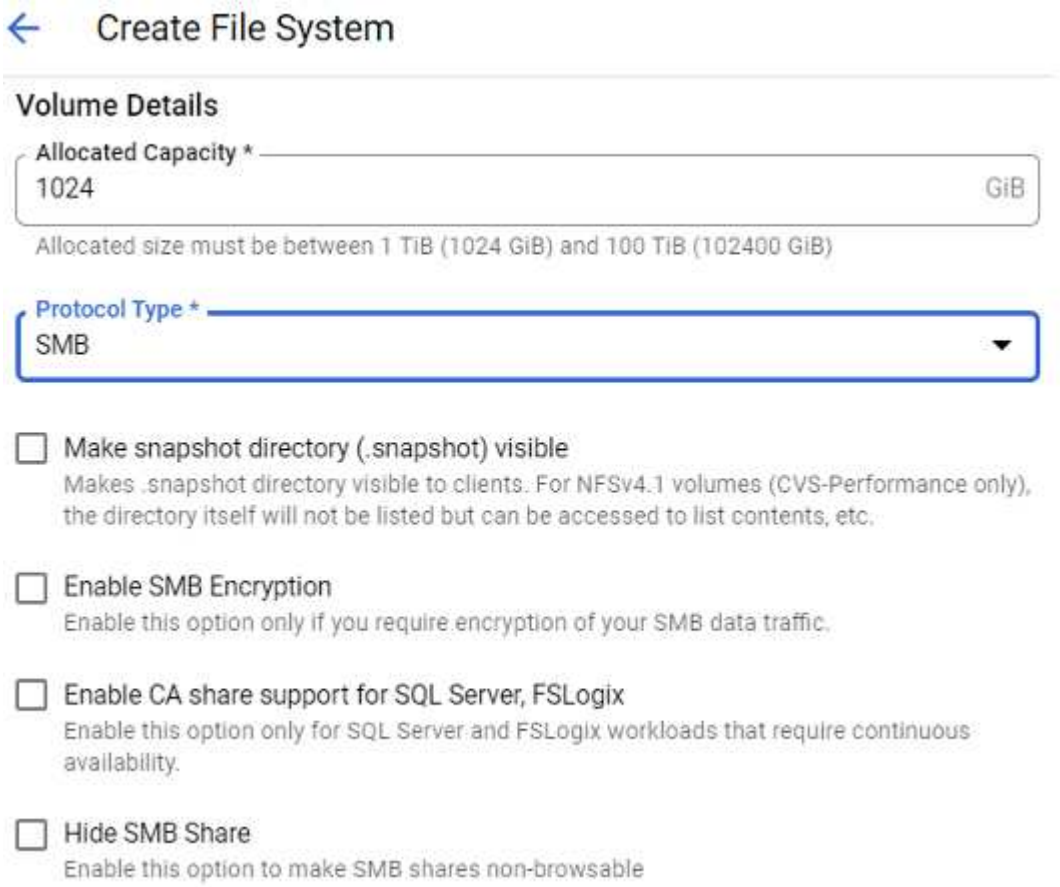
4. Specificare l'area di Google Cloud per il volume e il percorso del volume (il percorso del volume deve essere unico in tutti i volumi cloud del progetto)



5. Selezionare il livello di performance per il volume.



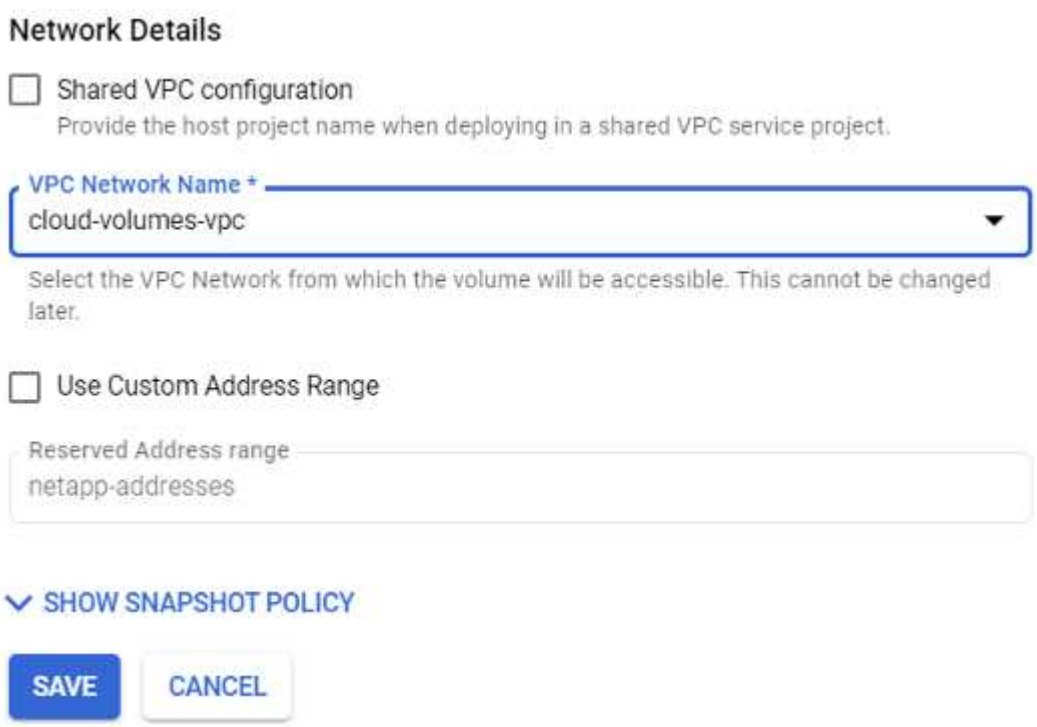
6. Specificare le dimensioni del volume e il tipo di protocollo. In questo test, viene utilizzato SMB.



7. In questa fase, selezionare la rete VPC da cui sarà possibile accedere al volume. Assicurarsi che il peering VPC sia in posizione.

   SUGGERIMENTO: Se il peering VPC non è stato eseguito, viene visualizzato un pulsante a comparsa che guida l'utente attraverso i comandi di peering. Aprire una sessione della shell cloud ed eseguire i comandi appropriati per mettere in relazione il VPC con il produttore Cloud Volumes

Service. Nel caso in cui si decida di preparare il peering VPC in anticipo, fare riferimento a questi "istruzioni".



8. Fare clic su Save (Salva) per creare il volume.

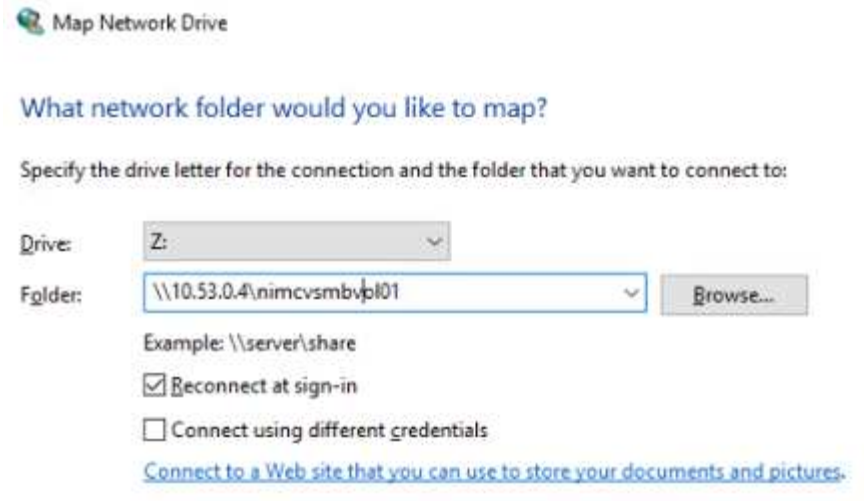
Per montare il volume SMB, procedere come segue:

1. Nella Cloud Console, andare a Cloud Volumes > Volumes (volumi cloud > volumi).
2. Accedere alla pagina Volumes (volumi)
3. Fare clic sul volume SMB per il quale si desidera mappare una condivisione SMB.
4. Scorrere verso destra, sotto Mostra altri, fare clic su istruzioni di montaggio.

Per eseguire il processo di montaggio dal sistema operativo guest di Windows della macchina virtuale VMware, attenersi alla seguente procedura:

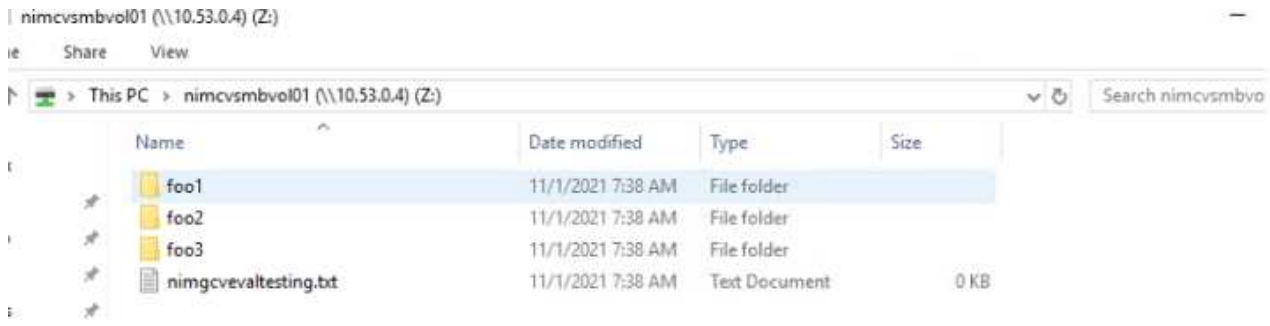
1. Fare clic sul pulsante Start, quindi su computer.
2. Fare clic su Map Network Drive (Connetti unità di rete
3. Nell'elenco Drive (unità), fare clic su una lettera di unità disponibile.
4. Nella casella della cartella, digitare:

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



Per connettersi ogni volta che si accede al computer, selezionare la casella di controllo Reconnect at sign-in (riconnessione all'accesso).

5. Fare clic su fine.



Disponibilità regionale per datastore NFS supplementari su AWS, Azure e GCP

Scopri di più sul supporto della Global Region per datastore NFS supplementari su AWS, Azure e Google Cloud Platform (GCP).

Disponibilità AWS Region

La disponibilità di datastore NFS supplementari su AWS / VMC è definita da Amazon. Innanzitutto, è necessario determinare se VMC e FSxN sono disponibili in una regione specifica. Quindi, è necessario determinare se il datastore NFS supplementare FSxN è supportato in quella regione.

- Verificare la disponibilità di VMC "qui".
- La guida ai prezzi di Amazon offre informazioni su dove è disponibile FSxN (FSX ONTAP). Queste informazioni sono disponibili "qui".
- La disponibilità del datastore NFS supplementare FSxN per VMC sarà presto disponibile.

Mentre le informazioni sono ancora in fase di rilascio, il seguente grafico identifica il supporto corrente per VMC, FSxN e FSxN come datastore NFS supplementare.

Americhe

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
US East (Virginia del Nord)	Sì	Sì	Sì
USA Est (Ohio)	Sì	Sì	Sì
US West (California settentrionale)	Sì	No	No
STATI UNITI occidentali (Oregon)	Sì	Sì	Sì
GovCloud (ovest degli Stati Uniti)	Sì	Sì	Sì
Canada (centrale)	Sì	Sì	Sì
Sud America (San Paolo)	Sì	Sì	Sì

Ultimo aggiornamento: 2 giugno 2022.

EMEA

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
Europa (Irlanda)	Sì	Sì	Sì
Europa (Londra)	Sì	Sì	Sì
Europa (Francoforte)	Sì	Sì	Sì
Europa (Parigi)	Sì	Sì	Sì
Europa (Milano)	Sì	Sì	Sì
Europa (Stoccolma)	Sì	Sì	Sì

Ultimo aggiornamento: 2 giugno 2022.

Asia Pacifico

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
Asia Pacifico (Sydney)	Sì	Sì	Sì
Asia Pacifico (Tokyo)	Sì	Sì	Sì
Asia Pacifico (Osaka)	Sì	No	No
Asia Pacifico (Singapore)	Sì	Sì	Sì
Asia Pacifico (Seul)	Sì	Sì	Sì
Asia Pacifico (Mumbai)	Sì	Sì	Sì

Asia Pacifico (Giacarta)	No	No	No
Asia Pacifico (Hong Kong)	Sì	Sì	Sì

Ultimo aggiornamento: 28 settembre 2022.

Disponibilità della regione di Azure

La disponibilità di datastore NFS supplementari su Azure / AVS è definita da Microsoft. Innanzitutto, è necessario determinare se AVS e ANF sono disponibili in una regione specifica. Quindi, è necessario determinare se il datastore NFS supplementare ANF è supportato in quella regione.

- Verificare la disponibilità di AVS e ANF "qui".
- Verificare la disponibilità del datastore NFS supplementare ANF "qui".

Disponibilità della regione GCP

La disponibilità della regione GCP verrà rilasciata quando GCP entrerà nella disponibilità pubblica.

Riepilogo e conclusione: Perché scegliere NetApp Hybrid Multifloud con VMware

NetApp Cloud Volumes e le soluzioni VMware per i principali hyperscaler offrono un grande potenziale alle organizzazioni che desiderano sfruttare il cloud ibrido. Il resto di questa sezione fornisce i casi di utilizzo che mostrano l'integrazione dei volumi cloud NetApp che consente di sfruttare le reali funzionalità del multicloud ibrido.

Caso d'utilizzo n. 1: Ottimizzazione dello storage

Quando si esegue un'esercitazione di dimensionamento utilizzando l'output di RVtools, è sempre evidente che la scalabilità della potenza (vCPU/VMEM) è parallela allo storage. Molte volte, le organizzazioni si trovano in una situazione in cui lo spazio di storage richiede unità di dimensioni del cluster ben superiori a quelle necessarie per la potenza.

Integrando NetApp Cloud Volumes, le organizzazioni possono realizzare una soluzione cloud basata su vSphere con un semplice approccio alla migrazione, senza re-platform, modifiche IP e modifiche architetturali. Inoltre, questa ottimizzazione consente di scalare l'impatto dello storage mantenendo il numero di host alla quantità minima richiesta in vSphere, senza modificare la gerarchia dello storage, la sicurezza o i file resi disponibili. In questo modo è possibile ottimizzare l'implementazione e ridurre il TCO complessivo del 35-45%. Questa integrazione consente inoltre di scalare lo storage dal warm storage alle performance a livello di produzione in pochi secondi.

Caso d'utilizzo n. 2: Migrazione del cloud

Le organizzazioni sono sotto pressione per migrare le applicazioni dai data center on-premise al cloud pubblico per diversi motivi: Una scadenza imminente del leasing, una direttiva finanziaria per passare dalla spesa in conto capitale (CAPEX) alla spesa in conto operativo (OPEX) o semplicemente un mandato top-down per spostare tutto nel cloud.

Quando la velocità è critica, è possibile solo un approccio di migrazione semplificato, perché il re-platform e il refactoring delle applicazioni per adattarsi alla specifica piattaforma IaaS del cloud è lento e costoso, spesso richiede mesi. Combinando i volumi NetApp Cloud con la replica SnapMirror efficiente in termini di larghezza di

banda per lo storage connesso agli ospiti (inclusi RDM in combinazione con copie Snapshot coerenti con l'applicazione e HCX, migrazione specifica per il cloud (ad esempio Azure Migrate) o prodotti di terze parti per la replica delle macchine virtuali), questa transizione è ancora più semplice che affidarsi a lunghi meccanismi di filtri i/O.

Caso d'utilizzo n. 3: Espansione del data center

Quando un data center raggiunge i limiti di capacità a causa di picchi stagionali della domanda o semplicemente di una crescita organica costante, il passaggio a VMware basato sul cloud insieme a NetApp Cloud Volumes è una soluzione semplice. L'utilizzo di NetApp Cloud Volumes consente la creazione, la replica e l'espansione dello storage in modo molto semplice, fornendo alta disponibilità nelle zone di disponibilità e funzionalità di scalabilità dinamica. L'utilizzo di NetApp Cloud Volumes consente di ridurre al minimo la capacità del cluster host, superando la necessità di stretch cluster.

Caso d'utilizzo n. 4: Disaster recovery nel cloud

In un approccio tradizionale, se si verifica un disastro, le macchine virtuali replicate nel cloud richiederebbero la conversione nella piattaforma hypervisor del cloud prima di poter essere ripristinate, non un'attività da gestire durante una crisi.

Utilizzando NetApp Cloud Volumes per lo storage connesso agli ospiti utilizzando la replica di SnapCenter e SnapMirror on-premise insieme alle soluzioni di virtualizzazione del cloud pubblico, è possibile definire un approccio migliore per il disaster recovery, consentendo il ripristino delle repliche delle macchine virtuali su un'infrastruttura SDDC VMware completamente coerente e con strumenti di recovery specifici per il cloud (Ad esempio Azure Site Recovery) o strumenti di terze parti equivalenti come Veeam. Questo approccio consente inoltre di eseguire rapidamente operazioni di disaster recovery e recovery dal ransomware. In questo modo è possibile scalare la produzione completa per il test o durante un disastro aggiungendo host on-demand.

Caso di utilizzo n. 5: Modernizzazione delle applicazioni

Una volta che le applicazioni si trovano nel cloud pubblico, le organizzazioni vorranno sfruttare le centinaia di potenti servizi cloud per modernizzarle ed estenderle. Con l'utilizzo di NetApp Cloud Volumes, la modernizzazione è un processo semplice perché i dati delle applicazioni non sono bloccati in vSAN e consentono la mobilità dei dati per un'ampia gamma di casi di utilizzo, tra cui Kubernetes.

Conclusione

Sia che tu stia prendendo in esame un cloud all-cloud o ibrido, NetApp Cloud Volumes offre opzioni eccellenti per implementare e gestire i carichi di lavoro delle applicazioni insieme ai file service e ai protocolli a blocchi, riducendo al contempo il TCO rendendo i requisiti dei dati perfetti a livello applicativo.

Qualunque sia il caso d'utilizzo, scegli il tuo cloud/hyperscaler preferito insieme a NetApp Cloud Volumes per una rapida realizzazione dei benefici 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 collegare lo storage. Ricorda che è solo la posizione dei dati che è cambiata con nuovi nomi; i tool e i processi rimangono tutti gli stessi e NetApp Cloud Volumes aiuta a ottimizzare l'implementazione complessiva.

Casi di utilizzo di VMware Hybrid Cloud

Casi di utilizzo per NetApp Hybrid Multibloud con VMware

Panoramica dei casi di utilizzo importanti per l'organizzazione IT durante la pianificazione

di implementazioni cloud ibrido o cloud-first.

Casi di utilizzo più comuni

I casi di utilizzo includono:

- Disaster recovery,
- Hosting dei carichi di lavoro durante la manutenzione del data center, * rapida esplosione in cui sono richieste risorse aggiuntive oltre a quanto previsto nel data center locale,
- Espansione del sito VMware,
- Migrazione rapida al cloud,
- Dev/test, e.
- Modernizzazione delle applicazioni sfruttando le tecnologie supplementari del cloud.

In questa documentazione, i riferimenti al workload cloud verranno dettagliati utilizzando i casi di utilizzo di VMware. Questi casi di utilizzo sono:

- Protect (include disaster recovery e backup/ripristino)
- Migrare
- Estendi

Dentro il percorso DELL'IT

La maggior parte delle organizzazioni è in viaggio verso la trasformazione e la modernizzazione. Nell'ambito di questo processo, le aziende stanno cercando di utilizzare gli investimenti VMware esistenti, sfruttando al contempo i vantaggi del cloud e esplorando i modi per rendere il processo di migrazione il più possibile perfetto. Questo approccio renderebbe molto semplice il loro impegno di modernizzazione perché i dati sono già nel cloud.

La risposta più semplice a questo scenario è rappresentata dalle offerte VMware in ogni hyperscaler. Come NetApp® Cloud Volumes, VMware offre un modo per spostare o estendere ambienti VMware on-premise su qualsiasi cloud, consentendo di mantenere risorse, competenze e strumenti on-premise esistenti durante l'esecuzione nativa dei carichi di lavoro nel cloud. Questo riduce i rischi perché non ci saranno interruzioni di servizio o necessità di modifiche IP e offre al team IT la possibilità di operare nel modo in cui si svolgono on-premise utilizzando le competenze e gli strumenti esistenti. Questo può portare a migrazioni del cloud accelerate e a una transizione molto più fluida verso un'architettura multicloud ibrida.

Comprendere l'importanza delle opzioni di storage NFS supplementari

Mentre VMware in qualsiasi cloud offre funzionalità ibride uniche a tutti i clienti, opzioni di storage NFS supplementari limitate hanno limitato la sua utilità per le organizzazioni con carichi di lavoro elevati in termini di storage. Poiché lo storage è direttamente legato agli host, l'unico modo per scalare lo storage è aggiungere più host, e questo può aumentare i costi del 35-40% o più per i carichi di lavoro a elevato utilizzo dello storage. Questi carichi di lavoro necessitano solo di storage aggiuntivo, non di potenza aggiuntiva. Ma ciò significa pagare per altri host.

Consideriamo questo scenario:

Un cliente richiede solo cinque host per CPU e memoria, ma ha molte esigenze di storage e ha bisogno di 12 host per soddisfare i requisiti di storage. Questo requisito finisce per mettere a punto la scala finanziaria dovendo acquistare la potenza aggiuntiva, quando è necessario solo incrementare lo storage.

Quando stai pianificando l'adozione e la migrazione del cloud, è sempre importante valutare l'approccio migliore e seguire il percorso più semplice per ridurre gli investimenti totali. L'approccio più comune e più semplice per qualsiasi migrazione applicativa è il rehosting (noto anche come Lift and Shift) in cui non esiste una macchina virtuale (VM) o una conversione dei dati. L'utilizzo di NetApp Cloud Volumes con il software-defined data center (SDDC) VMware, integrando al contempo vSAN, offre un'opzione semplice di "lift-and-shift".

Soluzioni NetApp per Amazon VMware Managed Cloud (VMC)

Scopri di più sulle soluzioni offerte da NetApp ad AWS.

VMware definisce i carichi di lavoro del cloud in una delle tre categorie seguenti:

- Protezione (inclusi disaster recovery e backup/ripristino)
- Migrare
- Estendi

Consultare le soluzioni disponibili nelle seguenti sezioni.

Proteggere

- "Disaster Recovery con VMC su AWS (connesso come guest)"
- "Backup Veeam Ripristino in VMC con FSX per ONTAP"
- "Disaster recovery (DRO) con FSX per ONTAP e VMC"
- "Utilizzo di Veeam Replication and FSX for ONTAP per il disaster recovery in VMware Cloud su AWS"

Migrare

- "Migrazione dei carichi di lavoro nel datastore FSxN con VMware HCX"

Estendi

PRESTO DISPONIBILE!

Soluzioni NetApp per Azure VMware Solution (AVS)

Scopri di più sulle soluzioni offerte da NetApp ad Azure.

VMware definisce i carichi di lavoro del cloud in una delle tre categorie seguenti:

- Protezione (inclusi disaster recovery e backup/ripristino)
- Migrare
- Estendi

Consultare le soluzioni disponibili nelle seguenti sezioni.

Proteggere

- "Disaster Recovery con ANF e JetStream (datastore NFS supplementare)"
- "Disaster Recovery con ANF e CVO (storage connesso guest)"
- "Disaster Recovery (DRO) con ANF e AVS"
- "Utilizzo di Veeam Replication e datastore Azure NetApp Files per il disaster recovery nella soluzione Azure VMware"

Migrare

- "Migrazione dei carichi di lavoro nel datastore Azure NetApp Files con VMware HCX"

Estendi

PRESTO DISPONIBILE!

Soluzioni NetApp per Google Cloud VMware Engine (GCVE)

Scopri di più sulle soluzioni offerte da NetApp per il GCP.

VMware definisce i carichi di lavoro del cloud in una delle tre categorie seguenti:

- Protezione (inclusi disaster recovery e backup/ripristino)
- Migrare
- Estendi

Consultare le soluzioni disponibili nelle seguenti sezioni.

Proteggere

- "Disaster recovery applicativo con replica SnapCenter, Cloud Volumes ONTAP e Veeam"
- "Disaster recovery coerente con l'applicazione con NetApp SnapCenter e replica Veeam su CVS NetApp su GCVE"

Migrare

- "Migrazione dei carichi di lavoro con VMware HCX al datastore NetApp Cloud Volume Service NFS"
- "Replica delle macchine virtuali con Veeam al datastore NFS del servizio volumi cloud di NetApp"

Estendi

PRESTO DISPONIBILE!

Funzionalità NetApp per AWS VMC

Scopri di più sulle funzionalità offerte da NetApp in AWS VMware Cloud (VMC), da NetApp come dispositivo di storage connesso come guest o come datastore NFS supplementare alla migrazione dei flussi di lavoro, all'estensione/diffusione nel cloud, al backup/ripristino e al disaster recovery.

Passare alla sezione relativa al contenuto desiderato selezionando una delle seguenti opzioni:

- "Configurazione di VMC in AWS"
- "Opzioni di storage NetApp per VMC"
- "Soluzioni cloud NetApp/VMware"

Configurazione di VMC in AWS

Come per i sistemi on-premise, la pianificazione di un ambiente di virtualizzazione basato sul cloud è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire VMware Cloud su AWS SDDC e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad AWS VMC.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementazione e configurazione di VMware Cloud per AWS
- Connetti VMware Cloud a FSX ONTAP

Visualizza i dettagli "Procedura di configurazione per VMC".

Opzioni di storage NetApp per VMC

Lo storage NetApp può essere utilizzato in diversi modi, sia come congettura connessa che come datastore NFS supplementare, all'interno di AWS VMC.

Visitare il sito "Opzioni di storage NetApp supportate" per ulteriori informazioni.

AWS supporta lo storage NetApp nelle seguenti configurazioni:

- FSX ONTAP come storage connesso guest
- Cloud Volumes ONTAP (CVO) come storage connesso guest
- FSX ONTAP come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per VMC". Visualizza i dettagli "Opzioni aggiuntive del datastore NFS per VMC".

Casi di utilizzo della soluzione

Con le soluzioni cloud NetApp e VMware, molti casi di utilizzo sono semplici da implementare nel tuo AWS VMC. I casi di utilizzo sono definiti per ciascuna delle aree cloud definite da VMware:

- Protect (include disaster recovery e backup/ripristino)
- Estendi
- Migrare

"Esplora le soluzioni NetApp per AWS VMC"

Protezione dei carichi di lavoro su AWS / VMC

TR-4931: Disaster recovery con VMware Cloud su Amazon Web Services e Guest Connect

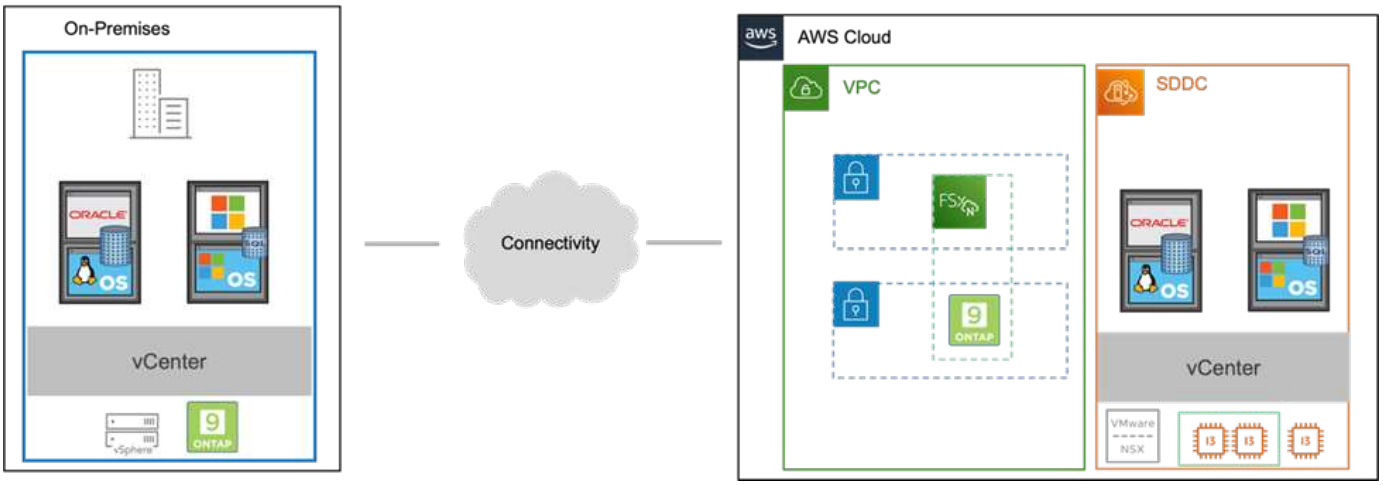
Autori: Chris Reno, Josh Powell e Suresh Thoppay - NetApp Solutions Engineering

Panoramica

Un ambiente e un piano di disaster recovery (DR) comprovati sono fondamentali per le organizzazioni per garantire che le applicazioni business-critical possano essere ripristinate rapidamente in caso di grave interruzione del servizio. Questa soluzione si concentra sulla dimostrazione dei casi di utilizzo del DR con particolare attenzione alle tecnologie VMware e NetApp, sia on-premise che con VMware Cloud su AWS.

NetApp vanta una lunga storia di integrazione con VMware, come dimostrano le decine di migliaia di clienti che hanno scelto NetApp come partner di storage per il loro ambiente virtualizzato. Questa integrazione continua con le opzioni di connessione guest nel cloud e le recenti integrazioni con i datastore NFS. Questa soluzione si concentra sul caso di utilizzo comunemente indicato come storage connesso al guest.

Nello storage connesso agli ospiti, il VMDK guest viene implementato su un datastore con provisioning VMware e i dati delle applicazioni vengono memorizzati su iSCSI o NFS e mappati direttamente sulla macchina virtuale. Le applicazioni Oracle e MS SQL vengono utilizzate per dimostrare uno scenario di DR, come illustrato nella figura seguente.



Presupposti, prerequisiti e panoramica dei componenti

Prima di implementare questa soluzione, esaminare la panoramica dei componenti, i prerequisiti necessari per implementare la soluzione e i presupposti della documentazione della soluzione.

"Requisiti, requisiti e pianificazione della soluzione DR"

Eseguire il DR con SnapCenter

In questa soluzione, SnapCenter fornisce snapshot coerenti con l'applicazione per i dati delle applicazioni SQL Server e Oracle. Questa configurazione, insieme alla tecnologia SnapMirror, offre una replica dei dati ad alta velocità tra il nostro cluster AFF on-premise e FSX ONTAP. Inoltre, Veeam Backup & Replication offre funzionalità di backup e ripristino per le nostre macchine virtuali.

In questa sezione viene descritta la configurazione di SnapCenter, SnapMirror e Veeam per il backup e il ripristino.

Le seguenti sezioni illustrano la configurazione e i passaggi necessari per completare un failover nel sito secondario:

Configurare le relazioni di SnapMirror e le pianificazioni di conservazione

SnapCenter può aggiornare le relazioni di SnapMirror all'interno del sistema di storage primario (primario > mirror) e ai sistemi di storage secondario (primario > vault) per l'archiviazione e la conservazione a lungo termine. A tale scopo, è necessario stabilire e inizializzare una relazione di replica dei dati tra un volume di destinazione e un volume di origine utilizzando SnapMirror.

I sistemi ONTAP di origine e di destinazione devono trovarsi in reti con peering tramite VPC Amazon, gateway di transito, connessione diretta AWS o VPN AWS.

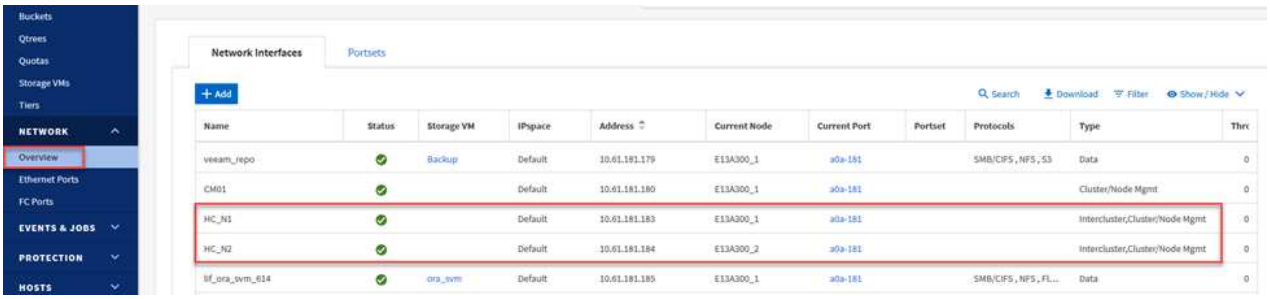
Per impostare le relazioni di SnapMirror tra un sistema ONTAP on-premise e FSX ONTAP sono necessari i seguenti passaggi:

Fare riferimento a. "FSX per ONTAP - Guida utente di ONTAP" Per ulteriori informazioni sulla creazione di relazioni SnapMirror con FSX.

Registrare le interfacce logiche Intercluster di origine e destinazione

Per il sistema ONTAP di origine residente on-premise, è possibile recuperare le informazioni LIF tra cluster da Gestore di sistema o dall'interfaccia CLI.

1. In Gestore di sistema di ONTAP, accedere alla pagina Panoramica di rete e recuperare gli indirizzi IP di tipo: Intercluster configurati per comunicare con il VPC di AWS su cui è installato FSX.



2. Per recuperare gli indirizzi IP dell'Intercluster per FSX, accedere alla CLI ed eseguire il seguente comando:

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

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

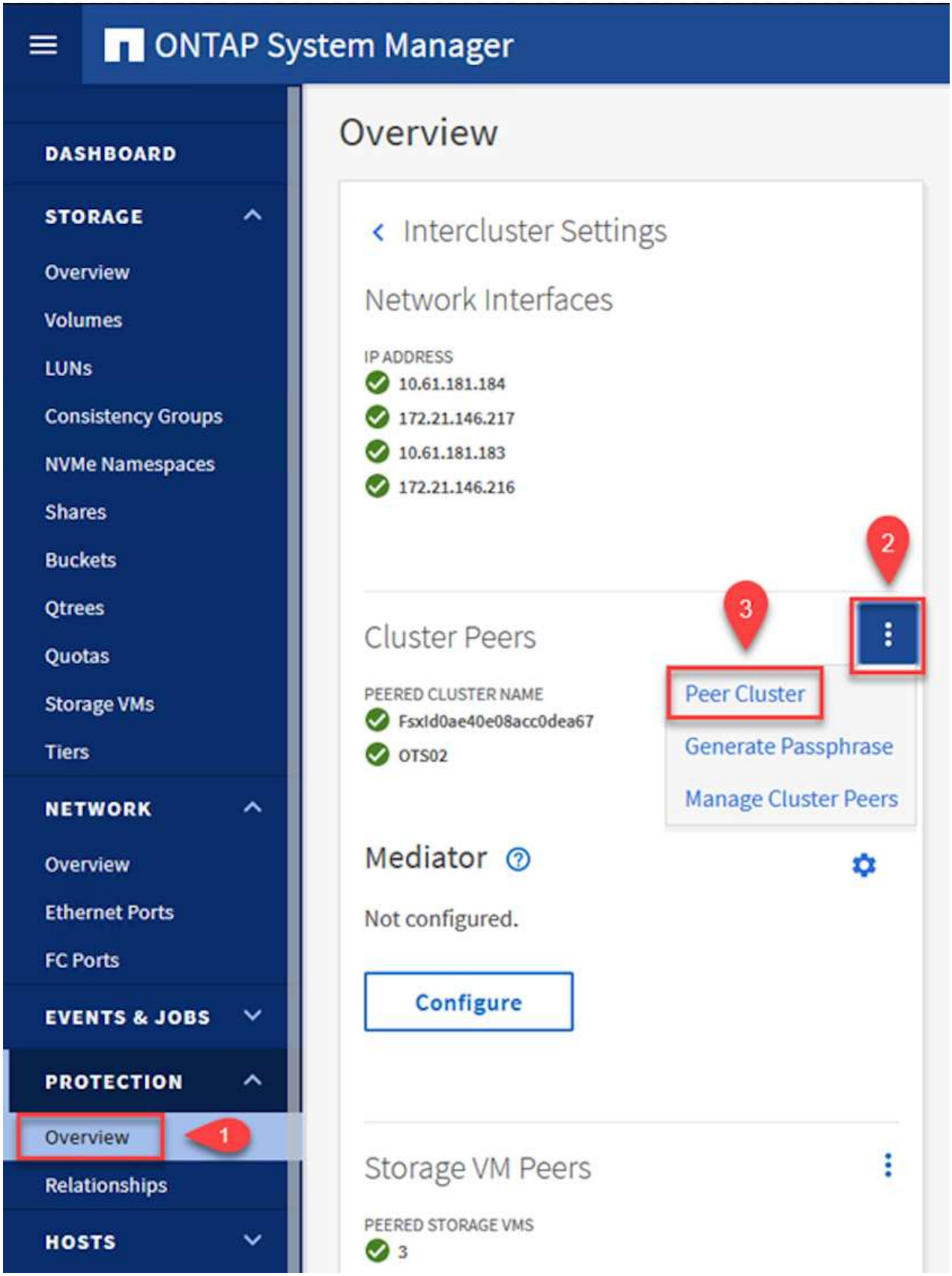
Stabilire il peering del cluster tra ONTAP e FSX

Per stabilire il peering del cluster tra i cluster ONTAP, è necessario confermare una passphrase univoca inserita nel cluster ONTAP di avvio nell'altro cluster peer.

1. Impostare il peering sul cluster FSX di destinazione utilizzando `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca da utilizzare in seguito nel cluster di origine per completare il processo di creazione.

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

2. Nel cluster di origine, è possibile stabilire la relazione peer del cluster utilizzando Gestore di sistema di ONTAP o l'interfaccia CLI. Da Gestore di sistema di ONTAP, accedere a protezione > Panoramica e selezionare cluster peer.

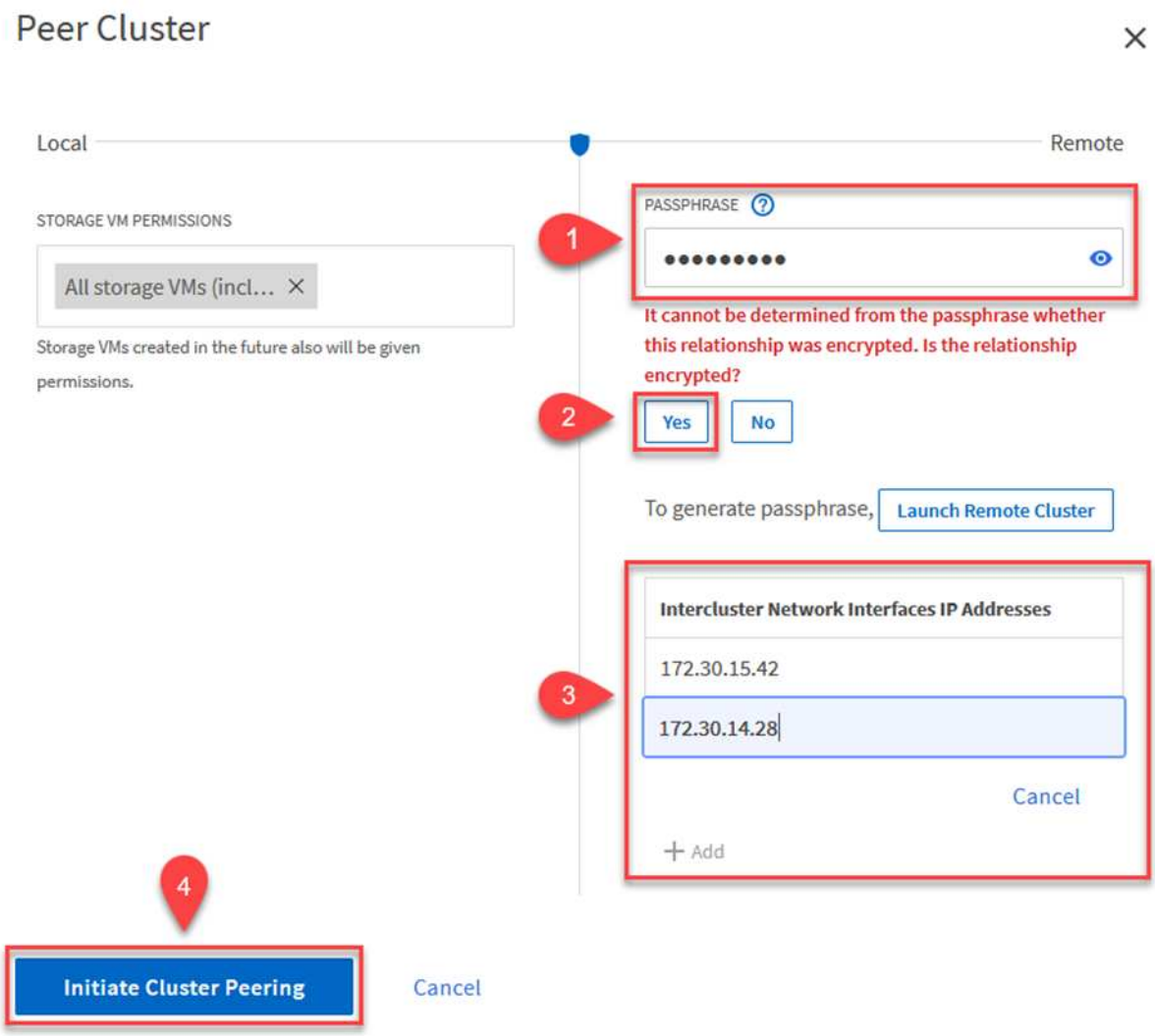


3. Nella finestra di dialogo Peer Cluster, inserire le informazioni richieste:
   a. Inserire la passphrase utilizzata per stabilire la relazione del cluster peer nel cluster FSX di destinazione.

b. Selezionare `Yes` per stabilire una relazione crittografata.

c. Inserire gli indirizzi IP LIF dell'intercluster del cluster FSX di destinazione.

d. Fare clic su Initiate Cluster peering (Avvia peering cluster) per completare il processo.



4. Verificare lo stato della relazione peer del cluster dal cluster FSX con il seguente comando:

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

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

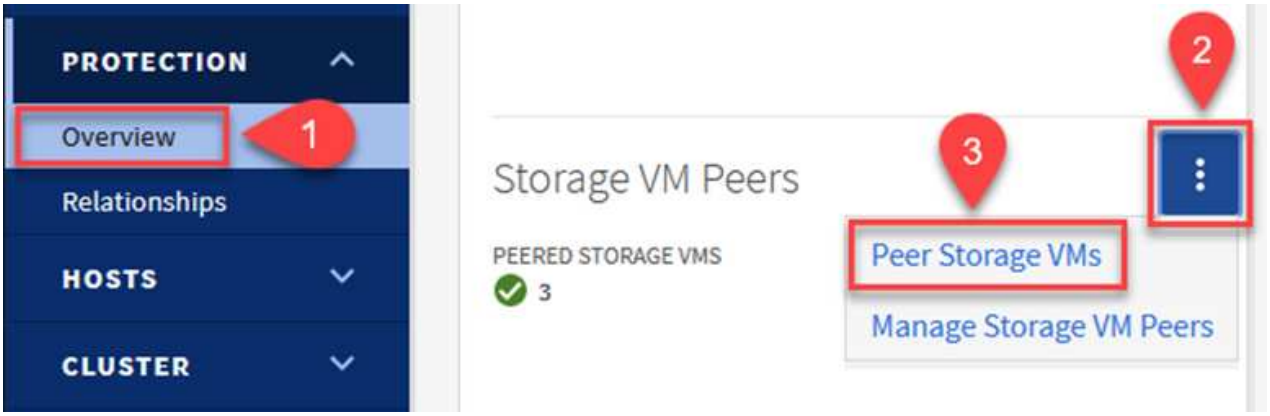
Stabilire una relazione di peering SVM

Il passaggio successivo consiste nell'impostare una relazione SVM tra le macchine virtuali dello storage di destinazione e di origine che contengono i volumi che si trovano nelle relazioni di SnapMirror.

1. Dal cluster FSX di origine, utilizzare il seguente comando dalla CLI per creare la relazione peer SVM:

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

2. Dal cluster ONTAP di origine, accettare la relazione di peering con Gestore di sistema ONTAP o CLI.
3. Da Gestore di sistema ONTAP, andare a protezione > Panoramica e selezionare le VM di storage peer in peer di macchine virtuali di storage.



4. Nella finestra di dialogo Peer Storage VM, compilare i campi obbligatori:
   - La VM di storage di origine
   - Il cluster di destinazione
   - La VM di storage di destinazione

5. Fare clic su Peer Storage VM per completare il processo di peering SVM.

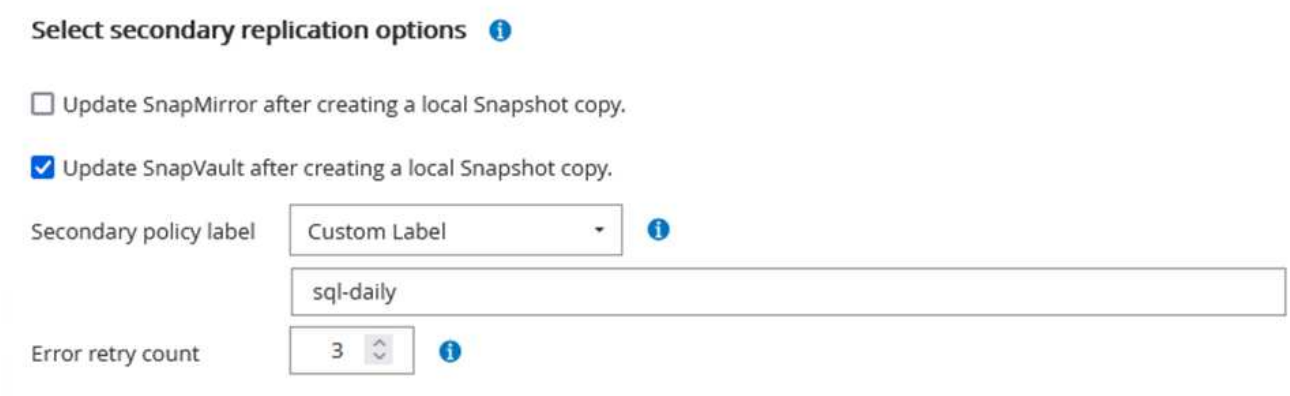
Creare un criterio di conservazione delle snapshot

SnapCenter gestisce le pianificazioni di conservazione per i backup che esistono come copie Snapshot sul sistema di storage primario. Questo viene stabilito quando si crea un criterio in SnapCenter. SnapCenter non gestisce le policy di conservazione per i backup conservati nei sistemi di storage secondari. Questi criteri vengono gestiti separatamente attraverso un criterio SnapMirror creato nel cluster FSX secondario e associato ai volumi di destinazione che si trovano in una relazione SnapMirror con il volume di origine.

Quando si crea un criterio SnapCenter, è possibile specificare un'etichetta di criterio secondaria che viene aggiunta all'etichetta SnapMirror di ogni snapshot generato quando viene eseguito un backup SnapCenter.

> Sullo storage secondario, queste etichette vengono associate alle regole dei criteri associate al volume di destinazione allo scopo di applicare la conservazione degli snapshot.

L'esempio seguente mostra un'etichetta SnapMirror presente su tutte le snapshot generate come parte di una policy utilizzata per i backup giornalieri del database SQL Server e dei volumi di log.



Per ulteriori informazioni sulla creazione di criteri SnapCenter per un database SQL Server, vedere "Documentazione SnapCenter".

È necessario innanzitutto creare un criterio SnapMirror con regole che determinano il numero di copie snapshot da conservare.

1. Creare il criterio SnapMirror sul cluster FSX.

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

2. Aggiungere regole al criterio con le etichette SnapMirror che corrispondono alle etichette dei criteri secondari specificate nei criteri SnapCenter.

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

Il seguente script fornisce un esempio di regola che è possibile aggiungere a un criterio:

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

Creare regole aggiuntive per ciascuna etichetta SnapMirror e il numero di snapshot da conservare (periodo di conservazione).

Creare volumi di destinazione

Per creare un volume di destinazione su FSX che riceverà le copie Snapshot dai volumi di origine, eseguire il seguente comando su FSX ONTAP:

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

Creare le relazioni di SnapMirror tra i volumi di origine e di destinazione

Per creare una relazione SnapMirror tra un volume di origine e un volume di destinazione, eseguire il seguente comando su FSX ONTAP:

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

Inizializzare le relazioni di SnapMirror

Inizializzare la relazione SnapMirror. Questo processo avvia un nuovo snapshot generato dal volume di origine e lo copia nel volume di destinazione.

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

Implementare e configurare Windows SnapCenter Server on-premise.

Implementazione del server Windows SnapCenter on-premise

Questa soluzione utilizza NetApp SnapCenter per eseguire backup coerenti con l'applicazione dei database SQL Server e Oracle. Insieme a Veeam Backup & Replication per il backup dei VMDK delle macchine virtuali, questo offre una soluzione completa di disaster recovery per data center on-premise e basati sul cloud.

Il software SnapCenter è disponibile sul sito di supporto NetApp e può essere installato su sistemi Microsoft Windows che risiedono in un dominio o in un gruppo di lavoro. Una guida dettagliata alla pianificazione e le istruzioni di installazione sono disponibili all'indirizzo "Centro di documentazione NetApp".

Il software SnapCenter è disponibile all'indirizzo "questo link".

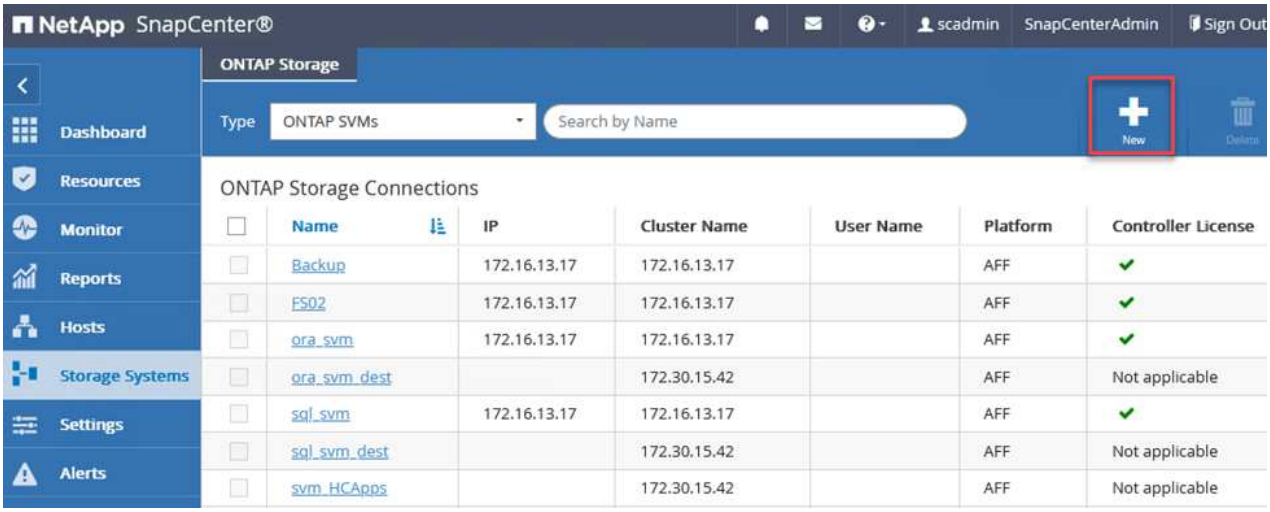
Una volta installata, è possibile accedere alla console SnapCenter da un browser Web utilizzando _ https://Virtual_Cluster_IP_or_FQDN:8146_.

Dopo aver effettuato l'accesso alla console, è necessario configurare SnapCenter per il backup dei database SQL Server e Oracle.

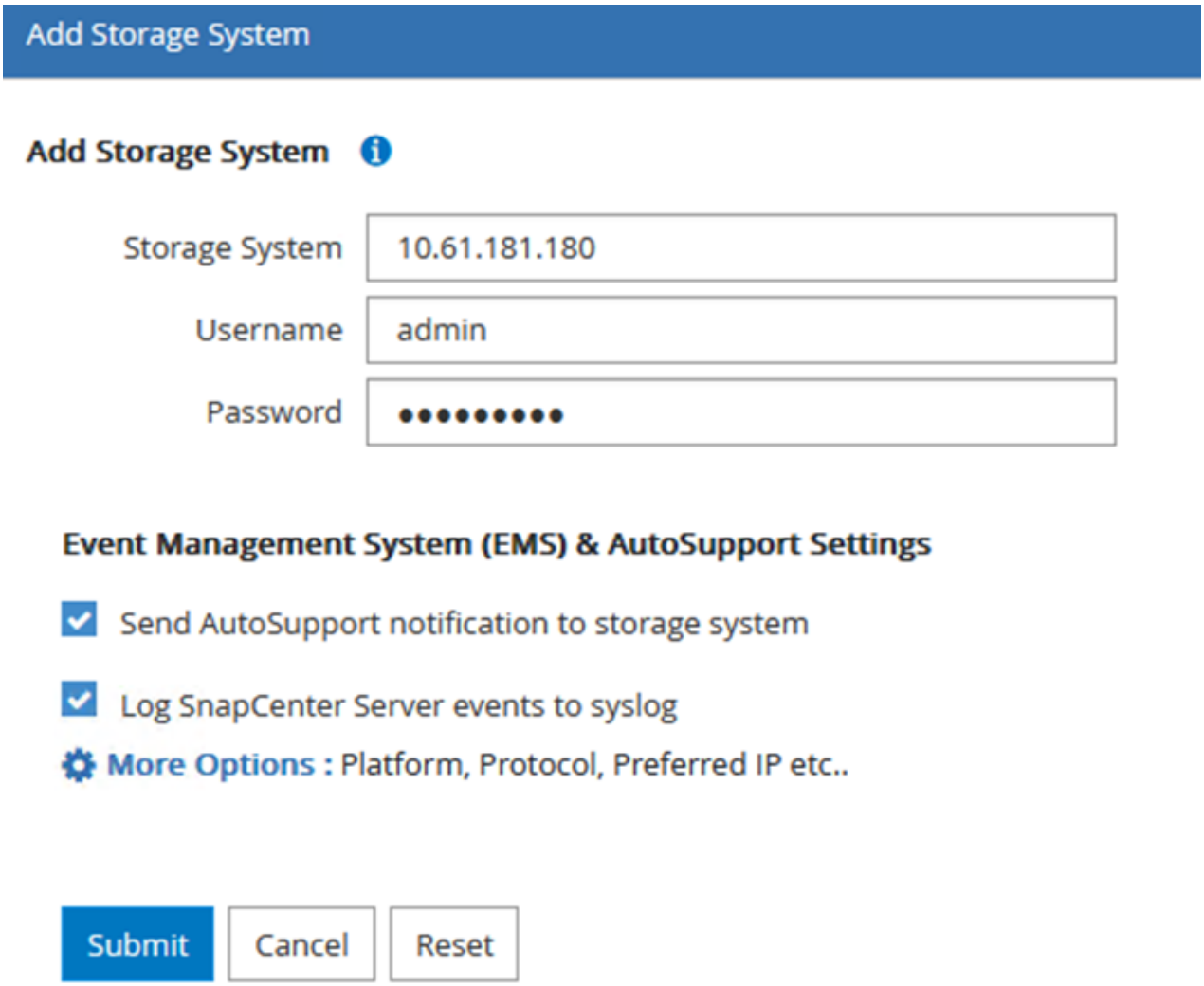
Aggiungere controller storage a SnapCenter

Per aggiungere controller di storage a SnapCenter, attenersi alla seguente procedura:

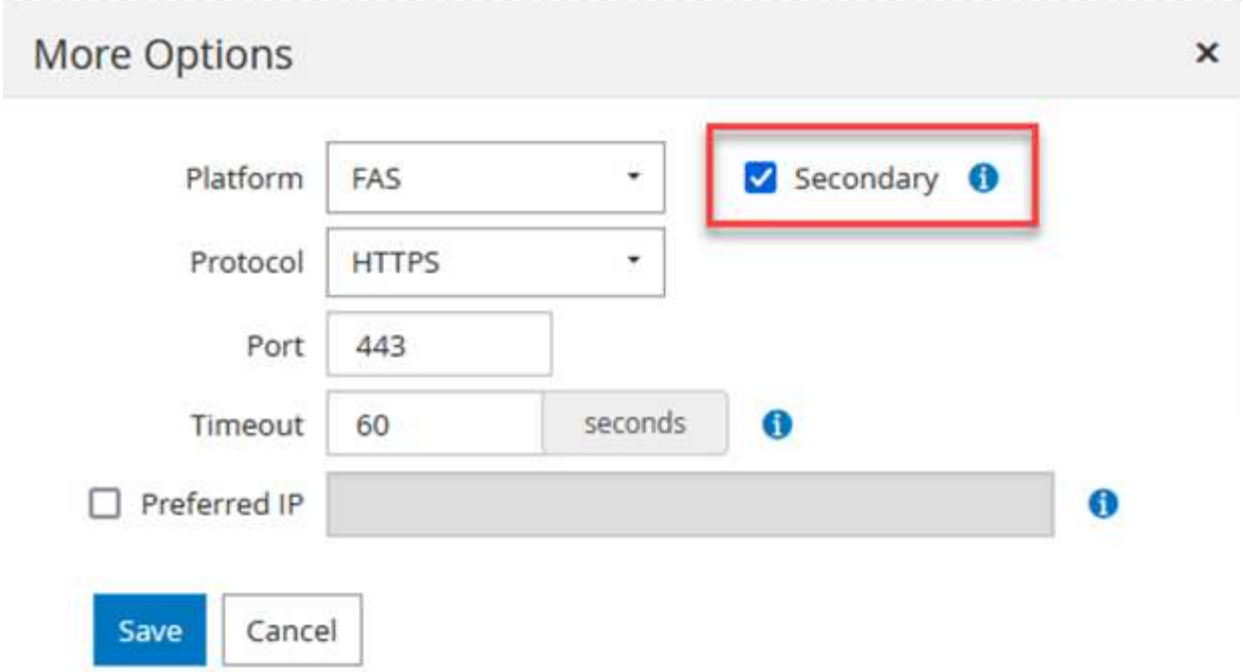
1. Dal menu a sinistra, selezionare sistemi storage, quindi fare clic su nuovo per avviare il processo di aggiunta dei controller storage a SnapCenter.



2. Nella finestra di dialogo Aggiungi sistema di storage, aggiungere l'indirizzo IP di gestione del cluster ONTAP locale on-premise e il nome utente e la password. Quindi fare clic su Submit (Invia) per avviare il rilevamento del sistema storage.



3. Ripetere questa procedura per aggiungere il sistema FSX ONTAP a SnapCenter. In questo caso, selezionare More Options (altre opzioni) nella parte inferiore della finestra Add Storage System (Aggiungi sistema di storage) e fare clic sulla casella di controllo Secondary (secondario) per designare il sistema FSX come sistema di storage secondario aggiornato con le copie SnapMirror o le snapshot di backup primarie.

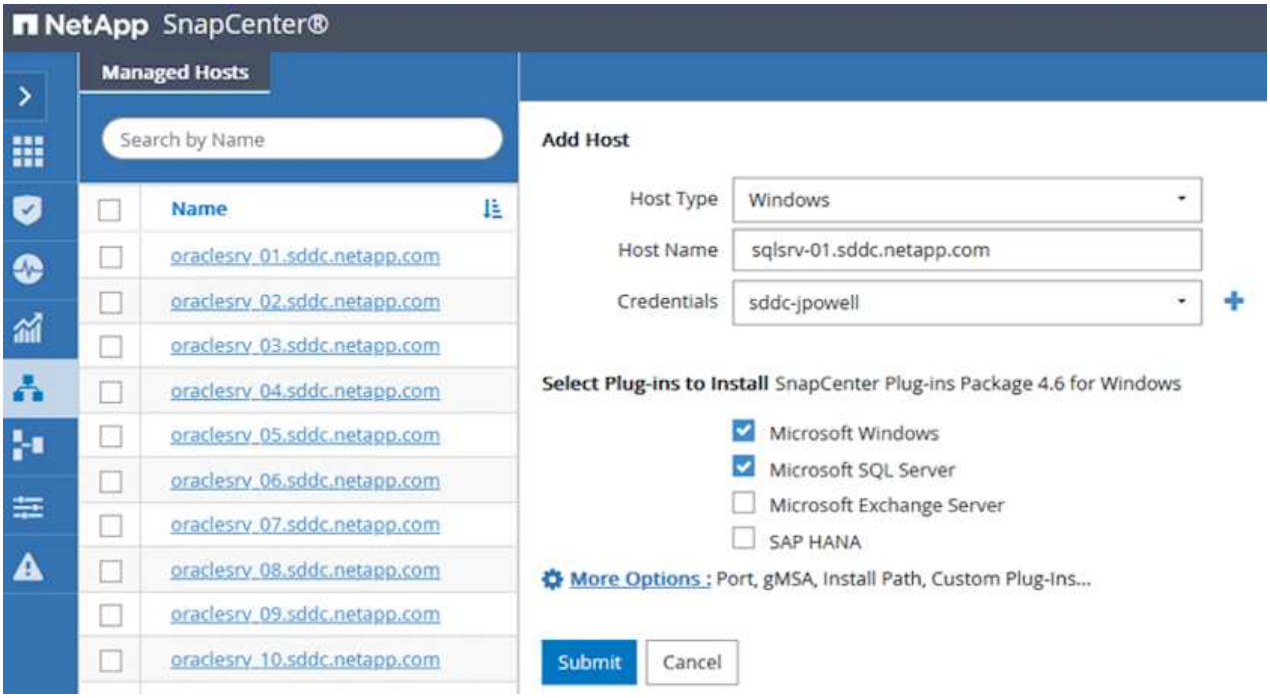


Per ulteriori informazioni sull'aggiunta di sistemi storage a SnapCenter, consultare la documentazione all'indirizzo "questo link".

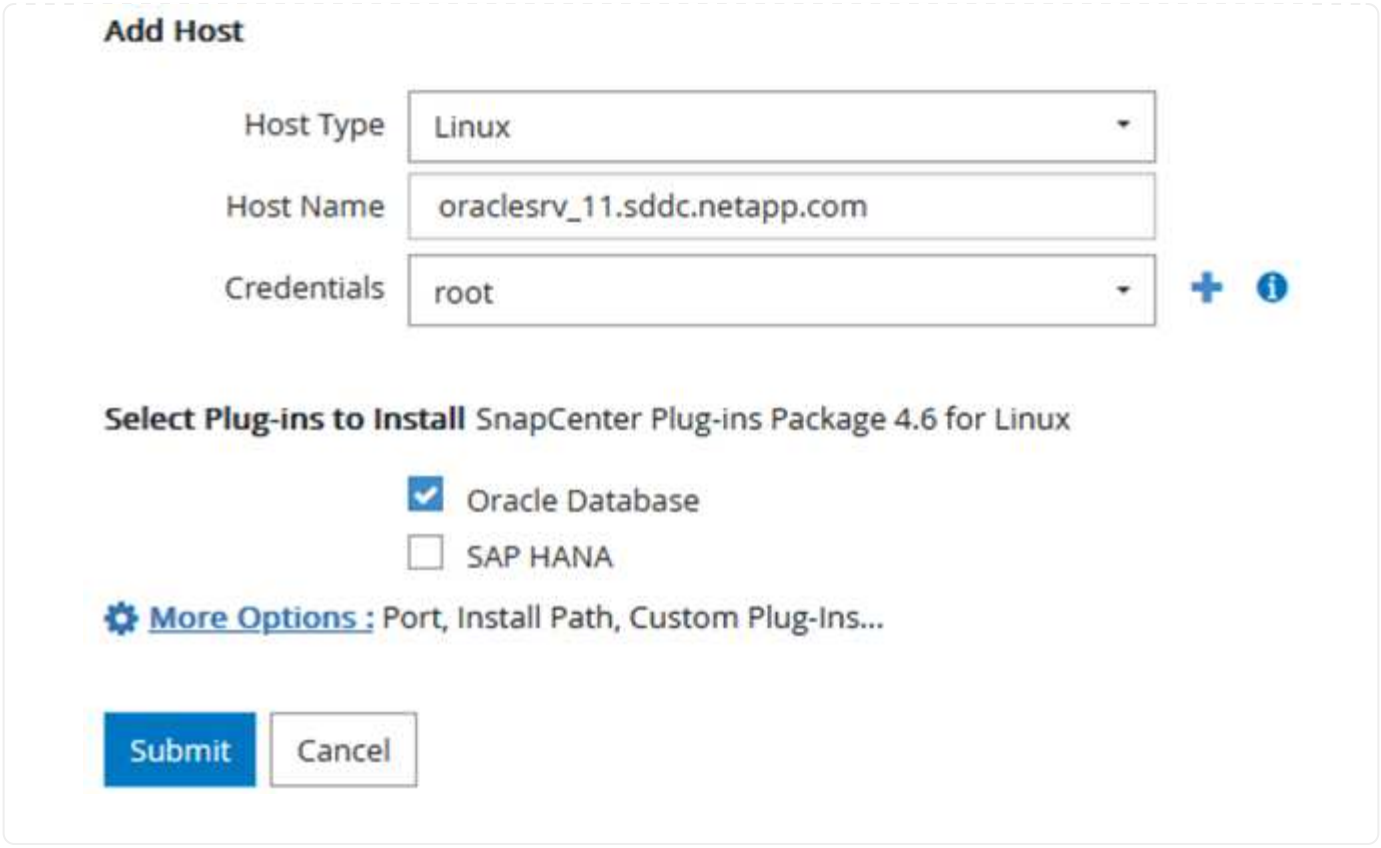
Aggiungere host a SnapCenter

Il passaggio successivo consiste nell'aggiungere server applicazioni host a SnapCenter. Il processo è simile sia per SQL Server che per Oracle.

1. Dal menu a sinistra, selezionare host, quindi fare clic su Aggiungi per avviare il processo di aggiunta dei controller di storage a SnapCenter.
2. Nella finestra Add hosts (Aggiungi host), aggiungere il tipo di host, il nome host e le credenziali del sistema host. Selezionare il tipo di plug-in. Per SQL Server, selezionare il plug-in Microsoft Windows e Microsoft SQL Server.



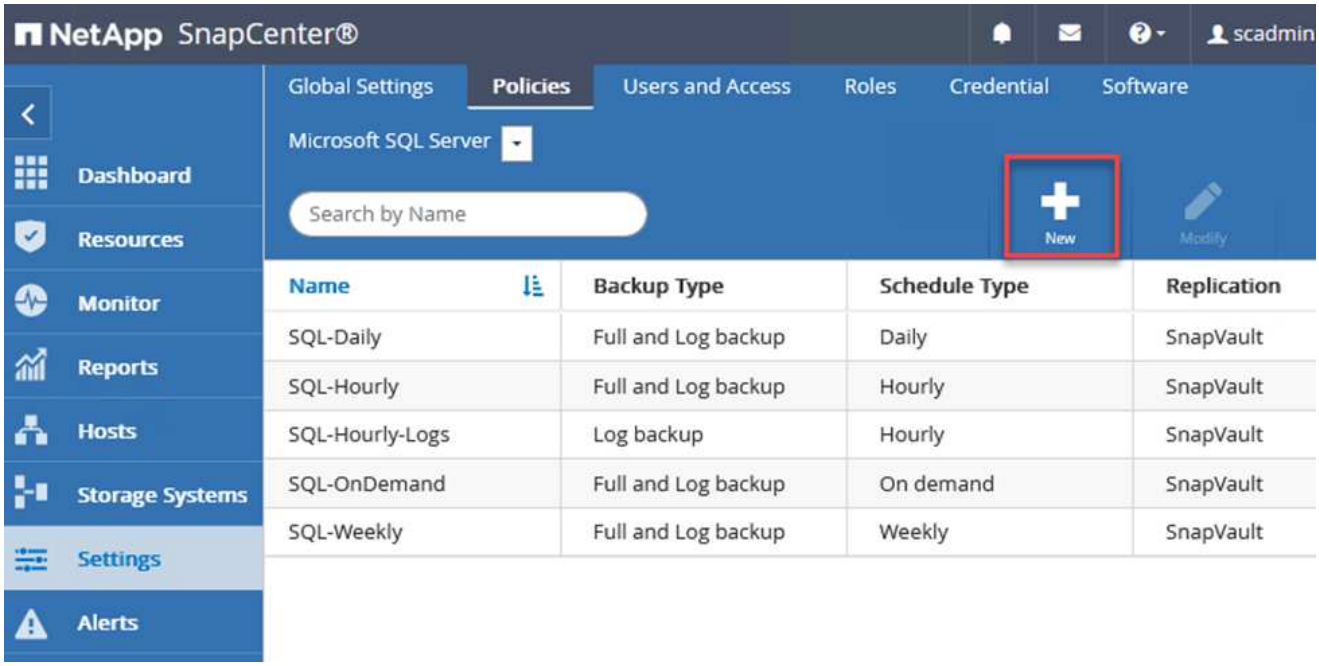
3. Per Oracle, compilare i campi obbligatori nella finestra di dialogo Add host (Aggiungi host) e selezionare la casella di controllo per il plug-in Oracle Database. Fare clic su Submit (Invia) per avviare il processo di rilevamento e aggiungere l'host a SnapCenter.


Add Host
Host Type
Linux
Host Name
oraclesrv_11.sddc.netapp.com
Credentials
root
Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux
Oracle Database
SAP HANA
More Options : Port, Install Path, Custom Plug-Ins...
Submit
Cancel

Creare policy SnapCenter

I criteri stabiliscono le regole specifiche da seguire per un processo di backup. Includono, a titolo esemplificativo ma non esaustivo, la pianificazione del backup, il tipo di replica e il modo in cui SnapCenter gestisce il backup e il troncamento dei log delle transazioni.

È possibile accedere ai criteri nella sezione Impostazioni del client Web di SnapCenter.



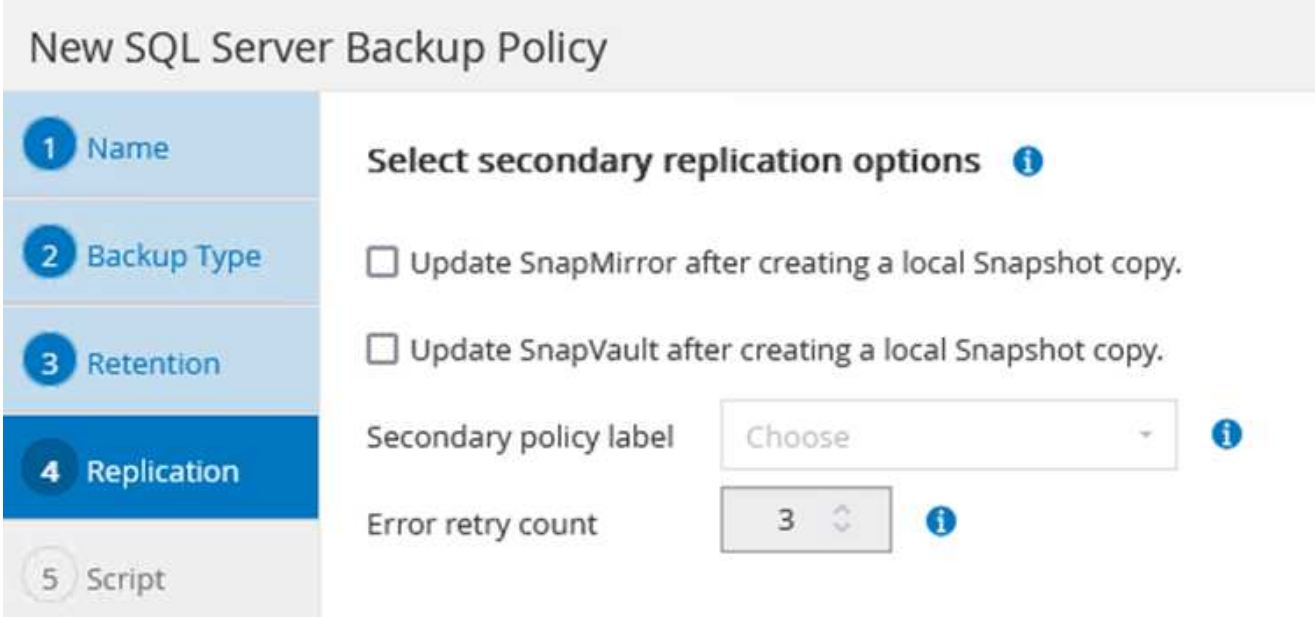
Per informazioni complete sulla creazione di criteri per i backup di SQL Server, vedere "Documentazione SnapCenter".

Per informazioni complete sulla creazione di policy per i backup Oracle, vedere "Documentazione SnapCenter".

Note:

- Durante la creazione guidata dei criteri, prendere nota della sezione Replication (Replica). In questa sezione vengono descritti i tipi di copie SnapMirror secondarie che si desidera eseguire durante il processo di backup.
- L'impostazione "Update SnapMirror after creating a local Snapshot copy" (Aggiorna SnapMirror dopo la creazione di una copia Snapshot locale) fa riferimento all'aggiornamento di una relazione SnapMirror quando tale relazione esiste tra due macchine virtuali di storage che risiedono sullo stesso cluster.
- L'impostazione "Aggiorna SnapVault dopo la creazione di una copia snapshot locale" viene utilizzata per aggiornare una relazione SnapMirror esistente tra due cluster separati e tra un sistema ONTAP on-premise e Cloud Volumes ONTAP o FSxN.

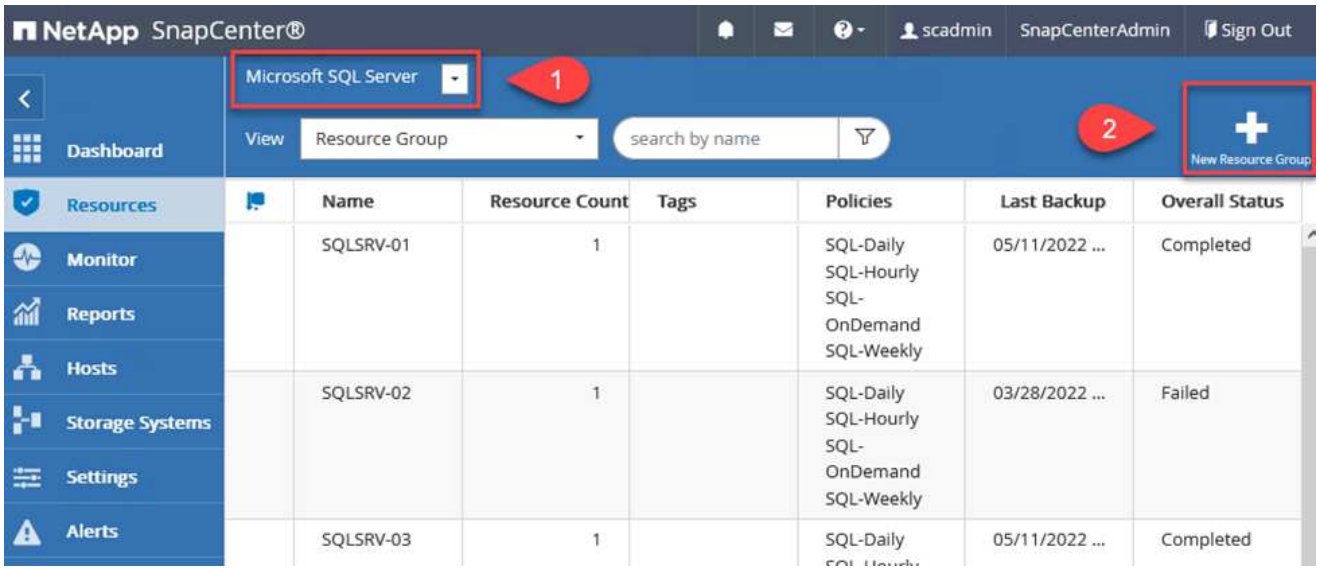
L'immagine seguente mostra le opzioni precedenti e l'aspetto della procedura guidata dei criteri di backup.



Creare gruppi di risorse SnapCenter

I gruppi di risorse consentono di selezionare le risorse di database che si desidera includere nei backup e i criteri seguiti per tali risorse.

1. Accedere alla sezione risorse nel menu a sinistra.
2. Nella parte superiore della finestra, selezionare il tipo di risorsa da utilizzare (in questo caso Microsoft SQL Server), quindi fare clic su New Resource Group (nuovo gruppo di risorse).



La documentazione di SnapCenter illustra i dettagli passo-passo per la creazione di gruppi di risorse per database SQL Server e Oracle.

Per eseguire il backup delle risorse SQL, seguire questa procedura "questo link".

Per eseguire il backup delle risorse Oracle, seguire questa procedura "questo link".

Implementare e configurare Veeam Backup Server

Il software Veeam Backup & Replication viene utilizzato nella soluzione per eseguire il backup delle macchine virtuali delle applicazioni e archiviare una copia dei backup in un bucket Amazon S3 utilizzando un repository di backup scale-out Veeeam (SOBR). Veeam viene implementato su un server Windows in questa soluzione. Per informazioni specifiche sull'implementazione di Veeam, vedere "Documentazione tecnica del centro di assistenza Veeam".

Configurare il repository di backup scale-out Veeam

Dopo aver implementato e ottenuto la licenza del software, è possibile creare un repository di backup scale-out (SOBR) come storage di destinazione per i processi di backup. È inoltre necessario includere un bucket S3 come backup dei dati delle macchine virtuali fuori sede per il disaster recovery.

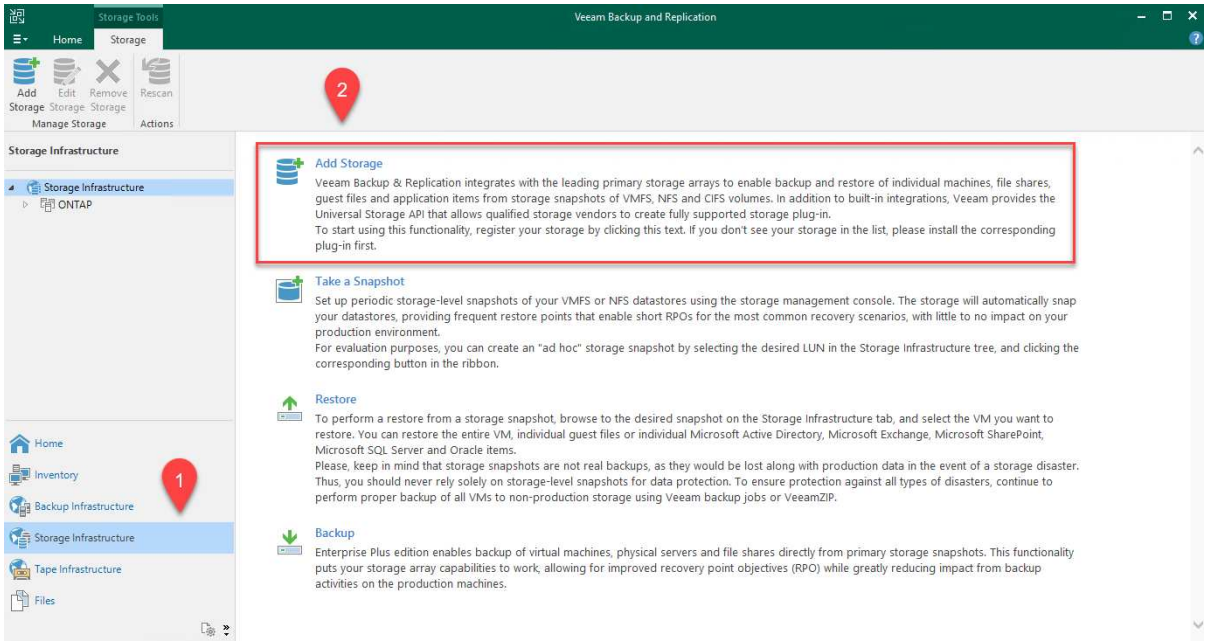
Prima di iniziare, consultare i seguenti prerequisiti.

1. Creare una condivisione di file SMB sul sistema ONTAP on-premise come storage di destinazione per i backup.
2. Crea un bucket Amazon S3 da includere nel SOBR. Si tratta di un repository per i backup fuori sede.

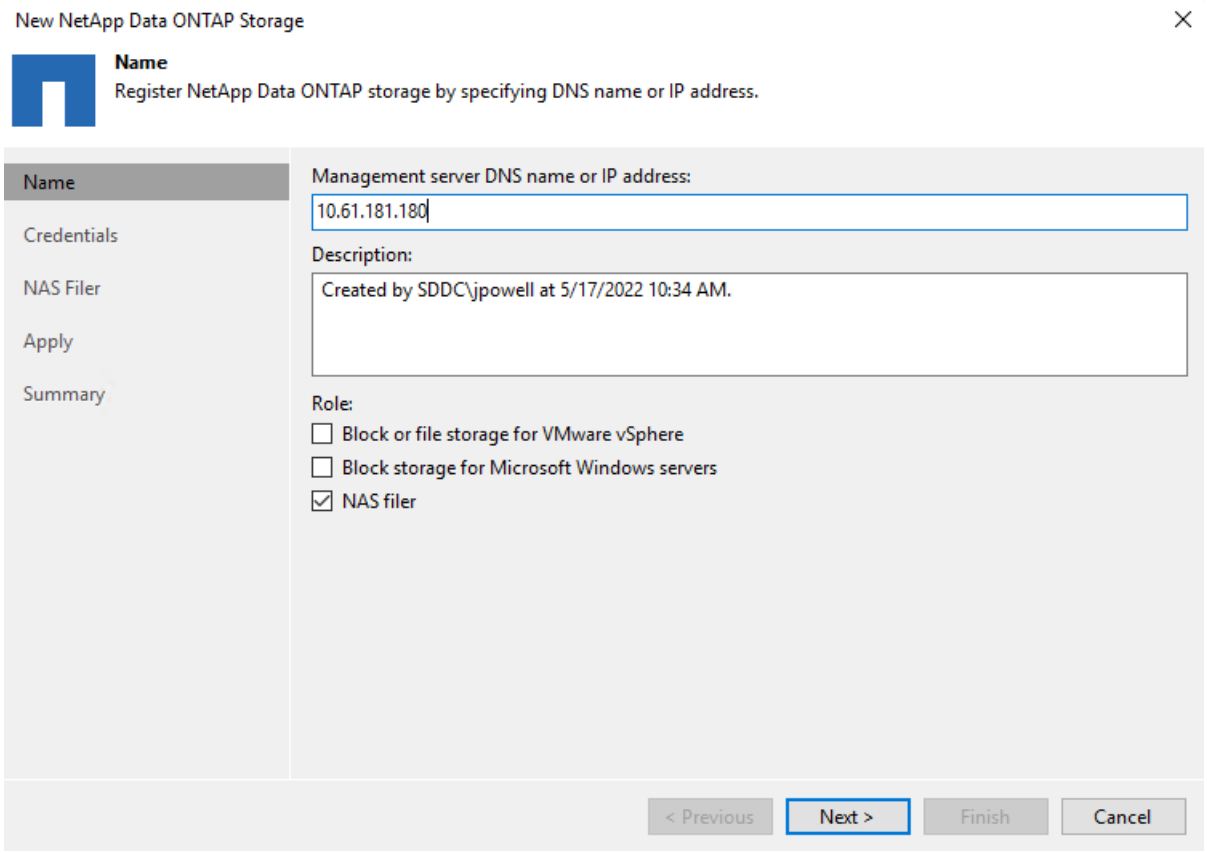
Aggiungere storage ONTAP a Veeam

Innanzitutto, aggiungere il cluster di storage ONTAP e il relativo file system SMB/NFS come infrastruttura storage in Veeam.

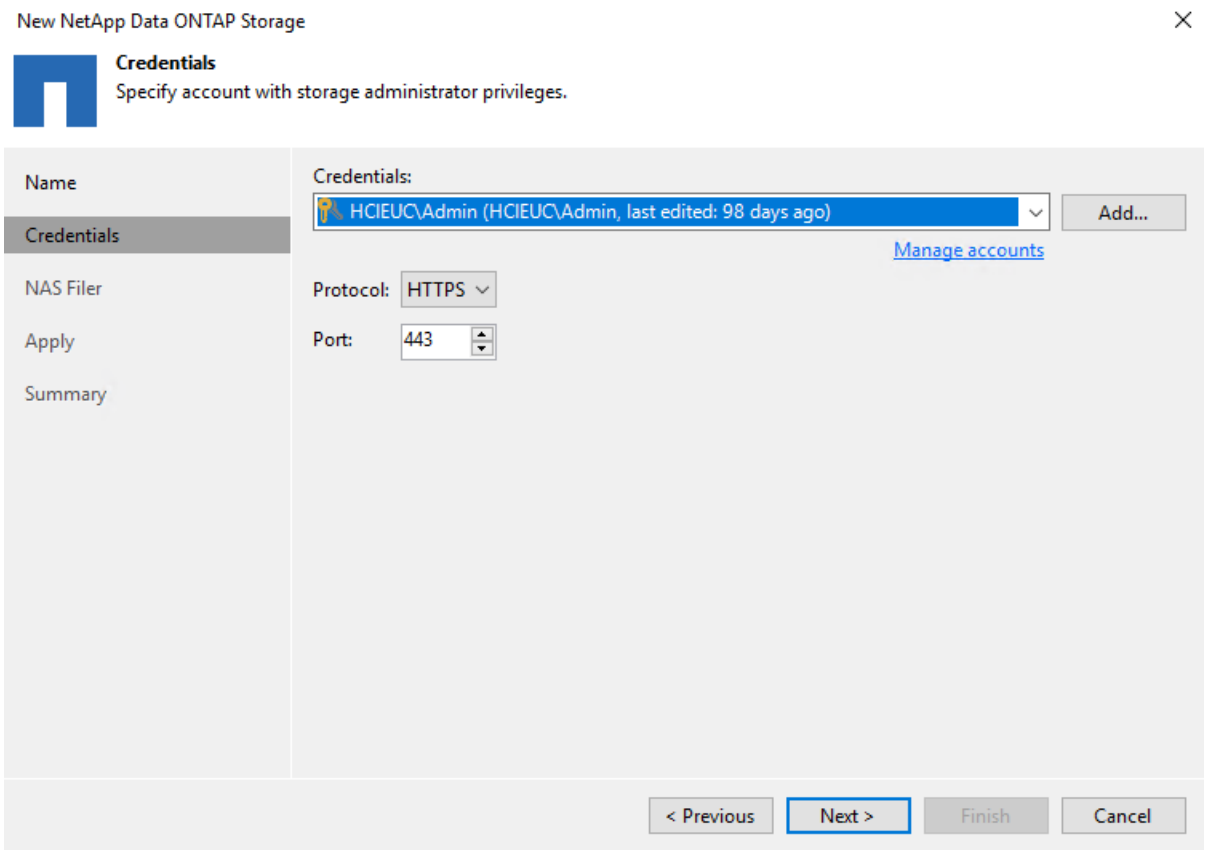
1. Aprire la console Veeam ed effettuare l'accesso. Accedere a Storage Infrastructure (infrastruttura storage) e selezionare Add Storage (Aggiungi storage).



2. Nella procedura guidata Aggiungi storage, selezionare NetApp come vendor dello storage, quindi selezionare Data ONTAP.
3. Inserire l'indirizzo IP di gestione e selezionare la casella NAS Filer (Filer NAS). Fare clic su Avanti.

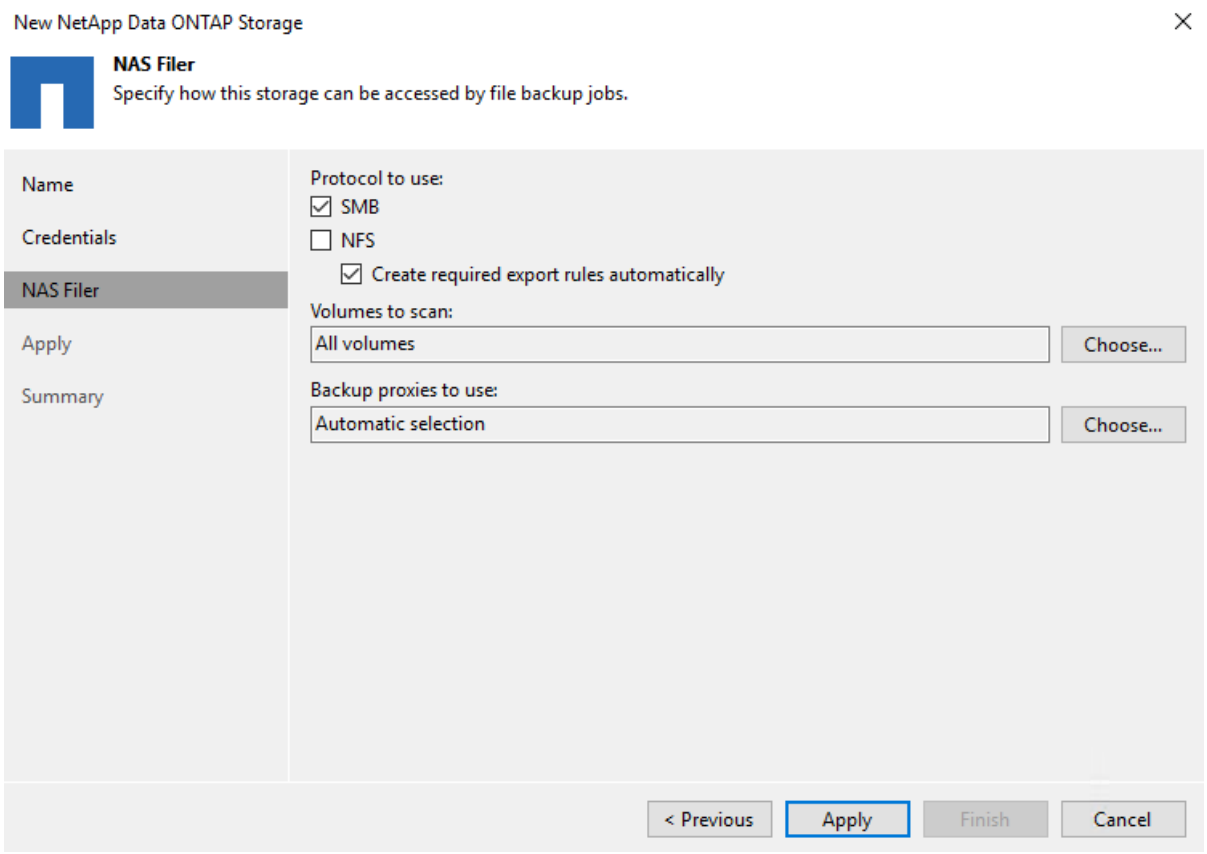


4. Aggiungere le credenziali per accedere al cluster ONTAP.

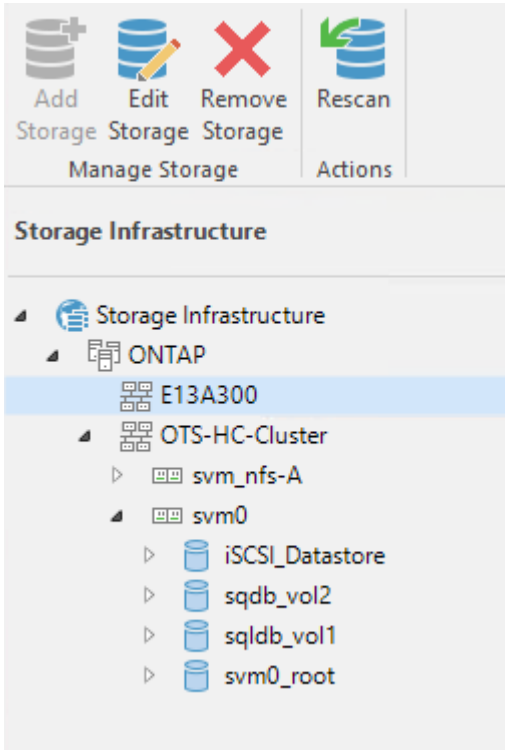


5. Nella pagina NAS Filer (Filer NAS), scegliere i protocolli desiderati per la scansione e

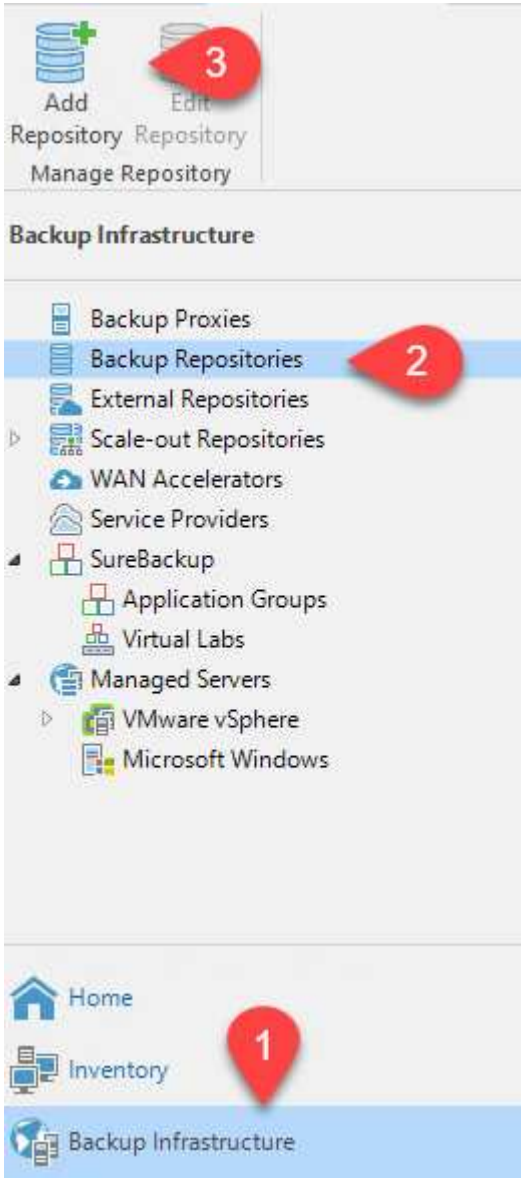
selezionare Next (Avanti).



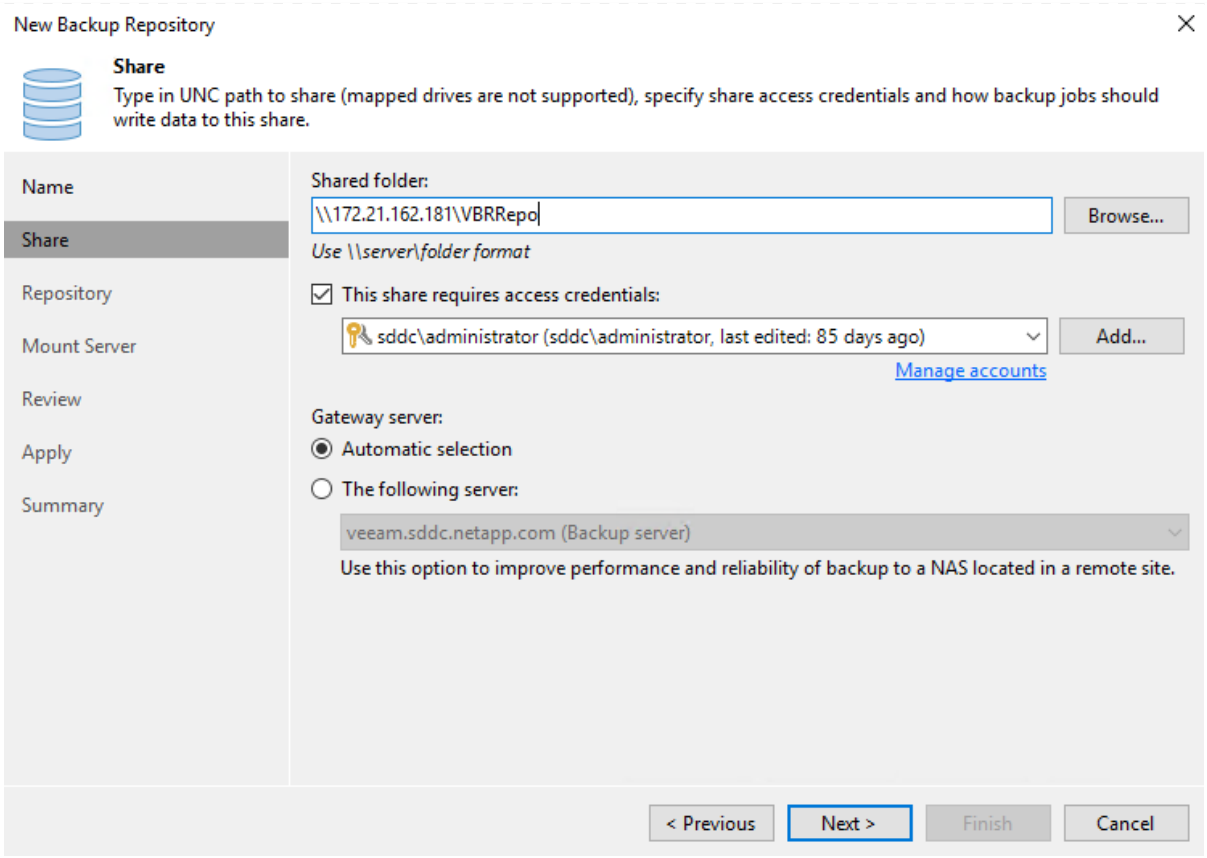
6. Completare le pagine Apply (Applica) e Summary (Riepilogo) della procedura guidata e fare clic su Finish (fine) per avviare il processo di rilevamento dello storage. Al termine della scansione, il cluster ONTAP viene aggiunto insieme ai filer NAS come risorse disponibili.



7. Creare un repository di backup utilizzando le condivisioni NAS appena rilevate. Da Backup Infrastructure (infrastruttura di backup), selezionare Backup Repository (repository di backup) e fare clic sulla voce di menu Add Repository (Aggiungi repository).



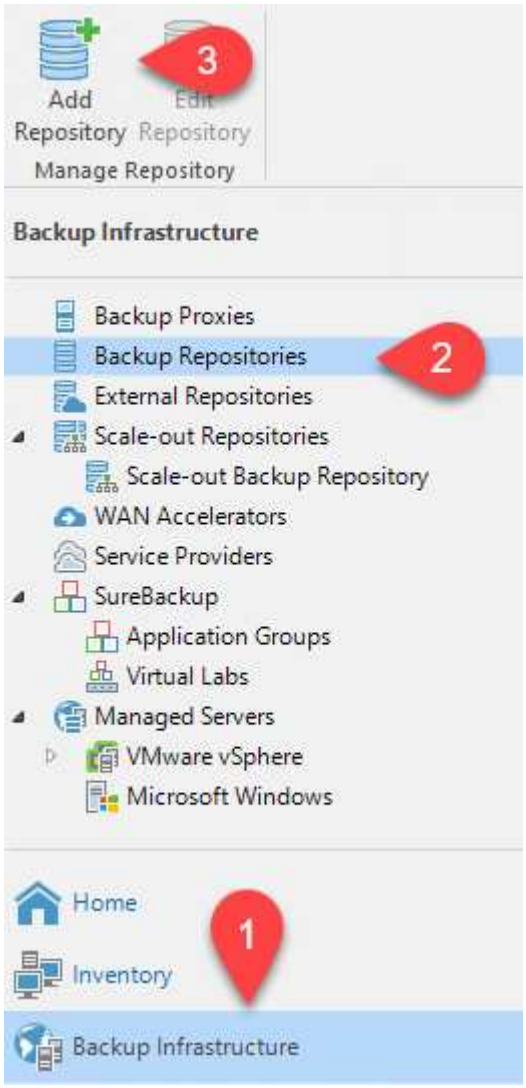
8. Seguire tutti i passaggi della procedura guidata nuovo repository di backup per creare il repository. Per informazioni dettagliate sulla creazione di repository di backup Veeam, vedere "Documentazione Veeam".


New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\172.21.162.181\VBRRepo
Browse...
Use \\server\folder format
This share requires access credentials:
sddc\administrator (sddc\administrator, last edited: 85 days ago)
Add...
Manage accounts
Gateway server:
Automatic selection
The following server:
veeam.sddc.netapp.com (Backup server)
Use this option to improve performance and reliability of backup to a NAS located in a remote site.
< Previous
Next >
Finish
Cancel

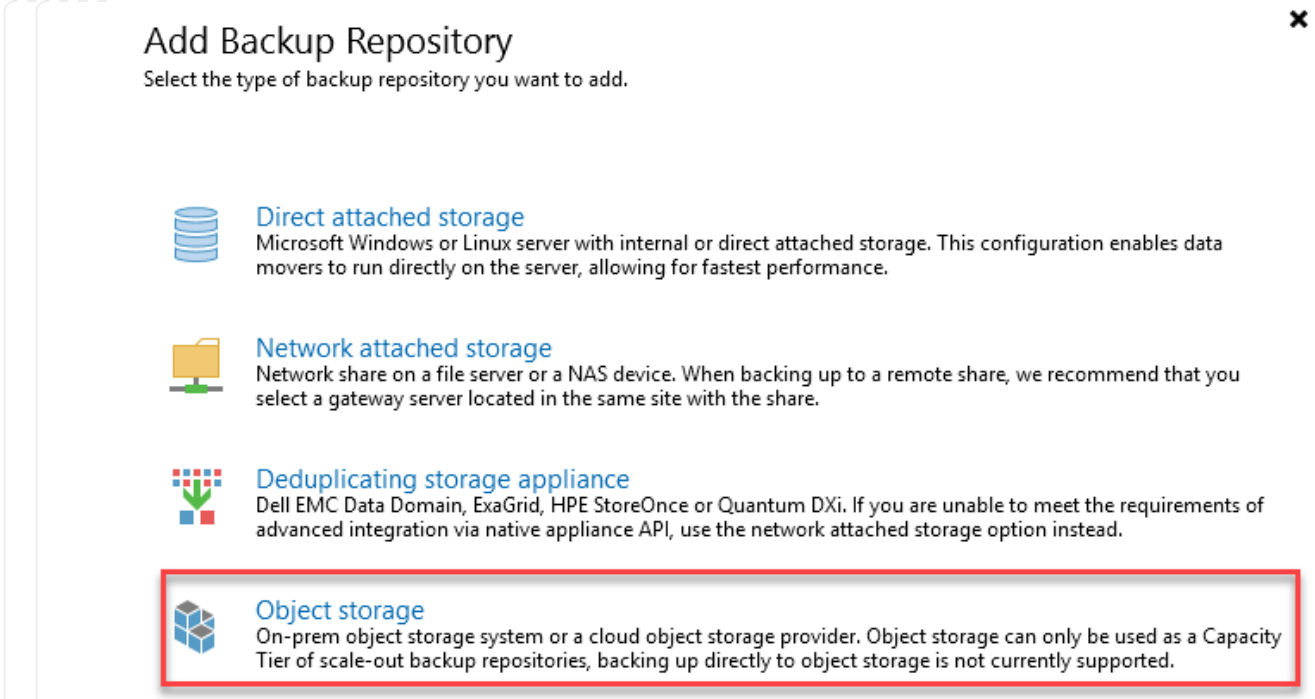
Aggiungi il bucket Amazon S3 come repository di backup

Il passaggio successivo consiste nell'aggiungere lo storage Amazon S3 come repository di backup.

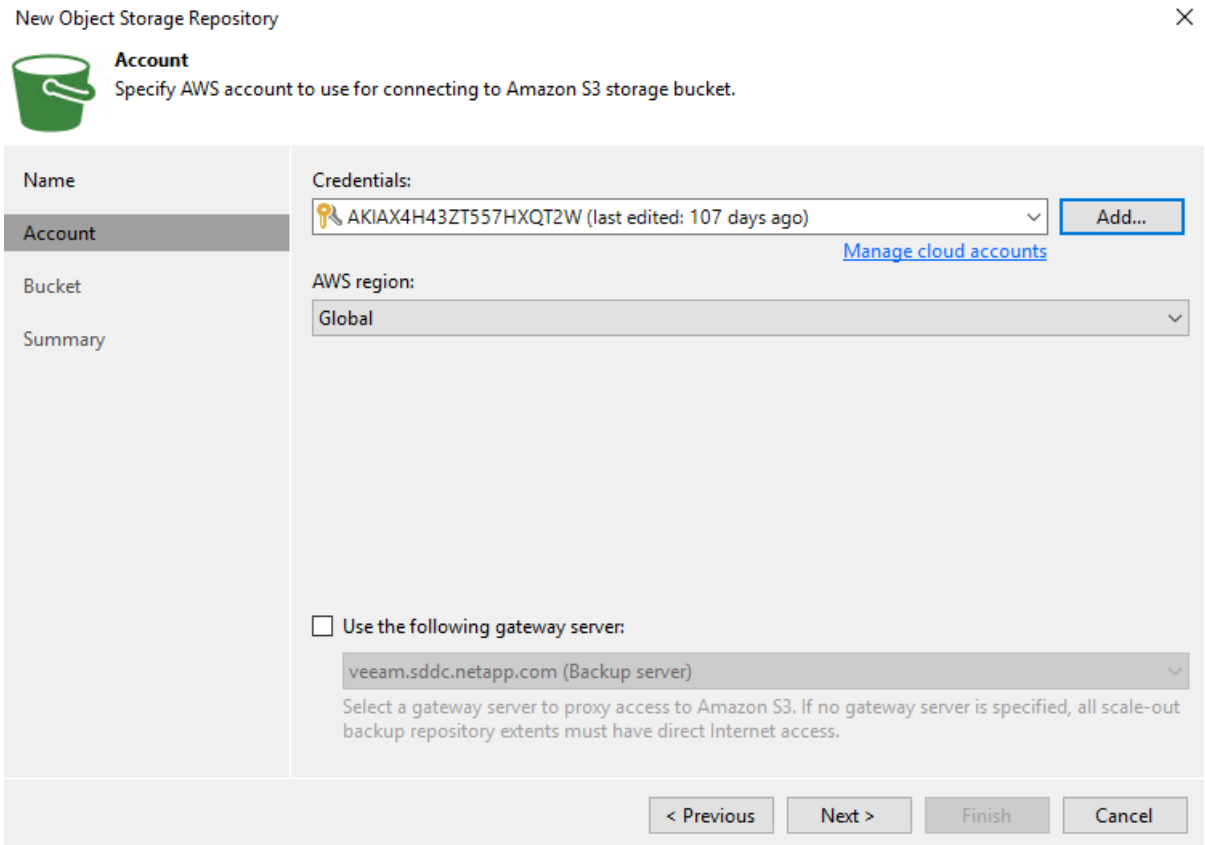
1. Accedere a infrastruttura di backup > Repository di backup. Fare clic su Add Repository (Aggiungi repository).



2. Nella procedura guidata Aggiungi repository di backup, selezionare Archivio oggetti, quindi Amazon S3. Viene avviata la procedura guidata nuovo archivio oggetti.



3. Fornire un nome per il repository di storage a oggetti e fare clic su Next (Avanti).
4. Nella sezione successiva, fornire le credenziali. Sono necessari una chiave di accesso AWS e una chiave segreta.

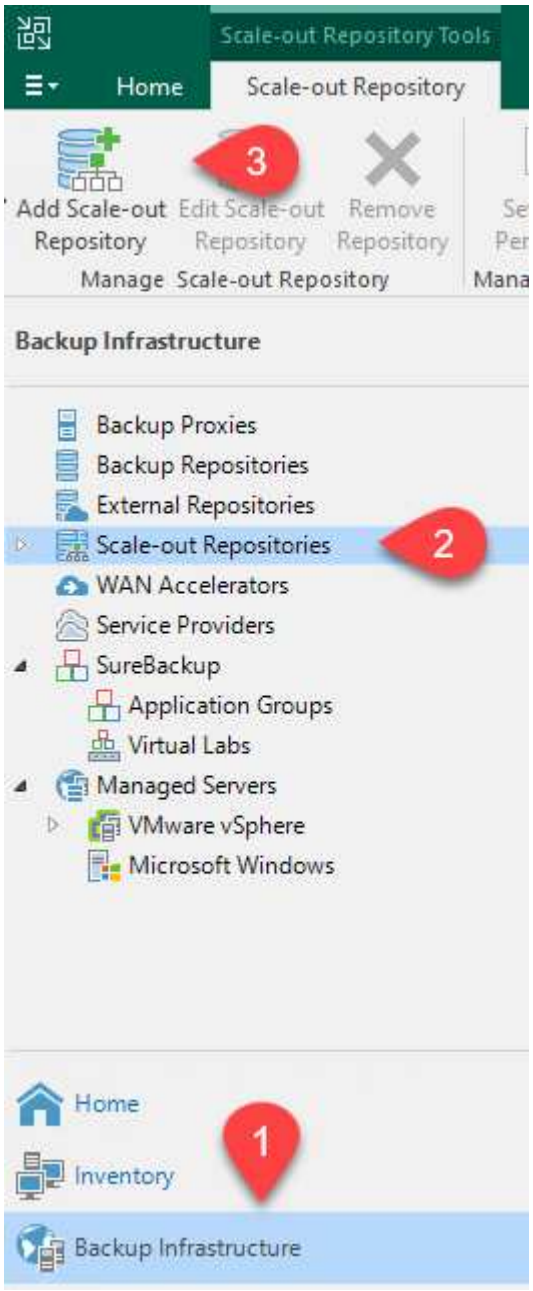


5. Una volta caricata la configurazione Amazon, scegliere il data center, il bucket e la cartella e fare clic su Apply (Applica). Infine, fare clic su fine per chiudere la procedura guidata.

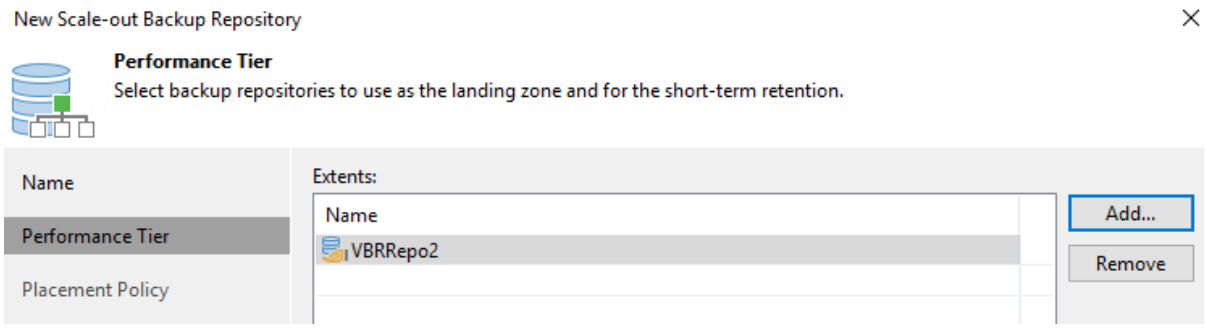
Creare un repository di backup scale-out

Ora che abbiamo aggiunto i nostri repository di storage a Veeam, possiamo creare il SOBR per tierare automaticamente le copie di backup nel nostro storage a oggetti Amazon S3 fuori sede per il disaster recovery.

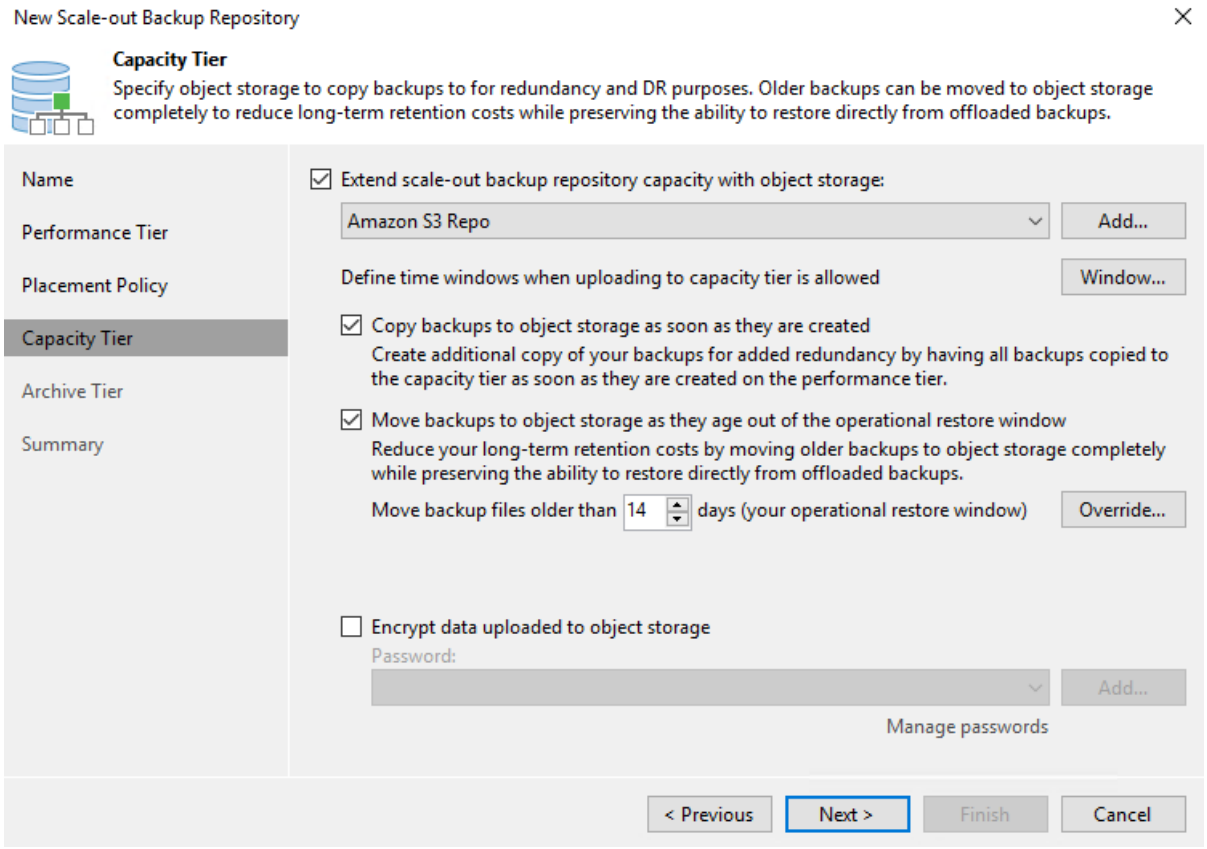
1. Da Backup Infrastructure (infrastruttura di backup), selezionare Scale-out Repository (repository scale-out), quindi fare clic sulla voce di menu Add Scale-out Repository (Aggiungi repository scale-out).



2. Nel nuovo repository di backup scale-out, immettere un nome per il SOBR e fare clic su Avanti.
3. Per il livello di performance, scegliere il repository di backup che contiene la condivisione SMB che risiede nel cluster ONTAP locale.



4. Per la policy di posizionamento, scegli la localizzazione dei dati o le performance in base ai tuoi requisiti. Selezionare Avanti.
5. Per il livello di capacità estendiamo il SOBR con lo storage a oggetti Amazon S3. Ai fini del disaster recovery, selezionare Copy Backup to Object Storage (Copia backup su storage a oggetti) non appena vengono creati per garantire la consegna tempestiva dei backup secondari.



6. Infine, selezionare Apply (Applica) e Finish (fine) per finalizzare la creazione del SOBR.

Creare i processi di repository di backup scale-out

L'ultima fase della configurazione di Veeam consiste nella creazione di processi di backup utilizzando il SOBR appena creato come destinazione di backup. La creazione di processi di backup è una parte normale del repertorio di qualsiasi amministratore dello storage e non viene descritta la procedura dettagliata. Per informazioni più complete sulla creazione di processi di backup in Veeam, vedere "Documentazione tecnica del Centro assistenza Veeam".

Configurazione e strumenti di backup e recovery di BlueXP

Per eseguire un failover delle macchine virtuali applicative e dei volumi di database sui servizi di volume cloud VMware in esecuzione in AWS, è necessario installare e configurare un'istanza in esecuzione del server SnapCenter e del server di backup e replica Veeeam. Una volta completato il failover, è necessario configurare questi strumenti per riprendere le normali operazioni di backup fino a quando non viene pianificato ed eseguito un failback al data center on-premise.

Implementare il server Windows SnapCenter secondario

Il server SnapCenter viene implementato nell'SDDC cloud VMware o installato su un'istanza EC2 che risiede in un VPC con connettività di rete all'ambiente cloud VMware.

Il software SnapCenter è disponibile sul sito di supporto NetApp e può essere installato su sistemi Microsoft Windows che risiedono in un dominio o in un gruppo di lavoro. Una guida dettagliata alla pianificazione e le istruzioni di installazione sono disponibili all'indirizzo "Centro di documentazione NetApp".

Il software SnapCenter è disponibile all'indirizzo "questo link".

Configurare il server secondario Windows SnapCenter

Per eseguire un ripristino dei dati applicativi mirrorati in FSX ONTAP, è necessario prima eseguire un ripristino completo del database SnapCenter on-premise. Una volta completato questo processo, la comunicazione con le macchine virtuali viene ristabilita e i backup delle applicazioni possono ora riprendere utilizzando FSX ONTAP come storage primario.

A tale scopo, è necessario completare i seguenti elementi sul server SnapCenter:

1. Configurare il nome del computer in modo che sia identico al server SnapCenter on-premise originale.
2. Configurare il networking per comunicare con VMware Cloud e l'istanza di FSX ONTAP.
3. Completare la procedura per ripristinare il database SnapCenter.
4. Verificare che SnapCenter sia in modalità di disaster recovery per assicurarsi che FSX sia ora lo storage primario per i backup.
5. Verificare che la comunicazione con le macchine virtuali ripristinate sia stata ristabilita.

Implementare il server di replica Veeam Backup & secondario

È possibile installare il server Veeam Backup & Replication su un server Windows in VMware Cloud su AWS o su un'istanza EC2. Per informazioni dettagliate sull'implementazione, vedere "Documentazione tecnica del Centro assistenza Veeam".

Configurare il server di replica di Veeam Backup & secondario

Per eseguire un ripristino delle macchine virtuali di cui è stato eseguito il backup sullo storage Amazon S3, è necessario installare Veeam Server su un server Windows e configurarlo per comunicare con VMware Cloud, FSX ONTAP e il bucket S3 che contiene il repository di backup originale. Deve inoltre disporre di un nuovo repository di backup configurato su FSX ONTAP per eseguire nuovi backup delle macchine virtuali dopo il ripristino.

Per eseguire questo processo, è necessario completare i seguenti elementi:

1. Configurare il networking per comunicare con VMware Cloud, FSX ONTAP e il bucket S3 contenente il repository di backup originale.
2. Configura una condivisione SMB su FSX ONTAP per diventare un nuovo repository di backup.
3. Montare il bucket S3 originale utilizzato come parte del repository di backup scale-out on-premise.
4. Dopo il ripristino della macchina virtuale, stabilire nuovi processi di backup per proteggere le macchine virtuali SQL e Oracle.

Per ulteriori informazioni sul ripristino delle macchine virtuali utilizzando Veeam, vedere la sezione "Ripristinare le macchine virtuali dell'applicazione con il ripristino completo di Veeam".

Backup del database SnapCenter per il disaster recovery

SnapCenter consente il backup e il ripristino del database MySQL sottostante e dei dati di configurazione allo scopo di ripristinare il server SnapCenter in caso di disastro. Per la nostra soluzione, abbiamo recuperato il database e la configurazione di SnapCenter su un'istanza di AWS EC2 che risiede nel nostro VPC. Per ulteriori informazioni su questo passaggio, vedere "questo link".

Prerequisiti per il backup di SnapCenter

Per il backup di SnapCenter sono necessari i seguenti prerequisiti:

- Un volume e una condivisione SMB creati sul sistema ONTAP on-premise per individuare i file di database e di configurazione di cui è stato eseguito il backup.
- Una relazione SnapMirror tra il sistema ONTAP on-premise e FSX o CVO nell'account AWS. Questa relazione viene utilizzata per trasportare lo snapshot contenente il database SnapCenter di cui è stato eseguito il backup e i file di configurazione.
- Windows Server installato nell'account cloud, su un'istanza EC2 o su una macchina virtuale nel VMware Cloud SDDC.
- SnapCenter installato sull'istanza di Windows EC2 o sulla macchina virtuale in VMware Cloud.

Riepilogo del processo di backup e ripristino di SnapCenter

- Creare un volume sul sistema ONTAP on-premise per ospitare i file di configurazione e di database di backup.
- Impostare una relazione SnapMirror tra on-premise e FSX/CVO.
- Montare la condivisione SMB.
- Recuperare il token di autorizzazione Swagger per eseguire le attività API.
- Avviare il processo di ripristino del db.
- Utilizzare l'utility xcopy per copiare la directory locale del file db e config nella condivisione SMB.
- Su FSX, creare un clone del volume ONTAP (copiato tramite SnapMirror da on-premise).
- Montare la condivisione SMB da FSX a EC2/VMware Cloud.
- Copiare la directory di ripristino dalla condivisione SMB in una directory locale.
- Eseguire il processo di ripristino di SQL Server da Swagger.

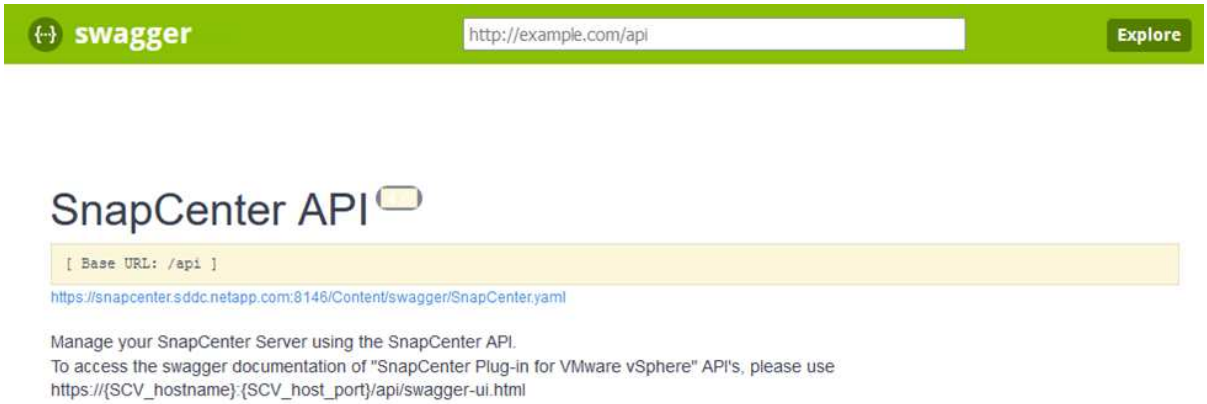
Eseguire il backup del database e della configurazione di SnapCenter

SnapCenter fornisce un'interfaccia client Web per l'esecuzione dei comandi API REST. Per informazioni sull'accesso alle API REST tramite Swagger, consultare la documentazione di SnapCenter all'indirizzo "questo link".

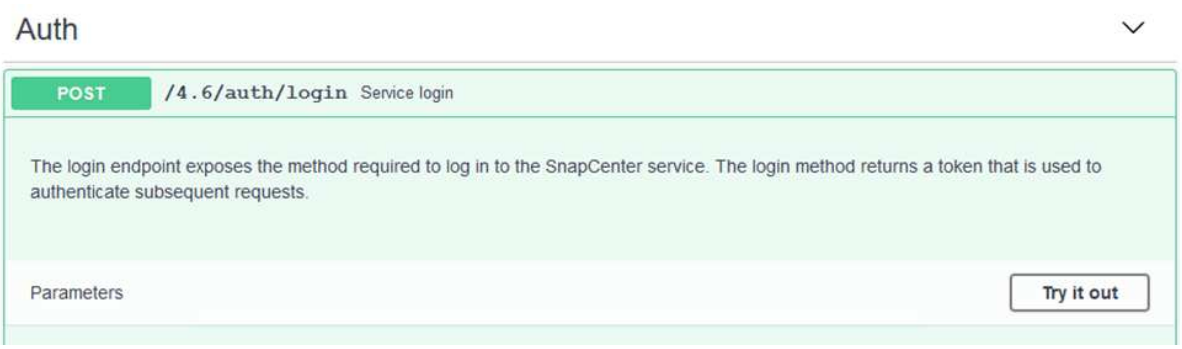
Accedere a Swagger e ottenere il token di autorizzazione

Una volta aperta la pagina Swagger, è necessario recuperare un token di autorizzazione per avviare il processo di ripristino del database.

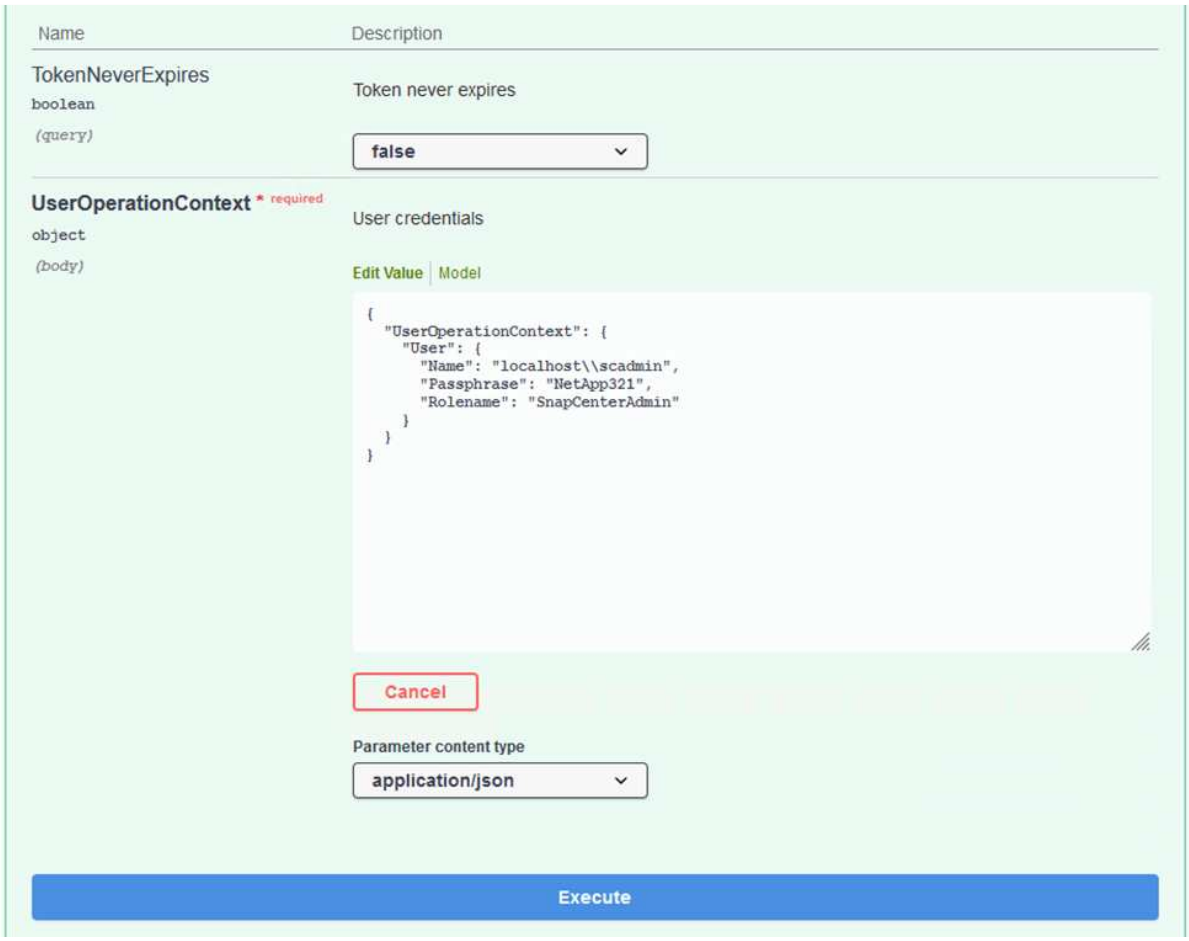
1. Accedere alla pagina Web dell'API di swagger SnapCenter all'indirizzo */https://<SnapCenter Server IP>:8146/swagger/*.



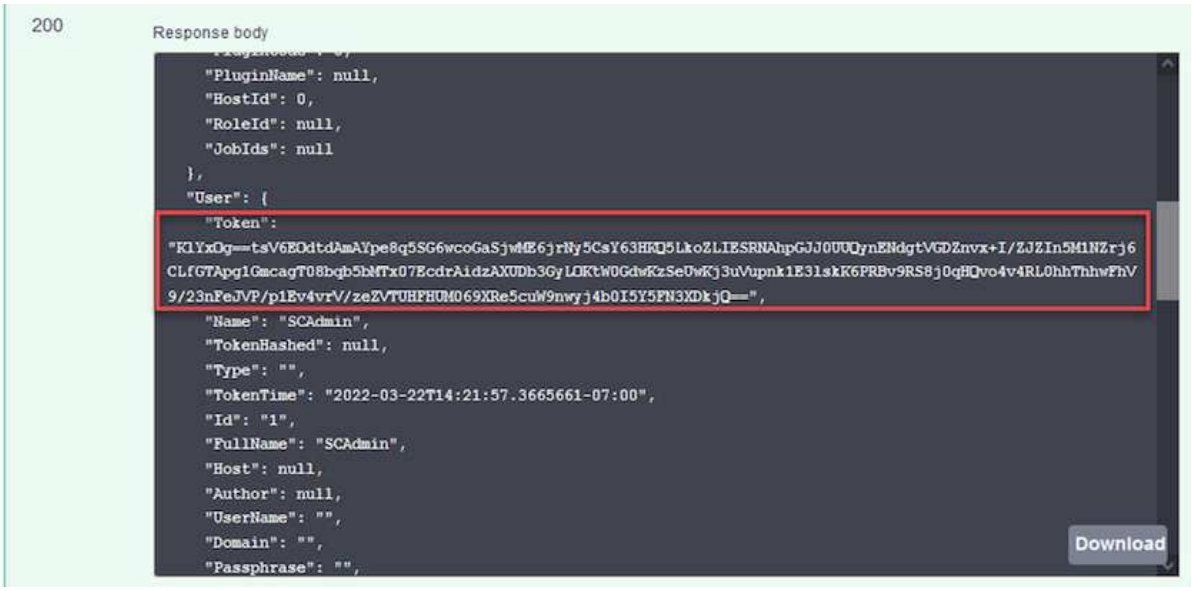
2. Espandere la sezione Auth e fare clic su Provalo.



3. Nell'area UserOperationContext, inserire le credenziali e il ruolo SnapCenter e fare clic su Esegui.



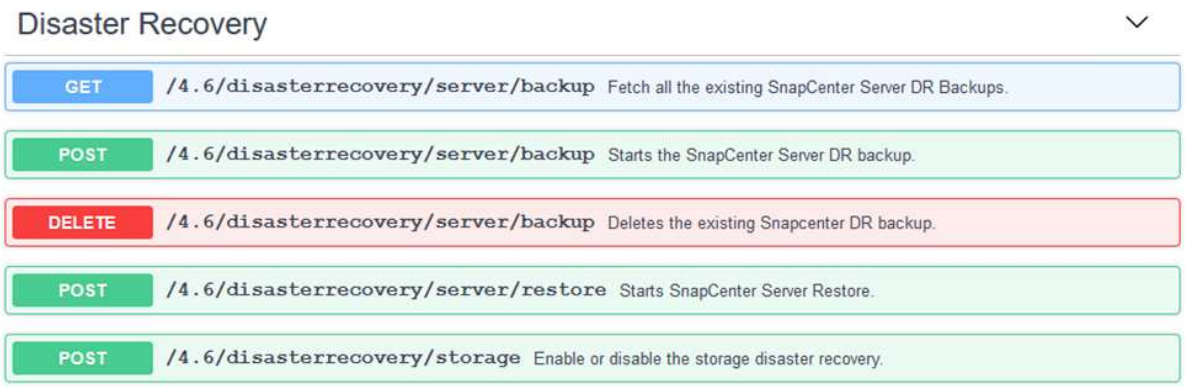
4. Nel corpo di risposta riportato di seguito, è possibile visualizzare il token. Copiare il testo del token per l'autenticazione durante l'esecuzione del processo di backup.



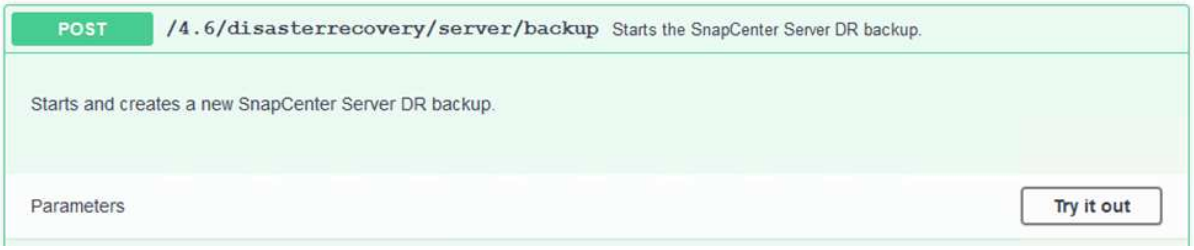
Eseguire un backup del database SnapCenter

Quindi, accedere all'area Disaster Recovery della pagina Swagger per avviare il processo di backup di SnapCenter.

1. Espandere l'area Disaster Recovery facendo clic su di essa.

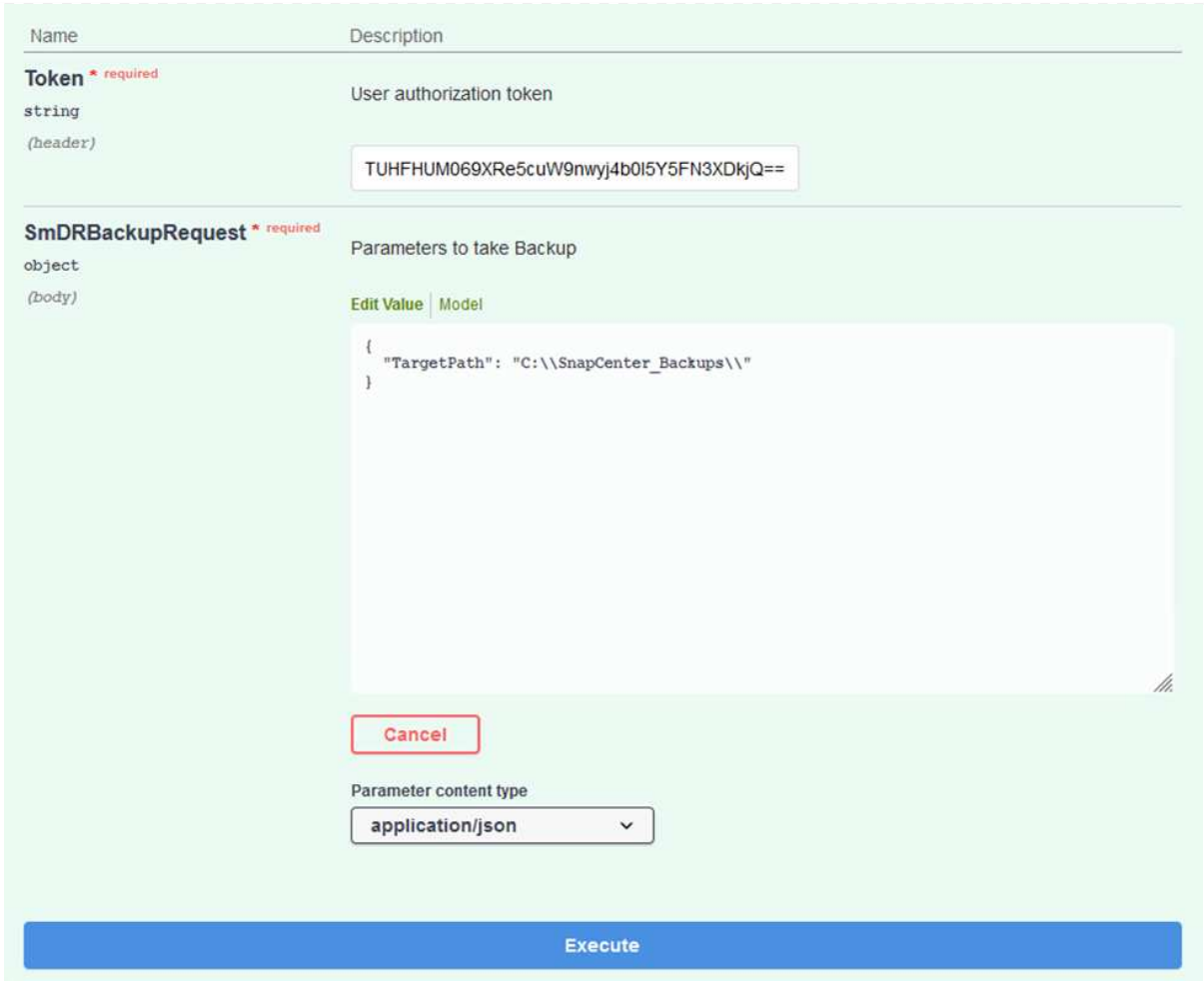


2. Espandere `/4.6/disasterrecovery/server/backup` E fare clic su Provalo.



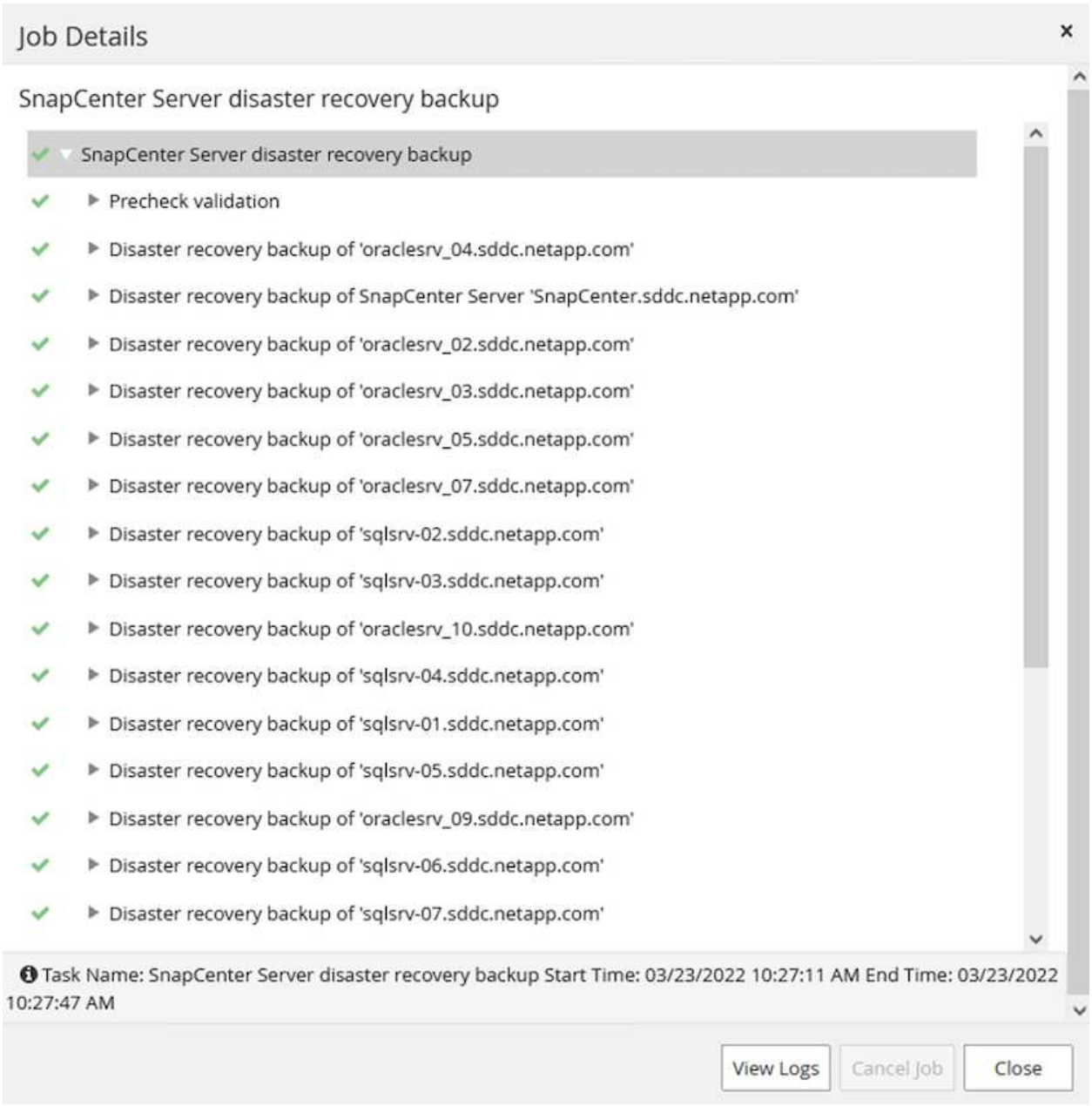
3. Nella sezione SmDRBackupRequest, aggiungere il percorso di destinazione locale corretto e selezionare Execute (Esegui) per avviare il backup del database e della configurazione di SnapCenter.

> Il processo di backup non consente il backup diretto su una condivisione file NFS o CIFS.


Name
Description
Token * required
string
(header)
User authorization token
TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ==
SmDRBackupRequest * required
object
(body)
Parameters to take Backup
Edit Value
Model
{
"TargetPath": "C:\\SnapCenter_Backups\\"
}
Cancel
Parameter content type
application/json
Execute

Monitorare il processo di backup da SnapCenter

Accedere a SnapCenter per esaminare i file di registro quando si avvia il processo di ripristino del database. Nella sezione Monitor, è possibile visualizzare i dettagli del backup di disaster recovery del server SnapCenter.



Utilizzare l'utility XCOPY per copiare il file di backup del database nella condivisione SMB

Quindi, spostare il backup dal disco locale sul server SnapCenter alla condivisione CIFS utilizzata per copiare i dati nella posizione secondaria situata sull'istanza FSX in AWS. Utilizzare xcopy con opzioni specifiche che conservano i permessi dei file.

Aprire un prompt dei comandi come Amministratore. Dal prompt dei comandi, immettere i seguenti comandi:

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X
/E /H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O
/X /E /H /K
```

Failover

Il disastro si verifica nel sito primario

In caso di disastro che si verifica nel data center primario on-premise, il nostro scenario include il failover su un sito secondario che risiede nell'infrastruttura Amazon Web Services utilizzando VMware Cloud su AWS. Supponiamo che le macchine virtuali e il nostro cluster ONTAP on-premise non siano più accessibili. Inoltre, le macchine virtuali SnapCenter e Veeam non sono più accessibili e devono essere ricostruite nel nostro sito secondario.

In questa sezione viene descritto il failover della nostra infrastruttura nel cloud e vengono trattati i seguenti argomenti:

- Ripristino del database SnapCenter. Una volta stabilito un nuovo server SnapCenter, ripristinare il database MySQL e i file di configurazione e attivare la modalità di disaster recovery per consentire allo storage FSX secondario di diventare il dispositivo di storage primario.
- Ripristinare le macchine virtuali dell'applicazione utilizzando Veeam Backup & Replication. Collegare lo storage S3 che contiene i backup delle macchine virtuali, importare i backup e ripristinarli su VMware Cloud su AWS.
- Ripristinare i dati dell'applicazione SQL Server utilizzando SnapCenter.
- Ripristinare i dati dell'applicazione Oracle utilizzando SnapCenter.

Processo di ripristino del database SnapCenter

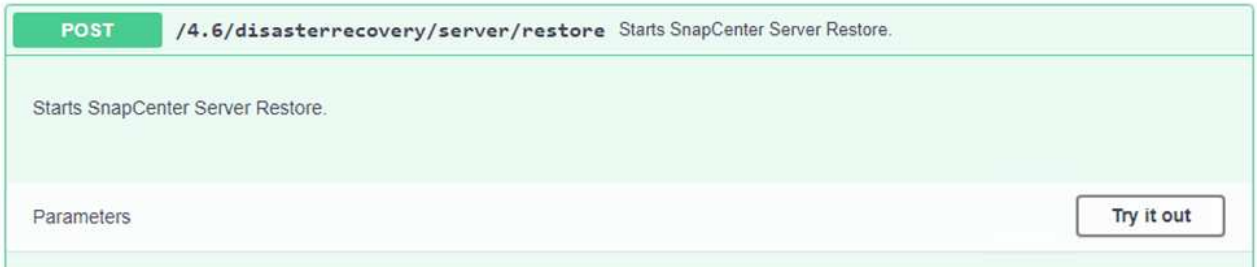
SnapCenter supporta scenari di disaster recovery consentendo il backup e il ripristino del database MySQL e dei file di configurazione. Ciò consente a un amministratore di mantenere backup regolari del database SnapCenter nel data center on-premise e di ripristinare successivamente tale database in un database SnapCenter secondario.

Per accedere ai file di backup di SnapCenter sul server SnapCenter remoto, attenersi alla seguente procedura:

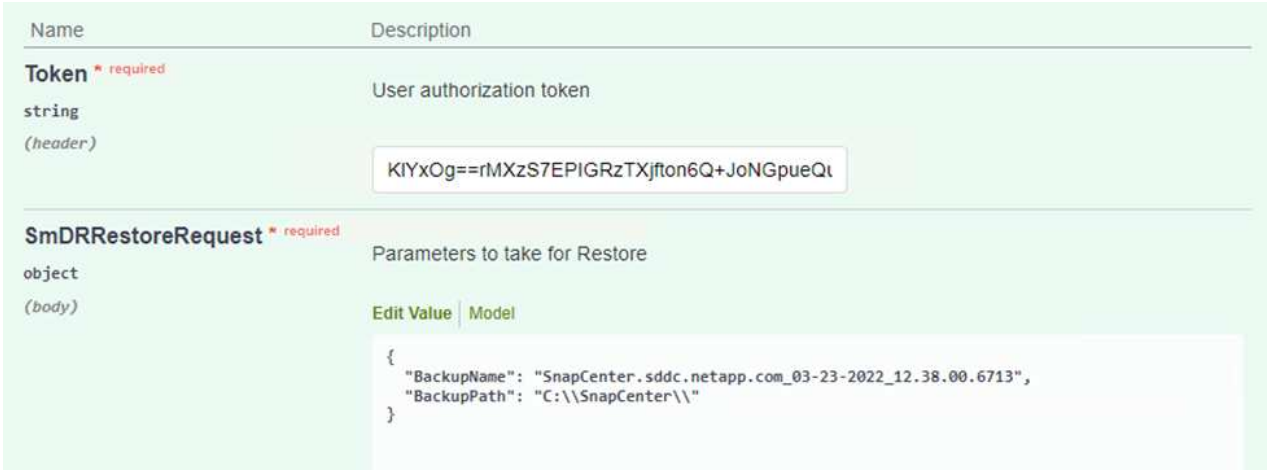
1. Interrompere la relazione di SnapMirror dal cluster FSX, che rende il volume in lettura/scrittura.
2. Creare un server CIFS (se necessario) e una condivisione CIFS che punta al percorso di giunzione del volume clonato.
3. Utilizzare xcopy per copiare i file di backup in una directory locale sul sistema SnapCenter secondario.
4. Installare SnapCenter v4.6.
5. Assicurarsi che il server SnapCenter abbia lo stesso nome FQDN del server originale. Questo è necessario per il ripristino del db.

Per avviare il processo di ripristino, attenersi alla seguente procedura:

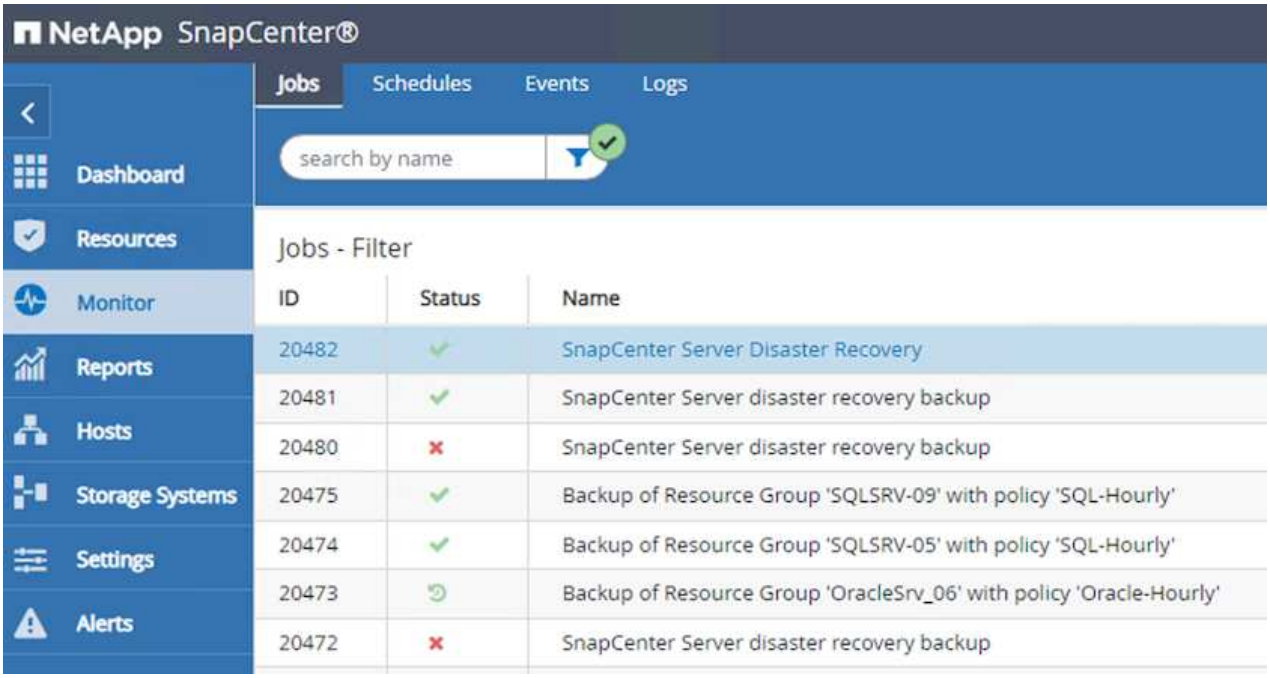
1. Accedere alla pagina Web API Swagger per il server SnapCenter secondario e seguire le istruzioni precedenti per ottenere un token di autorizzazione.
2. Accedere alla sezione Disaster Recovery della pagina Swagger e selezionare `/4.6/disasterrecovery/server/restore`E fare clic su Provalo.

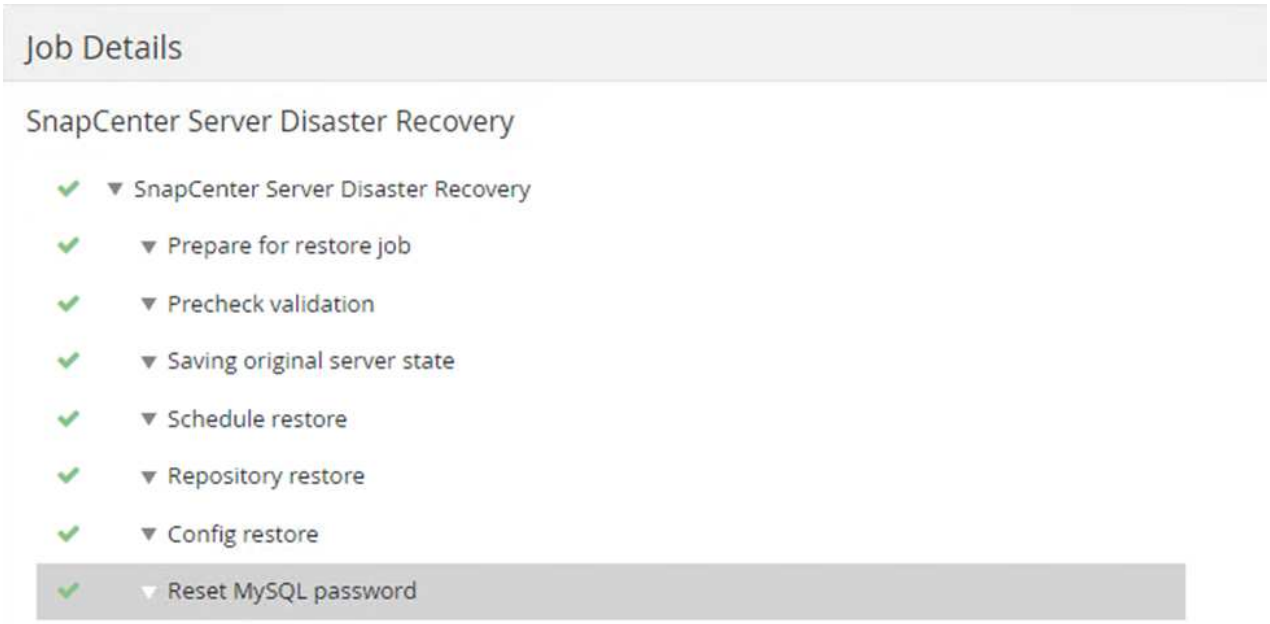


3. Incollare il token di autorizzazione e, nella sezione SmDRResterRequest, incollare il nome del backup e la directory locale sul server SnapCenter secondario.



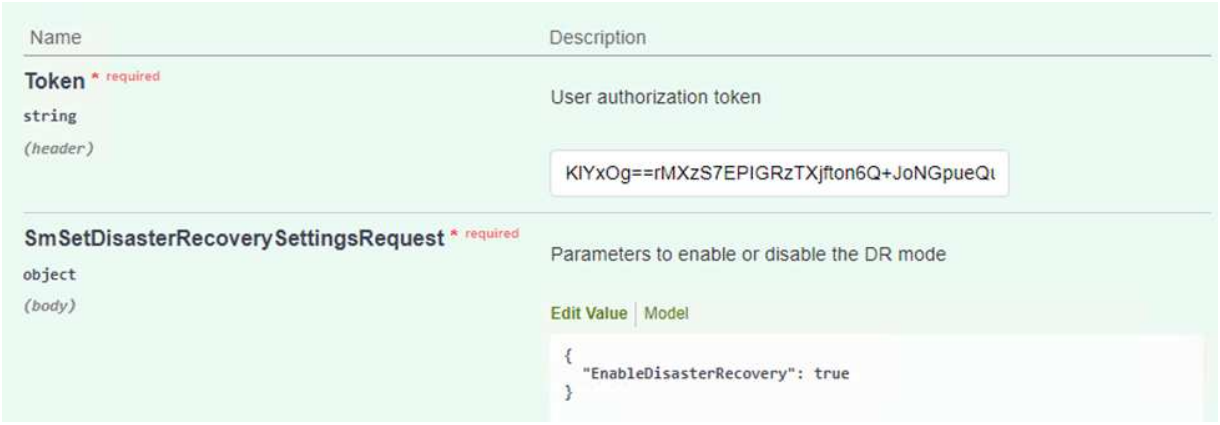
4. Selezionare il pulsante Execute (Esegui) per avviare il processo di ripristino.
5. Da SnapCenter, accedere alla sezione Monitor per visualizzare l'avanzamento del processo di ripristino.





6. Per abilitare i ripristini di SQL Server dallo storage secondario, è necessario attivare la modalità di disaster recovery nel database SnapCenter. Questa operazione viene eseguita come operazione separata e avviata sulla pagina Web API di Swagger.
   a. Accedere alla sezione Disaster Recovery e fare clic su `/4.6/disasterrecovery/storage`.
   b. Incollare il token di autorizzazione dell'utente.
   c. Nella sezione SmSetDisasterRecoverySettingsRequest, modificare `EnableDisasterRecover` a. `true`.

d. Fare clic su Execute (Esegui) per attivare la modalità di disaster recovery per SQL Server.



Vedere i commenti relativi alle procedure aggiuntive.

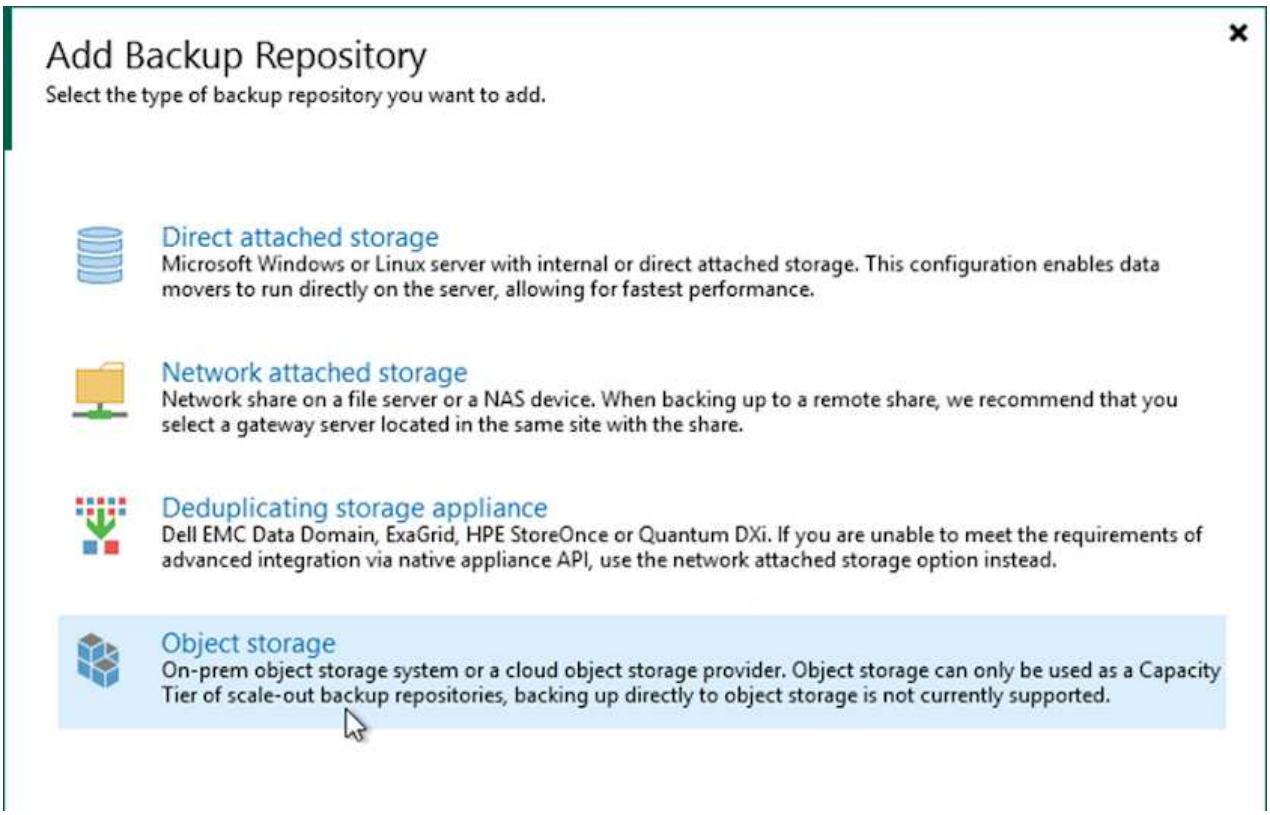
Ripristinare le macchine virtuali applicative con il ripristino completo di Veeam

Creare un repository di backup e importare i backup da S3

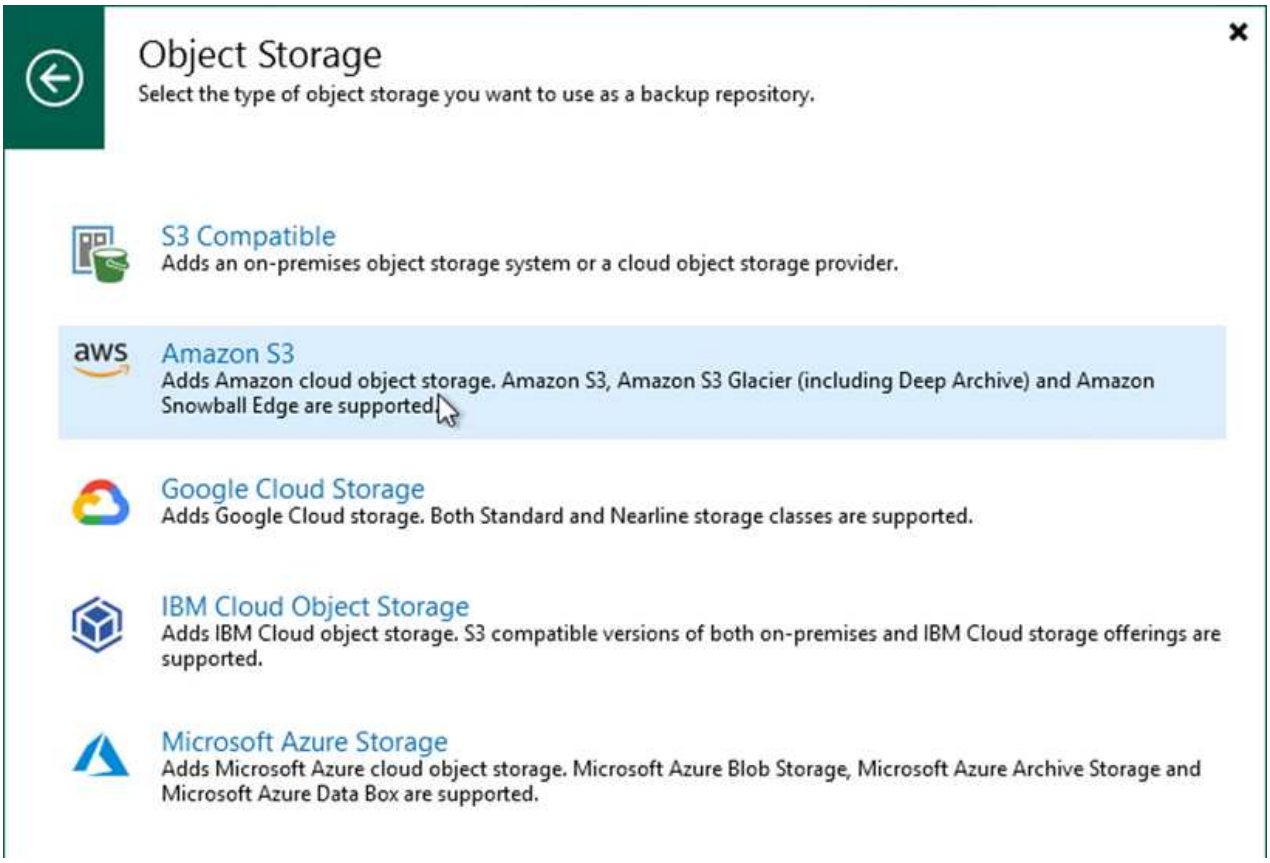
Dal server Veeam secondario, importare i backup dallo storage S3 e ripristinare le macchine virtuali SQL Server e Oracle nel cluster VMware Cloud.

Per importare i backup dall'oggetto S3 che faceva parte del repository di backup scale-out on-premise, attenersi alla seguente procedura:

1. Accedere a Backup Repository e fare clic su Add Repository (Aggiungi repository) nel menu in alto per avviare la procedura guidata Add Backup Repository (Aggiungi repository di backup). Nella prima pagina della procedura guidata, selezionare Object Storage come tipo di repository di backup.

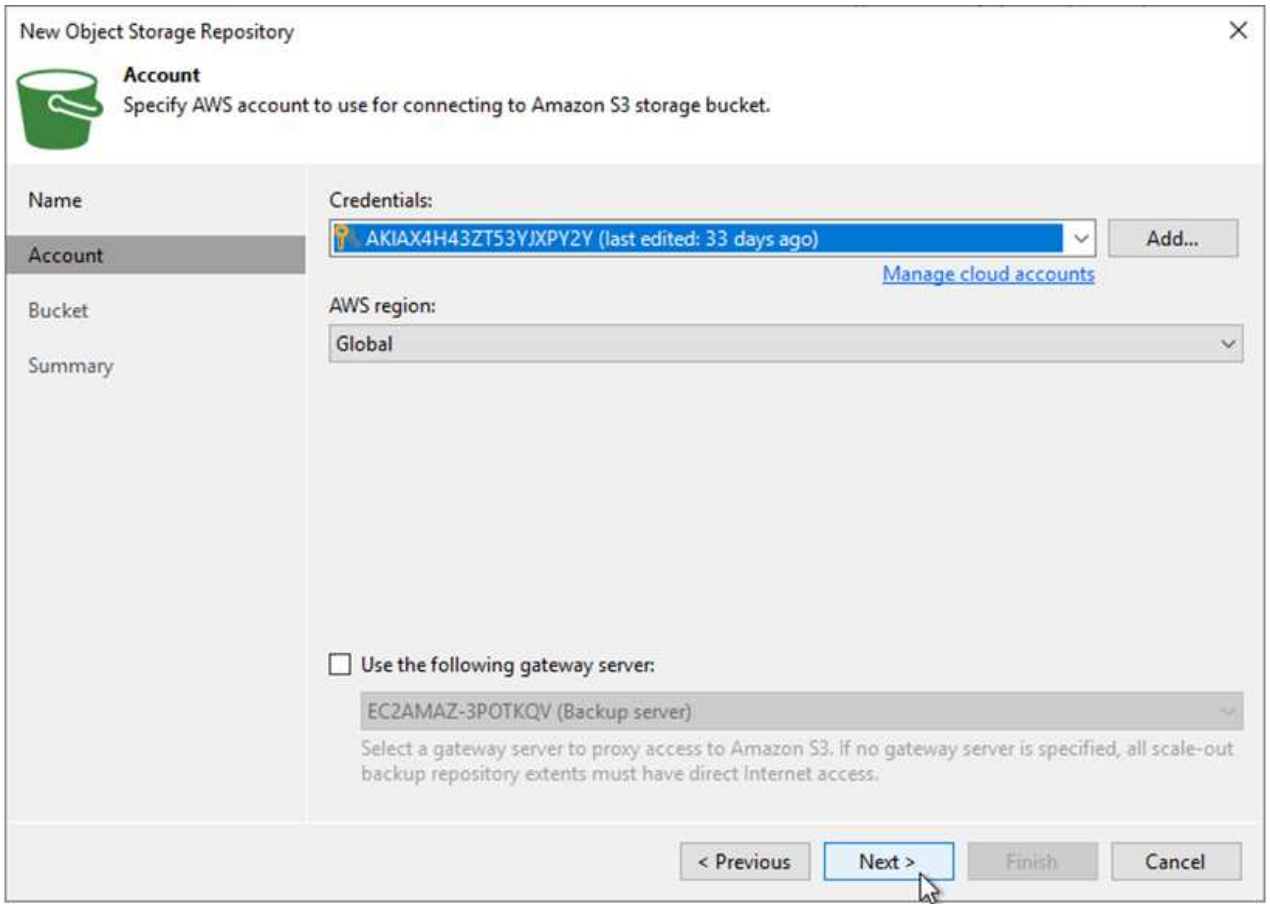


2. Selezionare Amazon S3 come tipo di storage a oggetti.

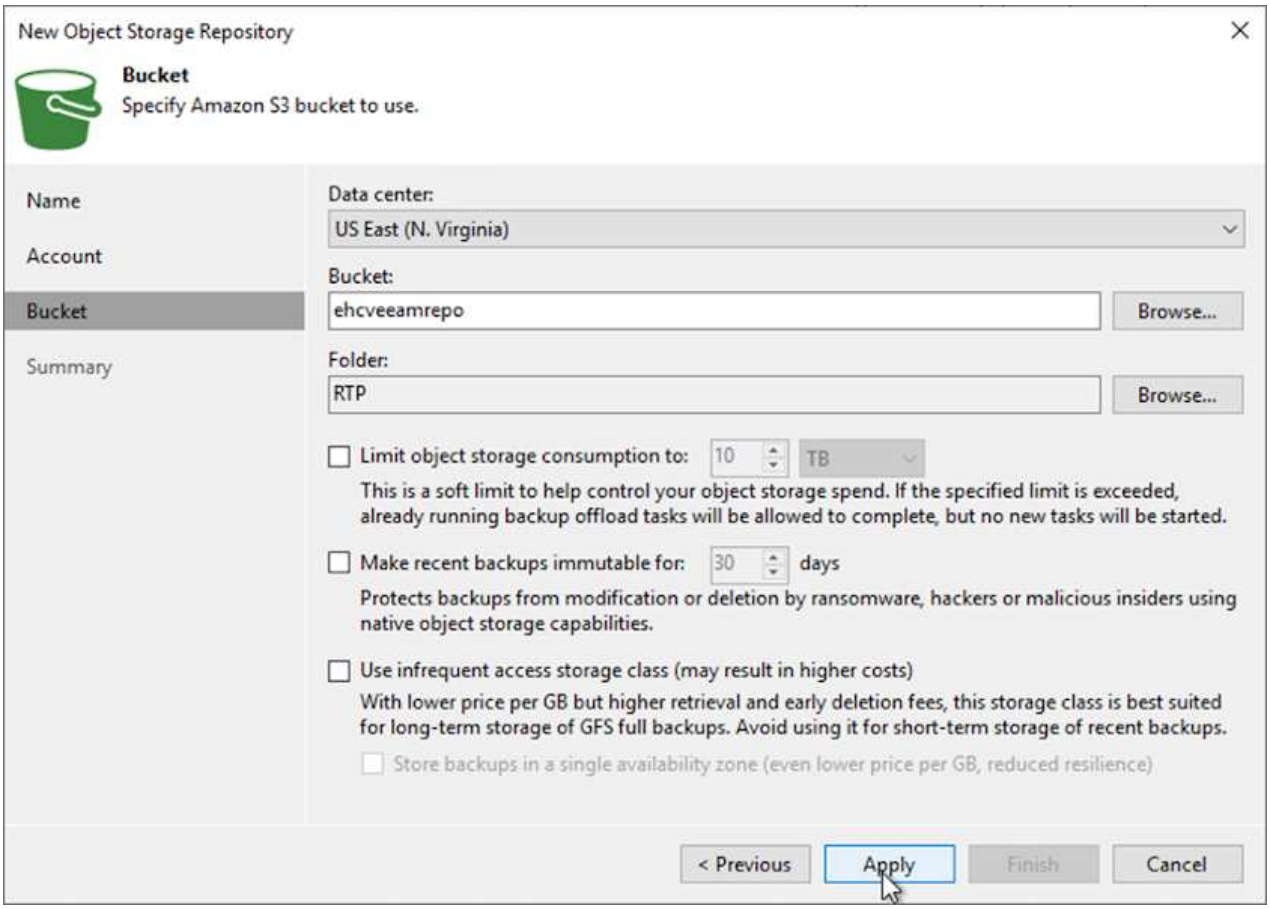


3. Dall'elenco di Amazon Cloud Storage Services, selezionare Amazon S3.

4. Selezionare le credenziali preinserite dall'elenco a discesa o aggiungere una nuova credenziale per accedere alla risorsa di storage cloud. Fare clic su Next (Avanti) per continuare.



5. Nella pagina bucket, inserire il data center, il bucket, la cartella e le opzioni desiderate. Fare clic su Applica.

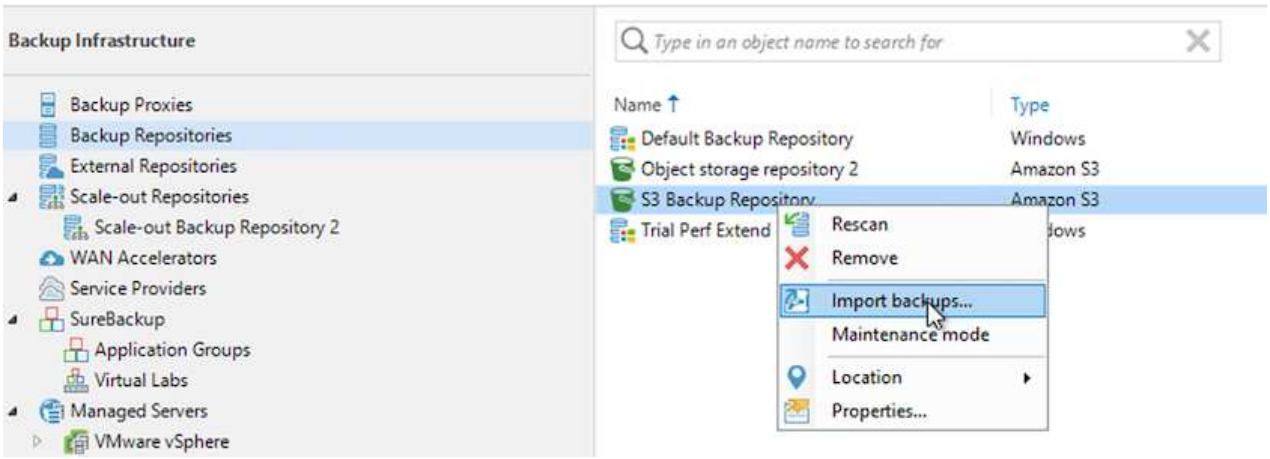


6. Infine, selezionare fine per completare il processo e aggiungere il repository.

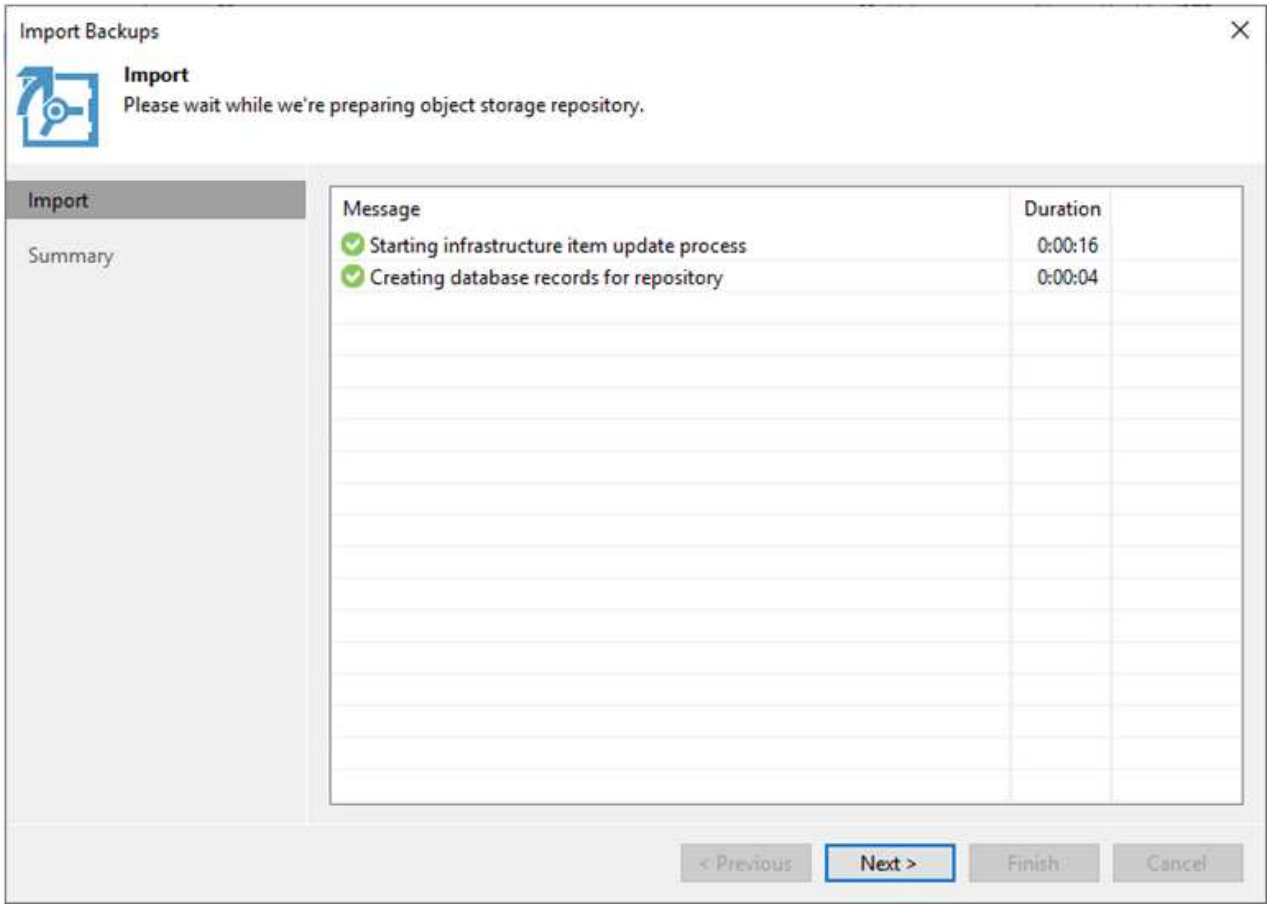
Importare backup dallo storage a oggetti S3

Per importare i backup dal repository S3 aggiunto nella sezione precedente, attenersi alla seguente procedura.

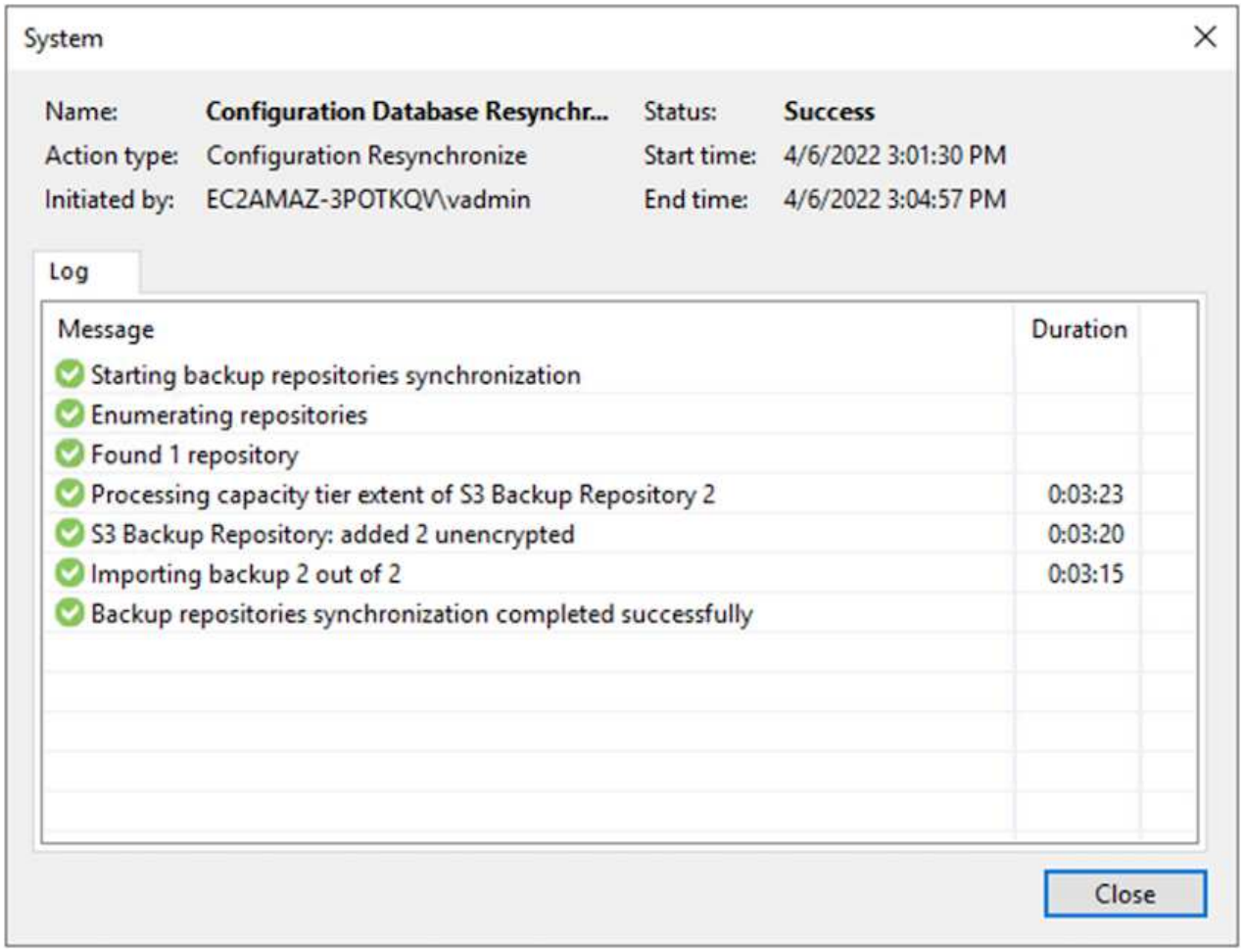
1. Dal repository di backup S3, selezionare Importa backup per avviare la procedura guidata di importazione dei backup.



2. Dopo aver creato i record del database per l'importazione, selezionare Avanti, quindi fine nella schermata di riepilogo per avviare il processo di importazione.



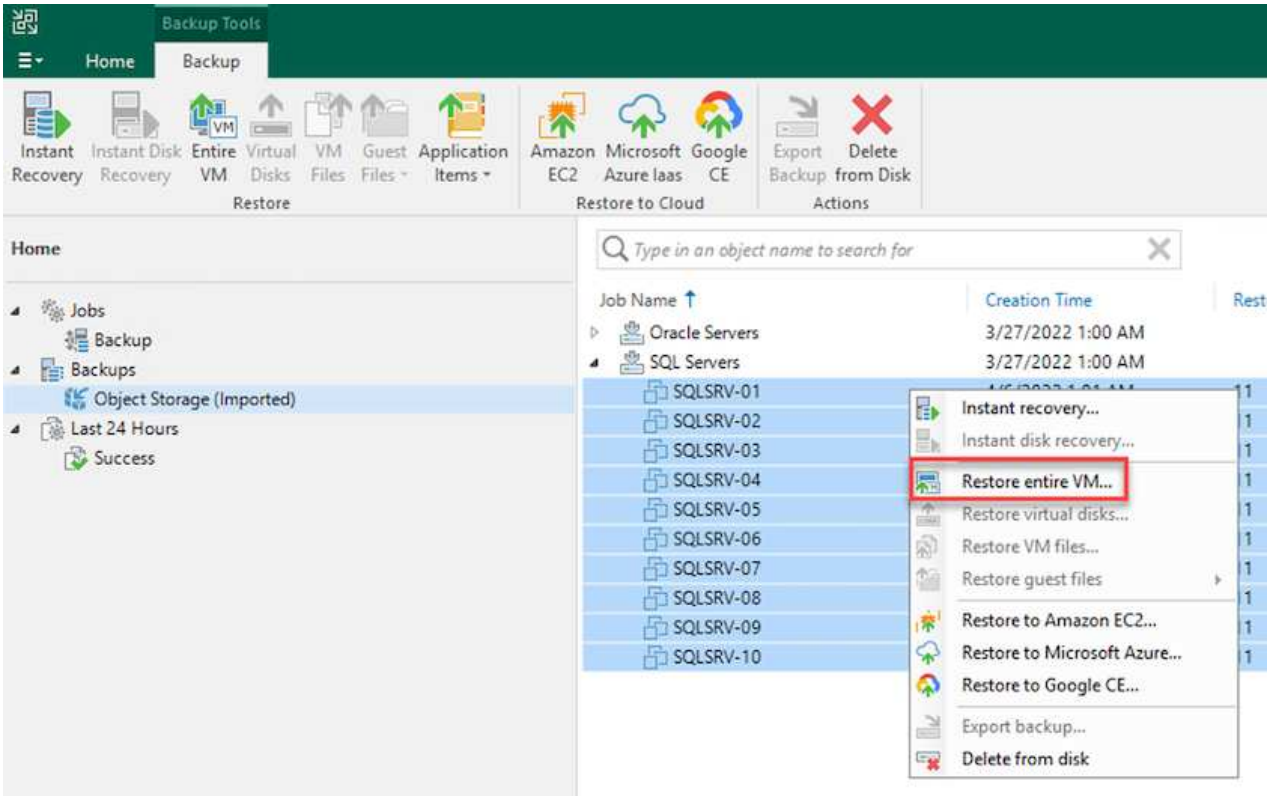
3. Una volta completata l'importazione, è possibile ripristinare le macchine virtuali nel cluster VMware Cloud.


System
Name: Configuration Database Resynchr...
Status: Success
Action type: Configuration Resynchronize
Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vadmin
End time: 4/6/2022 3:04:57 PM
Log
Message
Duration
Starting backup repositories synchronization
Enumerating repositories
Found 1 repository
Processing capacity tier extent of S3 Backup Repository 2
0:03:23
S3 Backup Repository: added 2 unencrypted
0:03:20
Importing backup 2 out of 2
0:03:15
Backup repositories synchronization completed successfully
Close

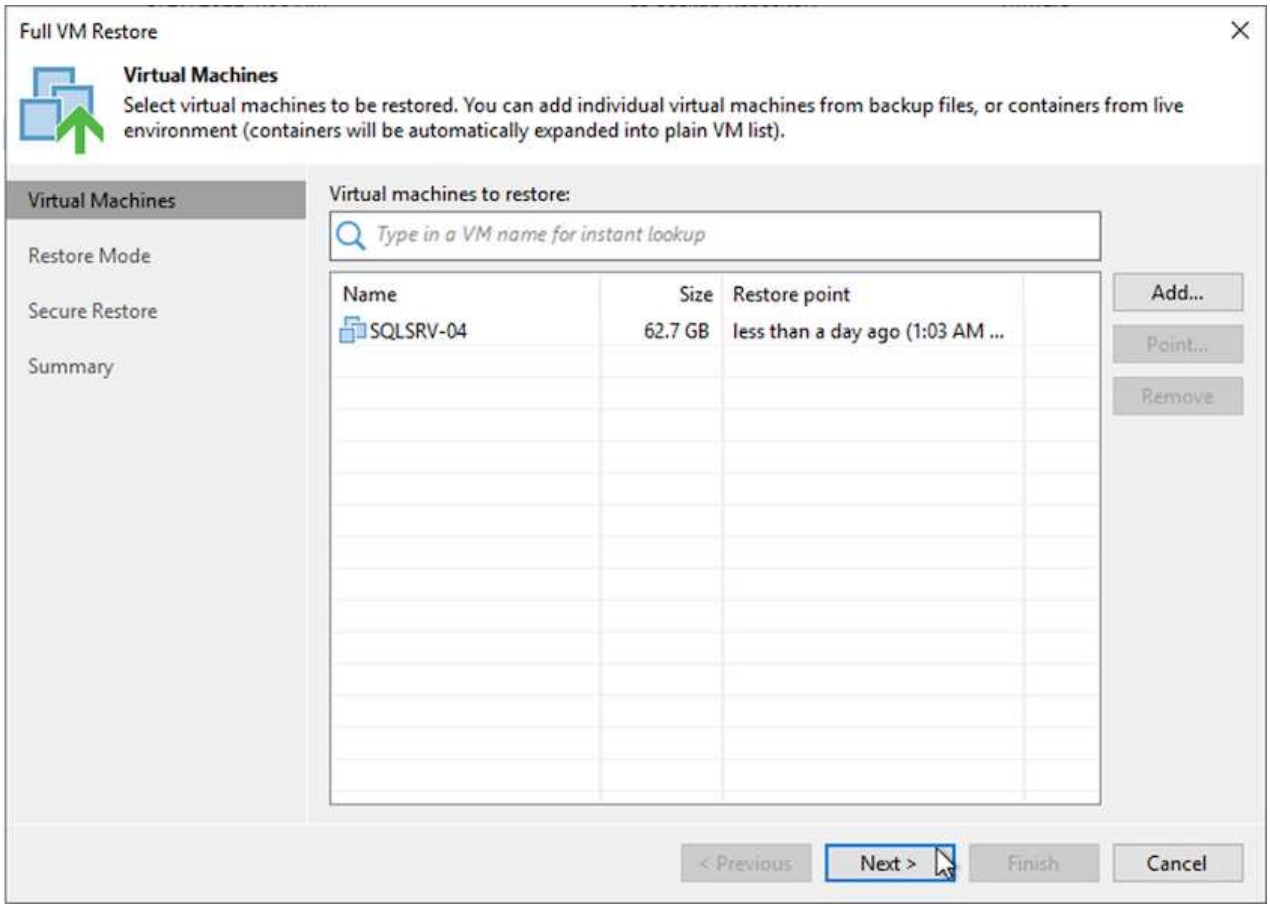
Ripristinare le macchine virtuali applicative con il ripristino completo di Veeam su VMware Cloud

Per ripristinare le macchine virtuali SQL e Oracle su VMware Cloud su cluster/dominio del carico di lavoro AWS, completare la seguente procedura.

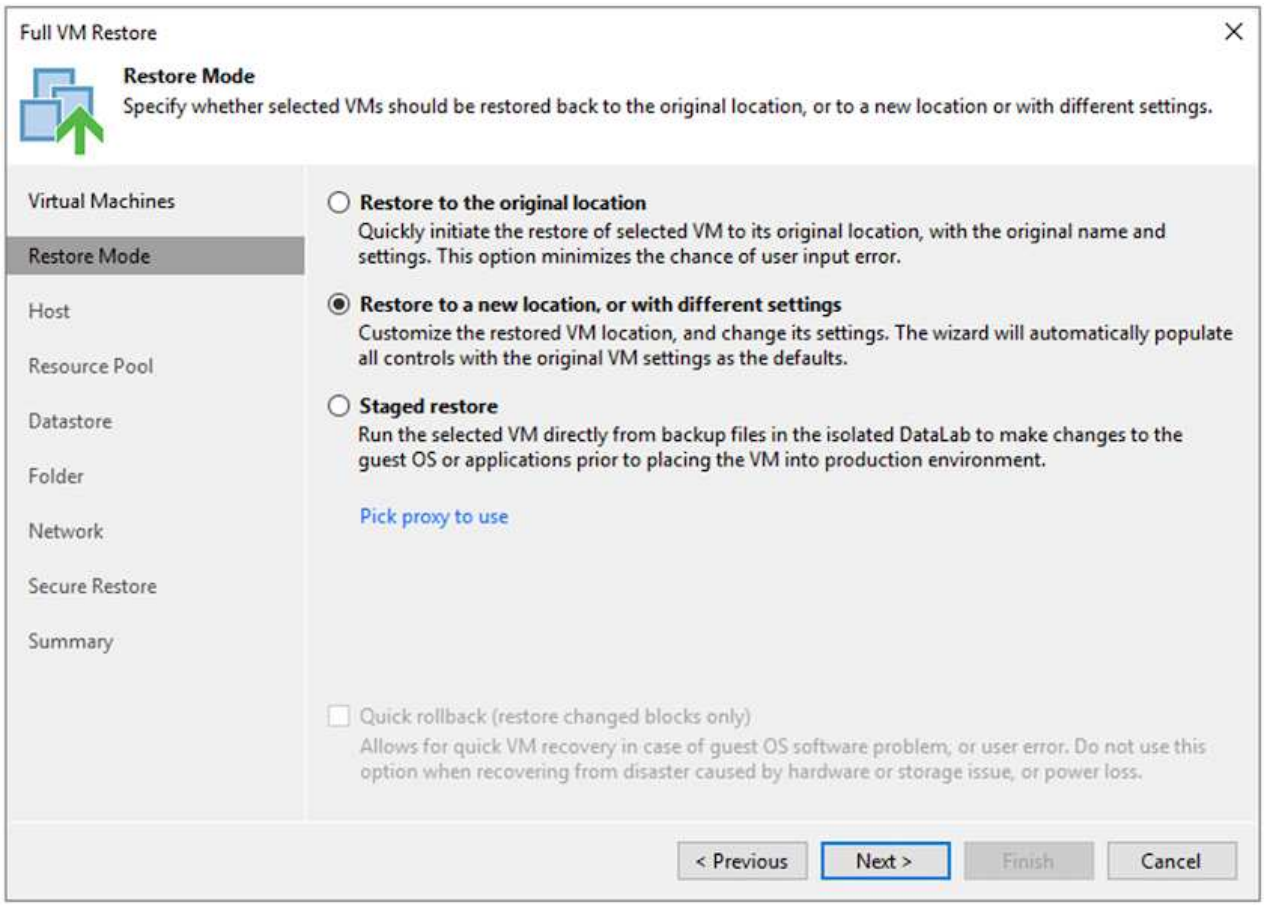
1. Dalla home page di Veeam, selezionare lo storage a oggetti contenente i backup importati, selezionare le macchine virtuali da ripristinare, quindi fare clic con il pulsante destro del mouse e selezionare Restore entire VM (Ripristina intera macchina virtuale).



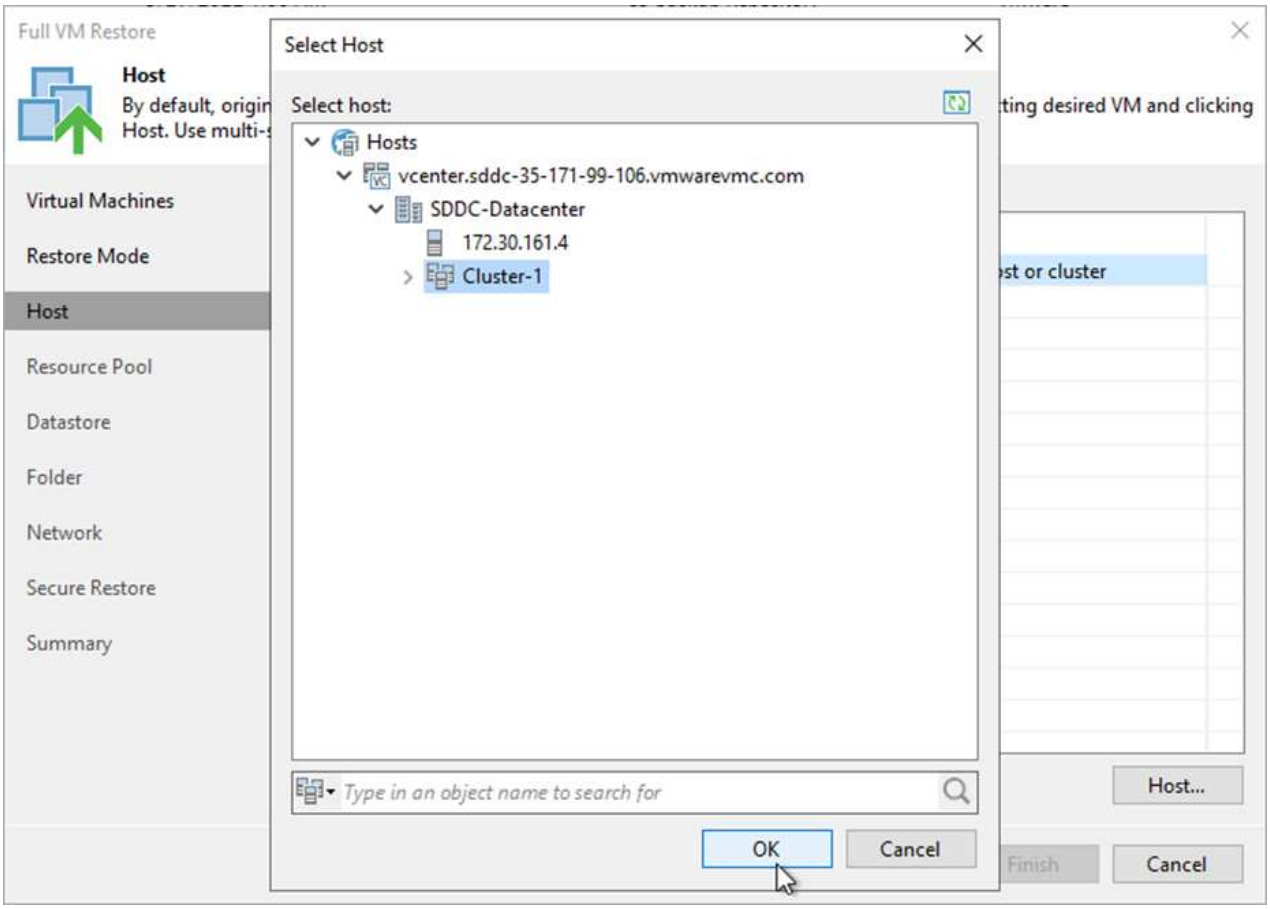
2. Nella prima pagina della procedura guidata di ripristino completo della macchina virtuale, modificare le macchine virtuali per il backup, se necessario, e selezionare Avanti.



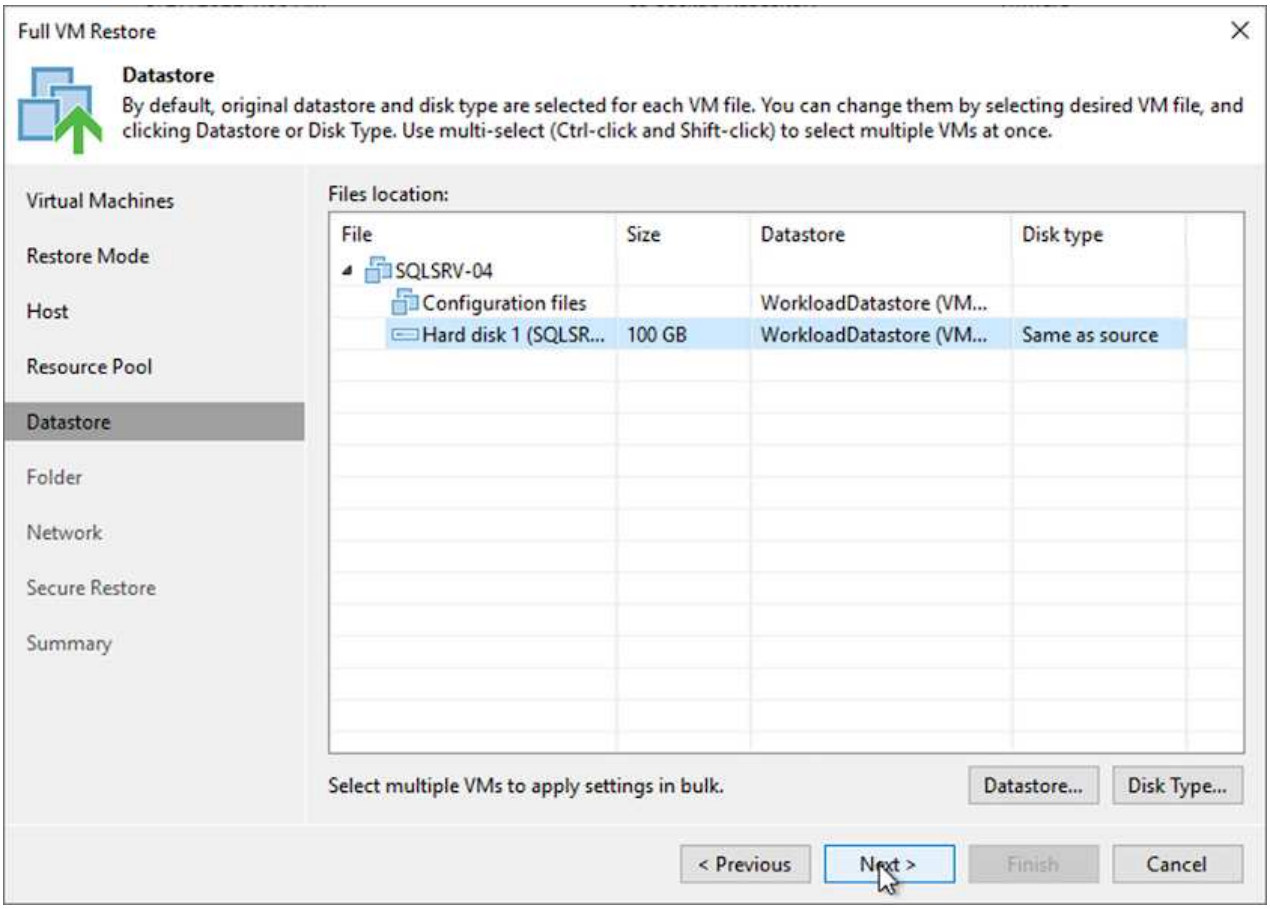
3. Nella pagina Restore Mode (modalità ripristino), selezionare Restore to a New Location (Ripristina in una nuova posizione) o with different Settings (con impostazioni diverse).



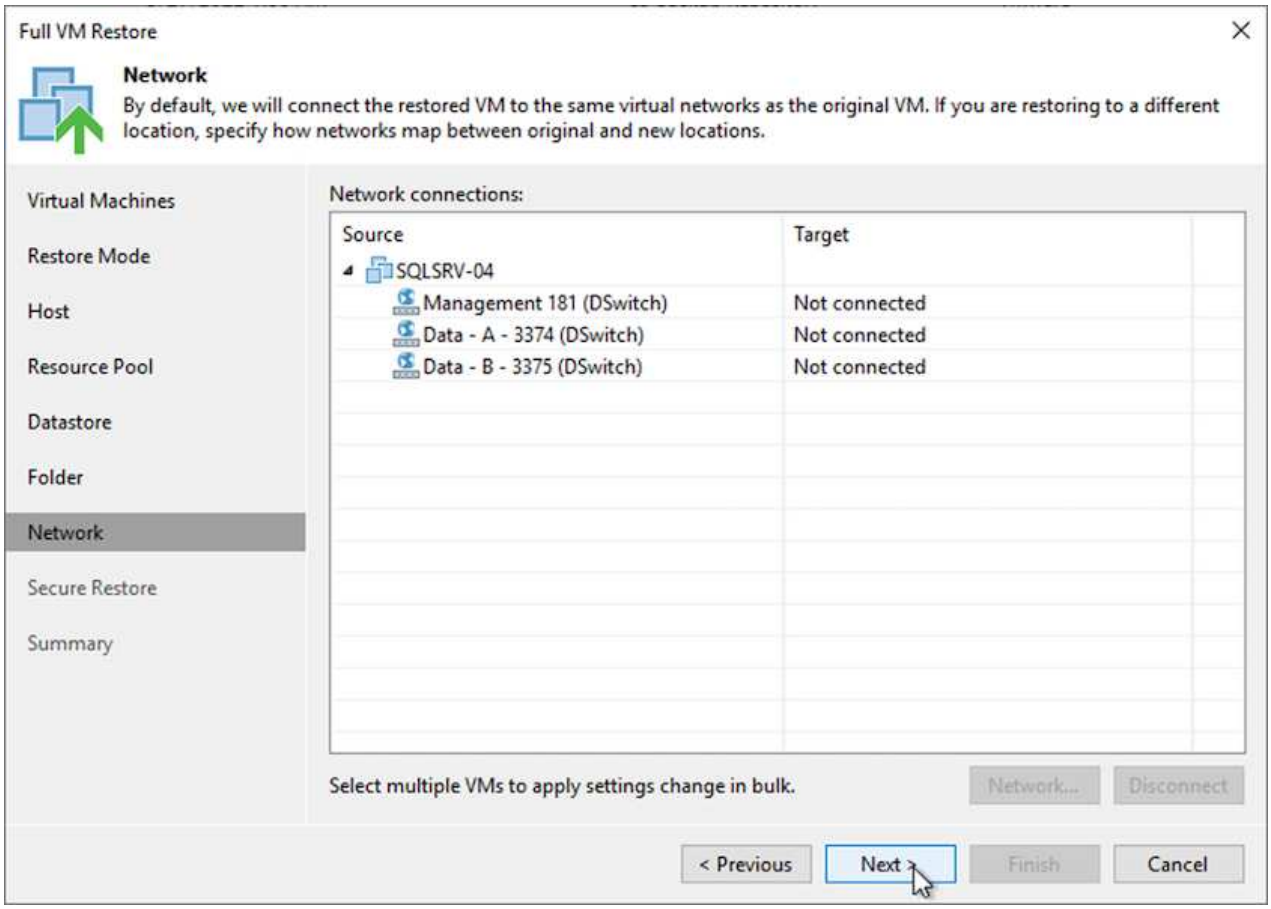
4. Nella pagina host, selezionare l'host o il cluster ESXi di destinazione su cui ripristinare la macchina virtuale.

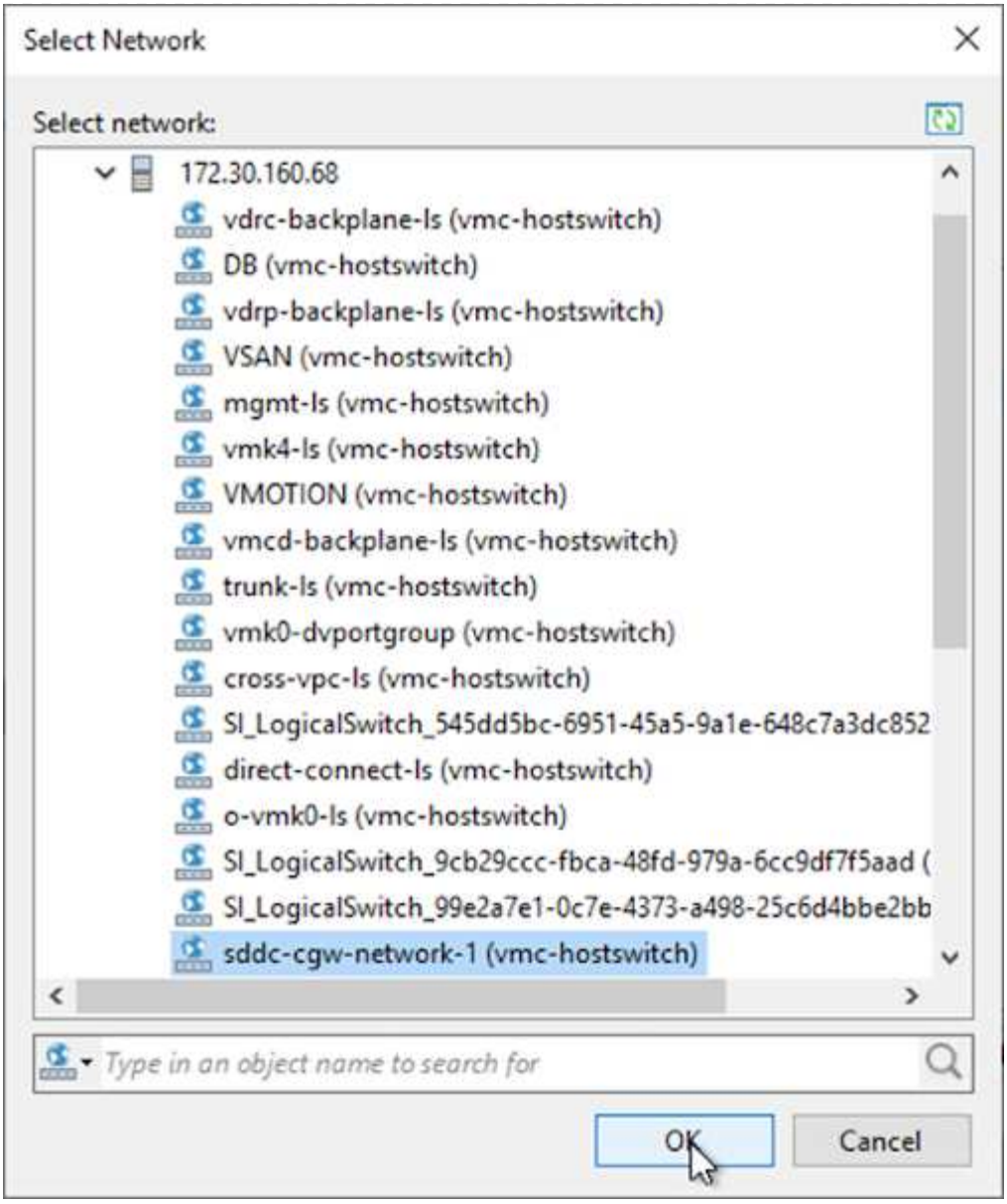


5. Nella pagina datastore, selezionare la posizione del datastore di destinazione per i file di configurazione e il disco rigido.



6. Nella pagina Network (rete), mappare le reti originali sulla macchina virtuale alle reti nella nuova posizione di destinazione.


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. Selezionare se eseguire la scansione della macchina virtuale ripristinata alla ricerca di malware, esaminare la pagina di riepilogo e fare clic su Finish (fine) per avviare il ripristino.

Ripristinare i dati dell'applicazione SQL Server

Il seguente processo fornisce istruzioni su come ripristinare un SQL Server in VMware Cloud Services in AWS in caso di disastro che rende il sito on-premise inutilizzabile.

Si presuppone che i seguenti prerequisiti siano completi per continuare con le fasi di ripristino:

1. La macchina virtuale Windows Server è stata ripristinata nel VMware Cloud SDDC utilizzando il ripristino completo di Veeam.
2. È stato stabilito un server SnapCenter secondario e il ripristino e la configurazione del database SnapCenter sono stati completati seguendo la procedura illustrata nella sezione "Riepilogo del processo di backup e ripristino di SnapCenter."

VM: Configurazione post-ripristino per SQL Server VM

Una volta completato il ripristino della macchina virtuale, è necessario configurare la rete e altri elementi in preparazione per il rispristino della macchina virtuale host in SnapCenter.

1. Assegnare nuovi indirizzi IP per Management e iSCSI o NFS.
2. Unire l'host al dominio Windows.
3. Aggiungere i nomi host al DNS o al file hosts sul server SnapCenter.

> Se il plug-in SnapCenter è stato distribuito utilizzando credenziali di dominio diverse da quelle del dominio corrente, è necessario modificare l'account di accesso per il plug-in per il servizio Windows sulla macchina virtuale di SQL Server. Dopo aver modificato l'account di accesso, riavviare i servizi SMCore, Plug-in per Windows e Plug-in per SnapCenter Server.

> Per riscoprire automaticamente le macchine virtuali ripristinate in SnapCenter, l'FQDN deve essere identico alla macchina virtuale originariamente aggiunta a SnapCenter on-premise.

Configurare lo storage FSX per il ripristino di SQL Server

Per eseguire il processo di ripristino del disaster recovery per una macchina virtuale SQL Server, è necessario interrompere la relazione SnapMirror esistente dal cluster FSX e concedere l'accesso al volume. A tale scopo, attenersi alla seguente procedura.

1. Per interrompere la relazione SnapMirror esistente per il database SQL Server e i volumi di log, eseguire il seguente comando dalla CLI FSX:

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

2. Concedere l'accesso al LUN creando un gruppo di iniziatori contenente l'IQN iSCSI della macchina virtuale Windows di SQL Server:

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

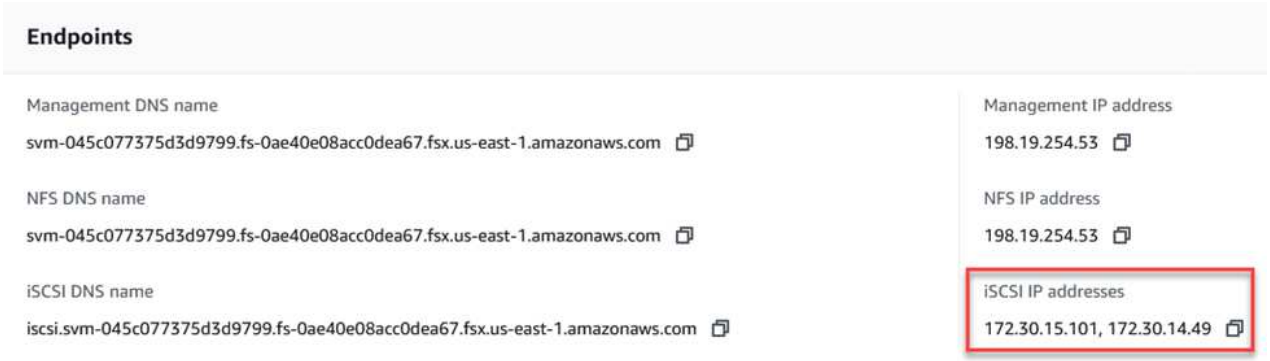
3. Infine, mappare le LUN al gruppo iniziatore appena creato:

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

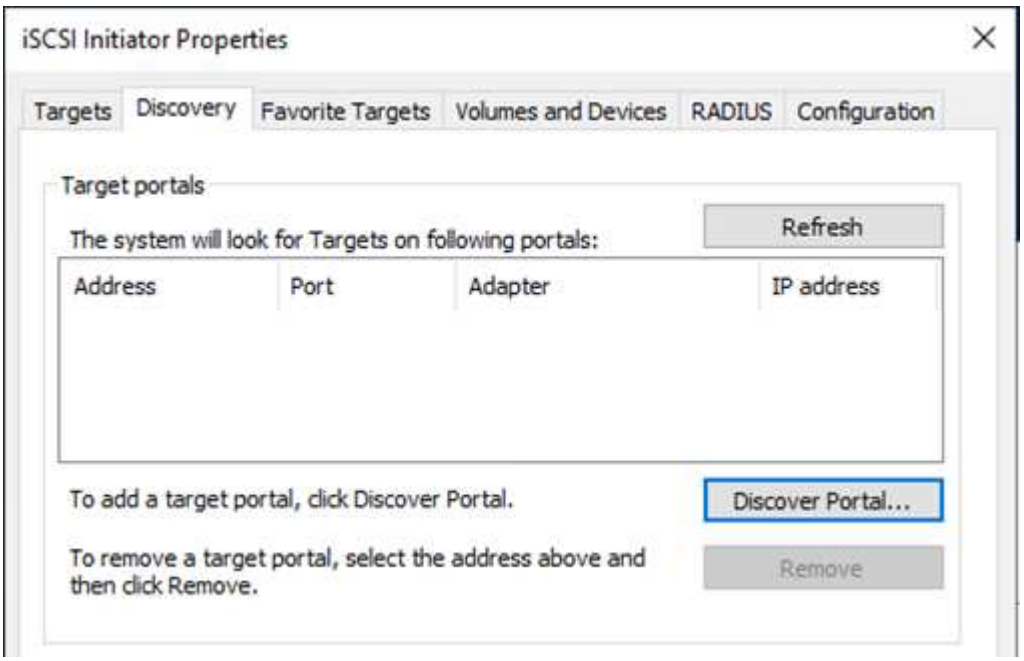
4. Per trovare il nome del percorso, eseguire `lun show` comando.

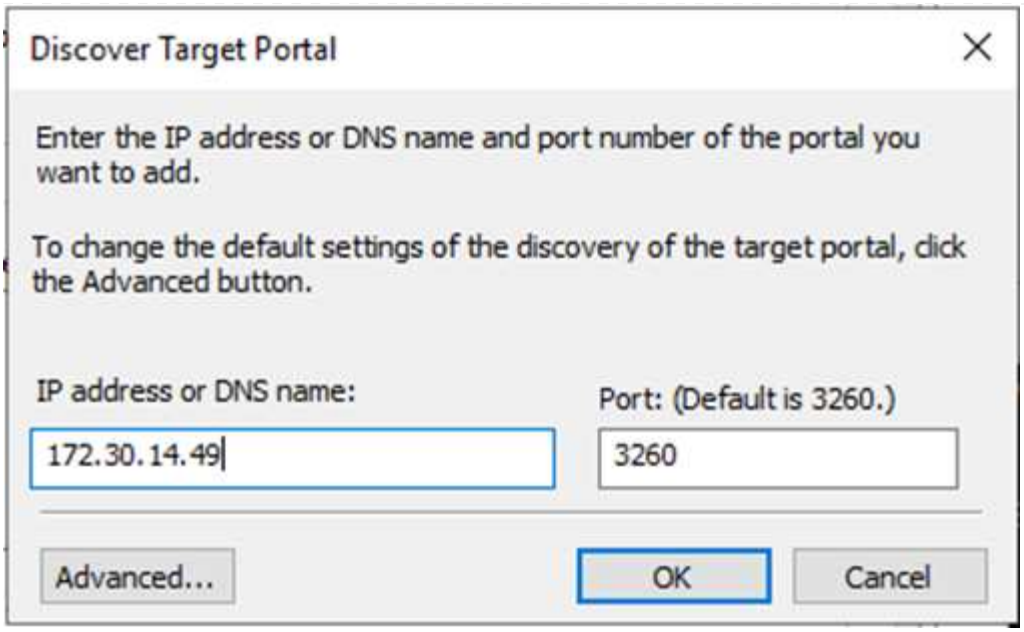
Configurare la macchina virtuale Windows per l'accesso iSCSI e rilevare i file system

1. Da SQL Server VM, configurare l'adattatore di rete iSCSI per comunicare sul gruppo di porte VMware stabilito con la connettività alle interfacce di destinazione iSCSI sull'istanza FSX.
2. Aprire l'utility iSCSI Initiator Properties (Proprietà iSCSI Initiator) e cancellare le vecchie impostazioni di connettività nelle schede Discovery (rilevamento), Favorite Targets (destinazioni preferite) e Targets (destinazioni).
3. Individuare gli indirizzi IP per l'accesso all'interfaccia logica iSCSI sull'istanza/cluster FSX. Questa opzione si trova nella console AWS in Amazon FSX > ONTAP > Storage Virtual Machines (Impostazioni > macchine virtuali di storage).

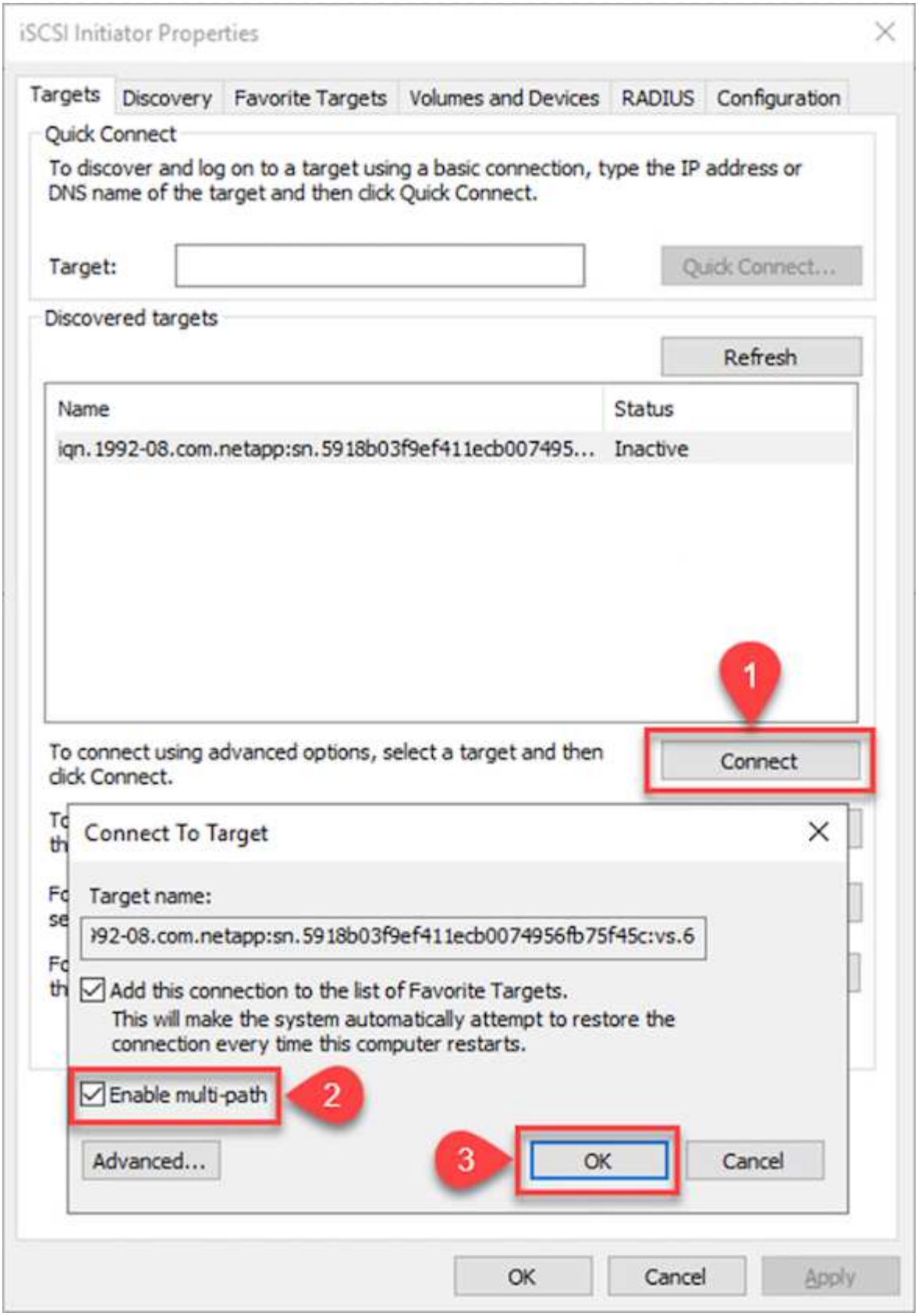


4. Dalla scheda Discovery (rilevamento), fare clic su Discover Portal (Scopri portale) e inserire gli indirizzi IP per le destinazioni iSCSI FSX.

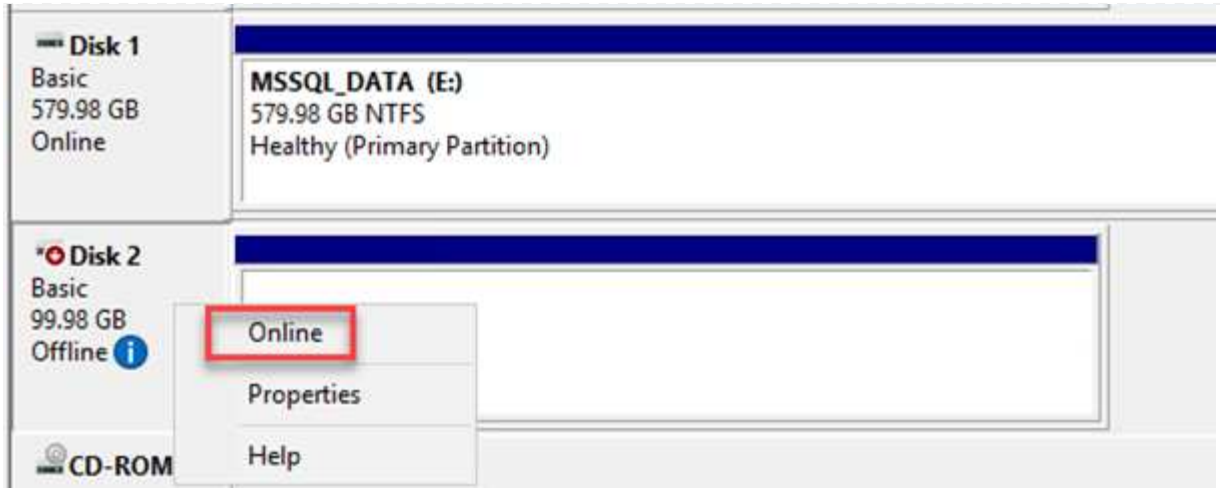




5. Nella scheda Target, fare clic su Connect (Connetti), selezionare Enable Multi-Path (attiva percorso multiplo) se appropriato per la configurazione, quindi fare clic su OK per connettersi alla destinazione.

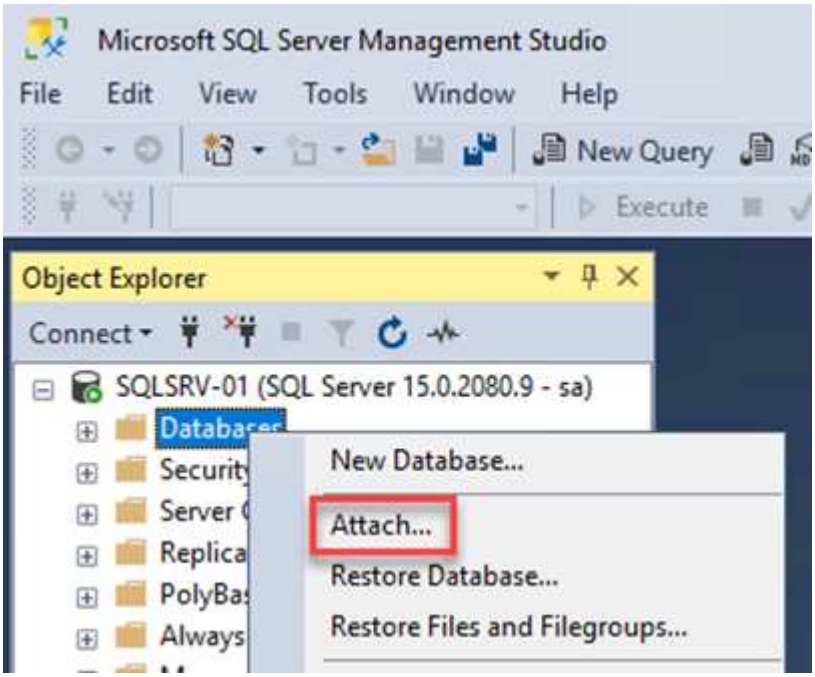


6. Aprire l'utility Gestione computer e portare i dischi in linea. Verificare che conservino le stesse lettere di unità in precedenza.

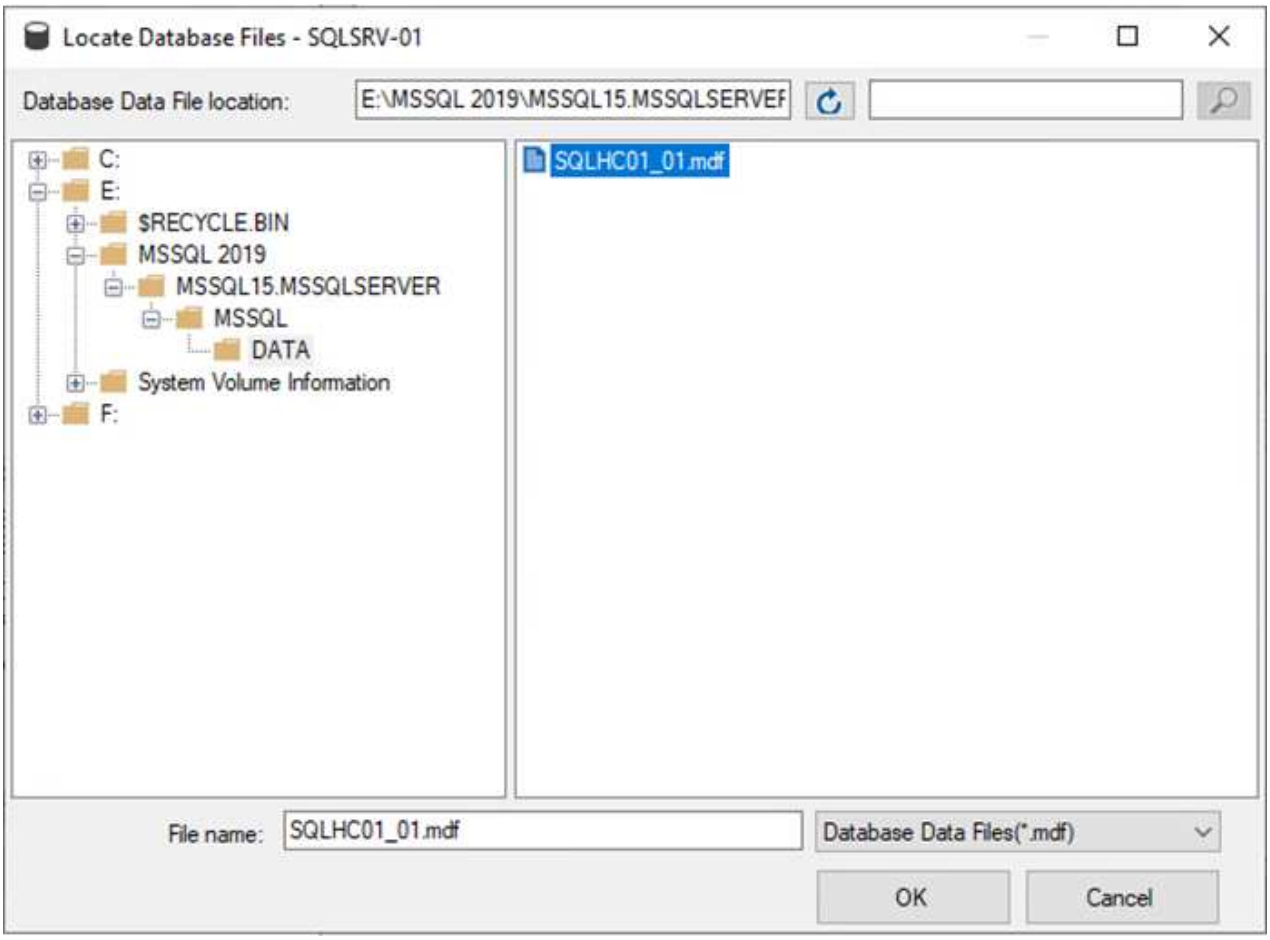

Disk 1
Basic
579.98 GB
Online
MSSQL_DATA (E:)
579.98 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
99.98 GB
Offline
Online
Properties
Help
CD-ROM

Collegare i database di SQL Server

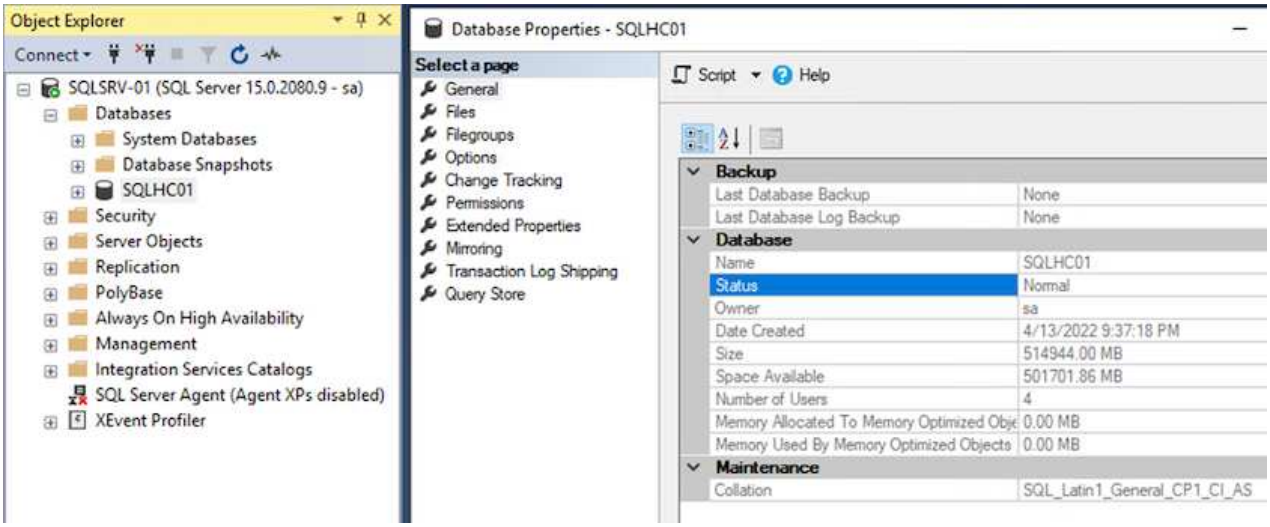
1. Da SQL Server VM, aprire Microsoft SQL Server Management Studio e selezionare Allega per avviare il processo di connessione al database.



2. Fare clic su Add (Aggiungi) e accedere alla cartella contenente il file di database primario di SQL Server, selezionarlo e fare clic su OK.



3. Se i log delle transazioni si trovano su un'unità separata, scegliere la cartella che contiene il log delle transazioni.
4. Al termine, fare clic su OK per allegare il database.

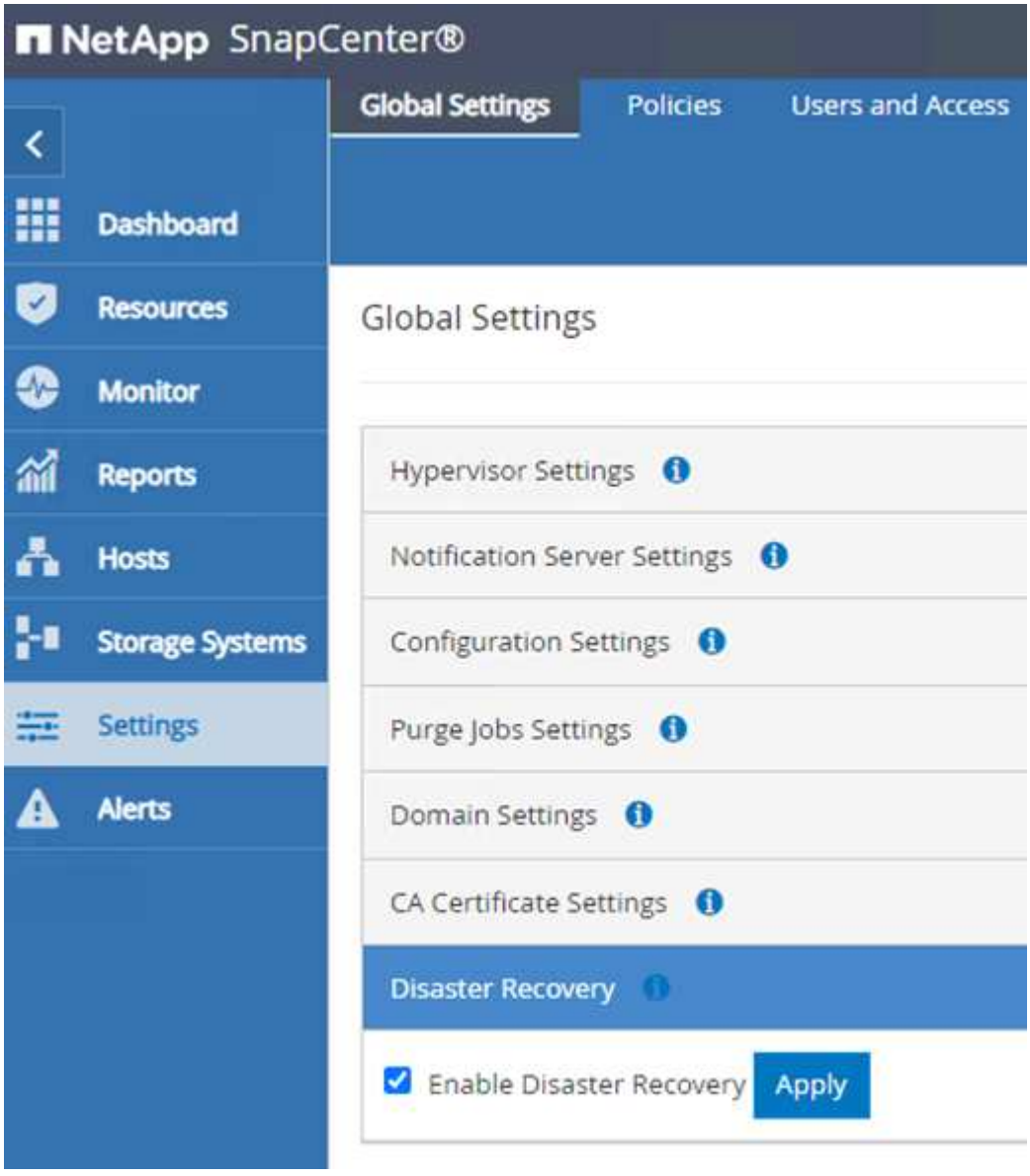


Confermare la comunicazione SnapCenter con il plug-in di SQL Server

Una volta ripristinato lo stato precedente, il database SnapCenter rileva automaticamente gli host di SQL Server. Affinché questo funzioni correttamente, tenere presente i seguenti prerequisiti:

- SnapCenter deve essere impostato sulla modalità di disaster recovery. Questa operazione può essere eseguita tramite l'API Swagger o in Impostazioni globali in Disaster Recovery.
- L'FQDN di SQL Server deve essere identico all'istanza in esecuzione nel data center on-premise.
- La relazione SnapMirror originale deve essere interrotta.
- Le LUN contenenti il database devono essere montate sull'istanza di SQL Server e sul database allegato.

Per verificare che SnapCenter sia in modalità di disaster recovery, accedere a Impostazioni dal client Web di SnapCenter. Accedere alla scheda Global Settings (Impostazioni globali) e fare clic su Disaster Recovery (Ripristino di emergenza). Assicurarsi che la casella di controllo Enable Disaster Recovery (attiva Disaster Recovery) sia attivata.



Ripristinare i dati delle applicazioni Oracle

Il seguente processo fornisce istruzioni su come ripristinare i dati delle applicazioni Oracle in VMware Cloud Services in AWS in caso di disastro che rende il sito on-premise inutilizzabile.

Completare i seguenti prerequisiti per continuare con la procedura di ripristino:

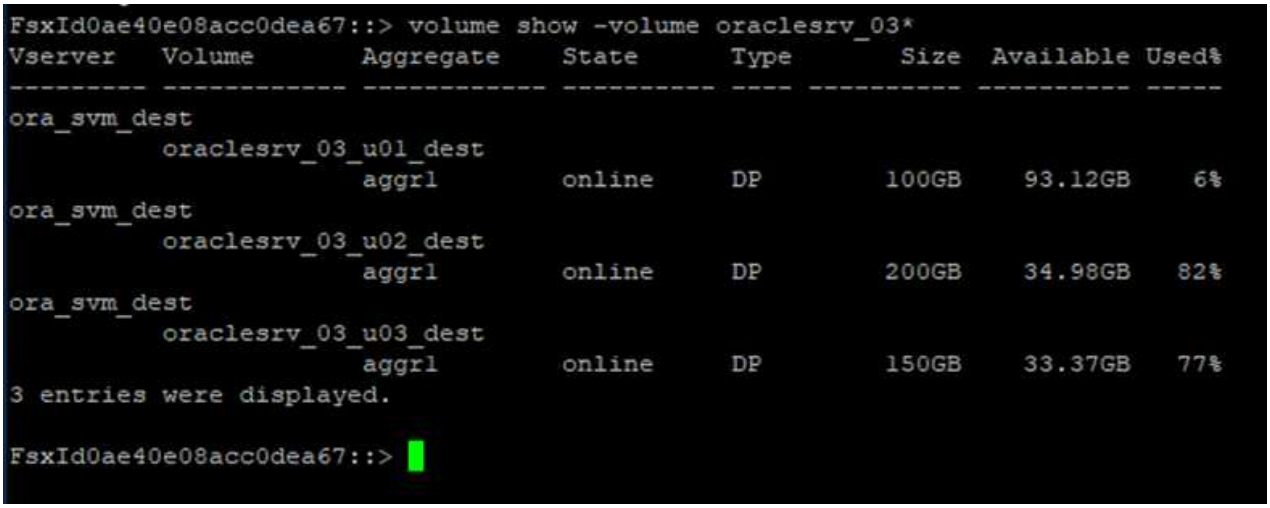
1. La macchina virtuale del server Oracle Linux è stata ripristinata su VMware Cloud SDDC utilizzando Veeam Full Restore.
2. È stato creato un server SnapCenter secondario e il database SnapCenter e i file di configurazione sono stati ripristinati seguendo la procedura descritta in questa sezione "Riepilogo del processo di backup e ripristino di SnapCenter."

Configurazione di FSX per il ripristino di Oracle - interruzione della relazione SnapMirror

Per rendere accessibili ai server Oracle i volumi di storage secondari ospitati sull'istanza FSxN, è necessario prima interrompere la relazione SnapMirror esistente.

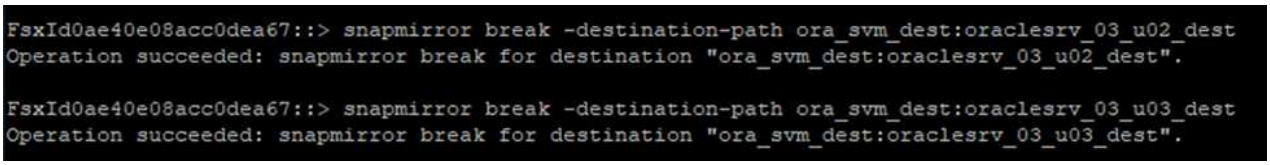
1. Dopo aver effettuato l'accesso alla CLI FSX, eseguire il seguente comando per visualizzare i volumi filtrati dal nome corretto.

```
FSx-Dest::> volume show -volume VolumeName*
```

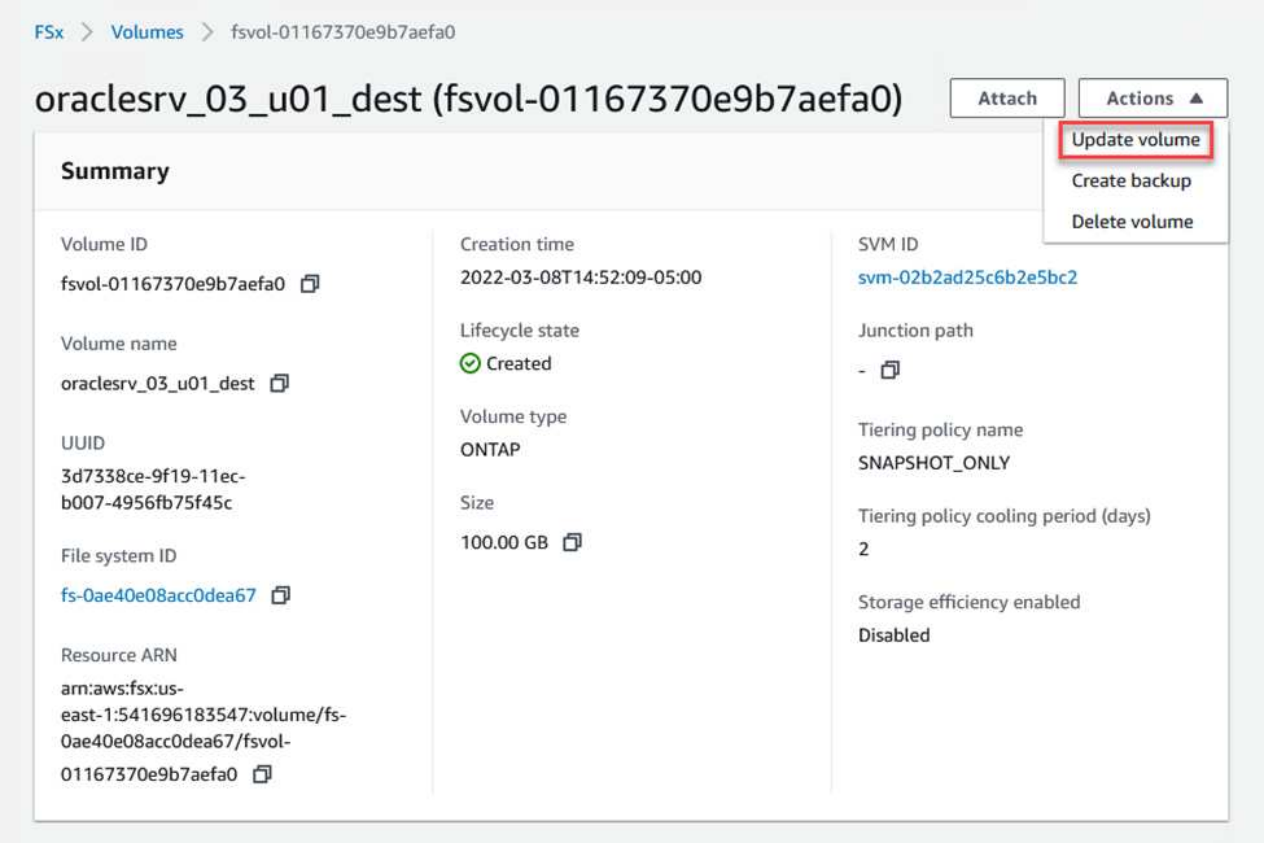


2. Eseguire il seguente comando per interrompere le relazioni SnapMirror esistenti.

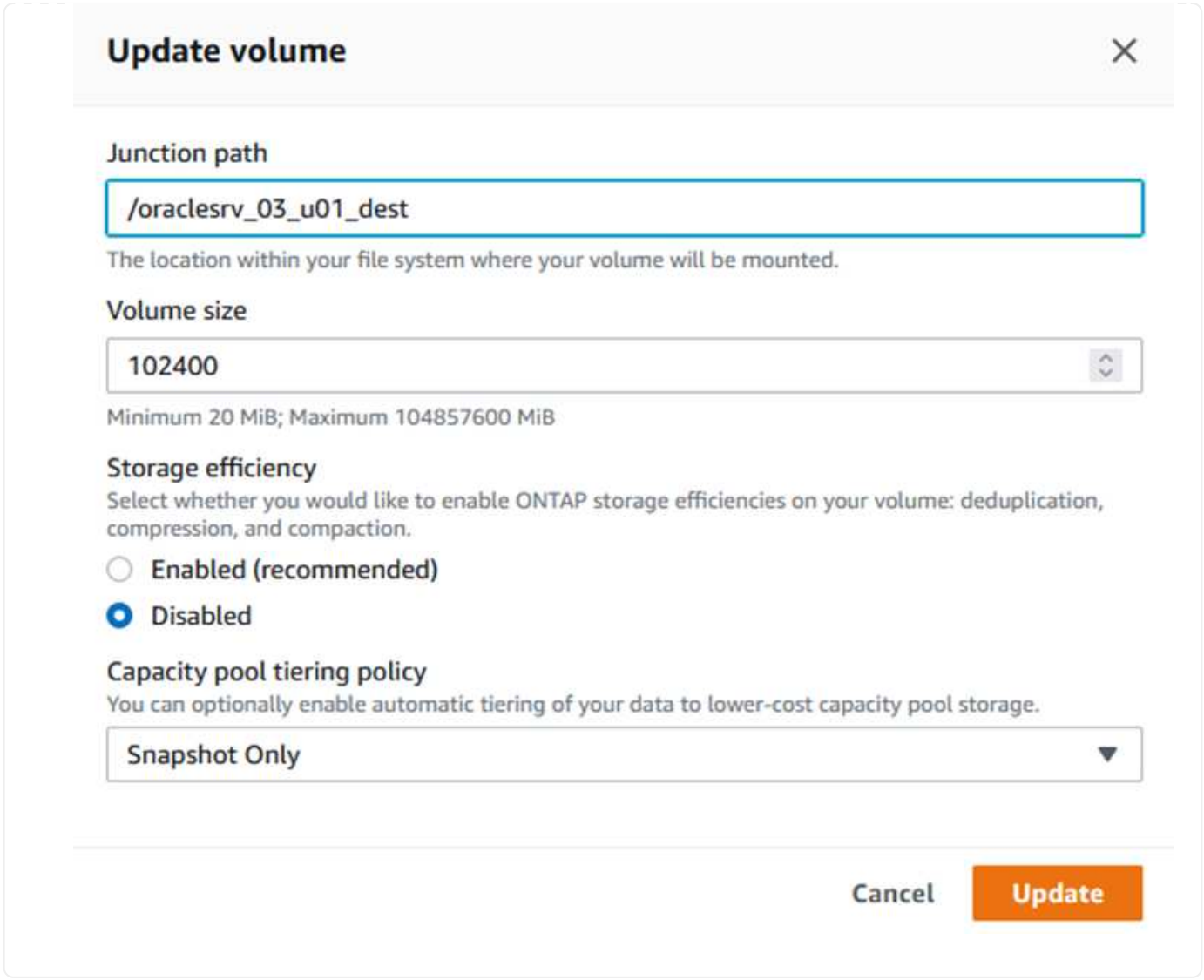
```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```



3. Aggiornare il percorso di giunzione nel client Web Amazon FSX:



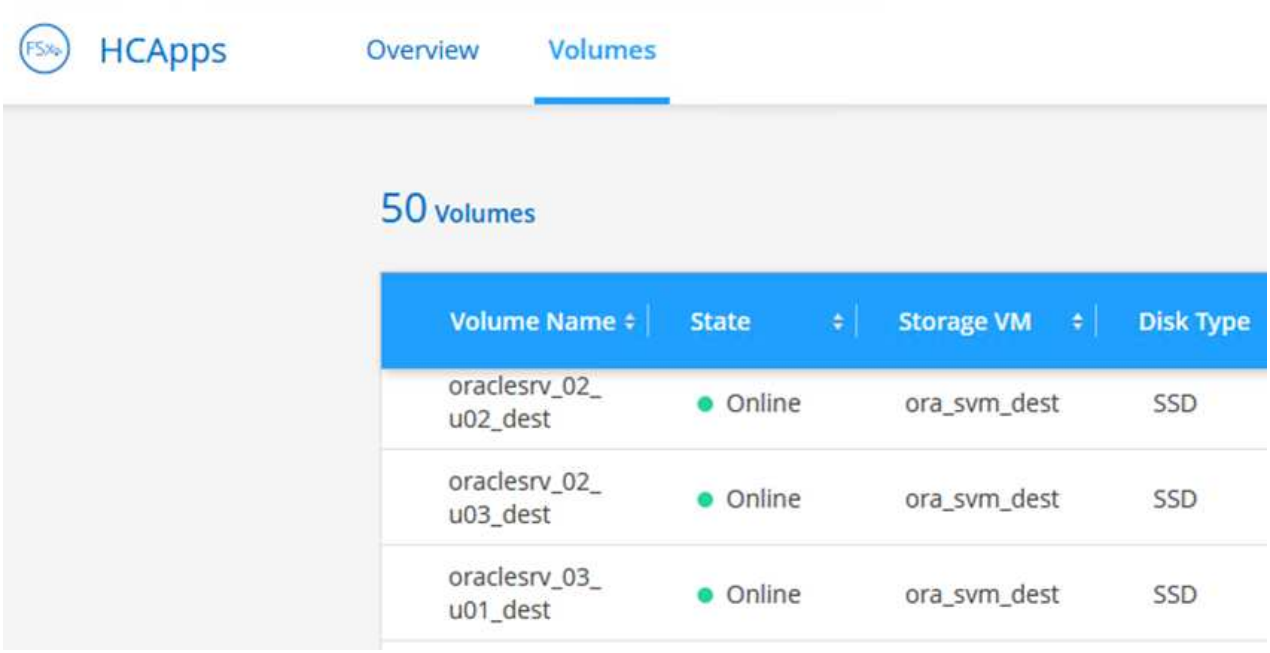
4. Aggiungere il nome del percorso di giunzione e fare clic su Update (Aggiorna). Specificare questo percorso di giunzione quando si monta il volume NFS dal server Oracle.


Update volume
Junction path
/oraclesrv_03_u01_dest
The location within your file system where your volume will be mounted.
Volume size
102400
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
Snapshot Only
Cancel
Update

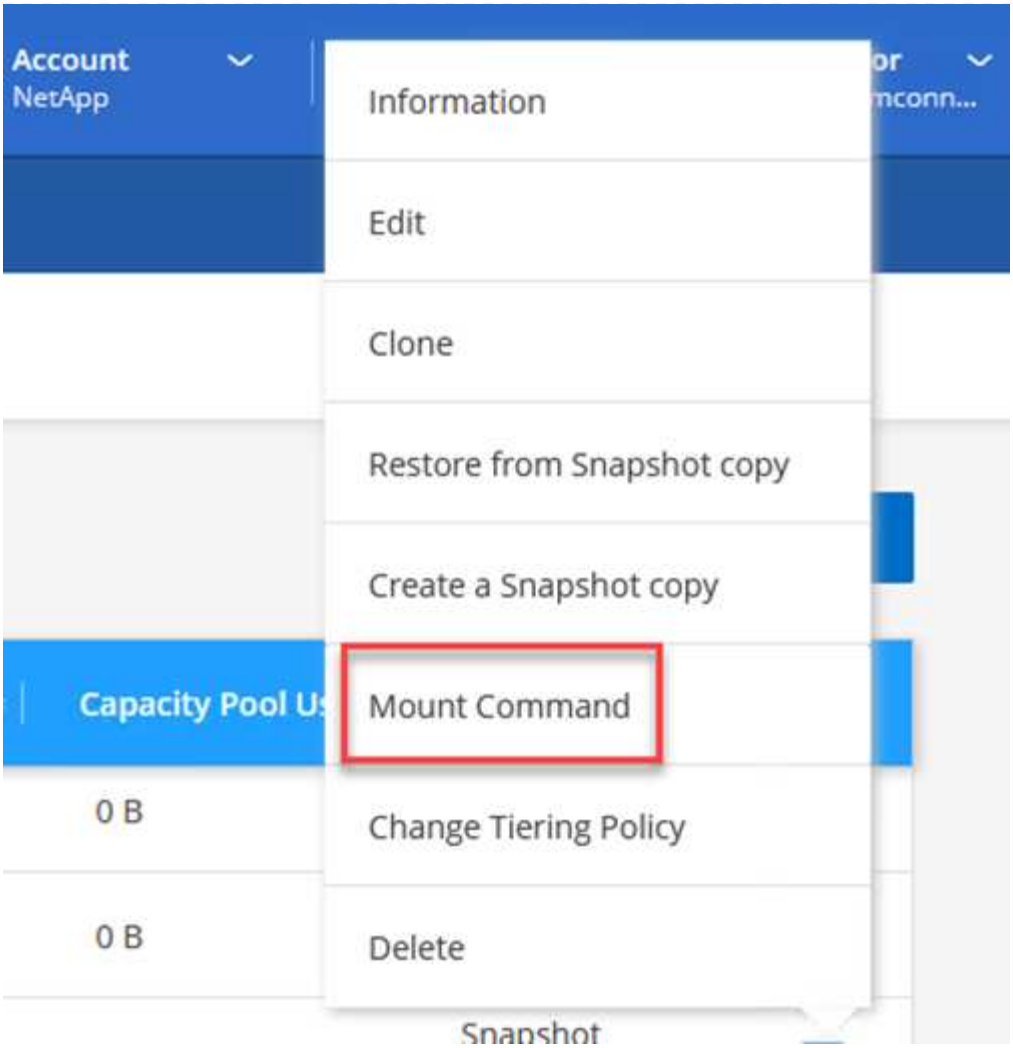
Montare volumi NFS su Oracle Server

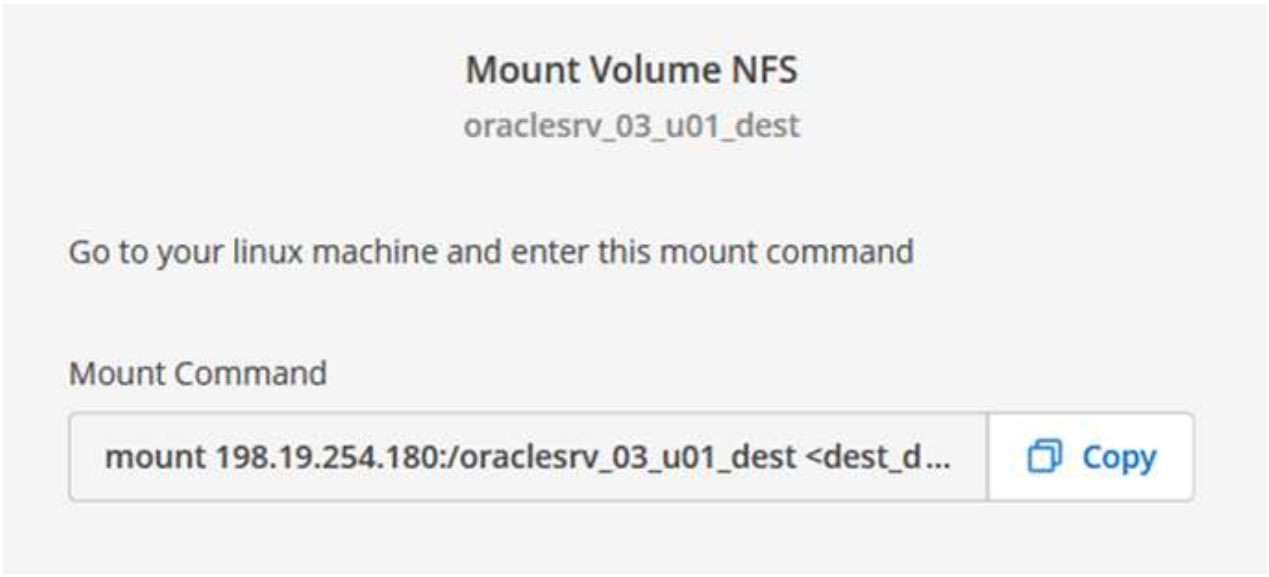
In Cloud Manager, è possibile ottenere il comando mount con l'indirizzo IP NFS LIF corretto per il montaggio dei volumi NFS che contengono i file di database e i log Oracle.

1. In Cloud Manager, accedi all'elenco dei volumi per il cluster FSX.



2. Dal menu delle azioni, selezionare Mount Command per visualizzare e copiare il comando mount da utilizzare sul server Oracle Linux.





3. Montare il file system NFS su Oracle Linux Server. Le directory per il montaggio della condivisione NFS esistono già sull'host Oracle Linux.
4. Dal server Oracle Linux, utilizzare il comando mount per montare i volumi NFS.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Ripetere questo passaggio per ogni volume associato ai database Oracle.

Per rendere persistente il montaggio NFS al riavvio, modificare `/etc/fstab` per includere i comandi di montaggio.

5. Riavviare il server Oracle. I database Oracle dovrebbero avviarsi normalmente e essere disponibili per l'utilizzo.

Failback

Una volta completato con successo il processo di failover descritto in questa soluzione, SnapCenter e Veeam riprendono le funzioni di backup in esecuzione in AWS, mentre FSX per ONTAP viene ora designato come storage primario senza relazioni SnapMirror esistenti con il data center on-premise originale. Una volta ripristinato il normale funzionamento on-premise, è possibile utilizzare un processo identico a quello descritto in questa documentazione per eseguire il mirroring dei dati nel sistema di storage ONTAP on-premise.

Come indicato anche in questa documentazione, è possibile configurare SnapCenter per eseguire il mirroring dei volumi di dati dell'applicazione da FSX per ONTAP a un sistema storage ONTAP residente on-premise. Allo stesso modo, puoi configurare Veeam per replicare le copie di backup su Amazon S3 utilizzando un repository di backup scale-out in modo che tali backup siano accessibili a un server di backup Veeam che risiede nel data center on-premise.

Il failback non rientra nell'ambito di questa documentazione, ma il failback non differisce molto dal processo dettagliato qui descritto.

Conclusione

Il caso d'utilizzo presentato in questa documentazione si concentra su tecnologie di disaster recovery comprovate che evidenziano l'integrazione tra NetApp e VMware. I sistemi di storage NetApp ONTAP offrono tecnologie di mirroring dei dati comprovate che consentono alle organizzazioni di progettare soluzioni di disaster recovery che abbracciano tecnologie on-premise e ONTAP che risiedono presso i principali cloud provider.

FSX per ONTAP su AWS è una soluzione di questo tipo che consente un'integrazione perfetta con SnapCenter e SyncMirror per la replica dei dati delle applicazioni nel cloud. Veeam Backup & Replication è un'altra tecnologia ben nota che si integra perfettamente con i sistemi storage NetApp ONTAP e può fornire il failover allo storage nativo vSphere.

Questa soluzione ha presentato una soluzione di disaster recovery che utilizza lo storage Connect guest da un sistema ONTAP che ospita i dati delle applicazioni SQL Server e Oracle. SnapCenter con SnapMirror offre una soluzione semplice da gestire per proteggere i volumi delle applicazioni sui sistemi ONTAP e replicarli su FSX o CVO che risiedono nel cloud. SnapCenter è una soluzione abilitata al DR per eseguire il failover di tutti i dati delle applicazioni su VMware Cloud su AWS.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Collegamenti alla documentazione della soluzione

  "Multicloud ibrido NetApp con soluzioni VMware"

  "Soluzioni NetApp"

Backup e ripristino di Veeam in VMware Cloud, con Amazon FSX per ONTAP

Autore: Josh Powell - NetApp Solutions Engineering

Panoramica

Veeam Backup & Replication è una soluzione efficace e affidabile per la protezione dei dati in VMware Cloud. Questa soluzione dimostra la corretta configurazione e configurazione per l'utilizzo di backup e replica Veeam per il backup e il ripristino delle macchine virtuali dell'applicazione che risiedono su datastore NFS FSX per ONTAP in VMware Cloud.

VMware Cloud (in AWS) supporta l'utilizzo di datastore NFS come storage supplementare, mentre FSX per NetApp ONTAP è una soluzione sicura per i clienti che hanno bisogno di memorizzare grandi quantità di dati per le loro applicazioni cloud, in grado di scalare indipendentemente dal numero di host ESXi nel cluster SDDC. Questo servizio di storage AWS integrato offre uno storage altamente efficiente con tutte le funzionalità tradizionali di NetApp ONTAP.

Casi di utilizzo

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup e ripristino di macchine virtuali Windows e Linux ospitate in VMC utilizzando FSX per NetApp ONTAP come repository di backup.
- Backup e ripristino dei dati delle applicazioni Microsoft SQL Server utilizzando FSX per NetApp ONTAP come repository di backup.
- Backup e ripristino dei dati delle applicazioni Oracle utilizzando FSX per NetApp ONTAP come repository di backup.

Archivi dati NFS che utilizzano Amazon FSX per ONTAP

Tutte le macchine virtuali di questa soluzione risiedono su datastore NFS supplementari FSX per ONTAP. L'utilizzo di FSX per ONTAP come datastore NFS supplementare offre diversi vantaggi. Ad esempio, consente di:

- Crea un file system scalabile e altamente disponibile nel cloud senza la necessità di complesse operazioni di configurazione e gestione.
- Integrazione con l'ambiente VMware esistente, che consente di utilizzare strumenti e processi familiari per gestire le risorse cloud.
- Sfrutta le funzionalità avanzate di gestione dei dati fornite da ONTAP, come snapshot e replica, per proteggere i tuoi dati e garantirne la disponibilità.

Panoramica sull'implementazione della soluzione

Questo elenco fornisce i passaggi di alto livello necessari per configurare il backup e la replica di Veeeam, eseguire processi di backup e ripristino utilizzando FSX per ONTAP come repository di backup ed eseguire ripristini di macchine virtuali e database SQL Server e Oracle:

1. Creare il file system FSX per ONTAP da utilizzare come repository di backup iSCSI per il backup e la replica Veeam.
2. Implementare Veeam Proxy per distribuire i carichi di lavoro di backup e montare repository di backup iSCSI ospitati su FSX per ONTAP.
3. Configurare Veeam Backup Jobs per il backup di macchine virtuali SQL Server, Oracle, Linux e Windows.
4. Ripristinare le macchine virtuali SQL Server e i singoli database.
5. Ripristinare le macchine virtuali Oracle e i singoli database.

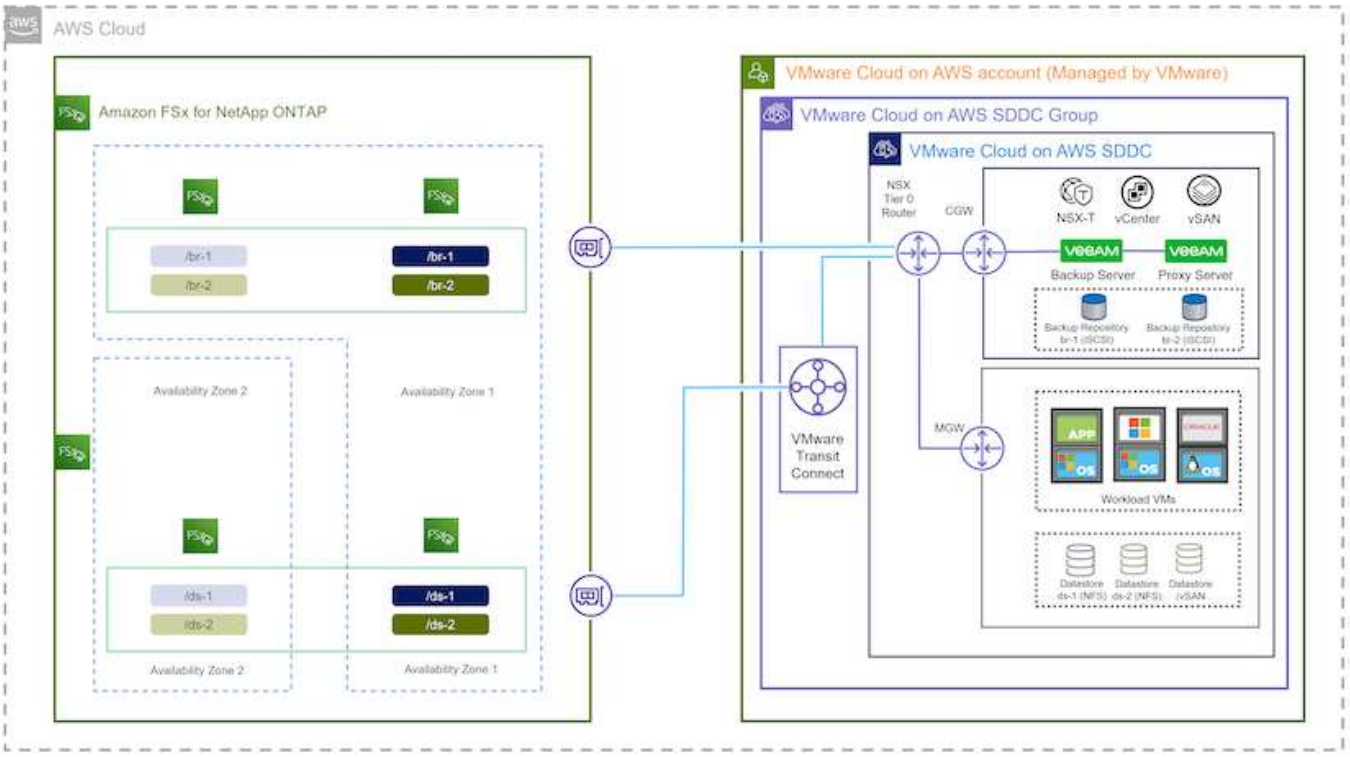
Prerequisiti

Lo scopo di questa soluzione è dimostrare la protezione dei dati delle macchine virtuali in esecuzione in VMware Cloud e situate su archivi dati NFS ospitati da FSX per NetApp ONTAP. Questa soluzione presuppone che i seguenti componenti siano configurati e pronti per l'uso:

1. File system FSX per ONTAP con uno o più datastore NFS connessi a VMware Cloud.
2. Macchina virtuale Microsoft Windows Server con software Veeam Backup & Replication installato.
    - Il server vCenter è stato rilevato dal server Veeam Backup & Replication utilizzando il proprio indirizzo IP o il nome di dominio completo.
3. Microsoft Windows Server VM da installare con i componenti di Veeam Backup Proxy durante l'implementazione della soluzione.
4. Macchine virtuali Microsoft SQL Server con VMDK e dati delle applicazioni che risiedono su FSX per datastore NFS di ONTAP. Per questa soluzione avevamo due database SQL su due VMDK separati.
    - Nota: Come Best practice, i file di log delle transazioni e dei database vengono collocati su dischi separati, in quanto ciò migliorerà le performance e l'affidabilità. Ciò è dovuto in parte al fatto che i log delle transazioni vengono scritti in sequenza, mentre i file di database vengono scritti in modo casuale.
5. VM di database Oracle con VMDK e dati delle applicazioni che risiedono su FSX per datastore NFS di ONTAP.
6. VM di file server Linux e Windows con VMDK residenti su FSX per datastore NFS ONTAP.
7. Veeam richiede porte TCP specifiche per la comunicazione tra server e componenti nell'ambiente di backup. Sui componenti dell'infrastruttura di backup Veeam, le regole firewall richieste vengono create automaticamente. Per un elenco completo dei requisiti delle porte di rete, consultare la sezione Porte del "Guida utente di Veeam Backup and Replication per VMware vSphere".

Architettura di alto livello

Il test/convalida di questa soluzione è stato eseguito in un laboratorio che potrebbe corrispondere o meno all'ambiente di implementazione finale. Per ulteriori informazioni, fare riferimento alle seguenti sezioni.



Componenti hardware/software

Lo scopo di questa soluzione è dimostrare la protezione dei dati delle macchine virtuali in esecuzione in VMware Cloud e situate su archivi dati NFS ospitati da FSX per NetApp ONTAP. Questa soluzione presuppone che i seguenti componenti siano già configurati e pronti per l'uso:

- Macchine virtuali Microsoft Windows situate su un archivio dati NFS FSX per ONTAP
- Macchine virtuali Linux (CentOS) situate su un archivio dati NFS FSX per ONTAP
- Macchine virtuali Microsoft SQL Server situate su un archivio dati NFS FSX per ONTAP
  - Due database ospitati su VMDK separati
- Oracle VM si trova su un archivio dati FSX per NFS ONTAP

Implementazione della soluzione

In questa soluzione forniamo istruzioni dettagliate per l'implementazione e la convalida di una soluzione che utilizza il software di backup e replica Veeam per eseguire il backup e il ripristino di macchine virtuali di file server SQL Server, Oracle e Windows e Linux in un VMware Cloud SDDC su AWS. Le macchine virtuali di questa soluzione risiedono su un datastore NFS supplementare ospitato da FSX per ONTAP. Inoltre, viene utilizzato un file system FSX separato per ONTAP per ospitare volumi iSCSI che verranno utilizzati per i repository di backup Veeam.

Passeremo a FSX per la creazione di file system ONTAP, il montaggio di volumi iSCSI da utilizzare come repository di backup, la creazione e l'esecuzione di processi di backup e il ripristino di macchine virtuali e database.

Per informazioni dettagliate su FSX per NetApp ONTAP, fare riferimento a. "Guida utente di FSX per ONTAP".

Per informazioni dettagliate su Veeam Backup e Replication, fare riferimento a. "Documentazione tecnica del

Centro assistenza Veeam" sito.

Per considerazioni e limitazioni sull'utilizzo di Veeam Backup and Replication con VMware Cloud su AWS, fare riferimento a. "VMware Cloud su AWS e VMware Cloud su supporto Dell EMC. Considerazioni e limitazioni".

Implementare il server proxy Veeam

Un server proxy Veeam è un componente del software Veeam Backup & Replication che funge da intermediario tra l'origine e la destinazione di backup o replica. Il server proxy consente di ottimizzare e accelerare il trasferimento dei dati durante i processi di backup elaborando i dati in locale e può utilizzare diverse modalità di trasporto per accedere ai dati utilizzando le API VMware vStorage per la protezione dei dati o attraverso l'accesso diretto allo storage.

Quando si sceglie un server proxy Veeam, è importante considerare il numero di attività simultanee e la modalità di trasporto o il tipo di accesso allo storage desiderato.

Per il dimensionamento del numero di server proxy e i relativi requisiti di sistema, fare riferimento a. "Veeeam VMware vSphere Best Practice Guide".

Veeam Data Mover è un componente di Veeam Proxy Server e utilizza una Transport Mode come metodo per ottenere i dati delle macchine virtuali dall'origine e trasferirli alla destinazione. La modalità di trasporto viene specificata durante la configurazione del processo di backup. È possibile aumentare l'efficienza dei backup dagli archivi dati NFS utilizzando l'accesso diretto allo storage.

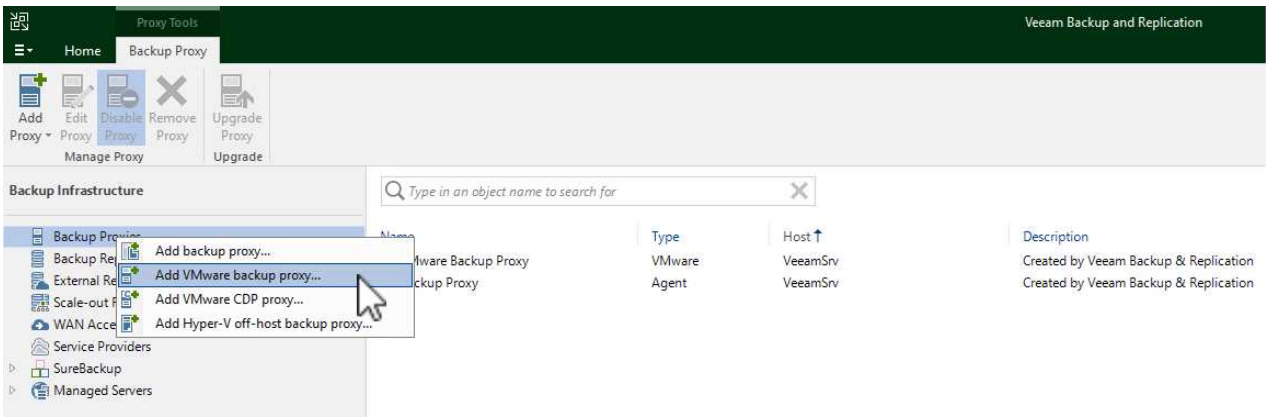
Per ulteriori informazioni sulle modalità di trasporto, fare riferimento a. "Guida utente di Veeam Backup and Replication per VMware vSphere".

Nella fase successiva verrà descritta l'implementazione di Veeam Proxy Server su una macchina virtuale Windows nel software SDDC VMware Cloud.

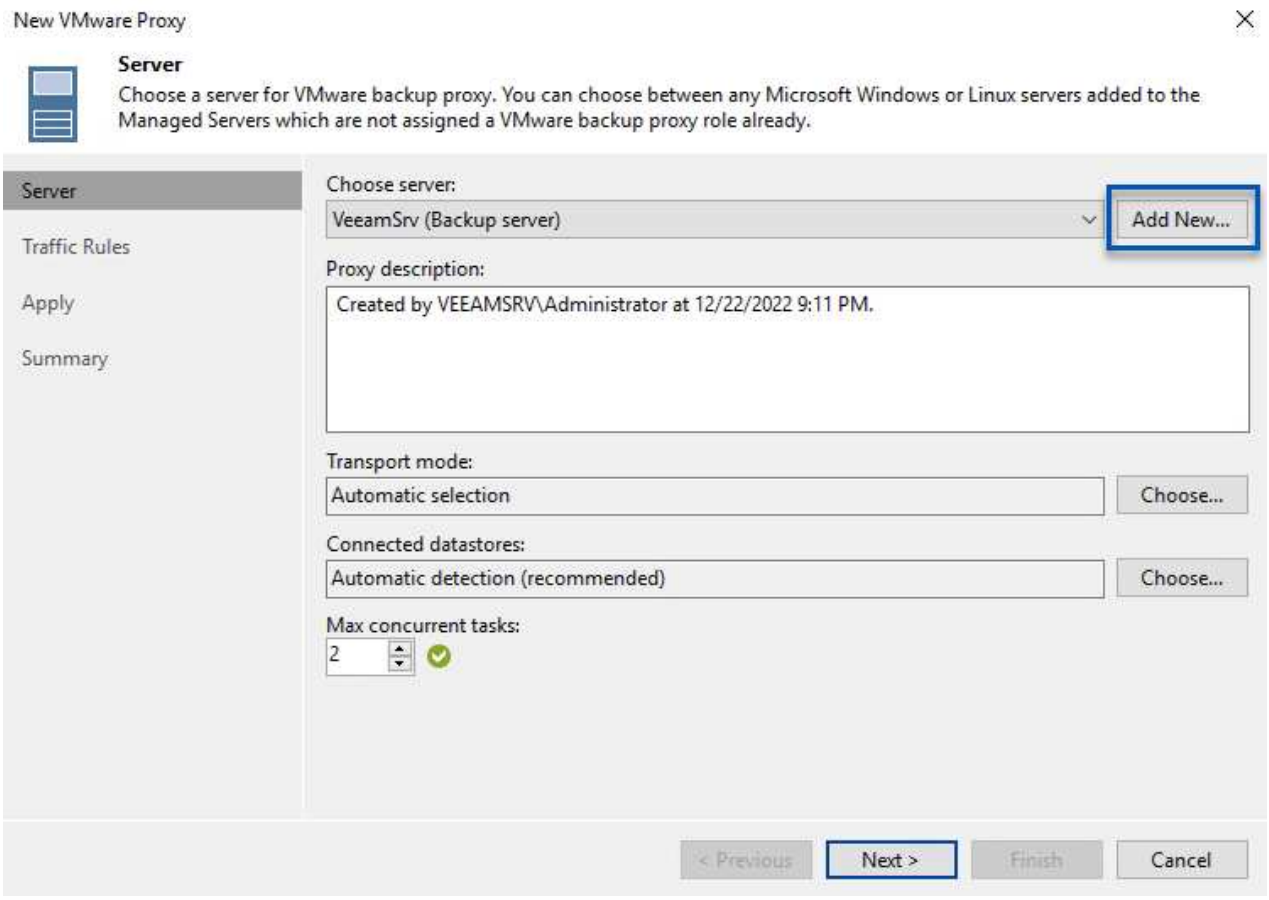
Implementare Veeam Proxy per distribuire i carichi di lavoro di backup

In questa fase, il proxy Veeam viene distribuito su una macchina virtuale Windows esistente. Ciò consente di distribuire i processi di backup tra il server di backup Veeam primario e il proxy Veeam.

1. Sul server Veeam Backup and Replication, aprire la console di amministrazione e selezionare **Backup Infrastructure** nel menu in basso a sinistra.
2. Fare clic con il pulsante destro del mouse su **Backup Proxy** e fare clic su **Add VMware backup proxy…** per aprire la procedura guidata.

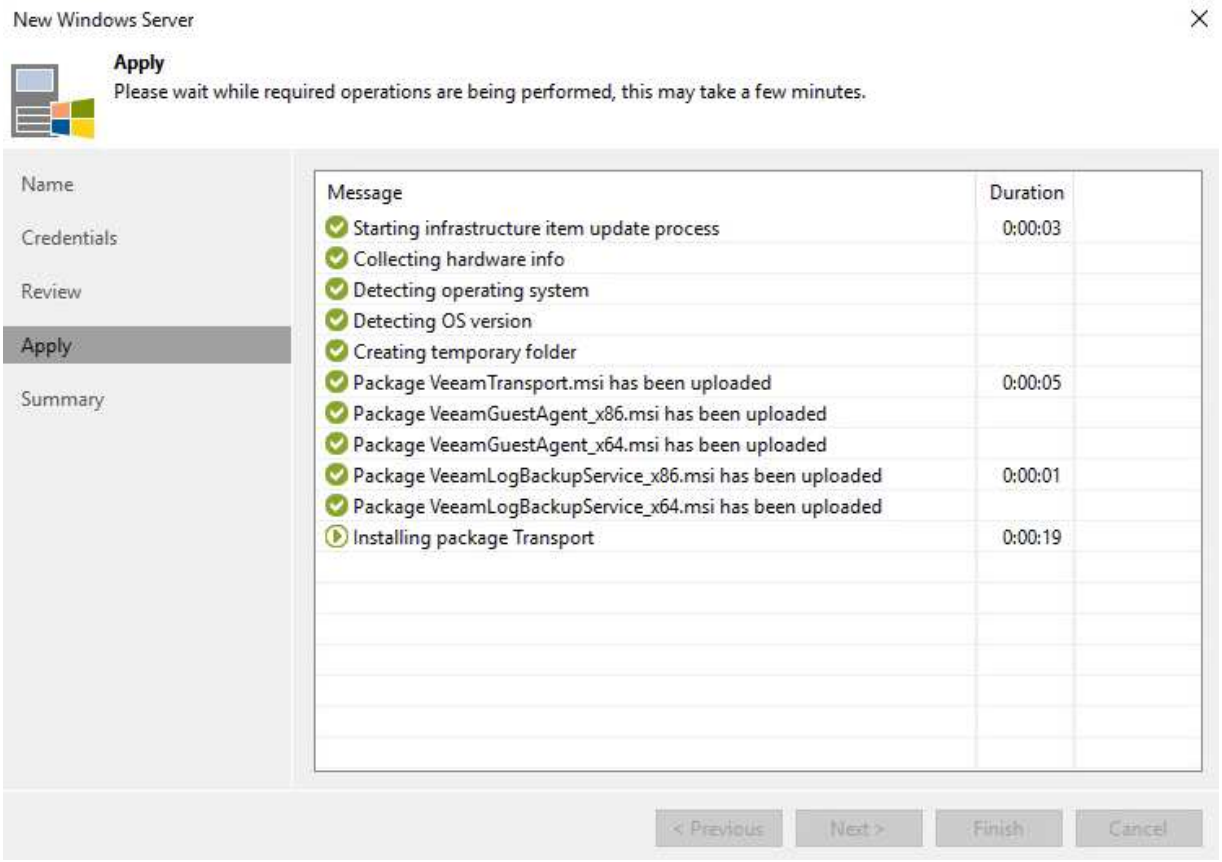


3. Nella procedura guidata **Add VMware Proxy** fare clic sul pulsante **Add New…** (Aggiungi nuovo…) per aggiungere un nuovo server proxy.

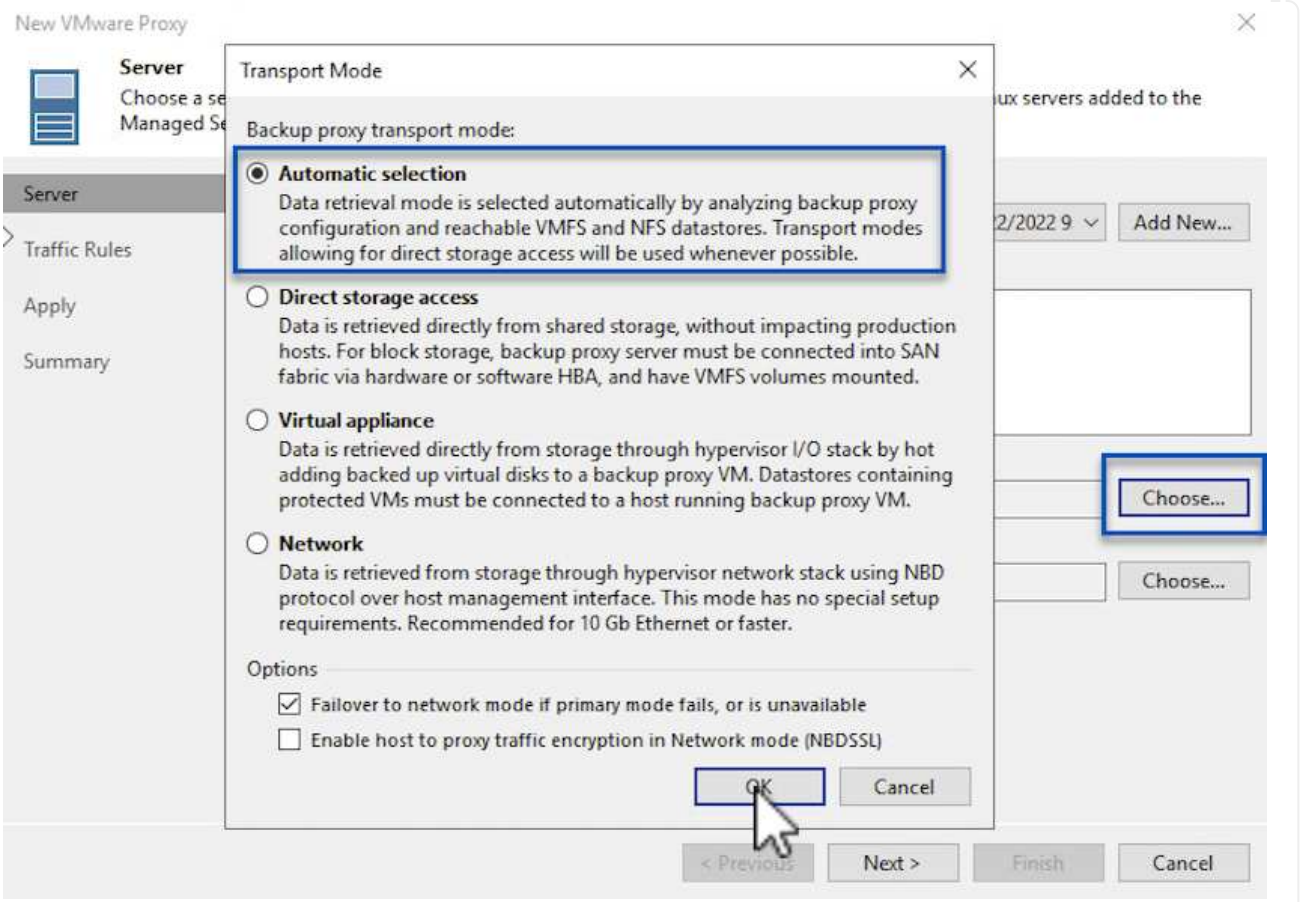


4. Selezionare per aggiungere Microsoft Windows e seguire le istruzioni per aggiungere il server:

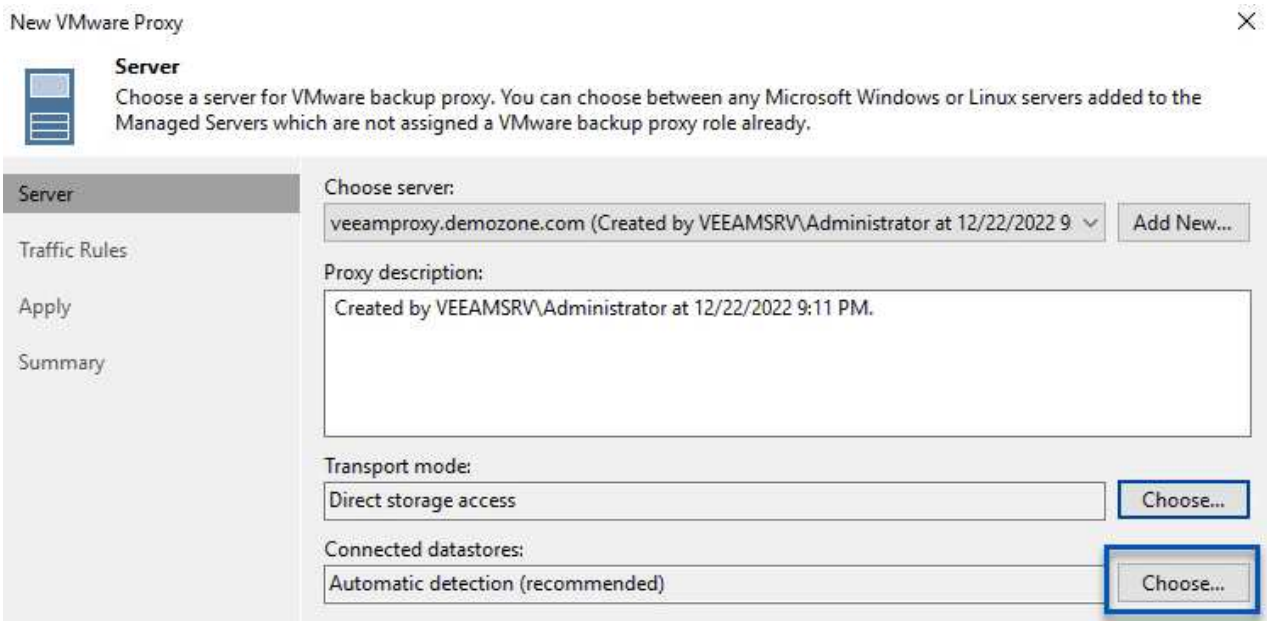
- Inserire il nome DNS o l'indirizzo IP
- Selezionare un account da utilizzare per le credenziali nel nuovo sistema o aggiungere nuove credenziali
- Esaminare i componenti da installare, quindi fare clic su **Apply** (Applica) per iniziare la distribuzione

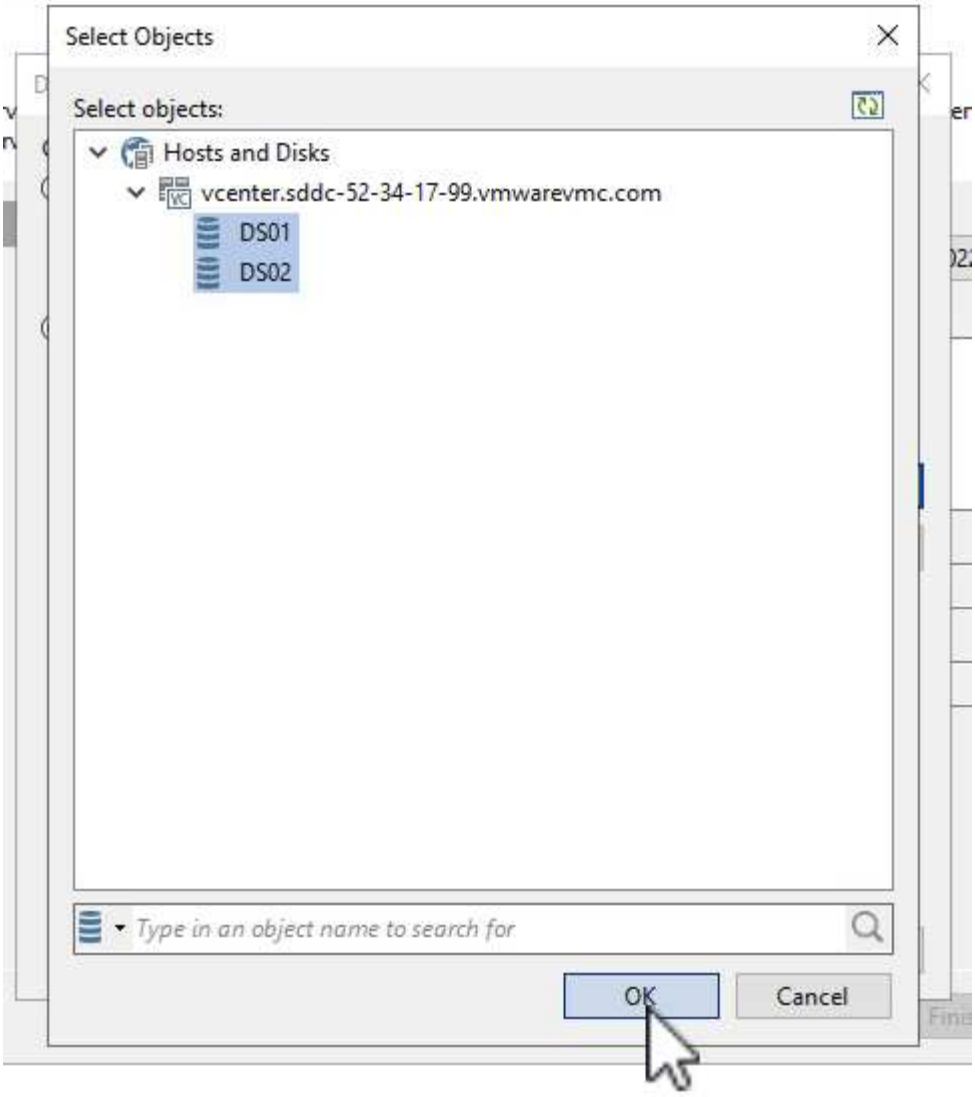


5. Nella procedura guidata **New VMware Proxy**, scegliere una modalità di trasporto. Nel nostro caso abbiamo scelto **selezione automatica**.

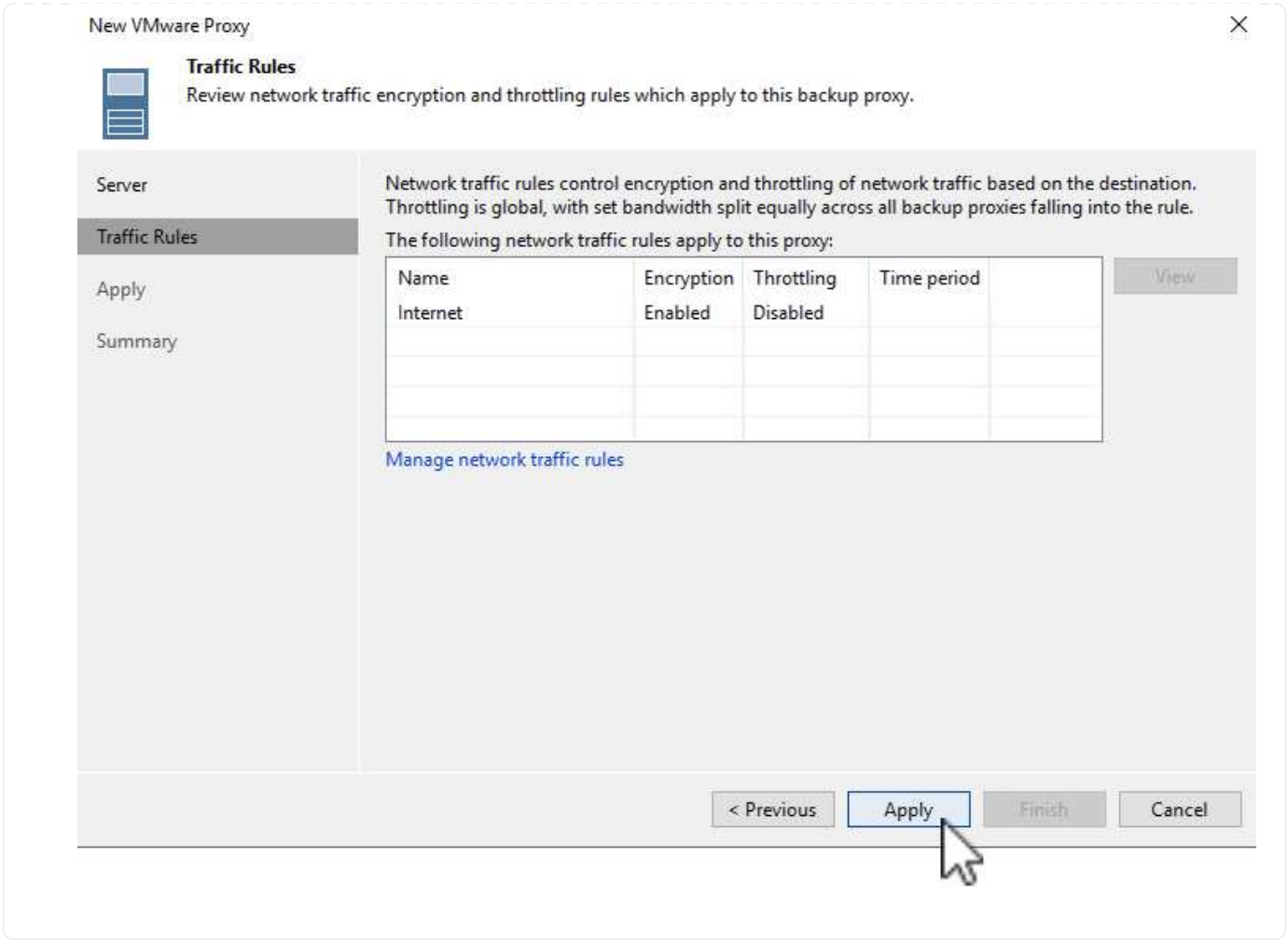


6. Selezionare gli archivi dati connessi ai quali si desidera che VMware Proxy abbia accesso diretto.





7. Configurare e applicare le regole di traffico di rete desiderate, ad esempio la crittografia o la limitazione. Al termine, fare clic sul pulsante **Apply** (Applica) per completare l'implementazione.



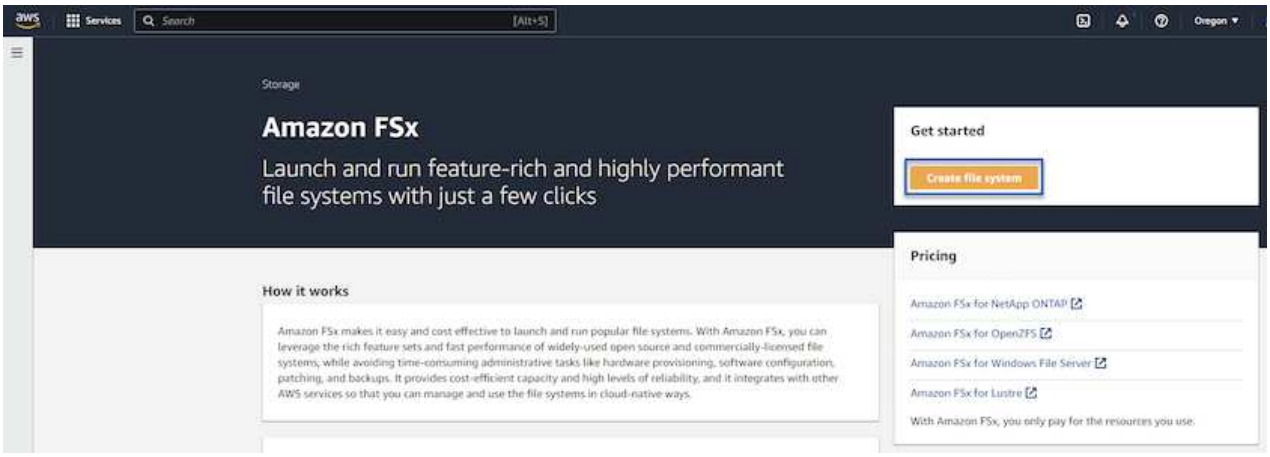
Configurare storage e repository di backup

Il server primario Veeam Backup e il server Veeam Proxy hanno accesso a un repository di backup sotto forma di storage a connessione diretta. In questa sezione viene descritta la creazione di un file system FSX per ONTAP, il montaggio di LUN iSCSI sui server Veeam e la creazione di repository di backup.

Creare FSX per il file system ONTAP

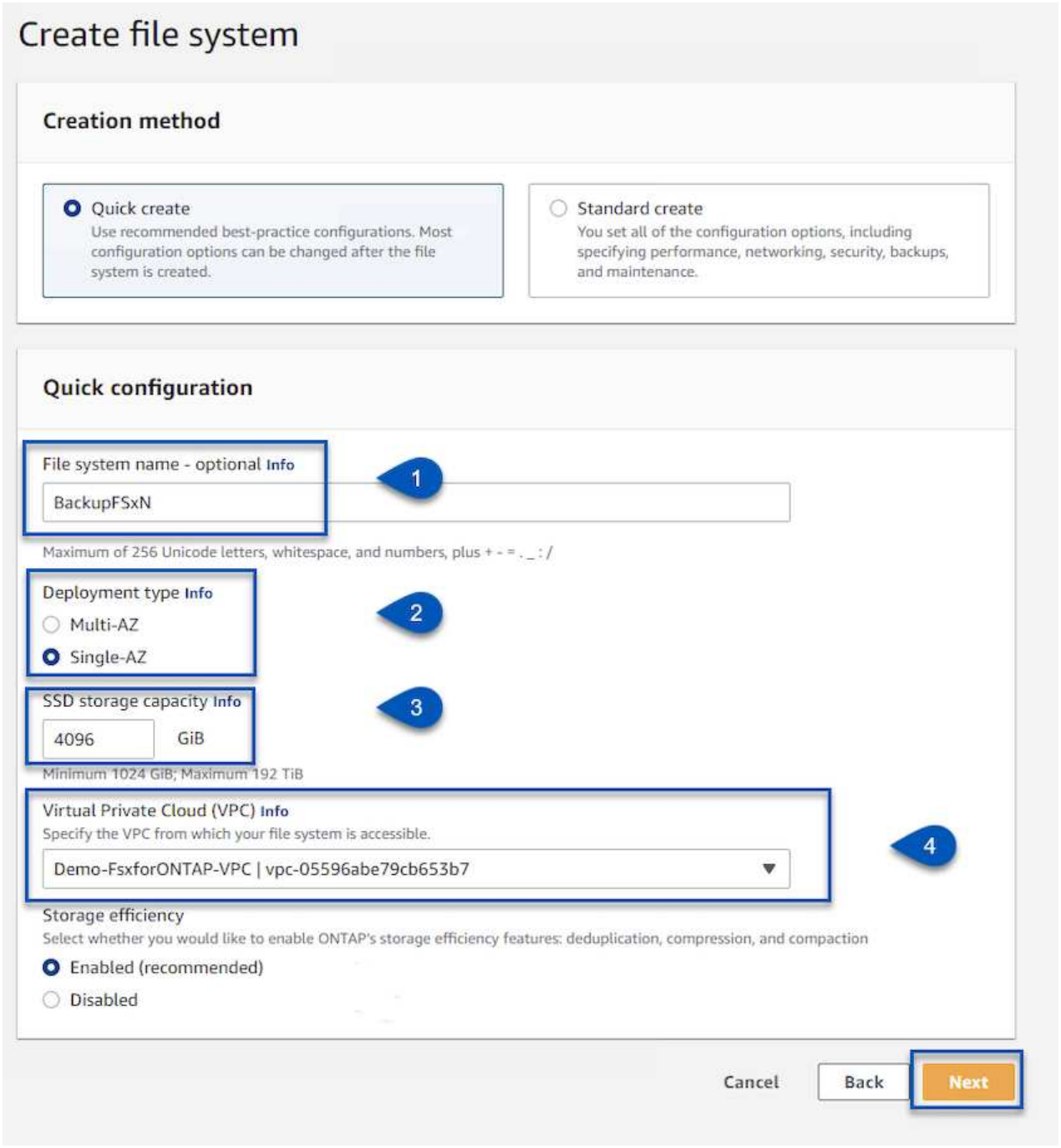
Creare un file system FSX per ONTAP che verrà utilizzato per ospitare i volumi iSCSI per i repository di backup Veeam.

1. Nella console AWS, andare a FSX e quindi a **Create file system**



2. Selezionare **Amazon FSX per NetApp ONTAP**, quindi **Avanti** per continuare.

3. Inserire il nome del file system, il tipo di implementazione, la capacità dello storage SSD e il VPC in cui si trova il cluster FSX per ONTAP. Deve essere un VPC configurato per comunicare con la rete di macchine virtuali in VMware Cloud. Fare clic su **Avanti**.



4. Esaminare le fasi di implementazione e fare clic su **Create file System** (Crea file system) per avviare il processo di creazione del file system.

Configurare e montare LUN iSCSI

Creare e configurare i LUN iSCSI su FSX per ONTAP e montarli sui server proxy e di backup Veeam. Questi LUN verranno utilizzati in seguito per creare repository di backup Veeam.

> La creazione di un LUN iSCSI su FSX per ONTAP è un processo multi-step. La prima fase della creazione dei volumi può essere eseguita nella console Amazon FSX o con la CLI NetApp ONTAP.

> Per ulteriori informazioni sull'utilizzo di FSX per ONTAP, consultare "Guida utente di FSX per ONTAP".

1. Dalla CLI di NetApp ONTAP creare i volumi iniziali utilizzando il seguente comando:

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. Creare LUN utilizzando i volumi creati nel passaggio precedente:

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Concedere l'accesso alle LUN creando un gruppo di iniziatori contenente l'IQN iSCSI dei server proxy e di backup Veeam:

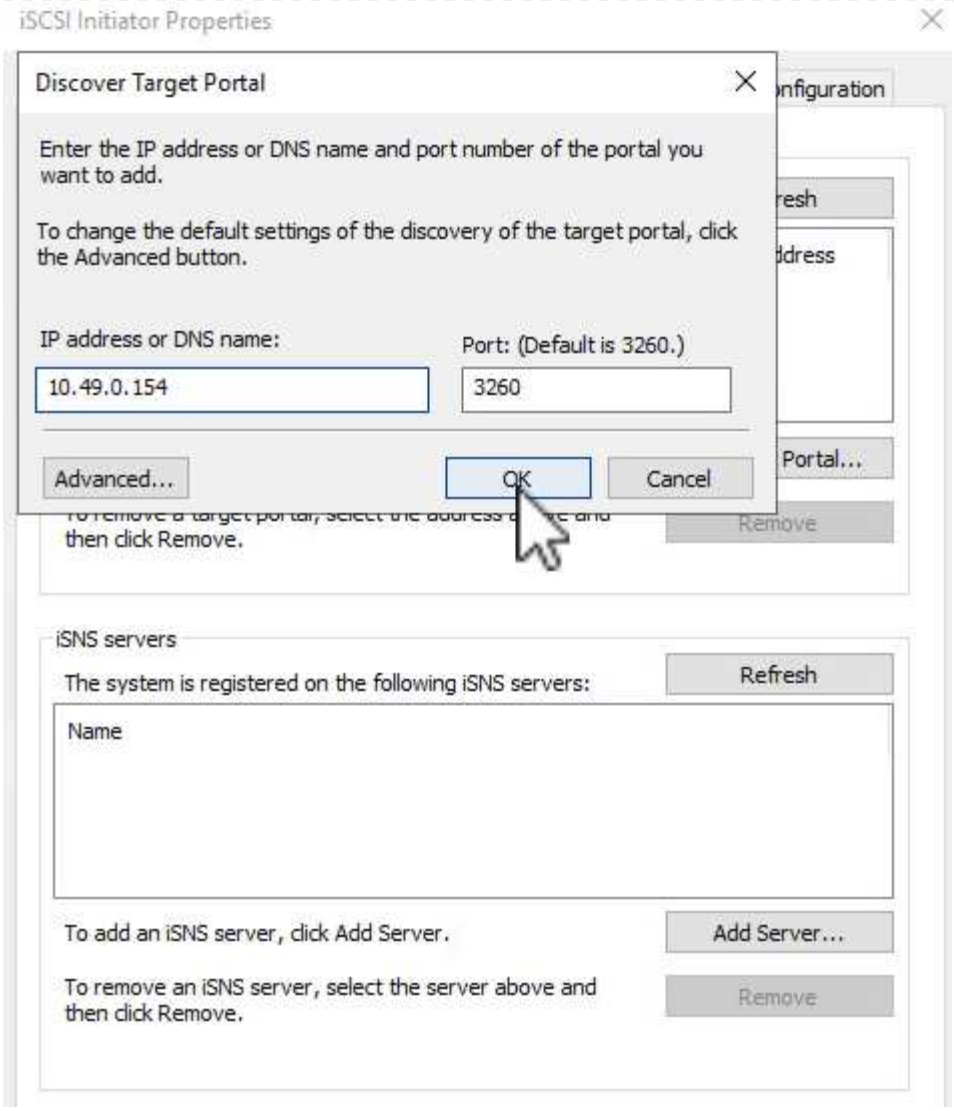
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

> Per completare il passaggio precedente, è necessario recuperare prima IQN dalle proprietà di iSCSI Initiator sui server Windows.

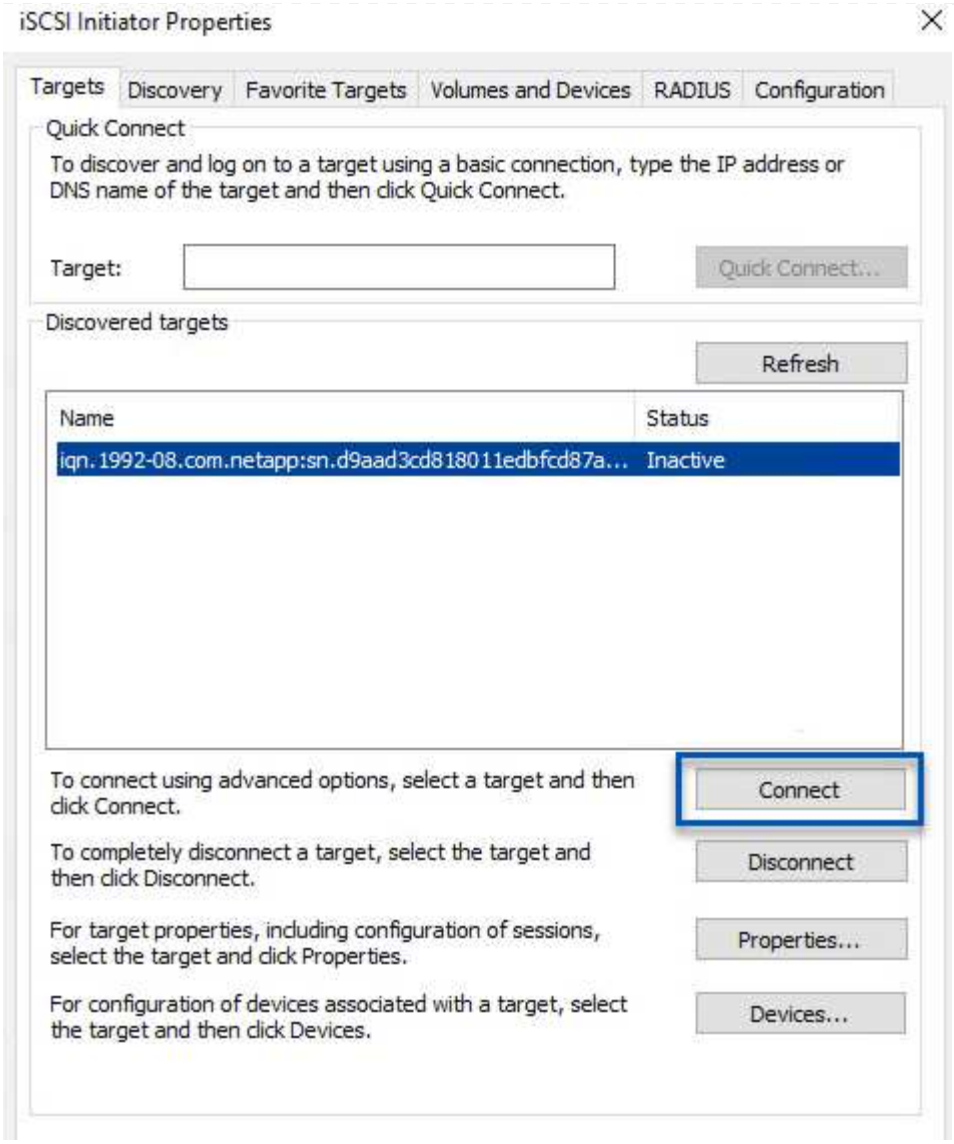
4. Infine, mappare le LUN al gruppo iniziatore appena creato:

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

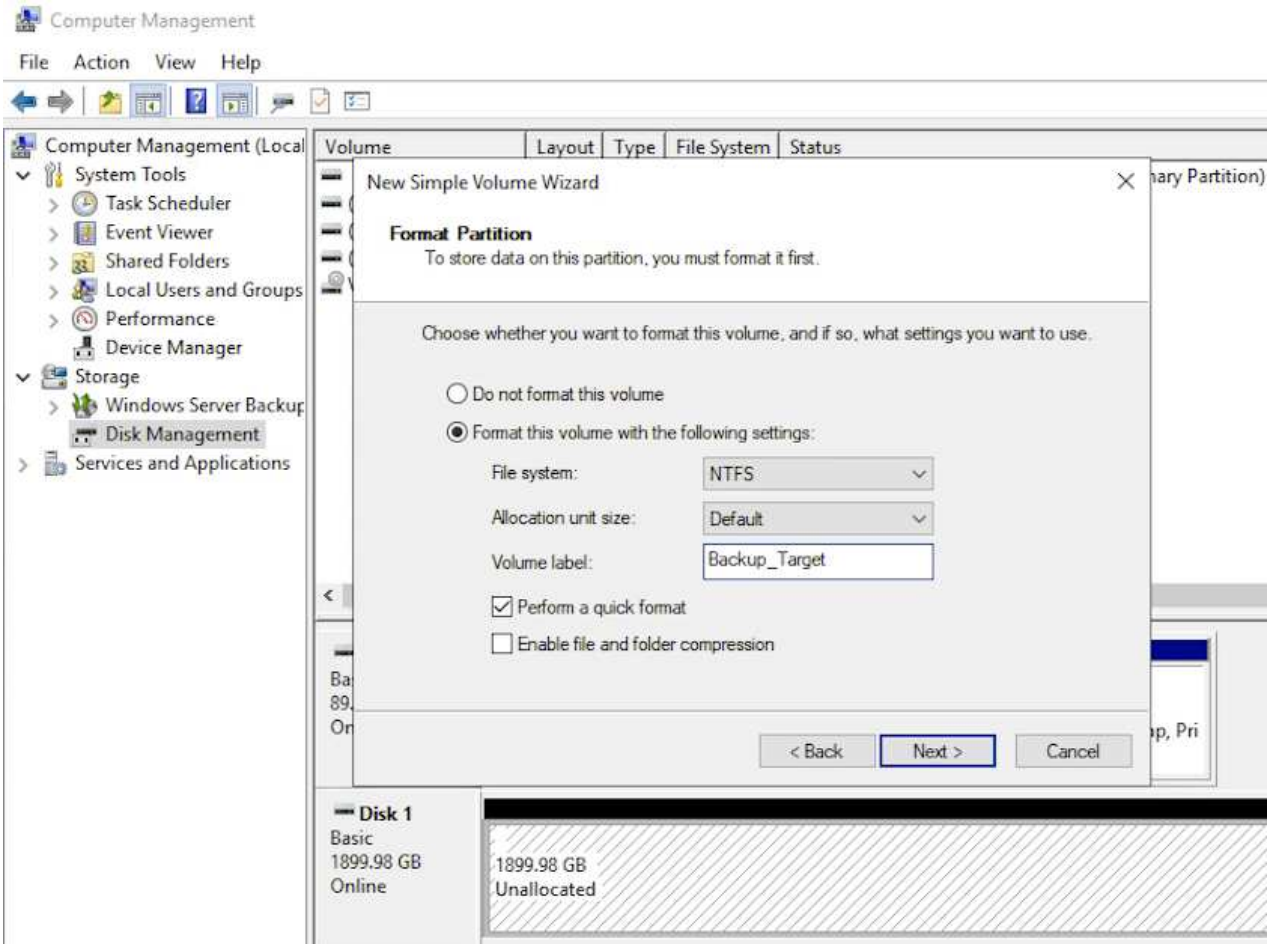
5. Per montare i LUN iSCSI, accedere a Veeam Backup & Replication Server e aprire iSCSI Initiator Properties. Accedere alla scheda **Discover** e inserire l'indirizzo IP di destinazione iSCSI.



6. Nella scheda **targets**, evidenziare il LUN inattivo e fare clic su **Connect**. Selezionare la casella **Enable multi-path** (attiva percorso multiplo) e fare clic su **OK** per connettersi al LUN.



7. Nell'utility Disk Management inizializza il nuovo LUN e crea un volume con il nome e la lettera del disco desiderati. Selezionare la casella **Enable multi-path** (attiva percorso multiplo) e fare clic su **OK** per connettersi al LUN.

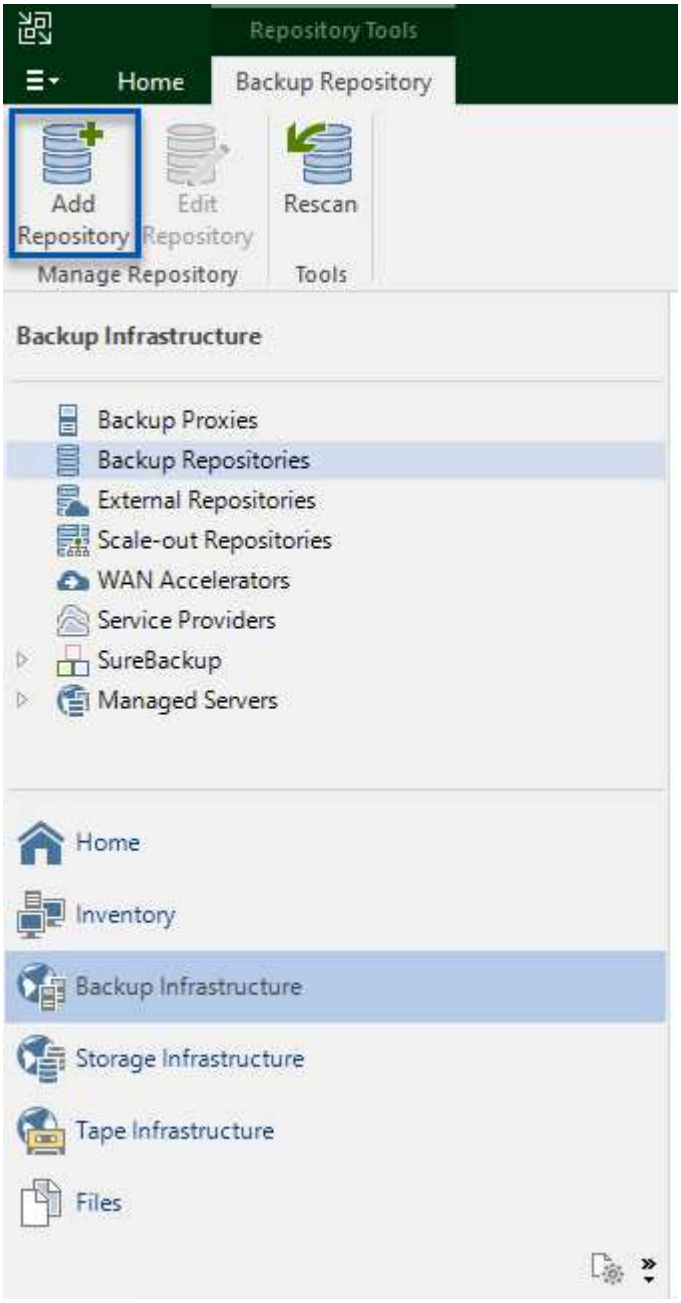


8. Ripetere questa procedura per montare i volumi iSCSI sul server Veeam Proxy.

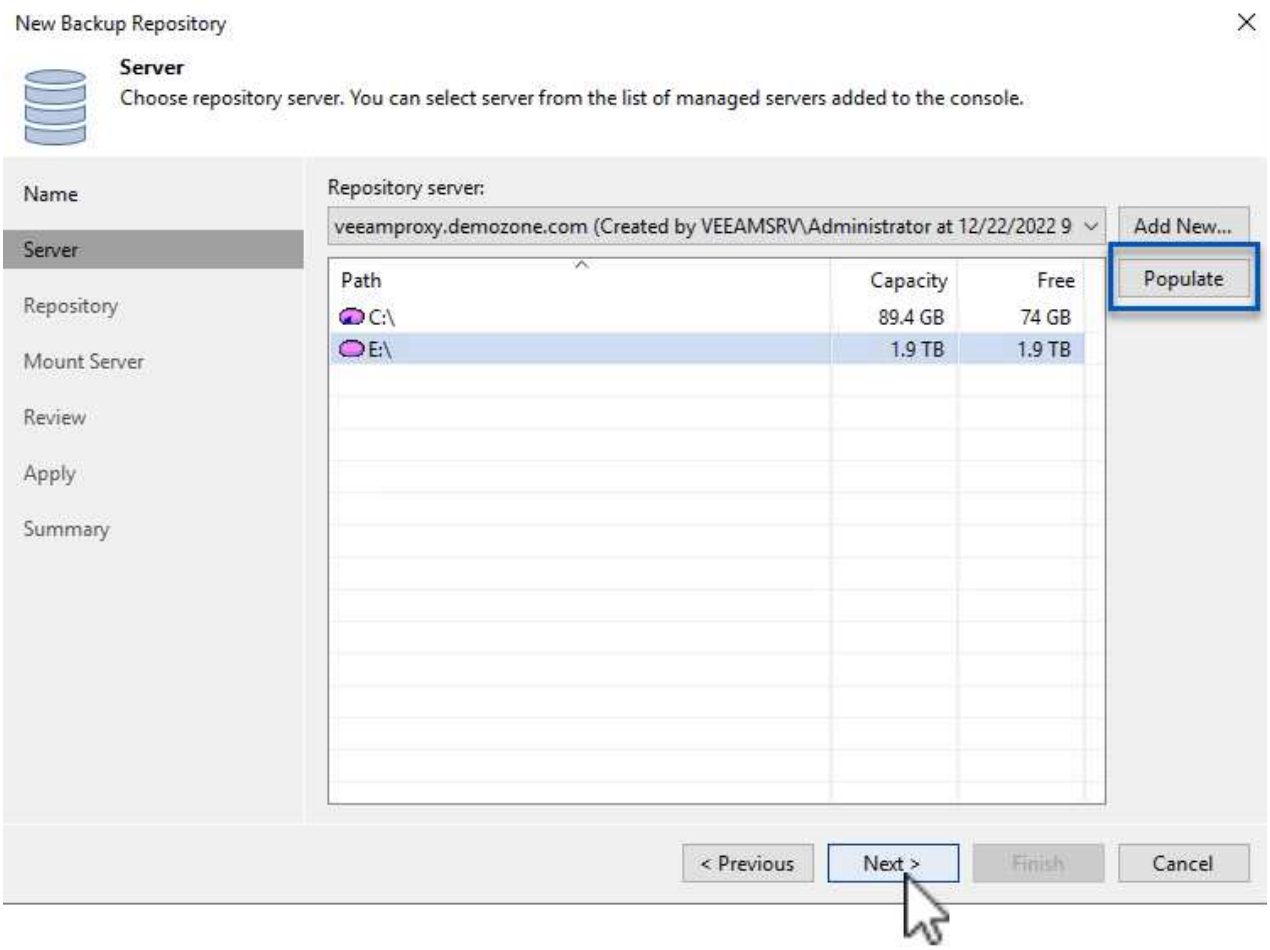
Creare repository di backup Veeam

Nella console di backup e replica di Veeam, creare repository di backup per i server Veeam Backup e Veeam Proxy. Questi repository verranno utilizzati come destinazioni di backup per i backup delle macchine virtuali.

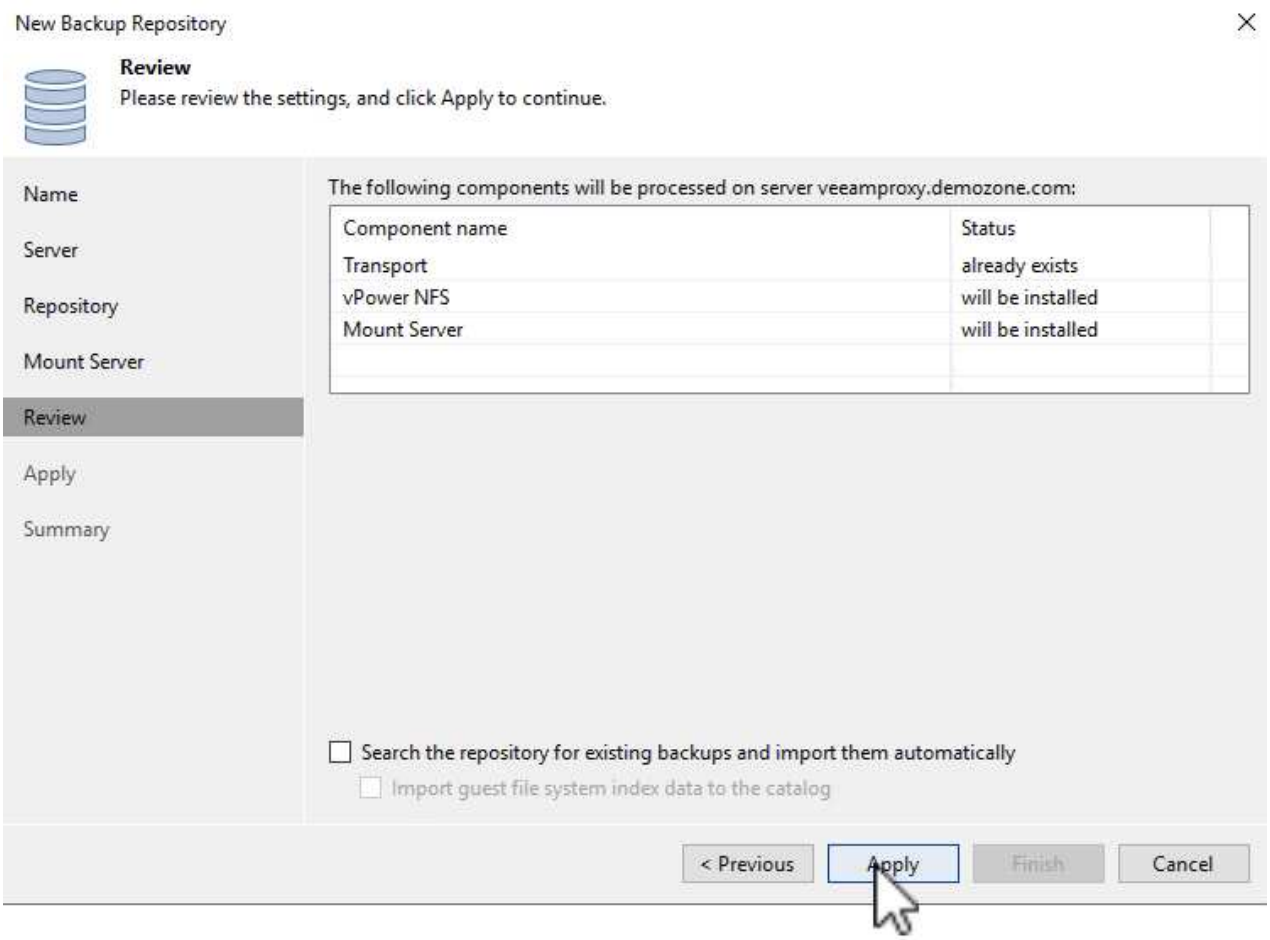
1. Nella console di backup e replica di Veeam, fare clic su **Backup Infrastructure** in basso a sinistra, quindi selezionare **Add Repository**



2. Nella procedura guidata nuovo repository di backup, immettere un nome per il repository, quindi selezionare il server dall'elenco a discesa e fare clic sul pulsante **popola** per scegliere il volume NTFS da utilizzare.



3. Nella pagina successiva, scegliere un server Mount che verrà utilizzato per montare i backup quando si eseguono ripristini avanzati. Per impostazione predefinita, si tratta dello stesso server a cui è collegato lo storage del repository.
4. Esaminare le selezioni e fare clic su **Apply** (Applica) per avviare la creazione del repository di backup.



5. Ripetere questa procedura per tutti i server proxy aggiuntivi.

Configurare i processi di backup Veeam

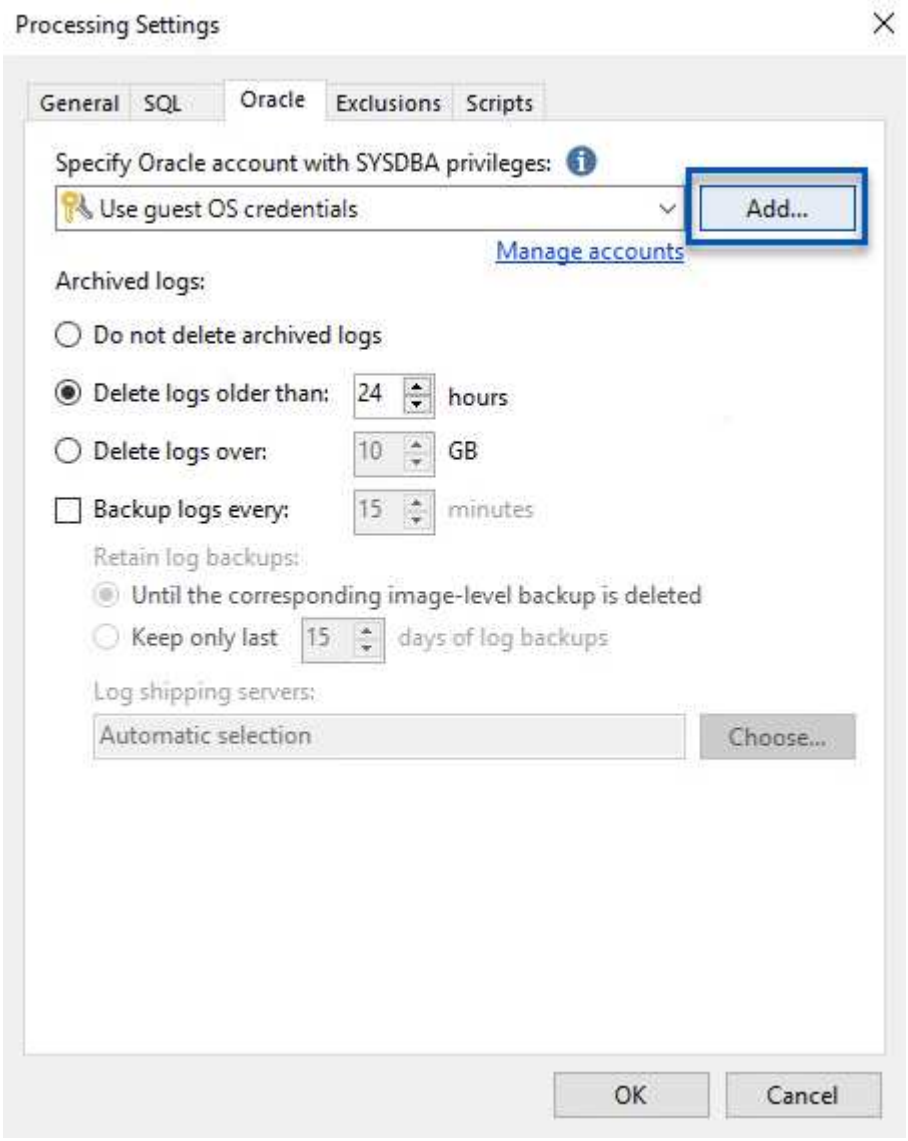
I processi di backup devono essere creati utilizzando i repository di backup nella sezione precedente. La creazione di processi di backup è una parte normale del repertorio di qualsiasi amministratore dello storage e non vengono descritte tutte le fasi qui descritte. Per informazioni più complete sulla creazione di processi di backup in Veeam, vedere "Documentazione tecnica del Centro assistenza Veeam".

In questa soluzione sono stati creati processi di backup separati per:

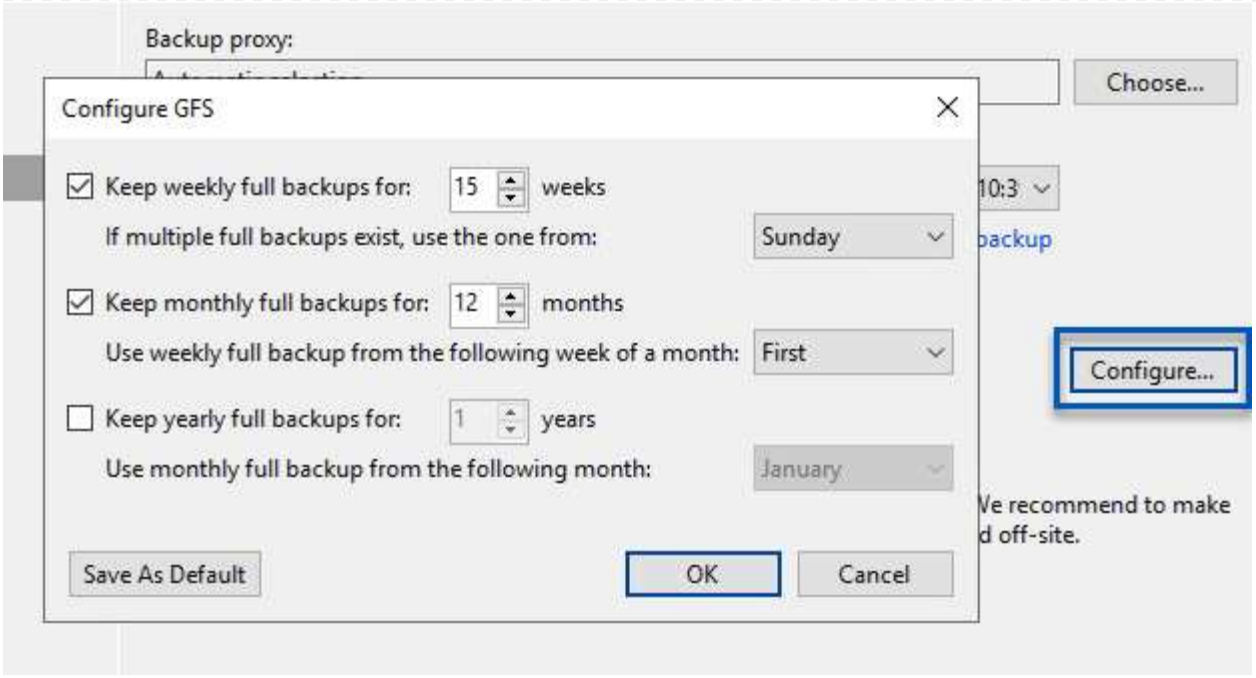
- Microsoft Windows SQL Server
- Server di database Oracle
- File server Windows
- File server Linux

Considerazioni generali per la configurazione dei processi di backup Veeam

1. Abilitare l'elaborazione basata sulle applicazioni per creare backup coerenti ed eseguire l'elaborazione del log delle transazioni.
2. Dopo aver abilitato l'elaborazione in base all'applicazione, aggiungere le credenziali corrette con privilegi di amministratore all'applicazione, poiché potrebbero essere diverse dalle credenziali del sistema operativo guest.



3. Per gestire il criterio di conservazione per il backup, selezionare **Mantieni alcuni backup completi più a lungo per scopi di archiviazione** e fare clic sul pulsante **Configura…** per configurare il criterio.



Ripristinare le macchine virtuali applicative con il ripristino completo di Veeam

Eseguire un ripristino completo con Veeam è il primo passo per eseguire un ripristino dell'applicazione. Abbiamo validato che i ripristini completi delle nostre macchine virtuali erano accesi e tutti i servizi funzionavano normalmente.

Il ripristino dei server è una parte normale del repertorio di qualsiasi amministratore dello storage e non vengono descritte tutte le fasi qui descritte. Per informazioni più complete sull'esecuzione di ripristini completi in Veeam, consultare la "Documentazione tecnica del Centro assistenza Veeam".

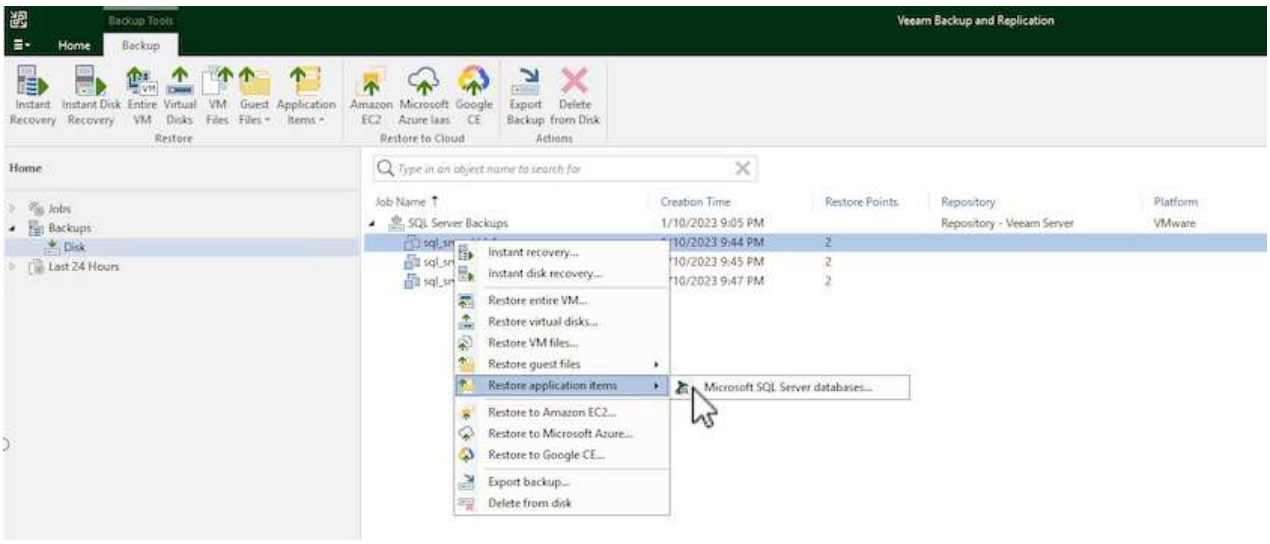
Ripristinare i database di SQL Server

Veeam Backup & Replication offre diverse opzioni per il ripristino dei database di SQL Server. Per questa convalida abbiamo utilizzato Veeam Explorer per SQL Server con Instant Recovery per eseguire ripristini dei database SQL Server. SQL Server Instant Recovery è una funzionalità che consente di ripristinare rapidamente i database di SQL Server senza dover attendere il ripristino completo del database. Questo rapido processo di recovery riduce al minimo i downtime e garantisce la continuità del business. Ecco come funziona:

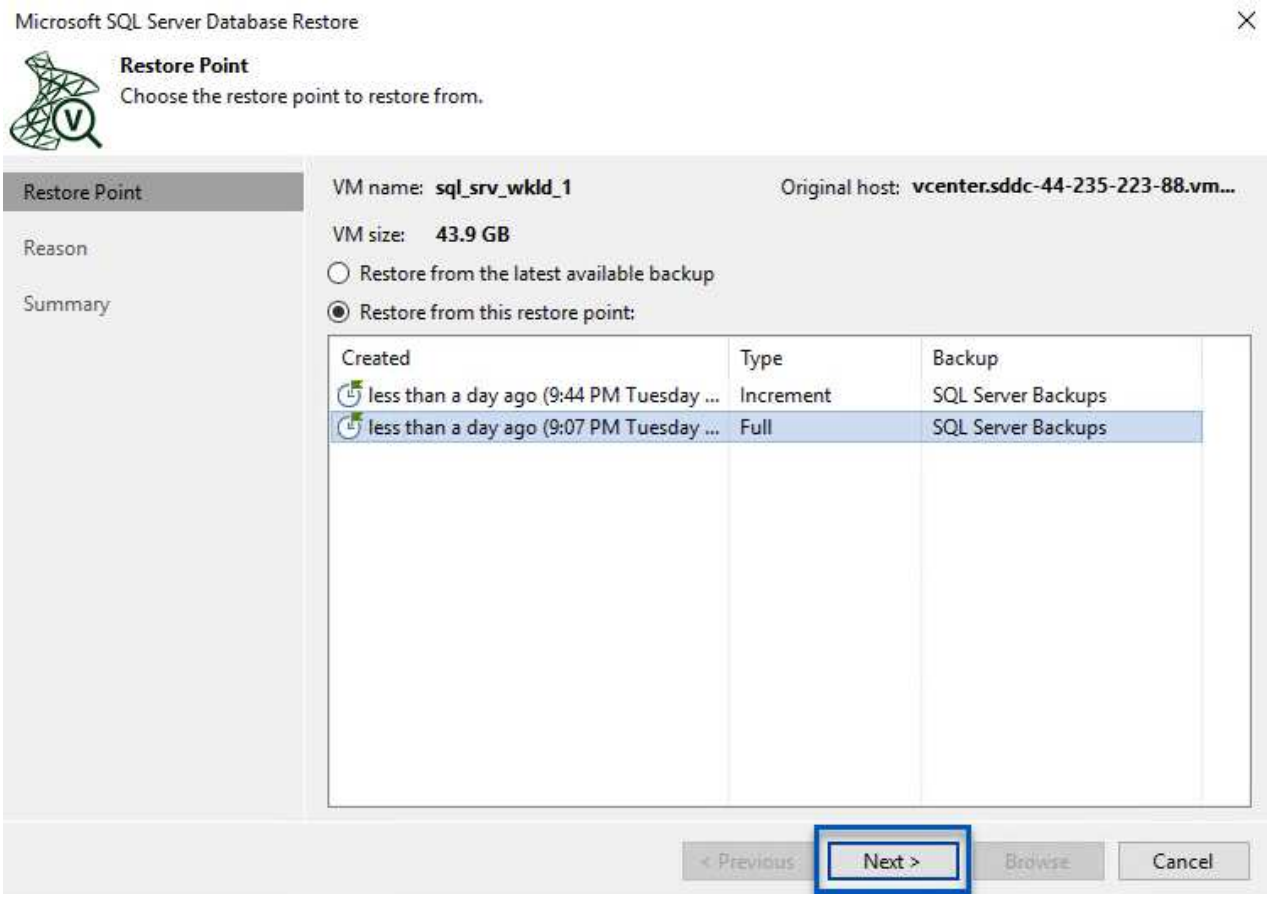
- Veeeam Explorer **monta il backup** contenente il database SQL Server da ripristinare.
- Il software **pubblica il database** direttamente dai file montati, rendendolo accessibile come database temporaneo sull'istanza di SQL Server di destinazione.
- Mentre il database temporaneo è in uso, Veeam Explorer **reindirizza le query utente** a questo database, garantendo che gli utenti possano continuare ad accedere e lavorare con i dati.
- In background, Veeam **esegue un ripristino completo del database**, trasferendo i dati dal database temporaneo alla posizione originale del database.
- Una volta completato il ripristino completo del database, Veeam Explorer **riporta le query dell'utente al database originale** e rimuove il database temporaneo.

Ripristinare il database SQL Server con Veeam Explorer Instant Recovery

1. Nella console di backup e replica di Veeam, accedere all'elenco dei backup di SQL Server, fare clic con il pulsante destro del mouse su un server e selezionare **Restore application ITEMS** (Ripristina elementi dell'applicazione), quindi **Microsoft SQL Server Databases…** (Database Microsoft SQL Server…).

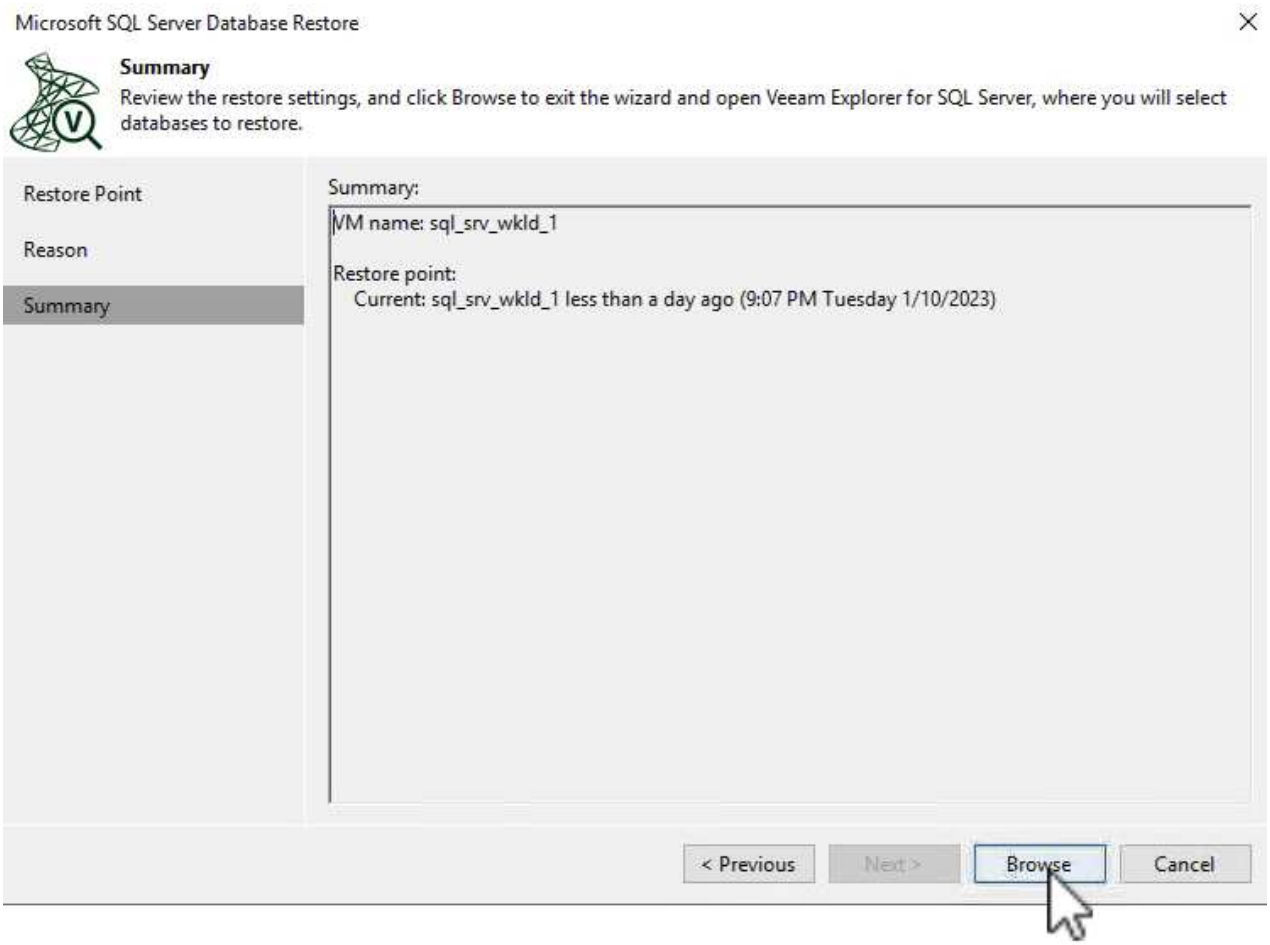


2. Nella finestra Ripristino guidato database di Microsoft SQL Server, selezionare un punto di ripristino dall'elenco e fare clic su **Avanti**.

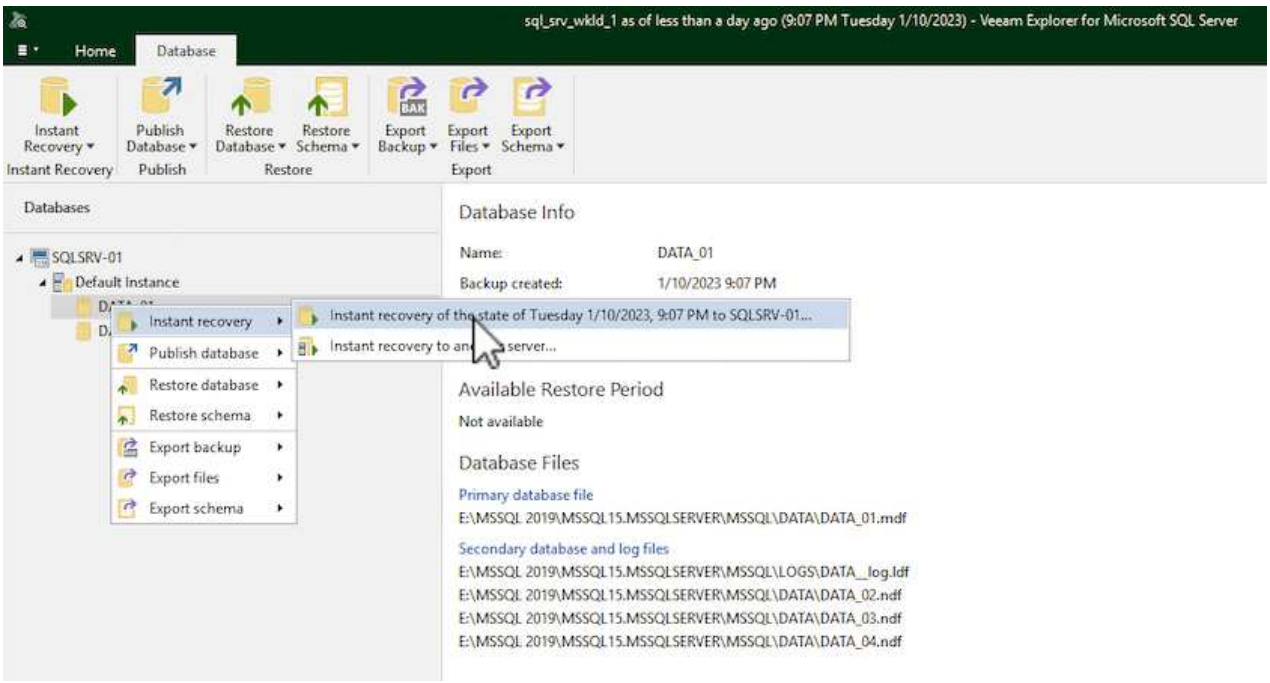


3. Inserire un valore di **Restore Reason** (motivo ripristino), se desiderato, quindi, nella pagina Summary

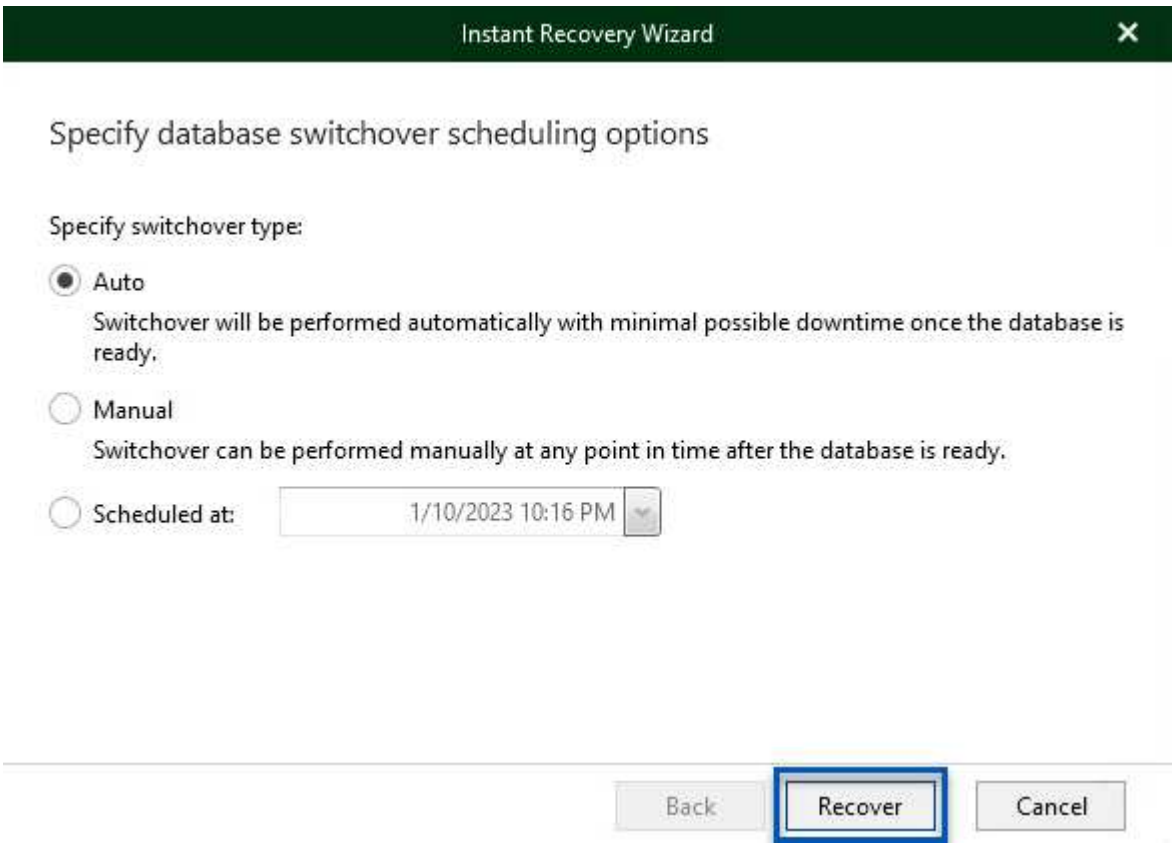
(Riepilogo), fare clic sul pulsante **Browse** (Sfoglia) per avviare Veeam Explorer per Microsoft SQL Server.



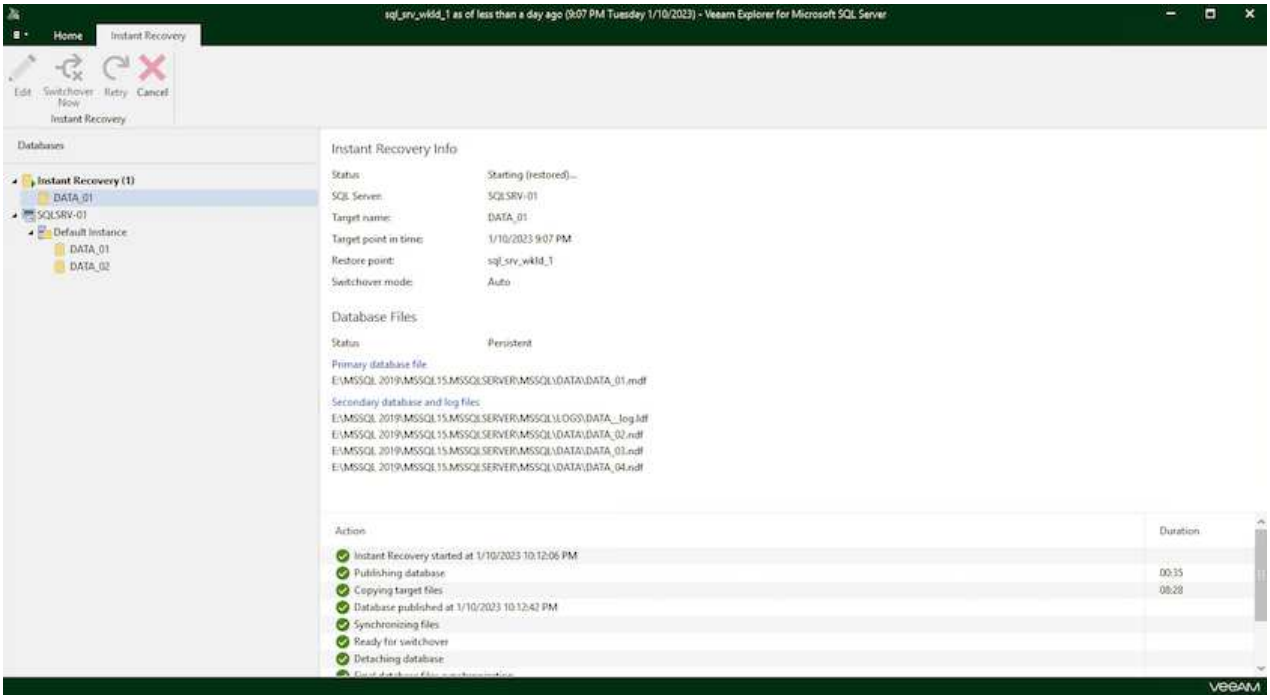
4. In Veeam Explorer espandere l'elenco delle istanze di database, fare clic con il pulsante destro del mouse e selezionare **Instant Recovery**, quindi il punto di ripristino specifico su cui eseguire il ripristino.



5. Nella procedura guidata di ripristino istantaneo, specificare il tipo di switchover. Questo può avvenire automaticamente con tempi di inattività minimi, manualmente o in un momento specifico. Quindi fare clic sul pulsante **Recover** (Ripristina) per avviare il processo di ripristino.



6. Il processo di ripristino può essere monitorato da Veeam Explorer.



Per informazioni più dettagliate sull'esecuzione delle operazioni di ripristino di SQL Server con Veeam

Explorer, consultare la sezione Microsoft SQL Server nella "Guida utente di Veeeam Explorers".

Ripristinare i database Oracle con Veeam Explorer

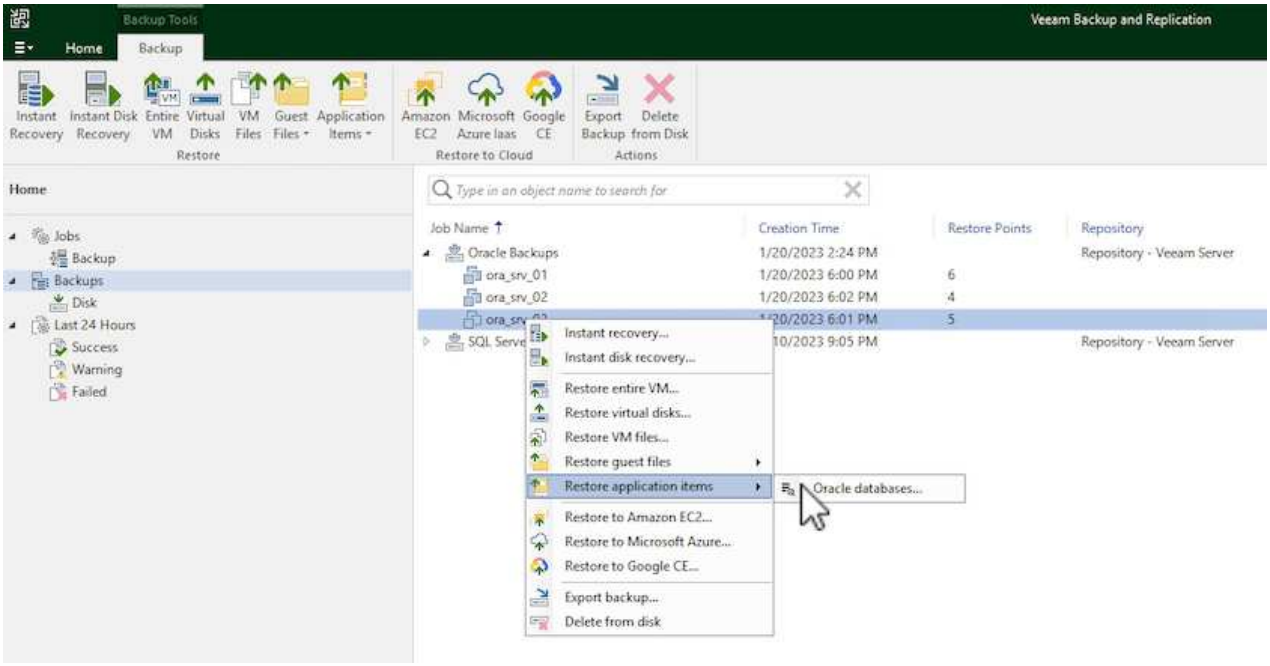
Veeeam Explorer per database Oracle offre la possibilità di eseguire un ripristino standard del database Oracle o un ripristino ininterrotto utilizzando Instant Recovery. Supporta inoltre la pubblicazione di database per un accesso rapido, il ripristino dei database Data Guard e i ripristini dai backup RMAN.

Per informazioni più dettagliate sull'esecuzione delle operazioni di ripristino del database Oracle con Veeam Explorer, fare riferimento alla sezione Oracle nella "Guida utente di Veeeam Explorers".

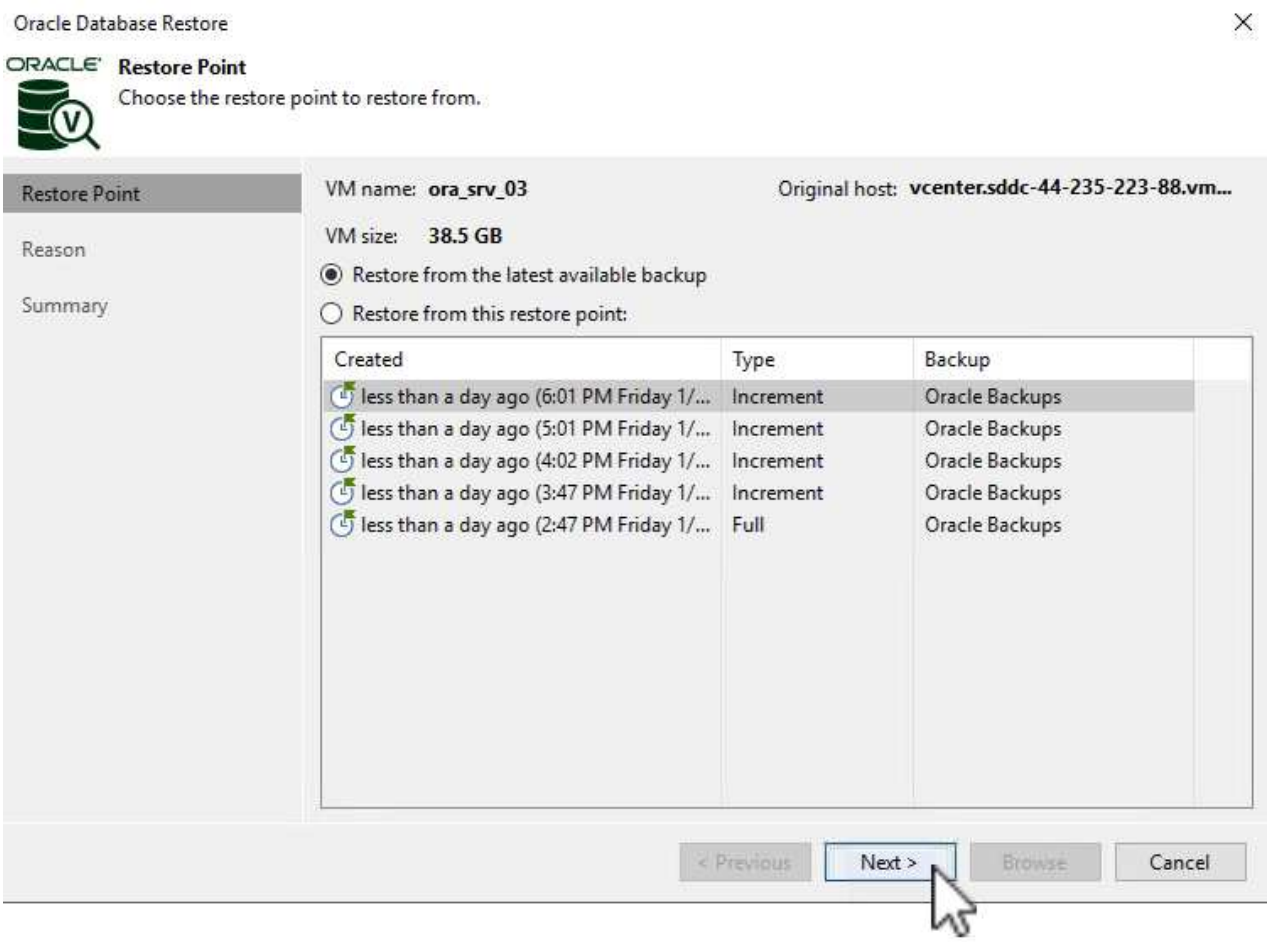
Ripristinare il database Oracle con Veeam Explorer

In questa sezione viene descritto un ripristino del database Oracle su un server diverso utilizzando Veeam Explorer.

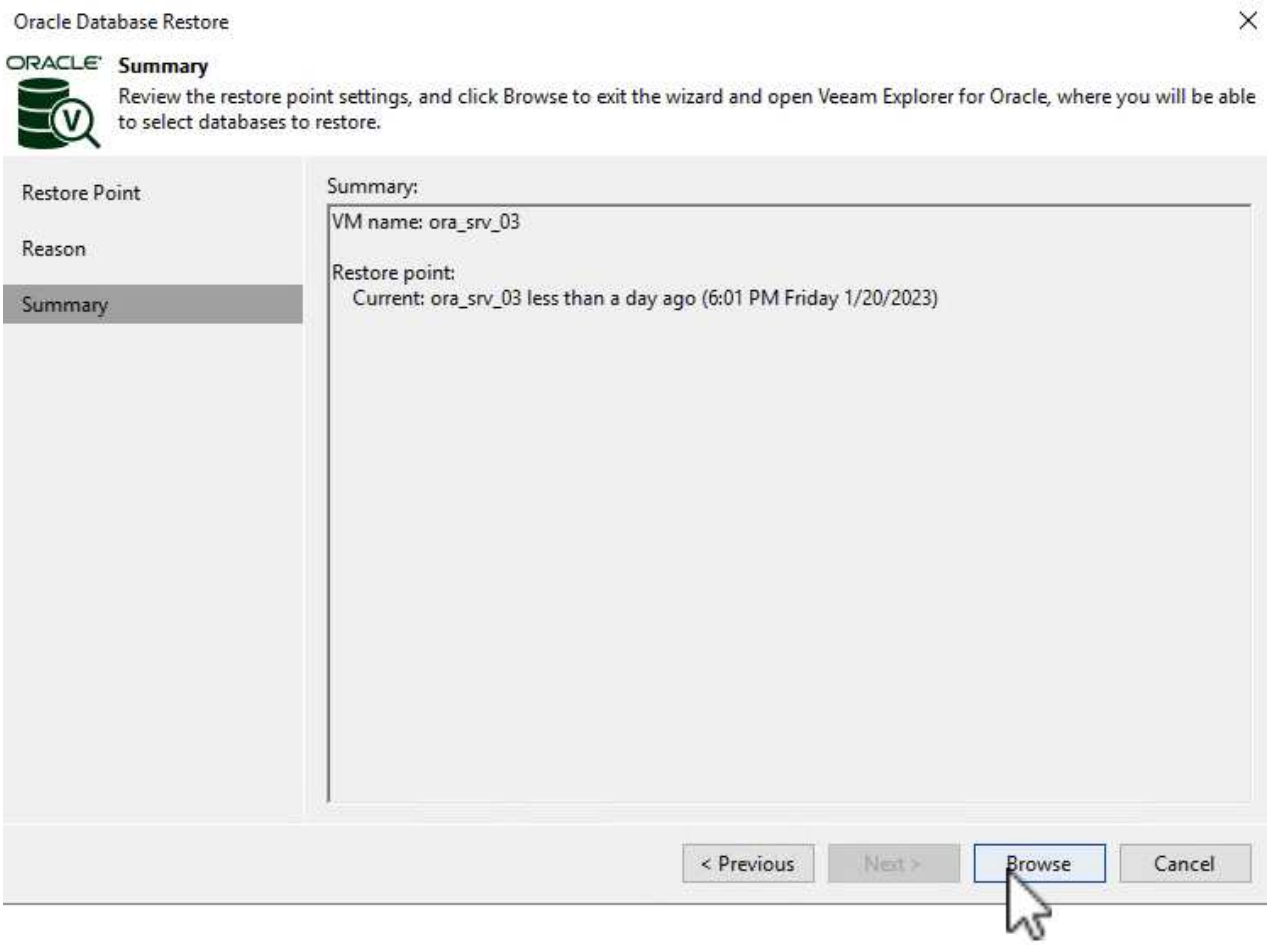
1. Nella console di backup e replica di Veeam, accedere all'elenco dei backup Oracle, fare clic con il pulsante destro del mouse su un server e selezionare **Restore application ITEMS** (Ripristina elementi dell'applicazione), quindi **Oracle Databases…** (Database Oracle…*).



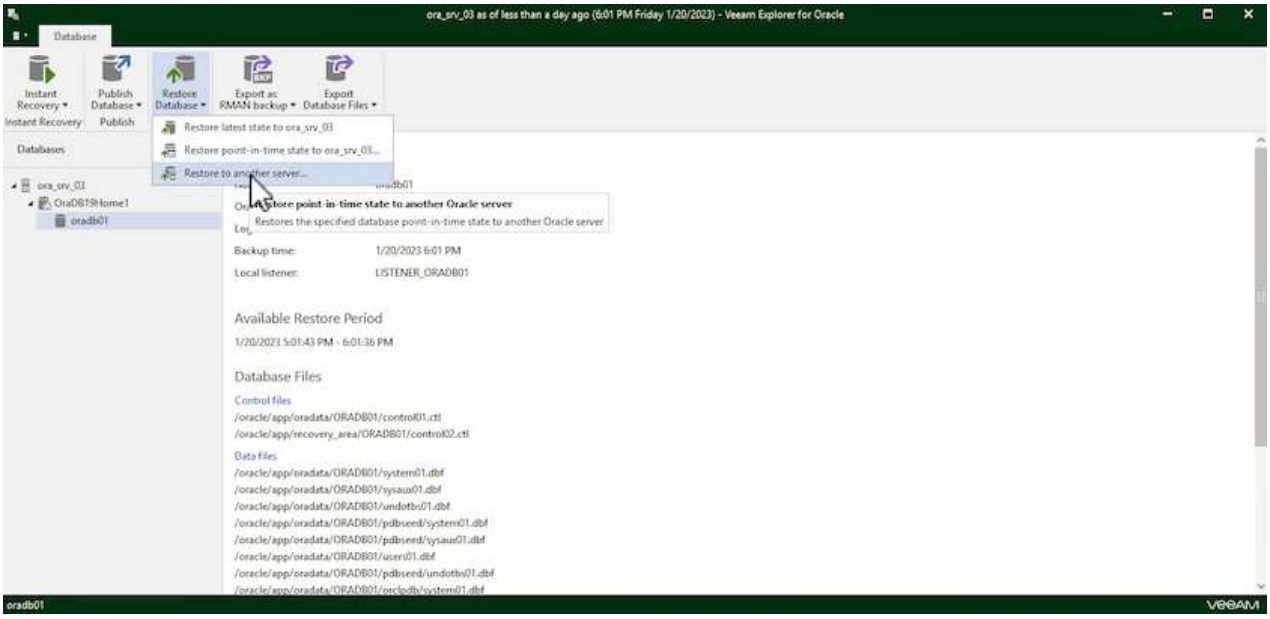
2. In Oracle Database Restore Wizard (Ripristino guidato database Oracle), selezionare un punto di ripristino dall'elenco e fare clic su **Next** (Avanti).



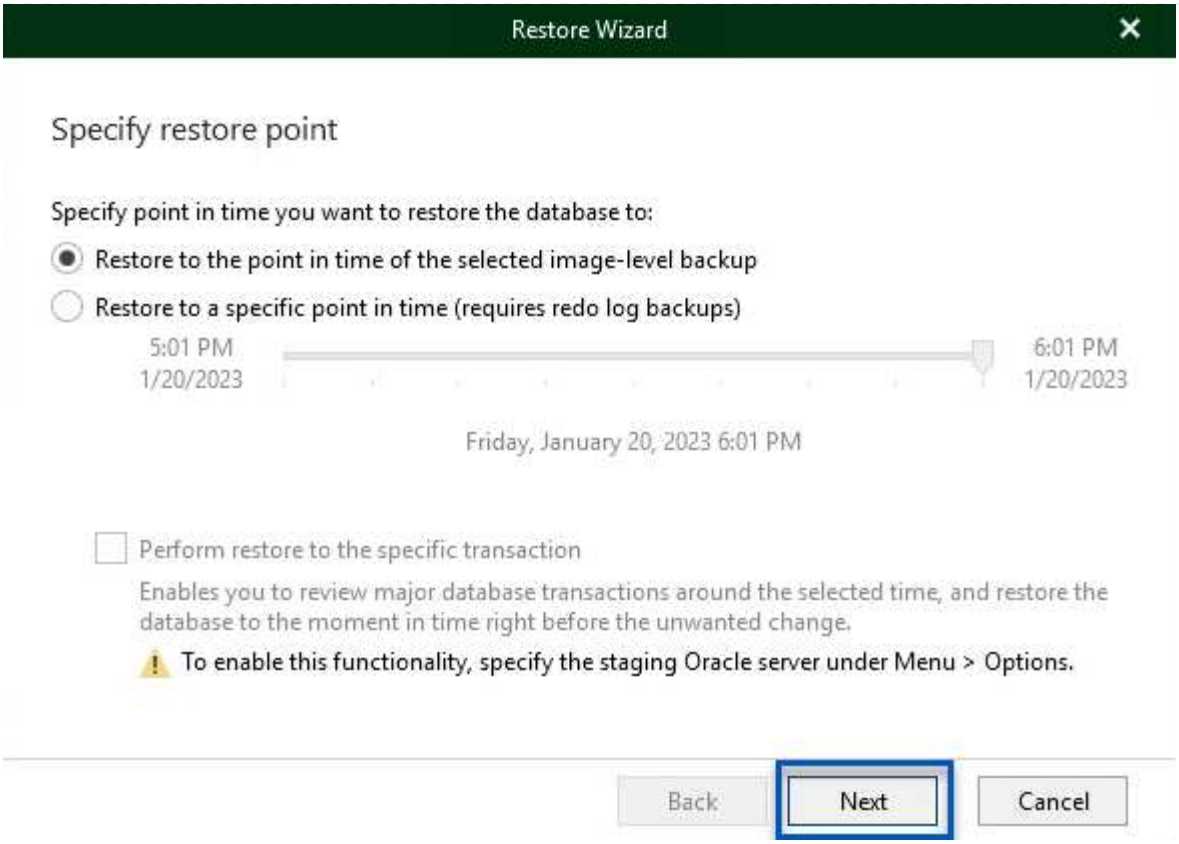
3. Inserire un **Restore Reason** (motivo ripristino), se desiderato, quindi, nella pagina Summary (Riepilogo), fare clic sul pulsante **Browse** (Sfoglia) per avviare Veeam Explorer per Oracle.



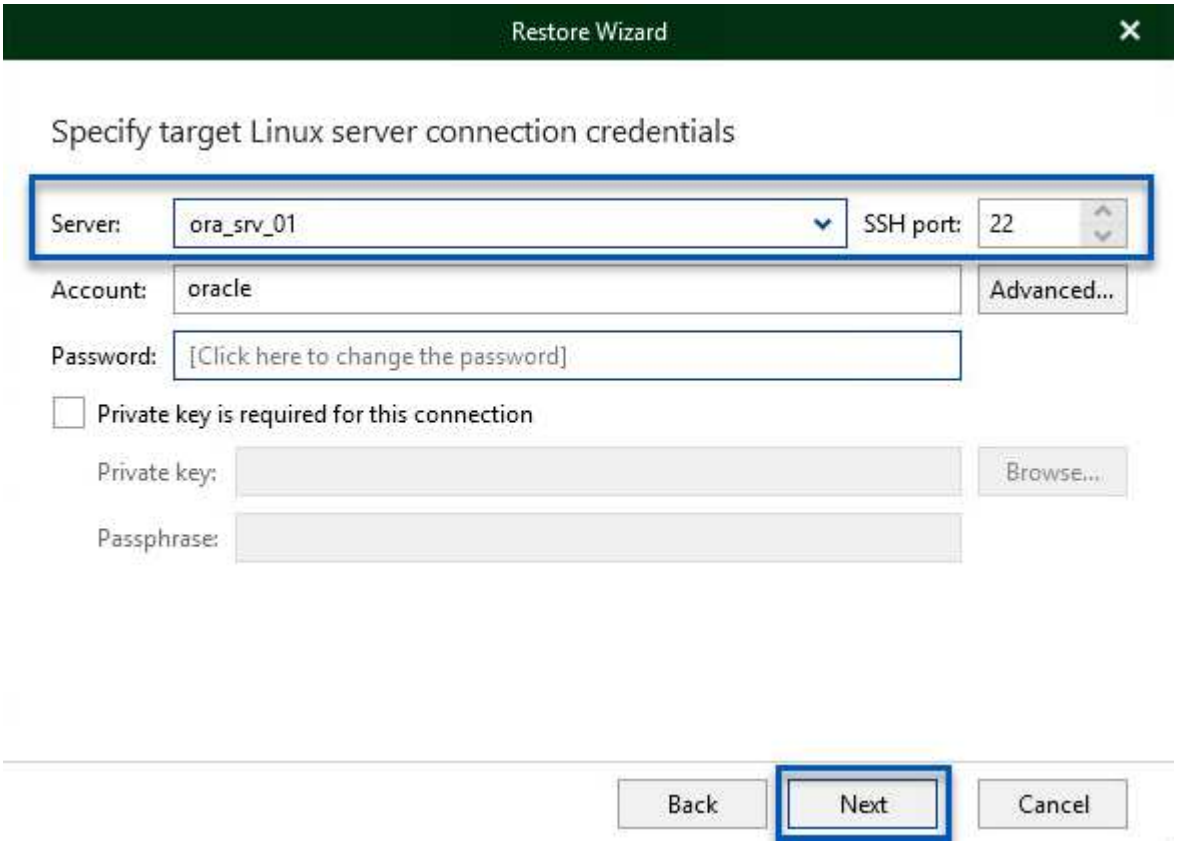
4. In Veeam Explorer espandere l'elenco delle istanze di database, fare clic sul database da ripristinare, quindi selezionare **Ripristina database** dal menu a discesa in alto. Selezionare **Ripristina su un altro server…**.



5. Nella procedura guidata di ripristino, specificare il punto di ripristino da cui eseguire il ripristino e fare clic su **Avanti**.

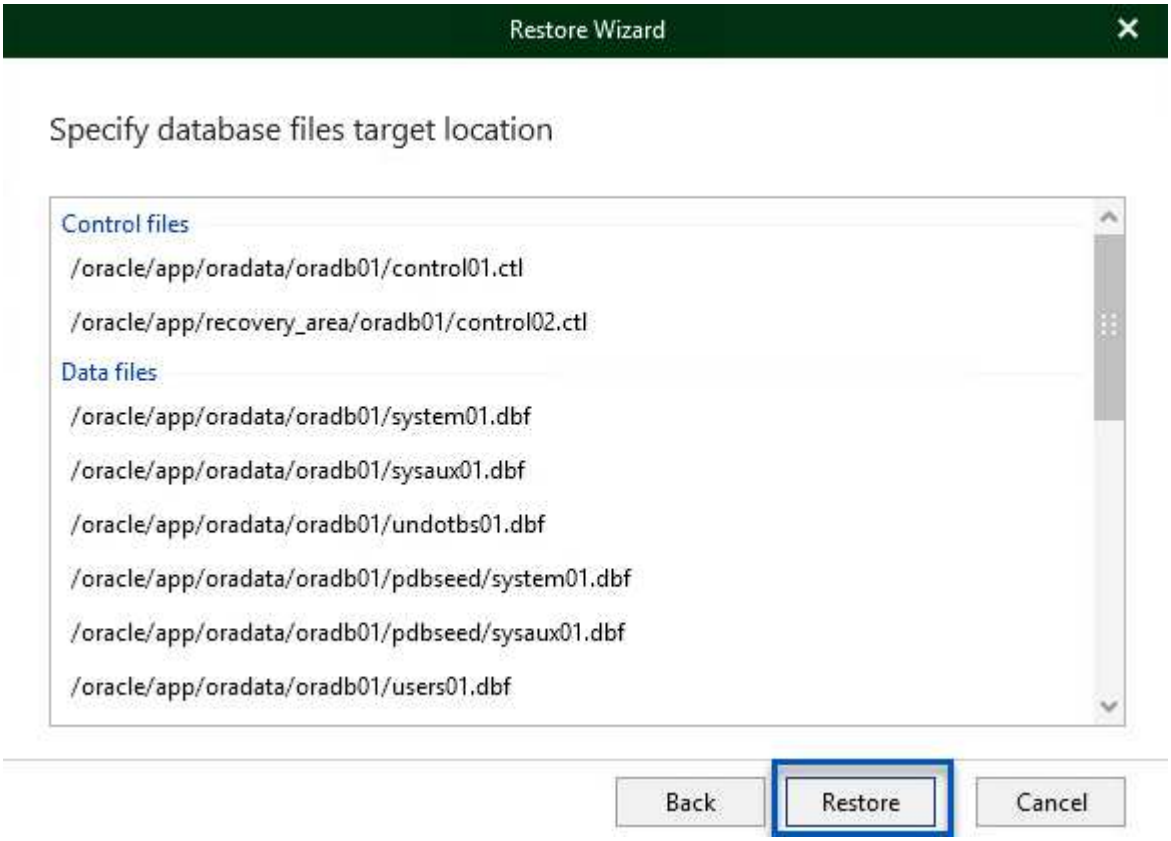


6. Specificare il server di destinazione in cui verrà ripristinato il database e le credenziali dell'account, quindi fare clic su **Avanti**.



7. Infine, specificare il percorso di destinazione dei file di database e fare clic sul pulsante **Restore** per

avviare il processo di ripristino.

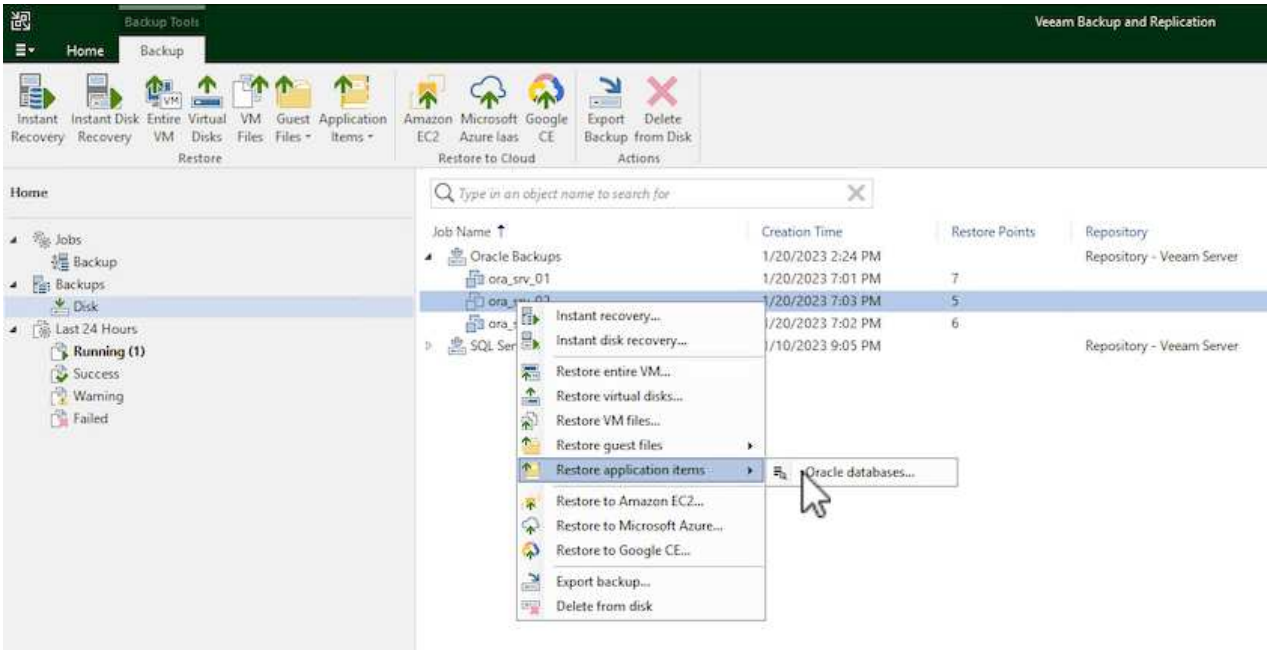


8. Una volta completato il ripristino del database, controllare che il database Oracle venga avviato correttamente sul server.

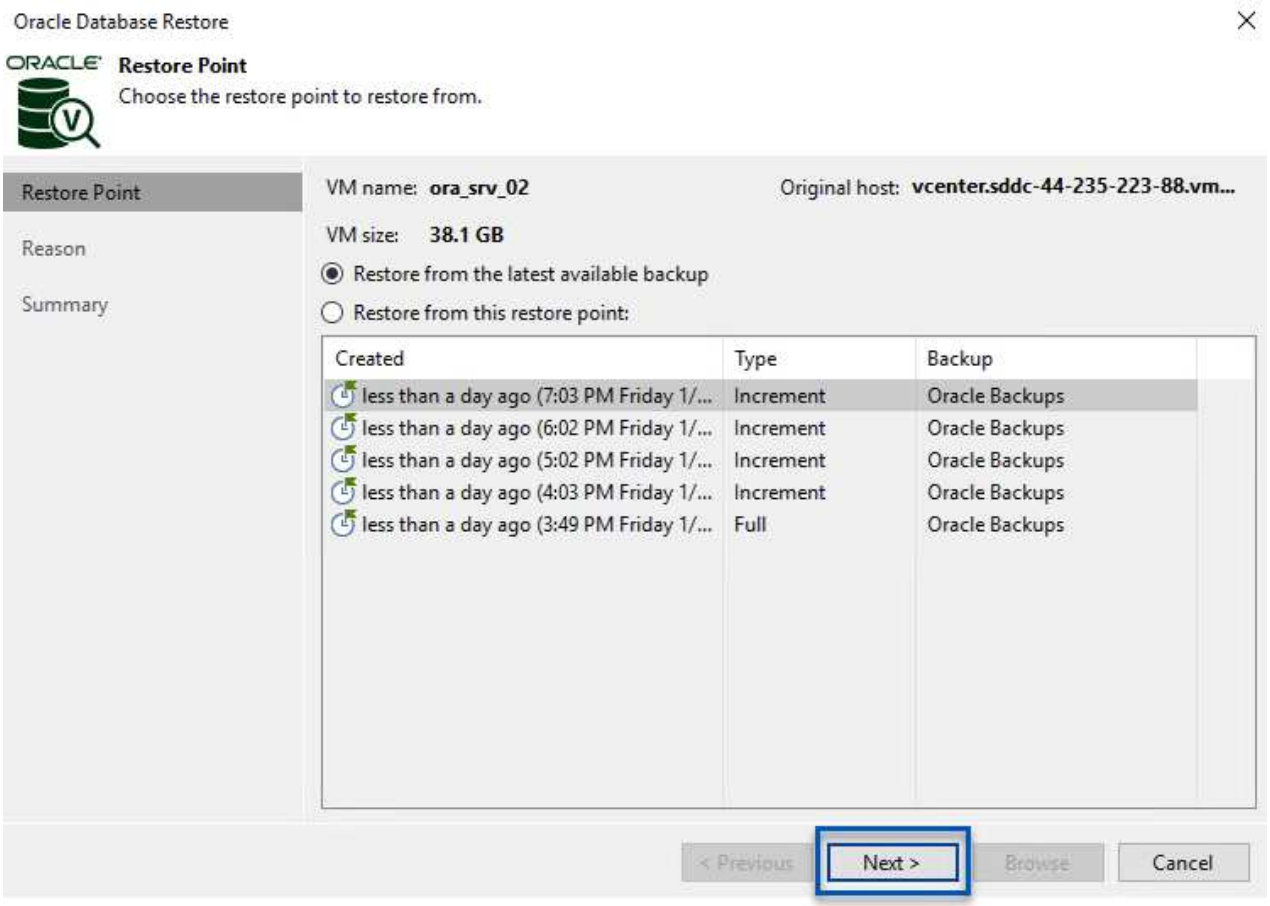
Pubblicare il database Oracle su un server alternativo

In questa sezione viene pubblicato un database su un server alternativo per un accesso rapido senza avviare un ripristino completo.

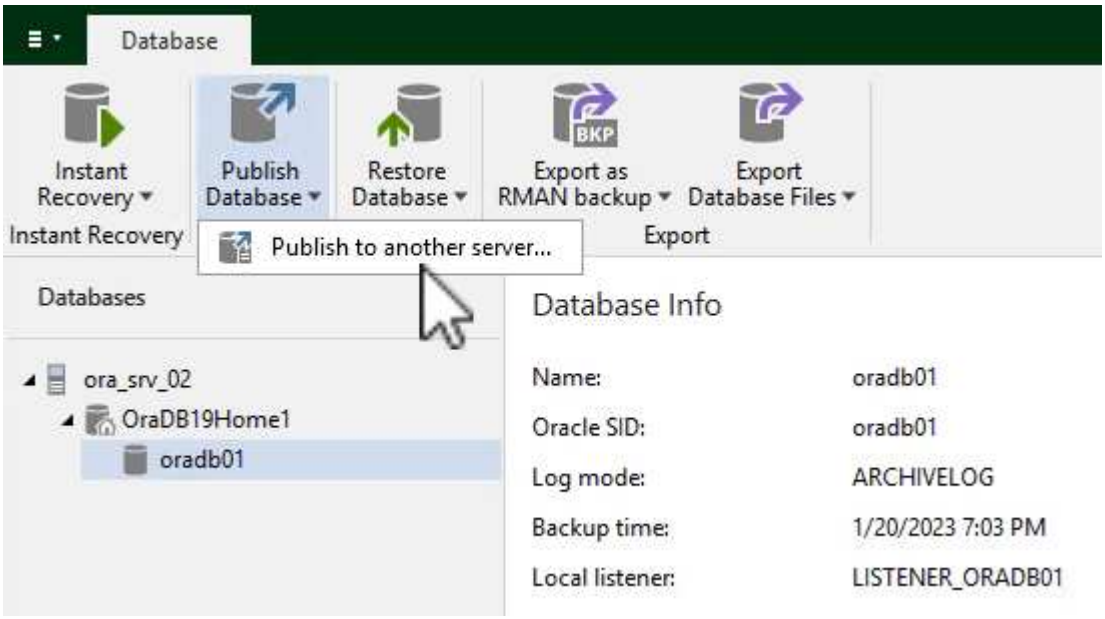
1. Nella console di backup e replica di Veeam, accedere all'elenco dei backup Oracle, fare clic con il pulsante destro del mouse su un server e selezionare **Restore application ITEMS** (Ripristina elementi dell'applicazione), quindi **Oracle Databases…** (Database Oracle…*).



2. In Oracle Database Restore Wizard (Ripristino guidato database Oracle), selezionare un punto di ripristino dall'elenco e fare clic su **Next** (Avanti).

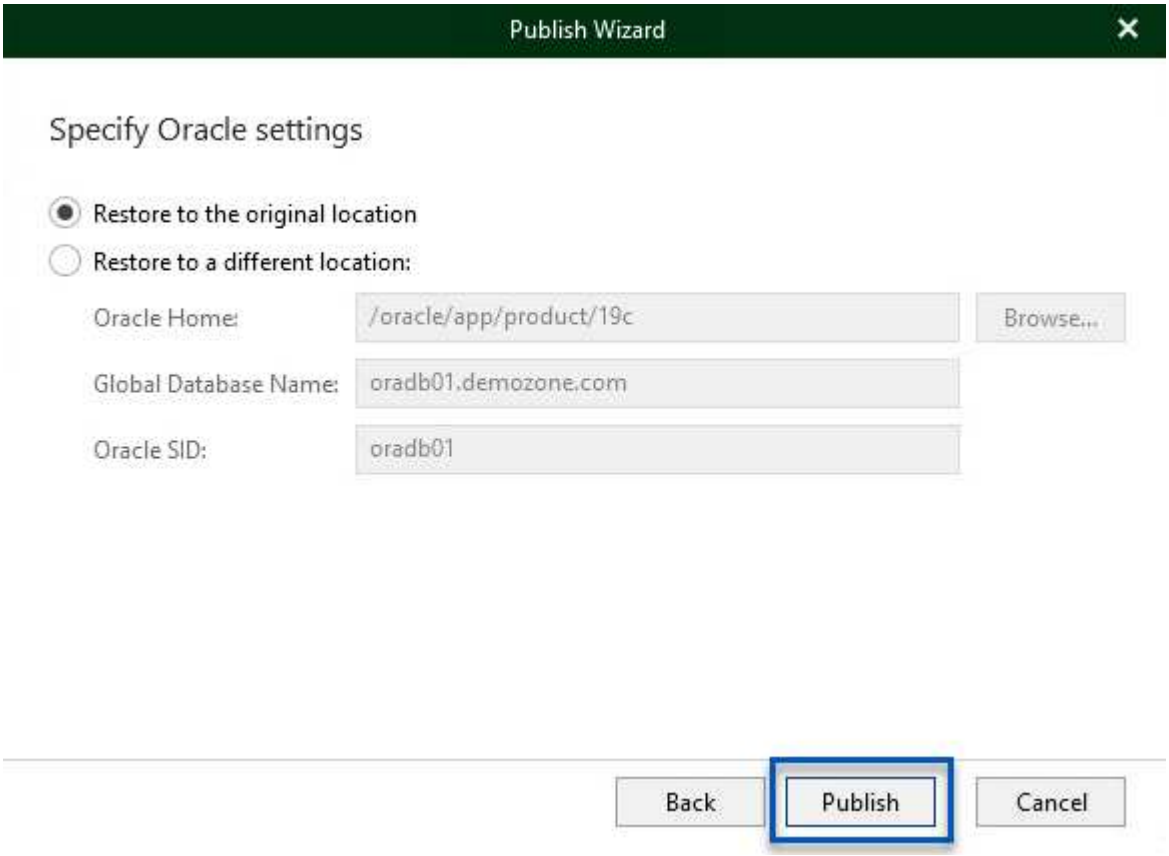


3. Inserire un **Restore Reason** (motivo ripristino), se desiderato, quindi, nella pagina Summary (Riepilogo), fare clic sul pulsante **Browse** (Sfoglia) per avviare Veeam Explorer per Oracle.
4. In Veeam Explorer espandere l'elenco delle istanze di database, fare clic sul database da ripristinare, quindi selezionare **pubblica database** dal menu a discesa in alto, quindi scegliere **pubblica su un altro server…**.



5. Nella Pubblicazione guidata, specificare il punto di ripristino da cui pubblicare il database e fare clic su **Avanti**.

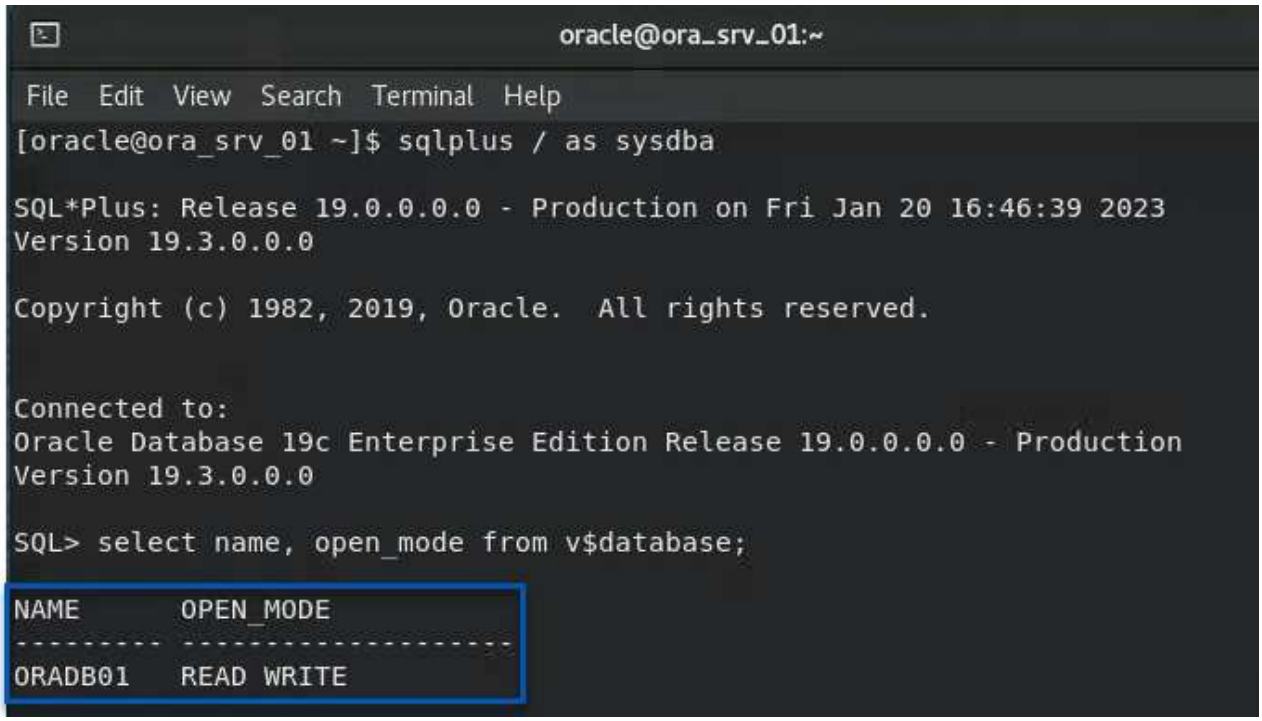
6. Infine, specificare la posizione del file system linux di destinazione e fare clic su **Publish** per avviare il processo di ripristino.



7. Una volta completata la pubblicazione, accedere al server di destinazione ed eseguire i seguenti comandi per assicurarsi che il database sia in esecuzione:

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



Conclusione

VMware Cloud è una potente piattaforma per l'esecuzione di applicazioni business-critical e l'archiviazione di dati sensibili. Una soluzione sicura per la protezione dei dati è essenziale per le aziende che si affidano a VMware Cloud per garantire la continuità del business e contribuire alla protezione dalle minacce informatiche e dalla perdita di dati. Scegliendo una soluzione di protezione dei dati affidabile e solida, le aziende possono essere sicure che i loro dati critici siano sicuri e sicuri, indipendentemente da cosa.

Il caso di utilizzo presentato in questa documentazione si concentra su tecnologie di data Protection comprovate che evidenziano l'integrazione tra NetApp, VMware e Veeeam. FSX per ONTAP è supportato come datastore NFS supplementari per VMware Cloud in AWS e viene utilizzato per tutti i dati delle macchine virtuali e delle applicazioni. Veeam Backup & Replication è una soluzione completa per la protezione dei dati progettata per aiutare le aziende a migliorare, automatizzare e ottimizzare i processi di backup e recovery. Veeam viene utilizzato insieme ai volumi target di backup iSCSI, ospitati su FSX per ONTAP, per fornire una soluzione di protezione dei dati sicura e facile da gestire per i dati applicativi residenti in VMware Cloud.

Ulteriori informazioni

Per ulteriori informazioni sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Guida utente di FSX per ONTAP"
- "Documentazione tecnica del Centro assistenza Veeam"
- "Supporto di VMware Cloud su AWS. Considerazioni e limitazioni"

TR-4955: Disaster recovery con FSX per ONTAP e VMC (AWS VMware Cloud)

Niyaz Mohamed, NetApp

Panoramica

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i carichi di lavoro da interruzioni del sito ed eventi di corruzione dei dati (ad esempio ransomware). Con la tecnologia NetApp SnapMirror, i carichi di lavoro VMware on-premise possono essere replicati su FSX per ONTAP in esecuzione in AWS.

È possibile utilizzare Disaster Recovery Orchestrator (DRO, una soluzione basata su script con interfaccia utente) per ripristinare senza problemi i carichi di lavoro replicati da on-premise a FSX per ONTAP. DRO automatizza il ripristino dal livello SnapMirror, attraverso la registrazione delle macchine virtuali su VMC, fino alle mappature di rete direttamente su NSX-T. Questa funzione è inclusa in tutti gli ambienti VMC.

Per iniziare

Implementare e configurare VMware Cloud su AWS

"VMware Cloud su AWS" Offre un'esperienza nativa del cloud per i carichi di lavoro basati su VMware nell'ecosistema AWS. Ogni VMware Software-Defined Data Center (SDDC) viene eseguito in un Amazon Virtual Private Cloud (VPC) e fornisce uno stack VMware completo (incluso vCenter Server), networking software-defined NSX-T, storage vSAN software-defined e uno o più host ESXi che forniscono risorse di calcolo e storage ai carichi di lavoro. Per configurare un ambiente VMC su AWS, seguire questa procedura "collegamento". È possibile utilizzare anche un cluster di spie pilota per scopi di DR.

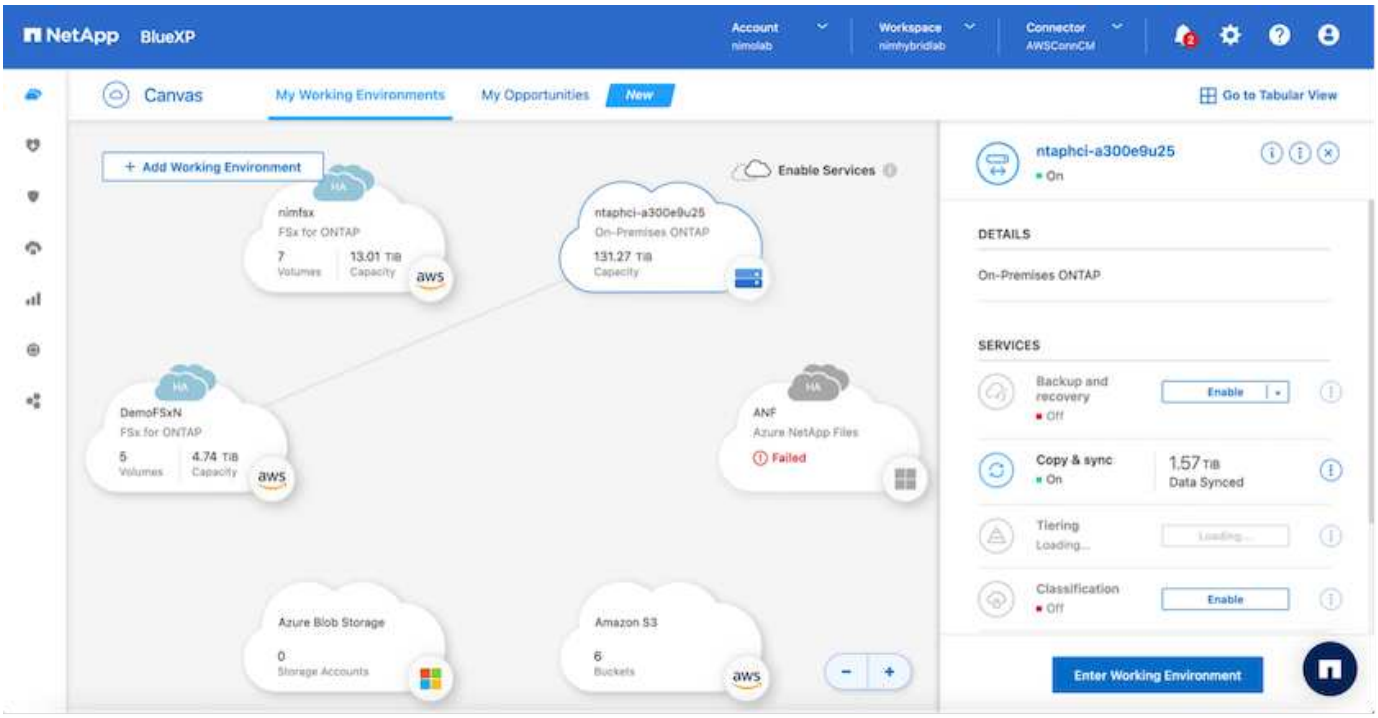
> Nella versione iniziale, DRO supporta un cluster pilota-light esistente. La creazione di SDDC on-demand sarà disponibile in una release imminente.

Provisioning e configurazione di FSX per ONTAP

Amazon FSX per NetApp ONTAP è un servizio completamente gestito che offre un file storage altamente affidabile, scalabile, dalle performance elevate e ricco di funzionalità, basato sul popolare file system ONTAP di NetApp. Seguire questa procedura "collegamento" Per eseguire il provisioning e la configurazione di FSX per ONTAP.

Implementare e configurare SnapMirror in FSX per ONTAP

Il passaggio successivo consiste nell'utilizzare NetApp BlueXP e individuare FSX per ONTAP su istanza AWS e replicare i volumi datastore desiderati da un ambiente on-premise a FSX per ONTAP con la frequenza appropriata e la conservazione delle copie Snapshot di NetApp:



Seguire la procedura descritta in questo collegamento per configurare BlueXP. È inoltre possibile utilizzare l'interfaccia utente di NetApp ONTAP per pianificare la replica seguendo questo collegamento.

Una relazione SnapMirror è un prerequisito e deve essere creata in anticipo.

Installazione DRO

Per iniziare a utilizzare DRO, utilizzare il sistema operativo Ubuntu su un'istanza EC2 o una macchina virtuale designata per assicurarsi di soddisfare i prerequisiti. Quindi installare il pacchetto.

Prerequisiti

- Assicurarsi che sia presente la connettività con i sistemi vCenter e storage di origine e di destinazione.
- Se si utilizzano i nomi DNS, la risoluzione DNS deve essere effettiva. In caso contrario, utilizzare gli indirizzi IP per vCenter e sistemi storage.
- Creare un utente con permessi root. È anche possibile utilizzare sudo con un'istanza EC2.

Requisiti del sistema operativo

- Ubuntu 20.04 (LTS) con almeno 2 GB e 4 vCPU
- I seguenti pacchetti devono essere installati sulla macchina virtuale dell'agente designata:
  - Docker
  - Docker-Componi
  - JQ

Modificare le autorizzazioni su `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.

Il `deploy.sh` lo script esegue tutti i prerequisiti richiesti.

Installare il pacchetto

1. Scaricare il pacchetto di installazione sulla macchina virtuale designata:

```
git clone https://github.com/NetApp/DRO-AWS.git
```

   L'agente può essere installato on-premise o all'interno di un VPC AWS.

2. Decomprimere il pacchetto, eseguire lo script di implementazione e immettere l'IP host (ad esempio, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Accedere alla directory ed eseguire lo script di distribuzione come segue:

```
sudo sh deploy.sh
```

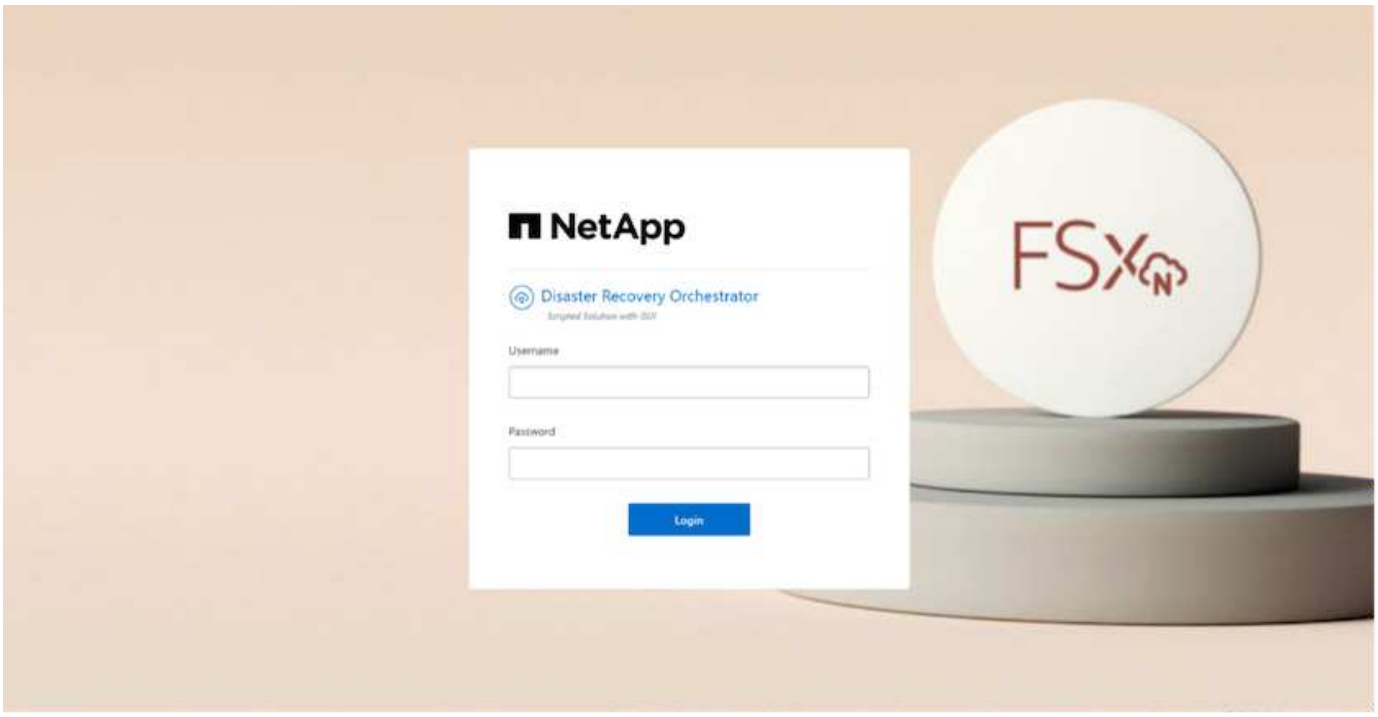
4. Accedere all'interfaccia utente utilizzando:

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

   con le seguenti credenziali predefinite:

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

   La password può essere modificata utilizzando l'opzione "Change Password" (Modifica password).



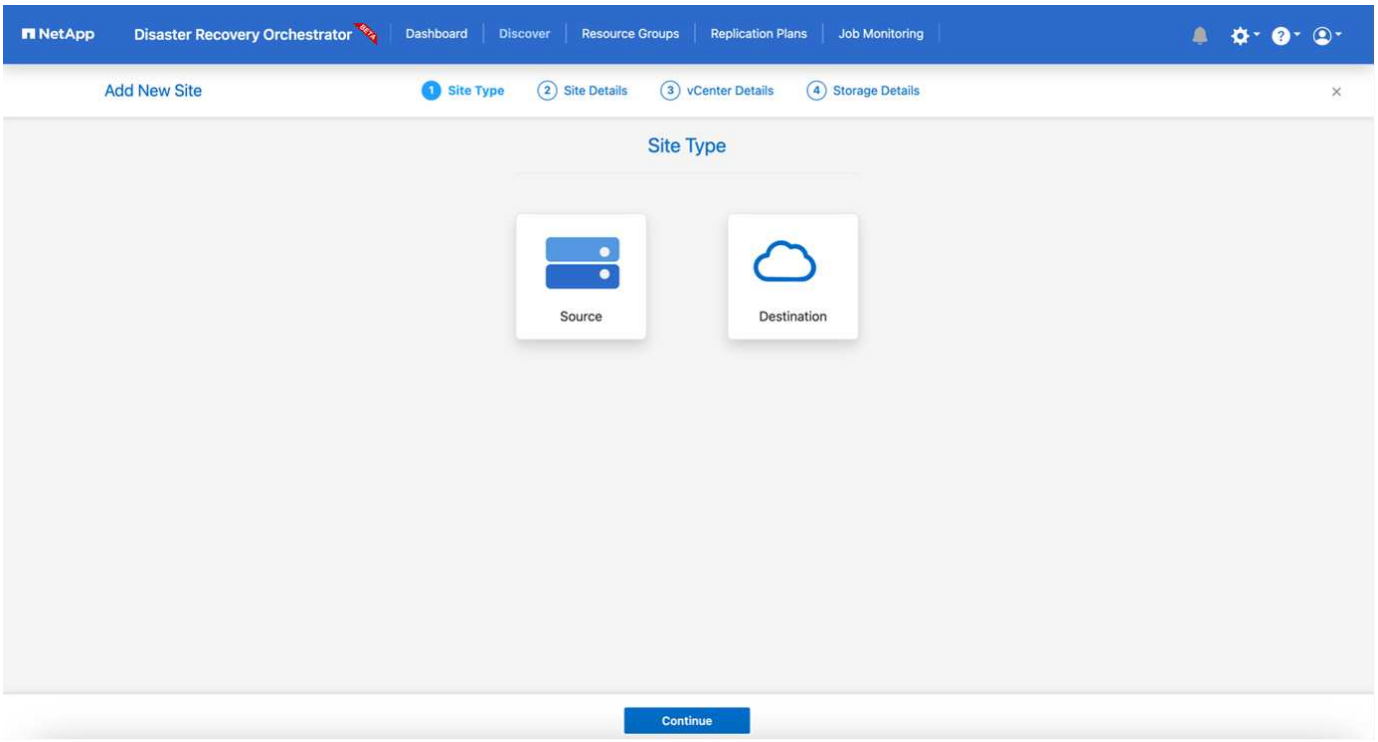
Configurazione DRO

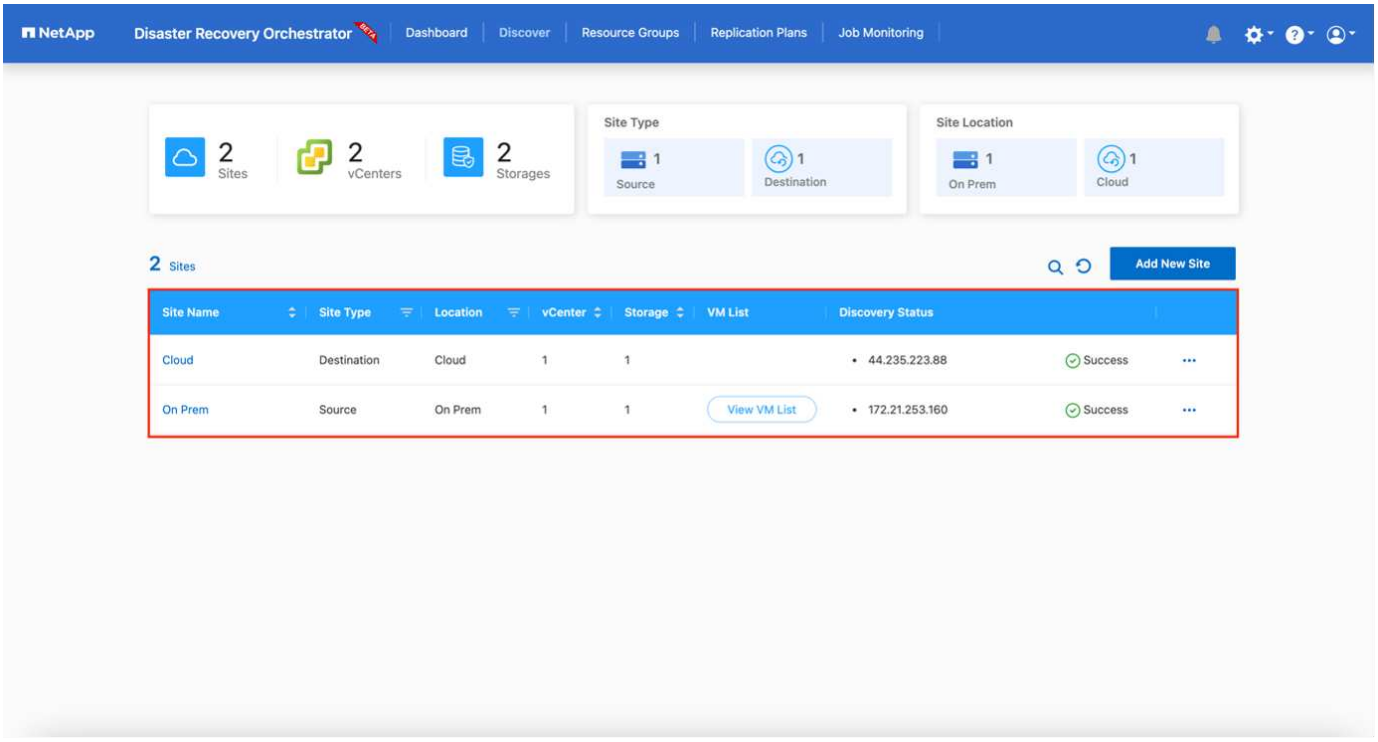
Dopo aver configurato correttamente FSX per ONTAP e VMC, è possibile iniziare a configurare DRO per automatizzare il ripristino dei carichi di lavoro on-premise su VMC utilizzando le copie SnapMirror di sola lettura su FSX per ONTAP.

NetApp consiglia di implementare l'agente DRO in AWS e anche sullo stesso VPC in cui viene implementato FSX per ONTAP (può anche essere collegato in modo peer), In modo che l'agente DRO possa comunicare attraverso la rete con i componenti on-premise e con le risorse FSX per ONTAP e VMC.

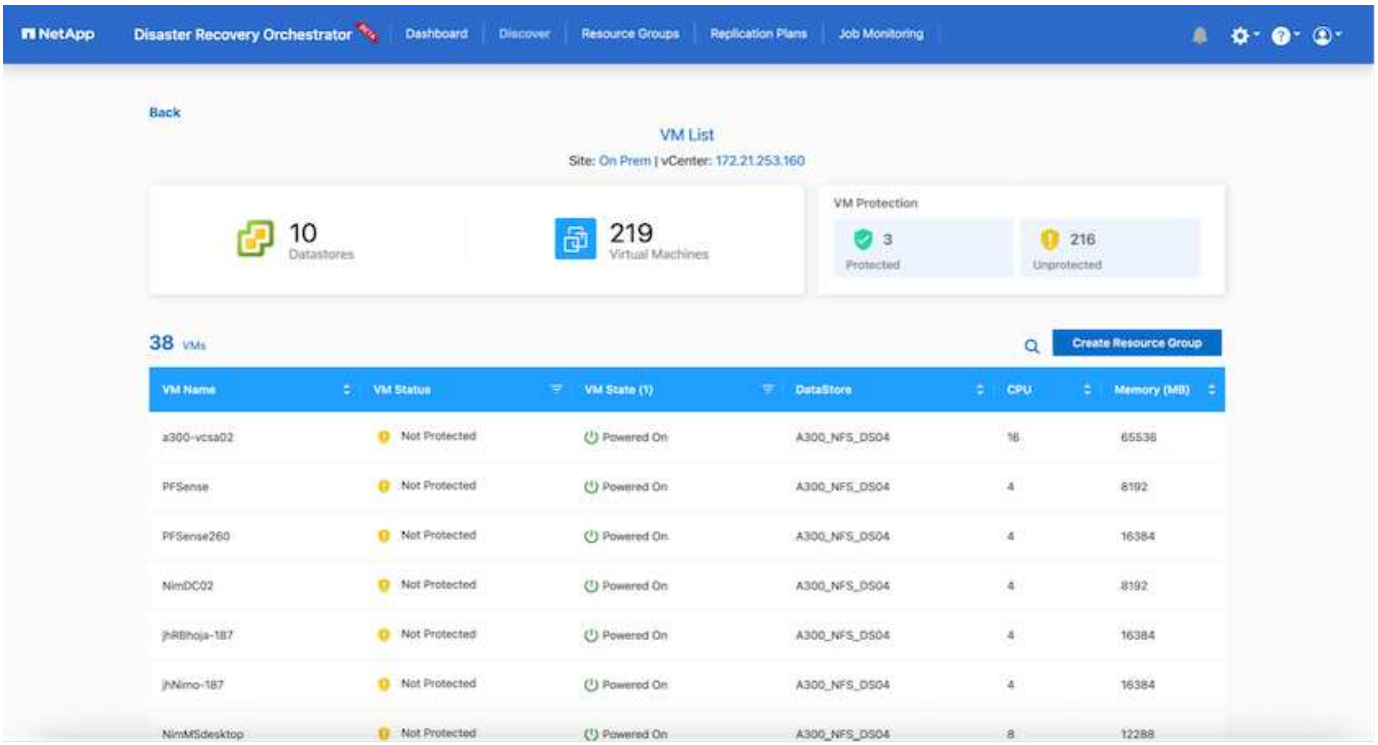
Il primo passo è scoprire e aggiungere le risorse on-premise e cloud (vCenter e storage) a DRO. Aprire DRO in un browser supportato e utilizzare il nome utente e la password predefiniti (admin/admin) e Add Sites (Aggiungi siti). I siti possono essere aggiunti anche utilizzando l'opzione Discover. Aggiungere le seguenti piattaforme:

- On-premise
  - VCenter on-premise
  - Sistema storage ONTAP
- Cloud
  - VMC vCenter
  - FSX per ONTAP





Una volta aggiunto, DRO esegue il rilevamento automatico e visualizza le macchine virtuali con le repliche SnapMirror corrispondenti dallo storage di origine a FSX per ONTAP. DRO rileva automaticamente le reti e i portgroup utilizzati dalle macchine virtuali e li popola.



Il passaggio successivo consiste nel raggruppare le macchine virtuali richieste in gruppi funzionali che fungono da gruppi di risorse.

Raggruppamenti di risorse

Una volta aggiunte le piattaforme, è possibile raggruppare le macchine virtuali da ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di macchine virtuali dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e validazioni opzionali delle applicazioni che possono essere eseguite al momento del ripristino.

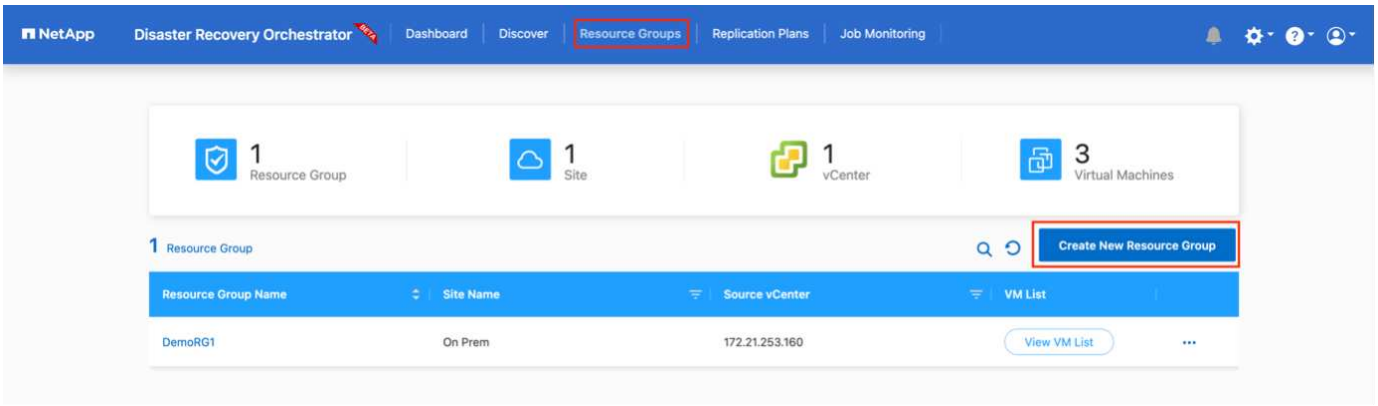
Per iniziare a creare gruppi di risorse, attenersi alla seguente procedura:

1. Accedere a **gruppi di risorse** e fare clic su **Crea nuovo gruppo di risorse**.
2. In **nuovo gruppo di risorse**, selezionare il sito di origine dal menu a discesa e fare clic su **Crea**.
3. Fornire **Dettagli gruppo di risorse** e fare clic su **continua**.
4. Selezionare le macchine virtuali appropriate utilizzando l'opzione di ricerca.
5. Selezionare l'ordine di avvio e il ritardo di avvio (sec) per le macchine virtuali selezionate. Impostare l'ordine della sequenza di accensione selezionando ciascuna macchina virtuale e impostando la relativa priorità. Tre è il valore predefinito per tutte le macchine virtuali.

   Le opzioni sono le seguenti:

   1 – la prima macchina virtuale ad accenderlo 3 – Default 5 – l'ultima macchina virtuale ad accenderlo

6. Fare clic su **Crea gruppo di risorse**.

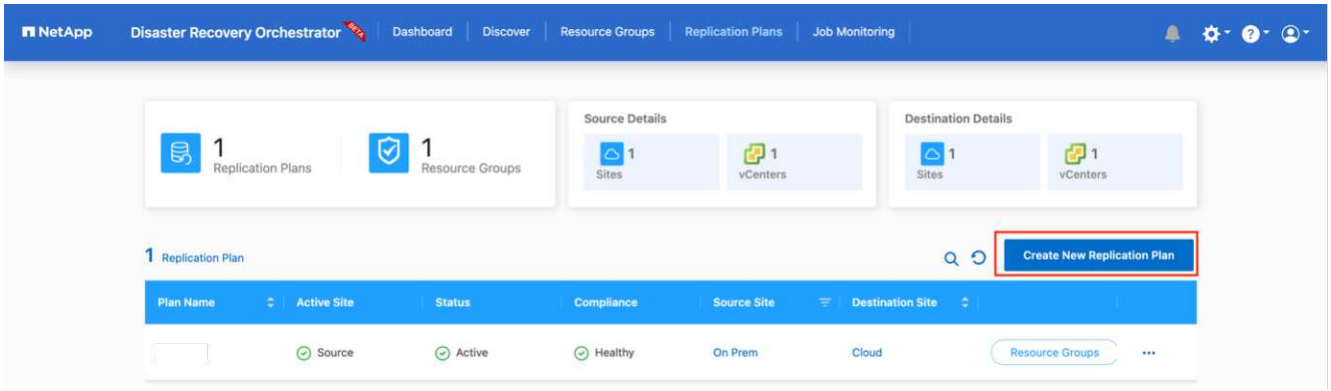


Piani di replica

Hai bisogno di un piano per il ripristino delle applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dall'elenco a discesa e scegliere i gruppi di risorse da includere in questo piano, oltre al raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, Tier-1, Tier-2 e così via). Tali piani sono talvolta chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda **Replication Plan** (piano di replica) e fare clic su **New Replication Plan** (nuovo piano di replica).

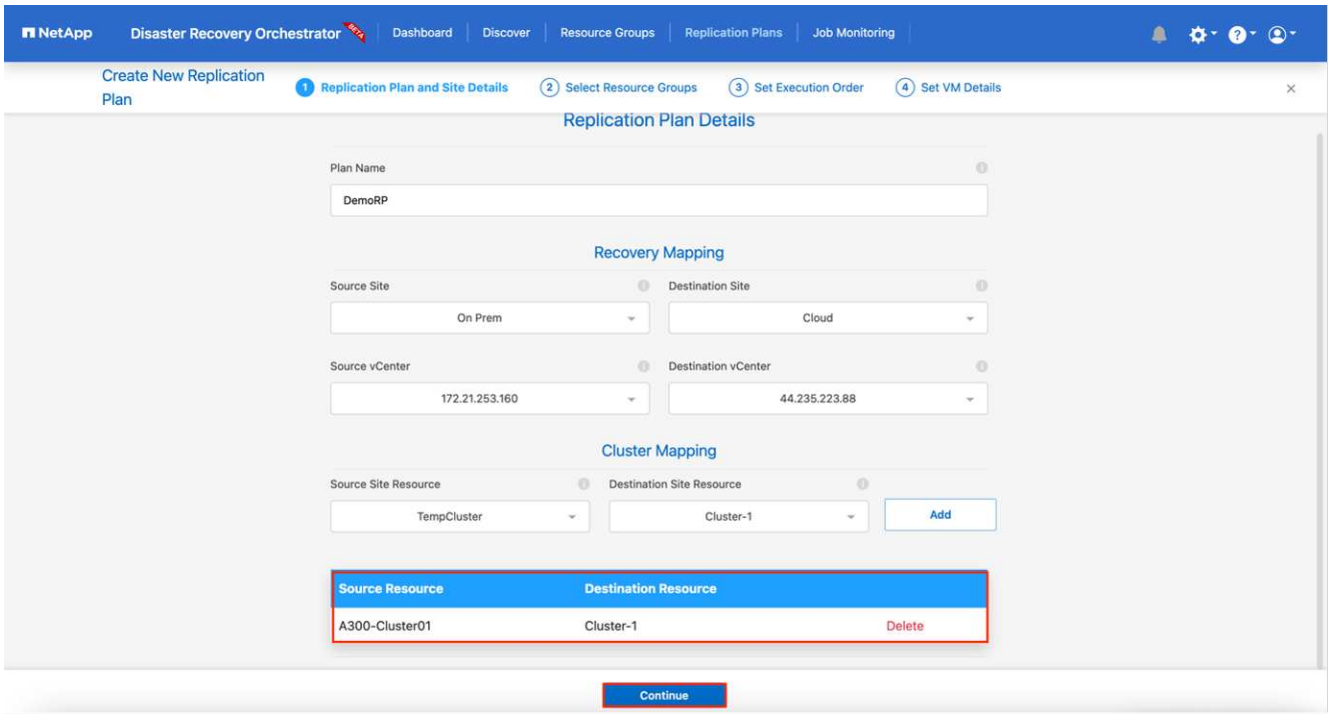
Per iniziare a creare un piano di replica, attenersi alla seguente procedura:

1. Accedere a **Replication Plans** e fare clic su **Create New Replication Plan** (Crea nuovo piano di replica).



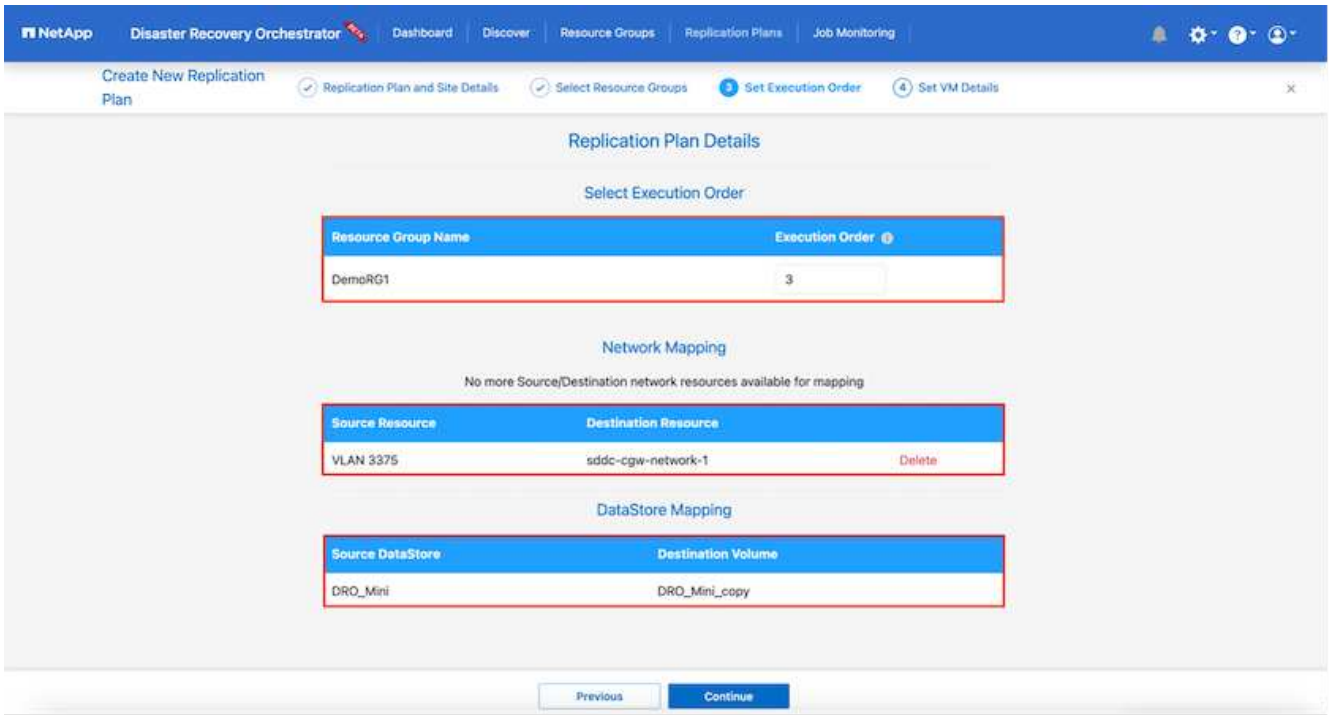
2. In **New Replication Plan** (nuovo piano di replica), specificare un nome per il piano e aggiungere i mapping di ripristino selezionando il sito di origine, il vCenter associato, il sito di destinazione e il vCenter associato.

3. Una volta completata la mappatura di ripristino, selezionare la mappatura del cluster.

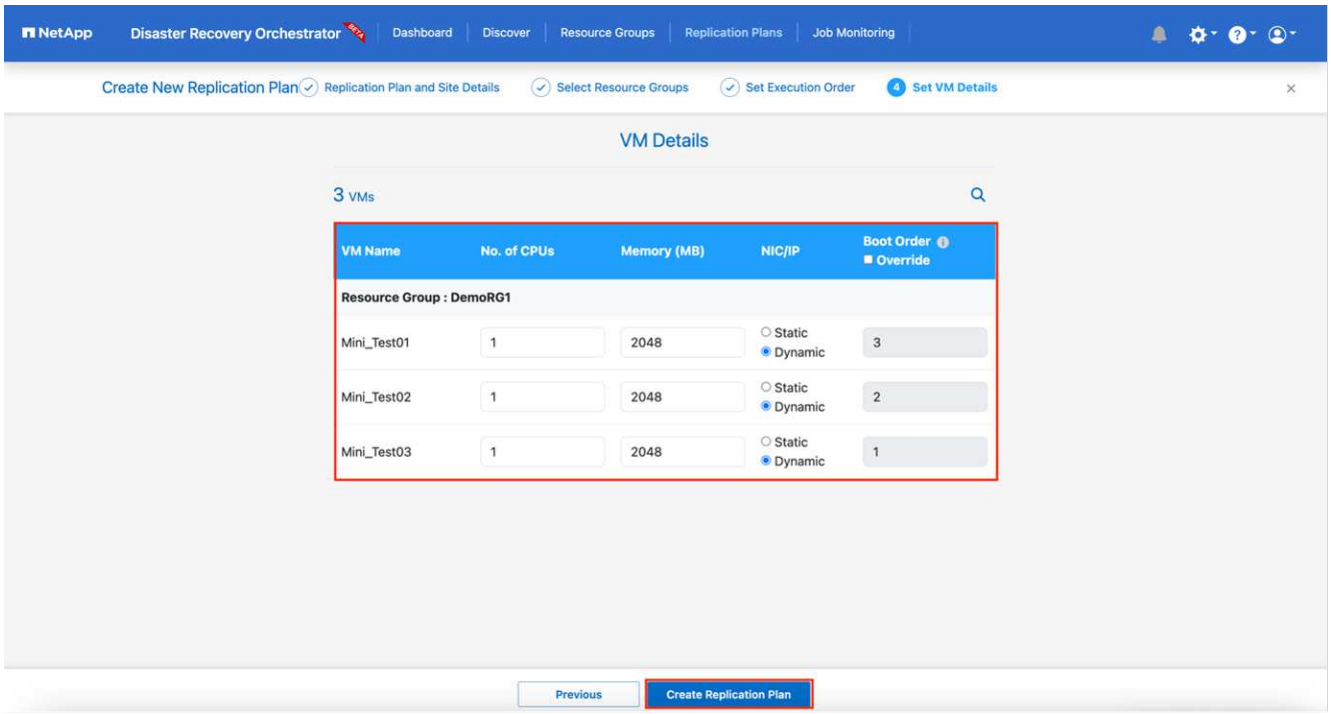


4. Selezionare **Dettagli gruppo di risorse** e fare clic su **continua**.
5. Impostare l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza di operazioni quando esistono più gruppi di risorse.
6. Al termine, selezionare la mappatura di rete per il segmento appropriato. I segmenti devono essere già sottoposti a provisioning all'interno di VMC, quindi selezionare il segmento appropriato per mappare la macchina virtuale.
7. In base alla selezione delle macchine virtuali, i mapping degli archivi dati vengono selezionati automaticamente.

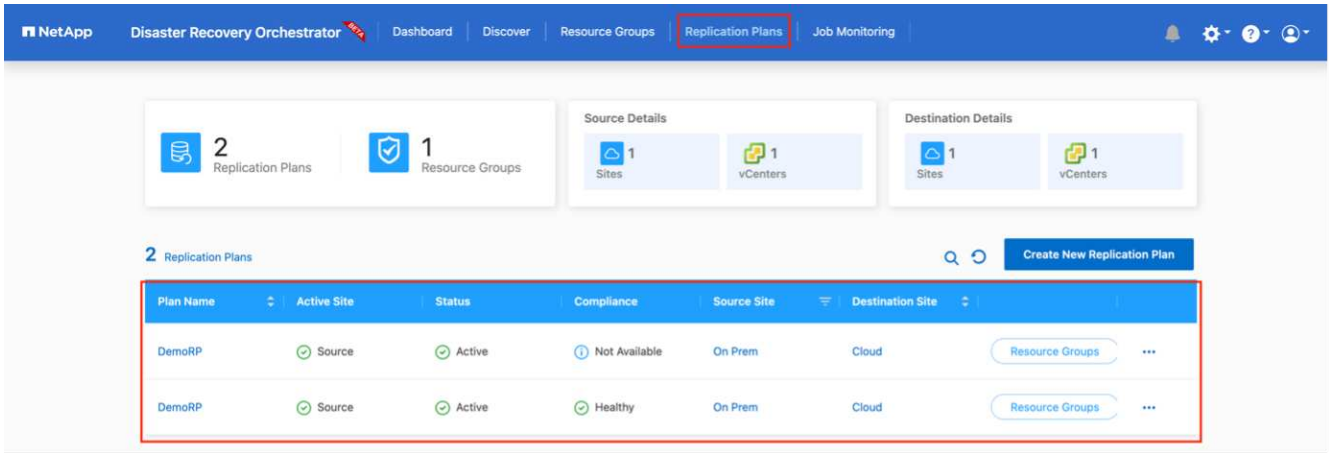
> SnapMirror è a livello di volume. Pertanto, tutte le macchine virtuali vengono replicate nella destinazione di replica. Assicurarsi di selezionare tutte le macchine virtuali che fanno parte dell'archivio dati. Se non sono selezionate, vengono elaborate solo le macchine virtuali che fanno parte del piano di replica.



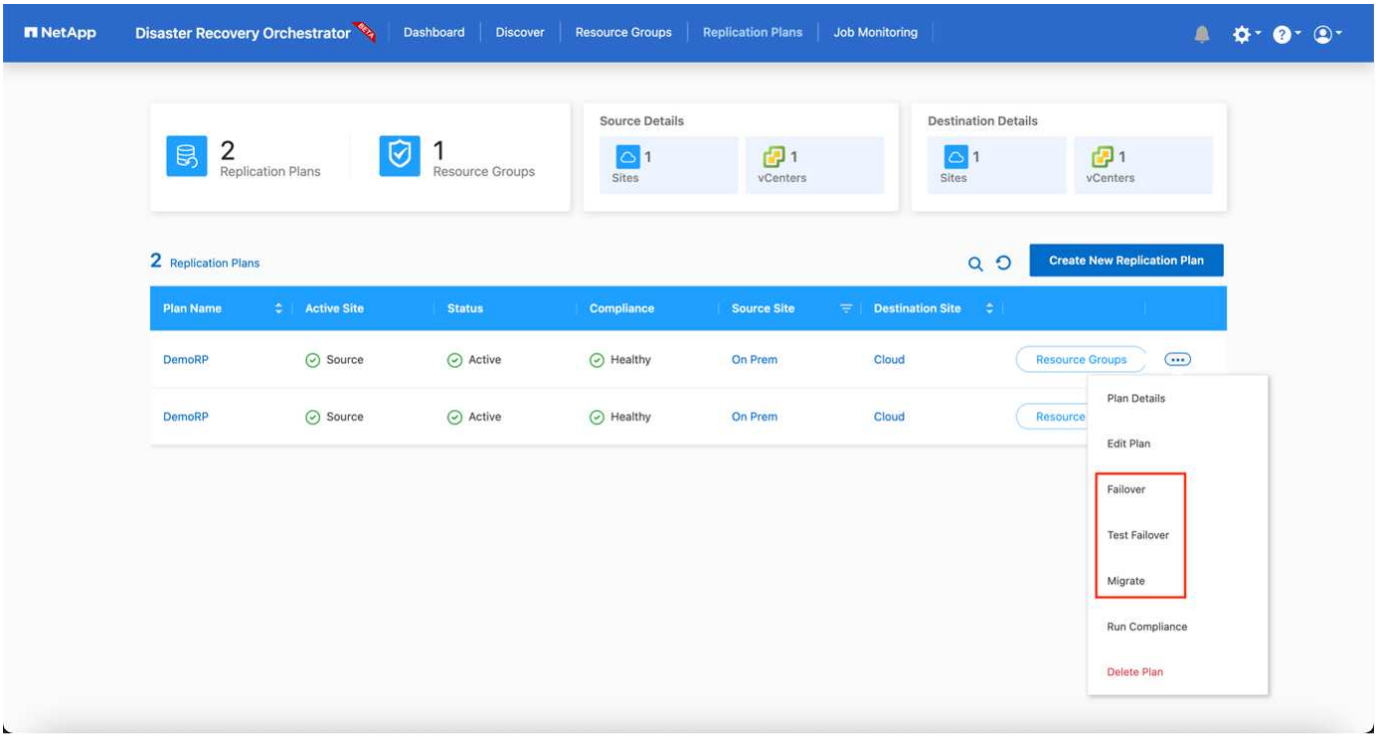
8. In base ai dettagli della macchina virtuale, è possibile ridimensionare i parametri della CPU e della RAM della macchina virtuale; ciò può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o per eseguire test di DR senza dover eseguire il provisioning di un'infrastruttura fisica VMware uno a uno. Inoltre, è possibile modificare l'ordine di avvio e il ritardo di avvio (secondi) per tutte le macchine virtuali selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche da quelle selezionate durante la selezione dell'ordine di avvio del gruppo di risorse. Per impostazione predefinita, viene utilizzato l'ordine di avvio selezionato durante la selezione del gruppo di risorse; tuttavia, in questa fase è possibile eseguire qualsiasi modifica.



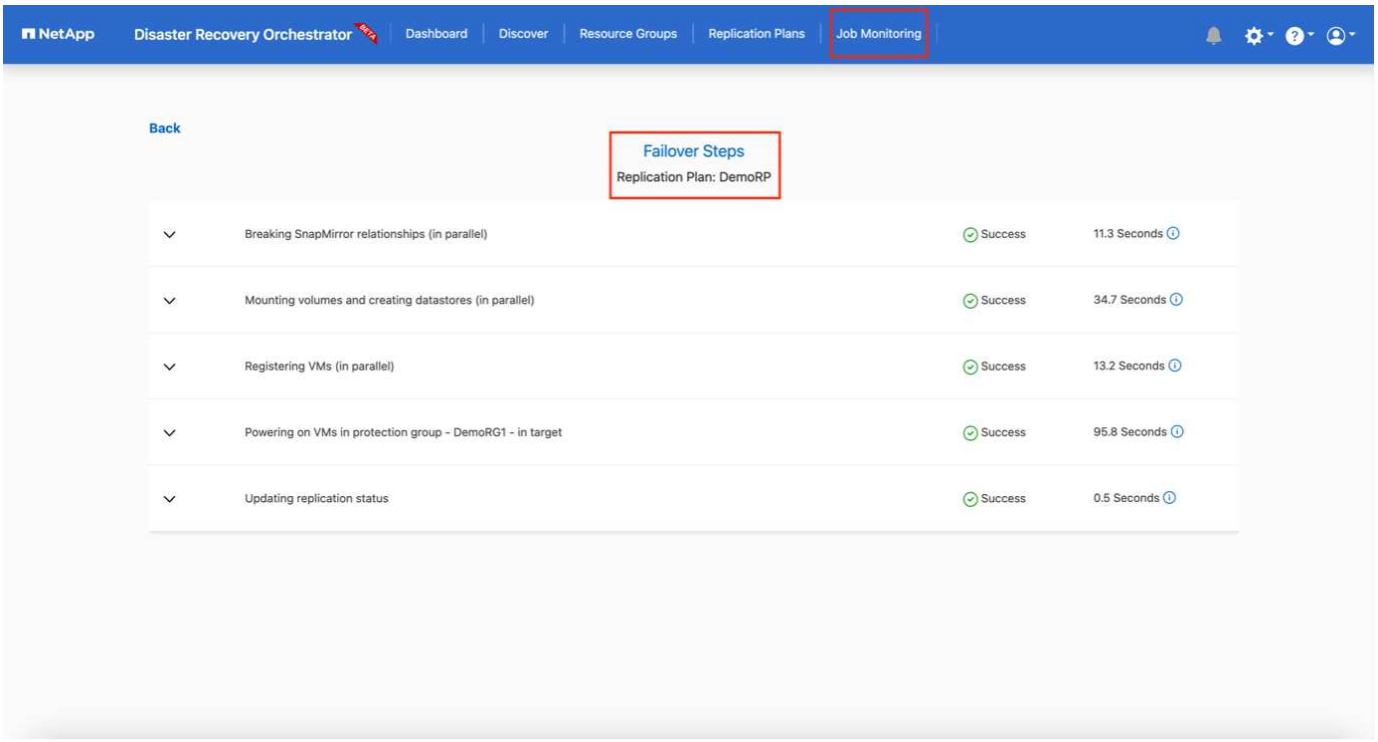
9. Fare clic su **Crea piano di replica**.



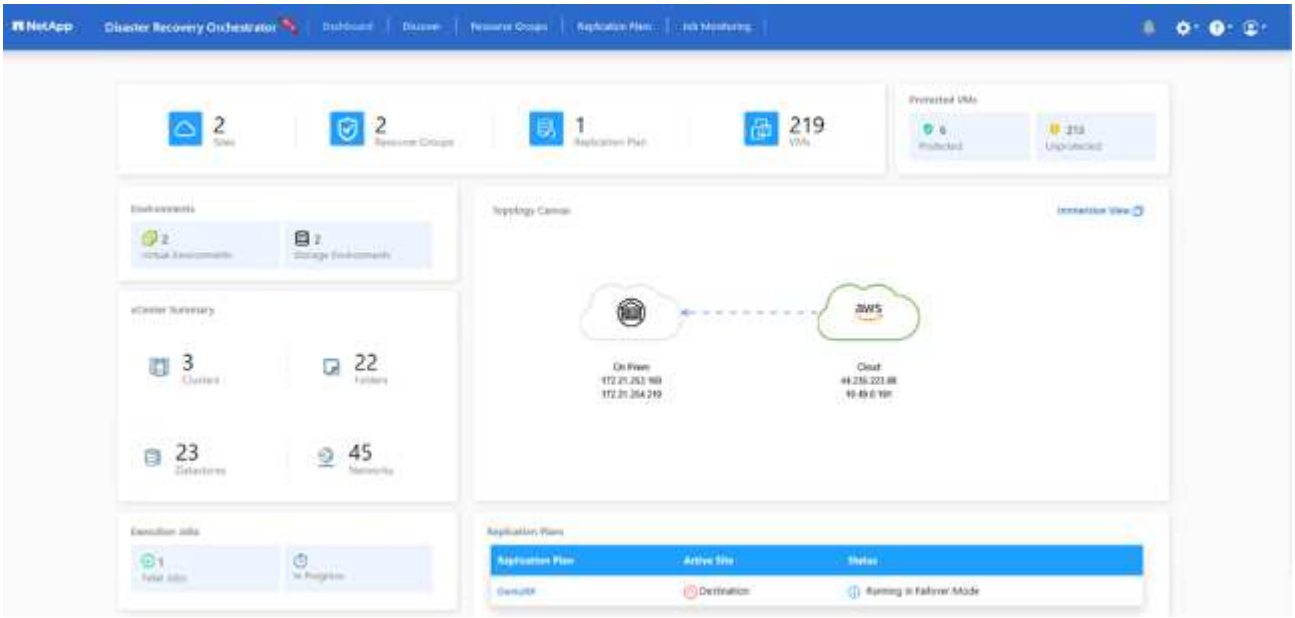
Una volta creato il piano di replica, è possibile utilizzare l'opzione di failover, l'opzione di test-failover o l'opzione di migrazione a seconda dei requisiti. Durante le opzioni di failover e test-failover, viene utilizzata la copia Snapshot SnapMirror più recente oppure è possibile selezionare una copia Snapshot specifica da una copia Snapshot point-in-time (in base alla policy di conservazione di SnapMirror). L'opzione point-in-time può essere molto utile se si sta affrontando un evento di corruzione come ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i punti disponibili nel tempo. Per attivare il failover o verificare il failover con la configurazione specificata nel piano di replica, fare clic su **failover** o **Test failover**.



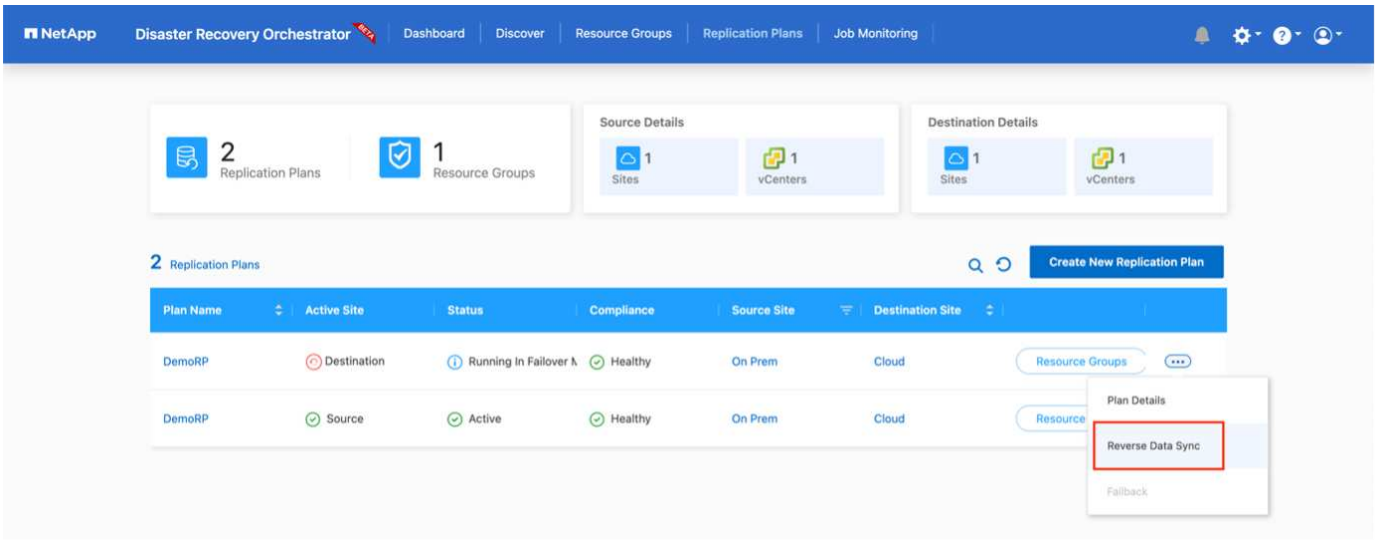
Il piano di replica può essere monitorato nel menu delle attività:

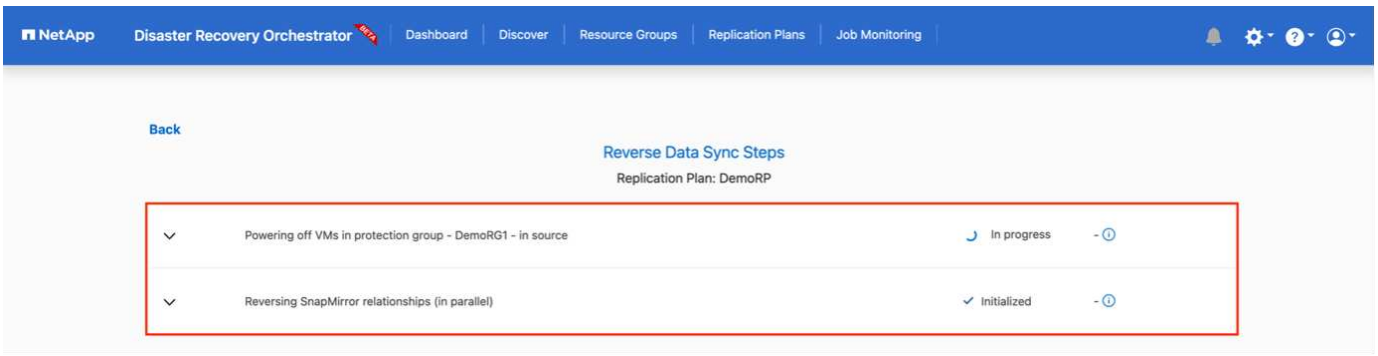


Dopo l'attivazione del failover, gli elementi ripristinati possono essere visualizzati in VMC vCenter (macchine virtuali, reti, datastore). Per impostazione predefinita, le macchine virtuali vengono ripristinate nella cartella workload.

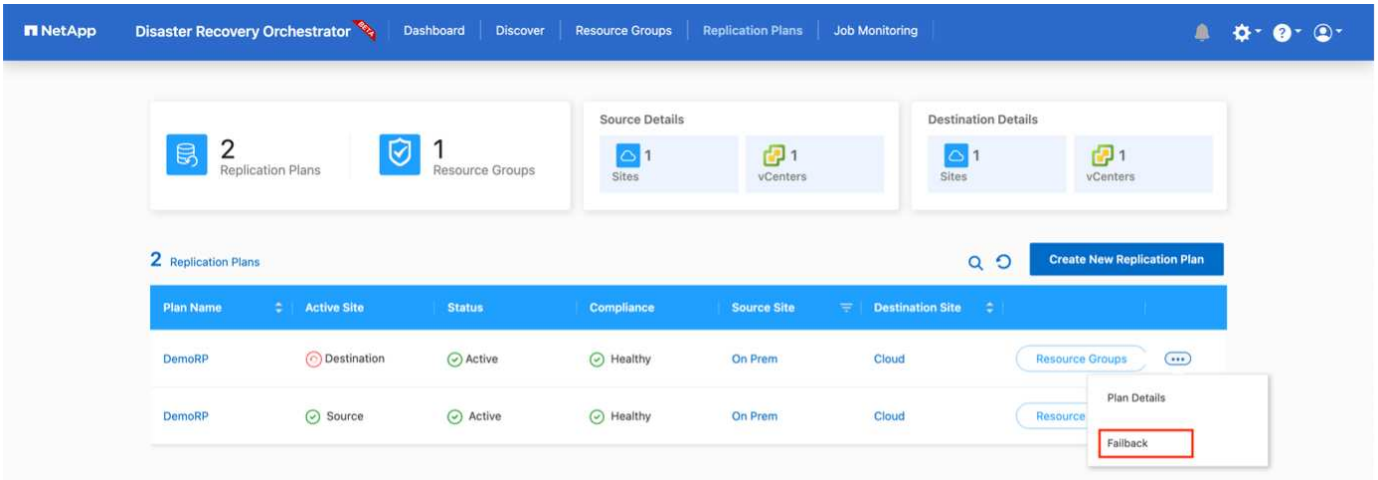


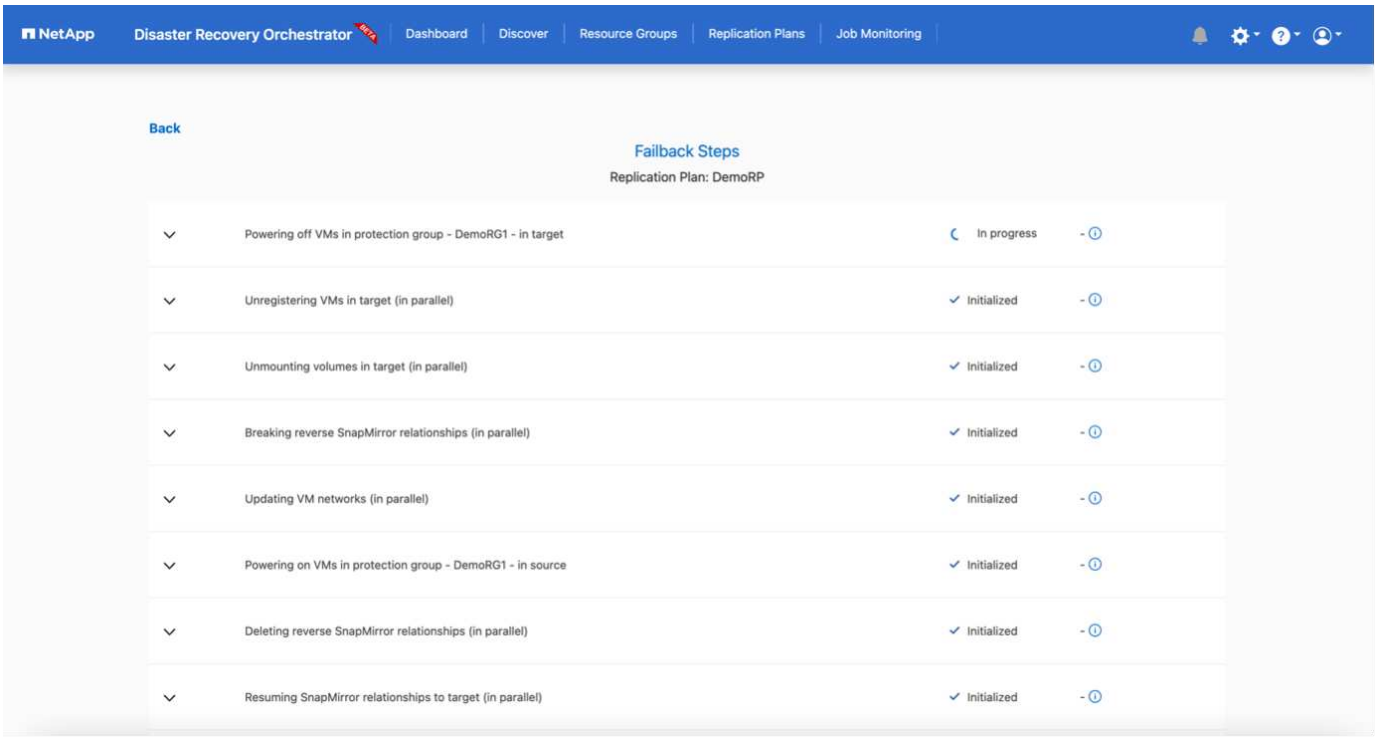
Il failback può essere attivato a livello di piano di replica. Per un failover di test, l'opzione di strappo può essere utilizzata per eseguire il rollback delle modifiche e rimuovere la relazione FlexClone. Il failback relativo al failover è un processo in due fasi. Selezionare il piano di replica e selezionare **Reverse data Sync**.



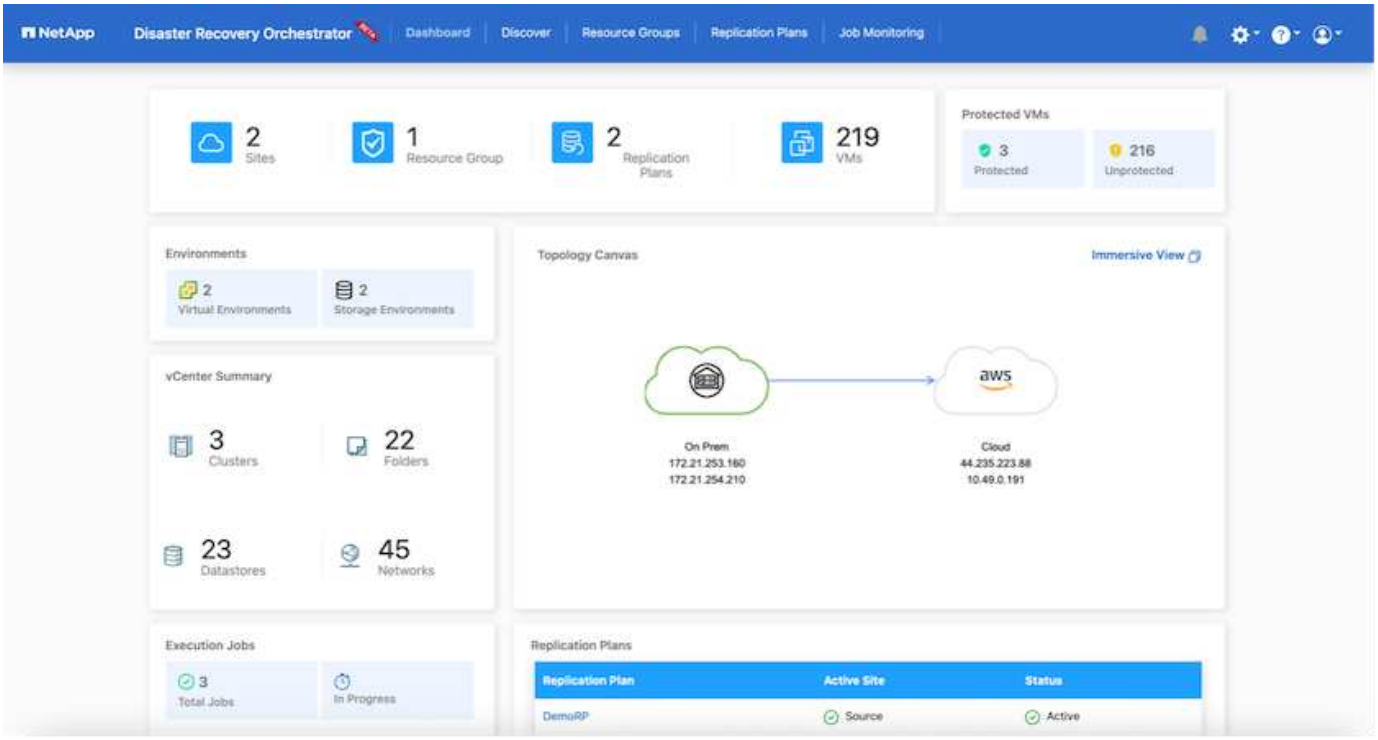


Una volta completato, è possibile attivare il failback per tornare al sito di produzione originale.





Da NetApp BlueXP, possiamo notare che lo stato di salute della replica è stato interrotto per i volumi appropriati (quelli mappati a VMC come volumi di lettura/scrittura). Durante il failover di test, DRO non esegue il mapping del volume di destinazione o di replica. Invece, crea una copia FlexClone dell'istanza SnapMirror (o Snapshot) richiesta ed espone l'istanza FlexClone, che non consuma ulteriore capacità fisica per FSX per ONTAP. Questo processo garantisce che il volume non venga modificato e che i processi di replica possano continuare anche durante i test di DR o i flussi di lavoro di triage. Inoltre, questo processo garantisce che, in caso di errori o di ripristino di dati corrotti, il ripristino possa essere pulito senza il rischio di distruzione della replica.



Recovery ransomware

Il ripristino dal ransomware può essere un compito scoraggiante. In particolare, può essere difficile per le organizzazioni IT individuare il punto di ritorno sicuro e, una volta stabilito, proteggere i carichi di lavoro recuperati da attacchi ricorrenti, ad esempio malware in sospensione o applicazioni vulnerabili.

DRO risolve questi problemi consentendo di ripristinare il sistema da qualsiasi punto in tempo disponibile. È inoltre possibile ripristinare i carichi di lavoro su reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro in una posizione in cui non sono esposte al traffico nord-sud. In questo modo, il tuo team di sicurezza è in una posizione sicura per condurre indagini legali e assicurarsi che non ci siano malware nascosti o inattivi.

Benefici

- Utilizzo della replica SnapMirror efficiente e resiliente.
- Ripristino in qualsiasi momento disponibile con la conservazione delle copie Snapshot.
- Automazione completa di tutte le fasi necessarie per ripristinare da centinaia a migliaia di macchine virtuali dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- Ripristino del workload con la tecnologia FlexClone di ONTAP che utilizza un metodo che non modifica il volume replicato.
  - Evita il rischio di corruzione dei dati per volumi o copie Snapshot.
  - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
  - Potenziale utilizzo dei dati di DR con risorse di cloud computing per flussi di lavoro che vanno oltre il DR, come DevTest, test di sicurezza, test di patch o upgrade e test di correzione.
- Ottimizzazione della CPU e della RAM per ridurre i costi del cloud consentendo il ripristino in cluster di calcolo più piccoli.

Utilizzo di Veeam Replication and FSX for ONTAP per il disaster recovery in VMware Cloud su AWS

Autore: Niyaz Mohamed - Ingegneria di soluzioni di NetApp

Panoramica

L'integrazione di Amazon FSX per NetApp ONTAP con VMware Cloud su AWS è un datastore NFS esterno gestito da AWS e costruito sul file system ONTAP di NetApp che può essere collegato a un cluster nell'SDDC. Offre ai clienti un'infrastruttura storage virtualizzata flessibile e dalle performance elevate, che può scalare in maniera indipendente dalle risorse di calcolo.

Per i clienti che desiderano utilizzare VMware Cloud su AWS SDDC come destinazione di disaster recovery, i datastore FSX per ONTAP possono essere utilizzati per replicare i dati dalle strutture on-premise utilizzando qualsiasi soluzione di terze parti validata che offre funzionalità di replica delle macchine virtuali. Aggiungendo un datastore di FSX per ONTAP, si otterrà un'implementazione ottimizzata dei costi rispetto alla costruzione di un cloud VMware su AWS SDDC con un'enorme quantità di host ESXi solo per ospitare lo storage.

Questo approccio aiuta inoltre i clienti a utilizzare cluster pilota leggero in VMC insieme ai datastore FSX per ONTAP per ospitare le repliche della macchina virtuale. Lo stesso processo può anche essere esteso come opzione di migrazione a VMware Cloud su AWS eseguendo con dignità il failover del piano di replica.

Descrizione del problema

Questo documento descrive come utilizzare il datastore FSX per ONTAP e la replica di Veeam Backup per

configurare il disaster recovery per le VM VMware on-premise su VMware Cloud su AWS utilizzando la funzionalità di replica delle VM.

Veeam Backup & Replication offre replica on-site e remota per il disaster recovery (DR). Quando le macchine virtuali vengono replicate, Veeam Backup & Replication crea una copia esatta delle macchine virtuali nel formato nativo di VMware vSphere sul cluster VMware Cloud di destinazione su AWS SDDC e mantiene la copia sincronizzata con la macchina virtuale originale.

La replica offre i migliori valori di RTO (Recovery Time Objective) poiché esiste una copia di una VM nello stato pronto per l'avvio. Questo meccanismo di replica garantisce l'avvio rapido dei carichi di lavoro in VMware Cloud su AWS SDDC in caso di evento di emergenza. Il software Veeam Backup & Replication ottimizza anche la trasmissione del traffico per la replica su WAN e le connessioni lente. Inoltre, filtra anche blocchi di dati duplicati, blocchi di dati zero, file di swap e file OS guest di VM esclusi e comprime il traffico di replica.

Per evitare che i processi di replica consumino l'intera larghezza di banda della rete, è possibile mettere in atto acceleratori WAN e regole di limitazione della rete. Il processo di replica in Veeam Backup & Replication è basato sul processo, il che significa che la replica viene eseguita configurando i processi di replica. In caso di evento di emergenza, è possibile attivare il failover per ripristinare le macchine virtuali con failover sulla copia di replica.

Una volta eseguito il failover, una VM replicata assume il ruolo della VM originale. Il failover può essere eseguito allo stato più recente di una replica o a qualsiasi punto di ripristino valido. Ciò abilita recovery dal ransomware o test isolati, se necessario. In Veeam Backup & Replication, il failover e il failback sono passaggi intermedi temporanei che devono essere ulteriormente finalizzati. Veeam Backup & Replication offre diverse opzioni per gestire diversi scenari di disaster recovery.

[Diagramma dello scenario di DR con replica Veeam e FSX ONTAP per VMC]

Implementazione della soluzione

Gradini di alto livello

1. Il software Veeam Backup and Replication è in esecuzione in un ambiente on-premise con appropriata connettività di rete.
2. Configurare VMware Cloud su AWS, vedere l'articolo VMware Cloud Tech zone "Guida all'integrazione di VMware Cloud su AWS con Amazon FSX per l'implementazione di NetApp ONTAP" Per eseguire l'implementazione, configura VMware Cloud su AWS SDDC e FSX per ONTAP come datastore NFS. (Per scopi di DR è possibile utilizzare un ambiente pilota con configurazione minima. In caso di incidente, è possibile eseguire il failover delle macchine virtuali su questo cluster e aggiungere nodi.
3. Impostare i lavori di replica per creare repliche VM utilizzando Veeam Backup and Replication.
4. Creazione di un piano di failover ed esecuzione di un failover.
5. Tornare alle macchine virtuali di produzione una volta che l'evento di disastro è completo e il sito primario è attivo.

Prerequisiti per la replica della macchina virtuale Veeam nei datastore VMC ed FSX per ONTAP

1. Garantire che la macchina virtuale di backup di Veeam Backup & Replication sia connessa al vCenter di origine e al cloud VMware di destinazione sui cluster AWS SDDC.
2. Il server di backup deve essere in grado di risolvere i nomi brevi e di connettersi ai centri virtuali di origine e di destinazione.
3. Il datastore FSX per ONTAP di destinazione deve avere spazio libero sufficiente per archiviare VMDK di macchine virtuali replicate

Per ulteriori informazioni, fare riferimento a "considerazioni e limitazioni" "qui".

Dettagli sull’implementazione

Fase 1: Replica delle VM

Veeam Backup & Replication sfrutta le funzionalità snapshot di VMware vSphere e, durante la replica, Veeam Backup & Replication richiede a VMware vSphere la creazione di una snapshot delle VM. L'istantanea della VM è la copia point-in-time di una VM che include dischi virtuali, stato del sistema, configurazione e così via. Veeam Backup & Replication utilizza la snapshot come origine dei dati per la replica.

Per replicare le VM, attenersi alla seguente procedura:

1. Apri la Veeam Backup & Replication Console.
2. Nella vista Home, selezionare processo di replica > macchina virtuale > VMware vSphere.
3. Specificare un nome di lavoro e selezionare la casella di controllo controllo avanzata appropriata. Fare clic su Avanti.
   - Selezionare la casella di controllo Replica seeding se la connettività tra on-premise e AWS ha limitato la larghezza di banda.
   - Selezionare la casella di controllo Network remapping (per i siti VMC AWS con reti diverse) se i segmenti su VMware Cloud su AWS SDDC non corrispondono a quelli delle reti dei siti on-premise.
   - Se lo schema di indirizzamento IP nel sito di produzione on-premise differisce dallo schema nel sito VMC di AWS, selezionare la casella di controllo Replica re-IP (per i siti di DR con schema di indirizzamento IP diverso).

     [dr. veeam fsx image2] | *dr-veeam-fsx-image2.png*
4. Seleziona le VM da replicare nel datastore FSX per ONTAP collegato a VMware Cloud su AWS SDDC nel passaggio **macchine virtuali**. Le macchine virtuali possono essere posizionate su vSAN per riempire la capacità del datastore vSAN disponibile. In un cluster spia pilota, la capacità utilizzabile di un cluster a 3 nodi sarà limitata. Il resto dei dati può essere replicato in datastore FSX per ONTAP. Fare clic su **Aggiungi**, quindi nella finestra **Aggiungi oggetto** selezionare le VM o i contenitori VM necessari e fare clic su **Aggiungi**. Fare clic su **Avanti**.

   [dr. veeam fsx image3] | *dr-veeam-fsx-image3.png*
5. Quindi, seleziona la destinazione come VMware Cloud su host/cluster SDDC di AWS e il pool di risorse, la cartella VM e il datastore FSX per le repliche VM di ONTAP. Quindi fare clic su **Avanti**.

   [dr. veeam fsx image4] | *dr-veeam-fsx-image4.png*
6. Nel passaggio successivo, creare la mappatura tra la rete virtuale di origine e di destinazione secondo necessità.

   [dr. veeam fsx image5] | *dr-veeam-fsx-image5.png*
7. Nel passaggio **Impostazioni processo**, specificare il repository di backup che memorizzerà i metadati per le repliche della VM, i criteri di conservazione e così via.
8. Aggiornare i server proxy **Source** e **Target** nel passo **trasferimento dati** e lasciare selezionata l'opzione **Automatic** (impostazione predefinita) e mantenere l'opzione **Direct** (diretto) e fare clic su **Next** (Avanti).
9. Nel passaggio **elaborazione guest**, selezionare **attiva elaborazione in base alle esigenze dell'applicazione**. Fare clic su **Avanti**.

[dr. veeam fsx image6] | *dr-veeam-fsx-image6.png*

10. Scegliere la pianificazione di replica per eseguire regolarmente il processo di replica.
11. Nel passo **Riepilogo** della procedura guidata, esaminare i dettagli del processo di replica. Per avviare il lavoro subito dopo la chiusura della procedura guidata, selezionare la casella di controllo **Esegui il lavoro quando si fa clic su fine**, altrimenti lasciare deselezionata la casella di controllo. Quindi fare clic su **fine** per chiudere la procedura guidata.

    [dr. veeam fsx image7] | *dr-veeam-fsx-image7.png*

Una volta avviato il processo di replica, le macchine virtuali con il suffisso specificato verranno popolate nel cluster/host VMC SDDC di destinazione.

[dr. veeam fsx image8] | *dr-veeam-fsx-image8.png*

Per ulteriori informazioni sulla replica Veeam, fare riferimento a. "Come funziona la replica".

Passaggio 2: Creare un piano di failover

Una volta completata la replica o il seeding iniziale, creare il piano di failover. Il piano di failover consente di eseguire automaticamente il failover per le VM dipendenti una alla volta o come gruppo. Il piano di failover è il modello per l'ordine in cui le macchine virtuali vengono elaborate, inclusi i ritardi di avvio. Il piano di failover aiuta inoltre a garantire che le VM dipendenti da fattori critici siano già in esecuzione.

Per creare il piano, passare alla nuova sottosezione denominata repliche e selezionare piano di failover. Scegliere le VM appropriate. Veeam Backup & Replication cercherà i punti di ripristino più vicini a questo punto nel tempo e li utilizzerà per avviare le repliche della VM.

ⓘ Il piano di failover può essere aggiunto solo una volta completata la replica iniziale e le repliche della VM sono nello stato Pronta.

ⓘ Il numero massimo di VM che possono essere avviate contemporaneamente quando si esegue un piano di failover è 10.

ⓘ Durante il processo di failover, le macchine virtuali di origine non verranno spente.

Per creare il **piano di failover**, procedere come segue:

1. Nella vista Home, selezionare **piano di failover > VMware vSphere**.
2. Quindi, fornire un nome e una descrizione al piano. Gli script pre e post-failover possono essere aggiunti secondo necessità. Ad esempio, eseguire uno script per arrestare le macchine virtuali prima di avviare le macchine virtuali replicate.

   [dr. veeam fsx image9] | *dr-veeam-fsx-image9.png*

3. Aggiungere le VM al piano e modificare l'ordine di avvio delle VM e i ritardi di avvio per soddisfare le dipendenze delle applicazioni.

   [dr. veeam fsx image10] | *dr-veeam-fsx-image10.png*

Per ulteriori informazioni sulla creazione di processi di replica, fare riferimento a. "Creazione di processi di replica".

Passaggio 3: Eseguire il piano di failover

Durante il failover, la macchina virtuale di origine nel sito di produzione viene commutata alla replica nel sito di disaster recovery. Come parte del processo di failover, Veeam Backup & Replication ripristina la replica della VM al punto di ripristino richiesto e sposta tutte le attività di i/o dalla VM di origine alla replica. Le repliche possono essere utilizzate non solo in caso di disastro, ma anche per simulare esercitazioni sul DR. Durante la simulazione del failover, la VM di origine rimane in esecuzione. Una volta eseguiti tutti i test necessari, è possibile annullare il failover e tornare alla normale operatività.

> Accertarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante le procedure di DR.

Per avviare il piano di failover, è sufficiente fare clic sulla scheda **piani di failover** e fare clic con il pulsante destro del mouse sul piano di failover. Selezionare **Start**. Il failover viene eseguito utilizzando gli ultimi punti di ripristino delle repliche della VM. Per eseguire il failover su punti di ripristino specifici delle repliche della VM, selezionare **Avvia a**.

[dr. veeam fsx image11] | *dr-veeam-fsx-image11.png*

[dr. veeam fsx image12] | *dr-veeam-fsx-image12.png*

Lo stato della replica della macchina virtuale cambia da Pronto a failover e le macchine virtuali vengono avviate sul VMware Cloud di destinazione sul cluster/host AWS SDDC.

[dr. veeam fsx image13] | *dr-veeam-fsx-image13.png*

Una volta completato il failover, lo stato delle macchine virtuali passa a "failover".

[dr. veeam fsx image14] | *dr-veeam-fsx-image14.png*

> Veeam Backup & Replication interrompe tutte le attività di replica per la VM di origine fino a quando la replica non viene riportata allo stato Ready.

Per informazioni dettagliate sui piani di failover, fare riferimento a. "Piani di failover".

Fase 4: Failback nel sito di produzione

Quando il piano di failover è in esecuzione, viene considerato come una fase intermedia e deve essere finalizzato in base al requisito. Le opzioni includono:

- **Failback to Production** - consente di tornare alla VM originale e di trasferire tutte le modifiche apportate durante l'esecuzione della replica della VM alla VM originale.

> Quando si esegue il failback, le modifiche vengono solo trasferite ma non pubblicate. Scegliere **Commit failback** (una volta che la VM originale è confermata per funzionare come previsto) o **Undo failback** per tornare alla replica della VM se la VM originale non funziona come previsto.

- **Annulla failover** - consente di tornare alla VM originale e di ignorare tutte le modifiche apportate alla replica della VM durante l'esecuzione.
- **Failover permanente** - consente di passare in modo permanente dalla VM originale a una replica della VM e di utilizzare questa replica come VM originale.

In questa demo, è stato scelto il failback in produzione. Il failback alla macchina virtuale originale è stato selezionato durante la fase di destinazione della procedura guidata ed è stata attivata la casella di controllo "accensione della macchina virtuale dopo il ripristino".

[dr. veeam fsx image15] | *dr-veeam-fsx-image15.png*

[dr. veeam fsx image16] | *dr-veeam-fsx-image16.png*

Il commit di failback è uno dei modi per finalizzare l'operazione di failback. Quando il failback viene eseguito, conferma che le modifiche inviate alla VM che ha avuto esito negativo (la VM di produzione) funzionano come previsto. Dopo l'operazione di commit, Veeam Backup & Replication riprende le attività di replica per la VM di produzione.

Per informazioni dettagliate sul processo di failback, fare riferimento alla documentazione Veeam per "Failover e failback per la replica".

[dr. veeam fsx image17] | *dr-veeam-fsx-image17.png*

[dr. veeam fsx image18] | *dr-veeam-fsx-image18.png*

Una volta eseguito il failback in produzione, le macchine virtuali vengono tutte ripristinate nel sito di produzione originale.

[dr. veeam fsx image19] | *dr-veeam-fsx-image19.png*

Conclusione

La funzionalità datastore di FSX per ONTAP permette a Veeam o a qualsiasi strumento di terze parti validato di fornire una soluzione DR a basso costo utilizzando il cluster pilota leggero e senza standing un elevato numero di host nel cluster solo per ospitare la copia della replica della VM. Questo offre una potente soluzione per gestire un piano di disaster recovery personalizzato e su misura e consente inoltre di riutilizzare i prodotti di backup esistenti in sede per soddisfare le esigenze di disaster recovery, consentendo in questo modo il disaster recovery basato sul cloud uscendo dai data center on-premise. Il failover può essere eseguito come failover pianificato o failover con un clic su un pulsante in caso di disastro e si decide di attivare il sito di DR.

Per ulteriori informazioni su questo processo, segui il video dettagliato.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

Migrazione dei carichi di lavoro su AWS / VMC

TR 4942: Migrazione dei carichi di lavoro al datastore FSX ONTAP con VMware HCX

Autore: NetApp Solutions Engineering

Panoramica: Migrazione di macchine virtuali con VMware HCX, datastore supplementari FSX ONTAP e VMware Cloud

Un caso di utilizzo comune per VMware Cloud (VMC) su Amazon Web Services (AWS), con il datastore NFS supplementare su Amazon FSX per NetApp ONTAP, è la migrazione dei workload VMware. VMware HCX è un'opzione preferita e offre diversi metodi di migrazione per spostare macchine virtuali (VM) on-premise e i relativi dati, in esecuzione su qualsiasi datastore supportato da VMware, negli archivi dati VMC, che includono datastore NFS supplementari su FSX per ONTAP.

VMware HCX è principalmente una piattaforma di mobilità progettata per semplificare la migrazione dei workload, il ribilanciamento dei workload e la business continuity tra i cloud. È incluso in VMware Cloud su AWS e offre diversi modi per migrare i carichi di lavoro e può essere utilizzato per le operazioni di disaster recovery (DR).

Questo documento fornisce istruzioni dettagliate per l'implementazione e la configurazione di VMware HCX, inclusi tutti i suoi componenti principali, on-premise e sul cloud data center, che abilita vari meccanismi di migrazione delle macchine virtuali.

Per ulteriori informazioni, vedere "Introduzione alle implementazioni HCX" e. "Installare l'elenco di controllo B - HCX con VMware Cloud su AWS SDDC Destination Environment".

Passaggi di alto livello

Questo elenco fornisce i passaggi di alto livello per installare e configurare VMware HCX:

1. Attivare HCX per il data center software-defined (SDDC) VMC tramite VMware Cloud Services Console.
2. Scaricare e implementare IL programma di installazione di HCX Connector OVA nel server vCenter on-premise.
3. Attivare HCX con una chiave di licenza.
4. Associare il connettore VMware HCX on-premise con VMC 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 estendere la rete ed evitare il re-IP.
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, vedere "Preparazione per l'installazione HCX". Una volta soddisfatti i prerequisiti, inclusa la connettività, configurare e attivare HCX generando una chiave di licenza dalla console VMware HCX in VMC. Dopo l'attivazione DI HCX, il plug-in vCenter viene implementato ed è possibile accedervi utilizzando vCenter Console per la gestione.

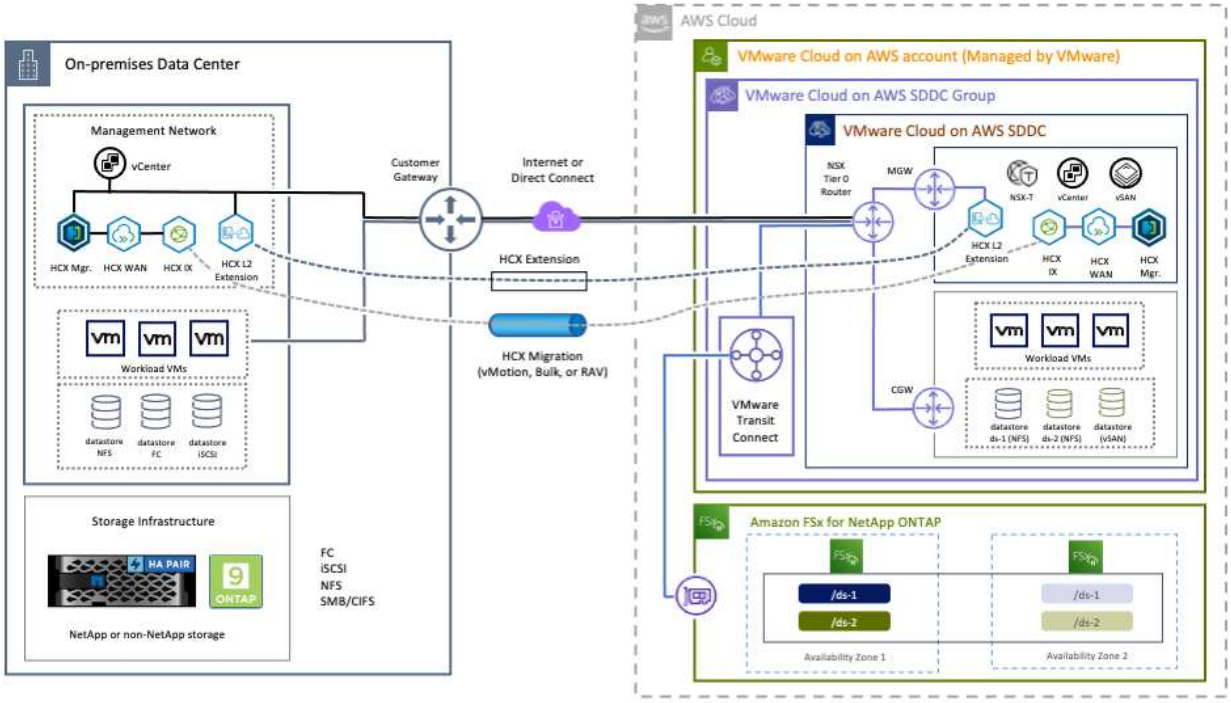
Prima di procedere con l'attivazione E l'implementazione DI HCX, è necessario completare i seguenti passaggi di installazione:

1. Utilizzare un SDDC VMC esistente o creare un nuovo SDDC in seguito "Link NetApp" o questo "Link VMware".
2. Il percorso di rete dall'ambiente vCenter on-premise all'SDDC VMC deve supportare la migrazione delle macchine virtuali utilizzando vMotion.
3. 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.
4. Il volume NFS FSX per ONTAP deve essere montato come datastore supplementare nell'SDDC VMC. Per collegare gli archivi dati NFS al cluster appropriato, seguire la procedura descritta in questa sezione "Link NetApp" o questo "Link VMware".

Architettura di alto livello

A scopo di test, l'ambiente di laboratorio on-premise utilizzato per questa convalida è stato collegato tramite una VPN sito-sito ad AWS VPC, che ha consentito la connettività on-premise ad AWS e a VMware Cloud SDDC tramite External Transit Gateway. La migrazione HCX e il traffico di estensione della rete fluiscono su Internet tra SDDC di destinazione cloud on-premise e VMware. Questa architettura può essere modificata per utilizzare le interfacce virtuali private Direct Connect.

L'immagine seguente mostra l'architettura di alto livello.



Implementazione della soluzione

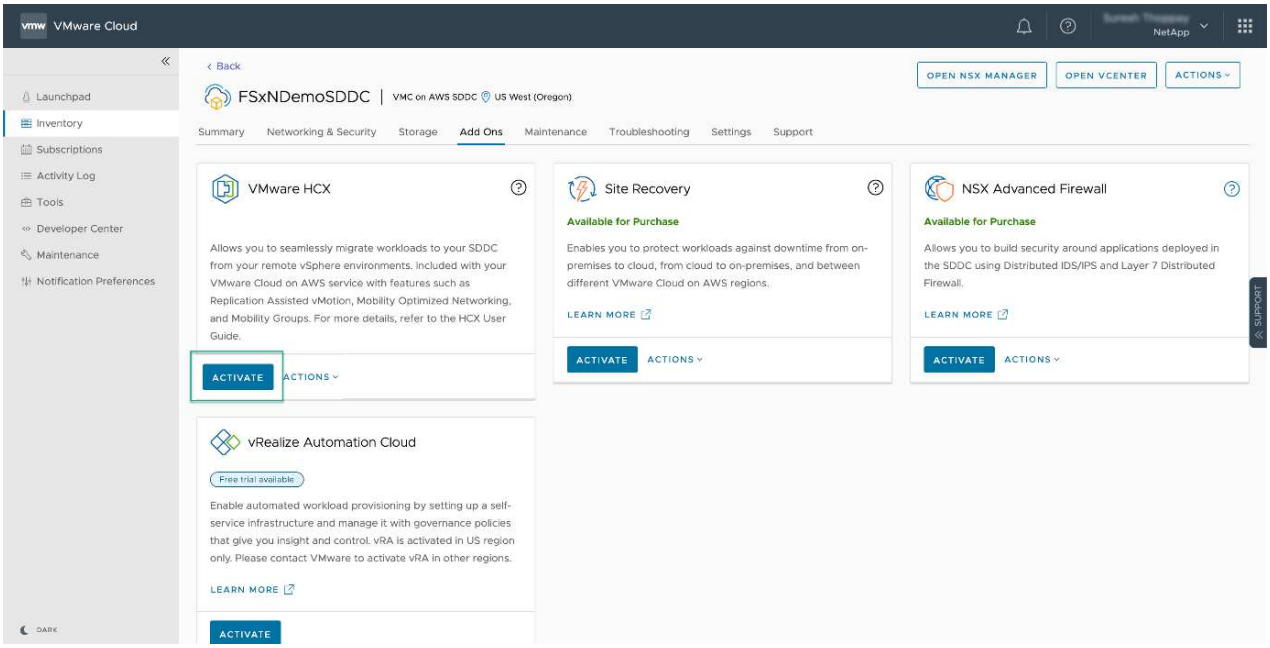
Seguire la serie di passaggi per completare l'implementazione di questa soluzione:

Fase 1: Attivare HCX tramite VMC SDDC utilizzando l'opzione Add-ons

Per eseguire l'installazione, attenersi alla seguente procedura:

1. Accedere alla console VMC all'indirizzo "vmc.vmware.com" E accedere all'inventario.
2. Per selezionare l'SDDC appropriato e accedere ai componenti aggiuntivi, fare clic su View Details (Visualizza dettagli) su SDDC e selezionare la scheda Add Ons (Aggiungi).
3. Fare clic su Activate for VMware HCX.

   Il completamento di questa fase richiede fino a 25 minuti.

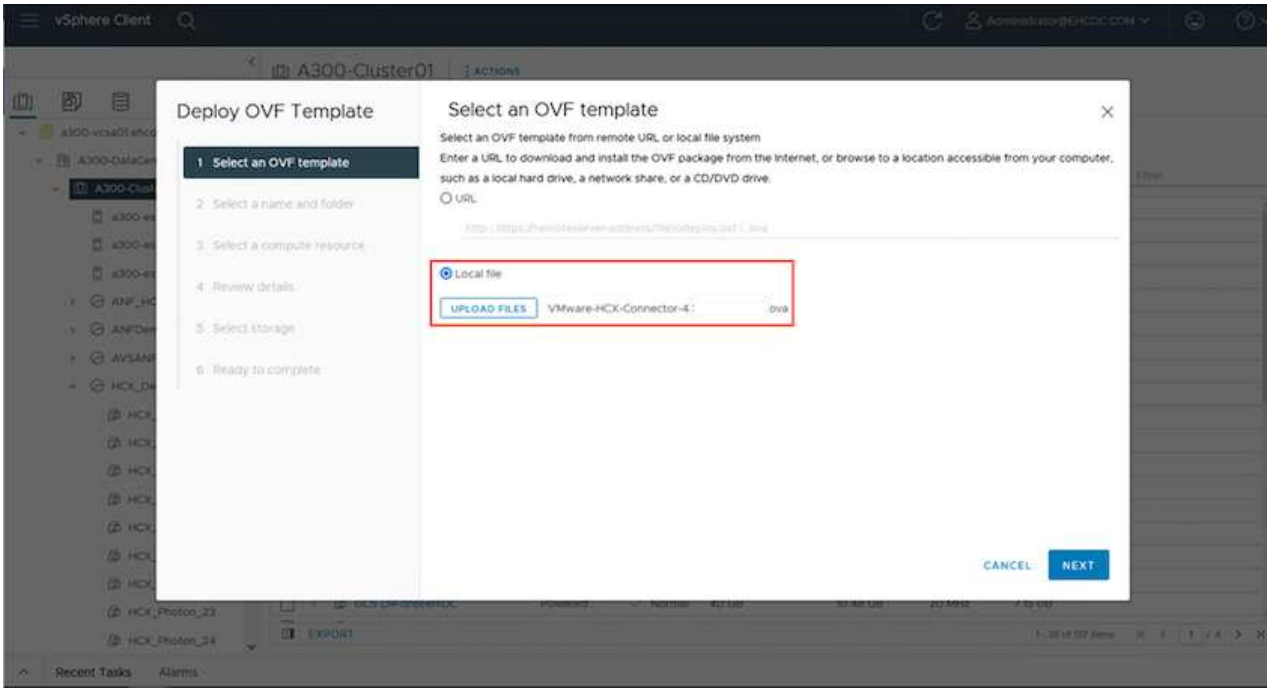


4. Una volta completata l'implementazione, convalidare l'implementazione confermando che HCX Manager e i relativi plug-in associati sono disponibili in vCenter Console.
5. Creare i firewall di Management Gateway appropriati per aprire le porte necessarie per accedere A HCX Cloud Manager.HCX Cloud Manager è ora pronto per le operazioni HCX.

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

Affinché il connettore on-premise comunichi con HCX Manager in VMC, assicurarsi che le porte firewall appropriate siano aperte nell'ambiente on-premise.

1. Dalla console VMC, accedere alla dashboard HCX, accedere a Administration (Amministrazione) e selezionare la scheda Systems Update (aggiornamento sistemi). Fare clic su Request a Download link for the HCX Connector OVA image (Richiedi un link di download per l'immagine OVA
2. Dopo aver scaricato HCX Connector, implementare OVA nel server vCenter on-premise. Fare clic con il pulsante destro del mouse su vSphere Cluster e selezionare l'opzione Deploy OVF Template.

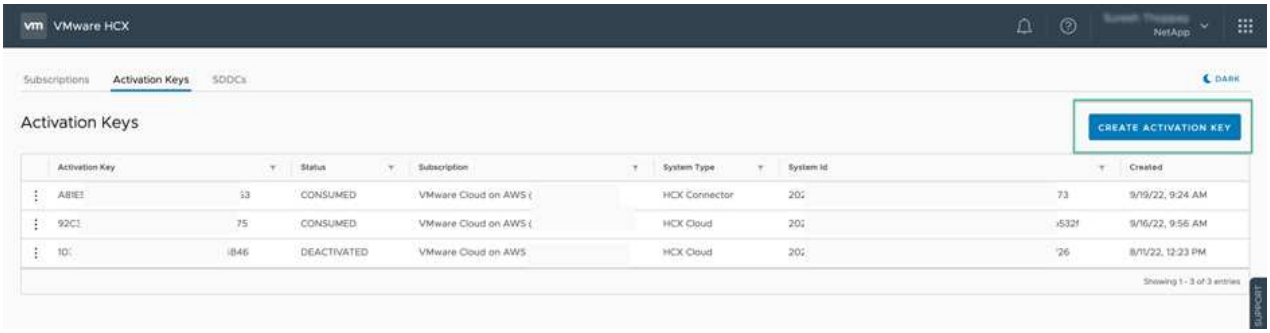


3. Inserire le informazioni richieste nella procedura guidata Deploy OVF Template (implementazione modello OVF), fare clic su Next (Avanti), quindi su Finish (fine) per implementare VMware HCX Connector OVA.
4. Accendere manualmente l'appliance virtuale.per istruzioni dettagliate, visitare il sito Web "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 dalla console VMware HCX in VMC e immettere la licenza durante la configurazione del connettore VMware HCX.

1. Da VMware Cloud Console, accedere a Inventory (inventario), selezionare SDDC e fare clic su View Details (Visualizza dettagli). Dalla scheda Add Ons (Aggiungi servizio), nel riquadro VMware HCX, fare clic su Open HCX (Apri HCX).
2. Dalla scheda Activation Keys (chiavi di attivazione), fare clic su Create Activation Key (Crea chiave di Selezionare il tipo di sistema come connettore HCX e fare clic su Confirm (Conferma) per generare la chiave. Copiare la chiave di attivazione.



> È necessaria una chiave separata per ciascun connettore HCX implementato on-premise.

3. Accedere a VMware HCX Connector on-premise all'indirizzo "https://hcxconnectorIP:9443" utilizzando le credenziali di amministratore.

> Utilizzare la password definita durante l'implementazione di OVA.

4. Nella sezione Licensing (licenze), inserire la chiave di attivazione copiata dal passaggio 2 e fare clic su Activate (attiva).

> Il connettore HCX on-premise deve disporre di accesso a Internet per completare correttamente l'attivazione.

5. Nella sezione Datacenter Location, specificare la posizione desiderata per l'installazione di VMware HCX Manager on-premise. Fare clic su continua.
6. In System Name (Nome sistema), aggiornare il nome e fare clic su Continue (continua).
7. Selezionare Sì, quindi continuare.
8. In Connect Your vCenter (Connetti il vCenter), fornire l'indirizzo IP o il nome di dominio completo (FQDN) e le credenziali per vCenter Server, quindi fare clic su Continue (continua).

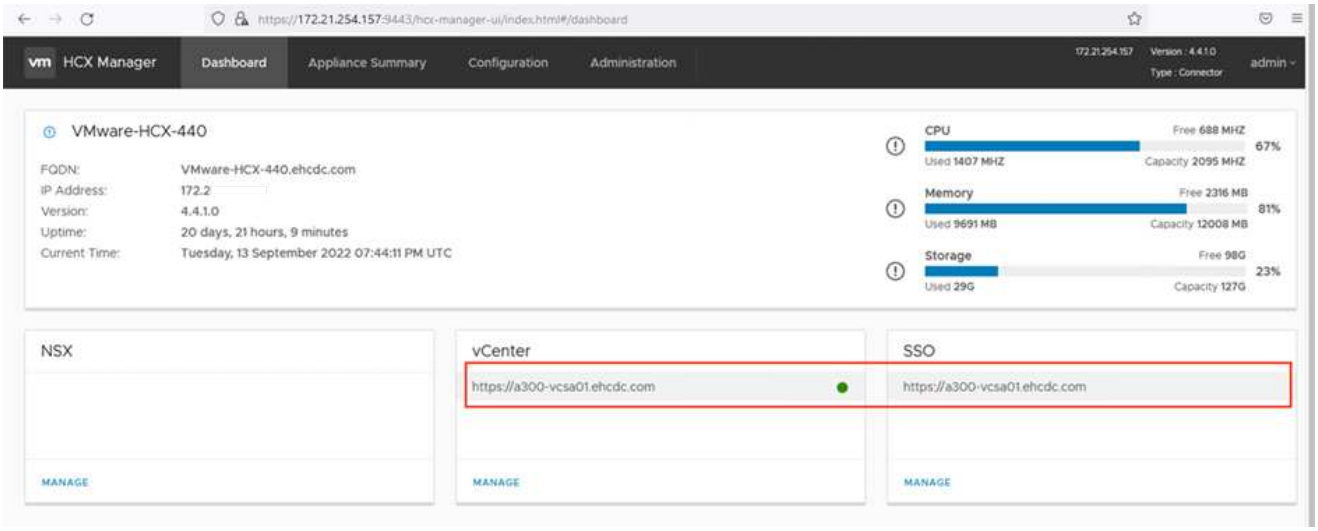
> Utilizzare l'FQDN per evitare problemi di comunicazione in un secondo momento.

9. In Configure SSO/PSC (Configura SSO/PSC), fornire l'indirizzo FQDN o IP del controller dei servizi della piattaforma e fare clic su Continue (continua).

Inserire l'indirizzo IP o l'FQDN del server vCenter.

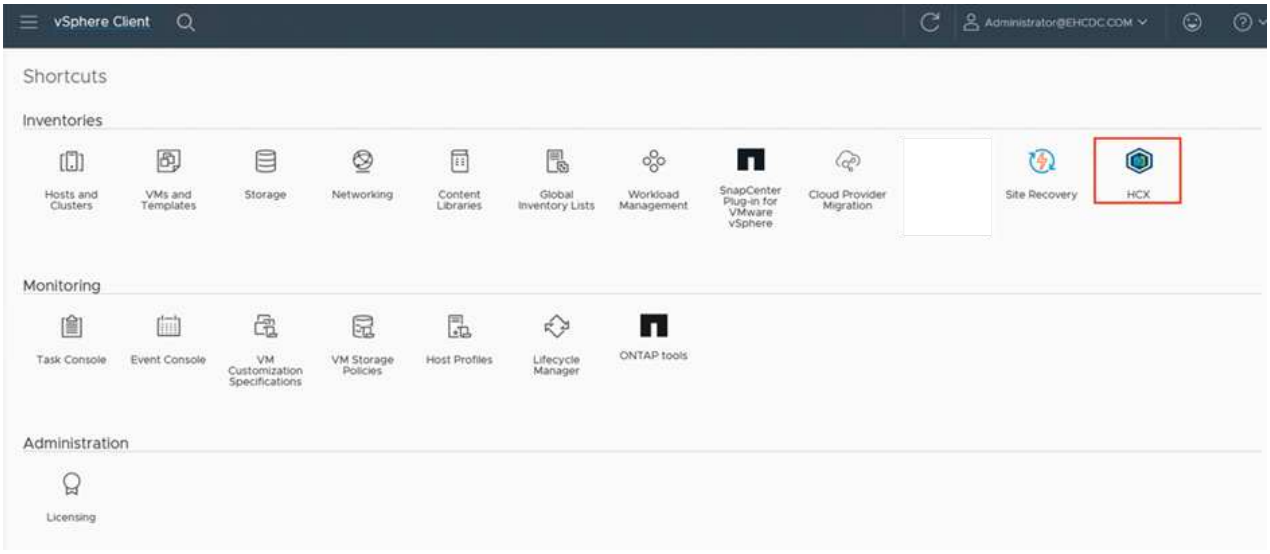
10. Verificare che le informazioni siano inserite correttamente e fare clic su Restart (Riavvia).
11. Al termine dell'operazione, vCenter Server viene visualizzato in verde. VCenter Server e SSO devono avere i parametri di configurazione corretti, che devono essere gli stessi della pagina precedente.

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

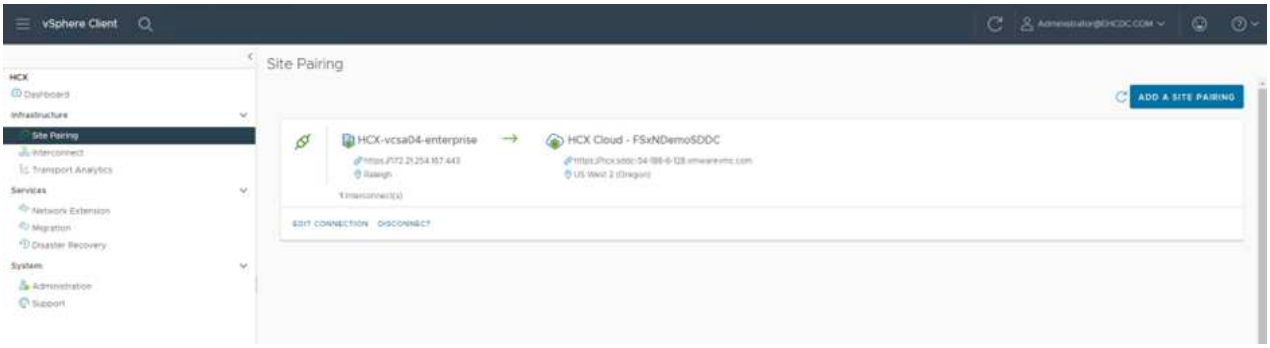


Fase 4: Associazione on-premise di VMware HCX Connector con VMC HCX Cloud Manager

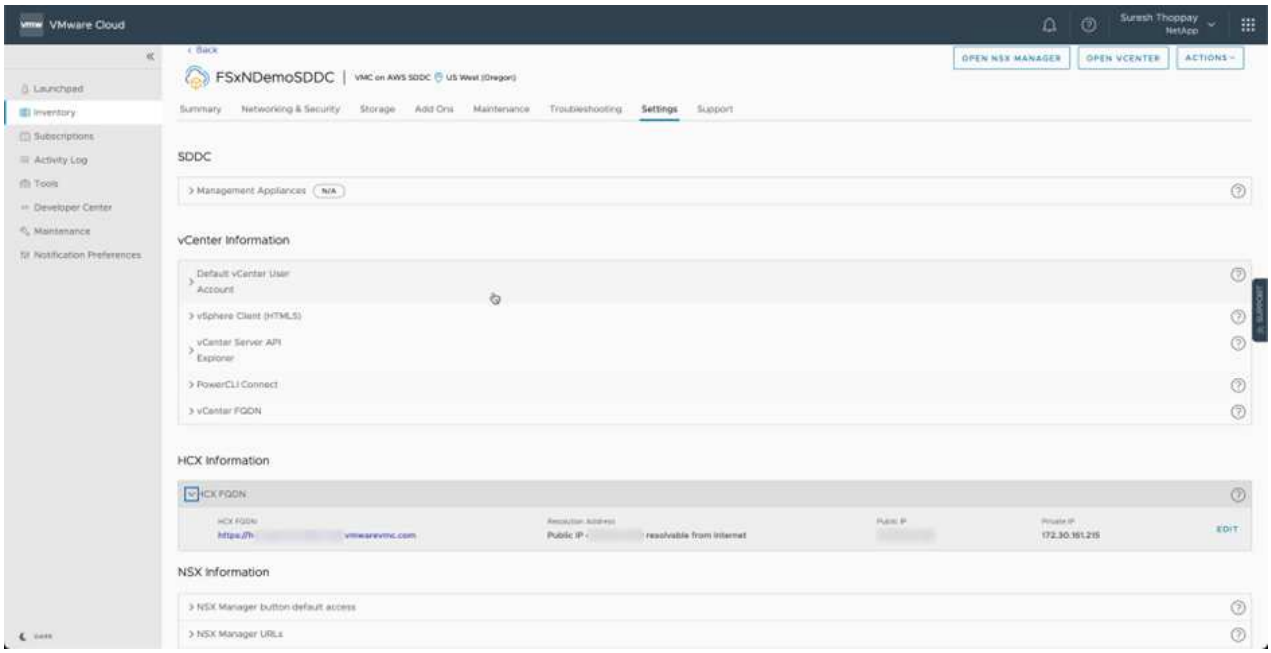
1. Per creare una coppia di siti tra vCenter Server on-premise e VMC SDDC, accedere al vCenter Server on-premise e al plug-in del client Web HCX vSphere.

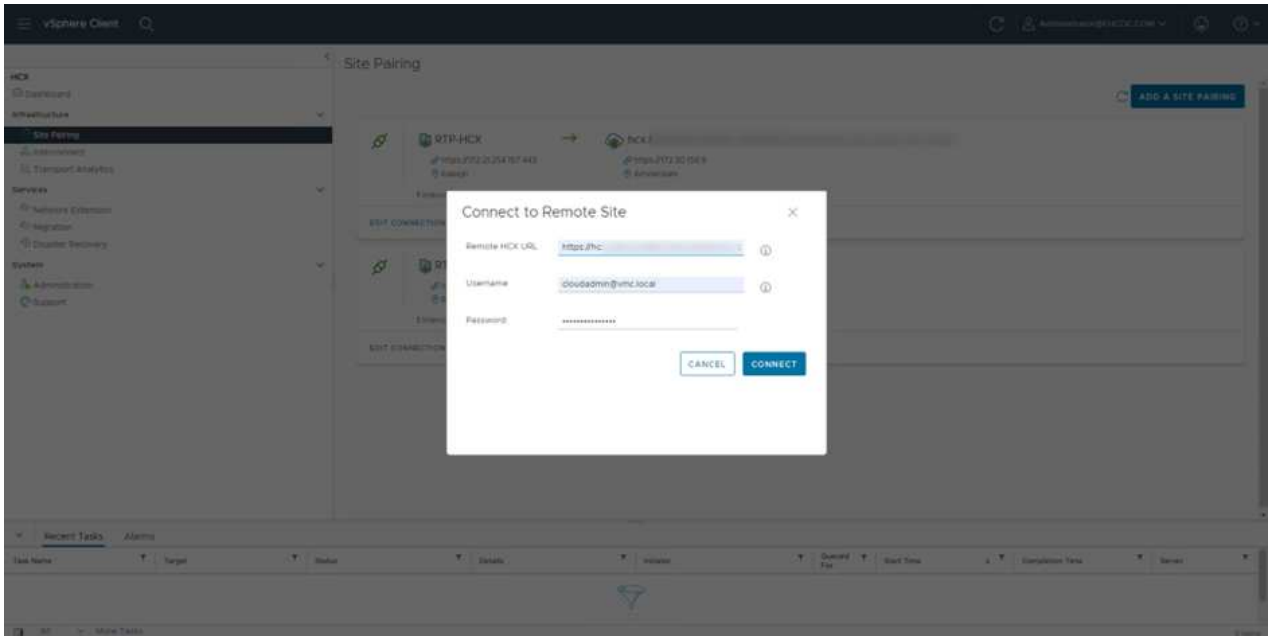


2. In infrastruttura, fare clic su Aggiungi associazione sito. Per autenticare il sito remoto, immettere l'URL o l'indirizzo IP di VMC HCX Cloud Manager e le credenziali per il ruolo CloudAdmin.



Le informazioni HCX possono essere recuperate dalla pagina Impostazioni SDDC.





3. Per avviare l'associazione del sito, fare clic su Connect (Connetti).

> VMware HCX Connector deve essere in grado di comunicare con HCX Cloud Manager IP sulla porta 443.

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

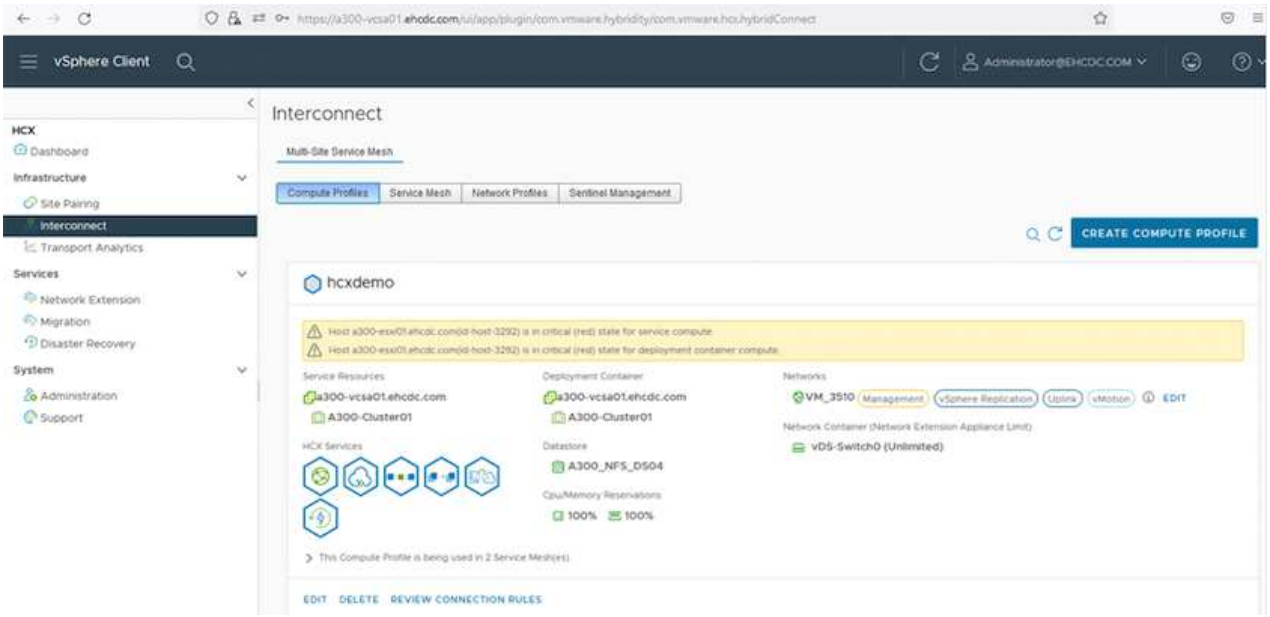
Fase 5: Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio

L'appliance VMware HCX Interconnect (HCX-IX) offre funzionalità di tunnel sicuro su Internet e connessioni private al sito di destinazione che consentono la replica e funzionalità basate su vMotion. L'interconnessione fornisce crittografia, ingegneria del traffico e una SD-WAN. Per creare l'appliance di interconnessione HCI-IX, attenersi alla seguente procedura:

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

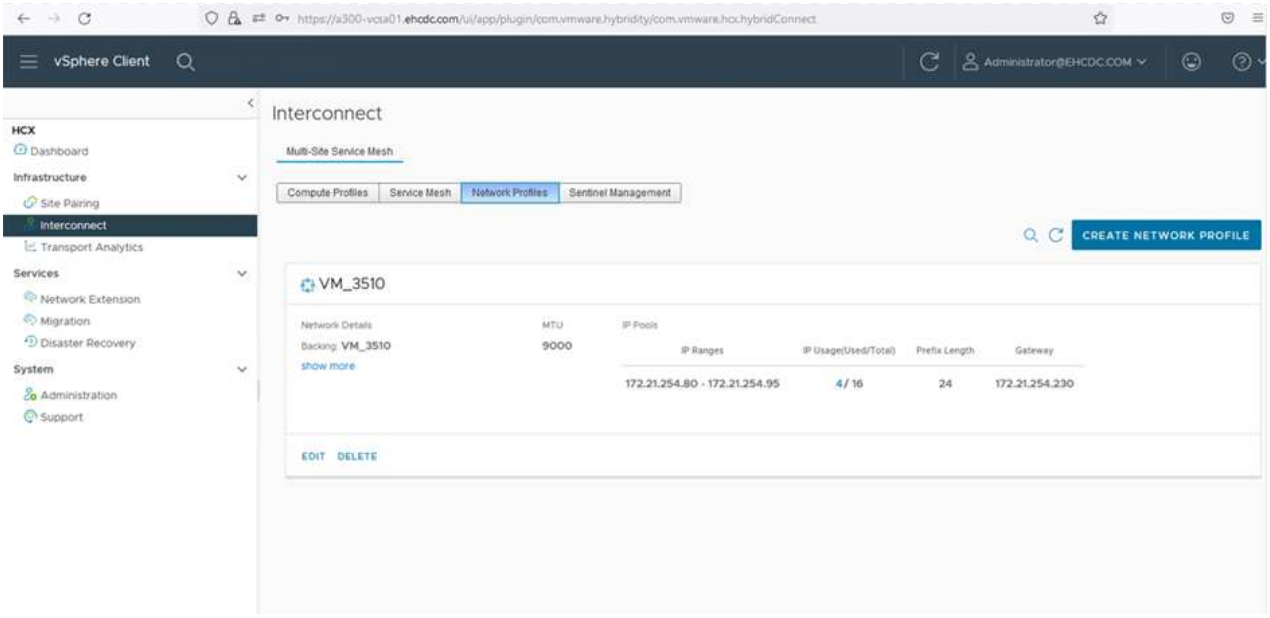
   I profili di calcolo contengono i parametri di calcolo, storage e implementazione di rete necessari per implementare un'appliance virtuale di interconnessione. Inoltre, specifica quale parte del data center VMware sarà accessibile al servizio HCX.

   Per istruzioni dettagliate, vedere "Creazione di un profilo di calcolo".



2. Una volta creato il profilo di calcolo, creare il profilo di rete selezionando Mesh servizio multi-sito > profili di rete > Crea profilo di rete.
3. Il profilo di rete definisce un intervallo di indirizzi IP e reti che VERRANNO utilizzati DA HCX per le proprie appliance virtuali.

   Questo richiede due o più indirizzi IP. Questi indirizzi IP verranno assegnati dalla rete di gestione alle appliance virtuali.

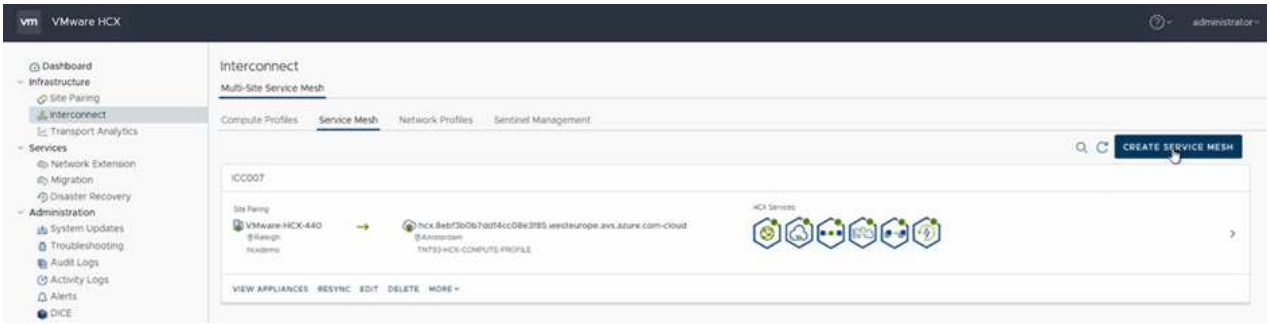


Per istruzioni dettagliate, vedere "Creazione di un profilo di rete".

Se si effettua la connessione a una SD-WAN tramite Internet, è necessario riservare gli IP pubblici nella sezione rete e sicurezza.

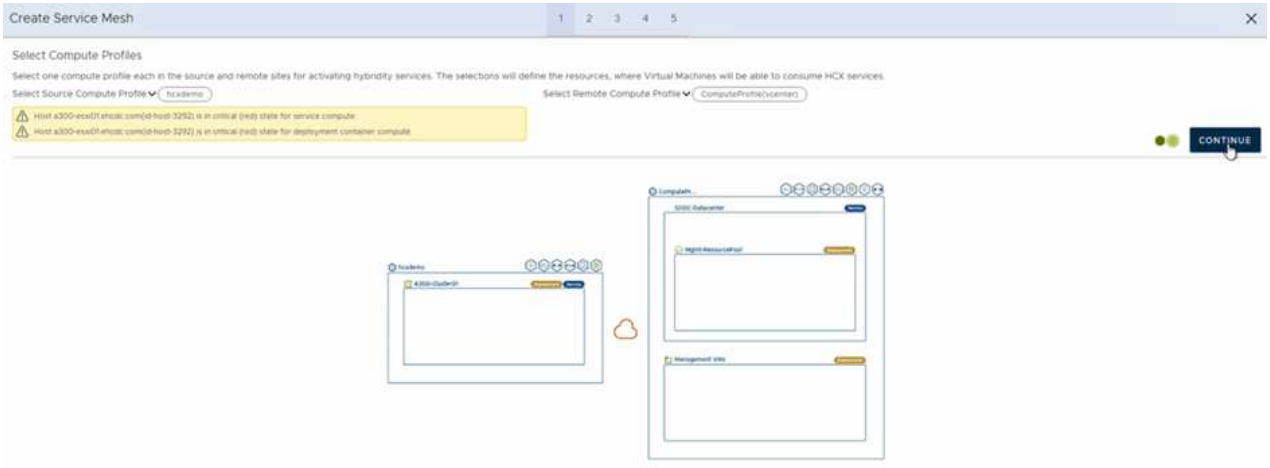
4. Per creare una mesh del servizio, selezionare la scheda Service Mesh (Mesh del servizio) all'interno dell'opzione Interconnect (interconnessione) e selezionare on-premise and VMC SDDC sites (siti SDDC on-premise e VMC).

   La mesh del servizio stabilisce una coppia di profili di rete e di calcolo locale e remoto.

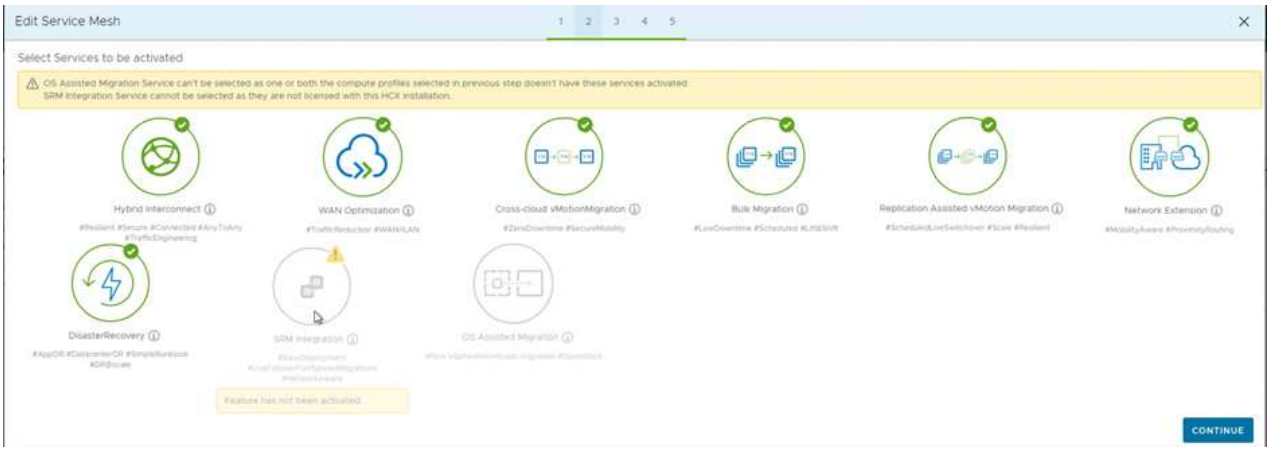


Parte di questo processo prevede l'implementazione di appliance HCX che verranno configurate automaticamente sui siti di origine e di destinazione, creando un fabric di trasporto sicuro.

5. Selezionare i profili di calcolo di origine e remoti e fare clic su Continue (continua).

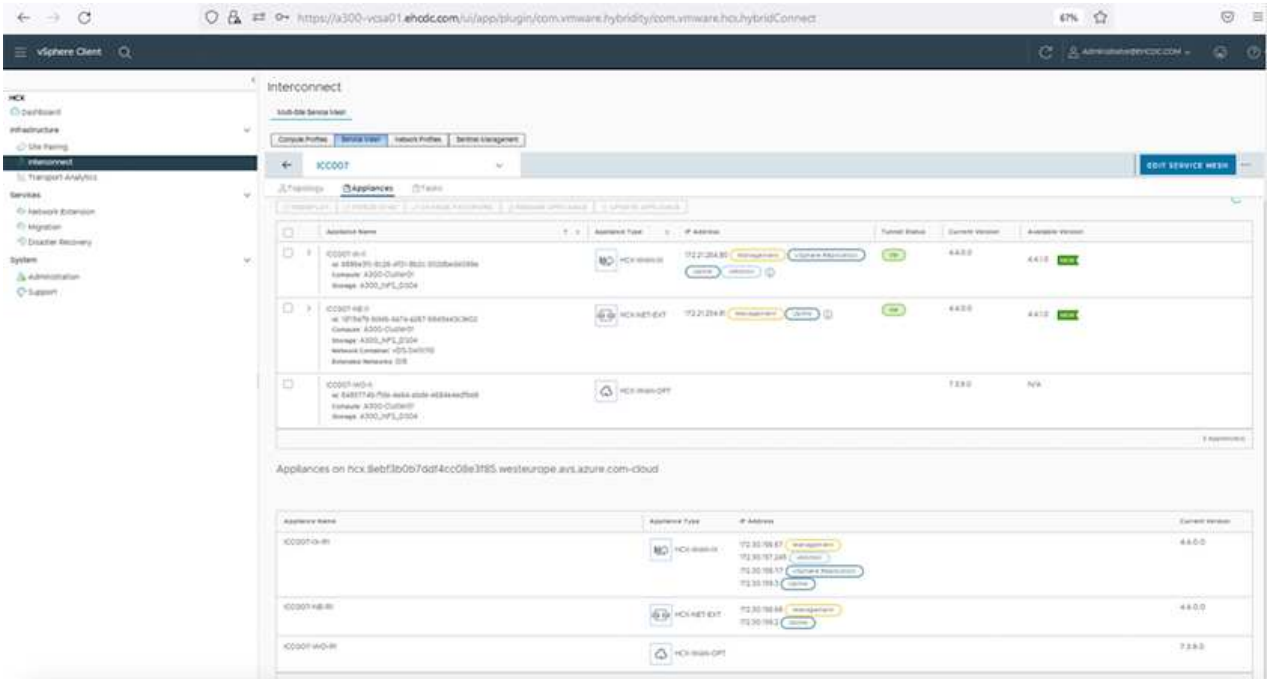


6. Selezionare il servizio da attivare e fare clic su Continue (continua).



Per la migrazione vMotion assistita da replica, l'integrazione SRM e la migrazione assistita dal sistema operativo è richiesta una licenza HCX Enterprise.

7. Creare un nome per la mesh del servizio e fare clic su Finish (fine) per avviare il processo di creazione. Il completamento dell'implementazione richiede circa 30 minuti. Dopo aver configurato la mesh del servizio, sono state create l'infrastruttura virtuale e il networking necessari per migrare le VM dei carichi di lavoro.


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

Fase 6: Migrazione dei carichi di lavoro

HCX offre servizi di migrazione bidirezionale tra due o più ambienti distinti, come gli SDDC on-premise e VMC. È possibile migrare i carichi di lavoro delle applicazioni da e verso i siti attivati DA HCX utilizzando una vasta gamma di 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 sulle tecnologie di migrazione HCX disponibili, consulta "Tipi di migrazione VMware HCX"

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

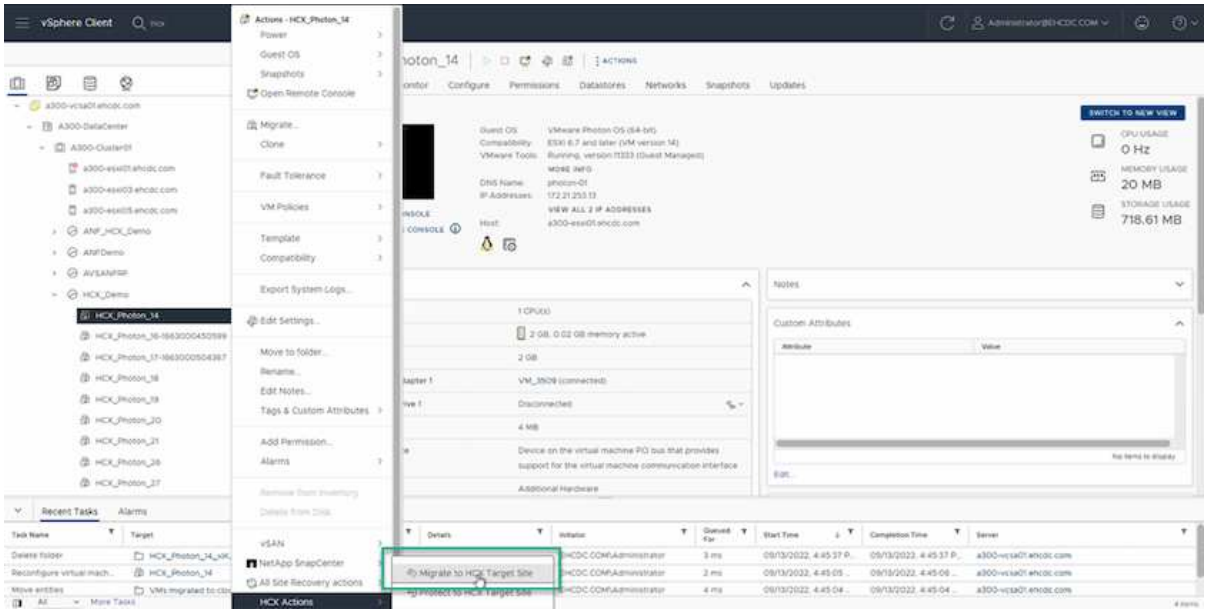
> L'appliance HCX-IX aggiunge il servizio Mobility Agent come oggetto host in vCenter Server. Il processore, la memoria, lo storage e le risorse di rete visualizzati su questo oggetto non rappresentano il consumo effettivo dell'hypervisor fisico che ospita l'appliance IX.

VMware HCX vMotion

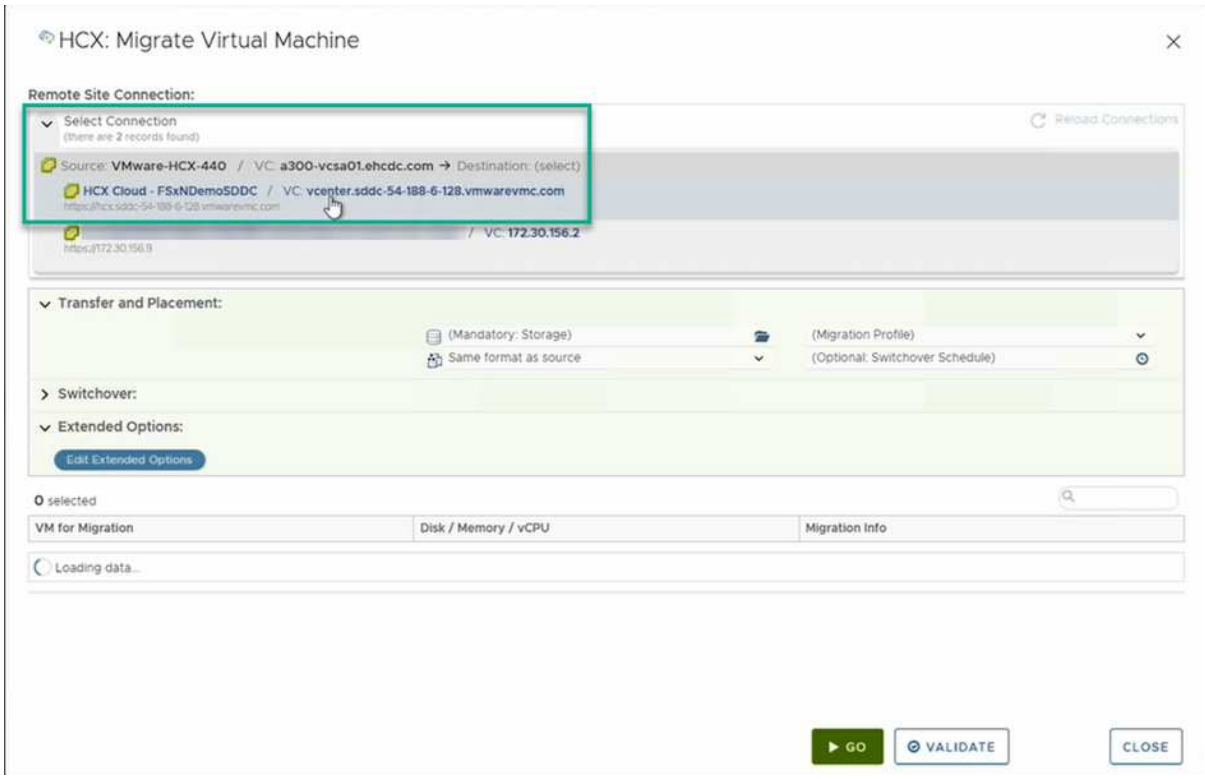
In questa sezione viene descritto il meccanismo vMotion DI HCX. Questa tecnologia di migrazione utilizza il protocollo VMware vMotion per migrare una macchina virtuale a VMC SDDC. L'opzione di migrazione vMotion viene utilizzata per la migrazione dello stato della macchina virtuale di una singola macchina 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.

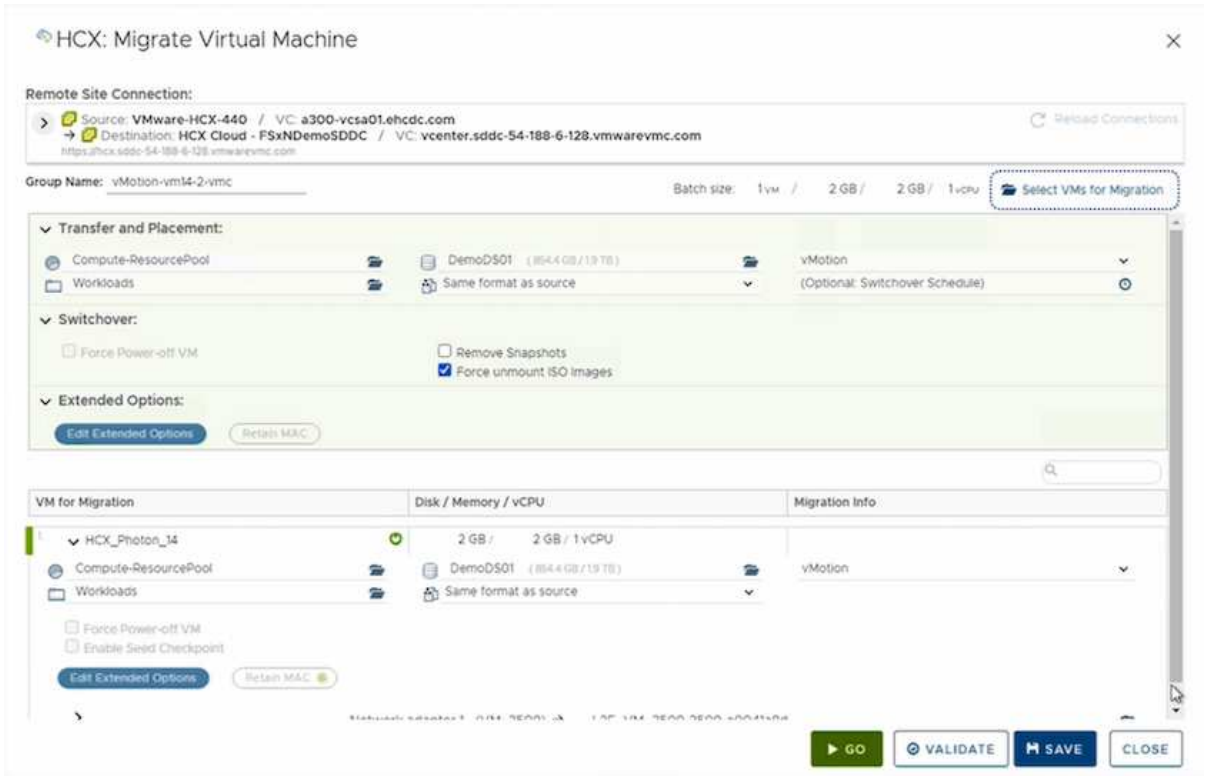
1. Dal client vSphere on-premise, accedere a Inventory (inventario), fare clic con il pulsante destro del mouse sulla macchina virtuale da migrare e selezionare HCX Actions (azioni HCX) > Migrate to HCX Target Site (Migra al sito di destinazione HCX).



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



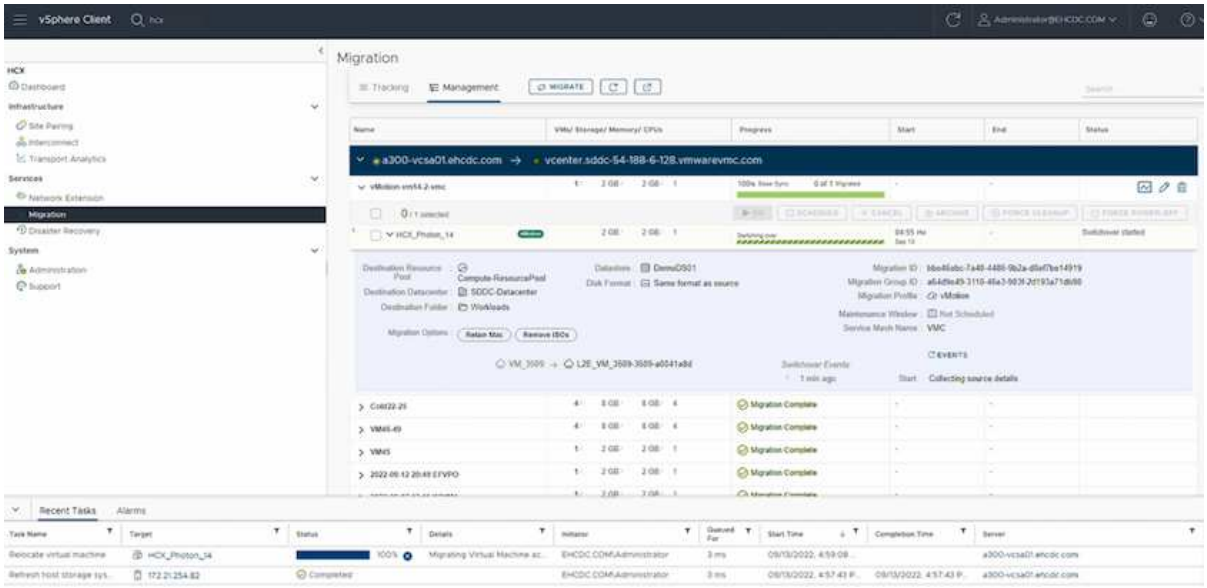
3. Aggiungere un nome di gruppo e, in Transfer and Placement (trasferimento e posizionamento), aggiornare i campi obbligatori (Cluster, Storage e Destination Network), quindi fare clic su Validate (convalida).



4. 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".

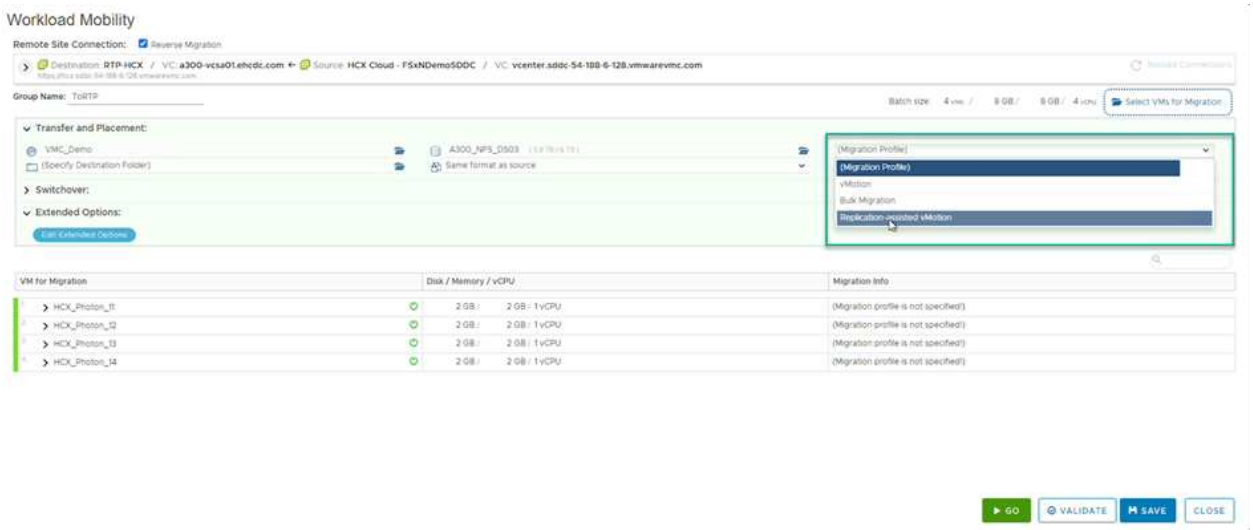
5. È possibile monitorare l'avanzamento e il completamento di vMotion dalla dashboard HCX > Migration (HCX > migrazione).



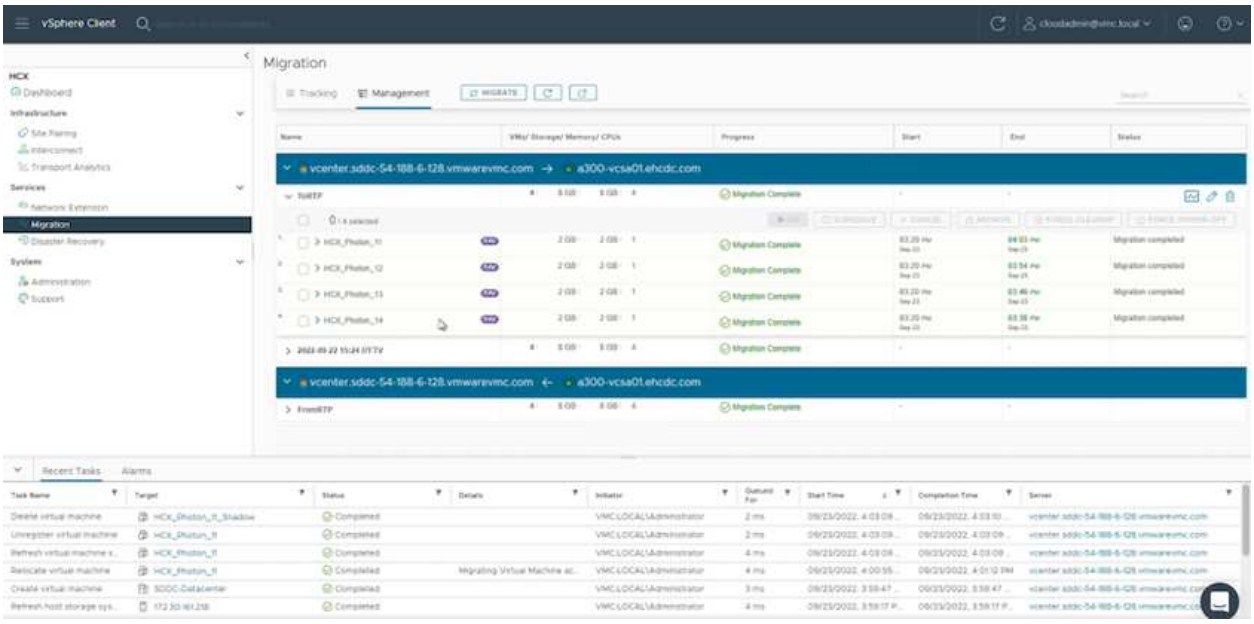
VMotion VMware Replication Assisted

Come si può notare dalla documentazione VMware, VMware HCX Replication Assisted vMotion (RAV) combina i vantaggi della migrazione in blocco e di vMotion. La migrazione in blocco utilizza la replica vSphere per migrare più macchine virtuali in parallelo: La macchina virtuale viene riavviata durante lo switchover. HCX vMotion esegue la migrazione senza downtime, ma viene eseguita in maniera seriale una macchina virtuale alla volta in un gruppo di replica. RAV replica la macchina virtuale in parallelo e la mantiene sincronizzata fino alla finestra di switchover. Durante il processo di switchover, effettua la migrazione di una macchina virtuale alla volta senza downtime per la macchina virtuale.

La seguente schermata mostra il profilo di migrazione come Replication Assisted vMotion.



La durata della replica potrebbe essere maggiore rispetto al vMotion di un numero ridotto di macchine virtuali. Con RAV, sincronizzare solo i delta e includere i contenuti della memoria. Di seguito viene riportata una schermata dello stato della migrazione, che mostra come l'ora di inizio della migrazione sia la stessa e l'ora di fine sia diversa per ciascuna macchina virtuale.



Per ulteriori informazioni sulle opzioni di migrazione HCX e su come migrare i carichi di lavoro da on-premise a VMware Cloud su AWS utilizzando HCX, consulta la "Guida utente di VMware HCX".

VMware HCX vMotion richiede un throughput di 100 Mbps o superiore.

Il datastore VMC FSX di destinazione per ONTAP deve disporre di spazio sufficiente per consentire 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, Amazon FSX per NetApp ONTAP insieme A HCX offrono opzioni eccellenti per implementare e migrare i carichi di lavoro riducendo al contempo il TCO rendendo i requisiti dei dati perfetti per il livello applicativo. Qualunque sia il caso d'utilizzo, scegli VMC insieme a FSX per il datastore ONTAP per una rapida realizzazione dei benefici 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 la replica VMware vSphere, VMware vMotion o persino la copia NFC.

Punti da asporto

I punti chiave di questo documento includono:

- Ora puoi utilizzare Amazon FSX ONTAP come datastore con VMC SDDC.
- È possibile migrare facilmente i dati da qualsiasi data center on-premise a VMC in esecuzione con FSX per datastore ONTAP
- È possibile espandere e ridurre facilmente il datastore FSX ONTAP per soddisfare i requisiti di capacità e performance durante l'attività di migrazione.

Dove trovare ulteriori informazioni

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

- Documentazione di VMware Cloud

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

- Documentazione di Amazon FSX per NetApp ONTAP

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

  Guida utente di VMware HCX

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

Disponibilità regionale: Datastore NFS supplementare per VMC

La disponibilità di datastore NFS supplementari su AWS / VMC è definita da Amazon. Innanzitutto, è necessario determinare se VMC e FSxN sono disponibili in una regione

specifica. Quindi, è necessario determinare se il datastore NFS supplementare FSxN è supportato in quella regione.

- Verificare la disponibilità di VMC "qui".
- La guida ai prezzi di Amazon offre informazioni su dove è disponibile FSxN (FSX ONTAP). Queste informazioni sono disponibili "qui".
- La disponibilità del datastore NFS supplementare FSxN per VMC sarà presto disponibile.

Mentre le informazioni sono ancora in fase di rilascio, il seguente grafico identifica il supporto corrente per VMC, FSxN e FSxN come datastore NFS supplementare.

Americhe

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
US East (Virginia del Nord)	Sì	Sì	Sì
USA Est (Ohio)	Sì	Sì	Sì
US West (California settentrionale)	Sì	No	No
STATI UNITI occidentali (Oregon)	Sì	Sì	Sì
GovCloud (ovest degli Stati Uniti)	Sì	Sì	Sì
Canada (centrale)	Sì	Sì	Sì
Sud America (San Paolo)	Sì	Sì	Sì

Ultimo aggiornamento: 2 giugno 2022.

EMEA

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
Europa (Irlanda)	Sì	Sì	Sì
Europa (Londra)	Sì	Sì	Sì
Europa (Francoforte)	Sì	Sì	Sì
Europa (Parigi)	Sì	Sì	Sì
Europa (Milano)	Sì	Sì	Sì
Europa (Stoccolma)	Sì	Sì	Sì

Ultimo aggiornamento: 2 giugno 2022.

Asia Pacifico

Regione AWS	Disponibilità VMC	Disponibilità FSX ONTAP	Disponibilità datastore NFS
Asia Pacifico (Sydney)	Sì	Sì	Sì
Asia Pacifico (Tokyo)	Sì	Sì	Sì
Asia Pacifico (Osaka)	Sì	No	No
Asia Pacifico (Singapore)	Sì	Sì	Sì
Asia Pacifico (Seul)	Sì	Sì	Sì
Asia Pacifico (Mumbai)	Sì	Sì	Sì

Asia Pacifico (Giacarta)	No	No	No
Asia Pacifico (Hong Kong)	Sì	Sì	Sì

Ultimo aggiornamento: 28 settembre 2022.

Funzionalità NetApp per Azure AVS

Scopri di più sulle funzionalità offerte da NetApp alla soluzione Azure VMware (AVS): Da NetApp come dispositivo di storage connesso come guest o come datastore NFS supplementare alla migrazione dei flussi di lavoro, all'estensione/diffusione nel cloud, al backup/ripristino e al disaster recovery.

Passare alla sezione relativa al contenuto desiderato selezionando una delle seguenti opzioni:

- "Configurazione di AVS in Azure"
- "Opzioni di storage NetApp per AVS"
- "Soluzioni cloud NetApp/VMware"

Configurazione di AVS in Azure

Come per i sistemi on-premise, la pianificazione di un ambiente di virtualizzazione basato sul cloud è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire Azure VMware Solution e utilizzarla in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP alla soluzione VMware Azure.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Registrare il provider di risorse e creare un cloud privato
- Connettersi a un gateway di rete virtuale ExpressRoute nuovo o esistente
- Convalidare la connettività di rete e accedere al cloud privato

Visualizza i dettagli "Procedura di configurazione per AVS".

Opzioni di storage NetApp per AVS

Lo storage NetApp può essere utilizzato in diversi modi, come congettura connessa o come datastore NFS supplementare, all'interno di Azure AVS.

Visitare il sito "Opzioni di storage NetApp supportate" per ulteriori informazioni.

Azure supporta lo storage NetApp nelle seguenti configurazioni:

- Azure NetApp Files (ANF) come storage connesso guest

- Cloud Volumes ONTAP (CVO) come storage connesso guest
- Azure NetApp Files (ANF) come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per AVS". Visualizza i dettagli "Opzioni aggiuntive del datastore NFS per AVS".

Casi di utilizzo della soluzione

Con le soluzioni cloud NetApp e VMware, molti casi di utilizzo sono semplici da implementare in Azure AVS. I casi se sono definiti per ciascuna delle aree cloud definite da VMware:

- Protect (include disaster recovery e backup/ripristino)
- Estendi
- Migrare

"Esplora le soluzioni NetApp per Azure AVS"

Protezione dei carichi di lavoro su Azure/AVS

Disaster Recovery con ANF e JetStream

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i carichi di lavoro da interruzioni del sito ed eventi di corruzione dei dati (ad esempio ransomware). Utilizzando il framework VMware VAIO, è possibile replicare i workload VMware on-premise sullo storage Azure Blob e ripristinarli, consentendo una perdita di dati minima o quasi nulla e un RTO quasi nullo.

Il DR Jetstream può essere utilizzato per ripristinare perfettamente i carichi di lavoro replicati da on-premise ad AVS e in particolare a Azure NetApp Files. Consente un disaster recovery conveniente utilizzando risorse minime presso il sito di DR e uno storage cloud conveniente. Jetstream DR automatizza il ripristino degli archivi dati ANF tramite Azure Blob Storage. Jetstream DR ripristina macchine virtuali indipendenti o gruppi di macchine virtuali correlate nell'infrastruttura del sito di ripristino in base alla mappatura di rete e fornisce un ripristino point-in-time per la protezione ransomware.

Il presente documento fornisce informazioni sui principi operativi di DR di JetStream e sui relativi componenti principali.

Panoramica sull'implementazione della soluzione

1. Installare il software DR JetStream nel data center on-premise.
   a. Scarica il pacchetto software DR JetStream da Azure Marketplace (ZIP) e implementa il DR MSA (OVA) JetStream nel cluster designato.
   b. Configurare il cluster con il pacchetto di filtri i/o (installare JetStream VIB).
   c. Provisioning di Azure Blob (Azure Storage account) nella stessa regione del cluster DR AVS.
   d. Implementare appliance DRVA e assegnare volumi di log di replica (VMDK da datastore esistente o storage iSCSI condiviso).
   e. Creare domini protetti (gruppi di macchine virtuali correlate) e assegnare DRVA e Azure Blob Storage/ANF.
   f. Protezione all'avviamento.
2. Installare il software DR JetStream nel cloud privato Azure VMware Solution.
   a. Utilizzare il comando Esegui per installare e configurare il DR JetStream.
   b. Aggiungere lo stesso container Azure Blob e individuare i domini utilizzando l'opzione Scan Domains (domini di scansione).
   c. Implementare le appliance DRVA richieste.
   d. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
   e. Importare domini protetti e configurare ROCvA (Recovery VA) per utilizzare il datastore ANF per il posizionamento delle macchine virtuali.
   f. Selezionare l'opzione di failover appropriata e avviare la reidratazione continua per domini RTO o macchine virtuali quasi a zero.
3. Durante un evento di emergenza, attivare il failover degli archivi dati Azure NetApp Files nel sito di DR AVS designato.
4. Richiamare il failback sul sito protetto dopo il ripristino del sito protetto.prima di iniziare, assicurarsi che i prerequisiti siano soddisfatti, come indicato in questa sezione "collegamento" Inoltre, eseguire il Bandwidth Testing Tool (BWT) fornito dal software JetStream per valutare le performance potenziali dello storage Azure Blob e la relativa larghezza di banda di replica se utilizzato con il software DR JetStream. Una volta implementati i prerequisiti, inclusa la connettività, impostare e sottoscrivere JetStream DR per AVS da "Azure Marketplace". Una volta scaricato il pacchetto software, procedere con la procedura di installazione descritta in precedenza.

Quando si pianifica e si avvia la protezione per un gran numero di macchine virtuali (ad esempio, 100+), utilizzare il Capacity Planning Tool (CPT) di JetStream DR Automation Toolkit. Fornire un elenco di macchine virtuali da proteggere insieme alle preferenze RTO e del gruppo di ripristino, quindi eseguire CPT.

CPT esegue le seguenti funzioni:

- Combinazione di macchine virtuali in domini di protezione in base al proprio RTO.
- Definizione del numero ottimale di DRVA e delle relative risorse.
- Stima della larghezza di banda di replica richiesta.
- Identificazione delle caratteristiche del volume del registro di replica (capacità, larghezza di banda e così via).
- Stima della capacità di storage a oggetti richiesta e molto altro ancora.

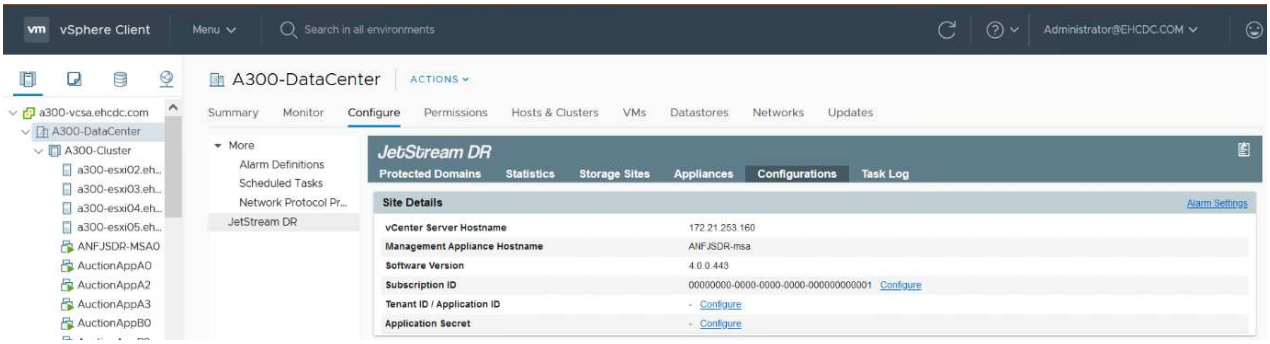
Il numero e il contenuto dei domini prescritti dipendono da diverse caratteristiche delle macchine virtuali, come IOPS medi, capacità totale, priorità (che definisce l'ordine di failover), RTO e altre.

Installare JetStream DR in Datacenter on-premise

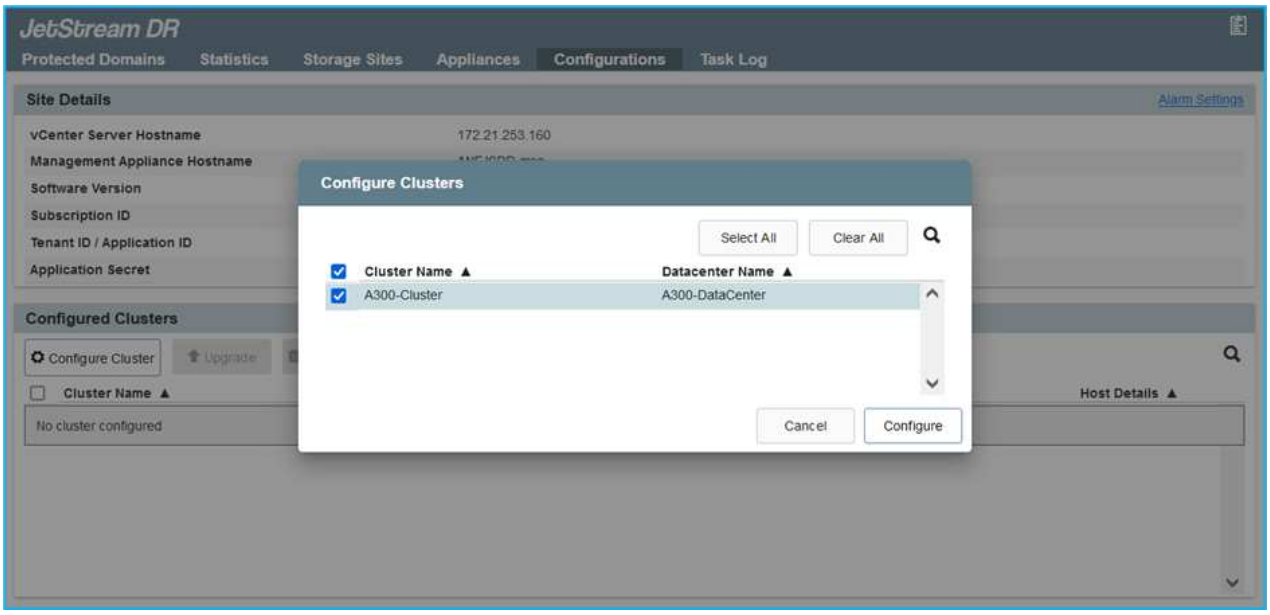
Il software Jetstream DR è costituito da tre componenti principali: Appliance virtuale Jetstream DR Management Server (MSA), appliance virtuale DR (DRVA) e componenti host (pacchetti di filtro i/o). MSA viene utilizzato per installare e configurare i componenti host sul cluster di calcolo e quindi per amministrare il software DR JetStream. Il seguente elenco fornisce una descrizione dettagliata del processo di installazione:

Come installare JetStream DR per on-premise

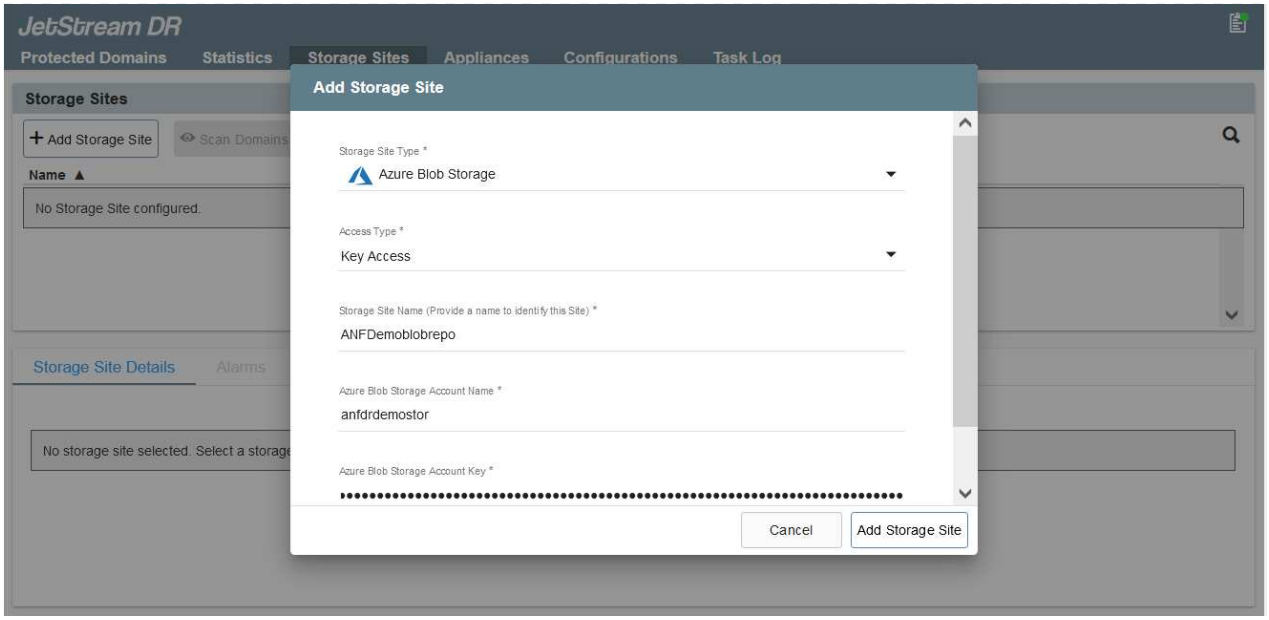
1. Verificare i prerequisiti.
2. Eseguire Capacity Planning Tool per ottenere consigli su risorse e configurazione (facoltativo ma consigliato per le prove proof-of-concept).
3. Implementare l'MSA DR JetStream su un host vSphere nel cluster designato.
4. Avviare MSA utilizzando il nome DNS in un browser.
5. Registrare il server vCenter con MSA.per eseguire l'installazione, attenersi alla seguente procedura dettagliata:
6. Una volta implementato JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR utilizzando vSphere Web Client. Per eseguire questa operazione, accedere a Datacenter > Configure > JetStream DR.



7. Dall'interfaccia DR di JetStream, selezionare il cluster appropriato.



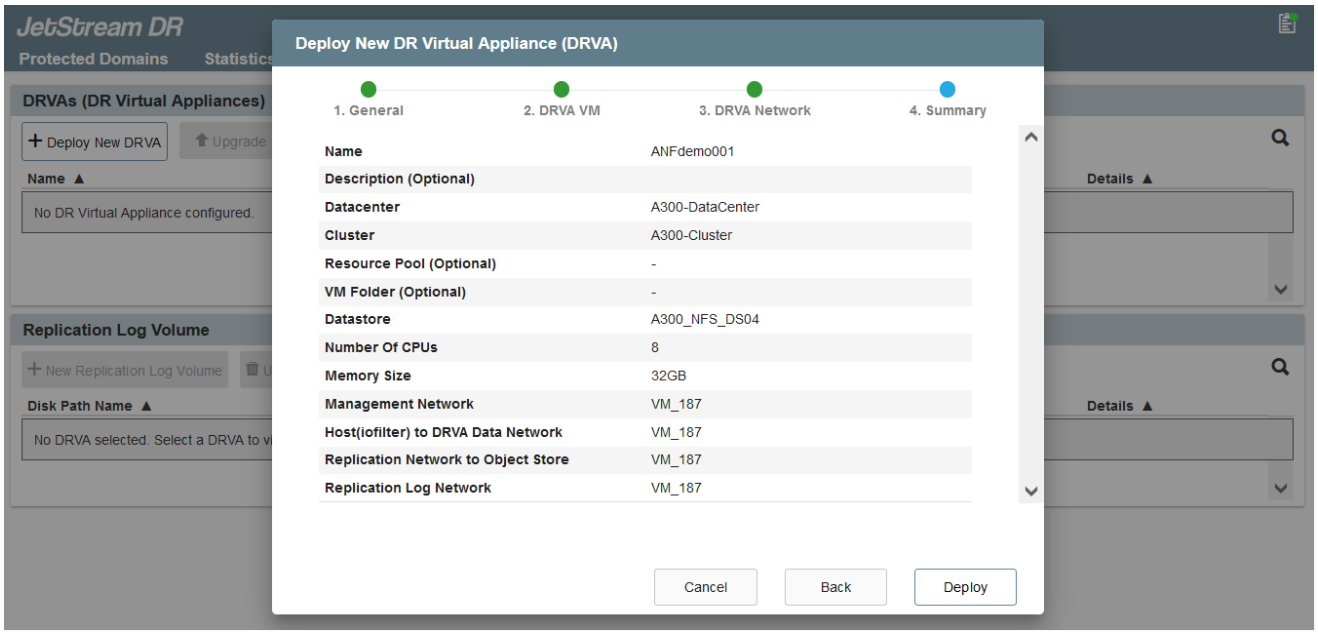
8. Configurare il cluster con il pacchetto di filtri i/O.



9. Aggiungere Azure Blob Storage situato nel sito di ripristino.
10. Implementare un'appliance virtuale DR (DRVA) dalla scheda Appliances (appliance).

> I DRA possono essere creati automaticamente dal CPT, ma per le prove POC consigliamo di configurare ed eseguire manualmente il ciclo di DR (protezione dell'avvio > failover > failback).

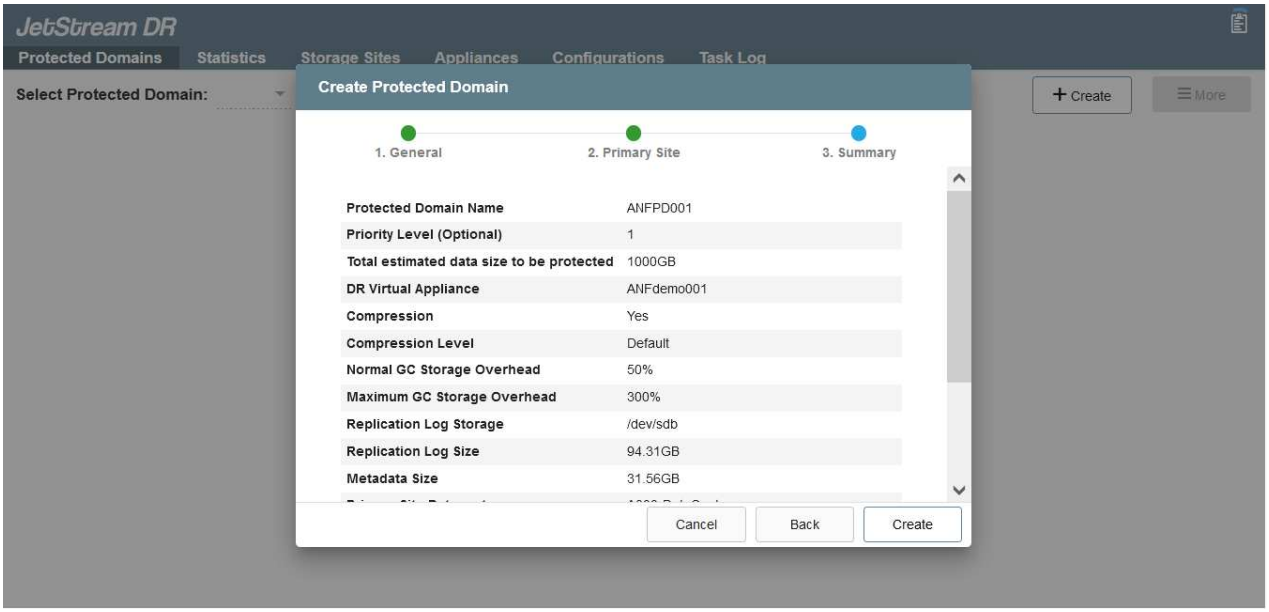
JetStream DRVA è un'appliance virtuale che facilita le funzioni chiave nel processo di replica dei dati. Un cluster protetto deve contenere almeno un DRVA e, in genere, un DRVA viene configurato per host. Ogni DRVA può gestire più domini protetti.



In questo esempio, sono stati creati quattro DRVA per 80 macchine virtuali.

1. Creare volumi di log di replica per ogni DRVA utilizzando VMDK dagli archivi dati disponibili o da pool di storage iSCSI condivisi indipendenti.

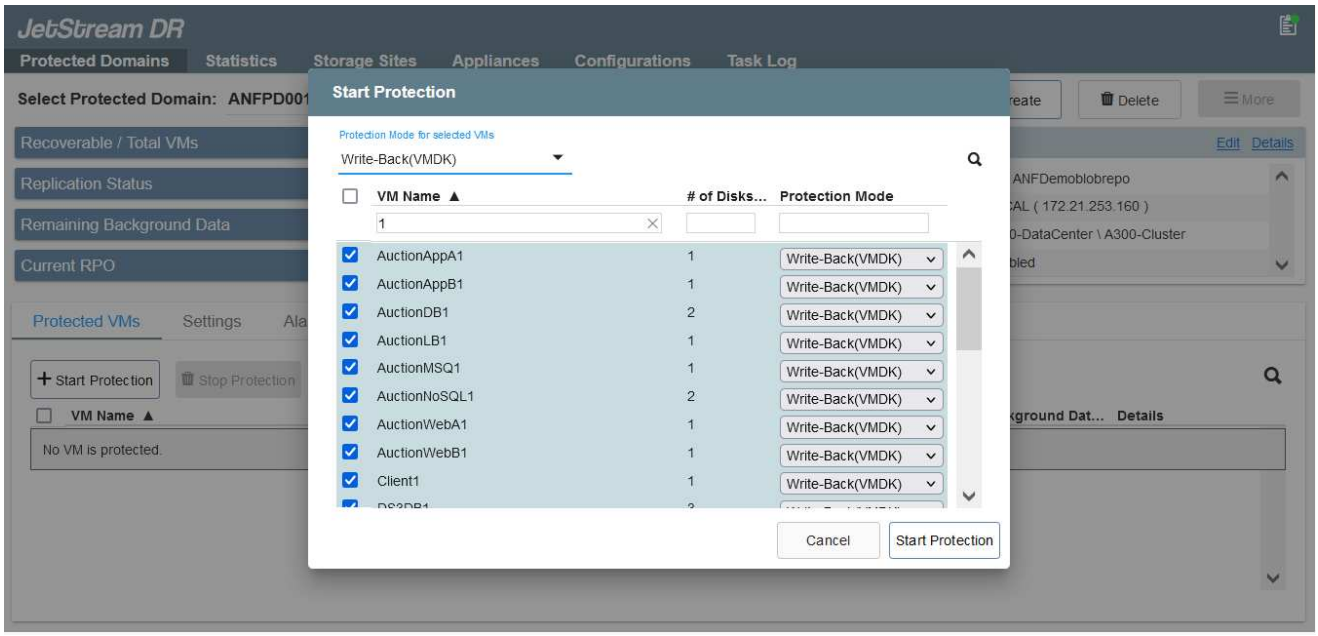
2. Dalla scheda Protected Domains (domini protetti), creare il numero richiesto di domini protetti utilizzando le informazioni relative al sito Azure Blob Storage, all'istanza DRVA e al registro di replica. Un dominio protetto definisce una macchina virtuale specifica o un insieme di macchine virtuali all'interno del cluster che sono protetti insieme e assegnati a un ordine di priorità per le operazioni di failover/failback.



3. Selezionare le macchine virtuali che si desidera proteggere e avviare la protezione delle macchine virtuali del dominio protetto. In questo modo viene avviata la replica dei dati nell'archivio Blob designato.

Verificare che venga utilizzata la stessa modalità di protezione per tutte le macchine virtuali in un dominio protetto.

La modalità Write-Back (VMDK) può offrire performance superiori.



Verificare che i volumi dei log di replica siano posizionati su uno storage dalle performance elevate.

> I run book di failover possono essere configurati per raggruppare le macchine virtuali (denominate Recovery Group), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

Installare JetStream DR per AVS in un cloud privato Azure VMware Solution utilizzando il comando Run

Una Best practice per un sito di recovery (AVS) consiste nella creazione anticipata di un cluster pilota a tre nodi. Ciò consente di preconfigurare l'infrastruttura del sito di ripristino, inclusi i seguenti elementi:

- Segmenti di rete di destinazione, firewall, servizi come DHCP e DNS e così via.
- Installazione di JetStream DR per AVS
- Configurazione dei volumi ANF come datastore e inoltre JetStream DR supporta la modalità RTO quasi zero per i domini mission-critical. Per questi domini, lo storage di destinazione deve essere preinstallato. ANF è un tipo di storage consigliato in questo caso.

> La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS per soddisfare i requisiti on-premise.

A seconda dei requisiti SLA e RTO, è possibile utilizzare il failover continuo o la normale modalità di failover (standard). Per un RTO vicino allo zero, è necessario avviare una procedura di reidratazione continua presso il sito di ripristino.

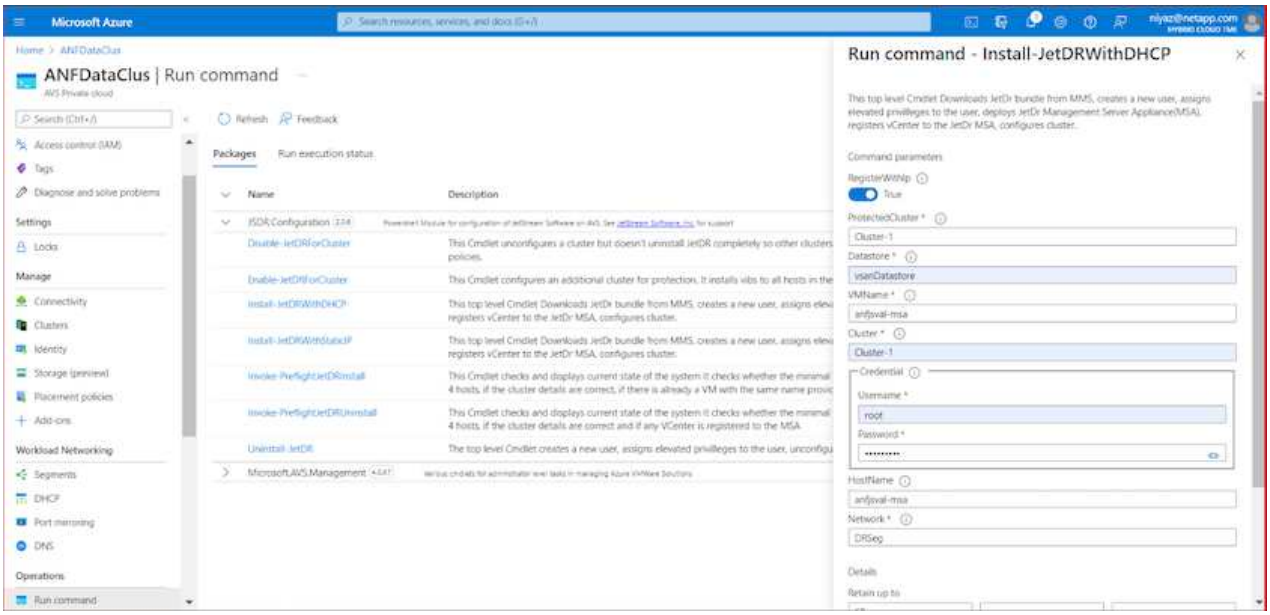
Come installare JetStream DR per AVS in un cloud privato

Per installare JetStream DR per AVS su un cloud privato Azure VMware Solution, attenersi alla seguente procedura:

1. Dal portale Azure, accedere alla soluzione Azure VMware, selezionare il cloud privato e selezionare Esegui comando > pacchetti > Configurazione JSDR.

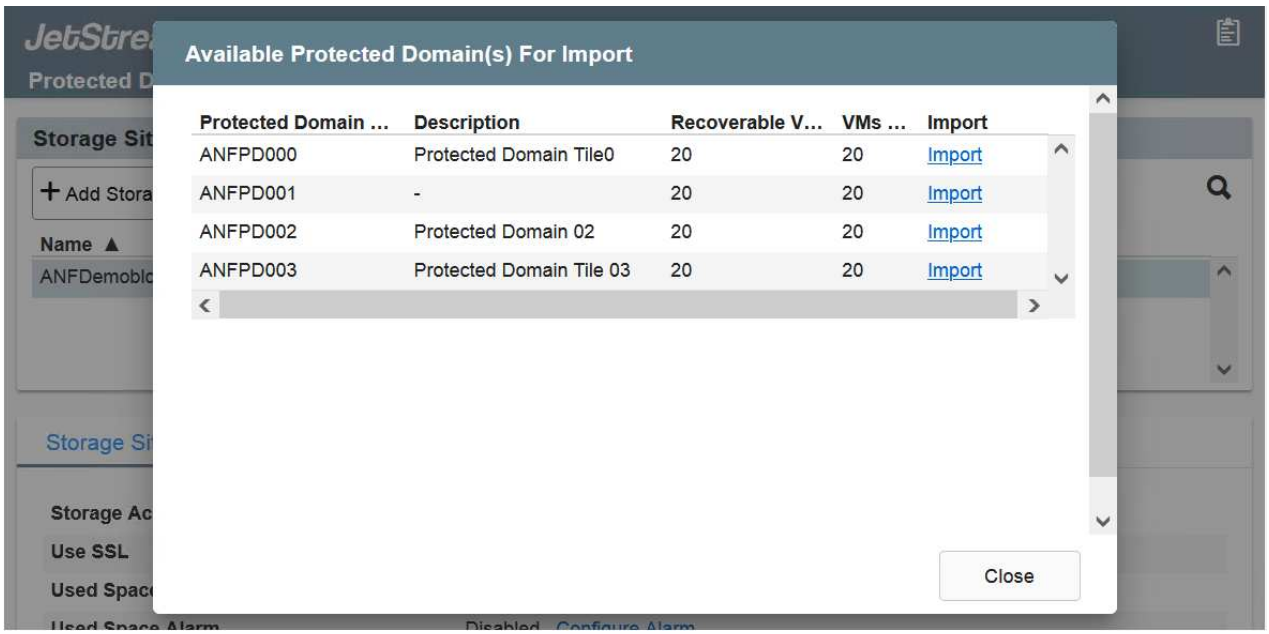
> L'utente CloudAdmin predefinito in Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente un'installazione semplificata e automatica del DR JetStream invocando il comando Azure VMware Solution Run per il DR JetStream.

La seguente schermata mostra l'installazione utilizzando un indirizzo IP basato su DHCP.



2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente DR JetStream, accedere a SDDC Datacenter > Configure > JetStream DR.

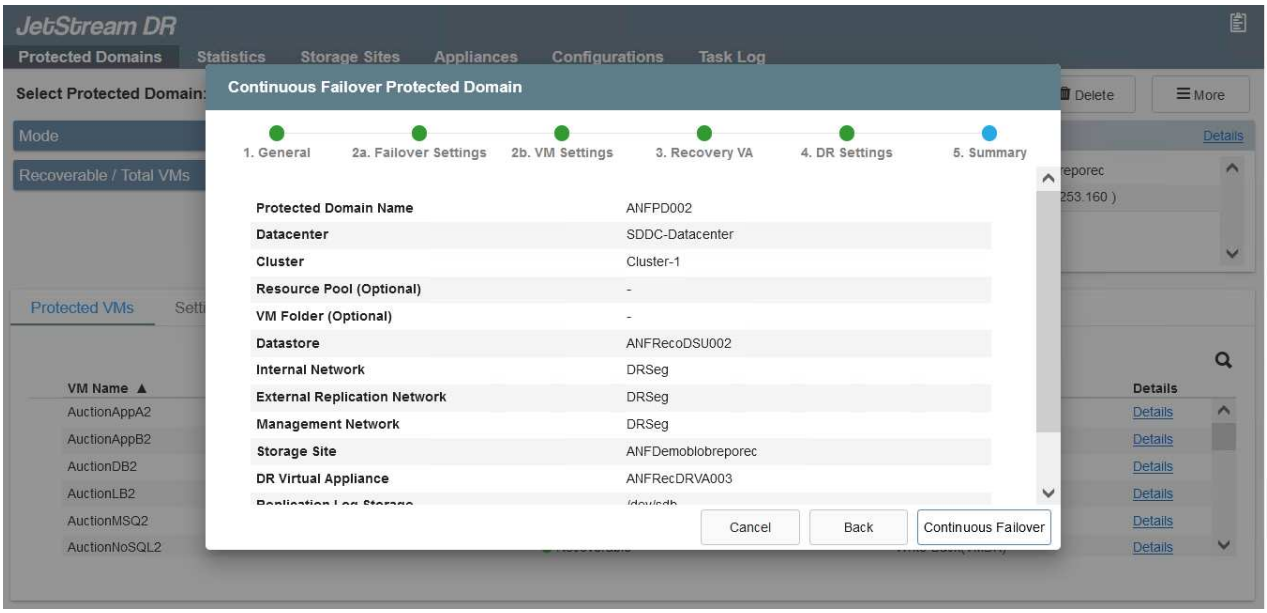
3. Dall'interfaccia DR di JetStream, aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster on-premise come sito di storage, quindi eseguire l'opzione Scan Domains.



4. Una volta importati i domini protetti, implementare le appliance DRVA. In questo esempio, la reidratazione continua viene avviata manualmente dal sito di ripristino utilizzando l'interfaccia utente DR JetStream.

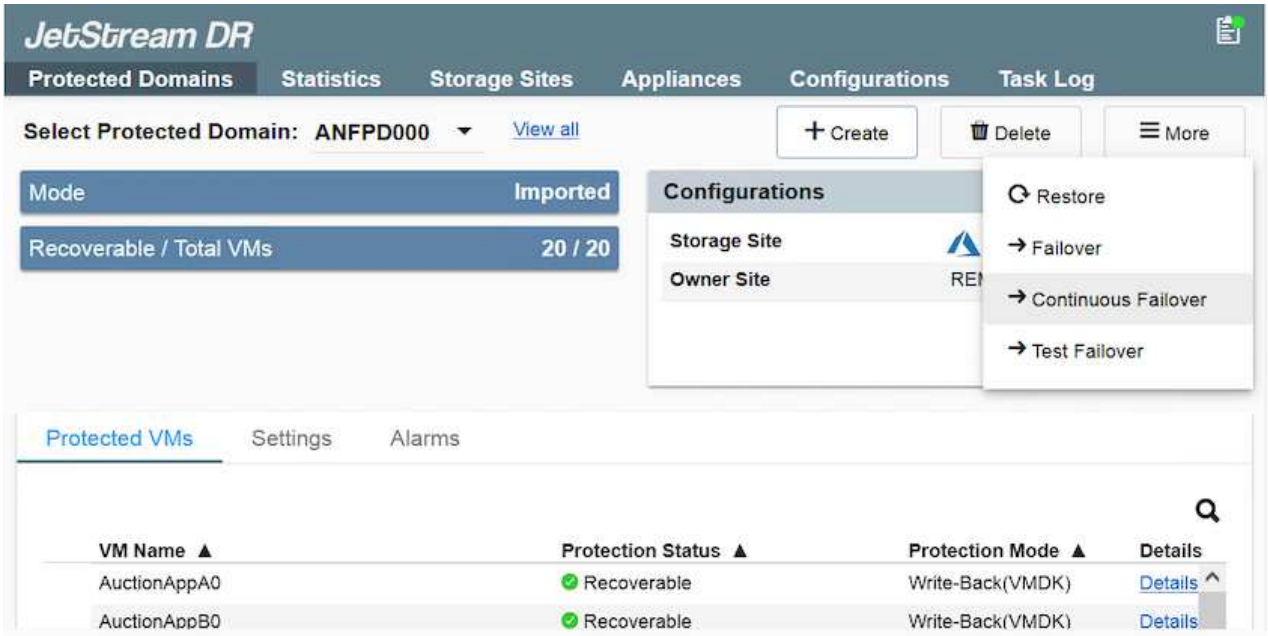
> Questi passaggi possono anche essere automatizzati utilizzando i piani creati da CPT.

5. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
6. Importare i domini protetti e configurare Recovery VA in modo che utilizzi il datastore ANF per il posizionamento delle macchine virtuali.



Assicurarsi che DHCP sia attivato sul segmento selezionato e che sia disponibile un numero sufficiente di IP. Gli IP dinamici vengono temporaneamente utilizzati durante il ripristino dei domini. Ogni macchina virtuale di ripristino (inclusa la reidratazione continua) richiede un IP dinamico individuale. Una volta completato il ripristino, l'IP viene rilasciato e può essere riutilizzato.

7. Selezionare l'opzione di failover appropriata (failover o failover continuo). In questo esempio, viene selezionata la reidratazione continua (failover continuo).



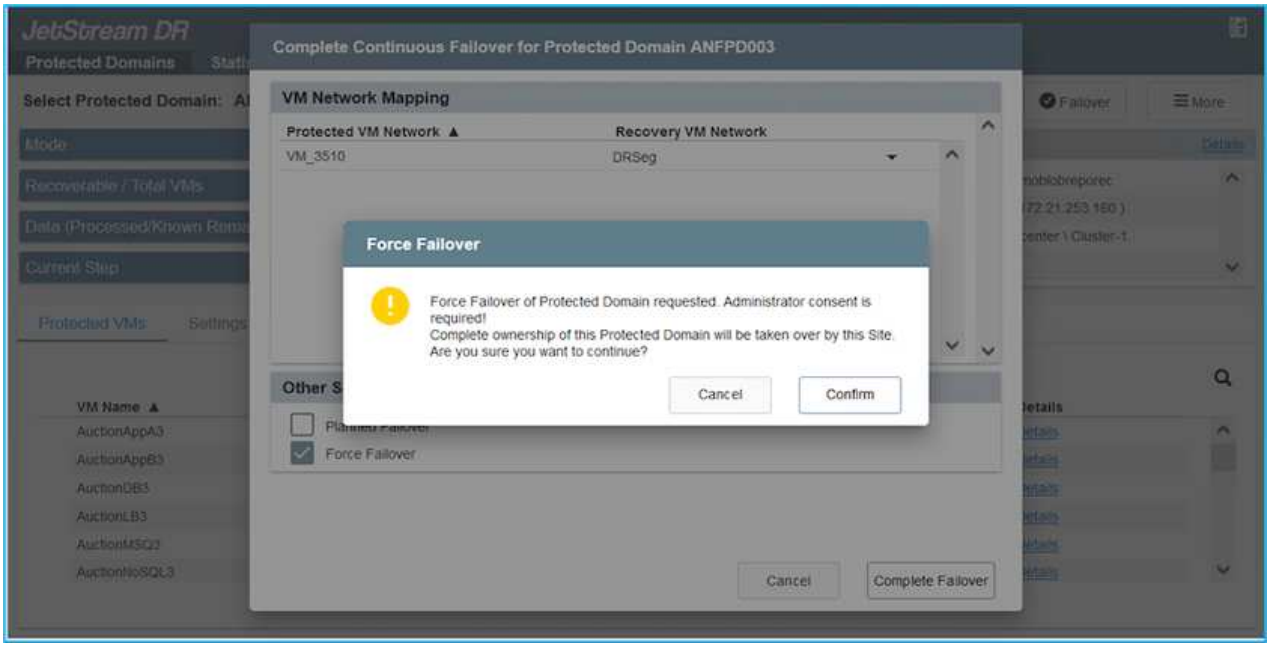
Esecuzione di failover/failover

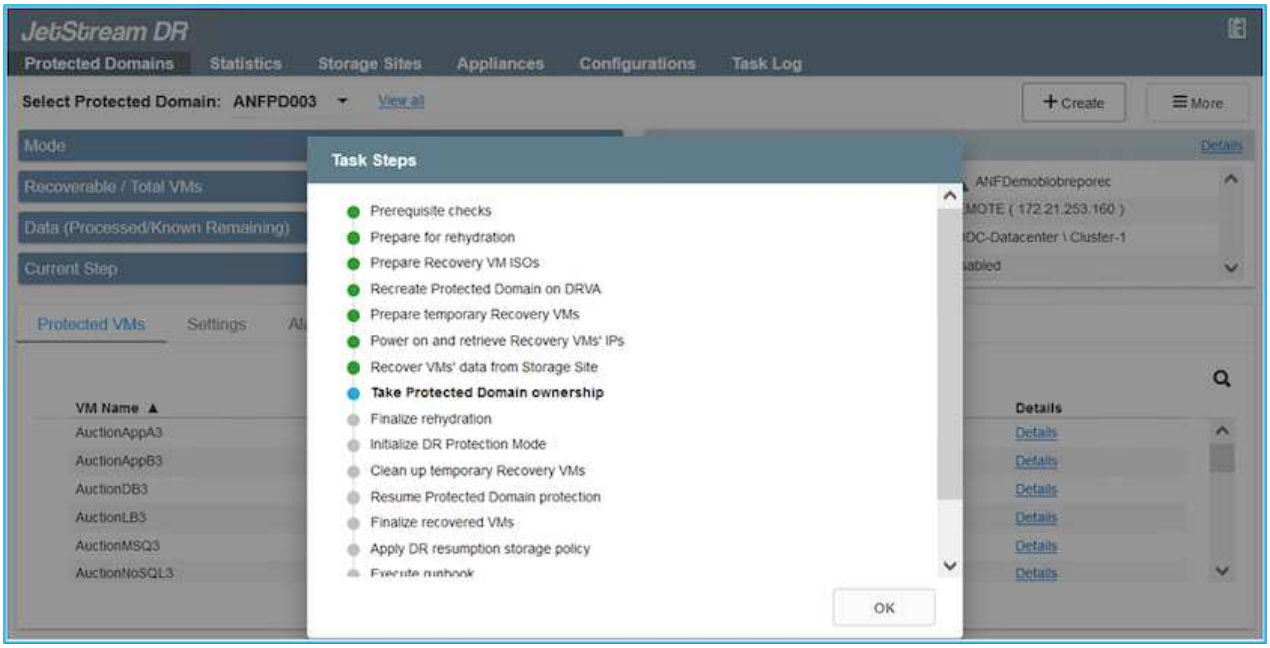
Come eseguire un failover/failover

1. In caso di disastro nel cluster protetto dell'ambiente on-premise (errore parziale o completo), attivare il failover.

   CPT può essere utilizzato per eseguire il piano di failover per ripristinare le macchine virtuali da Azure Blob Storage nel sito di ripristino del cluster AVS.

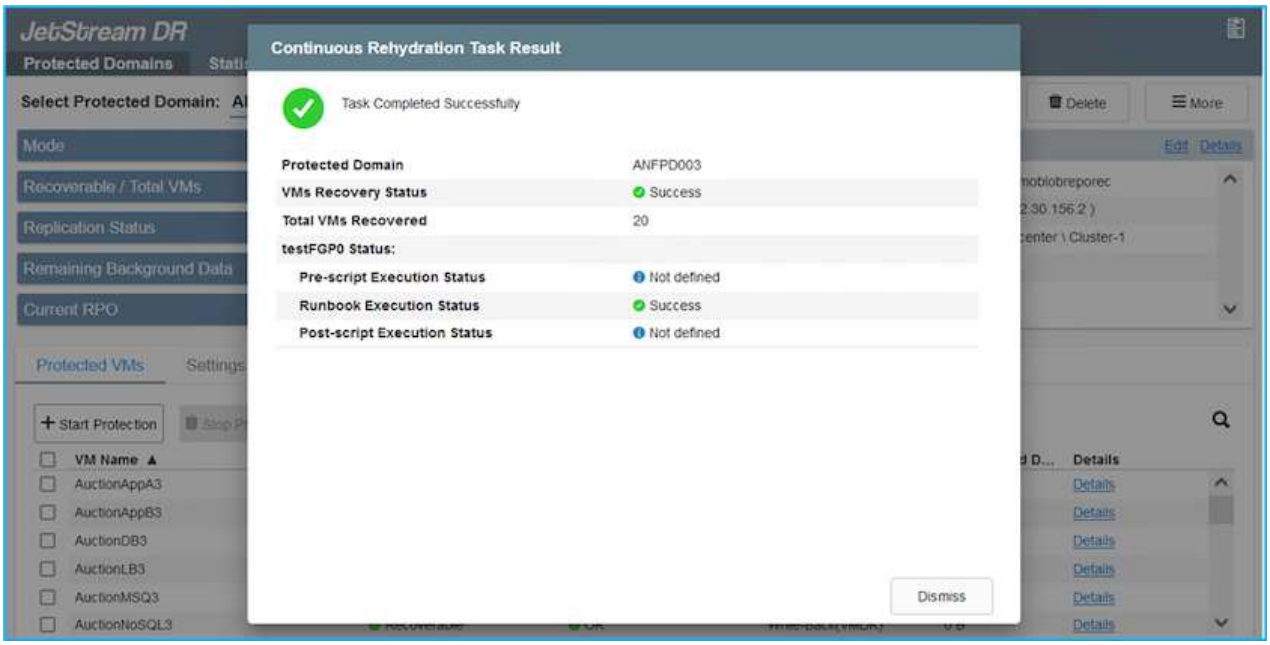
   Dopo il failover (per la reidratazione continua o standard) quando le macchine virtuali protette sono state avviate in AVS, la protezione viene automaticamente ripristinata e JetStream DR continua a replicare i propri dati nei container appropriati/originali in Azure Blob Storage.





La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

2. Una volta completata l'attività, accedere alle macchine virtuali ripristinate e il business continua normalmente.

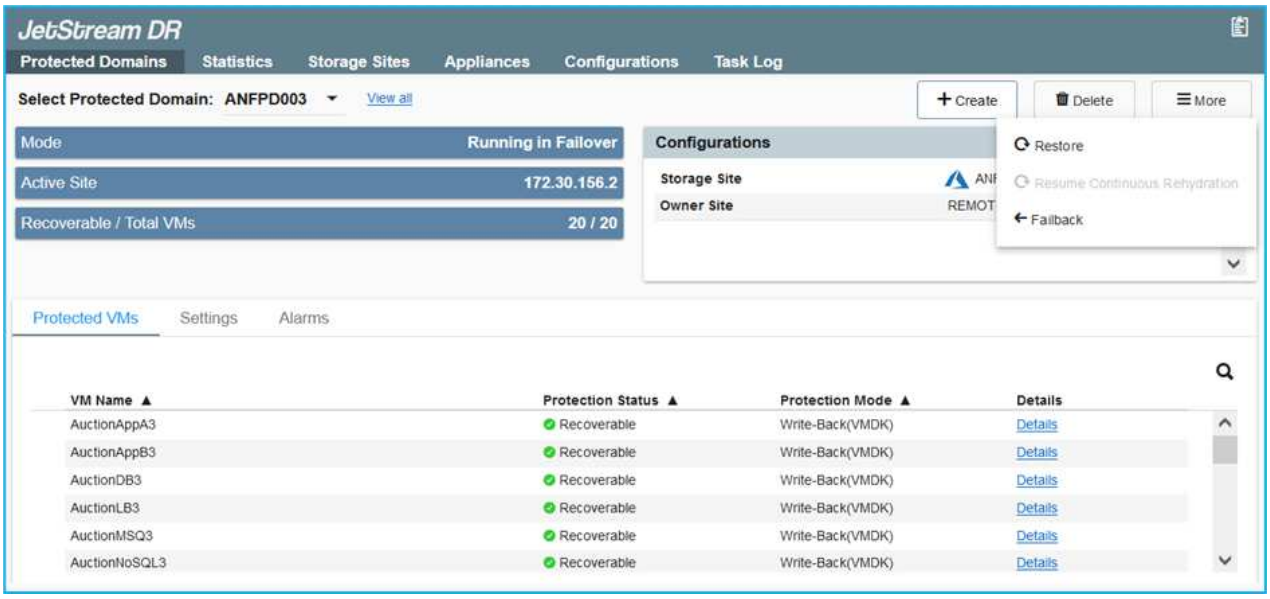


Una volta che il sito primario è stato nuovamente operativo, è possibile eseguire il failback. La protezione delle macchine virtuali viene ripristinata e la coerenza dei dati deve essere verificata.

3. Ripristinare l'ambiente on-premise. A seconda del tipo di incidente, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software DR JetStream.

> Nota: Il `recovery_utility_prepare_failback` Lo script fornito nel toolkit di automazione può essere utilizzato per pulire il sito protetto originale di tutte le macchine virtuali obsolete, le informazioni di dominio e così via.

4. Accedere all'ambiente on-premise ripristinato, accedere all'interfaccia utente DR Jetstream e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione failover nell'interfaccia utente.



Il piano di failback generato da CPT può anche essere utilizzato per avviare il ritorno delle macchine virtuali e dei relativi dati dall'archivio di oggetti all'ambiente VMware originale.

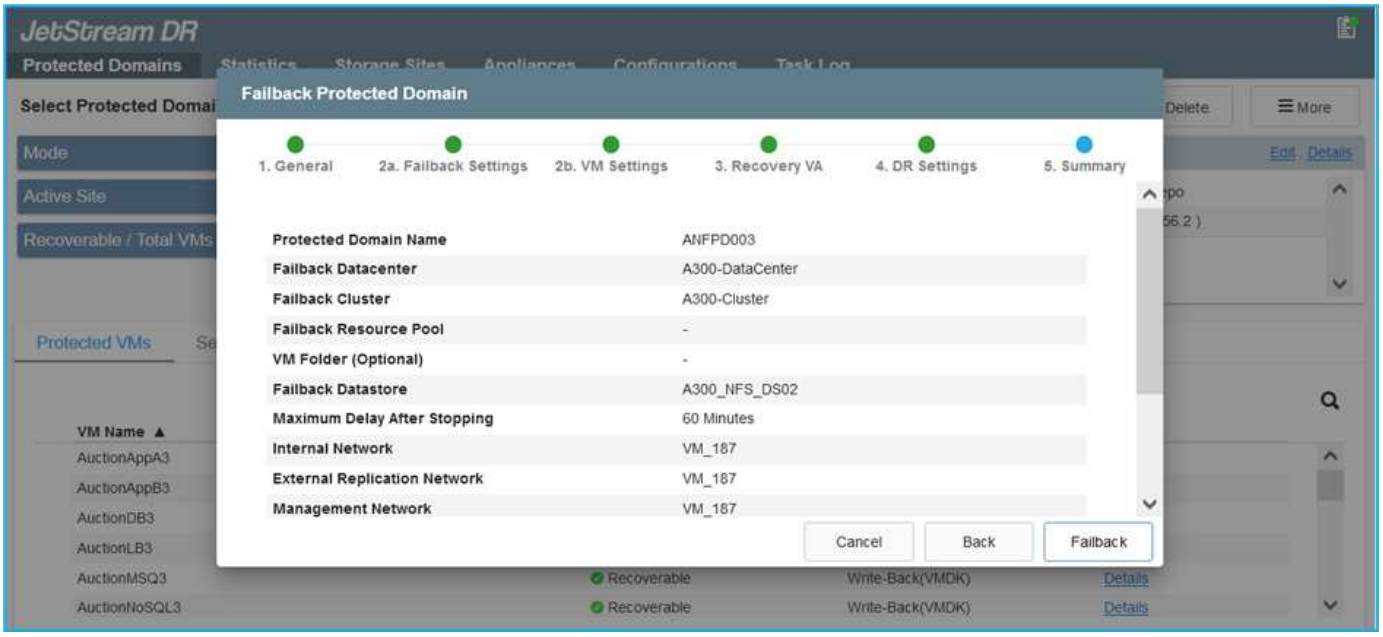
Specificare il ritardo massimo dopo la pausa delle macchine virtuali nel sito di ripristino e il riavvio nel sito protetto. Questo tempo include il completamento della replica dopo l'arresto delle macchine virtuali di failover, il tempo necessario per pulire il sito di recovery e il tempo necessario per ricreare le macchine virtuali in un sito protetto. Il valore consigliato da NetApp è di 10 minuti.

Completare il processo di failback, quindi confermare la ripresa della protezione delle macchine virtuali e la coerenza dei dati.

Recovery di Ransomeware

Il ripristino dal ransomware può essere un compito scoraggiante. In particolare, può essere difficile per le organizzazioni IT determinare il punto di ritorno sicuro e, una volta determinato, come garantire che i carichi di lavoro recuperati siano protetti dagli attacchi che si verificano nuovamente (dal malware in sospensione o attraverso applicazioni vulnerabili).

Jetstream DR per AVS e gli archivi dati Azure NetApp Files possono risolvere questi problemi consentendo alle organizzazioni di eseguire il ripristino dai punti disponibili nel tempo, in modo che i carichi di lavoro vengano ripristinati in una rete funzionale e isolata, se necessario. Il ripristino consente alle applicazioni di funzionare e comunicare tra loro senza esporre le applicazioni al traffico nord-sud, offrendo così ai team di sicurezza un luogo sicuro per eseguire analisi forensi e altre azioni correttive necessarie.



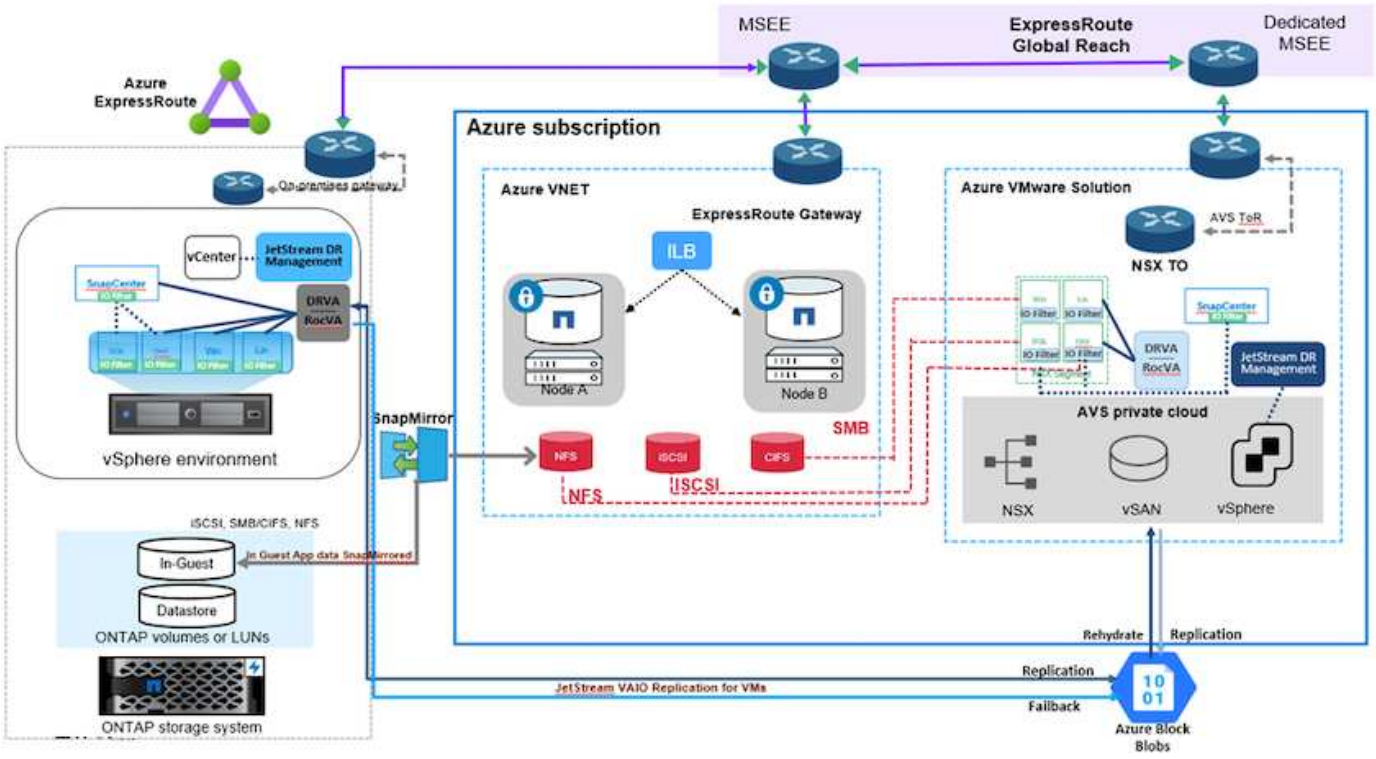
Disaster Recovery con CVO e AVS (storage connesso agli ospiti)

Panoramica

Autori: Ravi BCB e Niyaz Mohamed, NetApp

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i workload da interruzioni del sito e eventi di corruzione dei dati come ransomware. Con NetApp SnapMirror, è possibile replicare i workload VMware on-premise che utilizzano lo storage connesso con gli ospiti su NetApp Cloud Volumes ONTAP in esecuzione in Azure. Ciò riguarda i dati delle applicazioni, ma le macchine virtuali effettive. Il disaster recovery dovrebbe coprire tutti i componenti dipendenti, tra cui macchine virtuali, VMDK, dati applicativi e altro ancora. A tale scopo, SnapMirror e Jetstream possono essere utilizzati per ripristinare perfettamente i carichi di lavoro replicati da on-premise a Cloud Volumes ONTAP utilizzando lo storage vSAN per VM VMDK.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, JetStream e Azure VMware Solution (AVS).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.

> Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete virtuale Azure, utilizzare la portata globale di instradamento espresso o una WAN virtuale con un gateway VPN. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.

> Esistono diverse opzioni per connettere i data center on-premise ad Azure, che ci impediscono di delineare un workflow specifico in questo documento. Consultare la documentazione di Azure per il metodo di connettività on-premise-to-Azure appropriato.

Implementazione della soluzione DR

Panoramica sull'implementazione della soluzione

1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.
    a. Configurare SnapMirror per i volumi applicativi rilevanti.

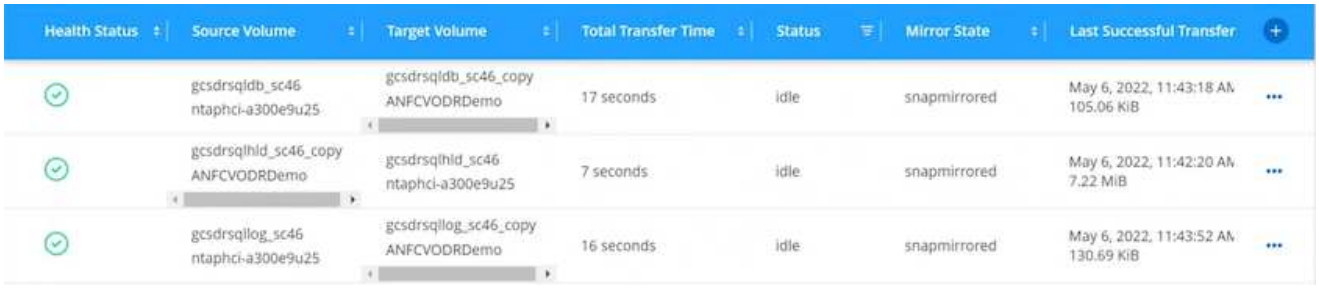
b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.

3. Installare il software DR JetStream nel data center on-premise e iniziare la protezione per le macchine virtuali.
4. Installare il software DR JetStream nel cloud privato Azure VMware Solution.
5. Durante un evento di emergenza, interrompere la relazione di SnapMirror utilizzando Cloud Manager e attivare il failover delle macchine virtuali su Azure NetApp Files o su datastore vSAN nel sito di DR AVS designato.
   a. Ricollegare I LUN ISCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
6. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Azure e replicare i volumi su CVO

Il primo passaggio consiste nel configurare Cloud Volumes ONTAP su Azure ("Collegamento") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritentioni di snapshot.



Configurare gli host AVS e l'accesso ai dati CVO

Due fattori importanti da considerare durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione VMware di Azure e il tempo necessario per mantenere il SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

La decisione di implementare un cluster AVS si basa principalmente sui requisiti RPO/RTO. Con la soluzione VMware Azure, il provisioning SDDC può essere eseguito in tempo, in preparazione di test o di un evento di disastro effettivo. Un SDDC implementato Just in Time consente di risparmiare sui costi degli host ESXi quando non si affronta un disastro. Tuttavia, questa forma di implementazione influisce sull'RTO di alcune ore durante il provisioning di SDDC.

L'opzione implementata più comunemente è l'esecuzione di SDDC in una modalità di funzionamento always-on, con illuminazione pilota. Questa opzione offre un ingombro ridotto di tre host sempre disponibili e accelera le operazioni di recovery fornendo una base di riferimento per le attività di simulazione e i controlli di conformità, evitando così il rischio di deriva operativa tra i siti di produzione e DR. Il cluster pilota-light può essere scalato rapidamente fino al livello desiderato quando necessario per gestire un evento DR effettivo.

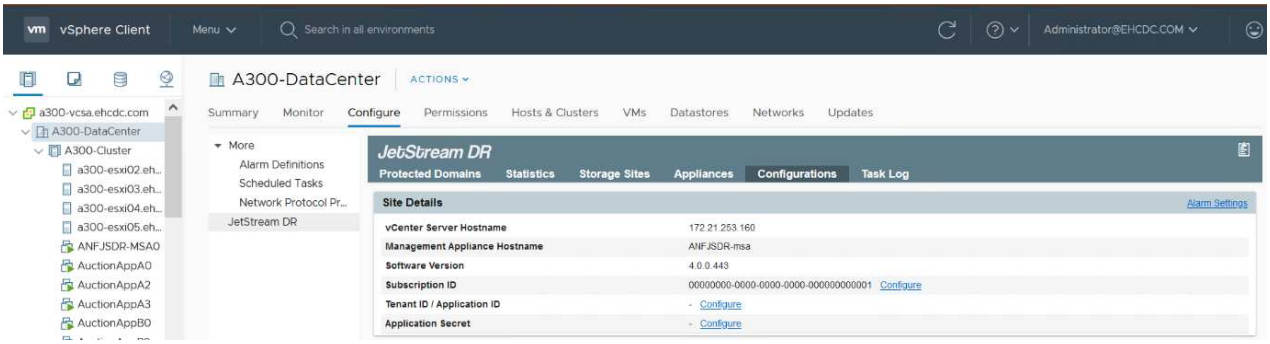
Per configurare AVS SDDC (sia esso on-demand o in modalità pilota-light), vedere "Implementare e configurare l'ambiente di virtualizzazione su Azure". Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host AVS siano in grado di utilizzare i dati provenienti da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e AVS, iniziare a configurare Jetstream per automatizzare il ripristino dei carichi di lavoro on-premise su AVS (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando il meccanismo VAIO e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

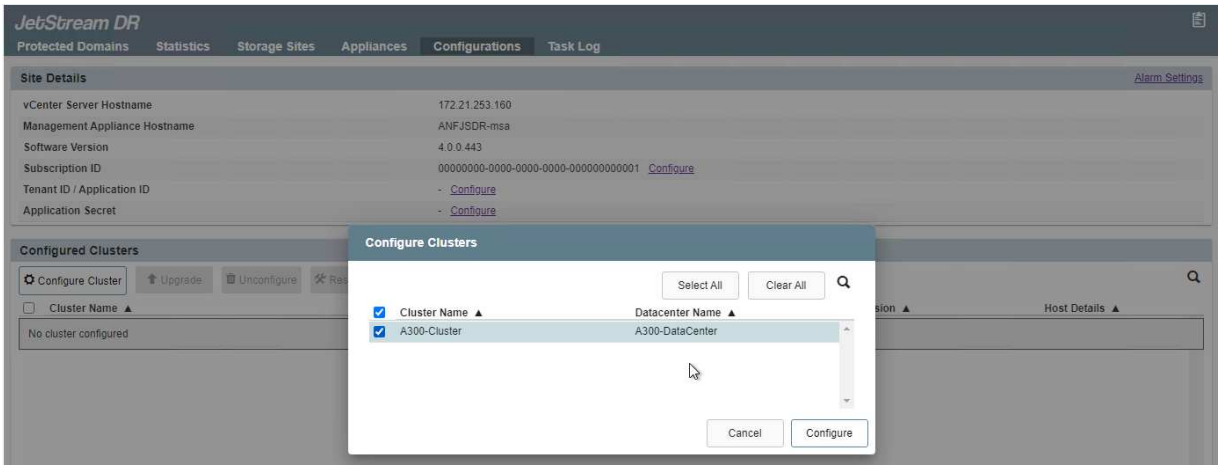
Installare JetStream DR nel data center on-premise

Il software Jetstream DR è costituito da tre componenti principali: L'appliance virtuale JetStream DR Management Server (MSA), l'appliance virtuale DR (DRVA) e i componenti host (pacchetti di filtri i/o). MSA viene utilizzato per installare e configurare i componenti host sul cluster di calcolo e quindi per amministrare il software DR JetStream. La procedura di installazione è la seguente:

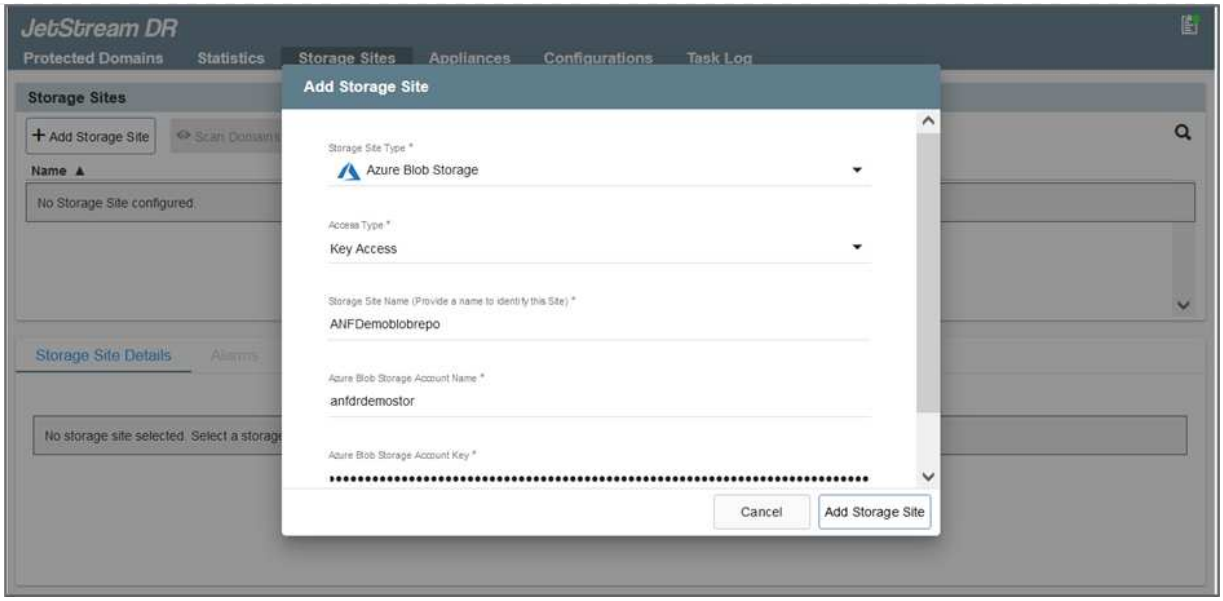
1. Verificare i prerequisiti.
2. Eseguire Capacity Planning Tool per consigli su risorse e configurazione.
3. Distribuire l'MSA DR JetStream su ciascun host vSphere nel cluster designato.
4. Avviare MSA utilizzando il nome DNS in un browser.
5. Registrare il server vCenter con MSA.
6. Una volta implementato JetStream DR MSA e registrato vCenter Server, accedere al plug-in JetStream DR con vSphere Web Client. Per eseguire questa operazione, accedere a Datacenter > Configure > JetStream DR.



7. Dall'interfaccia DR JetStream, completare le seguenti attività:
   a. Configurare il cluster con il pacchetto di filtri i/O.

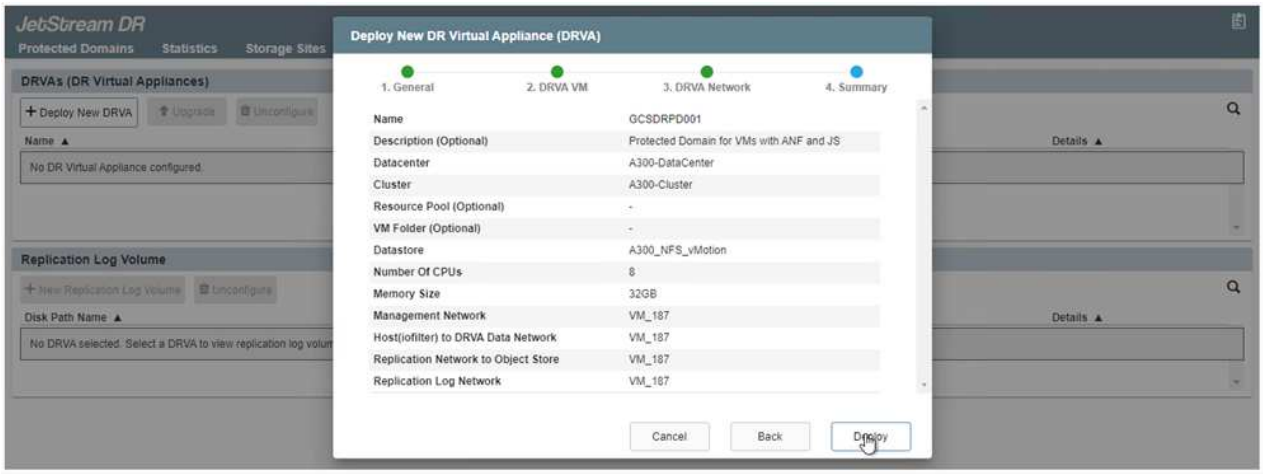


   b. Aggiungere lo storage Azure Blob situato nel sito di ripristino.

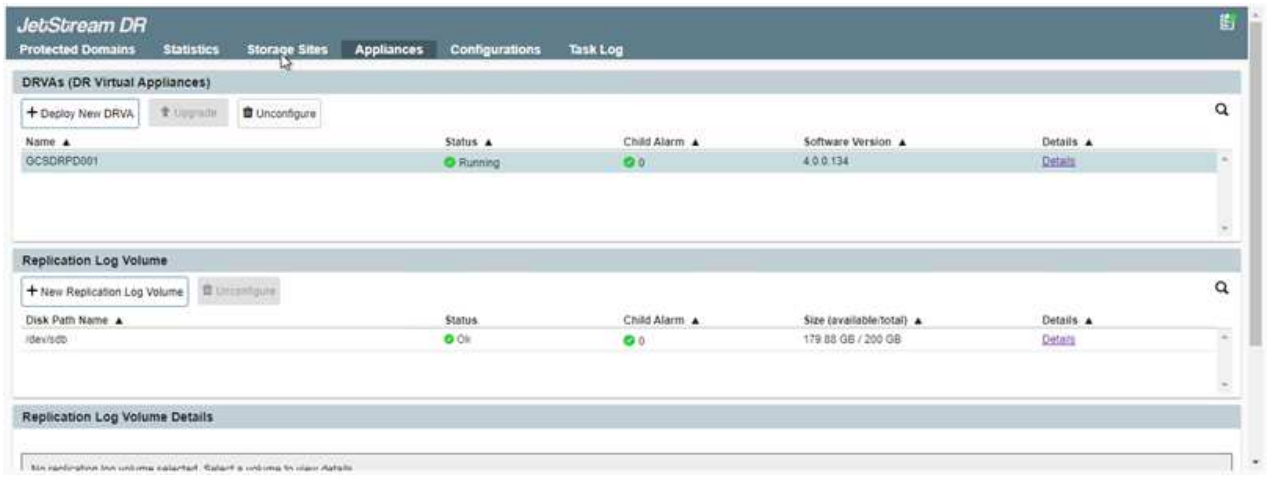


8. Implementare il numero richiesto di DRVA (DR Virtual Appliances) dalla scheda Appliances (appliance).

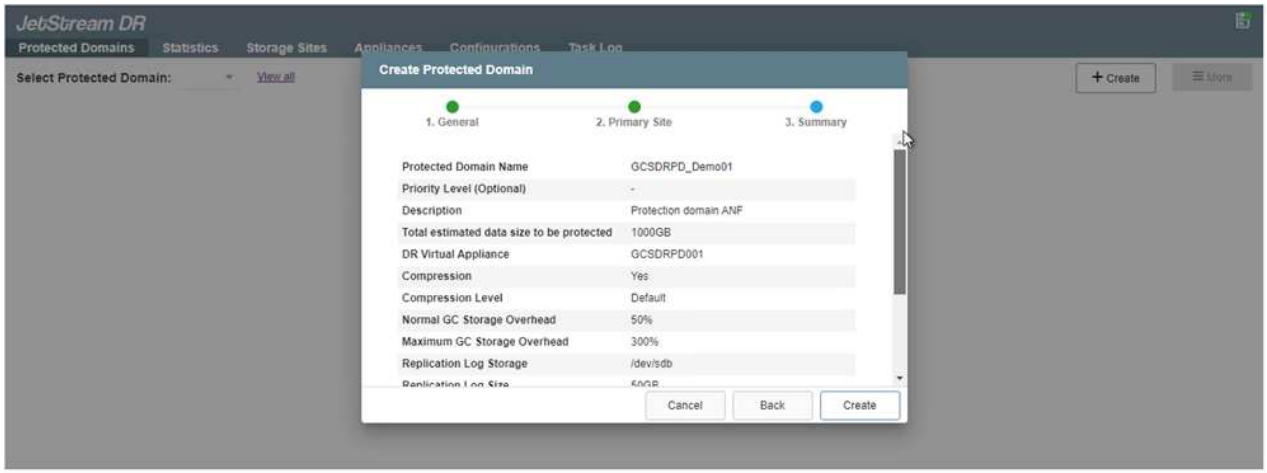
> Utilizzare lo strumento di pianificazione della capacità per stimare il numero di DRA richiesti.

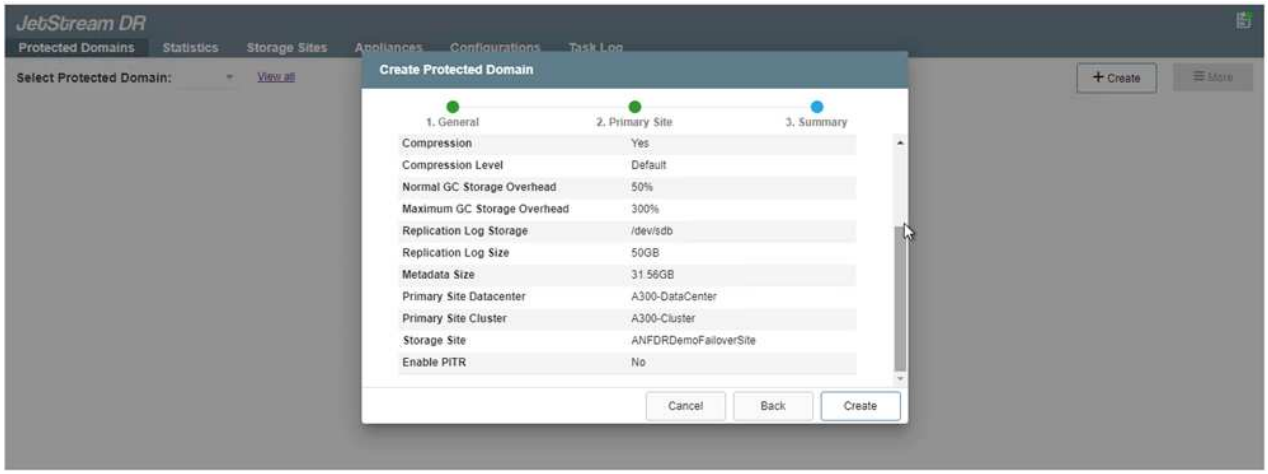


9. Creare volumi di log di replica per ogni DRVA utilizzando VMDK dagli archivi dati disponibili o dal pool di storage iSCSI condiviso indipendente.



10. Dalla scheda Protected Domains (domini protetti), creare il numero richiesto di domini protetti utilizzando le informazioni relative al sito Azure Blob Storage, all'istanza DRVA e al registro di replica. Un dominio protetto definisce una macchina virtuale specifica o un insieme di macchine virtuali dell'applicazione all'interno del cluster che sono protetti insieme e assegnati un ordine di priorità per le operazioni di failover/failback.

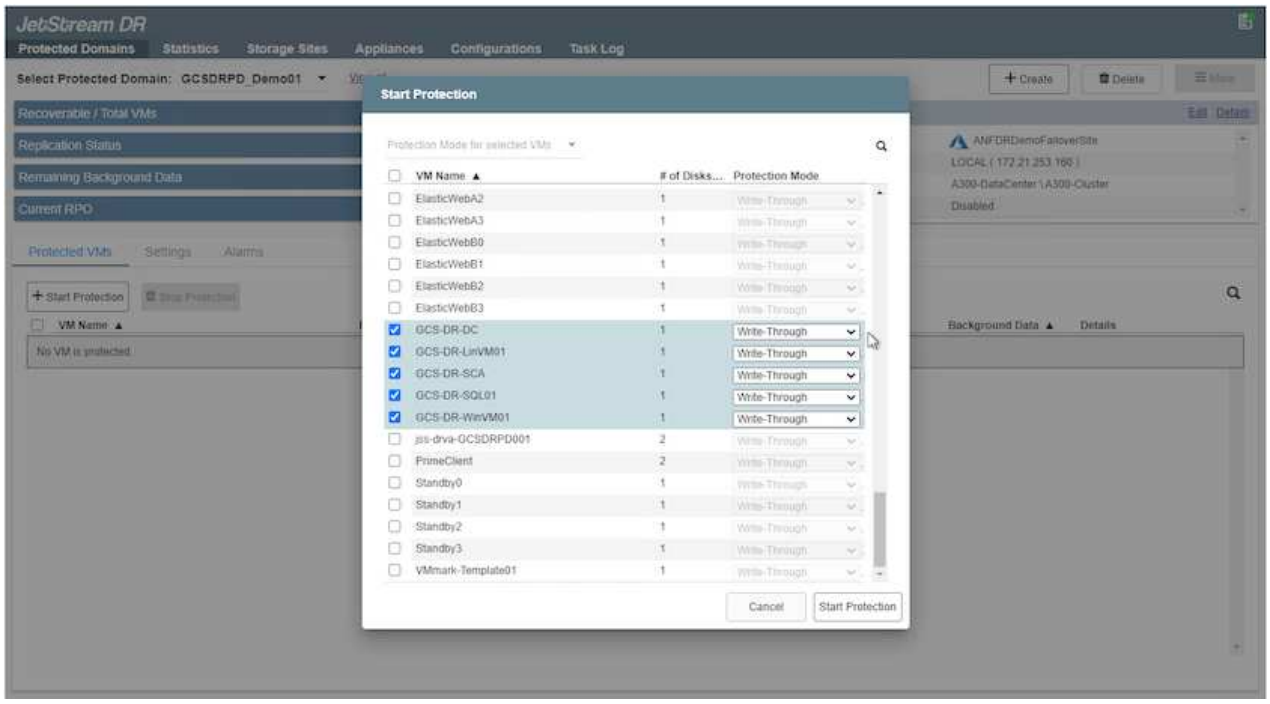




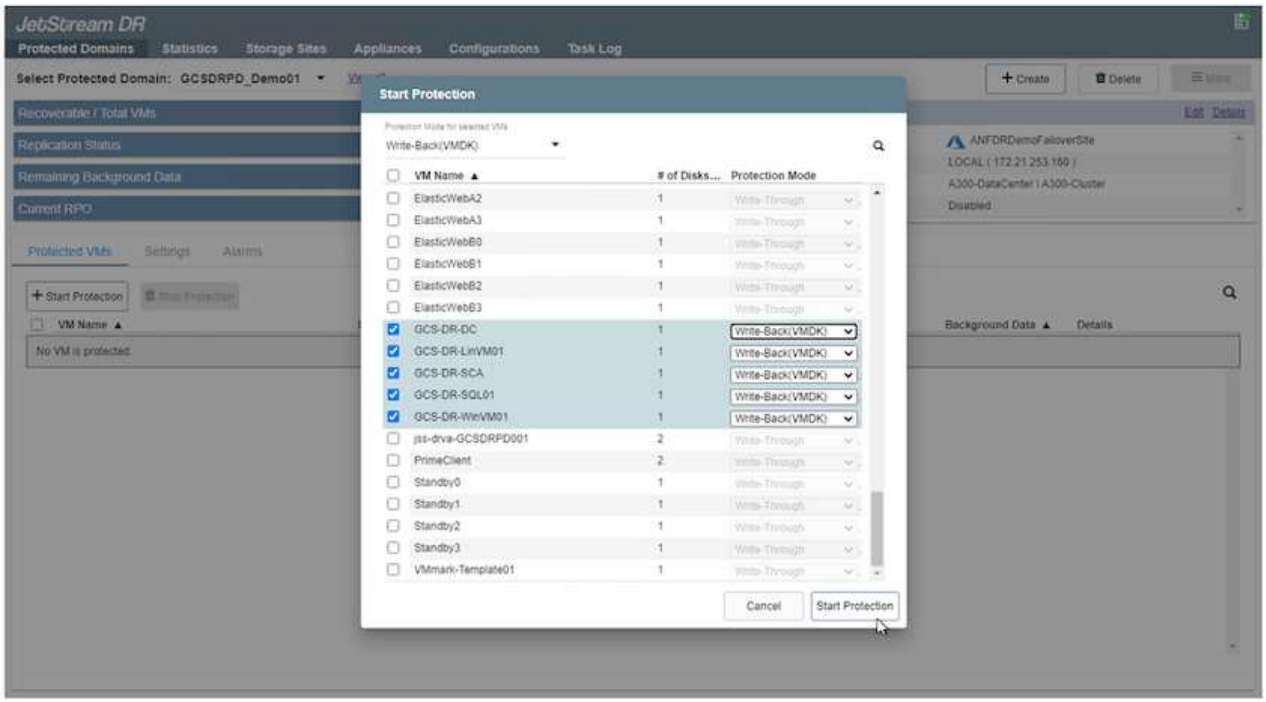
11. Selezionare le macchine virtuali da proteggere e raggrupparle in gruppi di applicazioni in base alla dipendenza. Le definizioni delle applicazioni consentono di raggruppare set di macchine virtuali in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e validazioni opzionali delle applicazioni che possono essere eseguite al momento del ripristino.

Assicurarsi di utilizzare la stessa modalità di protezione per tutte le macchine virtuali in un dominio protetto.

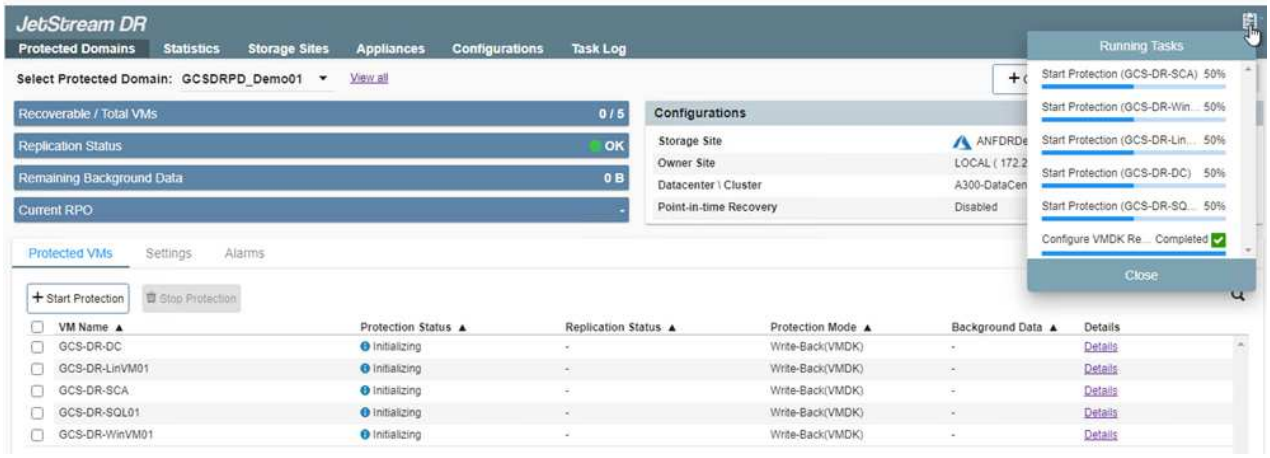
La modalità Write-Back (VMDK) offre performance superiori.



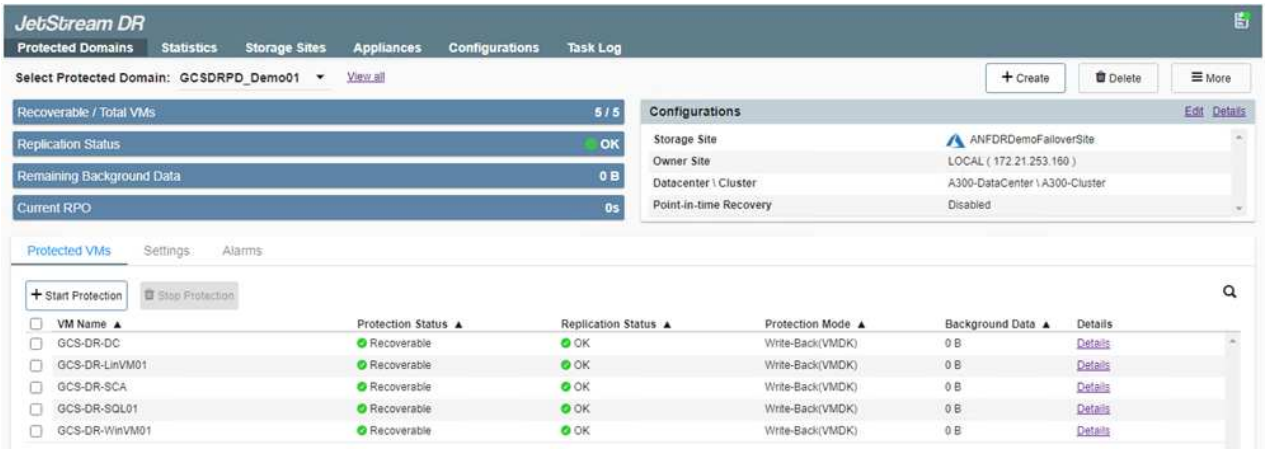
12. Assicurarsi che i volumi dei log di replica siano posizionati su uno storage dalle performance elevate.



13. Al termine dell'operazione, fare clic su Start Protection (Avvia protezione) per il dominio protetto. In questo modo viene avviata la replica dei dati per le macchine virtuali selezionate nell'archivio Blob designato.



14. Una volta completata la replica, lo stato di protezione della macchina virtuale viene contrassegnato come ripristinabile.

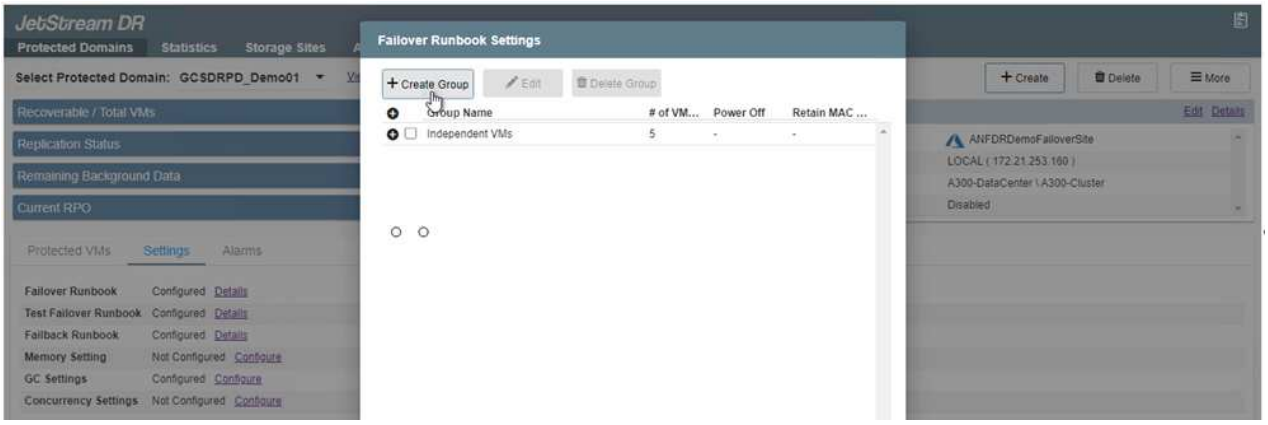


> Le runbook di failover possono essere configurate per raggruppare le macchine virtuali (denominate gruppo di ripristino), impostare la sequenza dell'ordine di avvio e modificare le impostazioni della CPU/memoria insieme alle configurazioni IP.

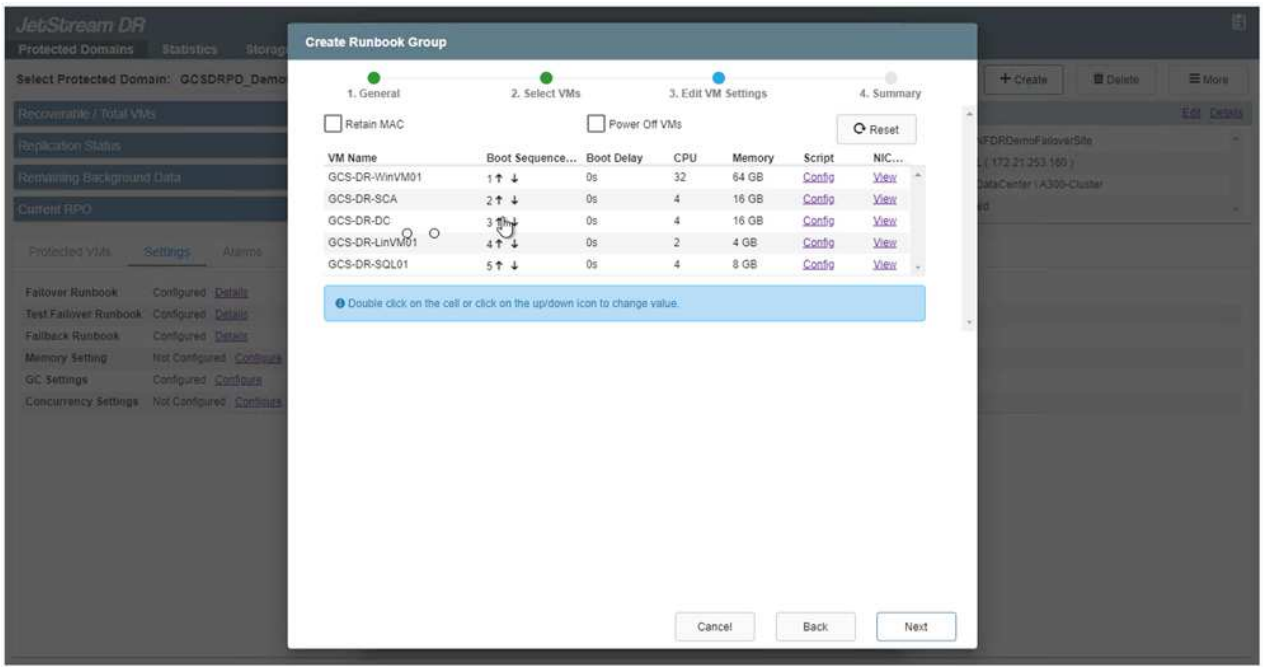
15. Fare clic su Impostazioni, quindi sul collegamento Configura runbook per configurare il gruppo runbook.

16. Fare clic sul pulsante Create Group (Crea gruppo) per iniziare a creare un nuovo gruppo di runbook.

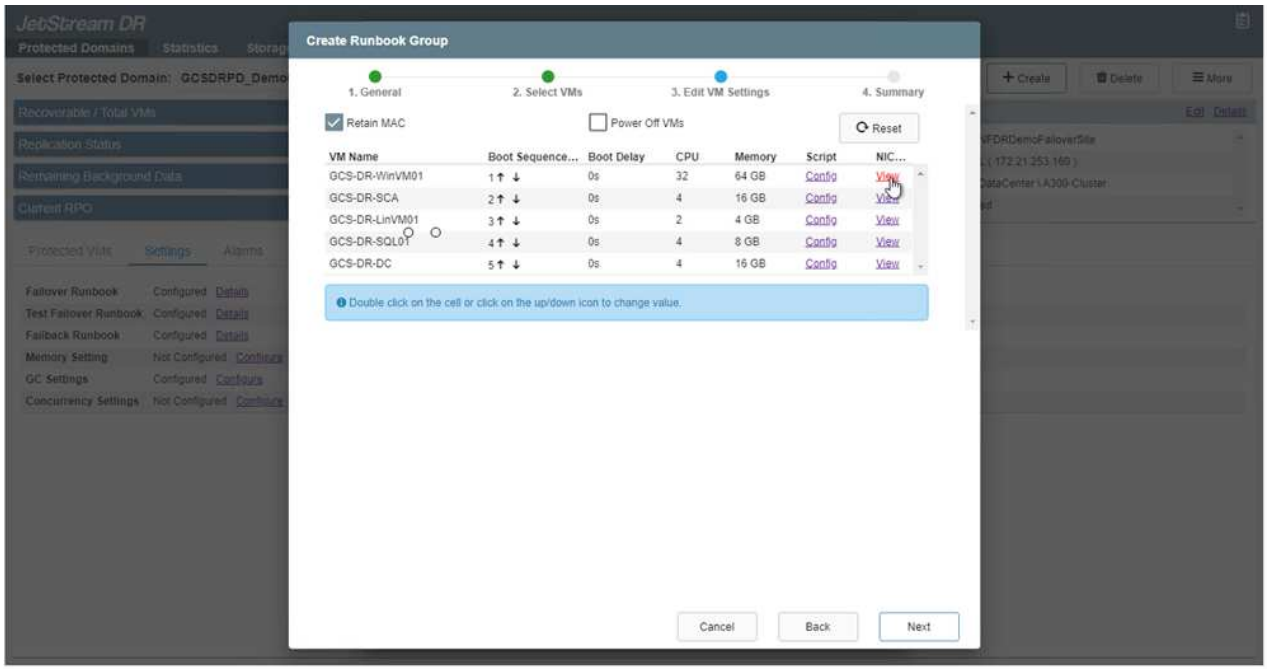
Se necessario, nella parte inferiore della schermata, applicare pre-script e post-script personalizzati da eseguire automaticamente prima e dopo l'operazione del gruppo di runbook. Assicurarsi che gli script Runbook risiedano sul server di gestione.



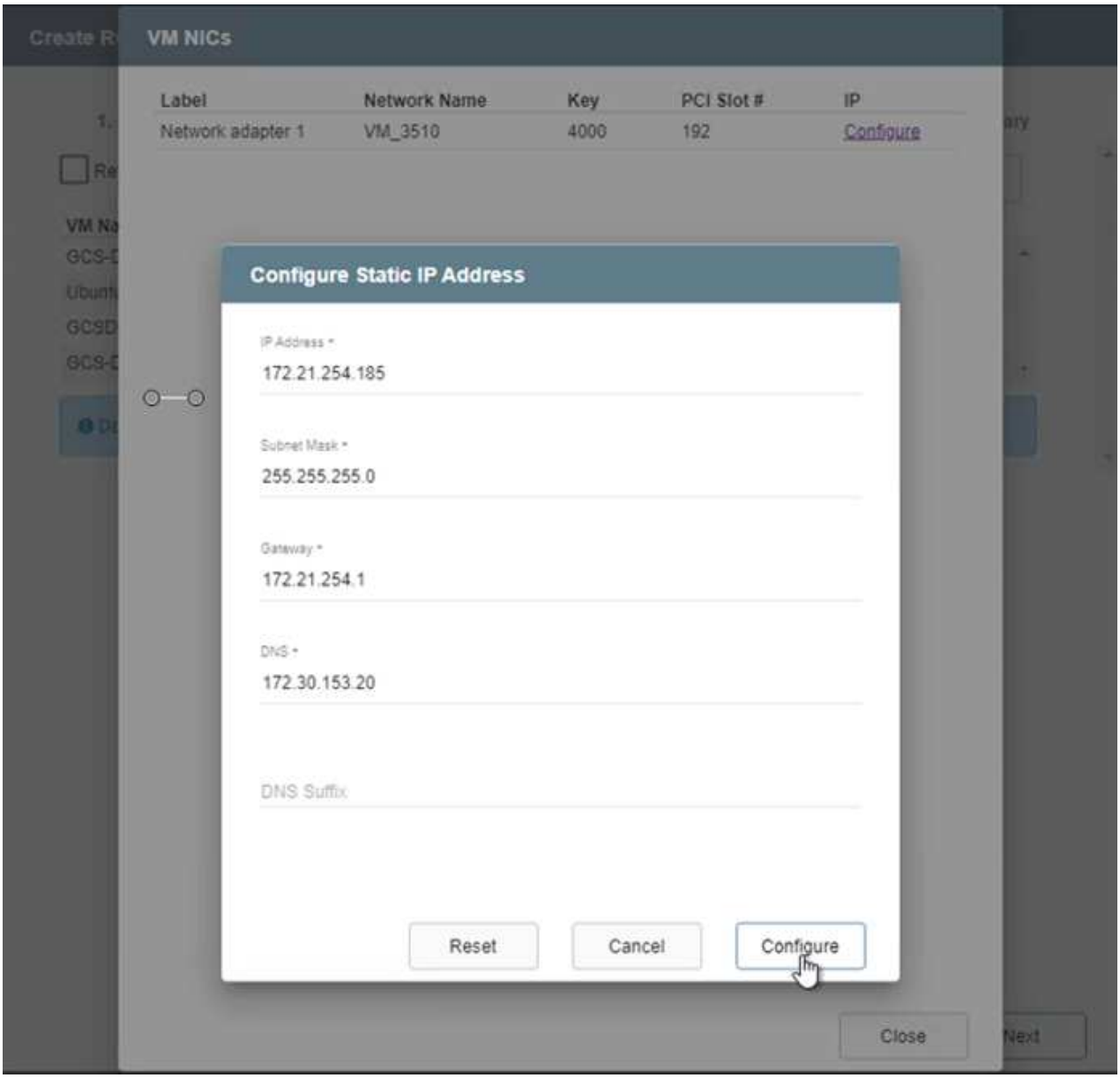
17. Modificare le impostazioni della macchina virtuale secondo necessità. Specificare i parametri per il ripristino delle macchine virtuali, tra cui la sequenza di avvio, il ritardo di avvio (specificato in secondi), il numero di CPU e la quantità di memoria da allocare. Modificare la sequenza di avvio delle macchine virtuali facendo clic sulle frecce verso l'alto o verso il basso. Sono inoltre disponibili opzioni per conservare MAC.

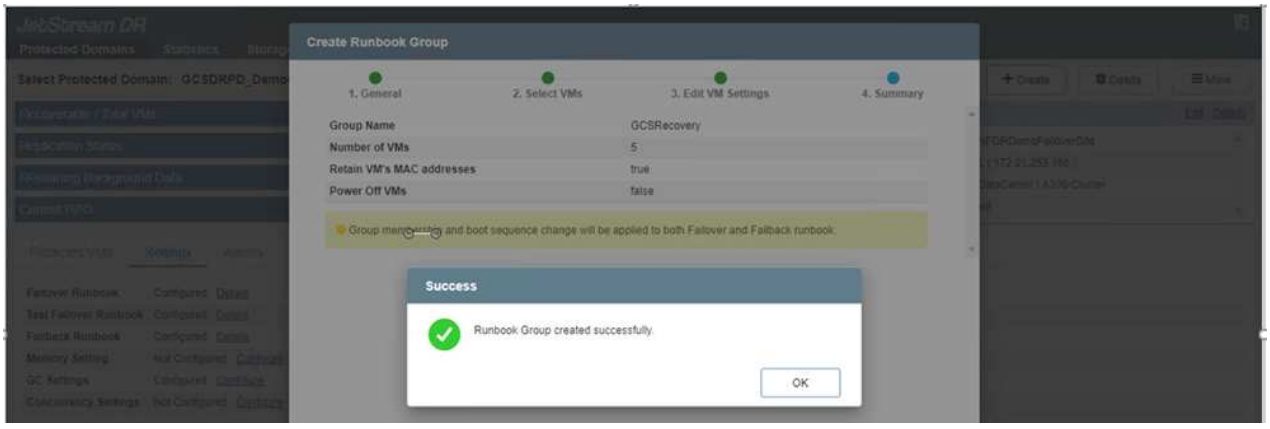


18. Gli indirizzi IP statici possono essere configurati manualmente per le singole macchine virtuali del gruppo. Fare clic sul collegamento NIC View (visualizzazione NIC) di una macchina virtuale per configurare manualmente le impostazioni dell'indirizzo IP.



19. Fare clic sul pulsante Configure (Configura) per salvare le impostazioni NIC per le rispettive macchine virtuali.





Lo stato dei runbook di failover e failback è ora elencato come configurato. I gruppi runbook di failover e failback vengono creati in coppie utilizzando lo stesso gruppo iniziale di macchine virtuali e impostazioni. Se necessario, le impostazioni di qualsiasi gruppo di runbook possono essere personalizzate singolarmente facendo clic sul relativo link Details (Dettagli) e apportando modifiche.

Installare JetStream DR per AVS nel cloud privato

Una Best practice per un sito di recovery (AVS) consiste nella creazione anticipata di un cluster pilota a tre nodi. Ciò consente di preconfigurare l'infrastruttura del sito di ripristino, tra cui:

- Segmenti di rete di destinazione, firewall, servizi come DHCP e DNS e così via
- Installazione di JetStream DR per AVS
- Configurazione dei volumi ANF come datastore e altro ancora

Jetstream DR supporta una modalità RTO quasi zero per i domini mission-critical. Per questi domini, lo storage di destinazione deve essere preinstallato. ANF è un tipo di storage consigliato in questo caso.

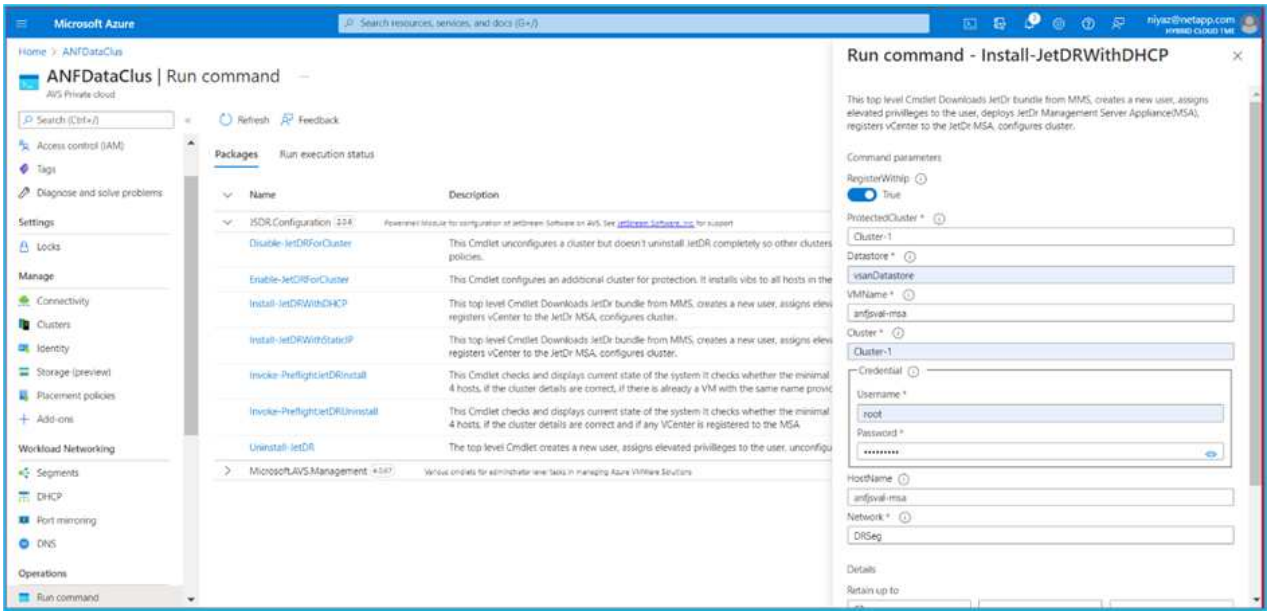
> La configurazione di rete, inclusa la creazione di segmenti, deve essere configurata sul cluster AVS per soddisfare i requisiti on-premise.

> A seconda dei requisiti SLA e RTO, è possibile utilizzare il failover continuo o la normale modalità di failover (standard). Per un RTO vicino allo zero, è necessario avviare una reidratazione continua nel sito di ripristino.

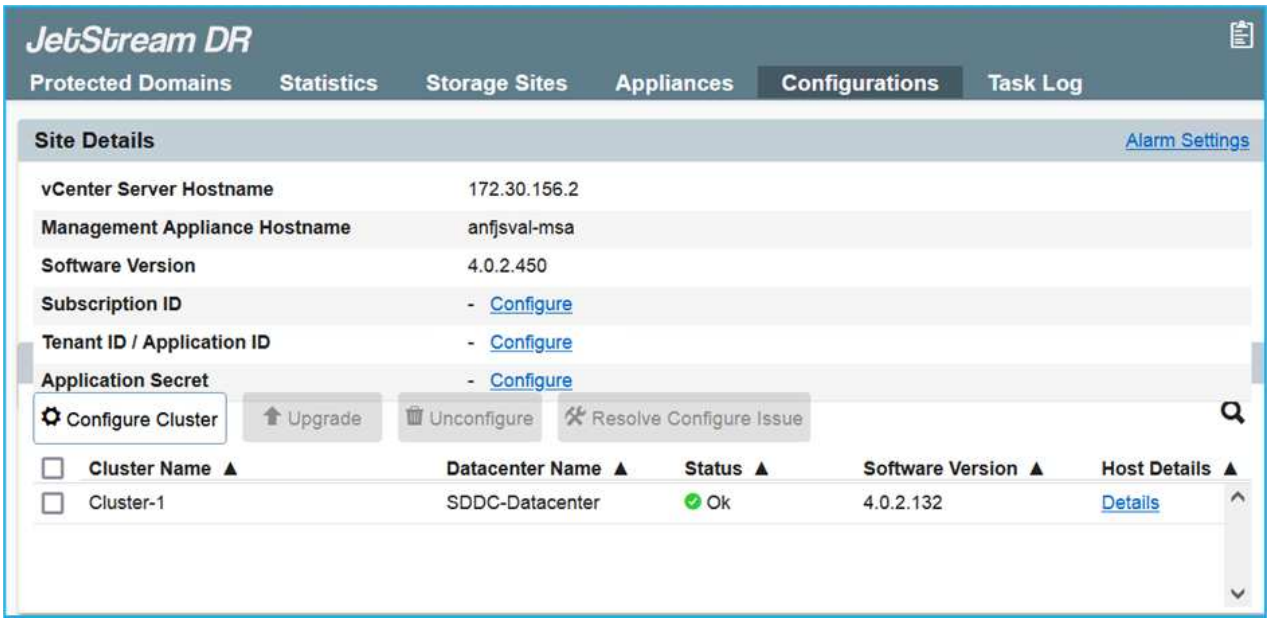
1. Per installare JetStream DR per AVS su un cloud privato Azure VMware Solution, utilizzare il comando Esegui. Dal portale Azure, accedere alla soluzione Azure VMware, selezionare il cloud privato e selezionare Esegui comando > pacchetti > Configurazione JSDR.

   > L'utente CloudAdmin predefinito di Azure VMware Solution non dispone di privilegi sufficienti per installare JetStream DR per AVS. Azure VMware Solution consente un'installazione semplificata e automatica del DR JetStream invocando il comando Azure VMware Solution Run per il DR JetStream.

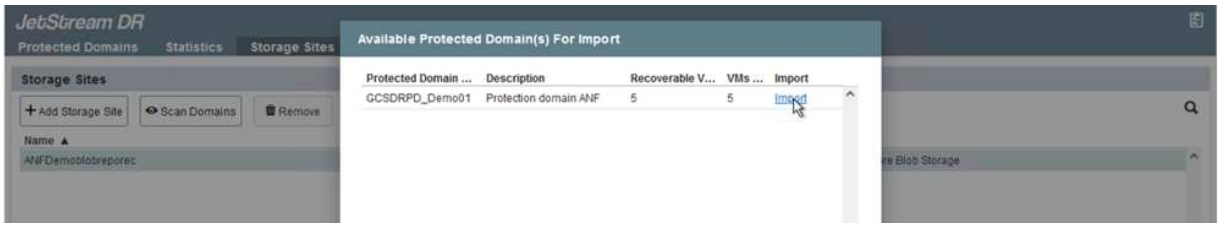
   La seguente schermata mostra l'installazione utilizzando un indirizzo IP basato su DHCP.



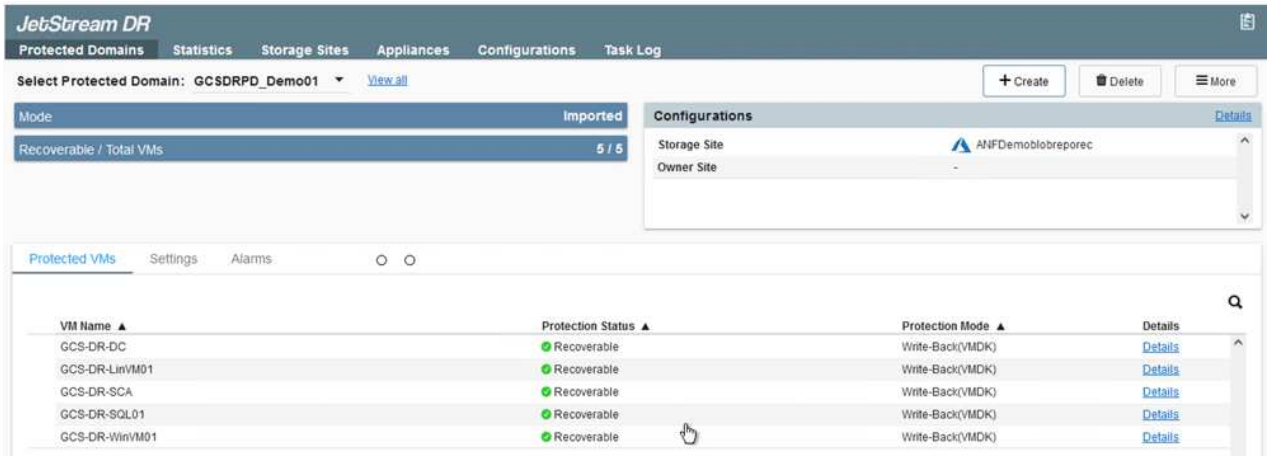
2. Una volta completata l'installazione di JetStream DR per AVS, aggiornare il browser. Per accedere all'interfaccia utente DR JetStream, accedere a SDDC Datacenter > Configure > JetStream DR.



3. Dall'interfaccia DR JetStream, completare le seguenti attività:
   a. Aggiungere l'account Azure Blob Storage utilizzato per proteggere il cluster on-premise come sito di storage, quindi eseguire l'opzione Scan Domains.
   b. Nella finestra di dialogo a comparsa visualizzata, selezionare il dominio protetto da importare, quindi fare clic sul relativo collegamento Importa.



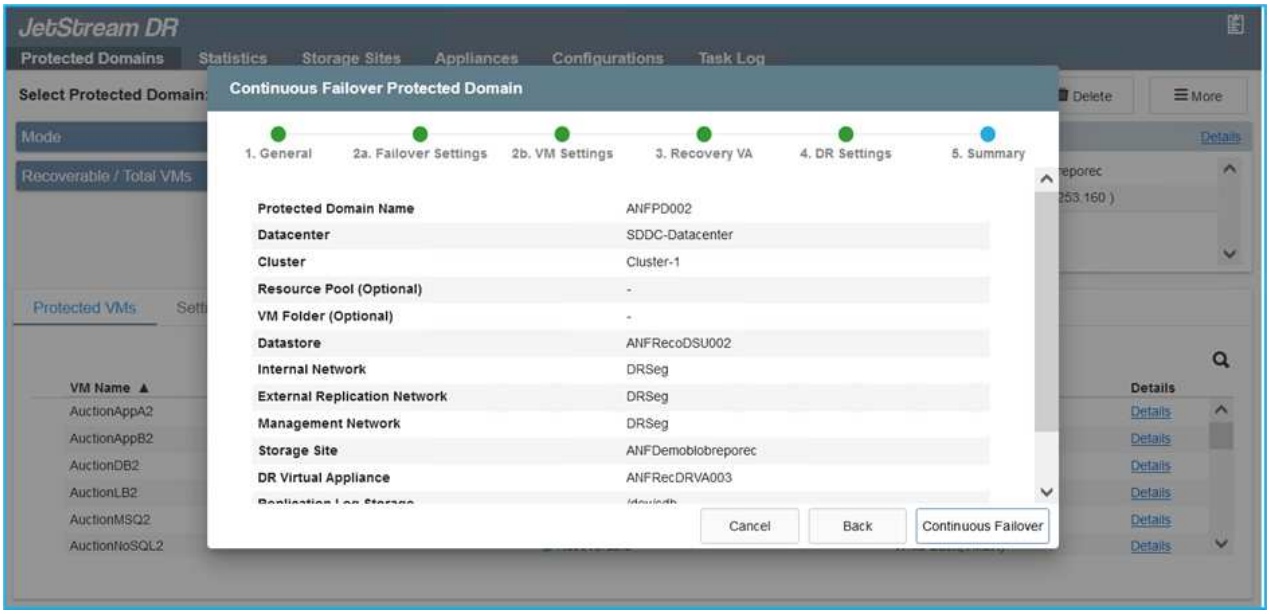
4. Il dominio viene importato per il ripristino. Accedere alla scheda Protected Domains (domini protetti) e verificare che sia stato selezionato il dominio desiderato oppure scegliere quello desiderato dal menu Select Protected Domain (Seleziona dominio protetto). Viene visualizzato un elenco delle macchine virtuali ripristinabili nel dominio protetto.



5. Una volta importati i domini protetti, implementare le appliance DRVA.

Questi passaggi possono anche essere automatizzati utilizzando piani creati da CPT.

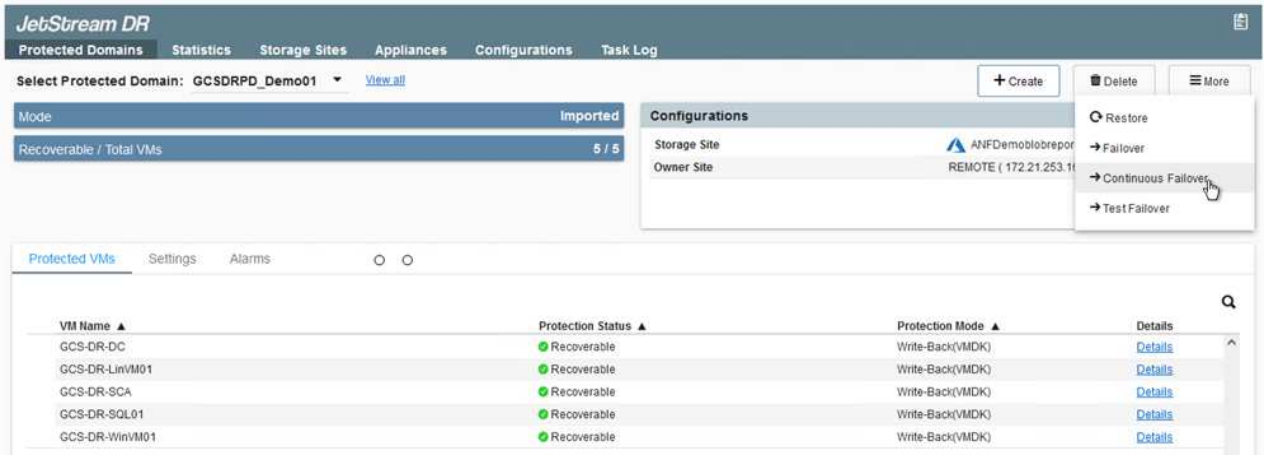
6. Creare volumi di log di replica utilizzando datastore vSAN o ANF disponibili.
7. Importare i domini protetti e configurare il VA di ripristino in modo che utilizzi un datastore ANF per il posizionamento delle macchine virtuali.



Assicurarsi che DHCP sia attivato sul segmento selezionato e che sia disponibile un numero sufficiente di IP. Gli IP dinamici vengono temporaneamente utilizzati durante il ripristino dei domini. Ogni macchina virtuale di ripristino (inclusa la reidratazione continua) richiede un IP dinamico individuale. Una volta completato il ripristino, l'IP viene rilasciato e può essere riutilizzato.

8. Selezionare l'opzione di failover appropriata (failover o failover continuo). In questo esempio, viene selezionata la reidratazione continua (failover continuo).

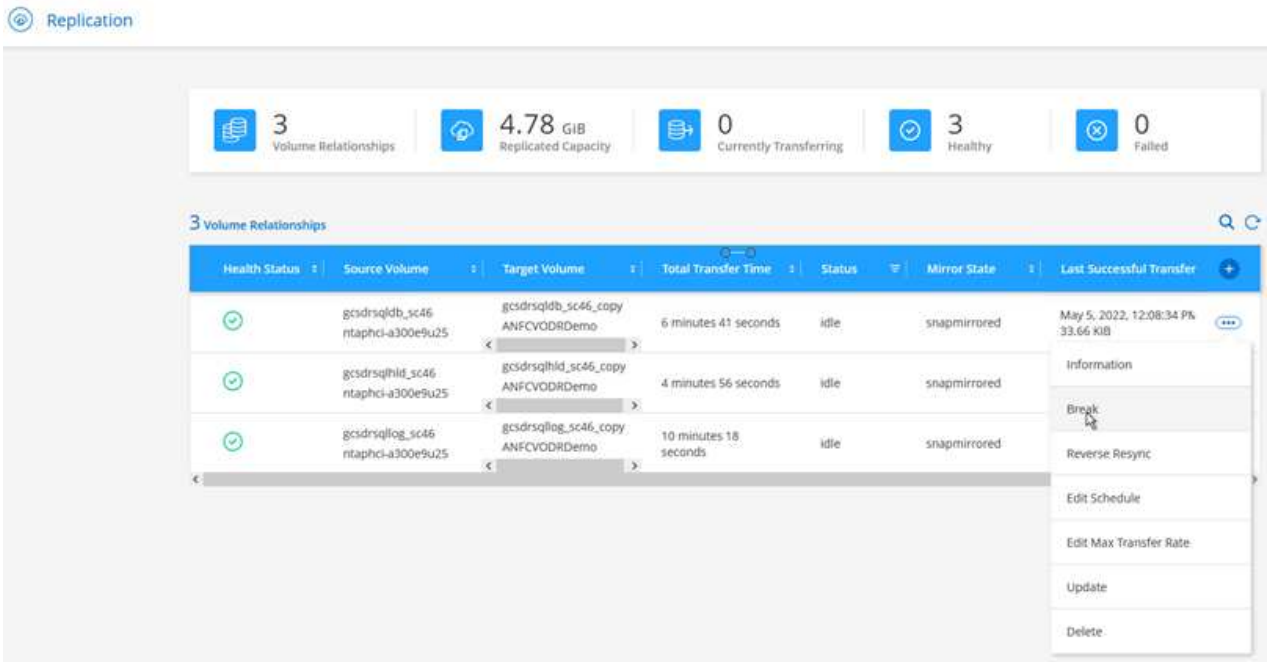
Anche se le modalità di failover continuo e failover differiscono quando viene eseguita la configurazione, entrambe le modalità di failover vengono configurate utilizzando le stesse procedure. I passaggi di failover vengono configurati ed eseguiti insieme in risposta a un evento di emergenza. È possibile configurare il failover continuo in qualsiasi momento e consentire l'esecuzione in background durante il normale funzionamento del sistema. In seguito a un evento di emergenza, il failover continuo viene completato per trasferire immediatamente la proprietà delle macchine virtuali protette al sito di ripristino (RTO quasi nullo).

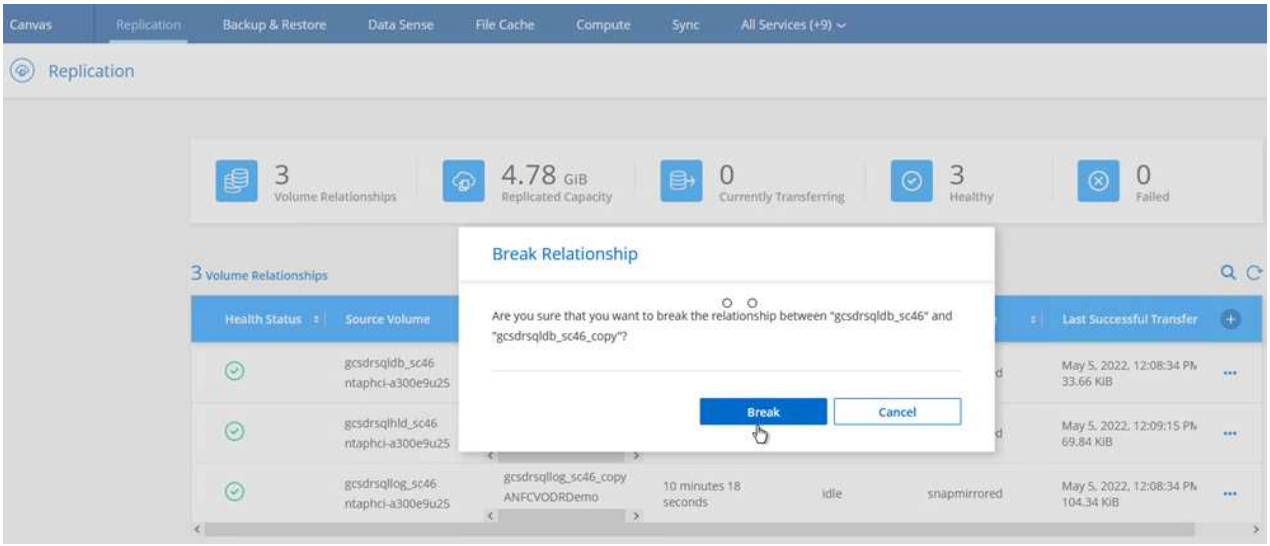


Viene avviato il processo di failover continuo, che può essere monitorato dall'interfaccia utente. Facendo clic sull'icona blu nella sezione Current Step (fase corrente) viene visualizzata una finestra a comparsa che mostra i dettagli della fase corrente del processo di failover.

Failover e failover

1. In caso di disastro nel cluster protetto dell'ambiente on-premise (errore parziale o completo), è possibile attivare il failover per le macchine virtuali utilizzando Jetstream dopo aver interrotto la relazione SnapMirror per i rispettivi volumi applicativi.

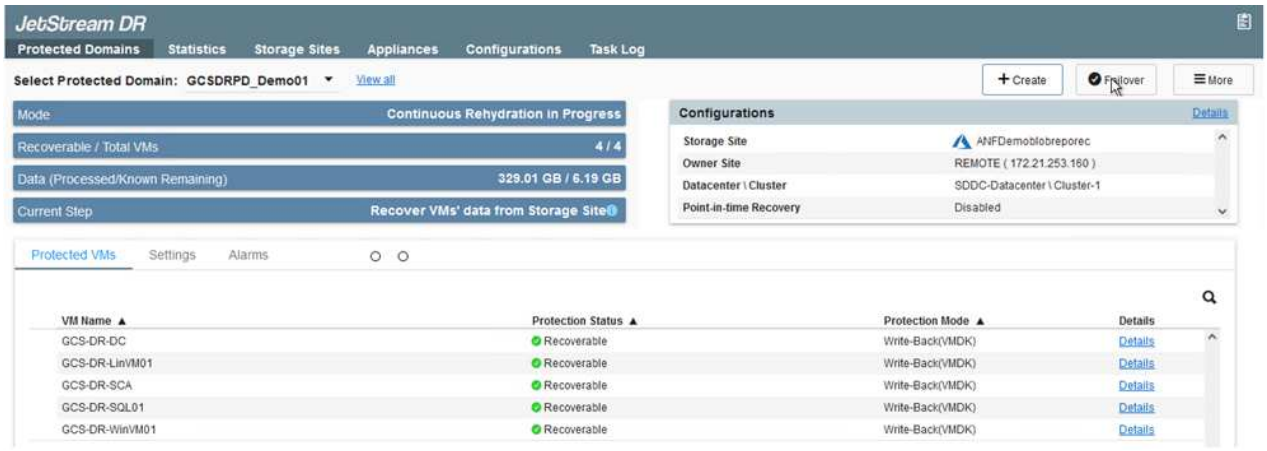


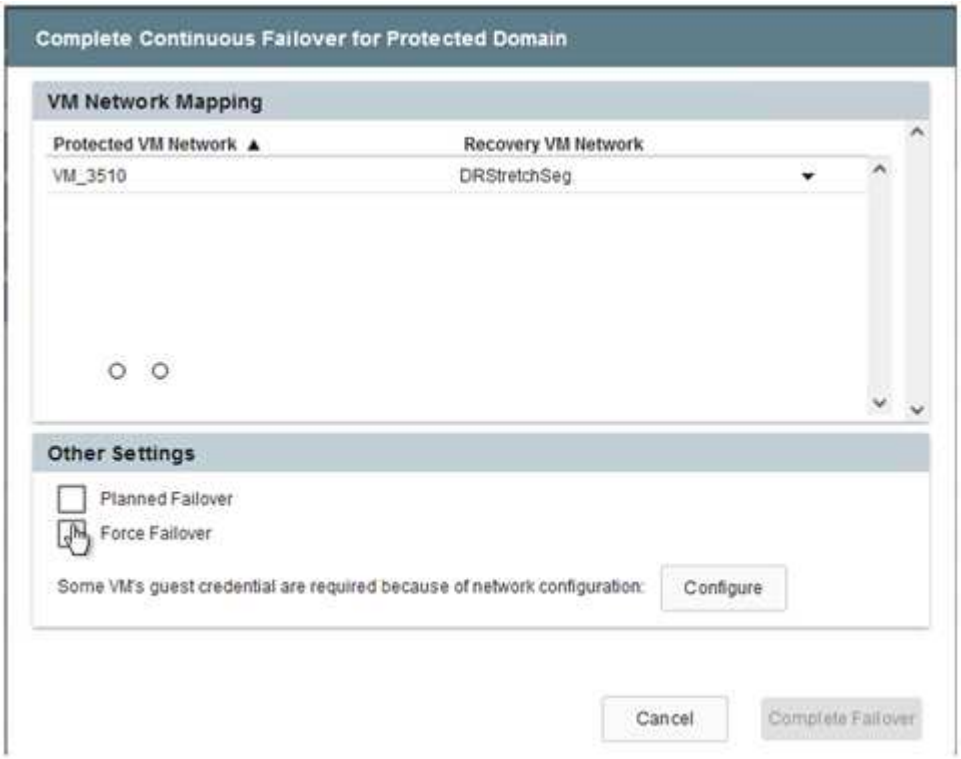


Questo passaggio può essere facilmente automatizzato per facilitare il processo di recovery.

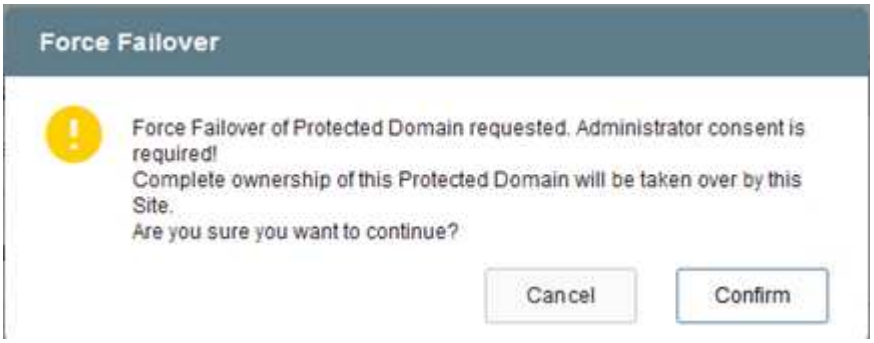
2. Accedere all'interfaccia utente Jetstream su AVS SDDC (lato destinazione) e attivare l'opzione di failover per completare il failover. La barra delle applicazioni mostra lo stato di avanzamento delle attività di failover.

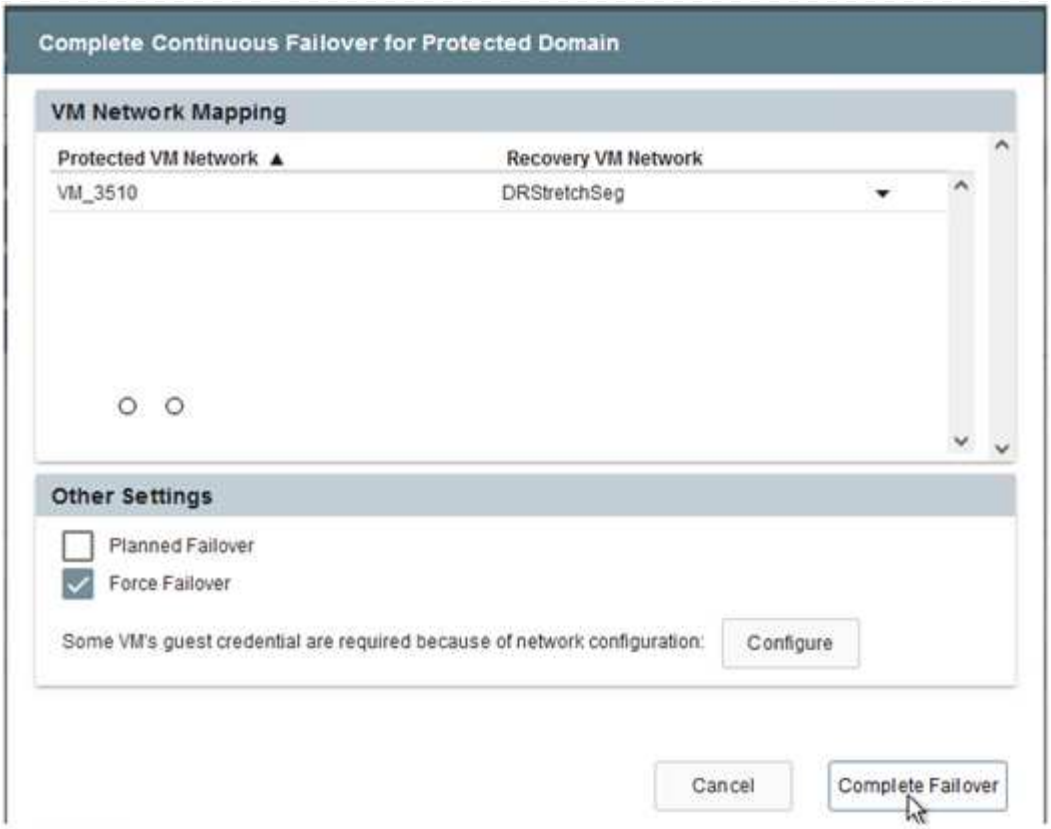
   Nella finestra di dialogo visualizzata al completamento del failover, è possibile specificare l'attività di failover come pianificata o presunta come forzata.





Il failover forzato presuppone che il sito primario non sia più accessibile e che la proprietà del dominio protetto debba essere direttamente assunta dal sito di ripristino.



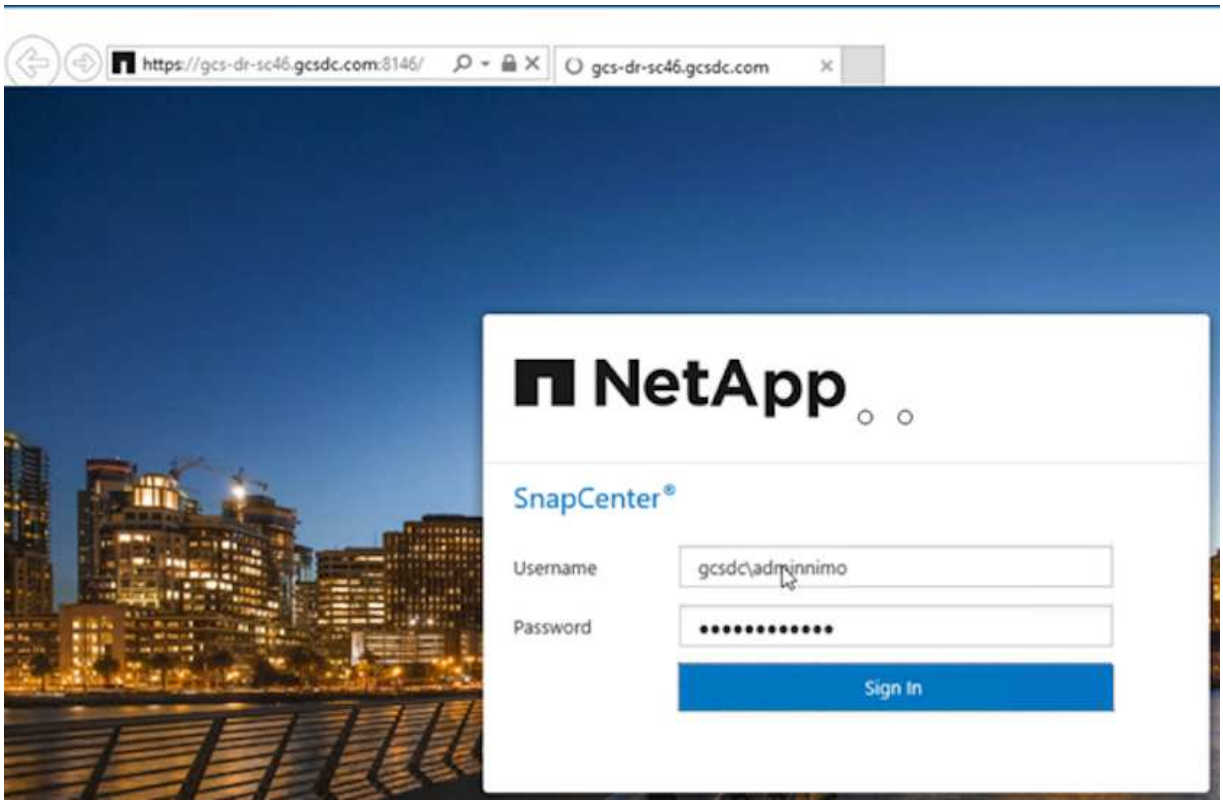


3. Una volta completato il failover continuo, viene visualizzato un messaggio che conferma il completamento dell'attività. Al termine dell'attività, accedere alle macchine virtuali ripristinate per configurare le sessioni ISCSI o NFS.

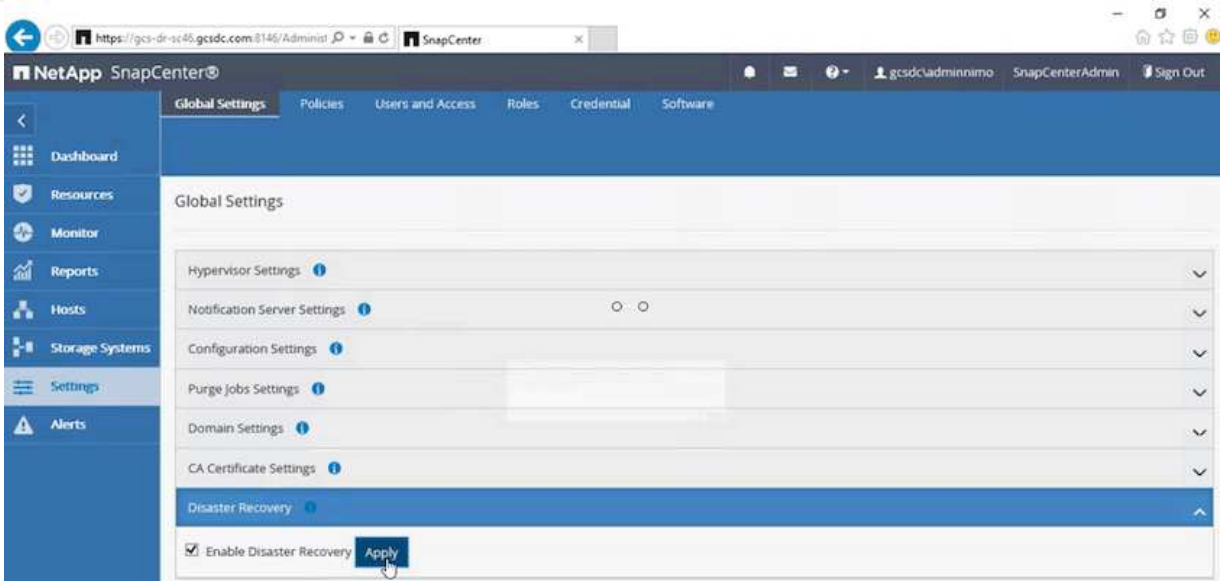
La modalità di failover diventa in esecuzione in failover e lo stato della macchina virtuale è ripristinabile. Tutte le macchine virtuali del dominio protetto sono ora in esecuzione nel sito di ripristino nello stato specificato dalle impostazioni del runbook di failover.

Per verificare la configurazione e l'infrastruttura di failover, è possibile utilizzare JetStream DR in modalità test (opzione Test failover) per osservare il ripristino delle macchine virtuali e dei relativi dati dall'archivio di oggetti in un ambiente di test recovery. Quando una procedura di failover viene eseguita in modalità test, il suo funzionamento assomiglia a un processo di failover effettivo.

4. Una volta ripristinate le macchine virtuali, utilizzare il disaster recovery dello storage per lo storage in-guest. Per dimostrare questo processo, in questo esempio viene utilizzato SQL Server.
5. Accedere alla macchina virtuale SnapCenter recuperata su AVS SDDC e attivare la modalità DR.
   a. Accedere all'interfaccia utente di SnapCenter utilizzando il browserN.



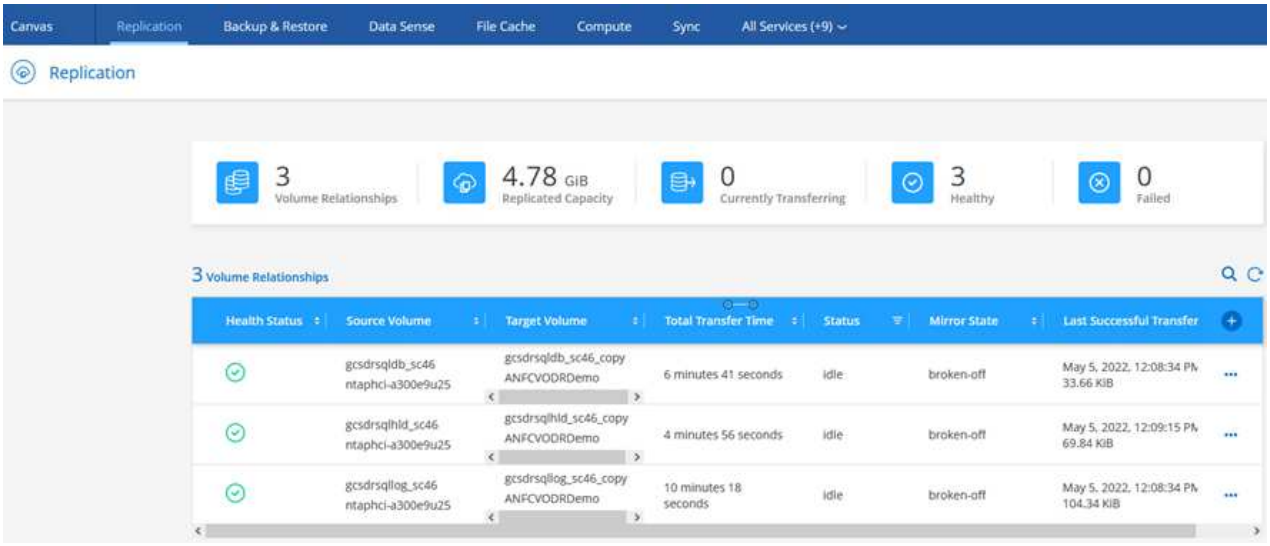
   b. Nella pagina Settings (Impostazioni), accedere a Settings (Impostazioni) > Global Settings (Impostazioni globali) > Disaster Recovery (Ripristino di emergenza).
   c. Selezionare Enable Disaster Recovery (attiva ripristino di emergenza).
   d. Fare clic su Applica.



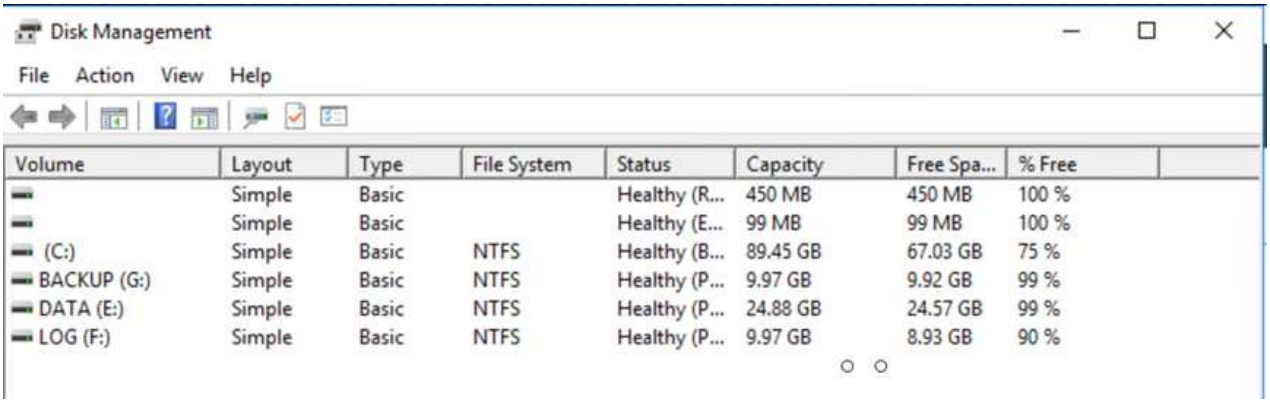
e. Verificare che il processo DR sia attivato facendo clic su Monitor > Jobs (Monitor > processi).

> Per il disaster recovery dello storage è necessario utilizzare NetApp SnapCenter 4.6 o versione successiva. Per le versioni precedenti, è necessario utilizzare snapshot coerenti con l'applicazione (replicati utilizzando SnapMirror) e eseguire il ripristino manuale nel caso in cui i backup precedenti debbano essere ripristinati nel sito di disaster recovery.

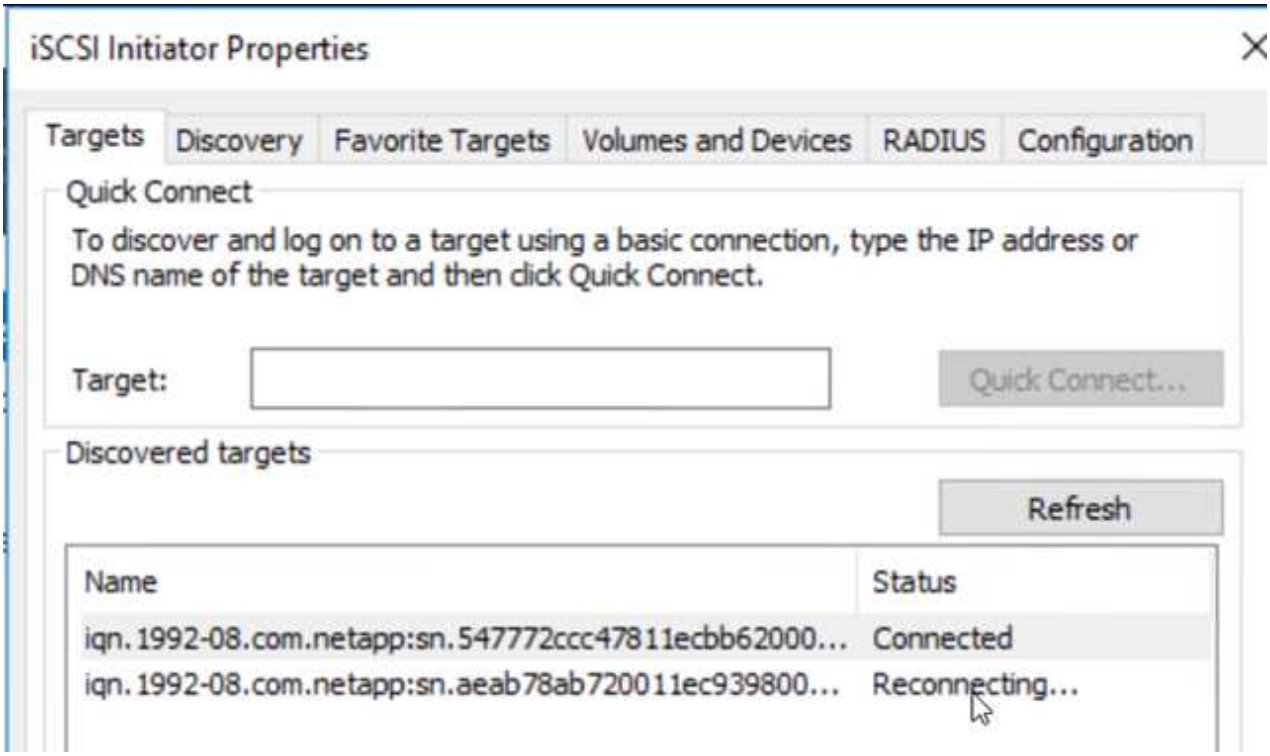
6. Verificare che la relazione di SnapMirror non sia più stabilita.



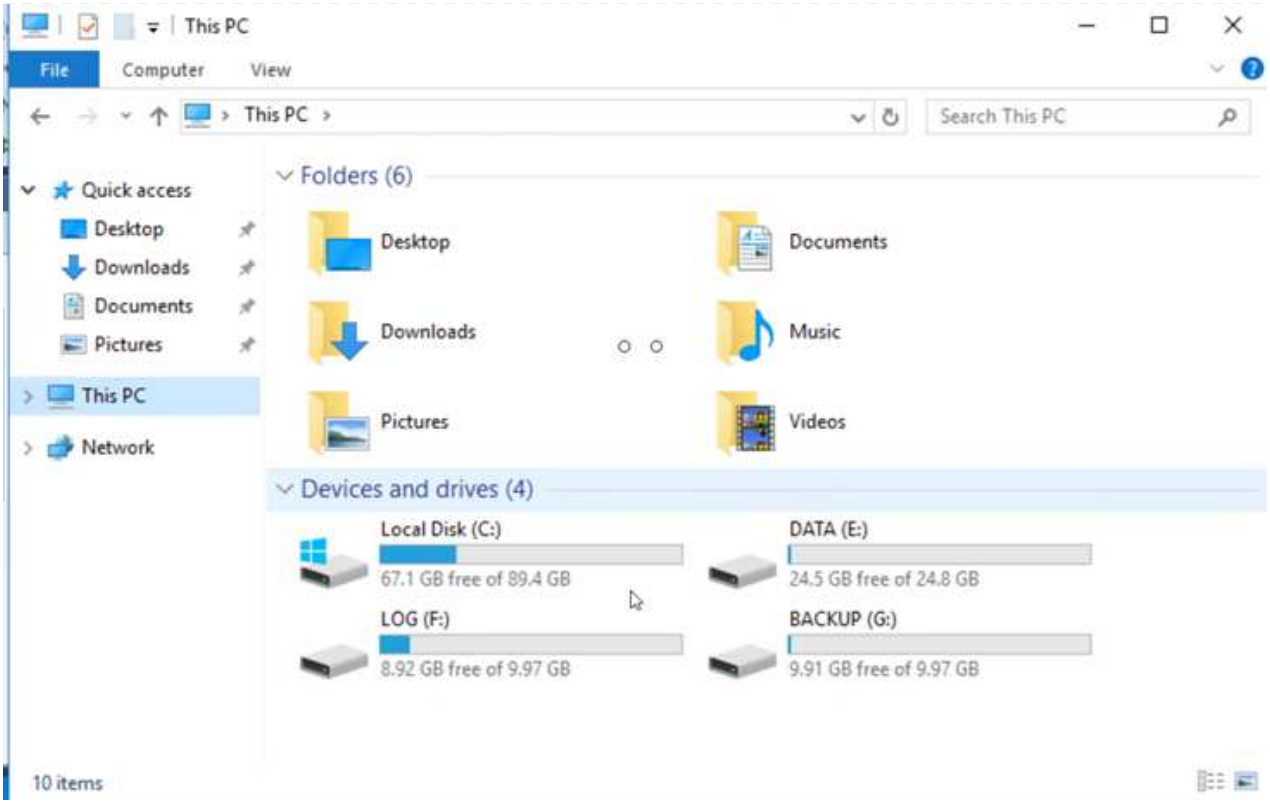
7. Collegare il LUN da Cloud Volumes ONTAP alla macchina virtuale SQL guest recuperata con le stesse lettere di unità.



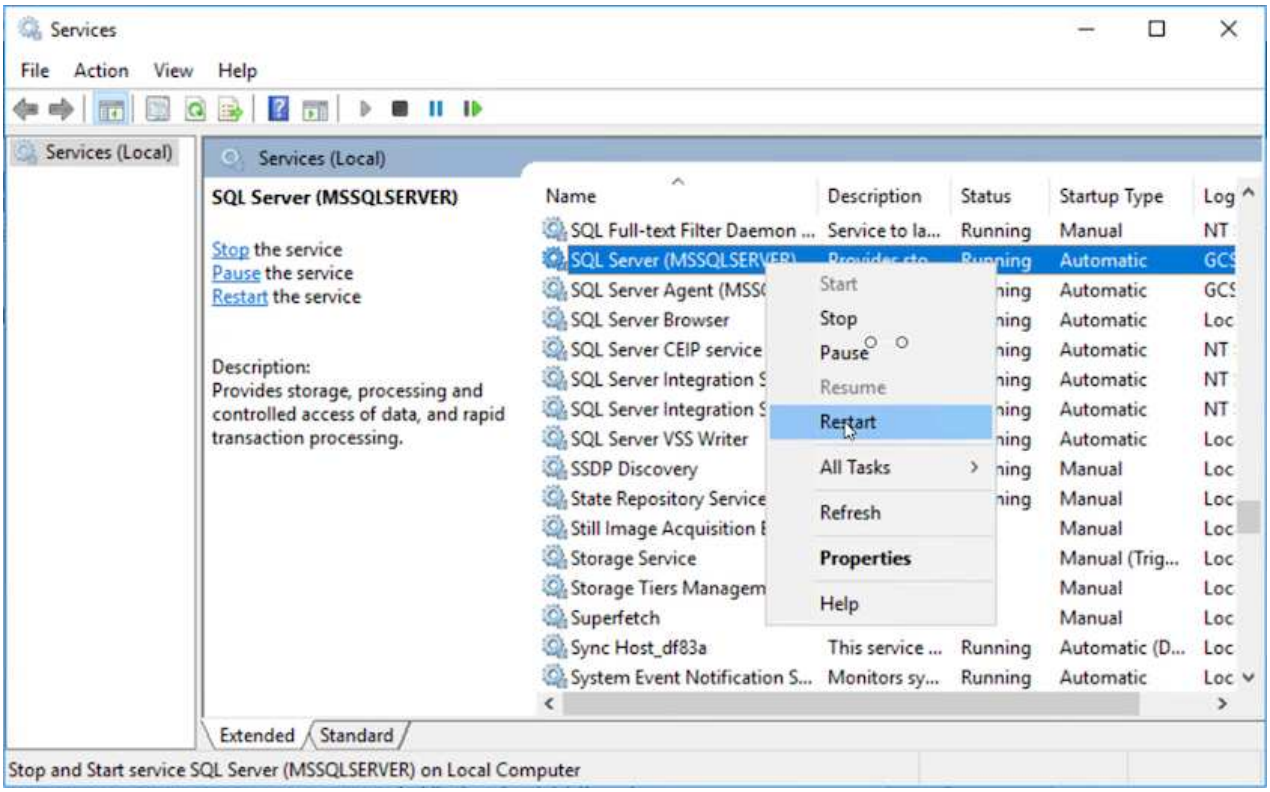
8. Aprire iSCSI Initiator, cancellare la sessione disconnessa precedente e aggiungere la nuova destinazione insieme al multipath per i volumi Cloud Volumes ONTAP replicati.



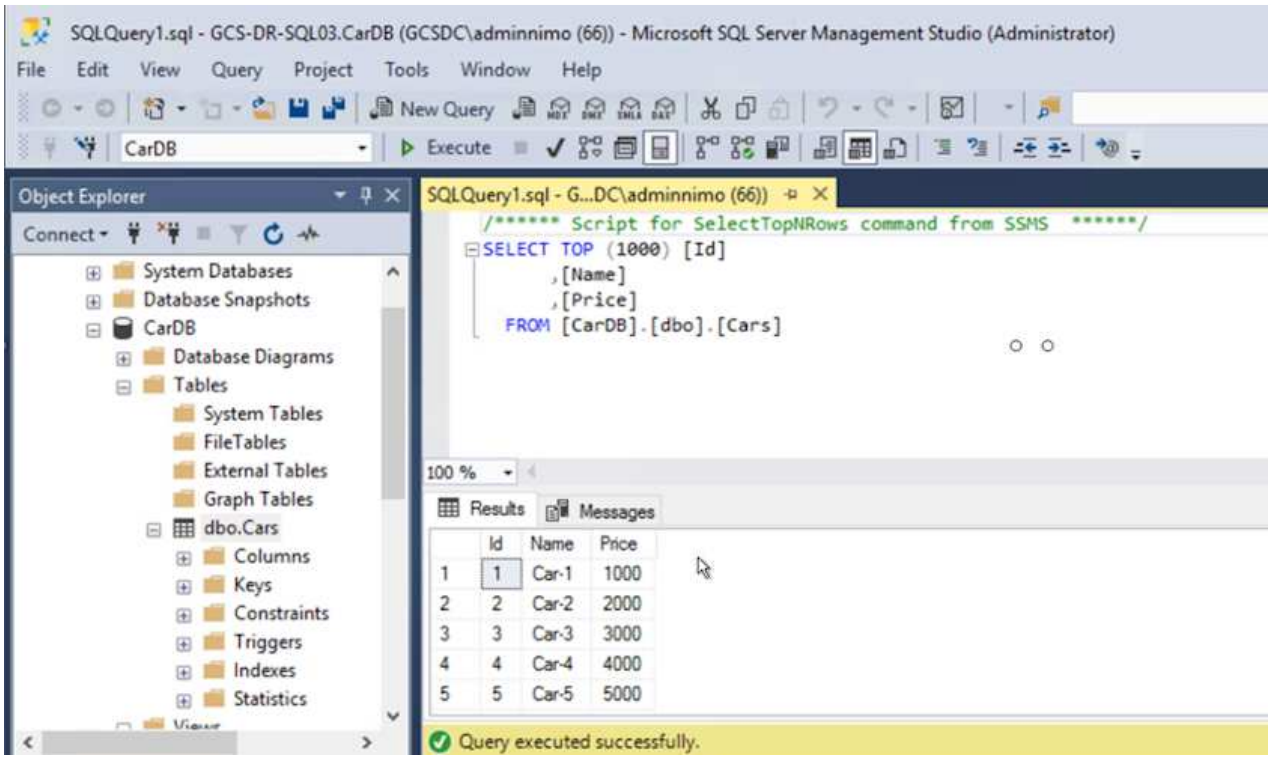
9. Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.



10. Riavviare il servizio del server MSSQL.



11. Assicurarsi che le risorse SQL siano nuovamente in linea.



Nel caso di NFS, collegare i volumi utilizzando il comando mount e aggiornare `/etc/fstab` voci.

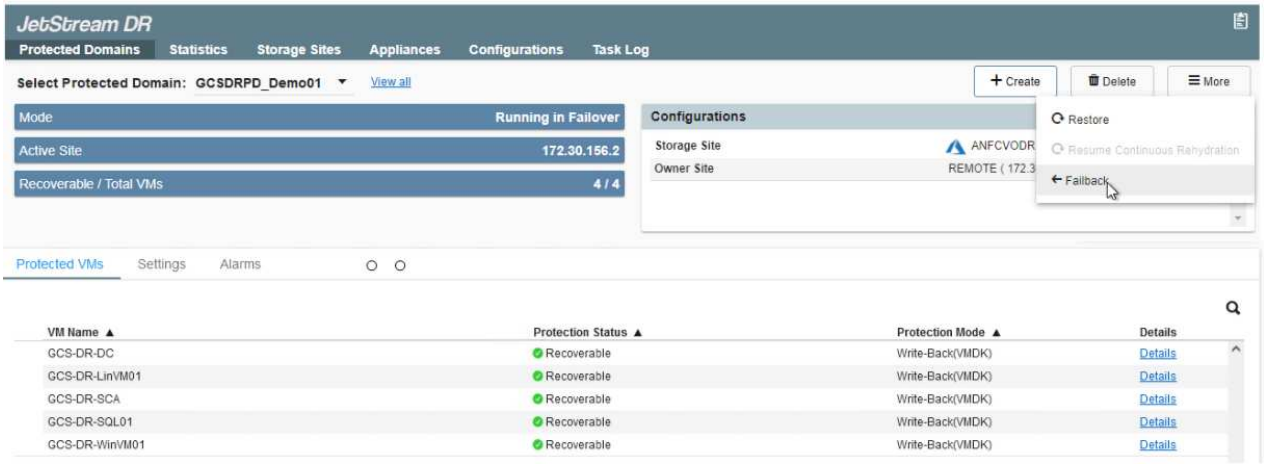
A questo punto, è possibile eseguire le operazioni e continuare normalmente il business.

Sull'estremità NSX-T, è possibile creare un gateway Tier-1 dedicato separato per simulare scenari di failover. Ciò garantisce che tutti i carichi di lavoro possano comunicare tra loro, ma che nessun traffico possa essere instradato all'interno o all'esterno dell'ambiente, in modo che qualsiasi attività di triage, contenimento o protezione avanzata possa essere eseguita senza rischi di contaminazione incrociata. Questa operazione non rientra nell'ambito del presente documento, ma può essere facilmente eseguita per simulare l'isolamento.

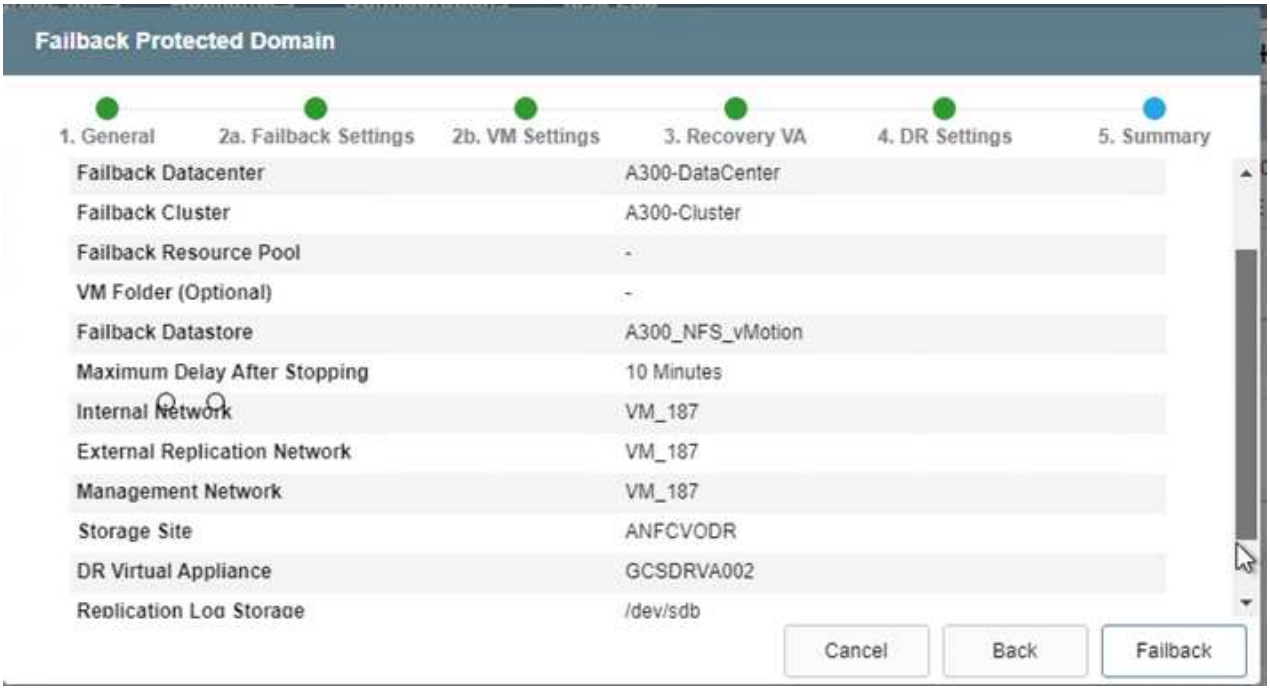
Una volta che il sito primario è stato nuovamente operativo, è possibile eseguire il failback. La protezione delle macchine virtuali viene ripristinata da Jetstream e la relazione SnapMirror deve essere invertita.

1. Ripristinare l'ambiente on-premise. A seconda del tipo di incidente, potrebbe essere necessario ripristinare e/o verificare la configurazione del cluster protetto. Se necessario, potrebbe essere necessario reinstallare il software DR JetStream.
2. Accedere all'ambiente on-premise ripristinato, accedere all'interfaccia utente DR Jetstream e selezionare il dominio protetto appropriato. Una volta che il sito protetto è pronto per il failback, selezionare l'opzione failover nell'interfaccia utente.

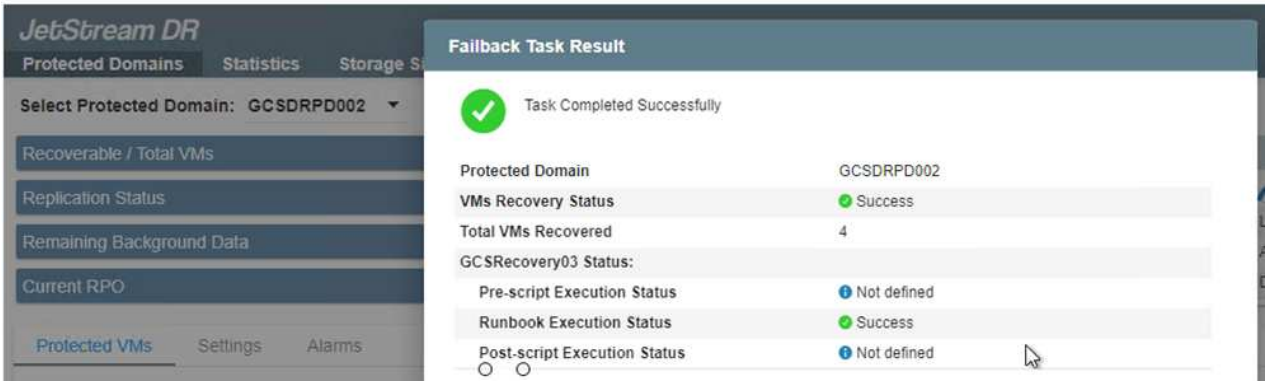
Il piano di failback generato da CPT può anche essere utilizzato per avviare il ritorno delle macchine virtuali e dei relativi dati dall'archivio di oggetti all'ambiente VMware originale.



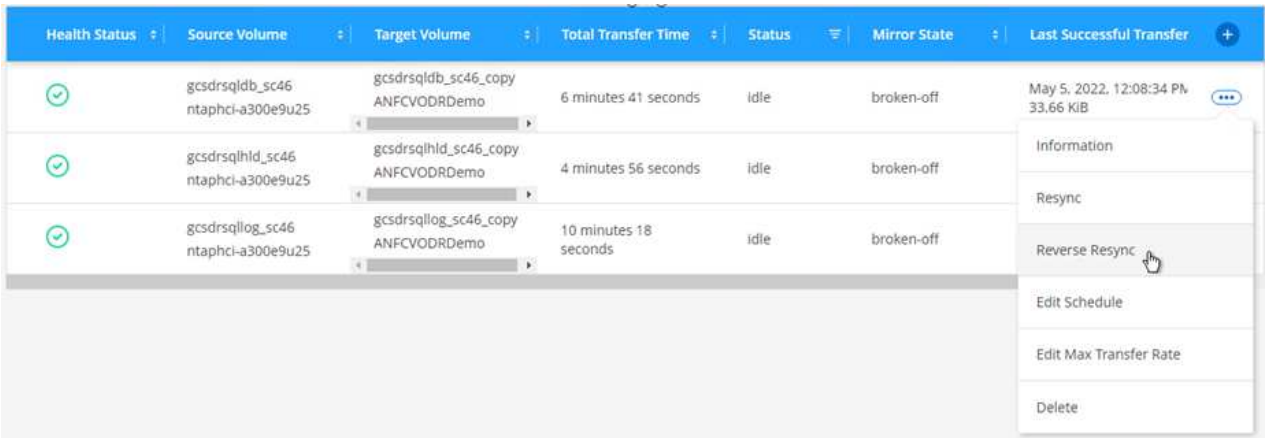
Specificare il ritardo massimo dopo la pausa delle macchine virtuali nel sito di ripristino e il riavvio nel sito protetto. Il tempo necessario per completare questo processo include il completamento della replica dopo l'arresto delle macchine virtuali di failover, il tempo necessario per pulire il sito di ripristino e il tempo necessario per ricreare le macchine virtuali nel sito protetto. NetApp consiglia 10 minuti.

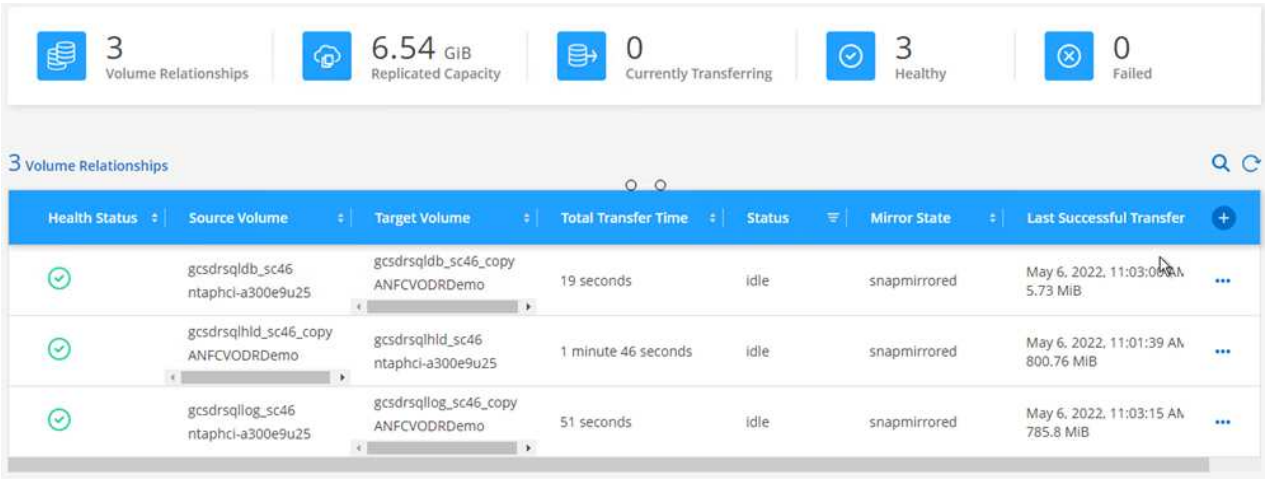


3. Completare il processo di failback e confermare la ripresa della protezione delle macchine virtuali e la coerenza dei dati.

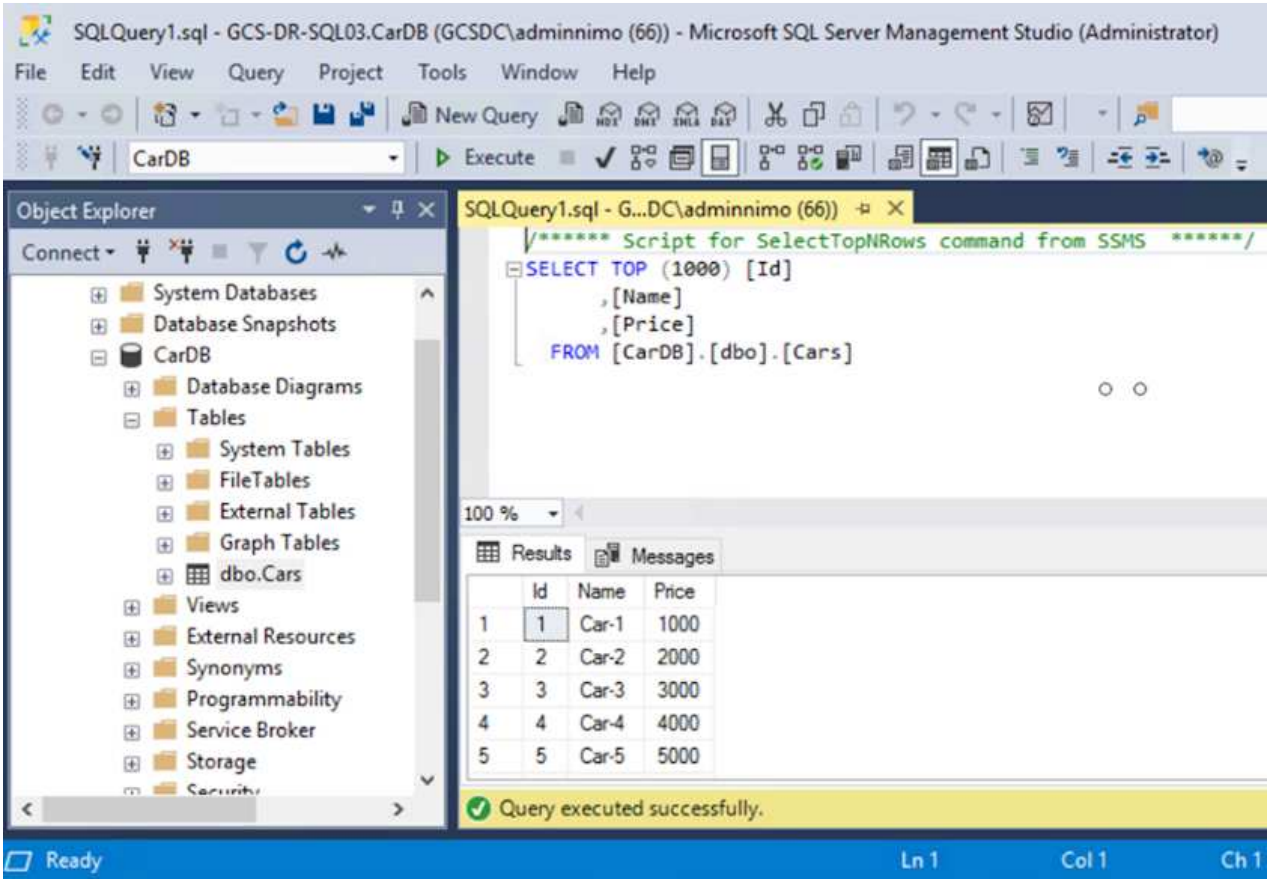


4. Una volta ripristinate le macchine virtuali, scollegare lo storage secondario dall'host e connettersi allo storage primario.





5. Riavviare il servizio del server MSSQL.
6. Verificare che le risorse SQL siano nuovamente in linea.



Per eseguire il failback allo storage primario, assicurarsi che la direzione della relazione rimanga la stessa di prima del failover eseguendo un'operazione di risincronizzazione inversa.

Per mantenere i ruoli dello storage primario e secondario dopo l'operazione di risincronizzazione inversa, eseguire nuovamente l'operazione di risincronizzazione inversa.

Questo processo è applicabile ad altre applicazioni come Oracle, ad altri tipi di database simili e ad altre applicazioni che utilizzano lo storage connesso al guest.

Come sempre, verifica le fasi necessarie per il ripristino dei carichi di lavoro critici prima di portarli in produzione.

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.
  - In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
  - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.

- Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.

- L'ottimizzazione della CPU e della RAM può contribuire a ridurre i costi del cloud consentendo il ripristino di cluster di calcolo più piccoli.

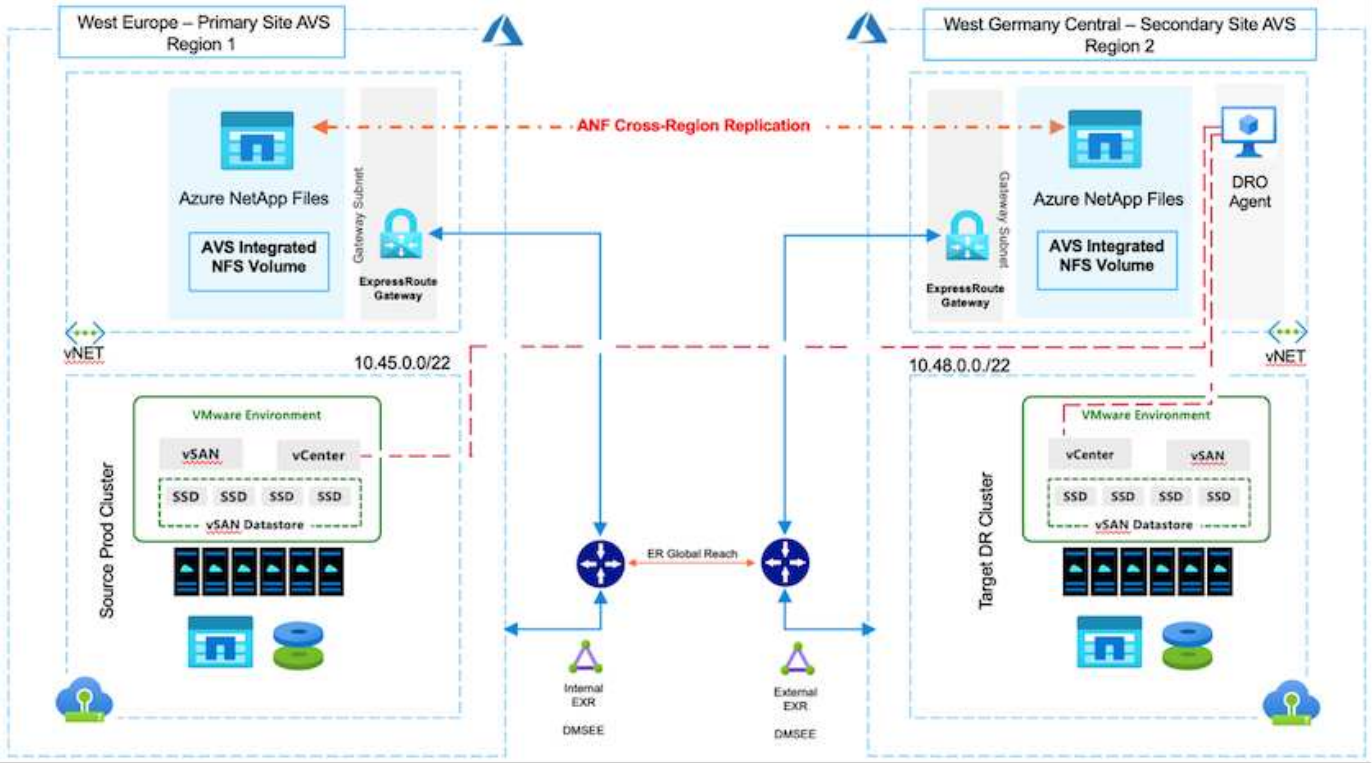
TR-4955: Disaster recovery con Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

Autore: Niyaz Mohamed, NetApp Solutions Engineering

Panoramica

Il disaster recovery che utilizza la replica a livello di blocco tra regioni all'interno del cloud è un metodo resiliente e conveniente per proteggere i carichi di lavoro da interruzioni del sito ed eventi di corruzione dei dati (ad esempio ransomware). Con la replica dei volumi Azure NetApp Files (ANF) cross-region, i carichi di lavoro VMware eseguiti su un sito SDDC Azure VMware Solution (AVS) utilizzando i volumi Azure NetApp Files come datastore NFS sul sito AVS primario possono essere replicati in un sito AVS secondario designato nella regione di recupero di destinazione.

Disaster Recovery Orchestrator (DRO) (una soluzione basata su script con un'interfaccia utente) può essere utilizzato per ripristinare senza problemi i carichi di lavoro replicati da un SDDC AVS a un altro. DRO automatizza il recovery interrompendo il peering delle repliche e montando il volume di destinazione come datastore, attraverso la registrazione delle macchine virtuali in AVS, sulle mappature di rete direttamente su NSX-T (incluso con tutti i cloud privati AVS).



Prerequisiti e raccomandazioni generali

- Verificare di aver attivato la replica tra regioni creando il peering delle repliche. Vedere "Creare la replica di un volume per Azure NetApp Files".

- È necessario configurare ExpressRoute Global Reach tra i cloud privati Azure VMware Solution di origine e di destinazione.

- È necessario disporre di un service principal in grado di accedere alle risorse.
- È supportata la seguente topologia: Dal sito AVS primario al sito AVS secondario.
- Configurare "replica" pianifica ciascun volume in modo appropriato in base alle esigenze aziendali e al tasso di cambiamento dei dati.

> Non sono supportate topologie a cascata e fan-in e fan-out.

Per iniziare

Implementare la soluzione VMware Azure

Il "Soluzione VMware Azure" (AVS) è un servizio di cloud ibrido che fornisce SDDC VMware completamente funzionali all'interno di un cloud pubblico Microsoft Azure. AVS è una soluzione di prima parte completamente gestita e supportata da Microsoft e verificata da VMware che utilizza l'infrastruttura Azure. Pertanto, i clienti ottengono VMware ESXi per la virtualizzazione del calcolo, vSAN per lo storage iperconvergente e NSX per il networking e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture di data center leader di settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure native. Una combinazione di SDDC e Azure NetApp Files per la soluzione VMware Azure offre le migliori performance con una latenza di rete minima.

Per configurare un cloud privato AVS su Azure, seguire la procedura descritta in questa sezione "collegamento" Per la documentazione NetApp e in questo "collegamento" Per la documentazione Microsoft. Un ambiente pilota con configurazione minima può essere utilizzato per scopi di DR. Questa configurazione contiene solo i componenti principali per supportare le applicazioni critiche e può scalare e generare più host per sostenere la maggior parte del carico in caso di failover.

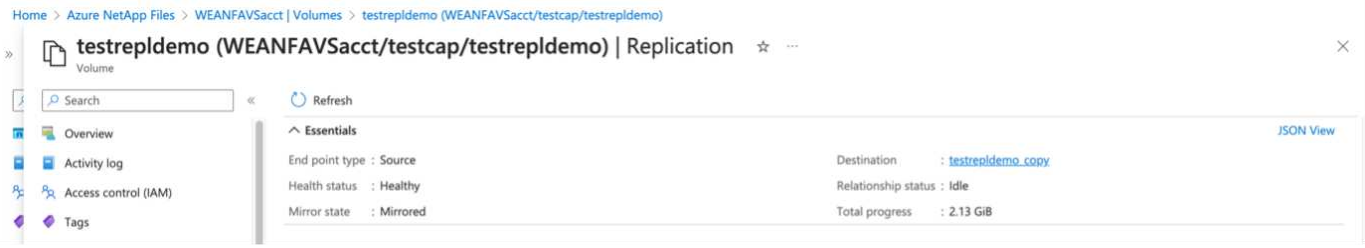
> Nella versione iniziale, DRO supporta un cluster SDDC AVS esistente. La creazione di SDDC on-demand sarà disponibile in una release imminente.

Provisioning e configurazione di Azure NetApp Files

"Azure NetApp Files" è un servizio di file storage misurato di livello enterprise dalle performance elevate. Seguire la procedura descritta in questa sezione "collegamento" Eseguire il provisioning e la configurazione di Azure NetApp Files come datastore NFS per ottimizzare le implementazioni di cloud privato AVS.

Creazione di replica di volumi per i volumi datastore basati su file di Azure NetApp

Il primo passaggio consiste nell'impostare la replica cross-region per i volumi del datastore desiderati dal sito primario AVS al sito secondario AVS con le frequenze e le ritention appropriate.



Seguire la procedura descritta in questa sezione "collegamento" per impostare la replica tra regioni creando il peering delle repliche. Il livello di servizio per il pool di capacità di destinazione può corrispondere a quello del pool di capacità di origine. Tuttavia, per questo caso di utilizzo specifico, è possibile selezionare il livello di servizio standard, quindi "modificare il livello di servizio" In caso di disastro reale o di simulazioni di DR.

Una relazione di replica tra regioni è un prerequisito e deve essere creata in anticipo.

Installazione DRO

Per iniziare a utilizzare DRO, utilizzare il sistema operativo Ubuntu sulla macchina virtuale Azure designata e assicurarsi di soddisfare i prerequisiti. Quindi installare il pacchetto.

Prerequisiti:

- Service Principal in grado di accedere alle risorse.
- Assicurarsi che esista una connettività appropriata alle istanze SDDC e Azure NetApp Files di origine e destinazione.
- Se si utilizzano i nomi DNS, la risoluzione DNS deve essere effettiva. In caso contrario, utilizzare gli indirizzi IP per vCenter.

Requisiti del sistema operativo:

- Ubuntu Focal 20.04 (LTS)i seguenti pacchetti devono essere installati sulla macchina virtuale dell'agente designata:
- Docker
- Docker - comporre
- JqChange `docker.sock` a questa nuova autorizzazione: `sudo chmod 666 /var/run/docker.sock`.

Il `deploy.sh` lo script esegue tutti i prerequisiti richiesti.

I passaggi sono i seguenti:

1. Scaricare il pacchetto di installazione sulla macchina virtuale designata:

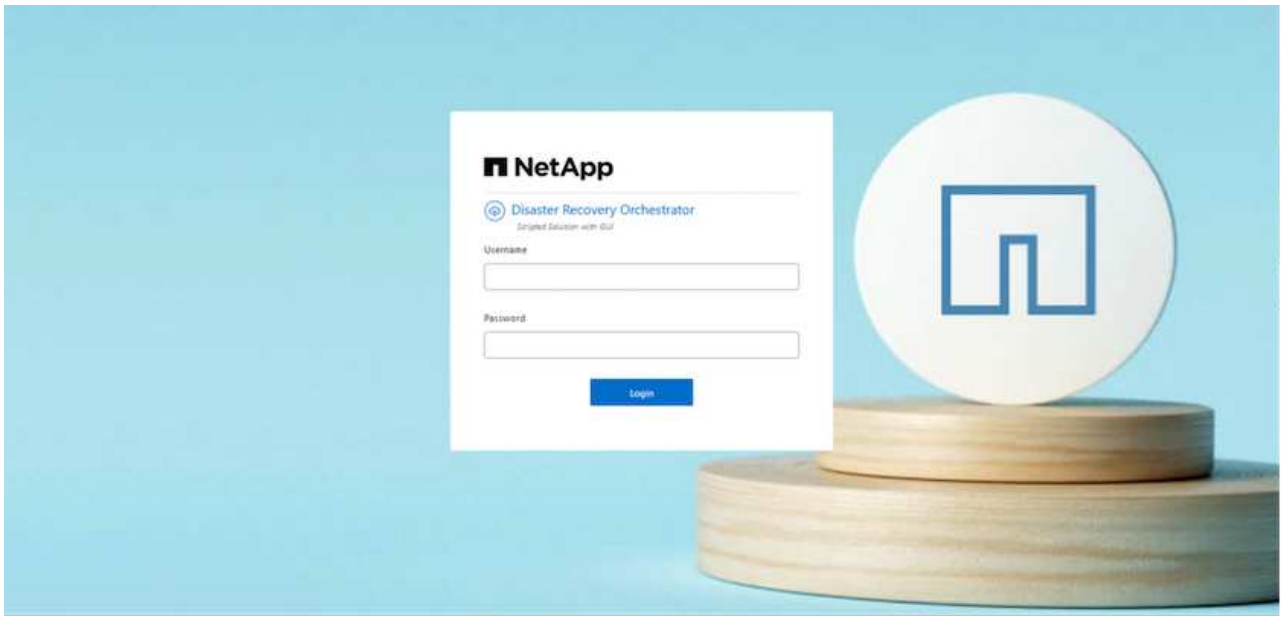
```
git clone https://github.com/NetApp/DRO-Azure.git
```

L'agente deve essere installato nell'area del sito AVS secondario o nell'area del sito AVS primario in un AZ separato da SDDC.

2. Decomprimere il pacchetto, eseguire lo script di implementazione e immettere l'IP host (ad esempio, `10.10.10.10`).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Accedere all'interfaccia utente utilizzando le seguenti credenziali:
   - Nome utente: `admin`
   - Password: `admin`



Configurazione DRO

Dopo aver configurato correttamente Azure NetApp Files e AVS, è possibile iniziare a configurare DRO per automatizzare il ripristino dei workload dal sito AVS primario al sito AVS secondario. NetApp consiglia di implementare l'agente DRO nel sito AVS secondario e di configurare la connessione del gateway ExpressRoute in modo che l'agente DRO possa comunicare tramite la rete con i componenti AVS e Azure NetApp Files appropriati.

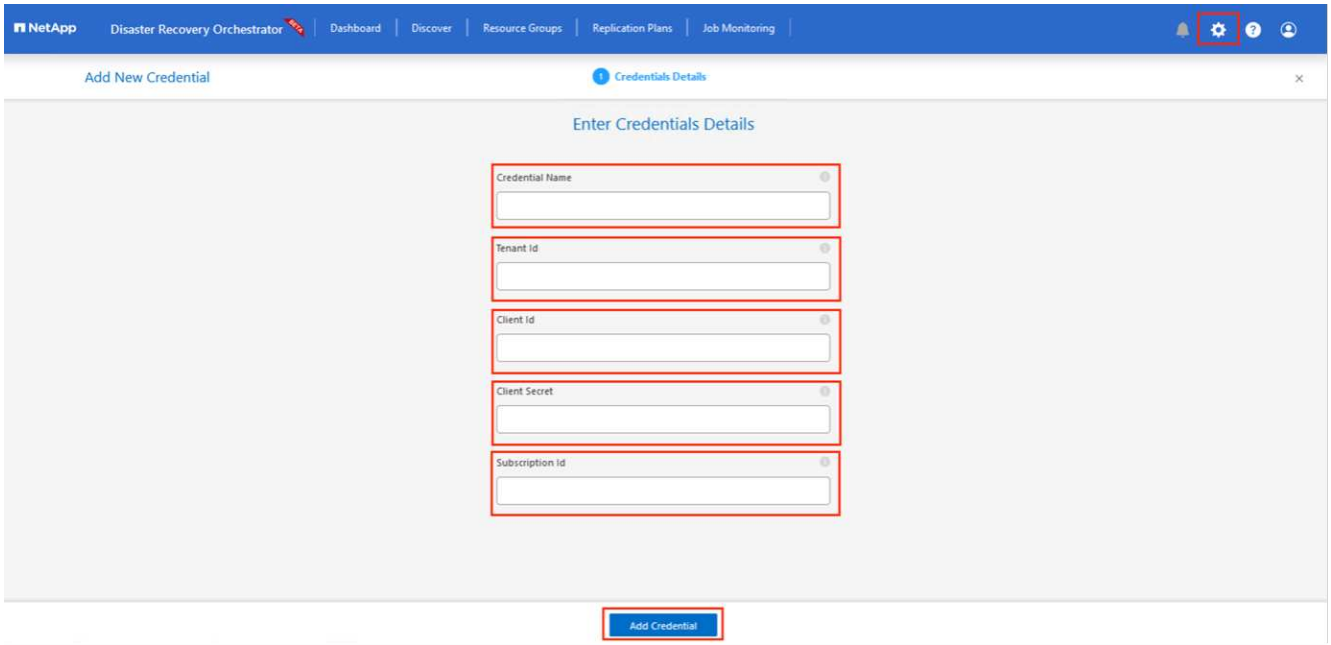
Il primo passaggio consiste nell'aggiungere credenziali. DRO richiede l'autorizzazione per scoprire Azure NetApp Files e la soluzione VMware Azure. È possibile concedere le autorizzazioni richieste a un account Azure creando e configurando un'applicazione Azure Active Directory (ad) e ottenendo le credenziali Azure necessarie a DRO. È necessario associare l'entità del servizio all'abbonamento Azure e assegnargli un ruolo personalizzato con le autorizzazioni necessarie pertinenti. Quando si aggiungono ambienti di origine e di destinazione, viene richiesto di selezionare le credenziali associate all'entità del servizio. È necessario aggiungere queste credenziali a DRO prima di fare clic su Add New Site (Aggiungi nuovo sito).

Per eseguire questa operazione, attenersi alla seguente procedura:

1. Aprire DRO in un browser supportato e utilizzare il nome utente e la password predefiniti (`admin`/`admin`). La password può essere reimpostata dopo il primo accesso utilizzando l'opzione Change Password (Modifica password).
2. Nella parte superiore destra della console DRO, fare clic sull'icona **Impostazioni** e selezionare **credenziali**.
3. Fare clic su Add New Credential (Aggiungi nuova credenziale) e seguire la procedura guidata.
4. Per definire le credenziali, immettere le informazioni relative all'entità del servizio Azure Active Directory che concede le autorizzazioni richieste:
    - Nome della credenziale
    - ID tenant
    - ID client
    - Segreto del client
    - ID abbonamento

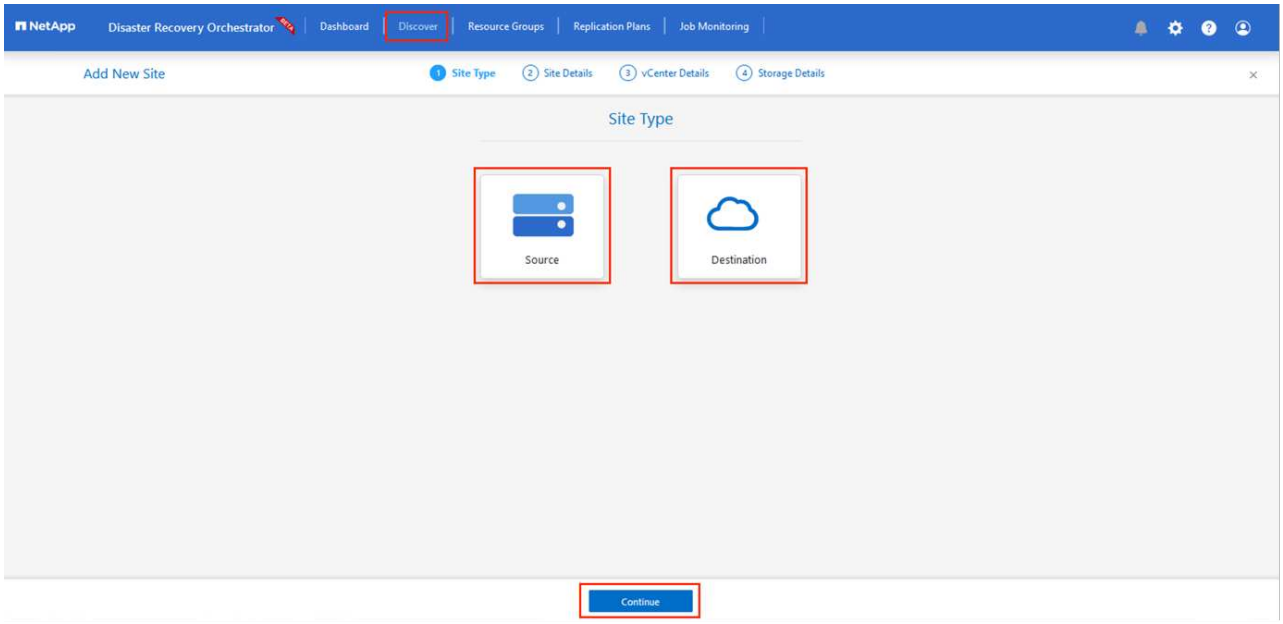
Queste informazioni dovrebbero essere state acquisite al momento della creazione dell'applicazione ad.

5. Confermare i dettagli relativi alle nuove credenziali e fare clic su Add Credential (Aggiungi credenziale).



Dopo aver aggiunto le credenziali, è il momento di individuare e aggiungere i siti AVS primari e secondari (sia vCenter che l'account storage Azure NetApp Files) a DRO. Per aggiungere il sito di origine e di destinazione, attenersi alla seguente procedura:

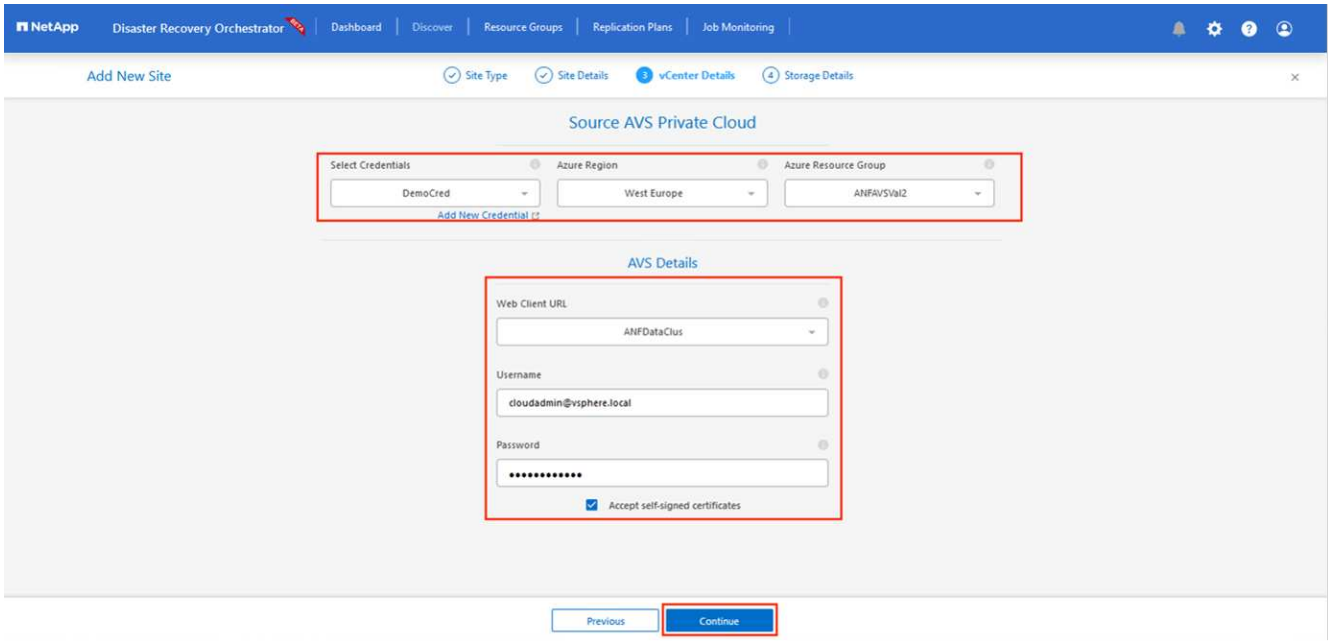
6. Accedere alla scheda **Discover**.
7. Fare clic su **Aggiungi nuovo sito**.
8. Aggiungere il seguente sito AVS primario (indicato come **origine** nella console).
   - VCenter SDDC
   - Account storage Azure NetApp Files
9. Aggiungere il seguente sito AVS secondario (indicato come **destinazione** nella console).
   - VCenter SDDC
   - Account storage Azure NetApp Files



10. Aggiungere i dettagli del sito facendo clic su **Source (origine),** immettendo un nome descrittivo del sito e selezionando il connettore. Quindi fare clic su **continua**.

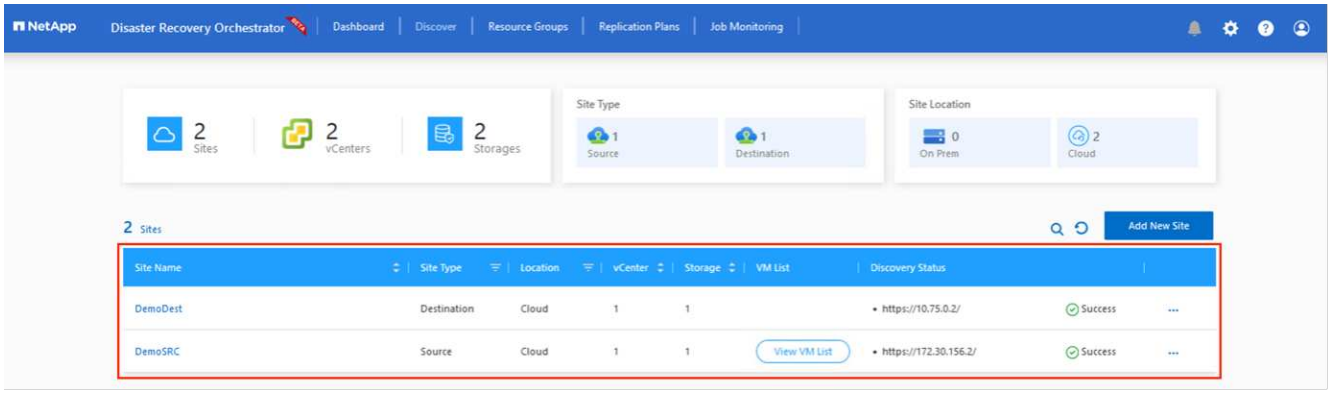
> A scopo dimostrativo, l'aggiunta di un sito di origine viene trattata in questo documento.

11. Aggiorna i dettagli di vCenter. A tale scopo, selezionare le credenziali, l'area Azure e il gruppo di risorse dal menu a discesa per l'AVS SDDC primario.
12. IL DRO elenca tutti gli SDDC disponibili all'interno della regione. Selezionare l'URL del cloud privato designato dal menu a discesa.
13. Inserire il `cloudadmin@vsphere.local` credenziali dell'utente. È possibile accedervi dal portale Azure. Seguire la procedura indicata in questo "collegamento". Al termine, fare clic su **Continue** (continua).

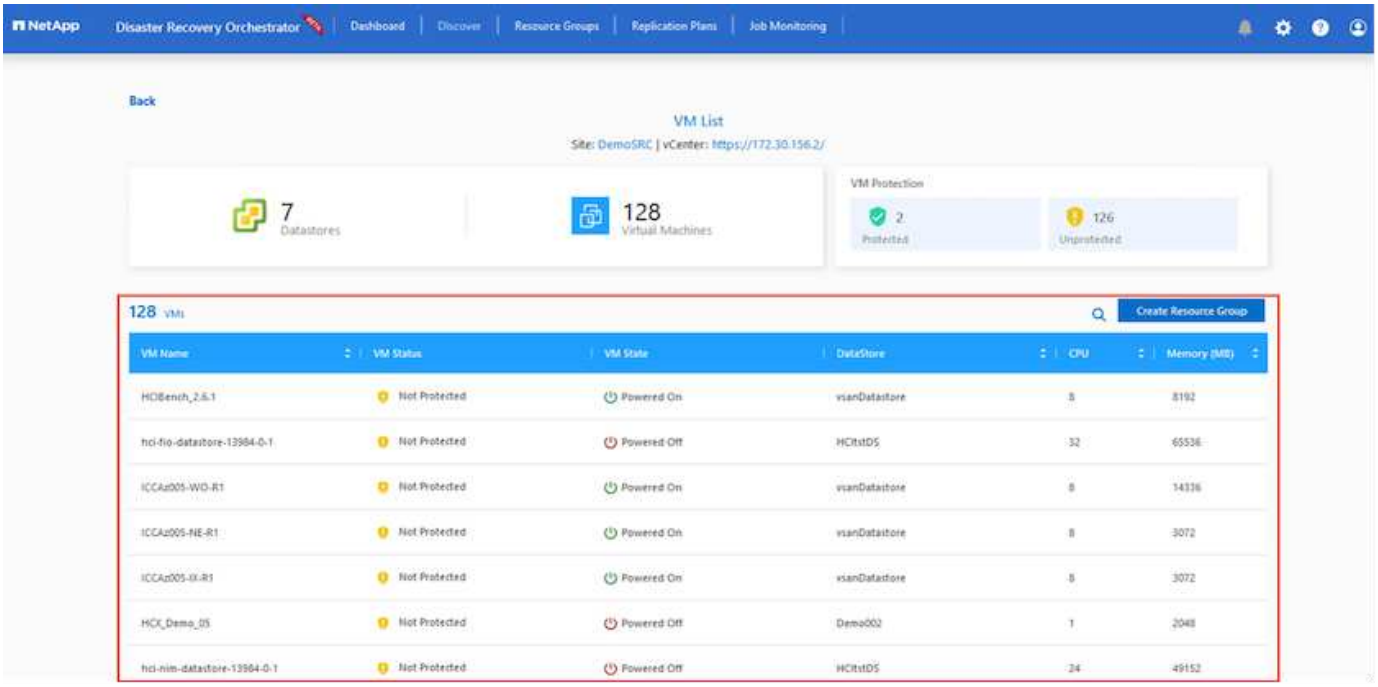


14. Selezionare i dettagli dell'archiviazione di origine (ANF) selezionando il gruppo Azure Resource e l'account NetApp.

15. Fare clic su **Create Site** (Crea sito).



Una volta aggiunto, DRO esegue il rilevamento automatico e visualizza le macchine virtuali con repliche tra regioni corrispondenti dal sito di origine al sito di destinazione. DRO rileva automaticamente le reti e i segmenti utilizzati dalle macchine virtuali e li popola.



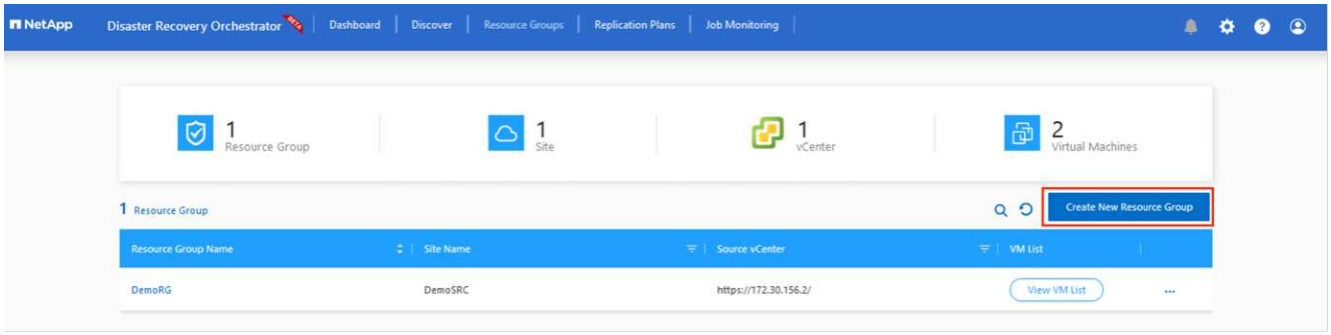
Il passaggio successivo consiste nel raggruppare le macchine virtuali richieste nei rispettivi gruppi funzionali come gruppi di risorse.

Raggruppamenti di risorse

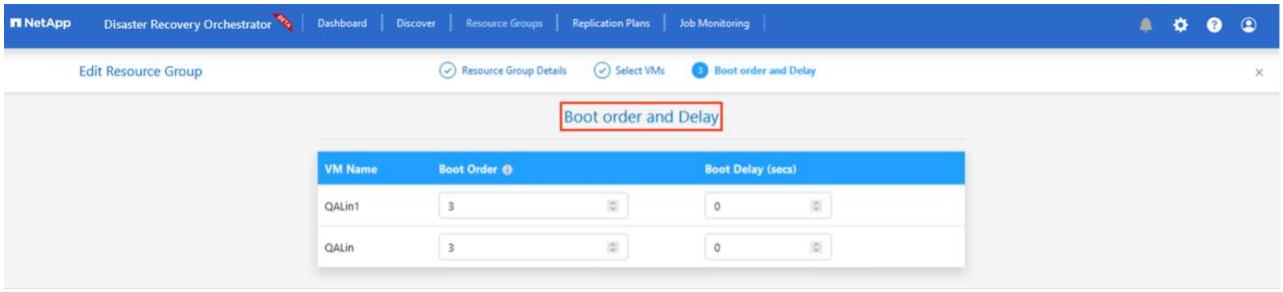
Una volta aggiunte le piattaforme, raggruppare le macchine virtuali che si desidera ripristinare in gruppi di risorse. I gruppi di risorse DRO consentono di raggruppare un set di macchine virtuali dipendenti in gruppi logici che contengono i relativi ordini di avvio, ritardi di avvio e validazioni opzionali delle applicazioni che possono essere eseguite al momento del ripristino.

Per iniziare a creare gruppi di risorse, fare clic sulla voce di menu **Crea nuovo gruppo di risorse**.

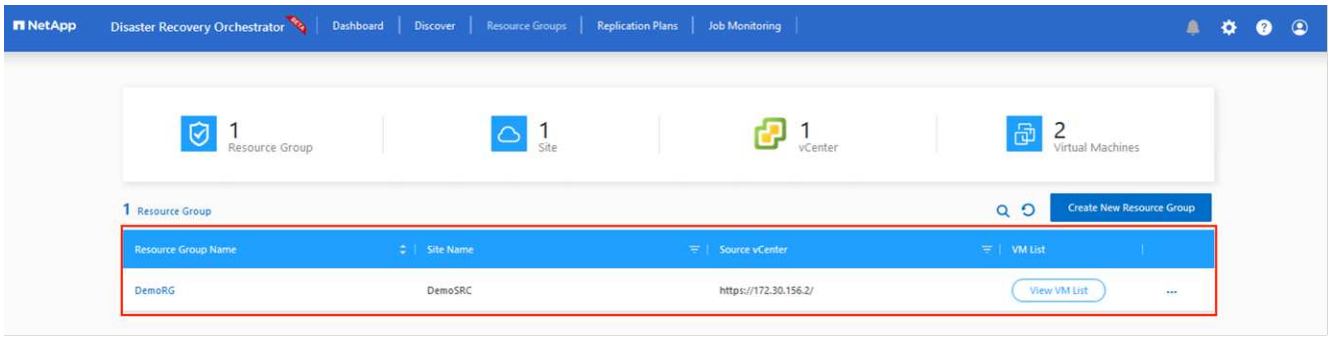
1. Accedere a **Resource Grou*ps e fare clic su *Create New Resource Group** (Crea nuovo gruppo di risorse).



2. In New Resource Group (nuovo gruppo di risorse), selezionare il sito di origine dal menu a discesa e fare clic su **Create** (Crea).
3. Fornire i dettagli del gruppo di risorse e fare clic su **continua**.
4. Selezionare le macchine virtuali appropriate utilizzando l'opzione di ricerca.
5. Selezionare **Boot Order** (Ordine di avvio) e **Boot Delay** (sec) per tutte le macchine virtuali selezionate. Impostare l'ordine della sequenza di accensione selezionando ciascuna macchina virtuale e impostando la relativa priorità. Il valore predefinito per tutte le macchine virtuali è 3. Le opzioni sono le seguenti:
   - La prima macchina virtuale ad accenderlo
   - Predefinito
   - L'ultima macchina virtuale ad accenderlo



6. Fare clic su **Crea gruppo di risorse**.



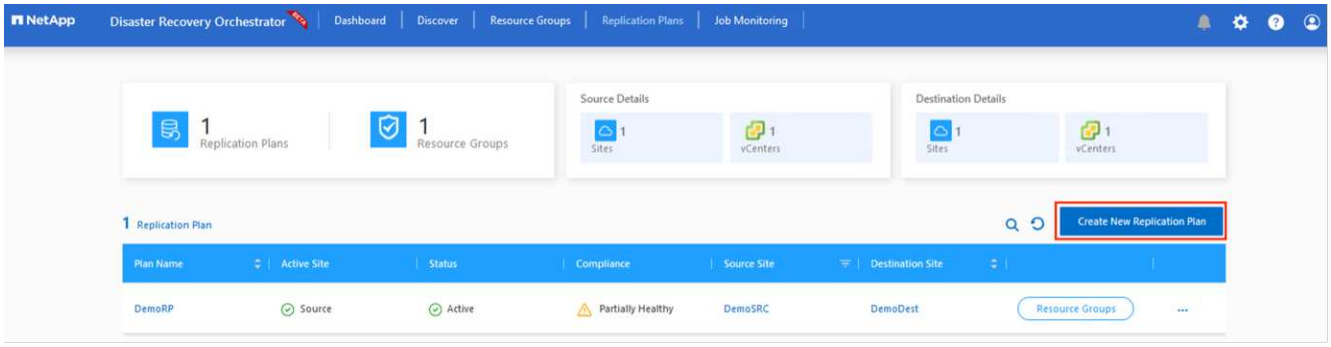
Piani di replica

È necessario disporre di un piano per il ripristino delle applicazioni in caso di disastro. Selezionare le piattaforme vCenter di origine e di destinazione dall'elenco a discesa, scegliere i gruppi di risorse da includere in questo piano e includere anche il raggruppamento delle modalità di ripristino e accensione delle applicazioni (ad esempio, controller di dominio, Tier-1, Tier-2 e così via). I piani sono spesso chiamati anche blueprint. Per definire il piano di ripristino, accedere alla scheda Replication Plan (piano di replica) e fare clic su **New**

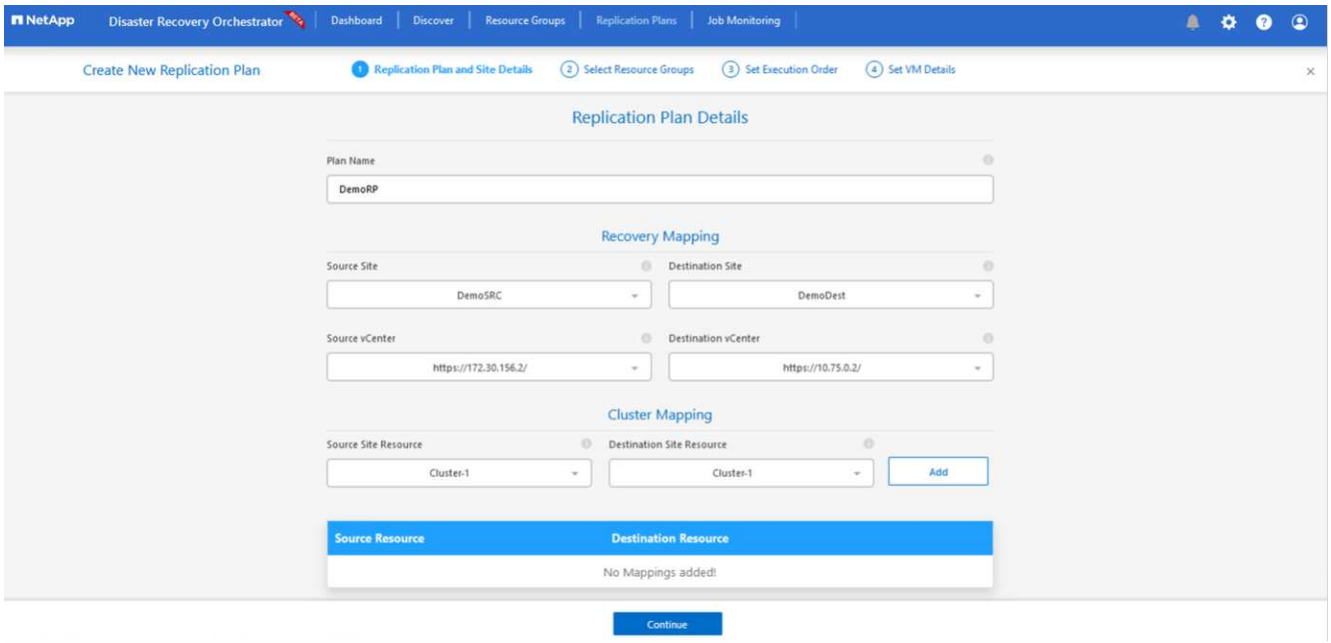
Replication Plan (nuovo piano di replica).

Per iniziare a creare un piano di replica, attenersi alla seguente procedura:

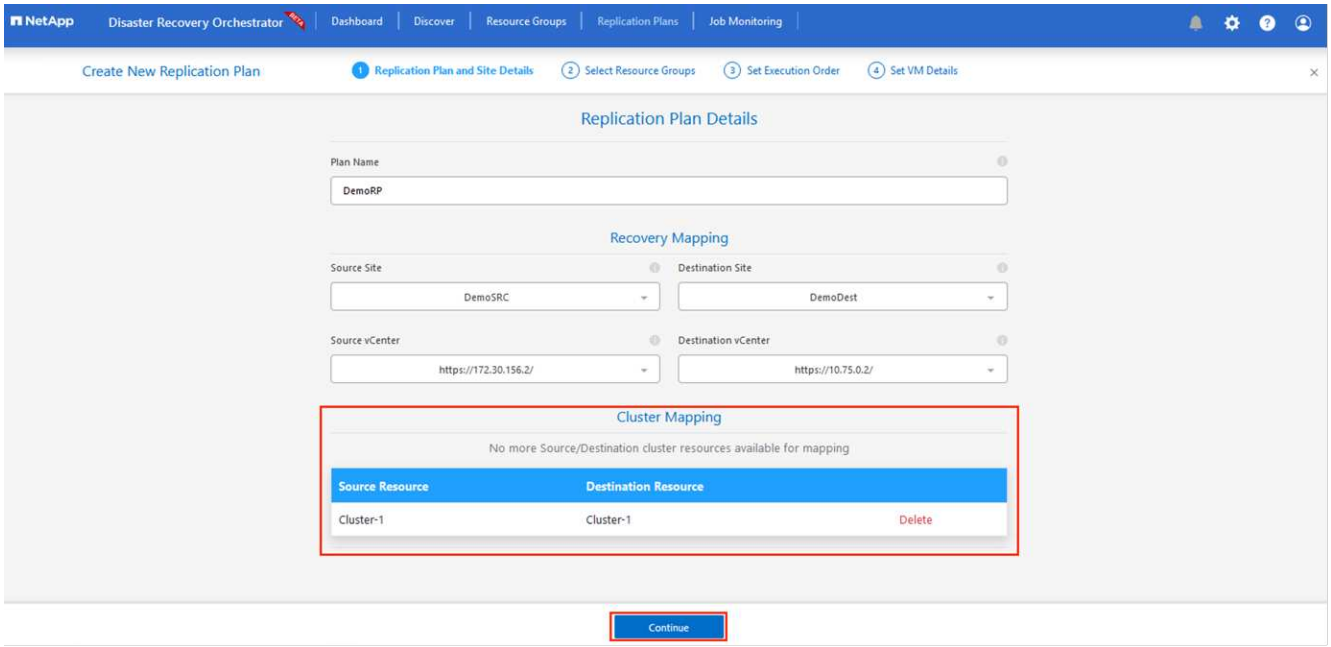
1. Selezionare **Replication Plans** (piani di replica) e fare clic su **Create New Replication Plan** (Crea nuovo piano di replica



2. In **New Replication Plan**, fornire un nome per il piano e aggiungere i mapping di ripristino selezionando Source Site (Sito di origine), Associated vCenter (vCenter associato), Destination Site (Sito di destinazione) e Associated vCenter (vCenter associato).

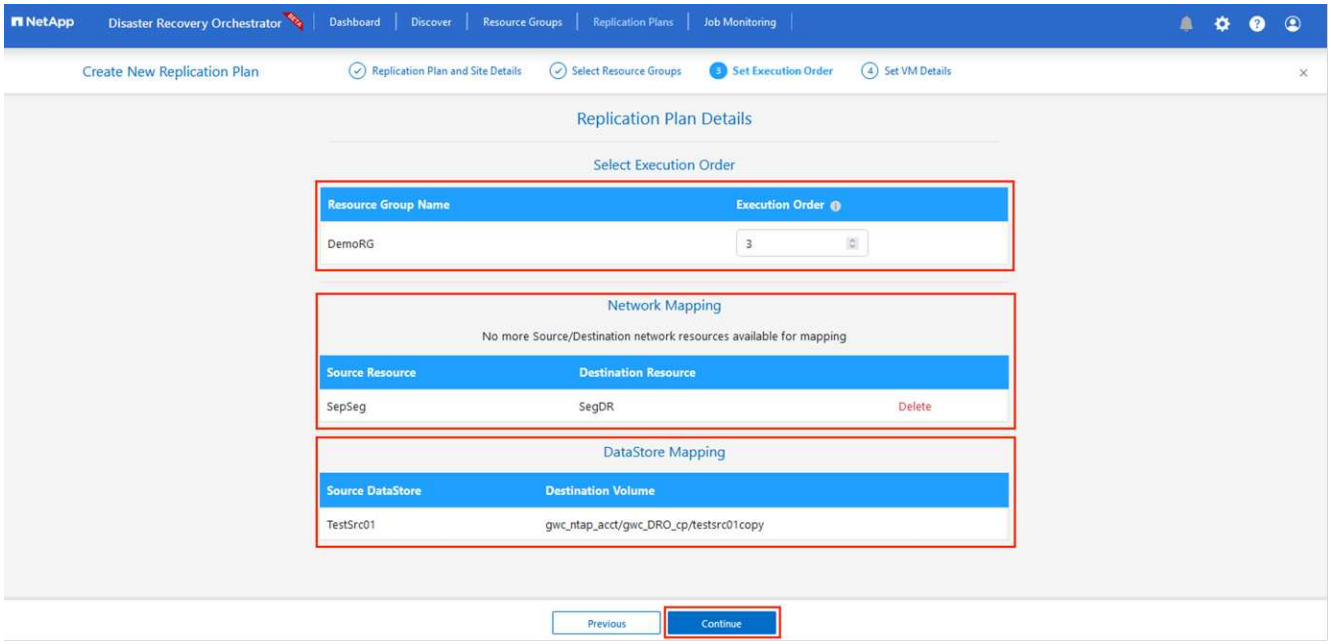


3. Una volta completata la mappatura di ripristino, selezionare **Cluster Mapping** (mappatura cluster).

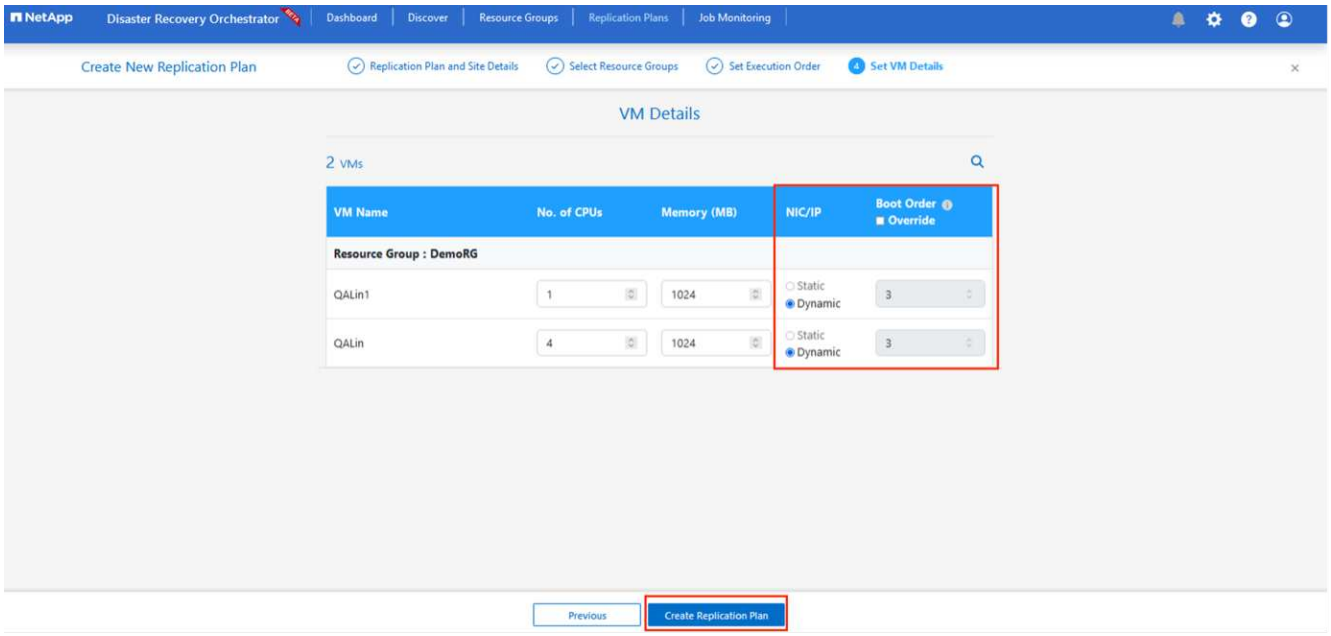


4. Selezionare **Dettagli gruppo di risorse** e fare clic su **continua**.
5. Impostare l'ordine di esecuzione per il gruppo di risorse. Questa opzione consente di selezionare la sequenza di operazioni quando esistono più gruppi di risorse.
6. Al termine, impostare la mappatura di rete sul segmento appropriato. I segmenti devono essere già sottoposti a provisioning sul cluster AVS secondario e, per mappare le macchine virtuali su di essi, selezionare il segmento appropriato.
7. I mapping degli archivi dati vengono selezionati automaticamente in base alla selezione delle macchine virtuali.

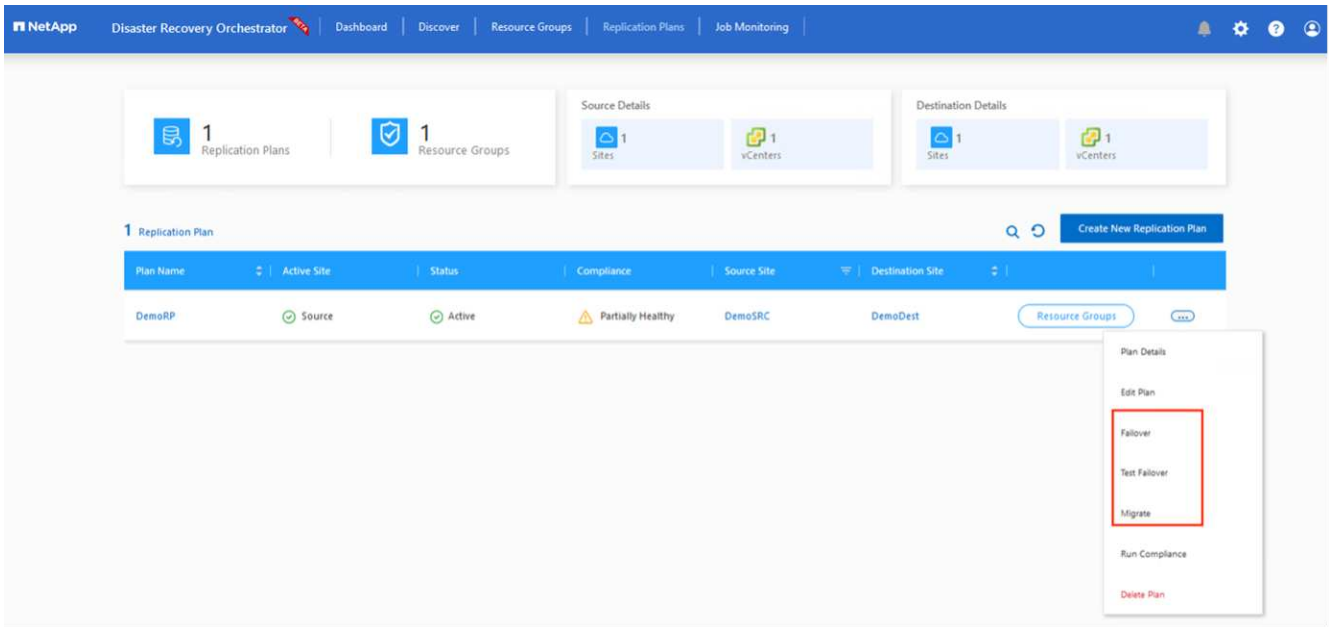
La replica cross-region (CRR) è a livello di volume. Pertanto, tutte le macchine virtuali che risiedono sul rispettivo volume vengono replicate nella destinazione CRR. Assicurarsi di selezionare tutte le macchine virtuali che fanno parte del datastore, in quanto vengono elaborate solo le macchine virtuali che fanno parte del piano di replica.



8. In VM details (Dettagli VM), è possibile ridimensionare i parametri della CPU e della RAM delle macchine virtuali. Questo può essere molto utile quando si ripristinano ambienti di grandi dimensioni in cluster di destinazione più piccoli o quando si eseguono test di DR senza dover eseguire il provisioning di un'infrastruttura fisica VMware uno a uno. Inoltre, modificare l'ordine di avvio e il ritardo di avvio (sec) per tutte le macchine virtuali selezionate nei gruppi di risorse. Esiste un'opzione aggiuntiva per modificare l'ordine di avvio se sono necessarie modifiche da ciò che è stato selezionato durante la selezione dell'ordine di avvio del gruppo di risorse. Per impostazione predefinita, viene utilizzato l'ordine di avvio selezionato durante la selezione del gruppo di risorse, tuttavia in questa fase è possibile eseguire qualsiasi modifica.

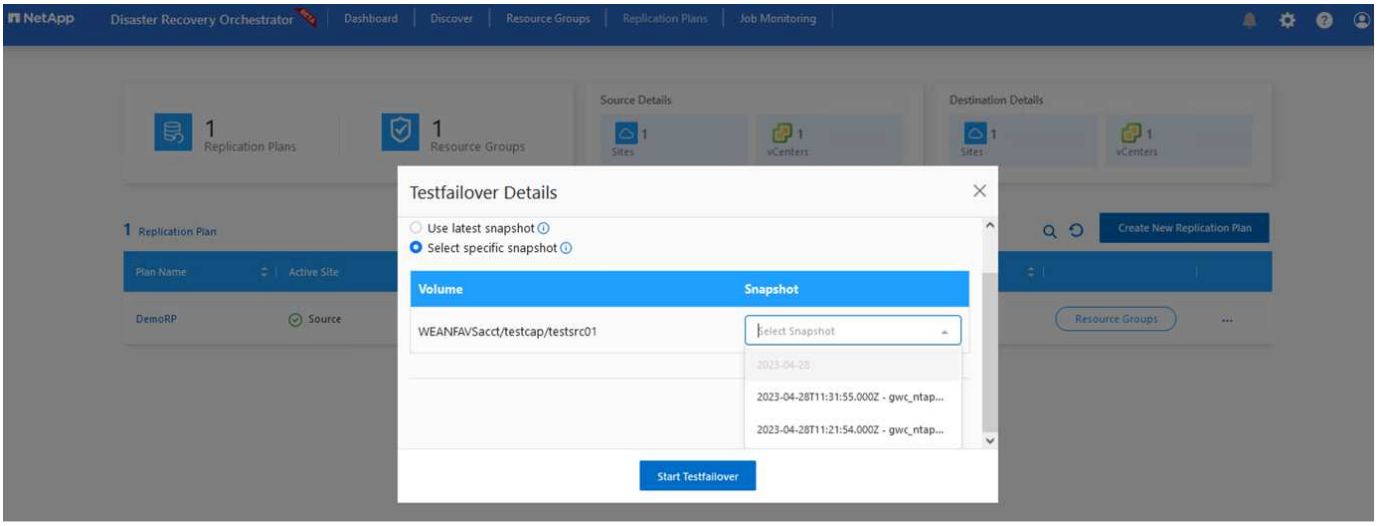


9. Fare clic su **Create Replication Plan** (Crea piano di replica). Una volta creato il piano di replica, è possibile eseguire il failover, il failover di test o le opzioni di migrazione in base ai requisiti.

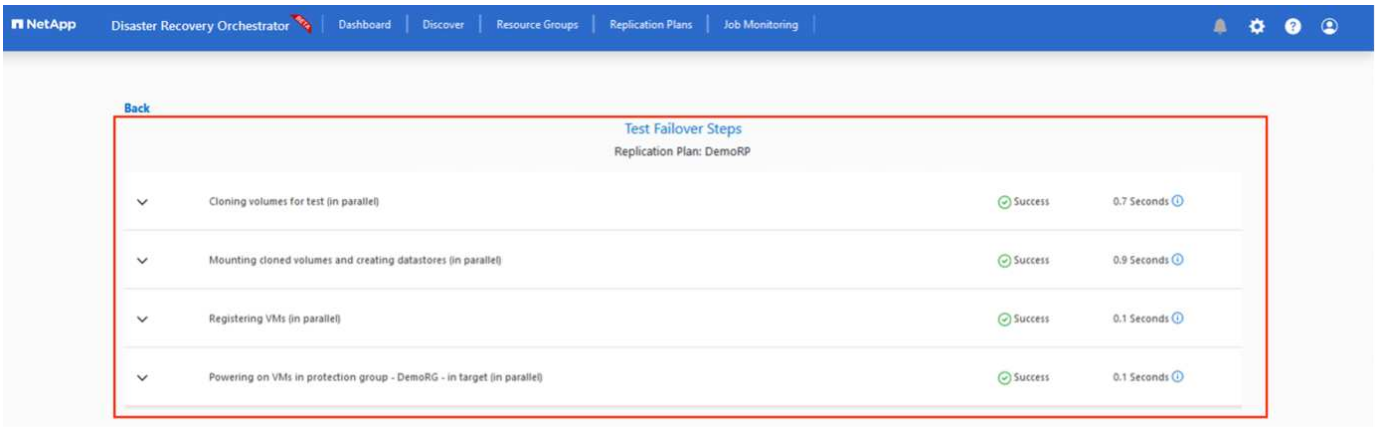


Durante le opzioni di failover e test di failover, viene utilizzato lo snapshot più recente oppure è possibile selezionare uno snapshot specifico da uno snapshot point-in-time. L'opzione point-in-time può essere molto

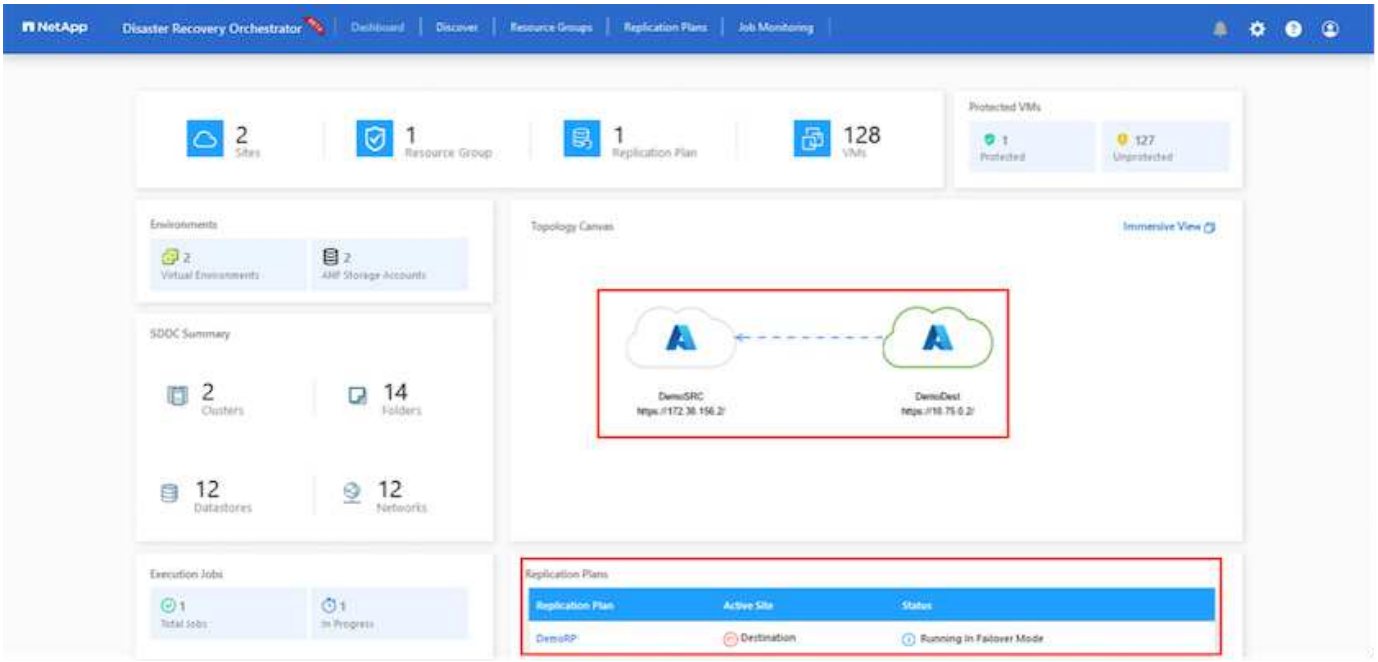
vantaggiosa se si sta affrontando un evento di corruzione come ransomware, in cui le repliche più recenti sono già compromesse o crittografate. DRO mostra tutti i tempi di rilevazione disponibili.



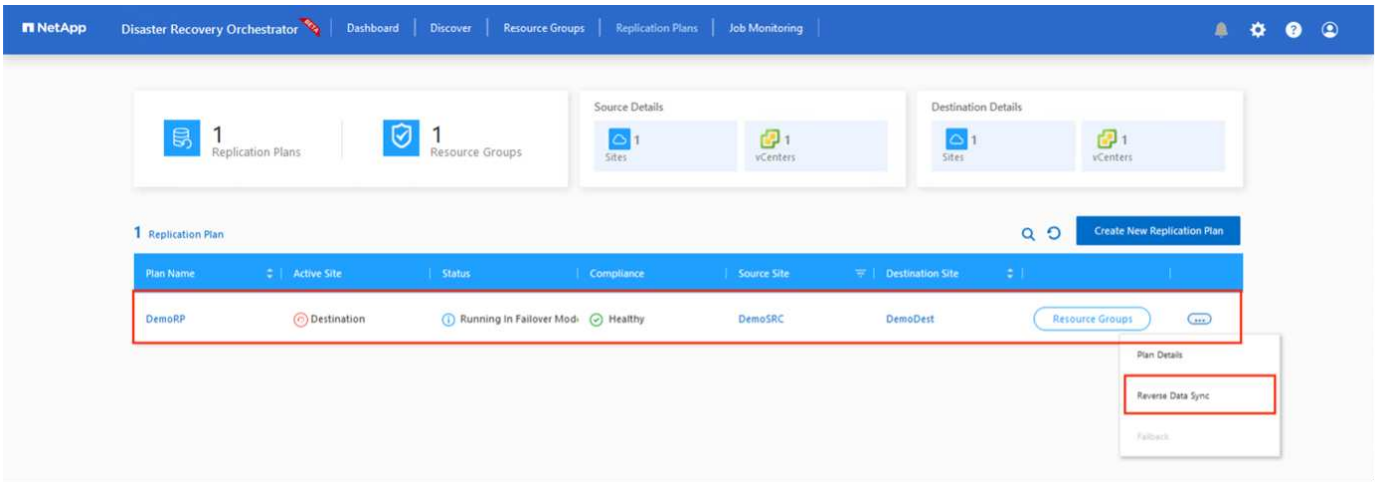
Per attivare il failover o verificare il failover con la configurazione specificata nel piano di replica, fare clic su **failover** o **Test failover**. È possibile monitorare il piano di replica nel menu delle attività.



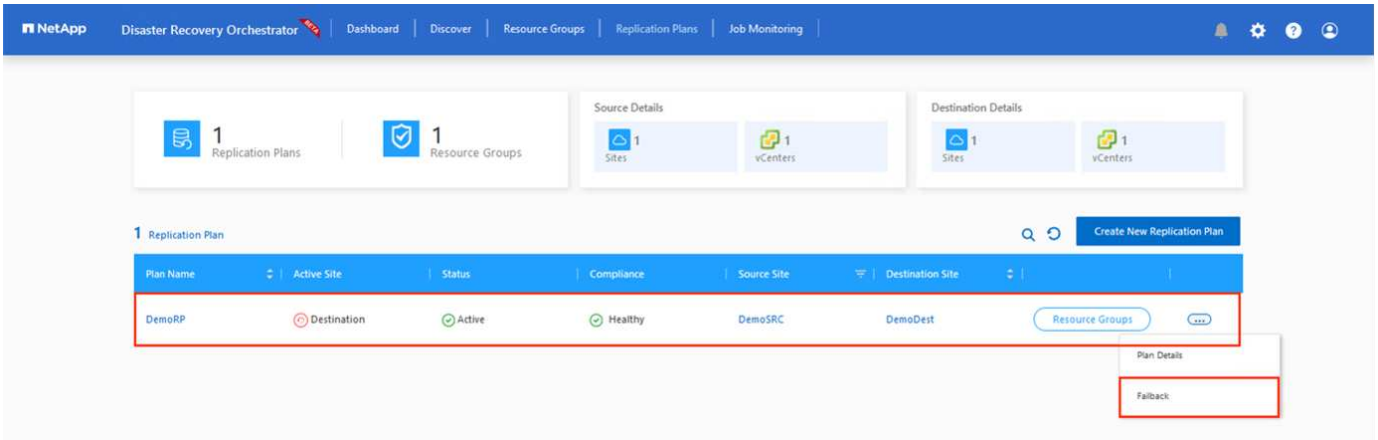
Dopo l'attivazione del failover, gli elementi ripristinati possono essere visualizzati nel sito secondario AVS SDDC vCenter (VM, reti e datastore). Per impostazione predefinita, le macchine virtuali vengono ripristinate nella cartella workload.

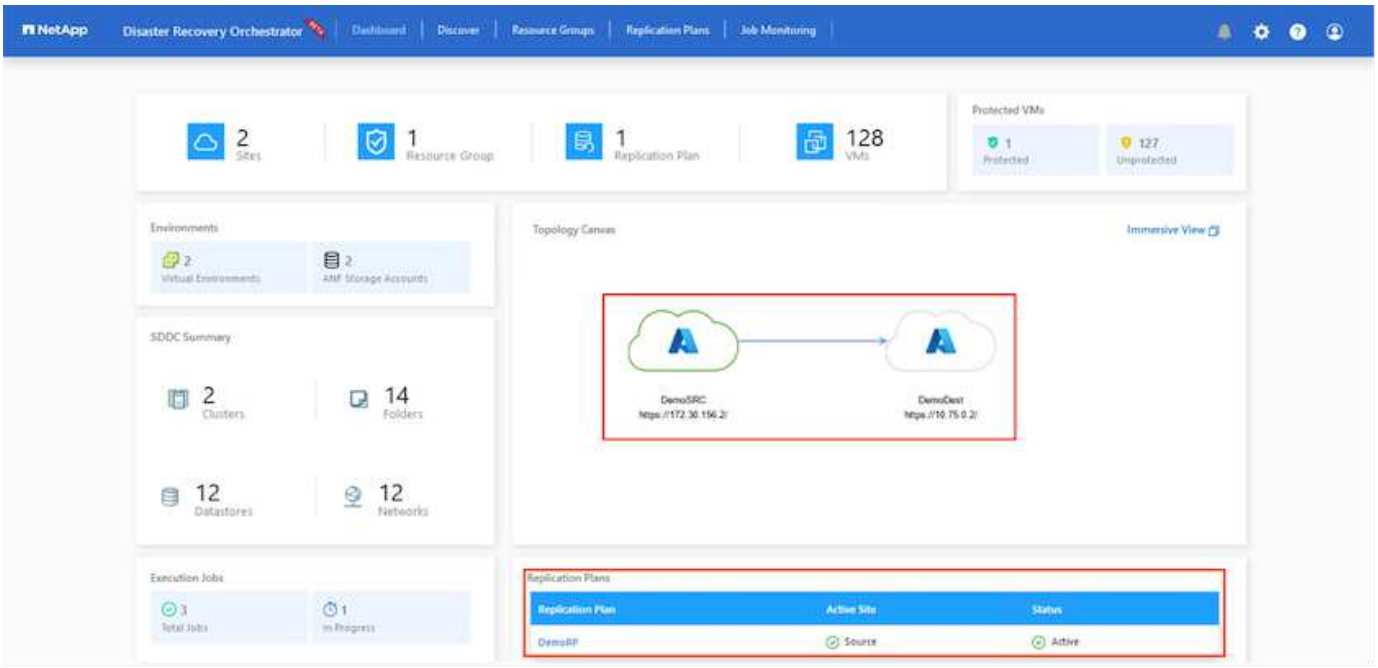


Il failback può essere attivato a livello di piano di replica. In caso di failover di test, l'opzione di strappo può essere utilizzata per eseguire il rollback delle modifiche e rimuovere il volume appena creato. I fallback relativi al failover sono un processo in due fasi. Selezionare il piano di replica e selezionare **Reverse Data Sync**.



Al termine di questa fase, attivare il failback per tornare al sito AVS primario.





Dal portale Azure, possiamo vedere che lo stato di salute della replica è stato interrotto per i volumi appropriati che sono stati mappati al sito secondario AVS SDDC come volumi di lettura/scrittura. Durante il failover di test, DRO non esegue il mapping del volume di destinazione o di replica. Al contrario, crea un nuovo volume dello snapshot di replica cross-region richiesto ed espone il volume come datastore, che consuma ulteriore capacità fisica dal pool di capacità e garantisce che il volume di origine non venga modificato. In particolare, i processi di replica possono continuare durante i test di DR o i flussi di lavoro di triage. Inoltre, questo processo garantisce che il ripristino possa essere ripulito senza il rischio che la replica venga distrutta in caso di errori o di ripristino di dati corrotti.

Recovery ransomware

Il ripristino dal ransomware può essere un compito scoraggiante. In particolare, può essere difficile per le organizzazioni IT individuare il punto di ritorno sicuro e, una volta stabilito, come garantire che i carichi di lavoro recuperati siano protetti dagli attacchi che si verificano (ad esempio, da malware in sospensione o attraverso applicazioni vulnerabili).

DRO risolve questi problemi consentendo alle organizzazioni di eseguire il ripristino da qualsiasi point-in-time disponibile. I carichi di lavoro vengono quindi ripristinati in reti funzionali ma isolate, in modo che le applicazioni possano funzionare e comunicare tra loro, ma non siano esposte al traffico nord-sud. Questo processo offre ai team di sicurezza un luogo sicuro per condurre indagini legali e identificare eventuali malware nascosti o inattivi.

Conclusione

La soluzione di disaster recovery Azure NetApp Files e Azure offre i seguenti vantaggi:

- Sfrutta una replica Azure NetApp Files cross-region efficiente e resiliente.
- Ripristino a qualsiasi point-in-time disponibile con la conservazione degli snapshot.
- Automatizzare completamente tutte le fasi necessarie per ripristinare da centinaia a migliaia di macchine virtuali dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- Il recupero del workload sfrutta il processo "Create new volumes from the most recent snapshot" (Crea nuovi volumi dalle snapshot più recenti), che non manipola il volume replicato.

- Evitare qualsiasi rischio di corruzione dei dati sui volumi o sugli snapshot.
- Evita le interruzioni della replica durante i flussi di lavoro dei test di DR.
- Sfrutta i dati di DR e le risorse di calcolo del cloud per i flussi di lavoro che vanno oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- L'ottimizzazione della CPU e della RAM può contribuire a ridurre i costi del cloud consentendo il ripristino a cluster di calcolo più piccoli.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Creare la replica di un volume per Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replica cross-region di volumi Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Soluzione VMware Azure"

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

- Implementare e configurare l'ambiente di virtualizzazione su Azure

  "Configura AVS su Azure"

- Implementare e configurare Azure VMware Solution

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Utilizzo di Veeam Replication e datastore Azure NetApp Files per il disaster recovery nella soluzione Azure VMware

Autore: Niyaz Mohamed - Ingegneria di soluzioni di NetApp

Panoramica

I datastore Azure NetApp Files (ANF) separano lo storage dal calcolo e liberano la flessibilità necessaria a qualsiasi organizzazione per portare i propri workload nel cloud. Offre ai clienti un'infrastruttura storage flessibile e dalle performance elevate, che scala in modo indipendente dalle risorse di calcolo. Le dimensioni del datastore di Azure NetApp Files semplificano e ottimizzano l'implementazione insieme alla soluzione Azure VMware (AVS) come sito di disaster recovery per gli ambienti VMware on-premise.

I datastore NFS basati su volume Azure NetApp Files (ANF) possono essere utilizzati per replicare i dati on-premise utilizzando qualsiasi soluzione di terze parti validata che offre funzionalità di replica delle VM. Aggiungendo datastore Azure NetApp Files, potrai ottimizzare i costi dell'implementazione rispetto a una soluzione SDDC Azure VMware con un'enorme quantità di host ESXi per ospitare lo storage. Questo approccio è chiamato "quadro spie pilota". Un cluster di spie pilota è una configurazione host AVS minima (3 nodi AVS) insieme alla capacità del datastore Azure NetApp Files.

L'obiettivo è mantenere un'infrastruttura a basso costo con tutti i componenti principali per gestire il failover. Un

cluster di spie pilota può scalare in orizzontale e fornire più host AVS se si verifica un failover. Inoltre, una volta completato il failover e ripristinate le normali operazioni, il cluster di spie può scalare di nuovo alla modalità operativa a basso costo.

Finalità del presente documento

Questo articolo descrive come utilizzare il datastore Azure NetApp Files con Veeam Backup e la replica per configurare il disaster recovery per le VM VMware on-premise su (AVS) utilizzando la funzionalità software di replica Veeam VM.

Veeam Backup & Replication è un'applicazione di backup e replica per ambienti virtuali. Quando le macchine virtuali vengono replicate, Veeam Backup & Replication viene replicato da AVS, il software crea una copia esatta delle VM nel formato VMware vSphere nativo sul cluster SDDC AVS di destinazione. Veeam Backup & Replication manterrà la copia sincronizzata con la VM originale. La replica offre il miglior recovery time objective (RTO) essendo presente una copia montata di una macchina virtuale nel sito di DR in uno stato ready-to-start.

Questo meccanismo di replica garantisce che i carichi di lavoro possano avviarsi rapidamente in un AVS SDDC in caso di evento di emergenza. Il software Veeam Backup & Replication ottimizza anche la trasmissione del traffico per la replica su WAN e le connessioni lente. Inoltre, filtra anche blocchi di dati duplicati, zero blocchi di dati, file swap e "file OS guest di macchine virtuali esclusi". Il software comprime anche il traffico di replica. Per evitare che i processi di replica consumino l'intera larghezza di banda della rete, è possibile utilizzare acceleratori WAN e regole di limitazione della rete.

Il processo di replica in Veeam Backup & Replication è basato sul processo, il che significa che la replica viene eseguita configurando i processi di replica. In caso di evento di emergenza, è possibile attivare il failover per ripristinare le macchine virtuali con failover sulla copia di replica. Una volta eseguito il failover, una VM replicata assume il ruolo della VM originale. Il failover può essere eseguito allo stato più recente di una replica o a uno dei suoi punti di ripristino noti. Ciò abilita recovery dal ransomware o test isolati, se necessario. Veeam Backup & Replication offre diverse opzioni per gestire diversi scenari di disaster recovery.

[]

Implementazione della soluzione

Gradini di alto livello

1. Il software Veeam Backup and Replication è in esecuzione in un ambiente on-premise con appropriata connettività di rete.
2. "Implementa la soluzione Azure VMware (AVS)" cloud privato e. "Collegare i datastore Azure NetApp Files" Agli host della soluzione Azure VMware.

   Un ambiente pilota configurato con una configurazione minima può essere utilizzato per scopi di DR. In caso di incidente, è possibile eseguire il failover delle macchine virtuali su questo cluster e aggiungere nodi.

3. Impostare il processo di replica per creare repliche VM utilizzando Veeam Backup and Replication.
4. Creazione di un piano di failover ed esecuzione di un failover.
5. Tornare alle macchine virtuali di produzione una volta che l'evento di disastro è completo e il sito primario è attivo.

Prerequisiti per la replica della macchina virtuale Veeam nei datastore AVS e ANF

1. Assicurarsi che la VM di backup di Veeam Backup & Replication sia connessa all'origine e ai cluster SDDC AVS di destinazione.
2. Il server di backup deve essere in grado di risolvere i nomi brevi e di connettersi ai centri virtuali di origine e di destinazione.
3. Il datastore Azure NetApp Files di destinazione deve avere spazio libero sufficiente per archiviare VMDK di macchine virtuali replicate.

Per ulteriori informazioni, fare riferimento a "considerazioni e limitazioni" "qui".

Dettagli sull'implementazione

Fase 1: Replica delle VM

Veeam Backup & Replication sfrutta le funzionalità snapshot di VMware vSphere/durante la replica, Veeam Backup & Replication richiede a VMware vSphere la creazione di una snapshot delle VM. Lo snapshot della VM è la copia point-in-time di una VM che include dischi virtuali, stato del sistema, configurazione e metadati. Veeam Backup & Replication utilizza la snapshot come origine dei dati per la replica.

Per replicare le VM, attenersi alla seguente procedura:

1. Apri la Veeam Backup & Replication Console.
2. Nella vista Home. Fare clic con il pulsante destro del mouse sul nodo processi e selezionare processo di replica > macchina virtuale.
3. Specificare un nome di lavoro e selezionare la casella di controllo controllo avanzata appropriata. Fare clic su Avanti.
   - Selezionare la casella di controllo Replica seeding se la connettività tra on-premise e Azure ha limitato la larghezza di banda.
     *Selezionare la casella di controllo Network remapping (per i siti AVS SDDC con reti diverse) se i segmenti della soluzione Azure VMware SDDC non corrispondono a quelli delle reti dei siti in sede.
   - Se lo schema di indirizzamento IP nel sito di produzione locale differisce dallo schema nel sito AVS di destinazione, selezionare la casella di controllo Replica re-IP (per siti DR con schema di indirizzamento IP diverso).

     []
4. Selezionare le VM da replicare nel datastore Azure NetApp Files collegato a un SDDC della soluzione Azure VMware nel passaggio **macchine virtuali***. Le macchine virtuali possono essere posizionate su vSAN per riempire la capacità del datastore vSAN disponibile. In un cluster spia pilota, la capacità utilizzabile di un cluster a 3 nodi sarà limitata. Il resto dei dati può essere posizionato facilmente nei datastore Azure NetApp Files, in modo che sia possibile ripristinare le macchine virtuali e espandere il cluster per soddisfare i requisiti di CPU/mem. Fare clic su **Aggiungi**, quindi nella finestra **Aggiungi oggetto** selezionare le VM o i contenitori VM necessari e fare clic su **Aggiungi**. Fare clic su **Avanti**.

   []
5. Quindi, seleziona la destinazione come cluster/host SDDC della soluzione Azure VMware e il pool di risorse, la cartella VM e il datastore FSX per le repliche delle VM di ONTAP. Quindi fare clic su **Avanti**.

   []
6. Nel passaggio successivo, creare la mappatura tra la rete virtuale di origine e di destinazione secondo necessità.

   []
7. Nel passaggio **Impostazioni processo**, specificare il repository di backup che memorizzerà i metadati per le repliche della VM, i criteri di conservazione e così via.
8. Aggiornare i server proxy **Source** e **Target** nel passo **trasferimento dati** e lasciare selezionata l'opzione **Automatic** (impostazione predefinita) e mantenere l'opzione **Direct** (diretto) e fare clic su **Next** (Avanti).

9. Nel passaggio **elaborazione guest**, selezionare **attiva elaborazione in base alle esigenze dell'applicazione**. Fare clic su **Avanti**.

   []

10. Scegliere la pianificazione di replica per eseguire regolarmente il processo di replica.

    []

11. Nel passo **Riepilogo** della procedura guidata, esaminare i dettagli del processo di replica. Per avviare il lavoro subito dopo la chiusura della procedura guidata, selezionare la casella di controllo **Esegui il lavoro quando si fa clic su fine**, altrimenti lasciare deselezionata la casella di controllo. Quindi fare clic su **fine** per chiudere la procedura guidata.

    []

Una volta avviato il processo di replica, le macchine virtuali con il suffisso specificato verranno popolate nel cluster/host AVS SDDC di destinazione.

[]

Per ulteriori informazioni sulla replica Veeam, fare riferimento "Come funziona la replica"

Passaggio 2: Creare un piano di failover

Una volta completata la replica o il seeding iniziale, creare il piano di failover. Il piano di failover consente di eseguire automaticamente il failover per le VM dipendenti una alla volta o come gruppo. Il piano di failover è il modello per l'ordine in cui le macchine virtuali vengono elaborate, inclusi i ritardi di avvio. Il piano di failover aiuta inoltre a garantire che le VM dipendenti da fattori critici siano già in esecuzione.

Per creare il piano, passare alla nuova sottosezione chiamata **repliche** e selezionare **piano di failover**. Scegliere le VM appropriate. Veeam Backup & Replication cercherà i punti di ripristino più vicini a questo punto nel tempo e li utilizzerà per avviare le repliche della VM.

Il piano di failover può essere aggiunto solo una volta completata la replica iniziale e le repliche della VM sono nello stato Pronta.

Il numero massimo di VM che possono essere avviate contemporaneamente quando si esegue un piano di failover è 10

Durante il processo di failover, le macchine virtuali di origine non verranno spente

Per creare il **piano di failover**, procedere come segue:

1. Nella vista Home. Fare clic con il pulsante destro del mouse sul nodo repliche e selezionare piani di failover > piano di failover > VMware vSphere.

   []

2. Fornire quindi un nome e una descrizione del piano. Gli script pre e post-failover possono essere aggiunti secondo necessità. Ad esempio, eseguire uno script per arrestare le macchine virtuali prima di avviare le macchine virtuali replicate.

   []

3. Aggiungere le VM al piano e modificare l'ordine di avvio delle VM e i ritardi di avvio per soddisfare le dipendenze delle applicazioni.

   []

Per ulteriori informazioni sulla creazione di processi di replica, fare riferimento a. "Creazione di processi di replica".

Passaggio 3: Eseguire il piano di failover

Durante il failover, la macchina virtuale di origine nel sito di produzione viene commutata alla replica nel sito di disaster recovery. Come parte del processo di failover, Veeam Backup & Replication ripristina la replica della VM al punto di ripristino richiesto e sposta tutte le attività di i/o dalla VM di origine alla replica. Le repliche possono essere utilizzate non solo in caso di disastro, ma anche per simulare esercitazioni sul DR. Durante la simulazione del failover, la VM di origine rimane in esecuzione. Una volta eseguiti tutti i test necessari, è possibile annullare il failover e tornare alla normale operatività.

Assicurarsi che la segmentazione della rete sia attiva per evitare conflitti IP durante il failover.

Per avviare il piano di failover, è sufficiente fare clic sulla scheda **piani di failover** e fare clic con il pulsante destro del mouse sul piano di failover. Selezionare ***Avvia**. Il failover viene eseguito utilizzando gli ultimi punti di ripristino delle repliche della VM. Per eseguire il failover su punti di ripristino specifici delle repliche della VM, selezionare **Avvia a**.

[]

[]

Lo stato della replica della macchina virtuale cambia da Pronto a failover e le macchine virtuali vengono avviate sul cluster/host SDDC di Azure VMware Solution (AVS) di destinazione.

[]

Una volta completato il failover, lo stato delle macchine virtuali passa a "failover".

[]

Veeam Backup & Replication interrompe tutte le attività di replica per la VM di origine fino a quando la replica non viene riportata allo stato Ready.

Per informazioni dettagliate sui piani di failover, consultare "Piani di failover".

Fase 4: Failback nel sito di produzione

Quando il piano di failover è in esecuzione, viene considerato come una fase intermedia e deve essere finalizzato in base al requisito. Le opzioni includono:

- **Failback to Production** - consente di tornare alla VM originale e di trasferire tutte le modifiche apportate durante l'esecuzione della replica della VM alla VM originale.

> Quando si esegue il failback, le modifiche vengono solo trasferite ma non pubblicate. Scegliere **commit failback** (una volta che la VM originale è confermata per funzionare come previsto) o Annulla failback per tornare alla replica della VM se la VM originale non funziona come previsto.

- **Annulla failover** - consente di tornare alla VM originale e di ignorare tutte le modifiche apportate alla replica della VM durante l'esecuzione.
- **Failover permanente** - consente di passare in modo permanente dalla VM originale a una replica della VM e di utilizzare questa replica come VM originale.

In questa demo, è stato scelto il failback in produzione. Il failback alla macchina virtuale originale è stato selezionato durante la fase di destinazione della procedura guidata ed è stata attivata la casella di controllo "accensione della macchina virtuale dopo il ripristino".

[]

[]

[]

[]

Il commit di failback è uno dei modi per finalizzare l'operazione di failback. Quando il failback viene eseguito, conferma che le modifiche inviate alla VM che ha avuto esito negativo (la VM di produzione) funzionano come previsto. Dopo l'operazione di commit, Veeam Backup & Replication riprende le attività di replica per la VM di produzione.

Per informazioni dettagliate sul processo di failback, fare riferimento alla documentazione Veeam per "Failover e failback per la replica".

[]

Una volta eseguito il failback in produzione, le macchine virtuali vengono tutte ripristinate nel sito di produzione originale.

[]

Conclusione

La funzionalità datastore di Azure NetApp Files consente a Veeam o a qualsiasi tool validato di terze parti di fornire una soluzione di DR a basso costo sfruttando i cluster leggeri pilota, anziché standar in un cluster grande solo per le repliche delle VM. Ciò fornisce un modo efficace per gestire un piano di disaster recovery personalizzato e su misura e riutilizzare i prodotti di backup esistenti in sede per il disaster recovery, consentendo il disaster recovery basato sul cloud in uscita dai data center di DR on-premise. È possibile eseguire il failover facendo clic su un pulsante in caso di emergenza o eseguendo il failover automatico in caso

di emergenza.

Per ulteriori informazioni su questo processo, segui il video dettagliato.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Migrazione dei carichi di lavoro su Azure/AVS

TR-4940: Migrazione dei carichi di lavoro al datastore Azure NetApp Files con VMware HCX - Guida rapida

Autore: NetApp Solutions Engineering

Panoramica: Migrazione di macchine virtuali con VMware HCX, datastore Azure NetApp Files e soluzione VMware Azure

Uno dei casi di utilizzo più comuni per la soluzione VMware Azure e il datastore Azure NetApp Files 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 Azure NetApp Files.

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 Azure VMware Solution Private Cloud e offre diversi modi per migrare i workload e può essere utilizzato per le operazioni di disaster recovery (DR).

Questo documento fornisce istruzioni dettagliate per il provisioning del datastore Azure NetApp Files, seguito dal download, dall'implementazione e dalla configurazione di VMware HCX, inclusi tutti i componenti principali in sede e il lato soluzione VMware Azure, tra cui interconnessione, estensione di rete 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, che intendono implementare la soluzione Azure NetApp Files con Azure VMware per un'implementazione cloud VMware conveniente.

Passaggi di alto livello

Questo elenco fornisce i passaggi di alto livello necessari per installare e configurare HCX Cloud Manager sul lato cloud di Azure e installare HCX Connector on-premise:

1. Installare HCX attraverso il portale Azure.
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 Azure VMware Solution 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

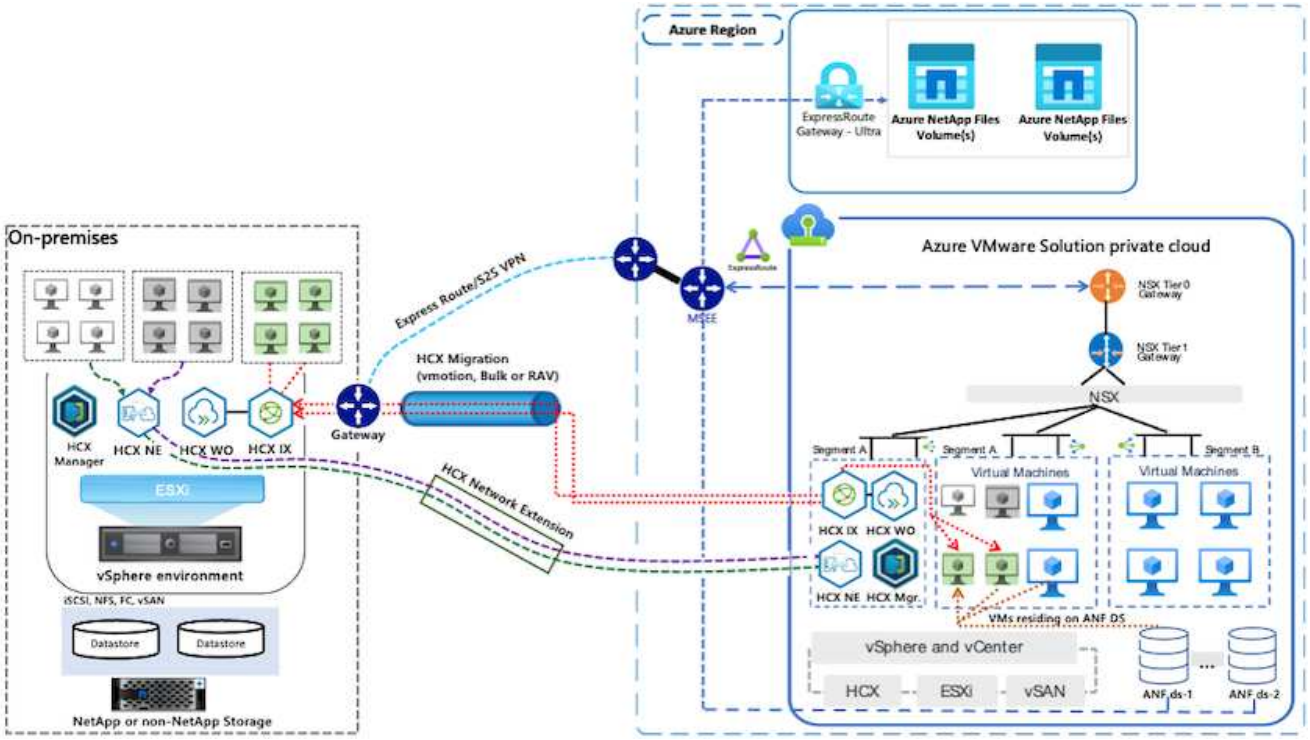
Prima di iniziare, assicurarsi che siano soddisfatti i seguenti prerequisiti. Per ulteriori informazioni, consulta questa sezione "collegamento". Una volta soddisfatti i prerequisiti, inclusa la connettività, configurare e attivare HCX generando la chiave di licenza dal portale Azure VMware Solution. 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.

- Utilizza un data center software-defined (SDDC) esistente per la soluzione Azure VMware o crea un cloud privato utilizzando questo "Link NetApp" o questo "Collegamento Microsoft".
- 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 VPN sito-sito o di accesso globale Express Route" tra l'ambiente on-premise e il rispettivo cloud privato.
- Il percorso di rete dall'ambiente VMware vCenter Server on-premise al cloud privato Azure VMware Solution 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. Nel cloud privato, il routing sulla rete vMotion è configurato per impostazione predefinita.
- Il volume NFS di Azure NetApp Files deve essere montato come datastore nella soluzione VMware di Azure. Seguire i passaggi descritti in questa sezione "collegamento" Per collegare datastore Azure NetApp Files agli host delle soluzioni VMware Azure.

Architettura di alto livello

A scopo di test, l'ambiente di laboratorio on-premise utilizzato per questa convalida è stato collegato tramite una VPN sito-sito, che consente la connettività on-premise con Azure VMware Solution.



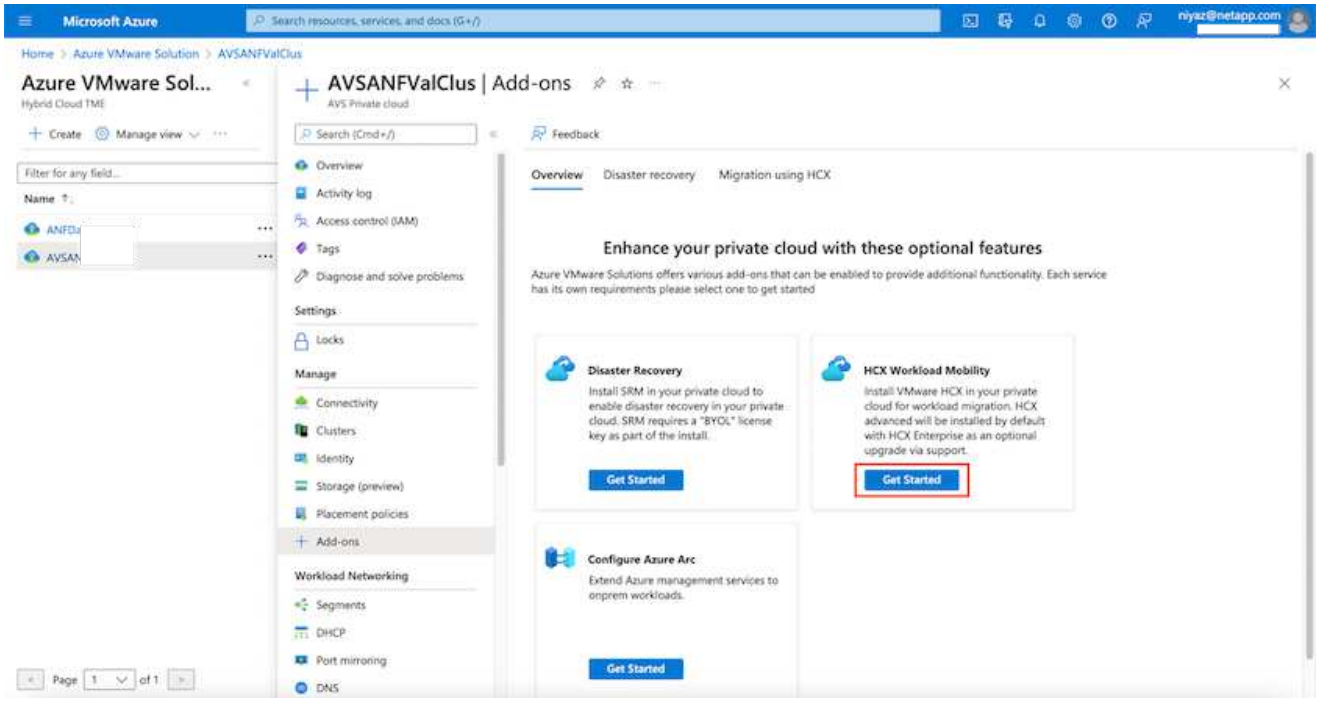
Implementazione della soluzione

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

Fase 1: Installare HCX attraverso Azure Portal utilizzando l'opzione Add-ons

Per eseguire l'installazione, attenersi alla seguente procedura:

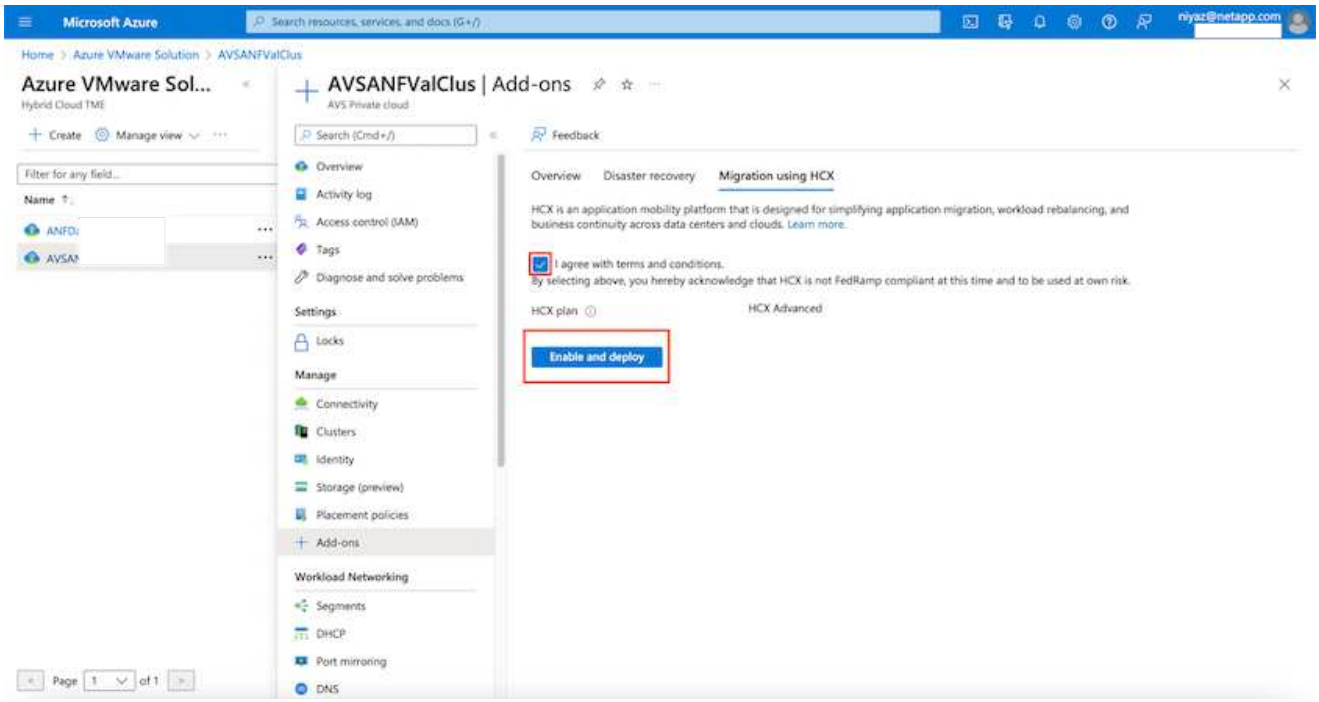
1. Accedi al portale Azure e accedi al cloud privato Azure VMware Solution.
2. Selezionare il cloud privato appropriato e accedere ai componenti aggiuntivi. Per eseguire questa operazione, accedere a **Gestisci > componenti aggiuntivi**.
3. Nella sezione HCX workload Mobility, fare clic su **Get Started** (inizia subito).



1. Selezionare l'opzione **Accetto i termini e le condizioni** e fare clic su **attiva e implementa**.

> L'implementazione predefinita è HCX Advanced. Aprire una richiesta di supporto per attivare l'edizione Enterprise.

> L'implementazione richiede da 25 a 30 minuti circa.


Microsoft Azure
Search resources, services, and docs (G+/)
niyaz@netapp.com
Home > Azure VMware Solution > AVSANFValClus
Azure VMware Sol...
Hybrid Cloud TME
Create
Manage view
Filter for any field...
Name
ANFDi
AVSAN
Page 1 of 1
AVSANFValClus | Add-ons
AVS Private cloud
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Clusters
Identity
Storage (preview)
Placement policies
Add-ons
Workload Networking
Segments
DHCP
Port mirroring
DNS
Feedback
Overview
Disaster recovery
Migration using HCX
HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. Learn more.
I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.
HCX plan
HCX Advanced
Enable and deploy

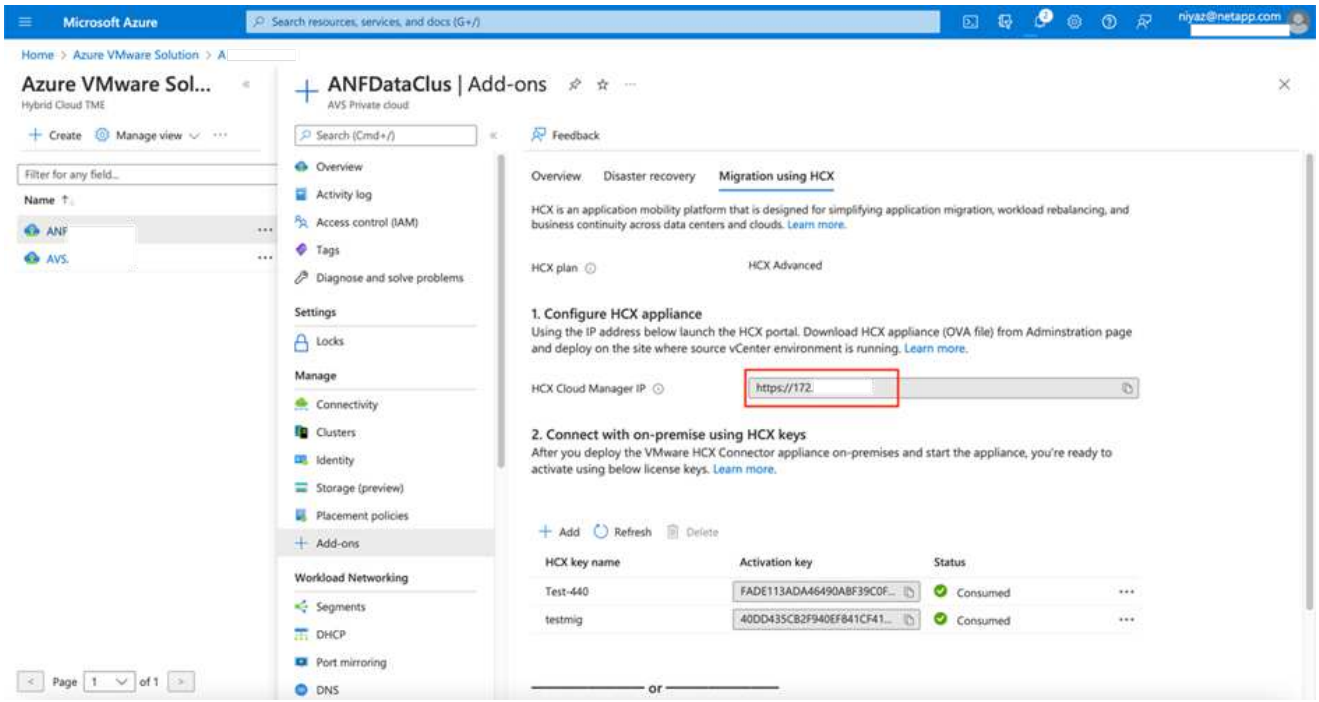
Fase 2: Implementazione dell'OVA del programma di installazione nel server vCenter on-premise

Affinché il connettore on-premise si connetta a HCX Manager in Azure VMware Solution, 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:

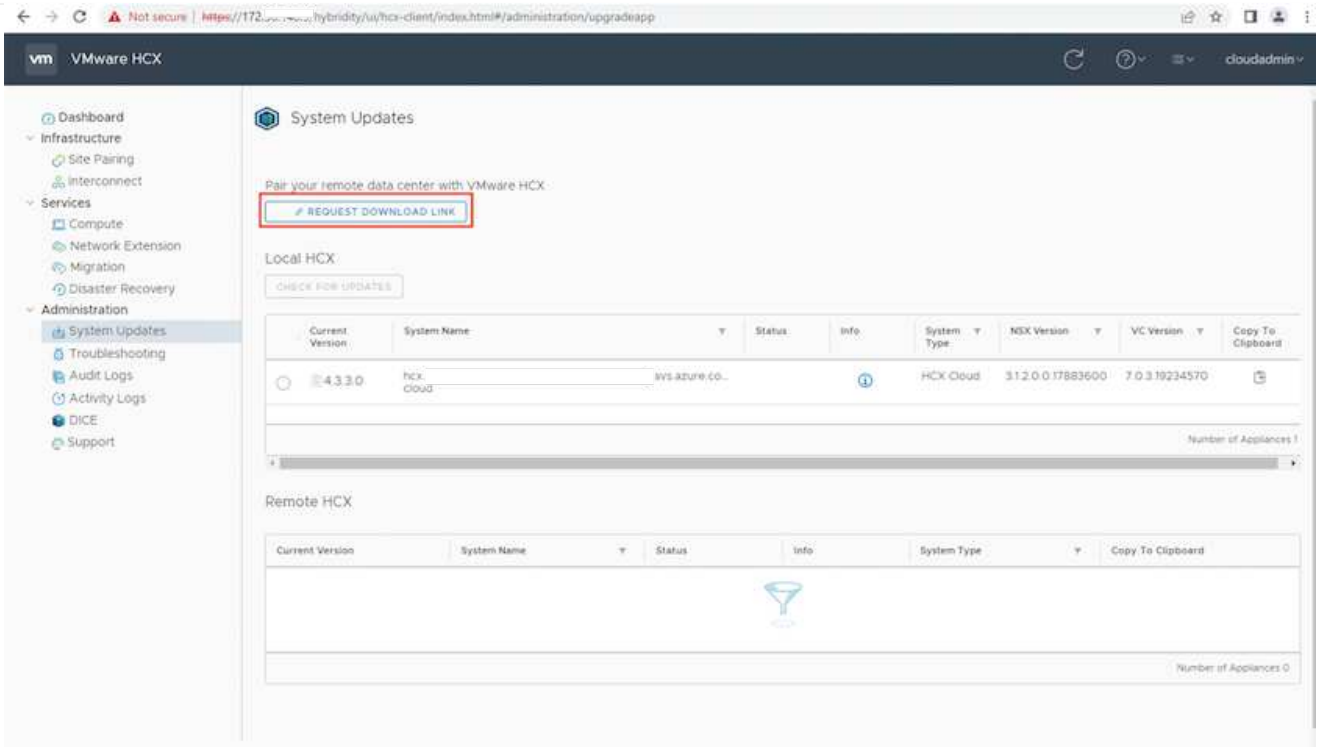
1. Dal portale Azure, accedere alla soluzione VMware Azure, selezionare il cloud privato, quindi selezionare **Gestisci > componenti aggiuntivi > migrazione** utilizzando HCX e copiare IL portale HCX Cloud Manager per scaricare il file OVA.

Utilizzare le credenziali utente predefinite di CloudAdmin per accedere al portale HCX.

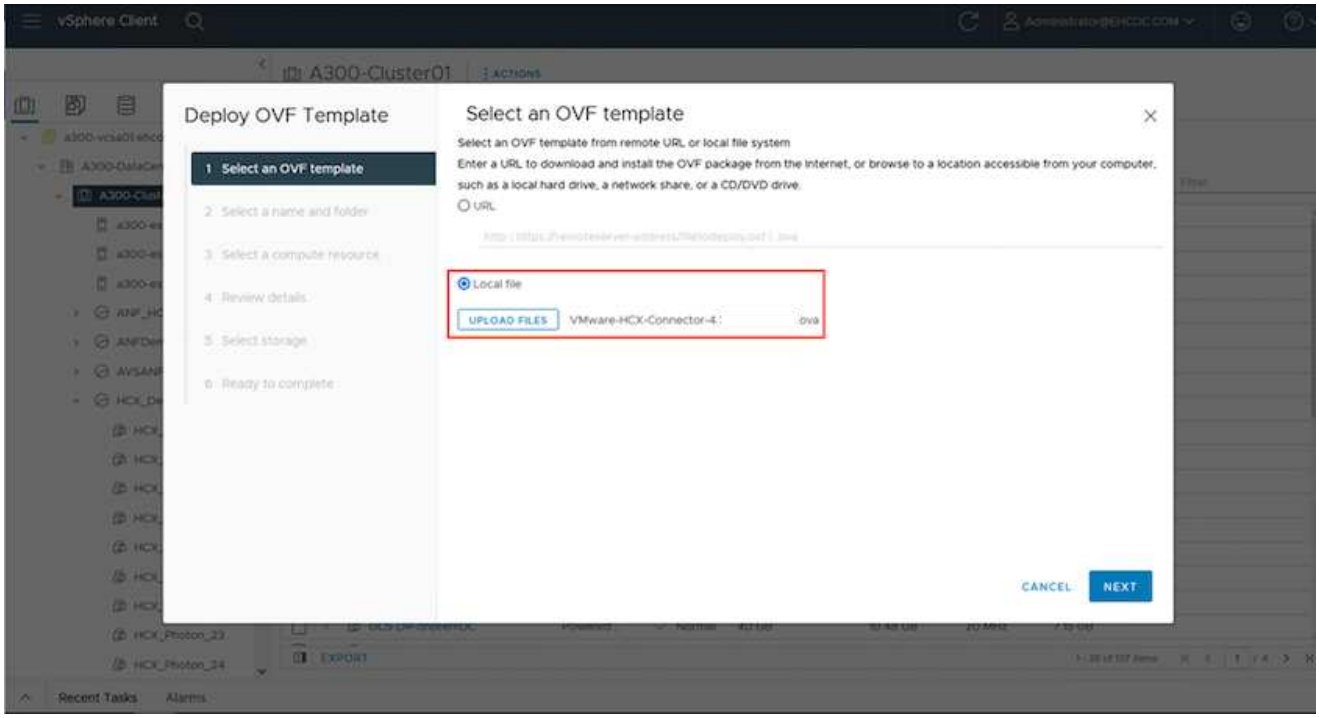


1. Dopo aver effettuato l'accesso al portale HCX con cloudadmin@vsphere.local utilizzando il jumphost, accedere a **Administration > System Updates** e fare clic su **Request Download link**.

Scaricare o copiare il collegamento a OVA e incollarlo in un browser per avviare il processo di download del file OVA di VMware HCX Connector da implementare sul server vCenter on-premise.



1. Una volta scaricato l'OVA, implementarlo nell'ambiente VMware vSphere on-premise utilizzando l'opzione **Deploy OVF Template**.



1. 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.

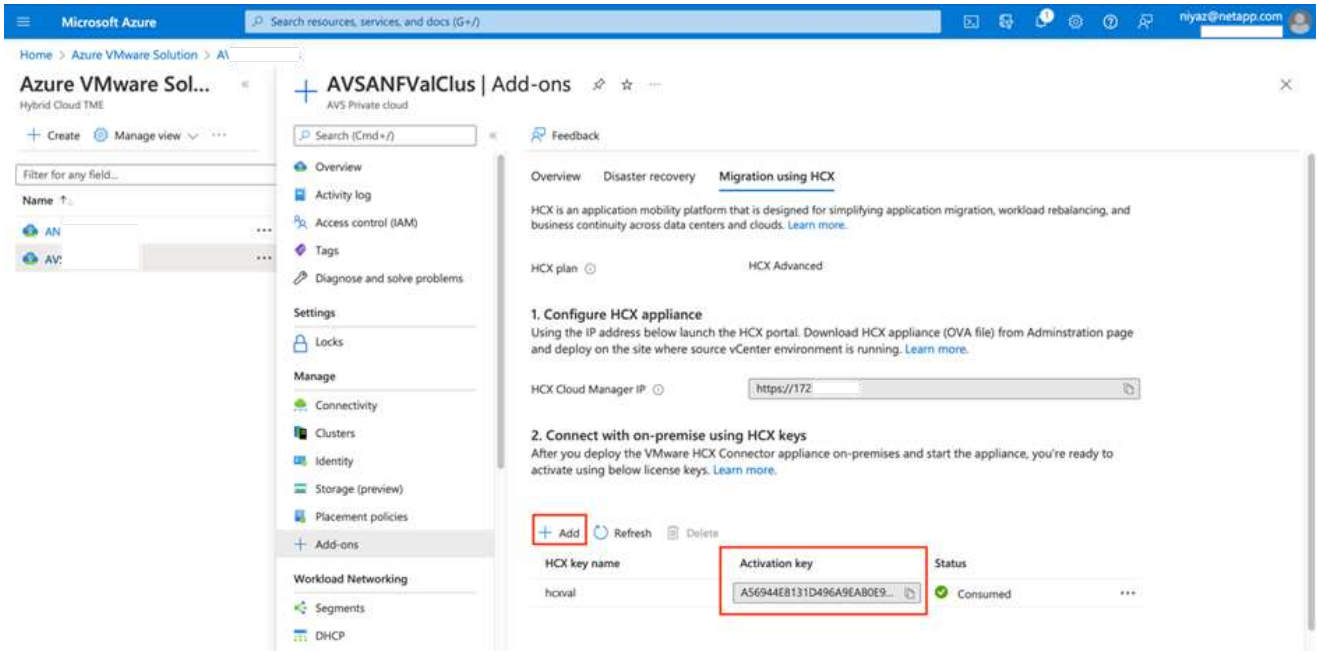
Accendere l'appliance virtuale manualmente.

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 Azure VMware Solution e attivarla in VMware HCX Manager.

1. Dal portale Azure, accedere alla soluzione VMware Azure, selezionare il cloud privato e selezionare **Gestisci > componenti aggiuntivi > migrazione con HCX**.
2. In **Connect with on-premise using HCX keys** (connessione con chiavi HCX on-premise), fare clic su **Add** (Aggiungi) e copiare la chiave di attivazione.



Per ciascun connettore HCX on-premise implementato è necessaria una chiave separata.

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

Utilizzare la password definita durante l'implementazione di OVA.

1. 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.

1. In **posizione del data center**, fornire la posizione più vicina per l'installazione di VMware HCX Manager on-premise. Fare clic su **continua**.
2. In **Nome sistema**, aggiornare il nome e fare clic su **continua**.
3. Fare clic su **Sì, continua**.
4. 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).

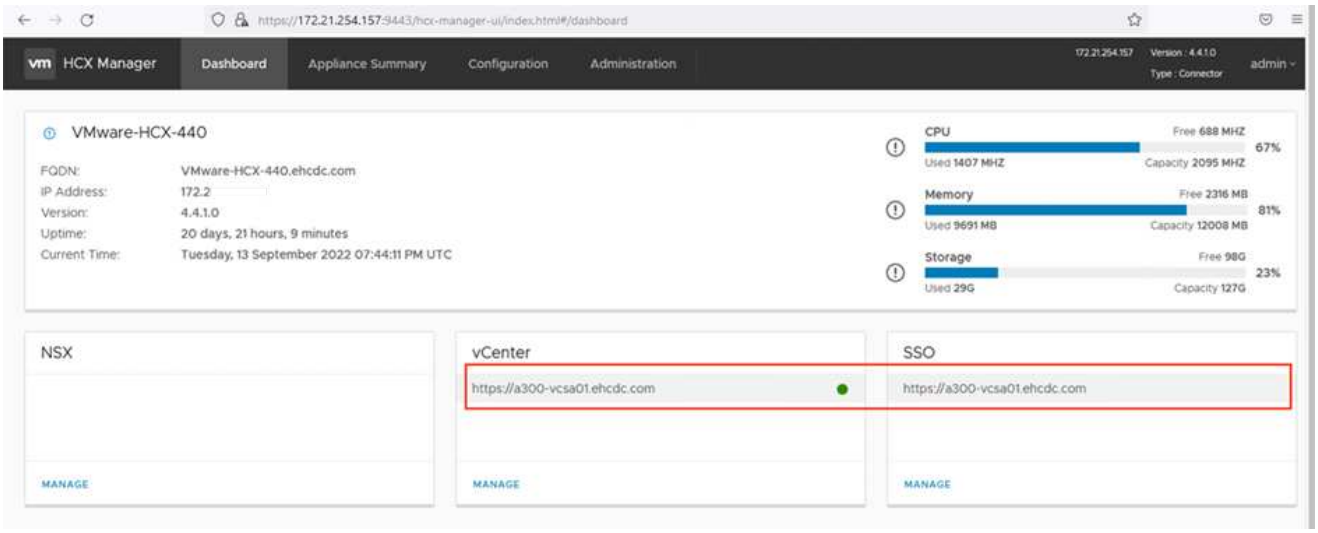
Utilizzare l'FQDN per evitare problemi di connettività in un secondo momento.

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

Immettere l'indirizzo IP o il nome FQDN di VMware vCenter Server.

1. Verificare che le informazioni immesse siano corrette e fare clic su **Restart** (Riavvia).
2. 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.

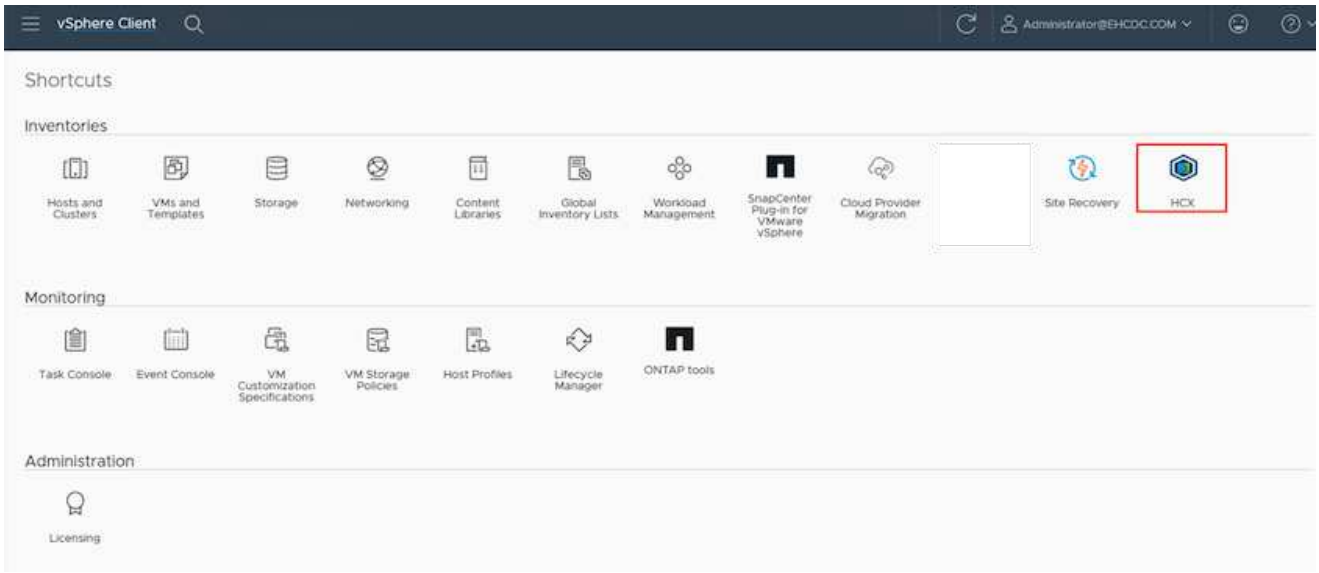
Questo processo richiede circa 10 - 20 minuti e l'aggiunta del plug-in al server vCenter.



Fase 4: Associazione on-premise di VMware HCX Connector con Azure VMware Solution HCX Cloud Manager

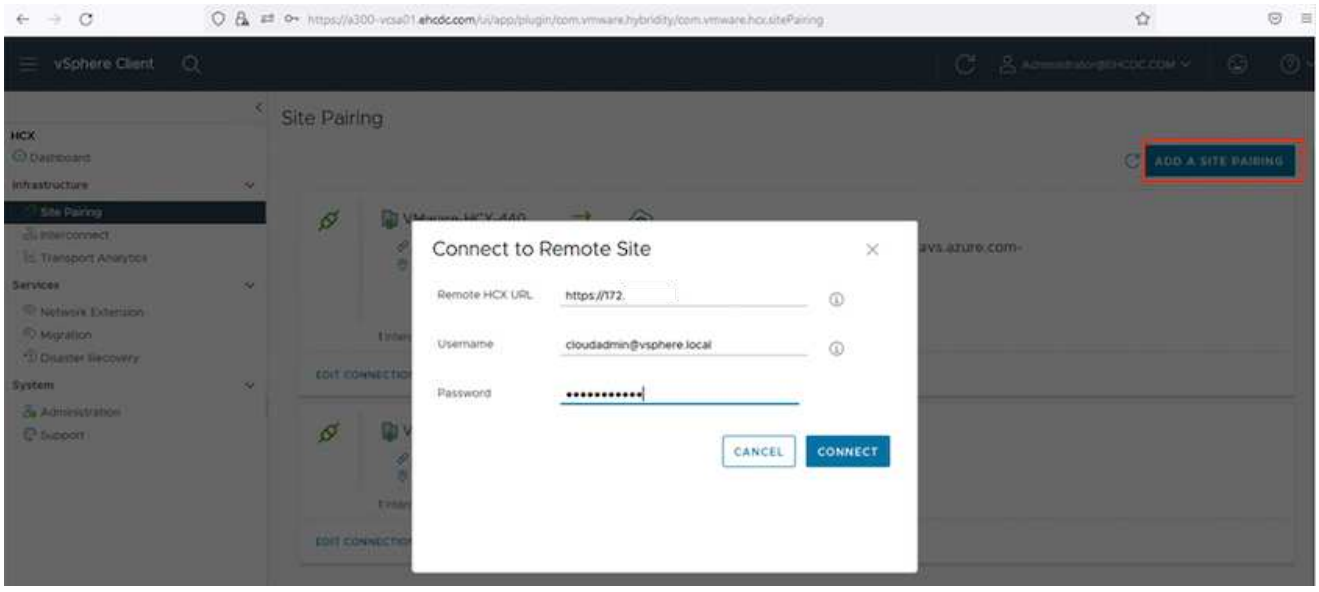
Dopo aver installato HCX Connector sia in sede che in Azure VMware Solution, configurare VMware HCX Connector on-premise per Azure VMware Solution Private Cloud aggiungendo l'accoppiamento. Per configurare l'associazione del sito, attenersi alla seguente procedura:

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



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

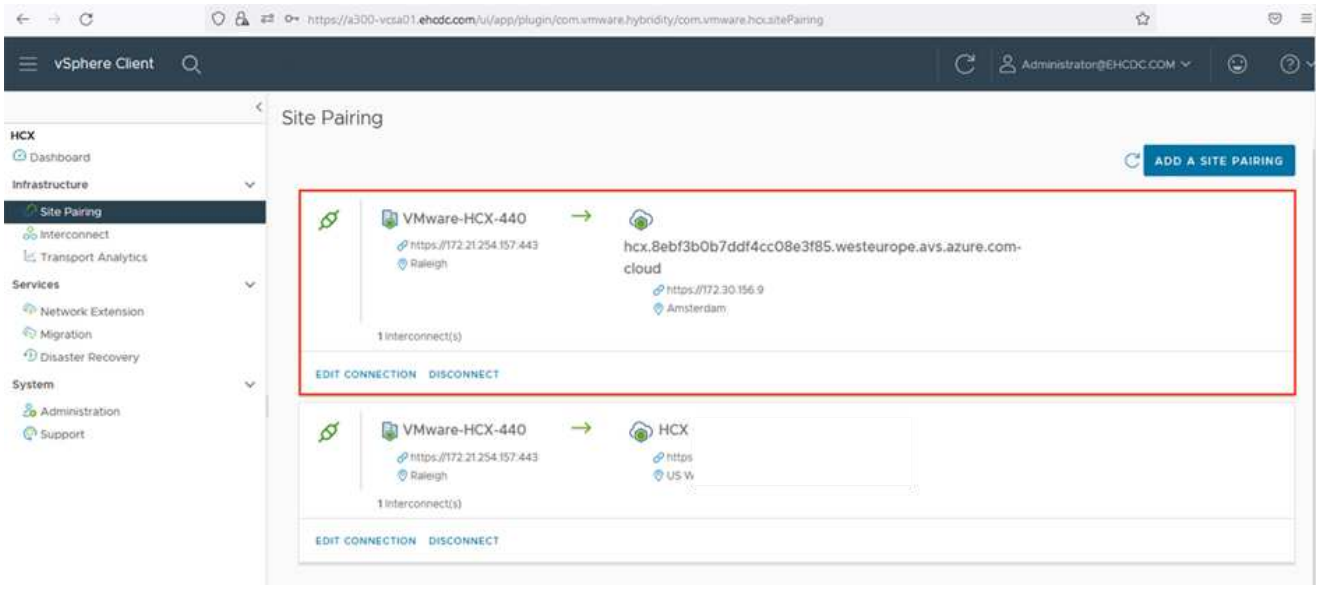
Immettere l'URL o l'indirizzo IP di Azure VMware Solution HCX Cloud Manager e le credenziali per il ruolo CloudAdmin per l'accesso al cloud privato.



1. 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.

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

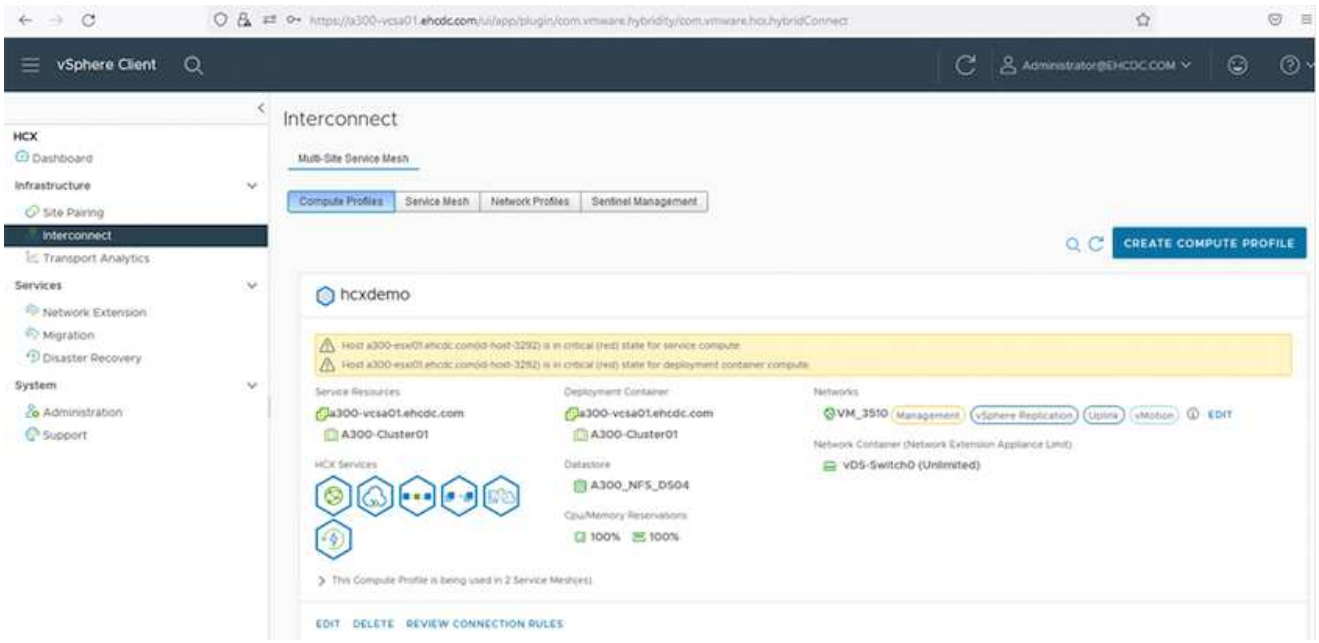


Fase 5: Configurare il profilo di rete, il profilo di calcolo e la mesh del servizio

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

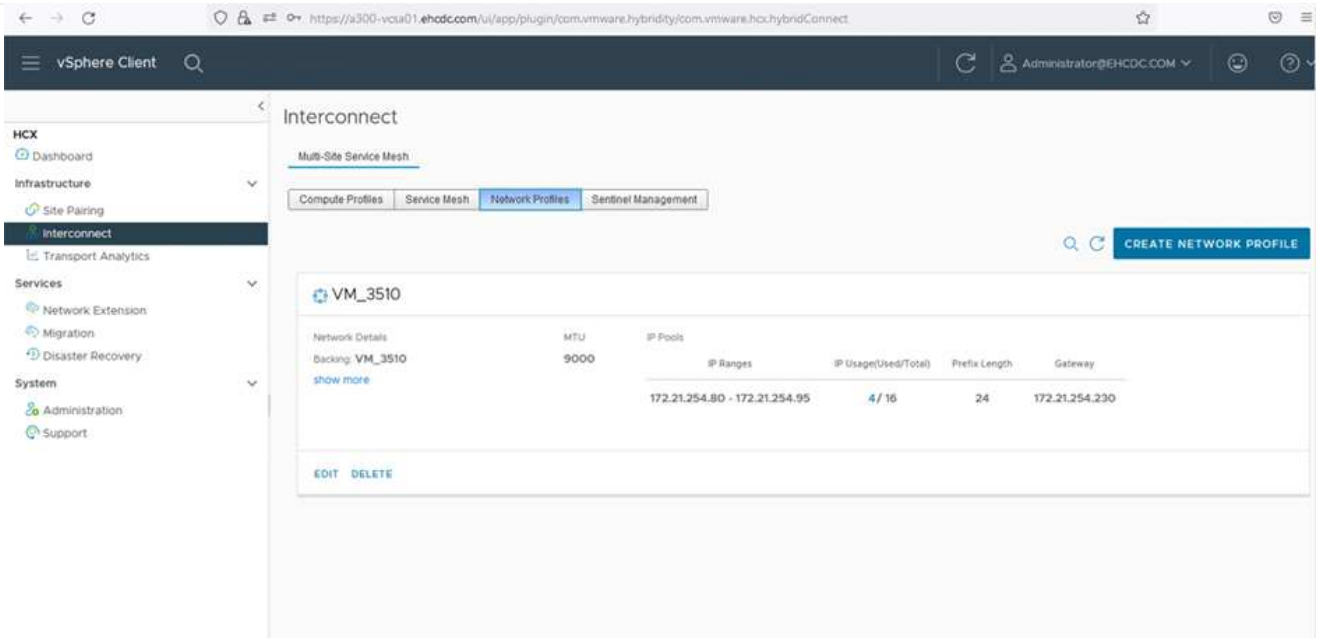
I profili di calcolo definiscono i parametri di implementazione, incluse le appliance implementate e la parte del data center VMware accessibile al servizio HCX.



1. 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).

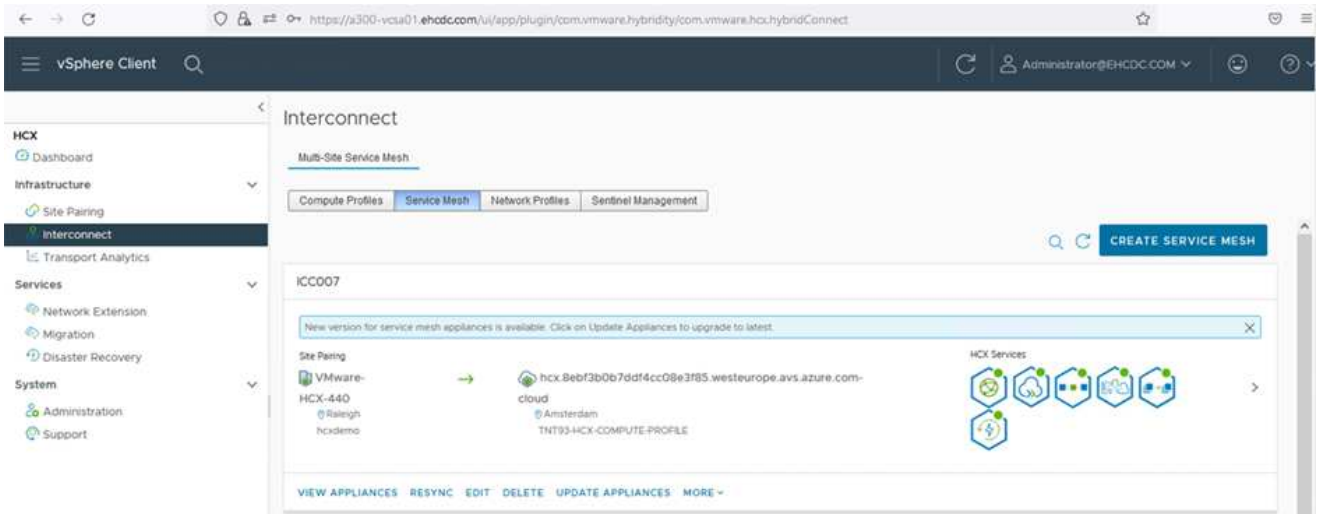
Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati DA HCX per le proprie appliance virtuali.

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

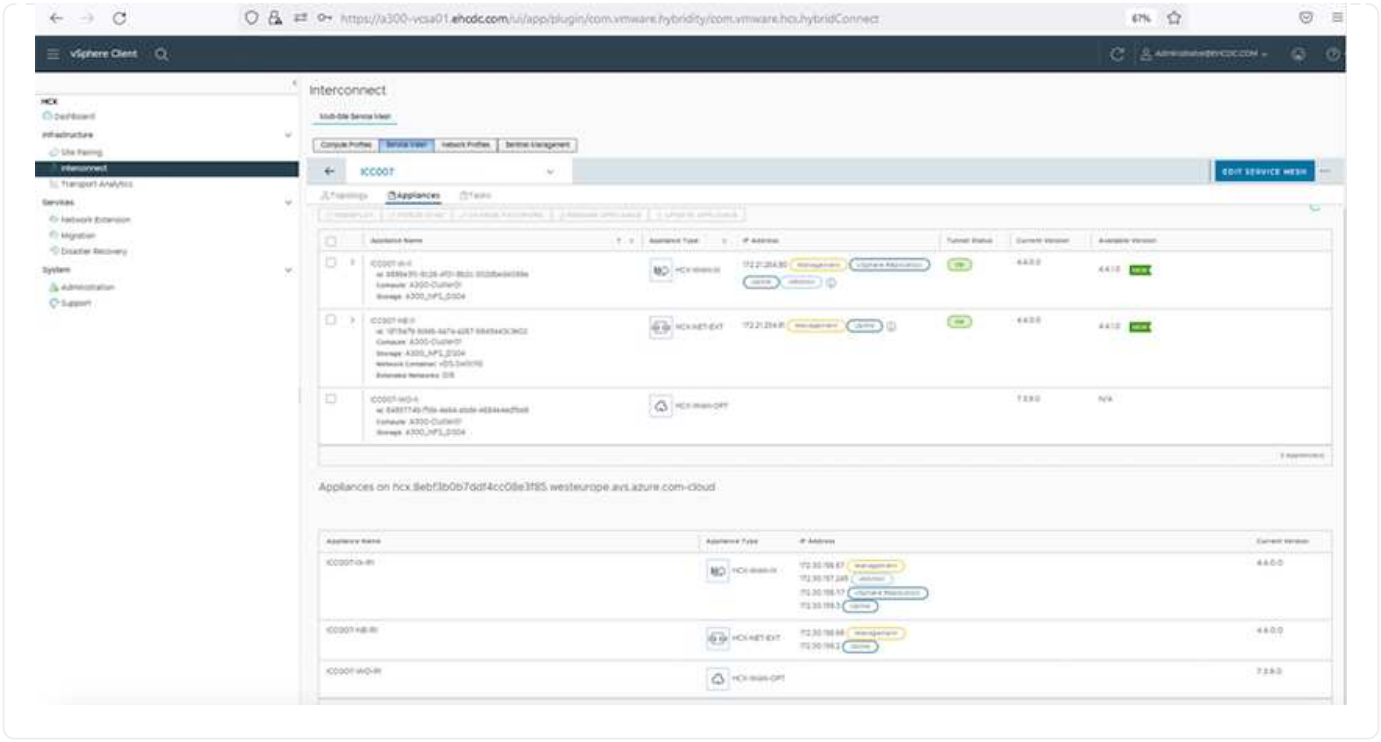


1. A questo punto, i profili di calcolo e di rete sono stati creati correttamente.
2. Creare la mesh del servizio selezionando la scheda **Mesh del servizio** all'interno dell'opzione **Interconnect** e selezionando i siti SDDC on-premise e Azure.
3. Service Mesh specifica una coppia di profili di rete 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.



1. 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.


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

Fase 6: Migrazione dei carichi di lavoro

I carichi di lavoro possono essere migrati bidirezionalmente tra gli SDDC on-premise e Azure 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).

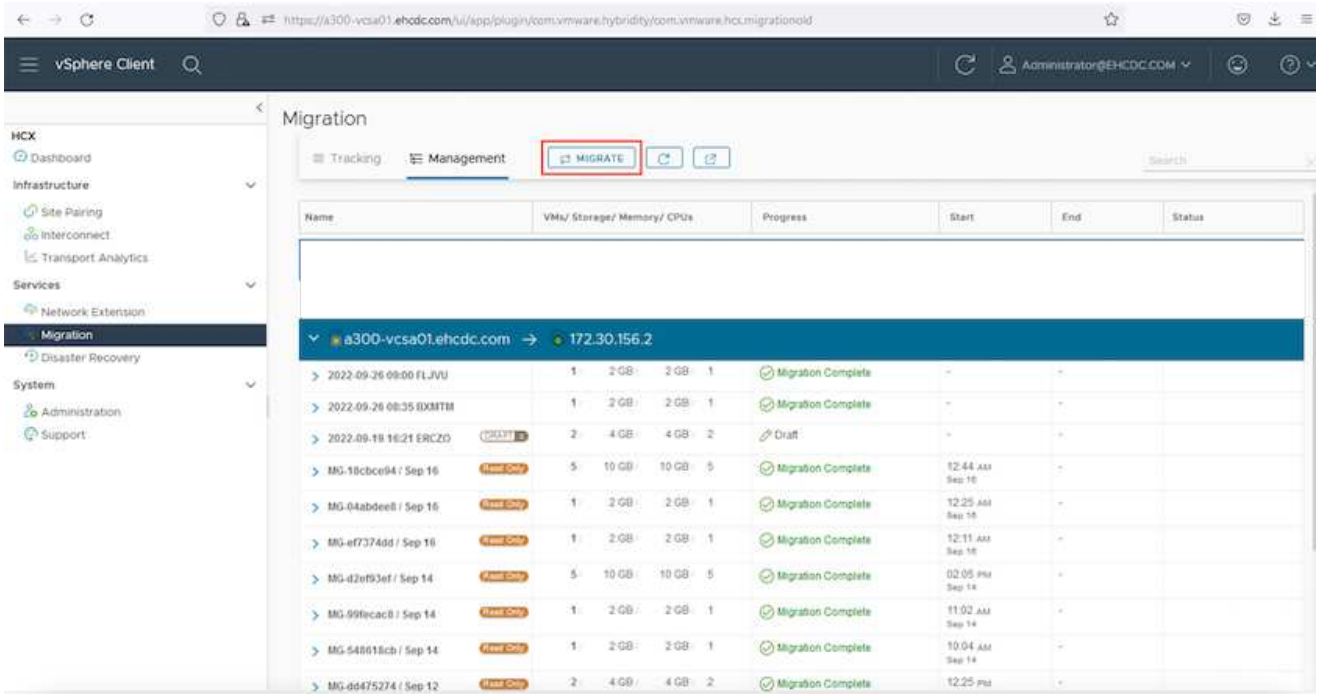
Per ulteriori informazioni sui vari meccanismi di migrazione HCX, vedere "Tipi di migrazione VMware HCX".

Migrazione in massa

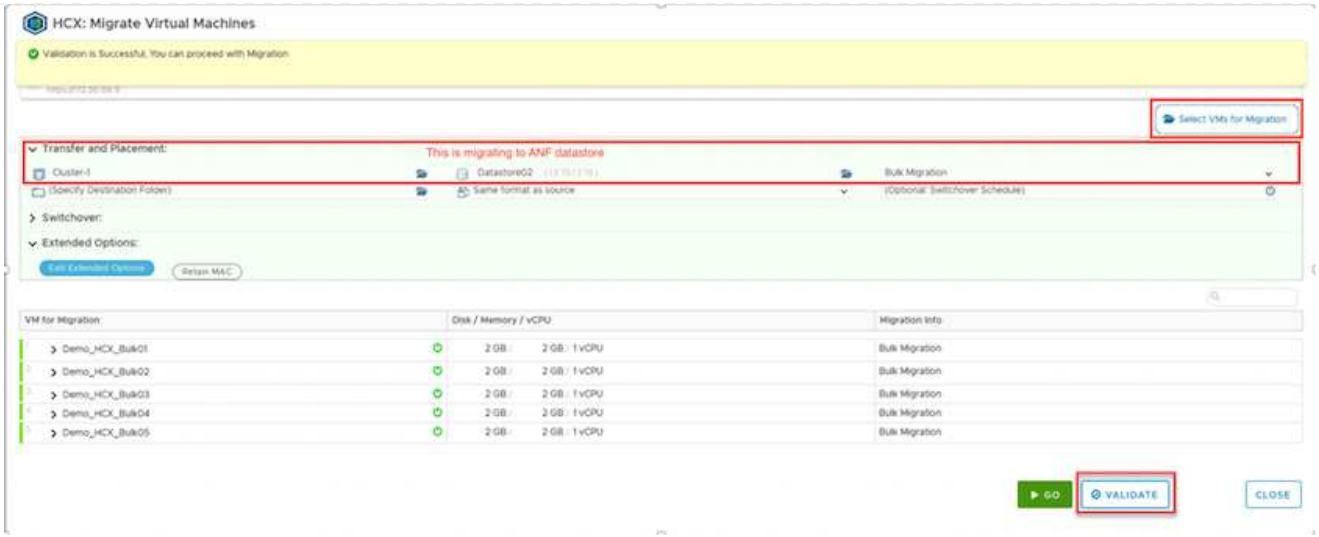
In questa sezione viene descritto in dettaglio il meccanismo di migrazione in blocco. Durante una migrazione in blocco, LA funzionalità di migrazione in blocco di HCX utilizza vSphere Replication per migrare i file disco ricreando la macchina virtuale sull'istanza di destinazione di vSphere HCX.

Per avviare migrazioni di macchine virtuali in blocco, attenersi alla seguente procedura:

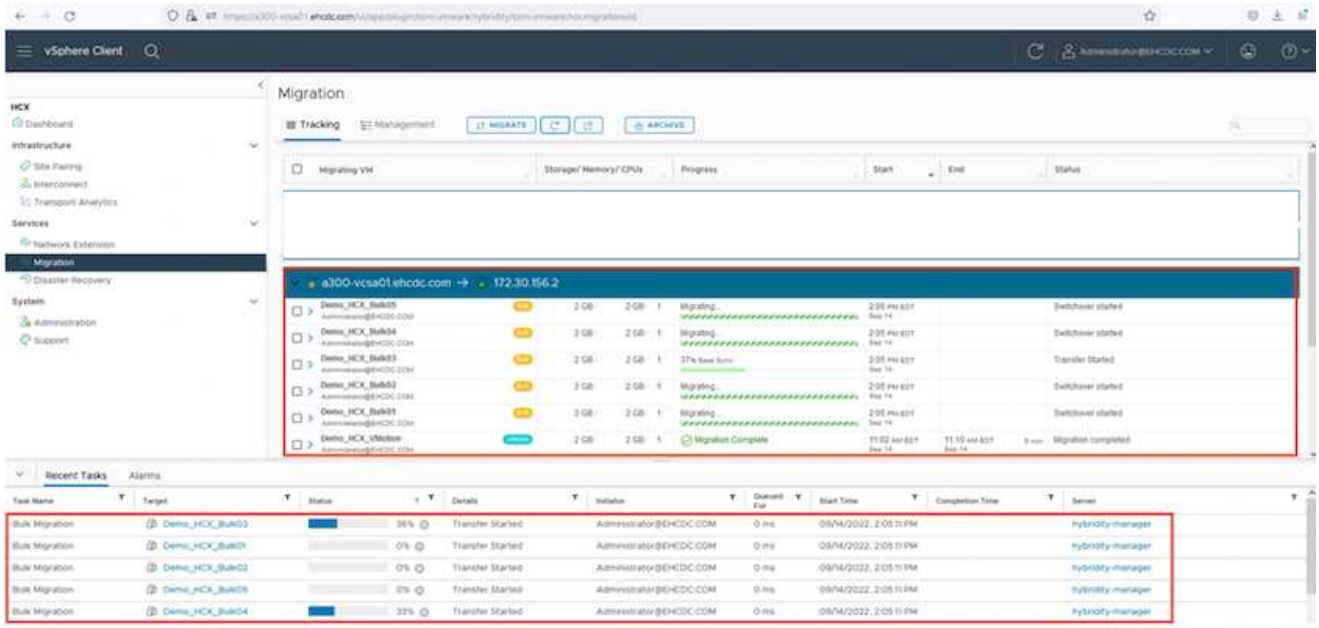
1. Accedere alla scheda **Migrate** in **servizi > migrazione**.



1. Nella sezione **connessione sito remoto**, selezionare la connessione del sito remoto e selezionare l'origine e la destinazione. In questo esempio, la destinazione è Azure VMware Solution SDDC HCX endpoint.
2. Fare clic su **Select VM for Migration** (Seleziona VM per la migrazione Questo fornisce un elenco di tutte le macchine virtuali on-premise. Selezionare le macchine virtuali in base all'espressione match:value e fare clic su **Add** (Aggiungi).
3. Nella sezione **Transfer and Placement** (trasferimento e posizionamento), aggiornare i campi obbligatori (**Cluster**, **Storage**, **Destination** e **Network**), incluso il profilo di migrazione, quindi fare clic su **Validate** (convalida).

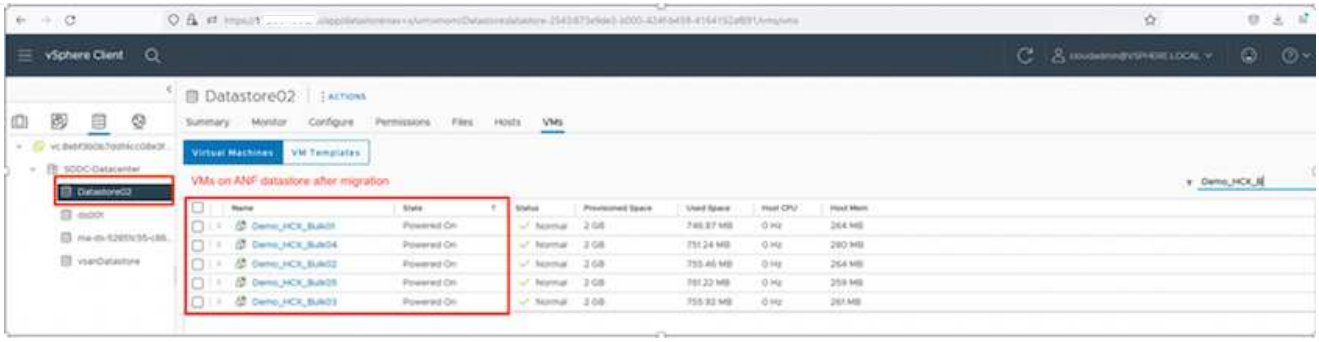


1. Al termine dei controlli di convalida, fare clic su **Go** per avviare la migrazione.



Durante questa migrazione, viene creato un disco segnaposto nel datastore Azure NetApp Files specificato all'interno del vCenter di destinazione per consentire la replica dei dati del disco VM di origine nei dischi segnaposto. L'HBR viene attivato per una sincronizzazione completa con la destinazione e, una volta completata la linea di base, viene eseguita una sincronizzazione incrementale in base al ciclo RPO (Recovery Point Objective). Una volta completata la sincronizzazione completa/incrementale, lo switchover viene attivato automaticamente, a meno che non venga impostata una pianificazione specifica.

1. Una volta completata la migrazione, validare la stessa accedendo al vCenter SDDC di destinazione.

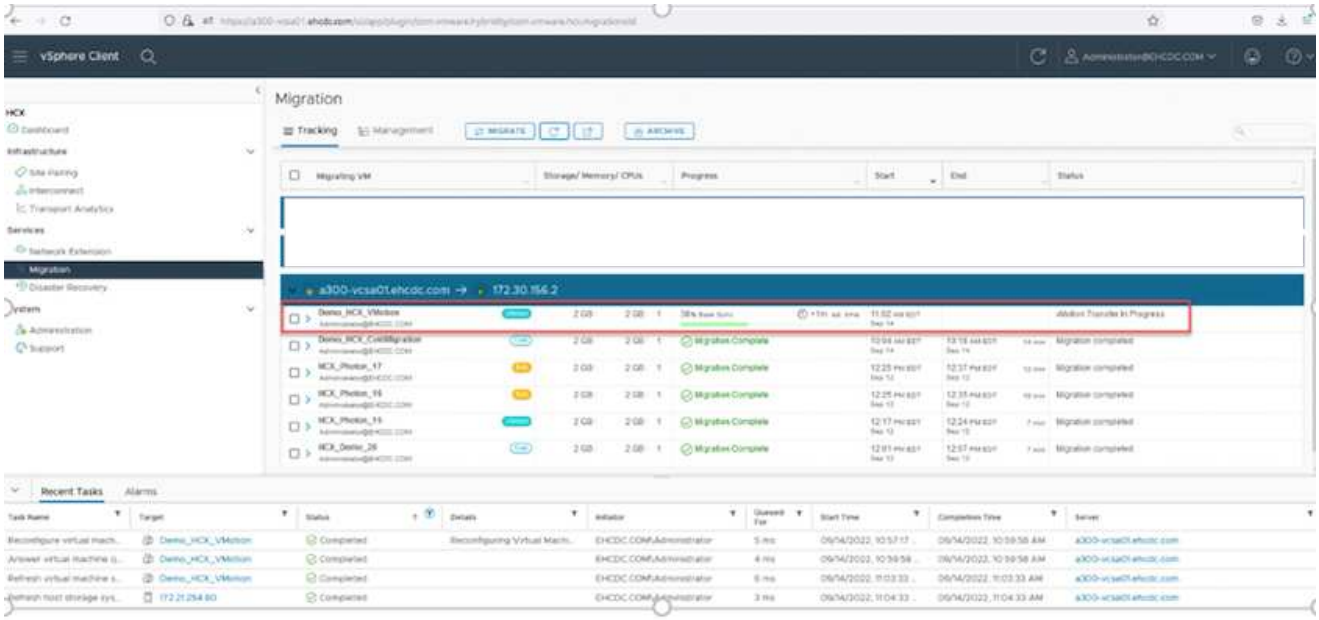


Per ulteriori e dettagliate informazioni sulle varie opzioni di migrazione e su come migrare i carichi di lavoro da una soluzione VMware on-premise a Azure utilizzando HCX, vedere "Guida utente di VMware HCX".

Per ulteriori informazioni su questo processo, guarda il seguente video:

Migrazione dei carichi di lavoro con HCX

Ecco una schermata dell'opzione HCX vMotion.



Per ulteriori informazioni su questo processo, guarda il seguente video:

HCX vMotion

Assicurarsi che sia disponibile una larghezza di banda sufficiente per gestire la migrazione.

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

Conclusione

Sia che tu stia prendendo come riferimento il cloud all-cloud o ibrido e i dati che risiedono su storage di

qualsiasi tipo/vendor in on-premise, Azure NetApp Files 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 a livello applicativo. Qualunque sia il caso d'utilizzo, scegli la soluzione VMware Azure insieme a Azure NetApp Files 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 Azure NetApp Files come datastore su Azure VMware Solution SDDC.
- È possibile migrare facilmente i dati da un datastore on-premise a un datastore Azure NetApp Files.
- È possibile espandere e ridurre facilmente il datastore Azure NetApp Files per soddisfare i requisiti di capacità e performance durante l'attività di migrazione.

Dove trovare ulteriori informazioni

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

- Documentazione della soluzione VMware Azure

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

- Documentazione Azure NetApp Files

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

- Guida utente di VMware HCX

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

Disponibilità regionale: Datastore NFS supplementare per ANF

La disponibilità di datastore NFS supplementari su Azure / AVS è definita da Microsoft. Innanzitutto, è necessario determinare se AVS e ANF sono disponibili in una regione specifica. Quindi, è necessario determinare se il datastore NFS supplementare ANF è supportato in quella regione.

- Verificare la disponibilità di AVS e ANF "qui".
- Verificare la disponibilità del datastore NFS supplementare ANF "qui".

Funzionalità NetApp per Google Cloud Platform GCVE

Scopri di più sulle funzionalità offerte da NetApp a Google Cloud Platform (GCP) Google Cloud VMware Engine (GCVE): Da NetApp come dispositivo storage connesso in guest o un datastore NFS supplementare alla migrazione dei flussi di lavoro, estensione/bursting nel cloud, backup/ripristino e disaster recovery.

Passare alla sezione relativa al contenuto desiderato selezionando una delle seguenti opzioni:

- "Configurazione di GCVE in GCP"
- "Opzioni di storage NetApp per GCVE"
- "Soluzioni cloud NetApp/VMware"

Configurazione di GCVE in GCP

Come per i sistemi on-premise, la pianificazione di un ambiente di virtualizzazione basato sul cloud è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire GCVE e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

> Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP e Cloud Volumes Services a GCVE.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementare e configurare GCVE
- Attiva accesso privato a GCVE

Visualizza i dettagli "Procedura di configurazione per GCVE".

Opzioni di storage NetApp per GCVE

Lo storage NetApp può essere utilizzato in diversi modi, come congettura connessa o come archivio dati NFS supplementare, all'interno di GCP GCVE.

Visitare il sito "Opzioni di storage NetApp supportate" per ulteriori informazioni.

Google Cloud supporta lo storage NetApp nelle seguenti configurazioni:

- Cloud Volumes ONTAP (CVO) come storage connesso guest
- Cloud Volumes Service (CVS) come storage connesso al guest
- Cloud Volumes Service (CVS) come datastore NFS supplementare

Visualizza i dettagli "Opzioni di storage di connessione guest per GCVE".

Scopri di più "Supporto del datastore NetApp Cloud Volumes Service per il motore VMware di Google Cloud (blog NetApp)" oppure "Come utilizzare NetApp CVS come datastore per Google Cloud VMware Engine (Google blog)"

Casi di utilizzo della soluzione

Con le soluzioni cloud NetApp e VMware, molti casi di utilizzo sono semplici da implementare in Azure AVS. I casi se sono definiti per ciascuna delle aree cloud definite da VMware:

- Protect (include disaster recovery e backup/ripristino)
- Estendi

- Migrare

"Esplora le soluzioni NetApp per Google Cloud GCVE"

Protezione dei carichi di lavoro su GCP/GCVE

Disaster recovery coerente con l'applicazione con replica NetApp SnapCenter e Veeam

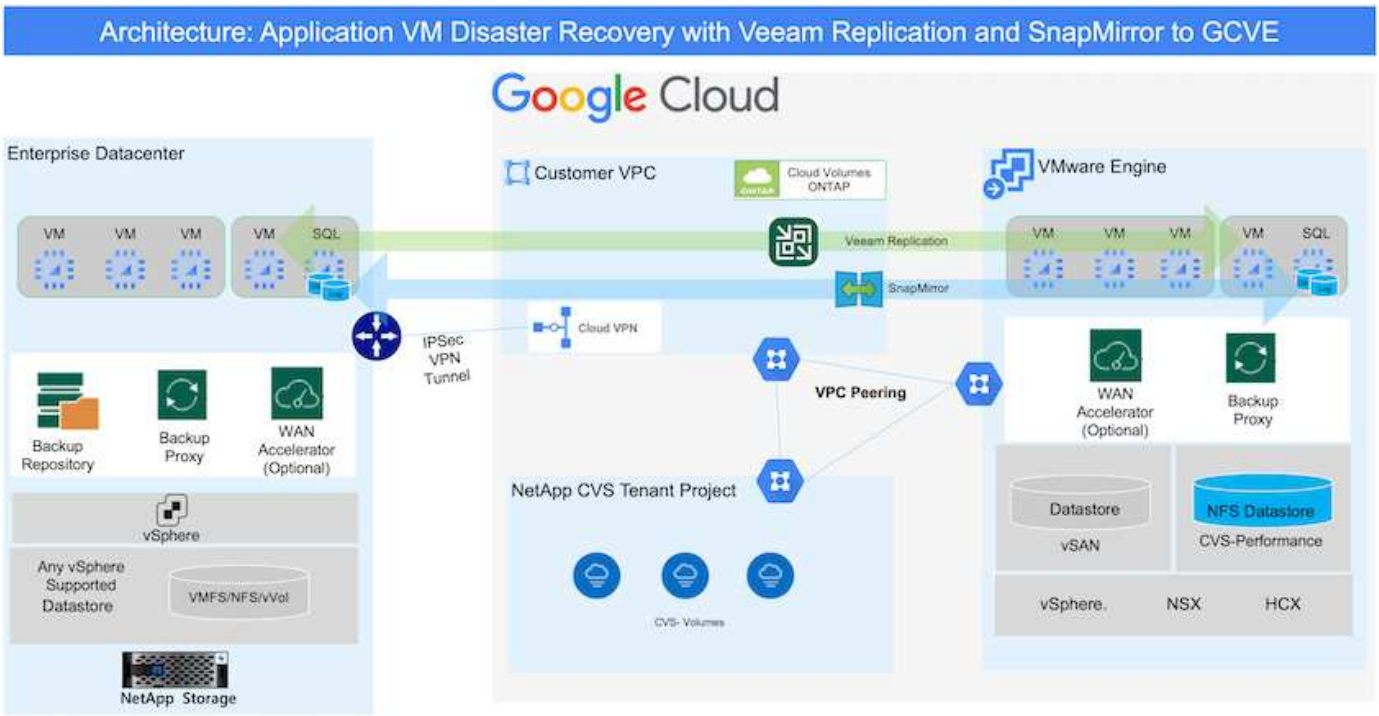
Autori: Suresh Thoppay, NetApp

Panoramica

Molti clienti cercano una soluzione di disaster recovery efficace per le loro macchine virtuali applicative ospitate su VMware vSphere. Molti di loro utilizzano la soluzione di backup esistente per eseguire il recovery durante il diaster.
Molte volte questa soluzione aumenta l'RTO e non soddisfa le loro aspettative. Per ridurre l'RPO e l'RTO, la replica delle macchine virtuali Veeam può essere utilizzata anche da on-premise a GCVE, purché siano disponibili connettività di rete e ambiente con autorizzazioni appropriate.
NOTA: Veeam VM Replication non protegge i dispositivi storage connessi guest delle VM, come i supporti iSCSI o NFS, all'interno della VM guest. Necessità di proteggerli separatamente.

Per una replica coerente delle applicazioni per SQL VM e per ridurre l'RTO, abbiamo utilizzato SnapCenter per orchestrare le operazioni di snapmirror dei volumi di log e del database SQL.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, Veeeam e Google Cloud VMware Engine (GCVE).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.

Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizza le opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.

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 alla documentazione di Google Cloud per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione DR

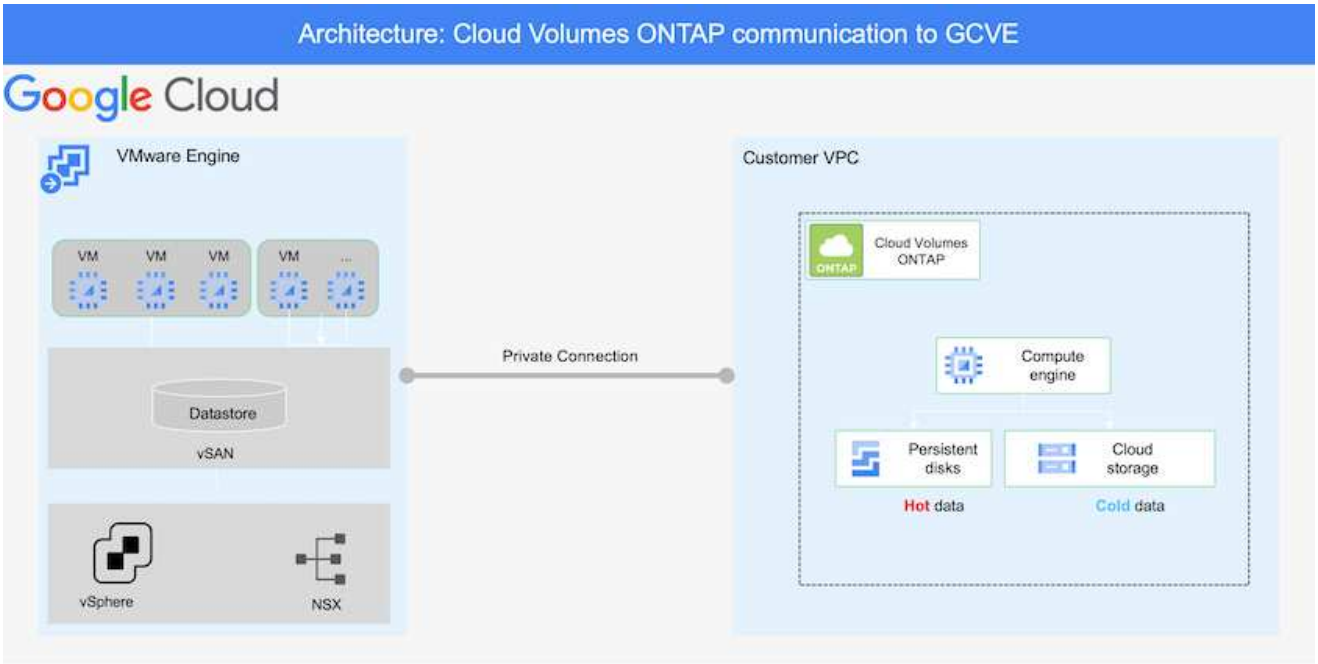
Panoramica sull'implementazione della soluzione

1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando BlueXP all'interno dell'abbonamento appropriato e della rete virtuale.
    a. Configurare SnapMirror per i volumi applicativi rilevanti.
    b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.
3. Installare il software Veeam e avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Durante un evento di emergenza, interrompere la relazione SnapMirror utilizzando BlueXP e attivare il failover delle macchine virtuali con Veeam.
    a. Ricollegare I LUN ISCSI e i montaggi NFS per le macchine virtuali dell'applicazione.
    b. Visualizzare le applicazioni online.
5. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Google Cloud e replicare i volumi su CVO

Il primo passo consiste nel configurare Cloud Volumes ONTAP su Google Cloud ("cvo") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritentioni di snapshot.



Per istruzioni dettagliate di esempio sull'impostazione di SnapCenter e la replica dei dati, fare riferimento a. "Configurazione della replica con SnapCenter"

Analisi della protezione di SQL VM con SnapCenter

Configurare gli host GCVE e l'accesso ai dati CVO

Due fattori importanti da prendere in considerazione durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e il tempo necessario per mantenere SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

Il servizio di volume cloud di NetApp per datastore NFS e Cloud Volumes ONTAP per database SQL e log possono essere implementati su qualsiasi VPC e deve disporre di una connessione privata a tale VPC per montare datastore NFS e connettere le macchine virtuali a LUN iSCSI.

Per configurare GCVE SDDC, vedere "Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform (GCP)". Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host GCVE siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e GCVE, iniziare a configurare Veeam per automatizzare il ripristino dei carichi di lavoro on-premise su GCVE (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando la funzione di replica Veeam e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

Installare i componenti Veeam

In base allo scenario di implementazione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere implementati. In questo caso di utilizzo, non è necessario implementare l'archivio di oggetti per Veeam e il repository scale-out.
"Fare riferimento alla documentazione Veeam per la procedura di installazione"
Per ulteriori informazioni, fare riferimento a. "Migrazione con Replica Veeam"

Configurazione della replica delle macchine virtuali con Veeam

VCenter on-premise e gCVE vCenter devono essere registrati con Veeam. "Processo di replica di vSphere VM" Nella fase di elaborazione guest della procedura guidata, selezionare Disable application processing (Disattiva elaborazione applicazioni), in quanto verrà utilizzato SnapCenter per il backup e il ripristino consapevoli dell'applicazione.

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

Failover di Microsoft SQL Server VM

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

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.
  - In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
  - Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
  - Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.
- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito DR.

Disaster recovery applicativo con replica SnapCenter, Cloud Volumes ONTAP e Veeam

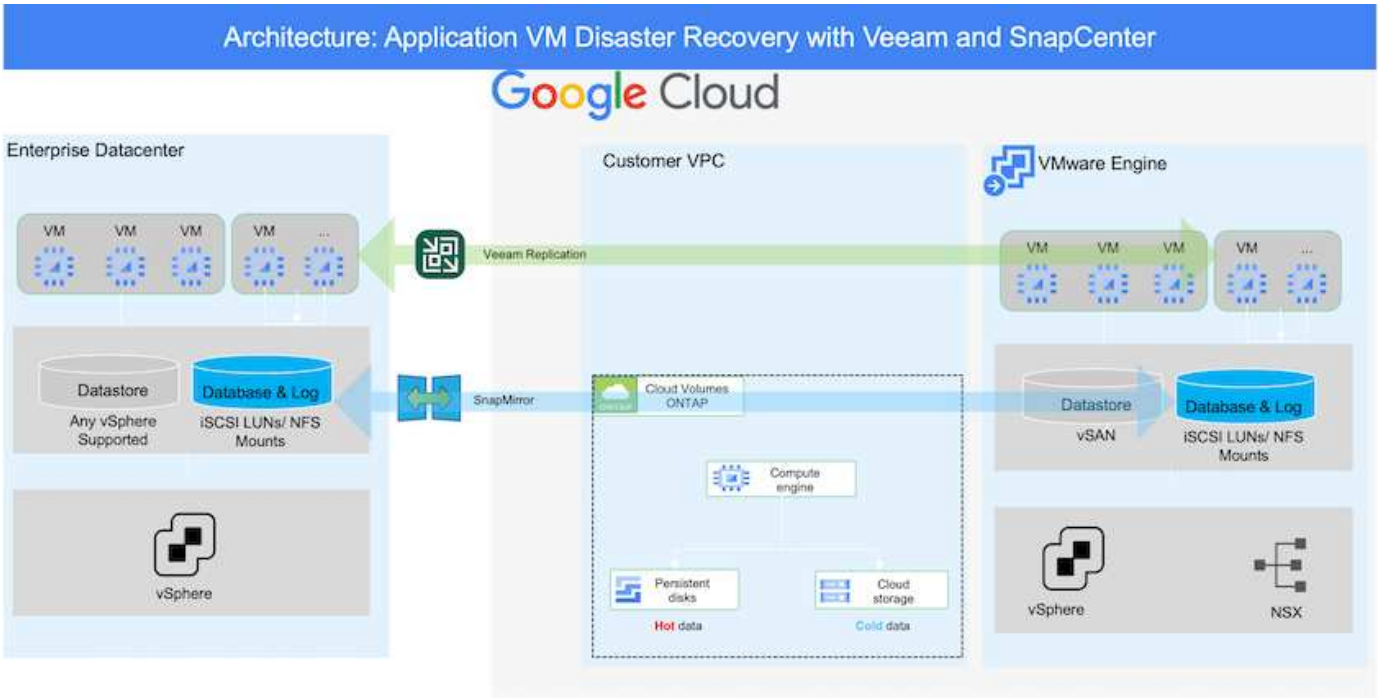
Autori: Suresh Thoppay, NetApp

Panoramica

Il disaster recovery nel cloud è un metodo resiliente e conveniente per proteggere i workload da interruzioni del sito e eventi di corruzione dei dati come ransomware. Con NetApp SnapMirror, è possibile replicare i workload VMware on-premise che utilizzano lo storage connesso agli ospiti su NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud. Ciò riguarda i dati delle applicazioni, ma le macchine virtuali effettive. Il disaster recovery dovrebbe coprire tutti i componenti dipendenti, tra cui macchine virtuali, VMDK, dati applicativi e altro ancora. A tale scopo, SnapMirror e Veeam possono essere utilizzati per ripristinare perfettamente i carichi di

lavoro replicati da on-premise a Cloud Volumes ONTAP utilizzando lo storage vSAN per VM VMDK.

Questo documento fornisce un approccio passo per passo per la configurazione e l'esecuzione del disaster recovery che utilizza NetApp SnapMirror, Veeeam e Google Cloud VMware Engine (GCVE).



Presupposti

Questo documento si concentra sullo storage in-guest per i dati delle applicazioni (noto anche come guest Connected) e si presume che l'ambiente on-premise stia utilizzando SnapCenter per backup coerenti con le applicazioni.

> Questo documento si riferisce a qualsiasi soluzione di backup o ripristino di terze parti. A seconda della soluzione utilizzata nell'ambiente, seguire le Best practice per creare policy di backup che soddisfino gli SLA dell'organizzazione.

Per la connettività tra l'ambiente on-premise e la rete Google Cloud, utilizza le opzioni di connettività come l'interconnessione dedicata o la VPN cloud. I segmenti devono essere creati in base alla progettazione della VLAN on-premise.

> 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 alla documentazione di Google Cloud per il metodo di connettività on-premise-to-Google appropriato.

Implementazione della soluzione DR

Panoramica sull'implementazione della soluzione

1. Assicurarsi che il backup dei dati dell'applicazione venga eseguito utilizzando SnapCenter con i requisiti RPO necessari.
2. Eseguire il provisioning di Cloud Volumes ONTAP con la dimensione dell'istanza corretta utilizzando Cloud Manager all'interno dell'abbonamento appropriato e della rete virtuale.

a. Configurare SnapMirror per i volumi applicativi rilevanti.

b. Aggiornare i criteri di backup in SnapCenter per attivare gli aggiornamenti di SnapMirror dopo i processi pianificati.

3. Installare il software Veeam e avviare la replica delle macchine virtuali sull'istanza di Google Cloud VMware Engine.
4. Durante un evento di disastro, interrompere la relazione SnapMirror utilizzando Cloud Manager e attivare il failover delle macchine virtuali con Veeam.

a. Ricollegare I LUN ISCSI e i montaggi NFS per le macchine virtuali dell'applicazione.

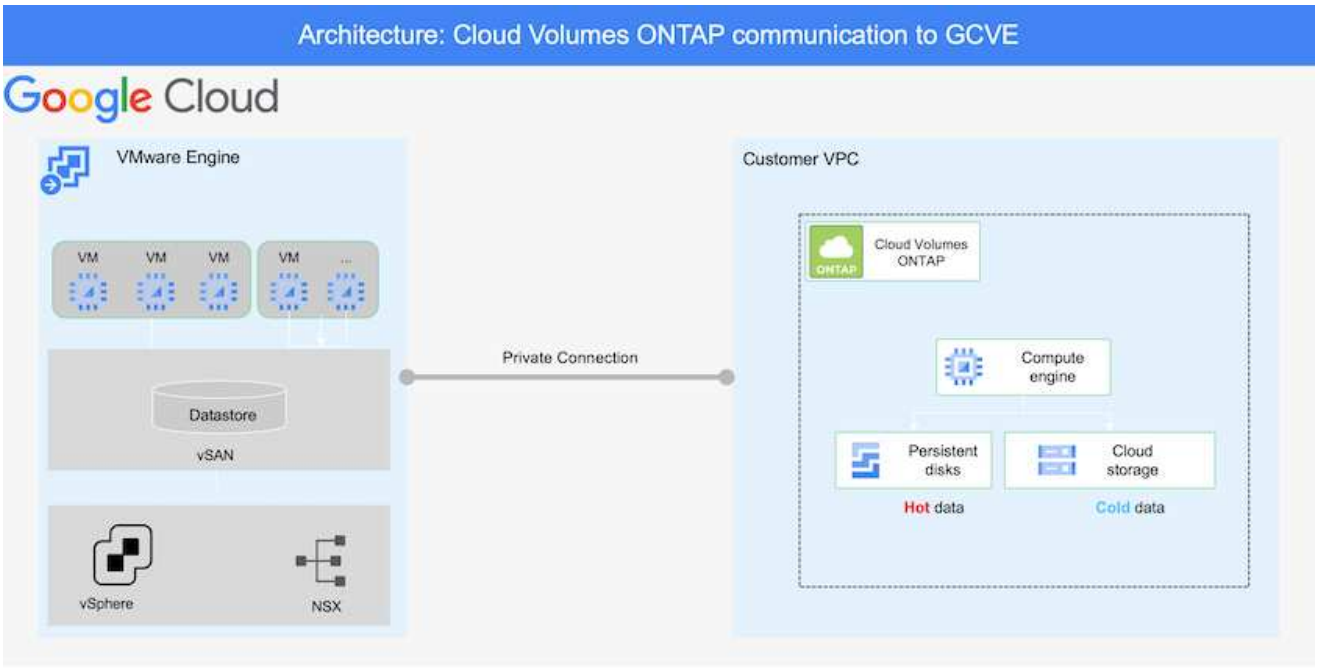
b. Visualizzare le applicazioni online.

5. Richiamare il failback sul sito protetto risyncing inverso di SnapMirror dopo il ripristino del sito primario.

Dettagli sull'implementazione

Configurare CVO su Google Cloud e replicare i volumi su CVO

Il primo passo consiste nel configurare Cloud Volumes ONTAP su Google Cloud ("cvo") E replicare i volumi desiderati su Cloud Volumes ONTAP con le frequenze desiderate e le ritentioni di snapshot.



Per istruzioni dettagliate di esempio sull'impostazione di SnapCenter e la replica dei dati, fare riferimento a. "Configurazione della replica con SnapCenter"

Configurazione della replica con SnapCenter

Configurare gli host GCVE e l'accesso ai dati CVO

Due fattori importanti da prendere in considerazione durante l'implementazione di SDDC sono le dimensioni del cluster SDDC nella soluzione GCVE e il tempo necessario per mantenere SDDC in servizio. Queste due considerazioni chiave per una soluzione di disaster recovery contribuiscono a ridurre i costi operativi complessivi. Il controller SDDC può contenere fino a tre host, fino a un cluster multi-host in un'implementazione su larga scala.

Cloud Volumes ONTAP può essere implementato su qualsiasi VPC e deve disporre di una connessione privata a tale VPC per consentire la connessione della macchina virtuale alle LUN iSCSI.

Per configurare GCVE SDDC, vedere "Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform (GCP)". Come prerequisito, verificare che le macchine virtuali guest che risiedono sugli host GCVE siano in grado di utilizzare i dati da Cloud Volumes ONTAP dopo aver stabilito la connettività.

Dopo aver configurato correttamente Cloud Volumes ONTAP e GCVE, iniziare a configurare Veeam per automatizzare il ripristino dei carichi di lavoro on-premise su GCVE (macchine virtuali con VMDK delle applicazioni e macchine virtuali con storage in-guest) utilizzando la funzione di replica Veeam e sfruttando SnapMirror per le copie dei volumi delle applicazioni su Cloud Volumes ONTAP.

Installare i componenti Veeam

In base allo scenario di implementazione, il server di backup Veeam, il repository di backup e il proxy di backup che devono essere implementati. In questo caso di utilizzo, non è necessario implementare l'archivio di oggetti per Veeam e il repository scale-out.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Fare riferimento alla documentazione Veeam per la procedura di installazione"]

Configurazione della replica delle macchine virtuali con Veeam

VCenter on-premise e gCVE vCenter devono essere registrati con Veeam. "Processo di replica di vSphere VM" Nella fase di elaborazione guest della procedura guidata, selezionare Disable application processing (Disattiva elaborazione applicazioni), in quanto verrà utilizzato SnapCenter per il backup e il ripristino consapevoli dell'applicazione.

Processo di replica di vSphere VM

Failover di Microsoft SQL Server VM

Failover di Microsoft SQL Server VM

Vantaggi di questa soluzione

- Utilizza la replica efficiente e resiliente di SnapMirror.
- Effettua il ripristino in qualsiasi punto disponibile in tempo con la conservazione delle snapshot di ONTAP.
- È disponibile un'automazione completa per tutte le fasi necessarie per il ripristino di centinaia o migliaia di macchine virtuali, dalle fasi di convalida di storage, calcolo, rete e applicazioni.
- SnapCenter utilizza meccanismi di cloning che non modificano il volume replicato.

- In questo modo si evita il rischio di corruzione dei dati per volumi e snapshot.
- Evita le interruzioni di replica durante i flussi di lavoro dei test di DR.
- Sfrutta i dati di DR per flussi di lavoro oltre il DR, come sviluppo/test, test di sicurezza, test di patch e upgrade e test di correzione.

- La replica Veeam consente di modificare gli indirizzi IP delle macchine virtuali sul sito DR.

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

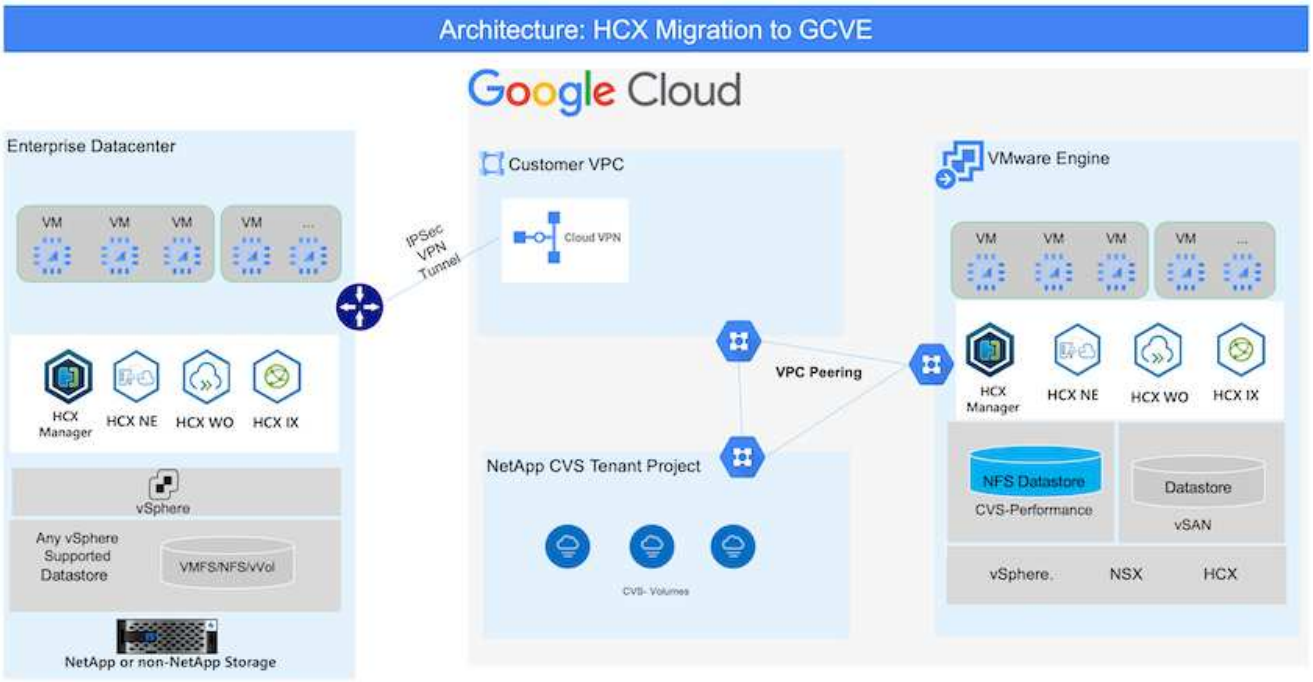
Prima di iniziare, assicurarsi che siano soddisfatti i seguenti prerequisiti. Per ulteriori informazioni, consulta questa sezione "collegamento". Una volta soddisfatti i prerequisiti, inclusa la connettività, scaricare la chiave di licenza HCX dal portale VMware Engine di Google Cloud. Una volta scaricato 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

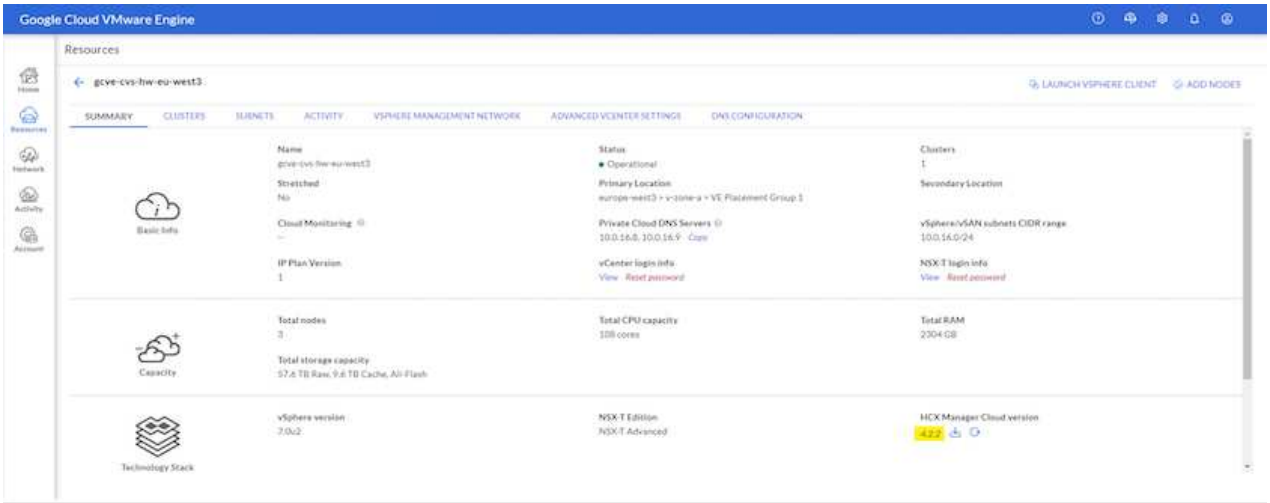
Seguire la serie di passaggi per completare l'implementazione di questa soluzione:

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

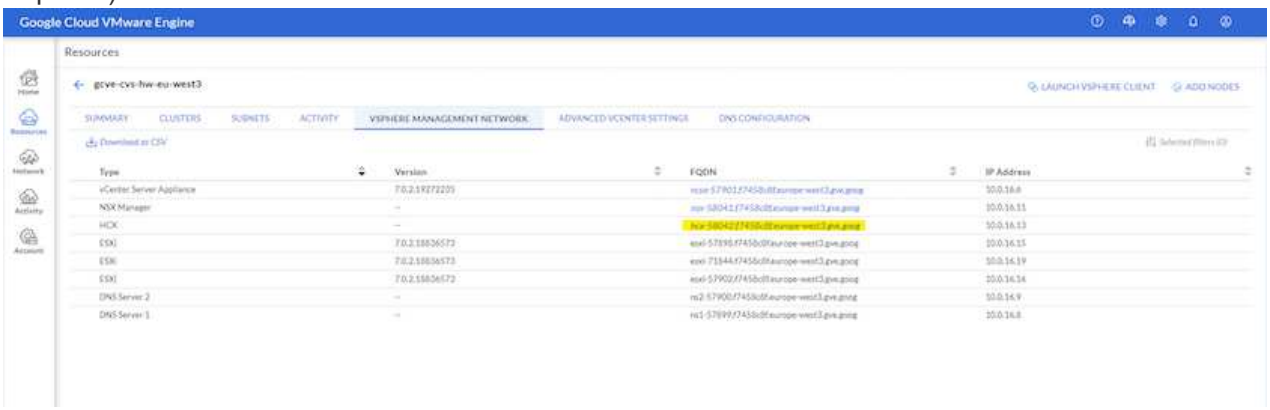
Il componente HCX Cloud Manager viene installato automaticamente durante il provisioning del cloud privato con VMware Engine. Per prepararsi all'associazione del sito, attenersi alla seguente procedura:

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

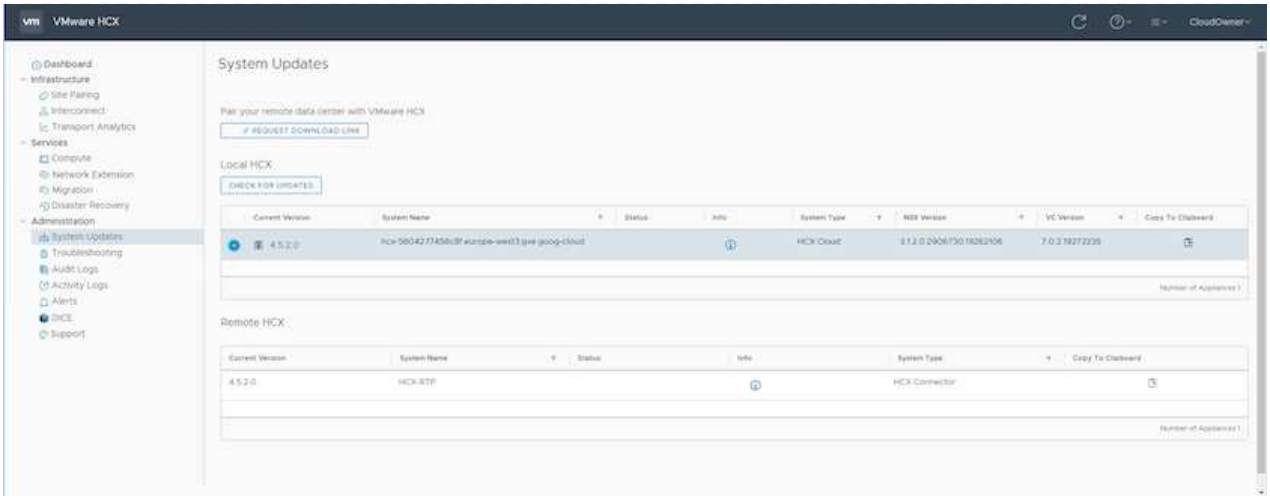
   È possibile accedere ALLA console HCX facendo clic sul collegamento alla versione HCX



   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.



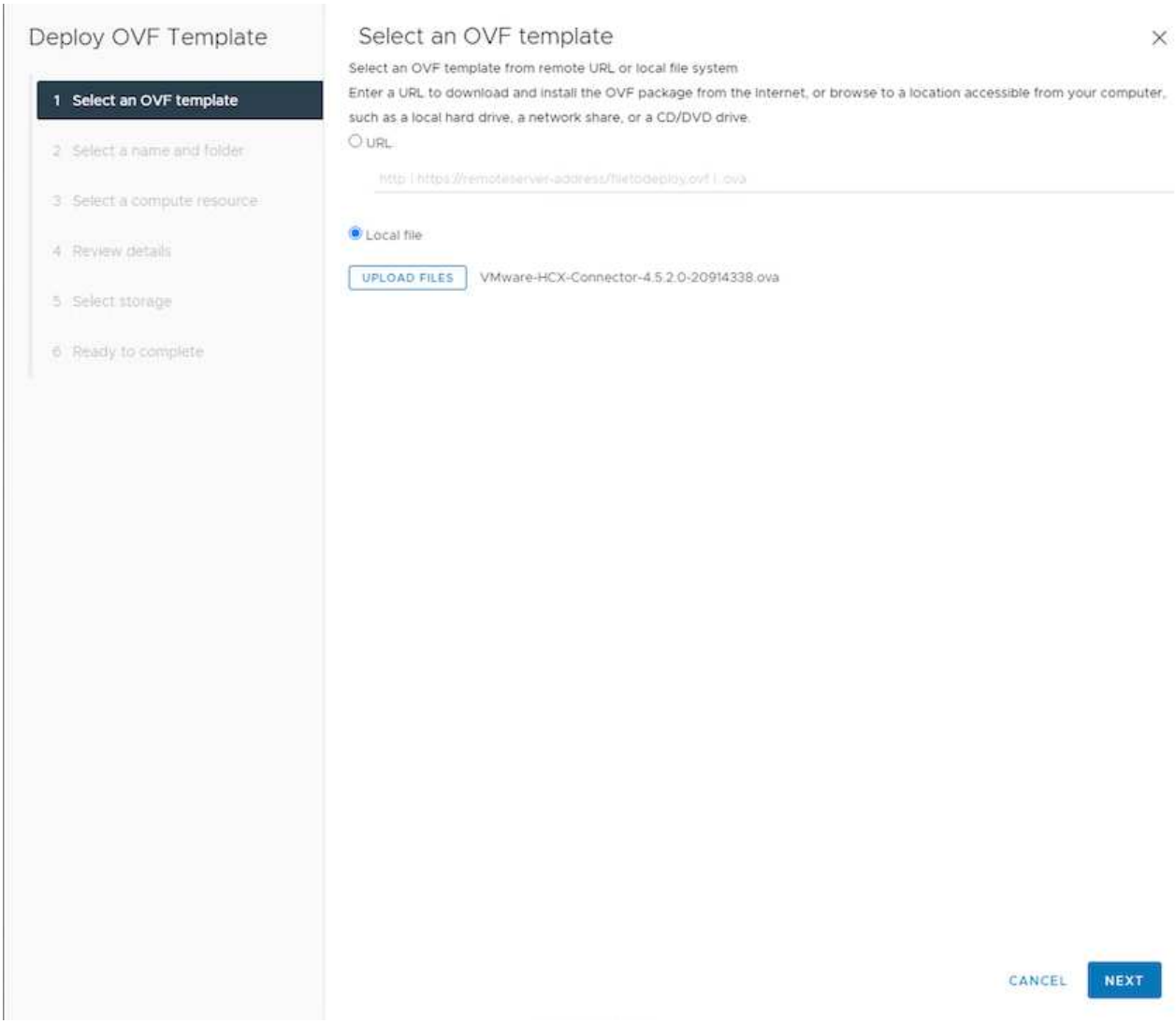
4. Aggiornare HCX Cloud Manager alla versione più recente disponibile dall'interfaccia utente DI HCX Cloud Manager.

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**.



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.

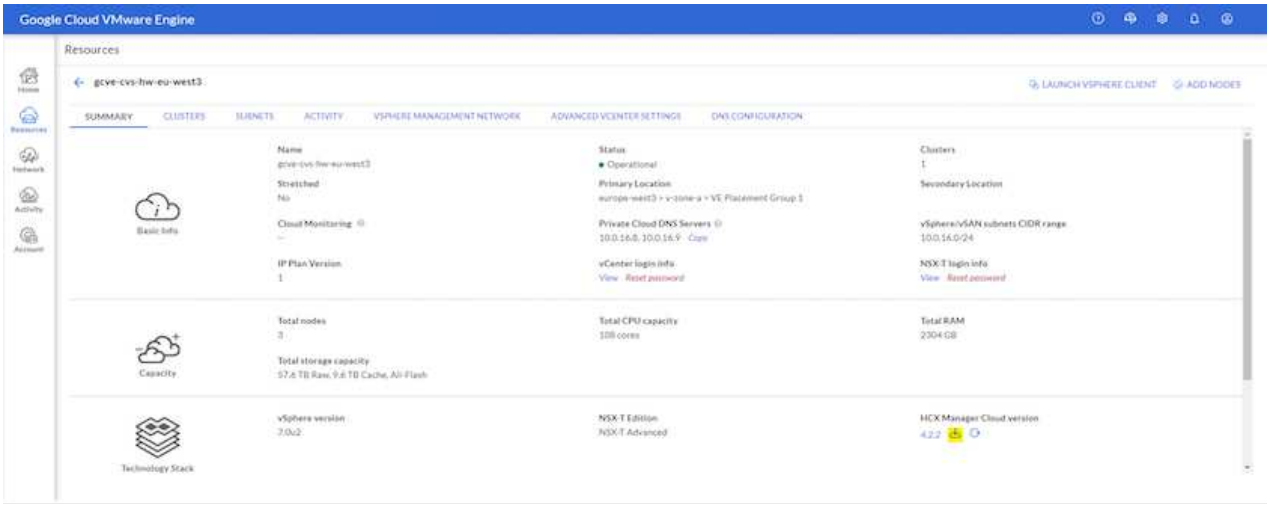
Accendere l'appliance virtuale manualmente.

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.

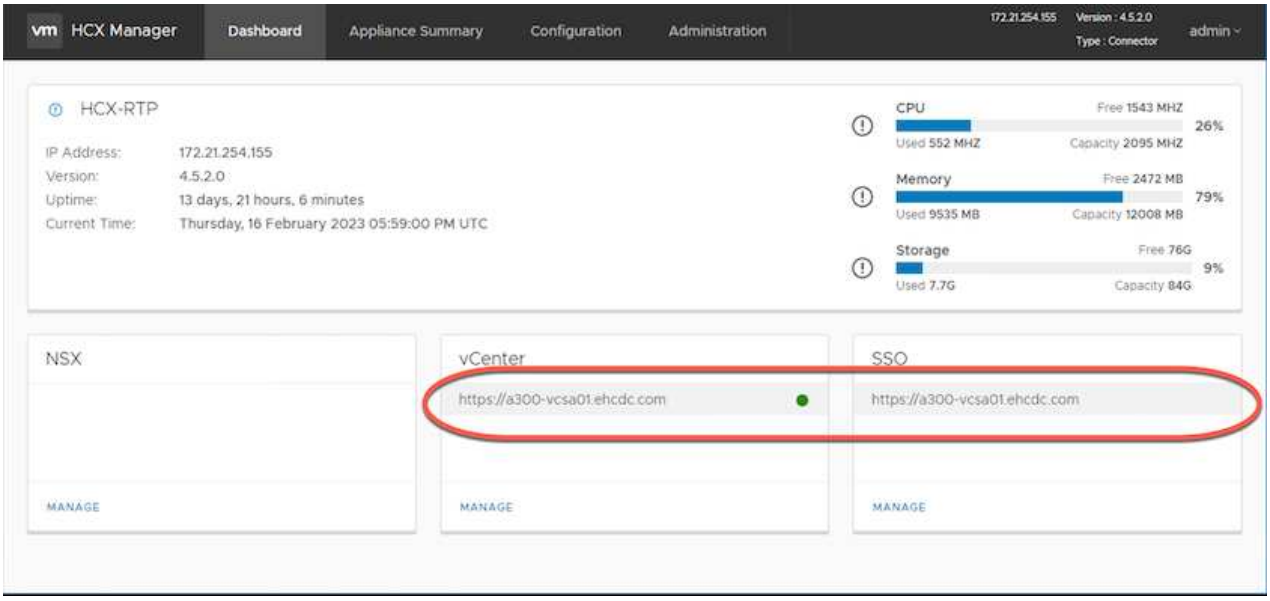
8. In **Configure SSO/PSC** (Configura SSO/PSC), fornire l'indirizzo IP o il nome FQDN del Platform Services Controller (PSC) e fare clic su **Continue** (continua).

> 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.

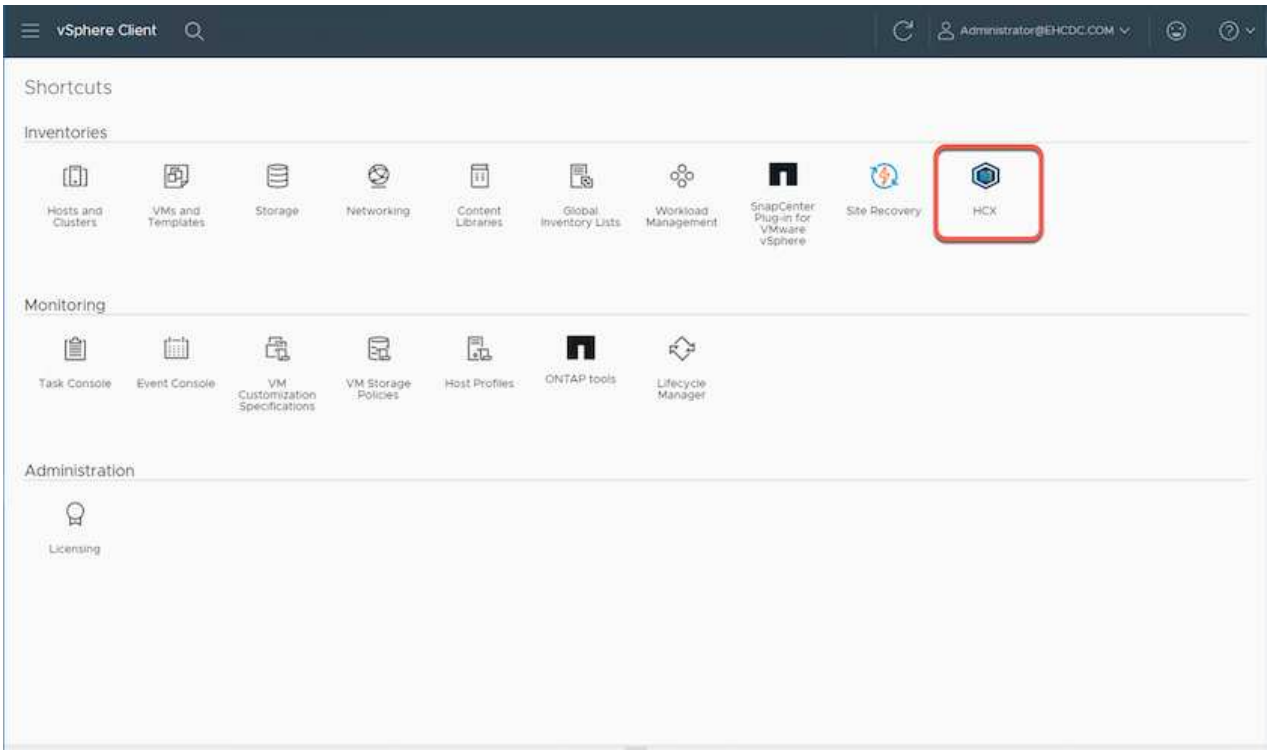
Questo processo richiede circa 10 - 20 minuti e l'aggiunta del plug-in al server vCenter.



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

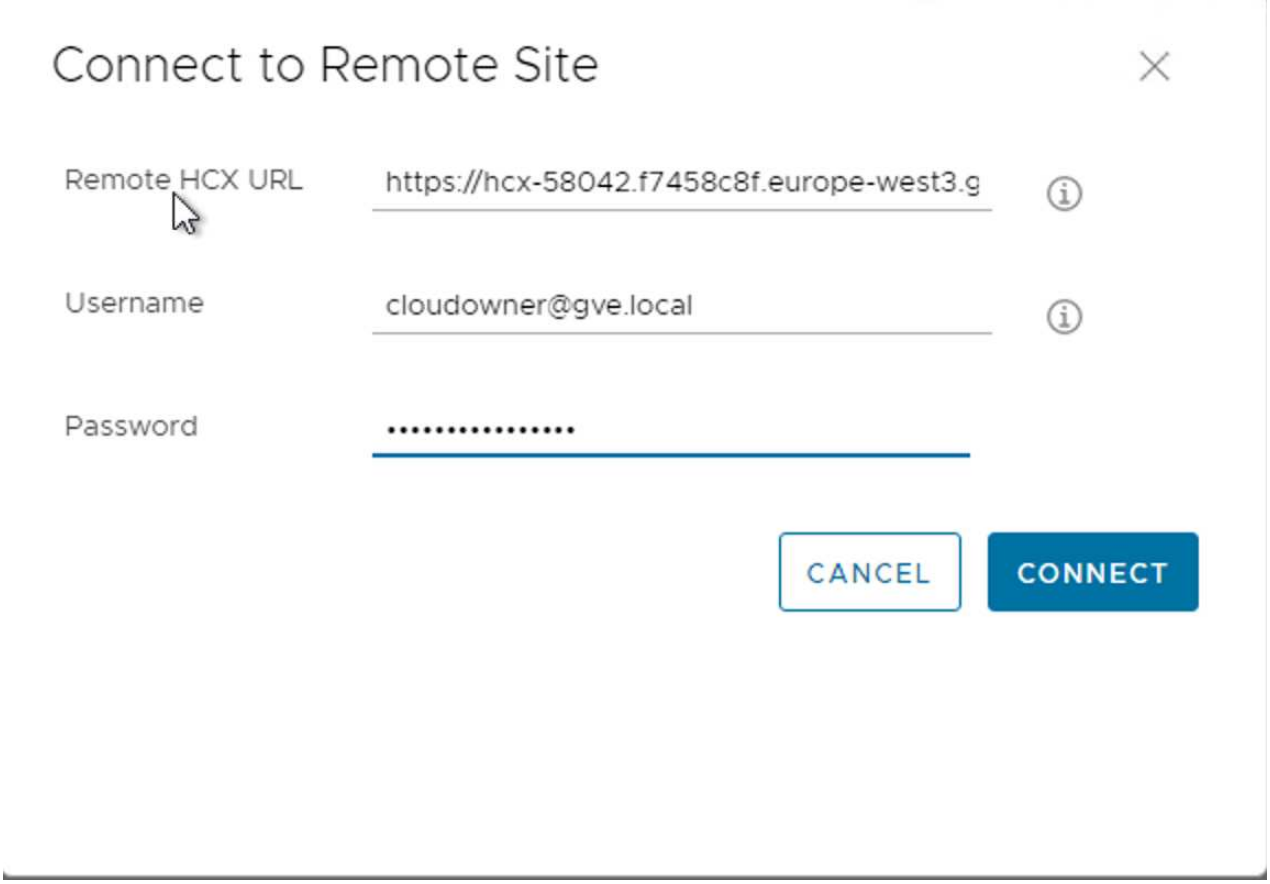
Una volta implementato E configurato IL connettore HCX on-premise vCenter, stabilire la connessione a Cloud Manager aggiungendo l'accoppiamento. Per configurare l'associazione del sito, attenersi alla seguente procedura:

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).

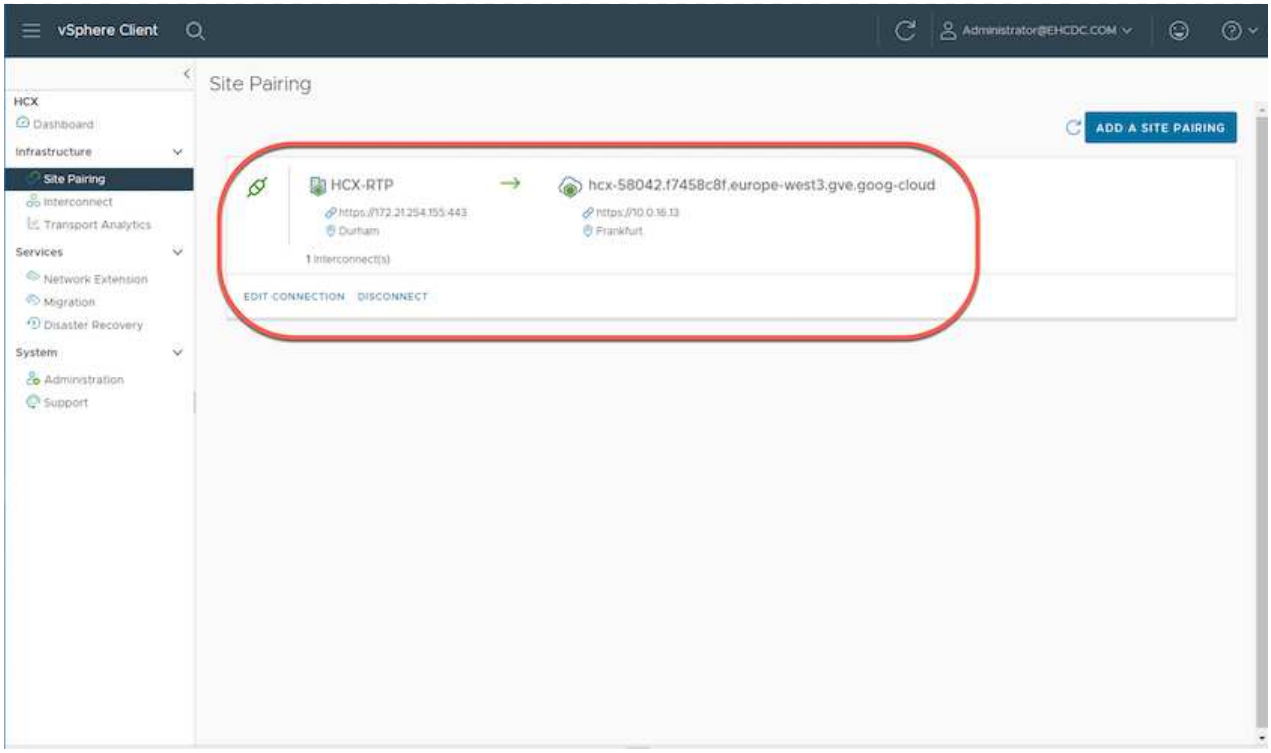
Inserire l'indirizzo IP o l'URL di Google Cloud VMware Engine HCX Cloud Manager e le credenziali per l'utente con privilegi di ruolo Cloud Owner per l'accesso al cloud privato.



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.

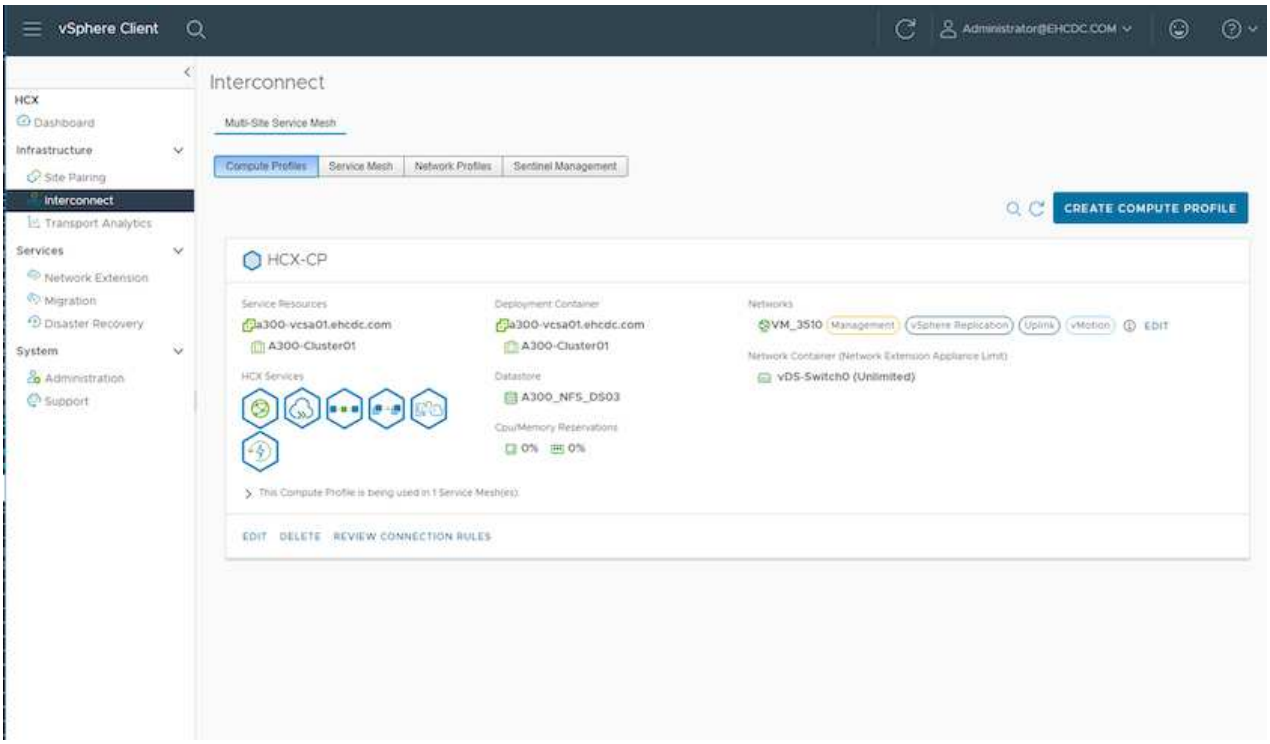

vSphere Client
Administrator@EHCDC.COM
HCX
Dashboard
Infrastructure
Site Pairing
Interconnect
Transport Analytics
Services
Network Extension
Migration
Disaster Recovery
System
Administration
Support
Site Pairing
ADD A SITE PAIRING
HCX-RTP
https://172.21.254.155:443
Durham
hcx-58042.f7458c8f.europe-west3.gve.goog-cloud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

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

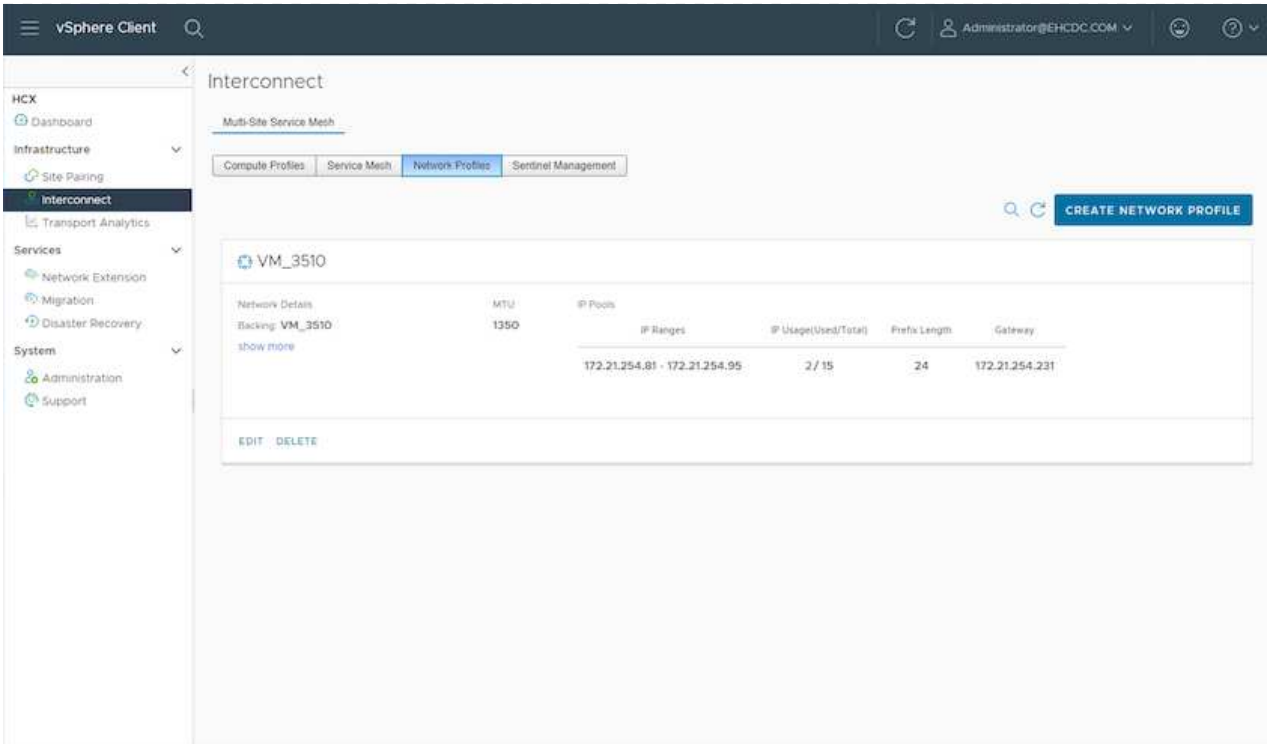
   I profili di calcolo definiscono i parametri di implementazione, incluse le appliance implementate e la parte del data center VMware accessibile al servizio HCX.



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).

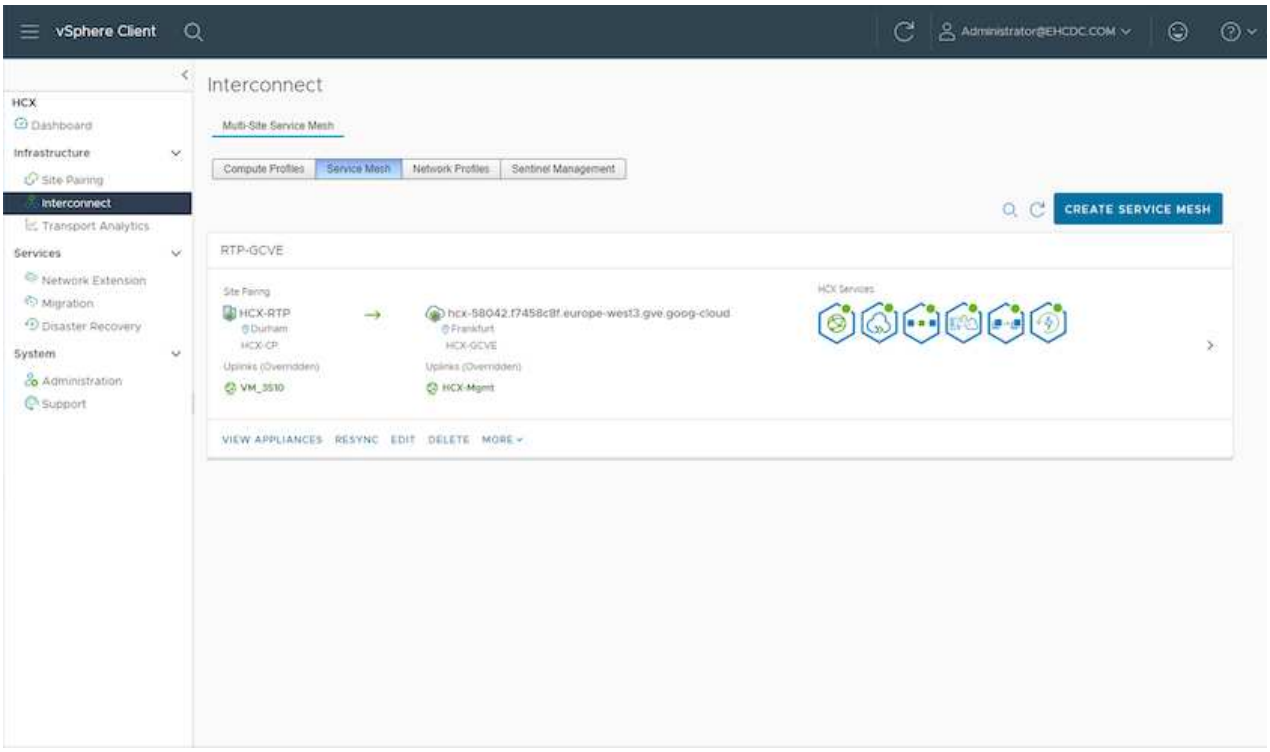
   Il profilo di rete definisce un intervallo di indirizzi IP e reti utilizzati DA HCX per le proprie appliance virtuali.

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

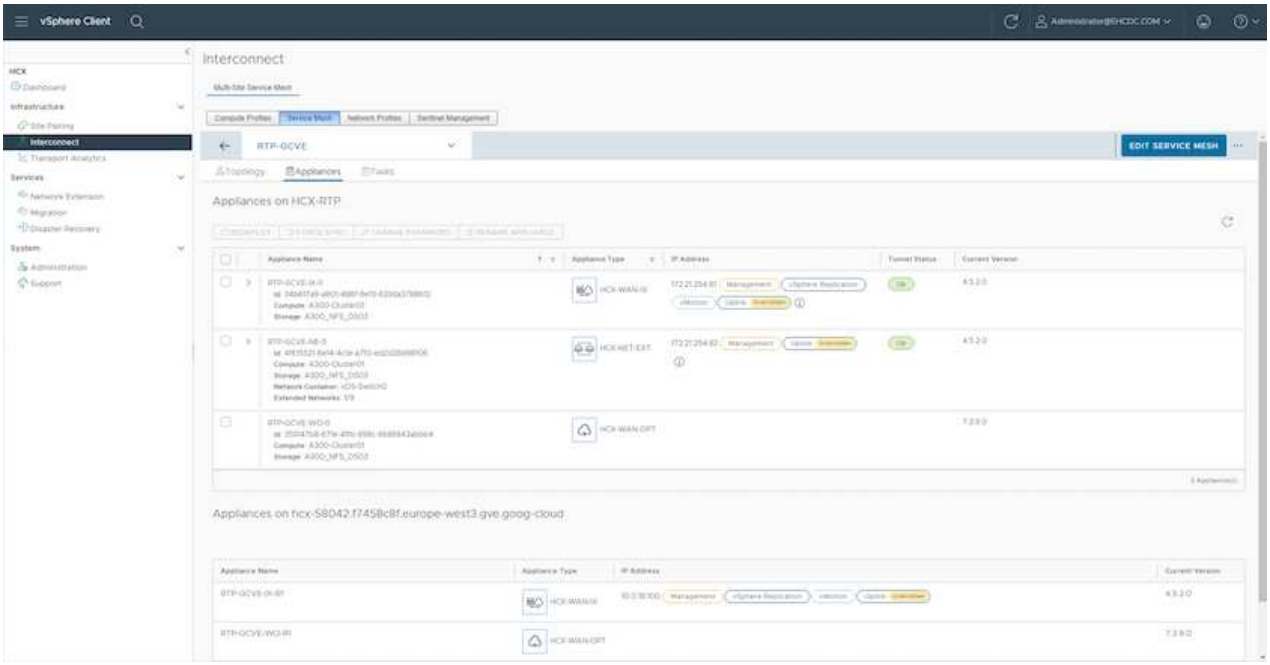


3. A questo punto, i profili di calcolo e di rete sono stati creati correttamente.
4. Creare la Service Mesh selezionando la scheda **Service Mesh** all'interno dell'opzione **Interconnect** e selezionando i siti SDDC on-premise e GCVE.
5. Service Mesh specifica una coppia di profili di rete e di calcolo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



6. 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).

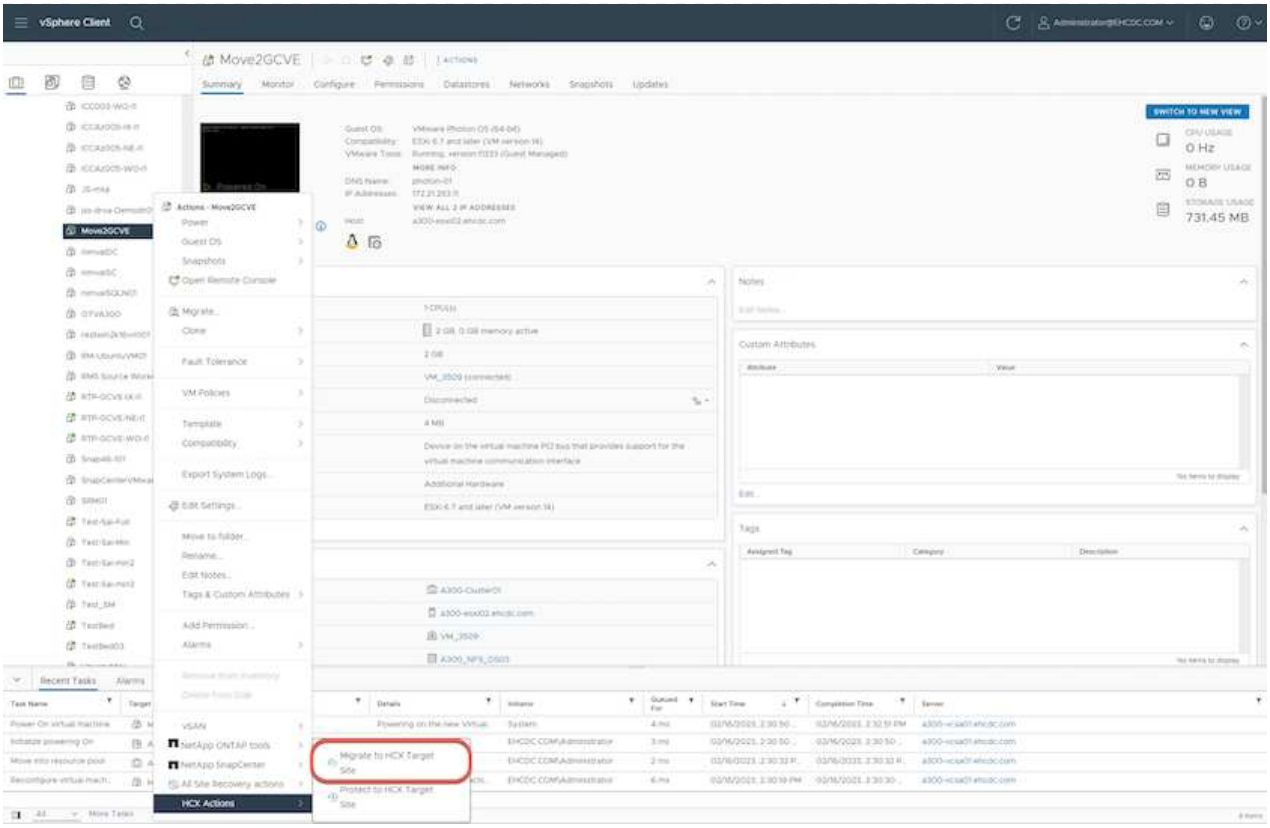
> L'appliance HCX-IX aggiunge il servizio Mobility Agent come oggetto host in vCenter Server. Il processore, la memoria, lo storage e le risorse di rete visualizzati su questo oggetto non rappresentano il consumo effettivo dell'hypervisor fisico che ospita l'appliance IX.

HCX vMotion

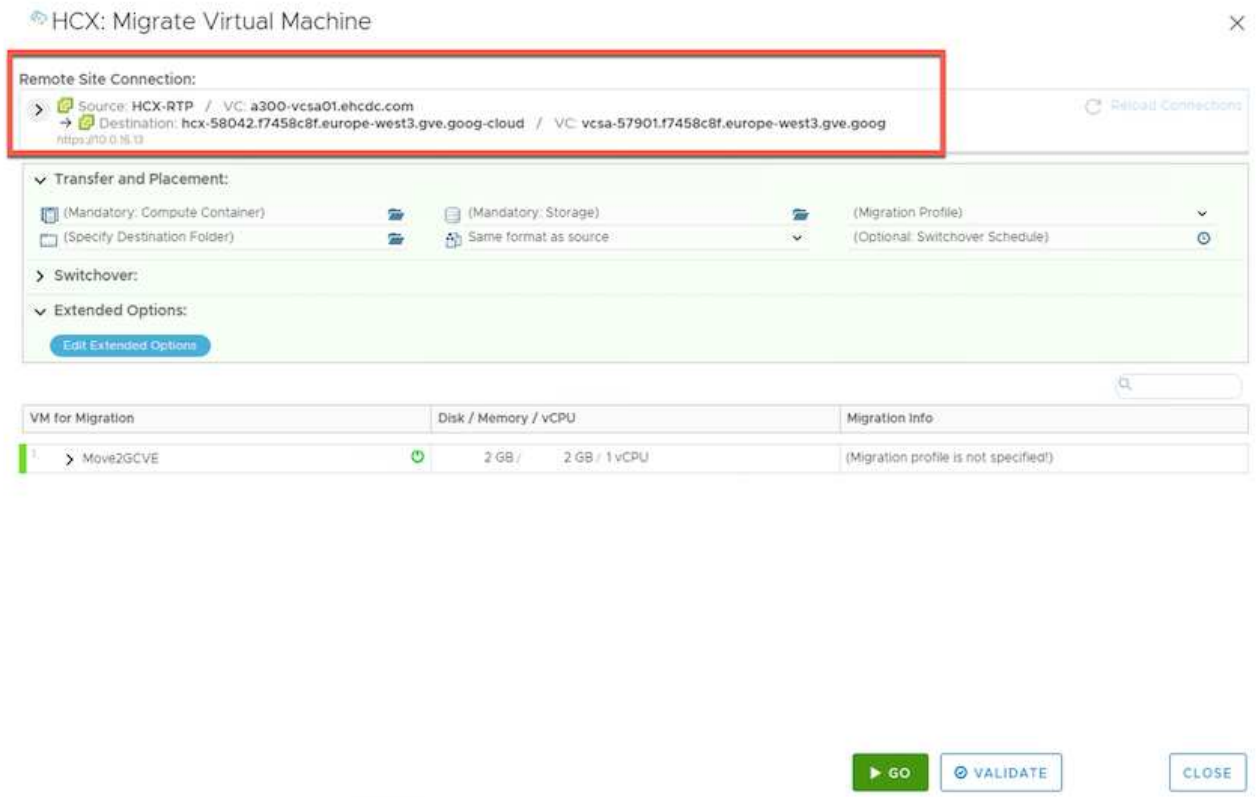
In questa sezione viene descritto il meccanismo vMotion DI HCX. Questa tecnologia di migrazione utilizza il protocollo VMware vMotion per migrare una macchina virtuale in GCVE. L'opzione di migrazione vMotion viene utilizzata per la migrazione dello stato della macchina virtuale di una singola macchina 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.

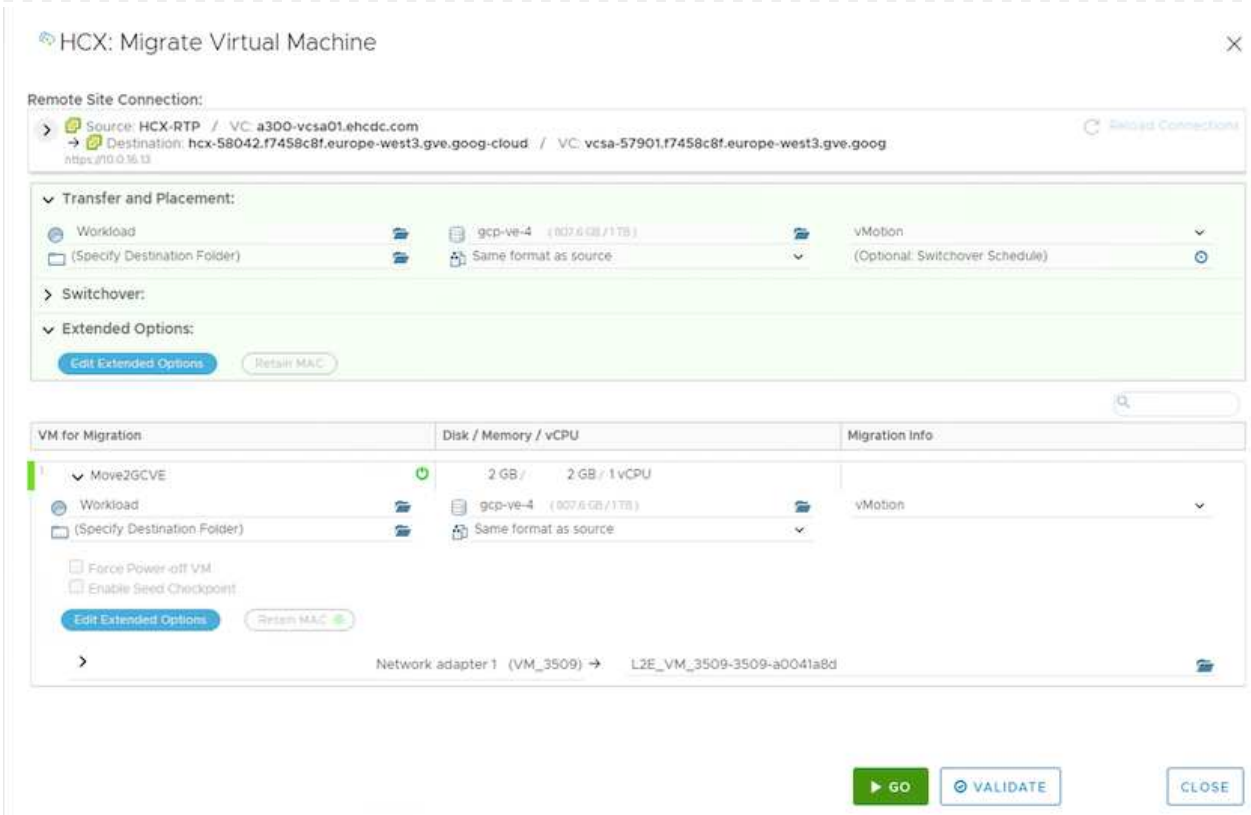
1. Dal client vSphere on-premise, accedere a Inventory (inventario), fare clic con il pulsante destro del mouse sulla macchina virtuale da migrare e selezionare HCX Actions (azioni HCX) > Migrate to HCX Target Site (Migra al sito di destinazione HCX).



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



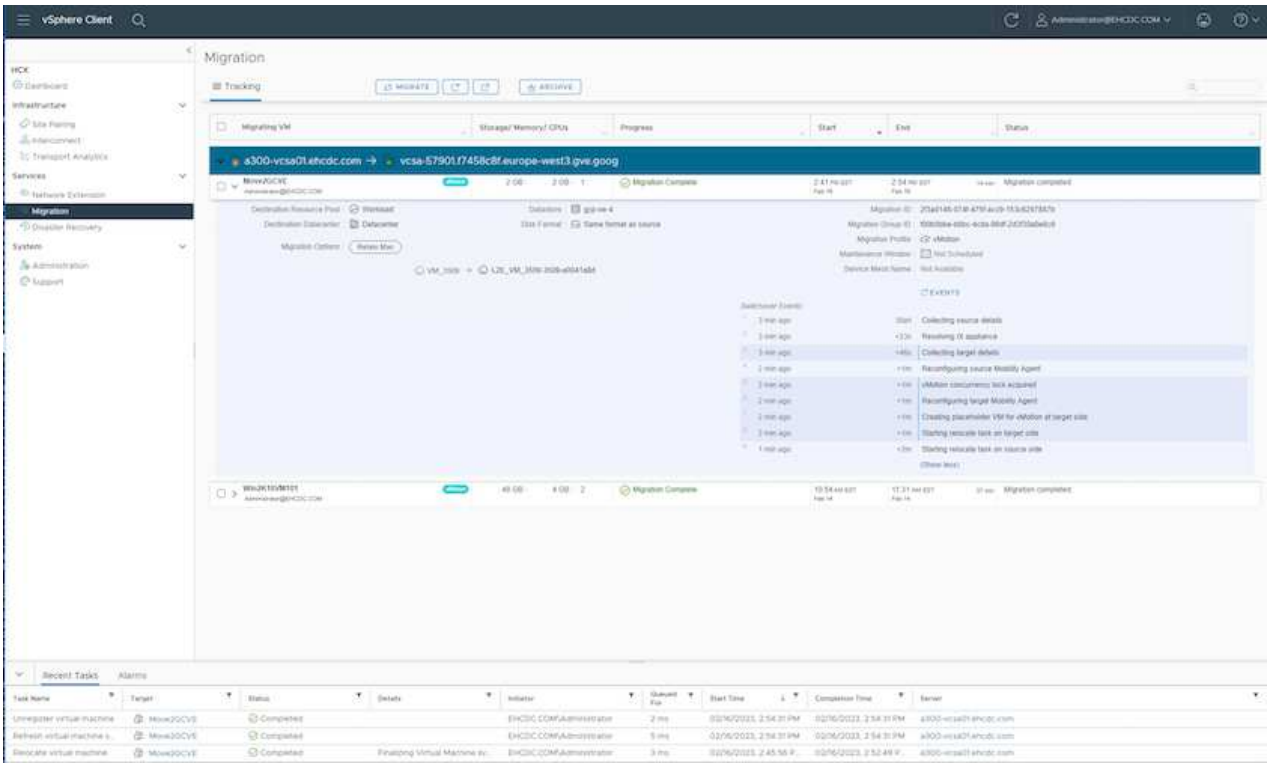
3. Aggiornare i campi obbligatori (Cluster, Storage e Destination Network), quindi fare clic su Validate (convalida).



4. 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".

5. 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"

- Documentazione Cloud Volume Service

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

- Guida utente di VMware HCX

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

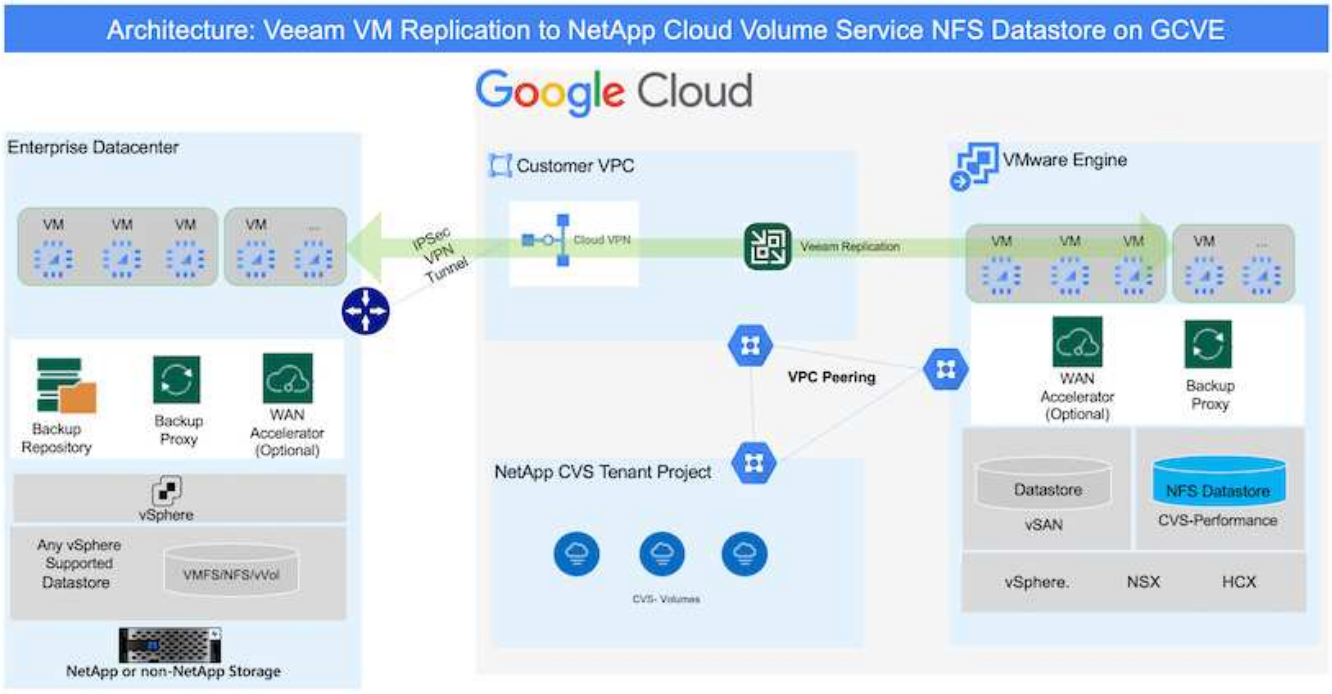
Migrazione delle macchine virtuali al servizio volumi cloud NetApp Datastore NFS su Google Cloud VMware Engine con la funzione di replica Veeam

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, Veeeam 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.

Disponibilità regionale: Datastore NFS supplementare per Google Cloud Platform (GCP)

Il datastore NFS supplementare per GCVE è supportato con il servizio volumi cloud di NetApp.

> Solo i volumi CVS-Performance possono essere utilizzati per GCVE NFS Datastore.
> Per la posizione disponibile, fare riferimento a. "Mappa geografica globale"

Google Cloud VMware Engine è disponibile presso le seguenti sedi

Per ridurre al minimo la latenza, il volume CVS di NetApp e GCVE in cui si intende montare il volume devono trovarsi nella stessa zona di disponibilità.
Collabora con gli architetti delle soluzioni Google e NetApp per ottenere le ottimizzazioni di disponibilità e TCO.

Panoramica sulla sicurezza - NetApp Cloud Volumes Service (CVS) in Google Cloud

TR-4918: Panoramica sulla sicurezza - NetApp Cloud Volumes Service in Google Cloud

Oliver Krause, Justin Parisi, NetApp

Scopo del documento

La sicurezza, in particolare nel cloud in cui l'infrastruttura non è sotto il controllo degli amministratori dello storage, è fondamentale per affidare i tuoi dati alle offerte di servizi fornite dai cloud provider. Questo documento offre una panoramica delle offerte di sicurezza offerte da NetApp "Cloud Volumes Service è disponibile in Google Cloud".

Pubblico previsto

I destinatari del presente documento includono, a titolo esemplificativo e non esaustivo, i seguenti ruoli:

- Cloud provider
- Amministratori dello storage
- Architetti dello storage
- Risorse sul campo
- Decision maker aziendali

In caso di domande sul contenuto di questo report tecnico, consulta la sezione ""Contattaci.""

Abbreviazione	Definizione
CVS-SW	Cloud Volumes Service, CVS tipo di servizio
Performance CVS	Cloud Volume Service, tipo di servizio CVS-Performance
PSA	

In che modo Cloud Volumes Service in Google Cloud protegge i tuoi dati

Cloud Volumes Service in Google Cloud offre una moltitudine di modi per proteggere in modo nativo i tuoi dati.

Architettura sicura e modello di tenancy

Cloud Volumes Service offre un'architettura sicura in Google Cloud segmentando la gestione del servizio (piano di controllo) e l'accesso ai dati (piano dati) tra diversi endpoint in modo che nessuno dei due possa influire sull'altro (vedere la sezione ""Architettura Cloud Volumes Service""). Utilizza Google "accesso ai servizi privati" (PSA) per fornire il servizio. Questo framework distingue tra il produttore di servizi, fornito e gestito da NetApp, e il consumatore di servizi, che è un cloud privato virtuale (VPC) in un progetto del cliente, che ospita i client che desiderano accedere alle condivisioni di file Cloud Volumes Service.

In questa architettura, i tenant (vedere la sezione ""Modello di tenancy"") Sono definiti come progetti Google Cloud che sono completamente isolati l'uno dall'altro, a meno che l'utente non sia esplicitamente connesso. I tenant consentono l'isolamento completo dei volumi di dati, dei servizi di nomi esterni e di altre parti essenziali della soluzione da parte di altri tenant utilizzando la piattaforma per volumi Cloud Volumes Service. Poiché la piattaforma Cloud Volumes Service è connessa tramite peering VPC, tale isolamento si applica anche ad essa.

È possibile abilitare la condivisione di volumi Cloud Volumes Service tra più progetti utilizzando un VPC condiviso (vedere la sezione ""VPC condivisi""). È possibile applicare i controlli di accesso alle condivisioni SMB e alle esportazioni NFS per limitare chi o cosa può visualizzare o modificare i set di dati.

Gestione efficace delle identità per il piano di controllo

Nel piano di controllo in cui avviene la configurazione Cloud Volumes Service, la gestione delle identità viene gestita tramite "IAM (Identity Access Management)". IAM è un servizio standard che consente di controllare l'autenticazione (accessi) e l'autorizzazione (autorizzazioni) per le istanze di progetto di Google Cloud. Tutta la configurazione viene eseguita con API Cloud Volumes Service su un trasporto HTTPS sicuro utilizzando la crittografia TLS 1.2 e l'autenticazione viene eseguita utilizzando token JWT per una maggiore sicurezza. L'interfaccia utente della console Google per Cloud Volumes Service converte l'input dell'utente in chiamate API Cloud Volumes Service.

Protezione avanzata - limita le superfici di attacco

Una parte della sicurezza effettiva consiste nel limitare il numero di superfici di attacco disponibili in un servizio. Le superfici di attacco possono includere una varietà di elementi, tra cui dati a riposo, trasferimenti in volo, accessi e set di dati stessi.

Un servizio gestito rimuove alcune delle superfici di attacco intrinsecamente nella sua progettazione. Gestione dell'infrastruttura, come descritto nella sezione ""Funzionamento del servizio"" è gestito da un team dedicato ed è automatizzato per ridurre il numero di volte in cui un umano tocca effettivamente le configurazioni, contribuendo a ridurre il numero di errori intenzionali e non intenzionali. La rete è disattivata in modo che solo i servizi necessari possano accedere l'uno all'altro. La crittografia viene inserita nello storage dei dati e solo il piano dati richiede attenzione per la sicurezza da parte degli amministratori di Cloud Volumes Service. Nascondendo la maggior parte della gestione dietro un'interfaccia API, la sicurezza viene ottenuta limitando le superfici di attacco.

Modello Zero Trust

Storicamente, la filosofia di sicurezza IT è stata quella di fidarsi, ma di verificare, e si è manifestata come affidandosi esclusivamente a meccanismi esterni (come firewall e sistemi di rilevamento delle intrusioni) per mitigare le minacce. Tuttavia, gli attacchi e le violazioni si sono evoluti per aggirare la verifica negli ambienti attraverso phishing, social engineering, minacce interne e altri metodi che forniscono la verifica per entrare nelle reti e causare caos.

Zero Trust è diventata una nuova metodologia per la sicurezza, con l'attuale mantra "fidarsi di nulla pur verificando tutto". Pertanto, per impostazione predefinita, non è consentito alcun accesso. Questo mantra viene applicato in diversi modi, tra cui firewall standard e sistemi di rilevamento delle intrusioni (IDS) e con i seguenti metodi:

- Metodi di autenticazione avanzata (ad esempio token Kerberos o JWT con crittografia AES)
- Singole fonti di identità sicure (come Windows Active Directory, Lightweight Directory Access Protocol (LDAP) e Google IAM)
- Segmentazione della rete e multi-tenancy sicura (solo i tenant possono accedere per impostazione predefinita)
- Controlli granulari degli accessi con policy di accesso con privilegi minimi
- Piccoli elenchi esclusivi di amministratori affidabili e dedicati con audit digitale e percorsi cartacei

Cloud Volumes Service eseguito in Google Cloud rispetta il modello Zero Trust implementando la posizione "Trust Nothing, Verify Everything".

Crittografia

Crittografare i dati inattivi (vedere la sezione ""Crittografia dei dati a riposo"") Utilizzando le crittografia XTS-AES-256 con NetApp Volume Encryption (NVE) e in-flight con ""Crittografia SMB"" O NFS Kerberos 5p. È facile sapere che i trasferimenti di replica tra regioni sono protetti dalla crittografia TLS 1.2 (vedere la sezione ""Replica tra regioni""). Inoltre, Google Networking fornisce anche comunicazioni crittografate (vedere la sezione ""Crittografia dei dati in transito"") per un ulteriore livello di protezione dagli attacchi. Per ulteriori informazioni sulla crittografia del trasporto, vedere la sezione ""Rete Google Cloud"".

Protezione dei dati e backup

La sicurezza non riguarda solo la prevenzione degli attacchi. Si tratta anche del modo in cui ripristiniamo gli attacchi in caso o quando si verificano. Questa strategia include backup e protezione dei dati. Cloud Volumes Service fornisce metodi per la replica in altre regioni in caso di interruzioni (vedere la sezione ""Replica tra regioni"") o se un set di dati è interessato da un attacco ransomware. Inoltre, può eseguire backup asincroni dei dati in posizioni esterne all'istanza di Cloud Volumes Service utilizzando "Backup Cloud Volumes Service". Con backup regolari, la mitigazione degli eventi di sicurezza può richiedere meno tempo e risparmiare denaro e angoscia per gli amministratori.

Riduzione rapida del ransomware con copie Snapshot leader del settore

Oltre alla protezione dei dati e ai backup, Cloud Volumes Service fornisce il supporto per copie Snapshot immutabili (vedere la sezione ""Copie Snapshot immutabili"") di volumi che consentono il ripristino da attacchi ransomware (vedere la sezione ""Funzionamento del servizio"") entro pochi secondi dalla scoperta del problema e con interruzioni minime. I tempi e gli effetti di recovery dipendono dalla pianificazione di Snapshot, ma è possibile creare copie Snapshot che forniscono solo un'ora di delta negli attacchi ransomware. Le copie Snapshot hanno un effetto trascurabile sulle performance e sull'utilizzo della capacità e rappresentano un approccio a basso rischio e con premi elevati per la protezione dei set di dati.

Considerazioni sulla sicurezza e superfici di attacco

Il primo passo per comprendere come proteggere i dati consiste nell'identificare i rischi e le potenziali superfici di attacco.

Questi includono (a titolo esemplificativo) i seguenti elementi:

- Amministrazione e accessi
- Dati inattivi
- Dati in volo
- Rete e firewall
- Ransomware, malware e virus

La comprensione delle superfici di attacco può aiutarti a proteggere meglio i tuoi ambienti. Cloud Volumes Service in Google Cloud prende già in considerazione molti di questi argomenti e implementa le funzionalità di sicurezza per impostazione predefinita, senza alcuna interazione amministrativa.

Garantire accessi sicuri

Quando si proteggono i componenti critici dell'infrastruttura, è fondamentale assicurarsi che solo gli utenti approvati possano accedere e gestire gli ambienti. Se gli attori danneggiati violano le credenziali amministrative, dispongono delle chiavi del castello e possono fare qualsiasi cosa: Modificare le configurazioni, eliminare volumi e backup, creare backdoor o disattivare le pianificazioni Snapshot.

Cloud Volumes Service per Google Cloud offre protezione dagli accessi amministrativi non autorizzati attraverso l'offuscamento dello storage come servizio (StaaS). Cloud Volumes Service è completamente gestito dal cloud provider senza alcuna disponibilità per l'accesso esterno. Tutte le operazioni di configurazione e configurazione sono completamente automatizzate, pertanto un amministratore umano non deve mai interagire con i sistemi, tranne in circostanze molto rare.

Se è necessario effettuare l'accesso, Cloud Volumes Service in Google Cloud protegge gli accessi mantenendo un elenco molto breve di amministratori attendibili che hanno accesso ai sistemi. Questo gatepeeping aiuta a ridurre il numero di potenziali attori danneggiati con accesso. Inoltre, il networking Google Cloud nasconde i sistemi dietro livelli di sicurezza di rete ed espone solo ciò che è necessario al mondo esterno. Per informazioni sull'architettura di Google Cloud e Cloud Volumes Service, consulta la sezione ""Architettura Cloud Volumes Service"."

Amministrazione e aggiornamenti dei cluster

Due aree con potenziali rischi per la sicurezza includono l'amministrazione del cluster (cosa succede se un attore cattivo ha accesso all'amministratore) e gli aggiornamenti (cosa succede se un'immagine software viene compromessa).

Protezione dell'amministrazione dello storage

Lo storage fornito come servizio elimina il rischio aggiunto di esposizione agli amministratori rimuovendo tale accesso agli utenti finali al di fuori del data center cloud. Invece, l'unica configurazione eseguita è per il piano di accesso ai dati da parte dei clienti. Ogni tenant gestisce i propri volumi e nessun tenant può raggiungere altre istanze di Cloud Volumes Service. Il servizio è gestito dall'automazione, con un elenco molto piccolo di amministratori attendibili che hanno accesso ai sistemi attraverso i processi descritti nella sezione ""Operazione di assistenza"."

Il tipo di servizio CVS-Performance offre la replica tra regioni come opzione per fornire la protezione dei dati a una regione diversa in caso di guasto di una regione. In questi casi, è possibile eseguire il failover di Cloud Volumes Service nella regione non interessata per mantenere l'accesso ai dati.

Aggiornamenti del servizio

Gli aggiornamenti aiutano a proteggere i sistemi vulnerabili. Ogni aggiornamento offre miglioramenti alla sicurezza e correzioni di bug che riducono al minimo le superfici di attacco. Gli aggiornamenti software vengono scaricati da repository centralizzati e convalidati prima che gli aggiornamenti siano autorizzati a verificare che le immagini ufficiali siano utilizzate e che gli aggiornamenti non siano compromessi dagli attori danneggiati.

Con Cloud Volumes Service, gli aggiornamenti vengono gestiti dai team dei provider di cloud, il che elimina l'esposizione ai rischi per i team di amministratori fornendo esperti con una buona esperienza nella configurazione e negli aggiornamenti che hanno automatizzato e testato completamente il processo. Gli aggiornamenti sono senza interruzioni e Cloud Volumes Service mantiene gli ultimi aggiornamenti per ottenere i migliori risultati complessivi.

Per informazioni sul team di amministratori che esegue questi aggiornamenti del servizio, vedere la sezione ""Operazione di assistenza"."

Protezione dei dati inattivi

La crittografia dei dati inattivi è importante per proteggere i dati sensibili in caso di furto, restituzione o riordinamento di un disco. I dati in Cloud Volumes Service sono protetti a riposo utilizzando la crittografia basata su software.

- Le chiavi generate da Google vengono utilizzate per CVS-SW.
- Per CVS-Performance, le chiavi per volume vengono memorizzate in un gestore di chiavi integrato in Cloud Volumes Service, che utilizza NetApp ONTAP CryptoMod per generare chiavi di crittografia AES-256. CryptoMod è elencato nell'elenco dei moduli validati di CMVP FIPS 140-2. Vedere "FIPS 140-2 Cert n. 4144".

A partire da novembre 2021, l'anteprima della funzionalità Customer-Managed Encryption (CMEK) è stata resa disponibile per CVS-Performance. Questa funzionalità consente di crittografare le chiavi per volume con chiavi master per progetto, per regione, ospitate in Google Key Management Service (KMS). KMS consente di collegare i key manager esterni.

Per ulteriori informazioni su come configurare KMS per CVS-Performance, "Consultare la documentazione di Cloud Volumes Service".

Per ulteriori informazioni sull'architettura, vedere la sezione ""Architettura Cloud Volumes Service"."

Protezione dei dati in volo

Oltre a proteggere i dati a riposo, è necessario essere in grado di proteggere i dati anche quando sono in volo tra l'istanza di Cloud Volumes Service e un client o una destinazione di replica. Cloud Volumes Service fornisce la crittografia per i dati in-flight su protocolli NAS utilizzando metodi di crittografia come la crittografia SMB utilizzando Kerberos, la firma/sigillatura dei pacchetti e NFS Kerberos 5p per la crittografia end-to-end dei trasferimenti di dati.

La replica dei volumi Cloud Volumes Service utilizza TLS 1.2, che sfrutta i metodi di crittografia AES-GCM.

La maggior parte dei protocolli insicuri in-flight, come telnet, NDMP e così via, sono disattivati per impostazione predefinita. Il DNS, tuttavia, non viene crittografato da Cloud Volumes Service (non supporta il DNS sec) e deve essere crittografato utilizzando la crittografia di rete esterna, se possibile. Vedere la sezione ""Crittografia dei dati in transito"" per ulteriori informazioni sulla protezione dei dati in volo.

Per informazioni sulla crittografia del protocollo NAS, vedere la sezione ""Protocolli NAS"."

Utenti e gruppi per le autorizzazioni NAS

Parte della protezione dei dati nel cloud implica un'autenticazione corretta di utenti e gruppi, in cui gli utenti che accedono ai dati vengono verificati come utenti reali nell'ambiente e i gruppi contengono utenti validi. Questi utenti e gruppi forniscono l'accesso iniziale alla condivisione e all'esportazione, nonché la convalida delle autorizzazioni per file e cartelle nel sistema di storage.

Cloud Volumes Service utilizza l'autenticazione standard di utenti e gruppi basata su Active Directory per le condivisioni SMB e le autorizzazioni di tipo Windows. Il servizio può anche sfruttare i provider di identità UNIX come LDAP per utenti e gruppi UNIX per le esportazioni NFS, la convalida dell'ID NFSv4, l'autenticazione Kerberos e gli ACL NFSv4.

Attualmente solo Active Directory LDAP è supportato con la funzionalità Cloud Volumes Service per LDAP.

Rilevamento, prevenzione e mitigazione di ransomware, malware e virus

Ransomware, malware e virus sono una minaccia persistente per gli amministratori e il rilevamento, la prevenzione e la mitigazione di tali minacce sono sempre in cima alla mente per le organizzazioni aziendali. Un singolo evento ransomware su un set di dati critico può potenzialmente costare milioni di dollari, quindi è utile fare ciò che è possibile per ridurre al minimo il rischio.

Sebbene Cloud Volumes Service attualmente non includa misure di rilevamento o prevenzione native, come la protezione antivirus o. "rilevamento automatico ransomware", Esistono diversi modi per eseguire rapidamente il ripristino da un evento ransomware attivando pianificazioni Snapshot regolari. Le copie Snapshot sono immutabili e i puntatori di sola lettura ai blocchi modificati nel file system, sono quasi istantanei, hanno un impatto minimo sulle performance e occupano spazio solo quando i dati vengono modificati o cancellati. È possibile impostare le pianificazioni per le copie Snapshot in modo che corrispondano all'obiettivo RPO (Acceptable Recovery Point Objective)/RTO (Recovery Time Objective) desiderato e mantenere fino a 1,024 copie Snapshot per volume.

Il supporto di Snapshot è incluso senza costi aggiuntivi (al di là dei costi di storage dei dati per blocchi modificati/dati conservati dalle copie Snapshot) con Cloud Volumes Service e, in caso di attacco ransomware, può essere utilizzato per eseguire il rollback su una copia Snapshot prima che si verifichi l'attacco. Il completamento dei ripristini Snapshot richiede pochi secondi e consente di tornare alla normale gestione dei dati. Per ulteriori informazioni, vedere "La soluzione NetApp per ransomware".

Per evitare che il ransomware influisca sul tuo business, è necessario un approccio multilivello che includa uno o più dei seguenti elementi:

- Protezione degli endpoint
- Protezione dalle minacce esterne attraverso firewall di rete
- Rilevamento di anomalie dei dati
- Backup multipli (on-site e off-site) di set di dati critici
- Test di ripristino regolari dei backup
- Copie Snapshot di NetApp immutabili in sola lettura
- Autenticazione a più fattori per infrastrutture critiche
- Controlli di sicurezza degli accessi al sistema

Questo elenco è lungi dall'essere esaustivo, ma è un buon modello da seguire quando si affronta il potenziale degli attacchi ransomware. Cloud Volumes Service in Google Cloud offre diversi modi per proteggere da eventi ransomware e ridurre i loro effetti.

Copie Snapshot immutabili

Cloud Volumes Service fornisce in modo nativo copie Snapshot immutabili in sola lettura, eseguite in base a una pianificazione personalizzabile per un rapido ripristino point-in-time in caso di eliminazione dei dati o se un intero volume è stato vittima di un attacco ransomware. I ripristini Snapshot delle copie Snapshot precedenti sono rapidi e riducono al minimo la perdita di dati in base al periodo di conservazione delle pianificazioni Snapshot e RTO/RPO. L'effetto delle performance con la tecnologia Snapshot è trascurabile.

Poiché le copie Snapshot in Cloud Volumes Service sono di sola lettura, non possono essere infettate dal ransomware a meno che il ransomware non sia proliferato nel dataset senza essere stato notato e siano state acquisite copie Snapshot dei dati infettati dal ransomware. Per questo motivo è necessario considerare anche il rilevamento ransomware in base alle anomalie dei dati. Cloud Volumes Service non fornisce attualmente il rilevamento nativo, ma è possibile utilizzare un software di monitoraggio esterno.

Backup e ripristini

Cloud Volumes Service offre funzionalità di backup standard del client NAS (ad esempio backup su NFS o SMB).

- CVS-Performance offre replica di volumi cross-region ad altri volumi CVS-Performance. Per ulteriori

informazioni, vedere "replica di un volume" Nella documentazione di Cloud Volumes Service.

- CVS-SW offre funzionalità di backup/ripristino dei volumi native del servizio. Per ulteriori informazioni, vedere "backup nel cloud" Nella documentazione di Cloud Volumes Service.

La replica dei volumi fornisce una copia esatta del volume di origine per un failover rapido in caso di disastro, inclusi gli eventi ransomware.

Replica tra regioni

CVS-Performance consente di replicare in modo sicuro i volumi nelle aree di Google Cloud per la protezione dei dati e archiviare i casi di utilizzo utilizzando la crittografia TLS1.2 AES 256 GCM su una rete di servizi back-end controllata da NetApp utilizzando interfacce specifiche utilizzate per la replica in esecuzione sulla rete di Google. Un volume primario (di origine) contiene i dati di produzione attivi e replica su un volume secondario (di destinazione) per fornire una replica esatta del dataset primario.

La replica iniziale trasferisce tutti i blocchi, ma gli aggiornamenti trasmettono solo i blocchi modificati in un volume primario. Ad esempio, se un database da 1 TB che risiede su un volume primario viene replicato nel volume secondario, nella replica iniziale viene trasferito 1 TB di spazio. Se il database contiene poche centinaia di righe (ipoteticamente, alcuni MB) che cambiano tra l'inizializzazione e il successivo aggiornamento, solo i blocchi con le righe modificate vengono replicati nel secondario (alcuni MB). In questo modo è possibile garantire che i tempi di trasferimento rimangano bassi e che gli addebiti di replica siano ridotti.

Tutte le autorizzazioni su file e cartelle vengono replicate nel volume secondario, ma le autorizzazioni di accesso alla condivisione (come criteri e regole di esportazione o condivisioni SMB e ACL di condivisione) devono essere gestite separatamente. In caso di failover di un sito, il sito di destinazione deve sfruttare gli stessi name service e le connessioni di dominio Active Directory per fornire una gestione coerente delle identità e delle autorizzazioni di utenti e gruppi. È possibile utilizzare un volume secondario come destinazione di failover in caso di disastro interrompendo la relazione di replica, che converte il volume secondario in lettura/scrittura.

Le repliche dei volumi sono di sola lettura, che fornisce una copia immutabile dei dati fuori sede per un rapido ripristino dei dati nei casi in cui un virus ha infettato i dati o ransomware ha crittografato il dataset primario. I dati di sola lettura non vengono crittografati, ma se il volume primario viene compromesso e si verifica la replica, anche i blocchi infetti vengono replicati. È possibile utilizzare copie Snapshot meno recenti e non interessate per il ripristino, ma gli SLA potrebbero non rientrare nell'intervallo dell'RTO/RPO promesso a seconda della velocità con cui viene rilevato un attacco.

Inoltre, puoi prevenire azioni amministrative dannose, come eliminazioni di volumi, eliminazioni Snapshot o modifiche di pianificazione Snapshot, con la gestione della replica cross-region (CRR) in Google Cloud. Ciò avviene creando ruoli personalizzati che separano gli amministratori dei volumi, che possono eliminare i volumi di origine ma non interrompere i mirror e quindi non eliminare i volumi di destinazione, dagli amministratori CRR, che non possono eseguire alcuna operazione sui volumi. Vedere "Considerazioni sulla sicurezza" Nella documentazione di Cloud Volumes Service per le autorizzazioni consentite da ciascun gruppo di amministratori.

Backup Cloud Volumes Service

Sebbene Cloud Volumes Service offra un'elevata durata dei dati, gli eventi esterni possono causare la perdita di dati. In caso di eventi di sicurezza come virus o ransomware, i backup e i ripristini diventano critici per la ripresa dell'accesso ai dati in modo tempestivo. Un amministratore potrebbe eliminare accidentalmente un volume Cloud Volumes Service. In alternativa, gli utenti vogliono semplicemente conservare le versioni di backup dei propri dati per molti mesi e mantenere lo spazio di copia Snapshot aggiuntivo all'interno del volume diventa una sfida in termini di costi. Sebbene le copie Snapshot siano il modo migliore per conservare le

versioni di backup delle ultime settimane per ripristinare i dati persi, sono contenute all'interno del volume e vengono perse se il volume scompare.

Per tutti questi motivi, NetApp Cloud Volumes Service offre servizi di backup tramite "Backup Cloud Volumes Service".

Il backup di Cloud Volumes Service genera una copia del volume su Google Cloud Storage (GCS). Esegue il backup solo dei dati effettivi memorizzati nel volume, non dello spazio libero. Funziona come incrementale per sempre, il che significa che trasferisce il contenuto del volume una volta e da lì continua a eseguire il backup solo dei dati modificati. Rispetto ai classici concetti di backup con più backup completi, consente di risparmiare grandi quantità di storage di backup, riducendo i costi. Poiché il prezzo mensile dello spazio di backup è inferiore rispetto a un volume, è il posto ideale per mantenere le versioni di backup più a lungo.

Gli utenti possono utilizzare un backup Cloud Volumes Service per ripristinare qualsiasi versione di backup sullo stesso volume o su un volume diverso all'interno della stessa regione. Se il volume di origine viene cancellato, i dati di backup vengono conservati e devono essere gestiti (ad esempio, eliminati) in modo indipendente.

Il backup Cloud Volumes Service è integrato in Cloud Volumes Service come opzione. Gli utenti possono decidere quali volumi proteggere attivando il backup Cloud Volumes Service per volume. Vedere "Documentazione di backup di Cloud Volumes Service" per informazioni sui backup, consultare "numero massimo di versioni di backup supportate", pianificazione e. "prezzi".

Tutti i dati di backup di un progetto vengono memorizzati all'interno di un bucket GCS, gestito dal servizio e non visibile all'utente. Ogni progetto utilizza un bucket diverso. Attualmente, i bucket si trovano nella stessa regione dei volumi Cloud Volumes Service, ma sono in corso di discussione ulteriori opzioni. Consultare la documentazione per conoscere lo stato più recente.

Il trasporto dei dati da un bucket Cloud Volumes Service a GCS utilizza reti Google interne al servizio con HTTPS e TLS1.2. I dati vengono crittografati a riposo con chiavi gestite da Google.

Per gestire il backup Cloud Volumes Service (creazione, eliminazione e ripristino dei backup), un utente deve disporre di "roles/netappclodvolumes.admin" ruolo.

Architettura

Panoramica

Parte dell'affidabilità di una soluzione cloud è la comprensione dell'architettura e del modo in cui è protetta. In questa sezione vengono descritti diversi aspetti dell'architettura Cloud Volumes Service di Google per ridurre i potenziali problemi relativi alla protezione dei dati, nonché le aree in cui potrebbero essere necessarie ulteriori procedure di configurazione per ottenere un'implementazione più sicura.

L'architettura generale di Cloud Volumes Service può essere suddivisa in due componenti principali: Il piano di controllo e il piano dati.

Piano di controllo

Il piano di controllo di Cloud Volumes Service è l'infrastruttura di back-end gestita dagli amministratori Cloud Volumes Service e dal software di automazione nativo NetApp. Questo piano è completamente trasparente per gli utenti finali e include networking, hardware per lo storage, aggiornamenti software e così via per contribuire a fornire valore a una soluzione residente nel cloud come Cloud Volumes Service.

Piano dati

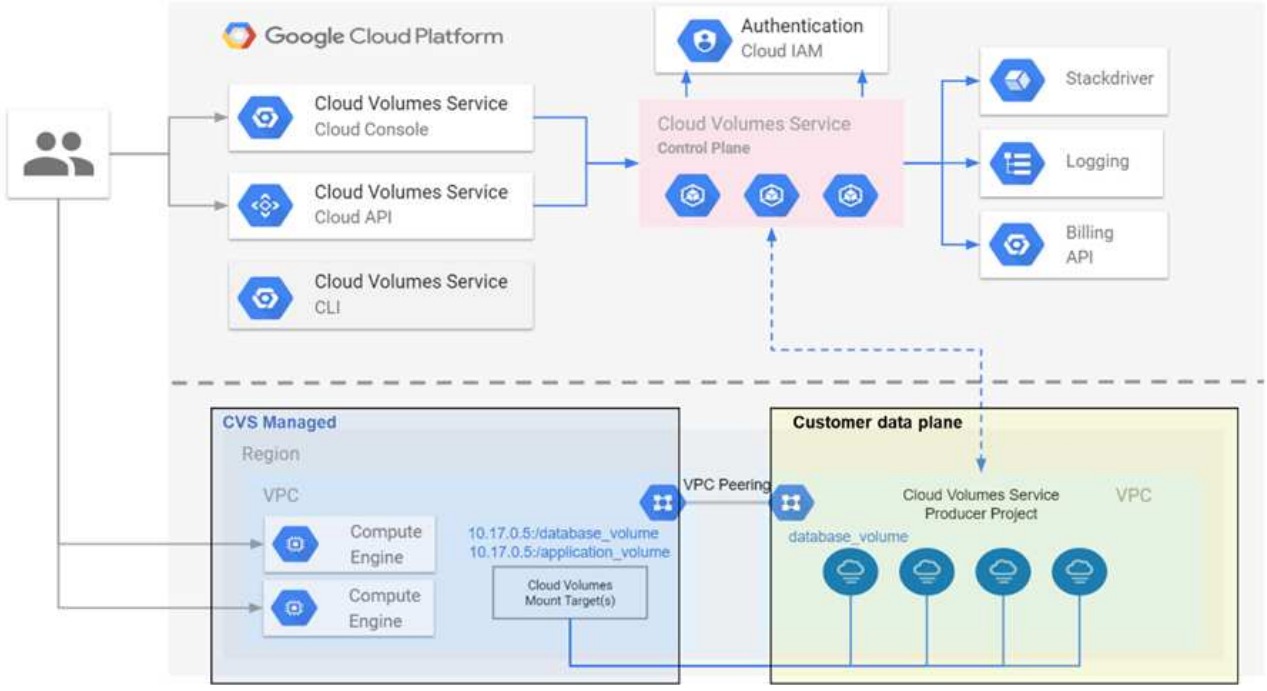
Il piano dati di Cloud Volumes Service include i volumi di dati effettivi e la configurazione generale di Cloud Volumes Service (ad esempio controllo degli accessi, autenticazione Kerberos e così via). Il data plane è interamente sotto il controllo degli utenti finali e dei consumatori della piattaforma Cloud Volumes Service.

Esistono differenze distinte nel modo in cui ciascun piano viene protetto e gestito. Le seguenti sezioni illustrano queste differenze, a partire da una panoramica dell'architettura Cloud Volumes Service.

Architettura Cloud Volumes Service

In modo simile ad altri servizi nativi di Google Cloud come CloudSQL, Google Cloud VMware Engine (GCVE) e FileStore, Cloud Volumes Service utilizza "PSA di Google" per fornire il servizio. In PSA, i servizi sono costruiti all'interno di un progetto di service Producer, che utilizza "Peering della rete VPC" per connettersi al cliente del servizio. Il produttore del servizio viene fornito e gestito da NetApp e il consumatore del servizio è un VPC in un progetto del cliente, che ospita i client che desiderano accedere alle condivisioni di file Cloud Volumes Service.

La figura seguente, a cui si fa riferimento da "sezione architettura" Della documentazione di Cloud Volumes Service, mostra una vista di alto livello.



La parte sopra la linea tratteggiata mostra il piano di controllo del servizio, che controlla il ciclo di vita del volume. La parte sotto la linea tratteggiata mostra il piano dati. La casella blu a sinistra rappresenta l'utente VPC (consumatore di servizi), la casella blu a destra rappresenta il produttore di servizi fornito da NetApp. Entrambi sono connessi tramite peering VPC.

Modello di tenancy

In Cloud Volumes Service, i singoli progetti sono considerati locatari unici. Ciò significa che la manipolazione di

volumi, copie Snapshot e così via viene eseguita in base al progetto. In altre parole, tutti i volumi sono di proprietà del progetto in cui sono stati creati e solo quel progetto può gestire e accedere ai dati all'interno di essi per impostazione predefinita. Questa è considerata la vista del piano di controllo del servizio.

VPC condivisi

Nella vista del piano dati, Cloud Volumes Service può connettersi a un VPC condiviso. È possibile creare volumi nel progetto di hosting o in uno dei progetti di servizio connessi al VPC condiviso. Tutti i progetti (host o servizio) connessi a quel VPC condiviso sono in grado di raggiungere i volumi a livello di rete (TCP/IP). Poiché tutti i client con connettività di rete sul VPC condiviso possono potenzialmente accedere ai dati attraverso protocolli NAS, il controllo dell'accesso sul singolo volume (come gli elenchi di controllo dell'accesso utente/gruppo (ACL) e i nomi host/indirizzi IP per le esportazioni NFS) deve essere utilizzato per controllare chi può accedere ai dati.

È possibile collegare Cloud Volumes Service a un massimo di cinque VPC per progetto del cliente. Sul piano di controllo, il progetto consente di gestire tutti i volumi creati, indipendentemente dal VPC a cui sono collegati. Sul piano dati, i VPC sono isolati l'uno dall'altro e ciascun volume può essere collegato solo a un VPC.

L'accesso ai singoli volumi è controllato da meccanismi di controllo degli accessi specifici del protocollo (NFS/SMB).

In altre parole, a livello di rete, tutti i progetti connessi al VPC condiviso sono in grado di vedere il volume, mentre, dal lato di gestione, il piano di controllo consente solo al progetto proprietario di vedere il volume.

Controlli del servizio VPC

I controlli dei servizi VPC stabiliscono un perimetro di controllo degli accessi intorno ai servizi Google Cloud collegati a Internet e accessibili in tutto il mondo. Questi servizi forniscono il controllo degli accessi attraverso le identità degli utenti, ma non possono limitare le richieste di posizione di rete da cui provengono. I controlli dei servizi VPC colmano questa lacuna introducendo le funzionalità per limitare l'accesso a reti definite.

Il piano dati Cloud Volumes Service non è connesso a Internet esterno ma a VPC privati con confini di rete ben definiti (perimetri). All'interno di tale rete, ciascun volume utilizza il controllo degli accessi specifico del protocollo. Qualsiasi connettività di rete esterna viene creata esplicitamente dagli amministratori di progetto di Google Cloud. Il piano di controllo, tuttavia, non fornisce le stesse protezioni del piano dati e può essere utilizzato da chiunque disponga di credenziali valide ("Token JWT").

In breve, il data plane Cloud Volumes Service offre la funzionalità di controllo dell'accesso alla rete, senza il requisito di supportare i controlli dei servizi VPC e non utilizza esplicitamente i controlli dei servizi VPC.

Considerazioni su sniffing/trace dei pacchetti

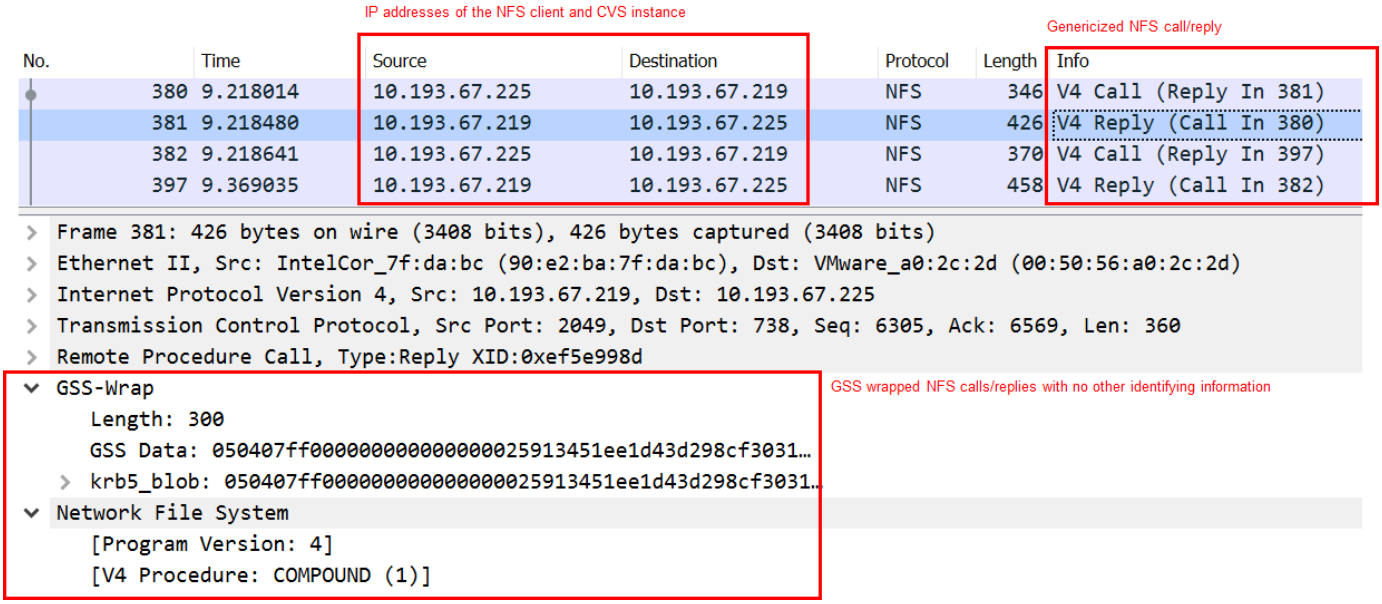
Le acquisizioni di pacchetti possono essere utili per la risoluzione di problemi di rete o di altro tipo (come permessi NAS, connettività LDAP e così via), ma possono anche essere utilizzate in modo malizioso per ottenere informazioni su indirizzi IP di rete, indirizzi MAC, nomi di utenti e gruppi e sul livello di sicurezza utilizzato sugli endpoint. A causa del modo in cui vengono configurate le regole di rete, VPC e firewall di Google Cloud, l'accesso indesiderato ai pacchetti di rete dovrebbe essere difficile da ottenere senza le credenziali di accesso dell'utente o. "Token JWT" nelle istanze cloud. Le acquisizioni di pacchetti sono possibili solo sugli endpoint (ad esempio macchine virtuali) e solo sugli endpoint interni al VPC, a meno che non venga utilizzato un VPC condiviso e/o un tunnel di rete esterno/inoltro IP per consentire esplicitamente il traffico esterno agli endpoint. Non esiste alcun modo per eseguire lo sniff del traffico al di fuori dei client.

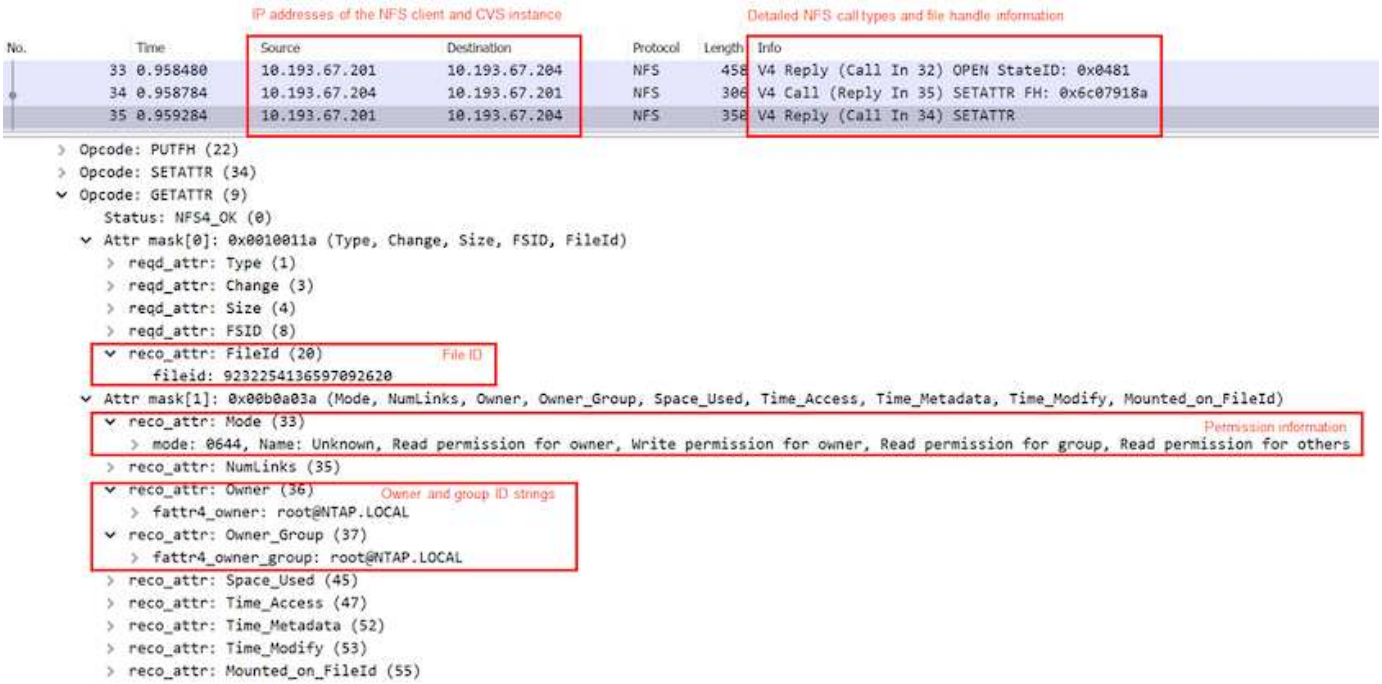
Quando si utilizzano VPC condivisi, la crittografia in-flight con NFS Kerberos e/o "Crittografia SMB" può mascherare gran parte delle informazioni raccolte dalle tracce. Tuttavia, parte del traffico viene ancora inviato in formato non crittografato, ad esempio "DNS" e. "Query LDAP". La figura seguente mostra un'acquisizione di

pacchetti da una query LDAP non crittografata proveniente da Cloud Volumes Service e le potenziali informazioni di identificazione esposte. Le query LDAP in Cloud Volumes Service attualmente non supportano la crittografia o LDAP su SSL. CVS-Performance supporta la firma LDAP, se richiesto da Active Directory. CVS-SW non supporta la firma LDAP.

UnixUserPassword viene interrogata da LDAP e non viene inviata in testo non crittografato, ma in un hash con salatura. Per impostazione predefinita, Windows LDAP non compila i campi unixUserPassword. Questo campo è necessario solo se è necessario sfruttare Windows LDAP per gli accessi interattivi tramite LDAP ai client. Cloud Volumes Service non supporta gli accessi LDAP interattivi alle istanze.

La figura seguente mostra un'acquisizione di pacchetti da una conversazione Kerberos NFS accanto a un'acquisizione di NFS su AUTH_SYS. Si noti come le informazioni disponibili in una traccia siano diverse tra le due e come l'abilitazione della crittografia in-flight offra una maggiore sicurezza generale per il traffico NAS.





Interfacce di rete delle macchine virtuali

Un trucco che gli autori degli attacchi potrebbero tentare di aggiungere una nuova scheda di interfaccia di rete (NIC) a una macchina virtuale in "modalità promiscua" (Mirroring delle porte) o attivare la modalità promiscua su una scheda di rete esistente per eseguire lo sniff di tutto il traffico. In Google Cloud, l'aggiunta di una nuova NIC richiede l'arresto completo di una macchina virtuale, che crea avvisi, in modo che gli hacker non possano farlo inosservato.

Inoltre, le NIC non possono essere impostate sulla modalità promiscua e attiveranno avvisi in Google Cloud.

Architettura del piano di controllo

Tutte le azioni di gestione di Cloud Volumes Service vengono eseguite tramite API. La gestione Cloud Volumes Service integrata nella console cloud GCP utilizza anche l'API Cloud Volumes Service.

Gestione di identità e accessi

Gestione di identità e accessi ("IAM") È un servizio standard che consente di controllare l'autenticazione (accessi) e l'autorizzazione (autorizzazioni) per le istanze di progetto di Google Cloud. Google IAM offre un audit trail completo delle autorizzazioni di autorizzazione e rimozione. Attualmente Cloud Volumes Service non fornisce il controllo del piano di controllo.

Panoramica delle autorizzazioni

IAM offre permessi granulari integrati per Cloud Volumes Service. È possibile trovare un "completa l'elenco delle autorizzazioni granulari qui".

IAM offre anche due ruoli predefiniti chiamati `netappcloudvolumes.admin` e. `netappcloudvolumes.viewer`. Questi ruoli possono essere assegnati a specifici utenti o account di servizio.

Assegnare ruoli e autorizzazioni appropriati per consentire agli utenti IAM di gestire Cloud Volumes Service.

Di seguito sono riportati alcuni esempi di utilizzo delle autorizzazioni granulari:

- Creare un ruolo personalizzato con solo autorizzazioni Get/List/create/Update in modo che gli utenti non possano eliminare i volumi.
- Utilizzare un ruolo personalizzato solo con `snapshot.*` Autorizzazioni per creare un account di servizio utilizzato per creare un'integrazione Snapshot coerente con l'applicazione.
- Creare un ruolo personalizzato da delegare `volumereplication.*` a utenti specifici.

Account di servizio

Per effettuare chiamate API Cloud Volumes Service tramite script o. "Terraform", è necessario creare un account di servizio con `roles/netappcloudvolumes.admin` ruolo. È possibile utilizzare questo account di servizio per generare i token JWT necessari per autenticare le richieste API Cloud Volumes Service in due modi diversi:

- Generare una chiave JSON e utilizzare le API di Google per derivare un token JWT da essa. Questo è l'approccio più semplice, ma implica la gestione manuale dei segreti (la chiave JSON).
- Utilizzare "Rappresentazione dell'account di servizio" con `roles/iam.serviceAccountTokenCreator`. Il codice (script, Terraform e così via). funziona con "Credenziali predefinite dell'applicazione" e rappresenta l'account del servizio per ottenere le autorizzazioni. Questo approccio riflette le Best practice di sicurezza di Google.

Vedere "Creazione dell'account di servizio e della chiave privata" Nella documentazione di Google Cloud per ulteriori informazioni.

API Cloud Volumes Service

L'API Cloud Volumes Service utilizza un'API basata SU REST utilizzando HTTPS (TLSv1.2) come trasporto di rete sottostante. È possibile trovare la definizione API più recente "qui" E informazioni su come utilizzare l'API all'indirizzo "Cloud Volumes API nella documentazione cloud di Google".

L'endpoint API viene gestito e protetto da NetApp utilizzando la funzionalità HTTPS standard (TLSv1.2).

Token JWT

L'autenticazione all'API viene eseguita con token bearer JWT ("RFC-7519"). I token JWT validi devono essere ottenuti utilizzando l'autenticazione IAM di Google Cloud. A tale scopo, è necessario recuperare un token da IAM fornendo una chiave JSON dell'account di servizio.

Registrazione dell'audit

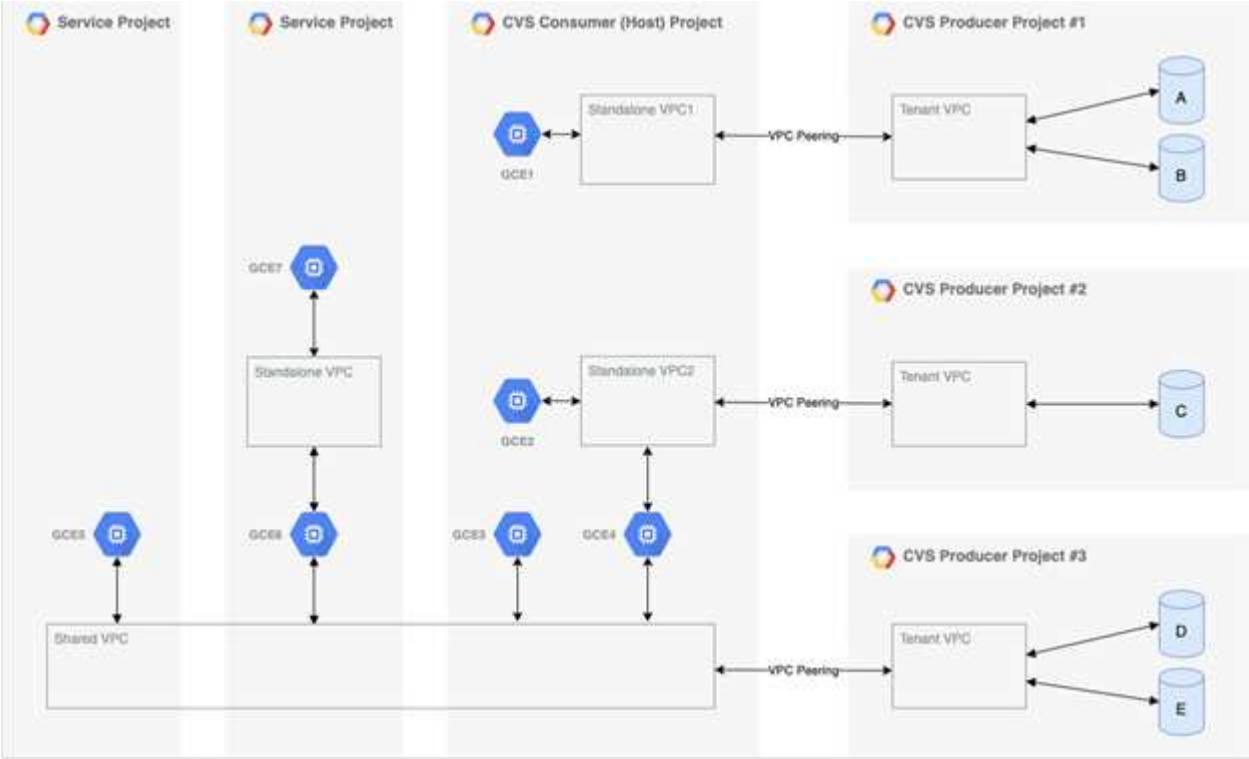
Attualmente, non sono disponibili registri di audit del piano di controllo accessibili dall'utente.

Architettura del data plane

Cloud Volumes Service per Google Cloud sfrutta Google Cloud "accesso ai servizi privati" framework. In questo framework, gli utenti possono connettersi a Cloud Volumes Service. Questo framework utilizza i costrutti di peering di Service Networking e VPC come altri servizi Google Cloud, garantendo un isolamento completo tra i tenant.

Per una panoramica dell'architettura di Cloud Volumes Service per Google Cloud, consulta "Architettura per Cloud Volumes Service".

Le VPC degli utenti (standalone o condiviso) vengono collegate ai VPC all'interno dei progetti di tenant gestiti da Cloud Volumes Service, che ospitano i volumi.



La figura precedente mostra un progetto (il progetto consumer CVS al centro) con tre reti VPC collegate a Cloud Volumes Service e più macchine virtuali del motore di calcolo (GCE1-7) che condividono volumi:

- VPC1 consente a GCE1 di accedere ai volumi A e B.
- VPC2 consente a GCE2 e GCE4 di accedere al volume C.
- La terza rete VPC è un VPC condiviso, condiviso con due progetti di servizio. Consente a GCE3, GCE4, GCE5 e GCE6 di accedere ai volumi D ed E. Le reti VPC condivise sono supportate solo per volumi del tipo di servizio CVS-Performance.

GCE7 non può accedere ad alcun volume.

I dati possono essere crittografati sia in transito (utilizzando la crittografia Kerberos e/o SMB) che a riposo in Cloud Volumes Service.

Crittografia dei dati in transito

I dati in transito possono essere crittografati a livello di protocollo NAS e la rete Google Cloud stessa viene crittografata, come descritto nelle sezioni seguenti.

Rete Google Cloud

Google Cloud crittografa il traffico a livello di rete come descritto in "Crittografia in transito" Nella documentazione di Google. Come indicato nella sezione "architettura dei servizi cloud Volumes", Cloud Volumes Service viene fornito da un progetto di produttore PSA controllato da NetApp.

Nel caso di CVS-SW, il tenant produttore esegue Google VM per fornire il servizio. Il traffico tra le macchine

virtuali dell'utente e le macchine virtuali Cloud Volumes Service viene crittografato automaticamente da Google.

Sebbene il percorso dei dati per CVS-Performance non sia completamente crittografato sul layer di rete, NetApp e Google utilizzano una combinazione "Di crittografia IEEE 802.1AE (MACsec)", "incapsulamento" (Crittografia dei dati) e reti con restrizioni fisiche per proteggere i dati in transito tra il tipo di servizio CVS-Performance di Cloud Volumes Service e Google Cloud.

Protocolli NAS

I protocolli NAS NFS e SMB forniscono una crittografia opzionale per il trasporto a livello di protocollo.

Crittografia SMB

"Crittografia SMB" Fornisce la crittografia end-to-end dei dati SMB e protegge i dati da eventi di intercettazione su reti non attendibili. È possibile attivare la crittografia sia per la connessione dati client/server (disponibile solo per i client compatibili con SMB3.x) che per l'autenticazione del server/controller di dominio.

Quando la crittografia SMB è attivata, i client che non supportano la crittografia non possono accedere alla condivisione.

Cloud Volumes Service supporta le crittografie di sicurezza RC4-HMAC, AES-128-CTS-HMAC-SHA1 e AES-256-CTS-HMAC-SHA1 per la crittografia SMB. SMB negozia con il tipo di crittografia più elevato supportato dal server.

NFSv4.1 Kerberos

Per NFSv4.1, CVS-Performance offre l'autenticazione Kerberos come descritto in "RFC7530". È possibile attivare Kerberos in base al volume.

Il tipo di crittografia attualmente più potente disponibile per Kerberos è AES-256-CTS-HMAC-SHA1. NetApp Cloud Volumes Service supporta AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 e DES per NFS. Supporta anche ARCFOUR-HMAC (RC4) per il traffico CIFS/SMB, ma non per NFS.

Kerberos offre tre diversi livelli di sicurezza per i montaggi NFS, che offrono la possibilità di scegliere il livello di sicurezza Kerberos.

Come da RedHat "Opzioni di montaggio comuni" documentazione:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

Di norma, più il livello di sicurezza Kerberos deve essere elevato, più le performance sono peggiori, in quanto client e server trascorrono del tempo a crittografare e decrittare le operazioni NFS per ogni pacchetto inviato. Molti client e server NFS supportano l'offload AES-NI sulle CPU per un'esperienza generale migliore, ma l'impatto delle performance di Kerberos 5p (crittografia completa end-to-end) è significativamente maggiore

dell'impatto di Kerberos 5 (autenticazione dell'utente).

La seguente tabella mostra le differenze in termini di sicurezza e performance di ciascun livello.

Livello di sicurezza	Sicurezza	Performance
NFSv3: SIS	• Meno sicuro; testo normale con ID utente/ID gruppo numerici • In grado di visualizzare UID, GID, indirizzi IP client, percorsi di esportazione, nomi file, permessi nelle acquisizioni di pacchetti	• Ideale per la maggior parte dei casi
NFSv4.x: SIS	• Più sicuro di NFSv3 (ID client, corrispondenza stringa nome/stringa di dominio) ma ancora testo normale • Possibilità di visualizzare UID, GID, indirizzi IP client, stringhe di nomi, ID di dominio, percorsi di esportazione, nomi di file, permessi nelle acquisizioni di pacchetti	• Ideale per carichi di lavoro sequenziali (come macchine virtuali, database, file di grandi dimensioni) • Cattivo con elevato numero di file/metadati elevati (30-50% peggiore)
NFS: Krb5	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: Esegue il wrapping di UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al montaggio deve disporre di un ticket Kerberos valido (tramite nome utente/password o scambio manuale della scheda della chiave); il ticket scade dopo un periodo di tempo specificato e l'utente deve eseguire nuovamente l'autenticazione per l'accesso • Nessuna crittografia per le operazioni NFS o i protocolli ausiliari come mount/portmapper/nlm (possono vedere percorsi di esportazione, indirizzi IP, handle di file, permessi, nomi di file, atime/mtime in pacchetti capture)	• Migliore nella maggior parte dei casi per Kerberos; peggiore di AUTH_SYS

Livello di sicurezza	Sicurezza	Performance
NFS: Krb5i	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: Esegue il wrapping di UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al montaggio deve disporre di un ticket Kerberos valido (tramite nome utente/password o scambio manuale della scheda delle chiavi); il ticket scade dopo un periodo di tempo specificato e l'utente deve eseguire nuovamente l'autenticazione per l'accesso • Nessuna crittografia per le operazioni NFS o i protocolli ausiliari come mount/portmapper/nlm (possono vedere percorsi di esportazione, indirizzi IP, handle di file, permessi, nomi di file, atime/mtime in pacchetti capture) • Il checksum GSS Kerberos viene aggiunto a ogni pacchetto per garantire che nulla intercetti i pacchetti. Se i checksum corrispondono, è consentita la conversazione.	• Meglio di krb5p perché il payload NFS non è crittografato; solo l'overhead aggiunto rispetto a krb5 è il checksum di integrità. Le performance di krb5i non saranno molto peggiori di krb5, ma si verificherà un certo degrado.

Livello di sicurezza	Sicurezza	Performance
NFS: Krb5p	• Crittografia Kerberos per le credenziali in ogni pacchetto NFS: Esegue il wrapping di UID/GID di utenti/gruppi nelle chiamate RPC nel wrapper GSS • L'utente che richiede l'accesso al montaggio deve disporre di un ticket Kerberos valido (tramite nome utente/password o scambio manuale di keytab); il ticket scade dopo il periodo di tempo specificato e l'utente deve eseguire nuovamente l'autenticazione per l'accesso • Tutti i payload dei pacchetti NFS sono crittografati con il wrapper GSS (non è possibile visualizzare handle di file, permessi, nomi di file, atime/mtime nelle acquisizioni di pacchetti). • Include il controllo dell'integrità. • Il tipo di operazione NFS è visibile (FSINFO, ACCESS, GETATTR e così via). • I protocolli ausiliari (mount, portmap, nlm e così via) non sono crittografati (possono vedere percorsi di esportazione, indirizzi IP)	• Performance peggiori dei livelli di sicurezza; krb5p deve crittografare/decrittare di più. • Performance migliori rispetto a krb5p con NFSv4.x per carichi di lavoro con elevato numero di file.

In Cloud Volumes Service, un server Active Directory configurato viene utilizzato come server Kerberos e server LDAP (per cercare le identità degli utenti da uno schema compatibile con RFC2307). Non sono supportati altri server Kerberos o LDAP. NetApp consiglia vivamente di utilizzare LDAP per la gestione delle identità in Cloud Volumes Service. Per informazioni su come NFS Kerberos viene mostrato nelle acquisizioni di pacchetti, consulta la sezione ""Considerazioni su sniffing/traccia dei pacchetti"."

Crittografia dei dati a riposo

Tutti i volumi in Cloud Volumes Service sono crittografati a riposo utilizzando la crittografia AES-256, il che significa che tutti i dati utente scritti sui supporti sono crittografati e possono essere decifrati solo con una chiave per volume.

- Per CVS-SW, vengono utilizzate chiavi generate da Google.
- Per CVS-Performance, i tasti per volume sono memorizzati in un gestore di chiavi integrato in Cloud Volumes Service.

A partire da novembre 2021, è stata resa disponibile l'anteprima delle chiavi di crittografia gestite dal cliente (CMEK). In questo modo è possibile crittografare le chiavi per volume con una chiave master per progetto, per regione, ospitata in "Google Key Management Service (KMS)." KMS consente di collegare i key manager esterni.

Per informazioni sulla configurazione di KMS per CVS-Performance, vedere "Impostazione delle chiavi di crittografia gestite dal cliente".

Firewall

Cloud Volumes Service espone più porte TCP per le condivisioni NFS e SMB:

- "Porte richieste per l'accesso NFS"
- "Porte richieste per l'accesso SMB"

Inoltre, le configurazioni SMB, NFS con LDAP, incluso Kerberos, e a doppio protocollo richiedono l'accesso a un dominio Active Directory di Windows. Le connessioni di Active Directory devono essere "configurato" in base all'area geografica. I controller di dominio Active Directory vengono identificati tramite "Rilevamento DC basato su DNS" Utilizzando i server DNS specificati. Vengono utilizzati tutti i controller di dominio restituiti. L'elenco dei controller di dominio idonei può essere limitato specificando un sito Active Directory.

Cloud Volumes Service raggiunge gli indirizzi IP dell'intervallo CIDR allocati con `gcloud compute address` comando mentre "A bordo del Cloud Volumes Service". È possibile utilizzare questo CIDR come indirizzi di origine per configurare i firewall in entrata nei controller di dominio Active Directory.

I controller di dominio Active Directory devono "Esporre le porte ai CIDR Cloud Volumes Service come indicato qui".

Protocolli NAS

Panoramica dei protocolli NAS

I protocolli NAS includono NFS (v3 e v4.1) e SMB/CIFS (2.x e 3.x). Questi protocolli sono il modo in cui CVS consente l'accesso condiviso ai dati tra più client NAS. Inoltre, Cloud Volumes Service può fornire l'accesso simultaneo ai client NFS e SMB/CIFS (dual-Protocol) rispettando tutte le impostazioni di identità e autorizzazioni su file e cartelle nelle condivisioni NAS. Per mantenere la massima sicurezza possibile per il trasferimento dei dati, Cloud Volumes Service supporta la crittografia del protocollo in uso con la crittografia SMB e NFS Kerberos 5p.

Dual-Protocol è disponibile solo con CVS-Performance.

Nozioni di base sui protocolli NAS

I protocolli NAS consentono a più client su una rete di accedere agli stessi dati su un sistema storage, ad esempio Cloud Volumes Service su GCP. NFS e SMB sono i protocolli NAS definiti e operano su base client/server, dove Cloud Volumes Service agisce come server. I client inviano al server richieste di accesso, lettura e scrittura e il server è responsabile del coordinamento dei meccanismi di blocco dei file, dell'archiviazione delle autorizzazioni e della gestione delle richieste di identità e

autenticazione.

Ad esempio, se un client NAS desidera creare un nuovo file in una cartella, viene seguita la seguente procedura generale.

1. Il client richiede al server informazioni sulla directory (permessi, proprietario, gruppo, ID file, spazio disponibile, e così via); il server risponde con le informazioni se il client richiedente e l'utente hanno le autorizzazioni necessarie sulla cartella padre.
2. Se le autorizzazioni sulla directory consentono l'accesso, il client chiede al server se il nome del file creato esiste già nel file system. Se il nome del file è già in uso, la creazione non riesce. Se il nome del file non esiste, il server comunica al client che può procedere.
3. Il client invia una chiamata al server per creare il file con l'handle di directory e il nome del file e imposta l'accesso e i tempi di modifica. Il server invia un ID file univoco al file per assicurarsi che non vengano creati altri file con lo stesso ID.
4. Il client invia una chiamata per controllare gli attributi del file prima dell'operazione DI SCRITTURA. Se le autorizzazioni lo consentono, il client scrive il nuovo file. Se il protocollo/applicazione utilizza il blocco, il client richiede al server un blocco per impedire ad altri client di accedere al file mentre sono bloccati per evitare il danneggiamento dei dati.

NFS

NFS è un protocollo di file system distribuito che è uno standard IETF aperto definito in Request for Comments (RFC) che consente a chiunque di implementare il protocollo.

I volumi in Cloud Volumes Service vengono condivisi ai client NFS esportando un percorso accessibile a un client o a un set di client. Le autorizzazioni per montare queste esportazioni sono definite da policy e regole di esportazione, configurabili dagli amministratori di Cloud Volumes Service.

L'implementazione NetApp NFS è considerata uno standard di riferimento per il protocollo e viene utilizzata in innumerevoli ambienti NAS aziendali. Le sezioni seguenti illustrano NFS e le funzionalità di sicurezza specifiche disponibili in Cloud Volumes Service e le relative modalità di implementazione.

Utenti e gruppi UNIX locali predefiniti

Cloud Volumes Service contiene diversi utenti e gruppi UNIX predefiniti per varie funzionalità di base. Questi utenti e gruppi non possono essere modificati o cancellati. Non è possibile aggiungere nuovi utenti e gruppi locali a Cloud Volumes Service. Gli utenti e i gruppi UNIX al di fuori degli utenti e dei gruppi predefiniti devono essere forniti da un name service LDAP esterno.

La seguente tabella mostra gli utenti e i gruppi predefiniti e i relativi ID numerici. NetApp consiglia di non creare nuovi utenti o gruppi in LDAP o sui client locali che riutilizzano questi ID numerici.

Utenti predefiniti: ID numerici	Gruppi predefiniti: ID numerici
• root:0 • pcuser:65534 • nessuno:65535	• root:0 • demone:1 • pcuser:65534 • nessuno:65535

Quando si utilizza NFSv4.1, l'utente root potrebbe essere visualizzato come nessuno quando si eseguono comandi di elenco di directory sui client NFS. Ciò è dovuto alla configurazione del mapping del dominio ID del client. Vedere la sezione chiamata NFSv4.1 e l'utente/gruppo nessuno per informazioni dettagliate su questo problema e su come risolverlo.

L'utente root

In Linux, l'account root ha accesso a tutti i comandi, file e cartelle in un file system basato su Linux. A causa della potenza di questo account, le Best practice di sicurezza spesso richiedono che l'utente root sia disattivato o limitato in qualche modo. Nelle esportazioni NFS, il potere di un utente root sui file e sulle cartelle può essere controllato in Cloud Volumes Service attraverso policy e regole di esportazione e un concetto noto come root squash.

Lo squashing root garantisce che l'utente root che accede a un montaggio NFS venga bloccato dall'utente numerico anonimo 65534 (vedere la sezione "L'utente anonimo") ed è attualmente disponibile solo quando si utilizza CVS-Performance selezionando Off per l'accesso root durante la creazione della regola dei criteri di esportazione. Se l'utente root viene bloccato nell'utente anonimo, non ha più accesso per eseguire chown o. "comandi setuid/setgid (il bit adesivo)" Su file o cartelle nel montaggio NFS, e i file o le cartelle creati dall'utente root mostrano l'UID anon come proprietario/gruppo. Inoltre, gli ACL NFSv4 non possono essere modificati dall'utente root. Tuttavia, l'utente root ha ancora accesso a chmod e ha eliminato i file per i quali non dispone di permessi espliciti. Se si desidera limitare l'accesso ai permessi di file e cartelle di un utente root, si consiglia di utilizzare un volume con ACL NTFS, creando un utente Windows denominato `root`e applicando le autorizzazioni desiderate ai file o alle cartelle.

L'utente anonimo

L'ID utente anonimo (anon) specifica un ID utente o un nome utente UNIX mappato alle richieste del client che arrivano senza credenziali NFS valide. Questo può includere l'utente root quando viene utilizzato lo squashing root. L'utente anon in Cloud Volumes Service è 65534.

Questo UID è normalmente associato al nome utente `nobody` oppure `nfsnobody` Negli ambienti Linux. Cloud Volumes Service utilizza anche 65534 come utente UNIX locale` pcuser` (vedere la sezione "Utenti e gruppi UNIX locali predefiniti"), che è anche l'utente di fallback predefinito per le mappature dei nomi da Windows a UNIX quando non è possibile trovare un utente UNIX valido corrispondente in LDAP.

A causa delle differenze nei nomi utente di Linux e Cloud Volumes Service per UID 65534, la stringa del nome per gli utenti mappati a 65534 potrebbe non corrispondere quando si utilizza NFSv4.1. Di conseguenza, potresti vedere `nobody` come utente di alcuni file e cartelle. Vedere la sezione "NFSv4.1 e l'utente/gruppo nessuno" per informazioni su questo problema e su come risolverlo.

Controllo degli accessi/esportazioni

L'accesso iniziale all'esportazione/condivisione per i montaggi NFS è controllato attraverso regole di policy di esportazione basate su host contenute in una policy di esportazione. Viene definito un IP host, un nome host, una subnet, un netgroup o un dominio per consentire l'accesso per montare la condivisione NFS e il livello di accesso consentito all'host. Le opzioni di configurazione delle regole dei criteri di esportazione dipendono dal livello Cloud Volumes Service.

Per CVS-SW, sono disponibili le seguenti opzioni per la configurazione dei criteri di esportazione:

- **Corrispondenza client.** elenco separato da virgole di indirizzi IP, elenco separato da virgole di nomi host, subnet, netgroup, nomi di dominio.
- **RO/RW access rules.** selezionare Read/write o Read only per controllare il livello di accesso

all'esportazione.CVS-Performance offre le seguenti opzioni:

- **Corrispondenza client.** elenco separato da virgole di indirizzi IP, elenco separato da virgole di nomi host, subnet, netgroup, nomi di dominio.
- **RO/RW access rules.** selezionare Read/write o Read only per controllare il livello di accesso all'esportazione.
- **Root access (on/off).** configura root squash (vedere la sezione "L'utente root" per ulteriori informazioni).
- **Protocol type.** (tipo di protocollo): Limita l'accesso al montaggio NFS a una versione specifica del protocollo. Quando si specificano NFSv3 e NFSv4.1 per il volume, lasciare entrambe le caselle vuote o selezionare entrambe le caselle.
- **Livello di sicurezza Kerberos (quando si seleziona Enable Kerberos).** fornisce le opzioni krb5, krb5i e/o krb5p per l'accesso in sola lettura o in lettura/scrittura.

Modifica proprietà (chown) e gruppo di cambiamento (chgrp)

NFS su Cloud Volumes Service consente solo all'utente root di eseguire chown/chgrp su file e cartelle. Altri utenti visualizzano un `Operation not permitted` errore: anche sui file di loro proprietà. Se si utilizza il root squash (come descritto nella sezione "L'utente root"), la root viene bloccata in un utente non root e non è consentito l'accesso a chown e chgrp. Attualmente non esistono soluzioni alternative in Cloud Volumes Service per consentire chown e chgrp agli utenti non root. Se sono necessarie modifiche alla proprietà, prendere in considerazione l'utilizzo di volumi a doppio protocollo e impostare lo stile di protezione su NTFS per controllare le autorizzazioni dal lato Windows.

Gestione delle autorizzazioni

Cloud Volumes Service supporta entrambi i bit di modalità (come 644, 777 e così via per rwx) e gli ACL NFSv4.1 per controllare le autorizzazioni sui client NFS per i volumi che utilizzano lo stile di sicurezza UNIX. La gestione dei permessi standard viene utilizzata per questi (come chmod, chown o nfs4_setfacl) e funziona con qualsiasi client Linux che li supporti.

Inoltre, quando si utilizzano volumi a doppio protocollo impostati su NTFS, i client NFS possono sfruttare la mappatura dei nomi Cloud Volumes Service per gli utenti Windows, che vengono poi utilizzati per risolvere le autorizzazioni NTFS. Questo richiede una connessione LDAP a Cloud Volumes Service per fornire traduzioni da ID numerico a nome utente, in quanto Cloud Volumes Service richiede un nome utente UNIX valido per eseguire correttamente il mapping a un nome utente Windows.

Fornitura di ACL granulari per NFSv3

Le autorizzazioni di bit di modalità coprono solo proprietario, gruppo e tutti gli altri membri della semantica, il che significa che non esistono controlli granulari degli accessi utente per NFSv3 di base. Cloud Volumes Service non supporta gli ACL POSIX, né gli attributi estesi (come chattr), pertanto gli ACL granulari sono possibili solo nei seguenti scenari con NFSv3:

- Volumi di sicurezza NTFS (server CIFS richiesto) con mappature valide da UNIX a utenti Windows.
- Gli ACL NFSv4.1 vengono applicati utilizzando un client di amministrazione che monta NFSv4.1 per applicare gli ACL.

Entrambi i metodi richiedono una connessione LDAP per la gestione delle identità UNIX e un utente UNIX valido e informazioni di gruppo compilate (vedere la sezione ""LDAP"") E sono disponibili solo con istanze CVS-Performance. Per utilizzare i volumi di sicurezza NTFS con NFS, è necessario utilizzare il protocollo doppio (SMB e NFSv3) o il protocollo doppio (SMB e NFSv4.1), anche se non vengono effettuate connessioni SMB. Per utilizzare gli ACL NFSv4.1 con i montaggi NFSv3, selezionare `Both (NFSv3/NFSv4.1)` come tipo di protocollo.

I bit in modalità UNIX standard non forniscono lo stesso livello di granularità delle autorizzazioni fornite dagli ACL NTFS o NFSv4.x. La tabella seguente confronta la granularità delle autorizzazioni tra i bit di modalità NFSv3 e gli ACL NFSv4.1. Per informazioni sugli ACL NFSv4.1, vedere "Nfs4_acl - elenchi di controllo degli accessi NFSv4".

Bit di modalità NFSv3	ACL NFSv4.1
• Impostare l'ID utente all'esecuzione • Impostare l'ID del gruppo all'esecuzione • Salva testo scambiato (non definito in POSIX) • Permesso di lettura per il proprietario • Permesso di scrittura per il proprietario • Autorizzazione di esecuzione per il proprietario di un file o autorizzazione di ricerca per il proprietario nella directory • Permesso di lettura per il gruppo • Permesso di scrittura per il gruppo • Autorizzazione di esecuzione per il gruppo su un file o autorizzazione di ricerca (ricerca) per il gruppo nella directory • Permesso di lettura per altri • Permesso di scrittura per altri • Autorizzazione di esecuzione per altri utenti su un file o autorizzazione di ricerca per altri utenti nella directory	Tipi di voci di controllo di accesso (ACE) (Allow/Nega/Audit) * flag di ereditarietà * eredità di directory * eredità di file * nessuna propagazione-eredita * eredita-solo Permessi * Read-data (file) / list-directory (directory) * write-data (file) / create-file (directory) * append-data (file) / create-subdirectory (directory) * execute (file) / change-directory (directory) * delete * delete-child * Read-attribute * write-attribute * Read-named-attribute * write-named * Read-ACL *-synchronize *-owner *-synchronize * -ACL *-synchronize *-lire

Infine, l'appartenenza al gruppo NFS (sia in NFSv3 che IN NFSV4.x) è limitata a un massimo predefinito di 16 per AUTH_SYS in base ai limiti dei pacchetti RPC. NFS Kerberos fornisce fino a 32 gruppi e gli ACL NFSv4 eliminano la limitazione attraverso ACL granulari di utenti e gruppi (fino a 1024 voci per ACE).

Inoltre, Cloud Volumes Service offre un supporto esteso per gruppi per estendere il numero massimo di gruppi supportati fino a 32. Questa operazione richiede una connessione LDAP a un server LDAP che contenga identità di gruppo e utenti UNIX valide. Per ulteriori informazioni sulla configurazione, vedere "Creazione e gestione di volumi NFS" Nella documentazione di Google.

ID utente e gruppo NFSv3

Gli ID utente e di gruppo NFSv3 vengono trasmessi in rete come ID numerici anziché come nomi. Cloud Volumes Service non risolve i nomi utente per questi ID numerici con NFSv3, con volumi di sicurezza UNIX che utilizzano solo i bit di modalità. Quando sono presenti ACL NFSv4.1, per risolvere correttamente l'ACL è necessario eseguire una ricerca di ID numerici e/o stringhe di nomi, anche quando si utilizza NFSv3. Con i volumi di sicurezza NTFS, Cloud Volumes Service deve risolvere un ID numerico a un utente UNIX valido e quindi eseguire il mapping a un utente Windows valido per negoziare i diritti di accesso.

Limitazioni di sicurezza degli ID utente e di gruppo NFSv3

Con NFSv3, il client e il server non devono mai confermare che l'utente che tenta una lettura o una scrittura con un ID numerico sia un utente valido; è semplicemente implicitamente attendibile. In questo modo, il file

system si apre a potenziali violazioni semplicemente eseguendo lo spoofing di qualsiasi ID numerico. Per evitare falle di sicurezza come questa, sono disponibili alcune opzioni per Cloud Volumes Service.

- L'implementazione di Kerberos per NFS obbliga gli utenti ad autenticarsi con un nome utente e una password o un file keytab per ottenere un ticket Kerberos per consentire l'accesso a un mount. Kerberos è disponibile con istanze CVS-Performance e solo con NFSv4.1.
- La limitazione dell'elenco di host nelle regole dei criteri di esportazione limita i client NFSv3 che hanno accesso al volume Cloud Volumes Service.
- L'utilizzo di volumi a doppio protocollo e l'applicazione di ACL NTFS al volume obbliga i client NFSv3 a risolvere gli ID numerici dei nomi utente UNIX validi per autenticarsi correttamente per accedere ai montaggi. Ciò richiede l'abilitazione di LDAP e la configurazione delle identità di utenti e gruppi UNIX.
- Lo squashing dell'utente root limita i danni che un utente root può fare a un montaggio NFS, ma non rimuove completamente i rischi. Per ulteriori informazioni, vedere la sezione "L'utente root."

In ultima analisi, la sicurezza NFS è limitata alla versione del protocollo in uso. NFSv3, pur essendo più performante in generale rispetto a NFSv4.1, non fornisce lo stesso livello di sicurezza.

NFSv4.1

NFSv4.1 offre maggiore sicurezza e affidabilità rispetto a NFSv3, per i seguenti motivi:

- Blocco integrato attraverso un meccanismo basato sul lease
- Sessioni stateful
- Tutte le funzionalità NFS su una singola porta (2049)
- Solo TCP
- Mapping del dominio ID
- Integrazione Kerberos (NFSv3 può utilizzare Kerberos, ma solo per NFS, non per protocolli ausiliari come NLM)

Dipendenze NFSv4.1

A causa delle funzionalità di sicurezza aggiuntive di NFSv4.1, sono coinvolte alcune dipendenze esterne che non erano necessarie per utilizzare NFSv3 (in modo simile a come SMB richiede dipendenze come Active Directory).

ACL NFSv4.1

Cloud Volumes Service offre il supporto per ACL NFSv4.x, che offrono vantaggi distinti rispetto alle normali autorizzazioni POSIX, come ad esempio:

- Controllo granulare dell'accesso degli utenti a file e directory
- Maggiore sicurezza NFS
- Maggiore interoperabilità con CIFS/SMB
- Rimozione del limite NFS di 16 gruppi per utente con sicurezza AUTH_SYS
- Gli ACL evitano la necessità di risoluzione degli ID di gruppo (GID), che rimuove efficacemente i GID limitNLSSv4.1 ACL sono controllati dai client NFS, non da Cloud Volumes Service. Per utilizzare gli ACL NFSv4.1, assicurarsi che la versione software del client li supporti e che siano installate le utility NFS appropriate.

Compatibilità tra ACL NFSv4.1 e client SMB

Gli ACL NFSv4 sono diversi dagli ACL a livello di file di Windows (ACL NTFS) ma presentano funzionalità simili. Tuttavia, in ambienti NAS multiprotocollo, se sono presenti ACL NFSv4.1 e si utilizza l'accesso a doppio protocollo (NFS e SMB sugli stessi set di dati), i client che utilizzano SMB2.0 e versioni successive non saranno in grado di visualizzare o gestire gli ACL dalle schede di sicurezza di Windows.

Come funzionano gli ACL NFSv4.1

Per riferimento, vengono definiti i seguenti termini:

- **Elenco di controllo di accesso (ACL).** elenco di voci delle autorizzazioni.
- **Voce di controllo di accesso (ACE).** una voce di autorizzazione nell'elenco.

Quando un client imposta un ACL NFSv4.1 su un file durante un'operazione SETATTR, Cloud Volumes Service imposta tale ACL sull'oggetto, sostituendo qualsiasi ACL esistente. Se un file non contiene ACL, le autorizzazioni di modalità per il file vengono calcolate dal PROPRIETARIO@, DAL GRUPPO@ e DA EVERYONE@. Se nel file sono presenti SUID/SGID/bit ADESIVI, questi non vengono influenzati.

Quando un client ottiene un ACL NFSv4.1 su un file durante un'operazione GETATTR, Cloud Volumes Service legge l'ACL NFSv4.1 associato all'oggetto, costruisce un elenco di ACE e restituisce l'elenco al client. Se il file ha un ACL NT o bit di modalità, un ACL viene costruito dai bit di modalità e restituito al client.

L'accesso viene negato se nell'ACL è presente un ACE DI NEGAZIONE; l'accesso viene concesso se esiste un ACE DI AUTORIZZAZIONE. Tuttavia, l'accesso viene negato anche se nessuna delle ACE è presente nell'ACL.

Un descrittore di sicurezza è costituito da un ACL di sicurezza (SACL) e da un ACL discrezionale (DACL). Quando NFSv4.1 interagisce con CIFS/SMB, il DACL viene mappato uno a uno con NFSv4 e CIFS. Il DACL è costituito dalle ACE DI AUTORIZZAZIONE e NEGAZIONE.

Se di base `chmod` Viene eseguito su un file o una cartella con gli ACL NFSv4.1 impostati, gli ACL degli utenti e dei gruppi esistenti vengono mantenuti, ma gli ACL PREDEFINITI DI PROPRIETARIO@, GRUPPO@, EVERYONE@ vengono modificati.

Un client che utilizza ACL NFSv4.1 può impostare e visualizzare ACL per file e directory nel sistema. Quando viene creato un nuovo file o sottodirectory in una directory che dispone di un ACL, tale oggetto eredita tutte le ACE nell'ACL che sono state contrassegnate con il appropriato "flag di ereditarietà".

Se un file o una directory dispone di un ACL NFSv4.1, tale ACL viene utilizzato per controllare l'accesso indipendentemente dal protocollo utilizzato per accedere al file o alla directory.

File e directory ereditano ACE da ACL NFSv4 nelle directory principali (possibilmente con modifiche appropriate), purché gli ACE siano stati contrassegnati con i flag di ereditarietà corretti.

Quando viene creato un file o una directory come risultato di una richiesta NFSv4, l'ACL del file o della directory risultante dipende dal fatto che la richiesta di creazione del file includa un ACL o solo permessi di accesso ai file UNIX standard. L'ACL dipende anche dalla presenza o meno di un ACL nella directory principale.

- Se la richiesta include un ACL, viene utilizzato tale ACL.
- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale non dispone di un ACL, la modalità file client viene utilizzata per impostare le autorizzazioni di accesso ai file UNIX standard.

- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale dispone di un ACL non ereditabile, un ACL predefinito basato sui bit di modalità passati alla richiesta viene impostato sul nuovo oggetto.
- Se la richiesta include solo autorizzazioni di accesso ai file UNIX standard ma la directory principale dispone di un ACL, le ACE nell'ACL della directory principale vengono ereditate dal nuovo file o directory, purché le ACE siano state contrassegnate con gli indicatori di ereditarietà appropriati.

Autorizzazioni ACE

Le autorizzazioni ACL NFSv4.1 utilizzano una serie di valori di lettere maiuscole e minuscole (ad esempio `rxtncy`) per controllare l'accesso. Per ulteriori informazioni sui valori delle lettere, vedere "PROCEDURA: Utilizzare l'ACL NFSv4".

Comportamento dell'ACL di NFSv4.1 con ereditarietà di umask e ACL

"Gli ACL NFSv4 offrono l'ereditarietà degli ACL". L'ereditarietà degli ACL indica che i file o le cartelle creati sotto gli oggetti con gli ACL NFSv4.1 impostati possono ereditare gli ACL in base alla configurazione di "Flag di ereditarietà ACL".

"Umask" viene utilizzato per controllare il livello di autorizzazione al quale i file e le cartelle vengono creati in una directory senza l'intervento dell'amministratore. Per impostazione predefinita, Cloud Volumes Service consente a umask di eseguire l'override degli ACL ereditati, il che è un comportamento previsto come indicato in "RFC 5661".

Formattazione ACL

Gli ACL NFSv4.1 hanno una formattazione specifica. Il seguente esempio è un insieme ACE su un file:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

L'esempio precedente segue le linee guida del formato ACL di:

```
type:flags:principal:permissions
```

Un tipo di `A` significa "consenti". In questo caso, i flag Inherit non vengono impostati, in quanto l'entità non è un gruppo e non include l'ereditarietà. Inoltre, poiché l'ACE non è una voce DI AUDIT, non è necessario impostare gli indicatori di audit. Per ulteriori informazioni sugli ACL NFSv4.1, vedere "http://linux.die.net/man/5/nfs4_acl".

Se l'ACL NFSv4.1 non è impostato correttamente (o una stringa di nomi non può essere risolta dal client e dal server), l'ACL potrebbe non funzionare come previsto oppure la modifica dell'ACL potrebbe non essere applicata e generare un errore.

Gli errori di esempio includono:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

NEGARE esplicitamente

Le autorizzazioni NFSv4.1 possono includere attributi DI NEGAZIONE esplicita per PROPRIETARIO, GRUPPO e CHIUNQUE. Ciò è dovuto al fatto che gli ACL di NFSv4.1 sono di tipo default-deny, il che significa che se un ACL non viene esplicitamente concesso da un ACE, viene negato. Gli attributi DI NEGAZIONE esplicita sovrascrivono le ACE DI ACCESSO, esplicite o meno.

GLI ACE DI NEGAZIONE vengono impostati con un tag di attributo di `D`.

Nell'esempio riportato di seguito, IL GRUPPO@ può disporre di tutte le autorizzazioni di lettura ed esecuzione, ma non di tutti gli accessi in scrittura.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

GLI ACE DI NEGAZIONE devono essere evitati ogni volta che è possibile perché possono essere confusi e complicati; GLI ACL CHE NON sono esplicitamente definiti sono implicitamente negati. Quando si impostano LE ACE DI NEGAZIONE, agli utenti potrebbe essere negato l'accesso quando si prevede di ottenere l'accesso.

Il set precedente di ACE equivale a 755 in bit di modalità, il che significa:

- Il proprietario ha tutti i diritti.
- I gruppi sono di sola lettura.
- Altri hanno la sola lettura.

Tuttavia, anche se le autorizzazioni vengono regolate sull'equivalente 775, l'accesso può essere negato a causa del NEGAZIONE esplicita impostata su EVERYONE.

Dipendenze di mappatura del dominio ID NFSv4.1

NFSv4.1 sfrutta la logica di mappatura del dominio ID come livello di sicurezza per verificare che un utente che tenta di accedere a un montaggio NFSv4.1 sia effettivamente quello che afferma di essere. In questi casi, il nome utente e il nome del gruppo provenienti dal client NFSv4.1 aggiunge una stringa di nome e la invia all'istanza di Cloud Volumes Service. Se la combinazione di nome utente/gruppo e stringa ID non corrisponde, l'utente e/o il gruppo vengono esclusi dall'impostazione predefinita None User specificata in `/etc/idmapd.conf` sul client.

Questa stringa ID è un requisito per il corretto rispetto delle autorizzazioni, in particolare quando vengono utilizzati ACL NFSv4.1 e/o Kerberos. Di conseguenza, le dipendenze dei server dei nomi, come i server LDAP, sono necessarie per garantire la coerenza tra client e Cloud Volumes Service per una corretta risoluzione delle identità dei nomi di utenti e gruppi.

Cloud Volumes Service utilizza un ID statico predefinito del nome di dominio `defaultv4iddomain.com`. Per impostazione predefinita, i client NFS utilizzano il nome di dominio DNS per le impostazioni del nome di

dominio ID, ma è possibile modificare manualmente il nome di dominio ID in `/etc/idmapd.conf`.

Se LDAP è attivato in Cloud Volumes Service, Cloud Volumes Service automatizza il dominio ID NFS per modificare ciò che è configurato per il dominio di ricerca in DNS e i client non dovranno essere modificati a meno che non utilizzino nomi di ricerca di dominio DNS diversi.

Quando Cloud Volumes Service è in grado di risolvere un nome utente o un nome di gruppo in file locali o LDAP, viene utilizzata la stringa di dominio e gli ID di dominio non corrispondenti vengono eliminati a nessuno. Se Cloud Volumes Service non riesce a trovare un nome utente o un nome di gruppo nei file locali o LDAP, viene utilizzato il valore ID numerico e il client NFS risolve il nome in modo corretto (simile al comportamento di NFSv3).

Senza modificare il dominio ID NFSv4.1 del client in modo che corrisponda a quello utilizzato dal volume Cloud Volumes Service, si verifica quanto segue:

- Gli utenti e i gruppi UNIX con voci locali in Cloud Volumes Service (come root, come definito in utenti e gruppi UNIX locali) vengono ridotti al valore None.
- Gli utenti e i gruppi UNIX con voci in LDAP (se Cloud Volumes Service è configurato per l'utilizzo di LDAP) non vengono visualizzati se i domini DNS sono diversi tra client NFS e Cloud Volumes Service.
- Gli utenti e i gruppi UNIX senza voci locali o LDAP utilizzano il valore numerico ID e si risolvono nel nome specificato sul client NFS. Se non esiste alcun nome sul client, viene visualizzato solo l'ID numerico.

Di seguito sono riportati i risultati dello scenario precedente:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Quando i domini ID client e server corrispondono, viene visualizzato lo stesso elenco di file:

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Per ulteriori informazioni su questo problema e su come risolverlo, vedere la sezione "NFSv4.1 e l'utente/gruppo nessuno."

Dipendenze Kerberos

Se si intende utilizzare Kerberos con NFS, è necessario disporre di quanto segue con Cloud Volumes Service:

- Dominio Active Directory per i servizi del centro di distribuzione Kerberos (KDC)
- Dominio Active Directory con attributi utente e gruppo popolati con informazioni UNIX per la funzionalità LDAP (NFS Kerberos in Cloud Volumes Service richiede un'associazione utente da SPN a utente UNIX per la corretta funzionalità).
- LDAP attivato sull'istanza di Cloud Volumes Service
- Dominio Active Directory per i servizi DNS

NFSv4.1 e l'utente/gruppo nessuno

Uno dei problemi più comuni riscontrati con una configurazione NFSv4.1 è quando un file o una cartella viene visualizzata in un elenco utilizzando `ls` di proprietà di `user:group` combinazione di `nobody:nobody`.

Ad esempio:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

E l'ID numerico è `99`.

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

In alcuni casi, il file potrebbe mostrare il proprietario corretto, ma `nobody` come gruppo.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

Chi non è nessuno?

Il `nobody` L'utente in NFSv4.1 è diverso da `nfsnobody` utente. È possibile visualizzare il modo in cui un client NFS vede ciascun utente eseguendo `id` comando:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Con NFSv4.1 `nobody` user (utente) è l'utente predefinito definito da `idmapd.conf` e può essere definito come qualsiasi utente che si desidera utilizzare.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Perché questo accade?

Poiché la sicurezza tramite il mapping della stringa del nome è un insieme di chiavi delle operazioni NFSv4.1, il comportamento predefinito quando una stringa del nome non corrisponde correttamente è quello di schiacciare l'utente a un utente che normalmente non avrà accesso a file e cartelle di proprietà di utenti e gruppi.

Quando vedi `nobody` Per l'utente e/o il gruppo negli elenchi di file, ciò significa generalmente che qualcosa in NFSv4.1 è configurato in modo errato. La distinzione tra maiuscole e minuscole può entrare in gioco qui.

Ad esempio, se user1@CVSDEMO.LOCAL (uid 1234, gid 1234) sta accedendo a un'esportazione, Cloud Volumes Service deve essere in grado di trovare user1@CVSDEMO.LOCAL (uid 1234, gid 1234). Se l'utente in Cloud Volumes Service è USER1@CVSDEMO.LOCAL, non corrisponde (USER1 maiuscolo e user1 minuscolo). In molti casi, nel file dei messaggi sul client è possibile visualizzare quanto segue:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

Il client e il server devono accettare che un utente sia effettivamente quello che dichiara di essere, quindi è necessario controllare quanto segue per assicurarsi che l'utente che il client vede abbia le stesse informazioni dell'utente che Cloud Volumes Service vede.

- **NFSv4.x ID domain.** Client: `idmapd.conf` File; utilizzi di Cloud Volumes Service `defaultv4iddomain.com` e non possono essere modificati manualmente. Se si utilizza LDAP con NFSv4.1, Cloud Volumes Service modifica il dominio ID in quello utilizzato dal dominio di ricerca DNS, che è lo stesso del dominio ad.
- **Nome utente e ID numerici.** determina dove il client cerca i nomi utente e sfrutta la configurazione dello switch del name service: Client: `nsswitch.conf` E/o passwd locale e file di gruppo; Cloud Volumes Service non consente modifiche a questo, ma aggiunge automaticamente LDAP alla configurazione quando è attivato.
- **Nome del gruppo e ID numerici.** determina la posizione in cui il client cerca i nomi dei gruppi e sfrutta la configurazione dello switch del name service: Client: `nsswitch.conf` E/o passwd locale e file di gruppo; Cloud Volumes Service non consente modifiche a questo, ma aggiunge automaticamente LDAP alla configurazione quando è attivato.

In quasi tutti i casi, se si vede `nobody` Negli elenchi di utenti e gruppi dei client, il problema è la traduzione dell'ID dominio del nome utente o del gruppo tra Cloud Volumes Service e il client NFS. Per evitare questo scenario, utilizzare LDAP per risolvere le informazioni relative a utenti e gruppi tra client e Cloud Volumes Service.

Visualizzazione delle stringhe di ID nome per NFSv4.1 sui client

Se si utilizza NFSv4.1, durante le operazioni NFS viene eseguita una mappatura di stringa nome, come descritto in precedenza.

Oltre all'utilizzo `/var/log/messages` Per trovare un problema con gli ID NFSv4, è possibile utilizzare "nfsidmap -l" Sul client NFS per visualizzare i nomi utente correttamente mappati al dominio NFSv4.

Ad esempio, questo è l'output del comando dopo che un utente può essere trovato dal client e Cloud Volumes Service accede a un montaggio NFSv4.x:

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Quando un utente non mappato correttamente nel dominio ID NFSv4.1 (in questo caso, `netapp-user`) tenta di accedere allo stesso mount e tocca un file, vengono assegnati `nobody:nobody`, come previsto.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

Il `nfsidmap -l` l'output mostra l'utente `pcuser` nel display ma non `netapp-user`; si tratta dell'utente anonimo nella nostra regola dei criteri di esportazione (`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

PMI

"PMI" È un protocollo di condivisione file di rete sviluppato da Microsoft che fornisce autenticazione centralizzata di utenti/gruppi, autorizzazioni, blocco e condivisione file a più client SMB su una rete Ethernet. I file e le cartelle vengono presentati ai client tramite condivisioni, che possono essere configurate con una vasta gamma di proprietà di condivisione e offrono il controllo degli accessi tramite permessi a livello di condivisione. SMB può essere presentato a qualsiasi client che offra supporto per il protocollo, inclusi client Windows, Apple e Linux.

Cloud Volumes Service supporta le versioni SMB 2.1 e 3.x del protocollo.

Controllo degli accessi/condivisioni SMB

- Quando un nome utente Windows richiede l'accesso al volume Cloud Volumes Service, Cloud Volumes Service cerca un nome utente UNIX utilizzando i metodi configurati dagli amministratori Cloud Volumes Service.
- Se viene configurato un provider di identità UNIX esterno (LDAP) e i nomi utente Windows/UNIX sono identici, i nomi utente di Windows verranno mappati 1:1 ai nomi utente UNIX senza alcuna configurazione aggiuntiva. Quando LDAP è attivato, Active Directory viene utilizzato per ospitare gli attributi UNIX per gli oggetti utente e gruppo.
- Se i nomi Windows e UNIX non corrispondono in modo identico, è necessario configurare LDAP in modo da consentire a Cloud Volumes Service di utilizzare la configurazione di mappatura dei nomi LDAP (vedere la sezione ""Utilizzo di LDAP per la mappatura asimmetrica dei nomi"").
- Se LDAP non è in uso, gli utenti SMB di Windows si associano a un utente UNIX locale predefinito denominato `pcuser` In Cloud Volumes Service. Ciò significa che i file scritti in Windows dagli utenti che eseguono il mapping a `pcuser` Mostra la proprietà UNIX come `pcuser` In ambienti NAS multiprotocollo. `pcuser` qui è effettivamente il `nobody` Utente in ambienti Linux (UID 65534).

Nelle implementazioni solo con SMB, il `pcuser` Il mapping continua a verificarsi, ma non è importante, perché la proprietà di utenti e gruppi di Windows viene visualizzata correttamente e l'accesso NFS al volume solo SMB non è consentito. Inoltre, i volumi solo SMB non supportano la conversione in NFS o volumi a doppio protocollo dopo la loro creazione.

Windows sfrutta Kerberos per l'autenticazione del nome utente con i domain controller di Active Directory, che richiede uno scambio di nome utente e password con i controller di dominio ad, esterni all'istanza di Cloud Volumes Service. L'autenticazione Kerberos viene utilizzata quando `\\SERVERNAME` Il percorso UNC viene utilizzato dai client SMB ed è vero quanto segue:

- La voce DNS A/AAAA esiste per NOMESERVER
- Esiste un SPN valido per l'accesso SMB/CIFS per NOMESERVER

Quando viene creato un volume SMB Cloud Volumes Service, il nome dell'account del computer viene creato come definito nella sezione ""Come viene visualizzato Cloud Volumes Service in Active Directory."" Il nome account del computer diventa anche il percorso di accesso condiviso SMB perché Cloud Volumes Service sfrutta il DNS dinamico (DDNS) per creare le voci A/AAAA e PTR necessarie nel DNS e le voci SPN necessarie sull'account principal del computer.

Per creare le voci PTR, la zona di ricerca inversa per l'indirizzo IP dell'istanza Cloud Volumes Service deve esistere sul server DNS.

Ad esempio, questo volume Cloud Volumes Service utilizza il seguente percorso di condivisione UNC: `\\cvs-east- 433d.cvsdemo.local`.

In Active Directory, queste sono le voci SPN generate dal servizio Cloud Volumes:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Questo è il risultato della ricerca DNS in avanti/indietro:

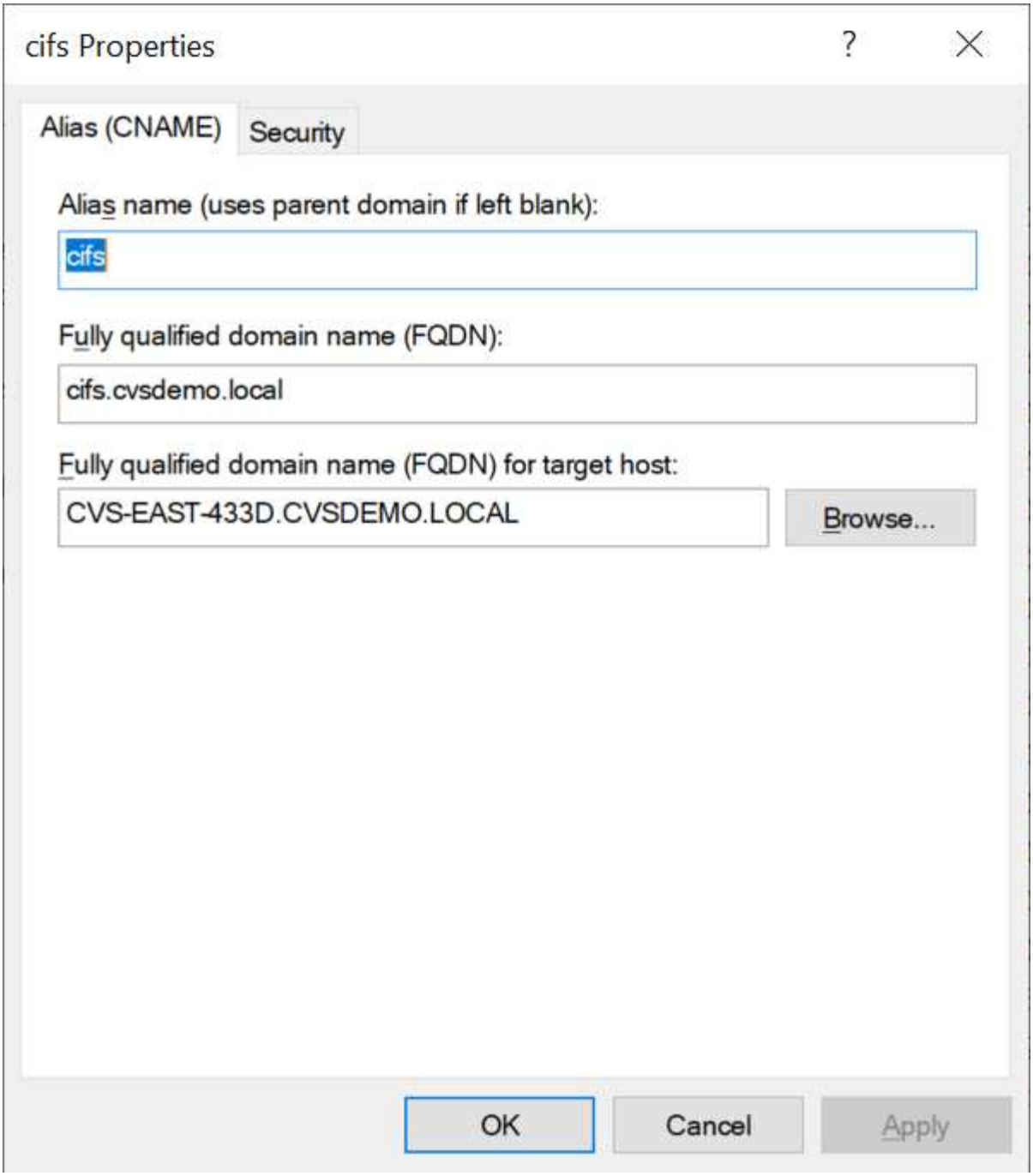
```
PS C:\> nslookup CVS-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    CVS-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Facoltativamente, è possibile applicare un maggiore controllo degli accessi attivando/richiedendo la crittografia SMB per le condivisioni SMB in Cloud Volumes Service. Se la crittografia SMB non è supportata da uno degli endpoint, l'accesso non è consentito.

Utilizzo degli alias dei nomi SMB

In alcuni casi, potrebbe essere un problema di sicurezza per gli utenti finali conoscere il nome dell'account del computer in uso per Cloud Volumes Service. In altri casi, è sufficiente fornire un percorso di accesso più semplice agli utenti finali. In questi casi, è possibile creare alias SMB.

Se si desidera creare alias per il percorso di condivisione SMB, è possibile sfruttare ciò che è noto come record CNAME in DNS. Ad esempio, se si desidera utilizzare il nome `\\CIFS` per accedere alle condivisioni anziché a. `\\cvs-east- 433d.cvsdemo.local`, Ma si desidera comunque utilizzare l'autenticazione Kerberos, un CNAME nel DNS che punta al record A/AAAA esistente e un ulteriore SPN aggiunto all'account del computer esistente fornisce l'accesso Kerberos.



Questo è il risultato della ricerca diretta DNS dopo l'aggiunta di un CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
Name:    CVS-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Questa è la query SPN risultante dopo l'aggiunta di nuovi numeri di servizio:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

In un'acquisizione di pacchetti, è possibile visualizzare la richiesta di configurazione della sessione utilizzando l'SPN legato al CNAME.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

Dialetti di autenticazione SMB

Cloud Volumes Service supporta quanto segue "dialetti" Per l'autenticazione SMB:

- LM
- NTLM
- NTLMv2
- Kerberos

L'autenticazione Kerberos per l'accesso alle condivisioni SMB è il livello di autenticazione più sicuro possibile. Con la crittografia AES e SMB attivata, il livello di sicurezza aumenta ulteriormente.

Cloud Volumes Service supporta anche la compatibilità con le versioni precedenti per l'autenticazione LM e NTLM. Quando Kerberos non è configurato correttamente (ad esempio quando si creano alias SMB), l'accesso alla condivisione viene ricallato ai metodi di autenticazione più deboli (ad esempio NTLMv2). Poiché questi meccanismi sono meno sicuri, sono disattivati in alcuni ambienti Active Directory. Se i metodi di autenticazione più deboli sono disattivati e Kerberos non è configurato correttamente, l'accesso alla condivisione non riesce perché non esiste un metodo di autenticazione valido.

Per informazioni sulla configurazione e la visualizzazione dei livelli di autenticazione supportati in Active Directory, vedere "Sicurezza di rete: Livello di autenticazione di LAN Manager".

Modelli di permesso

Permessi NTFS/file

Le autorizzazioni NTFS sono le autorizzazioni applicate a file e cartelle nei file system che aderiscono alla logica NTFS. È possibile applicare le autorizzazioni NTFS in `Basic` oppure `Advanced` e può essere impostato su `Allow` oppure `Deny` per il controllo degli accessi.

Le autorizzazioni di base includono:

- Controllo completo
- Modificare
- Lettura ed esecuzione
- Leggi
- Di scrittura

Quando si impostano le autorizzazioni per un utente o un gruppo, denominato ACE, si trova in un ACL. Le autorizzazioni NTFS utilizzano le stesse basi di lettura/scrittura/esecuzione dei bit in modalità UNIX, ma possono anche estendersi a controlli di accesso più granulari ed estesi (noti anche come permessi speciali), come Take Ownership, Create Folders/Append Data, Write Attributes e altro ancora.

I bit in modalità UNIX standard non forniscono lo stesso livello di granularità delle autorizzazioni NTFS (ad esempio, la possibilità di impostare autorizzazioni per singoli oggetti utente e gruppo in un ACL o di impostare attributi estesi). Tuttavia, gli ACL NFSv4.1 offrono le stesse funzionalità degli ACL NTFS.

Le autorizzazioni NTFS sono più specifiche delle autorizzazioni di condivisione e possono essere utilizzate insieme alle autorizzazioni di condivisione. Con le strutture di autorizzazione NTFS, si applicano le impostazioni più restrittive. Di conseguenza, le negazioni esplicite a un utente o a un gruppo sovrascrivono anche il controllo completo quando si definiscono i diritti di accesso.

Le autorizzazioni NTFS sono controllate dai client SMB di Windows.

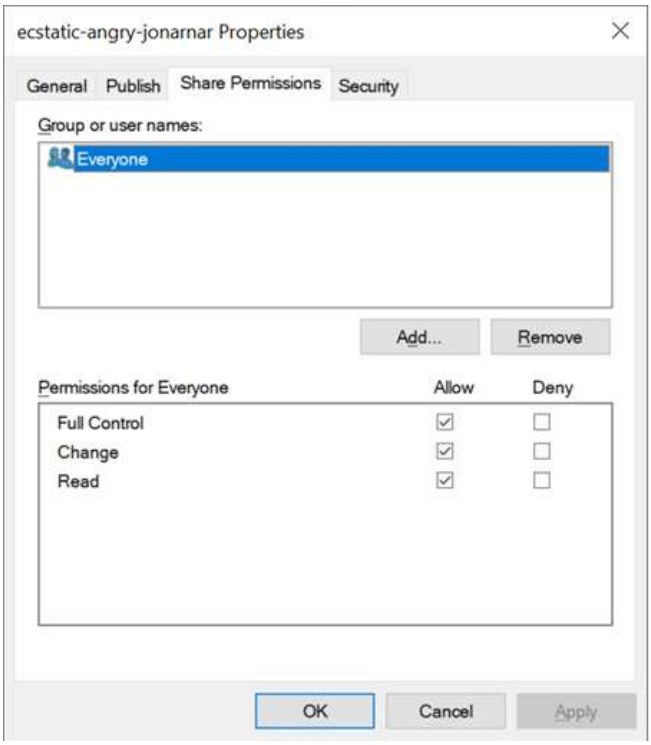
Autorizzazioni di condivisione

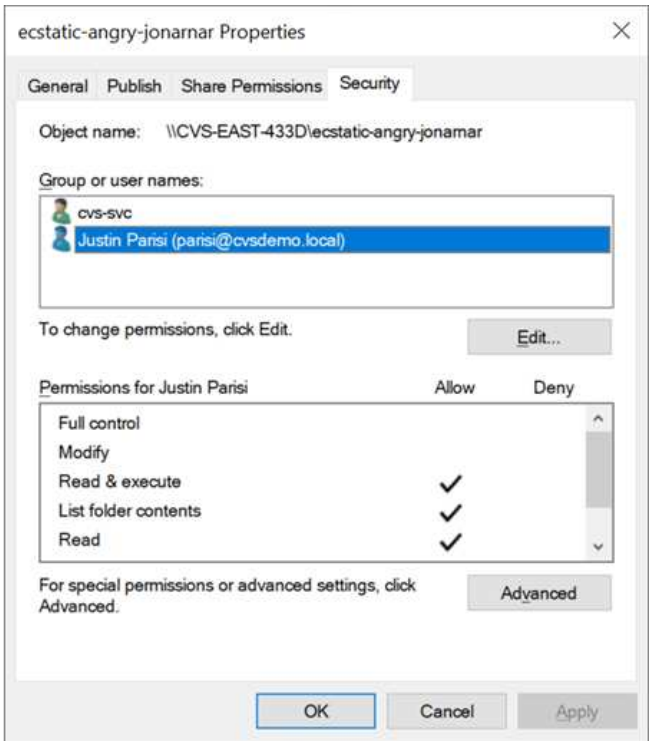
Le autorizzazioni di condivisione sono più generali delle autorizzazioni NTFS (solo lettura/modifica/controllo completo) e controllano la voce iniziale in una condivisione SMB, in modo simile al funzionamento delle regole dei criteri di esportazione NFS.

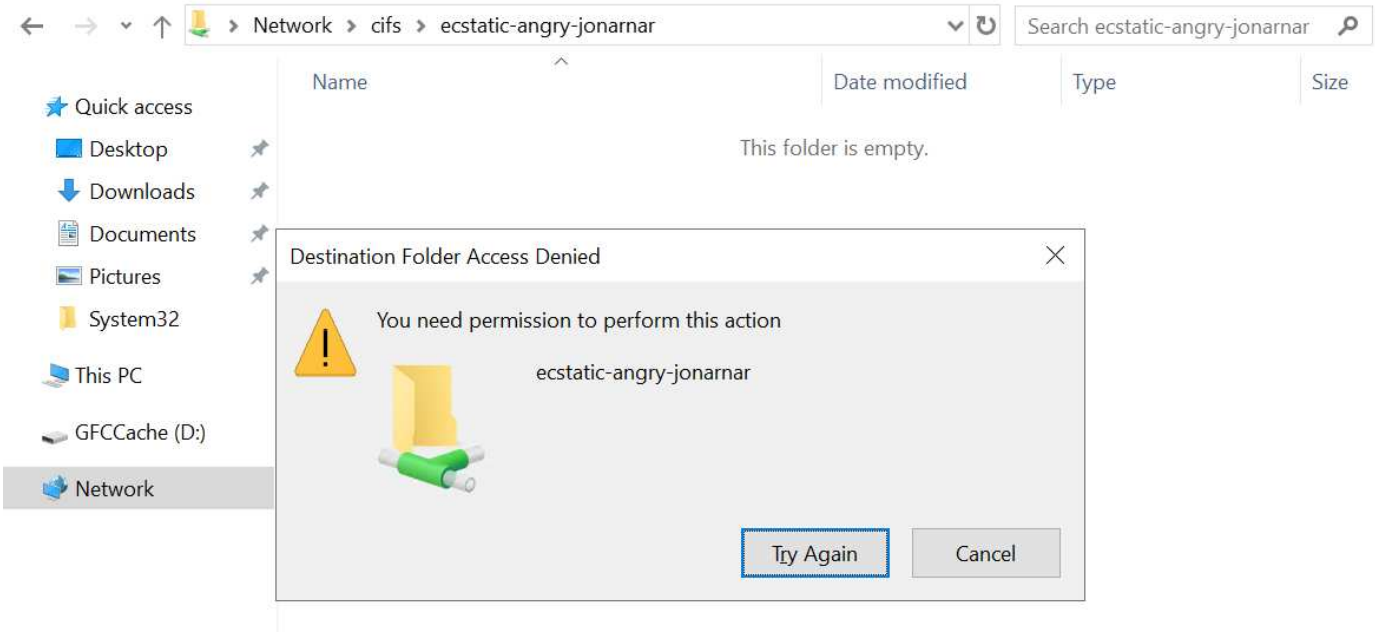
Sebbene le regole dei criteri di esportazione NFS controllino l'accesso attraverso informazioni basate su host come indirizzi IP o nomi host, le autorizzazioni di condivisione SMB possono controllare l'accesso utilizzando le ACE di utente e gruppo in un ACL condiviso. È possibile impostare gli ACL di condivisione dal client Windows o dall'interfaccia utente di gestione di Cloud Volumes Service.

Per impostazione predefinita, gli ACL di condivisione e gli ACL dei volumi iniziali includono Everyone con controllo completo. Gli ACL dei file devono essere modificati, ma le autorizzazioni di condivisione vengono ignorate dalle autorizzazioni dei file sugli oggetti nella condivisione.

Ad esempio, se a un utente è consentito solo l'accesso in lettura all'ACL del file di volume Cloud Volumes Service, viene negato l'accesso per creare file e cartelle anche se l'ACL di condivisione è impostato su Everyone con controllo completo, come illustrato nella figura seguente.







Per ottenere i migliori risultati di sicurezza, procedere come segue:

- Rimuovere tutti dagli ACL di file e condivisione e impostare l'accesso di condivisione per utenti o gruppi.
- Utilizzare i gruppi per il controllo degli accessi invece di singoli utenti per semplificare la gestione e velocizzare la rimozione/aggiunta degli utenti per condividere gli ACL attraverso la gestione dei gruppi.
- Consentire un accesso di condivisione meno restrittivo e più generale alle ACE sulle autorizzazioni di condivisione e bloccare l'accesso a utenti e gruppi con permessi di file per un controllo degli accessi più granulare.
- Evitare l'utilizzo generale di ACL di negazione esplicite, in quanto sovrascrivono gli ACL di consenso. Limitare l'utilizzo di ACL di negazione esplicite per utenti o gruppi che devono essere limitati all'accesso rapido a un file system.

- Assicurarsi di prestare attenzione a. "Ereditarietà ACL" impostazioni durante la modifica delle autorizzazioni; l'impostazione del flag di ereditarietà al livello superiore di una directory o di un volume con un numero elevato di file indica che ogni file sotto a tale directory o volume ha ereditato le autorizzazioni aggiunte, che possono creare comportamenti indesiderati come accesso/negazione non intenzionale e lunga modifica delle autorizzazioni quando ogni file viene regolato.

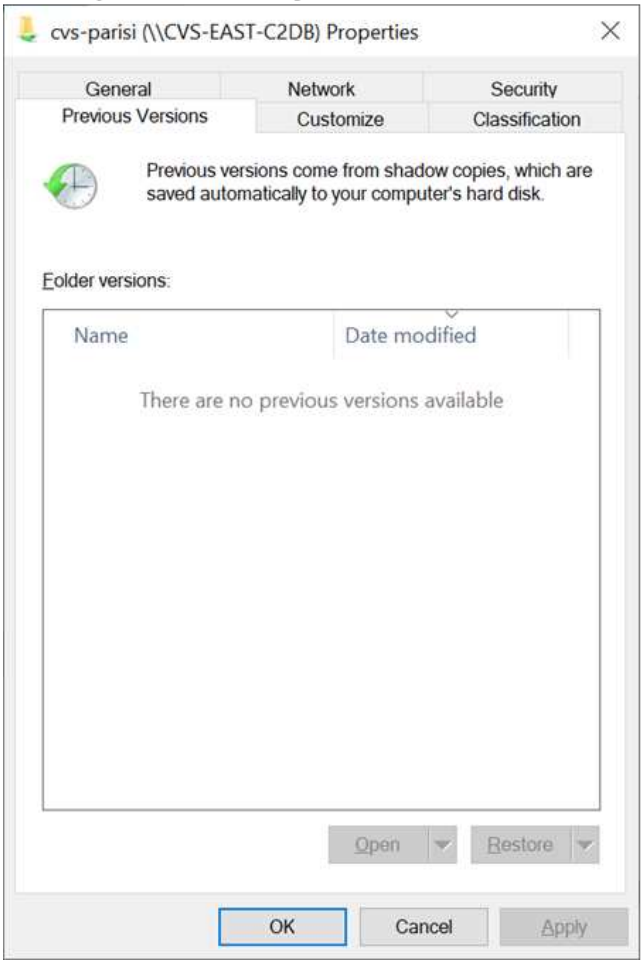
SMB condivide le funzionalità di sicurezza

La prima volta che si crea un volume con accesso SMB in Cloud Volumes Service, viene visualizzata una serie di opzioni per la protezione di tale volume.

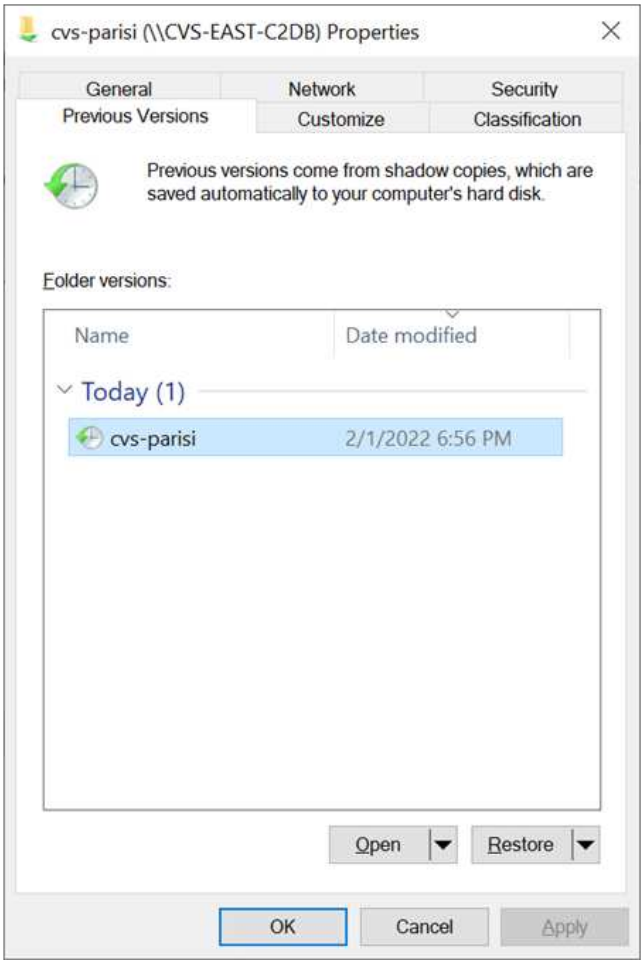
Alcune di queste scelte dipendono dal livello Cloud Volumes Service (prestazioni o software) e le scelte includono:

- **Rendi visibile la directory Snapshot (disponibile sia per CVS-Performance che per CVS-SW).** questa opzione controlla se i client SMB possono accedere o meno alla directory Snapshot in una condivisione SMB (`\\server\share\~snapshot` E/o versioni precedenti). L'impostazione predefinita non è selezionata, il che significa che il volume per impostazione predefinita nasconde e non consente l'accesso a `~snapshot` Directory e non vengono visualizzate copie Snapshot nella scheda versioni precedenti del volume.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



È possibile nascondere le copie Snapshot dagli utenti finali per motivi di sicurezza, di performance (nascondendo queste cartelle dalle scansioni AV) o di preferenza. Le istantanee di Cloud Volumes Service sono di sola lettura, quindi anche se sono visibili, gli utenti finali non possono eliminare o modificare i file nella

directory Snapshot. Si applicano le autorizzazioni per i file o le cartelle al momento dell'esecuzione della copia Snapshot. Se le autorizzazioni di un file o di una cartella cambiano tra le copie Snapshot, le modifiche si applicano anche ai file o alle cartelle nella directory Snapshot. Utenti e gruppi possono accedere a questi file o cartelle in base alle autorizzazioni. Sebbene non sia possibile eliminare o modificare i file nella directory Snapshot, è possibile copiare file o cartelle dalla directory Snapshot.

- **Attiva la crittografia SMB (disponibile sia per CVS-Performance che per CVS-SW).** la crittografia SMB è disattivata per impostazione predefinita nella condivisione SMB (non selezionata). Selezionando la casella viene attivata la crittografia SMB, il che significa che il traffico tra il client SMB e il server viene crittografato in-flight con i livelli di crittografia più elevati supportati negoziati. Cloud Volumes Service supporta la crittografia fino a AES-256 per le PMI. L'attivazione della crittografia SMB comporta una penalizzazione delle performance che potrebbe o meno essere evidente per i client SMB, approssimativamente nell'intervallo 10-20%. NetApp incoraggia vivamente i test per verificare se tale penalizzazione delle performance è accettabile.
- **Nascondi condivisione SMB (disponibile sia per CVS-Performance che CVS-SW).** l'impostazione di questa opzione nasconde il percorso di condivisione SMB dalla normale navigazione. Ciò significa che i client che non conoscono il percorso di condivisione non possono visualizzare le condivisioni quando accedono al percorso UNC predefinito (ad esempio `\\CVS-SMB`). Quando la casella di controllo è selezionata, solo i client che conoscono esplicitamente il percorso di condivisione SMB o che hanno il percorso di condivisione definito da un oggetto Criteri di gruppo possono accedervi (sicurezza tramite offuscamento).
- **Enable access-based enumeration (ABE) (solo CVS-SW).** questo è simile a nascondere la condivisione SMB, tranne che le condivisioni o i file sono nascosti solo agli utenti o ai gruppi che non dispongono delle autorizzazioni per accedere agli oggetti. Ad esempio, se utente Windows `joe` Non è consentito almeno l'accesso in lettura tramite le autorizzazioni, quindi l'utente Windows `joe` Impossibile visualizzare la condivisione SMB o i file. Questa opzione è disattivata per impostazione predefinita ed è possibile attivarla selezionando la casella di controllo. Per ulteriori informazioni su ABE, consultare l'articolo della Knowledge base di NetApp "Come funziona Access Based Enumeration (ABE)?"
- **Attiva il supporto delle condivisioni CA (Continuously Available) (solo CVS-Performance).** "Condivisioni SMB sempre disponibili" Fornire un modo per ridurre al minimo le interruzioni delle applicazioni durante gli eventi di failover replicando gli stati di blocco tra i nodi nel sistema di back-end Cloud Volumes Service. Non si tratta di una funzionalità di sicurezza, ma offre una migliore resilienza generale. Attualmente, solo le applicazioni SQL Server e FSLogix sono supportate per questa funzionalità.

Condivisioni nascoste predefinite

Quando viene creato un server SMB in Cloud Volumes Service, ne esistono "condivisioni amministrative nascoste" (Utilizzando la convenzione di naming in dollari) creati in aggiunta alla condivisione SMB del volume di dati. Questi includono l'accesso allo spazio dei nomi e l'IPC (sharing named pipe for communication between programs, come le chiamate di procedura remota (RPC) utilizzate per l'accesso a Microsoft Management Console (MMC)).

La condivisione IPC non contiene ACL di condivisione e non può essere modificata, ma viene utilizzata esclusivamente per le chiamate RPC e. "Per impostazione predefinita, Windows non consente l'accesso anonimo a queste condivisioni".

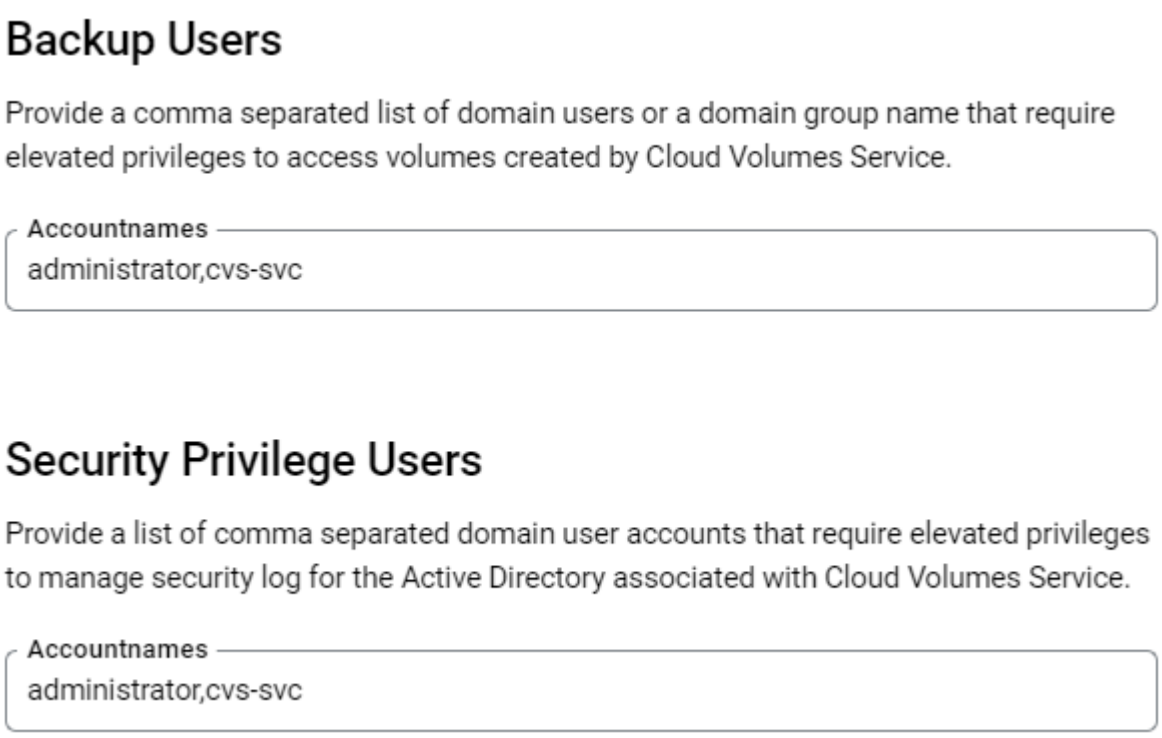
La condivisione consente l'accesso predefinito a BUILTIN/Administrators, ma l'automazione Cloud Volumes Service rimuove l'ACL della condivisione e non consente l'accesso a nessuno perché l'accesso alla condivisione consente la visibilità di tutti i volumi montati nei file system Cloud Volumes Service. Di conseguenza, tenta di accedere a. `\\SERVER\C$` non riuscito.

Account con diritti di amministratore/backup locali/BUILTIN

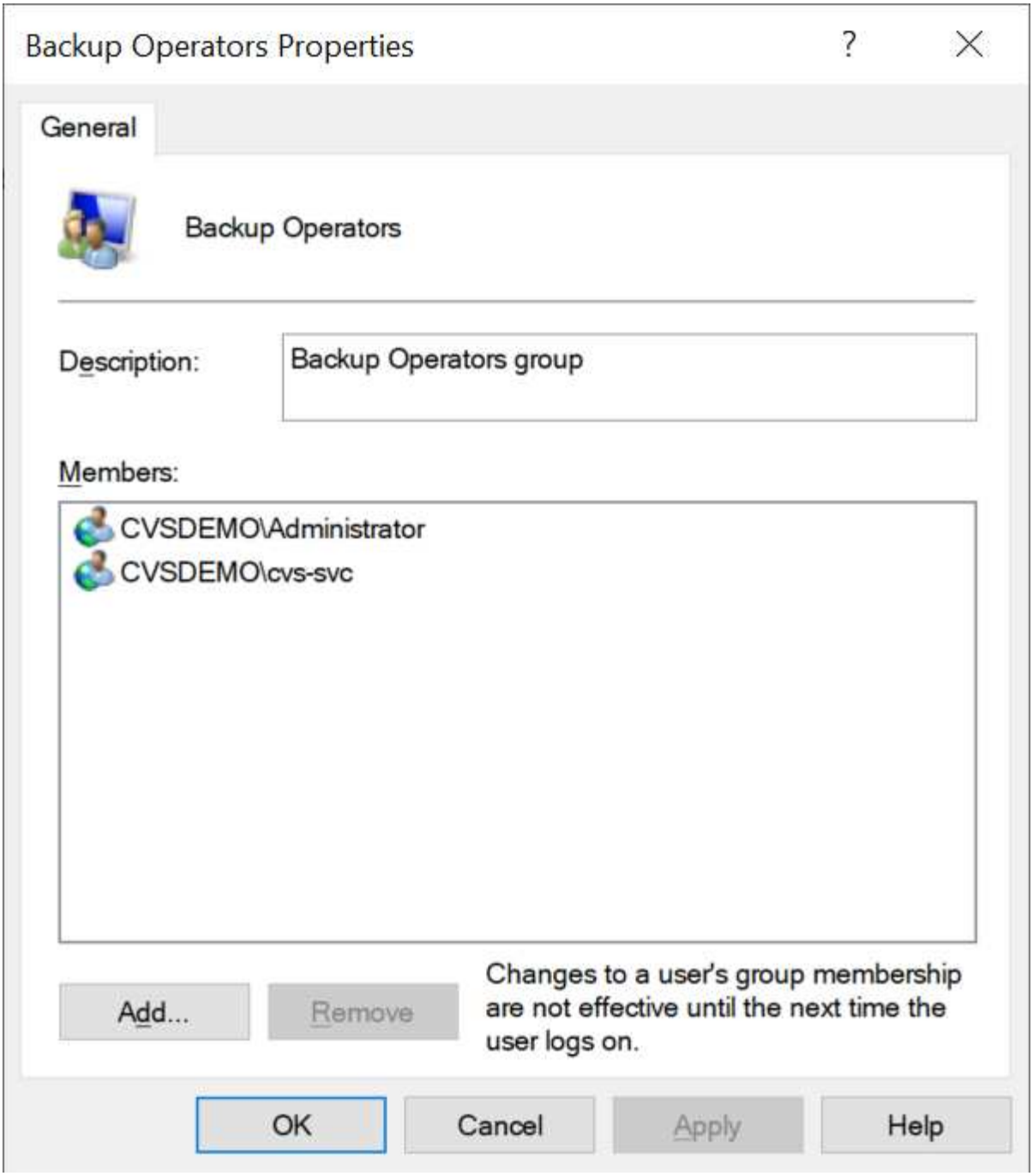
I server SMB di Cloud Volumes Service mantengono una funzionalità simile a quella dei normali server SMB di Windows, in quanto esistono gruppi locali (ad esempio BUILTIN/amministratori) che applicano i diritti di accesso a utenti e gruppi di dominio selezionati.

Quando si specifica un utente da aggiungere agli utenti di backup, l'utente viene aggiunto al gruppo BUILTIN/Backup Operators nell'istanza di Cloud Volumes Service che utilizza tale connessione, che ottiene quindi "SeBackupPrivilege e SeRestorePrivilege".

Quando si aggiunge un utente a Security Privilege Users, all'utente viene assegnato il privilegio SeSecurityPrivilege, utile in alcuni casi di utilizzo dell'applicazione, ad esempio "SQL Server su condivisioni SMB".



È possibile visualizzare le appartenenze ai gruppi locali di Cloud Volumes Service tramite MMC con i privilegi appropriati. La figura seguente mostra gli utenti aggiunti utilizzando la console di Cloud Volumes Service.

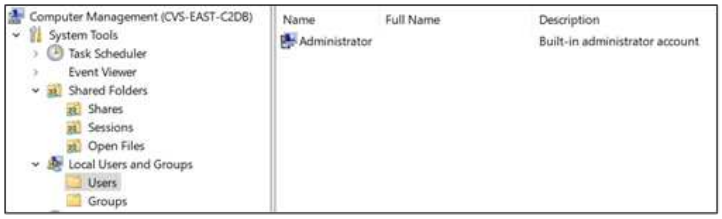


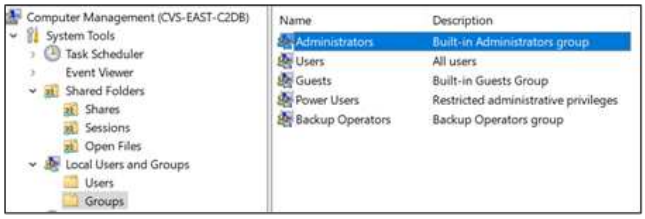
La seguente tabella mostra l'elenco dei gruppi BUILTIN predefiniti e gli utenti/gruppi aggiunti per impostazione predefinita.

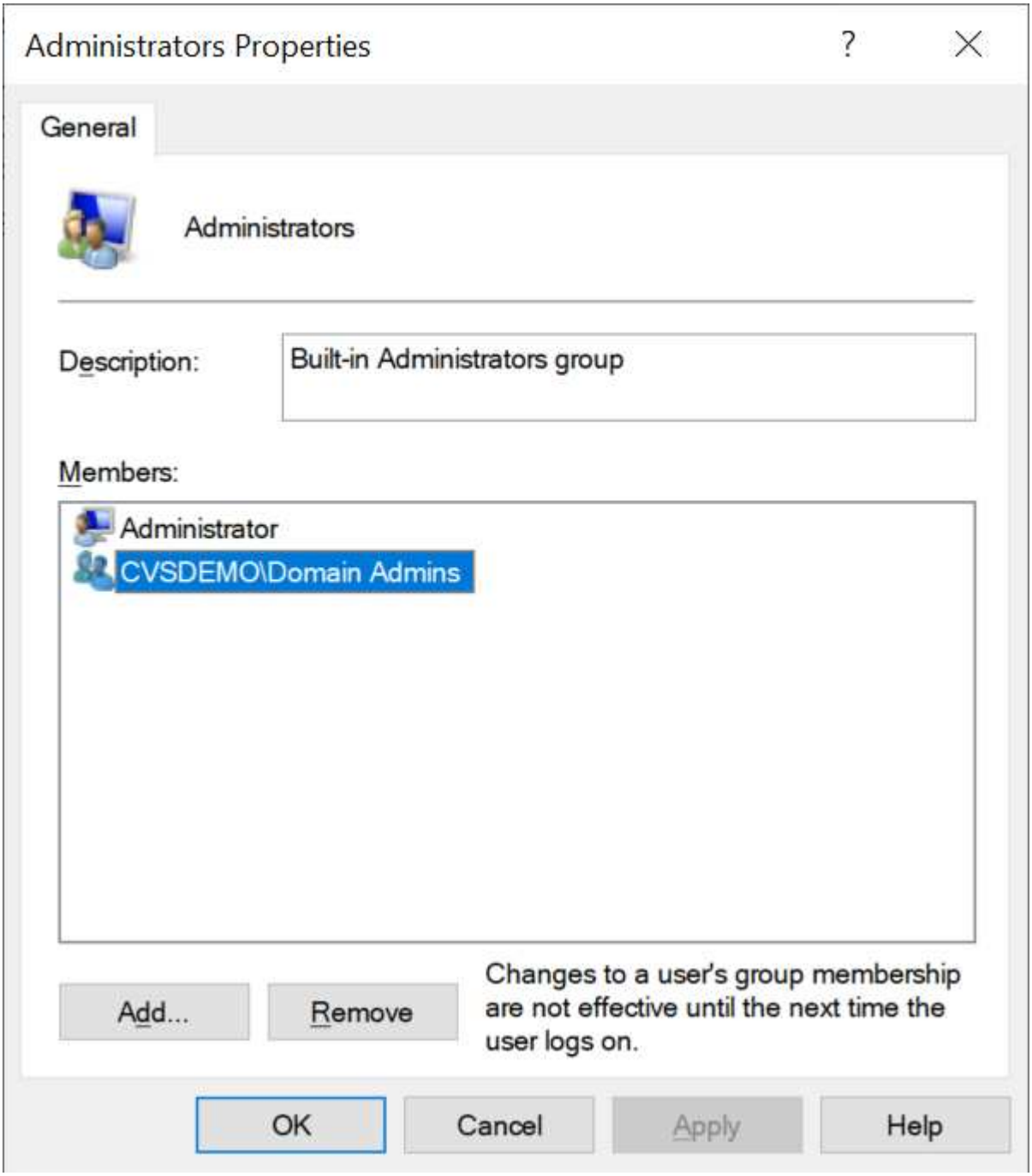
Locale/gruppo BUILTIN	Membri predefiniti
BUILTIN/amministratori*	AMMINISTRATORI DI DOMINIO/dominio
BUILTIN/Backup Operator*	Nessuno
BUILTIN/guest	Dominio/dominio guest
UTENTI BUILTIN/Power	Nessuno
UTENTI BUILTIN/dominio	UTENTI DI DOMINIO/dominio

*Appartenenza al gruppo controllata nella configurazione della connessione ad Active Directory di Cloud Volumes Service.

È possibile visualizzare gli utenti e i gruppi locali (e i membri del gruppo) nella finestra MMC, ma non è possibile aggiungere o eliminare oggetti o modificare le appartenenze ai gruppi da questa console. Per impostazione predefinita, solo il gruppo Domain Admins e l'amministratore vengono aggiunti al gruppo BUILTIN/Administrators in Cloud Volumes Service. Al momento, non è possibile modificarlo.







Accesso MMC/Gestione computer

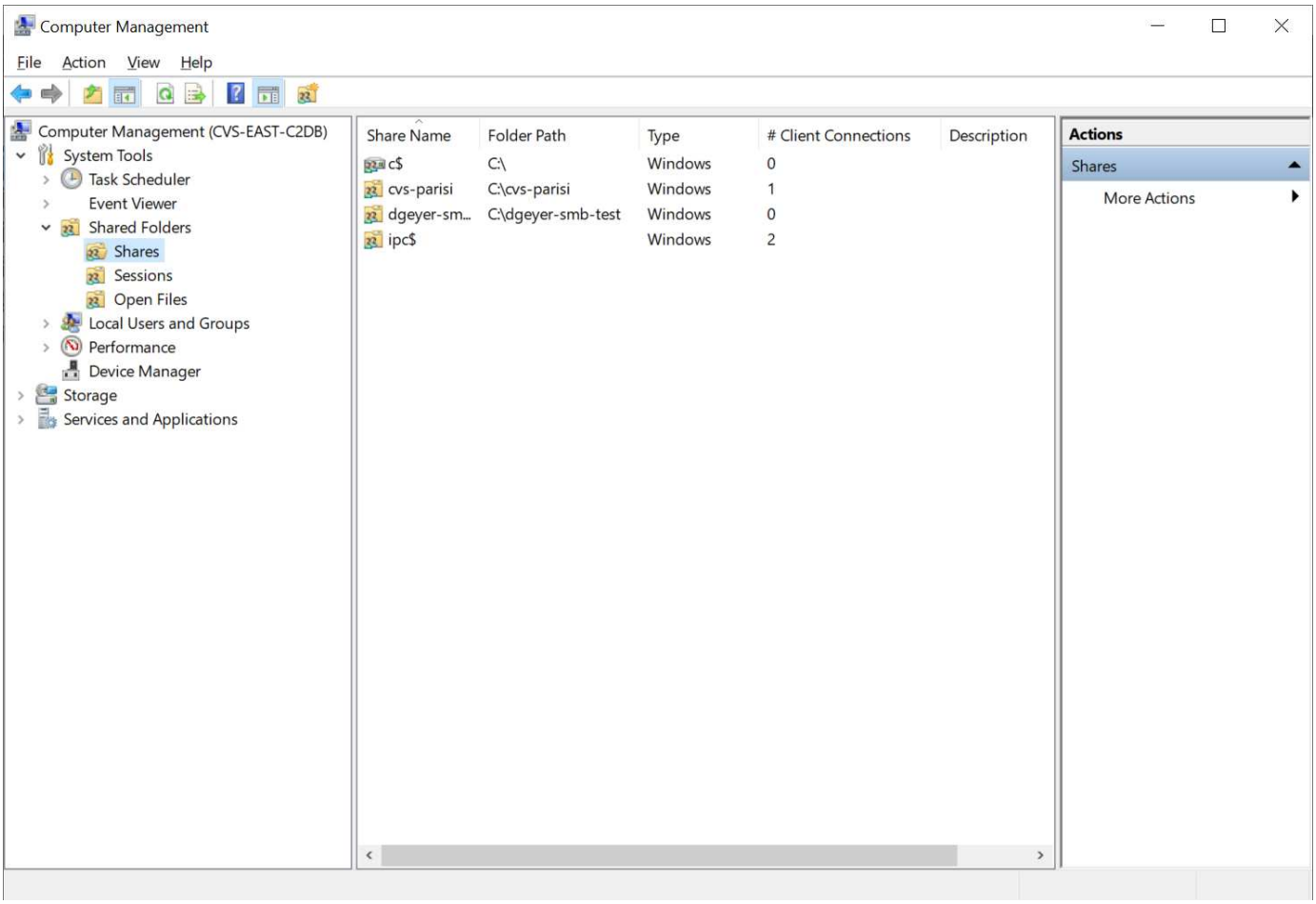
L'accesso SMB in Cloud Volumes Service fornisce la connettività alla MMC Gestione computer, che consente di visualizzare le condivisioni, gestire gli ACL delle condivisioni, visualizzare/gestire le sessioni SMB e aprire i file.

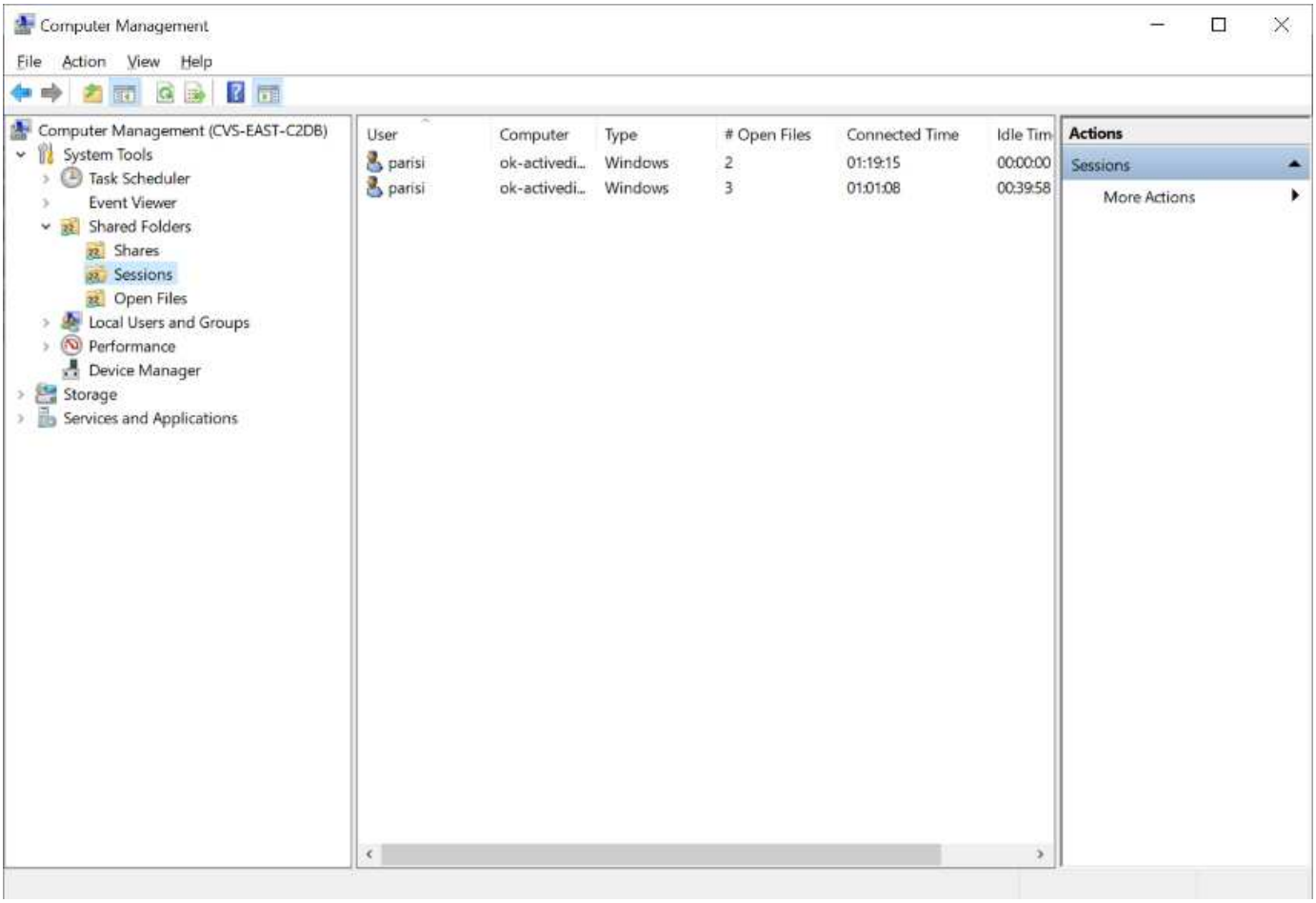
Per utilizzare MMC per visualizzare le condivisioni SMB e le sessioni in Cloud Volumes Service, l'utente attualmente connesso deve essere un amministratore di dominio. Agli altri utenti è consentito l'accesso per visualizzare o gestire il server SMB da MMC e ricevere una finestra di dialogo non si dispone delle autorizzazioni quando si tenta di visualizzare condivisioni o sessioni sull'istanza SMB di Cloud Volumes Service.

Per connettersi al server SMB, aprire Gestione computer, fare clic con il pulsante destro del mouse su Gestione computer, quindi selezionare Connetti a un altro computer. Viene visualizzata la finestra di dialogo Seleziona computer, in cui è possibile immettere il nome del server SMB (disponibile nelle informazioni sul volume Cloud Volumes Service).

Quando si visualizzano le condivisioni SMB con le autorizzazioni appropriate, vengono visualizzate tutte le condivisioni disponibili nell'istanza di Cloud Volumes Service che condividono la connessione Active Directory. Per controllare questo comportamento, impostare l'opzione Nascondi condivisioni SMB sull'istanza del volume Cloud Volumes Service.

Tenere presente che è consentita una sola connessione Active Directory per regione.





La seguente tabella mostra un elenco delle funzionalità supportate/non supportate per MMC.

Funzioni supportate	Funzioni non supportate
• Visualizza condivisioni • Visualizzare le sessioni SMB attive • Visualizzare i file aperti • Visualizzare utenti e gruppi locali • Visualizzare le appartenenze ai gruppi locali • Enumerare l'elenco di sessioni, file e connessioni ad albero nel sistema • Chiudere i file aperti nel sistema • Chiudere le sessioni aperte • Creare/gestire le condivisioni	• Creazione di nuovi utenti/gruppi locali • Gestione/visualizzazione di utenti/gruppi locali esistenti • Visualizza eventi o log delle performance • Gestione dello storage • Gestione di servizi e applicazioni

Informazioni sulla sicurezza dei server SMB

Il server SMB di Cloud Volumes Service utilizza una serie di opzioni che definiscono le policy di sicurezza per le connessioni SMB, tra cui l'inclinazione del clock Kerberos, l'età del ticket, la crittografia e molto altro ancora.

La seguente tabella contiene un elenco di queste opzioni, le loro funzioni, le configurazioni predefinite e se possono essere modificate con Cloud Volumes Service. Alcune opzioni non si applicano a Cloud Volumes

Service.

Opzione di sicurezza	Che cosa fa	Valore predefinito	Può cambiare?
Inclinazione massima del clock Kerberos (minuti)	Disallineamento massimo del tempo tra Cloud Volumes Service e i controller di dominio. Se l'intervallo di tempo supera i 5 minuti, l'autenticazione Kerberos non riesce. Viene impostato sul valore predefinito di Active Directory.	5	No
Durata ticket Kerberos (ore)	Tempo massimo in cui un ticket Kerberos rimane valido prima di richiedere un rinnovo. Se non si verifica alcun rinnovo prima delle 10 ore, è necessario ottenere un nuovo biglietto. Cloud Volumes Service esegue automaticamente questi rinnovi. 10 ore è il valore predefinito di Active Directory.	10	No
Rinnovo massimo ticket Kerberos (giorni)	Numero massimo di giorni in cui un ticket Kerberos può essere rinnovato prima che sia necessaria una nuova richiesta di autorizzazione. Cloud Volumes Service rinnova automaticamente i ticket per le connessioni SMB. Sette giorni è il valore predefinito di Active Directory.	7	No
Timeout connessione KDC Kerberos (sec)	Il numero di secondi prima del timeout di una connessione KDC.	3	No
Richiedi firma per traffico SMB in entrata	Impostazione per richiedere la firma per il traffico SMB. Se impostata su true, i client che non supportano la firma non riescono a connettersi.	Falso	

Opzione di sicurezza	Che cosa fa	Valore predefinito	Può cambiare?
Richiedi complessità password per account utente locali	Utilizzato per le password degli utenti SMB locali. Cloud Volumes Service non supporta la creazione di utenti locali, pertanto questa opzione non si applica a Cloud Volumes Service.	Vero	No
Utilizzare start_tls per le connessioni LDAP di Active Directory	Utilizzato per attivare le connessioni TLS iniziali per Active Directory LDAP. Cloud Volumes Service attualmente non supporta l'abilitazione di questa opzione.	Falso	No
AES-128 e AES-256 Encryption for Kerberos sono abilitati	In questo modo si controlla se la crittografia AES viene utilizzata per le connessioni Active Directory e viene controllata con l'opzione Enable AES Encryption for Active Directory Authentication (attiva crittografia AES per l'autenticazione Active Directory) quando si crea o si modifica la connessione Active Directory.	Falso	Sì
Livello di compatibilità LM	Livello dei dialetti di autenticazione supportati per le connessioni Active Directory. Vedere la sezione "Dialetti di autenticazione SMB" per ulteriori informazioni.	ntlmv2-krb	No
Richiedi crittografia SMB per traffico CIFS in entrata	Richiede la crittografia SMB per tutte le condivisioni. Questa opzione non viene utilizzata da Cloud Volumes Service; impostare invece la crittografia per volume (vedere la sezione "SMB condivide le funzionalità di sicurezza").	Falso	No

Opzione di sicurezza	Che cosa fa	Valore predefinito	Può cambiare?
Sicurezza della sessione client	Imposta la firma e/o il sealing per la comunicazione LDAP. Questa opzione non è attualmente impostata in Cloud Volumes Service, ma potrebbe essere necessaria nelle versioni future per risolvere . La risoluzione dei problemi di autenticazione LDAP dovuti alla patch di Windows è descritta nella sezione ""Associazione del canale LDAP"."".	Nessuno	No
Abilitazione SMB2 per connessioni DC	Utilizza SMB2 per le connessioni DC. Attivato per impostazione predefinita.	System-default	No
LDAP Referral Chasing	Quando si utilizzano più server LDAP, la ricerca dei riferimenti consente al client di fare riferimento ad altri server LDAP nell'elenco quando non viene trovata una voce nel primo server. Attualmente non è supportato da Cloud Volumes Service.	Falso	No
Utilizzare LDAPS per connessioni Active Directory sicure	Attiva l'utilizzo di LDAP su SSL. Attualmente non supportato da Cloud Volumes Service.	Falso	No
La crittografia è necessaria per la connessione DC	Richiede la crittografia per le connessioni DC riuscite. Disattivato per impostazione predefinita in Cloud Volumes Service.	Falso	No

Protocollo doppio/multiprotocollo

Cloud Volumes Service offre la possibilità di condividere gli stessi set di dati con client SMB e NFS mantenendo le autorizzazioni di accesso appropriate ("protocollo doppio"). Ciò avviene coordinando il mapping delle identità tra i protocolli e utilizzando un server LDAP backend centralizzato per fornire le identità UNIX a Cloud Volumes Service. È possibile utilizzare Windows Active Directory per fornire agli utenti Windows e UNIX una maggiore facilità di utilizzo.

Controllo degli accessi

- **Controlli di accesso alla condivisione.** determinare quali client e/o utenti e gruppi possono accedere a una condivisione NAS. Per NFS, le policy e le regole di esportazione controllano l'accesso dei client alle esportazioni. Le esportazioni NFS vengono gestite dall'istanza di Cloud Volumes Service. SMB utilizza le condivisioni CIFS/SMB e gli ACL di condivisione per fornire un controllo più granulare a livello di utente e gruppo. È possibile configurare gli ACL a livello di condivisione solo dai client SMB utilizzando "Gestione MMC/computer" Con un account che dispone dei diritti di amministratore sull'istanza di Cloud Volumes Service (vedere la sezione ""Account con diritti di backup/amministratore BUILTIN locale."").
- **File access control.** Controlla le autorizzazioni a livello di file o cartella e sono sempre gestite dal client NAS. I client NFS possono utilizzare i bit di modalità tradizionali (rwx) o gli ACL NFSv4. I client SMB sfruttano le autorizzazioni NTFS.

Il controllo dell'accesso per i volumi che servono dati a NFS e SMB dipende dal protocollo in uso. Per informazioni sulle autorizzazioni con protocollo doppio, vedere la sezione "Modello di permesso."

Mappatura dell'utente

Quando un client accede a un volume, Cloud Volumes Service tenta di mappare l'utente in entrata a un utente valido nella direzione opposta. Ciò è necessario per determinare l'accesso corretto tra i protocolli e per garantire che l'utente che richiede l'accesso sia effettivamente quello che afferma di essere.

Ad esempio, se un utente Windows ha denominato `joe` Tenta di accedere a un volume con autorizzazioni UNIX tramite SMB, quindi Cloud Volumes Service esegue una ricerca per trovare un utente UNIX corrispondente denominato `joe`. Se ne esiste uno, i file scritti in una condivisione SMB come utente Windows `joe` Viene visualizzato come utente UNIX `joe` Dai client NFS.

In alternativa, se si chiama un utente UNIX `joe` Tenta di accedere a un volume Cloud Volumes Service con autorizzazioni Windows, quindi l'utente UNIX deve essere in grado di eseguire il mapping a un utente Windows valido. In caso contrario, l'accesso al volume viene negato.

Attualmente, solo Active Directory è supportato per la gestione esterna delle identità UNIX con LDAP. Per ulteriori informazioni sulla configurazione dell'accesso a questo servizio, vedere "Creazione di una connessione ad".

Modello di permesso

Quando si utilizzano configurazioni a doppio protocollo, Cloud Volumes Service utilizza gli stili di sicurezza per i volumi per determinare il tipo di ACL. Questi stili di sicurezza vengono impostati in base al protocollo NAS specificato o, nel caso del protocollo doppio, è possibile scegliere al momento della creazione del volume Cloud Volumes Service.

- Se si utilizza solo NFS, i volumi Cloud Volumes Service utilizzano le autorizzazioni UNIX.
- Se si utilizza solo SMB, i volumi Cloud Volumes Service utilizzano le autorizzazioni NTFS.

Se si crea un volume a doppio protocollo, è possibile scegliere lo stile ACL alla creazione del volume. Questa decisione deve essere presa in base alla gestione delle autorizzazioni desiderata. Se gli utenti gestiscono le autorizzazioni dai client Windows/SMB, selezionare NTFS. Se gli utenti preferiscono utilizzare client NFS e chmod/chown, utilizzare gli stili di sicurezza UNIX.

Considerazioni per la creazione di connessioni Active Directory

Cloud Volumes Service consente di connettere l'istanza di Cloud Volumes Service a un

server Active Directory esterno per la gestione delle identità per gli utenti SMB e UNIX. Per utilizzare SMB in Cloud Volumes Service è necessario creare una connessione Active Directory.

La configurazione fornisce diverse opzioni che richiedono una certa considerazione per la sicurezza. Il server Active Directory esterno può essere un'istanza on-premise o nativo del cloud. Se si utilizza un server Active Directory on-premise, non esporre il dominio alla rete esterna (ad esempio con un DMZ o un indirizzo IP esterno). Utilizzare, invece, tunnel privati o VPN sicuri, trust di foresta unirway o connessioni di rete dedicate alle reti on-premise con "Accesso privato a Google". Per ulteriori informazioni su, consultare la documentazione di Google Cloud "Best practice per l'utilizzo di Active Directory in Google Cloud".

> CVS-SW richiede che i server Active Directory si trovino nella stessa regione. Se si tenta di stabilire una connessione CC in CVS-SW con un'altra regione, il tentativo non riesce. Quando si utilizza CVS-SW, assicurarsi di creare siti Active Directory che includono i controller di dominio Active Directory e specificare i siti in Cloud Volumes Service per evitare tentativi di connessione DC tra regioni.

Credenziali di Active Directory

Quando SMB o LDAP per NFS è attivato, Cloud Volumes Service interagisce con i controller di Active Directory per creare un oggetto account macchina da utilizzare per l'autenticazione. Questo non è diverso dal modo in cui un client SMB di Windows si unisce a un dominio e richiede gli stessi diritti di accesso alle unità organizzative (OU) in Active Directory.

In molti casi, i gruppi di protezione non consentono l'utilizzo di un account amministratore di Windows su server esterni come Cloud Volumes Service. In alcuni casi, l'utente amministratore di Windows viene disattivato completamente come procedura consigliata per la protezione.

Autorizzazioni necessarie per creare account di macchine SMB

Per aggiungere oggetti computer Cloud Volumes Service a un'Active Directory, un account che dispone di diritti amministrativi per il dominio o che dispone di "autorizzazioni delegate per creare e modificare oggetti account macchina" A un'unità organizzativa specificata. È possibile eseguire questa operazione con la delega guidata del controllo in Active Directory creando un'attività personalizzata che fornisce all'utente l'accesso alla creazione/eliminazione di oggetti computer con le seguenti autorizzazioni di accesso:

- Lettura/scrittura
- Crea/Elimina tutti gli oggetti figlio
- Lettura/scrittura di tutte le proprietà
- Modificare/reimpostare la password

Questa operazione consente di aggiungere automaticamente un ACL di sicurezza per l'utente definito all'unità organizzativa in Active Directory e di ridurre al minimo l'accesso all'ambiente Active Directory. Dopo la delega di un utente, il nome utente e la password possono essere forniti come credenziali Active Directory in questa finestra.

> Il nome utente e la password passati al dominio Active Directory sfruttano la crittografia Kerberos durante la query e la creazione dell'oggetto account del computer per una maggiore sicurezza.

Dettagli della connessione ad Active Directory

Il "Dettagli connessione Active Directory" Fornire agli amministratori campi per fornire informazioni specifiche sullo schema di Active Directory per il posizionamento degli account del computer, ad esempio:

- **Tipo di connessione Active Directory.** consente di specificare se la connessione Active Directory in una regione viene utilizzata per volumi di tipo Cloud Volumes Service o CVS-Performance. Se questa impostazione non è corretta su una connessione esistente, potrebbe non funzionare correttamente quando viene utilizzata o modificata.
- **Domain.** il nome di dominio di Active Directory.
- **Site.** limita i server Active Directory a un sito specifico per motivi di sicurezza e performance "considerazioni". Ciò è necessario quando più server Active Directory si estendono in aree diverse, in quanto Cloud Volumes Service attualmente non supporta l'autorizzazione di richieste di autenticazione Active Directory per i server Active Directory in un'area diversa dall'istanza di Cloud Volumes Service. Ad esempio, il controller di dominio Active Directory si trova in un'area supportata solo da CVS-Performance, ma si desidera una condivisione SMB in un'istanza CVS-SW.
- **Server DNS.** server DNS da utilizzare nelle ricerche dei nomi.
- **Nome NetBIOS (opzionale).** se lo si desidera, il nome NetBIOS del server. Questa opzione viene utilizzata quando vengono creati nuovi account computer utilizzando la connessione Active Directory. Ad esempio, se il nome NetBIOS è impostato su CVS-EAST, i nomi degli account del computer saranno CVS-EAST-{1234}. Vedere la sezione "Come viene visualizzato Cloud Volumes Service in Active Directory" per ulteriori informazioni.
- **Unità organizzativa (OU).** unità organizzativa specifica per la creazione dell'account del computer. Ciò è utile se si sta delegando il controllo a un utente per gli account di computer a una specifica unità organizzativa.
- **Crittografia AES.** è inoltre possibile selezionare o deselezionare la casella di controllo Enable AES Encryption for ad Authentication. L'attivazione della crittografia AES per l'autenticazione di Active Directory offre una maggiore sicurezza per le comunicazioni Cloud Volumes Service-Active Directory durante le ricerche di utenti e gruppi. Prima di attivare questa opzione, rivolgersi all'amministratore di dominio per verificare che i controller di dominio Active Directory supportino l'autenticazione AES.

> Per impostazione predefinita, la maggior parte dei server Windows non disattiva le crittografia più deboli (AD esempio DES o RC4-HMAC), ma se si sceglie di disattivare le crittografia più deboli, verificare che la connessione Active Directory di Cloud Volumes Service sia stata configurata per abilitare AES. In caso contrario, si verificano errori di autenticazione. L'attivazione della crittografia AES non disattiva le crittografie più deboli, ma aggiunge il supporto per le crittografie AES all'account della macchina SMB di Cloud Volumes Service.

Dettagli area di autenticazione Kerberos

Questa opzione non si applica ai server SMB. Viene invece utilizzato durante la configurazione di NFS Kerberos per il sistema Cloud Volumes Service. Quando questi dettagli vengono popolati, viene configurato l'ambiente Kerberos NFS (simile a un file krb5.conf su Linux) e viene utilizzato quando NFS Kerberos viene specificato nella creazione del volume Cloud Volumes Service, in quanto la connessione Active Directory agisce come centro di distribuzione Kerberos NFS (KDC).

> Attualmente i KDC non Windows non sono supportati per l'utilizzo con Cloud Volumes Service.

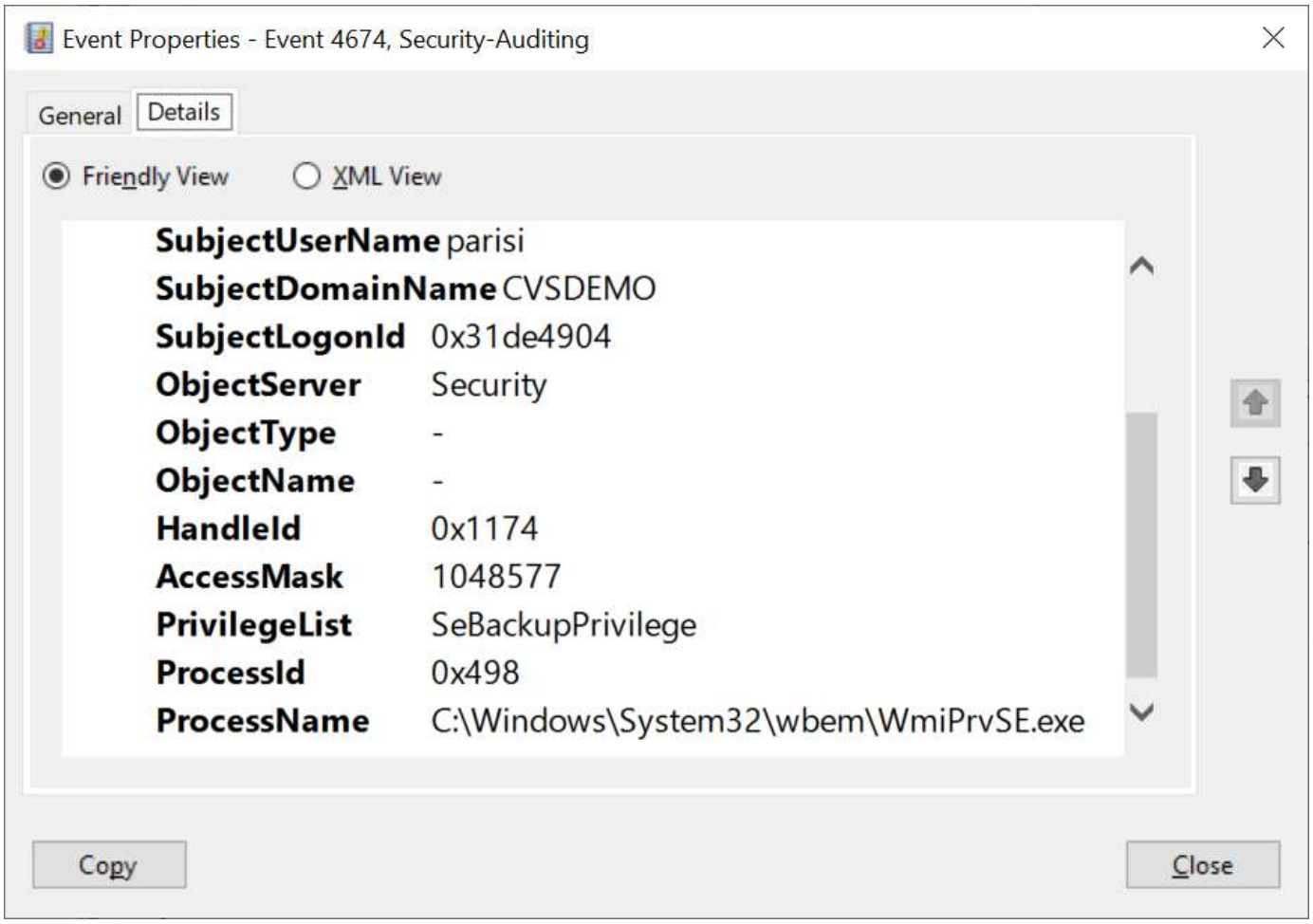
Regione

Una regione consente di specificare la posizione in cui risiede la connessione Active Directory. Questa regione deve essere la stessa del volume Cloud Volumes Service.

- **Local NFS Users with LDAP.** in questa sezione è disponibile anche un'opzione per consentire agli utenti NFS locali con LDAP. Questa opzione deve essere lasciata deselezionata se si desidera estendere il supporto dell'appartenenza al gruppo di utenti UNIX oltre la limitazione di 16 gruppi di NFS (gruppi estesi). Tuttavia, l'utilizzo di gruppi estesi richiede un server LDAP configurato per le identità UNIX. Se non si dispone di un server LDAP, lasciare deselezionata questa opzione. Se si dispone di un server LDAP e si desidera utilizzare anche utenti UNIX locali (ad esempio root), selezionare questa opzione.

Utenti di backup

Questa opzione consente di specificare gli utenti Windows che dispongono delle autorizzazioni di backup per il volume Cloud Volumes Service. I privilegi di backup (SeBackupPrivilege) sono necessari per consentire ad alcune applicazioni di eseguire correttamente il backup e il ripristino dei dati nei volumi NAS. Questo utente dispone di un elevato livello di accesso ai dati nel volume, pertanto è necessario prendere in considerazione l'opzione "abilitazione del controllo dell'accesso dell'utente". Una volta attivato, gli eventi di controllo vengono visualizzati nel Visualizzatore eventi > Log di Windows > protezione.



Utenti con privilegi di sicurezza

Questa opzione consente di specificare gli utenti Windows che dispongono delle autorizzazioni per la modifica della protezione per il volume Cloud Volumes Service. Alcuni privilegi di sicurezza (SeSecurityPrivilege) sono necessari per alcune applicazioni ("Ad esempio SQL Server") per impostare correttamente le autorizzazioni

durante l'installazione. Questo privilegio è necessario per gestire il registro di protezione. Sebbene questo privilegio non sia potente come SeBackupPrivilege, NetApp consiglia "controllo dell'accesso degli utenti" con questo livello di privilegio, se necessario.

Per ulteriori informazioni, vedere "Privilegi speciali assegnati al nuovo accesso".

Come viene visualizzato Cloud Volumes Service in Active Directory

Cloud Volumes Service viene visualizzato in Active Directory come un normale oggetto account del computer. Le convenzioni di denominazione sono le seguenti.

- CIFS/SMB e NFS Kerberos creano oggetti account macchina separati.
- NFS con LDAP attivato crea un account macchina in Active Directory per i binding LDAP Kerberos.
- I volumi a doppio protocollo con LDAP condividono l'account CIFS/SMB per LDAP e SMB.
- Gli account CIFS/SMB utilizzano una convenzione di naming name-1234 (ID casuale a quattro cifre con trattino aggiunto al nome <10 caratteri) per l'account del computer. È possibile definire IL NOME in base all'impostazione NetBIOS name (Nome NetBIOS) sulla connessione Active Directory (vedere la sezione "Dettagli della connessione ad Active Directory").
- NFS Kerberos utilizza NFS-NAME-1234 come convenzione di naming (fino a 15 caratteri). Se vengono utilizzati più di 15 caratteri, il nome è NFS-TRONCED-NAME-1234.
- Le istanze CVS-Performance solo NFS con LDAP attivato creano un account SMB Machine per l'associazione al server LDAP con la stessa convenzione di denominazione delle istanze CIFS/SMB.
- Quando viene creato un account SMB Machine, le condivisioni amministrative nascoste predefinite (vedere la sezione ""Condivisioni nascoste predefinite""), ma tali condivisioni non hanno ACL assegnati e non sono accessibili.
- Per impostazione predefinita, gli oggetti del centro di costo del computer vengono posizionati in CN=Computers, ma R è possibile specificare un'unità organizzativa diversa quando necessario. Vedere la sezione "Autorizzazioni necessarie per creare account di macchine SMB" Per informazioni sui diritti di accesso necessari per aggiungere/rimuovere oggetti account macchina per Cloud Volumes Service.

Quando Cloud Volumes Service aggiunge l'account del computer SMB ad Active Directory, vengono compilati i seguenti campi:

- cn (con il nome del server SMB specificato)
- DNSHostName (con SMBserver.domain.com)
- MSDS-SupportedEncryptionTypes (supporta DES_CBC_MD5, RC4_HMAC_MD5 se la crittografia AES non è attivata; se la crittografia AES è attivata, DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 sono consentiti per lo scambio di account con il ticket SMB)
- Nome (con il nome del server SMB)
- SAMAccountName (con SMBserver)
- ServicePrincipalName (con host/smbserver.domain.com e host/smbserver SPN per Kerberos)

Se si desidera disattivare i tipi di crittografia Kerberos più deboli (enctype) sull'account del computer, è possibile modificare il valore MSDS-SupportedEncryptionTypes sull'account del computer scegliendo uno dei valori nella tabella seguente per consentire solo AES.

Valore MSDS-SupportedEncryptionTypes	Entype attivato
2	DES_CBC_MD5
4	RC4_HMAC
8	SOLO AES128_CTS_HMAC_SHA1_96
16	SOLO AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 E AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 E AES256_CTS_HMAC_SHA1_96

Per attivare la crittografia AES per gli account dei computer SMB, fare clic su Enable AES Encryption for ad Authentication (attiva crittografia AES per l'autenticazione ad) quando si crea la connessione Active Directory.

Per attivare la crittografia AES per NFS Kerberos, "Consultare la documentazione di Cloud Volumes Service".

Altre dipendenze del servizio infrastruttura NAS (KDC, LDAP e DNS)

Quando si utilizza Cloud Volumes Service per le condivisioni NAS, potrebbero essere necessarie dipendenze esterne per un corretto funzionamento. Queste dipendenze sono in gioco in circostanze specifiche. La seguente tabella mostra le varie opzioni di configurazione e le eventuali dipendenze richieste.

Configurazione	Dipendenze richieste
Solo NFSv3	Nessuno
Solo NFSv3 Kerberos	Active Directory di Windows: * KDC * DNS * LDAP
Solo NFSv4.1	Configurazione mappatura ID client (/etc/idmap.conf)
Solo NFSv4.1 Kerberos	• Configurazione mappatura ID client (/etc/idmap.conf) • Active Directory di Windows: LDAP DNS KDC
Solo SMB	Active Directory: * KDC * DNS
NAS multiprotocollo (NFS e SMB)	• Configurazione del mapping dell'ID client (solo NFSv4.1; /etc/idmap.conf) • Active Directory di Windows: LDAP DNS KDC

La rotazione/password del keytab Kerberos viene reimpostata per gli oggetti account macchina

Con gli account delle macchine SMB, Cloud Volumes Service pianifica il ripristino periodico delle password per l'account delle macchine SMB. Queste password vengono reimpostate utilizzando la crittografia Kerberos e vengono eseguite ogni quarta domenica in un orario casuale compreso tra LE 23:00 e L'1:00. Queste reimpostazioni delle password modificano le versioni delle chiavi Kerberos, ruotano le linguette memorizzate nel sistema Cloud Volumes Service e contribuiscono a mantenere un livello di sicurezza maggiore per i server SMB in esecuzione in Cloud Volumes Service. Le password dell'account macchina sono casuali e non sono

note agli amministratori.

Per gli account delle macchine Kerberos NFS, la reimpostazione delle password avviene solo quando viene creata o scambiata una nuova keytab con il KDC. Attualmente, non è possibile eseguire questa operazione in Cloud Volumes Service.

Porte di rete per l'utilizzo con LDAP e Kerberos

Quando si utilizzano LDAP e Kerberos, è necessario determinare le porte di rete utilizzate da questi servizi. L'elenco completo delle porte utilizzate da Cloud Volumes Service è disponibile nella "Documentazione Cloud Volumes Service sulle considerazioni relative alla sicurezza".

LDAP

Cloud Volumes Service agisce come client LDAP e utilizza le query di ricerca LDAP standard per le ricerche di utenti e gruppi per le identità UNIX. LDAP è necessario se si intende utilizzare utenti e gruppi al di fuori degli utenti predefiniti standard forniti da Cloud Volumes Service. LDAP è necessario anche se si prevede di utilizzare NFS Kerberos con le identità dell'utente (ad esempio user1@domain.com). Attualmente, è supportato solo LDAP con Microsoft Active Directory.

Per utilizzare Active Directory come server LDAP UNIX, è necessario popolare gli attributi UNIX necessari per gli utenti e i gruppi che si intende utilizzare per le identità UNIX. Cloud Volumes Service utilizza un modello di schema LDAP predefinito che esegue query sugli attributi in base a. "RFC-2307-bis". Di conseguenza, la seguente tabella mostra gli attributi minimi necessari di Active Directory da popolare per utenti e gruppi e per quale scopo viene utilizzato ciascun attributo.

Per ulteriori informazioni sull'impostazione degli attributi LDAP in Active Directory, vedere "Gestione dell'accesso a doppio protocollo."

Attributo	Che cosa fa
uid*	Specifica il nome utente UNIX
UidNumber*	Specifica l'ID numerico dell'utente UNIX
GidNumber*	Specifica l'ID numerico del gruppo primario dell'utente UNIX
Objectclass*	Specifica il tipo di oggetto utilizzato; Cloud Volumes Service richiede che l'opzione "user" sia inclusa nell'elenco delle classi di oggetti (per impostazione predefinita, è inclusa nella maggior parte delle implementazioni di Active Directory).
nome	Informazioni generali sull'account (nome reale, numero di telefono e così via, anche noto come gecos)
UnixUserPassword	Non è necessario impostare questo valore; non utilizzato nelle ricerche di identità UNIX per l'autenticazione NAS. Impostando questa opzione, il valore unixUserPassword configurato viene visualizzato in testo non crittografato.

Attributo	Che cosa fa
UnixHomeDirectory	Definisce il percorso delle home directory UNIX quando un utente esegue l'autenticazione LDAP da un client Linux. Impostare questa opzione se si desidera utilizzare la funzionalità della home directory LDAP per UNIX.
LoginShell	Definisce il percorso della shell bash/profile per i client Linux quando un utente esegue l'autenticazione con LDAP.

*Indica che l'attributo è necessario per la corretta funzionalità con Cloud Volumes Service. Gli attributi rimanenti sono solo per uso lato client.

Attributo	Che cosa fa
cn*	Specifica il nome del gruppo UNIX. Quando si utilizza Active Directory per LDAP, questo viene impostato quando l'oggetto viene creato per la prima volta, ma può essere modificato in seguito. Questo nome non può essere uguale ad altri oggetti. Ad esempio, se l'utente UNIX denominato user1 appartiene a un gruppo denominato user1 sul client Linux, Windows non consente due oggetti con lo stesso attributo cn. Per risolvere questo problema, rinominare l'utente Windows con un nome univoco (ad esempio, user1-UNIX); LDAP in Cloud Volumes Service utilizza l'attributo uid per i nomi utente UNIX.
GidNumber*	Specifica l'ID numerico del gruppo UNIX.
Objectclass*	Specifica il tipo di oggetto utilizzato; Cloud Volumes Service richiede che il gruppo sia incluso nell'elenco delle classi di oggetti (questo attributo è incluso per impostazione predefinita nella maggior parte delle implementazioni di Active Directory).
MemberUid	Specifica quali utenti UNIX sono membri del gruppo UNIX. Con Active Directory LDAP in Cloud Volumes Service, questo campo non è necessario. Lo schema LDAP di Cloud Volumes Service utilizza il campo membro per le appartenenze ai gruppi.
Membro*	Richiesto per le appartenenze a gruppi/gruppi UNIX secondari. Questo campo viene compilato aggiungendo utenti Windows ai gruppi Windows. Tuttavia, se i gruppi Windows non hanno attributi UNIX popolati, non vengono inclusi negli elenchi di appartenenza del gruppo dell'utente UNIX. Tutti i gruppi che devono essere disponibili in NFS devono compilare gli attributi del gruppo UNIX richiesti elencati in questa tabella.

*Indica che l'attributo è necessario per la corretta funzionalità con Cloud Volumes Service. Gli attributi rimanenti sono solo per uso lato client.

Informazioni di binding LDAP

Per eseguire query agli utenti in LDAP, Cloud Volumes Service deve essere associato (login) al servizio LDAP. Questo accesso dispone di permessi di sola lettura e viene utilizzato per eseguire query sugli attributi LDAP UNIX per le ricerche di directory. Attualmente, i binding LDAP sono possibili solo utilizzando un account di macchina SMB.

È possibile attivare LDAP solo per `CVS-Performance` E utilizzarlo per volumi NFSv3, NFSv4.1 o a doppio protocollo. È necessario stabilire una connessione Active Directory nella stessa regione del volume Cloud Volumes Service per una corretta implementazione del volume abilitato LDAP.

Quando LDAP è attivato, in scenari specifici si verifica quanto segue.

- Se per il progetto Cloud Volumes Service viene utilizzato solo NFSv3 o NFSv4.1, viene creato un nuovo account computer nel controller di dominio Active Directory e il client LDAP in Cloud Volumes Service esegue l'associazione ad Active Directory utilizzando le credenziali dell'account del computer. Non vengono create condivisioni SMB per il volume NFS e le condivisioni amministrative nascoste predefinite (vedere la sezione ""Condivisioni nascoste predefinite"") Hanno rimosso gli ACL di condivisione.
- Se per il progetto Cloud Volumes Service vengono utilizzati volumi a doppio protocollo, viene utilizzato solo l'account singolo del computer creato per l'accesso SMB per associare il client LDAP in Cloud Volumes Service ad Active Directory. Non vengono creati account macchina aggiuntivi.
- Se i volumi SMB dedicati vengono creati separatamente (prima o dopo l'attivazione dei volumi NFS con LDAP), l'account del computer per i binding LDAP viene condiviso con l'account del computer SMB.
- Se è attivato anche NFS Kerberos, vengono creati due account macchina: Uno per le condivisioni SMB e/o le binding LDAP e uno per l'autenticazione Kerberos NFS.

Query LDAP

Anche se i binding LDAP sono crittografati, le query LDAP vengono trasmesse via cavo in testo non crittografato utilizzando la porta LDAP comune 389. Questa porta nota non può essere modificata in Cloud Volumes Service. Di conseguenza, un utente con accesso allo sniffing dei pacchetti nella rete può visualizzare i nomi degli utenti e dei gruppi, gli ID numerici e le appartenenze ai gruppi.

Tuttavia, le macchine virtuali Google Cloud non possono sniff il traffico unicast di altre macchine virtuali. Solo le macchine virtuali che partecipano attivamente al traffico LDAP (ovvero, sono in grado di eseguire il binding) possono visualizzare il traffico proveniente dal server LDAP. Per ulteriori informazioni sullo sniffing dei pacchetti in Cloud Volumes Service, consulta la sezione ""Considerazioni su sniffing/traccia dei pacchetti"."

Impostazioni predefinite della configurazione del client LDAP

Quando LDAP è attivato in un'istanza di Cloud Volumes Service, per impostazione predefinita viene creata una configurazione del client LDAP con dettagli di configurazione specifici. In alcuni casi, le opzioni non sono valide per Cloud Volumes Service (non supportate) o non sono configurabili.

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Elenco server LDAP	Consente di impostare i nomi dei server LDAP o gli indirizzi IP da utilizzare per le query. Non utilizzato per Cloud Volumes Service. Viene invece utilizzato Active Directory Domain per definire i server LDAP.	Non impostato	No
Dominio Active Directory	Imposta il dominio Active Directory da utilizzare per le query LDAP. Cloud Volumes Service sfrutta i record SRV per LDAP nel DNS per trovare i server LDAP nel dominio.	Impostare sul dominio Active Directory specificato nella connessione Active Directory.	No
Server Active Directory preferiti	Imposta i server Active Directory preferiti da utilizzare per LDAP. Non supportato da Cloud Volumes Service. Utilizzare i siti Active Directory per controllare la selezione del server LDAP.	Non impostato.	No
Eseguire il binding utilizzando le credenziali del server SMB	Esegue il binding a LDAP utilizzando l'account SMB Machine. Attualmente, l'unico metodo di binding LDAP supportato in Cloud Volumes Service.	Vero	No
Modello di schema	Modello di schema utilizzato per le query LDAP.	MS-AD-BIS	No
Porta del server LDAP	Il numero di porta utilizzato per le query LDAP. Attualmente Cloud Volumes Service utilizza solo la porta LDAP standard 389. LDAPS/porta 636 non è attualmente supportato.	389	No
LDAPS è attivato	Controlla se LDAP su SSL (Secure Sockets Layer) viene utilizzato per query e binding. Attualmente non supportato da Cloud Volumes Service.	Falso	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Timeout query (sec)	Timeout per query. Se le query richiedono più tempo del valore specificato, le query non vengono eseguite correttamente.	3	No
Livello minimo di autenticazione bind	Il livello minimo di binding supportato. Poiché Cloud Volumes Service utilizza account di computer per i binding LDAP e Active Directory non supporta i binding anonimi per impostazione predefinita, questa opzione non viene utilizzata per motivi di sicurezza.	Anonimo	No
DN di binding	Nome utente/distinto (DN) utilizzato per i binding quando viene utilizzato il binding semplice. Cloud Volumes Service utilizza account computer per i binding LDAP e attualmente non supporta l'autenticazione di binding semplice.	Non impostato	No
DN di base	Il DN di base utilizzato per le ricerche LDAP.	Il dominio Windows utilizzato per la connessione Active Directory, in formato DN (DC=dominio, DC=locale).	No
Ambito di ricerca di base	Ambito di ricerca per le ricerche DN di base. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service supporta solo le ricerche in sottostruttura.	Sottostruttura	No
DN utente	Definisce il DN in cui l'utente avvia le ricerche per le query LDAP. Attualmente non supportato per Cloud Volumes Service, pertanto tutte le ricerche degli utenti iniziano dal DN di base.	Non impostato	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Ambito della ricerca dell'utente	L'ambito di ricerca per le ricerche DN dell'utente. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service non supporta l'impostazione dell'ambito di ricerca dell'utente.	Sottostruttura	No
DN gruppo	Definisce il DN in cui iniziano le ricerche di gruppo per le query LDAP. Attualmente non supportato per Cloud Volumes Service, quindi tutte le ricerche di gruppo iniziano dal DN di base.	Non impostato	No
Ambito della ricerca di gruppo	Ambito di ricerca per le ricerche DN di gruppo. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service non supporta l'impostazione dell'ambito di ricerca di gruppo.	Sottostruttura	No
DN netgroup	Definisce il DN in cui inizia la ricerca delle query LDAP da parte del netgroup. Attualmente non supportato per Cloud Volumes Service, pertanto tutte le ricerche dei netgroup iniziano dal DN di base.	Non impostato	No
Ambito della ricerca nel netgroup	Ambito di ricerca per le ricerche DN dei netgroup. I valori possono includere base, onelevel o sottostruttura. Cloud Volumes Service non supporta l'impostazione dell'ambito di ricerca del netgroup.	Sottostruttura	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
USA start_tls su LDAP	Sfrutta Start TLS per connessioni LDAP basate su certificato sulla porta 389. Attualmente non supportato da Cloud Volumes Service.	Falso	No
Attiva la ricerca netgroup-by-host	Attiva le ricerche di netgroup in base al nome host piuttosto che espandere i netgroup per elencare tutti i membri. Attualmente non supportato da Cloud Volumes Service.	Falso	No
DN netgroup-by-host	Definisce il DN in cui iniziano le ricerche netgroup-by-host per le query LDAP. Netgroup-by-host attualmente non è supportato per Cloud Volumes Service.	Non impostato	No
Ambito di ricerca netgroup-by-host	Ambito di ricerca per le ricerche DN netgroup-by-host. I valori possono includere base, onelevel o sottostruttura. Netgroup-by-host attualmente non è supportato per Cloud Volumes Service.	Sottostruttura	No
Sicurezza della sessione client	Definisce il livello di sicurezza della sessione utilizzato da LDAP (Sign, Seal o NONE). La firma LDAP è supportata da CVS-Performance, se richiesto da Active Directory. CVS-SW non supporta la firma LDAP. Per entrambi i tipi di servizio, il sealing non è attualmente supportato.	Nessuno	No

Opzione del client LDAP	Che cosa fa	Valore predefinito	Può cambiare?
Ricerca di riferimenti LDAP	Quando si utilizzano più server LDAP, la ricerca dei riferimenti consente al client di fare riferimento ad altri server LDAP nell'elenco quando non viene trovata una voce nel primo server. Attualmente non è supportato da Cloud Volumes Service.	Falso	No
Filtro di appartenenza al gruppo	Fornisce un filtro di ricerca LDAP personalizzato da utilizzare quando si cerca l'appartenenza a un gruppo da un server LDAP. Attualmente non supportato con Cloud Volumes Service.	Non impostato	No

Utilizzo di LDAP per la mappatura asimmetrica dei nomi

Cloud Volumes Service, per impostazione predefinita, esegue il mapping bidirezionale degli utenti Windows e UNIX con nomi utente identici senza alcuna configurazione speciale. Finché Cloud Volumes Service trova un utente UNIX valido (con LDAP), viene eseguita la mappatura del nome 1:1. Ad esempio, se utente Windows `johnsmith` Viene utilizzato, quindi, se Cloud Volumes Service riesce a trovare un utente UNIX denominato `johnsmith` In LDAP, la mappatura dei nomi riesce per quell'utente, tutti i file/cartelle creati da `johnsmith` Mostrare la corretta proprietà dell'utente e tutti gli ACL che influiscono `johnsmith` Sono onorati indipendentemente dal protocollo NAS in uso. Questa funzione è nota come mappatura dei nomi simmetrica.

Il mapping asimmetrico dei nomi si verifica quando l'identità dell'utente Windows e UNIX non corrispondono. Ad esempio, se utente Windows `johnsmith` Ha un'identità UNIX di `jsmith`, Cloud Volumes Service ha bisogno di un modo per essere raccontata della variazione. Poiché Cloud Volumes Service attualmente non supporta la creazione di regole di mappatura dei nomi statiche, è necessario utilizzare LDAP per cercare l'identità degli utenti per le identità Windows e UNIX, al fine di garantire la corretta proprietà di file e cartelle e le autorizzazioni previste.

Per impostazione predefinita, Cloud Volumes Service include `LDAP` Nel ns-switch dell'istanza per il database della mappa dei nomi, in modo che per fornire la funzionalità di mappatura dei nomi utilizzando LDAP per i nomi asimmetrici, è sufficiente modificare alcuni attributi utente/gruppo per riflettere ciò che Cloud Volumes Service cerca.

La tabella seguente mostra gli attributi da inserire in LDAP per la funzionalità di mappatura asimmetrica dei nomi. Nella maggior parte dei casi, Active Directory è già configurato per eseguire questa operazione.

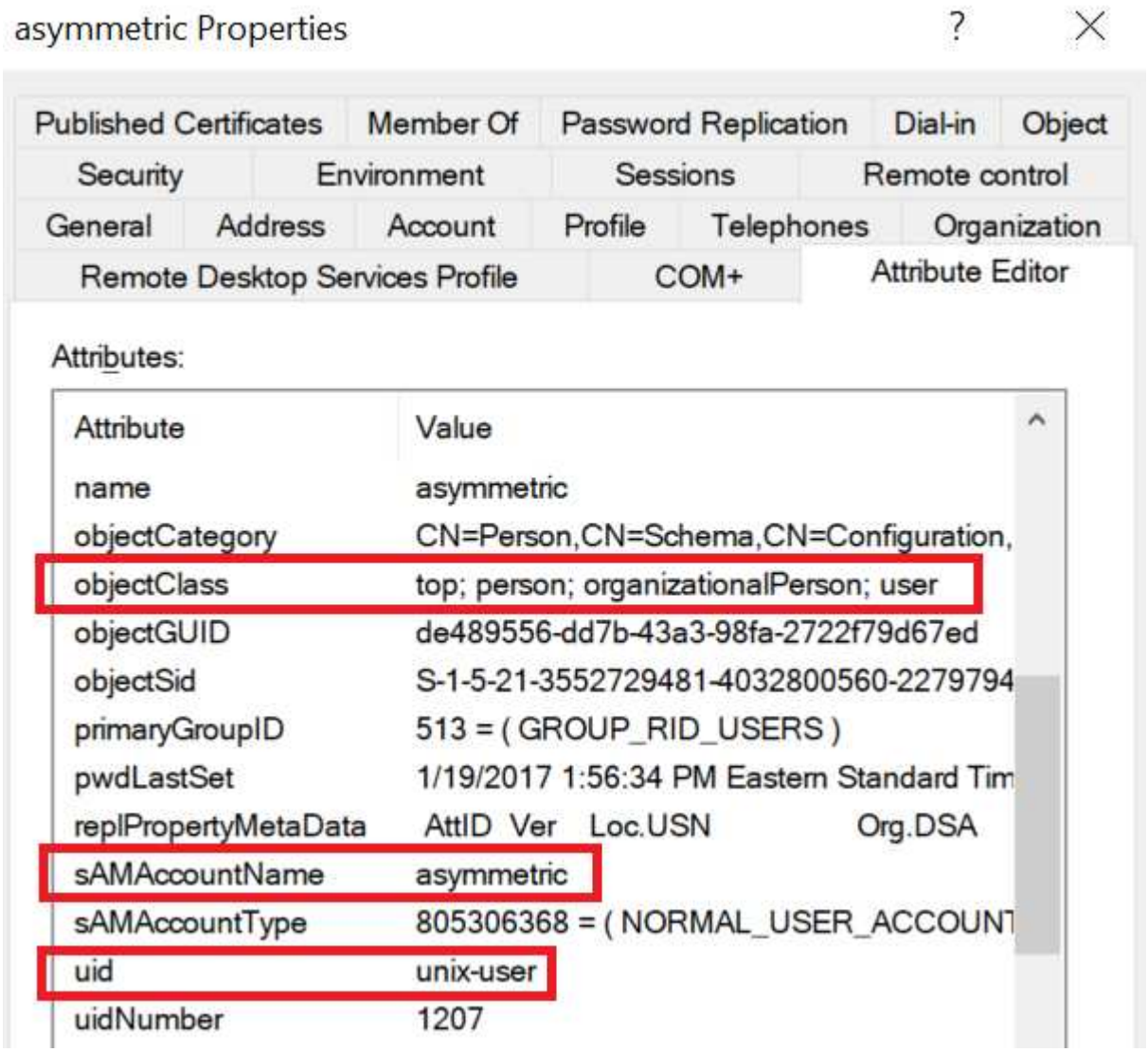
Attributo Cloud Volumes Service	Che cosa fa	Valore utilizzato da Cloud Volumes Service per la mappatura dei nomi
ObjectClass da Windows a UNIX	Specifica il tipo di oggetto utilizzato. (Ovvero, utente, gruppo, posixAccount e così via)	Deve includere l'utente (può contenere più altri valori, se lo si desidera).

Attributo Cloud Volumes Service	Che cosa fa	Valore utilizzato da Cloud Volumes Service per la mappatura dei nomi
Attributo da Windows a UNIX	Che definisce il nome utente Windows al momento della creazione. Cloud Volumes Service lo utilizza per le ricerche da Windows a UNIX.	Nessuna modifica necessaria; sAMAccountName corrisponde al nome di accesso di Windows.
UID	Definisce il nome utente UNIX.	Nome utente UNIX desiderato.

Cloud Volumes Service attualmente non utilizza prefissi di dominio nelle ricerche LDAP, pertanto gli ambienti LDAP di più domini non funzionano correttamente con le ricerche della mappa dei nomi LDAP.

Nell'esempio riportato di seguito viene illustrato un utente con il nome Windows `asymmetric`, Il nome UNIX `unix-user`E il comportamento che segue quando si scrivono file da SMB e NFS.

La figura seguente mostra l'aspetto degli attributi LDAP dal server Windows.



Da un client NFS, è possibile eseguire una query sul nome UNIX ma non sul nome di Windows:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Quando un file viene scritto da NFS come `unix-user`, Il seguente è il risultato del client NFS:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Da un client Windows, è possibile vedere che il proprietario del file è impostato sull'utente Windows appropriato:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Al contrario, i file creati dall'utente Windows `asymmetric` Da un client SMB mostrare il proprietario UNIX appropriato, come mostrato nel testo seguente.

PMI:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

Binding del canale LDAP

A causa di una vulnerabilità dei controller di dominio Active Directory di Windows, "Microsoft Security Advisory ADV190023" Modifica il modo in cui i controller di dominio consentono i binding LDAP.

L'impatto per Cloud Volumes Service è lo stesso di qualsiasi client LDAP. Cloud Volumes Service attualmente

non supporta il binding del canale. Poiché Cloud Volumes Service supporta la firma LDAP per impostazione predefinita attraverso la negoziazione, l'associazione del canale LDAP non dovrebbe rappresentare un problema. In caso di problemi di associazione a LDAP con l'associazione del canale attivata, seguire la procedura di risoluzione descritta in ADV190023 per consentire l'esecuzione dei binding LDAP da Cloud Volumes Service.

DNS

Active Directory e Kerberos hanno entrambe dipendenze dal DNS per la risoluzione dei nomi host all'IP/IP. Il DNS richiede che la porta 53 sia aperta. Cloud Volumes Service non appora alcuna modifica ai record DNS, né supporta attualmente l'utilizzo di "DNS dinamico" sulle interfacce di rete.

È possibile configurare il DNS di Active Directory per limitare i server che possono aggiornare i record DNS. Per ulteriori informazioni, vedere "DNS Windows sicuro".

Si noti che le risorse all'interno di un progetto Google utilizzano per impostazione predefinita il DNS di Google Cloud, che non è connesso al DNS di Active Directory. I client che utilizzano il DNS cloud non possono risolvere i percorsi UNC restituiti da Cloud Volumes Service. I client Windows associati al dominio Active Directory sono configurati per utilizzare il DNS di Active Directory e possono risolvere tali percorsi UNC.

Per aggiungere un client ad Active Directory, è necessario configurare la relativa configurazione DNS in modo che utilizzi il DNS di Active Directory. Facoltativamente, è possibile configurare il DNS cloud per inoltrare le richieste al DNS di Active Directory. Vedere "Perché il client non riesce a risolvere il nome NetBIOS SMB?"per ulteriori informazioni.

> Cloud Volumes Service attualmente non supporta DNSSEC e le query DNS vengono eseguite in formato non crittografato.

Controllo dell'accesso al file

Attualmente non supportato per Cloud Volumes Service.

Protezione antivirus

È necessario eseguire la scansione antivirus in Cloud Volumes Service sul client in una condivisione NAS. Attualmente non esiste alcuna integrazione antivirus nativa con Cloud Volumes Service.

Funzionamento del servizio

Il team di Cloud Volumes Service gestisce i servizi di back-end in Google Cloud e utilizza diverse strategie per proteggere la piattaforma e prevenire accessi indesiderati.

Ogni cliente ottiene la propria subnet univoca che ha accesso negato da altri clienti per impostazione predefinita e ogni tenant in Cloud Volumes Service ottiene il proprio namespace e la propria VLAN per l'isolamento totale dei dati. Dopo l'autenticazione di un utente, il Service Delivery Engine (SDE) può leggere solo i dati di configurazione specifici del tenant.

Sicurezza fisica

Con un'adeguata preapprovazione, solo i tecnici on-site e gli ingegneri di assistenza sul campo (FSE) con badge NetApp hanno accesso alla gabbia e ai rack per il lavoro fisico. La gestione dello storage e della rete non è consentita. Solo queste risorse on-site sono in grado di eseguire attività di manutenzione dell'hardware.

Per i tecnici in loco, viene presentato un ticket per la dichiarazione di lavoro (SOW) che include l'ID del rack e

la posizione del dispositivo (RU) e tutti gli altri dettagli sono inclusi nel ticket. Per gli FSE NetApp, è necessario inoltrare un ticket di visita del sito con IL COLO e il biglietto include i dettagli, la data e l'ora del visitatore per scopi di verifica. Il SOW del FSE viene comunicato internamente a NetApp.

Team operativo

Il team operativo di Cloud Volumes Service è composto da tecnici di produzione e da un tecnico di affidabilità del sito (SRE) per i servizi di volume cloud e da tecnici di assistenza sul campo e partner per l'hardware. Tutti i membri del team operativo sono accreditati per il lavoro in Google Cloud e vengono mantenuti record dettagliati di lavoro per ogni ticket generato. Inoltre, è in atto un rigoroso processo di approvazione e controllo delle modifiche per garantire che ogni decisione venga esaminata in modo appropriato.

Il team SRE gestisce il piano di controllo e il modo in cui i dati vengono instradati dalle richieste dell'interfaccia utente all'hardware e al software di back-end in Cloud Volumes Service. Il team SRE gestisce anche le risorse di sistema, ad esempio i massimi di volume e inode. Gli SRE non possono interagire con i dati dei clienti o accedervi. Gli SRE forniscono inoltre il coordinamento con le RMA (Return Material Authorization), come le richieste di sostituzione di nuovi dischi o memoria per l'hardware back-end.

Responsabilità del cliente

I clienti di Cloud Volumes Service gestiscono la gestione dei ruoli utente e di Active Directory della propria organizzazione, nonché le operazioni di volume e dati. I clienti possono avere ruoli amministrativi e delegare le autorizzazioni ad altri utenti finali all'interno dello stesso progetto Google Cloud utilizzando i due ruoli predefiniti forniti da NetApp e Google Cloud (Administrator e Viewer).

L'amministratore può eseguire il peer di qualsiasi VPC all'interno del progetto del cliente a Cloud Volumes Service che il cliente ritiene appropriato. È responsabilità del cliente gestire l'accesso al proprio Google Cloud Marketplace Subscription e i VPC che hanno accesso al data plane.

Protezione SRE dannosa

Una preoccupazione che potrebbe sorgere è come Cloud Volumes Service protegge da scenari in cui si verifica un SRE dannoso o quando le credenziali SRE sono state compromesse?

L'accesso all'ambiente di produzione avviene solo con un numero limitato di individui SRE. I privilegi amministrativi sono ulteriormente limitati a pochi amministratori esperti. Tutte le azioni eseguite da chiunque nell'ambiente di produzione Cloud Volumes Service vengono registrate e qualsiasi anomalia alla linea di base o alle attività sospette viene rilevata dalla nostra piattaforma di Threat intelligence per la gestione delle informazioni sulla sicurezza e degli eventi (SIEM). Di conseguenza, le azioni dannose possono essere monitorate e mitigate prima che venga eseguito un danno eccessivo al backend Cloud Volumes Service.

Ciclo di vita del volume

Cloud Volumes Service gestisce solo gli oggetti all'interno del servizio, non i dati all'interno dei volumi. Solo i client che accedono ai volumi possono gestire i dati, gli ACL, i proprietari dei file e così via. I dati in questi volumi vengono crittografati a riposo e l'accesso è limitato ai tenant dell'istanza di Cloud Volumes Service.

Il ciclo di vita del volume per Cloud Volumes Service è create-update-delete. I volumi conservano le copie Snapshot dei volumi fino all'eliminazione dei volumi e solo gli amministratori Cloud Volumes Service validati possono eliminare i volumi in Cloud Volumes Service. Quando un amministratore richiede l'eliminazione di un volume, per verificare l'eliminazione è necessario inserire un ulteriore passo per il nome del volume. Dopo l'eliminazione di un volume, il volume non viene più utilizzato e non può essere recuperato.

Nei casi in cui un contratto Cloud Volumes Service venga rescisso, NetApp contrassegna i volumi per l'eliminazione dopo un determinato periodo di tempo. Prima della scadenza di tale periodo di tempo, è

possibile ripristinare i volumi su richiesta del cliente.

Certificazioni

Cloud Volumes Services per Google Cloud è attualmente certificato in base agli standard ISO/IEC 27001:2013 e ISO/IEC 27018:2019. Il servizio ha inoltre ricevuto di recente il report di attestazione SOC2 di tipo I. Per informazioni sull'impegno di NetApp per la sicurezza e la privacy dei dati, vedere "Compliance: Sicurezza dei dati e privacy dei dati".

GDPR

I nostri impegni in materia di privacy e conformità al GDPR sono disponibili in diversi nostri "contratti con i clienti", come il nostro "Addendum per l'elaborazione dei dati dei clienti", che include "Clausole contrattuali standard" Fornito dalla Commissione europea. Inoltre, ci impegniamo a rispettare questi impegni nella nostra direttiva sulla privacy, supportata dai valori fondamentali stabiliti nel nostro Codice di condotta aziendale.

Ulteriori informazioni e informazioni di contatto

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Documentazione Google Cloud per Cloud Volumes Service

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

- Accesso al servizio privato di Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentazione sui prodotti NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- Programma del modulo di convalida crittografica: NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- La soluzione NetApp per ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: NFS Kerberos in ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Contattaci

Facci sapere come possiamo migliorare questo report tecnico.

Contattaci all'indirizzo doccomments@netapp.com. Includere IL REPORT TECNICO 4918 nell'oggetto.

Backup e recovery di BlueXP

Backup e recovery di BlueXP per le VM

Data Protection 3-2-1 per VMware con plug-in SnapCenter e backup e recovery BlueXP per le VM

Autore: Josh Powell - NetApp Solutions Engineering

Panoramica

La strategia di backup 3-2-1 è un metodo di protezione dei dati accettato dal settore, che offre un approccio completo alla protezione dei dati importanti. Questa strategia è affidabile e garantisce che, anche in caso di incidenti imprevisti, vi sia ancora una copia dei dati disponibili.

La strategia si articola in tre regole fondamentali:

1. Conservare almeno tre copie dei dati. In questo modo, anche se una copia viene smarrita o danneggiata, sono ancora disponibili almeno due copie rimanenti.
2. Memorizzare due copie di backup su diversi supporti o dispositivi di archiviazione. La diversificazione dei supporti storage contribuisce a proteggerli da guasti specifici dei dispositivi o dei supporti. Se un dispositivo viene danneggiato o un tipo di supporto si guasta, l'altra copia di backup rimane inalterata.
3. Infine, assicurarsi che almeno una copia di backup sia fuori sede. Lo storage offsite serve come protezione contro i disastri localizzati, come incendi o inondazioni, che potrebbero rendere le copie on-site inutilizzabili.

Questo documento di soluzione descrive una soluzione di backup 3-2-1 che utilizza il plug-in SnapCenter per VMware vSphere (SCV) per creare backup primari e secondari delle nostre macchine virtuali on-premise e backup e recovery BlueXP per le macchine virtuali per effettuare il backup di una copia dei nostri dati su cloud storage o StorageGRID.

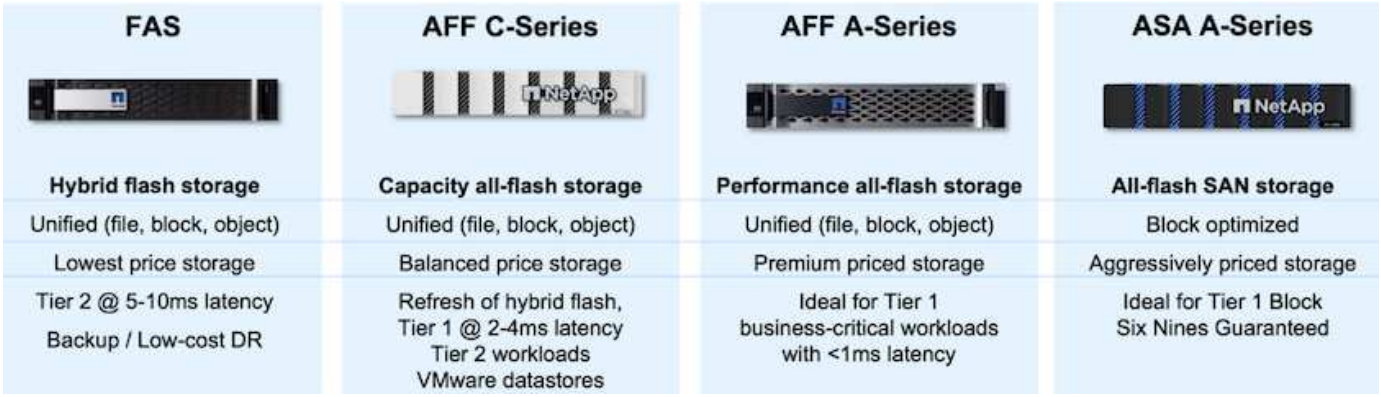
Casi di utilizzo

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup e ripristino di macchine virtuali e datastore on-premise utilizzando il plug-in SnapCenter per VMware vSphere.
- Backup e ripristino di macchine virtuali e datastore on-premise, in hosting su cluster ONTAP e backup su storage a oggetti utilizzando backup e recovery di BlueXP per le macchine virtuali.

Storage NetApp ONTAP

ONTAP è la soluzione di storage leader del settore di NetApp che offre storage unificato con accesso a protocolli SAN o NAS. La strategia di backup 3-2-1 garantisce la protezione dei dati on-premise su più tipi di supporto, mentre NetApp offre piattaforme che vanno da flash ad alta velocità a supporti a costi inferiori.



Per ulteriori informazioni su tutti i prodotti hardware della piattaforma NetApp, consulta l'articolo "Storage NetApp".

Plug-in SnapCenter per VMware vSphere

Il plug-in SnapCenter per VMware vSphere è un'offerta di protezione dei dati strettamente integrata con VMware vSphere e consente una facile gestione di backup e ripristini per le macchine virtuali. Come parte di questa soluzione, SnapMirror fornisce un metodo rapido e affidabile per creare una seconda copia di backup immutabile dei dati della macchina virtuale su un cluster di storage ONTAP secondario. Con questa architettura implementata, le operazioni di ripristino delle macchine virtuali possono essere avviate facilmente da posizioni di backup primarie o secondarie.

SCV viene installato come appliance virtuale linux utilizzando un file OVA. Il plug-in ora utilizza un plug-in remoto
architettura. Il plug-in remoto viene eseguito al di fuori del server vCenter e viene ospitato sull'appliance virtuale SCV.

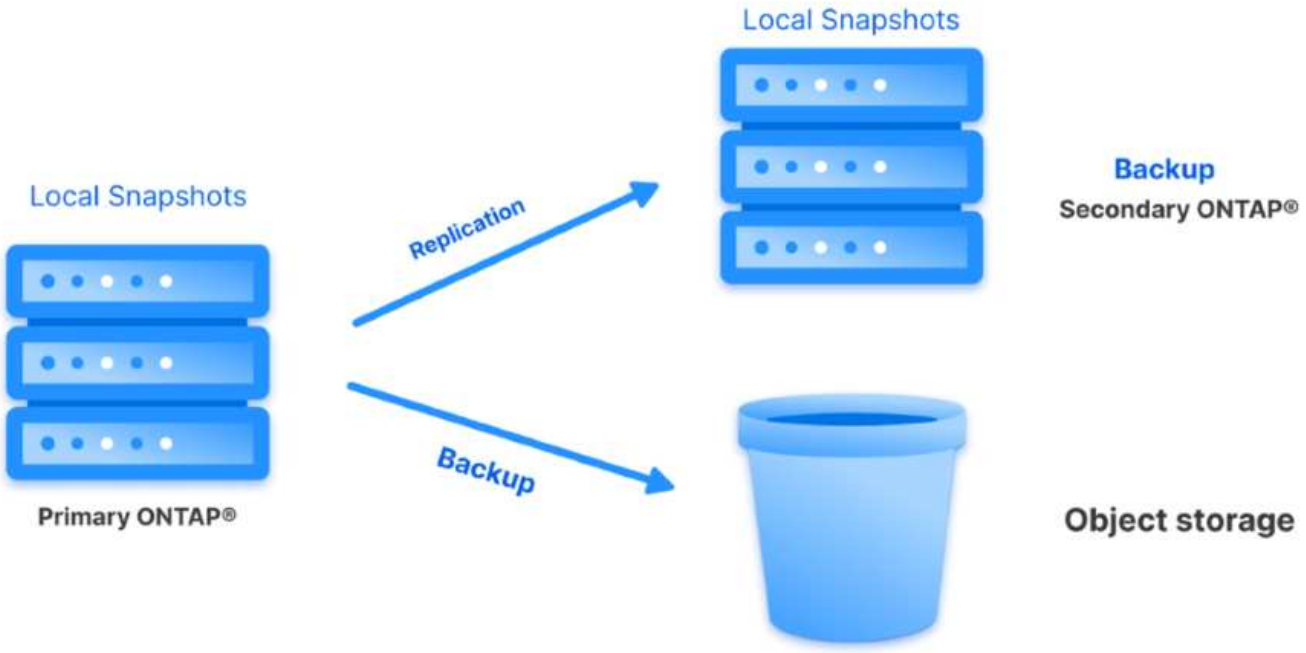
Per informazioni dettagliate sul distributore idraulico, fare riferimento a. "Plug-in SnapCenter per la documentazione di VMware vSphere".

Backup e recovery di BlueXP per le macchine virtuali

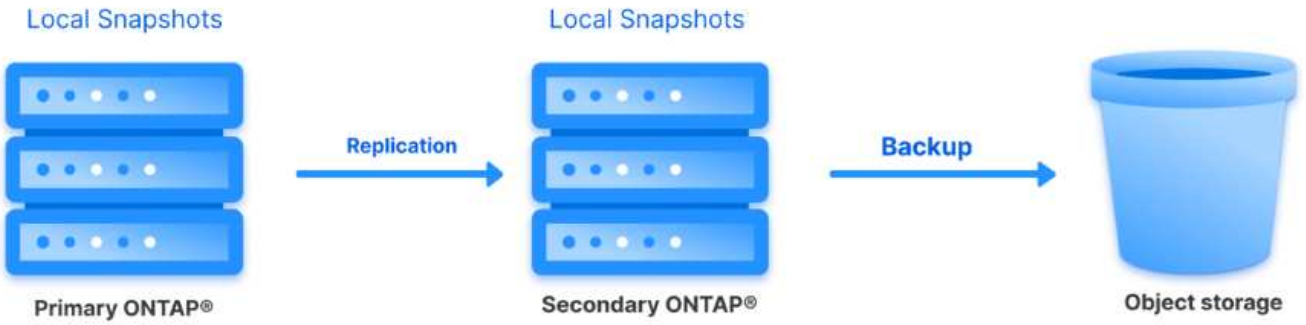
Il backup e recovery di BlueXP è uno strumento basato su cloud per la gestione dei dati che offre un singolo pannello di controllo per un'ampia gamma di operazioni di backup e recovery negli ambienti on-premise e cloud. Parte della suite di backup e recovery BlueXP di NetApp è una funzionalità che si integra con il plug-in SnapCenter per VMware vSphere (on-premise) per estendere una copia dei dati allo storage a oggetti nel cloud. In questo modo viene stabilita una terza copia dei dati fuori sede che provengono dai backup dello storage primario o secondario. Il backup e recovery di BlueXP semplifica la configurazione di policy dello storage che trasferiscono le copie dei dati da una di queste due posizioni on-premise.

La scelta tra backup primari e secondari come origine in BlueXP Backup and Recovery comporterà l'implementazione di una delle due topologie:

Topologia fan-out – quando un backup viene avviato dal plug-in SnapCenter per VMware vSphere, viene immediatamente creata una snapshot locale. SCV avvia quindi un'operazione SnapMirror che replica lo snapshot più recente nel cluster ONTAP secondario. In BlueXP Backup and Recovery, una policy specifica il cluster ONTAP primario come origine di una copia Snapshot dei dati da trasferire nello storage a oggetti nel cloud provider scelto.



Topologia a cascata – la creazione delle copie dei dati primari e secondari mediante SCV è identica alla topologia fan-out menzionata in precedenza. Tuttavia, questa volta viene creata una policy in BlueXP Backup and Recovery che specifica che il backup nello storage a oggetti avrà origine dal cluster ONTAP secondario.



Il backup e recovery di BlueXP può creare copie di backup degli snapshot ONTAP on-premise nello storage AWS Glacier, Azure Blob e GCP Archive.

AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

Inoltre, puoi utilizzare NetApp StorageGRID come destinazione del backup dello storage a oggetti. Per ulteriori informazioni su StorageGRID, fare riferimento alla "Landing page di StorageGRID".

Panoramica sull'implementazione della soluzione

Questo elenco fornisce i passaggi di alto livello necessari per configurare questa soluzione ed eseguire operazioni di backup e ripristino da SCV e BlueXP - Backup e ripristino:

1. Configurare la relazione SnapMirror tra i cluster ONTAP da utilizzare per le copie di dati primarie e secondarie.
2. Configura il plug-in SnapCenter per VMware vSphere.
   a. Aggiunta di sistemi storage
   b. Creare policy di backup
   c. Creare gruppi di risorse
   d. Eseguire i primi processi di backup
3. Configura backup e recovery di BlueXP per le macchine virtuali
   a. Aggiungi ambiente di lavoro
   b. Scopri le appliance SCV e vCenter
   c. Creare policy di backup
   d. Attivare i backup
4. Ripristinare le macchine virtuali dallo storage primario e secondario utilizzando SCV.
5. Ripristina le macchine virtuali dallo storage a oggetti utilizzando il backup e ripristino di BlueXP.

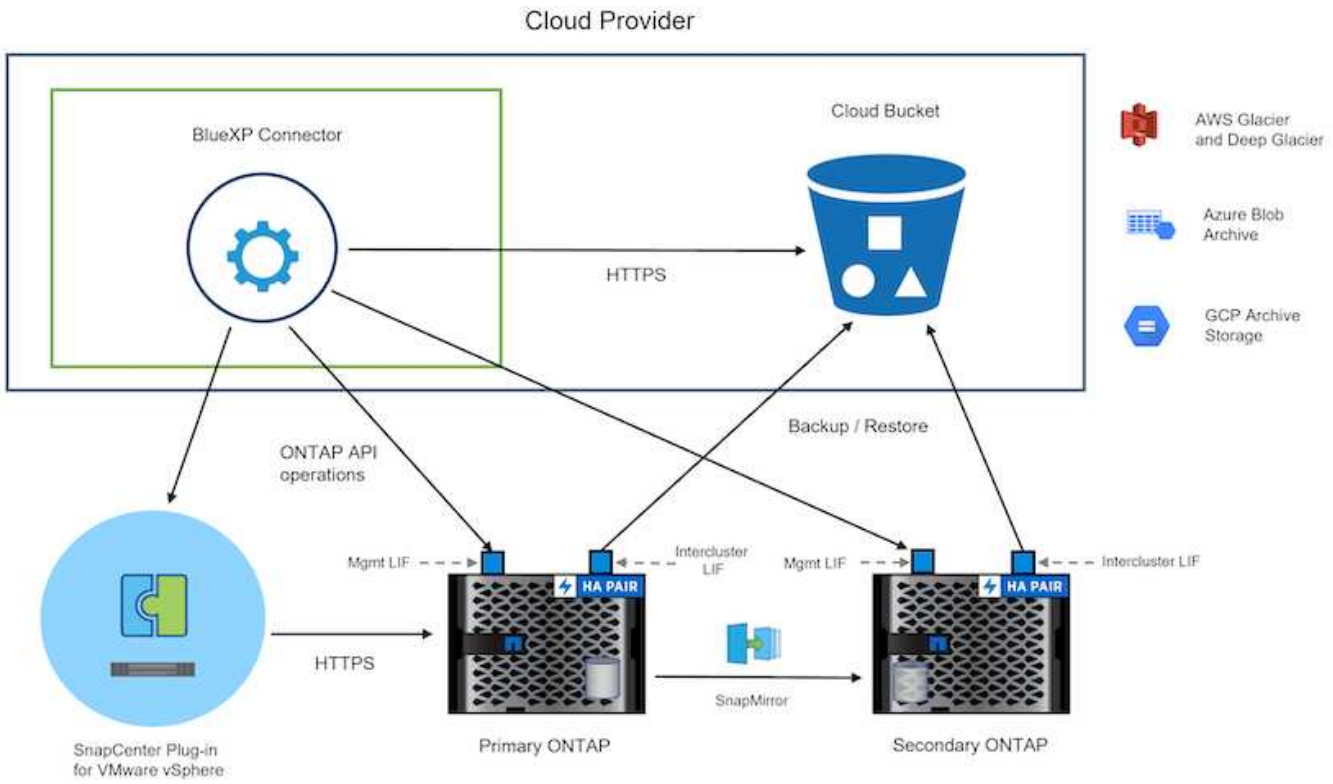
Prerequisiti

Lo scopo di questa soluzione è dimostrare la protezione dei dati delle macchine virtuali in esecuzione in VMware vSphere e situate negli archivi dati NFS ospitati da NetApp ONTAP. Questa soluzione presuppone che i seguenti componenti siano configurati e pronti per l'uso:

1. Cluster di storage ONTAP con datastore NFS o VMFS connessi a VMware vSphere. Sono supportati datastore NFS e VMFS. Per questa soluzione sono stati utilizzati datastore NFS.
2. Cluster di storage ONTAP secondario con relazioni SnapMirror stabilite per volumi usati per datastore NFS.
3. Connettore BlueXP installato per il cloud provider utilizzato per i backup dello storage a oggetti.
4. Le macchine virtuali di cui eseguire il backup si trovano su datastore NFS che si trovano sul cluster di storage ONTAP primario.
5. Connettività di rete tra il connettore BlueXP e le interfacce di gestione del cluster di storage ONTAP on-premise.
6. Connettività di rete tra il connettore BlueXP e la macchina virtuale di un'appliance SCV on-premise e tra il connettore BlueXP e vCenter.
7. Connettività di rete tra le LIF ONTAP on-premise e il servizio di storage a oggetti.
8. DNS configurato per l'SVM di gestione su cluster di storage ONTAP primari e secondari. Per ulteriori informazioni, fare riferimento a. "Configurare il DNS per la risoluzione del nome host".

Architettura di alto livello

Il test/convalida di questa soluzione è stato eseguito in un laboratorio che potrebbe corrispondere o meno all'ambiente di implementazione finale.



Implementazione della soluzione

Questa soluzione fornisce istruzioni dettagliate per l'implementazione e la convalida di una soluzione che utilizza il plug-in SnapCenter per VMware vSphere, oltre al backup e al recovery di BlueXP, per eseguire backup e recovery di macchine virtuali Windows e Linux all'interno di un cluster VMware vSphere situato in un data center on-premise. Le macchine virtuali di questo setup sono memorizzate su datastore NFS ospitati da un cluster di storage ONTAP A300. Inoltre, un cluster di storage ONTAP A300 separato funge da destinazione secondaria per i volumi replicati mediante SnapMirror. Inoltre, lo storage a oggetti ospitato su Amazon Web Services e Azure Blob è stato utilizzato come destinazione per una terza copia dei dati.

Ci occuperemo della creazione di relazioni SnapMirror per copie secondarie dei nostri backup gestiti da SCV e della configurazione dei lavori di backup nel backup e ripristino di SCV e BlueXP.

Per informazioni dettagliate sul plug-in SnapCenter per VMware vSphere, consultare la "Plug-in SnapCenter per la documentazione di VMware vSphere".

Per informazioni dettagliate sul backup e recovery di BlueXP, consulta la "Documentazione di backup e ripristino BlueXP".

Stabilire relazioni di SnapMirror tra cluster ONTAP

Il plug-in SnapCenter per VMware vSphere utilizza la tecnologia ONTAP SnapMirror per gestire il trasporto delle copie SnapMirror e/o SnapVault secondarie in un cluster ONTAP secondario.

Le policy di backup dei distributori idraulici possono utilizzare relazioni SnapMirror o SnapVault. La differenza principale consiste nel fatto che quando si utilizza l'opzione SnapMirror, la pianificazione della conservazione configurata per i backup nella policy sarà la stessa nelle posizioni principale e secondaria. SnapVault è progettato per l'archiviazione e, quando si utilizza questa opzione, è possibile stabilire una pianificazione della conservazione separata con la relazione di SnapMirror per le copie Snapshot sul cluster di storage ONTAP secondario.

La configurazione delle relazioni di SnapMirror può essere effettuata in BlueXP, dove molti dei passaggi sono automatizzati, o può essere fatta con System Manager e l'interfaccia a riga di comando di ONTAP. Tutti questi metodi sono discussi di seguito.

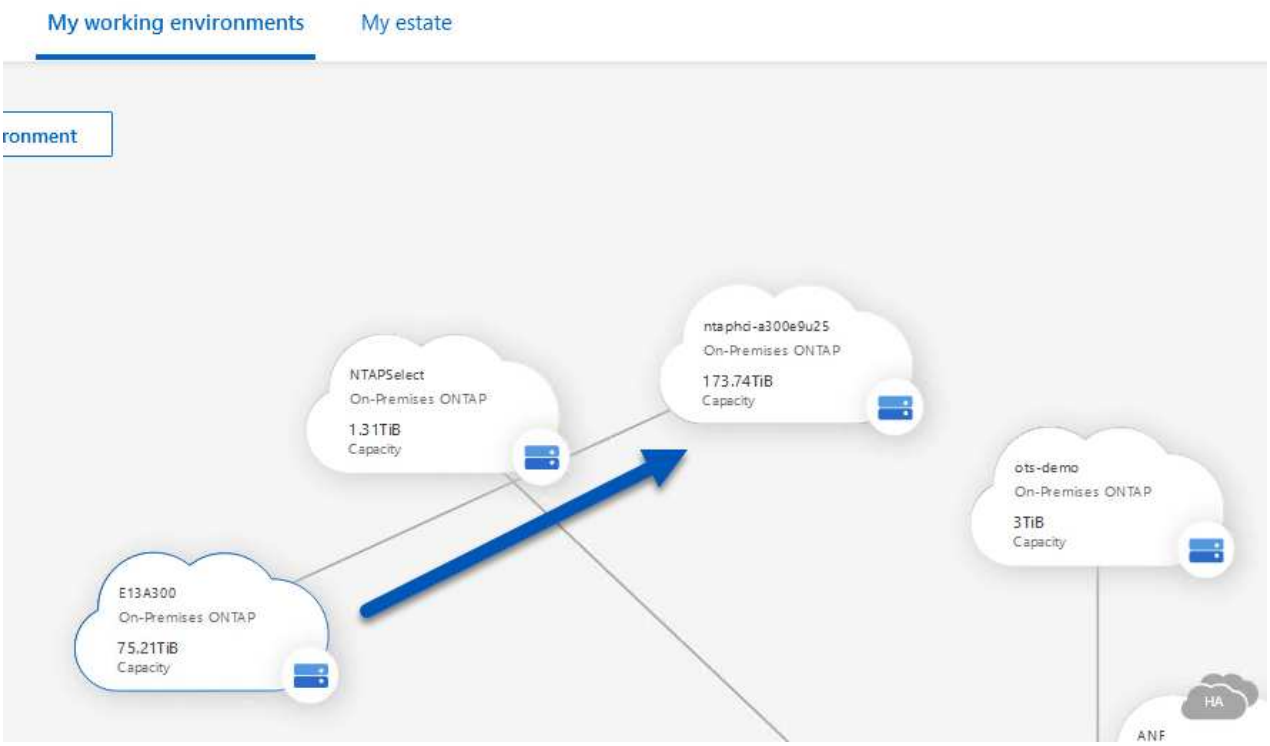
Stabilisci relazioni di SnapMirror con BlueXP

Dalla console web BlueXP devi completare i seguenti passaggi:

Configurazione della replica per sistemi di storage ONTAP primari e secondari

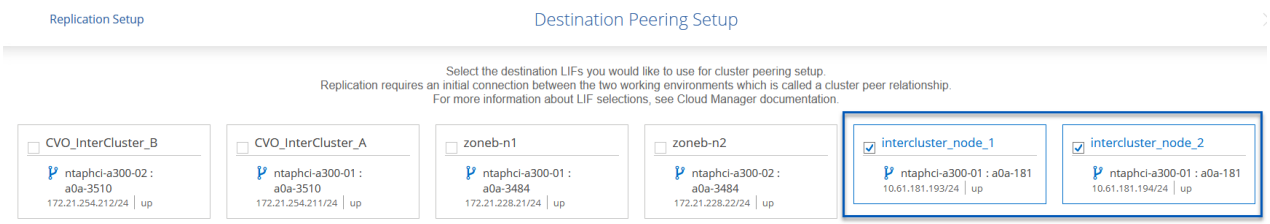
Iniziare accedendo alla console web BlueXP e navigando in Canvas.

1. Trascinare e rilasciare il sistema di storage ONTAP di origine (primario) nel sistema di storage ONTAP di destinazione (secondario).

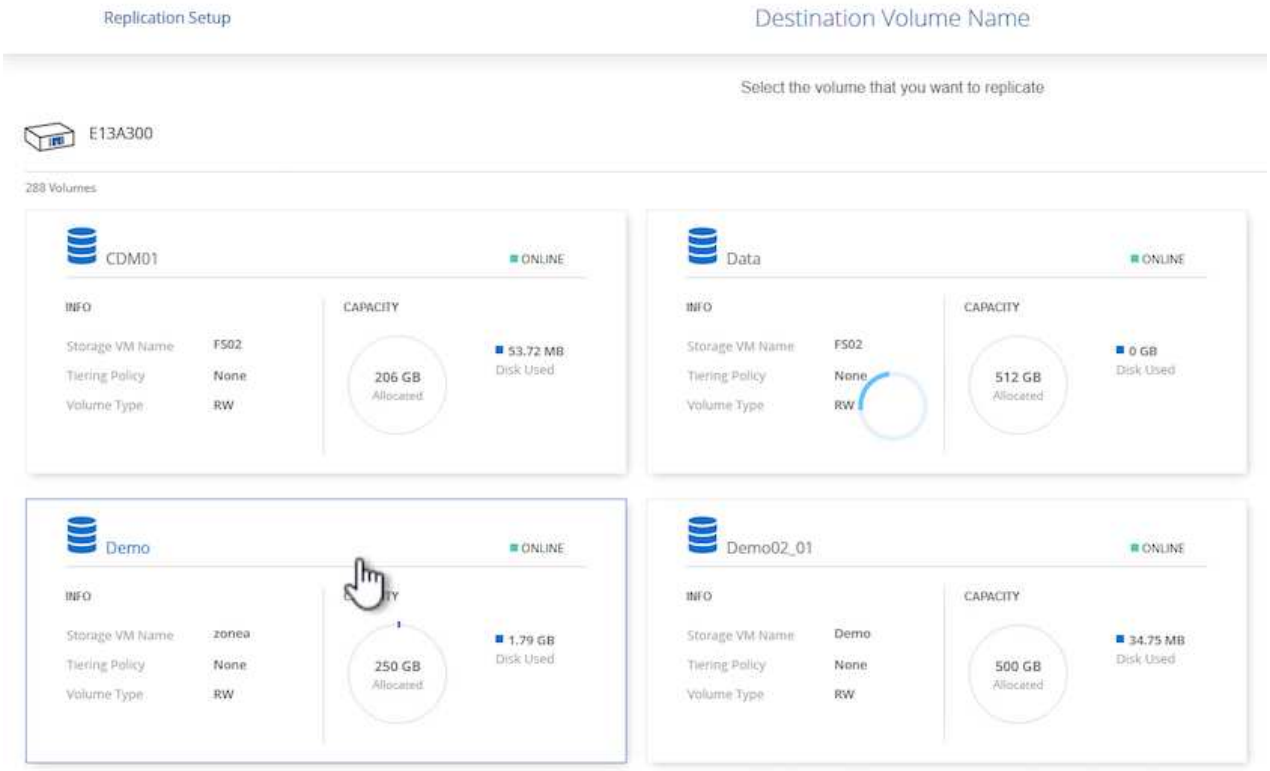


2. Dal menu visualizzato, selezionare **Replica**.

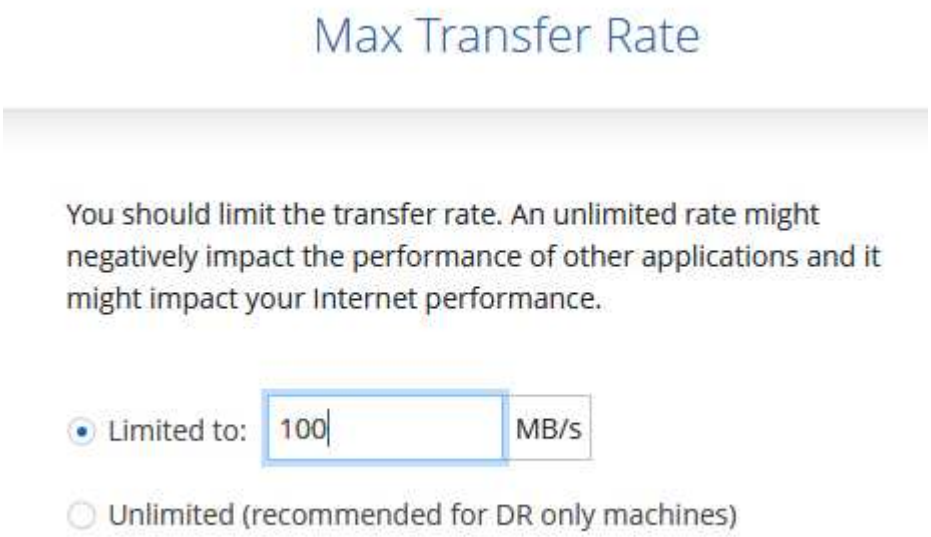
3. Nella pagina **impostazione peering di destinazione**, selezionare le LIF Intercluster di destinazione da utilizzare per la connessione tra sistemi storage.



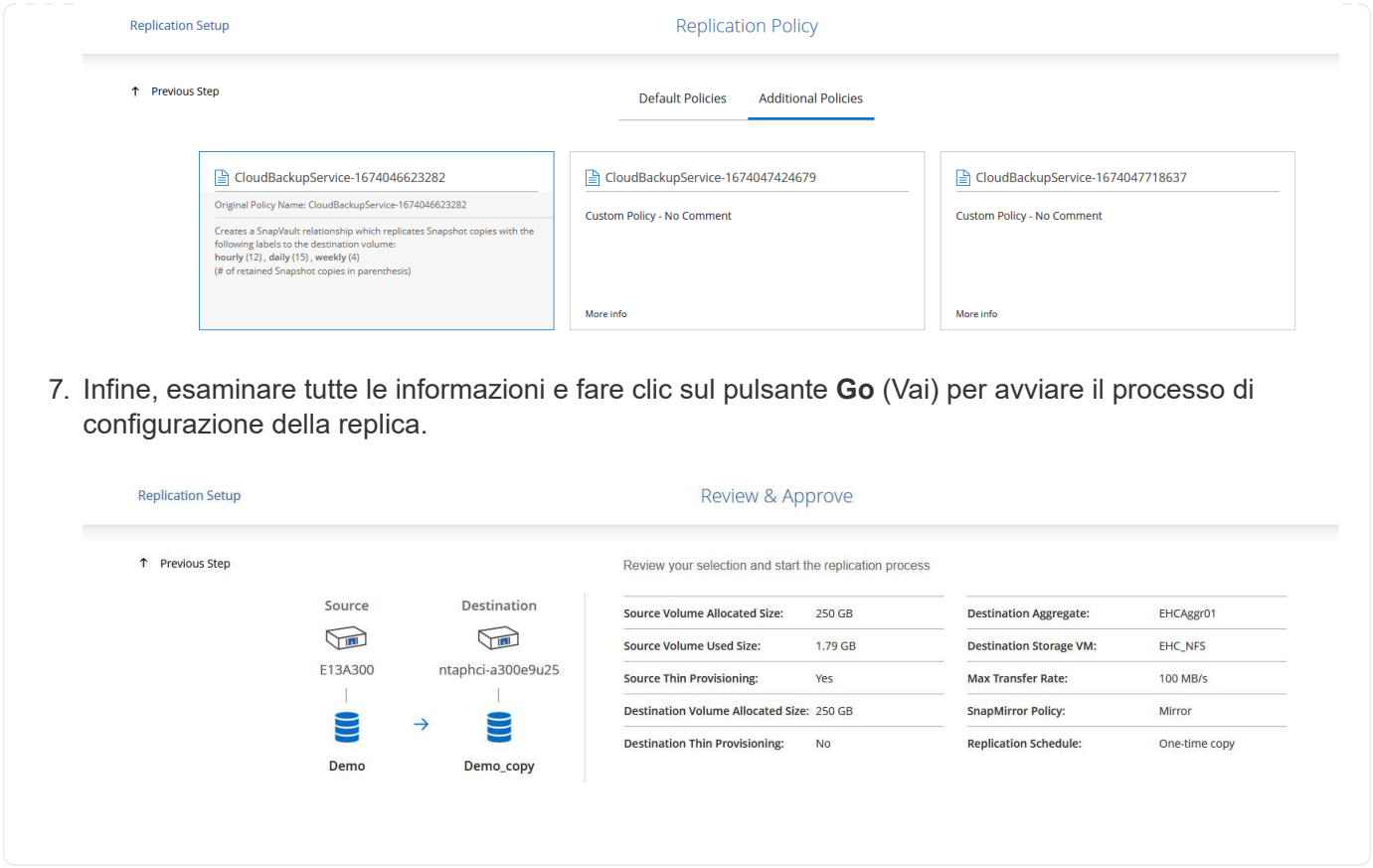
4. Nella pagina **Destination Volume Name** (Nome volume di destinazione), selezionare innanzitutto il volume di origine, quindi compilare il nome del volume di destinazione e selezionare la SVM e l'aggregato di destinazione. Fare clic su **Avanti** per continuare.



5. Scegliere la velocità di trasferimento massima alla quale eseguire la replica.



6. Scegliere il criterio che determinerà il programma di conservazione per i backup secondari. Questo criterio può essere creato in anticipo (vedere il processo manuale riportato di seguito nel passaggio **Crea un criterio di conservazione snapshot**) o può essere modificato in seguito, se lo si desidera.



7. Infine, esaminare tutte le informazioni e fare clic sul pulsante **Go** (Vai) per avviare il processo di configurazione della replica.

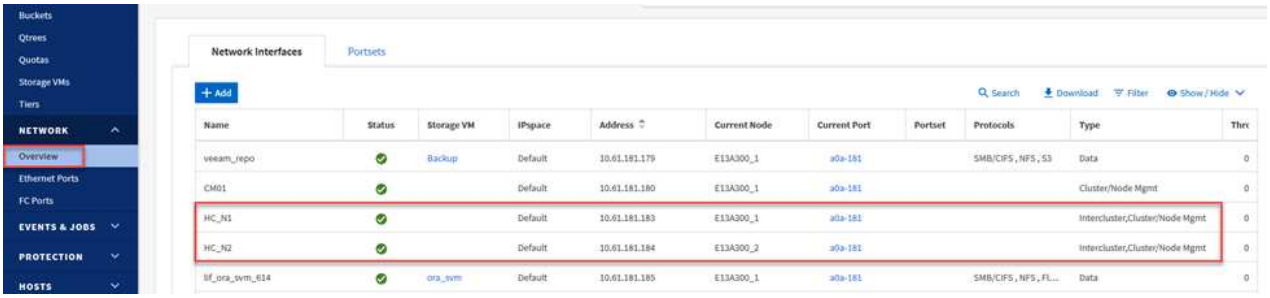
Stabilire relazioni di SnapMirror con System Manager e la CLI di ONTAP

Tutti i passaggi necessari per stabilire le relazioni SnapMirror possono essere eseguiti con System Manager o la CLI di ONTAP. La sezione seguente fornisce informazioni dettagliate su entrambi i metodi:

Registrare le interfacce logiche Intercluster di origine e destinazione

Per i cluster ONTAP di origine e di destinazione, puoi recuperare le informazioni LIF inter-cluster da System Manager o dalla CLI.

1. In Gestore di sistema di ONTAP, accedere alla pagina Panoramica di rete e recuperare gli indirizzi IP di tipo: Intercluster configurati per comunicare con il VPC di AWS su cui è installato FSX.



2. Per recuperare gli indirizzi IP di Intercluster utilizzando l'interfaccia CLI, eseguire il seguente comando:

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

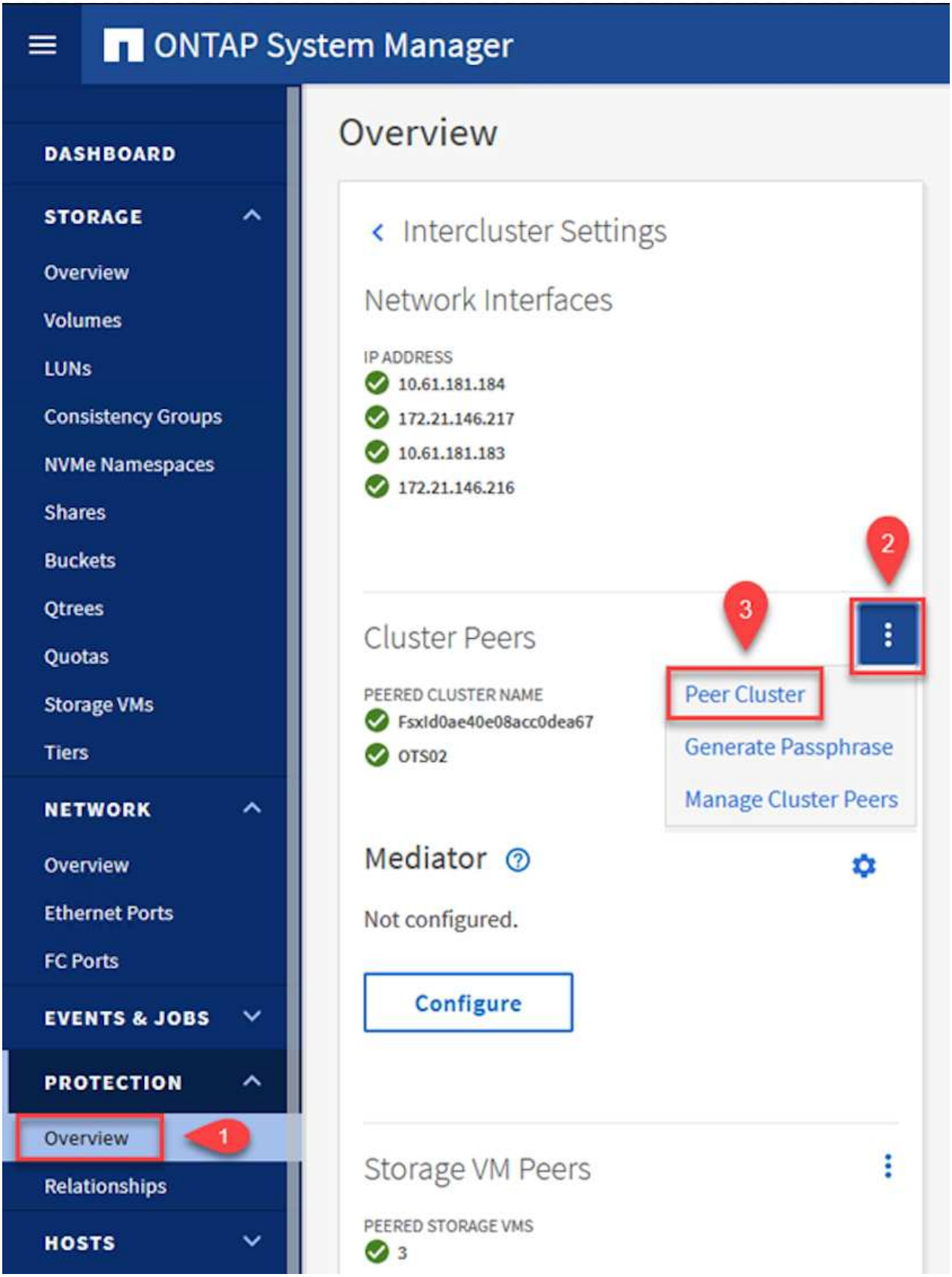
Stabilisci il peering dei cluster tra i cluster ONTAP

Per stabilire il peering del cluster tra i cluster ONTAP, è necessario confermare una passphrase univoca inserita nel cluster ONTAP di avvio nell'altro cluster peer.

1. Impostare il peering sul cluster ONTAP di destinazione utilizzando l' `cluster peer create` comando. Quando richiesto, immettere una passphrase univoca da utilizzare in seguito nel cluster di origine per completare il processo di creazione.

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

2. Nel cluster di origine, è possibile stabilire la relazione peer del cluster utilizzando Gestore di sistema di ONTAP o l'interfaccia CLI. Da Gestore di sistema di ONTAP, accedere a protezione > Panoramica e selezionare cluster peer.

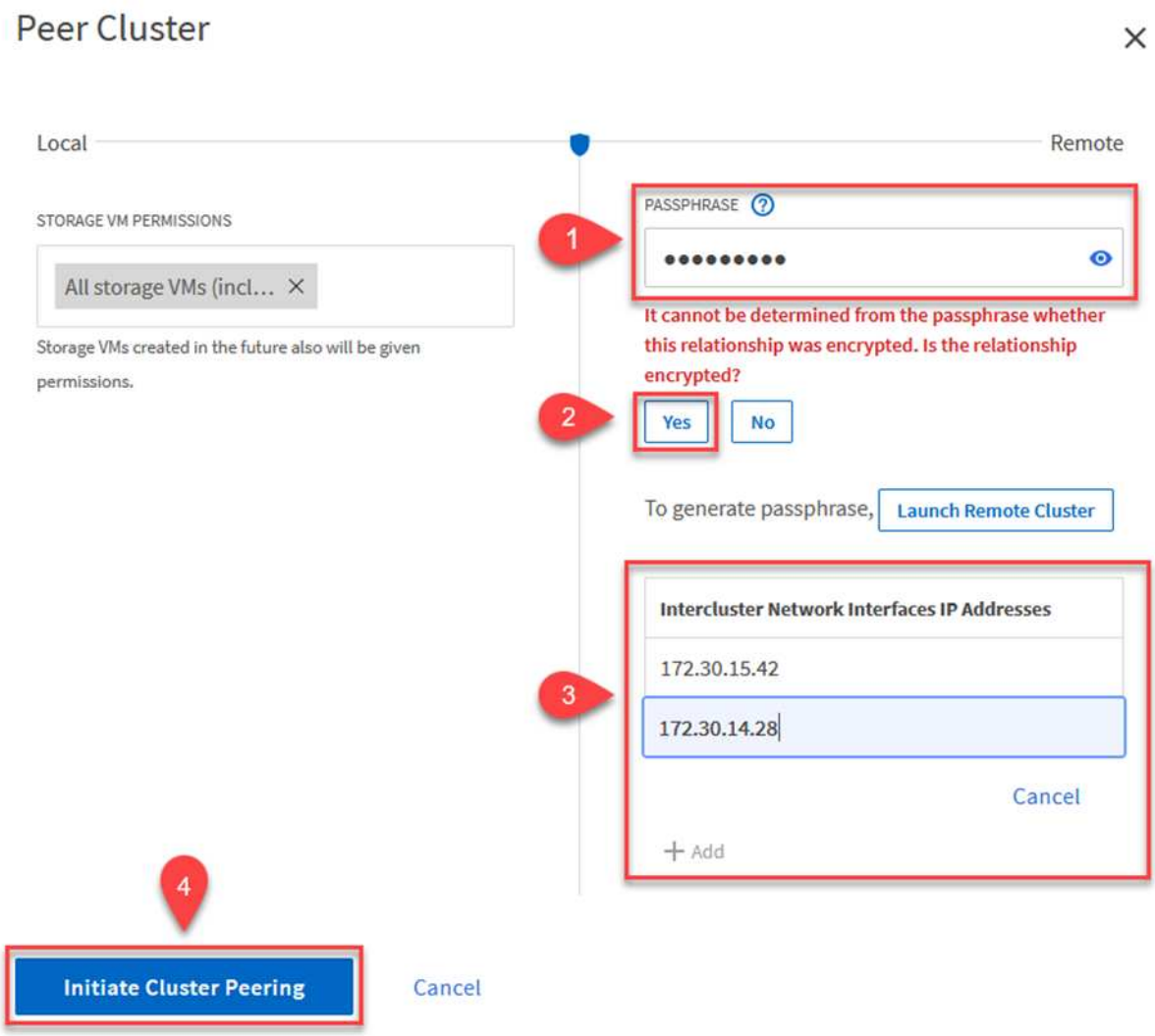


3. Nella finestra di dialogo Peer Cluster, inserire le informazioni richieste:
   a. Immettere la passphrase utilizzata per stabilire la relazione del cluster peer nel cluster ONTAP di destinazione.

b. Selezionare `Yes` per stabilire una relazione crittografata.

c. Inserire l'indirizzo IP intercluster LIF del cluster ONTAP di destinazione.

d. Fare clic su Initiate Cluster peering (Avvia peering cluster) per completare il processo.



4. Verificare lo stato della relazione di peer del cluster dal cluster ONTAP di destinazione con il seguente comando:

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

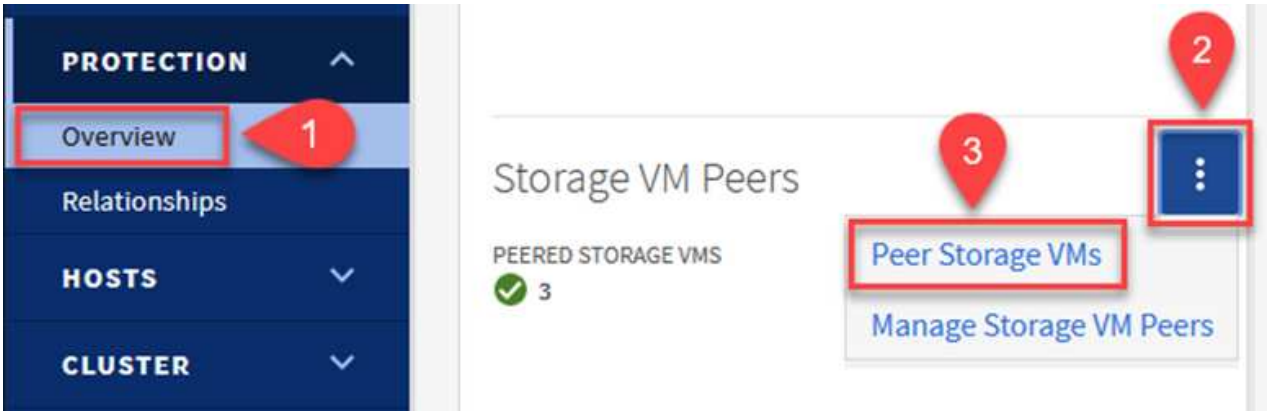
Stabilire una relazione di peering SVM

Il passaggio successivo consiste nell'impostare una relazione SVM tra le macchine virtuali dello storage di destinazione e di origine che contengono i volumi che si trovano nelle relazioni di SnapMirror.

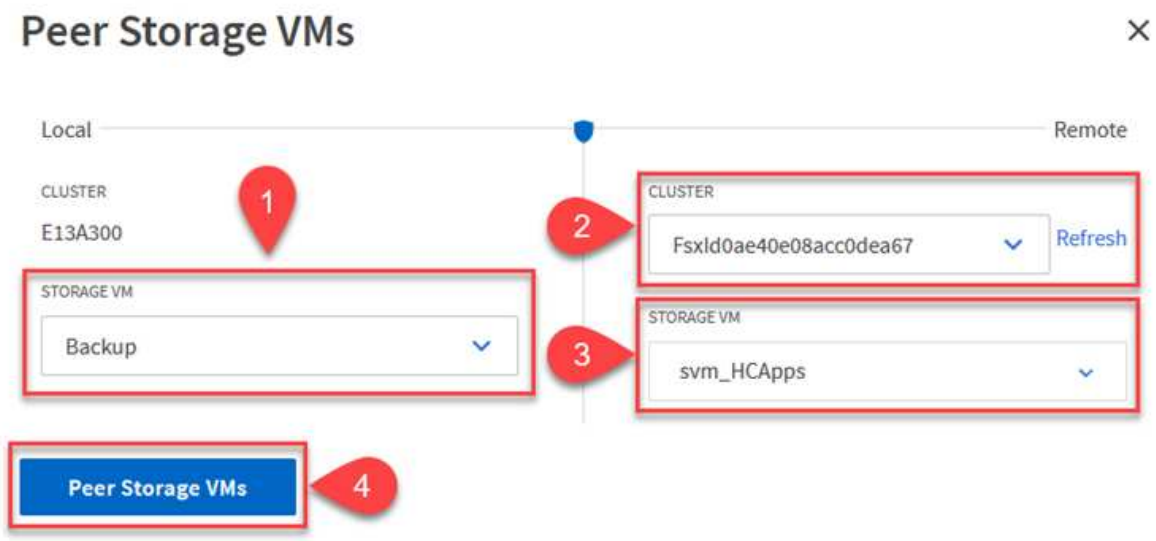
1. Dal cluster ONTAP di destinazione, utilizza il seguente comando dall'interfaccia CLI per creare la relazione peer SVM:

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

2. Dal cluster ONTAP di origine, accettare la relazione di peering con Gestore di sistema ONTAP o CLI.
3. Da Gestore di sistema ONTAP, andare a protezione > Panoramica e selezionare le VM di storage peer in peer di macchine virtuali di storage.



4. Nella finestra di dialogo Peer Storage VM, compilare i campi obbligatori:
   - La VM di storage di origine
   - Il cluster di destinazione
   - La VM di storage di destinazione



5. Fare clic su Peer Storage VM per completare il processo di peering SVM.

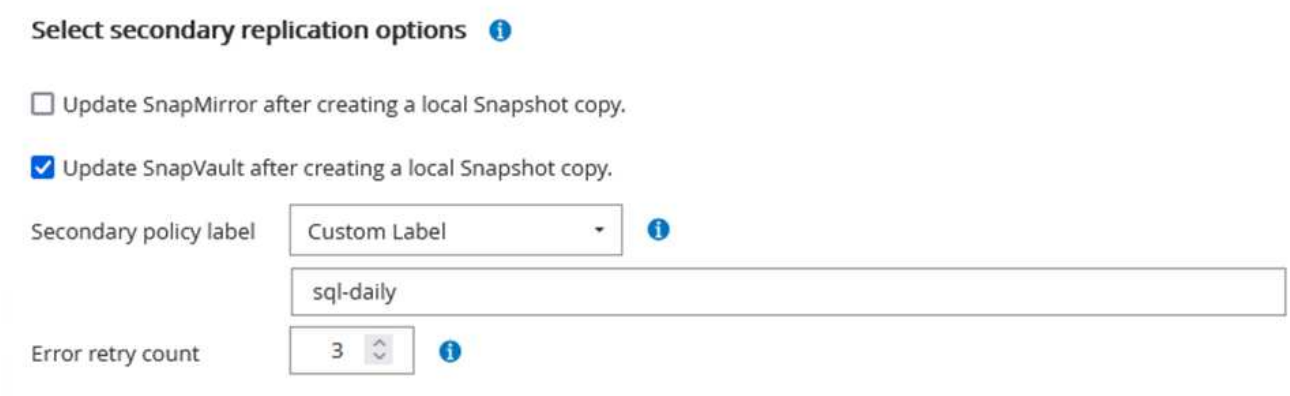
Creare un criterio di conservazione delle snapshot

SnapCenter gestisce le pianificazioni di conservazione per i backup che esistono come copie Snapshot sul sistema di storage primario. Questo viene stabilito quando si crea un criterio in SnapCenter. SnapCenter non gestisce le policy di conservazione per i backup conservati nei sistemi di storage secondari. Questi criteri vengono gestiti separatamente attraverso un criterio SnapMirror creato nel cluster FSX secondario e associato ai volumi di destinazione che si trovano in una relazione SnapMirror con il volume di origine.

Quando si crea un criterio SnapCenter, è possibile specificare un'etichetta di criterio secondaria che viene aggiunta all'etichetta SnapMirror di ogni snapshot generato quando viene eseguito un backup SnapCenter.

> Sullo storage secondario, queste etichette vengono associate alle regole dei criteri associate al volume di destinazione allo scopo di applicare la conservazione degli snapshot.

L'esempio seguente mostra un'etichetta SnapMirror presente su tutte le snapshot generate come parte di una policy utilizzata per i backup giornalieri del database SQL Server e dei volumi di log.



Per ulteriori informazioni sulla creazione di criteri SnapCenter per un database SQL Server, vedere "Documentazione SnapCenter".

È necessario innanzitutto creare un criterio SnapMirror con regole che determinano il numero di copie snapshot da conservare.

1. Creare il criterio SnapMirror sul cluster FSX.

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

2. Aggiungere regole al criterio con le etichette SnapMirror che corrispondono alle etichette dei criteri secondari specificate nei criteri SnapCenter.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

Il seguente script fornisce un esempio di regola che è possibile aggiungere a un criterio:

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

Creare regole aggiuntive per ciascuna etichetta SnapMirror e il numero di snapshot da conservare (periodo di conservazione).

Creare volumi di destinazione

Per creare un volume di destinazione su ONTAP che sarà destinatario di copie Snapshot dai volumi di origine, esegui il seguente comando sul cluster ONTAP di destinazione:

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

Creare le relazioni di SnapMirror tra i volumi di origine e di destinazione

Per creare una relazione di SnapMirror tra un volume di origine e di destinazione, esegui il seguente comando sul cluster ONTAP di destinazione:

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

Inizializzare le relazioni di SnapMirror

Inizializzare la relazione SnapMirror. Questo processo avvia un nuovo snapshot generato dal volume di origine e lo copia nel volume di destinazione.

Per creare un volume, esegui il seguente comando sul cluster ONTAP di destinazione:

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

Configurare il plug-in SnapCenter per VMware vSphere

Una volta installato, è possibile accedere al plug-in SnapCenter per VMware vSphere dall'interfaccia di gestione dell'appliance vCenter Server. SCV gestirà i backup degli archivi dati NFS montati sugli host ESXi e che contengono le macchine virtuali Windows e Linux.

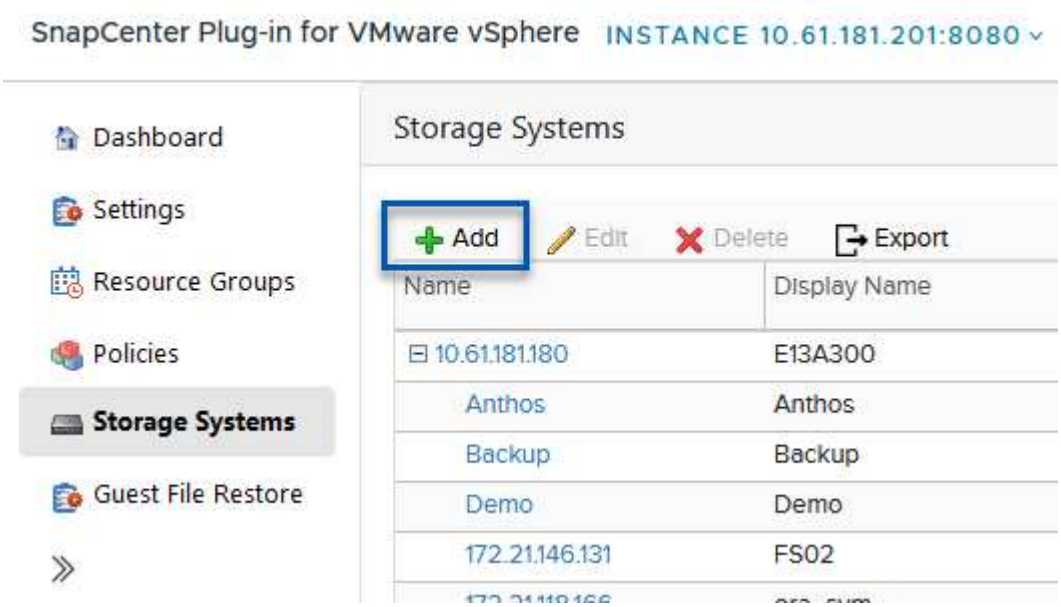
Esaminare "Workflow di data Protection" Sezione della documentazione del distributore idraulico per ulteriori informazioni sulle fasi di configurazione dei backup.

Per configurare backup di macchine virtuali e datastore, è necessario completare i seguenti passaggi dall'interfaccia del plug-in.

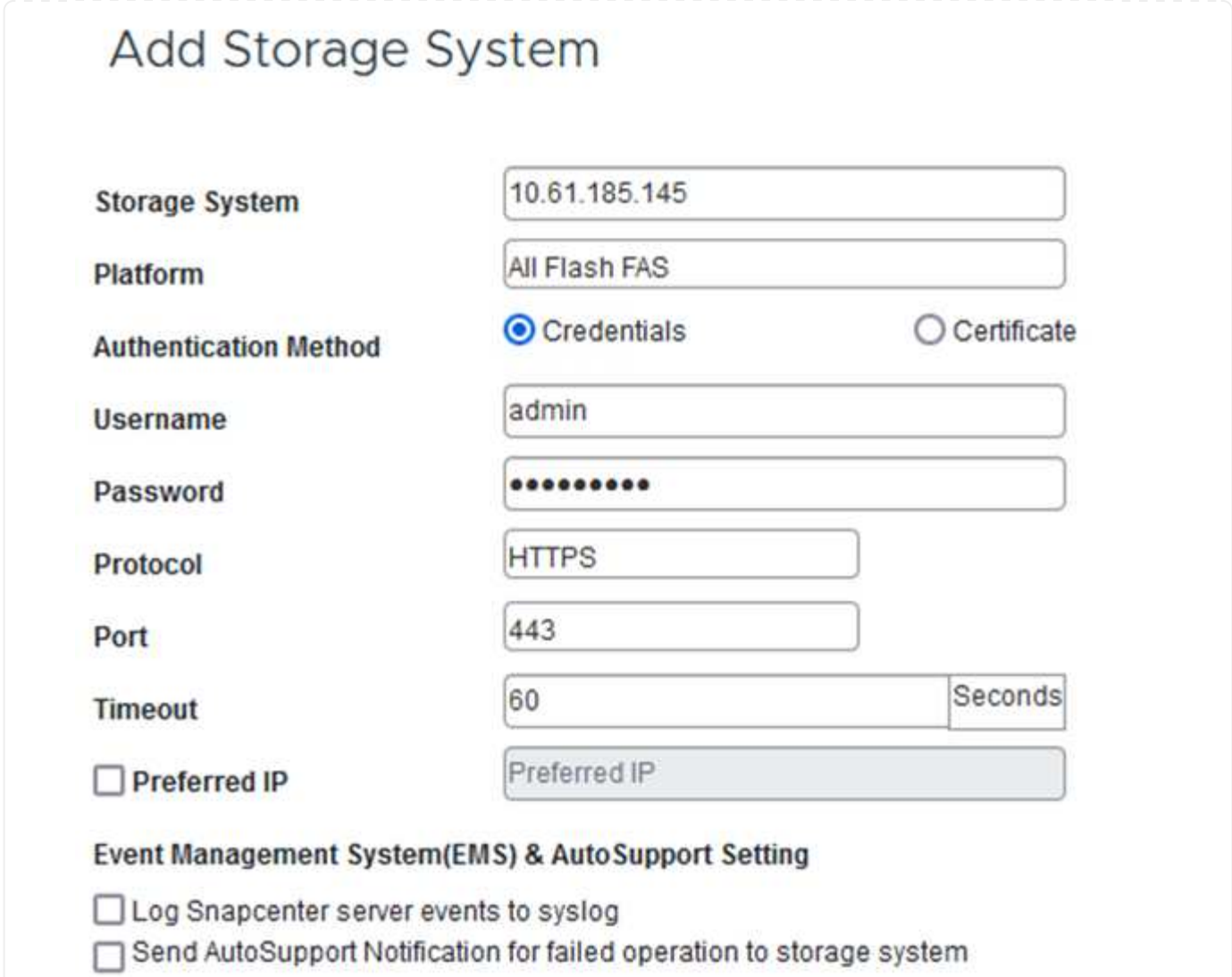
Sistemi storage Discovery ONTAP

Scopri i cluster di storage ONTAP da utilizzare per il backup primario e secondario.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **sistemi di archiviazione** nel menu a sinistra e fare clic sul pulsante **Aggiungi**.



2. Compilare le credenziali e il tipo di piattaforma per il sistema di storage ONTAP primario e fare clic su **Aggiungi**.



3. Ripetere questa procedura per il sistema di storage ONTAP secondario.

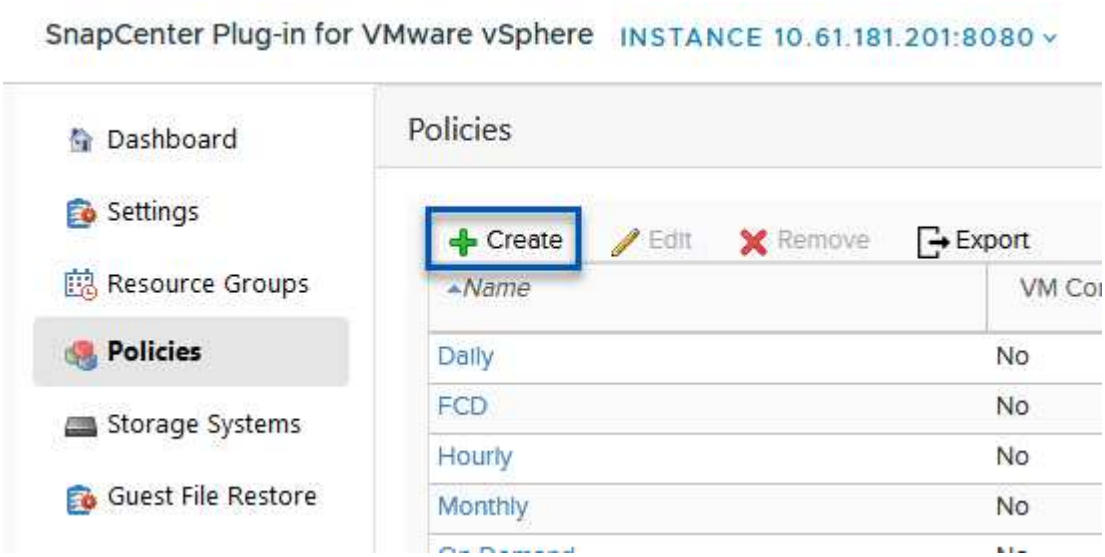
Creare le politiche di backup dei distributori idraulici

I criteri specificano il periodo di conservazione, la frequenza e le opzioni di replica per i backup gestiti da SCV.

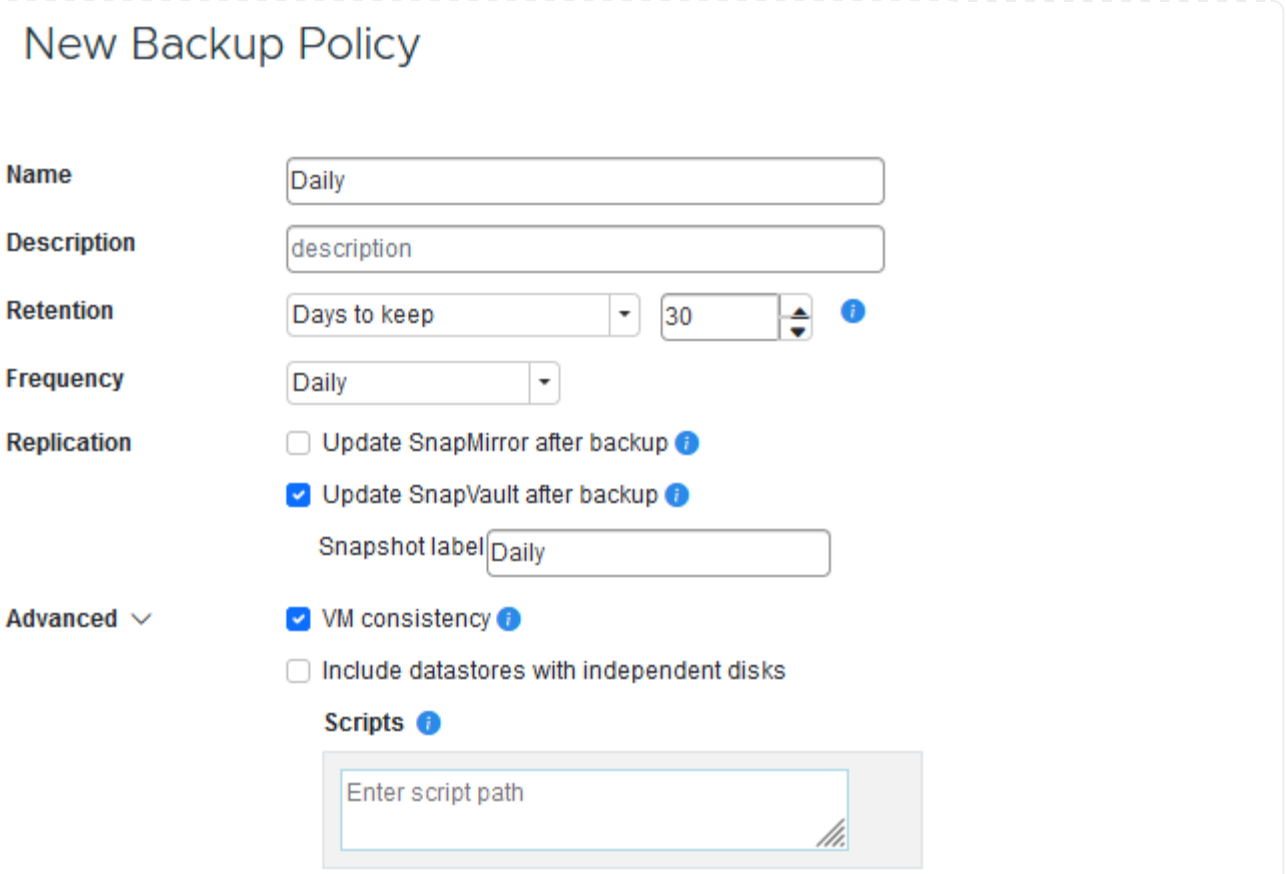
Esaminare "Creare policy di backup per macchine virtuali e datastore" della documentazione per ulteriori informazioni.

Per creare i criteri di backup, attenersi alla seguente procedura:

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **Policies** nel menu a sinistra e fare clic sul pulsante **Create**.



2. Specificare un nome per il criterio, il periodo di conservazione, la frequenza e le opzioni di replica e l'etichetta dello snapshot.



Quando si crea una policy nel plug-in di SnapCenter sono visualizzate le opzioni per SnapMirror e SnapVault. Scegliendo SnapMirror, il programma di conservazione specificato nella policy sarà lo stesso per gli snapshot primari e secondari. Scegliendo SnapVault, il programma di conservazione per la snapshot secondaria si baserà su una pianificazione separata implementata con la relazione di SnapMirror. Questa funzione è utile quando si desiderano periodi di conservazione più lunghi per backup secondari.

Le etichette degli Snapshot sono utili per attuare policy con uno specifico periodo di conservazione per le copie SnapVault replicate nel cluster ONTAP secondario. Quando SCV viene utilizzato con il backup e ripristino di BlueXP, il campo dell'etichetta dell'istantanea deve essere vuoto oppure match l'etichetta specificata nel criterio di backup di BlueXP.

3. Ripetere la procedura per ogni criterio richiesto. Ad esempio, separare i criteri per i backup giornalieri, settimanali e mensili.

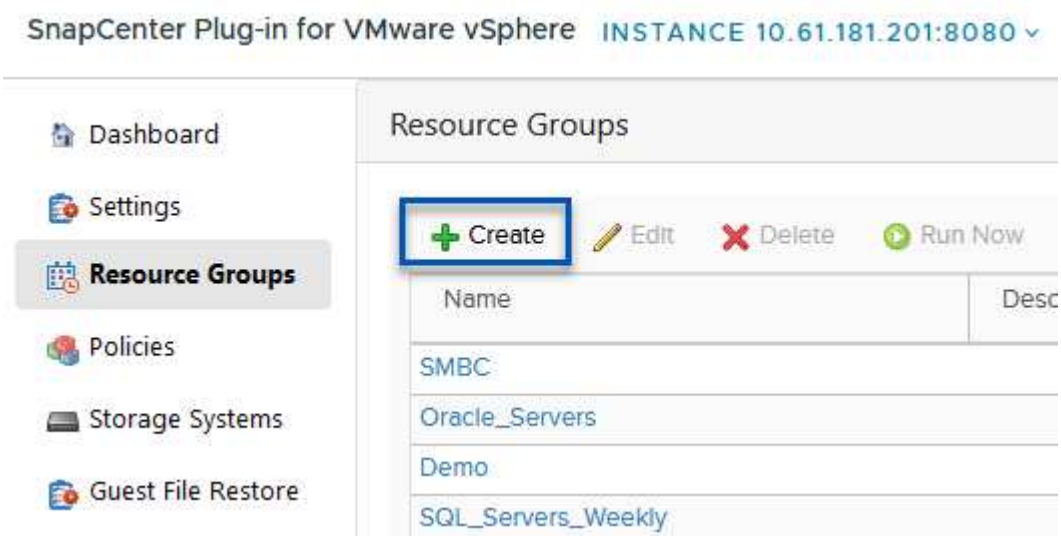
Creare gruppi di risorse

I gruppi di risorse contengono gli archivi dati e le macchine virtuali da includere in un processo di backup, insieme ai criteri e alla pianificazione di backup associati.

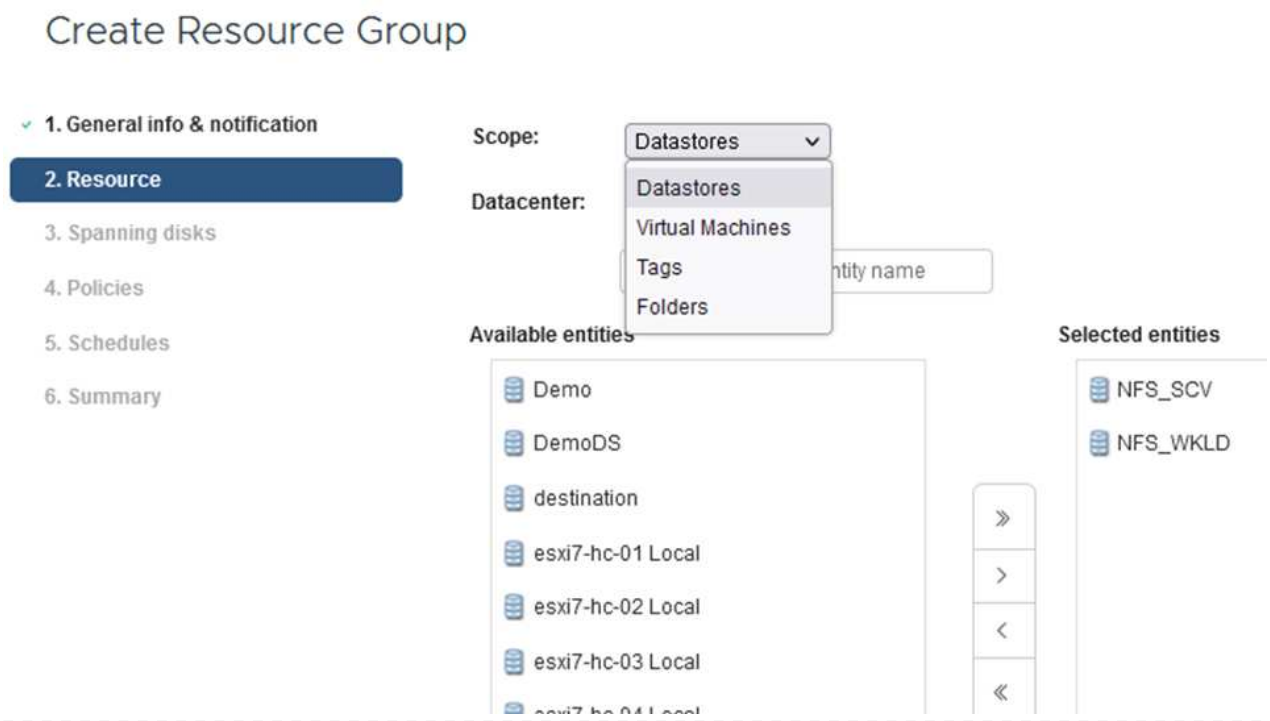
Esaminare "Creare gruppi di risorse" della documentazione per ulteriori informazioni.

Per creare gruppi di risorse, completare i seguenti passaggi.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **gruppi di risorse** nel menu a sinistra e fare clic sul pulsante **Crea**.

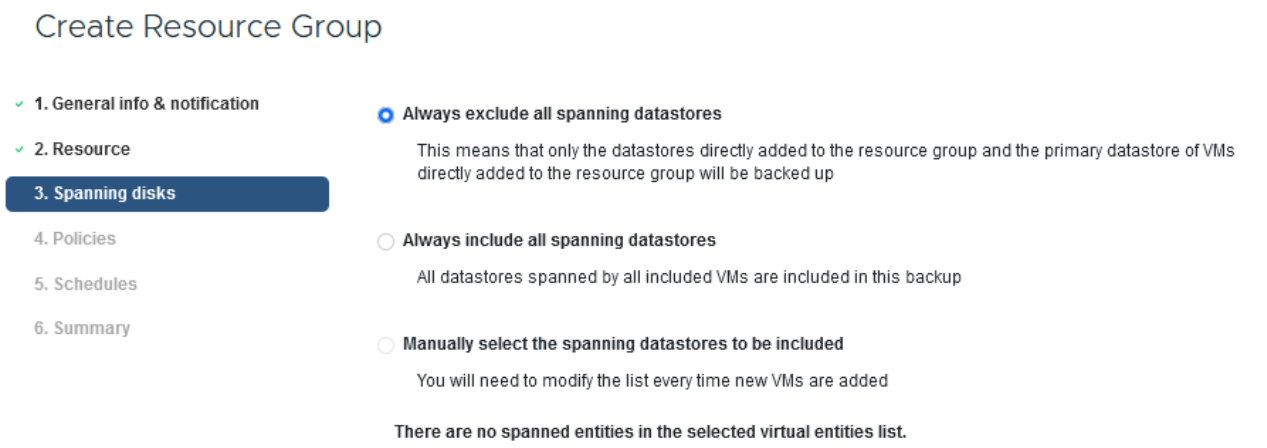


2. Nella procedura guidata Crea gruppo di risorse, immettere un nome e una descrizione per il gruppo, nonché le informazioni necessarie per ricevere le notifiche. Fare clic su **Avanti**
3. Nella pagina successiva selezionare i datastore e le macchine virtuali che si desidera includere nel processo di backup, quindi fare clic su **Avanti**.



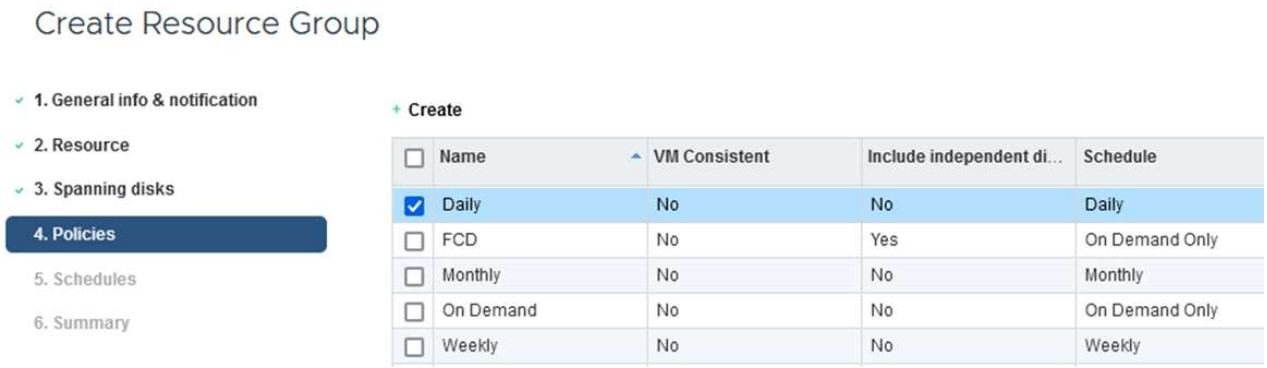
Hai la possibilità di selezionare macchine virtuali specifiche o interi datastore. Indipendentemente dal tipo di scelta effettuata, viene eseguito il backup dell'intero volume (e datastore) poiché il backup è il risultato di una snapshot del volume sottostante. Nella maggior parte dei casi, è più semplice scegliere l'intero datastore. Tuttavia, se si desidera limitare l'elenco delle VM disponibili durante il ripristino, è possibile scegliere solo un sottoinsieme di VM per il backup.

4. Scegli le opzioni per l'estensione dei datastore per le macchine virtuali con VMDK che risiedono in più datastore e fai clic su **Avanti**.



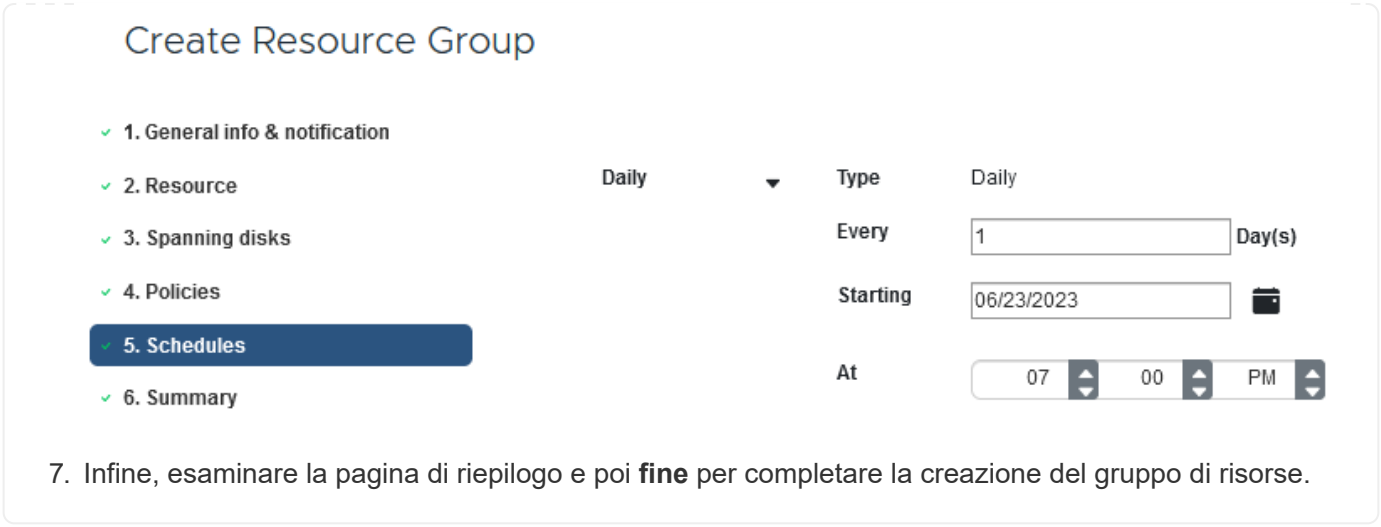
Il backup e recovery di BlueXP non supporta al momento il backup di macchine virtuali con VMDK che coprono più datastore.

5. Nella pagina successiva, selezionare i criteri da associare al gruppo di risorse e fare clic su **Avanti**.



Quando si esegue il backup di snapshot gestite da SCV su storage a oggetti utilizzando il backup e ripristino di BlueXP, ogni gruppo di risorse può essere associato solo a una singola policy.

6. Selezionare una pianificazione che determinerà a quale ora verranno eseguiti i backup. Fare clic su **Avanti**.

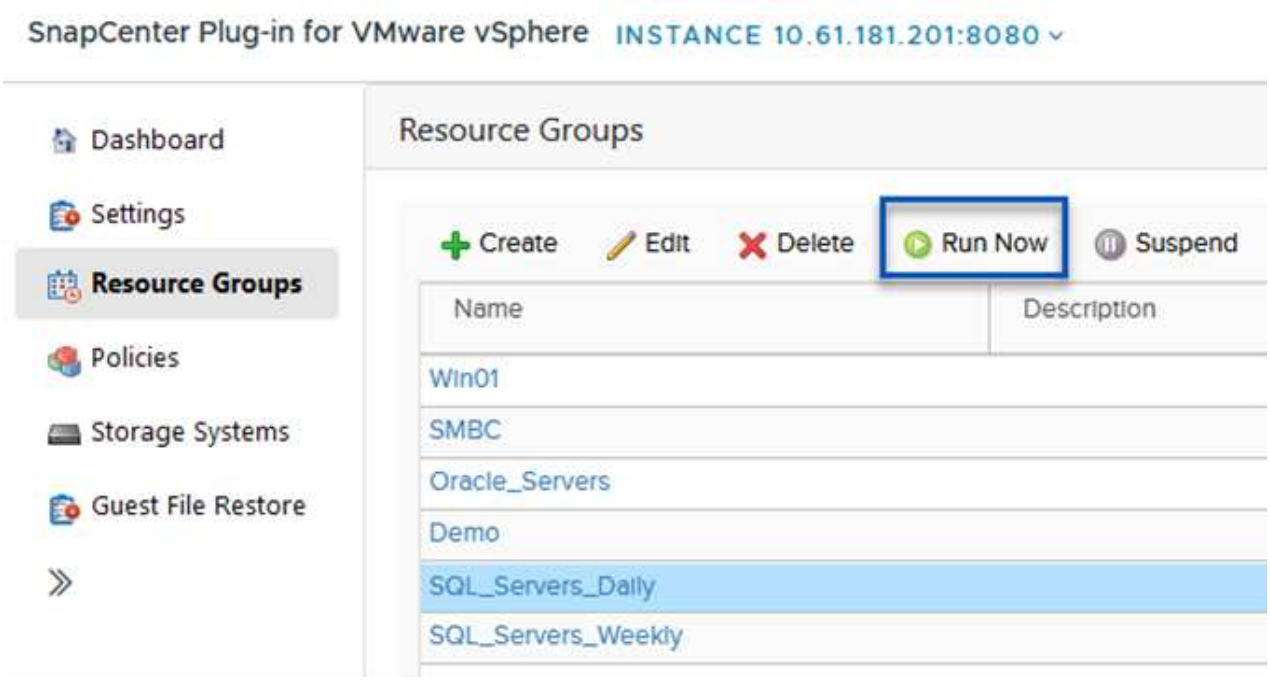


7. Infine, esaminare la pagina di riepilogo e poi **fine** per completare la creazione del gruppo di risorse.

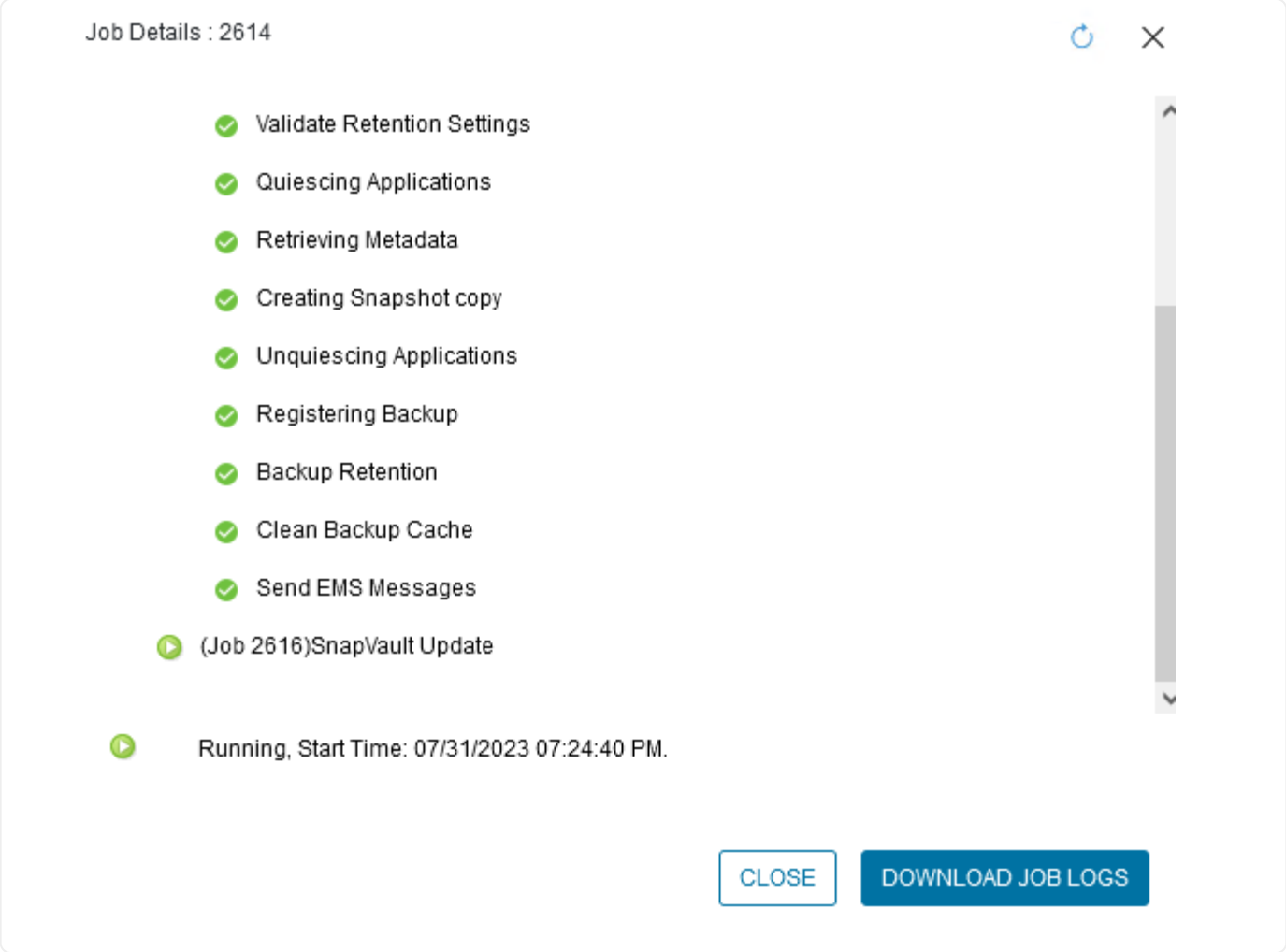
Eseguire un processo di backup

In questa fase finale, eseguire un lavoro di backup e monitorarne l'avanzamento. Almeno un processo di backup deve essere completato correttamente in SCV prima di poter rilevare le risorse dal backup e ripristino di BlueXP.

1. Nel plug-in SnapCenter per VMware vSphere, accedere a **gruppi di risorse** nel menu a sinistra.
2. Per avviare un processo di backup, selezionare il gruppo di risorse desiderato e fare clic sul pulsante **Esegui ora**.



3. Per monitorare il processo di backup, accedere a **Dashboard** nel menu a sinistra. In **attività processo recenti** fare clic sul numero ID processo per monitorare l'avanzamento del processo.



Configura i backup sullo storage a oggetti nel backup e recovery di BlueXP

Per consentire a BlueXP di gestire l'infrastruttura dati in modo efficace, richiede la previa installazione di un connettore. Il connettore esegue le azioni necessarie per rilevare le risorse e gestire le operazioni sui dati.

Per ulteriori informazioni sul connettore BlueXP, fare riferimento a. "Scopri di più sui connettori" Nella documentazione BlueXP.

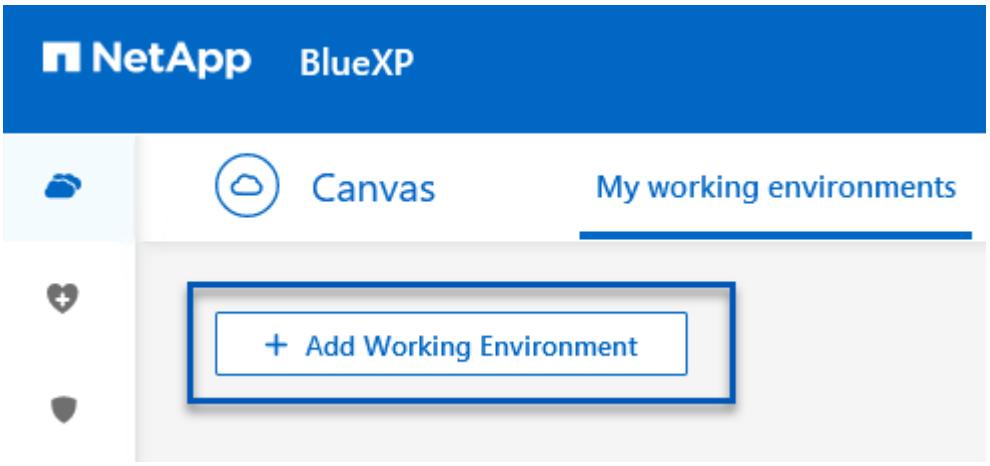
Una volta installato il connettore per il cloud provider utilizzato, una rappresentazione grafica dell'archivio oggetti sarà visibile da Canvas.

Per configurare il backup e ripristino BlueXP sui dati di backup gestiti da SCV on-premise, attenersi alla seguente procedura:

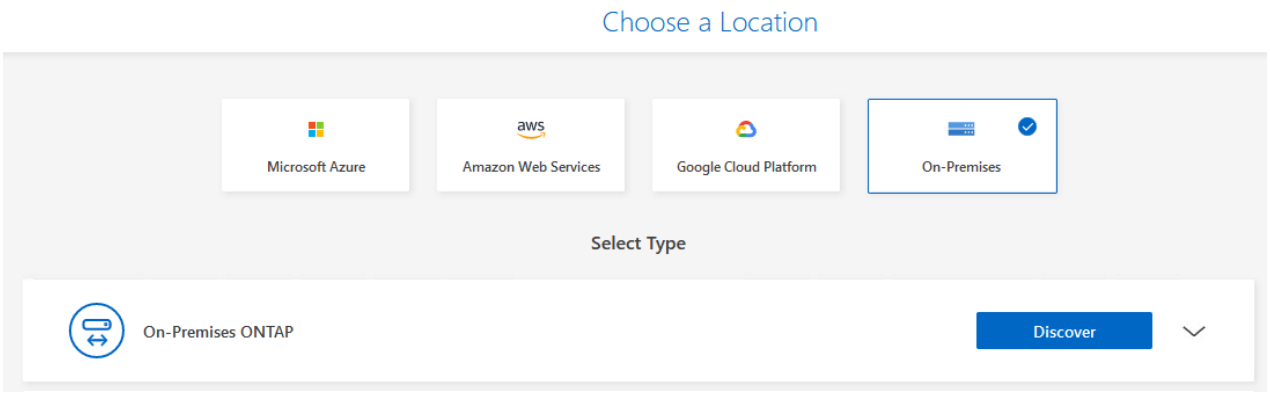
Aggiungere ambienti di lavoro al Canvas

Il primo passo è aggiungere i sistemi storage ONTAP on-premise ad BlueXP

1. Da Canvas selezionare **Aggiungi ambiente di lavoro** per iniziare.



2. Selezionare **on-Premises** (locale) dalla scelta delle località, quindi fare clic sul pulsante **Discover** (rileva).



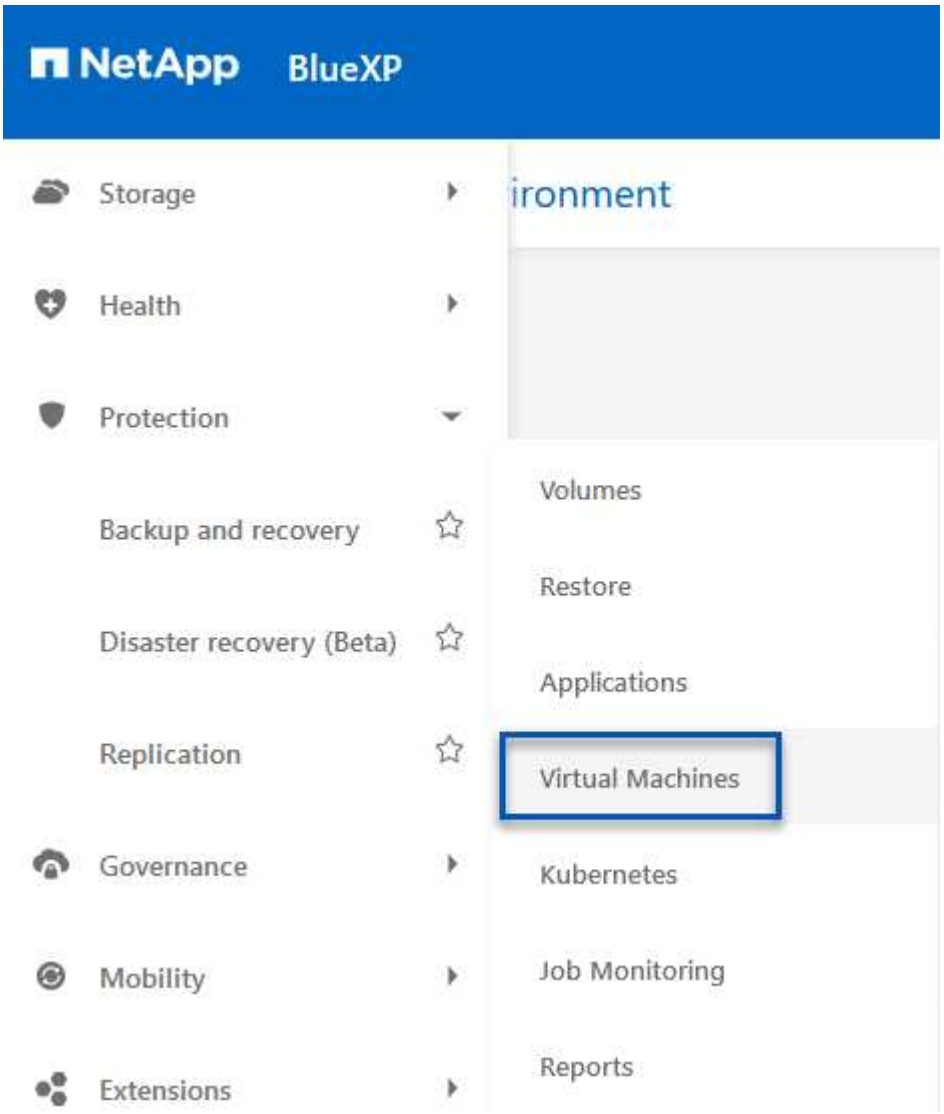
3. Compilare le credenziali per il sistema di archiviazione ONTAP e fare clic sul pulsante **Scopri** per aggiungere l'ambiente di lavoro.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

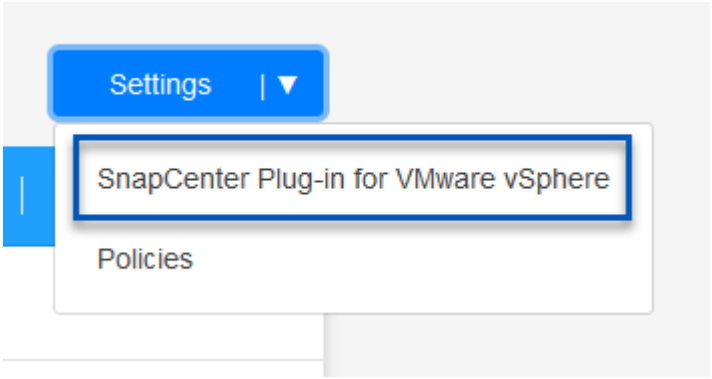
Scopri SCV appliance e vCenter on-premise

Per rilevare il datastore on-premise e le risorse delle macchine virtuali, Aggiungi le informazioni per il broker di dati SCV e le credenziali per l'appliance di gestione vCenter.

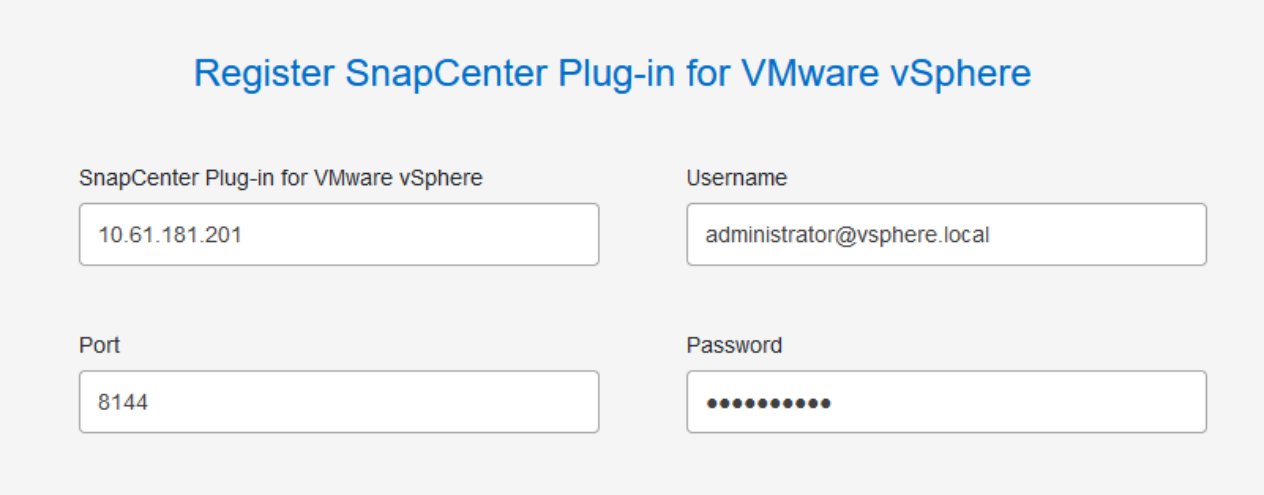
1. Dal menu a sinistra di BlueXP, selezionare **protezione > Backup e ripristino > macchine virtuali**



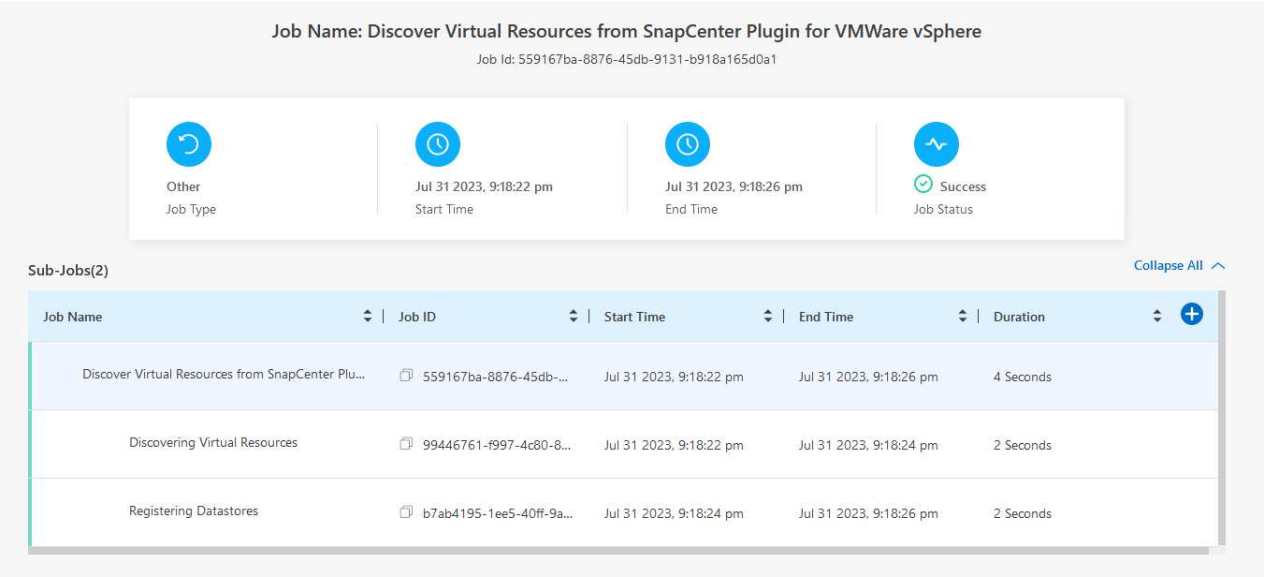
2. Dalla schermata principale macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare **Plug-in SnapCenter per VMware vSphere**.



3. Fare clic sul pulsante **Registra**, quindi immettere l'indirizzo IP e il numero di porta per l'appliance plug-in SnapCenter e il nome utente e la password per l'appliance di gestione vCenter. Fare clic sul pulsante **Registra** per avviare il processo di ricerca.



4. È possibile monitorare l'avanzamento dei lavori dalla scheda monitoraggio processi.



5. Una volta completato il rilevamento, sarà possibile visualizzare i datastore e le macchine virtuali in tutti gli apparecchi SCV rilevati.

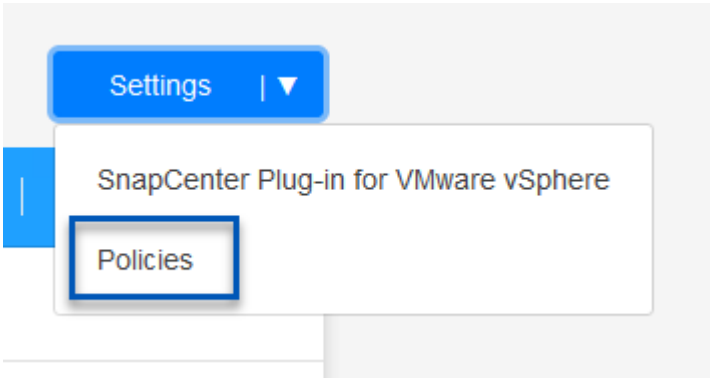
   Immagine::bxp-scv-Hybrid-23.png[Visualizza risorse disponibili]

Crea policy di backup BlueXP

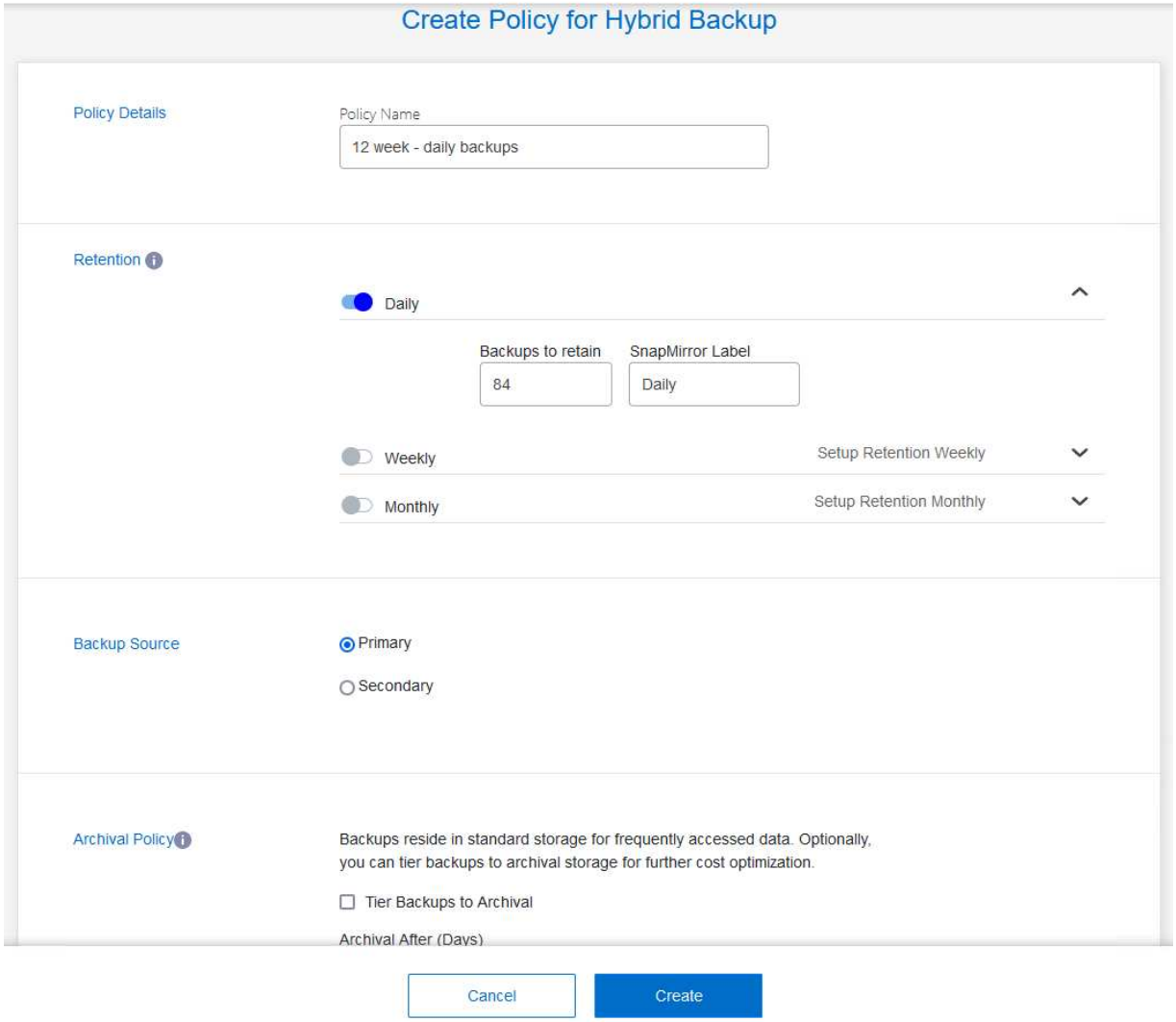
Nel backup e recovery di BlueXP per le macchine virtuali, crea policy per specificare il periodo di conservazione, l'origine di backup e la policy di archiviazione.

Per ulteriori informazioni sulla creazione dei criteri, consultare "Creare una policy per il backup dei datastore".

1. Dalla pagina principale di backup e ripristino di BlueXP per le macchine virtuali, accedere al menu a discesa **Impostazioni** e selezionare **Criteri**.



2. Fare clic su **Crea criterio** per accedere alla finestra **Crea criterio per il backup ibrido**.
   a. Aggiungere un nome per il criterio
   b. Selezionare il periodo di conservazione desiderato
   c. Seleziona se i backup devono provenire dal sistema di storage ONTAP on-premise primario o secondario
   d. In alternativa, è possibile specificare, dopo il periodo di tempo, il tiering dei backup nello storage di archivio, ottenendo ulteriori risparmi sui costi.



L'etichetta SnapMirror immessa qui viene utilizzata per identificare i backup da applicare anche la policy. Il nome dell'etichetta deve corrispondere al nome dell'etichetta nella politica SCV in loco corrispondente.

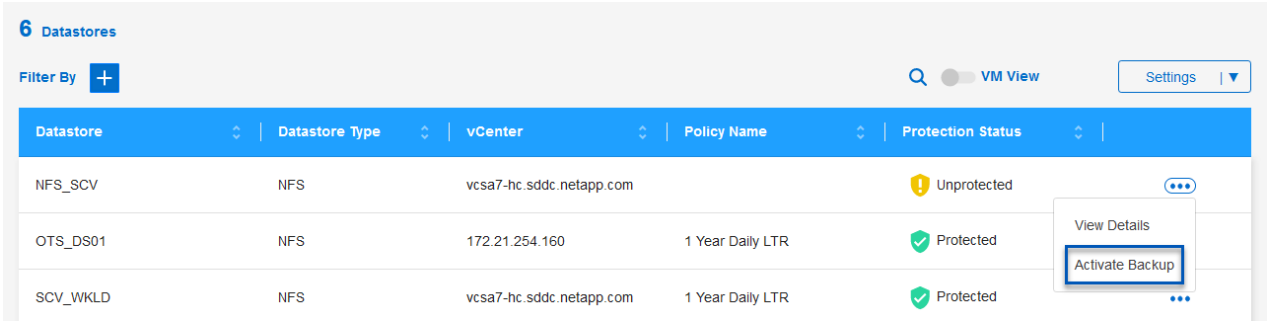
3. Fare clic su **Crea** per completare la creazione del criterio.

Effettuare il backup dei datastore su Amazon Web Services

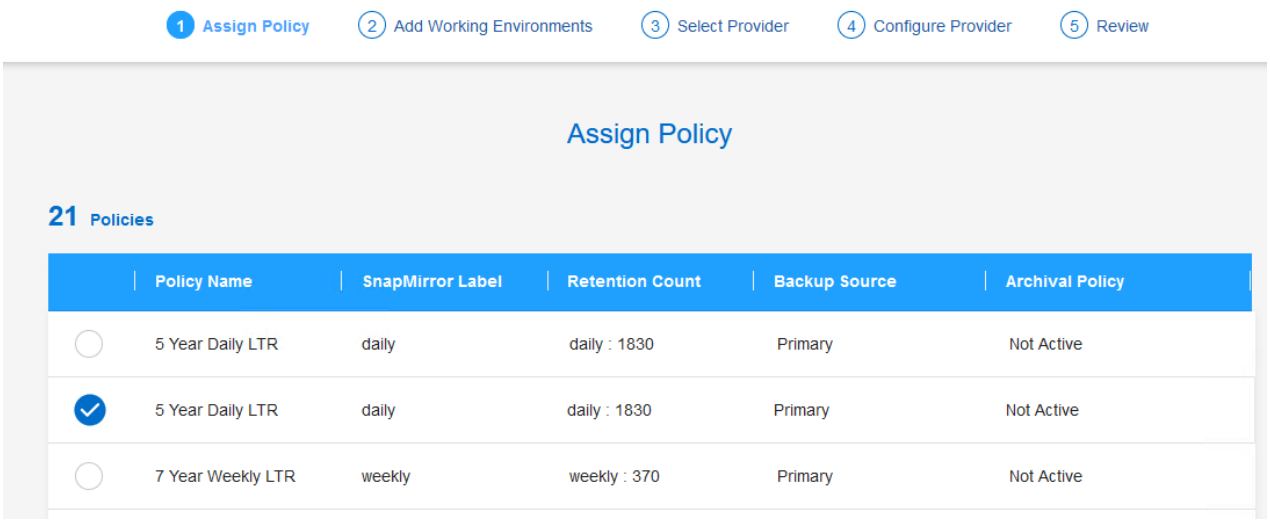
L'ultima fase consiste nell'attivare la data Protection per i singoli datastore e le macchine virtuali. Segue una descrizione della modalità di attivazione dei backup in AWS.

Per ulteriori informazioni, fare riferimento a. "Eseguire il backup dei datastore su Amazon Web Services".

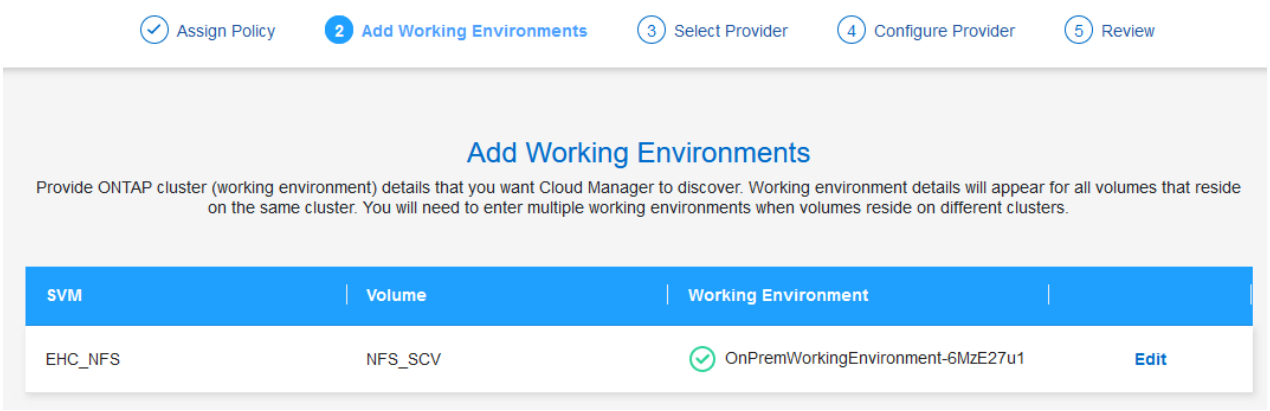
1. Dalla pagina principale di backup e recovery di BlueXP per le macchine virtuali, accedi al menu a discesa delle impostazioni per il datastore da sottoporre a backup e seleziona **attiva backup**.



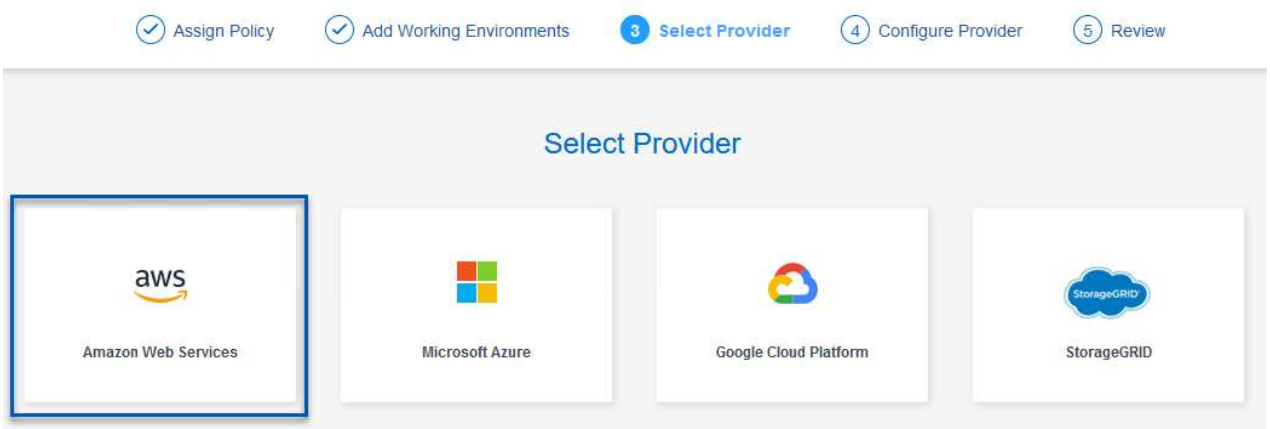
2. Assegnare il criterio da utilizzare per l'operazione di protezione dei dati e fare clic su **Avanti**.



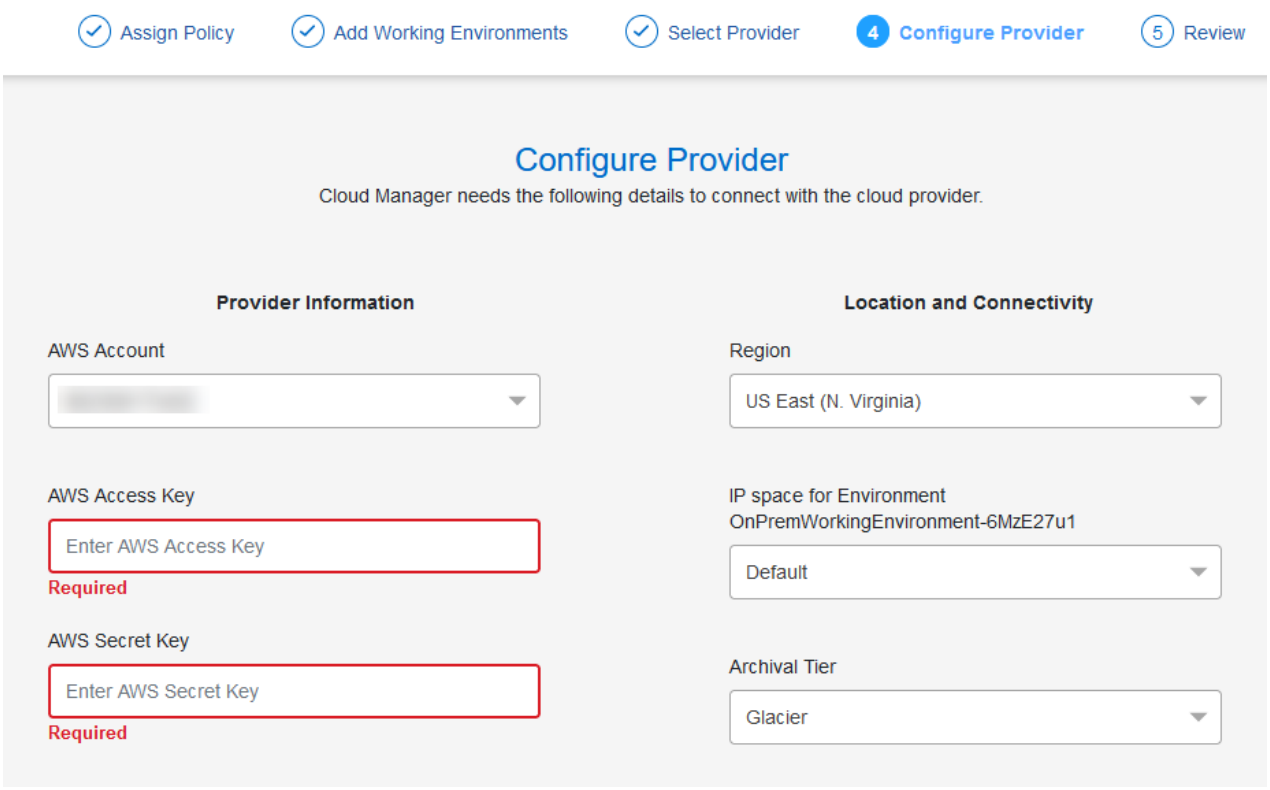
3. Nella pagina **Aggiungi ambienti di lavoro**, il datastore e l'ambiente di lavoro con un segno di spunta dovrebbero apparire se l'ambiente di lavoro è stato precedentemente rilevato. Se l'ambiente di lavoro non è stato rilevato in precedenza, è possibile aggiungerlo qui. Fare clic su **Avanti** per continuare.



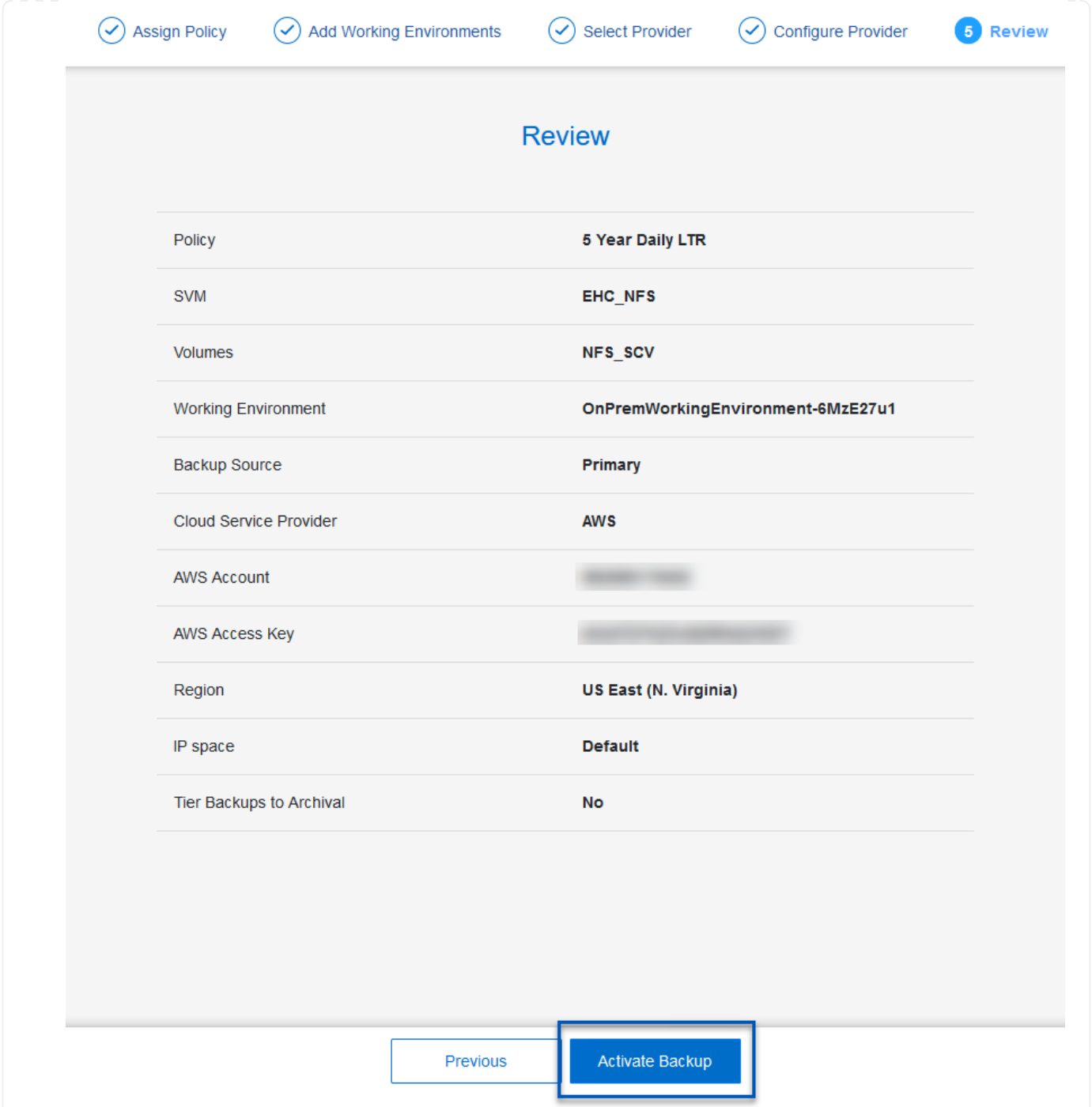
4. Nella pagina **Select Provider** (Seleziona fornitore), fare clic su AWS, quindi sul pulsante **Next** (Avanti) per continuare.



5. Compila le informazioni sulle credenziali specifiche del provider per AWS, inclusi la chiave di accesso AWS e la chiave segreta, la regione e il Tier di archivio da utilizzare. Inoltre, seleziona lo spazio IP ONTAP per il sistema storage ONTAP on-premise. Fare clic su **Avanti**.



6. Infine, esaminare i dettagli del processo di backup e fare clic sul pulsante **attiva backup** per avviare la protezione dei dati del datastore.



A questo punto il trasferimento dei dati potrebbe non iniziare immediatamente. Il backup e recovery di BlueXP analizza ogni ora le snapshot in sospeso e le trasferisce nello storage a oggetti.

Ripristino delle macchine virtuali in caso di perdita di dati

Garantire la protezione dei dati è solo un aspetto della protezione dati completa. Un aspetto altrettanto cruciale è la possibilità di ripristinare tempestivamente i dati da qualsiasi posizione in caso di perdita di dati o attacco ransomware. Questa funzionalità è fondamentale per mantenere operative di business perfette e soddisfare i recovery point objective.

NetApp offre una strategia 3-2-1 altamente adattabile, che offre un controllo customizzato sulle pianificazioni della conservazione nelle posizioni di storage primario, secondario e a oggetti. Questa strategia offre la flessibilità necessaria per personalizzare gli approcci di protezione dei dati in base a esigenze specifiche.

Questa sezione offre una panoramica del processo di ripristino dei dati dal plug-in SnapCenter per VMware vSphere e da backup e recovery BlueXP per le macchine virtuali.

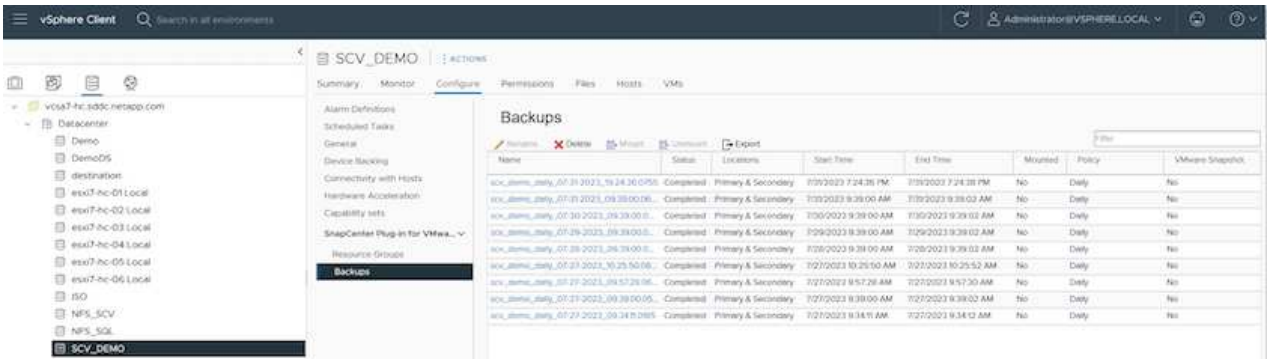
Ripristino di macchine virtuali dal plug-in SnapCenter per VMware vSphere

Per questa soluzione, le macchine virtuali sono state ripristinate in posizioni originali e alternative. Non tutti gli aspetti delle capacità di ripristino dei dati dei distributori idraulici saranno trattati in questa soluzione. Per informazioni dettagliate su tutto ciò che il distributore idraulico ha da offrire, fare riferimento alla "Ripristinare le macchine virtuali dai backup" nella documentazione del prodotto.

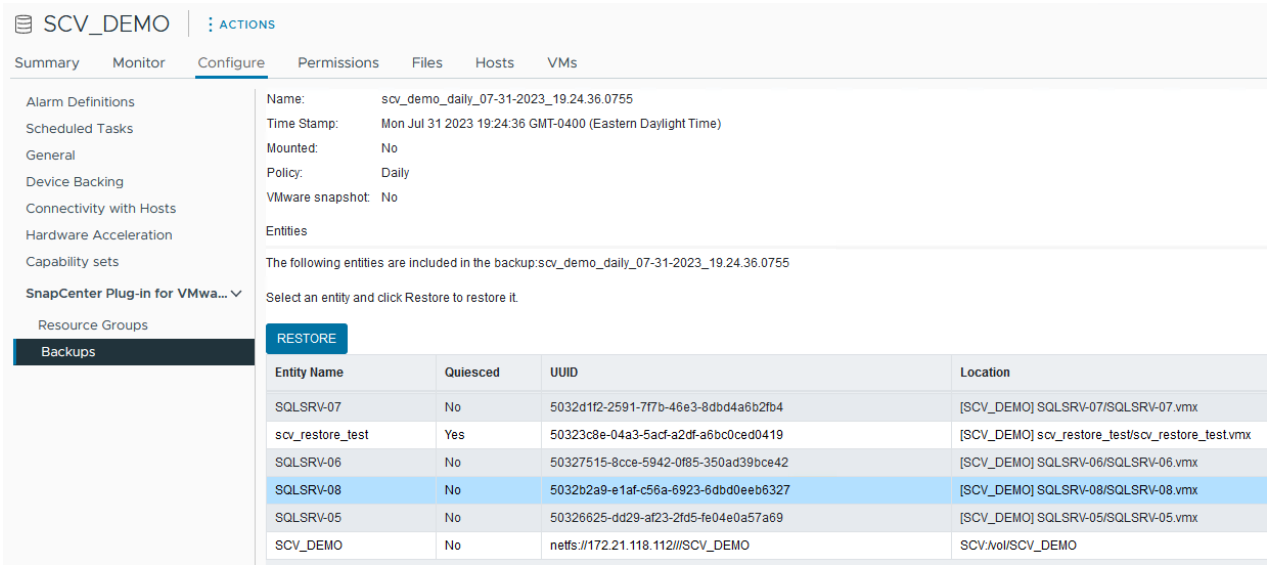
Ripristinare le macchine virtuali dal distributore idraulico

Completare i seguenti passaggi per ripristinare un ripristino di una macchina virtuale dallo storage primario o secondario.

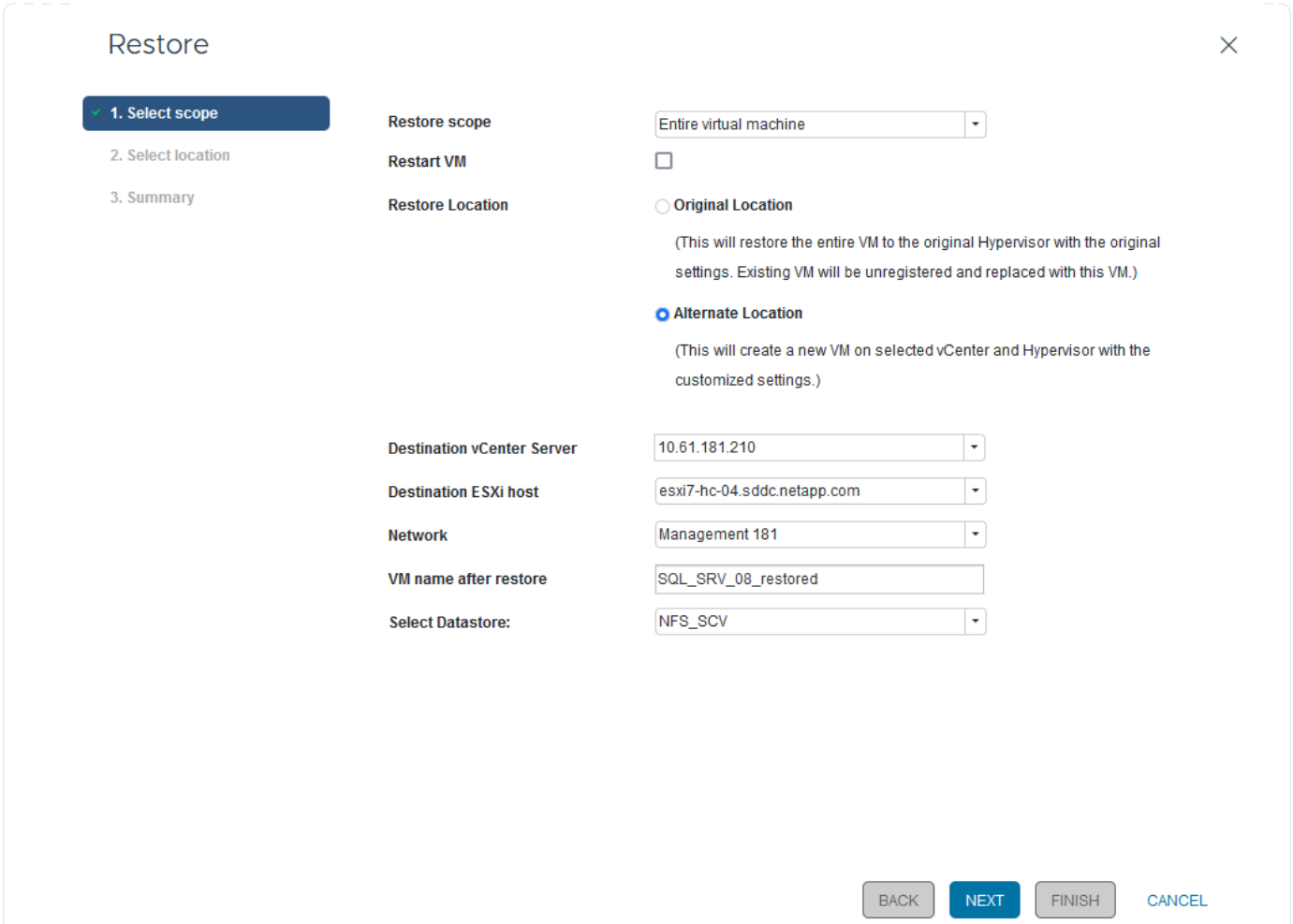
1. Dal client vCenter, accedere a **inventario > archiviazione** e fare clic sul datastore che contiene le macchine virtuali che si desidera ripristinare.
2. Dalla scheda **Configure** fare clic su **backups** per accedere all'elenco dei backup disponibili.



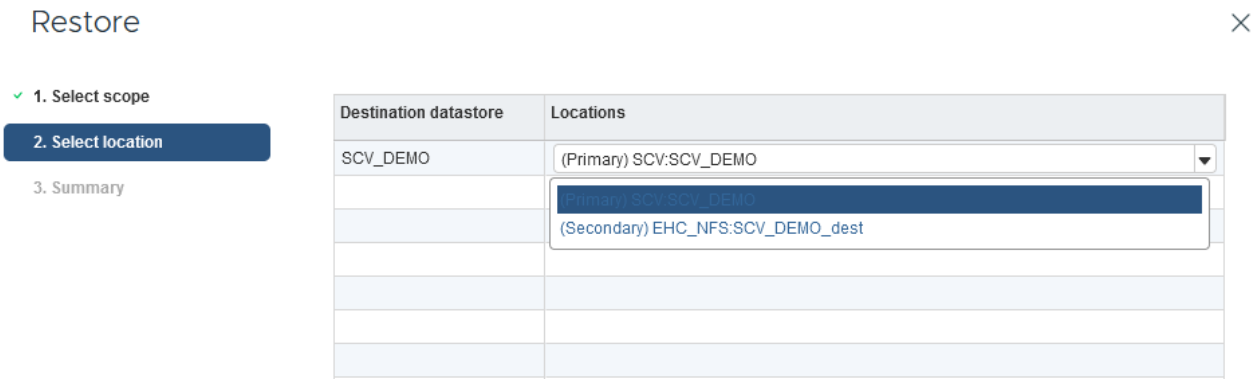
3. Fare clic su un backup per accedere all'elenco delle VM, quindi selezionare una VM da ripristinare. Fare clic su **Ripristina**.



4. Dalla procedura guidata di ripristino, selezionare per ripristinare l'intera macchina virtuale o un VMDK specifico. Seleziona per eseguire l'installazione nella posizione originale o in una posizione alternativa, fornisci il nome della macchina virtuale dopo il ripristino e il datastore di destinazione. Fare clic su **Avanti**.



5. Scegli di eseguire il backup dalla posizione dello storage primario o secondario.



6. Infine, esaminare un riepilogo del processo di backup e fare clic su fine per avviare il processo di ripristino.

Ripristino di macchine virtuali dal backup e recovery di BlueXP per le macchine virtuali

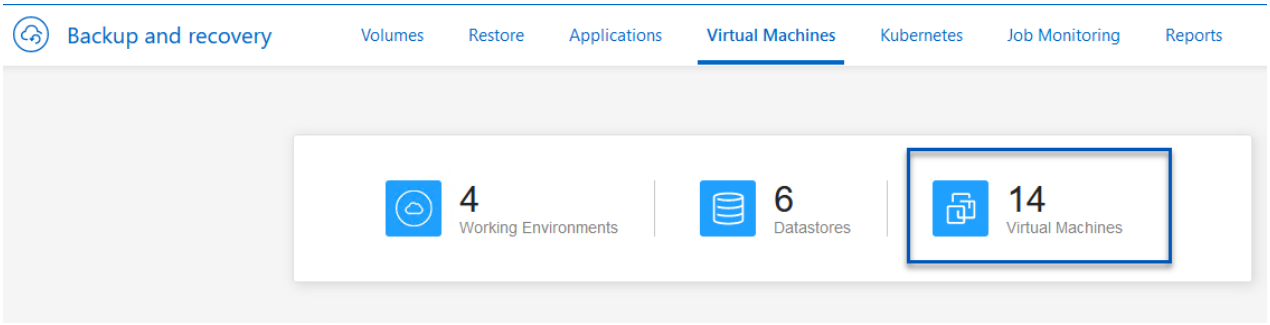
Il backup e recovery di BlueXP per le macchine virtuali consente di ripristinare le macchine virtuali nella loro posizione originale. È possibile accedere alle funzioni di ripristino dalla console web BlueXP.

Per ulteriori informazioni, fare riferimento a. "Ripristinare i dati delle macchine virtuali dal cloud".

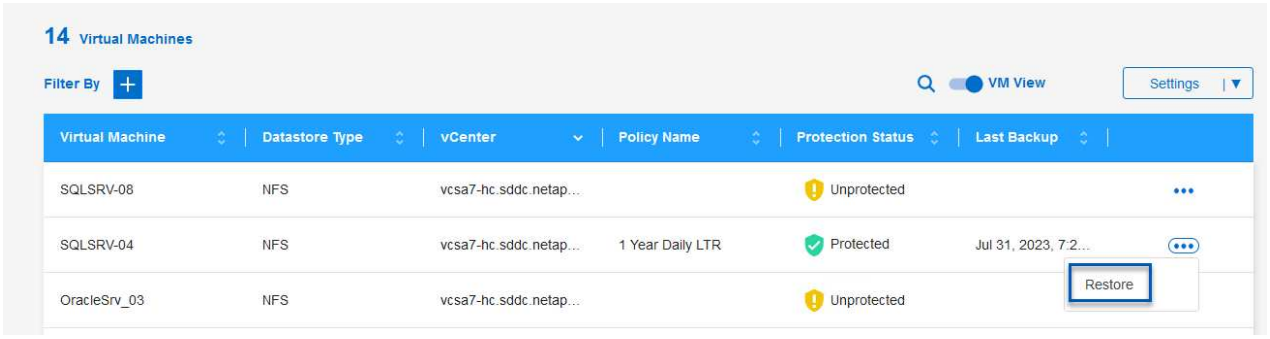
Ripristina le macchine virtuali dal backup e recovery di BlueXP

Per ripristinare una macchina virtuale dal backup e recovery di BlueXP, completa i seguenti passaggi.

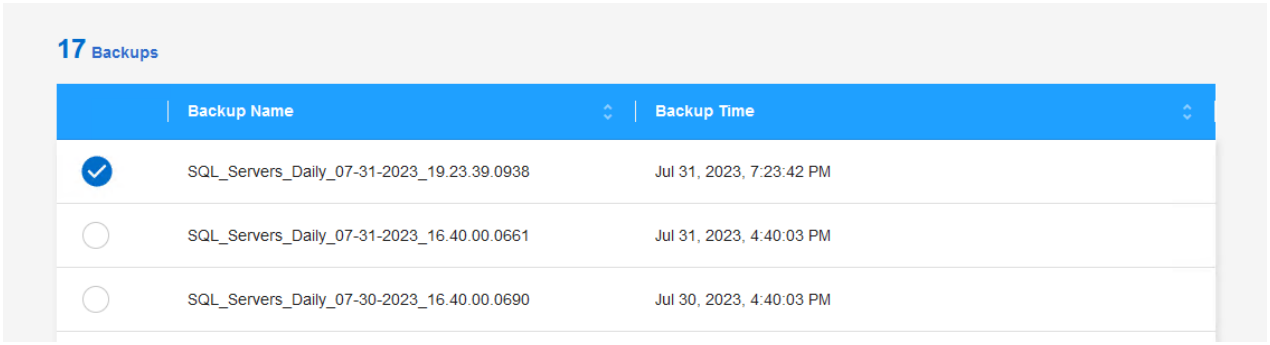
1. Accedere a **protezione > Backup e ripristino > macchine virtuali** e fare clic su macchine virtuali per visualizzare l'elenco delle macchine virtuali disponibili per il ripristino.



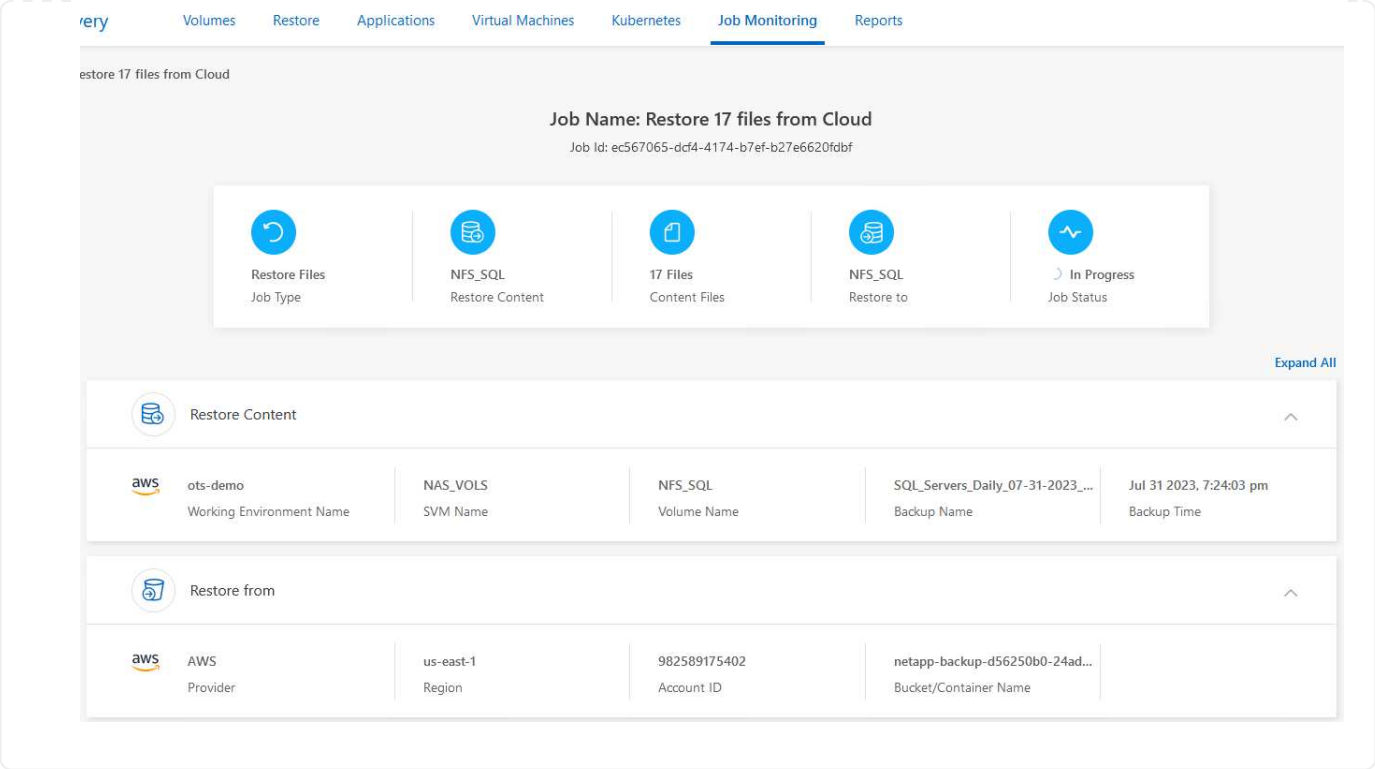
2. Accedere al menu a discesa delle impostazioni per la VM da ripristinare e selezionare



3. Selezionare il backup da cui eseguire il ripristino e fare clic su **Avanti**.



4. Esaminare un riepilogo del processo di backup e fare clic su **Ripristina** per avviare il processo di ripristino.
5. Monitorare l'avanzamento del processo di ripristino dalla scheda **monitoraggio processo**.



Conclusione

La strategia di backup 3-2-1, se implementata con il plug-in SnapCenter per backup e recovery di VMware vSphere e BlueXP per le macchine virtuali, offre una soluzione solida, affidabile e conveniente per la protezione dei dati. Questa strategia non solo garantisce ridondanza e accessibilità dei dati, ma offre anche la flessibilità di ripristinare i dati da qualsiasi posizione e da sistemi storage ONTAP on-premise e dallo storage a oggetti basato sul cloud.

Il caso di utilizzo presentato in questa documentazione si concentra sulle tecnologie comprovate di data Protection che evidenziano l'integrazione tra NetApp, VMware e i cloud provider leader. Il plug-in SnapCenter per VMware vSphere offre un'integrazione perfetta con VMware vSphere, consentendo una gestione efficiente e centralizzata delle operazioni di protezione dei dati. Questa integrazione semplifica i processi di backup e recovery per le macchine virtuali, consentendo operazioni di pianificazione, monitoraggio e ripristino flessibili all'interno dell'ecosistema VMware. Il backup e recovery di BlueXP per le macchine virtuali fornisce quello (1) in 3-2-1, fornendo backup sicuri e a corto di aria dei dati delle macchine virtuali sullo storage a oggetti basato sul cloud. L'interfaccia intuitiva e il flusso di lavoro logico offrono una piattaforma sicura per l'archiviazione a lungo termine dei dati critici.

Ulteriori informazioni

Per ulteriori informazioni sulle tecnologie presentate in questa soluzione, fare riferimento alle seguenti informazioni aggiuntive.

- "Plug-in SnapCenter per la documentazione di VMware vSphere"
- "Documentazione BlueXP"

VMware Sovereign Cloud

Risorse VMware per Sovereign Cloud

NetApp e VMware Sovereign Cloud

Panoramica di VMware Sovereign Cloud

Il concetto di sovranità sta emergendo come componente necessario del cloud computing per molte entità che elaborano e mantengono dati altamente sensibili, come ad esempio i governi nazionali e statali, e settori altamente regolamentati, come quello finanziario e sanitario. I governi nazionali stanno anche cercando di espandere la capacità economica digitale e di ridurre la dipendenza da aziende multinazionali per i propri servizi cloud.

Iniziativa VMware Sovereign Cloud

VMware definisce un cloud sovrano che:

- Protegge e sblocca il valore dei dati critici (ad esempio, dati nazionali, dati aziendali e dati personali) sia per le organizzazioni del settore pubblico che privato
- Offre una capacità nazionale per l'economia digitale
- Protegge i dati con controlli di sicurezza verificati
- Garantisce la conformità alle leggi sulla privacy dei dati
- Migliora il controllo dei dati fornendo sia la residenza dei dati che la sovranità dei dati con un controllo giurisdizionale completo

Partnership con un fornitore di servizi cloud VMware Sovereign di fiducia

Per garantire il successo, le organizzazioni devono collaborare con i partner di cui si fidano e che siano in grado di ospitare piattaforme cloud sovrane autentiche e autonome. I VMware Cloud Provider riconosciuti nell'ambito dell'iniziativa VMware Sovereign Cloud si impegnano a progettare e utilizzare soluzioni cloud basate su architetture software-defined moderne che incarnano i principi chiave e le Best practice delineate nel framework VMware Sovereign Cloud.

- **Sovranità dei dati e controllo giurisdizionale** – tutti i dati sono residenti e soggetti al controllo esclusivo e all'autorità dello Stato nazionale in cui sono stati raccolti. Le operazioni sono gestite completamente all'interno della giurisdizione
- **Accesso ai dati e integrità** – l'infrastruttura cloud è resiliente e disponibile in almeno due ubicazioni dei data center all'interno della giurisdizione con opzioni di connettività sicura e privata disponibili.
- **Sicurezza e conformità dei dati** – i controlli dei sistemi di gestione della sicurezza delle informazioni sono certificati in base a uno standard globale (o regionale) riconosciuto dal settore e sottoposti a verifiche periodiche.
- **Data Independence and Mobility** – supporto per le moderne architetture applicative per prevenire il vendor cloud lock-in e consentire la portabilità e l'indipendenza delle applicazioni

Per ulteriori informazioni su VMware, visitare il sito:

- "Panoramica di VMware Sovereign Cloud"
- "Che cos'è VMware Sovereign Cloud?"
- "Presentazione della nuova VMware Sovereign Cloud Initiative"
- "White paper tecnico su VMware Sovereign Cloud"

Netpp con VMware Sovereign Cloud: Casi di utilizzo

NetApp offre supporto per i concetti di VMware Sovereign Cloud attraverso l'integrazione di diverse tecnologie NetApp.

Utilizza i seguenti link per scoprire di più sulle integrazioni della tecnologia NetApp con VMware Sovereign Cloud:

- "NetApp StorageGRID come estensione dell'archivio oggetti"

NetApp StorageGRID come estensione dell'archivio oggetti

NetApp ha collaborato con VMware per integrare NetApp StorageGRID in VMware Cloud Director a supporto di VMware Sovereign Cloud. Questo plug-in di VMware Cloud Director consente ai service provider di utilizzare StorageGRID come offerta di storage a oggetti (indipendentemente dai casi d'utilizzo) e permette la gestione StorageGRID tramite la stessa soluzione VMware multi-tenant (VMware Cloud Director) utilizzata dai service provider per gestire altre parti del proprio catalogo di offerte.

I partner che offrono VMware Sovereign Cloud possono scegliere NetApp StorageGRID per gestire e mantenere ambienti cloud con dati non strutturati. La sua compatibilità universale nel supporto nativo per le API standard di settore, come le API Amazon S3, garantisce un'interoperabilità fluida su diversi ambienti cloud e innovazioni uniche, come la gestione automatizzata del ciclo di vita, contribuisce a garantire una protezione, uno storage e una conservazione a lungo termine dei dati non strutturati dei clienti con costi più contenuti.

L'integrazione di NetApp Sovereign Cloud con i clienti provider Cloud Director con:

- La garanzia che i dati sensibili, inclusi i metadati, rimangano sotto controllo sovrano impedendo al contempo l'accesso da parte di autorità straniere che potrebbero violare le leggi sulla privacy dei dati.
- Maggiore sicurezza e conformità per la protezione di applicazioni e dati da vettori di attacco in rapida evoluzione e al contempo garantire la conformità a un ambiente locale affidabile. infrastruttura, framework integrati ed esperti locali.
- Un'infrastruttura a prova di futuro per reagire rapidamente alle normative sulla privacy dei dati in continua evoluzione, alle minacce alla sicurezza e alla geopolitica.
- La possibilità di liberare il valore dei dati con condivisione e analisi sicure dei dati per favorire l'innovazione senza violare le leggi sulla privacy. L'integrità dei dati è protetta per garantire informazioni accurate.

Per ulteriori informazioni sull'integrazione di StorageGRID, consulta:

- "Annuncio NetApp"

Multicloud ibrido NetApp con carichi di lavoro container Red Hat OpenShift

Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

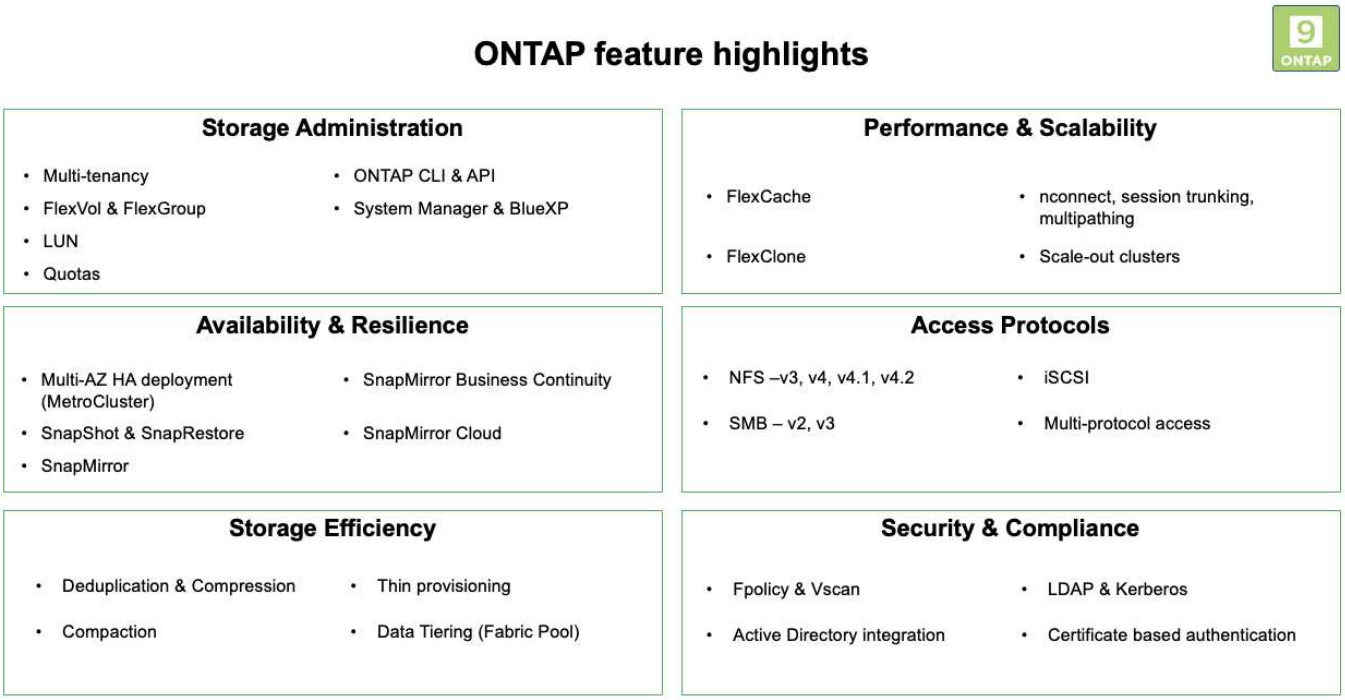
Panoramica

NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati, affidabilità e flessibilità per le implementazioni di container e Kubernetes.

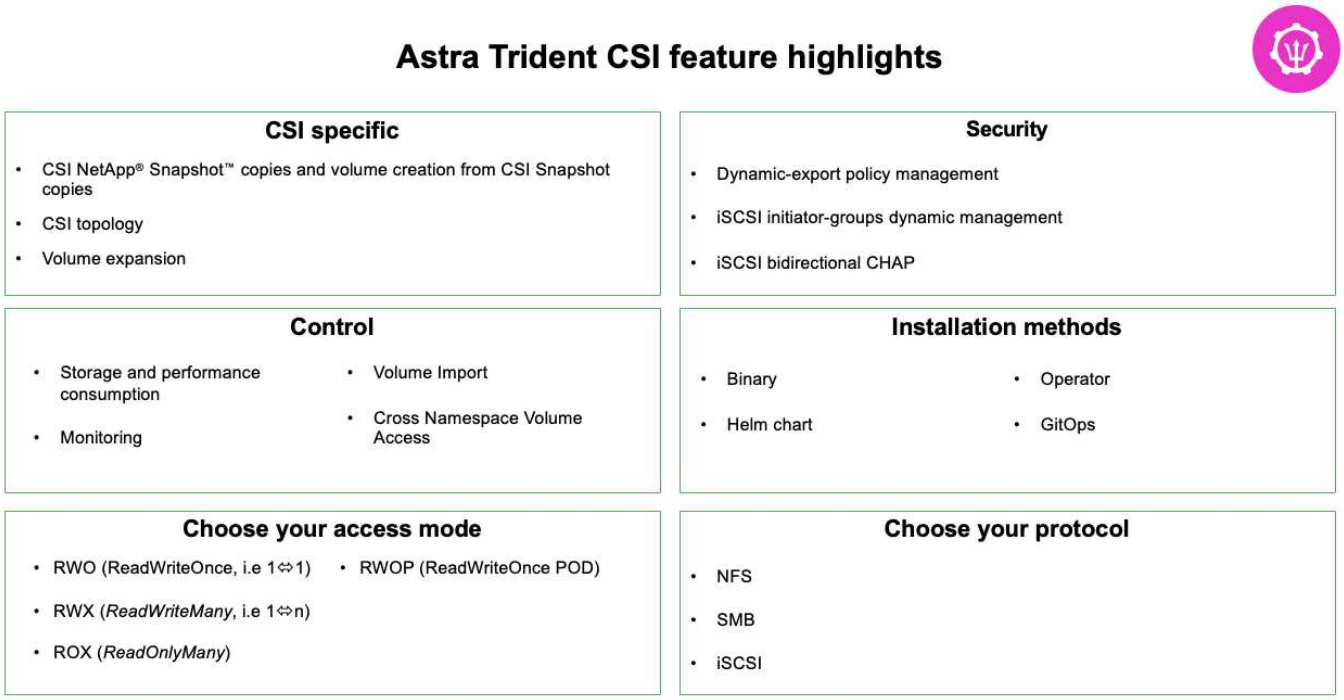
- Storage autogestita on-premise:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
  - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
  - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
  - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler



NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.



I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN) come storage persistente.

Proposte a valore delle soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

La maggior parte dei clienti non inizia a costruire ambienti basati su Kubernetes senza alcuna infrastruttura esistente. Forse si tratta di un negozio IT tradizionale che esegue la maggior parte delle applicazioni aziendali su macchine virtuali (ad esempio in ambienti VMware di grandi dimensioni). Quindi, iniziano a creare piccoli ambienti basati su

container per soddisfare le esigenze dei moderni team di sviluppo delle applicazioni. Queste iniziative di solito iniziano a poco e iniziano a diventare più pervasive man mano che i team imparano queste nuove tecnologie e competenze, e iniziano a riconoscere i numerosi benefici derivanti dall'adozione di queste tecnologie. La buona notizia per i clienti è che NetApp può soddisfare le esigenze di entrambi gli ambienti. Questo set di soluzioni per il multicloud ibrido con Red Hat OpenShift consentirà ai clienti NetApp di adottare tecnologie e servizi cloud moderni senza dover rivedere l'intera infrastruttura e organizzazione. Sia che le applicazioni e i dati dei clienti siano ospitati on-premise, nel cloud, eseguiti su macchine virtuali o su container, NetApp è in grado di fornire gestione, protezione, sicurezza e portabilità dei dati coerenti. Con queste nuove soluzioni, lo stesso valore offerto da NetApp in ambienti di data center on-premise per decenni sarà disponibile nell'intero orizzonte dei dati dell'azienda, senza richiedere investimenti significativi per il ritool, l'acquisizione di nuove competenze o la creazione di nuovi team. NetApp è in grado di aiutare i clienti a risolvere queste sfide aziendali indipendentemente dalla fase del loro percorso cloud.

Multi-cloud ibrido NetApp con Red Hat OpenShift:

- Offre ai clienti design e pratiche validati che dimostrano i modi migliori per gestire, proteggere, proteggere e migrare i dati e le applicazioni quando utilizzano Red Hat OpenShift con le soluzioni di storage basate su NetApp.
- Presentare le Best practice per i clienti che utilizzano Red Hat OpenShift con lo storage NetApp in ambienti VMware, infrastruttura bare metal o una combinazione di entrambi.
- Dimostra strategie e opzioni per ambienti sia on-premise che cloud, nonché per ambienti ibridi in cui vengono utilizzati entrambi.

Soluzioni supportate di NetApp Hybrid Multibloud per i carichi di lavoro dei container Red Hat OpenShift

La soluzione verifica e convalida la migrazione e la protezione centralizzata dei dati con la piattaforma container OpenShift, l'Advanced Cluster Manager (ACM) OpenShift, NetApp ONTAP, NetApp BlueXP e il centro di controllo NetApp Astra (ACC).

Per questa soluzione, i seguenti scenari sono testati e validati da NetApp. La soluzione è suddivisa in più scenari in base alle seguenti caratteristiche:

- on-premise
- cloud
  - Cluster OpenShift autogestiti e storage NetApp autogestiti
  - Cluster OpenShift gestiti dal provider e storage NetApp gestito dal provider

In futuro verranno sviluppate soluzioni e casi di utilizzo aggiuntivi.

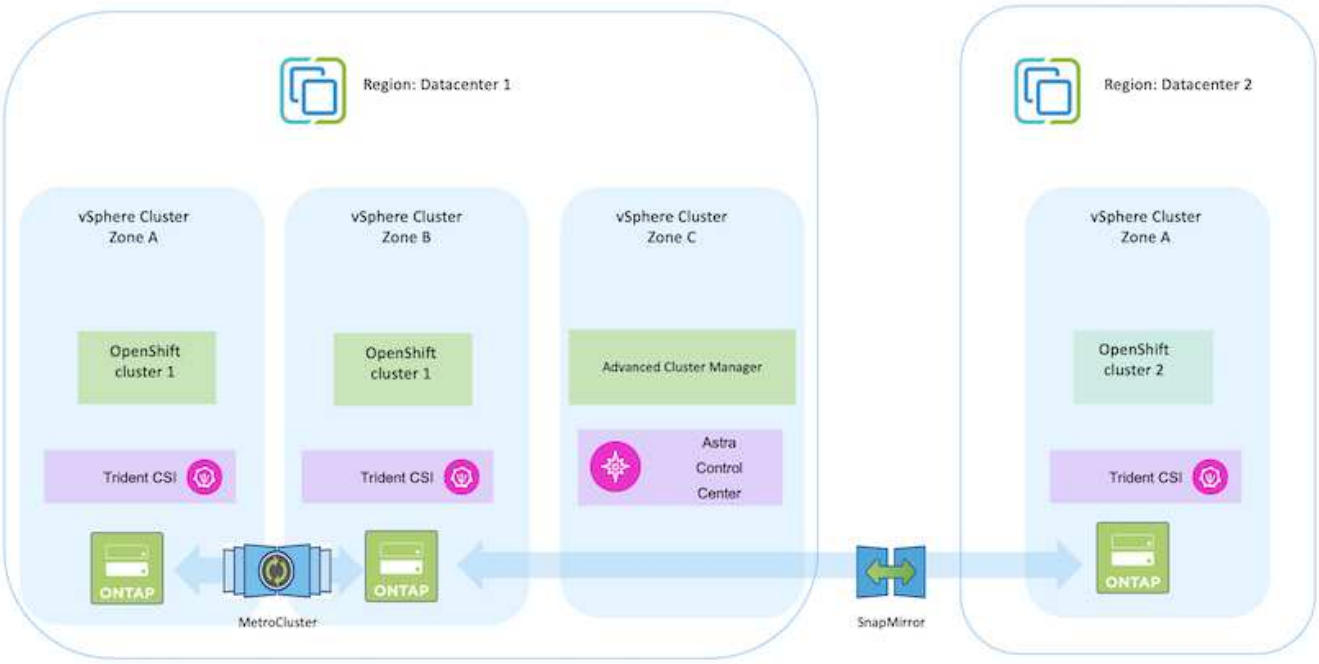
Scenario 1: Protezione dei dati e migrazione all'interno dell'ambiente on-premise con ACC

On-premise: Cluster OpenShift autogestiti e storage NetApp autogestiti

- Utilizzando ACC, è possibile creare copie Snapshot, backup e ripristini per la protezione dei dati.

- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.

Scenario 1

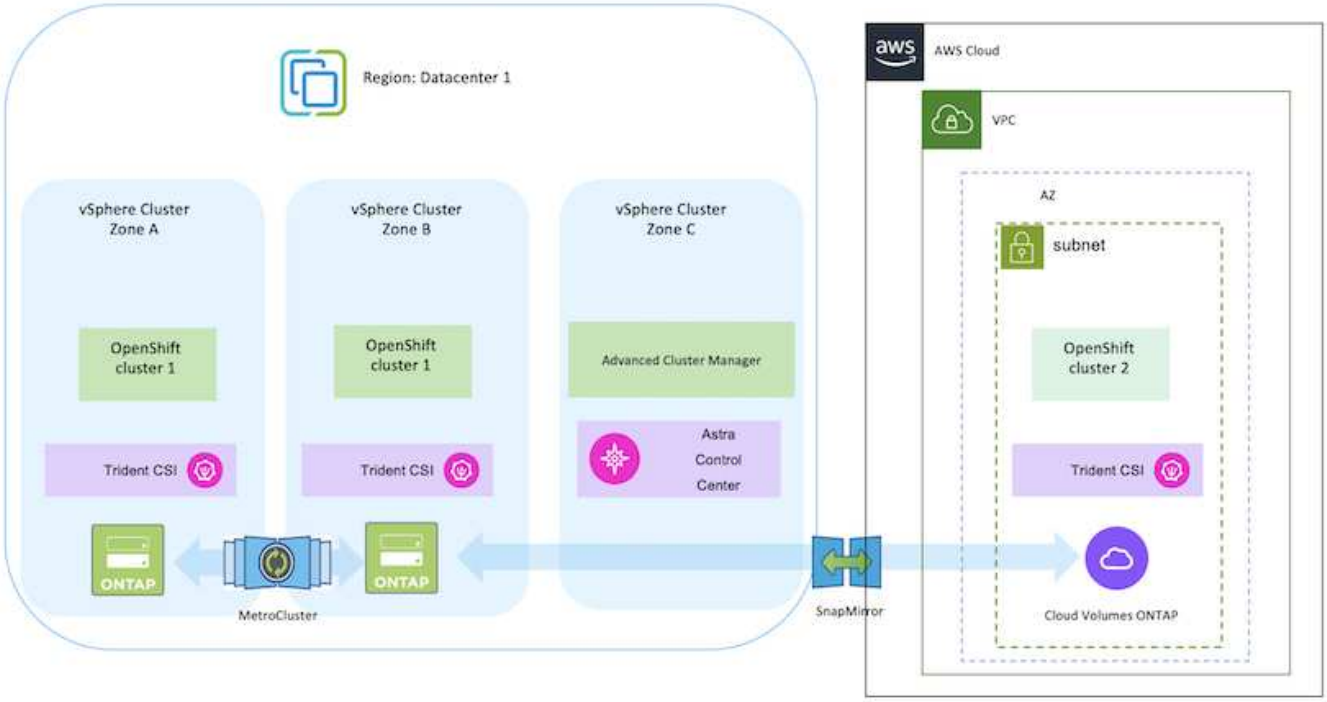


Scenario 2: Data Protection e migrazione dall'ambiente on-premise all'ambiente AWS con ACC

On-premise: Cluster OpenShift autogestiti e storage autogestiti AWS Cloud: Cluster OpenShift autogestiti e storage autogestiti

- Utilizzando ACC, eseguire backup e ripristini per la protezione dei dati.
- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.

Scenario 2

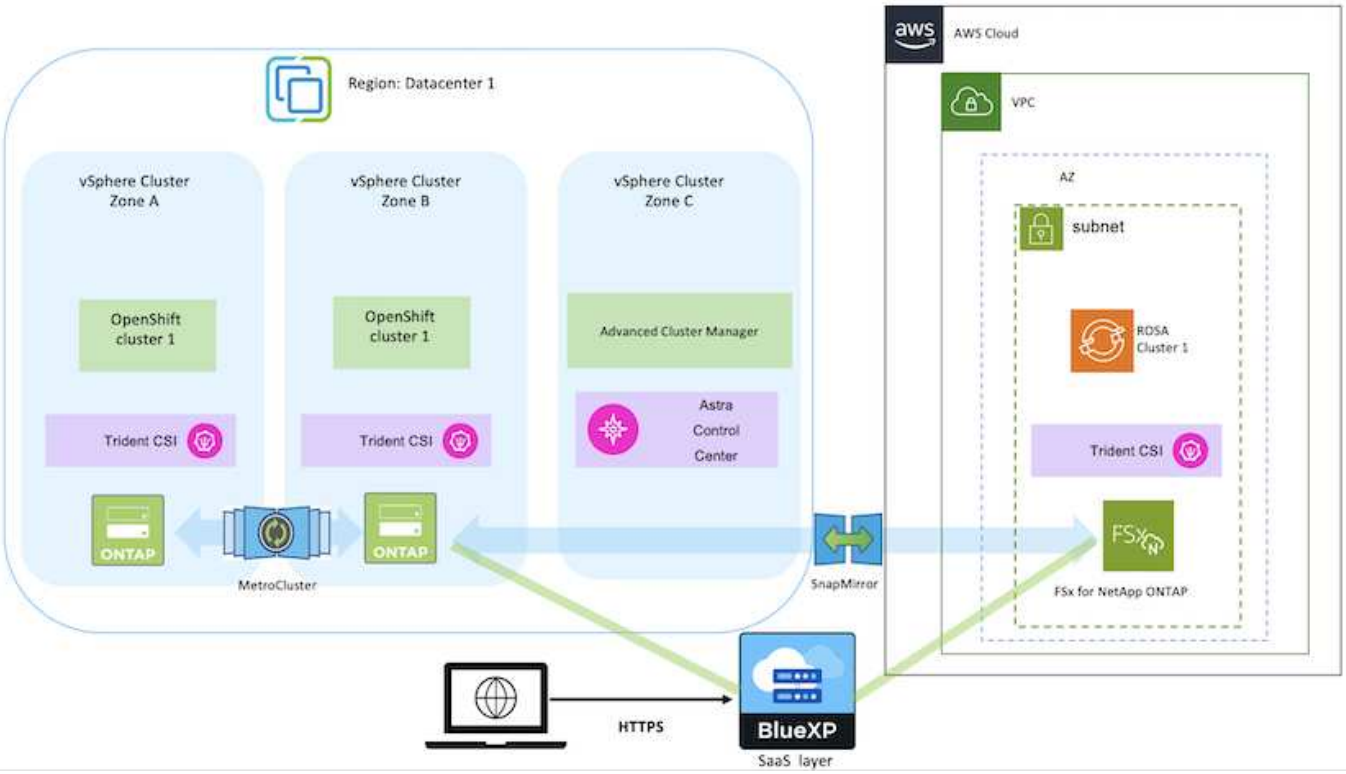


Scenario 3: Data Protection e migrazione dall'ambiente on-premise all'ambiente AWS

On-premise: Cluster OpenShift e storage autogestito AWS Cloud: Cluster OpenShift gestito dal provider (ROSA) e storage gestito dal provider (FSxN)

- Utilizzando BlueXP, eseguire la replica dei volumi persistenti (FSxN).
- Utilizzando OpenShift GitOps, ricreare i metadati dell'applicazione.

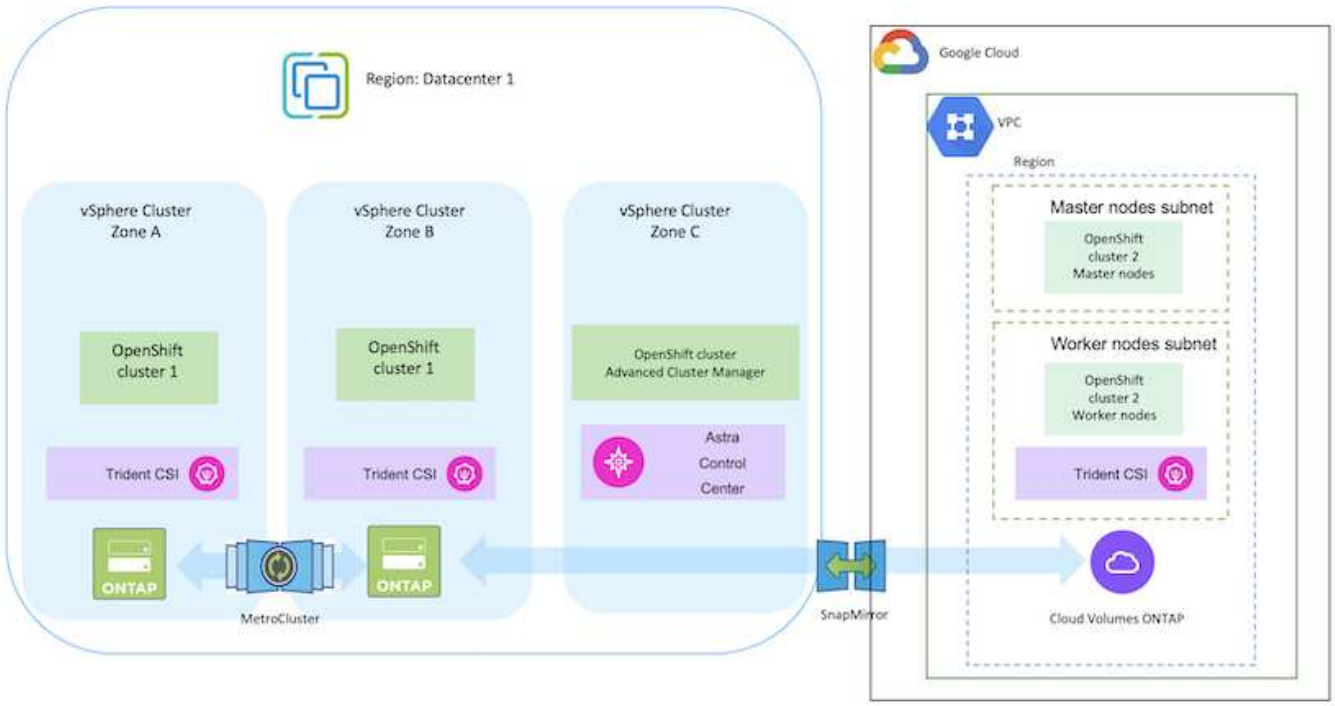
Scenario 3



Scenario 4: Protezione dei dati e migrazione dall'ambiente on-premise all'ambiente GCP tramite ACC

On-premise: Cluster OpenShift autogestito e storage autogestito
Google Cloud: Cluster OpenShift autogestito e storage autogestito

- Utilizzando ACC, eseguire backup e ripristini per la protezione dei dati.
- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.

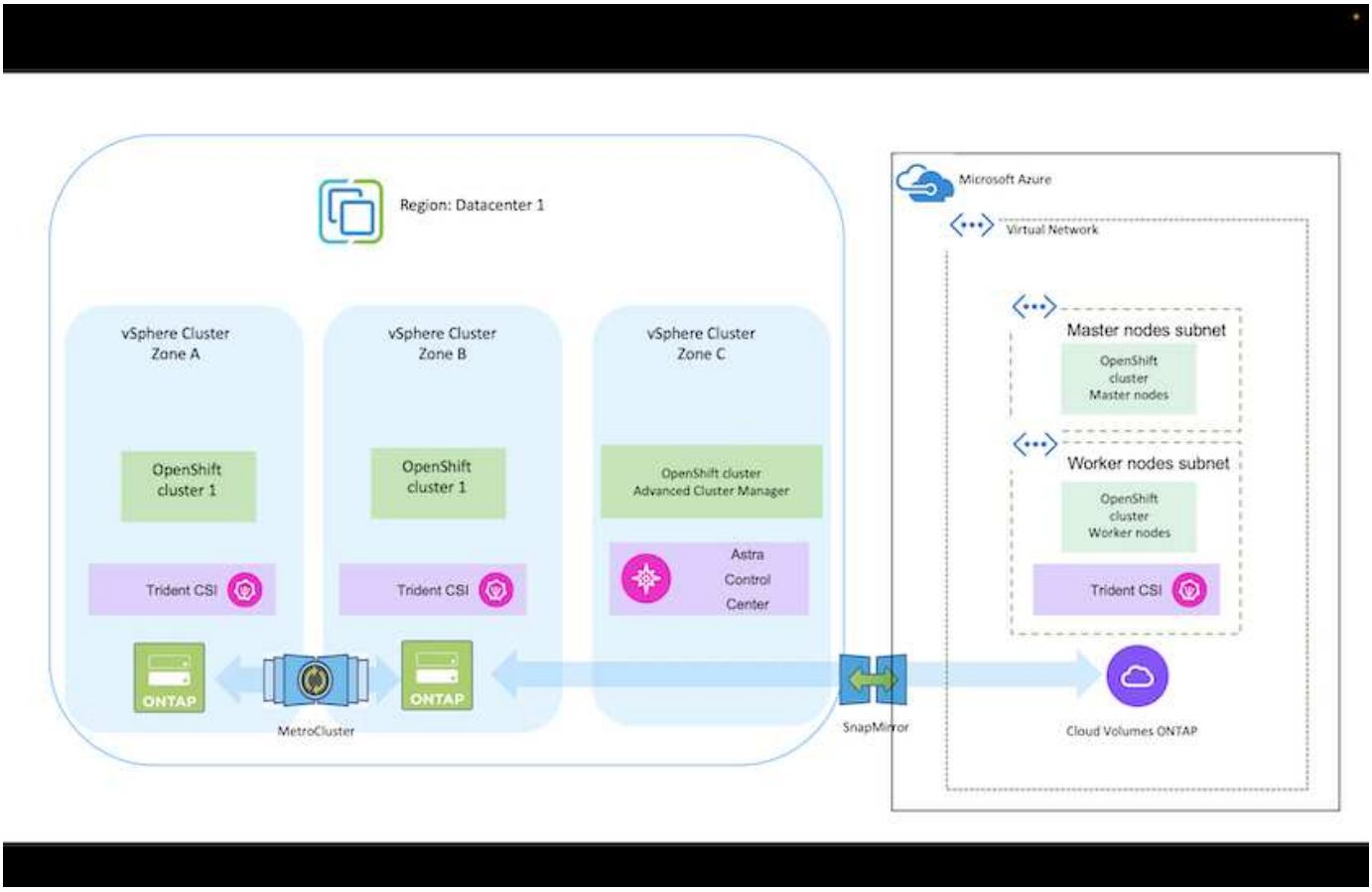


Per considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster, fare riferimento a. "qui".

Scenario 5: Protezione dei dati e migrazione dall'ambiente on-premise all'ambiente Azure con ACC

On-premise: Cluster OpenShift autogestito e storage autogestito
Azure Cloud: Cluster OpenShift autogestito e storage autogestito

- Utilizzando ACC, eseguire backup e ripristini per la protezione dei dati.
- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.



Per considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster, fare riferimento a. "qui".

Versioni dei vari componenti utilizzati nella convalida della soluzione

La soluzione testa e convalida la migrazione e la protezione centralizzata dei dati con la piattaforma container OpenShift, l'Advanced Cluster Manager OpenShift, NetApp ONTAP e il centro di controllo NetApp Astra.

Gli scenari 1, 2 e 3 della soluzione sono stati validati utilizzando le versioni indicate nella tabella seguente:

Componente	Versione
VMware	VSphere Client versione 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Cluster hub	OpenShift 4.11.34

Clusters di origine e destinazione	OpenShift 4.12.9 on-premise e in AWS
NetApp Astra Trident	Trident Server e Client 23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1
AWS FSX per NetApp ONTAP	AZ. Singola

Lo scenario 4 della soluzione è stato validato utilizzando le versioni indicate nella tabella seguente:

Componente	Versione
VMware	VSphere Client versione 8.0.2.00000 VMware ESXi, 8,0.2, 22380479
Cluster hub	OpenShift 4.13.13
Clusters di origine e destinazione	OpenShift 4.13.12 On-premise e in Google Cloud
NetApp Astra Trident	Trident Server e Client 23.07.0
NetApp Astra Control Center	ACC 23.07.0-25
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	AZ singolo, nodo singolo, 9.14.0

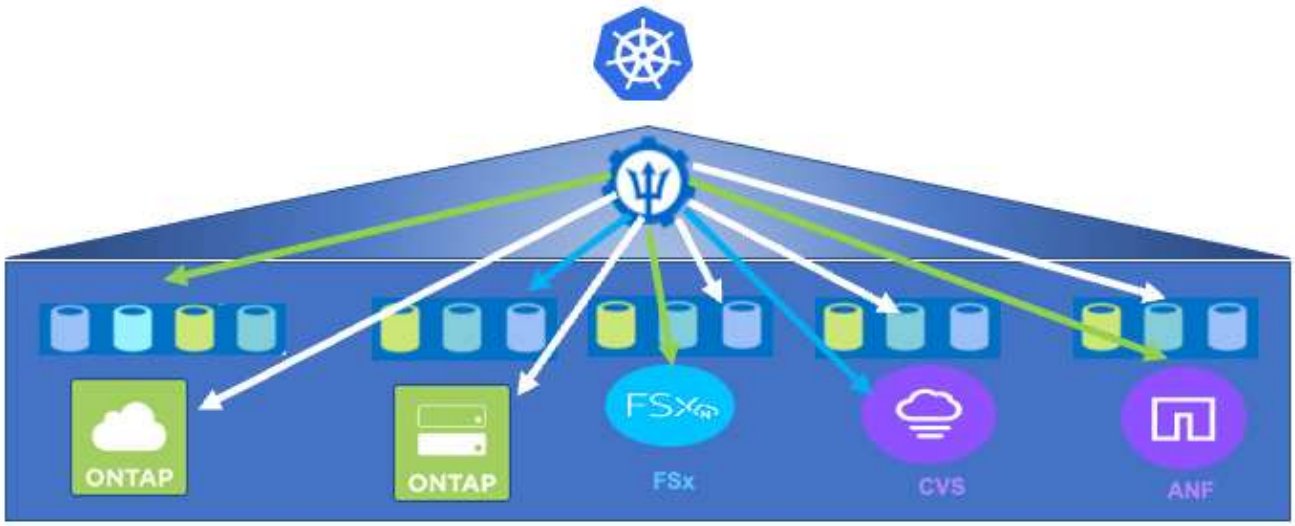
Lo scenario 5 della soluzione è stato validato utilizzando le versioni indicate nella tabella seguente:

Componente	Versione
VMware	VSphere Client versione 8.0.2.00000 VMware ESXi, 8,0.2, 22380479
Clusters di origine e destinazione	OpenShift 4.13.25 On-premise e in Azure
NetApp Astra Trident	Trident Server e Client e Astra Control Provisioner 23.10.0
NetApp Astra Control Center	ACC 23,10
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	AZ singolo, nodo singolo, 9.14.0

Integrazioni di storage NetApp supportate con Red Hat Open Shift Containers

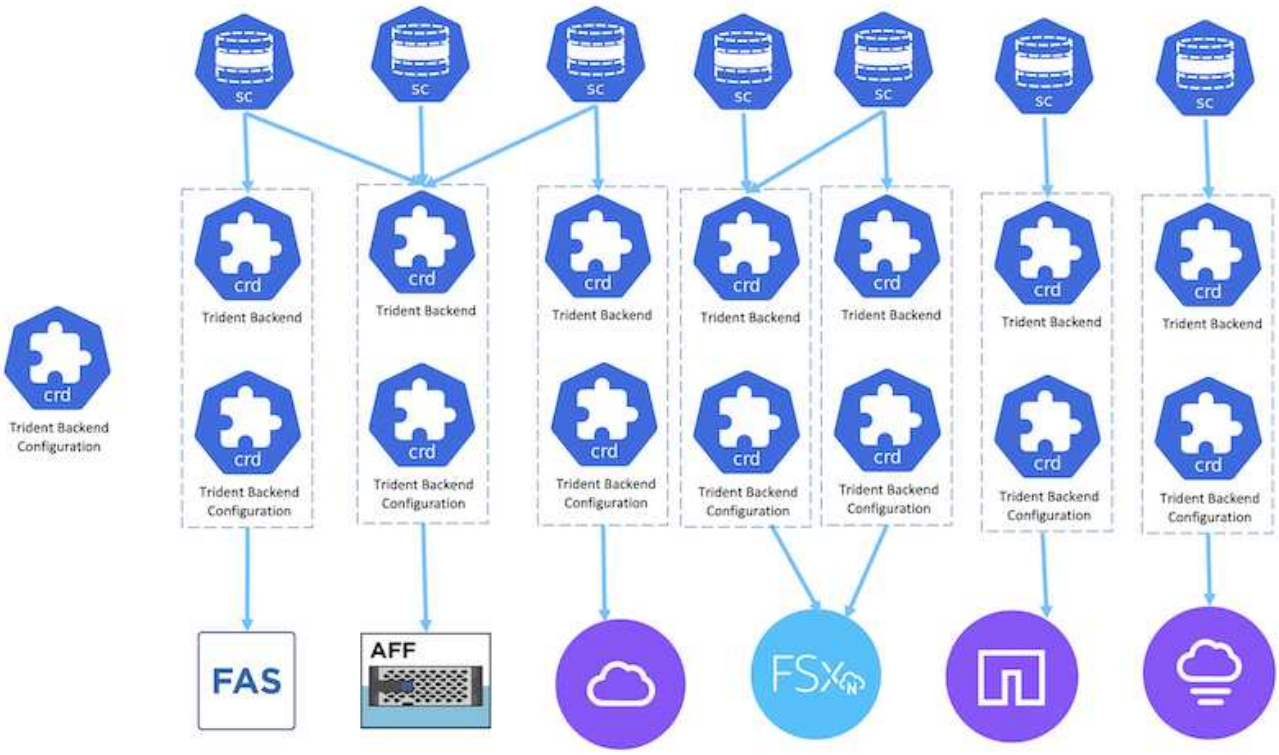
Sia che i container Red Hat Open Shift siano in esecuzione su VMware o negli hyperscaler, NetApp Astra Trident può essere utilizzato come provider CSI per i vari tipi di storage NetApp di back-end supportati.

Il seguente diagramma illustra i vari storage NetApp di back-end che possono essere integrati con i cluster OpenShift utilizzando NetApp Astra Trident.

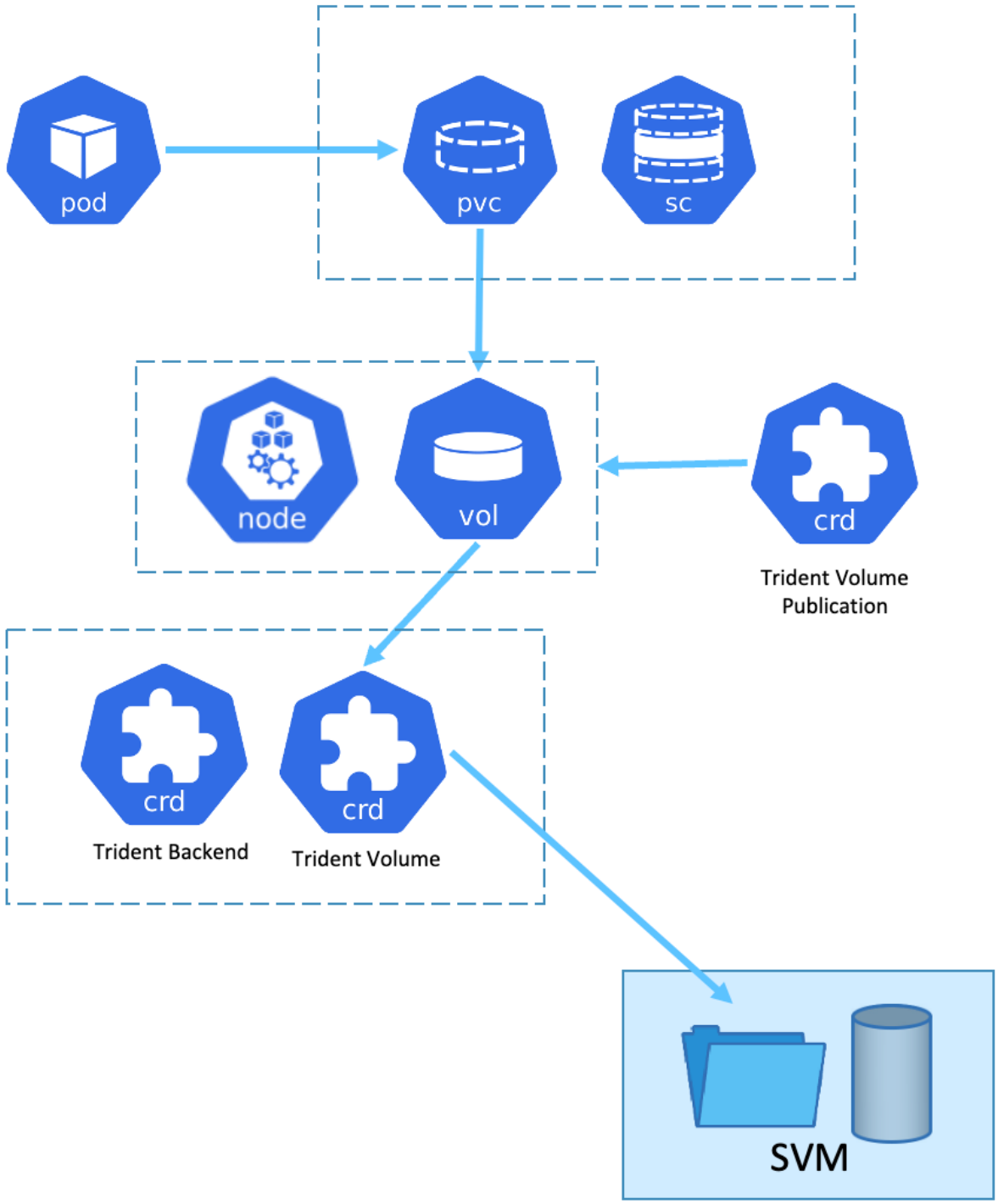


La macchina virtuale per lo storage ONTAP (SVM) offre una multi-tenancy sicura. Un singolo cluster OpenShift può connettersi a una singola SVM o a più SVM o persino a più cluster ONTAP. La classe di storage filtra lo storage back-end in base ai parametri o alle etichette. Gli amministratori dello storage definiscono i parametri per la connessione al sistema di storage utilizzando la configurazione backend trident. Una volta stabilita la connessione, crea il backend trident e popola le informazioni che la classe di storage può filtrare.

Di seguito viene illustrata la relazione tra lo storageclass e il backend.



Il proprietario dell'applicazione richiede un volume persistente utilizzando la classe di storage. La classe di storage filtra lo storage back-end. Di seguito viene illustrata la relazione tra il pod e lo storage back-end.



Opzioni CSI (Container Storage Interface)

Negli ambienti vSphere, i clienti possono scegliere il driver VMware CSI e/o Astra Trident CSI da integrare con ONTAP. Con VMware CSI, i volumi persistenti vengono consumati come dischi SCSI locali, mentre con Trident viene consumato con la rete. Poiché VMware CSI non supporta le modalità di accesso RWX con ONTAP, le applicazioni devono utilizzare Trident CSI se è richiesta la modalità RWX. Con le implementazioni basate su FC, VMware CSI è la soluzione preferita e SnapMirror Business Continuity (SMBC) offre disponibilità elevata a livello di zona.

Supporto di VMware CSI

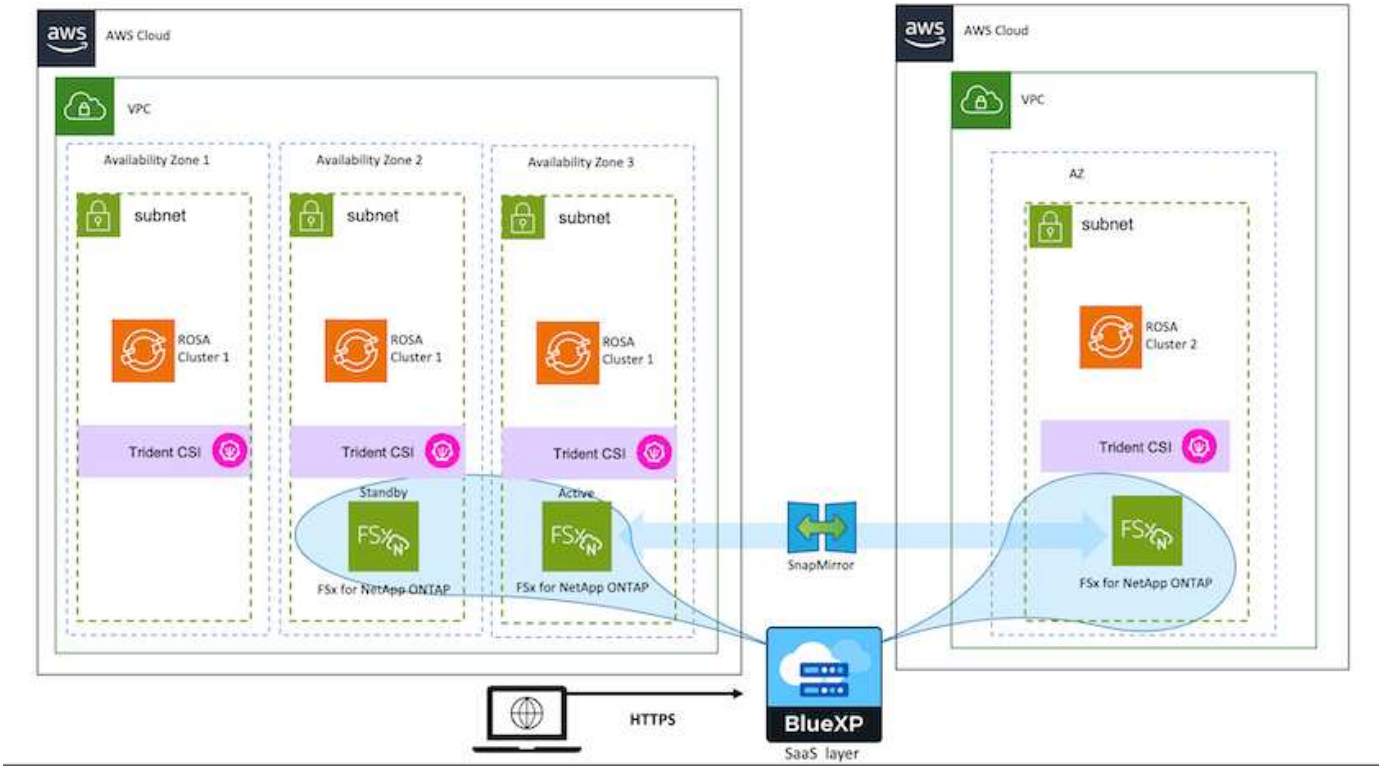
- Datastore basati su core block (FC, FCoE, iSCSI, NVMeoF)
- Archivi dati basati su file di base (NFS v3, v4)
- Datastore vVol (blocco e file)

Trident ha i seguenti driver per supportare ONTAP

- ontap-san (volume dedicato)
- ontap-san-economy (volume condiviso)
- ontap-nas (volume dedicato)
- ontap-nas-economy (volume condiviso)
- ontap-nas-flexgroup (volume dedicato su larga scala)

Per VMware CSI e Astra Trident CSI, ONTAP supporta nconnect, trunking di sessione, kerberos, ecc. per NFS e multipathing, autenticazione chap, ecc. per i protocolli a blocchi.

In AWS, FSX per NetApp ONTAP (FSxN) può essere implementato in una singola zona di disponibilità (AZ) o in più AZ. Per i carichi di lavoro di produzione che richiedono alta disponibilità, multi-AZ offre tolleranza di errore a livello zonale e una cache di lettura NVMe migliore rispetto a AZ singolo. Per ulteriori informazioni, consultare "Linee guida per le performance di AWS".
Per risparmiare sui costi del sito di disaster recovery, è possibile utilizzare un singolo ONTAP AZ FSX.



Per il numero di SVM supportati da FSX ONTAP, fare riferimento a. "Gestione della macchina virtuale per lo storage FSX ONTAP"

Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

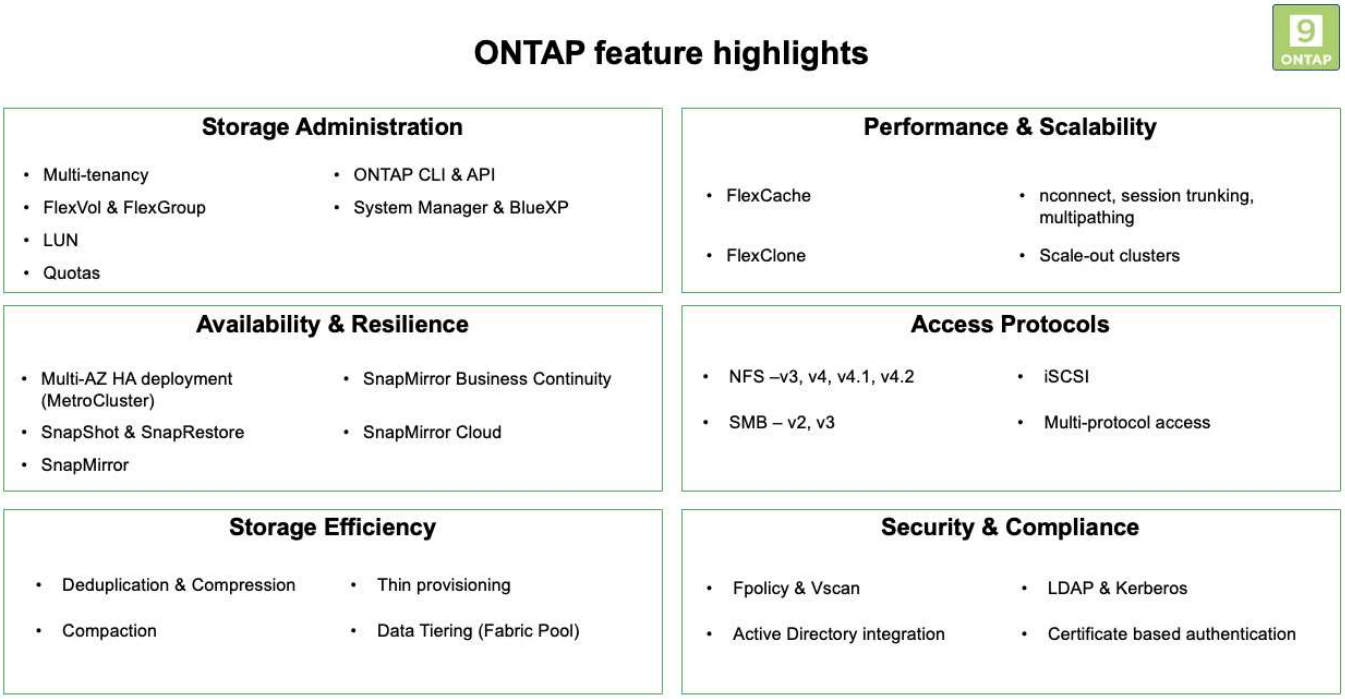
Panoramica

NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati, affidabilità e flessibilità per le implementazioni di container e Kubernetes.

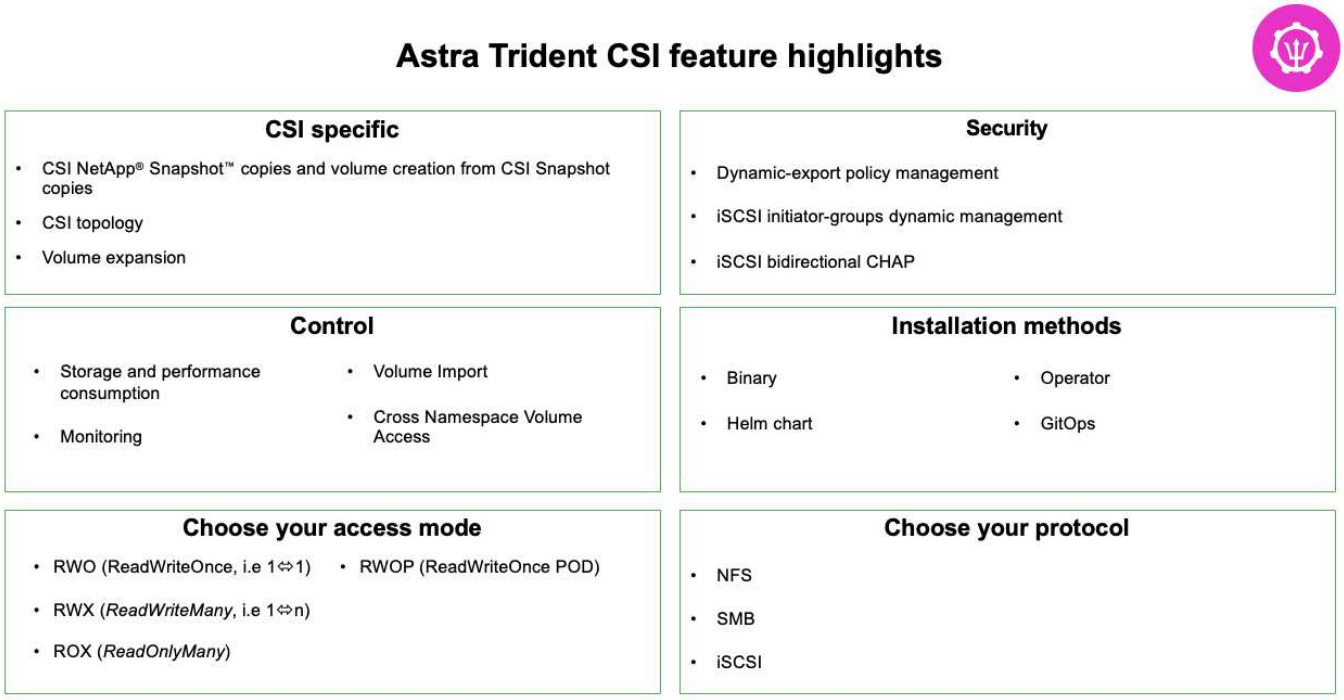
- Storage autogestita on-premise:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
  - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
  - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
  - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler



NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.



I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN)

come storage persistente.

Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift su VMware

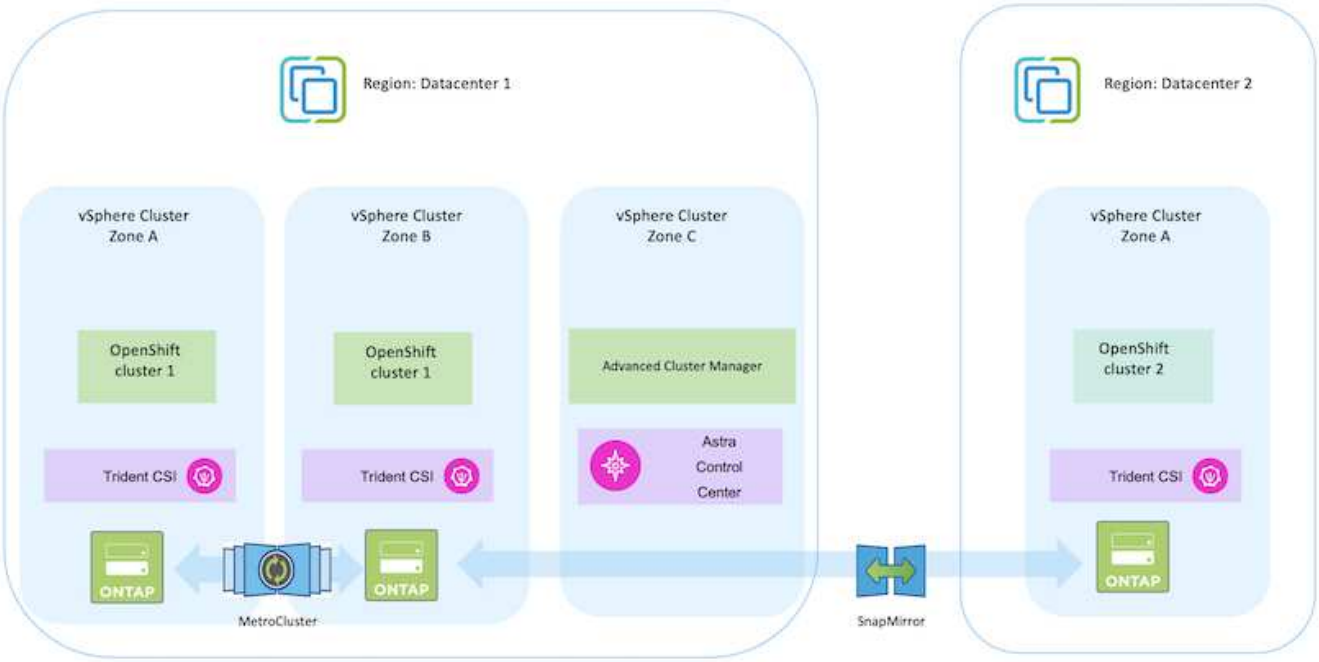
Se i clienti hanno la necessità di eseguire le loro moderne applicazioni containerizzate su un'infrastruttura nei propri data center privati, possono farlo. Devono pianificare e implementare la piattaforma container Red Hat OpenShift (OCP) per un ambiente pronto per la produzione di successo per l'implementazione dei carichi di lavoro dei container. I cluster OCP possono essere implementati su VMware o bare metal.

Lo storage NetApp ONTAP offre protezione dei dati, affidabilità e flessibilità per le implementazioni di container. Astra Trident funge da provider di storage dinamico per consumare storage ONTAP persistente per le applicazioni stateful dei clienti. Astra Control Center può essere utilizzato per orchestrare i numerosi requisiti di gestione dei dati delle applicazioni stateful come protezione dei dati, migrazione e business continuity.

Con VMware vSphere, i tool NetApp ONTAP forniscono un plug-in vCenter che può essere utilizzato per il provisioning dei datastore. Applica i tag e usali con OpenShift per memorizzare la configurazione del nodo e i dati. Lo storage basato su NVMe offre latenza inferiore e performance elevate.

Questa soluzione fornisce dettagli sulla protezione dei dati e sulla migrazione dei carichi di lavoro dei container utilizzando Astra Control Center. Per questa soluzione, i carichi di lavoro dei container vengono implementati nei cluster Red Hat OpenShift su vSphere all'interno dell'ambiente on-premise. NOTA: In futuro forniremo una soluzione per i carichi di lavoro container sui cluster OpenShift su bare metal.

Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift con Astra Control Center



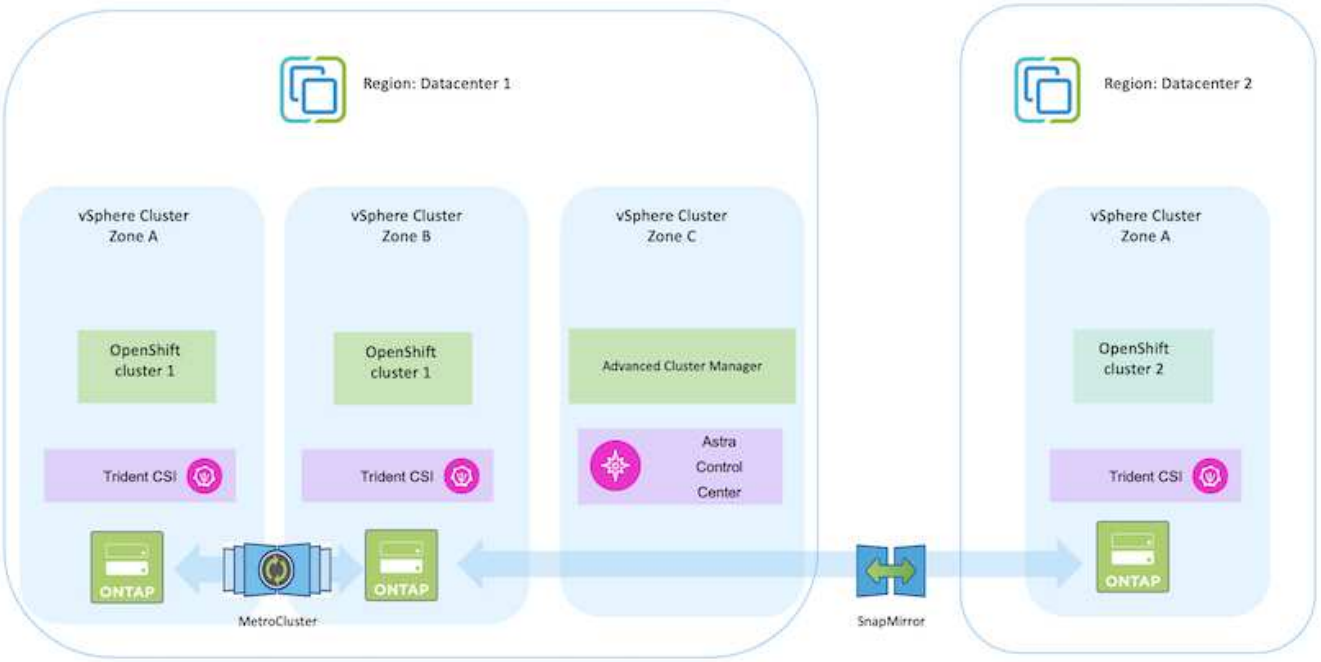
Implementare e configurare la piattaforma container Red Hat OpenShift su VMware

In questa sezione viene descritto un workflow di alto livello che illustra come configurare

e gestire i cluster OpenShift e gestire le applicazioni stateful su di essi. Mostra l'utilizzo degli storage array NetApp ONTAP con l'aiuto di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Di seguito è riportato un diagramma che illustra i cluster implementati su VMware in un data center.



Il processo di installazione può essere suddiviso nei seguenti passaggi:

Implementare e configurare una macchina virtuale CentOS

- Viene implementato nell'ambiente VMware vSphere.
- Questa macchina virtuale viene utilizzata per l'implementazione di alcuni componenti come NetApp Astra Trident e NetApp Astra Control Center per la soluzione.
- Un utente root viene configurato su questa macchina virtuale durante l'installazione.

Implementare e configurare un cluster OpenShift Container Platform su VMware vSphere (Hub Cluster)

Fare riferimento alle istruzioni del "Implementazione assistita" Metodo per implementare un cluster OCP.

Tenere presente quanto segue: - Creare una chiave pubblica e privata ssh da fornire all'installatore. Queste chiavi verranno utilizzate per accedere ai nodi master e worker, se necessario. - Scaricare il programma di installazione dal programma di installazione assistito. Questo programma viene utilizzato per avviare le macchine virtuali create nell'ambiente VMware vSphere per i nodi master e worker. Le macchine virtuali devono avere i requisiti minimi di CPU, memoria e disco rigido. (Fare riferimento ai comandi di creazione della macchina virtuale su "questo" Per i nodi master e worker che forniscono queste informazioni) - diskUID deve essere abilitato su tutte le macchine virtuali. - Creare un minimo di 3 nodi per master e 3 nodi per worker. Una volta rilevati dal programma di installazione, attivare il pulsante di attivazione/disattivazione dell'integrazione VMware vSphere.

Installare Advanced Cluster Management sul cluster Hub

Viene installato utilizzando Advanced Cluster Management Operator sul cluster Hub. Fare riferimento alle istruzioni "qui".

Installare un registro Red Hat Quay interno sul cluster Hub.

- Per inviare l'immagine Astra è necessario un registro interno. Un registro interno Quay viene installato utilizzando l'operatore nel cluster Hub.
- Fare riferimento alle istruzioni "qui"

Installare due cluster OCP aggiuntivi (origine e destinazione)

- I cluster aggiuntivi possono essere implementati utilizzando ACM sul cluster Hub.
- Fare riferimento alle istruzioni "qui".

Configurare lo storage NetApp ONTAP

- Installare un cluster ONTAP con connettività alle VM OCP nell'ambiente VMware.
- Creare una SVM.
- Configurare i dati NAS per accedere allo storage in SVM.

Installare NetApp Trident sui cluster OCP

- Installare NetApp Trident su tutti e tre i cluster: Hub, origine e destinazione
- Fare riferimento alle istruzioni "qui".
- Creare un backend di storage per ontap-nas .
- Creare una classe di storage per ontap-nas.
- Fare riferimento alle istruzioni "qui".

Installare NetApp Astra Control Center

- NetApp Astra Control Center viene installato utilizzando Astra Operator sul cluster Hub.
- Fare riferimento alle istruzioni "qui".

Punti da ricordare: * Scarica l'immagine di NetApp Astra Control Center dal sito di supporto. * Inserire l'immagine in un registro interno. * Fare riferimento alle istruzioni qui.

Implementare un'applicazione sul cluster di origine

Utilizza OpenShift GitOps per implementare un'applicazione. (es. Postgres, Ghost)

Aggiungere i cluster di origine e destinazione in Astra Control Center.

Dopo aver aggiunto un cluster alla gestione di Astra Control, è possibile installare le applicazioni sul cluster (all'esterno di Astra Control) e quindi passare alla pagina delle applicazioni in Astra Control per definire le applicazioni e le relative risorse. Fare riferimento a. "Inizia a gestire le app di Astra Control Center".

Il passaggio successivo consiste nell'utilizzare Astra Control Center per la protezione dei dati e la migrazione dei dati dal cluster di origine a quello di destinazione.

Protezione dei dati con Astra

Questa pagina mostra le opzioni di protezione dei dati per le applicazioni basate su container Red Hat OpenShift eseguite su VMware vSphere utilizzando Astra Control Center (ACC).

Mentre gli utenti intraprendono il percorso di modernizzazione delle proprie applicazioni con Red Hat OpenShift, è necessario adottare una strategia di protezione dei dati per proteggerli da cancellazioni accidentali o altri errori umani. Spesso, per proteggere i propri dati da un diaster, è necessaria anche una strategia di protezione a scopo normativo o di compliance.

I requisiti di protezione dei dati variano dal ritorno a una copia point-in-time al failover automatico a un dominio di errore diverso senza alcun intervento umano. Molti clienti scelgono ONTAP come piattaforma di storage preferita per le loro applicazioni Kubernetes per le sue ricche funzionalità come multi-tenancy, multi-protocollo, offerte di capacità e performance elevate, replica e caching per ubicazioni multi-sito, sicurezza e flessibilità.

La protezione dei dati in ONTAP può essere ottenuta utilizzando ad-hoc o policy controllate - **Snapshot** -

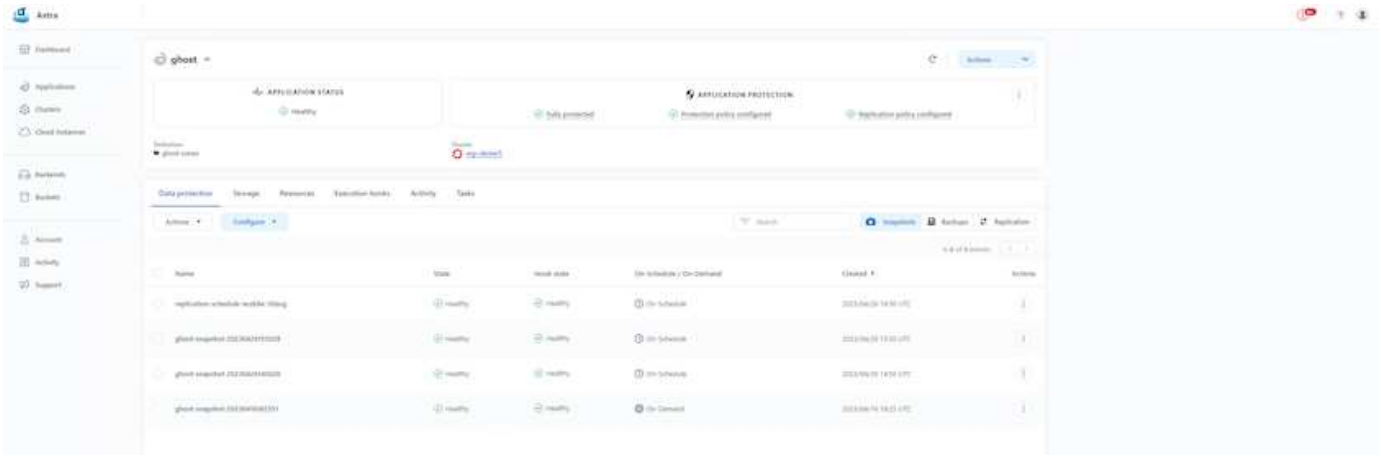
backup e ripristino

Sia le copie Snapshot che i backup proteggono i seguenti tipi di dati: - **I metadati dell'applicazione che rappresentano lo stato dell'applicazione - eventuali volumi di dati persistenti associati all'applicazione - eventuali artefatti delle risorse appartenenti all'applicazione**

Snapshot con ACC

È possibile acquisire una copia point-in-time dei dati utilizzando Snapshot con ACC. La policy di protezione definisce il numero di copie Snapshot da conservare. L'opzione di pianificazione minima disponibile è oraria. Le copie Snapshot manuali e on-demand possono essere eseguite in qualsiasi momento e a intervalli più brevi rispetto alle copie Snapshot pianificate. Le copie Snapshot vengono memorizzate sullo stesso volume sottoposto a provisioning dell'applicazione.

Configurazione di Snapshot con ACC

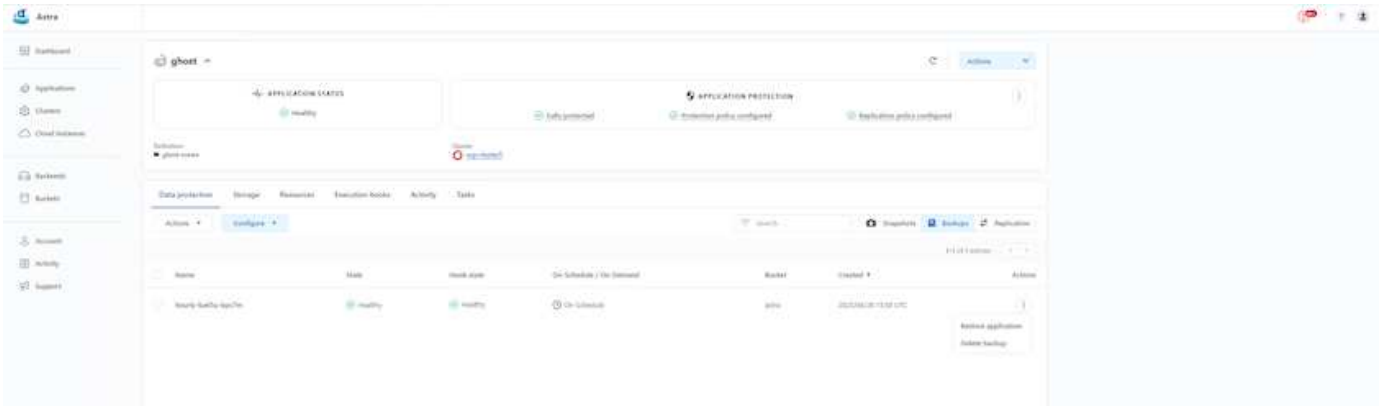


Backup e ripristino con ACC

Un backup si basa su un'istantanea. ACC può eseguire copie Snapshot utilizzando CSI ed eseguire il backup utilizzando la copia Snapshot point-in-time. Il backup viene memorizzato in un archivio di oggetti esterno (qualsiasi compatibile con s3, incluso ONTAP S3, in una posizione diversa). È possibile configurare i criteri di protezione per i backup pianificati e il numero di versioni di backup da conservare. L'RPO minimo è di un'ora.

Ripristino di un'applicazione da un backup mediante ACC

ACC ripristina l'applicazione dal bucket S3 in cui sono memorizzati i backup.



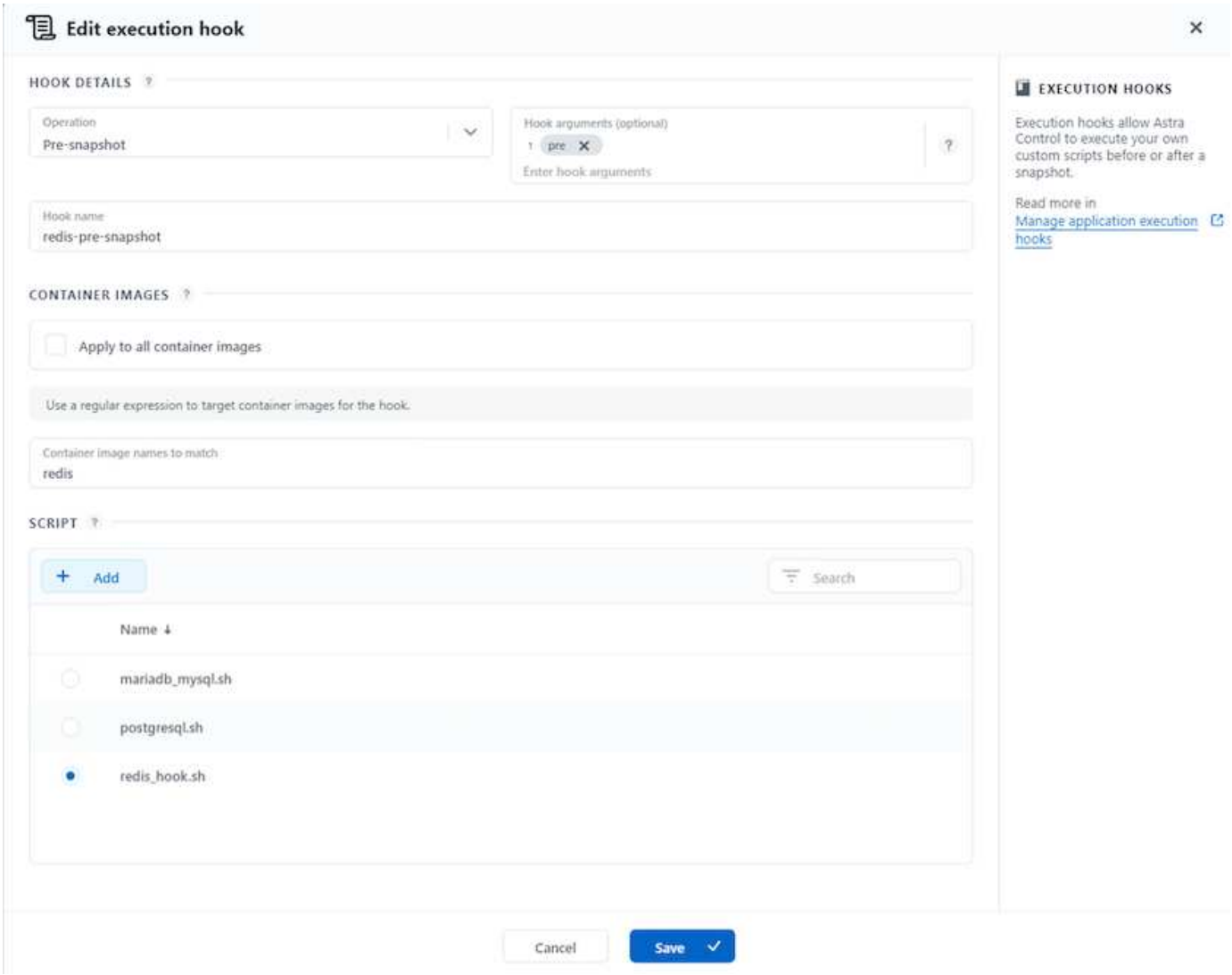
Hook di esecuzione specifici dell'applicazione

Inoltre, è possibile configurare gli hook di esecuzione per l'esecuzione in combinazione con un'operazione di protezione dei dati di un'applicazione gestita. Anche se sono disponibili funzionalità di protezione dei dati a livello di array di storage, spesso sono necessari ulteriori passaggi per rendere coerenti backup e ripristini. I passaggi aggiuntivi specifici dell'applicazione potrebbero essere: - Prima o dopo la creazione di una copia Snapshot. - prima o dopo la creazione di un backup. - Dopo il ripristino da una copia Snapshot o da un backup.

Astra Control può eseguire questi passaggi specifici dell'applicazione codificati come script personalizzati chiamati uncini di esecuzione.

"Progetto NetApp Verda GitHub" fornisce hook di esecuzione per le applicazioni native del cloud più diffuse per rendere la protezione delle applicazioni semplice, robusta e facile da orchestrare. Se si dispone di informazioni sufficienti per un'applicazione non presente nel repository, è possibile contribuire al progetto.

Esempio di gancio di esecuzione per pre-Snapshot di un'applicazione redis.



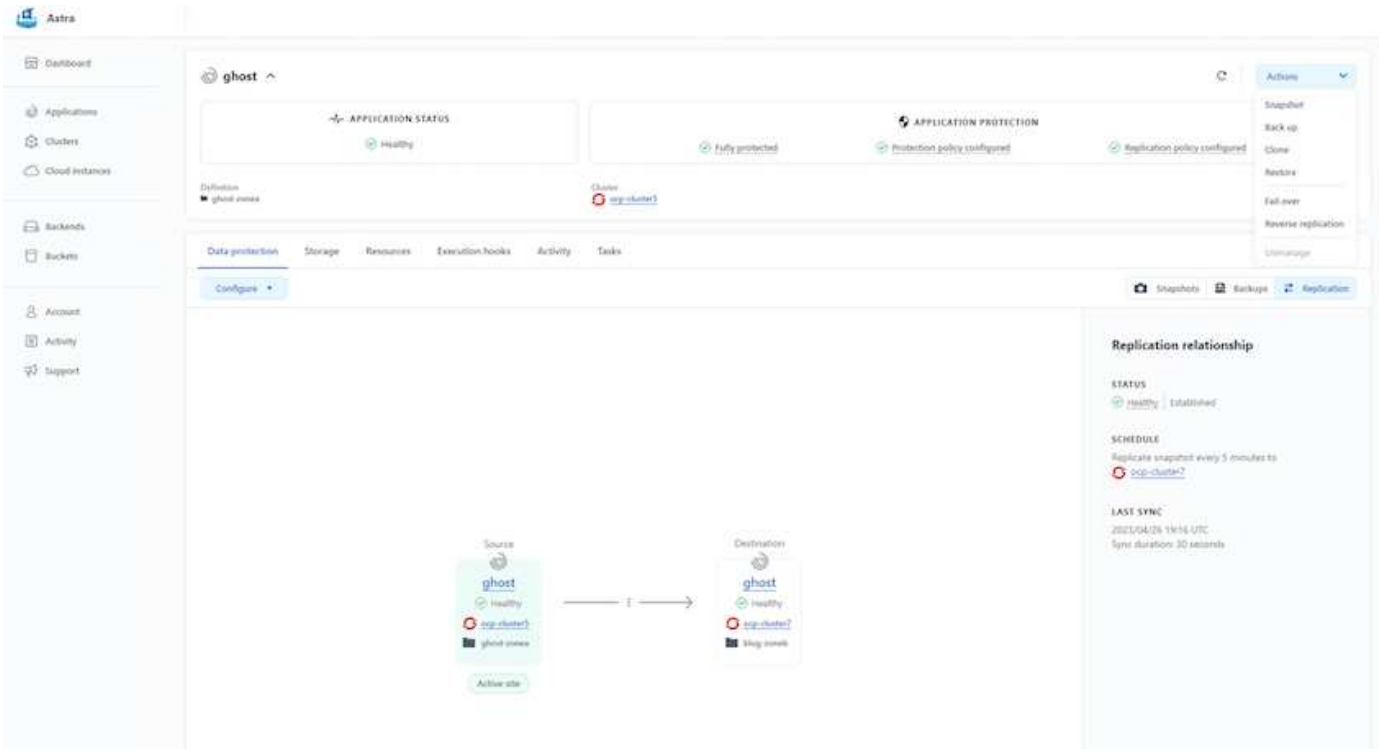
Replica con ACC

Per la protezione regionale o per una soluzione RPO e RTO bassa, un'applicazione può essere replicata in un'altra istanza di Kubernetes in esecuzione in un sito diverso, preferibilmente in un'altra regione. ACC utilizza SnapMirror asincrono ONTAP con RPO in soli 5 minuti. La replica viene eseguita replicando in ONTAP, quindi un failover crea le risorse Kubernetes nel cluster di destinazione.

Tenere presente che la replica è diversa dal backup e ripristino, dove il backup viene eseguito in S3 e il ripristino viene eseguito da S3. Fare riferimento al xref:./rhhc/ here per ulteriori dettagli sulle differenze tra i due tipi di protezione dei dati.

Fare riferimento a. "qui" Per le istruzioni di installazione di SnapMirror.

SnapMirror con ACC



i driver di storage san-economy e nas-economy non supportano la funzione di replica. Fare riferimento a. "qui" per ulteriori dettagli.

Video dimostrativo:

"Video dimostrativo del disaster recovery con Astra Control Center"

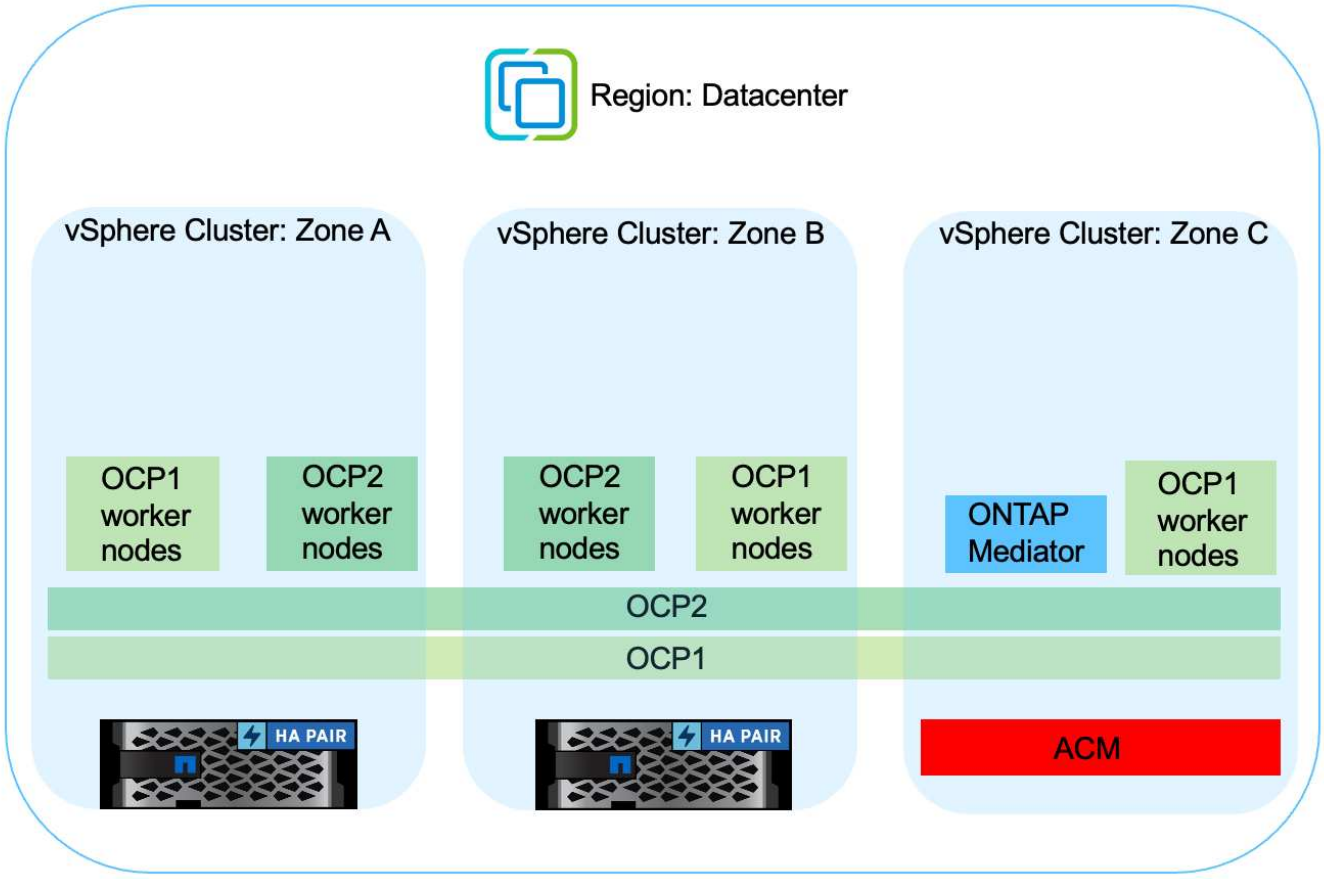
Data Protection con Astra Control Center

Continuità del business con MetroCluster

La maggior parte della nostra piattaforma hardware per ONTAP dispone di funzionalità ad alta disponibilità per la protezione dai guasti dei dispositivi, evitando la necessità di eseguire il disaster recovery. Tuttavia, per proteggere da incendi o altri disastri e continuare il business con un RPO zero e un RTO basso, spesso viene utilizzata una soluzione MetroCluster.

I clienti che attualmente dispongono di un sistema ONTAP possono estendere a MetroCluster aggiungendo sistemi ONTAP supportati entro i limiti di distanza per fornire il disaster recovery a livello di zona. Astra Trident, CSI (Container Storage Interface) supporta NetApp ONTAP, inclusa la configurazione MetroCluster e altre opzioni come Cloud Volumes ONTAP, Azure NetApp Files, AWS FSX per NetApp ONTAP, ecc. Astra Trident offre cinque opzioni di driver di storage per ONTAP, tutte supportate per la configurazione MetroCluster. Fare riferimento a. "qui" Per ulteriori informazioni sui driver di storage ONTAP supportati da Astra Trident.

La soluzione MetroCluster richiede un'estensione di rete Layer 2 o la capacità di accedere allo stesso indirizzo di rete da entrambi i domini di errore. Una volta eseguita la configurazione MetroCluster, la soluzione è trasparente per i proprietari delle applicazioni, in quanto tutti i volumi nella svm MetroCluster sono protetti e ottengono i benefici di SyncMirror (zero RPO).



Per la configurazione back-end Trident (TBC), non specificare dataLIF e SVM quando si utilizza la configurazione MetroCluster. Specificare l'IP di gestione SVM per la gestione LIF e utilizzare le credenziali del ruolo vsadmin.

Sono disponibili dettagli sulle funzioni di protezione dei dati di Astra Control Center "qui"

Migrazione dei dati con Astra Control Center

Questa pagina mostra le opzioni di migrazione dei dati per i carichi di lavoro container sui cluster Red Hat OpenShift con Astra Control Center (ACC).

Le applicazioni Kubernetes spesso devono essere spostate da un ambiente all'altro. Per migrare un'applicazione insieme ai suoi dati persistenti, è possibile utilizzare NetApp ACC.

Migrazione dei dati tra diversi ambienti Kubernetes

ACC supporta diversi tipi di Kubernetes, tra cui Google anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Kubernetes upstream, ecc. Per ulteriori dettagli, fare riferimento a. "qui".

Per migrare l'applicazione da un cluster a un altro, è possibile utilizzare una delle seguenti funzionalità di ACC:

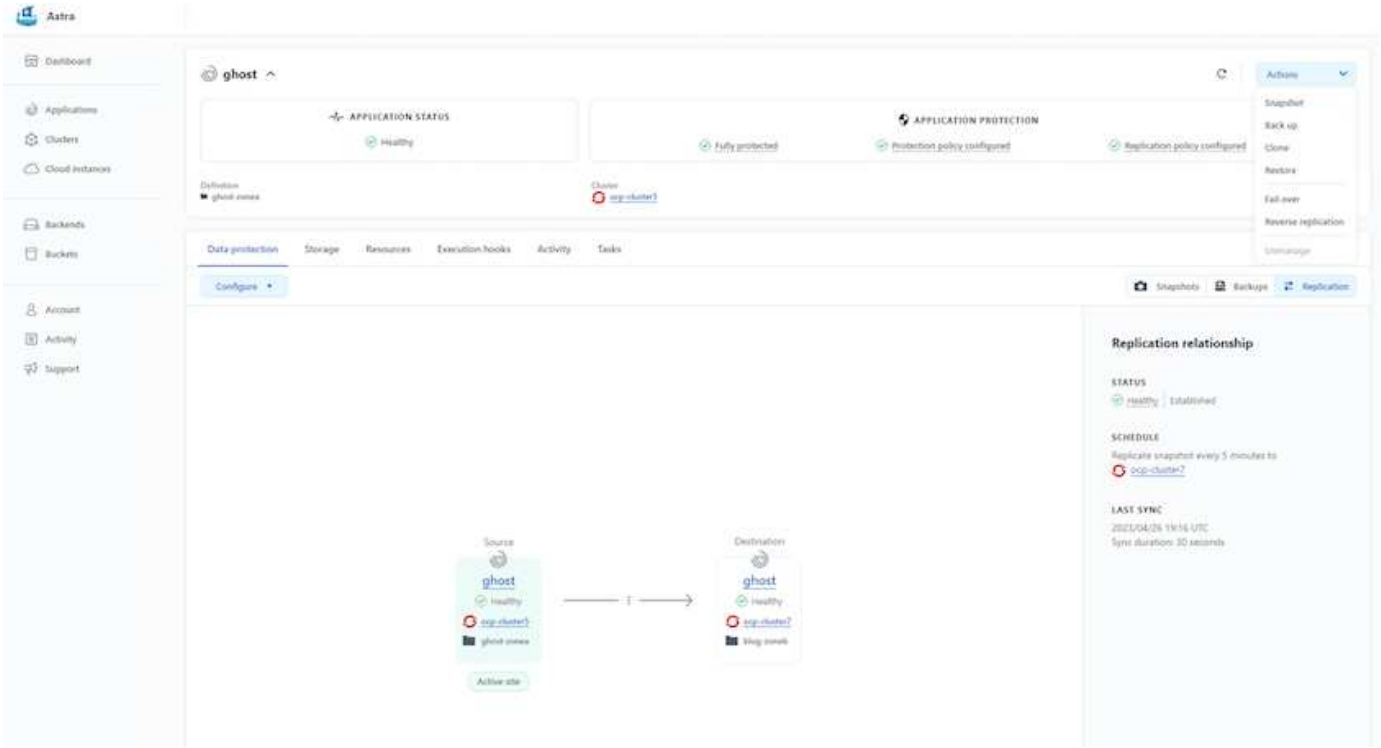
- **replica**
- **backup e ripristino**
- **clone**

Fare riferimento a. "sezione sulla protezione dei dati" per le opzioni **replica e backup e ripristino**.

Fare riferimento a. "qui" per ulteriori dettagli sulla clonazione **.

> La funzione di replica Astra è supportata solo con Trident Container Storage Interface (CSI). Tuttavia, la replica non è supportata dai driver nas-economy e san-economy.

Esecuzione della replica dei dati con ACC



Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

Panoramica

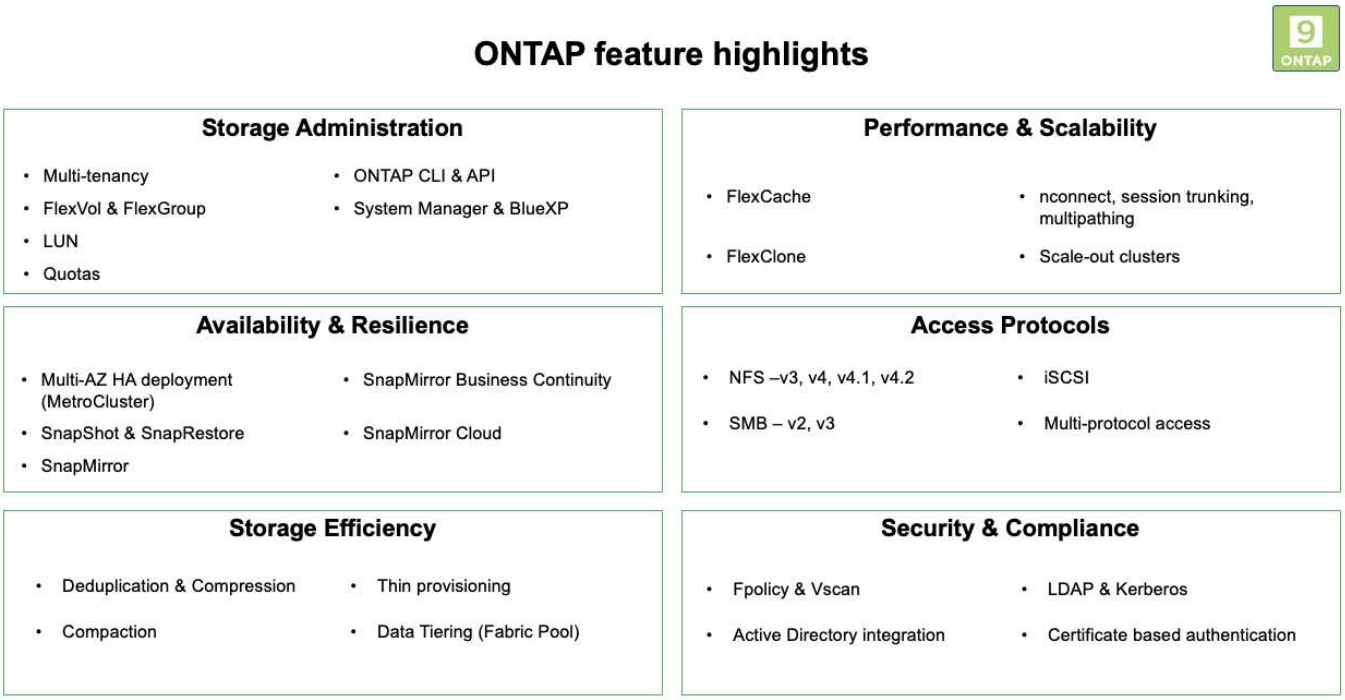
NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati,

affidabilità e flessibilità per le implementazioni di container e Kubernetes.

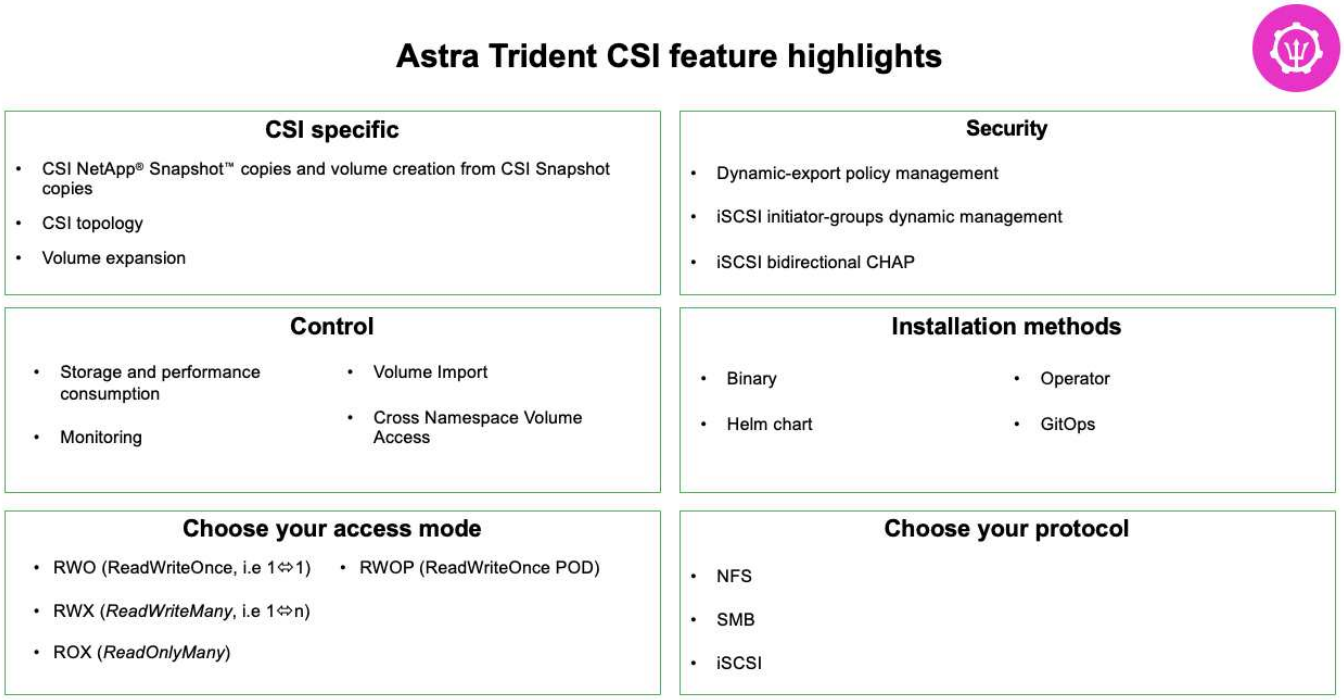
- Storage autogestita on-premise:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
  - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
  - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
  - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler



NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.



I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN) come storage persistente.

Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift nel cloud ibrido

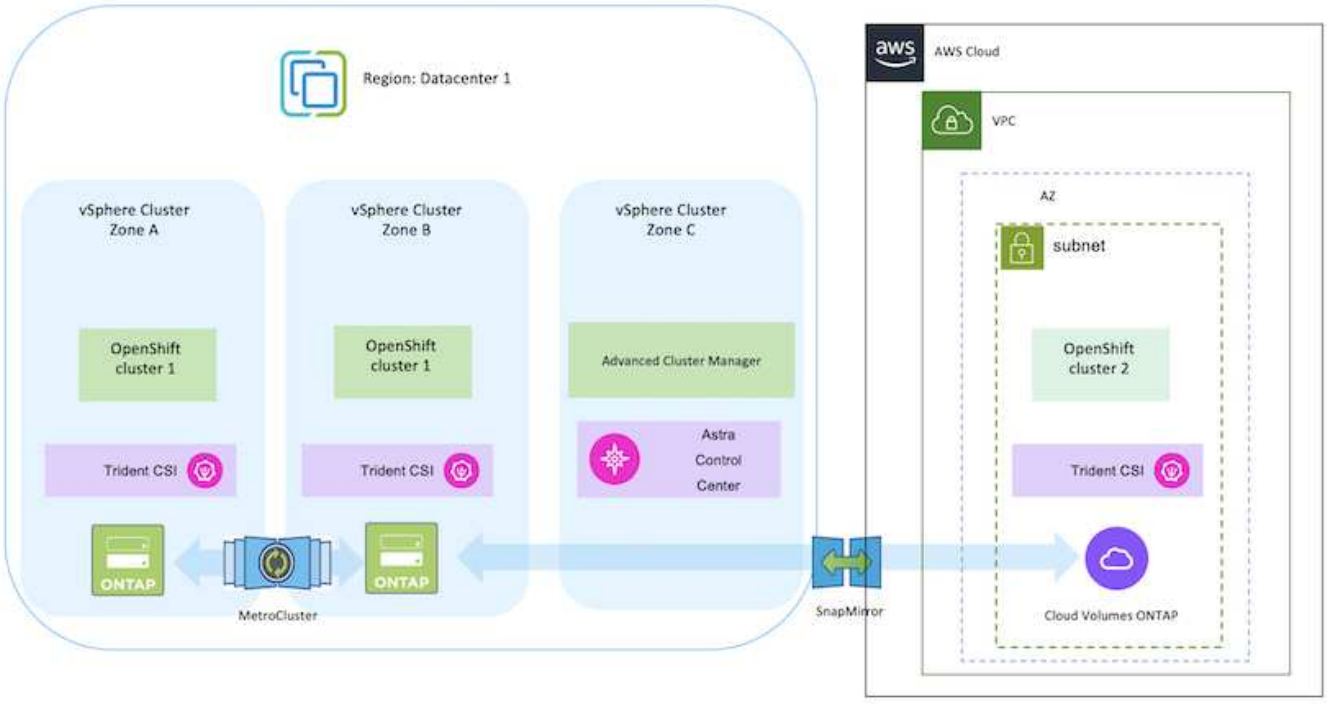
I clienti potrebbero trovarsi in un punto del loro percorso di modernizzazione quando sono pronti a spostare alcuni carichi di lavoro selezionati o tutti i carichi di lavoro dai data center al cloud. Possono scegliere di utilizzare container OpenShift autogestiti e storage NetApp autogestiti nel cloud per diversi motivi. Devono pianificare e implementare la piattaforma container Red Hat OpenShift (OCP) nel cloud per un ambiente pronto per la

produzione di successo per la migrazione dei carichi di lavoro dei container dai data center. I loro cluster OCP possono essere implementati su VMware o bare metal nei loro data center e su AWS, Azure o Google Cloud nell'ambiente cloud.

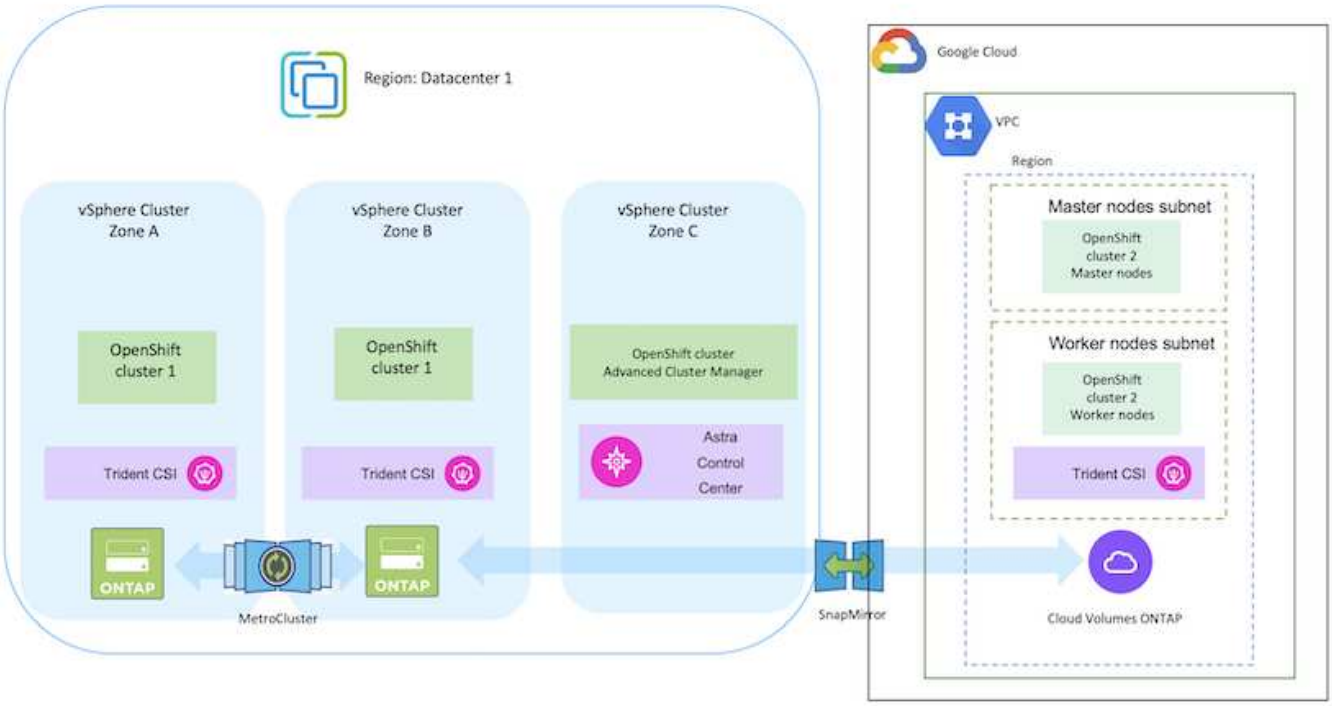
Lo storage NetApp Cloud Volumes ONTAP offre protezione dei dati, affidabilità e flessibilità per le implementazioni di container in AWS, Azure e Google Cloud. Astra Trident funge da provider di storage dinamico per consumare lo storage Cloud Volumes ONTAP persistente per le applicazioni stateful dei clienti. Astra Control Center può essere utilizzato per orchestrare i numerosi requisiti di gestione dei dati delle applicazioni stateful come protezione dei dati, migrazione e business continuity.

Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift in un cloud ibrido con Astra Control Center

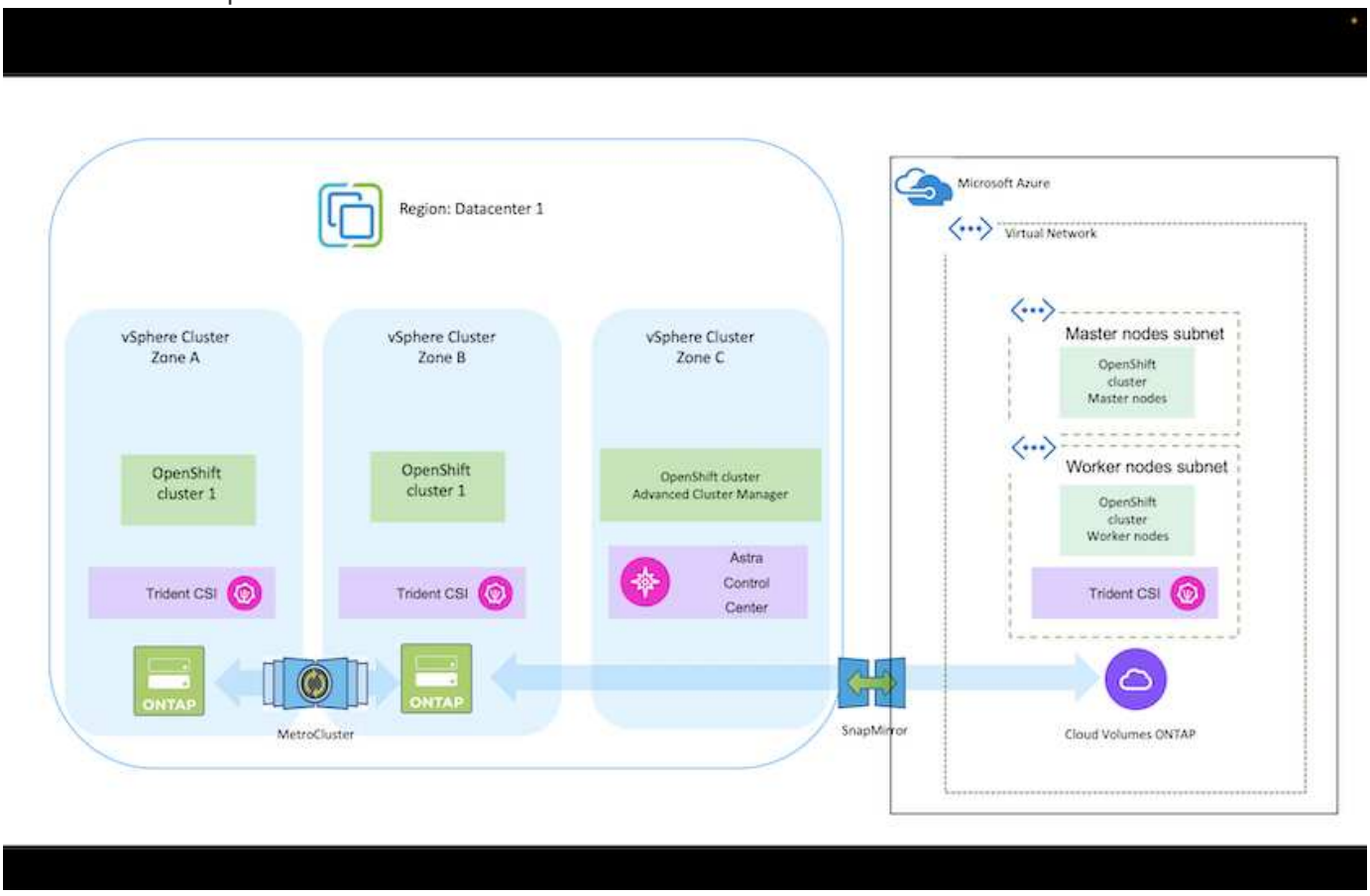
On-premise e in AWS



On-premise e Google Cloud



Azure Cloud e on-premise



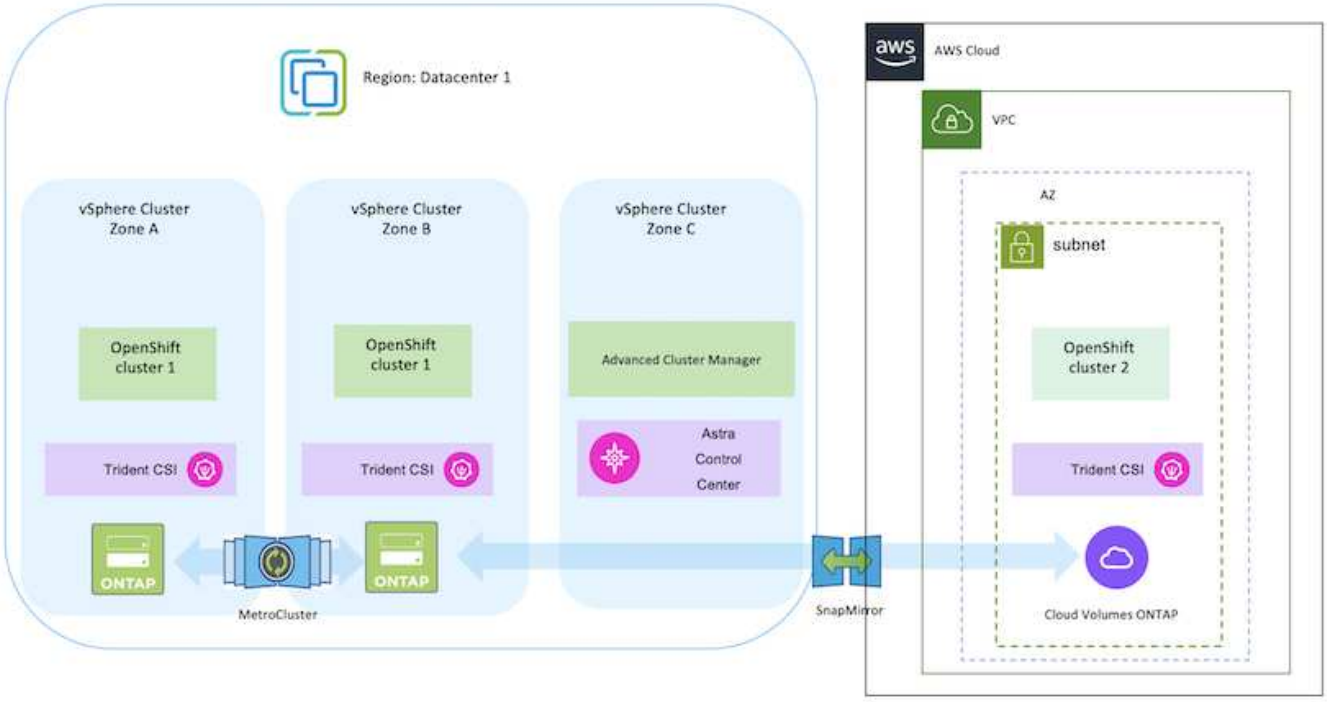
Implementa e configura la piattaforma container Red Hat OpenShift su AWS

In questa sezione viene descritto un workflow di alto livello che illustra come configurare

e gestire i cluster OpenShift in AWS e come implementare applicazioni stateful su di essi. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'aiuto di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift su AWS. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Di seguito è riportato un diagramma che illustra i cluster implementati su AWS e connessi al data center mediante una VPN.



Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare un cluster OCP su AWS da Advanced Cluster Management.

- Creare un VPC con una connessione VPN sito-sito (utilizzando pfsense) per connettersi alla rete on-premise.
- La rete on-premise dispone di connettività Internet.
- Creare 3 subnet private in 3 diversi AZS.
- Creare una zona host privata Route 53 e un resolver DNS per il VPC.

Creare il cluster OpenShift su AWS dalla procedura guidata Advanced Cluster Management (ACM). Fare riferimento alle istruzioni "qui".

Puoi anche creare il cluster in AWS dalla console OpenShift Hybrid Cloud. Fare riferimento a. "qui" per istruzioni.

Quando si crea il cluster utilizzando ACM, è possibile personalizzare l'installazione modificando il file yaml dopo aver inserito i dettagli nella vista del modulo. Una volta creato il cluster, è possibile accedere ssh ai nodi del cluster per la risoluzione dei problemi o per un'ulteriore configurazione manuale. Utilizzare la chiave ssh fornita durante l'installazione e il nome utente principale per effettuare il login.

Implementare Cloud Volumes ONTAP in AWS utilizzando BlueXP.

- Installare il connettore in ambiente VMware on-premise. Fare riferimento alle istruzioni "qui".
- Implementare un'istanza CVO in AWS utilizzando il connettore. Fare riferimento alle istruzioni "qui".

Il connettore può essere installato anche nell'ambiente cloud. Fare riferimento a. "qui" per ulteriori informazioni.

Installare Astra Trident nel cluster OCP

- Implementare Trident Operator utilizzando Helm. Fare riferimento alle istruzioni "qui"
- Creare un backend e una classe di storage. Fare riferimento alle istruzioni "qui".

Aggiungere il cluster OCP su AWS all'Astra Control Center.

Aggiungere il cluster OCP in AWS ad Astra Control Center.

Utilizzo della funzionalità topologia CSI di Trident per architetture multi-zona

I cloud provider, oggi, consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi dei cluster basati su zone. I nodi possono essere collocati in diverse zone di disponibilità all'interno di una regione o in diverse regioni. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multi-zona, Astra Trident utilizza la topologia CSI. Utilizzando la funzionalità topologia CSI, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle aree geografiche e alle zone di disponibilità. Fare riferimento a. "qui" per ulteriori dettagli.

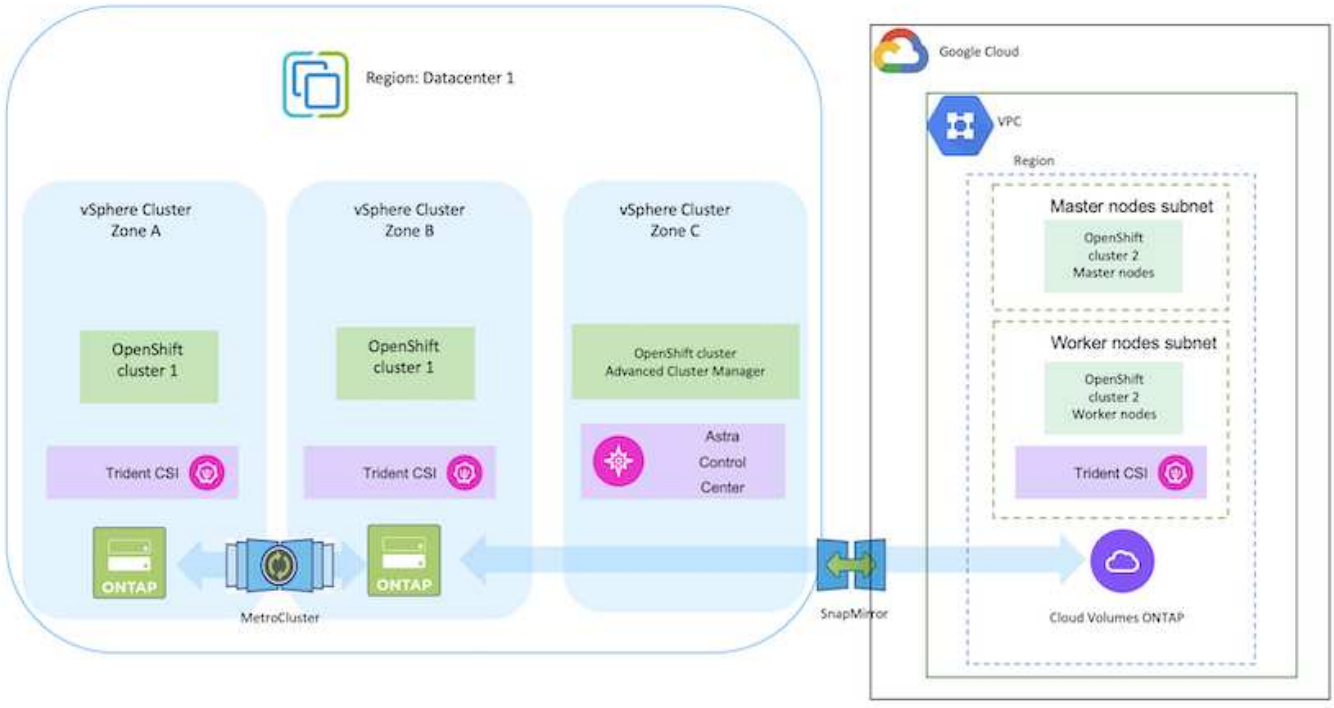
Kubernetes supporta due modalità di binding del volume: - Quando ***VolumeBindingMode* è impostato su *immediate*** (default), Astra Trident crea il volume senza alcuna consapevolezza della topologia. I volumi persistenti vengono creati senza alcuna dipendenza dai requisiti di pianificazione del pod richiedente. - Quando ***VolumeBindingMode* viene impostato su *WaitForFirstConsumer***, la creazione e il binding di un volume persistente per un PVC viene ritardata fino a quando un pod che utilizza il PVC viene pianificato e creato. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di storage Astra Trident possono essere progettati per eseguire il provisioning selettivo dei volumi in base alle zone di disponibilità (back-end compatibile con la topologia). Per StorageClasses che utilizzano tale backend, un volume viene creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass consapevole della topologia) fare riferimento "qui" per ulteriori dettagli.

Implementare e configurare la piattaforma Red Hat OpenShift Container su GCP

Implementare e configurare la piattaforma Red Hat OpenShift Container su GCP

In questa sezione viene descritto un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in GCP e distribuire le applicazioni stateful su di essi. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'aiuto di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

Segue un diagramma che mostra i cluster implementati in GCP e connessi al data center tramite una VPN.



Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift in GCP. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare un cluster OCP su GCP dalla CLI.

- Assicurarsi di aver soddisfatto tutti i prerequisiti indicati "qui".
- Per la connettività VPN tra on-premise e GCP, è stata creata e configurata una macchina virtuale pfsense. Per istruzioni, vedere "qui".
  - L'indirizzo del gateway remoto in pfsense può essere configurato solo dopo aver creato un gateway VPN in Google Cloud Platform.
  - Gli indirizzi IP della rete remota per la fase 2 possono essere configurati solo dopo l'esecuzione del programma di installazione del cluster OpenShift e la creazione dei componenti dell'infrastruttura per il cluster.
  - La VPN in Google Cloud può essere configurata solo dopo che i componenti di infrastruttura per il cluster sono stati creati dal programma di installazione.
- Installare ora il cluster OpenShift su GCP.
  - Ottenere il programma di installazione e il segreto pull e distribuire il cluster seguendo i passaggi forniti nella documentazione "qui".
  - L'installazione crea una rete VPC in Google Cloud Platform. Inoltre, crea una zona privata in DNS cloud e aggiunge record.
    - Utilizzare l'indirizzo del blocco CIDR della rete VPC per configurare pfsense e stabilire la connessione VPN. Assicurarsi che i firewall siano configurati correttamente.
    - Aggiungere Un record nel DNS dell'ambiente on-premise utilizzando l'indirizzo IP nei record A del DNS di Google Cloud.
  - L'installazione del cluster viene completata e viene fornito un file kubeconfig e un nome utente e una password per accedere alla console del cluster.

Implementa Cloud Volumes ONTAP in GCP usando BlueXP.

- Installare un connettore in Google Cloud. Fare riferimento alle istruzioni "qui".
- Implementa un'istanza CVO in Google Cloud usando Connector. Fare riferimento alle istruzioni riportate di seguito. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Installare Astra Trident nel cluster OCP in GCP

- Esistono molti metodi per implementare Astra Trident, come illustrato "qui".
- Per questo progetto, Astra Trident è stato installato distribuendo manualmente l'operatore Astra Trident utilizzando le istruzioni "qui".
- Creare classi di storage e backend. Fare riferimento alle istruzioni "qui".

Aggiungere il cluster OCP su GCP all'Astra Control Center.

- Creare un file KubeConfig separato con un ruolo cluster che contenga le autorizzazioni minime necessarie per gestire un cluster da Astra Control. Le istruzioni sono disponibili "qui".
- Aggiungere il cluster ad Astra Control Center seguendo le istruzioni "qui"

Utilizzo della funzionalità topologia CSI di Trident per architetture multi-zona

I cloud provider, oggi, consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi dei cluster basati su zone. I nodi possono essere collocati in diverse zone di disponibilità all'interno di una regione o in diverse regioni. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multi-zona, Astra Trident utilizza la topologia CSI. Utilizzando la funzionalità topologia CSI, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle aree geografiche e alle zone di disponibilità. Fare riferimento a. "qui" per ulteriori dettagli.

> Kubernetes supporta due modalità di binding del volume: - Quando ***VolumeBindingMode* è impostato su *immediate*** (default), Astra Trident crea il volume senza alcuna consapevolezza della topologia. I volumi persistenti vengono creati senza alcuna dipendenza dai requisiti di pianificazione del pod richiedente. - Quando ***VolumeBindingMode* viene impostato su *WaitForFirstConsumer***, la creazione e il binding di un volume persistente per un PVC viene ritardata fino a quando un pod che utilizza il PVC viene pianificato e creato. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di storage Astra Trident possono essere progettati per eseguire il provisioning selettivo dei volumi in base alle zone di disponibilità (back-end compatibile con la topologia). Per StorageClasses che utilizzano tale backend, un volume viene creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass consapevole della topologia) fare riferimento "qui" per ulteriori dettagli.

Video dimostrativo

Installazione del cluster OpenShift su Google Cloud Platform

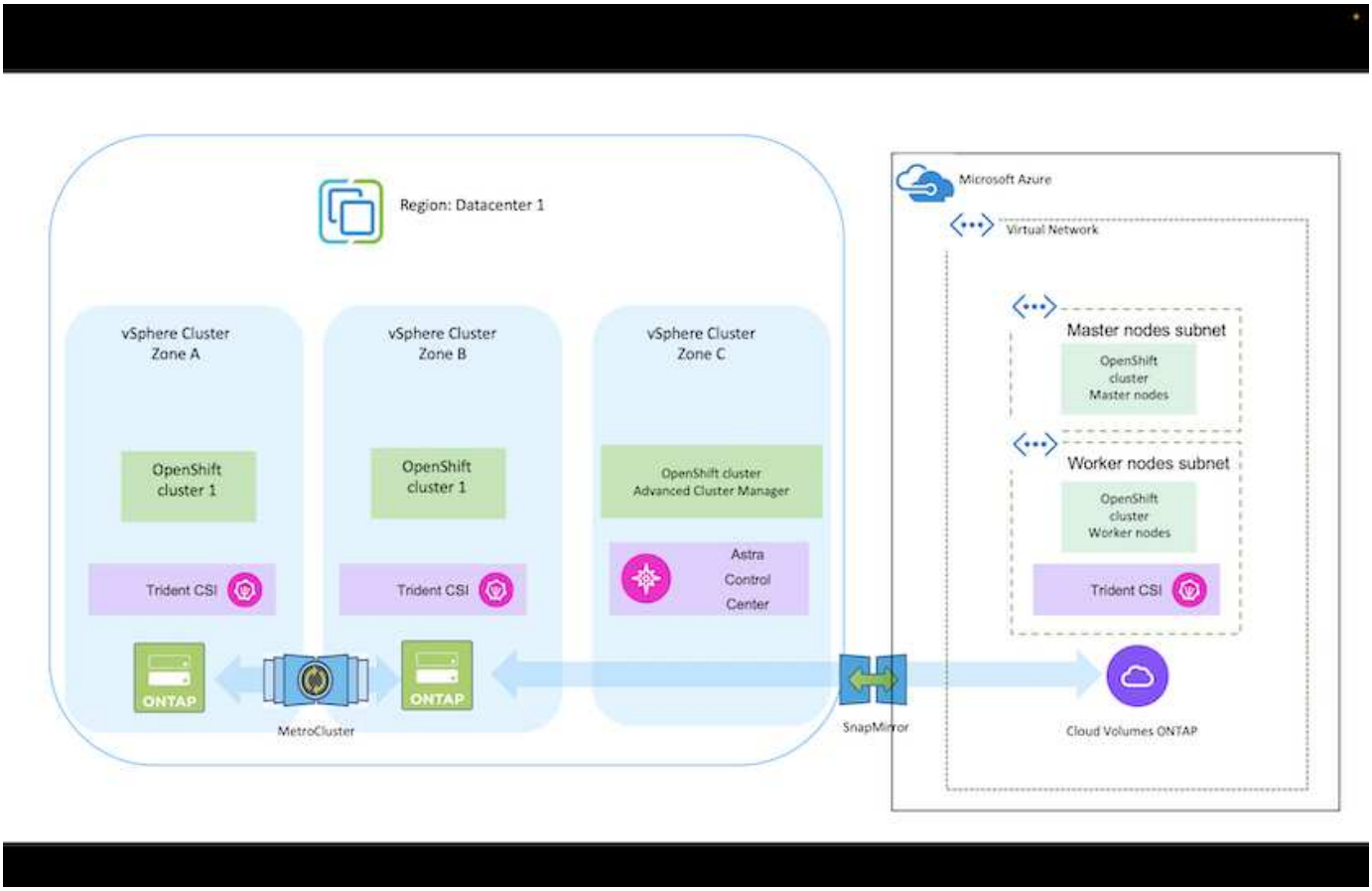
Importazione dei cluster OpenShift in Astra Control Center

Implementa e configura la piattaforma Red Hat OpenShift Container su Azure

Implementa e configura la piattaforma Red Hat OpenShift Container su Azure

In questa sezione viene descritto un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in Azure e distribuire applicazioni stateful su di essi. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'aiuto di Astra Trident/Astra Control Provivioner per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

Segue un diagramma che mostra i cluster implementati in Azure e connessi al data center tramite una VPN.



Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift in Azure. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare un cluster OCP in Azure dalla CLI.

- Assicurarsi di aver soddisfatto tutti i prerequisiti indicati "qui".
- Creare una VPN, subnet, gruppi di protezione della rete e una zona DNS privata. Creare un gateway VPN e una connessione VPN da sito a sito.
- Per la connettività VPN tra on-premise e Azure, è stata creata e configurata una macchina virtuale pfsense. Per istruzioni, vedere "qui".
- Ottenere il programma di installazione e il segreto pull e distribuire il cluster seguendo i passaggi forniti nella documentazione "qui".
- L'installazione del cluster viene completata e viene fornito un file kubeconfig e un nome utente e una password per accedere alla console del cluster.

Di seguito è riportato un esempio di file install-config.yaml.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
```

```
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

Implementa Cloud Volumes ONTAP in Azure utilizzando BlueXP.

- Installa un connettore in Azure. Fare riferimento alle istruzioni "qui".
- Implementa un'istanza CVO in Azure usando Connector. Fare riferimento alle istruzioni link:https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [qui].

Installa Astra Control Provisioner nel cluster OCP in Azure

- Per questo progetto, Astra Control Provisioner (ACP) è stato installato in tutti i cluster (cluster on-premise, cluster on-premise in cui viene implementato Astra Control Center e il cluster in Azure). Scopri di più su Astra Control Provisioner "qui".
- Creare classi di storage e backend. Fare riferimento alle istruzioni "qui".

Aggiungi il cluster OCP in Azure all'Astra Control Center.

- Creare un file KubeConfig separato con un ruolo cluster che contenga le autorizzazioni minime necessarie per gestire un cluster da Astra Control. Le istruzioni sono disponibili "qui".
- Aggiungere il cluster ad Astra Control Center seguendo le istruzioni "qui"

Utilizzo della funzionalità topologia CSI di Trident per architetture multi-zona

I cloud provider, oggi, consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi dei cluster basati su zone. I nodi possono essere collocati in diverse zone di disponibilità all'interno di una regione o in diverse regioni. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multi-zona, Astra Trident utilizza la topologia CSI. Utilizzando la funzionalità topologia CSI, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle aree geografiche e alle zone di disponibilità. Fare riferimento a. "qui" per ulteriori dettagli.

> Kubernetes supporta due modalità di binding del volume: - Quando ***VolumeBindingMode* è impostato su *immediate*** (default), Astra Trident crea il volume senza alcuna consapevolezza della topologia. I volumi persistenti vengono creati senza alcuna dipendenza dai requisiti di pianificazione del pod richiedente. - Quando ***VolumeBindingMode* viene impostato su *WaitForFirstConsumer***, la creazione e il binding di un volume persistente per un PVC viene ritardata fino a quando un pod che utilizza il PVC viene pianificato e creato. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di storage Astra Trident possono essere progettati per eseguire il provisioning selettivo dei volumi in base alle zone di disponibilità (back-end compatibile con la topologia). Per StorageClasses che utilizzano tale backend, un volume viene creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass consapevole della topologia) fare riferimento "qui" per ulteriori dettagli.

Video dimostrativo

Utilizzo di Astra Control per il failover e il failback delle applicazioni

Protezione dei dati mediante Astra Control Center

Questa pagina mostra le opzioni di protezione dei dati per le applicazioni basate su container Red Hat OpenShift in esecuzione su VMware vSphere o nel cloud tramite Astra Control Center (ACC).

Mentre gli utenti intraprendono il percorso di modernizzazione delle proprie applicazioni con Red Hat OpenShift, è necessario adottare una strategia di protezione dei dati per proteggerli da cancellazioni accidentali o altri errori umani. Spesso, per proteggere i propri dati da un diaster, è necessaria anche una strategia di protezione a scopo normativo o di compliance.

I requisiti di protezione dei dati variano dal ritorno a una copia point-in-time al failover automatico a un dominio di errore diverso senza alcun intervento umano. Molti clienti scelgono ONTAP come piattaforma di storage preferita per le loro applicazioni Kubernetes per le sue ricche funzionalità come multi-tenancy, multi-protocollo, offerte di capacità e performance elevate, replica e caching per ubicazioni multi-sito, sicurezza e flessibilità.

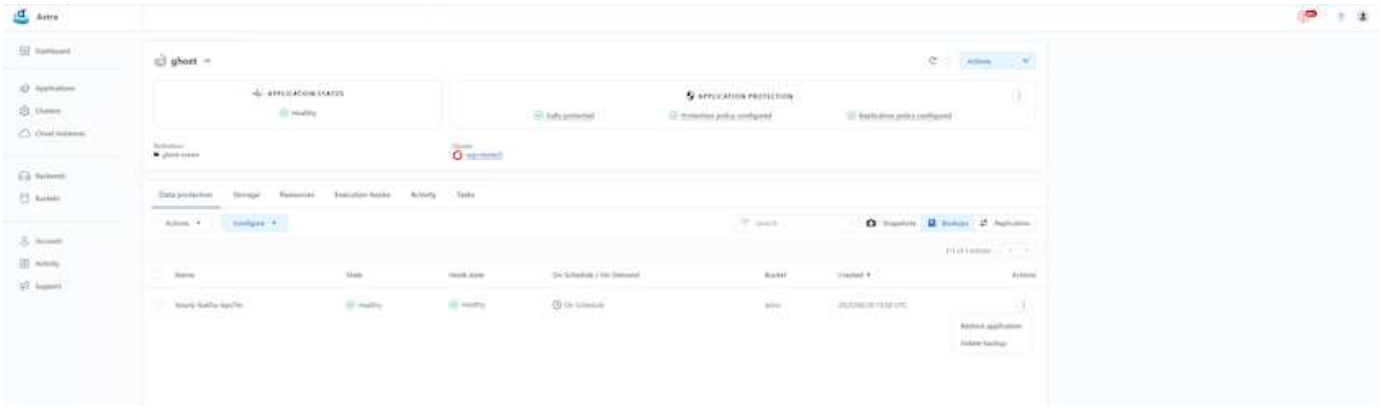
I clienti possono avere un ambiente cloud configurato come estensione del data center, in modo che possano sfruttare i benefici del cloud e essere in grado di spostare i propri carichi di lavoro in un momento futuro. Per tali clienti, il backup delle applicazioni OpenShift e dei dati nell'ambiente cloud diventa una scelta inevitabile.

Possono quindi ripristinare le applicazioni e i dati associati su un cluster OpenShift nel cloud o nel data center.

Backup e ripristino con ACC

I proprietari delle applicazioni possono rivedere e aggiornare le applicazioni rilevate da ACC. ACC può eseguire copie Snapshot utilizzando CSI ed eseguire il backup utilizzando la copia Snapshot point-in-time. La destinazione del backup può essere un archivio di oggetti nell'ambiente cloud. È possibile configurare i criteri di protezione per i backup pianificati e il numero di versioni di backup da conservare. L'RPO minimo è di un'ora.

Ripristino di un'applicazione da un backup mediante ACC

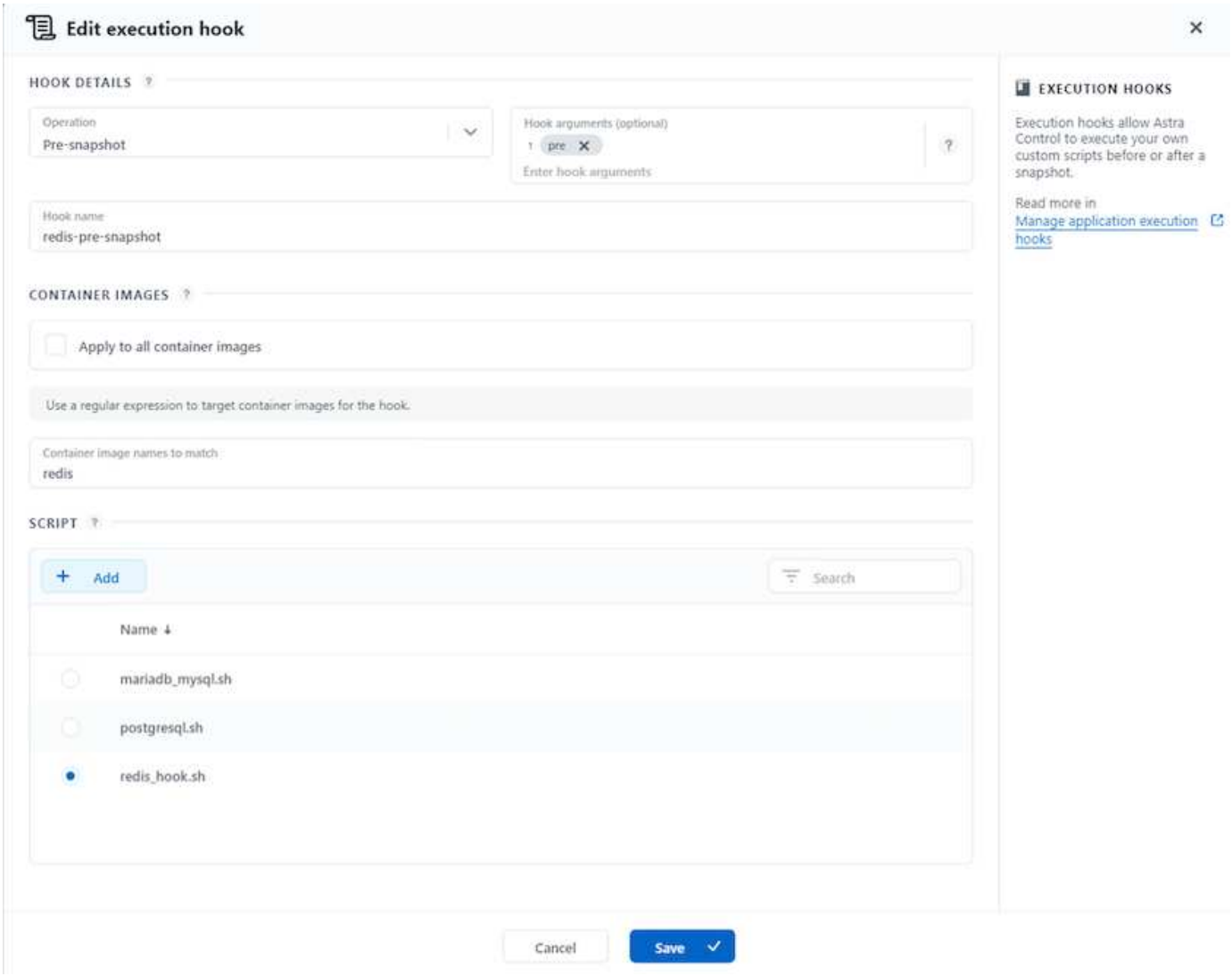


Hook di esecuzione specifici dell'applicazione

Anche se sono disponibili funzionalità di protezione dei dati a livello di array di storage, spesso sono necessari ulteriori passaggi per rendere coerenti le applicazioni di backup e ripristino. I passaggi aggiuntivi specifici dell'applicazione potrebbero essere: - Prima o dopo la creazione di una copia Snapshot. - prima o dopo la creazione di un backup. - Dopo il ripristino da una copia Snapshot o da un backup. Astra Control può eseguire questi passaggi specifici dell'applicazione codificati come script personalizzati chiamati uncini di esecuzione.

Di NetApp "Progetto open source Verda" fornisce hook di esecuzione per le applicazioni native del cloud più diffuse per rendere la protezione delle applicazioni semplice, robusta e facile da orchestrare. Se si dispone di informazioni sufficienti per un'applicazione non presente nel repository, è possibile contribuire al progetto.

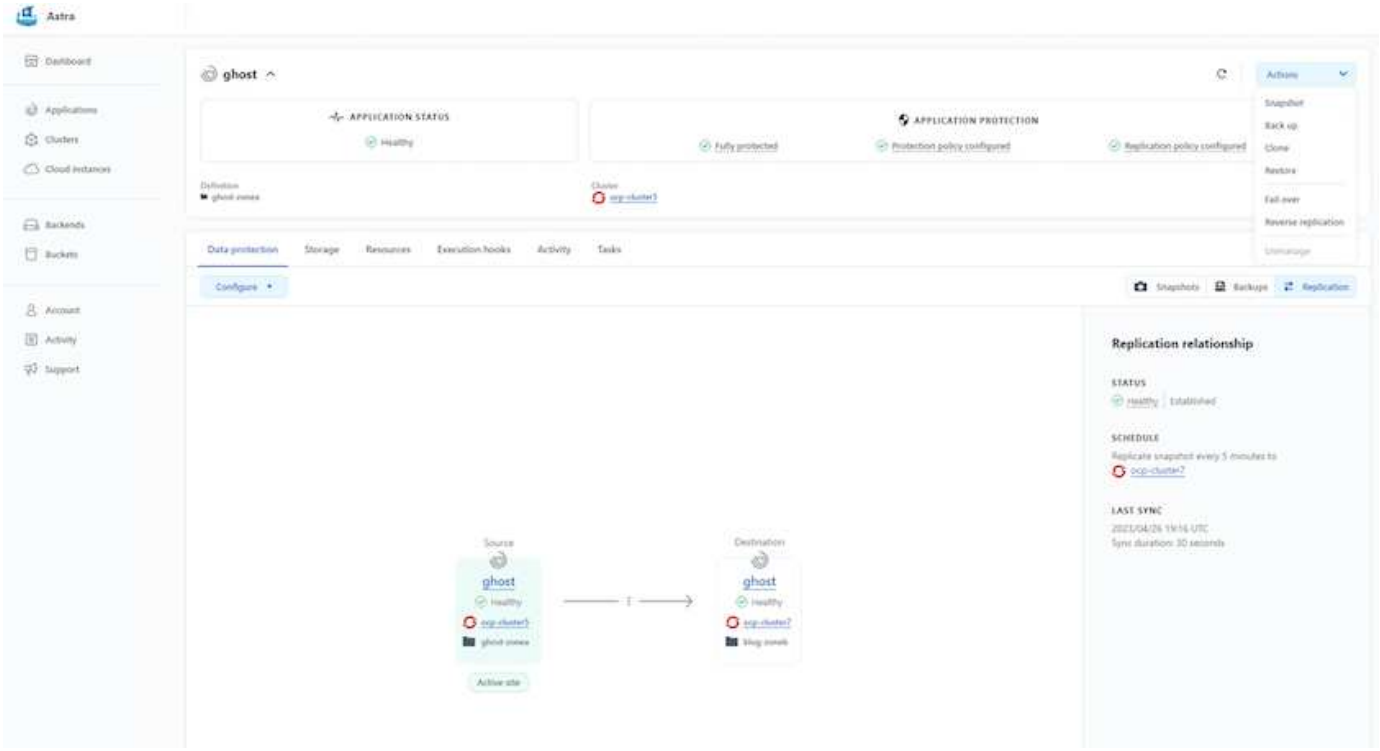
Esempio di gancio di esecuzione per pre-Snapshot di un'applicazione redis.



Replica con ACC

Per la protezione regionale o per una soluzione RPO e RTO bassa, un'applicazione può essere replicata in un'altra istanza di Kubernetes in esecuzione in un sito diverso, preferibilmente in un'altra regione. ACC utilizza SnapMirror asincrono ONTAP con RPO in soli 5 minuti. Fare riferimento a. "qui" Per le istruzioni di installazione di SnapMirror.

SnapMirror con ACC



i driver di storage san-economy e nas-economy non supportano la funzione di replica. Fare riferimento a. "qui" per ulteriori dettagli.

Video dimostrativo:

"Video dimostrativo del disaster recovery con Astra Control Center"

Data Protection con Astra Control Center

Sono disponibili dettagli sulle funzioni di protezione dei dati di Astra Control Center "qui"

Disaster recovery (failover e failback con replica) con ACC

Utilizzo di Astra Control per il failover e il failback delle applicazioni

Migrazione dei dati con Astra Control Center

Questa pagina mostra le opzioni di migrazione dei dati per i carichi di lavoro container sui cluster Red Hat OpenShift con Astra Control Center (ACC). In particolare, i clienti possono utilizzare l'ACC per trasferire alcuni workload selezionati o tutti i workload dai data center on-premise al cloud, clonare le loro applicazioni nel cloud a scopo di test o passare dal data center al cloud

Migrazione dei dati

Per migrare l'applicazione da un ambiente a un altro, è possibile utilizzare una delle seguenti funzionalità di ACC:

- **replica**
- **backup e ripristino**

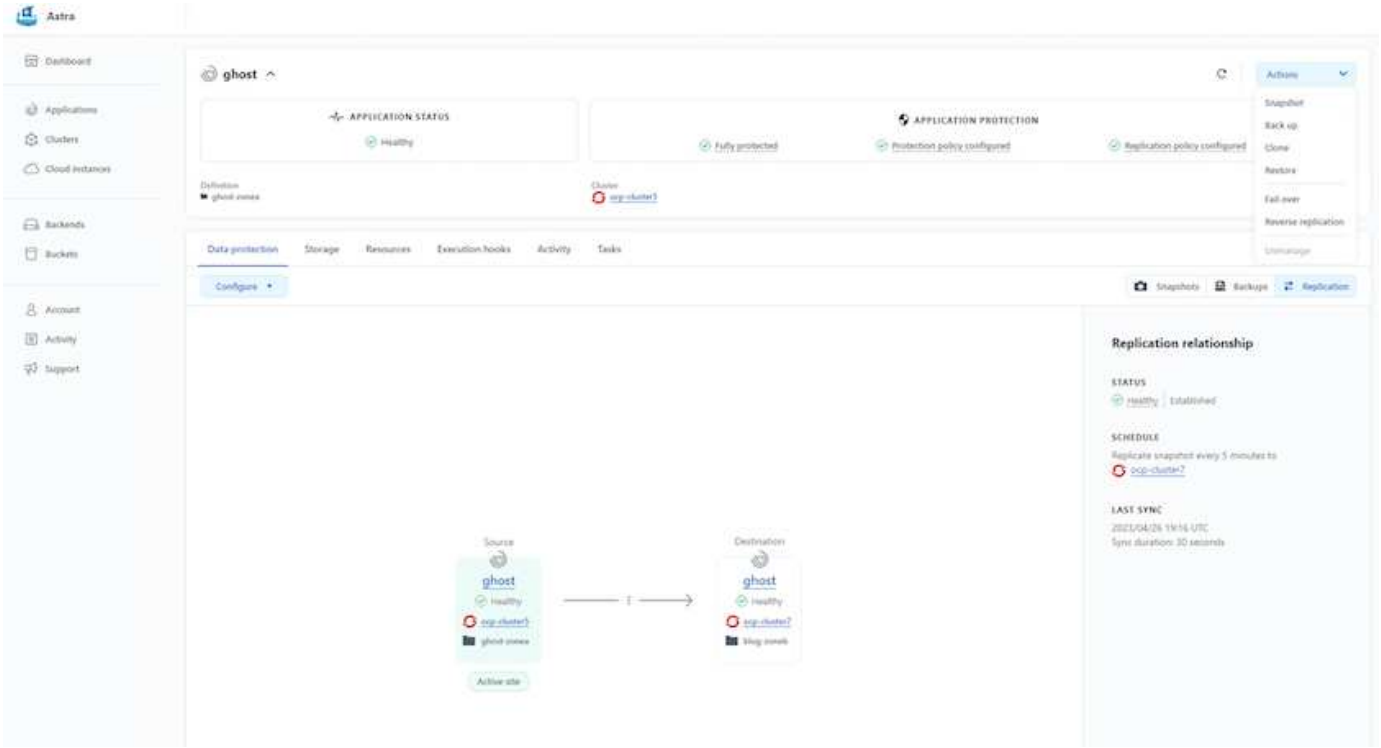
- **clone**

Fare riferimento a. "sezione sulla protezione dei dati" per le opzioni **replica e backup e ripristino**.

Fare riferimento a. "qui" per ulteriori dettagli sulla clonazione **.

> La funzione di replica Astra è supportata solo con Trident Container Storage Interface (CSI). Tuttavia, la replica non è supportata dai driver nas-economy e san-economy.

Esecuzione della replica dei dati con ACC



Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

Panoramica

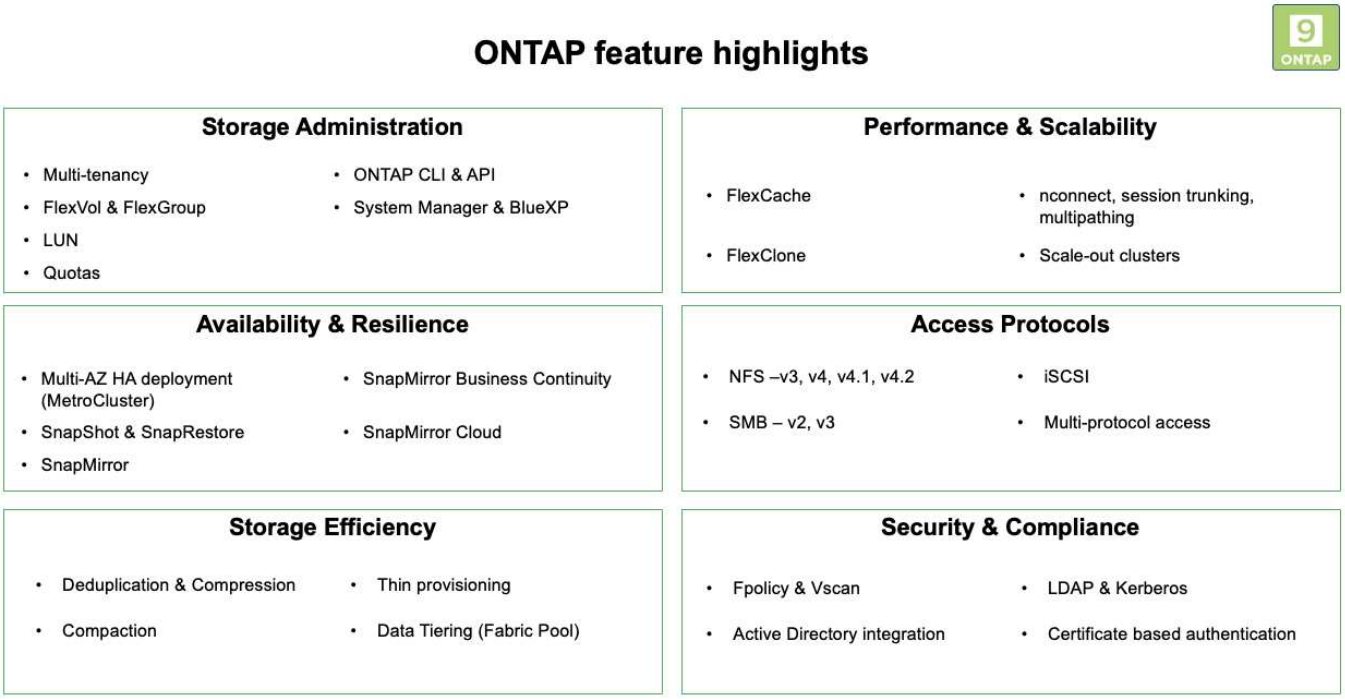
NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati, affidabilità e flessibilità per le implementazioni di container e Kubernetes.

- Storage autogestita on-premise:

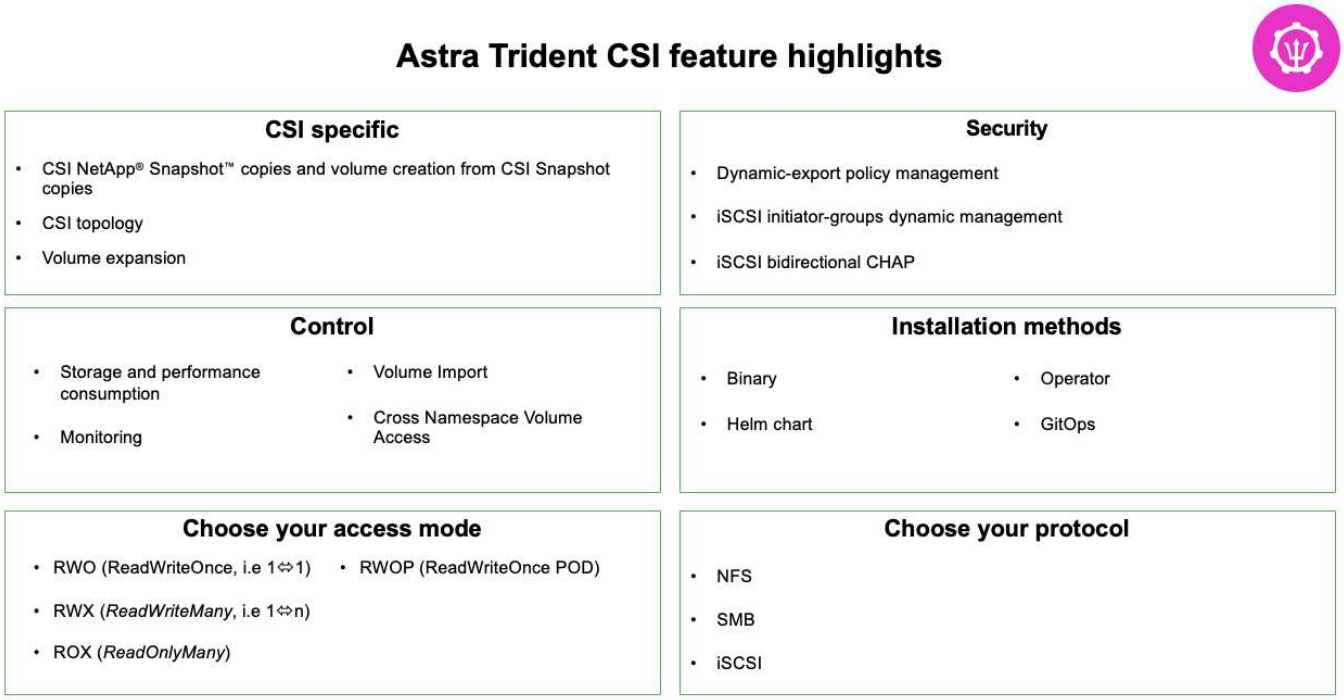
    - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
    - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
    - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
    - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler



NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.



I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN) come storage persistente.

Soluzione NetApp con workload gestiti della piattaforma container Red Hat OpenShift su AWS

Soluzione NetApp con workload gestiti della piattaforma container Red Hat OpenShift su AWS

I clienti possono "nascere nel cloud" o trovarsi in un punto del loro percorso di modernizzazione quando sono pronti a spostare alcuni carichi di lavoro selezionati o tutti i carichi di lavoro dai data center al cloud. Possono scegliere di utilizzare container

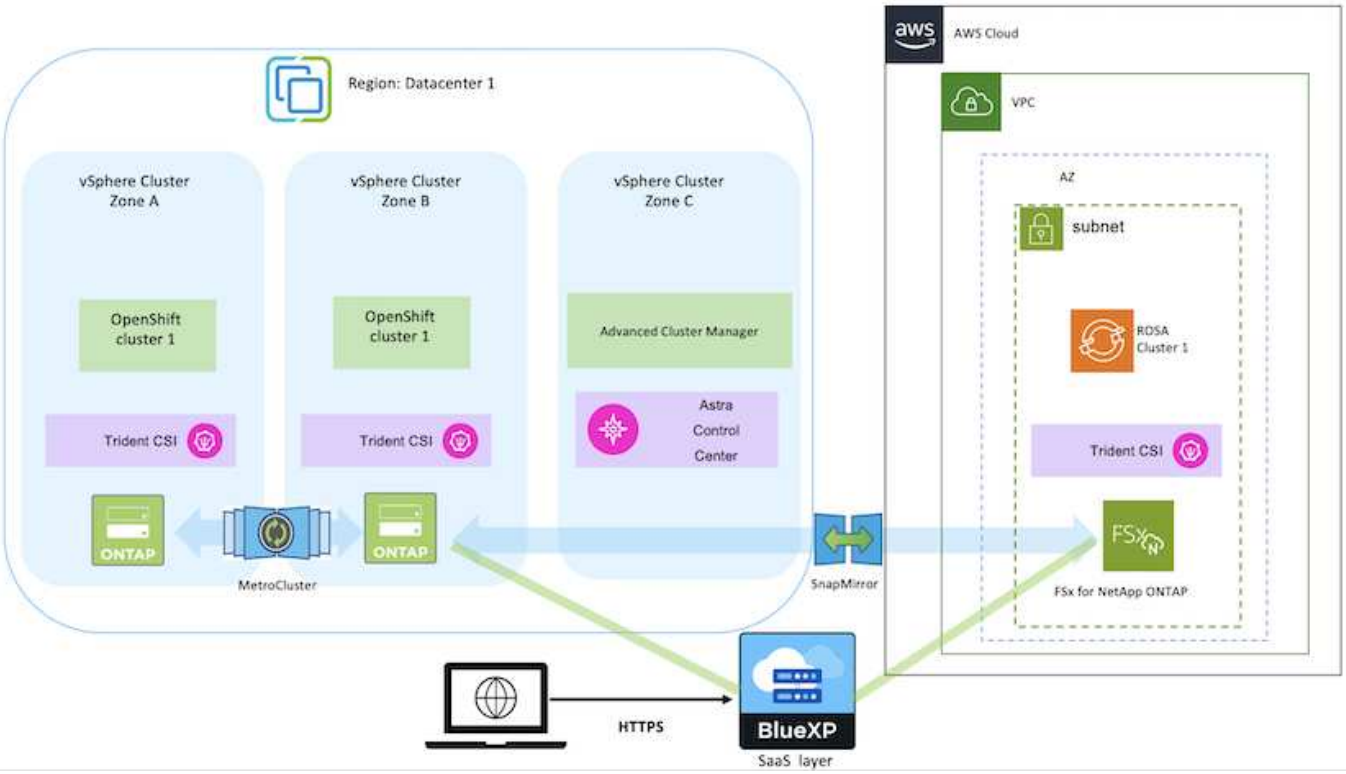
OpenShift gestiti da provider e storage NetApp gestito da provider nel cloud per l'esecuzione dei carichi di lavoro. Devono pianificare e implementare i cluster di container gestiti Red Hat OpenShift (ROSA) nel cloud per un ambiente pronto per la produzione di successo per i carichi di lavoro dei container. Quando si trovano nel cloud AWS, potrebbero anche implementare FSX per NetApp ONTAP per le esigenze di storage.

FSX per NetApp ONTAP offre protezione dei dati, affidabilità e flessibilità per le implementazioni di container in AWS. Astra Trident funge da provider di storage dinamico per consumare lo storage FSxN persistente per le applicazioni stateful dei clienti.

Poiché ROSA può essere implementato in modalità ha con nodi del piano di controllo distribuiti in più zone di disponibilità, FSX ONTAP può anche essere fornito con l'opzione Multi-AZ che fornisce alta disponibilità e protegge dai guasti AZ.

> Non sono previsti costi per il trasferimento dei dati quando si accede a un file system Amazon FSX dalla zona di disponibilità preferita (AZ) del file system. Per ulteriori informazioni sui prezzi, fare riferimento a. "qui".

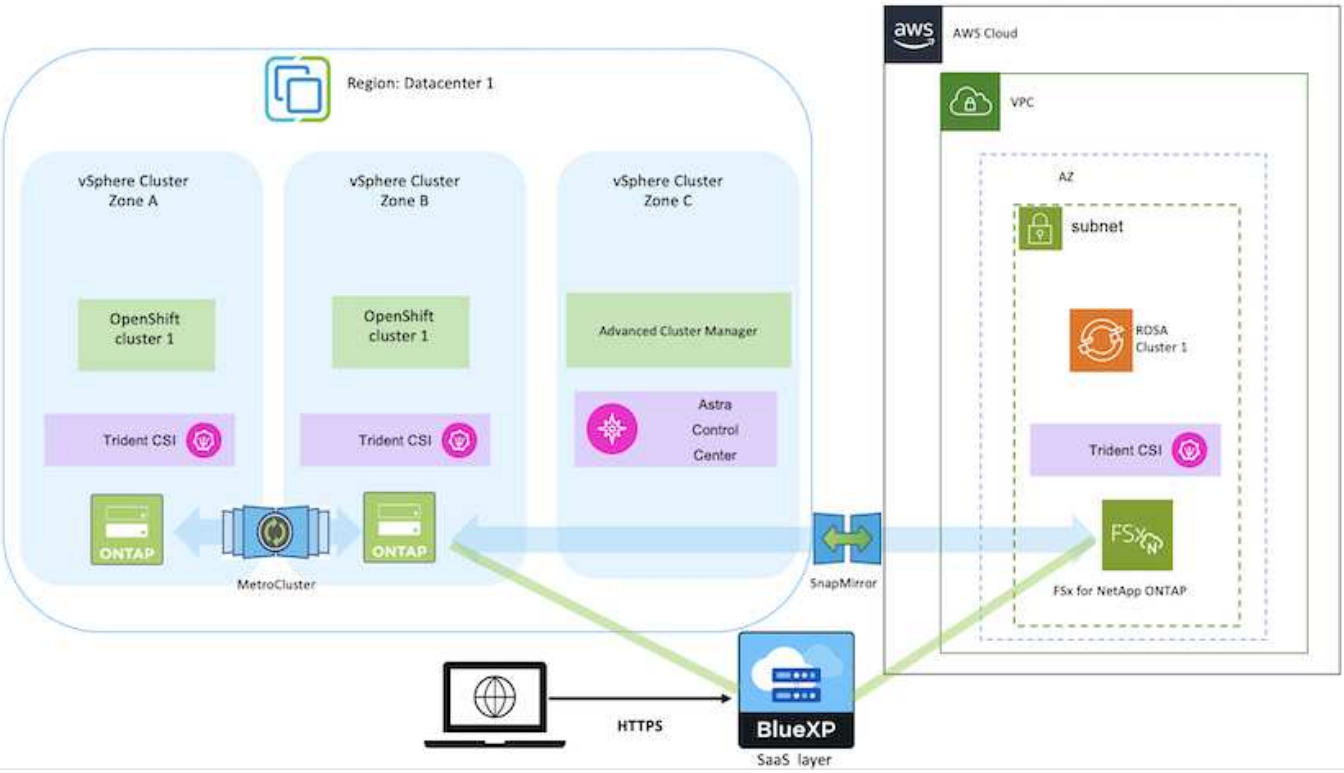
Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift



Implementa e configura la piattaforma container Managed Red Hat OpenShift su AWS

Questa sezione descrive un workflow di alto livello per la configurazione dei cluster Managed Red Hat OpenShift su AWS(ROSA). Mostra l'utilizzo di FSX gestito per NetApp ONTAP (FSxN) come back-end di storage di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'implementazione di FSxN su AWS utilizzando BlueXP. Inoltre, vengono forniti dettagli sull'utilizzo di BlueXP e OpenShift GitOps (Argo CD) per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful sui cluster ROSA.

Di seguito è riportato un diagramma che illustra i cluster ROSA implementati su AWS e che utilizzano FSxN come storage back-end.



Questa soluzione è stata verificata utilizzando due cluster ROSA in due VPC in AWS. Ogni cluster ROSA è stato integrato con FSxN utilizzando Astra Trident. Esistono diversi modi per implementare I cluster ROSA e FSxN in AWS. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare I cluster ROSA

- Creare due VPC e configurare la connettività di peering VPC tra i VPC.
- Fare riferimento a. "qui" Per istruzioni sull'installazione dei cluster ROSA.

Installare FSxN

- Installare FSxN sui VPC da BlueXP. Fare riferimento a. "qui" Per la creazione di un account BlueXP e per iniziare. Fare riferimento a. "qui" Per l'installazione di FSxN. Fare riferimento a. "qui" Per creare un connettore in AWS per gestire FSxN.
- Implementare FSxN utilizzando AWS. Fare riferimento a. "qui" Per l'implementazione utilizzando la console AWS.

Installare Trident sui cluster ROSA (utilizzando il grafico Helm)

- USA il grafico Helm per installare Trident sui cluster ROSA. url del grafico Helm: https://netapp.github.io/trident-helm-chart

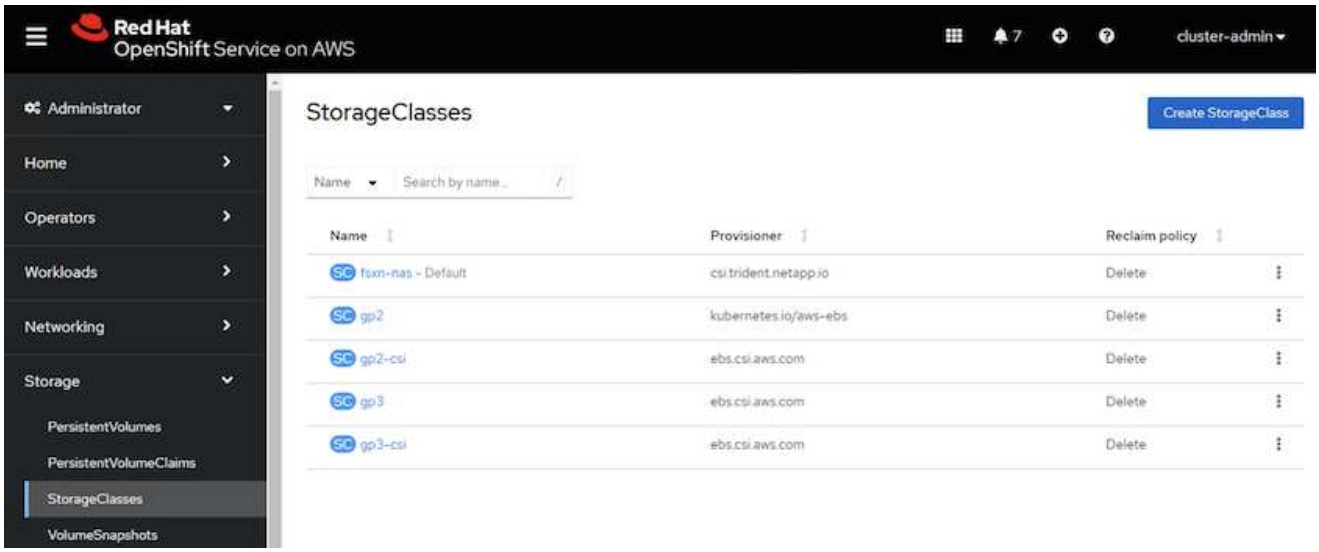
Integrazione di FSxN con Astra Trident per i cluster ROSA

OpenShift GitOps può essere utilizzato per implementare Astra Trident CSI su tutti i cluster gestiti, man mano che vengono registrati su ArgoCD utilizzando ApplicationSet.

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```

Creare classi di storage e backend utilizzando Trident (per FSxN)

- Fare riferimento a. "qui" per informazioni dettagliate sulla creazione di classe di storage e backend.
- Rendere la classe di storage creata per FsxN con Trident CSI come predefinita da OpenShift Console. Vedere la schermata riportata di seguito:



Implementare un'applicazione utilizzando OpenShift GitOps (CD Argo)

- Installare l'operatore OpenShift GitOps sul cluster. Fare riferimento alle istruzioni "qui".
- Configurare una nuova istanza del CD Argo per il cluster. Fare riferimento alle istruzioni "qui".

Aprire la console del CD Argo e implementare un'applicazione. Ad esempio, puoi implementare un'applicazione Jenkins utilizzando il CD Argo con Helm Chart. Durante la creazione dell'applicazione, sono stati forniti i seguenti dettagli: Progetto: Cluster predefinito: https://kubernetes.default.svcSpazio dei nomi: Jenkins l'URL per il grafico Helm: https://charts.bitnami.com/bitnami

Parametri Helm: Global.storageClass: Fsxn-nas

Protezione dei dati

Questa pagina mostra le opzioni di protezione dei dati per i cluster Managed Red Hat OpenShift on AWS (ROSA) utilizzando Astra Control Service. Astra Control Service (ACS) offre un'interfaccia grafica utente di facile utilizzo che consente di aggiungere cluster, definire le applicazioni in esecuzione ed eseguire attività di gestione dei dati integrate con le applicazioni. È possibile accedere alle funzioni ACS anche utilizzando un'API che consente l'automazione dei workflow.

L'alimentazione di Astra Control (ACS o ACC) è NetApp Astra Trident. Astra Trident integra diversi tipi di cluster Kubernetes come Red Hat OpenShift, EKS, AKS, SUSE Rancher, anthos ecc., con varie soluzioni di storage NetApp ONTAP come FAS/AFF, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files e Amazon FSX per NetApp ONTAP.

Questa sezione fornisce dettagli sulle seguenti opzioni di protezione dei dati con ACS:

- Un video che mostra il backup e il ripristino di un'applicazione ROSA in esecuzione in una regione e il ripristino in un'altra regione.
- Un video che mostra l'istantanea e il ripristino di un'applicazione ROSA.
- Dettagli dettagliati sull'installazione di un cluster ROSA, Amazon FSX per NetApp ONTAP, utilizzando NetApp Astra Trident per l'integrazione con il backend di storage, installazione di un'applicazione postgresql su un cluster ROSA, utilizzando ACS per creare una snapshot dell'applicazione e il ripristino dell'applicazione da esso.
- Un blog che mostra i dettagli passo per passo della creazione e del ripristino da uno snapshot per un'applicazione mysql su un cluster ROSA con FSX per ONTAP usando ACS.

Backup/Ripristino da backup

Il video seguente mostra il backup di un'applicazione ROSA in esecuzione in una regione e il ripristino in un'altra regione.

FSX NetApp ONTAP per il servizio Red Hat OpenShift su AWS

Snapshot/Ripristina da snapshot

Il video seguente mostra come scattare un'istantanea di un'applicazione ROSA e come eseguire il ripristino dall'istantanea dopo.

Snapshot/ripristino per le applicazioni su Red Hat OpenShift Service su cluster AWS (ROSA) con Amazon FSX per lo storage NetApp ONTAP

Blog in inglese

- "Utilizzo di Astra Control Service per la gestione dei dati delle app su cluster ROSA con storage Amazon FSX"

Dettagli dettagliati per creare snapshot e ripristinarle

Impostazione dei prerequisiti

- "Account AWS"
- "Account Red Hat OpenShift"
- Utente IAM con "autorizzazioni appropriate" Per creare e accedere al cluster ROSA
- "CLI AWS"
- "ROSA CLI"
- "CLI OpenShift"(oc)
- VPC con subnet e gateway e percorsi appropriati
- "ROSA Cluster installato" Nel VPC
- "Amazon FSX per NetApp ONTAP" Creato nello stesso VPC
- Accesso al gruppo ROSA da "Console di cloud ibrido OpenShift"

Passi successivi

1. Creare un utente amministratore e accedere al cluster.

2. Creare un file kubeconfig per il cluster.
3. Installare Astra Trident nel cluster.
4. Creare una configurazione backend, di classe storage e di classe Snapshot utilizzando il provisioner Trident CSI.
5. Implementare un'applicazione postgresql nel cluster.
6. Creare un database e aggiungere un record.
7. Aggiungere il cluster in ACS.
8. Definire l'applicazione in ACS.
9. Creare uno snapshot utilizzando ACS.
10. Eliminare il database nell'applicazione postgresql.
11. Ripristino da uno snapshot utilizzando ACS.
12. Verifica che l'app sia stata ripristinata dall'istantanea.

1. Creare un utente amministratore e accedere al cluster

Accedere al cluster ROSA creando un utente amministratore con il seguente comando: (È necessario creare un utente amministratore solo se non è stato creato uno al momento dell'installazione)

```
rosa create admin --cluster=<cluster-name>
```

Il comando fornirà un output simile a quello riportato di seguito. Accedere al cluster utilizzando `oc login` comando fornito nell'output.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

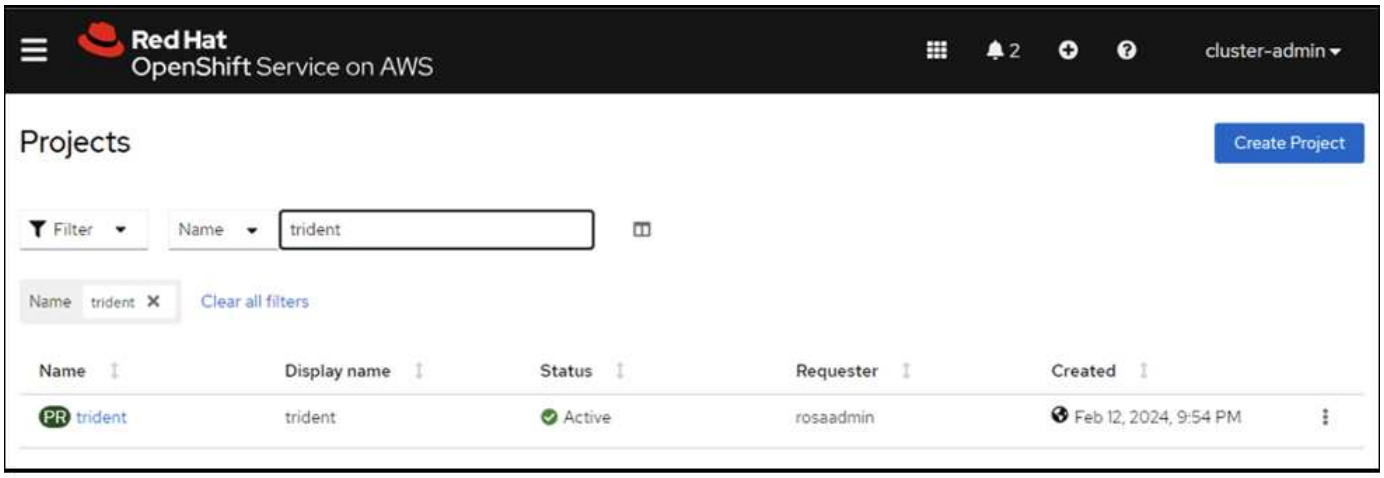
> È inoltre possibile accedere al cluster utilizzando un token. Se hai già creato un utente admin al momento della creazione del cluster, puoi accedere al cluster dalla console Red Hat OpenShift Hybrid Cloud con le credenziali admin-user. Quindi, facendo clic sull'angolo in alto a destra in cui viene visualizzato il nome dell'utente connesso, è possibile ottenere `oc login` comando (accesso token) per la riga di comando.

2. Creare un file kubeconfig per il cluster

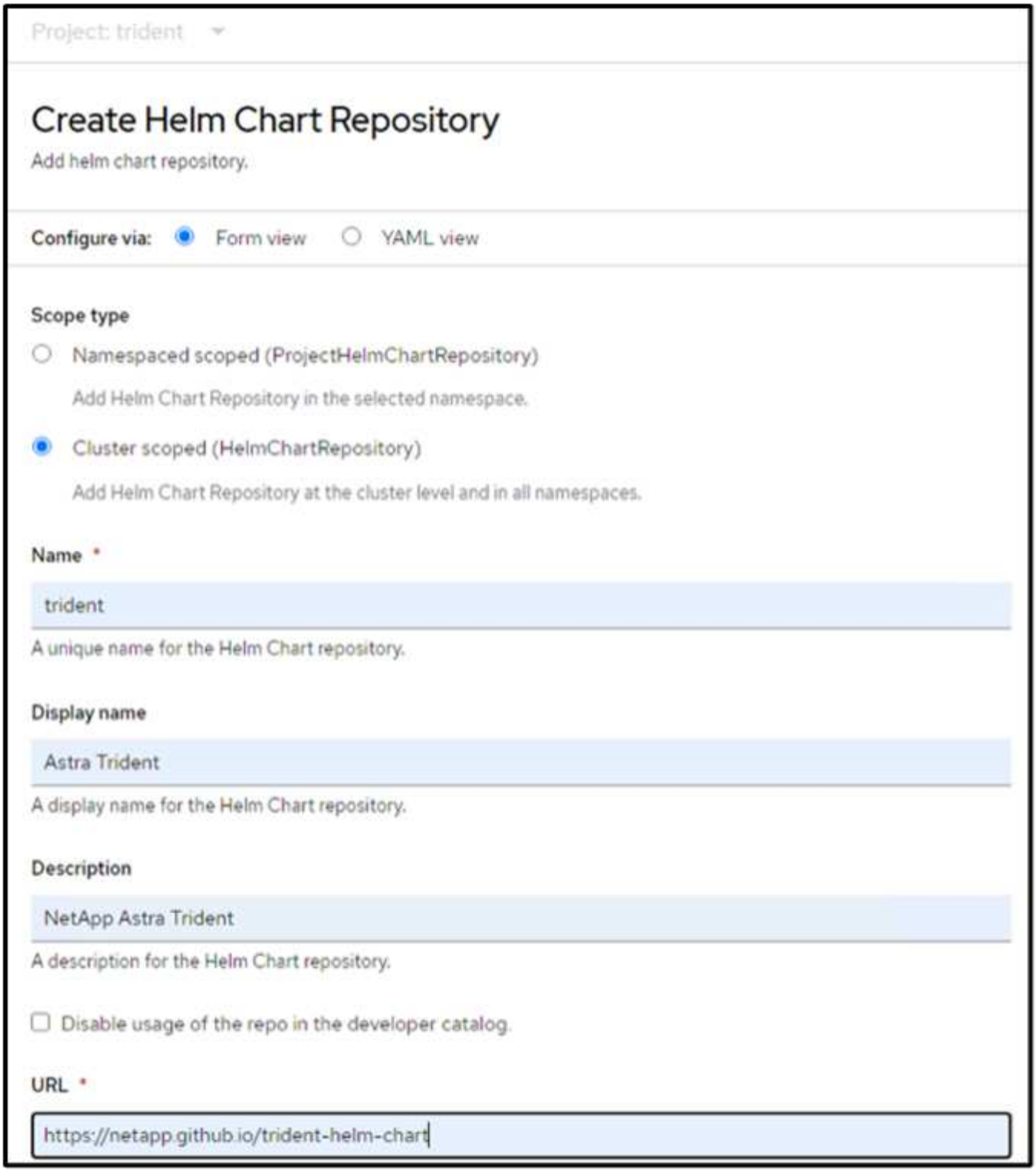
Seguire le procedure "qui" Per creare un file kubeconfig per il cluster ROSA. Questo file kubeconfig verrà utilizzato in seguito quando si aggiunge il cluster in ACS.

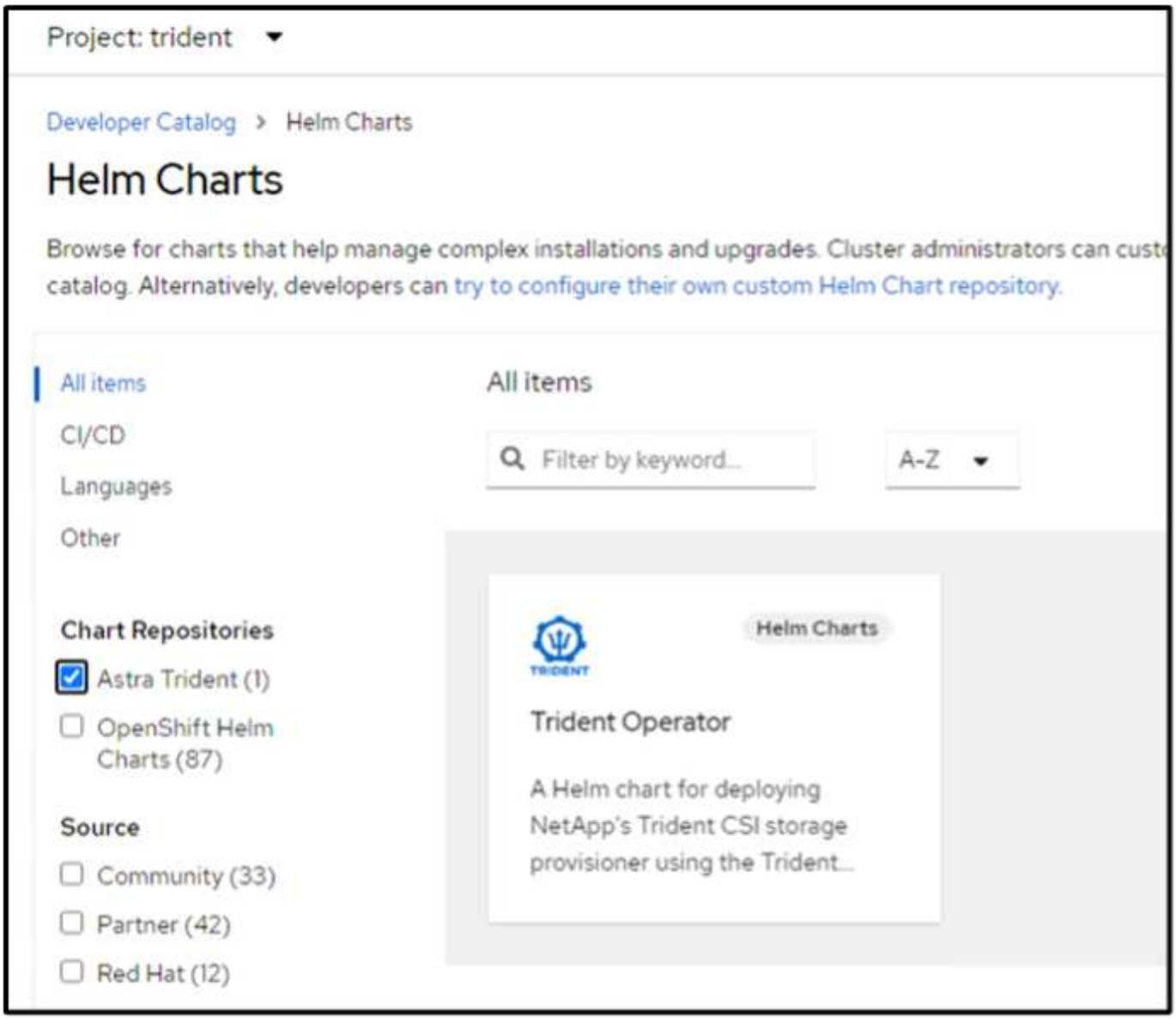
3. Installare Astra Trident sul cluster

Installare Astra Trident (versione più recente) sul cluster ROSA. A tale scopo, è possibile seguire una qualsiasi delle procedure indicate "qui". Per installare Trident utilizzando helm dalla console del cluster, creare prima un progetto chiamato Trident.

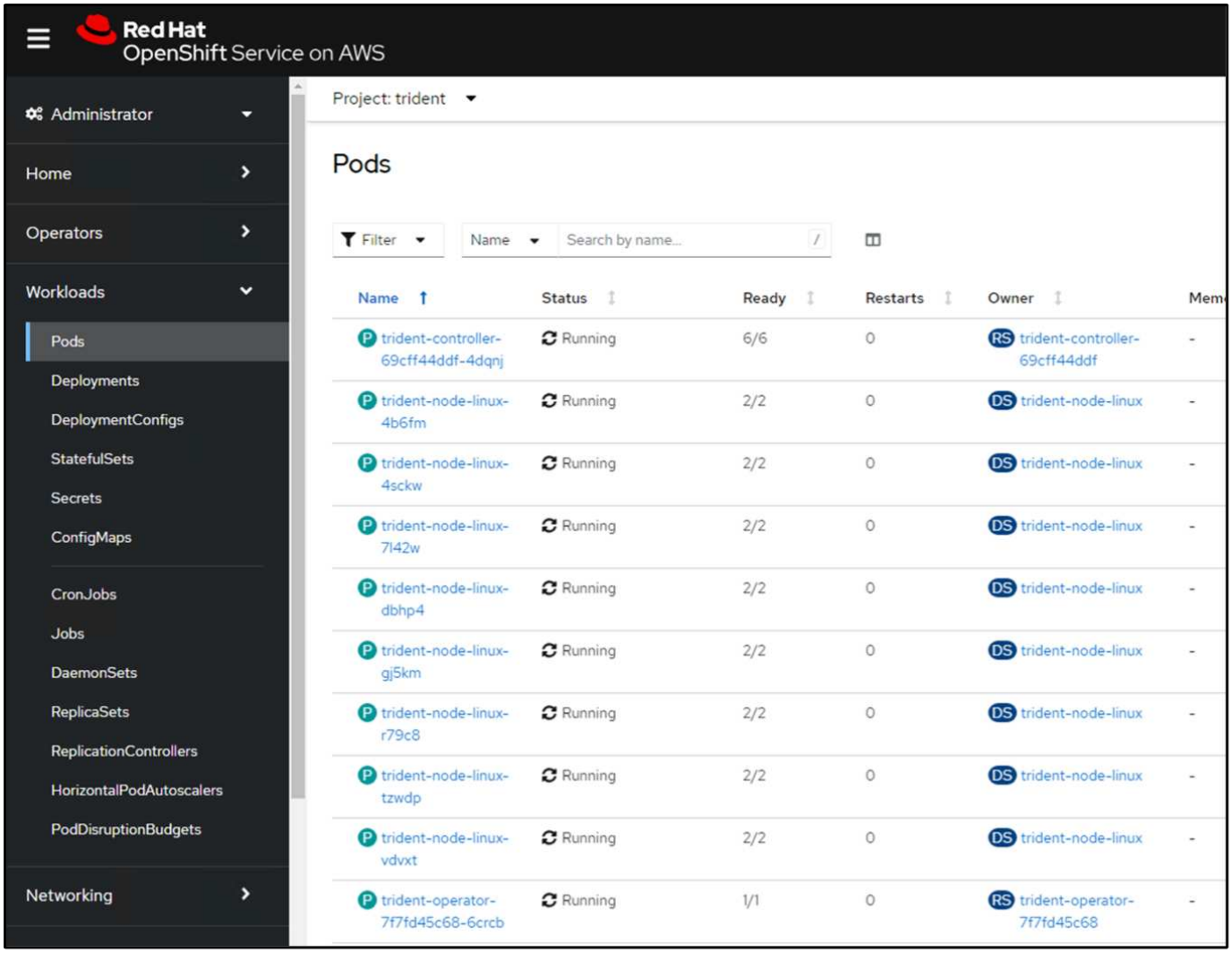


Quindi, dalla vista sviluppatore, creare un archivio grafico Helm. Per il campo URL utilizzare `'https://netapp.github.io/trident-helm-chart'`. Quindi, creare una release helm per l'operatore Trident.


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



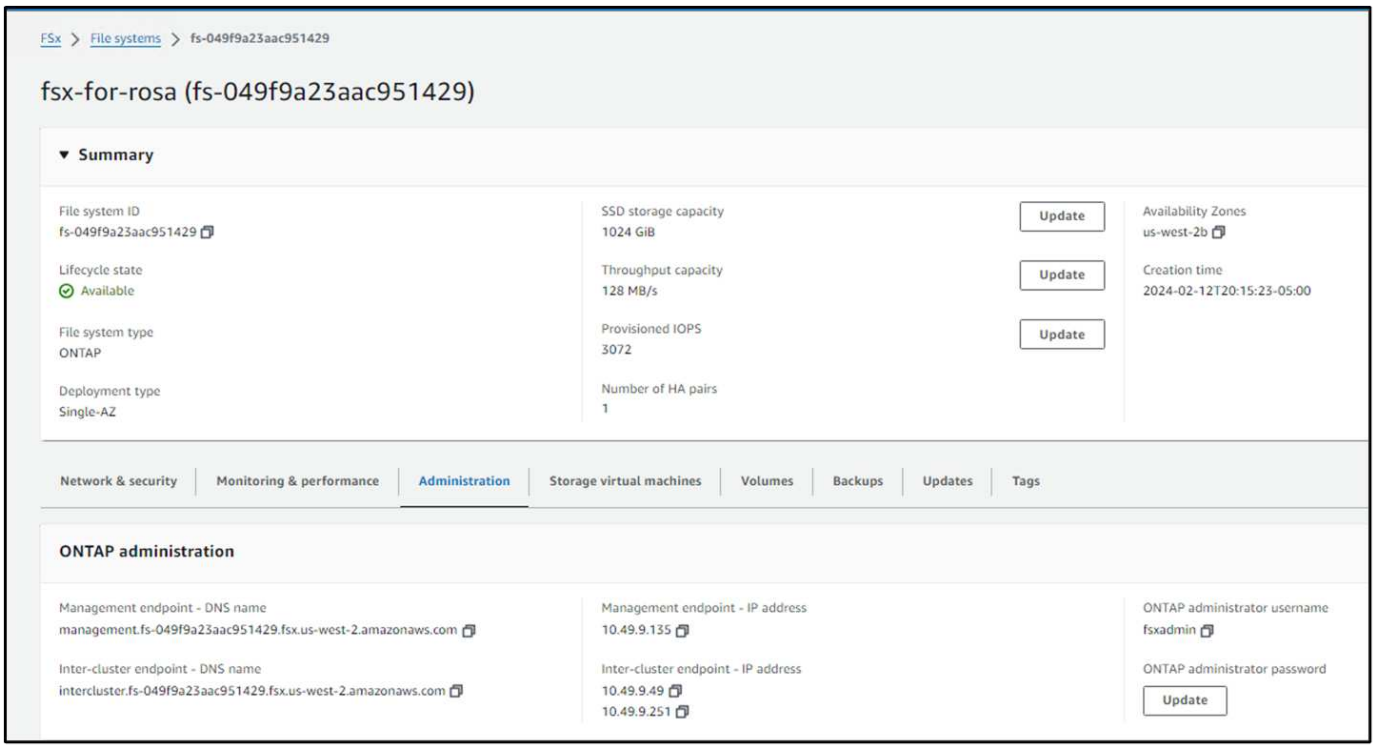
Verificare che tutti i pod di trident siano in esecuzione tornando alla vista Amministratore sulla console e selezionando i pod nel progetto trident.



4. Creare una configurazione backend, di classe storage e di classe snapshot utilizzando il provisioner Trident CSI

Utilizzare i file yaml illustrati di seguito per creare un oggetto backend tridente, un oggetto di classe di archiviazione e l'oggetto Volumesnapshot. Assicurati di fornire le credenziali al file system Amazon FSX per NetApp ONTAP che hai creato, la LIF di gestione e il nome del vserver del tuo file system nella configurazione yaml per il back-end. Per visualizzare questi dettagli, vai alla console AWS per Amazon FSX e seleziona il file system, quindi accedi alla scheda Administration (Amministrazione). Inoltre, fare clic su Update (Aggiorna) per impostare la password di `fsxadmin` utente.

È possibile utilizzare la riga di comando per creare gli oggetti o con i file yaml dalla console del cloud ibrido.



Configurazione del backend Trident

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

Classe di stoccaggio

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

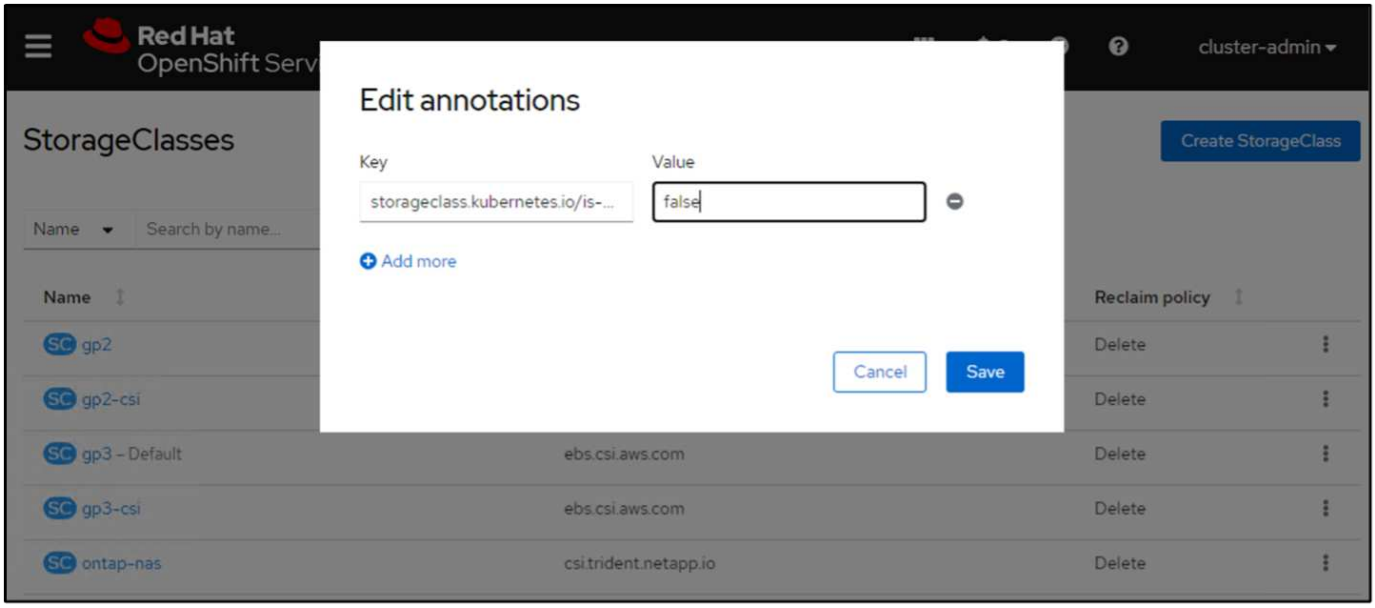
classe istantanea

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Verificare che gli oggetti backend, di storage e trident-snapshotclass siano creati inviando i comandi indicati di seguito.

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

In questo momento, un'importante modifica da apportare è impostare ontap-nas come classe di storage predefinita invece di GP3, in modo che l'app postgresql implementata in seguito possa utilizzare la classe di storage predefinita. Nella console OpenShift del cluster, in Storage selezionare StorageClasses. Modificare l'annotazione della classe predefinita corrente in modo che sia false e aggiungere l'impostazione della classe annotation storageclass.kuPensioni.io/is-default-class su true per la classe storage ontap-nas.



5. Distribuire un'applicazione postgresql sul cluster

È possibile distribuire l'applicazione dalla riga di comando nel modo seguente:

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

Se i pod delle applicazioni non sono in esecuzione, potrebbe essersi verificato un errore dovuto ai vincoli del contesto di protezione.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                    TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/postgresql      ClusterIP   172.30.245.50   <none>        5432/TCP   12m
service/postgresql-hl   ClusterIP   None            <none>        5432/TCP   12m

NAME                              READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer   persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate       statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate           statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

Correggere l'errore modificando `runAsUser` e. `fsGroup` campi in `statefuleset.apps/postgresql` oggetto con l'uid che si trova nell'output di `oc get project` comando come illustrato di seguito.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

L'app postgresql deve essere in esecuzione e utilizzare volumi persistenti supportati da Amazon FSX per lo storage NetApp ONTAP.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

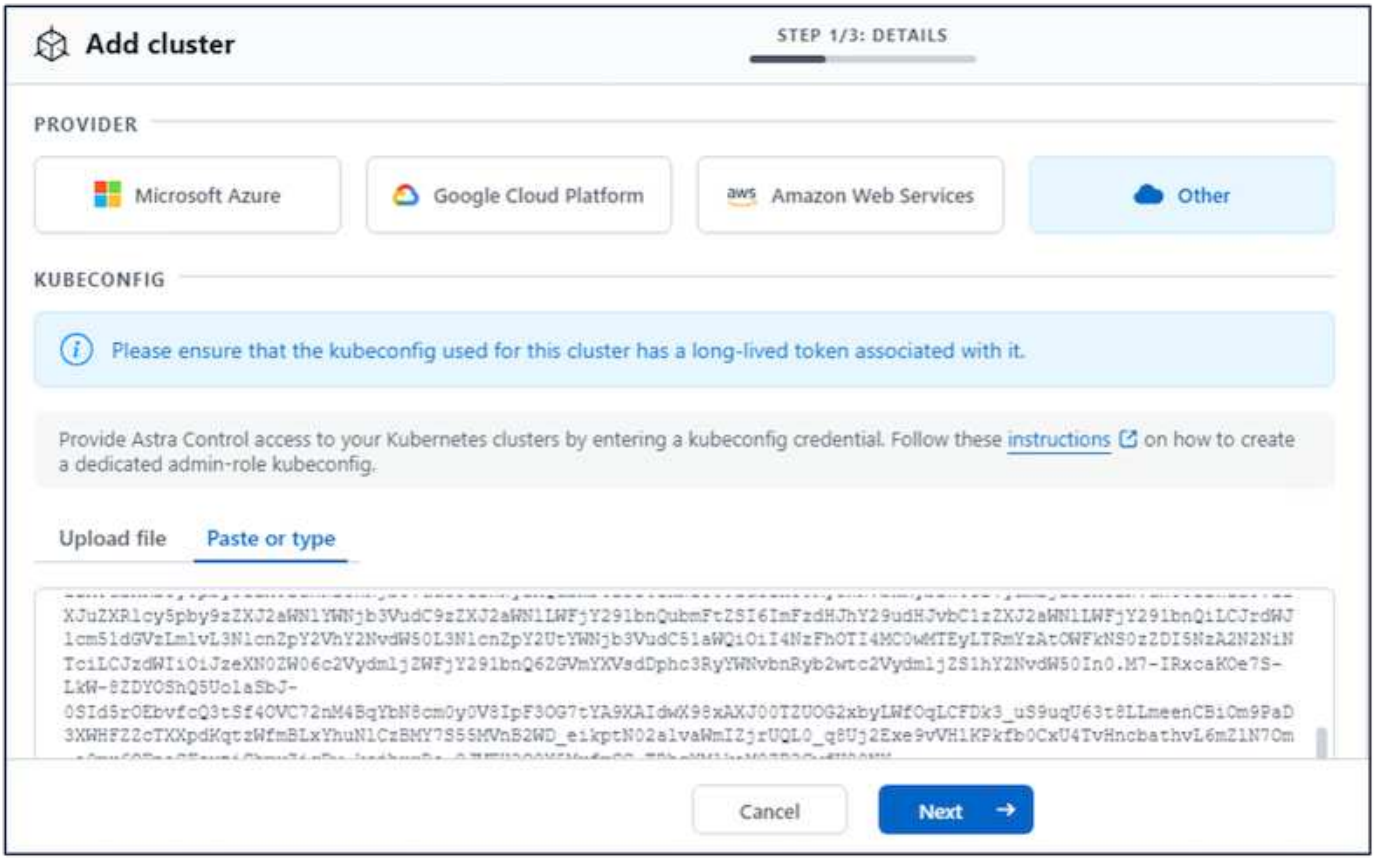
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6. Creare un database e aggiungere un record

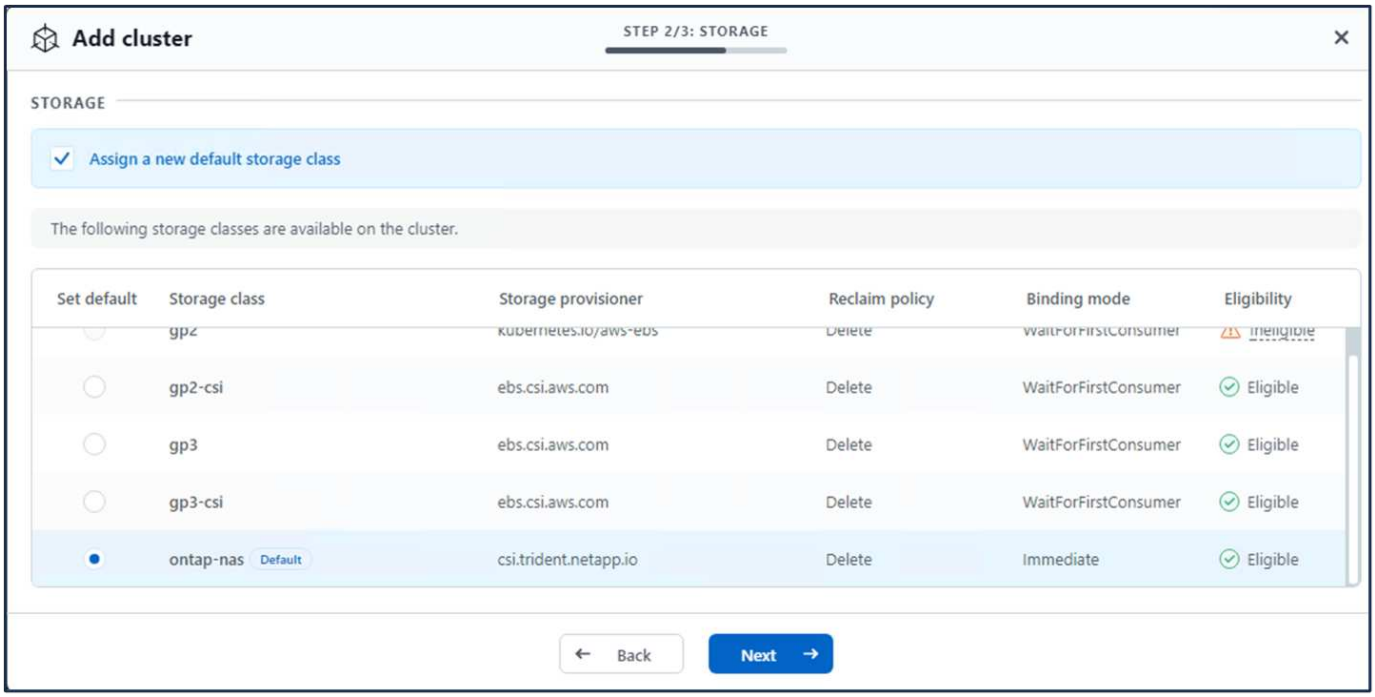
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
         List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7. Aggiungere il cluster in ACS

Accedere a ACS. Selezionare cluster e fare clic su Add. Selezionare Altro e caricare o incollare il file kubeconfig.



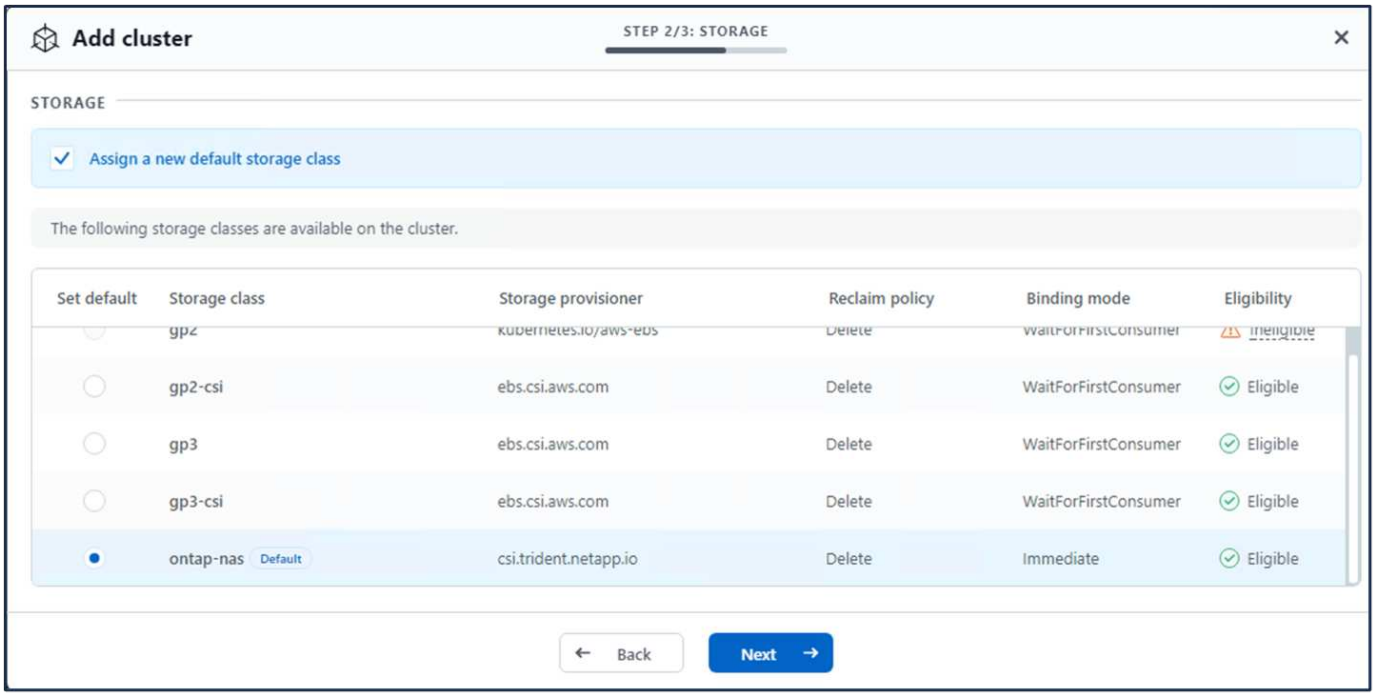
Fare clic su **Avanti** e selezionare ontap-nas come classe di storage predefinita per ACS. Fare clic su **Avanti**, rivedere i dettagli e **Aggiungi** il cluster.



8. Definire l'applicazione in ACS

Definire l'applicazione postgresql in ACS. Dalla pagina di destinazione, selezionare **applicazioni**, **Definisci** e inserire i dettagli appropriati. Fare clic su **Avanti** un paio di volte, rivedere i dettagli e fare clic su **Definisci**.

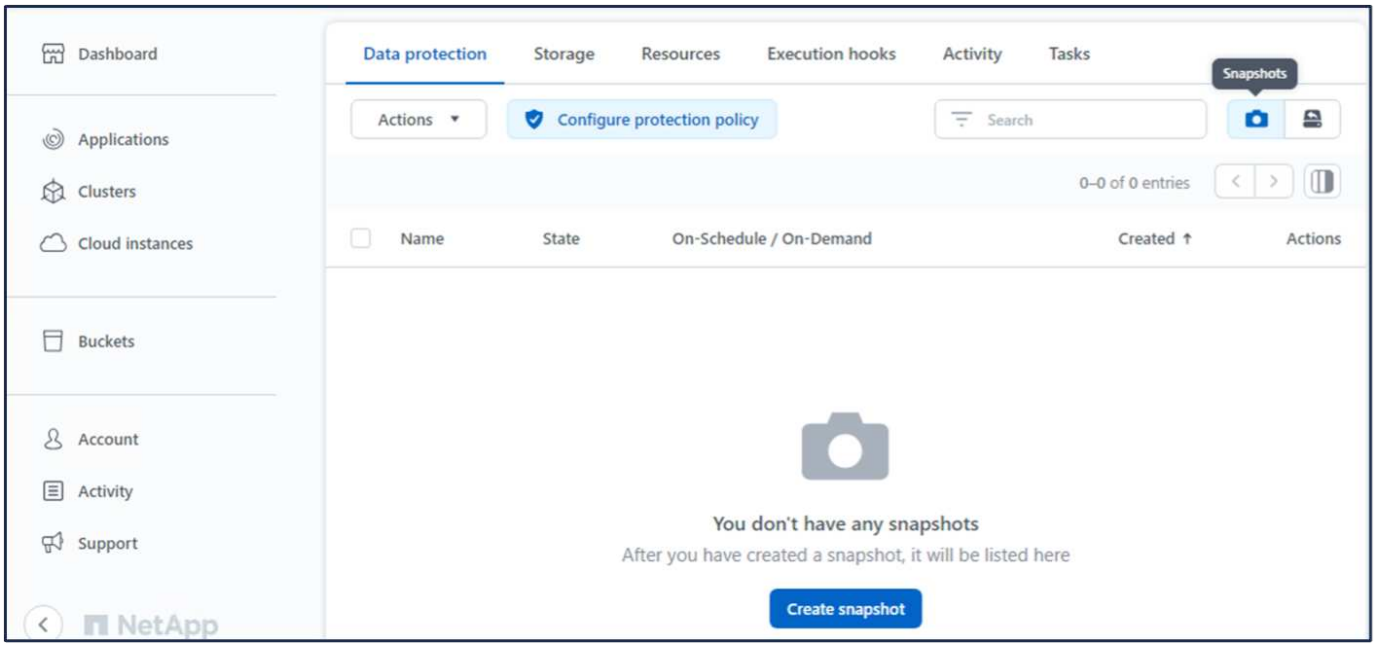
L'applicazione viene aggiunta a ACS.

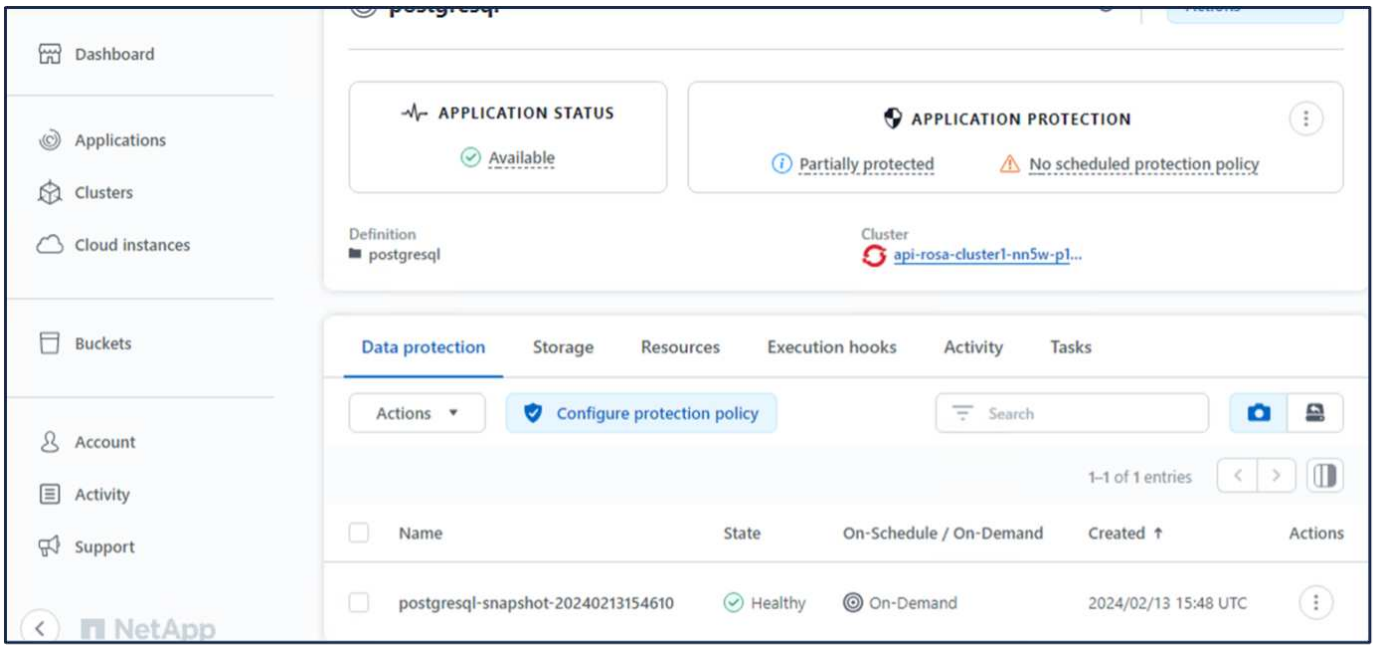


9. Creare un'istantanea utilizzando ACS

Esistono molti modi per creare uno snapshot in ACS. È possibile selezionare l'applicazione e creare un'istantanea dalla pagina che mostra i dettagli dell'applicazione. È possibile fare clic su Create Snapshot (Crea snapshot) per creare uno snapshot on-demand o configurare una policy di protezione.

Per creare un'istantanea su richiesta, è sufficiente fare clic su **Crea istantanea**, fornire un nome, rivedere i dettagli e fare clic su **istantanea**. Lo stato dell'istantanea diventa sano al termine dell'operazione.





10. Eliminare il database nell'applicazione postgresql

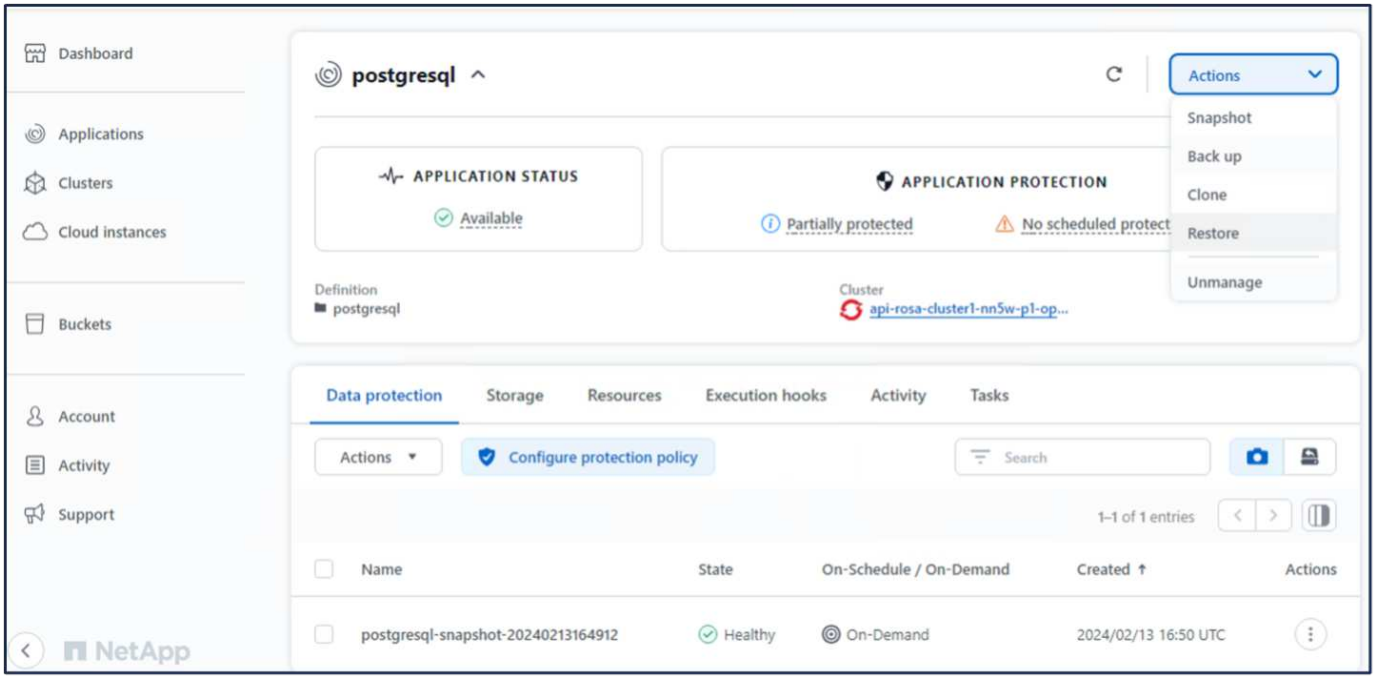
Accedere nuovamente a postgresql, elencare i database disponibili, eliminare quello creato in precedenza ed elencare nuovamente per assicurarsi che il database sia stato eliminato.

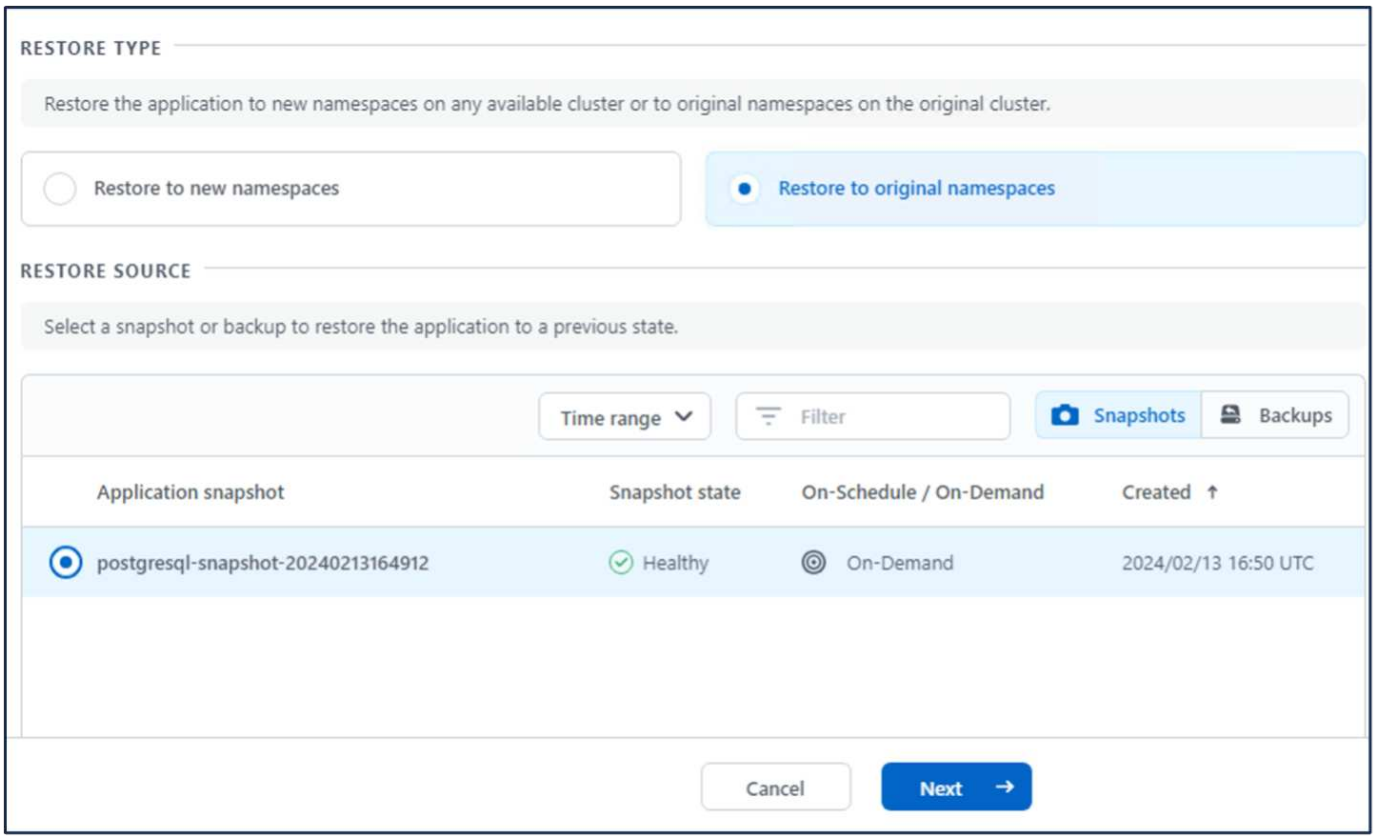
```
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-------------
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

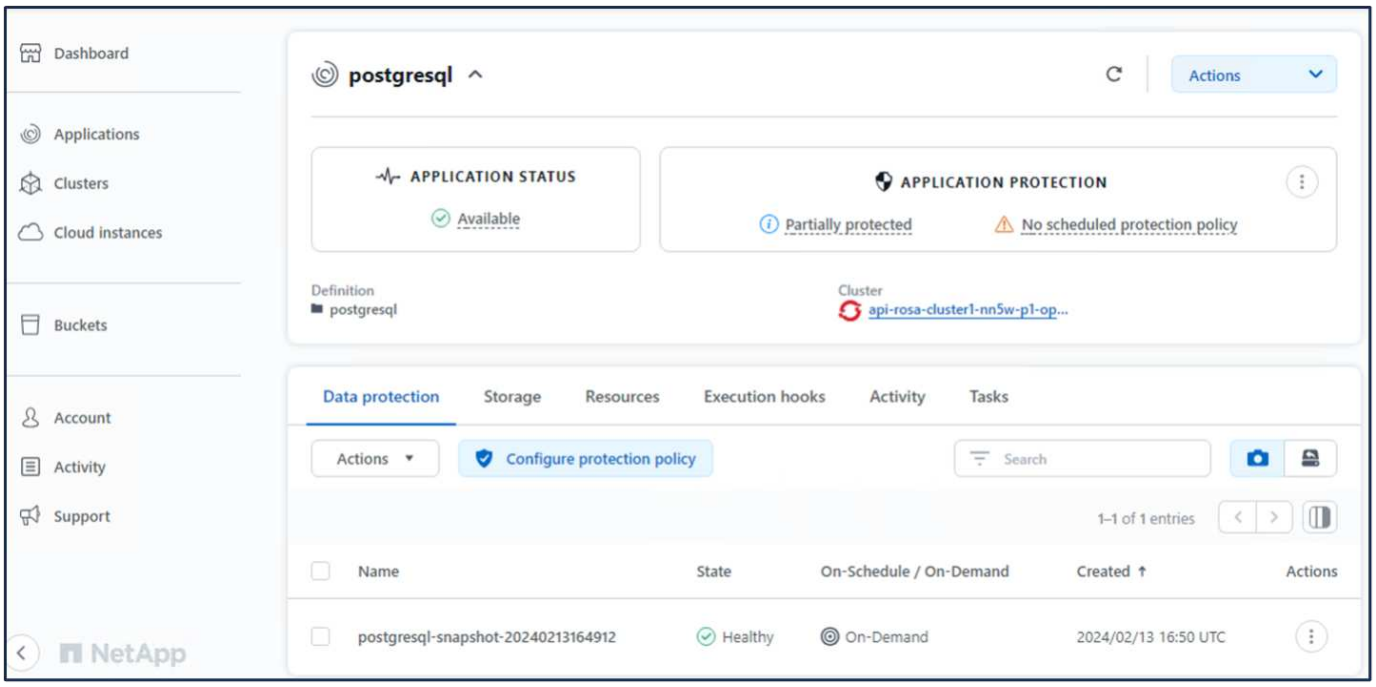
11. Ripristino da uno snapshot utilizzando ACS

Per ripristinare l'applicazione da uno snapshot, andare alla pagina di destinazione dell'interfaccia utente ACS,

selezionare l'applicazione e selezionare Ripristina. È necessario scegliere uno snapshot o un backup da cui eseguire il ripristino. (In genere, si creerebbero più criteri in base a un criterio configurato). Effettuare le scelte appropriate nelle due schermate successive, quindi fare clic su **Ripristina**. Lo stato dell'applicazione passa da Ripristino a disponibile dopo il ripristino dallo snapshot.







12. Verifica che l'app sia stata ripristinata dall'istantanea

Accedere al client postgresql e si dovrebbe ora vedere la tabella e il record nella tabella che si aveva in precedenza. Tutto qui. Basta fare clic su un pulsante per ripristinare lo stato precedente dell'applicazione. Con Astra Control, possiamo renderla semplice per i nostri clienti.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
        List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```


Migrazione dei dati

Questa pagina mostra le opzioni di migrazione dei dati per i carichi di lavoro container sui cluster gestiti Red Hat OpenShift che utilizzano FSX per NetApp ONTAP per lo storage persistente.

Migrazione dei dati

Il servizio Red Hat OpenShift su AWS e FSX per NetApp ONTAP (FSxN) fanno parte del loro portfolio di servizi di AWS. FSxN è disponibile nelle opzioni AZ singolo o AZ multiplo. L'opzione Multi-Az offre la protezione dei dati dai guasti della zona di disponibilità. FSxN può essere integrato con Astra Trident per fornire storage persistente per le applicazioni sui cluster ROSA.

Integrazione di FSxN con Trident utilizzando Helm Chart

Integrazione cluster ROSA con Amazon FSX per ONTAP

La migrazione delle applicazioni container comporta:

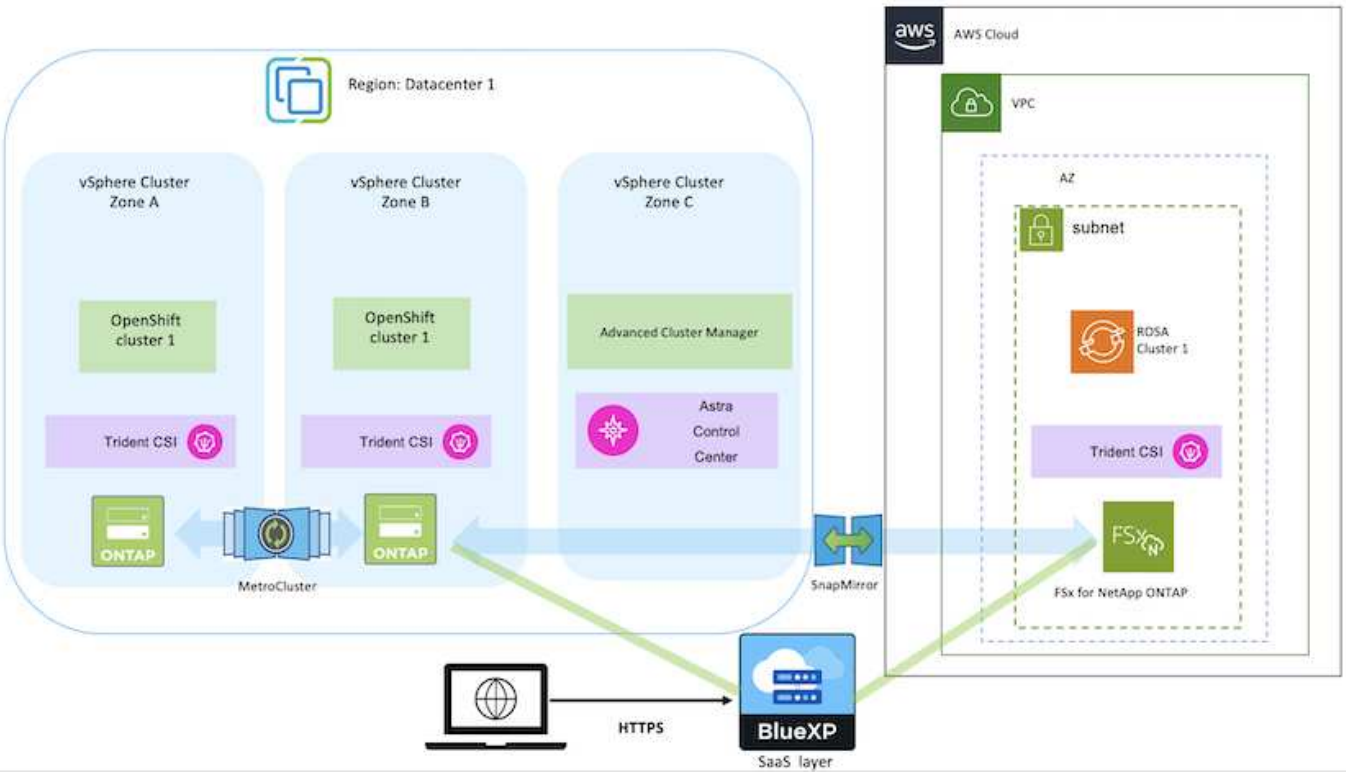
- Volumi persistenti: Questa operazione può essere eseguita utilizzando BlueXP. Un'altra opzione consiste nell'utilizzare Astra Control Center per gestire le migrazioni delle applicazioni container dall'ambiente on-premise a quello cloud. L'automazione può essere utilizzata per lo stesso scopo.
- Metadati dell'applicazione: È possibile eseguire questa operazione utilizzando OpenShift GitOps (Argo CD).

Failover e fail-back delle applicazioni sul cluster ROSA utilizzando FSxN per lo storage persistente

Il seguente video è una dimostrazione degli scenari di failover e fail-back delle applicazioni che utilizzano BlueXP e il CD Argo.

Failover e failback delle applicazioni sul cluster ROSA

Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift



Informazioni sul copyright

Informazioni sul marchio commerciale